(19)日本国特許庁(JP)

再公表特許(A1)

(11)国際公開番号
WO2006/093021

発行日　平成20年8月7日(2008.8.7)

(43)国際公開日　平成18年9月8日(2006.9.8)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/56	(2006.01)	H04L	12/56	A	5J104
H04L 29/08	(2006.01)	H04L	13/00	307A	5K030
H04L 9/08	(2006.01)	H04L	9/00	601C	5K034
H04L 12/66	(2006.01)	H04L	12/66	Z	

審査請求 未請求　予備審査請求 有　（全 169 頁）

出願番号　特願2007-505878 (P2007-505878)
(21)国際出願番号　PCT/JP2006/303294
(22)国際出願日　平成18年2月23日(2006.2.23)
(31)優先権主張番号　特願2005-54953 (P2005-54953)
(32)優先日　平成17年2月28日(2005.2.28)
(33)優先権主張国　日本国(JP)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100079005
弁理士　宇高　克己
(72)発明者　榎本　敦之
日本国東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　吉見　英朗
日本国東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　飛鷹　洋一
日本国東京都港区芝五丁目７番１号　日本電気株式会社内

最終頁に続く

(54)【発明の名称】通信装置、通信システム、通信方法、及びプログラム

(57)【要約】
ゲートウェイ装置内２０の中間ドライバ２００６においてＴＣＰ２００３を終端し、ゲートウェイ装置内３０の中間ドライバ３００６においてＴＣＰ３００３を終端し、中間ドライバ間をＵＤＰ等の輻輳制御のかからない方法で転送する。この上で、ＳＳＬ２００２とＳＳＬ３００２との間でＳＳＬセッションを構築し、セッション構築が完了したとことで、高速化エンジン制御から高速化エンジンに公開鍵および秘密鍵をイーサネットフレームにより送る。これにより、以降の端末２１とサーバ３１との間の通信において、ゲートウェイ装置はＣＰＵを介さず、ＮＩＣ内の高速化エンジンを用いて転送を行う。

【特許請求の範囲】
【請求項１】
通信システムであって、
ＴＣＰセッションを確立させて通信する通信装置間に、ＴＣＰのセッションを終端させる終端手段を設け、
前記終端手段は、前記通信装置の送信側から送信されるＴＣＰパケットを受信し、このＴＣＰパケットの応答パケットを送信側に送信し、独自の接続要求を前記通信装置の受信側に送信するように構成されていることを特徴とする通信システム。
【請求項２】
前記終端手段は、前記通信装置の送信側から送信される前記の接続要求を受信し、前記通信装置の受信側にＴＣＰパケットを送信するように構成されていることを特徴とする請求項１に記載の通信システム。
【請求項３】
前記終端手段は、前記通信装置の受信側から送信されるＴＣＰパケットの応答パケットを受信し、この応答パケットの受信確認パケットを受信側に送信し、独自の接続完了通知を前記通信装置の送信側に送信するように構成されていることを特徴とする請求項１に記載の通信システム。
【請求項４】
前記終端手段は、前記接続要求又は前記接続完了通知を、輻輳制御がない通信方法を用いて通信するように構成されていることを特徴とする請求項１に記載の通信システム。
【請求項５】
前記通信装置間に、
前記通信装置間で暗号化通信する際の暗号鍵を取得する暗号鍵取得手段と、
前記取得した暗号鍵を保存し、高速化処理開始命令を受信すると、この保存した暗号鍵を用いて前記通信装置間で送受信されるデータの暗号化又は復号化を行う暗号化手段と
を有することを特徴とする請求項１に記載の通信システム。
【請求項６】
前記通信装置の送信側と受信側とは互いに異なるネットワーク上に構成され、ファイアーウォールを介して通信する構成の場合、前記終端手段は各ネットワークに構成されていることを特徴とする請求項１に記載の通信システム。
【請求項７】
前記暗号化手段は、フラグメント分割されたデータを暗号化し、フラグメント解除前のデータを復号化するように構成されていることを特徴とする請求項５に記載の通信システム。
【請求項８】
通信システムであって、
暗号化通信する通信装置間に
前記通信装置間で暗号化通信する際の暗号鍵を取得する暗号鍵取得手段と、
前記取得した暗号鍵を保存し、高速化処理開始命令を受信すると、この保存した暗号鍵を用いて前記通信装置間で送受信されるデータの暗号化又は復号化を行う暗号化手段と
を有することを特徴とする通信システム。
【請求項９】
前記暗号化手段は、フラグメント分割されたデータを暗号化し、フラグメント解除前のデータを復号化するように構成されていることを特徴とする請求項８に記載の通信システム。
【請求項１０】
通信装置であって、
ＴＣＰセッション確立する際にＴＣＰパケットを送信するＴＣＰ手段と、
前記ＴＣＰパケットを受信し、このＴＣＰパケットの応答パケットを前記ＴＣＰ部に送信し、独自の接続要求を接続先に送信する終端手段と

を有することを特徴とする通信装置。
【請求項１１】
前記終端手段は、独自の接続要求を受信した場合、前記ＴＣＰ手段にＴＣＰパケットを送信するように構成されていることを特徴とする請求項９に記載の通信装置。
【請求項１２】
前記終端手段は、ＴＣＰパケットの応答パケットを前記ＴＣＰ手段から受信した場合、この応答パケットの受信確認パケットを前記ＴＣＰ手段に送信し、独自の接続完了通知を接続先に送信するように構成されていることを特徴とする請求項１０に記載の通信装置。
【請求項１３】
前記終端手段は、前記接続要求又は前記接続完了通知を、輻輳制御がない通信方法を用いて送受信するように構成されていることを特徴とする請求項１０に記載の通信装置。
【請求項１４】
暗号化通信する際の暗号鍵を取得する暗号鍵取得手段と、
前記取得した暗号鍵を保存し、高速化処理開始命令を受信後、この保存した暗号鍵を用いて前記通信装置間で送受信されるデータの暗号化又は復号化を行う暗号化手段と
を有することを特徴とする請求項１０に記載の通信装置。
【請求項１５】
前記暗号化手段は、フラグメント分割されたデータを暗号化し、フラグメント解除前のデータを復号化するように構成されていることを特徴とする請求項１４に記載の通信装置。
【請求項１６】
暗号化通信する通信装置であって、
暗号鍵を取得する暗号鍵取得手段と、
前記取得した暗号鍵を保存し、高速化処理開始命令を受信すると、この保存した暗号鍵を用いて前記データの暗号化又は復号化を行う暗号化手段と
を有することを特徴とする通信装置。
【請求項１７】
前記暗号化手段は、フラグメント分割されたデータを暗号化し、フラグメント解除前のデータを復号化するように構成されていることを特徴とする請求項１６に記載の通信装置。
【請求項１８】
通信方法であって、
ＴＣＰパケットを受信するＴＣＰ受信ステップと、
前記受信したＴＣＰパケットの応答パケットを送信する応答パケット送信ステップと、
独自の接続要求を送信する接続要求送信ステップと
を有することを特徴とする通信方法。
【請求項１９】
前記送信された接続要求を受信する接続要求受信ステップと、
前記接続要求受信後にＴＣＰパケットを送信するステップと
を有することを特徴とする請求項１８に記載の通信方法。
【請求項２０】
前記送信されたＴＣＰパケットの応答パケットを受信する応答パケット受信ステップと、
前記応答パケットの受信確認パケットを送信する受信確認送信ステップと、
前記受信確認パケットを送信後、独自の接続完了通知を送信する接続完了通知送信ステップと
を有することをを特徴とする請求項１８に記載の通信方法。
【請求項２１】
前記接続要求送信ステップと前記接続完了通知送信ステップは、輻輳制御がない通信方法を用いて前記接続要求又は前記接続完了通知を送信することを特徴とする請求項１８に

記載の通信方法。
【請求項２２】
暗号化通信する際の暗号鍵を取得する暗号鍵取得ステップと、
高速化処理開始命令を受信するステップと、
前記取得した暗号鍵を保存し、この保存した暗号鍵を用いて前記通信装置間で送受信されるデータの暗号化又は復号化を行う暗号化ステップと
を有することを特徴とする請求項１８に記載の通信方法。
【請求項２３】
前記暗号化ステップは、
フラグメント分割されたデータを暗号化するステップと、
フラグメント解除前のデータを復号化するステップと
を有することを特徴とする請求項２２に記載の通信方法。
【請求項２４】
暗号化通信を用いて通信する方法であって、
暗号化通信する際の暗号鍵を取得する暗号鍵取得ステップと、
高速化処理開始命令を受信するステップと、
前記取得した暗号鍵を保存し、この保存した暗号鍵を用いて前記通信装置間で送受信されるデータの暗号化又は復号化を行う暗号化ステップと
を有することを特徴とする通信方法。
【請求項２５】
前記暗号化ステップは、
フラグメント分割されたデータを暗号化するステップと、
フラグメント解除前のデータを復号化するステップと
を有することを特徴とする請求項２４に記載の通信方法。
【請求項２６】
情報処理装置のプログラムであって、前記プログラムは前記情報処理装置を、
ＴＣＰセッション確立する際にＴＣＰパケットを送信するＴＣＰ手段と、
前記ＴＣＰパケットを受信し、このＴＣＰパケットの応答パケットを前記ＴＣＰ部に送信し、独自の接続要求を接続先に送信する終端手段と
して機能させることを特徴とするプログラム。
【請求項２７】
前記終端手段は、独自の接続要求を受信した場合、前記ＴＣＰ手段にＴＣＰパケットを送信する手段として機能させることを特徴とする請求項２６に記載のプログラム。
【請求項２８】
前記終端手段は、ＴＣＰパケットの応答パケットを前記ＴＣＰ手段から受信した場合、この応答パケットの受信確認パケットを前記ＴＣＰ手段に送信し、独自の接続完了通知を接続先に送信する手段として機能させることを特徴とする請求項２６に記載のプログラム。
【請求項２９】
前記終端手段は、前記接続要求又は前記接続完了通知を、輻輳制御がない通信方法を用いて送受信する手段として機能させることを特徴とする請求項２６に記載のプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信技術に関し、特に、Ｅｔｈｅｒ　ｏｖｅｒ　ＳＳＬ通信において、データの転送速度の向上と、大規模収容を行うための技術に関する。
【背景技術】
【０００２】
まず、従来技術１について説明する。
従来、Ｅｔｈｅｒ　ｏｖｅｒ　ＳＳＬ通信により、インターネット等により相互に接続

された複数のイントラネットを相互に結び、同一のＬＡＮセグメントとして利用できるようにする技術が提案（非特許文献１）されている。

【０００３】

図１は、かかる従来技術におけるネットワークの構成を示すブロック図である。

【０００４】

インターネット１は、セッション中継装置１０、Ｆｉｒｅｗａｌｌ２３、及びＦｉｒｅｗａｌｌ３３、若しくはその他の機器で構成され、これら機器の相互間で通信を行うワイドエリアネットワーク（ＷＡＮ）である。図１において、インターネット１内の各機器は、ＨＵＢ１１を介して相互に接続されており、Ｆｉｒｅｗａｌｌ２３やＦｉｒｅｗａｌｌ３３を通じて、イントラネット２やイントラネット３とも接続されている。

【０００５】

セッション中継装置１０は、ＳｏｆｔＥｔｈｅｒ仮想ＨＵＢソフトウェアがインストールされたコンピュータである。セッション中継装置１０は、ＨＵＢ１１を介して、インターネット１内の各機器と接続されている。セッション中継装置１０は、ゲートウェイ装置２０とセッション中継装置１０の間で設定されるＳＳＬセッション内を流れるＥｔｈｅｒｎｅｔフレームを、ゲートウェイ装置３０とセッション中継装置１０の間で設定されるＳＳＬセッションに転送し、又、逆に、ゲートウェイ装置３０とセッション中継装置１０の間で設定されるＳＳＬセッション内を流れるＥｔｈｅｒｎｅｔフレームを、ゲートウェイ装置２０とセッション中継装置１０の間で設定されるＳＳＬセッションに転送する、セッション中継動作を行う。

【０００６】

ＨＵＢ１１は、セッション中継装置１０、Ｆｉｒｅｗａｌｌ２３、Ｆｉｒｅｗａｌｌ３３の各装置から入力されたＥｔｈｅｒｎｅｔフレームのＭＡＣ　ＤＡヘッダを参照し、適切な宛先ポート（適切な装置）に転送する、ブリッジ動作を行う。

【０００７】

イントラネット２は、ゲートウェイ装置２０、端末２１、ＨＵＢ２２、及びＦｉｒｅｗａｌｌ２３で構成され、これら機器の相互間で通信を行うローカルエリアネットワーク（ＬＡＮ）である。イントラネット２は、インターネット１と、Ｆｉｒｅｗａｌｌ２３を介して相互に接続されており、Ｆｉｒｅｗａｌｌ２３の動作により、インターネット１とイントラネット２の間の通信は、あらかじめ決められた設定に従って制限されている。

【０００８】

イントラネット２内の各装置は、ＨＵＢ２２を介して相互に接続されており、イントラネット２内の各装置間は、前述のＦｉｒｅｗａｌｌ２３等の制限を受けることなく、自由に通信を行うことができる。又、図においては、ゲートウェイ装置２０、ゲートウェイ装置３０、及びセッション中継装置１０により、イントラネット２とイントラネット３は、同一のＬＡＮとして動作するよう相互に接続されている為、イントラネット２内の各装置と、イントラネット３内の各装置間も、前述のＦｉｒｅｗａｌｌ２３等の制限を受けることなく、自由に通信を行うことができる。

【０００９】

ゲートウェイ装置２０は、ＳｏｆｔＥｔｈｅｒクラアントがインストールされたコンピュータである。ゲートウェイ装置２０は、ＨＵＢ２２を介して、イントラネット２内の各機器と接続されている。ゲートウェイ装置２０は、イントラネット２内を流れるＥｔｈｅｒｎｅｔフレームを、ゲートウェイ装置２０とセッション中継装置１０の間で設定されるＳＳＬセッション内に転送し、又、逆に、ゲートウェイ装置２０とセッション中継装置１０の間で設定されるＳＳＬセッション内を流れるＥｔｈｅｒｎｅｔフレームをイントラネット２内に転送する、ゲートウェイ動作を行う。

【００１０】

端末２１は、イントラネットの利用者が通常利用するコンピュータであり、イントラネット内の各機器（例えばサーバ３１）との間で通信を行う為のソフトウェア（例えば、インターネットブラウザやメーラー等）が動作する。端末２１は、ＨＵＢ２２を介してイン

トラネット２上の各機器と接続されている。

【００１１】

ＨＵＢ２２は、ＨＵＢ１１と同様に、ゲートウェイ装置２０、端末２１、Ｆｉｒｅｗａｌｌ２３の各装置から入力されたＥｔｈｅｒｎｅｔフレームのＭＡＣ　ＤＡヘッダを参照し、適切な宛先ポート（適切な装置）に転送する、ブリッジ動作を行う。

【００１２】

Ｆｉｒｅｗａｌｌ２３は、イントラネット２とインターネット１とを相互に接続するための機器であり、ＨＵＢ２２を介してイントラネット２上の各機器と接続され、ＨＵＢ１１を介してインターネット１上の各機器と接続されている。Ｆｉｒｅｗａｌｌ２３は、インターネット１とイントラネット２の間の通信を、予め決められた設定に従って制限する動作を行う。例えば、イントラネット２内部の装置からインターネット１の各装置へＴＣＰを用いて通信開始の要求をした場合、以降の通信は双方向で自由に行えるが、逆に、インターネット１の各装置からイントラネット２の各装置へＴＣＰを用いて通信開始の要求を行った場合、この要求は遮断され、以降の通信も双方向で遮断される。

【００１３】

イントラネット３は、ゲートウェイ３０、サーバ３１、ＨＵＢ３２、およびＦｉｒｅｗａｌｌ３３で構成され、これら機器の相互間で通信を行うローカルエリアネットワーク（ＬＡＮ）である。イントラネット３は、インターネット１と、Ｆｉｒｅｗａｌｌ３３を介して相互に接続されており、Ｆｉｒｅｗａｌｌ３３の動作により、インターネット１とイントラネット３の間の通信は、予め決められた設定に従って制限されている。

【００１４】

イントラネット３内の各装置は、ＨＵＢ３２を介して相互に接続されており、イントラネット３内の各装置間は、前述のＦｉｒｅｗａｌｌ３３等の制限を受けることなく、自由に通信を行うことができる。又、図１においては、ゲートウェイ装置２０、ゲートウェイ装置３０、及びセッション中継装置１０により、イントラネット２とイントラネット３は、同一のＬＡＮとして動作するよう相互に接続されている為、イントラネット３内の各装置と、イントラネット２内の各装置間も、前述のＦｉｒｅｗａｌｌ３３等の制限を受けることなく、自由に通信を行うことができる。

【００１５】

ゲートウェイ装置３０は、ゲートウェイ装置２０と同様の構成を有し、同様の動作を行うコンピュータである。図番号については、ゲートウェイ装置３０における３０００番台のものは、ゲートウェイ装置２０の２０００番台のものに、そのまま対応する。例えば、中間ドライバ３００６の構成および動作は、中間ドライバ２００６の構成および動作と同一である。ゲートウェイ装置３０は、ＳｏｆｔＥｔｈｅｒクラアントがインストールされ、ＨＵＢ３２を介して、イントラネット３内の各機器と接続されている。ゲートウェイ装置３０は、イントラネット３内を流れるＥｔｈｅｒｎｅｔフレームを、ゲートウェイ装置３０とセッション中継装置１０の間で設定されるＳＳＬセッション内に転送し、又、逆に、ゲートウェイ装置３０とセッション中継装置１０の間で設定されるＳＳＬセッション内を流れるＥｔｈｅｒｎｅｔフレームをイントラネット３内に転送する、ゲートウェイ動作を行う。

【００１６】

サーバ３１は、イントラネット内の端末からのアクセスを受けるコンピュータであり、イントラネット内の各端末（例えば端末２１）からの通信受け付ける為のソフトウェア（例えば、ＷＷＷサーバやＰＯＰサーバ等）が動作する。サーバ３１は、ＨＵＢ３２を介してイントラネット３上の各機器と接続されている。

【００１７】

ＨＵＢ３２は、ＨＵＢ１１やＨＵＢ２２と同様に、ゲートウェイ装置３０、サーバ３１、Ｆｉｒｅｗａｌｌ３３の各装置から入力されたＥｔｈｅｒｎｅｔフレームのＭＡＣ　ＤＡヘッダを参照し、適切な宛先ポート（適切な装置）に転送する等のブリッジ動作を行う。

【００１８】
Ｆｉｒｅｗａｌｌ３３は、イントラネット３とインターネット１とを相互に接続する為の機器であり、ＨＵＢ３２を介してイントラネット３上の各機器と接続され、ＨＵＢ１１を介してインターネット１上の各機器と接続されている。Ｆｉｒｅｗａｌｌ３３は、インターネット１とイントラネット３の間の通信を、予め決められた設定に従って制限する動作を行う。例えば、イントラネット３内部の装置からインターネット１の各装置へＴＣＰを用いて通信開始の要求をした場合、以降の通信は双方向で自由に行えるが、逆にインターネット１の各装置からイントラネット３の各装置へＴＣＰを用いて通信開始の要求を行った場合、この要求は遮断され、以降の通信も双方向で遮断される。

【００１９】
図２は、図１に示すネットワークにおいて、イントラネット２内（例えば端末２１とゲートウェイ装置２０の間）、及びイントラネット３内（例えば、サーバ３１とゲートウェイ装置３０の間）で送受信される、ＥｔｈｅｒｎｅｔフレームＦ２０のフレームフォーマットを示すブロック図である。

【００２０】
ＬＡＮ　ＭＡＣ　Ｆ２１は、イントラネット２、若しくはイントラネット３上で、レイヤ２（イーサネット：登録商標）での通信を行う為に必要なヘッダ（ＭＡＣ　ＤＡ、ＭＡＣ　ＳＡ、Ｅｔｈｅｒｎｅｔ　ＴＹＰＥ他ＩＥＥＥ８０２に規定のヘッダ）を示している。

【００２１】
ＬＡＮ　ＩＰ　Ｆ２２は、イントラネット２、若しくはイントラネット３上で、レイヤ３（ＩＰ）での通信を行う為に必要なヘッダ（ＩＰ　ＤＡ、ＩＰ　ＳＡ、ＩＰ　ＴＹＰＥ、他ＩＥＴＦに規定のヘッダ）を示している。

【００２２】
ＬＡＮ　ＴＣＰ　Ｆ２３は、イントラネット２、若しくはイントラネット３内に存在する各機器の間で、ＴＣＰによる通信を行うために必要なヘッダ（ポート番号やシーケンスナンバー等のＴＣＰヘッダ）を示している。

【００２３】
ＬＡＮ　ＤＡＴＡ　Ｆ２４は、イントラネット２、若しくはイントラネット３内に存在する各機器で動作するソフトウェアの間で交換されるデータである。

【００２４】
図３は、図１に示すネットワークにおいて、ゲートウェイ装置２０とセッション中継装置１０の間、及びゲートウェイ装置３０とセッション中継装置１０の間で送受信される、Ｅｔｈｅｒｎｅｔ　ｏｖｅｒ　ＳＳＬフレームＦ１０のフレームフォーマットを示すブロック図である。

【００２５】
ＩＮＥＴ　ＭＡＣ　Ｆ１１は、イントラネット２、若しくはイントラネット３とインターネット１との間で行われる通信（例えば、ゲートウェイ装置２０とセッション中継装置１０の間の通信）において、レイヤ２（イーサネット）での通信を行う為に必要なヘッダ（ＭＡＣ　ＤＡ、ＭＡＣ　ＳＡ、Ｅｔｈｅｒｎｅｔ　ＴＹＰＥ他ＩＥＥＥ８０２に規定のヘッダ）を示している。

【００２６】
ＩＮＥＴ　ＩＰ　Ｆ１２は、イントラネット２、若しくはイントラネット３とインターネット１との間で行われる通信（例えば、ゲートウェイ装置２０とセッション中継装置１０の間の通信）において、レイヤ３（ＩＰ）での通信を行う為に必要なヘッダ（ＩＰ　ＤＡ、ＩＰ　ＳＡ、ＩＰ　ＴＹＰＥ、他ＩＥＴＦに規定のヘッダ）を示している。

【００２７】
ＩＮＥＴ　ＴＣＰ　Ｆ１３は、イントラネット２、若しくはイントラネット３とインターネット１との間で行われる通信（例えば、ゲートウェイ装置２０とセッション中継装置１０の間の通信）において、ＴＣＰによる通信を行う為に必要なヘッダ（ポート番号やシ

ーケンスナンバー等のＴＣＰヘッダ）を示している。

【００２８】

ＩＮＥＴ　ＳＳＬ　Ｅｎｃｒｙｐｔｅｄ　ＤＡＴＡ　Ｆ１４は、イントラネット２、若しくはイントラネット３とインターネット１との間で行われる通信（例えば、ゲートウェイ装置２０とセッション中継装置１０の間の通信）において、各機器（例えば、ゲートウェイ装置２０やセッション中継装置１０）で動作するソフトウェアの間で交換されるデータである。このデータは暗号化されており、途中経路にある機器は、通常用いられる方法では、暗号を復号して内容を解読することができない。

【００２９】

図１に示す構成では、ＩＮＥＴ　ＳＳＬ　Ｅｎｃｒｙｐｔｅｄ　ＤＡＴＡ　Ｆ１４には、イントラネット２やイントラネット３上を流れるＥｔｈｅｒｎｅｔフレームＦ２０が格納される。

【００３０】

［従来技術１の動作例］

図１を用いて、端末２１からサーバ３１への通信（フレーム転送）を行う場合を例に、従来技術１の動作について説明する。

【００３１】

ここでは、サーバ３１と端末２１との間では、すでに何度か通信が行われており、ＨＵＢ２２やＨＵＢ３２がすでに端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ２３のＬＡＮ側，Ｆｉｒｅｗａｌｌ３３のＬＡＮ側、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。又、ＨＵＢ１１は、Ｆｉｒｅｗａｌｌ２３のＷＡＮ側、Ｆｉｒｅｗａｌｌ３３のＷＡＮ側、セッション中継装置１０の各装置のＭＡＣアドレスを学習しているものとする。更に、ゲートウェイ装置２０からセッション中継装置１０へのＳＳＬセッション（セキュアＴＣＰセッション）が既に設定されており、同様にゲートウェイ装置３０からセッション中継装置１０へのＳＳＬセッション（セキュアＴＣＰセッション）も、既に設定されているものとする。又、Ｆｉｒｅｗａｌｌ２３およびＦｉｒｅｗａｌｌ３３は、イントラネット内部の装置（ＬＡＮ側）からインターネットの各装置（ＷＡＮ側）へＴＣＰを用いて通信開始の要求をした場合、以降の通信は双方向で自由に行えるが、逆にインターネットの各装置（ＷＡＮ側）からイントラネットの各装置（ＬＡＮ側）へＴＣＰを用いて通信開始の要求を行った場合、この要求は遮断され、以降の通信も双方向で遮断されるとする。

【００３２】

先ず、端末２１からサーバ３１宛のフレームを送信する。このフレームはＥｔｈｅｒｎｅｔフレームＦ２０のフォーマットを有し、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスが設定される。又、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定される。

【００３３】

ＨＵＢ２２は、端末２１からのフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームをそのままゲートウェイ装置２０側のポートに出力する。

【００３４】

ゲートウェイ装置２０は、ＨＵＢ２２からフレームを受信すると、このフレームを、予めセッション中継装置１０との間で設定しているＳＳＬセッションに流す。つまり、Ｆ２０のフォーマットでゲートウェイ装置２０に入力されたフレームは、暗号化された上でＦ１４の領域に格納され、Ｅｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームＦ１０のフォーマットで、ゲートウェイ装置２０からＨＵＢ２２に転送される。

【００３５】

この時、ＩＮＥＴ　ＭＡＣ　Ｆ１１内のＭＡＣ　ＤＡにはＦｉｒｅｗａｌｌ２３のＬＡ

Ｎ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはゲートウェイ装置２０のＭＡＣアドレスが設定される。又、ＩＮＥＴ　ＩＰ　Ｆ１２内のＩＰ　ＤＡにはセッション中継装置１０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡにはゲートウェイ装置２０のＩＰアドレスが設定される。Ｆ２１～Ｆ２４の内容には変化がない。

【００３６】

ＨＵＢ２２は、ゲートウェイ装置２２からのフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ２３のＬＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームをそのままＦｉｒｅｗａｌｌ２３側のポートに出力する。

【００３７】

Ｆｉｒｅｗａｌｌ２３は、ＨＵＢ２２からのフレームを受信すると、Ｆ１２内のＩＰ　ＤＡを参照し、ＩＰ　ＤＡがインターネット１側に存在するものであることから、Ｆ１１内のＭＡＣ　ＤＡをセッション中継装置１０のＭＡＣアドレスに書き換え、更にＦ１１内のＭＡＣ　ＳＡをＦｉｒｅｗａｌｌ２３のＷＡＮ側のＭＡＣアドレスに書き換えて、Ｆ１０のフレームフォーマットのまま、ＨＵＢ１１に転送する。Ｆ２１～Ｆ２４の内容には変化がない。

【００３８】

ＨＵＢ１１は、Ｆｉｒｅｗａｌｌ２３からのフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがセッション中継装置１０のものであることから、過去のルーティング学習結果に基づき、このフレームをそのままセッション中継装置１０側のポートに出力する。

【００３９】

セッション中継装置１０は、ＨＵＢ１１からフレームを受信すると、Ｆ１４の暗号化を一旦解除し、Ｆ２１内のＭＡＣ　ＤＡを参照して、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを予めゲートウェイ装置３０との間で設定しているＳＳＬセッションに流す。つまり、Ｆ１０のフォーマットでセッション中継装置１０に入力されたフレームは、暗号化を解除されてＦ２０のフォーマットになり、再び暗号化にされて、Ｆ１０のフォーマットにおけるＦ１４の領域に格納され、Ｆ１０のフォーマットで、セッション中継装置１０からＨＵＢ１１に転送される。

【００４０】

この時、ＩＮＥＴ　ＭＡＣ　Ｆ１１内のＭＡＣ　ＤＡにはＦｉｒｅｗａｌｌ３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはセッション中継装置１０のＭＡＣアドレスが設定される。又、ＩＮＥＴ　ＩＰ　Ｆ１２内のＩＰ　ＤＡにはゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡにはセッション中継装置１０のＩＰアドレスが設定される。Ｆ２１～Ｆ２４の内容には変化がない。

【００４１】

ＨＵＢ１１は、セッション中継装置１０からのフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＷＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームをそのままＦｉｒｅｗａｌｌ３３側のポートに出力する。

【００４２】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ１１からのフレームを受信すると、Ｆ１２内のＩＰ　ＤＡを参照し、ＩＰ　ＤＡがイントラネット３側に存在するものであることから、Ｆ１１内のＭＡＣ　ＤＡをゲートウェイ装置３０のＭＡＣアドレスに書き換え、更にＦ１１内のＭＡＣ　ＳＡをＦｉｒｅｗａｌｌ３３のＬＡＮ側のＭＡＣアドレスに書き換えて、Ｆ１０のフレームフォーマットのまま、ＨＵＢ３２に転送する。Ｆ２１～Ｆ２４の内容には変化がない。

【００４３】

ＨＵＢ３２は、Ｆｉｒｅｗａｌｌ３３からのフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがゲートウェイ装置３０のものであることから、過去のル

ーティング学習結果に基づき、このフレームをそのままゲートウェイ装置３０側のポートに出力する。

【００４４】

ゲートウェイ装置３０は、ＨＵＢ３２からＦ１０のフォーマットでフレームを受信すると、Ｆ１４の暗号化を解除してＦ１４に格納されているＥｔｈｅｒｎｅｔフレームＦ２０を取り出し、このフレームをＦ２０のフォーマットでＨＵＢ３２に転送する。

【００４５】

このフレームは、端末２１から送信された時の状態そのままに保たれており、ＬＡＮ ＭＡＣ Ｆ２１内のＭＡＣ ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ ＭＡＣ Ｆ２１内のＭＡＣ ＳＡには端末２１のＭＡＣアドレスが設定されている。又、ＬＡＮ ＩＰ Ｆ２２内のＩＰ ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ ＩＰ Ｆ２２内のＩＰ ＳＡには、端末２１のＩＰアドレスが設定されている。

【００４６】

ＨＵＢ３２は、ゲートウェイ装置３０からのフレームを受信すると、Ｆ２１内のＭＡＣ ＤＡを参照し、ＭＡＣ ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームをそのままサーバ３１側のポートに出力する。

【００４７】

サーバ３１は、ＨＵＢ３２から送信されたフレームを受信し、端末２１からサーバ３１への一連のフレーム転送が完了する。

【００４８】

サーバ３１から端末２１へのフレーム転送も、上記の逆の経路をたどることで、同様に実現される。

【００４９】

以上のようにして、従来技術１を用いると、端末２１とサーバ３１は、あたかも同一ＬＡＮ上に存在しているかのように、Ｆｉｒｅｗａｌｌ等による制限を受けることなく通信できる。

