(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5084372号
(P5084372)
(45)発行日　平成24年11月28日(2012.11.28)　(24)登録日　平成24年9月14日(2012.9.14)

(51)Int.Cl.　　F I
G06F 1/32 (2006.01)　　G06F 1/00 332B
G06F 3/12 (2006.01)　　G06F 3/12 K

請求項の数 7　(全 24 頁)

(21)出願番号　特願2007-175327(P2007-175327)
(22)出願日　平成19年7月3日(2007.7.3)
(65)公開番号　特開2009-15507(P2009-15507A)
(43)公開日　平成21年1月22日(2009.1.22)
審査請求日　平成22年7月2日(2010.7.2)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100145827
弁理士　水垣　親房
(72)発明者　新倉　康史
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　三浦　みちる

最終頁に続く

(54)【発明の名称】データ処理装置およびデータ処理装置の制御方法

(57)【特許請求の範囲】
【請求項１】
データ処理装置であって、
データを受信する受信手段と、
前記受信手段により受信されたデータに対して所定の変換処理を実行する変換装置と、
前記受信手段により受信されたデータに対して前記所定の変換処理を実行可能な制御手段と、
前記変換装置に電力を供給する電力供給手段とを有し、
前記制御手段は、前記変換装置に電力が供給されている状態であるか否かを判断し、前記変換装置に電力が供給されている状態であると判断した場合は前記受信手段により受信されたデータに対して前記所定の変換処理を前記変換装置に実行させ、
前記制御手段は、前記変換装置に電力が供給されていない状態であると判断した場合は前記受信手段により受信されたデータに対して前記所定の変換処理を実行し、
前記所定の変換処理は、所定の通信プロトコルに従ったデータを変換する変換処理であることを特徴とするデータ処理装置。
【請求項２】
前記制御手段は、前記変換装置に電力が供給されている状態であると判断した場合は前記所定の変換処理を前記変換装置に実行させるとともに前記所定の変換処理とは異なる他の処理を実行するよう制御することを特徴とする請求項１に記載のデータ処理装置。
【請求項３】

前記制御手段は、前記所定の変換処理をソフトウェアにより実行することを特徴とする請求項１又は２に記載のデータ処理装置。
【請求項４】
前記制御手段は、前記受信手段がデータを受信したときに前記変換装置に電力が供給されていない状態であると判断した場合であっても、前記受信手段が受信したデータに含まれる宛先ポート番号が予め設定されたポート番号と一致する場合には、前記変換装置に電力を供給させ、前記所定の変換処理を前記変換装置に実行させることを特徴とする請求項３に記載のデータ処理装置。
【請求項５】
前記受信手段は、前記データを含むパケットを受信し、
前記制御手段は、前記受信手段により受信されたパケットに含まれるヘッダに基づいて前記データが前記所定の通信プロトコルに従ったデータであるか否かを判定することを特徴とする請求項４に記載のデータ処理装置。
【請求項６】
前記所定の通信プロトコルは、ＩＰＳｅｃプロトコル又はＳＳＬプロトコルのいずれかであることを特徴とする請求項４又は５に記載のデータ処理装置。
【請求項７】
データを受信する受信手段と、前記受信手段により受信されたデータに対して所定の変換処理を実行する変換装置と、前記受信手段により受信されたデータに対して前記所定の変換処理を実行可能な制御手段と、前記変換装置に電力を供給する電力供給手段とを有するデータ処理装置の制御方法であって、
前記制御手段が、前記変換装置に電力が供給されている状態であるか否かを判断し、前記変換装置に電力が供給されている状態であると判断した場合は前記所定の変換処理を前記変換装置に実行させ、
前記制御手段が、前記変換装置に電力が供給されていない状態であると判断した場合は前記所定の変換処理を実行するステップを有し、
前記所定の変換処理は、所定の通信プロトコルに従ったデータを変換する変換処理であることを特徴とするデータ処理装置の制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データ処理装置およびデータ処理装置の制御方法に関する。
【背景技術】
【０００２】
従来、データ処理をソフトウェアで行うとＣＰＵに高負荷を与えるため、データ処理するためのハードウェアアクセラレータをデータ処理装置に搭載する事が一般的である。
【０００３】
特許文献１には、ハードウェアによりプロトコル処理を行う処理部と、ソフトウェアによりプロトコル処理を行う処理部とを有する装置が開示されている。
【特許文献１】特開２００２－３５４０６４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
ところで、データ処理装置が実行するデータ処理の一例として、ＩＰＳｅｃ（Internet Protocol Security Protocol）処理が知られている。ＩＰＳｅｃとは、ＯＳＩ参照モデル（OpenSystem Interconnection reference model）の第３層であるネットワーク層において認証処理及び暗号化処理を行うためのプロトコルのことをいう。
【０００５】
そして、ＩＰＳｅｃを処理するためのハードウェアアクセラレータを搭載する事で、ＣＰＵへの負荷は下がるが、どの様な状況でも電源を入れておく必要があり、システム全体

の平均消費電力を押し上げることとなる。

【０００６】

本発明は、上記の問題点を解決するためになされたものである。本発明の目的は、同種の処理実行可能な複数の処理手段への電力供給を適切に制御して、データ処理速度を維持しつつデータ処理装置の省電力化を図ることである。

【課題を解決するための手段】

【０００７】

本発明は、データ処理装置であって、データを受信する受信手段と、前記受信手段により受信されたデータに対して所定の変換処理を実行する変換装置と、前記受信手段により受信されたデータに対して前記所定の変換処理を実行可能な制御手段と、前記変換装置に電力を供給する電力供給手段とを有し、前記制御手段は、前記変換装置に電力が供給されている状態であるか否かを判断し、前記変換装置に電力が供給されている状態であると判断した場合は前記受信手段により受信されたデータに対して前記所定の変換処理を前記変換装置に実行させ、前記制御手段は、前記変換装置に電力が供給されていない状態であると判断した場合は前記受信手段により受信されたデータに対して前記所定の変換処理を実行し、前記所定の変換処理は、所定の通信プロトコルに従ったデータを変換する変換処理であることを特徴とする。

【発明の効果】

【０００８】

本発明によれば、同種の処理実行可能な複数の処理手段への電力供給を適切に制御して、データ処理速度を維持しつつデータ処理装置の省電力化を図ることができる。

【発明を実施するための最良の形態】

【０００９】

〔第１実施形態〕

以下、本発明の一実施形態ついて図面を参照しながら説明する。

【００１０】

図１は、本発明の第１実施形態を示すデータ処理装置の構成を示したブロック図である。

【００１１】

図１において、１００は、本発明の一実施形態を示すデータ処理装置である。

【００１２】

データ処理装置１００において、１０１はＣＰＵ（Central Processing Unit）であり、ＲＯＭ１０２等に格納されたプログラムを実行して装置全体の動作を制御する。

【００１３】

ＲＯＭ（Read Only Memory）１０２は、後述する図３の３０３，３０５，３０６，３０７に示す機能や、プリンタ１０４や、ディスプレイ１０６を動作させるためのプログラムがプリセットされている。

【００１４】

１０３はＲＡＭ（Randam Access Memory）であり、データ処理装置１００内で行われるデータのやり取りや、プログラムのワークエリアとして機能する。

【００１５】

プリンタ１０４は、ＬＡＮ Ｉ／Ｆ１０７から受け取ったデータや、ユーザがキーボード１０５から入力したデータを印刷する機能を持っている。

【００１６】

キーボード１０５は、データ処理装置１００における各種設定の入力や、後述する図３に示すフローチャートで指定されるポート番号や優先内容選択の為に使用される入力機器である。

【００１７】

ディスプレイ１０６は、キーボード１０５で入力された情報や、各種設定値、システムの状態を表示する表示機器である。

【００１８】
ＬＡＮ Ｉ／Ｆ１０７は、ネットワーク１０９からのデータを受信し、後述するＰＨＹ処理，ＭＡＣ処理等を行い、必要に応じてネットワーク１０９へデータを送信するインタフェースである。
【００１９】
１１０はＩＰＳｅｃアクセラレータであり（詳細は図４）、後述するＩＰＳｅｃハードウェア処理部３０４を備え、ＩＰＳｅｃ処理を実行する。
【００２０】
バス１０８は、ＣＰＵ１０１、ＲＯＭ１０２、ＲＡＭ１０３、プリンタ１０４、キーボード１０５、ディスプレイ１０６、ＬＡＮ Ｉ／Ｆ１０７、ＩＰＳｅｃアクセラレータ１１０のそれぞれを接続し、データの送受信を行う機能である。なお、図示しないが、ハードディスク等の外部記憶装置を備え、この外部記憶装置に格納されるプログラムをＲＡＭ１０３にロードしてＣＰＵ１０１が実行することにより、データ処理装置１００を制御するように構成してもよい。
【００２１】
なお、データ処理装置１００をネットワークプリンタとした場合、キーボード１０５，ディスプレイ１０６はネットワークプリンタの操作部を構成する。
【００２２】
なお、図１では、データ処理装置１００の一例としてネットワークプリンタ等を想定しているが、本発明を適用可能なデータ処理装置１００は、ネットワークプリンタに限られるものではない。ＩＰＳｅｃ通信可能な機器であれば、パーソナルコンピュータでも、その他のネットワーク機器でも、本発明を適用可能なデータ処理装置１００として用いることが可能である。
【００２３】
図２は、ＯＳＩ参照モデルと一般的なＴＣＰ/ＩＰプロトコルによる階層構造を示した図である。
【００２４】
図２において、２０１～２０４はＴＣＰ／ＩＰプロトコルの階層構造を示す。
【００２５】
ネットワークインタフェース層２０１は、ＯＳＩ参照モデルの第１層（物理層）と第２層（データリンク層）を合わせた層である。このネットワークインタフェース層２０１は、後述する図３に示すＥｔｈｅｒｎｅｔ（登録商標）のＰＨＹ処理部３０１とＭＡＣ処理部３０２に対応する。
【００２６】
インターネット層２０２は、ＯＳＩ参照モデルの第３層（ネットワーク層）であり、図３に示すＩＰ処理部３０３とＩＰＳｅｃハードウェア処理部３０４とＩＰＳｅｃソフトウェア処理部３０５に対応する。
【００２７】
トランスポート層２０３は、ＯＳＩ参照モデルの第４層（トランスポート層）であり、図３に示すＴＣＰ／ＵＤＰ処理部３０６に対応たる。
【００２８】
アプリケーション層は、ＯＳＩ参照モデルの第５層（セッション層）と第６層（プレゼンテーション層）と第７層（アプリケーション層）を合わせた層であり、図３に示すアプリケーション処理部３０７に対応する。
【００２９】
図３は、データ処理装置１００で実行されるＬＡＮインタフェース処理の内容を示した図である。
【００３０】
図３において、３００はＬＡＮインタフェース処理部であり、３０１～３０７に示す各処理部により構成される。