【００５０】

続いて従来技術２について説明する。

従来、コンピュータの内部に搭載されるＣＰＵ（Ｃｅｎｔｒａｌ ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ：中央演算装置）において、セキュリティエンジンと呼ばれる暗号化／復号化機能を付加したものが知られている（非特許文献２）。

【００５１】

図４は、従来技術２のコンピュータへの適用例を示すブロック図である。

【００５２】

従来技術２は、図１に示す従来技術１において、ゲートウェイ装置２０、ゲートウェイ装置３０、若しくはセッション中継装置１０に対して適用することができる。

【００５３】

図４においては、セキュリティエンジンと呼ばれる暗号化／復号化を行うハードウェアが、ＰＣＩバス等の高速なインタフェースでＣＰＵと接続されている。このセキュリティエンジンにより、従来技術１における暗号化および復号化の動作をハードウェアにより処理することで、従来のソフトウェア処理に比べて高速な暗号化および復号化を実現できる。

【非特許文献１】「ＳｏｆｔＥｔｈｅｒ．ｃｏｍ － ＳｏｆｔＥｔｈｅｒ仮想イーサネットシステム － ＳｏｆｔＥｔｈｅｒ ＶＰＮ Ｓｙｓｔｅｍ」［平成１６年１２月６日検索］、インターネット＜ＵＲＬ：ｈｔｔｐ：／／ｗｗｗ．ｓｏｆｔｅｔｈｅｒ．ｃｏｍ／ｊｐ／＞

【非特許文献２】「ＭＰＣ８７５ Ｐｒｏｄｕｃｔ Ｓｕｍｍａｒｙ Ｐａｇｅ」［平成１６年１２月６日検索］、インターネット＜ＵＲＬ：ｈｔｔｐ：／／ｗｗｗ．ｆｒｅｅｓｃａｌｅ．ｃｏｍ／ｗｅｂａｐｐｓ／ｓｐｓ／ｓｉｔｅ／ｐｒｏｄ＿ｓｕｍｍａｒｙ．ｊｓｐ？ｃｏｄｅ＝ＭＰＣ８７５＞

【発明の開示】

【００５４】

図１～図３に示す従来技術１においては、ゲートウェイ装置で行われる、ＳＳＬセッション内にＥｔｈｅｒｎｅｔフレームを流してＥｔｈｅｒｎｅｔフレームＦ２０からＥｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームＦ１０を作るカプセル化と呼ばれる処理をＣＰＵにおいてソフトウェアで行っている為、フレームの高速転送ができない問題が有った。そして、上記処理をそのまま単純にハードウェア化すると、ＴＣＰ　Ｏｆｆｌｏａｄ　Ｅｎｇｉｎｅ（ＴＯＥ）等の大がかりな仕組みが必要になる為、回路規模、コスト共に増大してしまう問題も有る。

【００５５】

更に、従来技術１では、カプセル化に加えて、ＳＳＬにおける暗号化／復号化処理もＣＰＵにおいてソフトウェアで行っている為、この点でもフレームの高速転送ができない問題があった。

【００５６】

又、従来技術１では、イントラネット内のフレームをＳＳＬセッションに流した場合、Ｆ１０に示すフレームフォーマットになる。このフォーマットにおいては、Ｆ１３およびＦ２３の双方にＴＣＰヘッダが存在していることからわかる通り、１フレームの転送に際してＴＣＰ処理が２重に行われる「ＴＣＰ　ｏｖｅｒ　ＴＣＰ」という状態になる。そして、ＴＣＰ　ｏｖｅｒ　ＴＣＰでは、ＴＣＰの輻輳制御が２重に行われてしまう為、転送性能が劣化して高速転送できない問題が発生することが知られている。（非特許文献３）

【非特許文献３】「Ｗｈｙ　ＴＣＰ　Ｏｖｅｒ　ＴＣＰ　Ｉｓ　Ａ　Ｂａｄ　Ｉｄｅａ」［平成１６年１２月６日検索］、インターネット＜ＵＲＬ：ｈｔｔｐ：／／ｓｉｔｅｓ．ｉｎｋａ．ｄｅ／ｓｉｔｅｓ／ｂｉｇｒｅｄ／ｄｅｖｅｌ／ｔｃｐ－ｔｃｐ．ｈｔｍｌ＞

【００５７】

図４に示す従来技術２では、従来技術１におけるＳＳＬの暗号化処理は、ハードウェアにより高速処理できるが、カプセル化処理はハードウェア化できず、未だＣＰＵにおいてソフトウェアで行う為、依然としてフレームの高速転送が出来ない問題が有った。

【００５８】

又、従来技術１で発生しているＴＣＰ　ｏｖｅｒ　ＴＣＰ問題も、従来技術２では依然として残ったままとなる。

【００５９】

そして、カプセル化を行うハードウェアを、セキュリティエンジンとは別に付加した場合、セキュリティエンジンとは別にカプセル化用のハードウェアを用意する必要があり、暗号化／復号化とカプセル化を同一ハードウェア上で行った場合と比べて、高速化の為に要するコストが多くかかる問題が有った。

【００６０】

更に、このような暗号化／復号化を行うハードウェアは、高速なバスを介してＣＰＵと接続する必要があるが、高速バスのインタフェースを持たせると、開発コストやハードウェアの部材コストが、低速なバスに比べて多くかかる問題が有った。

【００６１】

従って、本発明が解決しようとする課題は、コストを抑えながらフレームの高速転送を可能とするトンネリング通信装置、トンネリング通信システム、トンネリング通信方法およびトンネリング通信プログラムを提供することである。

【００６２】

上記課題を解決するための第１の発明は、

通信システムであって、

ＴＣＰセッションを確立させて通信する通信装置間に、ＴＣＰのセッションを終端させる終端手段を設け、

前記終端手段は、前記通信装置の送信側から送信されるＴＣＰパケット（ＳＹＮ）を受

信し、このＴＣＰパケットの応答パケット（ＳＹＮ＋ＡＣＫ）を送信側に送信し、独自の接続要求を前記通信装置の受信側に送信するように構成されていることを特徴とする。

【００６３】

上記課題を解決するための第２の発明は、上記第１の発明において、

前記終端手段は、前記通信装置の送信側から送信される独自の接続要求を受信し、前記通信装置の受信側にＴＣＰパケット（ＳＹＮ）を送信するように構成されていることを特徴とする。

【００６４】

上記課題を解決するための第３の発明は、上記第１又は第２の発明において、

前記終端手段は、前記通信装置の受信側から送信されるＴＣＰパケットの応答パケット（ＳＹＮ＋ＡＣＫ）を受信し、この応答パケットの受信確認パケットを受信側に送信し、独自の接続完了通知を前記通信装置の送信側に送信するように構成されていることを特徴とする。

【００６５】

上記課題を解決するための第４の発明は、上記第１から第３のいずれかの発明において、

前記終端手段は、前記接続要求又は前記接続完了通知を、輻輳制御がない通信方法を用いて通信するように構成されていることを特徴とする。

【００６６】

上記課題を解決するための第５の発明は、上記第１から第４のいずれかの発明において、

前記通信装置間に、

前記通信装置間で暗号化通信する際の暗号鍵を取得する暗号鍵取得手段と、

前記取得した暗号鍵を保存し、高速化処理開始命令を受信すると、この保存した暗号鍵を用いて前記通信装置間で送受信されるデータの暗号化又は復号化を行う暗号化手段と

を有することを特徴とする。

【００６７】

上記課題を解決するための第６の発明は、上記第１から第５のいずれかの発明において、

前記通信装置の送信側と受信側とは互いに異なるネットワーク上に構成され、ファイアーウォールを介して通信する構成の場合、前記終端手段は各ネットワークに構成されていることを特徴とする。

【００６８】

上記課題を解決するための第７の発明は、

通信システムであって、

暗号化通信する通信装置間に

前記通信装置間で暗号化通信する際の暗号鍵を取得する暗号鍵取得手段と、

前記取得した暗号鍵を保存し、高速化処理開始命令を受信すると、この保存した暗号鍵を用いて前記通信装置間で送受信されるデータの暗号化又は復号化を行う暗号化手段と

を有することを特徴とする。

【００６９】

上記課題を解決するための第８の発明は、上記第５から第７の発明において、

前記暗号化手段は、フラグメント分割されたデータを暗号化し、フラグメント解除前のデータを復号化するように構成されていることを特徴とする。

【００７０】

上記課題を解決するための第９の発明は、

通信装置であって、

ＴＣＰセッション確立する際にＴＣＰパケットを送信するＴＣＰ手段と、

前記ＴＣＰパケット（ＳＹＮ）を受信し、このＴＣＰパケットの応答パケット（ＳＹＮ＋ＡＣＫ）を前記ＴＣＰ部に送信し、独自の接続要求を接続先に送信する終端手段と

を有することを特徴とする。

【００７１】

上記課題を解決するための第１０の発明は、上記第９の発明において、

前記終端手段は、独自の接続要求を受信した場合、前記ＴＣＰ手段にＴＣＰパケット（ＳＹＮ）を送信するように構成されていることを特徴とする。

【００７２】

上記課題を解決するための第１１の発明は、上記第９又は第１０の発明において、

前記終端手段は、ＴＣＰパケットの応答パケット（ＳＹＮ＋ＡＣＫ）を前記ＴＣＰ手段から受信した場合、この応答パケットの受信確認パケットを前記ＴＣＰ手段に送信し、独自の接続完了通知を接続先に送信するように構成されていることを特徴とする。

【００７３】

上記課題を解決するための第１２の発明は、上記第９から第１１のいずれかの発明において、

前記終端手段は、前記接続要求又は前記接続完了通知を、輻輳制御がない通信方法を用いて送受信するように構成されていることを特徴とする。

【００７４】

上記課題を解決するための第１３の発明は、上記第９から第１２のいずれか発明において、

暗号化通信する際の暗号鍵を取得する暗号鍵取得手段と、

前記取得した暗号鍵を保存し、高速化処理開始命令を受信後、この保存した暗号鍵を用いて前記通信装置間で送受信されるデータの暗号化又は復号化を行う暗号化手段と

を有することを特徴とする。

【００７５】

上記課題を解決するための第１４の発明は、

暗号化通信する通信装置であって、

暗号鍵を取得する暗号鍵取得手段と、

前記取得した暗号鍵を保存し、高速化処理開始命令を受信すると、この保存した暗号鍵を用いて前記データの暗号化又は復号化を行う暗号化手段と

を有することを特徴とする。

【００７６】

上記課題を解決するための第１５の発明は、上記第１３又は第１４の発明において、

前記暗号化手段は、フラグメント分割されたデータを暗号化し、フラグメント解除前のデータを復号化するように構成されていることを特徴とする。

【００７７】

上記課題を解決するための第１６の発明は、

通信方法であって、

ＴＣＰパケット（ＳＹＮ）を受信するＴＣＰ受信ステップと、

前記受信したＴＣＰパケットの応答パケット（ＳＹＮ＋ＡＣＫ）を送信する応答パケット送信ステップと、

独自の接続要求を送信する接続要求送信ステップと

を有することを特徴とする。

【００７８】

上記課題を解決するための第１７の発明は、上記第１６の発明において、

前記送信された接続要求を受信する接続要求受信ステップと、

前記接続要求受信後にＴＣＰパケット（ＳＹＮ）を送信するステップと

を有することを特徴とする。

【００７９】

上記課題を解決するための第１８の発明は、上記第１６又はの第１７の発明において、

前記送信されたＴＣＰパケットの応答パケット（ＳＹＮ＋ＡＣＫ）を受信する応答パケット受信ステップと、

前記応答パケットの受信確認パケットを送信する受信確認送信ステップと、
前記受信確認パケットを送信後、独自の接続完了通知を送信する接続完了通知送信ステップと
を有することをを特徴とする。

【００８０】
上記課題を解決するための第１９の発明は、上記第１６から第１８のいずれかの発明において、
前記接続要求送信ステップと前記接続完了通知送信ステップは、輻輳制御がない通信方法を用いて前記接続要求又は前記接続完了通知を送信することを特徴とする。

【００８１】
上記課題を解決するための第２０の発明は、上記第１６から第１９のいずれかの発明において、
暗号化通信する際の暗号鍵を取得する暗号鍵取得ステップと、
高速化処理開始命令を受信するステップと、
前記取得した暗号鍵を保存し、この保存した暗号鍵を用いて前記通信装置間で送受信されるデータの暗号化又は復号化を行う暗号化ステップと
を有することを特徴とする。

【００８２】
上記課題を解決するための第２１の発明は、
暗号化通信を用いて通信する方法であって、
暗号化通信する際の暗号鍵を取得する暗号鍵取得ステップと、
高速化処理開始命令を受信するステップと、
前記取得した暗号鍵を保存し、この保存した暗号鍵を用いて前記通信装置間で送受信されるデータの暗号化又は復号化を行う暗号化ステップと
を有することを特徴とする。

【００８３】
上記課題を解決するための第２２の発明は、上記第２１の発明において、
前記暗号化ステップは、
フラグメント分割されたデータを暗号化するステップと、
フラグメント解除前のデータを復号化するステップと
を有することを特徴とする。

【００８４】
上記課題を解決するための第２３の発明は、
情報処理装置のプログラムであって、前記プログラムは前記情報処理装置を、
ＴＣＰセッション確立する際にＴＣＰパケットを送信するＴＣＰ手段と、
前記ＴＣＰパケット（ＳＹＮ）を受信し、このＴＣＰパケットの応答パケット（ＳＹＮ＋ＡＣＫ）を前記ＴＣＰ部に送信し、独自の接続要求を接続先に送信する終端手段として機能させることを特徴とする。

【００８５】
上記課題を解決するための第２４の発明は、上記第２３の発明において、
前記終端手段は、独自の接続要求を受信した場合、前記ＴＣＰ手段にＴＣＰパケット（ＳＹＮ）を送信する手段として機能させることを特徴とする。

【００８６】
上記課題を解決するための第２５の発明は、上記第２３又は第２４の発明において、
前記終端手段は、ＴＣＰパケットの応答パケット（ＳＹＮ＋ＡＣＫ）を前記ＴＣＰ手段から受信した場合、この応答パケットの受信確認パケットを前記ＴＣＰ手段に送信し、独自の接続完了通知を接続先に送信する手段として機能させることを特徴とする。

【００８７】
上記課題を解決するための第２６の発明は、上記第２３から第２５のいずれかの発明において、

前記終端手段は、前記接続要求又は前記接続完了通知を、輻輳制御がない通信方法を用いて送受信する手段として機能させることを特徴とする。

【００８８】

本発明のゲートウェイ装置およびセッション中継装置は、ＳＳＬセッションの確立と高速化エンジンへの公開鍵、秘密鍵および共通鍵の配布を行う高速化エンジン制御と、ＴＣＰの処理を終端し、又、高速化エンジンの制御を行うための制御フレーム生成する中間ドライバと、ハードウェアにより暗号化、復号化、およびカプセル化処理を行う高速化エンジンとを備え、ＳＳＬセッション確立後のフレーム転送をハードウェアで処理するよう動作する。このような構成を採用し、ＣＰＵ（ソフトウェア処理）によるカプセル化処理および暗号化／復号化処理を高速化エンジン（ハードウェア）で実現して高速化することにより、上記の課題が解決される。

【００８９】

本発明のゲートウェイ装置は、ＳＳＬセッションの確立と中間ドライバへのセッション情報の通知を行うゲートウェイアプリケーションと、ＴＣＰを終端して輻輳制御の掛からないフレームを作成する中間ドライバを備え、ヘッダＦ１３の位置のＴＣＰによる輻輳制御と再送制御が発生しないよう動作する。このような構成を採用し、ＴＣＰ　ｏｖｅｒ　ＴＣＰ問題の発生を回避して高速化することにより、上記の課題が解決される。

【００９０】

本発明の端末およびサーバは、ＴＣＰを終端して輻輳制御のかからないフレームを作成する中間ドライバを備え、ヘッダＦ２３の位置のＴＣＰによる輻輳制御と再送制御が発生しないよう動作する。このような構成を採用し、ＴＣＰ　ｏｖｅｒ　ＴＣＰ問題の発生を回避して高速化することにより、上記の課題が解決される。

【００９１】

本発明のゲートウェイ装置は、中間ドライバからの要求に基づいてＴＣＰセッションの確立を行うカプセル化処理を備え、本発明の端末は、ＴＣＰを終端しまた前記カプセル化処理にＴＣＰセッション構築の要求を行う中間ドライバを備え、ヘッダＦ２３の位置のＴＣＰによる輻輳制御と再送制御が発生しないよう中間ドライバでＴＣＰを終端し、カプセル化処理よりＴＣＰセッションを再構築するよう動作する。このような構成を採用し、ＴＣＰ　ｏｖｅｒ　ＴＣＰ問題の発生を回避して高速化することにより、上記の課題が解決される。

【００９２】

本発明のゲートウェイ装置は、中間ドライバからの要求に基づいてＴＣＰセッションの確立を行うカプセル化処理と、中間ドライバからの要求に基づいてＩＰアドレスおよびＭＡＣアドレスを書き換えるＩＰスタックとを備え、本発明の端末は、ＴＣＰを終端しまた前記カプセル化処理にＴＣＰセッション構築の要求を行う中間ドライバを備え、ヘッダＦ２３の位置のＴＣＰによる輻輳制御と再送制御が発生しないよう中間ドライバでＴＣＰを終端し、カプセル化処理よりＴＣＰセッションを再構築するよう動作する。このような構成を採用し、ＴＣＰ　ｏｖｅｒ　ＴＣＰ問題の発生を回避して高速化することにより、上記の課題が解決される。

【００９３】

本発明のゲートウェイ装置およびセッション中継装置は、ＳＳＬセッションの確立と高速化エンジンへの公開鍵、秘密鍵および共通鍵の配布を行うゲートウェイアプリケーションと、ハードウェアにより暗号化、復号化、およびカプセル化処理を行う高速化エンジンとを備え、ＳＳＬセッション確立後の暗号化と復号化をハードウェアで処理するよう動作する。このような構成を採用し、ＣＰＵ（ソフトウェア処理）による暗号化／復号化処理を高速化エンジン（ハードウェア）で実現して高速化することにより、上記の課題が解決される。

【００９４】

本発明のゲートウェイ装置は、ＳＳＬセッションの確立と高速化エンジンや中間ドライバへの公開鍵、秘密鍵および共通鍵の配布を行うゲートウェイアプリケーションと、ＴＣ

Ｐを終端する中間ドライバと、ハードウェアにより暗号化／復号化処理を行う高速化エンジンとを備え、ＳＳＬセッション確立後の暗号化／復号化をハードウェアで処理するよう動作する。このような構成を採用し、ＣＰＵ（ソフトウェア処理）による暗号化／復号化処理を高速化エンジン（ハードウェア）で実現して高速化することにより、上記の課題が解決される。

【図面の簡単な説明】

【００９５】

【図１】従来技術１のネットワーク構成例を示すブロック図である。

【図２】従来技術１のＥｔｈｅｒｎｅｔフレームフォーマット Ｆ２０の構成を示すブロック図である。

【図３】従来技術１のＥｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームフォーマット Ｆ１０の構成を示すブロック図である。

【図４】従来技術２のコンピュータへの適用例を示すブロック図である。

【図５】本発明の第１の実施の形態のセッション中継装置１０の構成を示すブロック図である。

【図６】本発明の第１の実施の形態におけるＣＰＵ１００内のソフトウェア構成を示すブロック図である。

【図７】本発明の第１の実施の形態における中間ドライバ１００８の構成を示すブロック図である。

【図８】本発明の第１の実施の形態におけるＮＩＣ１０１の構成を示すブロック図である。

【図９】本発明の第１の実施の形態におけるＨＵＢ１１の構成を示すブロック図である。

【図１０】本発明の第１の実施の形態におけるＣＰＵ２００内のソフトウェア構成を示すブロック図である。

【図１１】本発明の第１の実施の形態におけるＮＩＣ２０１の構成を示すブロック図である。

【図１２】本発明の第１の実施の形態における高速化エンジン２０１４の構成を示すブロック図である。

【図１３】本発明の第１の実施の形態におけるＣＰＵ２１０内のソフトウェア構成を示すブロック図である。

【図１４】本発明の第１の実施の形態におけるＦｉｒｅｗａｌｌ２３の構成を示すブロック図である。

【図１５】本発明の第１の実施の形態におけるＣＰＵ２３０内のソフトウェア構成を示すブロック図である。

【図１６】本発明の第１の実施の形態におけるネットワーク構成および通信経路を示すブロック図である。

【図１７】本発明の第２の実施の形態におけるネットワーク構成例を示すブロック図

【図１８】本発明の第２の実施の形態におけるネットワーク構成および通信経路を示すブロック図である。

【図１９】本発明の第３の実施の形態におけるネットワーク構成および通信経路を示すブロック図である。

【図２０】本発明の第４の実施の形態におけるネットワーク構成および通信経路を示すブロック図である。

【図２１】本発明の第５の実施の形態におけるネットワーク構成および通信経路を示すブロック図である。

【図２２】本発明の第６の実施の形態におけるネットワーク構成および通信経路を示すブロック図である。

【図２３】本発明の第７の実施の形態におけるネットワーク構成および通信経路を示すブロック図である。

【図２４】本発明の第８の実施の形態におけるネットワーク構成および通信経路を示すブ

ロック図である。
【図２５】本発明の第８の実施の形態における高速化エンジンＸ２０１４の構成を示すブロック図である。
【図２６】本発明の第９の実施の形態におけるネットワーク構成および通信経路を示すブロック図である。
【図２７】本発明の第９の実施の形態における高速化エンジＹ２０１４の構成を示すブロック図である。
【図２８】本発明の第９の実施の形態における中間ドライバＹ３００６の構成を示すブロック図である。
【図２９】本発明の第１０の実施の形態におけるネットワーク構成および通信経路を示すブロック図である。
【図３０】本発明の第１１の実施の形態におけるネットワーク構成および通信経路を示すブロック図である。
【図３１】本発明の第１２の実施の形態における中間ドライバ１００８の構成を示すブロック図である。
【図３２】本発明の第１２の実施の形態における高速化エンジン２０１４の構成を示すブロック図である。
【図３３】本発明の特徴を説明するための図である。
【発明を実施するための最良の形態】
【００９６】
［第１の実施の形態］
本発明の第１の実施の形態は、図３３に示すように、ＳＳＬセッションを確立させる際、セッション中継装置１０内のＣＰＵ１００のＴＣＰと中間ドライバのＴＣＰとの間でＴＣＰセッションを確立させ、更にゲートウェイ装置２０のＴＣＰと中間ドライバのＴＣＰとの間でＴＣＰセッションを確立させ、セッション中継装置１０とゲートウェイ装置２０との間でＴＣＰにおける輻輳制御を行わないようにしている。同様に、セッション中継装置１０内のＣＰＵ１００のＴＣＰと中間ドライバのＴＣＰとの間でＴＣＰセッションを確立させ、更にゲートウェイ装置３０内のＣＰＵ２００のＴＣＰと中間ドライバのＴＣＰとの間でＴＣＰセッションを確立させ、セッション中継装置１０とゲートウェイ装置２０との間でＴＣＰにおける輻輳制御を行わないようにしている。また、同様に、ゲートウェイ装置１０内のＣＰＵのＴＣＰと中間ドライバのＴＣＰとの間でＴＣＰセッションを確立させ、セッション中継装置１０とゲートウェイ装置１０との間でＴＣＰにおける輻輳制御を行わないようにしている。尚、本発明において、ＣＰＵ内のＴＣＰと中間ドライバのＴＣＰとの間でＴＣＰセッションを確立させることをＴＣＰのセッションを終端させるという。
更に、ゲートウェイ装置２０内のＮＩＣ（Network Interface Card）２０１に高速化エンジンを備えている。これらにより、ゲートウェイ装置２０におけるカプセル化処理や、暗号化／復号化処理を高速化する他、ＴＣＰ ｏｖｅｒ ＴＣＰ問題を回避し、更に、暗号化／復号化処理とカプセル化処理を同一箇所で実現し、又、ＮＩＣ内の比較的安価なインタフェース上に実装することで、低価格化を実現する。
【００９７】
第１の実施の形態のネットワーク構成は、図１に示す従来技術１と同様である。
【００９８】
しかしながら、ゲートウェイ装置２０と、セッション中継装置１０の内部構成が、従来技術に対して異なっている。
【００９９】
［構成の説明］
図５は、第１の実施の形態におけるセッション中継装置１０の構成を詳細に示したブロック図である。

【０１００】
セッション中継装置１０は、ＣＰＵ１００と、ＮＩＣ１０１と、メモリ１０２と、ＨＤＤ１０３と、キーボード１０４と、マウス１０５と、グラフィック１０６により構成される。

【０１０１】
ＣＰＵ１００は、中央演算装置と呼ばれ、ＨＤＤ１０３に記録されているソフトウェア（プログラム）を読み込み、メモリ１０２を用いてプログラムに記載された処理を実行するハードウェアである。この処理に際しては、キーボード１０４や、マウス１０５から、ユーザによる命令を受ける他、結果をグラフィック１０６に出力することがある。又、ＮＩＣ１０１からデータを受信し、若しくはＮＩＣ１０１に対してデータを出力することもある。

【０１０２】
ＮＩＣ１０１は、ネットワークインタフェースカード（Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）と呼ばれ、イーサネット等のネットワーク用ケーブルを接続する為に、コンピュータに挿入するハードウェアである。ネットワーク（イーサネットケーブル等のケーブル）からフレーム（データ）を受信し、バス等のインタフェースを経由してＣＰＵ１００に送る他、逆に、ＣＰＵ１００からバス等のインタフェースを経由してフレーム（データ）を受け取りネットワークに適した形に変換してネットワーク（イーサネットケーブル等のケーブル）に送出する。

【０１０３】
メモリ１０２は、ＣＰＵ１００がソフトウェアを処理実行する際に利用される揮発性記憶装置である。又、ＣＰＵ１００から書き込み命令と共に送られたデータを指定されたアドレスに保存する。そして、ＣＰＵ１００からの読み出し命令を受けると、指定されたアドレスからデータが読み出され、ＣＰＵに送付される。通常は、電源が切れると、記憶内容が失われる揮発性になっている。

【０１０４】
ＨＤＤ１０３は、ハードディスクドライブと呼ばれ、ソフトウェア（プログラム）を記憶する為の不揮発性記憶装置である。ＣＰＵ１００から書き込み命令と共に送られたデータを指定されたアドレスに保存する。そして、ＣＰＵ１００からの読み出し命令を受けると、指定されたアドレスからデータが読み出され、ＣＰＵに送付される。不揮発性記憶装置は、電源が切れても、記憶内容が失われない記憶装置であり、本実施の形態では、不揮発性記憶装置を代表してＨＤＤを用いて説明する。尚、ＨＤＤ以外の不揮発性記憶装置（フラッシュメモリ、フロッピーディスク：登録商標、磁気テープ等）を用いても、同様の動作を実現できる。

【０１０５】
キーボード１０４は、ユーザからのキー押下による命令を、電気信号に変換し、ＣＰＵ１００に伝達する入力装置である。

【０１０６】
マウス１０５は、ユーザからのマウス１０５の移動による命令を、電気信号に変換し、ＣＰＵ１００に伝達する入力装置である。

【０１０７】
グラフィック１０６は、ＣＰＵ１００からの描画命令を受け、ブラウン管や液晶画面などの表示装置に適した信号に変換する為に、コンピュータに挿入もしくはメイン基板上に実装されるハードウェアである。

【０１０８】
図６は、図５におけるＣＰＵ１００内で動作するソフトウェアの構成を示したブロック図である。

【０１０９】
ＣＰＵ１００内で動作するソフトウェアは、中継アプリケーション１００１、ＳＳＬ１００２、ＴＣＰ１００３、ＳＳＬ１００４、ＴＣＰ１００５、ＩＰルーティング１００６

、ＩＰスタック１００７、中間ドライバ１００８、ドライバ１００９により構成される。

【０１１０】

図６に挙げたソフトウェアの中、ＴＣＰ１００３、ＴＣＰ１００５、ＩＰルーティング１００６、ＩＰスタック１００７は、通常はＷｉｎｄｏｗｓ（登録商標）、Ｌｉｎｕｘ、ＢＳＤ等のＯＳ（オペレーティングシステム）に含まれるソフトウェアである。特に、Ｗｉｎｄｏｗｓの場合は、一般的には、ユーザがこのソフトウェアのプログラムを書き換えることは出来ない。

【０１１１】

ＣＰＵ１００内では、実際には、図６に示したソフトウェア以外にも多くのソフトウェアが動作しているが、図６においては、本発明に無関係なソフトウェアは省略されている。

【０１１２】

中継アプリケーション１００１は、図９におけるＨＵＢ１１内のブリッジ１１４と同様の動作をソフトウェアにより実現する、フレーム転送ソフトウェアである。従来技術１においては仮想ＨＵＢと呼ばれる。

【０１１３】

中継アプリケーション１００１は、ＳＳＬ１００２もしくはＳＳＬ１００４からデータ（フレーム）を受信して宛先ＭＡＣアドレス（ＭＡＣ　ＤＡ）を参照して転送先のＳＳＬを選択し、適切なＳＳＬ（ＳＳＬ１００２もしくはＳＳＬ１００４）に受信したフレームをそのまま転送する。更に、フレーム受信時に、送信元ＭＡＣアドレス（ＭＡＣ　ＳＡ）を参照し、ＭＡＣアドレスの学習を行い、どのＭＡＣアドレスをもつ端末が、どのＳＳＬ側に接続されているのかを記録する機能を有する。仮に、フレーム受信時に、宛先ＭＡＣアドレスを参照しても、ＭＡＣアドレスを学習していない場合は、フレームを、フレームが入力されたＳＳＬ以外の全てのＳＳＬにブロードキャストする機能を有する。

【０１１４】

中継アプリケーション１００１は、又、中間ドライバ１００８内の設定管理部１００８Ｌに対して、ＳＳＬセッションの対向となる機器のＩＰアドレス（図１においてゲートウェイ装置２０と、ゲートウェイ装置３０）や、ＳＳＬセッションの送信元ポート番号および宛先ポート番号を通知する。この通知は、セッションの確立時、切断時の他にも、定期的に行われる。

【０１１５】

ＳＳＬ１００２は、中継アプリケーション１００１からデータ（フレーム）を受け取り、暗号化を行って、ＴＣＰ１００３にデータを送り、又はＴＣＰ１００３からデータを受け取り、復号化を行って、中継アプリケーション１００１にデータを送る機能、及び暗号化に用いる証明書や公開鍵、秘密鍵および共通鍵等の情報を交換する機能を有する。ＳＳＬを使用するか否かは、中継アプリケーション１００１からの設定により決定され、ＳＳＬを使用しない場合は、中継アプリケーション１００１からのデータを暗号化せず、そのままＴＣＰ１００３に送り、又、ＴＣＰ１００３からのデータを復号化せず、そのまま中継アプリケーション１００１に送る機能を有する。