【００３１】
ＰＨＹ処理部３０１は、ＬＡＮ１０９との物理的な接続を行い、受信した信号のデータ変換や、送信データの信号変換処理を行うハードウェアであり、ＬＡＮ Ｉ／Ｆ１０７内に設けられる。
【００３２】
ＭＡＣ処理部３０２は、ＰＨＹ処理部３０１で受信したデータを、自分宛のデータであるかＭＡＣアドレスを用いてフィルタ処理を行うハードウェアであり、ＬＡＮ Ｉ／Ｆ１０７内に設けられる。
【００３３】
ＩＰ処理部３０３は、本システムに一意にアドレス（ＩＰアドレス）を割り当てたり、割り当てられたＩＰアドレスを元に、指定された他の機器に送り届ける処理を行うソフトウェア処理部である。また、ＩＰ処理部３０３は、ＩＰＳｅｃ通信であるか否かを判断する機能も有する。
【００３４】
ＩＰＳｅｃハードウェア処理部３０４（第１処理部）は、暗号化されたパケットデータであるＥＳＰ（Encapsulating Security Payload）の伸張・圧縮を行うためのハードウェアである。なお、このＩＰＳｅｃハードウェア処理部３０４は、ＩＰＳｅｃアクセラレータ１１０内に設けられる。
【００３５】
ＩＰＳｅｃソフトウェア処理部３０５（第２処理部）は、ＩＰＳｅｃハードウェア処理部３０４と同様に、暗号化されたパケットデータであるＥＳＰの伸張・圧縮を行うためのソフトウェア処理部である。
【００３６】
なお、ＩＰＳｅｃソフトウェア処理部３０５と、ＩＰＳｅｃハードウェア処理部３０４は、同種の処理機能を持っている。ここでいいう同種の処理機能とは、ＩＰＳｅｃ処理機能をいう。
【００３７】
ＴＣＰ／ＵＤＰ処理部３０６は、ＲＦＣ７９３で定義されているＴＣＰプロトコルや、ＲＦＣ７６８で定義されているＵＤＰプロトコルを制御する機能を持っているソフトウェア処理部である。
【００３８】
アプリケーション処理部３０７は、ＴＣＰ／ＵＤＰ処理部３０６で送受信されたデータを利用して、ＳＭＴＰ・ＨＴＴＰなどの各種アプリケーションの処理を行うソフトウェア処理部である。
【００３９】
なお、上述のＩＰ処理部３０３，ＩＰＳｅｃソフトウェア処理部３０５，ＴＣＰ／ＵＤＰ処理部３０６，アプリケーション処理部３０７は、ＣＰＵ１０１がＲＯＭ１０２に格納されるプログラムを実行することにより実現される機能である。
【００４０】
図４は、図１に示したＩＰＳｅｃアクセラレータ１１０の概略構成の一例を示すブロック図である。
【００４１】
図４において、８８８はコネクタであり、データ処理装置１００のバス１０８と接続するためのものである。９９９は電源コントローラであり、データ処理装置１００の図示しない電源部から電力を得てＩＰＳｅｃアクセラレータ１１０内の各部へ電力を供給する。
【００４２】
なお、電源コントローラ９９９は、ＣＰＵ１０１からの指示により、ＩＰＳｅｃハードウェア処理部３０４への電力の供給／遮断を切り替えることができる。
【００４３】
以下、図５のフローチャートを参照して、本実施形態のＩＰＳｅｃハードウェア処理部

停止監視処理について説明する。

【００４４】

図５は、本発明における第１の制御処理手順の一例を示すフローチャートであり、ＩＰＳｅｃハードウェア処理部停止監視処理（第１制御処理）に対応する。なお、このフローチャートで示す機能は、ＣＰＵ１０１がＲＯＭ１０２に格納されたプログラムを実行することにより実現される。

【００４５】

まず、ＣＰＵ１０１は、データ処理装置１００の状態がＩＰＳｅｃハードウェア処理部３０４の停止条件（ハード停止条件）に一致しているか否かを監視する（Ｓ５０１）。

【００４６】

具体的には、ＣＰＵ１０１は「データを受信していない場合」又は「データを受信していてもＩＰＳｅｃ処理を行っていない（ＩＰＳｅｃ通信でない）場合」又は「ＩＰＳｅｃ通信でデータ受信しているがＩＰＳｅｃソフトウェア処理部３０５の処理で問題ない場合」のいずれかの条件に一致する場合、ＩＰＳｅｃハードウェア処理部３０４の停止条件に一致すると判断する。一方、上記いずれかの条件にも一致しない場合、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４の停止条件に一致しないと判断する。

【００４７】

なお、上記「・・・ＩＰＳｅｃソフトウェア処理部３０５の処理で問題ない」か否かは、受信データのプロトコルで判断するものとする。例えば、ＩＣＭＰ／ＡＲＰプロトコルなどのパケットは、数パケットでやり取りが完了するため、ＩＰＳｅｃソフトウェア処理部３０５の処理で問題ないと判断する。一方、ＬＰＲ／ｒａｗＴＣＰプロトコルなど、ＰＣからの受信プリントを行うプロトコルは、パケット量が多いため、ＩＰＳｅｃソフトウェア処理部３０５の処理では遅く、プリントの速度（ｐｐｍ）が低下してしまう。そのためＩＰＳｅｃソフトウェア処理部３０５の処理では問題が発生すると判断する。このような問題が発生するプロトコル（ＬＰＲ／ｒａｗＴＣＰ等）のポート番号を予めユーザ等にキーボードから入力させてＲＡＭ１０３内の不揮発性メモリ領域に格納（設定）しておくものとする。（又は、出荷前に工場等で予めＲＯＭ１０２内に格納しておくものとする。）

【００４８】

そしてＣＰＵ１０１は、受信データ（ＴＣＰ／ＵＤＰパケット）に含まれる宛先ポート番号が上記予め設定されたポート番号（ＬＰＲ／ｒａｗＴＣＰ等に対応するポート番号）と一致しない場合はＩＰＳｅｃソフトウェア処理部３０５の処理で問題ないと判断する。一方、ＣＰＵ１０１は、受信データに含まれる宛先ポート番号が上記予め設定されたポート番号と一致する場合にはＩＰＳｅｃソフトウェア処理部３０５の処理では問題あると判断する。

【００４９】

ＣＰＵ１０１は、データ処理装置１００の状態がハード停止条件に一致していないと判定した場合（Ｓ５０１でＮｏ）、そのままステップＳ５０１のハード停止条件の監視処理を継続する。

【００５０】

一方、データ処理装置１００の状態がハード停止条件に一致していると判定した場合（Ｓ５０１でＹｅｓ）、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア停止処理を実行する（Ｓ５０２）。具体的には、ＣＰＵ１０１は、ＩＰＳｅｃアクセラレータ１１０内の電源コントローラ９９９に対してＩＰＳｅｃハードウェア処理部３０４の電源を停止するよう指示する。この指示を受けた電源コントローラ９９９は、ＩＰＳｅｃハードウェア処理部３０４への電源供給を停止する。このように、ＩＰＳｅｃハードウェア処理部３０４の電源を落とすことで、消費電力を低下させることができる。

【００５１】

次に、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４が停止中（ＩＰＳｅｃハードウェア処理部３０４に電源が供給されていない）か否かを監視する（Ｓ５０３）。

【００５２】
そして、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４が停止中（ＩＰＳｅｃハードウェア処理部３０４に電源が供給されていない）と判定した場合（Ｓ５０３でＹｅｓ）、そのままステップＳ５０３の監視処理を継続する。
【００５３】
一方、ＩＰＳｅｃハードウェア処理部３０４が停止中でない（ＩＰＳｅｃハードウェア処理部３０４に電源が供給されている）と判定した場合（Ｓ５０３でＮｏ）、ＣＰＵ１０１は、再び、ハード停止条件の一致を監視する（Ｓ５０１）。
【００５４】
以下、図６のフローチャートを参照して、図３に示したＬＡＮインタフェース処理の動作について説明する。
【００５５】
図６は、本発明における第２の制御処理手順の一例を示すフローチャートであり、図３に示したＬＡＮインタフェース処理の動作に対応する。なお、このフローチャートのＳ４０１～Ｓ４０５，Ｓ４０７～Ｓ４１１は、ＣＰＵ１０１がＲＯＭ１０２に格納されたプログラムを実行することにより実現される各処理部（３０３～３０６）により実行される。また、Ｓ４０６はＩＰＳｅｃハードウェア処理部３０４により実行される。
【００５６】
まず、ＩＰ処理部３０３（ＣＰＵ１０１）は、ネットワーク１０９から１パケットデータ（ＩＰパケット）を受信するまでデータ受信の監視処理を継続する（Ｓ４０１）。
【００５７】
そして、ネットワーク１０９より１パケットデータ受信したと判定した場合には、ＩＰ処理部３０３は、ＩＰヘッダ解析を実行する（Ｓ４０２）。具体的には、ＩＰ処理部３０３は、受信データ（ＩＰパケット）のＩＰヘッダにある「送信元ＩＰアドレス」，「宛先ＩＰアドレス」を抽出し、自装置宛のデータである事を確認する。さらに、ＩＰ処理部３０３は、ＩＰヘッダにある「ＩＰプロトコル番号」の抽出も行う。
【００５８】
次に、ＩＰ処理部３０３は、受信データにＩＰＳｅｃの処理が必要か否かを判断する（Ｓ４０３）。具体的には、ＩＰ処理部３０３は、ステップＳ４０２で取得した「ＩＰプロトコル番号」がＩＰＳｅｃのデータであるＥＳＰの番号（５０）である場合にＩＰＳｅｃの処理が必要と判断する。一方、ＩＰ処理部３０３は、ステップＳ４０２で取得した「ＩＰプロトコル番号」がＥＳＰの番号（５０）でない場合にＩＰＳｅｃの処理が必要でないと判断する。
【００５９】
ＩＰＳｅｃの処理が必要でないと判断した場合には、ＩＰ処理部３０３は、ＩＰパケットのデータ部をＴＣＰ／ＵＤＰパケットとしてＴＣＰ／ＵＤＰ処理部３０６に渡す。
【００６０】
そして、ＴＣＰ／ＵＤＰ処理部３０６（ＣＰＵ１０１）は、ＴＣＰ／ＵＤＰパケットを受け取ると、ＴＣＰ／ＵＤＰヘッダ解析処理を行い（Ｓ４１１）。具体的には、ＴＣＰ／ＵＤＰ処理部３０６は、ＲＦＣ７９３で定義されているＴＣＰプロトコルやＲＦＣ７６８で定義されているＵＤＰプロトコルを制御する処理等を行う。そして、ＴＣＰ／ＵＤＰ処理部３０６は、受信データ（ＴＣＰ／ＵＤＰパケットのデータ部）をアプリケーション処理部３０７へ渡す（Ｓ４１０）。なお、ＩＰ処理部３０３は、ステップＳ４０３の処理が終了すると、再度、ステップＳ４０１のデータ受信の監視処理を継続する。
【００６１】
一方、ステップＳ４０３において、ＩＰ処理部３０３が受信データにＩＰＳｅｃの処理が必要であると判断した場合、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４が停止中か否かを判断する（Ｓ４０４）。
【００６２】
ＩＰＳｅｃハードウェア処理部３０４が停止中でない（電源が入っている）と判断した

場合（Ｓ４０４でＮｏ）、ＣＰＵ１０１は、ＩＰ処理部３０３からＩＰＳｅｃハードウェア処理部３０４へ暗号化されたパケットデータであるＥＳＰを渡すように制御する。

【００６３】

ＩＰＳｅｃハードウェア処理部３０４は、ＩＰ処理部３０３から受け取ったＥＳＰをデコード（伸張）し、ＴＣＰ／ＵＤＰパケットに変換して、ＴＣＰ／ＵＤＰ処理部３０６に渡す（Ｓ４０５）。

【００６４】

一方、ＩＰＳｅｃハードウェア処理部３０４が停止中（電源が入っていない）と判断した場合（Ｓ４０４でＹｅｓ）、ＣＰＵ１０１は、ＩＰ処理部３０３からＩＰＳｅｃソフトウェア処理部３０５へ暗号化されたパケットデータであるＥＳＰを渡すように制御する。

【００６５】

ＩＰＳｅｃソフトウェア処理部３０５（ＣＰＵ１０１）は、ＩＰ処理部３０３から受け取ったＥＳＰをデコードし、ＴＣＰ／ＵＤＰパケットに変換して、ＴＣＰ／ＵＤＰ処理部３０６に渡す（Ｓ４０６）。

【００６６】

そして、ＴＣＰ／ＵＤＰ処理部３０６は、ＩＰＳｅｃハードウェア処理部３０４又はＩＰＳｅｃソフトウェア処理部３０５からＴＣＰ／ＵＤＰパケットを受け取ると、ＴＣＰ／ＵＤＰヘッダ解析処理を行う（Ｓ４０７）。具体的には、ＴＣＰ／ＵＤＰ処理部３０６は、ＲＦＣ７９３で定義されているＴＣＰプロトコルやＲＦＣ７６８で定義されているＵＤＰプロトコルを制御する処理を行う（ＴＣＰ／ＵＤＰヘッダ部より「宛先ポート番号」の抽出も行う）。

【００６７】

ここでＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４のハード開始条件の一致を判定する（Ｓ４０８）。これにより、ＩＰＳｅｃハードウェア処理部３０４の電源を入れるか否かを判断する。なお、「ハード開始条件」とは、「ＩＰＳｅｃハードウェア処理部３０４が停止中」且つ「Ｓ４０１で受信したデータの処理がＩＰＳｅｃソフトウェア処理部３０５の処理で問題がある」の条件に対応する。

【００６８】

具体的には、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４が停止中か否かを判定し、停止中でない場合には、「ハード開始条件」に一致しないと判定する。

【００６９】

一方、ＩＰＳｅｃハードウェア処理部３０４が停止中であると判定した場合、ＣＰＵ１０１は、Ｓ４０１で受信したデータの処理がＩＰＳｅｃソフトウェア処理部３０５の処理で問題があるか否かを判定する。具体的には、ＣＰＵ１０１は、Ｓ４０７で取得した「宛先ポート番号」が予め設定されたポート番号（図５のＳ５０１で説明したパケット量が多いプロトコル（例えばＬＰＲ／ｒａｗＴＣＰ等）のポート番号）と一致するか否かを判定する。そして、Ｓ４０７で取得した「宛先ポート番号」が予め設定されたポート番号と一致する場合には、ＣＰＵ１０１は、ＩＰＳｅｃソフトウェア処理部３０５の処理で問題があると判定する。一方、Ｓ４０７で取得した「宛先ポート番号」が予め設定されたポート番号と一致しない場合には、ＣＰＵ１０１は、ＩＰＳｅｃソフトウェア処理部３０５の処理で問題がないと判定する。

【００７０】

そして、Ｓ４０１で受信したデータの処理がＩＰＳｅｃソフトウェア処理部３０５の処理で問題がないと判定した場合には、ＣＰＵ１０１は「ハード開始条件」に一致しないと判定する。一方、Ｓ４０１で受信したデータの処理がＩＰＳｅｃソフトウェア処理部３０５の処理で問題があると判定した場合には、ＣＰＵ１０１は「ハード開始条件」に一致すると判定する。

【００７１】

そして、ＩＰＳｅｃハードウェア処理部３０４の開始条件に一致しないと判定した場合（Ｓ４０８でＮｏ）には、そのままステップＳ４１０に処理を進める。

【００７２】
一方、ＩＰＳｅｃハードウェア処理部３０４の開始条件に一致すると判定した場合（Ｓ４０８でＹｅｓ）には、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア開始処理を実行する（Ｓ４０９）。具体的には、ＣＰＵ１０１は、ＩＰＳｅｃアクセラレータ１１０内の電源コントローラ９９９に対してＩＰＳｅｃハードウェア処理部３０４に電源供給を開始するよう指示する。この指示を受けた電源コントローラ９９９は、ＩＰＳｅｃハードウェア処理部３０４への電源供給を開始する。
【００７３】
そして、ステップＳ４１０において、ＴＣＰ／ＵＤＰ処理部３０６は、受信データ（ＴＣＰ／ＵＤＰパケットのデータ部）をアプリケーション処理部３０７へ渡す。なお、ＩＰ処理部３０３は、ステップＳ４０３の処理が終了すると、再度、ステップＳ４０１のデータ受信の監視処理を継続する。
【００７４】
なお、Ｓ４０１～Ｓ４０７，Ｓ４１０，Ｓ４１１を第２制御処理、Ｓ４０８，Ｓ４０９を第３制御処理と呼ぶ。
【００７５】
以下、図７～図１０に示す場合について図６のＬＡＮインタフェース処理の動作を具体的に説明する。
【００７６】
まず、図７に示す通常のＩＰパケットを受信する場合のＬＡＮインタフェース処理について説明する。
【００７７】
図７は、通常のＩＰパケットを受信した場合のＬＡＮインタフェース処理を説明する図である。
【００７８】
まず、ステップＳ４０１において、ネットワーク１０９より１パケットのデータをＩＰ処理部３０３（ＣＰＵ１０１）が受信すると、ステップＳ４０２において、ＩＰ処理部３０３は、ＩＰヘッダ解析処理を実行する（「ＩＰプロトコル番号」の抽出を含む）。
【００７９】
次に、ＩＰ処理部３０３は、受信データにＩＰＳｅｃの処理が必要であるか否かを判断する（Ｓ４０３）。図７に示す例は通常のＩＰパケットを受信した場合であるので、受信データのＩＰプロトコル番号がＩＰＳｅｃのデータであるＥＳＰの番号（５０）と一致しない。よって、ステップＳ４０３では、ＩＰ処理部３０３は、受信データにＩＰＳｅｃの処理が必要でないと判断し、受信データをＴＣＰ／ＵＤＰパケットに変換してＴＣＰ／ＵＤＰ処理部３０６に渡す。
【００８０】
次に、ステップＳ４１１において、ＴＣＰ／ＵＤＰ処理部３０６（ＣＰＵ１０１）は、受け取ったＴＣＰ／ＵＤＰパケットについてＲＦＣ７９３で定義されているＴＣＰプロトコルやＲＦＣ７６８で定義されているＵＤＰプロトコルを制御する処理を行う。そして、ステップＳ４１０において、ＴＣＰ／ＵＤＰ処理部３０６は、ＴＣＰ／ＵＤＰパケットのデータ部をアプリケーション処理部３０７へ渡す（Ｓ４１０）。
【００８１】
以上、図７に示した通常のＩＰパケット送受信では、データを受信していてもＩＰＳｅｃ処理を行わない。このため、図５に示したＩＰＳｅｃハード停止管理処理では、ステップＳ５０１のハード停止条件に一致し、図５のステップＳ５０２において、ＩＰＳｅｃハードウェア処理部３０４の電源が停止され、消費電力が下がることになる。
【００８２】
次に、図８に示すＩＰＳｅｃハードウェア処理部３０４が停止していない状態でＩＰＳｅｃパケットを受信する場合のＬＡＮインタフェース処理について説明する。
【００８３】