【０１１６】

本実施の形態においては、通常は暗号化を行う設定とする。

【０１１７】

ＴＣＰ１００３は、以下の（１）～（４）に示すような通常のＴＣＰ処理によりデータを一定形式のフォーマットに整えてパケット化し、又はパケットからデータを復元する機能を有する。

（１）　ＳＳＬ１００２から、若しくはＳＳＬ１００２を使用しない場合は中継アプリケーション１００１から、データを受け取り、このデータにパケットの欠落や順序逆転を検知する為のＴＣＰヘッダを付加して、ＩＰルーティング１００６に送る。ここで、大きなデータの場合は、分割（フラグメントとも言う）処理を行う。

（２）　ＩＰルーティング１００６からパケットを受け取り、ＴＣＰヘッダを参照して順

序逆転やパケットの欠落を検知する。そして、順序逆転も欠落も発生していない場合は、パケットからＴＣＰヘッダを外してＳＳＬ１００２に、ＳＳＬ１００２を使用していない場合は、中継アプリケーション１００１に送る。この際、パケットが届いたことを知らせる受信確認パケット（ＡＣＫパケット）を、パケットの送信元を宛先に設定して返信する。

（３）　（２）において、仮に、パケットの欠落が発生している場合は、再送要求パケットを送信する。又、順序逆転やフラグメントが発生している場合には、後から届くパケットを待って、データを復元する。

（４）　ＴＣＰセッションを確立させる際にＴＣＰセッション確立要求（ＳＹＮパケット）を送信し、これに応答して送信されたＡＣＫパケットを受け取り、（１）におけるパケットの送信速度を調整して輻輳制御する。

【０１１８】

ＳＳＬ１００４は、ＳＳＬ１００２と同様の動作を行う。

【０１１９】

ＴＣＰ１００５は、ＴＣＰ１００３と同様の動作を行う。

【０１２０】

ＩＰルーティング１００６は、ＴＣＰ１００３、ＴＣＰ１００５、若しくはＩＰスタック１００７からパケットを受け取り、宛先ＩＰアドレスと宛先ポート番号を参照して、ＩＰスタック１００７、ＴＣＰ１００３、若しくはＴＣＰ１００５に、パケットを転送する機能を有する。

【０１２１】

ＩＰスタック１００７は、以下に示す機能を有する。

（１）　ＩＰルーティング１００６からパケットを受け取り、ＭＡＣアドレス等のＥｔｈｅｒｎｅｔヘッダを付加してフレームを生成して中間ドライバ１００８に渡す。

（２）　中間ドライバ１００８から受信したフレームよりＭＡＣヘッダを削除して、ＩＰルーティング１００６に渡す。

（３）　（１）において付加するＭＡＣアドレス等を決定する為、ＡＲＰプロトコルを送受信する。

（４）　ＤＨＣＰプロトコル若しくは手動設定によりＩＰアドレス、デフォルトルート、ネットマスクなどＩＰ通信に必要な設定を受け、これを管理する。

【０１２２】

中間ドライバ１００８は、以下に挙げる４つの機能を有する。尚、構成の詳細については後述する。

（１）　ＴＣＰ処理機能を有し、ＴＣＰ１００３、又はＴＣＰ１００５とのＴＣＰ処理を終端する。尚、ＴＣＰ処理を終端させるとは、ＴＣＰ１００３、又はＴＣＰ１００５と、中間ドライバ１００８内のＴＣＰとの間でＴＣＰセッションを確立させるための一連の処理を行うということである。

（２）　フラグメント処理機能（フラグメント分割処理、フラグメント組立処理）を有し、ドライバ１００９側に流れるフレームのサイズが大きな場合は分割し、又、ドライバ１００９側から到着するフレームが予め分割されている場合は、組立処理を行う。

（３）　カプセル化およびカプセル化解除機能を有し、ＩＰスタック１００７側から送られてくるパケットに適切なヘッダを付加もしくは適切な値にヘッダを修正し、ドライバ１００９側に転送する。又、ドライバ１００９側から送られて来るフレームからヘッダを削除、若しくは適切な値にヘッダを修正し、ＩＰスタック１００７側に転送する。

（４）　上記（１）～（３）の処理対象となるフレームの識別に必要な情報を、中継アプリケーション１００１より受け取る。

（５）　アプリケーションからの要求に基づき、制御フレームを作成して、ドライバ１００９に送信する。又、ドライバ１００９より到着した制御フレームを受信し、アプリケーションに通知する。

【０１２３】

ドライバ１００９は、ＮＩＣ１０１と、ＣＰＵ１００内で動作する各種ソフトウェアとの間の仲介をするソフトウェアであり、ＮＩＣ１０１からフレームを受け取り、中間ドライバ１００８若しくはＩＰスタック１００７に送る機能を有し、更に、中間ドライバ１００８若しくはＩＰスタック１００７からフレームを受け取り、ＮＩＣ１０１に送る機能を有する。

【０１２４】

図７は、図６における中間ドライバ１００８の内部構成を詳細に記したブロック図である。

【０１２５】

中間ドライバ１００８は、ＴＣＰ１００８Ａとフラグメント分割１００８Ｂと、フラグメント組立１００８Ｃと、再カプセル化１００８Ｄと、再カプセル化１００８Ｅと、カプセル化解除１００８Ｆと、カプセル化解除１００８Ｇと、フレーム解析１００８Ｈと、フレーム解析１００８Ｉと、マルチプレクサ１００８Ｊと、マルチプレクサ１００８Ｋとで構成される。

【０１２６】

中間ドライバ１００８の構成要素の中、ＴＣＰ１００８Ａとフラグメント分割１００８Ｂと、フラグメント組立１００８Ｃと、再カプセル化１００８Ｄと、再カプセル化１００８Ｅと、カプセル化解除１００８Ｆと、カプセル化解除１００８Ｇとの各部位は、ＴＣＰセッションを確立する処理の高速化を行うＴＣＰセッションの数と同じ数だけ複数設置する場合がある。例えば、セッション中継装置１０において、ＴＣＰ１００３とＴＣＰ１００５との双方の高速化を行う場合は、中間ドライバ１００８の各構成要素を２組用意する必要がある。例えば、ＴＣＰ１００３のみ高速化を行い、ＴＣＰ１００５は従来通りの転送をする場合、中間ドライバ１００８の各構成要素は、一組のみで良い。

【０１２７】

ＴＣＰ１００８Ａは、ＴＣＰ１００３と同様の動作、つまり以下に挙げる四つの機能を有する。

（１）　フラグメント組立１００８Ｃからデータを受け取り、このデータにパケットの欠落や順序逆転を検知する為のＴＣＰヘッダを付加して、再カプセル化１００８Ｅに送る。ここで、大きなデータの場合は、分割（フラグメント分割処理とも言う）処理を行う。

（２）　カプセル化解除１００８Ｆからパケットを受け取り、ＴＣＰヘッダを参照して順序逆転やパケットの欠落を検知し、順序逆転も欠落も発生していない場合は、パケットからＴＣＰヘッダを外し、フラグメント分割１００８Ｂに送る。この際、パケットが届いたことを知らせるＡＣＫパケットをパケットの送信元、即ち、ＴＣＰ１００３若しくはＴＣＰ１００５に、再カプセル化１００８Ｅを経由して返信する。

（３）　（２）において、仮に、パケットの欠落が発生している場合は、再送要求パケットをＴＣＰ１００３若しくはＴＣＰ１００５に対して、再カプセル化１００８Ｅを経由して送信する。又、順序逆転やフラグメント分割が発生している場合には、後から届くパケットを待ってデータを復元し（再送待機処理、フラグメント結合処理）、フラグメント分割１００８Ｂに転送する。

（４）　ＴＣＰ１００３若しくはＴＣＰ１００５によって送信されるＴＣＰ規格に沿ったパケットを受け取り、（１）におけるパケットの送信速度を調整する。ＴＣＰ１００８Ａは、ＴＣＰセッション確立要求（ＳＹＮパケット）を受け取ると、接続要求パケットを生成する。また、ＴＣＰ１００８Ａは、ＴＣＰセッション確立要求に対する応答パケット（ＳＹＮ＋ＡＣＫパケット）を受信すると、これに対してＡＣＫパケットを返答し、接続完了通知パケットを生成する。尚、この接続要求パケット及び接続完了通知パケットは、ＴＣＰ規格に沿ったパケットではなく、本発明の通信システムにおける独自のパケットである。

フラグメント分割１００８Ｂは、ＴＣＰ１００８Ａからパケットを受け取り、再カプセル化１００８Ｄに転送する。この時、仮に、パケットのサイズが予め設定された大きさよりも大きい場合は、パケットを分割（フラグメント分割処理）してから、再カプセル化１

００８Ｄに転送する。

【０１２８】

フラグメント組立１００８Ｃは、カプセル化解除１００８Ｇからパケットを受け取り、ＴＣＰ１００８Ａに転送する。この時、仮に、パケットに分割を示すフラグが付加されていた場合は、パケットを一旦保存し、後から届くパケットを待ってパケットを結合し、ＴＣＰ１００８Ａに転送する。この処理をフラグメント組立処理と呼ぶ。

【０１２９】

再カプセル化１００８Ｄは、フラグメント分割１００８Ｂより送られてくるデータ（図３におけるＦ１４）に、ＩＮＥＴ ＭＡＣ Ｆ１１、ＩＮＥＴ ＩＰ Ｆ１２、ＩＮＥＴ ＴＣＰ Ｆ１３の各ヘッダを付加し、マルチプレクサ１００８Ｋに転送する。付加するＦ１１～Ｆ１３の各ヘッダの値は、カプセル化解除１００８Ｆより通知を受ける。尚、設定によりＩＮＥＴ ＴＣＰ Ｆ１３の位置に、ＴＣＰヘッダではなく、ＵＤＰヘッダを設定することも出来る。

【０１３０】

再カプセル化１００８Ｄにおいて、ＴＣＰヘッダＦ１３を付加するのは、通信経路上に存在するＦｉｒｅｗａｌｌや、ＮＡＴルータ等（図１の例ではＦｉｒｅｗａｌｌ２３）で、パケットが遮断されることを防ぐ為である。Ｆ１３にＵＤＰヘッダを設定した場合は、通信経路上にＦｉｒｅｗａｌｌやＮＡＴルータ等が存在する場合に、通信が遮断される可能性が有る。再カプセル化１００８Ｄにおいて付加したＴＣＰヘッダは、フレームフォーマットはＴＣＰの形式を有するが、実際には、ＴＣＰは付加したヘッダでは無いので、輻輳制御や再送制御には用いられない。ここで付加するヘッダＦ１３は、厭くまで、ＦｉｒｅｗａｌｌやＮＡＴを通過する為のものであり、実際の輻輳制御や再送制御は、端末２１やサーバ３１内に存在するＴＣＰ（図３のフレームフォーマットＦ１０におけるＦ２３のＴＣＰヘッダ部分）によって行われる。

【０１３１】

再カプセル化１００８Ｅは、ＴＣＰ１００８Ａより送られてくるデータ（Ｆ１２，Ｆ１３，Ｆ１４）に、ＩＮＥＴ ＭＡＣ ヘッダＦ１１を付加してマルチプレクサ１００８Ｊに渡す。付加するヘッダ（Ｆ１１）の値は、カプセル化解除１００８Ｇより通知を受ける。

【０１３２】

カプセル化解除１００８Ｆは、フレーム解析１００８Ｈから送られてくるパケット（Ｅｔｈｅｒ ｏｖｅｒ ＳＳＬフレームフォーマットＦ１０形式）から、ＩＮＥＴ ＭＡＣ Ｆ１１ヘッダを削除し、ＴＣＰ１００８Ａに転送する。この時、削除したヘッダＦ１１の内容、及びヘッダＦ１２、ヘッダＦ１３の各ヘッダの内容を、再カプセル化１００８Ｄに通知する。

【０１３３】

カプセル化解除１００８Ｇは、フレーム解析１００８Ｉから送られてくるパケット（Ｅｔｈｅｒ ｏｖｅｒ ＳＳＬフレームフォーマットＦ１０形式）から、ＩＮＥＴ ＭＡＣ Ｆ１１、ＩＮＥＴ ＩＰ Ｆ１２、ＩＮＥＴ ＴＣＰ Ｆ１３の各ヘッダを削除し、フラグメント組立１００８Ｃに転送する。この時、削除したＦ１１～Ｆ１３の各のヘッダの内容を、再カプセル化１００８Ｅに通知する。尚、設定によりＩＮＥＴ ＴＣＰ Ｆ１３の位置に、ＴＣＰヘッダではなくＵＤＰヘッダが設定されている場合は、このＵＤＰヘッダの内容を、再カプセル化１００８Ｅに通知する。

【０１３４】

フレーム解析１００８Ｈは、ＩＰスタック１００７からフレームを受信し、フレームが高速化処理に関係するフレームか否かを、ＭＡＣアドレス、ＩＰアドレス、ＴＣＰヘッダ、ＵＤＰヘッダ等を基に判別し、ＴＣＰセッションの確立処理の高速化に関係するフレームであれば、カプセル化解除１００８Ｆに転送し、その他のフレームであれば、マルチプレクサ１００８Ｋに転送する。フレームの判定に必要な情報は、中継アプリケーション１００１より設定管理部１００８Ｌを通じて通知を受ける。

【０１３５】
フレーム解析１００８Ｉは、ドライバ１００９からフレームを受信し、フレームがＴＣＰセッションの高速化処理に関係するフレームか否かを、ＭＡＣアドレス、ＩＰアドレス、ＴＣＰヘッダ、ＵＤＰヘッダ等を基に判別し、高速化処理に関係するフレームであれば、カプセル化解除１００８Ｇに転送し、その他のフレームであれば、マルチプレクサ１００８Ｊに転送する。フレームの判定に必要な情報は、中継アプリケーション１００１より設定管理部１００８Ｌを通じて通知を受ける。

【０１３６】
更に、フレーム解析１００８Ｉは、ドライバ１００９からフレームを受信し、フレームが機器や高速化エンジンの制御に関わる特殊なフレーム（以降、制御フレームと呼ぶ）である場合は、この制御フレームを制御フレーム送受信部１００８Ｍに転送する。特殊フレームであるか否かは、通常は、ＭＡＣ　ＤＡとＭＡＣ　ＳＡにより判断する。ＭＡＣ　ＤＡ又はＭＡＣ　ＳＡの何れかに、予め、規定したアドレス範囲のＭＡＣアドレス（制御用ＭＡＣアドレスと呼ぶ。例えば０００００４Ｃ００００ｘｘ）が記載されている場合は、このフレームを制御フレームと判断する。

【０１３７】
マルチプレクサ１００８Ｊは、フレーム解析１００８Ｉと、再カプセル化１００８Ｅからフレームを受信し、ＩＰスタック１００７に転送する。この際、フレームの同時到着により、欠落が発生しないようバッファ動作を行う。

【０１３８】
マルチプレクサ１００８Ｋは、フレーム解析１００８Ｈと、再カプセル化１００８Ｄからフレームを受信し、ドライバ１００９に転送する。この際、フレームの同時到着により、欠落が発生しないようバッファ動作を行う。

【０１３９】
設定管理部１００８Ｍは、中継アプリケーション１００１より、高速化処理に関連するセッションの情報（ＩＰアドレス、ポート番号等）の通知を受け、フレーム解析１００８Ｈ及びフレーム解析１００８Ｉの設定を行う。

【０１４０】
制御フレーム送受信部１００８Ｌは、マルチプレクサ１００８Ｋに機器や高速化エンジンの制御に関わる特殊なフレーム（以降、制御フレームと呼ぶ）を送り、又、フレーム解析１００８Ｉより制御フレームを受信する。制御フレームは、高速化エンジン制御２００１等のアプリケーションからの要求により送信される。又、受信した制御フレームは、適切なアプリケーションに転送される。

【０１４１】
上記を纏めると、中間ドライバで１００８は、フラグメントに関連する処理を２カ所で行っている。一つ目は、ＴＣＰ１００８Ａで、ここでは、ＴＣＰ１００３やＴＣＰ１００５との間でフラグメント処理を行う。二つ目は、フラグメント分割１００８Ｂとフラグメント組立１００８Ｃで、ここでは、高速化エンジン２０１４との間でフラグメント処理を行う。

【０１４２】
ここで、中間ドライバ１００８、高速化エンジン２０１４、ＴＣＰ１００３、更にＴＣＰ１００４によるフラグメント処理は、出来れば発生させないことが望ましい。可能であれば、端末２１内のＴＣＰ２１０２において最大フレーム長を小さく設定することで、箇所におけるフラグメント処理の発生を防止する。特に、高速化エンジン２０１４におけるフラグメント組立処理は、ハードウェア構成が複雑になる為、これを出来るだけ行わないように、端末２１やサーバ３１内のＴＣＰ最大フレーム長を設定する。

【０１４３】
図８は、図５におけるＮＩＣ１０１の構成を詳細に示したブロック図である。

【０１４４】
ＮＩＣ１０１は、ＭＡＣ１０１１、ＰＨＹ１０１２、及びポート１０１３により構成さ

れる。

【０１４５】

ＭＡＣ１０１１は、ＣＰＵ１００とＰＣＩバス等の高速なインタフェースで接続され、ＰＨＹ１０１２とＭＩＩ等のインタフェースで接続され、これら両インタフェースの間の仲介を行うハードウェアである。ＭＡＣ１０１１は、ＣＰＵ１００側からデータ（フレーム）を受け取ると、送信元ＭＡＣアドレス（ＭＡＣ　ＳＡ）の付加などの制御を行い、受け取ったフレームをＰＨＹ１０１２側に転送する。逆に、ＰＨＹ１０１２側からフレームを受け取り、宛先ＭＡＣアドレス（ＭＡＣ　ＤＡ）により自ノード宛か否かを判断し、自ノード宛もしくはブロードキャスト・マルチキャストのフレームであれば、ＣＰＵ１００側に転送する。

【０１４６】

ＰＨＹ１０１２は、ＭＡＣ１０１１とＭＩＩ等のインタフェースで接続され、ポート１０１３とＩＥＥＥ８０２．３規格（１０ＢＡＳＥ－Ｔ、１００ＢＡＳＥ－ＴＸ、１０００ＢＡＳＥ－Ｔ、１０００ＢＡＳＥ－ＳＸ等）のインタフェースで接続され、これら両インタフェースの仲介を行うハードウェアである。ＰＨＹ１０１２は、ＭＡＣ１０１１側からデータ（フレーム）を受け取ると、ポート１０１３側に適した信号（電気信号もしくは光信号）に変換し、ポート１０１３を通してケーブルに送信する。又、ポート１０１３側から信号（電気信号もしくは光信号）を受信し、ＭＡＣ１０１１側のインタフェース（ＭＩＩ等）に適した信号に変換し、ＭＡＣ１０１１側にデータ（フレーム）を送信する。

【０１４７】

ポート１０１３は、イーサネットケーブル（ＵＴＰや光ファイバなど）を接続する接続口である。

【０１４８】

図９は、第１の実施の形態におけるＨＵＢ１１の構成を詳細に示したブロック図である。

【０１４９】

ＨＵＢ１１は、ポート１１１と、ポート１１２と、ポート１１３と、ブリッジ１１４により構成される。

【０１５０】

ポート１１１は、図８のＮＩＣ１０１におけるポート１０１３と同様に、イーサネットケーブル（ＵＴＰや光ファイバなど）を接続する接続口である。

【０１５１】

ポート１１２は、ポート１１１と同様である。

【０１５２】

ポート１１３は、ポート１１１と同様である。

【０１５３】

ブリッジ１１４は、ポート１１１～ポート１１３よりフレームを受け取り、宛先ＭＡＣアドレスを参照して、ポート１１１～ポート１１３の何れかにフレームを転送する機能を有する。更に、フレーム受信時に、送信元ＭＡＣアドレスを参照し、ＭＡＣアドレスの学習を行い、どのＭＡＣアドレスをもつ端末が、どのポートに接続されているのかを記録する機能を有する。仮に、フレーム受信時に、宛先ＭＡＣアドレスを参照しても、ＭＡＣアドレスを学習していない場合は、フレームを、フレームが入力されたポート以外のポートにブロードキャストする機能を有する。

【０１５４】

ブリッジ１１４は、ハードウェアで構成される場合と、ＣＰＵ上で動作するソフトウェアにより構成される場合との両方の場合が存在する。仮に、ソフトウェアで構成される場合は、ＣＰＵ内ではブリッジソフトウェアの他、ドライバ等の関連するソフトウェアも動作する。

【０１５５】

図９においては、図８に記載のＮＩＣに相当する部分を省略して記載している。つまり

、図８におけるＭＡＣは、ブリッジ１１４の一部機能としてブリッジ１１４に内蔵されるか、若しくはポート１１１～１１３の一部機能としてポート１１１～１１３に内蔵される。同様に、ＰＨＹも、ブリッジ１１４の一部機能としてブリッジ１１４に内蔵されるか、若しくはポート１１１～１１３の一部機能としてポート１１１～１１３に内蔵される。

【０１５６】

図１０は、第１の実施の形態におけるゲートウェイ装置２０内に存在する、ＣＰＵ２００内で動作するソフトウェア構成を詳細に示したブロック図である。

【０１５７】

ＣＰＵ２００内で動作するソフトウェアは、高速化エンジン制御２００１，ＳＳＬ２００２，ＴＣＰ２００３，ＩＰルーティング２００４，ＩＰスタック２００５、中間ドライバ２００６、ドライバ２００７で構成される。

【０１５８】

尚、ゲートウェイ装置２０は、図５に示すセッション中継装置１０と同様のハードウェア構成を有するが、図５におけるＣＰＵ１００がＣＰＵ２００となり、ＮＩＣ１０１がＮＩＣ２０１になる点等、付番において異なる。

【０１５９】

図１０に挙げたソフトウェアの中、ＴＣＰ２００３、ＩＰルーティング２００４、ＩＰスタック２００５は、通常は、Ｗｉｎｄｏｗｓ、Ｌｉｎｕｘ、ＢＳＤ等のＯＳ（オペレーティングシステム）に含まれるソフトウェアである。特に、Ｗｉｎｄｏｗｓの場合は、一般的には、ユーザがこのソフトウェアのプログラムを書き換えることは出来ない。

【０１６０】

ＣＰＵ２００内では、実際には、図１０に示したソフトウェア以外にも多くのソフトウェアが動作しているが、図１０においては本発明に無関係なソフトウェアは省略している。

【０１６１】

高速化エンジン制御２００１は、以下に挙げる動作を行う。

（１） セッション中継装置１０内の中継アプリケーション１００１との間のＳＳＬセッションの接続および切断に必要な設定を、ＳＳＬ２００２に対して行う。

（２） ＳＳＬセッションの相手方機器（セッション中継装置１０）のＩＰアドレスや宛先ポート、及び自ノード（ゲートウェイ装置２０）側のＳＳＬセッションの送信元ポート番号や送信元ＩＰアドレス、更にはＳＳＬセッションの相手方機器（セッション中継装置１０）のＩＰアドレスに対してＡＲＰ問い合わせを行った結果、得られる宛先ＭＡＣアドレスと自ノードの送信元ＭＡＣアドレスとを、中間ドライバ２００６を経由して、高速化エンジン２０１４に通知する。中間ドライバ２００６から高速化エンジン２０１４の間は、制御フレームを用いてアドレス等を転送する。

（３） ＳＳＬ２００２からＳＳＬセッションの相手方（セッション１００１内のＳＳＬ１００２）の認証完了通知を受けると、高速化処理開始命令と、相手方の公開鍵と自身の秘密鍵、さらには共通鍵を、中間ドライバ２００６を経由して、高速化エンジン２０１４に転送する。中間ドライバ２００６から高速化エンジン２０１４の間は、制御フレームを用いて公開鍵、秘密鍵および共通鍵を転送する。尚、本実施の形態における高速化処理開始命令は、相手方の公開鍵と自身の秘密鍵と共通鍵とを、中間ドライバ２００６を経由して高速化エンジン２０１４に転送する構成を用いて説明するが、相手方の公開鍵と自身の秘密鍵と共通鍵とを総合して高速化処理開始命令としても良い。

（４） ＳＳＬセッションの設定完了時、及び切断時に、中間ドライバ２００６を経由して、高速化エンジン２０１４に、暗号化処理の開始、及び終了を命令する。この時、中間ドライバ２００６から高速化エンジン２０１４の間は、制御フレームを用いて暗号化処理の開始、及び終了の命令を転送する

（５） 高速化エンジン２０１４より中間ドライバ２００６を経由して通知されるＳＳＬセッションの切断要求を受信し、ＳＳＬ２００２に対して切断要求を行う。

【０１６２】

ＳＳＬ２００２は、暗号化に用いる証明書や公開鍵、秘密鍵および共通鍵等の情報を交換する機能を有する。本実施の形態においては、ＳＳＬ２００２はＳＳＬ１００２との間で証明書（公開鍵）を交換する。そして、ＰＫＩ等の方式に従って証明書の署名確認等を行い、認証された場合には、高速化エンジン制御２００１に認証完了を通知する。

【０１６３】

通常、ＳＳＬは暗号化および複号化の処理も併せて行うが、本実施の形態においては、ゲートウェイ装置２０では暗号化および複号化の処理を行わず、高速化エンジン２０１４において暗号化および復号化を行っている。本実施の形態において、セッション中継装置１０では、ＳＳＬ１００２及びＳＳＬ１００４において、暗号化および復号化を行う。

【０１６４】

ＴＣＰ２００３は、以下の（１）～（４）に示すような通常のＴＣＰ処理によりデータを一定形式のフォーマットに整えてパケット化し、又はパケットからデータを復元するの機能を有する。

（１） ＳＳＬ２００２から、若しくはＳＳＬ２００２を使用しない場合は高速化エンジン制御２００１から、データを受け取り、受け取ったデータにパケットの欠落や順序逆転を検知する為のＴＣＰヘッダを付加して、ＩＰルーティング２００４に送る。ここで、大きなデータの場合は、分割（フラグメントとも言う）処理を行う。

（２） ＩＰルーティング２００４からパケットを受け取り、ＴＣＰヘッダを参照して順序逆転やパケットの欠落を検知し、順序逆転も欠落も発生していない場合は、パケットからＴＣＰヘッダを外し、ＳＳＬ２００２に、若しくはＳＳＬ２００２を使用していない場合は、カプセル化アプリケーション２００１に送る。この際、パケットが届いたことを知らせるＡＣＫパケットをパケットの送信元に返信する。

（３） （２）において、仮に、パケットの欠落が発生している場合は、再送要求パケットを送信する。又、順序逆転やフラグメントが発生している場合には、後から届くパケットを待って、データを復元する。

（４） ＴＣＰセッションを確立させる際にＴＣＰセッション確立要求パケット（ＳＹＮパケット）を送信する。ＡＣＫパケットを受け取り、（１）におけるパケットの送信速度を調整して輻輳制御する。

【０１６５】

ＩＰルーティング２００４は、ＴＣＰ２００３、若しくはＩＰスタック２００５からパケットを受け取り、宛先ＩＰアドレスと宛先ポート番号を参照して、ＩＰスタック２００５、若しくはＴＣＰ２００３に、パケットを転送する機能を有する。

【０１６６】

ＩＰスタック２００５は、以下に示す機能を有する。

（１） ＩＰルーティング２００４からパケットを受け取り、ＭＡＣアドレス等のＥｔｈｅｒｎｅｔヘッダを付加してブリッジ２００６に渡す。

（２） ブリッジ２００６から受信したパケットよりＭＡＣヘッダを削除して、ＩＰルーティング２００４に渡す。

（３） （１）において付加するＭＡＣアドレス等を決定する為、ＡＲＰプロトコルを送受信する。

（４） ＤＨＣＰプロトコル若しくは手動設定により、ＩＰアドレス、デフォルトルート、ネットマスク等のＩＰ通信に必要な設定を受け、これを管理する。

【０１６７】

中間ドライバ２００６は、図７に示す中間ドライバ１００８と同様の中間ドライバである。中間ドライバ２００６は、以下に挙げる５つの機能を有する。尚、中間ドライバ２００６の詳細については、中間ドライバ１００８と同様であるため省略する。

（１） ＴＣＰ処理機能を有し、ＴＣＰ２００３を終端する。

（２） フラグメント処理機能（フラグメント分割処理、フラグメント組立処理）を有し、ドライバ２００７側に流れるフレームのサイズが大きな場合は分割し、又、ドライバ２００７側から到着するフレームが予め分割されている場合は、組立処理を行う。

（３） カプセル化およびカプセル化解除機能を有し、ＩＰスタック２００５側から送られて来るパケットに適切なヘッダを付加、削除、若しくは修正し、ドライバ２００７側に転送する。又、ドライバ２００７側から送られてくるパケットのヘッダを削除、付加、若しくは修正し、ＩＰスタック２００５側に転送する。
（４） 上記（１）～（３）の処理対象となるフレームの識別に必要な情報を、高速化エンジン制御２００１より受け取る。
（５） 高速化エンジン制御２００１からの要求に基づき、制御フレームを作成して、ドライバ２００７に送信する。又、ドライバ２００７より到着した制御フレームを受信し、高速化エンジン２００１に通知する。

【０１６８】
ドライバ２００７は、ＮＩＣ２０１と、ＣＰＵ２００内で動作するソフトウェアとの間の仲介をするソフトウェアであり、ＮＩＣ２０１からパケットを受け取り中間ドライバ２００６に送る機能を有し、更に、中間ドライバ２００６からフレームを受け取り、ＮＩＣ２０１に送る機能を有する
図１１は、第１の実施の形態におけるゲートウェイ装置２０内に存在する、ＮＩＣ２０１の構成を詳細に示したブロック図である。

【０１６９】
ＮＩＣ２０１は、ＭＡＣ２０１１，ＰＨＹ２０１２、ポート２０１３、及び高速化エンジン２０１４により構成される。

【０１７０】
ＭＡＣ２０１１は、図８におけるＭＡＣ１０１１と同様の動作を行う。

【０１７１】
ＰＨＹ２０１２は、図８におけるＰＨＹ１０１２と同様の動作を行う。

【０１７２】
ポート２０１３は、イーサネットケーブル（ＵＴＰや光ファイバなど）を接続する接続口である。

【０１７３】
高速化エンジン２０１４は、ＭＡＣ２０１１とＰＨＹ２０１２との間のインタフェース（ＭＩＩ等）に割り込む形で実装され、ＳＳＬセッションを用いて通信する際の暗号化、復号化、カプセル化、カプセル化解除、フラグメント分割、フラグメント組立の各処理を行うハードウェアである。又、高速化エンジン２０１４の動作に必要な設定情報を送受信する為に、制御フレームの送受信を行う。通常は、ＦＰＧＡやＡＳＩＣ等の集積回路により高速化エンジン２０１４実現される。