図８は、ＩＰＳｅｃハードウェア処理部３０４が停止していない状態でＩＰＳｅｃパケットを受信する場合のＬＡＮインタフェース処理を説明する図である。

【００８４】

まず、ステップＳ４０１において、ネットワーク１０９より１パケットのデータをＩＰ処理部３０３（ＣＰＵ１０１）が受信すると、ステップＳ４０２において、ＩＰ処理部３０３は、ＩＰヘッダ解析処理を実行する（「ＩＰプロトコル番号」の抽出を含む）。

【００８５】

次に、ＩＰ処理部３０３は、受信データにＩＰＳｅｃの処理が必要であるか否かを判断する（Ｓ４０３）。図８に示す例はＩＰＳｅｃパケットを受信した場合であるので、受信データのＩＰプロトコル番号がＩＰＳｅｃのデータであるＥＳＰの番号（５０）と一致する。よって、ステップＳ４０３では、ＩＰ処理部３０３は、受信データにＩＰＳｅｃの処理が必要であると判断する。

【００８６】

そして、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４が停止中であるか否かを判断する（Ｓ４０４）。図８に示す例はＩＰＳｅｃハードウェア処理部３０４が停止していない状態であるので、ＣＰＵ１０１は、ＩＰ処理部３０３からＩＰＳｅｃハードウェア処理部３０４へ受信データ（ＥＳＰ）を渡すように制御する（Ｓ４０５へ処理を進める）。

【００８７】

そして、ステップＳ４０５において、ＩＰＳｅｃハードウェア処理部３０４は、ＩＰ処理部３０３から送られてきたＥＳＰをデコード（伸張）し、ＴＣＰ／ＵＤＰパケットに変換して、ＴＣＰ／ＵＤＰ処理部３０６（ＣＰＵ１０１）に渡す。

【００８８】

次に、ステップＳ４０７において、ＴＣＰ／ＵＤＰ処理部３０６は、ＩＰＳｅｃハードウェア処理部３０４からＴＣＰ／ＵＤＰパケットを受け取ると、ＴＣＰ／ＵＤＰヘッダ解析処理を行う（「宛先ポート番号」の抽出を含む）。

【００８９】

そしてステップＳ４０８において、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４開始条件に一致するか否かを判断する。図８に示す例はＩＰＳｅｃハードウェア処理部３０４が停止していない状態であるので、ＩＰ処理部３０３は、ＩＰＳｅｃハードウェア処理部３０４開始条件に一致しないと判断し、ステップＳ４１０へ処理を進める。

【００９０】

そして、ステップＳ４１０において、ＴＣＰ／ＵＤＰ処理部３０６は、受信データのデータ部をアプリケーション処理部３０７へ渡す。

【００９１】

以上、図８のＩＰＳｅｃハードウェア処理部３０４が停止していない状態でＩＰＳｅｃパケットを受信する場合、図５に示したＩＰＳｅｃハード停止管理処理では、ステップＳ５０１の条件に一致せず、ＩＰＳｅｃハードウェア処理部３０４の電源を落さない。しかし、ＩＰＳｅｃハードウェア処理部３０４が動作しているため、ＣＰＵ１０１の処理負荷は上がらず、ＣＰＵ１０１が他の処理を行うことが可能となる。

【００９２】

次に、図９に示すＩＰＳｅｃハードウェア処理部３０４が停止している状態で、ＩＰＳｅｃの処理をソフトウェアのみで行えるＩＰＳｅｃデータを受信した場合のＬＡＮインタフェース処理について説明する。

【００９３】

図９は、ＩＰＳｅｃハードウェア処理部３０４が停止している状態で、ＩＰＳｅｃの処理をソフトウェアのみで行えるＩＰＳｅｃデータ（ＩＣＭＰ／ＡＲＰプロトコル等のデータ）を受信した場合のＬＡＮインタフェース処理を説明する図である。

【００９４】

まず、図６のステップＳ４０１において、ネットワーク１０９より１パケットのデータ

をＩＰ処理部３０３（ＣＰＵ１０１）が受信すると、ステップＳ４０２において、ＩＰ処理部３０３は、ＩＰヘッダ解析処理を実行する（「ＩＰプロトコル番号」の抽出を含む）。

【００９５】

次に、ＩＰ処理部３０３は、受信データにＩＰＳｅｃの処理が必要であるか否かを判断する（Ｓ４０３）。図９に示す例はＩＰＳｅｃパケットを受信した場合であるので、受信データのＩＰプロトコル番号がＩＰＳｅｃのデータであるＥＳＰの番号（５０）と一致する。よって、ステップＳ４０３では、ＩＰ処理部３０３は、受信データにＩＰＳｅｃの処理が必要であると判断する。

【００９６】

そして、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４が停止中であるか否かを判断する（Ｓ４０４）。図９に示す例はＩＰＳｅｃハードウェア処理部３０４が停止している状態であるので、ＣＰＵ１０１は、ＩＰ処理部３０３からＩＰＳｅｃソフトウェア処理部３０５へ受信データ（ＥＳＰ）を渡すように制御する（Ｓ４０６へ処理を進める）。

【００９７】

そして、ステップＳ４０６において、ＩＰＳｅｃソフトウェア処理部３０５は、ＩＰ処理部３０３から送られてきたＥＳＰをデコード（伸張）し、ＴＣＰ／ＵＤＰパケットに変換して、ＴＣＰ／ＵＤＰ処理部３０６（ＣＰＵ１０１）に渡す。

【００９８】

次に、ステップＳ４０７において、ＴＣＰ／ＵＤＰ処理部３０６は、ＩＰＳｅｃソフトウェア処理部３０４からＴＣＰ／ＵＤＰパケットを受け取ると、ＴＣＰ／ＵＤＰヘッダ解析処理を行う（「宛先ポート番号」の抽出を含む）。

【００９９】

そしてステップＳ４０８において、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４開始条件に一致するか否かを判断する。図９に示す例はＩＰＳｅｃハードウェア処理部３０４が停止している状態である。よって、Ｓ４０７で取得した「宛先ポート番号」と予め設定されたポート番号（図５のＳ５０１で説明したパケット量が多いプロトコル（例えばＬＰＲ／ｒａｗＴＣＰ等）のポート番号）を比較する。なお、図９に示す例はＩＰＳｅｃの処理をソフトウェアのみで行えるＩＰＳｅｃデータ（ＩＣＭＰ／ＡＲＰプロトコル等のデータ）を受信する場合であるので、Ｓ４０７で取得した「宛先ポート番号」と予め設定されたポート番号とが不一致となる。よって、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４開始条件に一致しないと判断し、ステップＳ４１０へ処理を進める。

【０１００】

そして、ステップＳ４１０において、ＴＣＰ／ＵＤＰ処理部３０６は、受信データのデータ部をアプリケーション処理部３０７へ渡す。

【０１０１】

以上、図９に示した場合では、ＩＰＳｅｃハードウェア処理部３０４が停止し、ＴＣＰ／ＵＤＰパケット内の「宛先ポート番号」が予め設定されている所定のプロトコルのポート番号ではない。よって、ＩＰＳｅｃハードウェア開始条件に一致せず、ＩＰＳｅｃハードウェア処理部３０４の電源は落したまま（停止したまま）となるので、消費電力を抑えることができる。

【０１０２】

次に、図１０に示すＩＰＳｅｃハードウェア処理部３０４が停止している状態で、ＩＰＳｅｃの処理をソフトウェアのみで行えないＩＰＳｅｃデータ（ＬＰＲ／ｒａｗＴＣＰプロトコル等のデータ）を受信した場合のＬＡＮインタフェース処理について説明する。

【０１０３】

図１０は、ＩＰＳｅｃハードウェア処理部３０４が停止している状態で、ＩＰＳｅｃの処理をソフトウェアのみで行えないＩＰＳｅｃデータ（ＬＰＲ／ｒａｗＴＣＰプロトコル等のデータ）を受信する場合のＬＡＮインタフェース処理を説明する図である。

【０１０４】
まず、ステップＳ４０１において、ネットワーク１０９より１パケットのデータをＩＰ処理部３０３（ＣＰＵ１０１）が受信すると、ステップＳ４０２において、ＩＰ処理部３０３は、ＩＰヘッダ解析処理を実行する（「ＩＰプロトコル番号」の抽出を含む）。
【０１０５】
次に、ＩＰ処理部３０３は、受信データにＩＰＳｅｃの処理が必要であるか否かを判断する（Ｓ４０３）。図１０に示す例はＩＰＳｅｃパケットを受信した場合であるので、受信データのＩＰプロトコル番号がＩＰＳｅｃのデータであるＥＳＰの番号（５０）と一致する。よって、ステップＳ４０３では、ＩＰ処理部３０３は、受信データにＩＰＳｅｃの処理が必要であると判断する。
【０１０６】
そして、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４が停止中であるか否かを判断する（Ｓ４０４）。図１０に示す例はＩＰＳｅｃハードウェア処理部３０４が停止している状態であるので、ＣＰＵ１０１は、ＩＰ処理部３０３からＩＰＳｅｃソフトウェア処理部３０５へ受信データ（ＥＳＰ）を渡すように制御する（Ｓ４０６へ処理を進める）。
【０１０７】
そして、ステップＳ４０６において、ＩＰＳｅｃソフトウェア処理部３０５は、ＩＰ処理部３０３から送られてきたＥＳＰをデコード（伸張）し、ＴＣＰ／ＵＤＰパケットに変換して、ＴＣＰ／ＵＤＰ処理部３０６（ＣＰＵ１０１）に渡す。
【０１０８】
次に、ステップＳ４０７において、ＴＣＰ／ＵＤＰ処理部３０６は、ＩＰＳｅｃソフトウェア処理部３０４からＴＣＰ／ＵＤＰパケットを受け取ると、ＴＣＰ／ＵＤＰヘッダ解析処理を行う（「宛先ポート番号」の抽出を含む）。
【０１０９】
そしてステップＳ４０８において、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４開始条件に一致するか否かを判断する。図１０に示す例はＩＰＳｅｃハードウェア処理部３０４が停止している状態である。よって、Ｓ４０７で取得した「宛先ポート番号」と予め設定されたポート番号（図５のＳ５０１で説明したパケット量が多いプロトコル（例えばＬＰＲ／ｒａｗＴＣＰ等）のポート番号）を比較する。なお、図１０に示す例はＩＰＳｅｃの処理をソフトウェアのみで行えないＩＰＳｅｃデータ（ＬＰＲ／ｒａｗＴＣＰプロトコル等のデータ）を受信する場合であるので、Ｓ４０７で取得した「宛先ポート番号」と予め設定されたポート番号とが一致する。よって、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４開始条件に一致すると判断し、ステップＳ４０９へ処理を進める。
【０１１０】
そして、ステップＳ４０９において、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４の開始処理を行い、再びＩＰＳｅｃハードウェア処理部３０４でのハードウェア処理４０５を使用できる状態にする。具体的には、ＣＰＵ１０１は、ＩＰＳｅｃアクセラレータ１１０内の電源コントローラ９９９に対してＩＰＳｅｃハードウェア処理部３０４に電源供給を開始するよう指示する。この指示を受けた電源コントローラ９９９は、ＩＰＳｅｃハードウェア処理部３０４への電源供給を開始する。
【０１１１】
そして、ステップＳ４１０において、ＴＣＰ／ＵＤＰ処理部３０６は、受信データのデータ部をアプリケーション処理部３０７へ渡す。以上、図１０の矢印（１）に示す処理に相当する。
【０１１２】
なお、ステップＳ４０９で、ＩＰＳｅｃハードウェア処理部３０４に電源供給を開始したことにより、以後、処理されるＩＰＳｅｃパケットは、ステップＳ４０４でＮｏと判定されて、ＩＰＳｅｃハードウェア処理部３０４で処理されることになる。詳細には、Ｓ４

０１→Ｓ４０２→Ｓ４０３→Ｓ４０４→Ｓ４０５→Ｓ４０７→Ｓ４０８→Ｓ４１０のステップで処理されることになる。これは、図１０の矢印（２）に示す処理に相当する。

【０１１３】

以上、図１０に示した場合では、ＩＰＳｅｃハードウェア処理部３０４が停止状態から開始状態になることから、ＣＰＵ１０１の処理負荷は上がらず、ＣＰＵ１０１が他の処理を行うことが可能となる。そして、図５に示したＩＰＳｅｃハード停止管理処理では、ステップＳ５０３でＮｏとなり、再び、ステップＳ５０１のハード停止条件一致の監視処理を行うことになる。

【０１１４】

〔第２実施形態〕

上記第１実施形態では、ＬＰＲ／ｒａｗＴＣＰプロトコル等の処理するパケット量が多いプロトコルのポート番号を予めユーザ等にキーボードから入力させてＲＡＭ１０３内の不揮発性メモリ領域に格納（設定）しておく構成について説明した。本実施形態では、上記プロトコルのポート番号の代わりにプロトコル名（ＬＰＲ／ｒａｗＴＣＰ等）を予めユーザ等にキーボードから入力させてＲＡＭ１０３内の不揮発性メモリ領域に格納（設定）しておくように構成する。

【０１１５】

この構成の場合、図５のステップＳ５０１で、ＣＰＵ１０１が、「ＩＰＳｅｃ通信でデータ受信しているがＩＰＳｅｃソフトウェア処理部３０５の処理で問題ない場合」を判定する際、以下のような処理を行うものとする。

【０１１６】

まず、ＣＰＵ１０１は、予めＲＯＭ１０２内に格納されたテーブルを用いて、受信データ（ＴＣＰ／ＵＤＰパケット）に含まれる宛先ポート番号からプロトコル名を取得する。

【０１１７】

そしてＣＰＵ１０１は、上記取得したプロトコル名が上記予め設定されたプロトコル名（ＬＰＲ／ｒａｗＴＣＰ等）と一致しない場合にはＩＰＳｅｃソフトウェア処理部３０５の処理で問題ないと判断する。一方、ＣＰＵ１０１は、上記取得したプロトコル名が上記予め設定されたポート名と一致する場合にはＩＰＳｅｃソフトウェア処理部３０５の処理では問題あると判断する。

【０１１８】

また、図６のステップＳ４０７のＴＣＰ／ＵＤＰヘッダ解析処理では、ＴＣＰ／ＵＤＰ処理部３０６は、ＴＣＰ／ＵＤＰヘッダ部より「宛先ポート番号」を抽出し、該抽出した「宛先ポート番号」から「プロトコル名」を取得する。

【０１１９】

そして、図４のステップＳ４０９で、ＣＰＵ１０１が、「Ｓ４０１で受信したデータの処理がＩＰＳｅｃソフトウェア処理部３０５の処理で問題があるか否か」を判定する際、以下のような処理を行うものとする。

【０１２０】

ＣＰＵ１０１は、Ｓ４０７で取得した「プロトコル名」が予め設定されたプロトコル名と一致するか否かを判定する。そして、Ｓ４０７で取得した「プロトコル名」が予め設定されたプロトコル名（ＬＰＲ／ｒａｗＴＣＰ等）と一致する場合には、ＣＰＵ１０１は、ＩＰＳｅｃソフトウェア処理部３０５の処理で問題があると判定する。一方、Ｓ４０７で取得した「プロトコル名」が予め設定されたプロトコル名と一致しない場合には、ＣＰＵ１０１は、ＩＰＳｅｃソフトウェア処理部３０５の処理で問題がないと判定するものとする。

【０１２１】

以下、本実施形態の構成について、上述の図１０に示した場合（ＩＰＳｅｃハードウェア処理部３０４が停止している状態で、ＩＰＳｅｃの処理をソフトウェアのみで行えないＩＰＳｅｃデータを受信する場合）を例に具体的に説明する。

【０１２２】

ステップＳ４０１～Ｓ４０６の処理は第１実施形態の場合と同一であるので説明は省略し、ステップＳ４０７以降の処理について説明する。

【０１２３】

ステップＳ４０７において、ＴＣＰ／ＵＤＰ処理部３０６は、ＩＰＳｅｃソフトウェア処理部３０４からＴＣＰ／ＵＤＰパケットを受け取ると、ＴＣＰ／ＵＤＰヘッダ解析処理を行う。具体的には、ＴＣＰ／ＵＤＰ処理部３０６は、ＲＦＣ７９３で定義されているＴＣＰプロトコルやＲＦＣ７６８で定義されているＵＤＰプロトコルを制御する処理を行い、ＴＣＰ／ＵＤＰヘッダ部より「宛先ポート番号」の抽出を行う。さらに、ＣＰＵ１０１が、予めＲＯＭ１０２内に格納されたテーブルを用いて、上記「宛先ポート番号」から「プロトコル名」を取得する。

【０１２４】

次に、ステップＳ４０８において、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４開始条件に一致するか否かを判断する。図１０に示した例はＩＰＳｅｃハードウェア処理部３０４が停止している状態である。よって、Ｓ４０７で取得した「プロトコル名」と予め設定された「プロトコル名」（上述した処理パケット量が多いプロトコル（例えばＬＰＲ／ｒａｗＴＣＰ等））を比較する。なお、図１０に示す例はＩＰＳｅｃの処理をソフトウェアのみで行えないＩＰＳｅｃデータ（ＬＰＲ／ｒａｗＴＣＰプロトコル等のデータ）を受信する場合であるので、Ｓ４０７で取得した「プロトコル名」と予め設定された「プロトコル名」とが一致する。よって、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４開始条件に一致すると判断し、ステップＳ４０９へ処理を進める。