【０１７４】
高速化エンジン２０１４の詳細について説明する。
図１２は、図１１における高速化エンジン２０１４の構成を詳細に示したブロック図である。

【０１７５】
高速化エンジン２０１４は、インタフェース２０１４Ａ、フレーム解析２０１４Ｂ、インタフェース２０１４Ｃ、制御フレーム解析２０１４Ｄ、マルチプレクサ２０１４Ｅ、マルチプレクサ２０１４Ｆ、暗号化２０１４Ｇ、フラグメント分割２０１４Ｈ、カプセル化２０１４Ｉ、カプセル化解除２０１４Ｊ、フラグメント解除２０１４Ｋ、復号化２０１４Ｌ、制御フレーム送受信部２０１４Ｍにより構成される。

【０１７６】
インタフェース２０１４Ａは、ＰＨＹ２０１２と接続されたバス（ＭＩＩ）等と高速化エンジンの仲介をする部分である。ＰＨＹ２０１２側から到着したフレームを、高速化エンジンの動作に適した信号に変換してフレーム解析２０１４Ｂに転送する。又、高速化エンジン側、即ち、マルチプレクサ２０１４ＦからＰＨＹ２０１２側に送信するフレームを、ＰＨＹ２０１２と接続されたバス（ＭＩＩ）等に適した信号に変換する。

【０１７７】

フレーム解析２０１４Ｂは、インタフェース２０１４Ａからフレームを受信し、以下に示す（１）～（４）の順序で宛先を決定して転送する。
（１）　自ノード宛て、かつ、予め設定されたＳＳＬセッションのフレームであれば（セッション中継装置１０によって暗号化されたフレームであれば）、このフレームをカプセル化解除２０１４Ｊに転送する。
（２）　（１）以外の自ノード宛てフレームであれば、受信したフレームをマルチプレクサ２０１４Ｅに転送する。
（３）　ＭＡＣ　ＤＡにブロードキャストＭＡＣ、若しくはブロードキャストＭＡＣが付加されたブロードキャストフレーム、又はマルチキャストフレームであれば、マルチプレクサ２０１４Ｅと暗号化２０１４Ｇとに、このフレームをコピーして転送する。
（４）　（１）～（３）以外のフレームであれば、暗号化２０１４Ｇに転送する。

【０１７８】
インタフェース２０１４Ｃは、ＭＡＣ２０１１と接続されたバス（ＭＩＩ）等と高速化エンジンとの仲介をする部分である。ＭＡＣ２０１１側から到着したフレームを、高速化エンジンの動作に適した信号に変換し、制御フレーム解析２０１４Ｄに転送する。又、高速化エンジン側、即ち、マルチプレクサ２０１４ＥからＭＡＣ２０１１側に送信するフレームを、ＭＡＣ２０１１と接続されたバス（ＭＩＩ）等に適した信号に変換する。

【０１７９】
制御フレーム解析２０１４Ｄは、インタフェース２０１４Ｃからフレームを受信し、このフレームが高速化エンジンの制御に関わる特殊なフレーム（以降、制御フレームと呼ぶ）である場合は、フレームを制御フレーム送受信部２０１４Ｍに転送する。特殊フレームで無い場合は、マルチプレクサ２０１４Ｆに転送する。特殊フレームであるか否かは、通常は、ＭＡＣ　ＤＡとＭＡＣ　ＳＡにより判断する。ＭＡＣ　ＤＡ若しくはＭＡＣ　ＳＡの何れかに、予め規定したアドレス範囲のＭＡＣアドレス（制御用ＭＡＣアドレスと呼ぶ。例えば０００００４Ｃ０００００００～ＦＦ）が記載されている場合は、フレームを制御フレームと判断する。

【０１８０】
マルチプレクサ２０１４Ｅは、フレーム解析２０１４Ｂおよび制御フレーム送受信部２０１４Ｍよりフレームを受信し、必要であれば、キューに保存して送信タイミングを調整し、インタフェース２０１４Ｃに送信する。キューに保存するのは、フレーム解析２０１４Ｂ側から到着するフレームと、制御フレーム送受信部２０１４Ｍ側から到着するフレームの衝突を避ける為である。

【０１８１】
マルチプレクサ２０１４Ｆは、制御フレーム解析２０１４Ｄ及びカプセル化２０１４Ｉ、更に復号化２０１４Ｌよりフレームを受信し、必要であれば、キューに保存して送信タイミングを調整し、インタフェース２０１４Ａに送信する。キューに保存するのは、制御フレーム解析２０１４Ｄ、カプセル化２０１４Ｉ、更に復号化２０１４Ｌの各々から到着するフレームの衝突を避ける為である。

【０１８２】
暗号化２０１４Ｇは、フレーム解析２０１４Ｂよりフレームを受信し、３ＤＥＳ等の方法で暗号化を行い、フラグメント分割２０１４Ｈに転送する。暗号化に用いる公開鍵と共通鍵は、制御フレーム送受信部２０１４Ｍより通知を受けたものを利用する。

【０１８３】
フラグメント分割２０１４Ｈは、図７に示す中間ドライバ１００８内のフラグメント分割１００８Ｂと同様の動作を行う。すなわち、暗号化２０１４Ｇからパケットを受け取り、カプセル化２０１４Ｉに転送する。この時、仮に、パケットのサイズが予め設定された大きさよりも大きい場合は、パケットを分割（フラグメント分割処理）してから、カプセル化２０１４Ｉに転送する。

【０１８４】
カプセル化２０１４Ｉは、図７に示す中間ドライバ１００８内の再カプセル化１００８

Ｄと同様の動作を行う。すなわち、フラグメント分割２０１４Ｈより送られて来るデータ（図３におけるＦ１４）に、ＩＮＥＴ　ＭＡＣ　Ｆ１１、ＩＮＥＴ　ＩＰ　Ｆ１２、ＩＮＥＴ　ＴＣＰ　Ｆ１３の各ヘッダを付加し、マルチプレクサ２０１４Ｆに転送する。付加するＦ１１～Ｆ１３の各ヘッダの値は、制御フレーム送受信部２０１４Ｍより通知を受ける。尚、設定により、ＩＮＥＴ　ＴＣＰ　Ｆ１３の位置に、ＴＣＰヘッダでは無く、ＵＤＰヘッダを設定することも出来る。

【０１８５】

カプセル化２０１４Ｉにおいて、ＴＣＰヘッダＦ１３を付加するのは、通信経路上に存在するＦｉｒｅｗａｌｌやＮＡＴルータ等（図１の例ではＦｉｒｅｗａｌｌ２３）でパケットが遮断されることを防ぐ為である。Ｆ１３にＵＤＰヘッダを設定した場合は、通信経路上にＦｉｒｅｗａｌｌやＮＡＴルータ等が存在する場合に、通信が遮断される可能性がある。カプセル化２０１４Ｉにおいて付加したＴＣＰヘッダは、フレームフォーマットはＴＣＰの形式を有するが、実際には、ＴＣＰは付加したヘッダでは無いので、輻輳制御や再送制御には用いられない。ここで付加するヘッダＦ１３は、厭くまで、ＦｉｒｅｗａｌｌやＮＡＴを通過する為のものであり、実際の輻輳制御や再送制御は、端末２１やサーバ３１内に存在するＴＣＰ（図３のフレームフォーマットＦ１０におけるＦ２３のＴＣＰヘッダ部分）によって行われる。

【０１８６】

カプセル化解除２０１４Ｊは、図７に示す中間ドライバ１００８内のカプセル化解除１００８Ｇと同様の動作を行う。カプセル化解除２０１４Ｊは、フレーム解析２０１４Ｂから送られて来るパケット（Ｅｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームフォーマットＦ１０形式）から、ＩＮＥＴ　ＭＡＣ　Ｆ１１、ＩＮＥＴ　ＩＰ　Ｆ１２、ＩＮＥＴ　ＴＣＰ　Ｆ１３の各ヘッダを削除し、フラグメント解除２０１４Ｋに転送する。尚、設定により、ＩＮＥＴ　ＴＣＰ　Ｆ１３の位置に、ＴＣＰヘッダでは無く、ＵＤＰヘッダが設定されている場合も、ＴＣＰヘッダの場合と同様の処理を行う。

【０１８７】

フラグメント解除２０１４Ｋは、図７に示す中間ドライバ１００８内のフラグメント組立１００８Ｃと同様の動作を行う。フラグメント解除２０１４Ｋは、カプセル化解除２０１４Ｊからパケットを受け取り、復号化２０１４Ｌに転送する。この時、仮に、パケットに分割を示すフラグが付加されていた場合は、パケットを一旦保存し、後から届くパケットを待ってパケットを結合し、復号化２０１４Ｌに転送する。この処理をフラグメント組立処理と呼ぶ。

【０１８８】

復号化２０１４Ｌは、フラグメント解除２０１４Ｋよりフレームを受信し、３ＤＥＳ等の方法で復号化を行い、マルチプレクサ２０１４Ｆに転送する。復号化に用いる秘密鍵と共通鍵は、制御フレーム送受信部２０１４Ｍより通知を受けたものを利用する。

【０１８９】

制御フレーム送受信部２０１４Ｍは、図７に示す中間ドライバ１００８内の制御フレーム送受信部１００８Ｍとの間で、制御フレームの送受信を行う。制御フレーム送受信部２０１４Ｍは、マルチプレクサ２０１４Ｅに高速化エンジンの制御に関わる特殊なフレーム（以降、制御フレームと呼ぶ）を送り、又、制御フレーム解析２０１４Ｄより制御フレームを受信する。制御フレームで公開鍵を受け取った場合は、暗号化２０１４Ｇに通知する。制御フレームで秘密鍵を受け取った場合は、復号化２０１４Ｌに通知する。制御フレームで共通鍵を受け取った場合は、暗号化２０１４Ｇと復号化２０１４Ｌに通知する。制御フレームで、ＳＳＬセッションの相手方機器（セッション中継装置１０）のＩＰアドレスや宛先ポート、及び自ノード（ゲートウェイ装置２０）側のＳＳＬセッションの送信元ポート番号や送信元ＩＰアドレス、更には宛先ＭＡＣアドレスと、自ノードの送信元ＭＡＣアドレスを受け取った場合、フレーム解析２０１４Ｂに通知する。更に、制御フレームで暗号化処理の開始、及び終了の命令を受け取った場合、フレーム解析２０１４Ｂに通知する。

【０１９０】
以上のように、高速化エンジン２０１４は、中間ドライバ２００６や、中間ドライバ１００８と対になって処理を行う。
【０１９１】
図１３は、第１の実施の形態における端末２１内に存在する、ＣＰＵ２１０内で動作するソフトウェア構成を詳細に示したブロック図である。
【０１９２】
ＣＰＵ２１０内で動作するソフトウェアは、アプリケーション２１０１、ＴＣＰ２１０２、ＩＰルーティング２１０３、ＩＰスタック２１０４、及びドライバ２１０５で構成される。
【０１９３】
尚、端末２１は、図５に示すセッション中継装置１０と同様のハードウェア構成を有するが、図５におけるＣＰＵ１００がＣＰＵ２１０となり、ＮＩＣ１０１がＮＩＣ２１１になる点において異なる。
【０１９４】
図１３に挙げたソフトウェアの中、ＴＣＰ２１０２、ＩＰルーティング２１０３、ＩＰスタック２１０４は、通常は、Ｗｉｎｄｏｗｓ、Ｌｉｎｕｘ、ＢＳＤ等のＯＳ（オペレーティングシステム）に含まれるソフトウェアである。特に、Ｗｉｎｄｏｗｓの場合は、一般的には、ユーザがプログラムを書き換えることは出来ない。
【０１９５】
ＣＰＵ２１０内では、実際には、図１３に示したソフトウェア以外にも多くのソフトウェアが動作しているが、図１３においては、本発明に無関係なソフトウェアは省略している。
【０１９６】
アプリケーション２１０１は、サーバ３１内のアプリケーション３１０１と双方向の通信を行うアプリケーションである。アプリケーション２１０１は、代表的には、ＷＥＢブラウザソフトが適用されるが、この場合、サーバ３１内のアプリケーション３１０１は、ＷＥＢサーバアプリケーションが適用される。アプリケーション２１０１は、ＷＥＢブラウザソフトの他、ＴＥＬＮＥＴクライアントソフト、ＦＴＰクライアントソフト、会計クライアントソフト、ファイル共有クライアントソフト、データベースクライアントソフト等、各種のアプリケーションが適用可能である。
【０１９７】
この場合、サーバ３１内のアプリケーション３１０１も、アプリケーション２１０１に対応し、ＴＥＬＮＥＴサーバソフト、ＦＴＰサーバソフト、会計サーバソフト、ファイル共有サーバソフト、データベースサーバソフト等が適用される。
【０１９８】
ＴＣＰ２１０２は、図１０に示すＴＣＰ２００３や、図６に示すＴＣＰ１００３、及びＴＣＰ１００５と同様の動作を行う。すなわち、ＴＣＰ２１０２は、以下の（１）～（４）の処理により、データを一定形式のフォーマットに整えてパケット化し又はパケットからデータを復元する機能を有する。
（１）　アプリケーション２１０１からデータを受け取り、このデータにパケットの欠落や順序逆転を検知する為のＴＣＰヘッダを付加して、ＩＰルーティング２１０３に送る。ここで、大きなデータの場合は、分割（フラグメントとも言う）処理を行う。
（２）　ＩＰルーティング２１０３からパケットを受け取り、ＴＣＰヘッダを参照して順序逆転やパケットの欠落を検知し、順序逆転も欠落も発生していない場合は、パケットからＴＣＰヘッダを外し、アプリケーション２１０１に送る。この際、パケットが届いたことを知らせるＡＣＫパケットをパケットの送信元に返信する。
（３）　（２）において、仮に、パケットの欠落が発生している場合は、再送要求パケットを送信する。又、順序逆転やフラグメントが発生している場合には、後から届くパケットを待って、データを復元する。

（４）　ＡＣＫパケットを受け取り、（１）におけるパケットの送信速度を調整する。

【０１９９】

ここで、ＴＣＰ２１０２においては、最大フレーム長を小さく設定する。これは、中間ドライバ１００８、高速化エンジン２０１４、ＴＣＰ１００３、更にはＴＣＰ１００４によるフラグメント処理を防止する為である。

【０２００】

ＩＰルーティング２１０３は、図１０に示すＩＰルーティング２００４や、図６に示すＩＰルーティング１００６と同様の動作を行う。すなわち、ＩＰルーティング２１０３は、ＴＣＰ２１０２、若しくはＩＰスタック２１０４からパケットを受け取り、宛先ＩＰアドレスと宛先ポート番号を参照して、ＩＰスタック２１０４、若しくはＴＣＰ２１０２に、パケットを転送する機能を有する。

【０２０１】

ＩＰスタック２１０４は、図１０に示すＩＰスタック２００５や、図６に示すＩＰスタック１００７と同様の動作を行う。すなわち、ＩＰスタック２１０４は、以下に示す機能を有する。

（１）　ＩＰルーティング２１０３からパケットを受け取り、ＭＡＣアドレス等のＥｔｈｅｒｎｅｔヘッダを付加してドライバ２１０５に渡す。

（２）　ドライバ２１０５から受信したパケットよりＭＡＣヘッダを削除して、ＩＰルーティング２１０３に渡す。

（３）　（１）において付加するＭＡＣアドレス等を決定する為、ＡＲＰプロトコルを送受信する。

（４）　ＤＨＣＰプロトコル若しくは手動設定により、ＩＰアドレス、デフォルトルート、ネットマスクなどＩＰ通信に必要な設定を受け、これを管理する。

【０２０２】

ドライバ２１０５は、図１０に示すドライバ２００７や、図６に示すＩＰスタック１００７と同様の動作を行う。すなわち、ドライバ２１０５は、ＮＩＣ２１１と、ＣＰＵ２１０内で動作するソフトウェアとの間の仲介をするソフトウェアであり、ＮＩＣ２１１からパケットを受け取り、ＩＰスタック２１０４に送る機能を有し、更に、ＩＰスタック２１０４からパケットを受け取り、ＮＩＣ２１１に送る機能を有する。

【０２０３】

図１４は、第１の実施の形態におけるＦｉｒｅｗａｌｌ２３の構成を詳細に示したブロック図である。

【０２０４】

Ｆｉｒｅｗａｌｌ２３は、図５に示すセッション中継装置１０に、ＮＩＣ２３２を追加した構成のコンピュータである。Ｆｉｒｅｗａｌｌ２３は、ＣＰＵ２３０と、ＮＩＣ２３１と、ＮＩＣ２３２と、メモリ２３３と、ＨＤＤ２３４と、キーボード２３５と、マウス２３６と、グラフィック２３７により構成されるが、キーボード、マウス、グラフィックは接続されない場合もある。

【０２０５】

ＣＰＵ２３０は、図５におけるＣＰＵ１００と同様である。

【０２０６】

ＮＩＣ２３１は、図５におけるＮＩＣ１０１と同様である。

【０２０７】

ＮＩＣ２３２は、図５におけるＮＩＣ１０１と同様である。

【０２０８】

メモリ２３３と、ＨＤＤ２３４と、キーボード２３５と、マウス２３６と、グラフィック２３７についても、各々、図５におけるメモリ１０２と、ＨＤＤ１０３と、キーボード１０４と、マウス１０５と、グラフィック１０６と同様である。

【０２０９】

図１５は、第１の実施の形態におけるＦｉｒｅｗａｌｌ２３内に存在する、ＣＰＵ２３

０内で動作するソフトウェア構成を詳細に示したブロック図である。

【０２１０】

ＣＰＵ２３０内で動作するソフトウェアは、ＩＰルーティング２３０１、ＩＰスタック２３０２、ＩＰスタック２３０３、ドライバ２３０４、およびドライバ２３０５で構成される。

【０２１１】

図１５に挙げたソフトウェアの中、ＩＰルーティング２３０１、ＩＰスタック２３０２、及びＩＰスタック２３０３は、通常は、Ｗｉｎｄｏｗｓ、Ｌｉｎｕｘ、ＢＳＤ等のＯＳ（オペレーティングシステム）に含まれるソフトウェアである。特に、Ｗｉｎｄｏｗｓの場合は、一般的には、ユーザがこのソフトウェアのプログラムを書き換えることは出来ない。

【０２１２】

ＣＰＵ２３０内では、実際には、図１５に示したソフトウェア以外にも多くのソフトウェアが動作しているが、図１５においては、本発明に無関係なソフトウェアは省略している。

【０２１３】

ＩＰルーティング２３０１は、ＩＰスタック２３０２、もしくはＩＰスタック２３０３からパケットを受け取り、宛先ＩＰアドレスと宛先ポート番号を参照して、ＩＰスタック２３０３、若しくはＩＰスタック２３０２に、パケットを転送する機能を有する。この際、ＩＰルーティング２３０１は、インターネット１（ＩＰスタック２３０３側）とイントラネット２（ＩＰスタック２３０２側）の間の通信を、予め決められた設定に従って制限する動作を行う。例えば、イントラネット２内部の装置からインターネット１の各装置へＴＣＰを用いて通信開始の要求をした場合、以降の通信は双方向で自由に行えるが、逆に、インターネット１の各装置からイントラネット２の各装置へＴＣＰを用いて通信開始の要求を行った場合、この要求を遮断し、以降の通信も双方向で遮断する。遮断の際は、パケットを廃棄する処理を行う。

【０２１４】

ＩＰスタック２３０２は、図１３に示すＩＰスタック２１０４、図１０に示すＩＰスタック２００５や、図６に示すＩＰスタック１００７と同様の動作を行う。すなわち、ＩＰスタック２３０２は、以下に示す機能を有する。

（１） ＩＰルーティング２３０１からパケットを受け取り、ＭＡＣアドレス等のＥｔｈｅｒｎｅｔヘッダを付加してドライバ２３０４に渡す。

（２） ドライバ２３０４から受信したパケットよりＭＡＣヘッダを削除して、ＩＰルーティング２３０１に渡す。

（３） （１）において付加するＭＡＣアドレス等を決定する為、ＡＲＰプロトコルを送受信する。

（４） ＤＨＣＰプロトコル若しくは手動設定により、ＩＰアドレス、デフォルトルート、ネットマスクなどＩＰ通信に必要な設定を受け、これを管理する。

【０２１５】

ＩＰスタック２３０３は、ＩＰスタック２３０２と同様の動作を行う。

【０２１６】

ドライバ２３０２は、図１０に示すドライバ２００７や、図６に示すＩＰスタック１００７と同様の動作を行う。すなわち、ドライバ２３０２は、ＮＩＣ２３１と、ＣＰＵ２３０内で動作するソフトウェアとの間の仲介をするソフトウェアであり、ＮＩＣ２３１からパケットを受け取りＩＰスタック２３０２に送る機能を有し、更に、ＩＰスタック２３０２からパケットを受け取り、ＮＩＣ２３１に送る機能を有する。

【０２１７】

ドライバ２３０５は、ドライバ２３０２と同様の動作を行う。

【０２１８】

［動作の説明］

［ＳＳＬセッションの確立動作］

図１６を用いて、第１の実施の形態において、ゲートウェイ装置２０からセッション中継装置１０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合を例に挙げて、動作の説明を行う。

【０２１９】

この際、ＨＵＢ２２やＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ２３のＬＡＮ側，Ｆｉｒｅｗａｌｌ３３のＬＡＮ側、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。又、ＨＵＢ１１は、Ｆｉｒｅｗａｌｌ２３のＷＡＮ側、Ｆｉｒｅｗａｌｌ３３のＷＡＮ側、セッション中継装置１０の各装置のＭＡＣアドレスを学習しているものとする。又、Ｆｉｒｅｗａｌｌ２３およびＦｉｒｅｗａｌｌ３３は、イントラネット内部の装置（ＬＡＮ側）からインターネットの各装置（ＷＡＮ側）へＴＣＰを用いて通信開始の要求をした場合、通信開始の要求以降の通信は双方向で自由に行えるが、逆に、インターネットの各装置（ＷＡＮ側）からイントラネットの各装置（ＬＡＮ側）へＴＣＰを用いて通信開始の要求を行った場合、この要求は遮断され、以降の通信も双方向で遮断されるとする。

【０２２０】

セッション中継装置１０内の中継アプリケーション１００１は、起動後ゲートウェイ装置２０からの接続待ち受け状態になると、中間ドライバ１００８に対して、待ち受け開始を通知する。この通知には、セッション中継装置１０のＩＰアドレス、中継アプリケーション１００１の待ち受けポート番号が含まれる。

【０２２１】

中間ドライバ１００８は、中継アプリケーション１００１からの通知を受けると、フレーム解析処理において、中継アプリケーション１００１宛てのパケットが到着した際に、ＴＣＰ接続/終端などの処理が出来るように設定を行う。

【０２２２】

ゲートウェイ装置２０内の高速化エンジン制御２００１は、ユーザからのセッション中継装置１０内の中継アプリケーション１００１への接続要求を受け、ＳＳＬ２００２にセッション中継装置１０内の中継アプリケーション１００１への通信開始を指示する。同時に、中間ドライバ２００６に対して、セッション中継装置１０内の中継アプリケーション１００１への通信開始を通知する。この通知には、セッション中継装置１０のＩＰアドレス、中継アプリケーション１００１のポート番号、及び高速化エンジン制御２００１の送信元ポート番号、更にゲートウェイ装置２０のＩＰアドレスが含まれる。

【０２２３】

ＳＳＬ２００２は、高速化エンジン制御２００１からの通信開始指示を受け、ＳＳＬ１００２との間でＳＳＬセッションを確立する為に、ＴＣＰ２００３にセッション中継装置１０内の中継アプリケーション１００１への通信開始を指示する。

【０２２４】

ＴＣＰ２００３は、ＳＳＬ２００２からの通信開始指示を受け、ＴＣＰ１００３との間でＴＣＰセッションを確立する為に、ＩＰルーティング２００４に対して、ＴＣＰ１００３とのＴＣＰセッション確立要求パケット（ＳＹＮ）を送信する。このパケットはＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにセッション中継装置１０宛、宛先ポート番号にＴＣＰ１００３が設定されている。このＴＣＰセッション確立要求パケットとは、ＴＣＰセッションの確立時に、スリーウェイハンドシェーク（ｔｈｒｅｅ ｗａｙ ｈａｎｄｓｈａｋｅ）の為に送信される、ＳＹＮパケットのことである。本明細書においては、ＴＣＰセッション確立動作の説明を簡略化するため、スリーウェイハンドシェークで送受信されるパケットうち、ＳＹＮパケットをＴＣＰセッション確立要求パケットと呼び、ＳＹＮパケット＋ＡＣＫパケットを応答パケットと呼んでいる。また実際にはＡＣＫパケットも送信されるが、ＡＣＫパケットについてはＳＹＮパケットと同様に転送されるため、本動作の説明では説明を省略する。

【０２２５】

ＩＰルーティング２００４は、ＴＣＰ２００３から受信したパケットの宛先ＩＰアドレスと宛先ポート番号を参照し、パケットをＩＰスタック２００５に転送する。

【０２２６】

ＩＰスタック２００５は、ＩＰルーティング２００４より受信したパケットに、Ｆｉｒｅｗａｌｌ１２３内のイントラネット２側のＭＡＣアドレスを宛先ＭＡＣアドレスとして付加し、更に送信元ＭＡＣアドレスに自ノードのＭＡＣアドレスを設定してフレームを作成し、中間ドライバ２００６に転送する。

【０２２７】

中間ドライバ２００６は、ＩＰスタック２００５からフレームを受信し、フレーム解析を行う。解析の結果、フレームは予め高速化エンジン制御２００１より通知された宛先ＩＰ、宛先ポート、送信元ＩＰ、送信元ポートが付加されたフレームであるので、カプセル化解除においてＭＡＣヘッダを取り外し、パケットにする。そして、中間ドライバ２００６のＴＣＰでＴＣＰ２００３からＴＣＰ１００３へのＴＣＰ処理を終端させる。すなわち、ＴＣＰ２００３は、元々は、ＴＣＰ１００３に対してＴＣＰセッション確立要求を送信したが、実際は、この要求に対して中間ドライバ２００６内のＴＣＰが受信して保留し、ＴＣＰ２００３と中間ドライバ２００６内のＴＣＰとの間で、ＴＣＰセッションの確立を終端する。

【０２２８】

中間ドライバ２００６は、上記確立要求の処理を終端させる際、中間ドライバ１００８に対して、ＴＣＰ１００３との間でセッション（ＵＤＰ等の輻輳制御の無いセッション）の接続を要求する為に、ドライバ２００７に接続要求のパケットを送る。尚、この接続要求パケットはＴＣＰ規格に沿ったパケットではなく、本発明の通信システムにおける独自のパケットである。この接続要求パケットには宛先ＩＰアドレスとしてセッション中継装置１０を、宛先ポート番号としてＴＣＰ１００３を設定する。そしてこのパケットにＦｉｒｅｗａｌｌ２３内のイントラネット２側のＭＡＣアドレスを宛先ＭＡＣアドレスとして付加し、更に送信元ＭＡＣアドレスに自ノードのＭＡＣアドレスを設定して、接続要求フレームが生成する。

【０２２９】

ドライバ２００７は中間ドライバ２００６から接続要求フレームを受信し、ＭＡＣ２０１１に転送する。

【０２３０】

ＭＡＣ２０１１はドライバ２００７から接続要求フレームを受信し、高速化エンジン２０１４に転送する。

【０２３１】

高速化エンジン２０１４は、ＭＡＣ２０１１から接続要求フレームを受信し、そのままＰＨＹ２０１２に転送する。

【０２３２】

ＰＨＹ２０１２は、高速化エンジン２０１４から接続要求フレームを受信し、ポート２０１３に転送する。

【０２３３】

ポート２０１３は、ＰＨＹ２０１２から接続要求フレームを受信し、イーサネットケーブルを経由してポート２２２に転送する。

【０２３４】

ポート２２２は、ポート２０１３から接続要求フレームを受信し、ブリッジ２２４に転送する。

【０２３５】

ブリッジ２２４は、ポート２２２からの接続要求フレームを受信すると、ＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ２３のＬＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームをそのままＦｉｒｅｗａｌｌ２３側のポート（ポート２２３）に出力する。

【０２３６】
ポート２２３は、ブリッジ２２４から接続要求フレームを受信し、イーサネットケーブルを経由してＦｉｒｅｗａｌｌ２３内のポート２３１３に転送する。
【０２３７】
Ｆｉｒｅｗａｌｌ２３は、ＨＵＢ２２内のポート２２３から接続要求フレームを受信し、ポート２３１３、ＰＨＹ２３１２、ＭＡＣ２３１１、ドライバ２３０４、ＩＰスタック２３０２、ＩＰルーティング２３０１、ＩＰスタック２３０４、ドライバ２３０５、ＭＡＣ２３２１、ＰＨＹ２３２２、ポート２３２３の経路でフレームを転送し、ＨＵＢ１１内のポート１１に転送する。
【０２３８】
ＨＵＢ１１内のポート１１１は、ポート２３２３から接続要求フレームを受信し、ブリッジ１１４に転送する。
【０２３９】
ブリッジ１１４は、ポート１１１からの接続要求フレームを受信すると、ＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがセッション中継装置１０側のものであることから、過去のルーティング学習結果に基づき、このフレームをそのままセッション中継装置１０側のポート（ポート１１２）に出力する。
【０２４０】
ポート１１２は、ブリッジ１１４から接続要求フレームを受信し、イーサネットケーブルを経由してセッション中継装置１０内のポート１０１３に転送する。
【０２４１】
セッション中継装置１０は、ＨＵＢ２２内のポート１１２から接続要求フレームを受信し、ポート１０１３、ＰＨＹ１０１２、ＭＡＣ１０１１、ドライバ１００９の経路でフレームを転送し、中間ドライバ１００８に転送する。
【０２４２】
中間ドライバ１００８は、ドライバ１００９から接続要求フレームを受信し、フレームの解析を行う。
解析の結果、このフレームは予め中継アプリケーション１００１より通知された、中継アプリケーション１００１への宛先ＩＰ、及び宛先ポートが付加されたフレームであるので、このフレームを受信し、カプセル化解除においてＭＡＣヘッダを取り外し、パケットにする。このパケットは、中間ドライバ２００６から中間ドライバ１００８に向けて送信された、ＴＣＰ１００３への接続要求パケットである為、中間ドライバ１００８内のＴＣＰは、ＴＣＰ１００３との間でＴＣＰセッションを確立する為に、ＴＣＰ１００３とのセッション確立に必要なパケットを送信する。このパケットはＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにセッション中継装置１０宛、宛先ポート番号にＴＣＰ１００３が設定され、更に送信元ＩＰアドレスにはゲートウェイ装置２０のＩＰアドレスが設定され、送信元ポート番号にはＴＣＰ２００３のポート番号が設定される。そしてこのパケットには、中間ドライバ１００８内の再カプセル化１００８ＥによってＭＡＣアドレスが付加され、フレームの形にしてＩＰスタック１００７に転送される。セッション確立に必要なパケットとは、ＴＣＰセッションの確立時に、スリーウェイハンドシェーク（ｔｈｒｅｅ　ｗａｙ　ｈａｎｄｓｈａｋｅ）の為に送信される、ＳＹＮパケットパケットのことである。本明細書においては、ＴＣＰセッション確立動作の説明を簡略化するため、スリーウェイハンドシェークで送受信されるパケットうち、ＳＹＮパケットをＴＣＰセッション確立要求パケットと呼び、ＳＹＮ＋ＡＣＫパケットを応答パケットと呼んでいる。また実際にはＡＣＫパケットも送信されるが、ＡＣＫパケットについてはＳＹＮパケットと同様に転送されるため、説明を省略する。
【０２４３】
中間ドライバ１００８内のＴＣＰは、ＴＣＰ２００３の名前をかたってＴＣＰ１００３に対して接続要求を送信する。従って、ＴＣＰ１００３は恰もＴＣＰ２００３と通信しているかのように認識し、更にＴＣＰ２００３は恰もＴＣＰ１００３と通信しているかのよ