【０１２５】

以下、ステップＳ４０９，Ｓ４１０の処理は第１実施形態と同一であるので説明は省略する。

【０１２６】

〔第３実施形態〕

上記第１，２実施形態では、ＩＰＳｅｃデータを受信した場合の処理について説明したが、ＩＰＳｅｃデータをデータ処理装置１００からネットワーク１０９を介して他の装置に送信する場合にも本発明は適用可能である。

【０１２７】

ＴＣＰ／ＵＤＰ処理部３０６でＴＣＰ／ＵＤＰパケットが生成されると、ＣＰＵ１０１は、該ＴＣＰ／ＵＤＰパケットの送信にＩＰＳｅｃを使用するか否かを判定する。

【０１２８】

そして、ＩＰＳｅｃを使用しないと判定した場合には、ＣＰＵ１０１は、上記ＴＣＰ／ＵＤＰパケットを、ＩＰ処理部３０３に渡す。ＩＰ処理部３０３では、受け取ったＴＣＰ／ＵＤＰパケットに基づいて処理を行い、ＭＡＣ処理部３０２，ＰＨＹ処理部３０１を介して、ネットワークへデータを送信する。

【０１２９】

一方、ＴＣＰ／ＵＤＰパケットの送信にＩＰＳｅｃを使用すると判定した場合には、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア処理部３０４が停止中か否かを判断する。

【０１３０】

そして、ＩＰＳｅｃハードウェア処理部３０４が停止中でない（電源が入っている）と判断した場合には、ＣＰＵ１０１は、ＴＣＰ／ＵＤＰ処理部３０６からＩＰＳｅｃハードウェア処理部３０４へＴＣＰ／ＵＤＰパケットを渡すように制御する。

【０１３１】

ＩＰＳｅｃハードウェア処理部３０４は、ＴＣＰ／ＵＤＰ処理部３０６から受け取ったＴＣＰ／ＵＤＰパケットをＥＳＰでエンコードし、ＥＳＰに変換して、ＩＰ処理部３０３に渡す。ＩＰ処理部３０３では、受け取ったＴＣＰ／ＵＤＰパケットに基づいて処理を行い、ＭＡＣ処理部３０２，ＰＨＹ処理部３０１を介して、ネットワークへデータを送信する。

【０１３２】

一方、ＩＰＳｅｃハードウェア処理部３０４が停止中である（電源が入っていない）と判断した場合には、ＣＰＵ１０１は、ＴＣＰ／ＵＤＰ処理部３０６からＩＰＳｅｃソフトウェア処理部３０５へＴＣＰ／ＵＤＰパケットを渡すように制御する。

【０１３３】

ＩＰＳｅｃソフトウェア処理部３０５は、ＴＣＰ／ＵＤＰ処理部３０６から受け取ったＴＣＰ／ＵＤＰパケットをＥＳＰでエンコードし、ＥＳＰに変換して、ＩＰ処理部３０３に渡す。ＩＰ処理部３０３では、受け取ったＴＣＰ／ＵＤＰパケットに基づいて処理を行い、ＭＡＣ処理部３０２，ＰＨＹ処理部３０１を介して、ネットワークへデータを送信する。

【０１３４】

なお、ＣＰＵ１０１は、上記ＴＣＰ／ＵＤＰパケットをＩＰＳｅｃソフトウェア処理部３０５へ渡した際に、ＩＰＳｅｃハードウェア処理部３０４のハード開始条件の一致を判定する。これにより、ＩＰＳｅｃハードウェア処理部３０４の電源を入れるか否かを判断する。

【０１３５】

ここで「ハード開始条件」とは、「送信データの処理がＩＰＳｅｃソフトウェア処理部３０５の処理で問題がある」の条件に対応する。

【０１３６】

具体的には、ＣＰＵ１０１は、送信するＴＣＰ／ＵＤＰパケットの「宛先ポート番号」が予め設定されたポート番号（パケット量が多いプロトコル（例えばＬＰＲ／ｒａｗＴＣＰ等）のポート番号）と一致するか否かを判定する。そして、送信するＴＣＰ／ＵＤＰパケットの「宛先ポート番号」が予め設定されたポート番号と一致する場合には、ＣＰＵ１０１は、ＩＰＳｅｃソフトウェア処理部３０５の処理で問題があると判定する。一方、送信するＴＣＰ／ＵＤＰパケットの「宛先ポート番号」が予め設定されたポート番号と一致しない場合には、ＣＰＵ１０１は、ＩＰＳｅｃソフトウェア処理部３０５の処理で問題がないと判定する。

【０１３７】

そして、「送信データの処理がＩＰＳｅｃソフトウェア処理部３０５の処理で問題がない」即ち「ハード開始条件」に一致しないと判定した場合には、ＣＰＵ１０１は、特に処理を行わない。

【０１３８】

一方、「送信データの処理がＩＰＳｅｃソフトウェア処理部３０５の処理で問題がある」即ち「ハード開始条件」に一致しないと判定した場合には、ＣＰＵ１０１は、ＩＰＳｅｃハードウェア開始処理を実行する。具体的には、ＣＰＵ１０１は、ＩＰＳｅｃアクセラレータ１１０内の電源コントローラ９９９に対してＩＰＳｅｃハードウェア処理部３０４に電源供給を開始するよう指示する。この指示を受けた電源コントローラ９９９は、ＩＰＳｅｃハードウェア処理部３０４への電源供給を開始する。

【０１３９】

これにより、以後、処理されるＴＣＰ／ＵＤＰパケットは、ＩＰＳｅｃハードウェア処理部３０４で処理されることになる。これにより、パケット量が多いプロトコルを処理する際の、ＣＰＵ１０１の負荷が軽減される。

【０１４０】

〔第４実施形態〕

本実施形態では、データ処理装置１００の動作モードとして、速度優先モード、消費電力優先モードを設けた構成について説明する。

【０１４１】

本実施形態では、ユーザ等がキーボード１０５から動作モードとして「速度優先モード」又は「消費電力優先モード」を選択指示すると、ＣＰＵ１０１が、指示された動作モードをＲＡＭ１０３内の不揮発性メモリ領域に格納（設定）しておくものとする。なお、デフォルトでは「速度優先モード」に設定されているものとする。

【０１４２】
そして、速度優先モードにあっては、ＣＰＵ１０１は、上述の図６に示した処理動作を実行する。即ち、図６のＳ４０８，Ｓ４０９に示したように、ＣＰＵ１０１は、データ処理装置１００の状態がハード開始条件（図６のＳ４０８）に一致すると判断した場合には、ＩＰＳｅｃハードウェア処理部３０４への電力供給を開始するように制御する。この構成により、ＩＰＳｅｃ処理時におけるＣＰＵ１０１の負荷を軽減して、ＩＰＳｅｃ処理時におけるデータ処理装置１００の処理速度低下を抑えることができる。
【０１４３】
一方、消費電力優先モードにあっては、ＣＰＵ１０１は、上述の図６のＳ４０８，Ｓ４０９に示した動作とは異なる動作を実行する。具体的には、ＣＰＵ１０１は、データ処理装置１００の状態がハード開始条件（図６のＳ４０８）に一致する場合であっても、ＩＰＳｅｃハードウェア処理部３０４への電力供給を開始しないように制御する。この構成により、データ処理装置１００での消費電力を抑えることができる。
【０１４４】
従って、ユーザは動作モードを選択設定するだけで、ＩＰＳｅｃ処理時におけるデータ処理装置１００の処理速度低下を抑えたり、データ処理装置１００での消費電力を抑えることができる。
【０１４５】
〔第５実施形態〕
本実施形態では、ＩＰＳｅｃアクセラレータ１１０を設ける代わりに、ＬＡＮ Ｉ／Ｆ１０７内にＩＰＳｅｃハードウェア処理部３０４を設けた構成について説明する。
【０１４６】
図１１は、本発明の第４実施形態を示すデータ処理装置１００の構成を示したブロック図である。
【０１４７】
図１２は、図１１に示したＬＡＮ Ｉ／Ｆ１０７の概略構成の一例を示した図である。
【０１４８】
図１２において、８８８はコネクタであり、バス１０８と接続するためのものである。
【０１４９】
９９９は電源コントローラであり、データ処理システム１００の図示しない電源部から電力を得てＬＡＮ Ｉ／Ｆ１０７内の各部へ電力を供給する。
【０１５０】
なお、電源コントローラ９９９は、ＣＰＵ１０１からの指示により、ＩＰｓｅｃハードウェア処理部３０４への電力の供給／遮断を切り替えることができる。
【０１５１】
なお、他の構成は上記各実施形態と同様であるので説明は省略する。
【０１５２】
〔第６実施形態〕
上記各実施形態では、ＩＰＳｅｃプロトコル処理を実行するハードウェア及びソフトウェアの制御について説明したが、本発明のデータ処理装置はＩＰＳｅｃプロトコルの処理を実行するハードウェア及びソフトウェアの制御に限定されるものではない。例えば、ＳＳＬプロトコル等、その他のＣＰＵに負荷がかかるプロトコル処理を実行するハードウェア及びソフトウェアの制御についても本発明は適用可能である。
【０１５３】
即ち、データ処理装置１００に、ＳＳＬプロトコル処理をハードウェア処理により実行するＳＳＬハードウェア処理部と、ＳＳＬハードウェア処理部と同一の処理をソフトウェア処理により実行可能なＳＳＬソフトウェア処理部とを設ける。
【０１５４】
そして、ＣＰＵ１０１は、データ処理装置１００の状態が電力供給停止条件（ＳＳＬデータを受信していない、又は、ＳＳＬデータを受信したがＳＳＬソフトウェア処理部で問