うに認識する。しかしながら、実際のＴＣＰの確立処理は、ＴＣＰ２００３と中間ドライバ２００６内のＴＣＰとの間、及び、中間ドライバ１００８とＴＣＰ１００３との間で行われ、更に、中間ドライバ２００６と中間ドライバ１００８との間は、ＵＤＰ等の輻輳制御のない方法（本発明の通信システムにおける独自のパケット）で、別途に通信が行われる。そして、ＴＣＰ２００３と中間ドライバ２００６間のＴＣＰセッションと、中間ドライバ２００６と中間ドライバ１００８の間のＵＤＰ等何らかの通信セッション、更に中間ドライバ１００８とＴＣＰ１００３の間のＴＣＰセッションが、中間ドライバ２００６及び中間ドライバ１００８によって相互に接続・中継されることにより、恰もＴＣＰ２００３とＴＣＰ１００３との間でＴＣＰセッションが確立しているかのように通信が行われる。

【０２４４】
ＩＰスタック１００７は、中間ドライバからフレームを受信し、ＭＡＣヘッダを外してパケットにしてＩＰルーティング１００６に転送する。

【０２４５】
ＩＰルーティング１００６は、ＩＰスタック１００７より受信したパケットの宛先ポート番号を参照し、ＴＣＰ１００３側のポート番号が付加されていることから、このパケットをＴＣＰ１００３に転送する。

【０２４６】
ＴＣＰ１００３は、ＩＰルーティング１００６よりパケットを受信する。このパケットはＴＣＰセッション確立要求パケット（ＳＹＮ）であるので、ＴＣＰプロトコルに従い、セッションの確立要求に対して応答パケット（ＳＹＮ＋ＡＣＫ）を返送する。この際、ＴＣＰ１００３は、ＴＣＰセッション確立要求は、ＴＣＰ２００３から届いたものであると認識する。これは、実際の確立要求は中間ドライバ１００８内のＴＣＰから送信されたものであるが、中間ドライバ１００８内のＴＣＰは、ＴＣＰ２００３を騙ってＴＣＰ１００３にＴＣＰセッション確立要求を行った為、ＴＣＰ１００３は、恰も、ＴＣＰ２００３とセッションを確立すると認識する。

【０２４７】
従って、ＴＣＰ１００３は、応答パケット（ＳＹＮ＋ＡＣＫ）を、ＴＣＰ２００３宛てに送信する。すなわち、応答パケットの宛先ＩＰはゲートウェイ装置２０のＩＰアドレスが設定され、応答パケットの宛先ポートは、ＴＣＰ２００３のポート番号が設定される。

【０２４８】
応答パケットは、ＩＰルーティング１００６を経由して、ＩＰスタック１００７に送られ、ここでＭＡＣヘッダを付加されて応答フレームとなり、中間ドライバ１００８に届く。

【０２４９】
中間ドライバ１００８は、応答フレームを受信すると、中間ドライバ１００８内のカプセル化解除において応答フレームのＭＡＣヘッダを外して応答パケットを取り出し、ＴＣＰでこの応答パケット（ＳＹＮ＋ＡＣＫ）を受信してＡＣＫパケットを返答してＴＣＰ処理を終端する。そして中間ドライバ２００６に対して、セッション（ＵＤＰ等の輻輳制御の無いセッション）の接続完了通知の為の接続完了通知パケットを送信する。この接続完了通知パケットは、ＴＣＰ規格に沿ったパケットではなく、本発明の通信システムにおける独自のパケットであり、宛先ＩＰアドレスとしてゲートウェイ送装置２０を、宛先ポート番号としてＴＣＰ２００３を、送信元ＩＰアドレスとしてセッション中継装置１０を、送信元ポート番号としてＴＣＰ１００３を設定する。そして中間ドライバ１００８内の再カプセル化１００８Ｄにおいて、接続完了通知パケットにＭＡＣヘッダを付加し、接続完了通知フレームを生成する。

【０２５０】
接続完了通知フレームは、接続要求とは逆の経路、即ち、ドライバ１００９，ＮＩＣ１０１，ＨＵＢ１１，ＮＩＣ２３２、ＣＰＵ２３０，ＮＩＣ２３１、ＨＵＢ２２，ＮＩＣ２０１を経由して、ＣＰＵ２００内の中間ドライバ２００６に届く。

【０２５１】
中間ドライバ２００６は、接続完了通知フレームを受信し、フレーム解析を行う。解析の結果、受信したフレームは予め高速化エンジン制御２００１より通知された、高速化エンジン制御２００１への宛先ＩＰ、及び宛先ポートが付加されたフレームであるので、このパケットを受信し、カプセル化解除においてＭＡＣヘッダを取り外し、パケットにする。パケットは、中間ドライバ１００８から中間ドライバ２００６に向けて送信された、ＴＣＰ１００３と中間ドライバ１００８との間の接続完了通知パケットである為、中間ドライバ２００６内のＴＣＰは、ＴＣＰプロトコルに従い、セッション確立の為に必要な応答パケット（ＳＹＮ＋ＡＣＫ）をＴＣＰ２００３に送る為、ＩＰスタック２００５に対して、応答パケットを送信する。

【０２５２】
応答パケットは、ＩＰスタック２００５、ＩＰルーティング２００４を経由し、ＴＣＰ２００３に到達する。

【０２５３】
ＴＣＰ２００３は、ＩＰルーティング２００４より応答パケット（ＳＹＮ＋ＡＣＫ）を受信する。このパケットはＴＣＰセッションの確立要求に対する応答パケットであるので、ＳＳＬ２００２に対して、ＴＣＰ１００３とのＴＣＰセッション接続完了を通知する。この際、ＴＣＰ２００３は、受信した応答パケット（ＳＹＮ＋ＡＣＫ）が、ＴＣＰ１００３から届いたものであると認識する。これは、実際の応答パケットは中間ドライバ２００６内のＴＣＰから送信されたものであるが、中間ドライバ２００６内のＴＣＰは、ＴＣＰ１００３を騙ってＴＣＰ２００３にセッション確立の応答を行った為、ＴＣＰ２００３は、恰も、ＴＣＰ１００３から応答があったと認識する。

【０２５４】
ＴＣＰ２００３は応答パケット（ＳＹＮ＋ＡＣＫ）を受信すると、この応答パケットに対してＡＣＫパケットを生成してＴＣＰ１００３宛に送信する。このＡＣＫパケットは、中間ドライバ２００６のＴＣＰがＩＰルーティング２００４及びＩＰスタック２００５を介して受信し、ＴＣＰ処理を終端させる。

【０２５５】
ＳＳＬ２００２は、ＴＣＰ２００３からの接続完了通知を受け、ＳＳＬ１００２との間でＳＳＬセッションを確立する為、ＳＳＬプロトコルに従い、ＳＳＬセッションの確立要求の為のパケット（ＳＳＬセッション確立要求パケット）を送信する。

【０２５６】
ＳＳＬセッション確立要求パケットは、ＴＣＰ２００３で受信されると、ＴＣＰ２００３と中間ドライバ２００６内のＴＣＰとの間で設定されたＴＣＰセッションを通り、中間ドライバ２００６に到着する。

【０２５７】
中間ドライバ２００６は、ＳＳＬセッション確立要求パケットのＴＣＰを終端し、ＵＤＰ等の輻輳制御の掛からないヘッダを付け、パケットを中間ドライバ１００８に向け送信する。パケットはＮＩＣ２０１、ＨＵＢ２２，ＮＩＣ２３１，ＣＰＵ２３０，ＮＩＣ２３２、ＨＵＢ１１、ＮＩＣ１０１を経由して、中間ドライバ１００８に到着する。この際、ＮＩＣ２０１内の高速化エンジン２０１４は、ＭＡＣ１０１１から受信したパケットを、そのままＰＨＹ２０１２に転送する。

【０２５８】
中間ドライバ１００８は、ＳＳＬセッション確立要求パケットを受信すると、中間ドライバ１００８内のＴＣＰとＴＣＰ１００３との間で設定されたＴＣＰセッションを通り、ＴＣＰ１００３に到着する。

【０２５９】
ＴＣＰ１００３は、パケットをＳＳＬ１００２に転送する。

【０２６０】
ＳＳＬ１００２は、ＳＳＬセッション確立要求の内容を検証し、問題が無ければ、中継

アプリケーション１００１に対して、ＳＳＬ２００２とのセッション確立を通知すると同時に、ＳＳＬプロトコルに従い、ＳＳＬ２００２に対してＳＳＬセッション確立応答パケットを送信する。

【０２６１】

ＳＳＬセッション確立応答パケットは、ＳＳＬセッション確立要求パケットとは逆の経路、即ち、ＴＣＰ１００３と中間ドライバ１００８との間のＴＣＰセッションを経由して中間ドライバ１００８に到達し、中間ドライバ１００８と中間ドライバ２００６の間のＵＤＰ等の輻輳制御のないセッションを経由して中間ドライバ２００６に到達する。更に、中間ドライバ２００６とＴＣＰ２００３との間のＴＣＰセッションを経由して、ＳＳＬ２００２に到達する。

【０２６２】

ＳＳＬ２００２は、ＳＳＬセッション確立要求の内容をＳＳＬプロトコルに従って検証し、問題が無ければ、高速化エンジン制御２００１に対して、ＳＳＬ２００２とＳＳＬ１００２との間のＳＳＬセッション確立を通知する。

【０２６３】

高速化エンジン制御２００１は、ＳＳＬセッション確立通知を受けると、中間ドライバ２００６に対して、ＳＳＬセッション確立通知によって受信したＳＳＬ１００２の公開鍵と、ＳＳＬ２００２の秘密鍵、さらにはＳＳＬ１００２とＳＳＬ２００２の間の共通鍵を通知する。

【０２６４】

中間ドライバ２００６は、公開鍵、秘密鍵および共通鍵の通知を受けると、公開鍵、秘密鍵および共通鍵、ＳＳＬセッションの相手方機器のＩＰアドレス（セッション中継装置１０のＩＰアドレス）、ＳＳＬセッションの相手方機器の宛先ポート（ＴＣＰ１００３のポート）、自ノード側のＳＳＬセッションの送信元ポート番号（ＴＣＰ２００３のポート）、送信元ＩＰアドレス（ゲートウェイ装置２０のＩＰアドレス）、及び開始命令を制御フレームに載せ、高速化エンジン２０１４に通知する。

【０２６５】

制御フレームは、ドライバ２００７、ＭＡＣ２０１１を通じて高速化エンジン２０１４に到達する。

【０２６６】

高速化エンジン２０１４は、ＭＡＣアドレス等により制御フレームを判別し、制御フレーム送受信部で受信する。そして、公開鍵、秘密鍵および共通鍵を、各々、復号化および暗号化に使用する為保存し、ＩＰアドレスやポート番号をフレーム解析の為に保存する。そして、高速化処理開始命令を受け、フレーム解析、暗号化、及び複号化の処理を開始する。

【０２６７】

高速化エンジン２０１４は、高速化処理開始命令以前は、制御フレーム以外のＭＡＣ２０１１から受信したフレームは、全てそのままＰＨＹ２０１２に送信し、ＰＨＹ２０１２から受信したフレームは、全てそのままＭＡＣ２０１１に送信していた。しかしながら、高速化処理開始命令以降は、制御フレーム以外のＭＡＣ２０１１から受信したフレームを全てそのままＰＨＹ２０１２に送信する動作には変わりないが、ＰＨＹ２０１２から受信したフレームについては、以下のような処理を行う。

（１）　ゲートウェイ装置２０宛て、かつ、ＳＳＬ１００２で暗号化されたフレームであれば、ＵＤＰ等のカプセル化を解除し、必要であれば、フラグメントを解除し、フレームを復号化し、ＰＨＹ２０１２側に送信する。

（２）　（１）以外の自ノード宛てフレームであれば、ＭＡＣ２０１１に転送する。

（３）　ブロードキャストフレーム、若しくはマルチキャストフレームであれば、フレームをコピーして、一方はそのままＭＡＣ２０１１に転送し、もう一方は暗号化とカプセル化を行い、ＳＳＬ１００２（ＰＨＹ２０１２側）に送信する。必要であれば、フラグメントを分割も行う。

（４）　（１）～（３）以外のフレームであれば、暗号化とカプセル化を行い、ＳＳＬ１００２（ＰＨＹ２０１２側）に送信する。必要であれば、フラグメントを分割も行う。

【０２６８】

以上のようにして、高速化エンジン２０１４と中間ドライバ１００８との間で、フレーム転送の為のＵＤＰ等の輻輳制御の無いセッションが確立される。又、高速化エンジン２０１４とＳＳＬ１００２との間で、ＳＳＬセッションが確立される。

【０２６９】

すなわち、セッション中継装置１０のＳＳＬ１００２は、ＳＳＬセッション確立要求時のみ、ゲートウェイ装置のＳＳＬ２００２と遣り取りを行うが、ＳＳＬセッション確立が終了すると、ＳＳＬセッション確立以降は高速化エンジン２０１４との間で、ＳＳＬの暗号化および復号化の遣り取りを行う。

【０２７０】

又、セッション中継装置１０の中間ドライバ１００８は、ＳＳＬセッション確立要求時のみ、ゲートウェイ装置２０の中間ドライバ２００６とフレームの遣り取りを行うが、ＳＳＬセッションが確立した後は、高速化エンジン２０１４との間でフレームの遣り取りを行う。

【０２７１】

以上により、第１の実施の形態において、ゲートウェイ装置２０からセッション中継装置１０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合の動作が完了する。

【０２７２】

尚、上述した実施例では、ゲートウェイ装置２０からセッション中継装置１０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合を例に挙げて、動作の説明をしたが、ゲートウェイ装置３０からセッション中継装置１０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する動作は、同様の動作が行われる。

また、上述した実施例では、ＴＣＰ１００３に対してのＴＣＰセッション確立要求を中間ドライバ２００６内のＴＣＰが受信して保留し、接続完了通知を受信してから応答パケット（ＳＹＮ＋ＡＣＫ）をＴＣＰ２００３に送信する構成を用いて説明したが、これに限るものではない。即ち、ＴＣＰセッション確立要求を中間ドライバ２００６内のＴＣＰが受信すると、応答パケット（ＳＹＮ＋ＡＣＫ）をＴＣＰ２００３に送信する構成であっても良い。

【０２７３】

［端末２１からサーバ３１へのフレーム転送動作］

図１６を用いて、第１の実施の形態において、端末２１からサーバ３１へフレームを送信する場合を例に挙げて、動作の説明を行う。

【０２７４】

この際、ＨＵＢ２２やＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ２３のＬＡＮ側，Ｆｉｒｅｗａｌｌ３３のＬＡＮ側、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。又、ＨＵＢ１１は、Ｆｉｒｅｗａｌｌ２３のＷＡＮ側、Ｆｉｒｅｗａｌｌ３３のＷＡＮ側、セッション中継装置１０の各装置のＭＡＣアドレスを学習しているものとする。又、Ｆｉｒｅｗａｌｌ２３及びＦｉｒｅｗａｌｌ３３は、イントラネット内部の装置（ＬＡＮ側）からインターネットの各装置（ＷＡＮ側）へＴＣＰを用いて通信開始の要求をした場合、以降の通信は双方向で自由に行えるが、逆に、インターネットの各装置（ＷＡＮ側）からイントラネットの各装置（ＬＡＮ側）へＴＣＰを用いて通信開始の要求を行った場合、この要求は遮断され、以降の通信も双方向で遮断されるとする。

【０２７５】

更に、ゲートウェイ装置２０からセッション中継装置１０へのＳＳＬセッション（セキュアＴＣＰセッション）が、上述の動作例により既に設定されており、同様にゲートウェイ装置３０からセッション中継装置１０へのＳＳＬセッション（セキュアＴＣＰセッショ

ン）も、ゲートウェイ装置２０からセッション中継装置１０へのＳＳＬセッションと同様の方法により、既に設定されているものとする。

【０２７６】

又、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション（アプリケーション３１０１）との間で、既にＴＣＰセッションが構築されているとする。

【０２７７】

端末２１内のアプリケーション２１０１が、サーバ３１内のアプリケーション宛のデータ（図２におけるＦ２４にあたる）を、ＴＣＰ２１０２に渡す。

【０２７８】

ＴＣＰ２１０２は、アプリケーション２１０１からデータを受け取り、ＴＣＰプロトコルに従ってＴＣＰヘッダ（図２におけるＦ２３）やＩＰヘッダ（図２におけるＦ２２）を付けてＩＰパケットとし、ＩＰルーティング２１０３に渡す。この時、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定される。

【０２７９】

ＩＰルーティング２１０３は、ＴＣＰ２１０２から受信したパケットの宛先ＩＰアドレス（サーバ３１宛て）および宛先ポート（ＴＣＰ３００３宛て）を参照し、データをそのままＩＰスタック２１０４に転送する。

【０２８０】

ＩＰスタック２１０４は、ＩＰルーティング２１０３からパケットを受信し、ＭＡＣヘッダ（図２におけるＦ２１）を付けてＥｔｈｅｒｎｅｔフレームを作成し、ドライバ２１０５に渡す。このフレームはＥｔｈｅｒｎｅｔフレームＦ２０のフォーマットを有する。この時、ＩＰスタック２１０４は、ＡＲＰの結果を参照して、フレームのＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスを設定し、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスを設定する。

【０２８１】

ドライバ２１０５は、ＩＰスタック２１０５より上記フレームを受け取り、ＮＩＣ２１１に転送する。

【０２８２】

ＮＩＣ２１１は、ドライバ２１０５よりフレームを受け取り、ＭＡＣ２１１１，ＰＨＹ２１１２，ポート２１１３を経由して、ＨＵＢ２２にフレームを転送する。

【０２８３】

ＨＵＢ２２は、端末２１のＮＩＣ２１１側のポート２２１からフレームを受信すると、ブリッジ２２４においてＦ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームをそのままゲートウェイ装置２０側のポート２２２に出力する。

【０２８４】

ゲートウェイ装置２０内のＮＩＣ２０１は、ポート２０１３でＨＵＢ２２からのフレームを受信し、ＰＨＹ２０１２を経由して、高速化エンジン２０１４に渡す。

【０２８５】

高速化エンジン２０１４は、到着したフレームの宛先ＭＡＣがサーバ３１宛てであることから、高速化エンジン２０１４内の暗号化２０１４Ｇにおいてフレームを暗号化して図３におけるデータＦ１４を作成し、さらにカプセル化２０１４Ｉにおいて図３におけるＦ１１～Ｆ１３の各ヘッダを付加してＥｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームＦ１０のフォーマットにして、再びＰＨＹ２０１２側に転送する。

【０２８６】

この時、ＩＮＥＴ　ＭＡＣ　Ｆ１１内のＭＡＣ　ＤＡにはＦｉｒｅｗａｌｌ２３のＬＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはゲートウェイ装置２０のＭＡＣアドレスが設定される。又、ＩＮＥＴ　ＩＰ　Ｆ１２内のＩＰ　ＤＡにはセッション中継装置１０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡにはゲートウェイ装置

２０のＩＰアドレスが設定される。ＩＮＥＴ　ＴＣＰ　Ｆ１３に関しては、Ｆｉｒｅｗａｌｌ２３を通過する為に、恰も、セッション中継装置１０内のＴＣＰ１００３と通信してるかのように見せかける為のＴＣＰヘッダを付加する。しかし、このＴＣＰヘッダは、実際には中間ドライバ１００８において一旦取り外される為、ＴＣＰ１００３の輻輳制御には影響しない。よって、ここで付加するＦ１３は、ＴＣＰヘッダの形式を持つが、実際には、ＵＤＰの働きしかしない。仮に、Ｆｉｒｅｗａｌｌ２３が存在しなければ、Ｆ１３はＵＤＰヘッダでも構わない。

【０２８７】

ＰＨＹ２０１２は、高速化エンジン２０１４よりフレームを受信すると、ポート２０１３を経由してＨＵＢ２２にフレームを転送する。

【０２８８】

ＨＵＢ２２は、ゲートウェイ装置２２側のポート２２２からフレームを受信すると、ブリッジ２２４においてＦ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ２３のＬＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームをそのままポート２２３よりＦｉｒｅｗａｌｌ２３に出力する。

【０２８９】

Ｆｉｒｅｗａｌｌ２３は、ＮＩＣ２３１でＨＵＢ２２からのフレームを受信し、ポート２３１３，ＰＨＹ２３１２、ＭＡＣ２３１１、ドライバ２３０４の順で転送し、ＩＰスタック２３０２に渡す。

【０２９０】

ＩＰスタック２３０２は、ＭＡＣヘッダＦ１１を取り外して、ＩＰルーティング２３０１に送る。

【０２９１】

ＩＰルーティング２３０１は、受信したフレームのヘッダＦ１２内のＩＰ　ＤＡを参照し、ＩＰ　ＤＡがインターネット１側に存在するものであることから、フレームをＩＰスタック２３０４に転送する。

【０２９２】

ＩＰスタック２３０４は、ＩＰルーティング２３０１よりフレームを受け取り、ヘッダＦ１１を付ける。ここで、Ｆ１１内のＭＡＣ　ＤＡにはセッション中継装置１０のＭＡＣアドレスを設定し、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ２３のＷＡＮ側のＭＡＣアドレスを設定する。このようにして、受信フレームをフレームフォーマットＦ１０の形にして、ドライバ２３０５、ＭＡＣ２３２１、ＰＨＹ２３２２、ポート２３２３を経由して、ＨＵＢ１１に転送する。

【０２９３】

ＨＵＢ１１は、ポート１１１よりＦｉｒｅｗａｌｌ２３からのフレームを受信すると、ブリッジ１１４においてＦ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがセッション中継装置１０のものであることから、過去のルーティング学習結果に基づき、このフレームをそのままセッション中継装置１０側のポート１１２に出力する。

【０２９４】

セッション中継装置１０は、ＨＵＢ１１からのフレームをポート１０１３より受信すると、ＰＨＹ１０１２、ＭＡＣ１０１１、ドライバ１００９を経由して、中間ドライバ１００８に転送する。

【０２９５】

中間ドライバ１００８は、ドライバ１００９よりフレームを受信する。このフレームは、受信時にはフレームフォーマットＦ１０の形をしているが、カプセル化解除１００８Ｇにおいてヘッダ Ｆ１１、ヘッダＦ１２、ヘッダＦ１３を削除し、暗号化されたデータＦ１４のみを残す。そして、データＦ１４をＴＣＰ１００８Ａに渡し、予め、ＴＣＰ１００３と中間ドライバ内のＴＣＰ１００８Ａとの間で設定されたＴＣＰセッションに流す。

【０２９６】

中間ドライバ１００８内のＴＣＰ１００８Ａは、受信したデータＦ１４に、ＴＣＰ１０

０３とのＴＣＰ通信に必要なＴＣＰヘッダＦ１３と、ＩＰヘッダＦ１２を付けて、再カプセル化１００８Ｅに送る。Ｆ１２内のＩＰ　ＤＡにはセッション中継装置１０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡにはゲートウェイ装置２０のＩＰアドレスが設定される。

【０２９７】

中間ドライバ１００８内の再カプセル化１００８Ｅは、ＴＣＰ１００８Ａよりデータを受信すると、これにヘッダＦ１１を付けて、ＩＰスタック１００７に送る。ここで、Ｆ１１内のＭＡＣ　ＤＡにはセッション中継装置１０のＭＡＣアドレスを設定し、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ２３のＷＡＮ側のＭＡＣアドレスを設定する。このようにして、ＴＣＰ１００８Ａからの受信フレームをフレームフォーマットＦ１０の形にして、ＩＰスタック１００７に転送する。

【０２９８】

ＩＰスタック１００７は、中間ドライバ１００８から受信したフレームのＭＡＣヘッダＦ１１を取り外して、ＩＰルーティング１００６に送る。

【０２９９】

ＩＰルーティング１００６は、受信したフレームのヘッダＦ１２内のＩＰ　ＤＡと、Ｆ１３内の宛先ポート番号を参照し、フレームをＴＣＰ１００３に転送する。

【０３００】

ＴＣＰ１００３は、ＩＰルーティング１００６からフレームを受信すると、ＴＣＰプロトコルに従ってＡＣＫパケットを返送するなどの処理を行う。そして、受信したフレームから、ＴＣＰヘッダＦ１３とＩＰヘッダＦ１２を取り外し、データＦ１４をＳＳＬ１００２に転送する。

【０３０１】

ＳＳＬ１００２は、ＴＣＰ１００３からデータＦ１４を受信すると、復号化処理により暗号化を解除し、データＦ１４からＥｔｈｅｒｎｅｔフレームＦ２０、即ち、Ｆ２１～Ｆ２４を取り出し、中継アプリケーション１００１に転送する。

【０３０２】

中継アプリケーション１００１は、ＳＳＬ１００２からフレームＦ２０を受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照して、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを予めゲートウェイ装置３０との間で設定しているＳＳＬセッションに流す。よって、フレームをそのままＳＳＬ１００４側に転送する。

【０３０３】

これ以降、Ｆ２０フォーマットのフレームは、セッション中継装置１０内で再び暗号化され、更にＦ１０のフォーマットにおけるＦ１４の領域に格納され、Ｆ１０のフォーマットで、セッション中継装置１０からＨＵＢ１１、Ｆｉｒｅｗａｌｌ３３、ＨＵＢ３２，ゲートウェイ装置３０の経路でゲートウェイ装置３０に転送される。

【０３０４】

そして、ゲートウェイ装置３０は、ＨＵＢ３２からＦ１０のフォーマットでフレームを受信すると、Ｆ１４の暗号化を解除してＦ１４に格納されているＥｔｈｅｒｎｅｔフレームＦ２０を取り出し、このフレームをＦ２０のフォーマットでＨＵＢ３２を経由してサーバ３１に転送する。

【０３０５】

このフレームは、端末２１からＨＵＢ２２に送信された時の状態そのままに保たれており、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスが設定されている。又、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定されている。

【０３０６】

サーバ３１はＨＵＢ３２から送信されたフレームを受信し、端末２１内のアプリケーション２１０１からサーバ３１内のアプリケーション３１０１への一連のフレーム転送が完了する。

【０３０７】

上記の例とは逆の経路を辿ることで、サーバ３１内のアプリケーション３１０１から端末２１内のアプリケーション２１０１への一連のフレーム転送も、同様に実現可能である。

【０３０８】

尚、本実施の形態では、セッション中継装置内のソフトウェアにおいて、中間ドライバとＴＣＰの間（例えば中間ドライバ１００８とＴＣＰ１００３の間）で、一時的にＴＣＰ ｏｖｅｒ ＴＣＰ形式の処理になる。しかしながら、中間ドライバとＴＣＰの間では、パケットが欠落する可能性が殆ど無い為、ＴＣＰ ｏｖｅｒ ＴＣＰによる速度低下が発生する可能性は、極めて低い。これは、ＴＣＰ ｏｖｅｒ ＴＣＰ問題とは、パケットロスが発生した時に著しい速度低下が発生する問題であり、仮に、パケットロスが発生しなければ、ＴＣＰ ｏｖｅｒ ＴＣＰ形式の処理を行っても、ヘッダＦ１３側のＴＣＰのウインドウサイズは常に大きくなり、速度低下などの問題は発生しないからである。

【０３０９】

上記の方法でヘッダＦ１３側のＴＣＰの輻輳制御と再送制御を事実上停止させても、ヘッダＦ２３側のＴＣＰの輻輳制御と再送制御は通常通り機能する為、端末２１とサーバ３１の各々のアプリケーションから見た場合、端末２１内のＴＣＰとサーバ３１内のＴＣＰの働きにより、輻輳制御、再送制御ともに問題なく行われる。

【０３１０】

［発明の効果］

次に、本実施の形態の効果について説明する。

【０３１１】

本実施の形態に挙げた発明を利用すると、端末２１とサーバ３１との間で、フレームの高速転送が可能になる。

【０３１２】

これは、ＳＳＬセッション確立後、高速化エンジン２０１４を利用することで、ゲートウェイ装置２０やゲートウェイ装置３０におけるＣＰＵ（ソフトウェア処理）によるカプセル化処理および暗号化／復号化処理を排除し、これら処理を全て高速化エンジン（ハードウェア）で実現できる為である。

【０３１３】

更に、これは、ゲートウェイ装置２０とセッション中継装置１０との間の通信において、ヘッダＦ１３の位置のＴＣＰによる輻輳制御と再送制御が発生しないよう、セッション中継装置１０内の中間ドライバ１００８、又はゲートウェイ装置２０内の中間ドライバ２００６において、ＴＣＰセッションの確立要求を終端し、ＴＣＰ ｏｖｅｒ ＴＣＰ問題の発生を回避しているからである。

【０３１４】

又、本実施の形態に挙げた発明を利用すると、高速化処理の為のハードウェア（高速化エンジン）の開発費用や部材費用を、比較的低く抑えることが出来る。

【０３１５】

これは、ＳＳＬの暗号化及び復号化とカプセル化を同一ハードウェア（ＦＰＧＡ／ＡＳＩＣ）で行うことが出来るからである。

【０３１６】

又、これは、比較的安価なＭＡＣとＰＨＹ間のインタフェースに、上記ハードウェアを実装することが出来るからである。

【０３１７】

又、これは、ハードウェアへの実装が難しいＴＣＰ処理をソフトウェアに残し、ハードウェアへの実装が比較的容易で、かつ、高速化処理の効果が大きなＳＳＬの暗号化／復号

化とカプセル化のみをハードウェアで処理できるからである。

【０３１８】

［第２の実施の形態］

本発明の第２の実施の形態は、第１の実施の形態に対して、イントラネット２とイントラネット３を、インターネット１を介さずに直接接続し、更に、ゲートウェイ装置２０とゲートウェイ装置３０との間で、セッション中継装置１０を介さずに、直接、ＳＳＬセッション（セキュアＴＣＰセッション）を設定する点において異なる。

【０３１９】

第２の実施の形態における、端末２１，サーバ３１、ＨＵＢ２２，ＨＵＢ３２、ゲートウェイ装置２０，ゲートウェイ層と３０、イントラネット２、イントラネット３の構成および動作は、ゲートウェイ装置３０からゲートウェイ装置２０、若しくはゲートウェイ装置３０からゲートウェイ装置２０に向けてセッションを張る動作以外は、第１の実施の形態と同じである。

【０３２０】

第２の実施の形態において、イントラネット２は、閉域ＬＡＮだけでなく、インターネット等のオープンなＷＡＮを用いても構わない。

【０３２１】

［構成の説明］

図１７は、第２の実施の形態におけるネットワーク構成を示すブロック図である。

【０３２２】

イントラネット２は、ゲートウェイ装置２０、端末２１、ＨＵＢ２２、及びＦｉｒｅｗａｌｌ３３で構成され、これら機器の相互間で通信を行うローカルエリアネットワーク（ＬＡＮ）である。イントラネット２は、イントラネット３と、Ｆｉｒｅｗａｌｌ３３のＷＡＮ側を介して相互に接続されており、Ｆｉｒｅｗａｌｌ３３の動作により、イントラネット２とイントラネット３の間の通信は、予め決められた設定に従って制限されている。

【０３２３】

イントラネット２内の各装置は、ＨＵＢ２２を介して相互に接続されており、イントラネット２内の各装置間は、前述のＦｉｒｅｗａｌｌ３３等の制限を受けること無く、自由に通信を行うことができる。又、図１７においては、ゲートウェイ装置２０、ゲートウェイ装置３０により、イントラネット２とイントラネット３は、同一のＬＡＮとして動作するよう相互に接続されている為、イントラネット２内の各装置と、イントラネット３内の各装置間も、前述のＦｉｒｅｗａｌｌ３３等の制限を受けること無く、自由に通信を行うことが出来る。

【０３２４】

イントラネット３は、ゲートウェイ３０、サーバ３１、ＨＵＢ３２、及びＦｉｒｅｗａｌｌ３３で構成され、これら機器の相互間で通信を行うローカルエリアネットワーク（ＬＡＮ）である。イントラネット３は、イントラネット２と、Ｆｉｒｅｗａｌｌ３３を介して相互に接続されており、Ｆｉｒｅｗａｌｌ３３の動作により、イントラネット２とイントラネット３の間の通信は、予め決められた設定に従って制限されている。

【０３２５】

イントラネット３内の各装置は、ＨＵＢ３２を介して相互に接続されており、イントラネット３内の各装置間は、前述のＦｉｒｅｗａｌｌ３３等の制限を受けることなく、自由に通信を行うことが出来る。又、図１７においては、ゲートウェイ装置２０、ゲートウェイ装置３０により、イントラネット２とイントラネット３は、同一のＬＡＮとして動作するよう相互に接続されている為、イントラネット３内の各装置と、イントラネット２内の各装置間も、前述のＦｉｒｅｗａｌｌ３３等の制限を受けること無く、自由に通信を行うことが出来る。

【０３２６】

図１８は、第２の実施の形態における、各機器の構成と、フレームの転送経路を詳細に示したブロック図である。

【０３２７】
ゲートウェイ装置２０は、第１の実施の形態におけるゲートウェイ装置２０と同様の構成である。但し、ゲートウェイ装置２０内の高速化エンジン制御２００１の動作については、第１の実施の形態における動作のほか、他のゲートウェイ装置（ゲートウェイ装置３０等）からのセッション接続要求の受信も可能になっている。
【０３２８】
ゲートウェイ装置３０は、第１の実施の形態におけるゲートウェイ装置３０と同様の構成である。すなわち、ゲートウェイ装置２０と、同様の構成を有し、同様の動作を行う。但し、ゲートウェイ装置３０内の高速化エンジン制御３００１の動作については、第１の実施の形態における動作の外、他のゲートウェイ装置（ゲートウェイ装置２０等）からのセッション接続要求の受信も可能になっている。
【０３２９】
端末２１、サーバ３１、ＨＵＢ２２、ＨＵＢ３２に関しては、第１の実施の形態と同様の構成を有し、同様の動作を行う。
【０３３０】
Ｆｉｒｅｗａｌｌ３３は、イントラネット３とイントラネット２とを相互に接続する為の機器であり、ＬＡＮ側ポートはＨＵＢ３２を介してイントラネット３上の各機器と接続され、ＷＡＮ側ポートはＨＵＢ２２を介してイントラネット２上の各機器と接続されている。
【０３３１】
Ｆｉｒｅｗａｌｌ３３は、イントラネット２とイントラネット３の間の通信を、予め決められた設定に従って制限する動作を行う。例えば、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断する。
【０３３２】
従って、第２の実施の形態では、ゲートウェイ装置２０とゲートウェイ装置３０との間で、予めＳＳＬセッションを設定している場合のみ、イントラネット２内の機器からイントラネット３内の機器へのアクセスが可能になる。
【０３３３】
［動作の説明］
［ＳＳＬセッションの確立動作］
図１８を用いて、第２の実施の形態において、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合を例に挙げて、動作の説明を行う。
【０３３４】
この際、ＨＵＢ２２やＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３のＷＡＮ側，Ｆｉｒｅｗａｌｌ３３のＬＡＮ側、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。
【０３３５】
又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間のゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。
【０３３６】
ゲートウェイ装置２０内の高速化エンジン制御２００１は、起動後ゲートウェイ装置３０からの接続待ち受け状態になると、中間ドライバ２００６に対して、待ち受け開始を通知する。この通知には、ゲートウェイ装置２０のＩＰアドレス、高速化エンジン制御２００１の待ち受けポート番号が含まれる。
【０３３７】
中間ドライバ２００６は、高速化エンジン制御２００１からの通知を受けると、フレーム解析処理において、高速化エンジン制御２００１宛てのパケットが到着した際に、ＴＣ

Ｐセッションの接続/終端などの処理ができるよう設定を行う。

【０３３８】

ゲートウェイ装置３０内の高速化エンジン制御３００１は、ユーザからのゲートウェイ装置２０内の高速化エンジン制御２００１への接続要求を受け、ＳＳＬ３００２にゲートウェイ装置２０内の高速化エンジン制御２００１への通信開始を指示する。同時に、中間ドライバ３００６に対して、ゲートウェイ装置２０内の高速化エンジン制御２００１への通信開始を通知する。この通知には、ゲートウェイ装置２０のＩＰアドレス、高速化エンジン制御２００１のポート番号、及び高速化エンジン制御３００１の送信元ポート番号、更にゲートウェイ装置３０のＩＰアドレスが含まれる。

【０３３９】

ＳＳＬ３００２は、高速化エンジン制御３００１からの通信開始指示を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為に、ＴＣＰ３００３にゲートウェイ装置２０内の高速化エンジン制御２００１への通信開始を指示する。

【０３４０】

ＴＣＰ３００３は、ＳＳＬ３００２からの通信開始指示を受け、ＴＣＰ２００３との間でＴＣＰセッションを確立する為に、ＩＰルーティング３００４に対して、ＴＣＰ２００３とのセッション確立要求パケット（ＳＹＮ）を送信する。このパケットはＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにゲートウェイ装置２０宛、宛先ポート番号にＴＣＰ２００３が設定されている。このＴＣＰセッション確立要求パケットとは、ＴＣＰセッションの確立時に、スリーウェイハンドシェーク（ｔｈｒｅｅ ｗａｙ ｈａｎｄｓｈａｋｅ）の為に送信される、ＳＹＮパケットパケットのことである。本明細書においては、ＴＣＰセッション確立動作の説明を簡略化するため、スリーウェイハンドシェークで送受信されるパケットうち、ＳＹＮパケットをＴＣＰセッション確立要求パケットと呼び、ＳＹＮ＋ＡＣＫパケットを応答パケットと呼んでいる。また実際にはＡＣＫパケットも送信されるが、ＡＣＫパケットについてはＳＹＮパケットと同様に転送されるため、本動作の説明では説明を省略する。

【０３４１】

ＩＰルーティング３００４は、ＴＣＰ３００３から受信したパケットの宛先ＩＰアドレスと宛先ポート番号を参照し、パケットをＩＰスタック３００５に転送する。

【０３４２】

ＩＰスタック３００５は、ＩＰルーティング３００４より受信したパケットに、Ｆｉｒｅｗａｌｌ３３内のイントラネット３側のＭＡＣアドレスを宛先ＭＡＣアドレスとして付加し、更に送信元ＭＡＣアドレスに自ノードのＭＡＣアドレスを設定してフレームを生成し、中間ドライバ３００６に転送する。

【０３４３】

中間ドライバ３００６は、ＩＰスタック３００５からフレームを受信し、フレーム解析を行う。解析の結果、フレームは予め高速化エンジン制御３００１より通知された宛先ＩＰ、宛先ポート、送信元ＩＰ、送信元ポートが付加されたフレームであるので、カプセル化解除においてＭＡＣヘッダを取り外し、パケットにする。そして、中間ドライバ３００６のＴＣＰ部でＴＣＰ３００３からＴＣＰ２００３へのＴＣＰセッションの確立要求の処理を終端する。すなわち、ＴＣＰ３００３は、元々は、ＴＣＰ２００３に対してＴＣＰセッションの確立要求を行ったが、実際は、この要求に対して中間ドライバ３００６内のＴＣＰが受信して保留にし、ＴＣＰ３００３と中間ドライバ３００６内のＴＣＰとの間で、ＴＣＰセッションの確立要求の処理を終端させる。

【０３４４】

中間ドライバ３００６は、上記確立要求の処理を終端させる際、中間ドライバ２００６に対して、ＴＣＰ２００３との間でＴＣＰセッションを確立するよう要求する為、ドライバ３００７にＴＣＰ２００３との接続を要求する為の接続要求パケットを送る。この接続要求パケットには、宛先ＩＰアドレスにゲートウェイ装置２０が、宛先ポート番号にはＴＣＰ２００３が設定される。そしてこのパケットに宛先ＭＡＣアドレスと送信元ＭＡＣア

ドレスとを設定して接続要求フレームとなる。尚、上記接続要求パケットはＴＣＰ規格に沿ったパケットではなく、独自のパケットである。

【０３４５】

ドライバ３００７は中間ドライバ３００６から接続要求フレームを受信し、ＭＡＣ３０１１に転送する。

【０３４６】

ＭＡＣ３０１１はドライバ３００７からフレームを受信し、高速化エンジン３０１４に転送する。

【０３４７】

高速化エンジン３０１４は、ＭＡＣ３０１１からフレームを受信し、そのままＰＨＹ３０１２に転送する。

【０３４８】

ＰＨＹ３０１２は、高速化エンジン３０１４からフレームを受信し、ポート３０１３に転送する。

【０３４９】

ポート３０１３は、ＰＨＹ３０１２からフレームを受信し、イーサネットケーブルを経由してＨＵＢ３２に転送する。

【０３５０】

ＨＵＢ３２は、フレームを受信すると、ＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＬＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３側のポートに出力する。

【０３５１】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からパケットを受信し、ゲートウェイ装置３０からゲートウェイ装置２０への通信の為、これを許可し、ＨＵＢ２２に転送する。

【０３５２】

ＨＵＢ２２は、Ｆｉｒｅｗａｌｌ３３からフレームを受信し、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０に転送する。

【０３５３】

ゲートウェイ装置２０は、ＨＵＢ２２内からフレームを受信し、ポート２０１３、ＰＨＹ２０１２、高速化エンジン２０１４、ＭＡＣ２０１１、ドライバ２００７の経路でフレームを転送し、中間ドライバ２００６に転送する。この時、高速化エンジン２０１４は、ＰＨＹから受信したフレームを、そのまま、ＭＡＣ　２０１１に転送する。

【０３５４】

中間ドライバ２００６は、ドライバ２００７から接続要求フレームを受信し、フレーム解析を行う。解析の結果、このフレームは、予め、高速化エンジン制御２００１より通知された、高速化エンジン制御２００１への宛先ＩＰ、及び宛先ポートが付加されたフレームであるので、このフレームを受信し、カプセル化解除においてＭＡＣヘッダを取り外してパケットにする。パケットは、中間ドライバ３００６から中間ドライバ２００６に向けて送信された、ＴＣＰ２００３への接続要求パケットである為、中間ドライバ２００６内のＴＣＰは、ＴＣＰ２００３との間でＴＣＰセッションを確立する為に、ＩＰスタック２００５に対して、ＴＣＰ２００３とのセッション確立に必要なＴＣＰセッション確立要求パケットを送信する。このパケットはＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにゲートウェイ装置２０宛、宛先ポート番号にＴＣＰ２００３が設定され、更に送信元ＩＰアドレスにはゲートウェイ装置３０のＩＰアドレスが設定され、送信元ポート番号にはＴＣＰ３００３のポート番号が設定される。そして、このパケットには、中間ドライバ２００６内の再カプセル化においてＭＡＣアドレスが付加され、フレームの形にしてＩＰスタック２００５に転送される。

【０３５５】

すなわち、中間ドライバ２００６内のＴＣＰは、ＴＣＰ３００３の名前を騙ってＴＣＰ２００３に対してＴＣＰセッションの確立要求を行う。従って、ＴＣＰ２００３は恰もＴ

ＣＰ３００３と通信しているかのように認識し、更にＴＣＰ３００３は、恰も、ＴＣＰ２００３と通信しているかのように認識する。しかしながら、実際のＴＣＰセッションの確立処理は、ＴＣＰ３００３と中間ドライバ３００６内のＴＣＰとの間、及び、中間ドライバ２００６とＴＣＰ２００３との間で行われ、更に中間ドライバ３００６と中間ドライバ２００６との間は、ＵＤＰ等の輻輳制御の無い方法（本発明の通信システムにおける独自のパケット）で、別途に通信が行われることになる。そして、ＴＣＰ３００３と中間ドライバ３００６との間のＴＣＰセッションと、中間ドライバ３００６と中間ドライバ２００６との間のＵＤＰ等の通信セッションと、更に中間ドライバ２００６とＴＣＰ２００３の間のＴＣＰセッションとが、中間ドライバ３００６及び中間ドライバ２００６によって相互に接続・中継されることにより、恰も、ＴＣＰ３００３とＴＣＰ２００３との間でＴＣＰセッションが確立しているかのように通信が行われる。

【０３５６】

ＩＰスタック２００５は、中間ドライバ２００６からフレームを受信し、ＭＡＣヘッダを外してパケットにしてＩＰルーティング２００４に転送する。

【０３５７】

ＩＰルーティング２００４は、ＩＰスタック２００５より受信したパケットの宛先ポート番号を参照し、ＴＣＰ２００３側のポート番号が付加されていることから、このパケットをＴＣＰ２００３に転送する。

【０３５８】

ＴＣＰ２００３は、ＩＰルーティング２００４よりパケットを受信する。このパケットはＴＣＰセッション確立要求パケット（ＳＹＮ）であるので、ＴＣＰプロトコルに従い、ＴＣＰセッション確立の為に必要な応答パケット（ＳＹＮ＋ＡＣＫ）を返送する。この際、ＴＣＰ２００３は、ＴＣＰセッション確立要求はＴＣＰ３００３から届いたものであると認識する。これは、実際の確立要求は中間ドライバ２００６内のＴＣＰから送信されたものであるが、中間ドライバ２００６内のＴＣＰは、ＴＣＰ３００３を騙ってＴＣＰ２００３にセッション確立要求を行った為、ＴＣＰ２００３は、恰も、ＴＣＰ３００３とセッションを確立すると認識する。

【０３５９】

従って、ＴＣＰ２００３は、応答パケット（ＳＹＮ＋ＡＣＫ）を、ＴＣＰ３００３宛てに送信する。すなわち、応答パケットの宛先ＩＰは、ゲートウェイ装置３０のＩＰアドレスが設定され、応答パケットの宛先ポートは、ＴＣＰ３００３のポート番号が設定される。

【０３６０】

ＴＣＰ２００３からの応答パケットは、ＩＰルーティング２００４、ＩＰスタック２００５に送られ、ここでＭＡＣヘッダを付加されて応答フレームとなり中間ドライバ２００６に届く。

【０３６１】

中間ドライバ２００６は、応答フレームを受信すると、中間ドライバ２００６内のカプセル化解除において応答フレームのＭＡＣヘッダを外して応答パケットを取り出し、ＴＣＰでこのパケット（ＳＹＮ＋ＡＣＫ）を受信して、この応答パケットに対するＡＣＫパケットをＴＣＰ２００３に送信してＴＣＰの処理を終端させる。そして、中間ドライバ３００６に対して、接続完了通知のための接続完了通知パケットを送信する。この接続完了通知パケットは、ＴＣＰ規格に沿ったパケットではなく、本発明の通信システムにおける独自のパケットである。このパケットの宛先ＩＰアドレスにはゲートウェイ送装置３０が、宛先ポート番号にはＴＣＰ３００３が、送信元ＩＰアドレスにはゲートウェイ装置２０が、送信元ポート番号にはＴＣＰ２００３が設定される。そして、中間ドライバ内の再カプセル化において、接続完了通知パケットにＭＡＣヘッダを付加して接続完了通知フレームを生成する。

【０３６２】

接続完了通知フレームは、接続要求とは逆の経路、即ち、ドライバ２００７，ＮＩＣ２

０１，ＨＵＢ２２，Ｆｉｒｅｗａｌｌ３３、ＨＵＢ３２，ＮＩＣ３０１を経由して、ＣＰＵ３００内の中間ドライバ３００６に届く。

【０３６３】

中間ドライバ３００６は、接続完了通知フレームを受信し、フレーム解析を行う。解析の結果、フレームは、予め、高速化エンジン制御３００１より通知された、高速化エンジン制御３００１への宛先ＩＰ、及び宛先ポートが付加されたフレームであるので、このフレームを受信してカプセル化解除においてＭＡＣヘッダを取り外してパケットにする。パケットは、中間ドライバ２００６から中間ドライバ３００６に向けて送信された、ＴＣＰ２００３と中間ドライバ２００６との間の接続完了通知パケットである為、中間ドライバ３００６内のＴＣＰは、ＴＣＰプロトコルに従い、セッション確立の為に必要な応答パケット（ＳＹＮ＋ＡＣＫ）をＴＣＰ３００３に送る為に、ＩＰスタック３００５に対して、応答パケットを送信する。

【０３６４】

応答パケット（ＳＹＮ＋ＡＣＫ）は、ＩＰスタック３００５、ＩＰルーティング３００４を経由し、ＴＣＰ３００３に到達する。

【０３６５】

ＴＣＰ３００３は、ＩＰルーティング３００４より応答パケット（ＳＹＮ＋ＡＣＫ）を受信する。このパケットはＴＣＰセッションの確立要求に対する応答パケットであるので、ＳＳＬ３００２に対して、ＴＣＰ２００３とのＴＣＰセッション接続完了を通知する。この際、ＴＣＰ３００３は、受信した応答パケット（ＳＹＮ＋ＡＣＫ）が、ＴＣＰ２００３から届いたものであると認識する。実際は、この応答パケットは中間ドライバ３００６内のＴＣＰから送信されたものであるが、中間ドライバ３００６内のＴＣＰは、ＴＣＰ２００３を騙ってＴＣＰ３００３にセッション確立に対しての応答パケットを送信した為、ＴＣＰ３００３は、恰も、ＴＣＰ２００３から応答パケットがあったと認識する。

【０３６６】

ＴＣＰ３００３は応答パケット（ＳＹＮ＋ＡＣＫ）を受信すると、この応答パケットに対してＡＣＫパケットを生成してＴＣＰ２００３宛に送信する。このＡＣＫパケットは、中間ドライバ３００６のＴＣＰがＩＰルーティング２００４及びＩＰスタック２００５を介して受信し、ＴＣＰ処理を終端させる。

【０３６７】

ＳＳＬ３００２は、ＴＣＰ３００３からの接続完了通知を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為、ＳＳＬプロトコルに従い、セッション確立要求の為のパケット（ＳＳＬセッション確立要求パケット）を送信する。

【０３６８】

ＳＳＬセッション確立要求パケットは、ＴＣＰ３００３で受信されると、ＴＣＰ３００３と中間ドライバ３００６内のＴＣＰとの間で設定されたＴＣＰセッションを通り、中間ドライバ３００６に到着する。

【０３６９】

中間ドライバ３００６は、ＳＳＬセッション確立要求パケットのＴＣＰ処理を終端し、ＵＤＰ等の輻輳制御の掛からないヘッダを付け、パケットを中間ドライバ２００６に向け送信する。パケットは、ＮＩＣ３０１、ＨＵＢ３２，Ｆｉｒｅｗａｌｌ３３、ＨＵＢ２２、ＮＩＣ２０１を経由して、中間ドライバ２００６に到着する。この際、ＮＩＣ３０１内の高速化エンジン３０１４は、ＭＡＣ３０１１受信したパケットを、そのまま、ＰＨＹ３０１２に転送し、ＮＩＣ２０１内の高速化エンジン２０１４は、ＰＨＹ２０１２から受信したパケットを、そのまま、ＭＡＣ２０１１に転送する。

【０３７０】

中間ドライバ２００６は、ＳＳＬセッション確立要求パケットを受信すると、中間ドライバ２００６内のＴＣＰとＴＣＰ２００３との間で設定されたＴＣＰセッションを通り、ＴＣＰ２００３に到着する。

【０３７１】

ＴＣＰ２００３は、パケットをＳＳＬ２００２に転送する。

【０３７２】

ＳＳＬ２００２は、ＳＳＬセッション確立要求の内容を検証し、問題が無ければ、高速化エンジン制御２００１に対して、ＳＳＬ３００２とのセッション確立を通知すると同時に、ＳＳＬプロトコルに従い、ＳＳＬ３００２に対してＳＳＬセッション確立応答パケットを送信する。

【０３７３】

高速化エンジン制御２００１は、ＳＳＬ２００２からのＳＳＬセッション確立通知を受けると、中間ドライバ２００６に対して、ＳＳＬセッション確立通知によって受信したＳＳＬ３００２の公開鍵とＳＳＬ２００２の秘密鍵、さらにはＳＳＬ２００２とＳＳＬ３００２の間の共通鍵を通知する。

中間ドライバ２００６は、公開鍵、秘密鍵および共通鍵の通知を受けると、公開鍵、秘密鍵および共通鍵、ＳＳＬセッションの相手方機器のＩＰアドレス（ゲートウェイ装置３０のＩＰアドレス）、ＳＳＬセッションの相手方機器の宛先ポート（ＴＣＰ３００３のポート）、自ノード側のＳＳＬセッションの送信元ポート番号（ＴＣＰ２００３のポート）、送信元ＩＰアドレス（ゲートウェイ装置２０のＩＰアドレス）、及び開始命令を制御フレームに載せ、高速化エンジン２０１４に通知する。

【０３７４】

制御フレームは、ドライバ２００７、ＭＡＣ２０１１を通じて高速化エンジン２０１４に到達する。

【０３７５】

高速化エンジン２０１４は、ＭＡＣアドレス等により制御フレームを判別し、制御フレーム送受信部で受信する。そして、公開鍵、秘密鍵および共通鍵を、各々、復号化および暗号化に使用する為に保存し、ＩＰアドレスやポート番号をフレーム解析の為に保存する。そして、高速化処理開始命令を受け、フレーム解析、暗号化、及び複号化の処理を開始する。

【０３７６】

高速化エンジン２０１４は、高速化処理開始命令以前は、制御フレーム以外のＭＡＣ２０１１から受信したフレームは、全て、そのまま、ＰＨＹ２０１２に送信し、ＰＨＹ２０１２から受信したフレームは、全て、そのまま、ＭＡＣ２０１１に送信していた。しかしながら、高速化処理開始命令以降は、制御フレーム以外のＭＡＣ２０１１から受信したフレームを、全て、そのまま、ＰＨＹ２０１２に送信する動作には変わりないが、ＰＨＹ２０１２から受信したフレームについては、以下のような処理を行う。

（１）　ゲートウェイ装置２０宛て、かつ、ＳＳＬ３００２で暗号化されたフレームであれば、ＵＤＰ等のカプセル化を解除し、必要であれば、フラグメントを解除し、フレームを復号化し、ＰＨＹ２０１２側に送信する。

（２）　（１）以外の自ノード宛てフレームであれば、ＭＡＣ２０１１に転送する。

（３）　ブロードキャストフレーム、若しくはマルチキャストフレームであれば、フレームをコピーして、一方はそのままＭＡＣ２０１１に転送し、もう一方は暗号化とカプセル化を行い、ＳＳＬ３００２（ＰＨＹ２０１２側）に送信する。必要であれば、フラグメントを分割も行う。

（４）　（１）～（３）以外のフレームであれば、暗号化とカプセル化を行い、ＳＳＬ３００２（ＰＨＹ２０１２側）に送信する。必要であれば、フラグメントを分割も行う。

【０３７７】

ＳＳＬ２００２より送信された、ＳＳＬセッション確立応答パケットは、ＳＳＬセッション確立要求パケットとは逆の経路、即ち、ＴＣＰ２００３と中間ドライバ２００６との間のＴＣＰセッションを経由して中間ドライバ２００６に到達し、中間ドライバ２００６と中間ドライバ３００６の間のＵＤＰ等の輻輳制御のないセッションを経由して中間ドライバ３００６に到達する。更に、中間ドライバ３００６とＴＣＰ３００３との間のＴＣＰセッションを経由して、ＳＳＬ３００２に到達する。

【０３７８】
ＳＳＬ３００２は、ＳＳＬセッション確立応答の内容をＳＳＬプロトコルに従い検証し、問題が無ければ、高速化エンジン制御３００１に対して、ＳＳＬ３００２とＳＳＬ２００２との間のＳＳＬセッション確立を通知する。
【０３７９】
高速化エンジン制御３００１は、高速化エンジン制御２００１と同様の方法、即ち、中間ドライバ３００６を経由して、高速化エンジン３０１４に対して、ゲートウェイ装置２０の公開鍵、ゲートウェイ装置３０の秘密鍵、ゲートウェイ装置２０とゲートウェイ装置３０の間の共通鍵及び高速化処理開始命令等を送る。
【０３８０】
高速化エンジン３０１４は、高速化エンジン制御３００１からの公開鍵などの通知を受け、高速化エンジン２０１４と同様に動作する。
【０３８１】
以上のようにして、ＳＳＬ２００２とＳＳＬ３００２との間で、ＳＳＬセッションが確立されると、以降はＳＳｌ２００２やＳＳＬ３００２を経由すること無く、高速化エンジン２０１４と高速化エンジン３０１４との間でＳＳＬによる通信が行われる。
【０３８２】
以上により、第２の実施の形態において、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合の動作が完了する。
【０３８３】
［端末２１からサーバ３１へのフレーム転送動作］
図１８を用いて、第２の実施の形態において、端末２１からサーバ３１へフレームを送信する場合を例に、動作の説明を行う。
【０３８４】
この際、ＨＵＢ２２やＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。
【０３８５】
又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。
【０３８６】
更に、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）が、上述の動作例により既に設定されているものとする。
【０３８７】
又、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション（アプリケーション３１０１）との間で、既に、ＴＣＰセッションが構築されているとする。
【０３８８】
端末２１内のアプリケーション２１０１が、サーバ３１内のアプリケーション３１０１宛のデータを、ＴＣＰ２１０２に渡す。
【０３８９】
ＴＣＰ２１０２は、アプリケーション２１０１からデータを受け取り、ＴＣＰプロトコルに従ってＴＣＰヘッダ（図２におけるＦ２３）やＩＰヘッダ（図２におけるＦ２２）を付けてＩＰパケットとし、ＩＰルーティング２１０３に渡す。この時、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定される。
【０３９０】
ＩＰルーティング２１０３は、ＴＣＰ２１０２から受信したパケットの宛先ＩＰアドレス（サーバ３１宛て）および宛先ポート（ＴＣＰ３１０２宛て）を参照し、データをその

ままＩＰスタック２１０４に転送する。

【０３９１】

ＩＰスタック２１０４は、ＩＰルーティング２１０３からパケットを受信し、ＭＡＣヘッダ（図２におけるＦ２１）を付けてＥｔｈｅｒｎｅｔフレームを作成し、ドライバ２１０５に渡す。このフレームは、ＥｔｈｅｒｎｅｔフレームＦ２０のフォーマットを有する。この時、ＩＰスタック２１０４は、ＡＲＰの結果を参照して、フレームのＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスを設定し、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスを設定する。

【０３９２】

ドライバ２１０５は、ＩＰスタック２１０５より上記フレームを受け取り、ＮＩＣ２１１に転送する。

【０３９３】

ＮＩＣ２１１は、ドライバ２１０５よりフレームを受け取り、ＭＡＣ２１１１，ＰＨＹ２１１２，ポート２１１３を経由して、ＨＵＢ２２にフレームを転送する。

【０３９４】

ＨＵＢ２２は、端末２１のＮＩＣ２１１側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０側のポートに出力する。

【０３９５】

ゲートウェイ装置２０内のＮＩＣ２０１は、ポート２０１３でＨＵＢ２２からのフレームを受信し、ＰＨＹ２０１２を経由して、高速化エンジン２０１４に渡す。

【０３９６】

高速化エンジン２０１４は、到着したフレームの宛先ＭＡＣがサーバ３１宛てであることから、高速化エンジン２０１４内の暗号化２０１４Ｇにおいてフレームを暗号化して図３におけるデータＦ１４を作成し、更にカプセル化２０１４Ｉにおいて図３におけるＦ１１～Ｆ１３の各ヘッダを付加してＥｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームＦ１０のフォーマットにして、再び、ＰＨＹ２０１２側に転送する。

【０３９７】

この時、ＩＮＥＴ　ＭＡＣ　Ｆ１１内のＭＡＣ　ＤＡにはＦｉｒｅｗａｌｌ３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはゲートウェイ装置２０のＭＡＣアドレスが設定される。又、ＩＮＥＴ　ＩＰ　Ｆ１２内のＩＰ　ＤＡにはゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡにはゲートウェイ装置２０のＩＰアドレスが設定される。ＩＮＥＴ　ＴＣＰ　Ｆ１３に関しては、Ｆｉｒｅｗａｌｌ３３を通過する為に、恰も、ゲートウェイ装置３０内のＴＣＰ３００３と通信しているかのように見せかける為のＴＣＰヘッダを付加する。しかし、このＴＣＰヘッダは、実際には、中間ドライバ３００６において一旦取り外される為、ＴＣＰ１３００３の輻輳制御には影響しない。従って、ここで付加するＦ１３は、ＴＣＰヘッダの形式を持つが、実際には、ＵＤＰの働きしかしない。仮に、Ｆｉｒｅｗａｌｌ３３の代わりにルータが設置されている場合は、Ｆ１３はＵＤＰヘッダでも構わない。

【０３９８】

ＰＨＹ２０１２は、高速化エンジン２０１４よりフレームを受信すると、ポート２０１３を経由してＨＵＢ２２にフレームを転送する。

【０３９９】

ＨＵＢ２２は、ゲートウェイ装置２２側のポートからフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＷＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３に出力する。

【０４００】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からのフレームを受信し、ＩＰ　ＤＡを参照して

ＭＡＣヘッダＦ１１を変更し、受信フレームをフレームフォーマットＦ１０の形のまま、ＨＵＢ３２に転送する。

【０４０１】

ここで、Ｆ１１内のＭＡＣ　ＤＡにはゲートウェイ装置３０のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＬＡＮ側のＭＡＣアドレスが設定される。