題ない）に一致する場合にはＳＳＬハードウェア処理部への電力供給を停止する。
【０１５５】
また、データにＳＳＬプロトコル処理を施す際に、ＳＳＬハードウェア処理部が電力供給状態の場合には、ＣＰＵ１０１は、ＳＳＬプロトコル処理をＳＳＬハードウェア処理部に実行させるように制御する。一方、ＳＳＬハードウェア処理部が電力供給状態でない場合（電力停止状態の場合）には、ＣＰＵ１０１は、ＳＳＬプロトコル処理をＳＳＬソフトウェア処理部に実行させるように制御する。
【０１５６】
さらに、データ処理装置１００の状態が電力供給開始条件（ＳＳＬデータを受信し、且つ、該ＳＳＬデータがＳＳＬソフトウェア処理部で問題がある）に一致する場合には、ＣＰＵ１０１は、ＳＳＬハードウェア処理部への電力供給を開始するように制御するように構成する。
【０１５７】
〔第７実施形態〕
本発明のデータ処理装置は、通信プロトコルの処理を実行するハードウェア及びソフトウェアの制御に限定されるものではない。例えば、３Ｄ処理等のＣＰＵに負荷がかかる処理を実行するハードウェア及びソフトウェアの制御についても本発明は適用可能である。以下、３Ｄ処理を例として説明する。
【０１５８】
即ち、データ処理装置１００に、３Ｄ処理をハードウェア処理により実行する３Ｄハードウェア処理部と、３Ｄハードウェア処理部と同一の処理をソフトウェア処理により実行可能な３Ｄソフトウェア処理部とを設ける。
【０１５９】
そして、ＣＰＵ１０１は、データ処理装置１００の状態が電力供給停止条件（３Ｄ処理のコマンドが存在しない、又は、３Ｄ処理のコマンドは存在するが３Ｄソフトウェア処理部で問題ない）に一致する場合には３Ｄハードウェア処理部への電力供給を停止する。
【０１６０】
また、３Ｄ処理を施す際に、３Ｄハードウェア処理部が電力供給状態の場合には、ＣＰＵ１０１は、３Ｄ処理を３Ｄハードウェア処理部に実行させるように制御する。一方、３Ｄハードウェア処理部が電力供給状態でない場合（電力停止状態の場合）には、ＣＰＵ１０１は、３Ｄ処理を３Ｄソフトウェア処理部に実行させるように制御する。
【０１６１】
さらに、データ処理装置１００の状態が電力供給開始条件（３Ｄ処理のコマンドが存在し、且つ、該３Ｄ処理のコマンドが３Ｄソフトウェア処理部では問題がある）に一致する場合には、ＣＰＵ１０１は、３Ｄハードウェア処理部への電力供給を開始するように制御するように構成する。なお、３Ｄソフトウェア処理部での処理で問題のある３Ｄコマンドを予めキーボード１０５等から設定しておくものとする。
【０１６２】
以上説明したように、本発明の各実施形態によれば、ＩＰＳｅｃ等を処理するハードウェアアクセラレータを搭載することでＣＰＵへの負荷は下がるがデータ処理装置１００全体の平均消費電力を押し上げてしまうという従来の問題点を克服することが可能になる。即ち、ＩＰＳｅｃ等を処理するハードウェアアクセラレータを搭載してＣＰＵの処理負荷を下げつつ、データ処理装置１００全体の平均消費電力の増加も抑えることが可能になる。
【０１６３】
従って、同種の処理実行可能な複数の処理手段への電力供給を適切に制御して、データ処理速度を維持しつつデータ処理装置の省電力化を図ることができる等の効果を奏する。
【０１６４】
上述した各種データの構成及びその内容はこれに限定されるものではなく、用途や目的に応じて、様々な構成や内容で構成されることは言うまでもない。

【０１６５】
以上、一実施形態について示したが、本発明は、例えば、システム、装置、方法、プログラムもしくは記憶媒体等としての実施態様をとることが可能である。具体的には、複数の機器から構成されるシステムに適用しても良いし、また、一つの機器からなる装置に適用しても良い。
【０１６６】
以下、図１３に示すメモリマップを参照して、本発明に係るデータ処理装置で読み取り可能な各種データ処理プログラムを格納する記録媒体（記憶媒体）のメモリマップの構成について説明する。
【０１６７】
図１３は、本発明に係るデータ処理装置で読み取り可能な各種データ処理プログラムを格納する記憶媒体（記録媒体）のメモリマップを説明する図である。
【０１６８】
なお、特に図示しないが、記憶媒体に記憶されるプログラム群を管理する情報、例えばバージョン情報，作成者等も記憶され、かつ、プログラム読み出し側のOS等に依存する情報、例えばプログラムを識別表示するアイコン等も記憶される場合もある。
【０１６９】
さらに、各種プログラムに従属するデータも上記ディレクトリに管理されている。また、各種プログラムをコンピュータにインストールするためのプログラムや、インストールするプログラムが圧縮されている場合に、解凍するプログラム等も記憶される場合もある。
【０１７０】
本実施形態における図５，図６に示す機能が外部からインストールされるプログラムによって、ホストコンピュータにより遂行されていてもよい。そして、その場合、CD-ROMやフラッシュメモリやＦＤ等の記憶媒体により、あるいはネットワークを介して外部の記憶媒体から、プログラムを含む情報群を出力装置に供給される場合でも本発明は適用されるものである。
【０１７１】
以上のように、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給する。そして、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読出し実行することによっても、本発明の目的が達成されることは言うまでもない。
【０１７２】
この場合、記憶媒体から読み出されたプログラムコード自体が本発明の新規な機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。
【０１７３】
従って、プログラムの機能を有していれば、オブジェクトコード、インタプリタにより実行されるプログラム、OSに供給するスクリプトデータ等、プログラムの形態を問わない。
【０１７４】
プログラムを供給するための記憶媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、MO、CD-ROM、CD-R、CD-RW、磁気テープ、不揮発性のメモリカード、ROM、DVDなどを用いることができる。
【０１７５】
この場合、記憶媒体から読出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。
【０１７６】
その他、プログラムの供給方法としては、クライアントコンピュータのブラウザを用い

てインターネットのホームページに接続し、該ホームページから本発明のプログラムそのものをハードディスク等の記憶媒体にダウンロードすることによっても供給できる。また、該ホームページから圧縮され自動インストール機能を含むファイルをハードディスク等の記憶媒体にダウンロードすることによっても供給できる。また、本発明のプログラムを構成するプログラムコードを複数のファイルに分割し、それぞれのファイルを異なるホームページからダウンロードすることによっても実現可能である。つまり、本発明の機能処理をコンピュータで実現するためのプログラムファイルを複数のユーザに対してダウンロードさせるWWWサーバやFTPサーバ等も本発明の請求項に含まれるものである。

【０１７７】

また、本発明のプログラムを暗号化してCD-ROM等の記憶媒体に格納してユーザに配布する。さらに、所定の条件をクリアしたユーザに対し、インターネットを介してホームページから暗号化を解く鍵情報をダウンロードさせる。さらに、その鍵情報を使用することにより暗号化されたプログラムを実行してコンピュータにインストールさせて実現することも可能である。

【０１７８】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、以下のような構成も含まれることは言うまでもない。例えば、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているOS（オペレーティングシステム）等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１７９】

さらに、記憶媒体から読み出されたプログラムコードを、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込む。そして、該メモリに書き込まれたプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１８０】

また、本発明は、複数の機器から構成されるシステムに適用しても、１つの機器からなる装置に適用してもよい。また、本発明は、システムあるいは装置にプログラムを供給することによって達成される場合にも適応できることは言うまでもない。この場合、本発明を達成するためのソフトウェアによって表されるプログラムを格納した記憶媒体を該システムあるいは装置に読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【０１８１】

本発明は上記実施形態に限定されるものではなく、本発明の趣旨に基づき種々の変形（各実施形態の有機的な組合せを含む）が可能であり、それらを本発明の範囲から除外するものではない。

【０１８２】

本発明の様々な例と実施形態を示して説明したが、当業者であれば、本発明の趣旨と範囲は、本明細書内の特定の説明に限定されるのではない。

【０１８３】

なお、上述した各実施形態およびその変形例を組み合わせた構成も全て本発明に含まれるものである。

【図面の簡単な説明】

【０１８４】

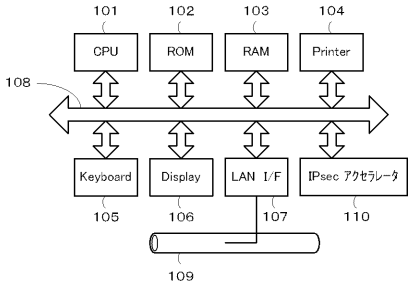
【図１】本発明の第１実施形態を示すデータ処理装置の構成を示したブロック図である。