【０４０２】

ＨＵＢ３２は、Ｆｉｒｅｗａｌｌ３３からのフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがゲートウェイ装置３０のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置３０側のポートに出力する。

【０４０３】

ゲートウェイ装置３０内のＮＩＣ３０１は、ポート３０１３でＨＵＢ３２からのフレームを受信し、ＰＨＹ３０１２を経由して、高速化エンジン３０１４に渡す。

【０４０４】

高速化エンジン３０１４は、到着したフレームの宛先ＭＡＣがゲートウェイ装置３０宛てであり、既にゲートウェイ装置２０において暗号化されていることから、高速化エンジン３０１４内のカプセル化３０１４Ｊにおいて Ｆ１１～Ｆ１３の各ヘッダを削除して図３におけるデータＦ１４のみを取り出し、復号化３０１４Ｌにおいてデータ Ｆ１４を復号化して、データＦ１４内に格納されているＦ２１～Ｆ２４のデータ（Ｅｔｈｅｒｎｅｔフレーム Ｆ２０）を取り出し、再び、ＰＨＹ３０１２側に転送する。

【０４０５】

このフレームは、端末２１からＨＵＢ２２に送信された時の状態そのままに保たれており、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスが設定されている。又、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定されている。

【０４０６】

ＰＨＹ３０１２は、高速化エンジン３０１４よりフレームを受信すると、ポート３０１３を経由してＨＵＢ３２にフレームを転送する。

【０４０７】

ＨＵＢ３２は、ゲートウェイ装置３０側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、サーバ３１側のポートに出力する。

【０４０８】

サーバ３１はＨＵＢ３２から送信されたフレームを受信し、ドライバ３１０５，ＩＰスタック３１０４、ＩＰルーティング３１０３、ＴＣＰ３１０２を経由して、フレーム内のデータＦ２４をアプリケーション３１０１に渡す。

【０４０９】

以上のようにして、端末２１内のアプリケーション２１０１からサーバ３１内のアプリケーション３１０１への一連のフレーム転送が完了する。

【０４１０】

上記の例とは逆の経路を辿ることで、サーバ３１内のアプリケーション３１０１から端末２１内のアプリケーション２１０１への一連のフレーム転送も、同様に実現可能である。

【０４１１】

上記の方法でヘッダＦ１３側のＴＣＰの輻輳制御と再送制御を事実上停止させても、ヘッダＦ２３側のＴＣＰの輻輳制御と再送制御は通常通り機能する為、端末２１とサーバ３

１の各々のアプリケーションから見た場合、端末２１内のＴＣＰとサーバ３１内のＴＣＰの働きにより、輻輳制御、再送制御ともに問題なく行われる。

【０４１２】

尚、本実施の形態では、サーバ３１と端末２１の設置場所を入れ替えることも出来る。

【０４１３】

［発明の効果］

次に、本実施の形態の効果について説明する。

【０４１４】

本実施の形態に挙げた発明を利用すると、端末２１とサーバ３１との間で、フレームの高速転送が可能になる。

【０４１５】

これは、高速化エンジン２０１４及び３０１４を利用することで、ゲートウェイ装置２０、及びゲートウェイ装置３０におけるＣＰＵ（ソフトウェア処理）によるカプセル化処理および暗号化／復号化処理を排除し、これら処理を全て高速化エンジン（ハードウェア）で実現できる為である。

【０４１６】

更に、これは、ゲートウェイ装置２０とゲートウェイ装置３０との間の通信において、ヘッダＦ１３の位置のＴＣＰによる輻輳制御と再送制御が発生しないよう、ゲートウェイ装置３０内の中間ドライバと、ゲートウェイ装置２０内の中間ドライバにおいて、ゲートウェイ装置２０内のＴＣＰと、ゲートウェイ装置３０内のＴＣＰを終端し、ＴＣＰ　ｏｖｅｒ　ＴＣＰ問題の発生を回避しているからである。

【０４１７】

又、本実施の形態に挙げた発明を利用すると、高速化処理の為のハードウェア（高速化エンジン）の開発費用や部材費用を、比較的低く抑えることが出来る。

【０４１８】

これは、暗号化／復号化とカプセル化を同一ハードウェア（ＦＰＧＡ／ＡＳＩＣ）上で行うことが出来るからである。

【０４１９】

又、これは、比較的安価なＭＡＣとＰＨＹ間のインタフェースに、ハードウェアを実装することが出来るからである。

【０４２０】

又、これは、ハードウェアへの実装が難しいＴＣＰ処理をソフトウェアに残し、ハードウェアへの実装が比較的容易で、かつ、高速化処理の効果が大きな暗号化／復号化とカプセル化のみをハードウェア処理できるからである。

【０４２１】

［第３の実施の形態］

本発明の第３の実施の形態は、第２の実施の形態に対して、ゲートウェイ装置３０内に高速化エンジン３０１４が無く、高速化エンジン制御３００１の代わりにゲートウェイアプリケーション３００１Ａが存在している点において異なる。

【０４２２】

第３の実施の形態における端末２１，サーバ３１、ＨＵＢ２２，ＨＵＢ３２、ゲートウェイ装置２０、イントラネット２、イントラネット３の構成および動作は、第２の実施の形態と同じである。

【０４２３】

第３の実施の形態においては、イントラネット２は、閉域ＬＡＮだけでなく、インターネット等のオープンなＷＡＮを用いても構わない。

【０４２４】

［構成の説明］

図１９は、第３の実施の形態における、各機器の構成と、フレームの転送経路を詳細に示したブロック図である。

【０４２５】
ゲートウェイ装置３０は、第２の実施の形態におけるゲートウェイ装置３０に対して、高速化エンジン３０１４が無く、高速化エンジン制御３００１の代わりにゲートウェイアプリケーション３００１Ａが存在している点、更にブリッジ３００８，ドライバ３００９，仮想ＮＩＣ３０１０が追加されている点において異なる。
【０４２６】
ゲートウェイアプリケーション３００１Ａは、以下に挙げる動作を行う。
（１） 仮想ＮＩＣ３０１０から到着するフレームを、ＳＳＬ３００２に転送する。すなわち、ゲートウェイアプリケーション３００１Ａと高速化エンジン制御２００１との間に設定されるＳＳＬセッション内に、仮想ＮＩＣ３０１０から到着するフレームをデータとして載せ、高速化エンジン制御２００１宛てに送信する。尚、ここで、ゲートウェイアプリケーション３００１Ａからは、通信の相手方は高速化エンジン制御２００１に見えているが、実際の通信の相手方は、高速化エンジン２０１４になる。
（２） ＳＳＬ３００２より、ゲートウェイアプリケーション３００１Ａと高速化アプリケーション２００１との間に設定されるＳＳＬセッションを通じて到着するデータを、フレームとして仮想ＮＩＣ３０１０に転送する。
（３） 高速化エンジン制御２００１との間のＳＳＬセッションの接続および切断に必要な動作を行う。ゲートウェイアプリケーション３００１Ａ側から高速化エンジン制御２００１側へ接続要求することは、勿論、高速化アプリケーション２００１側からゲートウェイアプリケーション３００１Ａ側への接続要求も受信することが出来る。
【０４２７】
ブリッジ３００８は、中間ドライバ３００６からフレームを受け取り、宛先ＭＡＣアドレスを参照して、ドライバ３００９もしくはドライバ３００７にフレームを転送する機能を有する。通常はＯＳの機能として実装される。又、ドライバ３００９からフレームを受け取り、宛先ＭＡＣアドレスを参照して、ドライバ３００７若しくは中間ドライバ３００６にフレームを転送する機能を有する。又、ドライバ３００７からフレームを受け取り、宛先ＭＡＣアドレスを参照して、ドライバ３００９若しくは中間ドライバ３００６にフレームを転送する機能を有する。
【０４２８】
更に、ブリッジ３００８は、フレーム受信時に、送信元ＭＡＣアドレスを参照し、ＭＡＣアドレスの学習を行い、どのＭＡＣアドレスを持つ端末が、どのインタフェース（即ち、中間ドライバ３００６、ドライバ３００９、ドライバ３００７）側に接続されているのかを記録する機能を有する。仮に、フレーム受信時に、宛先ＭＡＣアドレスを参照しても、ＭＡＣアドレスを学習していない場合は、
フレームを、フレームが入力された中間ドライバ若しくはドライバ以外のドライバ又は中間ドライバにブロードキャストする機能を有する。
【０４２９】
ドライバ３００９は、仮想ＮＩＣ３０１０とＯＳの仲介をするソフトウェアであり、仮想ＮＩＣからフレームを受け取りＯＳに送り、更に、ＯＳからフレームを受け取り、仮想ＮＩＣに送る機能を有する。
【０４３０】
仮想ＮＩＣ３０１０は、ドライバ３００９と、ゲートウェイアプリケーション３００１Ａを仲介するソフトウェアである。仮想ＮＩＣ３０１０は、ドライバ３００９からフレームを受け取り、ゲートウェイアプリケーション３００１Ａに渡す機能を有する。更に、ゲートウェイアプリケーション３００１Ａからフレームを受け取り、ドライバ３０１０に送る機能を有する。本来、ＮＩＣはハードウェアで構成されるが、仮想ＮＩＣ３０１０はソフトウェアで構成される。仮想ＮＩＣ３０１０は、ＯＳからは、恰も、ハードウェアであるかのように認識される。
【０４３１】
仮想ＮＩＣ３０１０、ドライバ３００９、ブリッジ３００８は、中間ドライバ３００６

にその機能を纏め、一体化させることも出来る。この場合、ゲートウェイアプリケーション３００１Ａから出たフレームは、中間ドライバ３００６を経由してドライバ３００７に渡され、又、ドライバ３００７から入力した自ノード宛て以外のユニキャストフレーム若しくはブロードキャストフレームは、中間ドライバ３００６からゲートウェイアプリケーション３００１Ａに送られる。

【０４３２】

第３の実施の形態では、ゲートウェイ装置３０内に存在するＳＳＬ３００２、ＴＣＰ３００３、ＩＰルーティング３００４、ＩＰスタック３００５、中間ドライバ３００６、ドライバ３００７は、第２の実施の形態におけるＳＳＬ３００２、ＴＣＰ３００３、ＩＰルーティング３００４、ＩＰスタック３００５、中間ドライバ３００６、ドライバ３００７と、各々、同様の構成を有し、同様の動作を行う。

【０４３３】

端末２１、サーバ３１、ゲートウェイ装置２０、Ｆｉｒｅｗａｌｌ３３，ＨＵＢ２２、ＨＵＢ３２に関しては、第２の実施の形態と同様の構成を有し、同様の動作を行う。

【０４３４】

従って、第３の実施の形態では、ゲートウェイ装置２０とゲートウェイ装置３０との間で、予め、ＳＳＬセッションを設定している場合のみ、イントラネット２内の機器からイントラネット３内の機器へのアクセスが可能になる。

【０４３５】

［動作の説明］

［ＳＳＬセッションの確立動作］

図１９を用いて、第３の実施の形態において、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合を例に挙げて、動作の説明を行う。

【０４３６】

この際、ブリッジ３００８、ＨＵＢ２２やＨＵＢ３２がすでに端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３のＷＡＮ側，Ｆｉｒｅｗａｌｌ３３のＬＡＮ側、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。

【０４３７】

又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。

【０４３８】

ゲートウェイ装置２０内の高速化エンジン制御２００１は、起動後ゲートウェイ装置３０からの接続待ち受け状態になると、中間ドライバ２００６に対して、待ち受け開始を通知する。この通知には、ゲートウェイ装置２０のＩＰアドレス、高速化エンジン制御２００１の待ち受けポート番号が含まれる。

【０４３９】

中間ドライバ２００６は、高速化エンジン制御２００１からの通知を受けると、フレーム解析処理において、高速化エンジン制御２００１宛てのパケットが到着した際に、ＴＣＰセッションの接続/終端などの処理が出来るよう設定を行う。

【０４４０】

ゲートウェイ装置３０内のゲートウェイアプリケーション３００１Ａは、ユーザからのゲートウェイ装置２０内の高速化エンジン制御２００１への接続要求を受け、ＳＳＬ３００２にゲートウェイ装置２０内の高速化エンジン制御２００１への通信開始を指示する。同時に、中間ドライバ３００６に対して、ゲートウェイ装置２０内の高速化エンジン制御２００１への通信開始を通知する。この通知には、ゲートウェイ装置２０のＩＰアドレス、高速化エンジン制御２００１のポート番号、及びゲートウェイアプリケーション３００１Ａの送信元ポート番号、さらにゲートウェイ装置３０のＩＰアドレスが含まれる。

【０４４１】

ＳＳＬ３００２は、ゲートウェイアプリケーション３００１Ａからの通信開始指示を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為に、ＴＣＰ３００３にゲートウェイ装置２０内の高速化エンジン制御２００１への通信開始を指示する。

【０４４２】

ＴＣＰ３００３は、ＳＳＬ３００２からの通信開始指示を受け、ＴＣＰ２００３との間でＴＣＰセッションを確立する為に、ＩＰルーティング３００４に対して、ＴＣＰ２００３とのＴＣＰセッション確立要求パケット（ＳＹＮ）を送信する。このパケットはＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにゲートウェイ装置２０宛、宛先ポート番号にＴＣＰ２００３が設定されている。このＴＣＰセッション確立要求パケットとは、ＴＣＰセッションの確立時に、スリーウェイハンドシェーク（ｔｈｒｅｅ ｗａｙ ｈａｎｄｓｈａｋｅ）の為に送信される、ＳＹＮパケットパケットのことである。本明細書においては、ＴＣＰセッション確立動作の説明を簡略化するため、スリーウェイハンドシェークで送受信されるパケットうち、ＳＹＮパケットをＴＣＰセッション確立要求パケットと呼び、ＳＹＮ＋ＡＣＫパケットを応答パケットと呼んでいる。また実際にはＡＣＫパケットも送信されるが、ＡＣＫパケットについてはＳＹＮパケットと同様に転送されるため、本動作の説明では説明を省略する。

【０４４３】

ＩＰルーティング３００４は、ＴＣＰ３００３から受信したパケットの宛先ＩＰアドレスと宛先ポート番号を参照し、パケットをＩＰスタック３００５に転送する。

【０４４４】

ＩＰスタック３００５は、ＩＰルーティング３００４より受信したパケットに、Ｆｉｒｅｗａｌｌ３３内のイントラネット３側のＭＡＣアドレスを宛先ＭＡＣアドレスとして付加し、更に送信元ＭＡＣアドレスに自ノードのＭＡＣアドレスを設定してフレームを生成し、中間ドライバ３００６に転送する。

【０４４５】

中間ドライバ３００６は、ＩＰスタック３００５からＴＣＰセッション確立要求のフレームを受信し、フレーム解析を行う。解析の結果、このフレームは、予め、ゲートウェイアプリケーション３００１より通知された宛先ＩＰ、宛先ポート、送信元ＩＰ、送信元ポートが付加されたフレームであるので、カプセル解除において、ＭＡＣヘッダを取り外してパケットにする。そして中間ドライバ３００６のＴＣＰ部でＴＣＰ３００３からＴＣＰ２００３へのＴＣＰ処理を終端させる。すなわち、ＴＣＰ３００３は、元々は、ＴＣＰ２００３に対してＴＣＰセッションの確立要求を行ったが、実際は、この要求に対して中間ドライバ内のＴＣＰで保留してＴＣＰセッションの確立を終端させ、ＴＣＰ３００３と中間ドライバ３００６内のＴＣＰとの間でＴＣＰセッションの確立処理を行う。

【０４４６】

中間ドライバ３００６は、終端処理を行う際、中間ドライバ２００６に対して、ＴＣＰ２００３との間でＴＣＰセッションを確立するよう要求する為、ドライバ３００７に接続要求のための接続要求パケットを生成する。この接続要求パケットの宛先ＩＰアドレスにはゲートウェイ装置２０が、宛先ポート番号にはＴＣＰ２００３が設定される。そしてこのパケットに宛先ＭＡＣアドレスを付加し、更に送信元ＭＡＣアドレスに自ノードのＭＡＣアドレスを設定して接続要求フレームにする。この接続要求フレームは、ＴＣＰ規格に沿ったパケットではなく、本発明の通信システムにおける独自のパケットである。

【０４４７】

ドライバ３００７は、中間ドライバ３００６から接続要求フレームを受信し、ＭＡＣ３０１１に転送する。

【０４４８】

ＭＡＣ３０１１は、ドライバ３００７からフレームを受信し、ＰＨＹ３０１２に転送する。

【０４４９】

ＰＨＹ３０１２は、ＭＡＣ３０１１からフレームを受信し、ポート３０１３に転送する

。

【０４５０】

ポート３０１３は、ＰＨＹ３０１２からフレームを受信し、イーサネットケーブルを経由してＨＵＢ３２に転送する。

【０４５１】

ＨＵＢ３２は、フレームを受信すると、ＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＬＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３側のポートに出力する。

【０４５２】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からパケットを受信し、ゲートウェイ装置３０からゲートウェイ装置２０への通信の為、これを許可し、ＨＵＢ２２に転送する。

【０４５３】

ＨＵＢ２２は、Ｆｉｒｅｗａｌｌ３３からフレームを受信し、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０に転送する。

【０４５４】

ゲートウェイ装置２０は、ＨＵＢ２２内から接続要求のフレームを受信し、ポート２０１３、ＰＨＹ２０１２、高速化エンジン２０１４、ＭＡＣ２０１１、ドライバ２００７の経路でフレームを転送し、中間ドライバ２００６に転送する。この時、高速化エンジン２０１４は、ＰＨＹから受信したフレームを、そのまま、ＭＡＣ　２０１１に転送する。

【０４５５】

中間ドライバ２００６は、ドライバ２００７から接続要求フレームを受信し、フレーム解析を行う。解析の結果、このフレームは、予め、高速化エンジン制御２００１より通知された、高速化エンジン制御２００１への宛先ＩＰ、及び宛先ポートが付加された接続要求フレームであるので、このフレームを受信してカプセル化解除においてＭＡＣヘッダを取り外してパケットにする。このパケットは、中間ドライバ３００６から中間ドライバ２００６に向けて送信されたＴＣＰ２００３への接続要求パケットである為、中間ドライバ２００６内のＴＣＰは、ＴＣＰ２００３との間でＴＣＰセッションを確立する為に、ＩＰスタック２００５に対して、ＴＣＰ２００３とのセッション確立に必要なパケットを送信する。このパケットはＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにゲートウェイ装置２０宛、宛先ポート番号にＴＣＰ２００３が設定され、更に、送信元ＩＰアドレスにはゲートウェイ装置３０のＩＰアドレスが設定され、送信元ポート番号にはＴＣＰ３００３のポート番号が設定される。そして、このパケットには、中間ドライバ２００６内の再カプセル化によってＭＡＣアドレスが付加され、フレームの形にしてＩＰスタック２００５に転送される。

【０４５６】

すなわち、中間ドライバ２００６内のＴＣＰは、ＴＣＰ３００３の名前を騙ってＴＣＰ２００３に対してＴＣＰセッションの確立要求を行う。従って、ＴＣＰ２００３は、恰も、ＴＣＰ３００３と通信しているかのように認識し、更にＴＣＰ３００３は、恰も、ＴＣＰ２００３と通信しているかのように認識する。しかしながら、実際のＴＣＰ処理は、ＴＣＰ３００３と中間ドライバ３００６内のＴＣＰとの間、及び中間ドライバ２００６とＴＣＰ２００３との間で行われ、更に中間ドライバ３００６と中間ドライバ２００６との間は、ＵＤＰ等の輻輳制御のない方法（本発明の通信システムにおける独自のパケット）で、別途に通信が行われる。そして、ＴＣＰ３００３と中間ドライバ３００６間のＴＣＰセッションと、中間ドライバ３００６と中間ドライバ２００６の間のＵＤＰ等何らかの通信セッション、更に中間ドライバ２００６とＴＣＰ２００３の間のＴＣＰセッションが、中間ドライバ３００６及び中間ドライバ２００６によって相互に接続・中継されることにより、恰も、ＴＣＰ３００３とＴＣＰ２００３との間でＴＣＰセッションが確立しているかのように通信が行われる。

【０４５７】

ＩＰスタック２００５は、中間ドライバ２００６からフレームを受信し、ＭＡＣヘッダ

を外してパケットにし、ＩＰルーティング２００４に転送する。

【０４５８】

ＩＰルーティング２００４は、ＩＰスタック２００５より受信したパケットの宛先ポート番号を参照し、ＴＣＰ２００３側のポート番号が付加されていることから、このパケットをＴＣＰ２００３に転送する。

【０４５９】

ＴＣＰ２００３は、ＩＰルーティング２００４よりパケットを受信する。このパケットはＴＣＰセッション確立要求パケット（ＳＹＮ）であるので、ＴＣＰプロトコルに従い、セッション確立要求に対して応答パケット（ＳＹＮ＋ＡＣＫ）を返送する。この際、ＴＣＰ２００３は、ＴＣＰセッション確立要求は、ＴＣＰ３００３から届いたものであると認識する。これは、実際の確立要求は中間ドライバ２００６内のＴＣＰから送信されたものであるが、中間ドライバ２００６内のＴＣＰは、ＴＣＰ３００３を騙ってＴＣＰ２００３にセッション確立要求を行った為、ＴＣＰ２００３は、恰も、ＴＣＰ３００３とセッションを確立すると認識する。

【０４６０】

従って、ＴＣＰ２００３は、ＴＣＰセッション確立要求に対して応答パケット（ＳＹＮ＋ＡＣＫ）を、ＴＣＰ３００３宛てに送信する。すなわち、応答パケットの宛先ＩＰはゲートウェイ装置３０のＩＰアドレスが設定され、応答パケットの宛先ポートはＴＣＰ３００３のポート番号が設定される。

【０４６１】

応答パケットは、ＩＰルーティング２００４を経由して、ＩＰスタック２００５に送られ、ここでＭＡＣヘッダが付加されて応答フレームになり中間ドライバ２００６に届く。

【０４６２】

中間ドライバ２００６は、応答フレームを受信すると、中間ドライバ２００６内のカプセル化解除において応答フレームのＭＡＣヘッダを外して応答パケットを取り出し、ＴＣＰでこの応答パケット（ＳＹＮ＋ＡＣＫ）を受信して、この応答パケットに対してＡＣＫパケットをＴＣＰ２００３に送信してＴＣＰ処理を終端させる。そして、中間ドライバ３００６に対して、接続完了通知のパケットを生成する。上記接続完了通のパケットは、ＴＣＰ規格に沿ったものではなく、独自のパケットである。この接続完了通知パケットは、宛先ＩＰアドレスにはゲートウェイ送装置３０が、宛先ポート番号にはＴＣＰ３００３が、送信元ＩＰアドレスにはゲートウェイ装置２０が、送信元ポート番号にはＴＣＰ２００３が設定される。そして、中間ドライバ２００６内の再カプセル化において、接続完了通知パケットにＭＡＣヘッダを付加して接続完了通知フレームとなる。

【０４６３】

接続完了通知フレームは、接続要求フレームとは逆の経路、即ち、ドライバ２００７，ＮＩＣ２０１，ＨＵＢ２２，Ｆｉｒｅｗａｌｌ３３、ＨＵＢ３２，ＮＩＣ３０１を経由して、ＣＰＵ３００内の中間ドライバ３００６に届く。

【０４６４】

中間ドライバ３００６は、接続完了通知フレームを受信し、フレーム解析を行う。解析の結果、パケットは、予め、ゲートウェイアプリケーション３００１Ａより通知された、ゲートウェイアプリケーション３００１Ａへの宛先ＩＰ、及び宛先ポートが付加された接続完了通知フレームであるので、このフレームを受信する。受信したフレームは、カプセル化解除においてＭＡＣヘッダを取り外し、パケットにする。パケットは中間ドライバ２００６から中間ドライバ３００６に向けて送信されたＴＣＰ２００３と中間ドライバ２００６との間の接続完了通知パケットである為、中間ドライバ３００６内のＴＣＰは、ＴＣＰプロトコルに従って、ＴＣＰセッション確立の為に必要な応答パケット（ＳＹＮ＋ＡＣＫ）をＴＣＰ３００３に送る為、ＩＰスタック３００５に対して、ＴＣＰプロトコルに従って生成した応答パケットを送信する。

【０４６５】

応答パケットは、ＩＰスタック３００５、ＩＰルーティング３００４を経由し、ＴＣＰ

３００３に到達する。

【０４６６】

ＴＣＰ３００３は、ＩＰルーティング３００４より応答パケット（ＳＹＮ＋ＡＣＫ）を受信する。このパケットはＴＣＰセッションの確立要求に対する応答パケットであるので、ＳＳＬ３００２に対して、ＴＣＰ２００３とのＴＣＰセッション接続完了を通知する。この際、ＴＣＰ３００３は、応答パケット（ＳＹＮ＋ＡＣＫ）が、ＴＣＰ２００３から届いたものであると認識する。これは、実際の応答は中間ドライバ３００６内のＴＣＰから送信されたものであるが、中間ドライバ３００６内のＴＣＰは、ＴＣＰ２００３を騙ってＴＣＰ３００３にセッション確立応答を行った為、ＴＣＰ３００３は、恰も、ＴＣＰ２００３から応答があったと認識する。

【０４６７】

ＴＣＰ３００３は応答パケット（ＳＹＮ＋ＡＣＫ）を受信すると、この応答パケットに対してＡＣＫパケットを生成してＴＣＰ１００３宛に送信する。このＡＣＫパケットは、中間ドライバ３００６のＴＣＰがＩＰルーティング２００４及びＩＰスタック２００５を介して受信し、ＴＣＰ処理を終端させる。

【０４６８】

ＳＳＬ３００２は、ＴＣＰ３００３からの接続完了通知を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為、ＳＳＬプロトコルに従い、セッション確立要求の為のパケット（ＳＳＬセッション確立要求パケット）を送信する。

【０４６９】

ＳＳＬセッション確立要求パケットは、ＴＣＰ３００３で受信されると、ＴＣＰ３００３と中間ドライバ３００６内のＴＣＰとの間で設定されたＴＣＰセッションを通り、中間ドライバ３００６に到着する。

【０４７０】

中間ドライバ３００６は、ＳＳＬセッション確立要求パケットを受信してＴＣＰを終端させ、ＵＤＰ等の輻輳制御の掛からないヘッダを付け、ＳＳＬセッション確立要求パケットを中間ドライバ２００６に向け送信する。ＳＳＬセッション確立要求パケットは、ＮＩＣ３０１、ＨＵＢ３２，Ｆｉｒｅｗａｌｌ３３、ＨＵＢ２２、ＮＩＣ２０１を経由して、中間ドライバ２００６に到着する。この際、ＮＩＣ２０１内の高速化エンジン２０１４は、ＰＨＹ２０１２から受信したパケットを、そのまま、ＭＡＣ２０１１に転送する。

【０４７１】

中間ドライバ２００６は、ＳＳＬセッション確立要求パケットを受信すると、中間ドライバ２００６内のＴＣＰとＴＣＰ２００３との間で設定されたＴＣＰセッションを通り、ＴＣＰ２００３に到着する。

【０４７２】

ＴＣＰ２００３は、パケットをＳＳＬ２００２に転送する。

【０４７３】

ＳＳＬ２００２は、ＳＳＬセッション確立要求の内容を検証し、問題が無ければ、高速化エンジン制御２００１に対して、ＳＳＬ３００２とのセッション確立を通知すると同時に、ＳＳＬプロトコルに従い、ＳＳＬ３００２に対してＳＳＬセッション確立応答パケットを送信する。

【０４７４】

ＳＳＬセッション確立応答パケットは、ＳＳＬセッション確立要求パケットとは逆の経路、即ち、ＴＣＰ２００３と中間ドライバ２００６との間のＴＣＰセッションを経由して中間ドライバ２００６に到達し、中間ドライバ２００６と中間ドライバ３００６との間のＵＤＰ等の輻輳制御の無いセッションを経由して中間ドライバ３００６に到達する。更に、中間ドライバ３００６とＴＣＰ３００３との間のＴＣＰセッションを経由して、ＳＳＬ３００２に到達する。

【０４７５】

ＳＳＬ３００２は、ＳＳＬセッション確立応答の内容をＳＳＬプロトコルに従い検証し

、問題が無ければ、ゲートウェイアプリケーション３００１Ａに対して、ＳＳＬ３００２とＳＳＬ２００２との間のＳＳＬセッション確立を通知する。

【０４７６】

高速化エンジン制御２００１は、ＳＳＬ２００２からのＳＳＬセッション確立通知を受けると、中間ドライバ２００６に対して、ＳＳＬセッション確立通知によって受信したＳＳＬ３００２の公開鍵と、ＳＳＬ２００２の秘密鍵、ＳＳＬ２００２とＳＳＬ３００２の間の共通鍵を通知する。

【０４７７】

中間ドライバ２００６は、公開鍵、秘密鍵および共通鍵の通知を受けると、公開鍵、秘密鍵および共通鍵、ＳＳＬセッションの相手方機器のＩＰアドレス（ゲートウェイ装置３０のＩＰアドレス）、ＳＳＬセッションの相手方機器の宛先ポート（ＴＣＰ３００３のポート）、自ノード側のＳＳＬセッションの送信元ポート番号（ＴＣＰ２００３のポート）、送信元ＩＰアドレス（ゲートウェイ装置２０のＩＰアドレス）、及び開始命令を制御フレームに載せ、高速化エンジン２０１４に通知する。

【０４７８】

制御フレームは、ドライバ２００７、ＭＡＣ２０１１を通じて高速化エンジン２０１４に到達する。

【０４７９】

高速化エンジン２０１４は、ＭＡＣアドレス等により制御フレームを判別し、制御フレーム送受信部で受信する。そして、公開鍵、秘密鍵および共通鍵を、それぞれ復号化および暗号化に使用するため保存し、ＩＰアドレスやポート番号をフレーム解析の為に保存する。そして、高速化処理開始命令を受け、フレーム解析、暗号化、及び複号化の処理を開始する。

【０４８０】

高速化エンジン２０１４は、高速化処理開始命令以前は、制御フレーム以外のＭＡＣ２０１１から受信したフレームは、全て、そのまま、ＰＨＹ２０１２に送信し、ＰＨＹ２０１２から受信したフレームは、全て、そのまま、ＭＡＣ２０１１に送信していた。しかしながら、高速化処理開始命令以降は、制御フレーム以外のＭＡＣ２０１１から受信したフレームを、全て、そのまま、ＰＨＹ２０１２に送信する動作には変わりないが、ＰＨＹ２０１２から受信したフレームについては、以下のような処理を行う。

（１）　ゲートウェイ装置２０宛て、かつ、ＳＳＬ３００２で暗号化されたフレームであれば、ＵＤＰ等のカプセル化を解除し、必要であれば、フラグメントを解除し、フレームを復号化し、ＰＨＹ２０１２側に送信する。