【図２】ＯＳＩ参照モデルと一般的なＴＣＰ/ＩＰプロトコルによる階層構造を示した図である。

【図３】データ処理装置１００で実行されるＬＡＮインタフェース処理の内容を示した図である。

【図４】図１に示したＩＰＳｅｃアクセラレータ１１０の概略構成の一例を示すブロック図である。
【図５】本発明における第１の制御処理手順の一例を示すフローチャートである。
【図６】本発明における第２の制御処理手順の一例を示すフローチャートである。
【図７】通常のＩＰパケットを受信した場合のＬＡＮインタフェース処理を説明する図である。
【図８】ＩＰＳｅｃハードウェア処理部３０４が停止していない状態でＩＰＳｅｃパケットを受信する場合のＬＡＮインタフェース処理を説明する図である。
【図９】ＩＰＳｅｃハードウェア処理部３０４が停止している状態で、ＩＰＳｅｃの処理をソフトウェアのみで行えるＩＰＳｅｃデータ（ＩＣＭＰ／ＡＲＰプロトコル等のデータ）を受信した場合のＬＡＮインタフェース処理を説明する図である。
【図１０】ＩＰＳｅｃハードウェア処理部３０４が停止している状態で、ＩＰＳｅｃの処理をソフトウェアのみで行えないＩＰＳｅｃデータ（ＬＰＲ／ｒａｗＴＣＰプロトコル等のデータ）を受信する場合のＬＡＮインタフェース処理を説明する図である。
【図１１】本発明の第４実施形態を示すデータ処理装置１００の構成を示したブロック図である。
【図１２】図１１に示したＬＡＮ　Ｉ／Ｆ１０７の概略構成の一例を示した図である。
【図１３】本発明に係るデータ処理装置で読み取り可能な各種データ処理プログラムを格納する記憶媒体（記録媒体）のメモリマップを説明する図である。
【符号の説明】
【０１８５】
１００　データ処理装置
１０１　ＣＰＵ
１０２　ＲＯＭ
１０３　ＲＡＭ
１０４　ＬＡＮ　Ｉ／Ｆ
１１０　ＩＰＳｅｃアクセラレータ
３０４　ＩＰＳｅｃハードウェア処理部
３０５　ＩＰＳｅｃソフトウェア処理部

【図１】



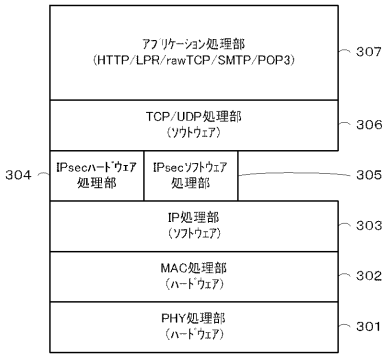
100 データ処理装置

【図２】

第7層 アプリケーション層	アプリケーション層 204	HTTP	LPR	rawTCP	SMTP	POP3
第6層 プレゼンテーション層						
第5層 セッション層						
第4層 トランスポート層	トランスポート層 203	TCP/UDP				
第3層 ネットワーク層	インターネット層 202	IP				
第2層 データリンク層	ネットワーク インタフェース層 201	Ethernet				
第1層 物理層						

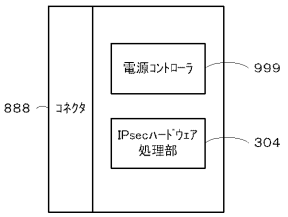
OSIモデル

【図３】



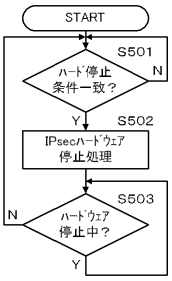
300 LANインタフェース処理部

【図４】



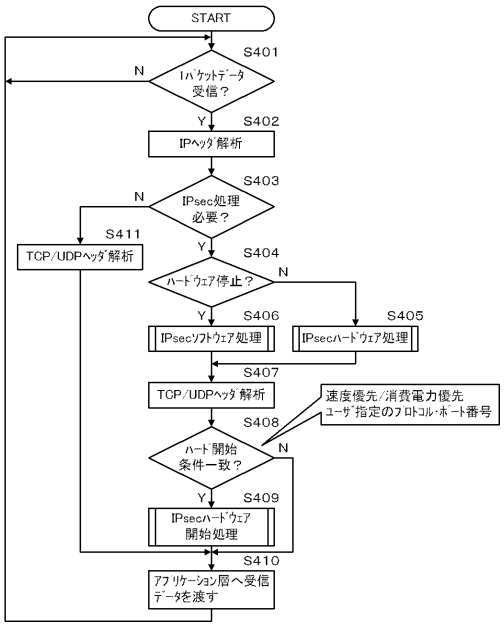
110 IPsecアクセラレータ

【図５】

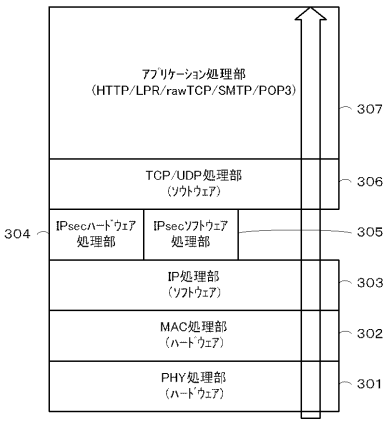


IPsecハード停止監視フロー

【図６】

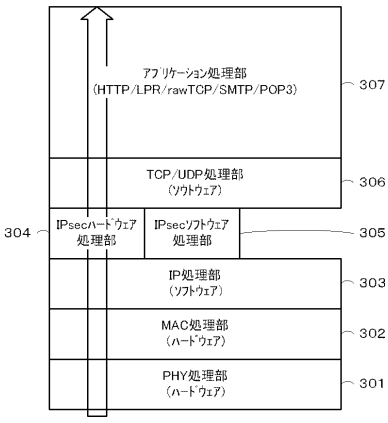


【図７】



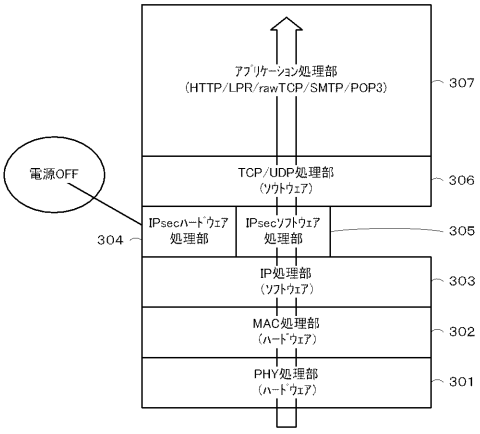
通常のIPパケット受信

【図８】



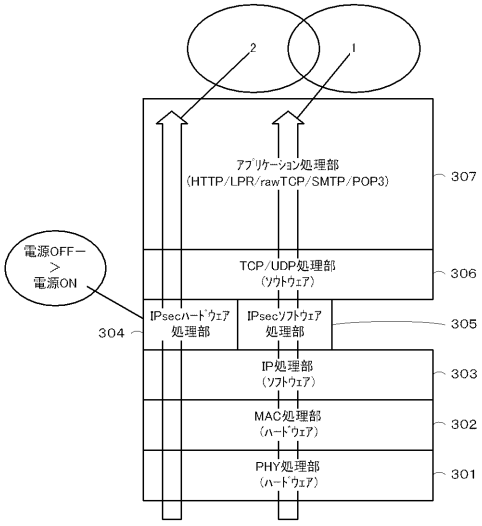
IPsec受信

【図９】



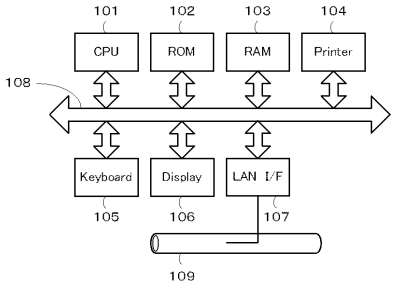
IPsecハードウェアを起動する必要が無い場合

【図１０】



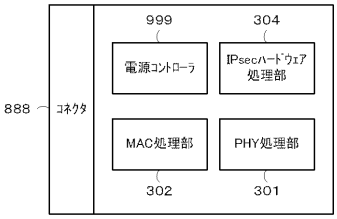
IPsecソフトウェア送受信後に、ハード処理に変更

【図１１】



100 ﾃﾞｰﾀ処理装置

【図１２】



107 LAN I/F

【図１３】

FD/CD-ROM等の記憶媒体

ディレクトリ情報
第1の処理ﾌﾟﾛｸﾞﾗﾑ 図5に示すﾌﾛｰﾁｬｰﾄのｽﾃｯﾌﾟに対応するﾌﾟﾛｸﾞﾗﾑｺｰﾄﾞ群
第2の処理ﾌﾟﾛｸﾞﾗﾑ 図6に示すﾌﾛｰﾁｬｰﾄのｽﾃｯﾌﾟに対応するﾌﾟﾛｸﾞﾗﾑｺｰﾄﾞ群

記憶媒体のﾒﾓﾘﾏｯﾌﾟ

フロントページの続き

(56)参考文献 特開２００２－３５４０６４（ＪＰ，Ａ）
特開２００４－０２１４２３（ＪＰ，Ａ）
特開２００４－３０４６９６（ＪＰ，Ａ）
特開２００５－１１７２３２（ＪＰ，Ａ）
特開２００６－００７６３８（ＪＰ，Ａ）
特開２００６－２０３８７１（ＪＰ，Ａ）
特開２００７－１７９２２５（ＪＰ，Ａ）
特開２００８－１３９９３２（ＪＰ，Ａ）
特開２００８－１４１２９０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　１／３２
Ｇ０６Ｆ　　３／１２