（２）　（１）以外の自ノード宛てフレームであれば、ＭＡＣ２０１１に転送する。

（３）　ブロードキャストフレーム、若しくはマルチキャストフレームであれば、フレームをコピーして、一方はそのままＭＡＣ２０１１に転送し、もう一方は暗号化とカプセル化を行い、ＳＳＬ３００２（ＰＨＹ２０１２側）に送信する。必要であれば、フラグメントを分割も行う。

（４）　（１）～（３）以外のフレームであれば、暗号化とカプセル化を行い、ＳＳＬ３００２（ＰＨＹ２０１２側）に送信する。必要であれば、フラグメントを分割も行う。

【０４８１】

以上のようにして、高速化エンジン２０１４と中間ドライバ３００６との間で、フレーム転送の為のＵＤＰ等の輻輳制御の無いセッションが確立される。又、高速化エンジン２０１４とＳＳＬ３００２との間で、ＳＳＬセッション（ＳＳＬトンネル）が確立される。

【０４８２】

すなわち、ＳＳＬ２００２は、ＳＳＬセッション確立要求時のみ、ＳＳＬ３００２と遣り取りするが、ＳＳＬセッション確立が終了すると、以後は、高速化エンジン２０１４とＳＳＬ３００２との間で、ＳＳＬの暗号化および復号化の遣り取りを行う。

【０４８３】

又、中間ドライバ２００６は、ＳＳＬセッション確立の際にのみ、中間ドライバ３００

６とフレームの遣り取りを行うが、ＳＳＬセッションが確立した後は、高速化エンジン２０１４と中間ドライバ３００６との間でフレームの遣り取りを行う。

【０４８４】

以上により、第３の実施の形態において、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合の動作が完了する。

【０４８５】

［端末２１からサーバ３１へのフレーム転送動作］

図１９を用いて、第３の実施の形態において、端末２１からサーバ３１へフレームを送信する場合を例に挙げて、動作の説明を行う。

【０４８６】

この際、ブリッジ３００８、ＨＵＢ２２やＨＵＢ３２がすでに端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。

【０４８７】

又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。

【０４８８】

更に、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）が、上述の動作例により既に設定されているものとする。

【０４８９】

又、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション（アプリケーション３１０１）との間で、既に、ＴＣＰセッションが構築されているとする。

【０４９０】

端末２１内のアプリケーション２１０１が、サーバ３１内のアプリケーション３１０１宛のデータを、ＴＣＰ２１０２に渡す。

【０４９１】

ＴＣＰ２１０２は、アプリケーション２１０１からデータを受け取り、ＴＣＰプロトコルに従ってＴＣＰヘッダ（図２におけるＦ２３）やＩＰヘッダ（図２におけるＦ２２）を付けてＩＰパケットとし、ＩＰルーティング２１０３に渡す。この時、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定される。

【０４９２】

ＩＰルーティング２１０３は、ＴＣＰ２１０２から受信したパケットの宛先ＩＰアドレス（サーバ３１宛て）および宛先ポート（ＴＣＰ３１０２宛て）を参照し、データを、そのまま、ＩＰスタック２１０４に転送する。

【０４９３】

ＩＰスタック２１０４は、ＩＰルーティング２１０３からパケットを受信し、ＭＡＣヘッダ（図２におけるＦ２１）をつけてＥｔｈｅｒｎｅｔフレームを作成し、ドライバ２１０５に渡す。このフレームはＥｔｈｅｒｎｅｔフレームＦ２０のフォーマットを有する。この時、ＩＰスタック２１０４は、ＡＲＰの結果を参照して、フレームのＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスを設定し、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスを設定する。

【０４９４】

ドライバ２１０５は、ＩＰスタック２１０５より上記フレームを受け取り、ＮＩＣ２１１に転送する。

【０４９５】

ＮＩＣ２１１は、ドライバ２１０５よりフレームを受け取り、ＭＡＣ２１１１，ＰＨＹ２１１２，ポート２１１３を経由して、ＨＵＢ２２にフレームを転送する。

【０４９６】
ＨＵＢ２２は、端末２１のＮＩＣ２１１側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０側のポートに出力する。
【０４９７】
ゲートウェイ装置２０内のＮＩＣ２０１は、ポート２０１３でＨＵＢ２２からのフレームを受信し、ＰＨＹ２０１２を経由して、高速化エンジン２０１４に渡す。
【０４９８】
高速化エンジン２０１４は、到着したフレームの宛先ＭＡＣがサーバ３１宛てであることから、高速化エンジン２０１４内の暗号化２０１４Ｇにおいてフレームを暗号化して図３におけるデータＦ１４を作成し、更にカプセル化２０１４Ｉにおいて図３におけるＦ１１～Ｆ１３の各ヘッダを付加してＥｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームＦ１０のフォーマットにして、再びＰＨＹ２０１２側に転送する。
【０４９９】
この時、ＩＮＥＴ　ＭＡＣ　Ｆ１１内のＭＡＣ　ＤＡにはＦｉｒｅｗａｌｌ３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはゲートウェイ装置２０のＭＡＣアドレスが設定される。又、ＩＮＥＴ　ＩＰ　Ｆ１２内のＩＰ　ＤＡにはゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡにはゲートウェイ装置２０のＩＰアドレスが設定される。ＩＮＥＴ　ＴＣＰ　Ｆ１３に関しては、Ｆｉｒｅｗａｌｌ３３を通過する為に、恰も、ゲートウェイ装置３０内のＴＣＰ３００３と通信しているかのように見せかける為のＴＣＰヘッダを付加する。しかし、このＴＣＰヘッダは、実際には中間ドライバ３００６において一旦取り外される為、ＴＣＰ１３００３の輻輳制御には影響しない。従って、ここで付加するＦ１３は、ＴＣＰヘッダの形式を持つが、実際には、ＵＤＰの働きしかしない。仮に、Ｆｉｒｅｗａｌｌ３３の代わりにルータが設置されている場合は、Ｆ１３はＵＤＰヘッダでも構わない。
【０５００】
ＰＨＹ２０１２は、高速化エンジン２０１４よりフレームを受信すると、ポート２０１３を経由してＨＵＢ２２にフレームを転送する。
【０５０１】
ＨＵＢ２２は、ゲートウェイ装置２２側のポートからフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＷＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３に出力する。
【０５０２】
Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からのフレームを受信し、ＩＰ　ＤＡを参照してＭＡＣヘッダＦ１１を変更し、受信フレームをフレームフォーマットＦ１０の形のまま、ＨＵＢ３２に転送する。
【０５０３】
ここで、Ｆ１１内のＭＡＣ　ＤＡにはゲートウェイ装置３０のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＬＡＮ側のＭＡＣアドレスが設定される。
【０５０４】
ＨＵＢ３２は、Ｆｉｒｅｗａｌｌ３３からのフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがゲートウェイ装置３０のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置３０側のポートに出力する。
【０５０５】
ゲートウェイ装置３０は、ＨＵＢ３２からのフレームをポート３０１３より受信すると、ＰＨＹ３０１２、ＭＡＣ３０１１、ドライバ３００７、ブリッジ３００８を経由して、

中間ドライバ３００６に転送する。

【０５０６】

中間ドライバ３００６は、ブリッジ３００８よりフレームを受信する。このフレームは、受信時にはフレームフォーマットＦ１０の形をしているが、カプセル化解除３００６Ｇにおいてヘッダ Ｆ１１、ヘッダＦ１２、ヘッダＦ１３を削除し、暗号化されたデータＦ１４のみを残す。そして、データＦ１４をＴＣＰ３００６Ａに渡し、予め、ＴＣＰ３００３と中間ドライバ内のＴＣＰ３００６Ａとの間で設定されたＴＣＰセッションに流す。

【０５０７】

中間ドライバ３００６内のＴＣＰ３００６Ａは、受信したデータＦ１４に、ＴＣＰ３００３とのＴＣＰ通信に必要なＴＣＰヘッダＦ１３と、ＩＰヘッダＦ１２を付けて、再カプセル化３００６Ｅに送る。Ｆ１２内のＩＰ　ＤＡにはゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡにはゲートウェイ装置２０のＩＰアドレスが設定される。

【０５０８】

中間ドライバ３００６内の再カプセル化３００６Ｅは、ＴＣＰ３００６Ａよりデータを受信すると、これにヘッダＦ１１を付けて、ＩＰスタック３００５に送る。ここで、Ｆ１１内のＭＡＣ　ＤＡにはゲートウェイ装置３０のＭＡＣアドレスを設定し、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＷＡＮ側のＭＡＣアドレスを設定する。このようにして、ＴＣＰ３００６Ａからの受信フレームをフレームフォーマットＦ１０の形にして、ＩＰスタック３００５に転送する。

【０５０９】

ＩＰスタック３００５は、中間ドライバ３００６から受信したフレームのＭＡＣヘッダＦ１１を取り外して、ＩＰルーティング３００４に送る。

【０５１０】

ＩＰルーティング３００４は、受信したフレームのヘッダＦ１２内のＩＰ　ＤＡと、Ｆ１３内の宛先ポート番号を参照し、フレームをＴＣＰ３００３に転送する。

【０５１１】

ＴＣＰ３００３は、ＩＰルーティング３００４からフレームを受信すると、ＴＣＰプロトコルに従ってＡＣＫパケットを返送するなどの処理を行う。そして、受信したフレームから、ＴＣＰヘッダＦ１３とＩＰヘッダＦ１２を取り外し、データＦ１４をＳＳＬ３００２に転送する。

【０５１２】

ＳＳＬ３００２は、ＴＣＰ３００３からデータＦ１４を受信すると、復号化処理により暗号化を解除し、データＦ１４からＥｔｈｅｒｎｅｔフレームＦ２０、即ち、Ｆ２１～Ｆ２４を取り出し、ゲートウェイアプリケーション３００１Ａに転送する。

【０５１３】

ゲートウェイアプリケーション３００１Ａは、ＳＳＬ３００２からフレームＦ２０を受信すると、このフレームを、そのまま、仮想ＮＩＣ３０１０に流す。

【０５１４】

このフレームは、端末２１からＨＵＢ２２に送信された時の状態そのままに保たれており、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスが設定されている。又、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定されている。

【０５１５】

ゲートウェイアプリケーション３００１Ａより仮想ＮＩＣ３０１０に渡されたフレームは、ドライバ３００９、ブリッジ３００８、ＮＩＣ３０１を経由して、ＨＵＢ３２に転送される。

【０５１６】

ＨＵＢ３２は、ゲートウェイ装置３０側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームをそのままサーバ３１側のポートに出力する。

【０５１７】

サーバ３１はＨＵＢ３２から送信されたフレームを受信し、ドライバ３１０５，ＩＰスタック３１０４、ＩＰルーティング３１０３、ＴＣＰ３１０２を経由して、フレーム内のデータＦ２４をアプリケーション３１０１に渡す。

【０５１８】

以上のようにして、端末２１内のアプリケーション２１０１からサーバ３１内のアプリケーション３１０１への一連のフレーム転送が完了する。

【０５１９】

上記の例とは逆の経路を辿ることで、サーバ３１内のアプリケーション３１０１から端末２１内のアプリケーション２１０１への一連のフレーム転送も、同様に実現可能である。

【０５２０】

尚、本実施の形態でも、第１の実施の形態におけるセッション中継装置１０内のソフトウェア処理と同様に、ゲートウェイ装置３０内のソフトウェアにおいて、中間ドライバ３００６とＴＣＰ３００３の間で、一時的にＴＣＰ　ｏｖｅｒ　ＴＣＰ形式の処理になる。しかしながら、中間ドライバとＴＣＰの間では、パケットが欠落する可能性が殆ど無い為、ＴＣＰ　ｏｖｅｒ　ＴＣＰによる速度低下が発生する可能性は極めて低い。これは、ＴＣＰ　ｏｖｅｒ　ＴＣＰ問題とは、パケットロスが発生した時に著しい速度低下が発生する問題であり、仮に、パケットロスが発生しなければ、ＴＣＰ　ｏｖｅｒ　ＴＣＰ形式の処理を行っても、ヘッダＦ１３側のＴＣＰのウインドウサイズは常に大きくなり、速度低下などの問題は発生しないからである。

【０５２１】

上記の方法でヘッダＦ１３側のＴＣＰの輻輳制御と再送制御を事実上停止させても、ヘッダＦ２３側のＴＣＰの輻輳制御と再送制御は通常通り機能する為、端末２１とサーバ３１の各々のアプリケーションから見た場合、端末２１内のＴＣＰとサーバ３１内のＴＣＰの働きにより、輻輳制御、再送制御ともに問題なく行われる。

【０５２２】

本実施の形態では、ゲートウェイ装置３０側に中間ドライバ等を実装し、ゲートウェイ装置２０側に中間ドライバおよび高速化エンジンを実装する例を示したが、これとは逆に、ゲートウェイ装置２０側に中間ドライバ等を実装し、ゲートウェイ装置３０側に中間ドライバおよび高速化エンジンを実装することも可能である。更に、本実施の形態では、サーバ３１と端末２１の設置場所を入れ替えることも出来る。

【０５２３】

［発明の効果］

次に、本実施の形態の効果について説明する。

【０５２４】

本実施の形態に挙げた発明を利用すると、端末２１とサーバ３１との間で、フレームの高速転送が可能になる。

【０５２５】

これは、高速化エンジン２０１４を利用することで、ゲートウェイ装置２０のＣＰＵ２００（ソフトウェア処理）におけるカプセル化処理および暗号化／復号化処理を排除し、これら処理を全て高速化エンジン（ハードウェア）で実現できる為である。

【０５２６】

更に、これは、ゲートウェイ装置２０とゲートウェイ装置３０との間の通信において、ヘッダＦ１３の位置のＴＣＰによる輻輳制御と再送制御が発生しないよう、ゲートウェイ装置３０内の中間ドライバと、ゲートウェイ装置２０内の中間ドライバにおいて、ゲートウェイ装置２０内のＴＣＰ、又はゲートウェイ装置３０内でＴＣＰの処理を終端し、ＴＣ

Ｐ　ｏｖｅｒ　ＴＣＰ問題の発生を回避しているからである。

【０５２７】

又、本実施の形態に挙げた発明を利用すると、高速化処理の為のハードウェア（高速化エンジン）の開発費用や部材費用を、比較的低く抑えることが出来る。

【０５２８】

これは、暗号化／復号化とカプセル化を同一ハードウェア（ＦＰＧＡ／ＡＳＩＣ）上で行うことが出来るからである。

【０５２９】

又、これは、比較的安価なＭＡＣとＰＨＹ間のインタフェースに、ハードウェアを実装することが出来るからである。

【０５３０】

又、これは、ハードウェアへの実装が難しいＴＣＰ処理をソフトウェアに残し、ハードウェアへの実装が比較的容易で、かつ、高速化処理の効果が大きな暗号化／復号化とカプセル化のみをハードウェア処理できるからである。

【０５３１】

［第４の実施の形態］

本発明の第４の実施の形態は、第３の実施の形態に対して、ゲートウェイ装置２０内に高速化エンジン２０１４が無く、高速化エンジン制御２００１の代わりにゲートウェイアプリケーション２００１Ａが存在している点において異なる。すなわち、ゲートウェイ装置２０が、第３の実施の形態におけるゲートウェイ装置３０と、同様の構成を有し、同様の動作を行う。

【０５３２】

第４の実施の形態における端末２１，サーバ３１、ＨＵＢ２２，ＨＵＢ３２、ゲートウェイ装置３０、イントラネット２、イントラネット３の構成および動作は、第３の実施の形態と同じである。

【０５３３】

第４の実施の形態においては、イントラネット２は、閉域ＬＡＮだけ無く、インターネット等のオープンなＷＡＮを用いても構わない。

【０５３４】

［構成の説明］

図２０は、第４の実施の形態における各機器の構成と、フレームの転送経路を詳細に示したブロック図である。

【０５３５】

ゲートウェイ装置２０は、第３の実施の形態におけるゲートウェイ装置２０に対して、高速化エンジン２０１４が無く、高速化エンジン制御２００１の代わりにゲートウェイアプリケーション２００１Ａが存在している点、更にブリッジ２００８，ドライバ２００９，仮想ＮＩＣ２０１０が追加されている点において異なる。

【０５３６】

ゲートウェイアプリケーション２００１Ａ、ブリッジ２００８、ドライバ２００９、仮想ＮＩＣ２０１０は、ゲートウェイ装置３０内のゲートウェイアプリケーション３００１Ａ、ブリッジ３００８、ドライバ３００９、仮想ＮＩＣ３０１０と、各々、同様の動作を行う。

【０５３７】

仮想ＮＩＣ３０１０、ドライバ３００９、ブリッジ３００８は、中間ドライバ３００６にその機能を纏め、一体化させることも出来る。この場合、ゲートウェイアプリケーション３００１Ａから出たフレームは、中間ドライバ３００６を経由してドライバ３００７に渡され、又、ドライバ３００７から入力した自ノード宛て以外のユニキャストフレーム若しくはブロードキャストフレームは、中間ドライバ３００６からゲートウェイアプリケーション３００１Ａに送られる。

【０５３８】

端末２１、サーバ３１、ゲートウェイ装置２０、Ｆｉｒｅｗａｌｌ３３，ＨＵＢ２２、ＨＵＢ３２に関しては、第３の実施の形態と同様の構成を有し、同様の動作を行う。

【０５３９】

従って、第４の実施の形態では、ゲートウェイ装置２０とゲートウェイ装置３０との間で、予め、ＳＳＬセッションを設定している場合のみ、イントラネット２内の機器からイントラネット３内の機器へのアクセスが可能になる。

【０５４０】

［動作の説明］

［ＳＳＬセッションの確立動作］

図２０を用いて、第４の実施の形態において、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合を例に挙げて、動作の説明を行う。

【０５４１】

この際、ブリッジ２００８，ブリッジ３００８、ＨＵＢ２２やＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３のＷＡＮ側，Ｆｉｒｅｗａｌｌ３３のＬＡＮ側、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。

【０５４２】

又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。

【０５４３】

ゲートウェイ装置２０内のゲートウェイアプリケーション２００１Ａは、起動後ゲートウェイ装置３０からの接続待ち受け状態になると、中間ドライバ２００６に対して、待ち受け開始を通知する。この通知には、ゲートウェイ装置２０のＩＰアドレス、ゲートウェイアプリケーション２００１Ａの待ち受けポート番号が含まれる。

【０５４４】

中間ドライバ２００６は、ゲートウェイアプリケーション２００１Ａからの通知を受けると、フレーム解析処理において、ゲートウェイアプリケーション２００１Ａ宛てのパケットが到着した際に、ＴＣＰ接続/終端などの処理が出来るよう設定を行う。

【０５４５】

ゲートウェイ装置３０内のゲートウェイアプリケーション３００１Ａは、ユーザからのゲートウェイ装置２０内のゲートウェイアプリケーション２００１Ａへの接続要求を受け、ＳＳＬ３００２にゲートウェイ装置２０内のゲートウェイアプリケーション２００１Ａへの通信開始を指示する。同時に、中間ドライバ３００６に対して、ゲートウェイ装置２０内のゲートウェイアプリケーション２００１Ａへの通信開始を通知する。この通知には、ゲートウェイ装置２０のＩＰアドレス、ゲートウェイアプリケーション２００１Ａのポート番号、及びゲートウェイアプリケーション３００１Ａの送信元ポート番号、更にゲートウェイ装置３０のＩＰアドレスが含まれる。

【０５４６】

ＳＳＬ３００２は、ゲートウェイアプリケーション３００１Ａからの通信開始指示を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為に、ＴＣＰ３００３にゲートウェイ装置２０内のゲートウェイアプリケーション２００１Ａへの通信開始を指示する。

【０５４７】

ＴＣＰ３００３は、ＳＳＬ３００２からの通信開始指示を受け、ＴＣＰ２００３との間でＴＣＰセッションを確立する為に、ＩＰルーティング３００４に対して、ＴＣＰ２００３とのＴＣＰセッション確立要求パケット（ＳＹＮ）を送信する。このセッション確立要求パケットはＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにゲートウェイ装置２０宛、宛先ポート番号にＴＣＰ２００３が設定されている。セッション確立要求パケットとは、ＴＣＰセッションの確立時に、スリーウェイハンドシェーク（ｔｈｒｅｅ　ｗａｙ

ｈａｎｄｓｈａｋｅ）の為に送信される、ＳＹＮパケットパケットのことである。本明細書においては、ＳＳＬセッション確立動作の説明を簡略化するため、スリーウェイハンドシェークで送受信されるパケットうち、ＳＹＮパケットをＴＣＰセッション確立要求パケットと呼び、ＳＹＮ＋ＡＣＫパケットを応答パケットと呼んでいる。また実際にはＡＣＫパケットも送信されるが、ＡＣＫパケットについてはＳＹＮパケットと同様に転送されるため、本動作の説明では説明を省略する。

【０５４８】

ＩＰルーティング３００４は、ＴＣＰ３００３から受信したパケットの宛先ＩＰアドレスと宛先ポート番号を参照し、セッション確立要求パケットをＩＰスタック３００５に転送する。

【０５４９】

ＩＰスタック３００５は、ＩＰルーティング３００４より受信したパケットに、Ｆｉｒｅｗａｌｌ１３３内のイントラネット３側のＭＡＣアドレスを宛先ＭＡＣアドレスとして付加し、更に送信元ＭＡＣアドレスに自ノードのＭＡＣアドレスを設定してセッション確立要求のフレームを生成し、中間ドライバ３００６に転送する。

【０５５０】

中間ドライバ３００６は、ＩＰスタック３００５からフレームを受信し、フレーム解析を行う。解析の結果、フレームは予めゲートウェイアプリケーション３００１より通知された宛先ＩＰ、宛先ポート、送信元ＩＰ、送信元ポートが付加されたフレームであるので、カプセル化解除においてＭＡＣヘッダを取り外し、中間ドライバ３００６のＴＣＰ部でＴＣＰ３００３からＴＣＰ２００３へのＴＣＰの処理を終端する。すなわち、ＴＣＰ３００３は、本来は、ＴＣＰ２００３に対してセッション確立要求を送信したが、実際は、この要求に対して中間ドライバ３００６内のＴＣＰが受信して保留し、ＴＣＰ３００３と中間ドライバ３００６内のＴＣＰとの間でＴＣＰセッションの確立処理を行い、終端させる。

【０５５１】

中間ドライバ３００６は、ＴＣＰ終端処理を行う際、中間ドライバ２００６に対して、ＴＣＰ２００３との間でＴＣＰセッションを確立するよう要求する為、ブリッジ３００８を経由してドライバ３００７に接続要求のパケットを送る。尚、この接続要求パケットはＴＣＰ規格に沿ったパケットではなく、本発明の通信システム独自のパケットである。このパケットは、宛先ＩＰアドレスにゲートウェイ装置２０を、宛先ポート番号にＴＣＰ２００３を設定する。そしてこのパケットに宛先ＭＡＣアドレスを付加して、更に送信元ＭＡＣアドレスに自ノードを設定して接続要求フレームを生成する。

【０５５２】

ドライバ３００７は、中間ドライバ３００６からフレームを受信し、ＭＡＣ３０１１に転送する。

【０５５３】

ＭＡＣ３０１１は、ドライバ３００７からフレームを受信し、ＰＨＹ３０１２に転送する。

【０５５４】

ＰＨＹ３０１２は、ＭＡＣ３０１１からフレームを受信し、ポート３０１３に転送する。

【０５５５】

ポート３０１３は、ＰＨＹ３０１２からフレームを受信し、イーサネットケーブルを経由してＨＵＢ３２に転送する。

【０５５６】

ＨＵＢ３２は、フレームを受信すると、ＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ１３３のＬＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ１３３側のポートに出力する。

【０５５７】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からフレームを受信し、ゲートウェイ装置３０からゲートウェイ装置２０への通信の為、これを許可し、ＨＵＢ２２に転送する。

【０５５８】

ＨＵＢ２２は、Ｆｉｒｅｗａｌｌ３３からフレームを受信し、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０に転送する。

【０５５９】

ゲートウェイ装置２０は、ＨＵＢ２２内からフレームを受信し、ポート２０１３、ＰＨＹ２０１２、ＭＡＣ２０１１、ドライバ２００７、ブリッジ２００８の経路でフレームを転送し、中間ドライバ２００６に転送する。

【０５６０】

中間ドライバ２００６は、ドライバ２００７からフレームを受信し、フレーム解析を行う。解析の結果、このフレームは予めゲートウェイアプリケーション２００１Ａより通知された、ゲートウェイアプリケーション２００１Ａへの宛先ＩＰ、及び宛先ポートが付加された接続要求のフレームであるので、このフレームを受信し、カプセル化解除においてＭＡＣヘッダを取り外してパケットにする。このパケットは、中間ドライバ３００６から中間ドライバ２００６に向けて送信されたＴＣＰ２００３への接続要求パケットである為、中間ドライバ２００６内のＴＣＰは、ＴＣＰ２００３との間でＴＣＰセッションを確立する為に、ＩＰスタック２００５に対して、ＴＣＰ２００３とのセッション確立に必要なセッション確立要求パケットを送信する。このパケットはＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにゲートウェイ装置２０宛、宛先ポート番号にＴＣＰ２００３が設定され、更に、送信元ＩＰアドレスにはゲートウェイ装置３０のＩＰアドレスが設定され、送信元ポート番号にはＴＣＰ３００３のポート番号が設定される。

【０５６１】

すなわち、中間ドライバ２００６内のＴＣＰは、ＴＣＰ３００３の名前を騙ってＴＣＰ２００３に対してＴＣＰセッション確立要求を行う。従って、ＴＣＰ２００３は、恰も、ＴＣＰ３００３と通信しているかのように認識し、更にＴＣＰ３００３は、恰も、ＴＣＰ２００３と通信しているかのように認識する。しかしながら、実際のＴＣＰ処理は、ＴＣＰ３００３と中間ドライバ３００６内のＴＣＰとの間、及び中間ドライバ２００６とＴＣＰ２００３との間で行われ、更に中間ドライバ３００６と中間ドライバ２００６との間は、ＵＤＰ等の輻輳制御の無い方法（本発明の通信システムにおける独自のパケット）で、別途に通信が行われる。そして、ＴＣＰ３００３と中間ドライバ３００６間のＴＣＰセッションと、中間ドライバ３００６と中間ドライバ２００６の間のＵＤＰ等何らかの通信セッション、更に中間ドライバ２００６とＴＣＰ２００３の間のＴＣＰセッションが、中間ドライバ３００６及び中間ドライバ２００６によって相互に接続・中継されることにより、恰も、ＴＣＰ３００３とＴＣＰ２００３との間でＴＣＰセッションが確立しているかのように通信が行われる。

【０５６２】

ＩＰスタック２００５は、中間ドライバ２００６からフレームを受信し、ＭＡＣヘッダを外してパケットにしてＩＰルーティング２００４に転送する。

【０５６３】

ＩＰルーティング２００４は、ＩＰスタック２００５より受信したパケットの宛先ポート番号を参照し、ＴＣＰ２００３側のポート番号が付加されていることから、このパケットをＴＣＰ２００３に転送する。

【０５６４】

ＴＣＰ２００３は、ＩＰルーティング２００４よりパケットを受信する。このパケットは、ＴＣＰセッション確立要求パケット（ＳＹＮ）であるので、ＴＣＰセッション確立の為に、ＴＣＰプロトコルに従いって必要な応答パケット（ＳＹＮ＋ＡＣＫ）を返送する。この際、ＴＣＰ２００３は、受信したＴＣＰセッション確立要求は、ＴＣＰ３００３から届いたものであると認識する。これは、実際の確立要求は中間ドライバ２００６内のＴＣＰから送信されたものであるが、中間ドライバ２００６内のＴＣＰは、ＴＣＰ３００３を

騙ってＴＣＰ２００３にセッション確立要求を行った為、ＴＣＰ２００３は、恰も、ＴＣＰ３００３とセッションを確立すると認識する。

【０５６５】

従って、ＴＣＰ２００３は、ＴＣＰ規格に沿って生成した応答パケット（ＳＹＮ＋ＡＣＫ）を、ＴＣＰ３００３宛てに送信する。すなわち、応答パケットの宛先ＩＰはゲートウェイ装置３０のＩＰアドレスが設定され、応答パケットの宛先ポートは、ＴＣＰ３００３のポート番号が設定される。

【０５６６】

応答パケットは、ＩＰルーティング２００４を経由してＩＰスタック２００５に送られ、ここでＭＡＣヘッダが付加されて応答フレームになり、中間ドライバ２００６に届く。

【０５６７】

中間ドライバ２００６は、応答フレームを受信すると、中間ドライバ２００６内のカプセル化解除において応答フレームのＭＡＣヘッダを外して応答パケットを取り出し、中間ドライバ２００６のＴＣＰで受信して、応答パケットに対するＡＣＫパケットをＴＣＰ２００３に送信してＴＣＰ処理を終端させる。そして、中間ドライバ３００６に対して、接続完了通知の為の接続完了通知パケットを送信する。この接続完了通知パケットはＴＣＰの規格に沿ったパケットではなく、独自のパケットである。この接続完了通知パケットの宛先ＩＰアドレスにはゲートウェイ送装置３０が、宛先ポート番号にはＴＣＰ３００３が、送信元ＩＰアドレスにはゲートウェイ装置２０が、送信元ポート番号にはＴＣＰ２００３が設定される。そして中間ドライバ２００６内の再カプセル化において、接続完了通知パケットにＭＡＣヘッダを付加されて接続完了通知フレームが生成される。

【０５６８】

接続完了通知フレームは、接続要求フレームとは逆の経路、即ち、ドライバ２００７，ＮＩＣ２０１，ＨＵＢ２２，Ｆｉｒｅｗａｌｌ３３、ＨＵＢ３２，ＮＩＣ３０１を経由して、ＣＰＵ３００内の中間ドライバ３００６に届く。

【０５６９】

中間ドライバ３００６は、接続完了通知フレームを受信し、フレーム解析を行う。解析の結果、受信したフレームは、予め、ゲートウェイアプリケーション３００１Ａより通知された、ゲートウェイアプリケーション３００１Ａへの宛先ＩＰ、及び宛先ポートが付加されたフレームであるので、このフレームを受信して、カプセル化解除におｋ手ＭＡＣヘッダを取り外してパケットにする。このパケットは、中間ドライバ２００６から中間ドライバ３００６に向けて送信されたＴＣＰ２００３と中間ドライバ２００６との間の接続完了通知パケットである為、中間ドライバ３００６内のＴＣＰは、ＴＣＰプロトコルに従い、ＴＣＰセッション確立の為に必要な応答パケット（ＳＹＮ＋ＡＣＫ）をＴＣＰ３００３に送る為、ＩＰスタック３００５に対して、応答パケットを送信する。

【０５７０】

応答パケットは、ＩＰスタック３００５、ＩＰルーティング３００４を経由し、ＴＣＰ３００３に到達する。

【０５７１】

ＴＣＰ３００３は、ＩＰルーティング３００４よりパケットを受信する。このパケットは、ＴＣＰセッションの確立要求に対する応答パケットであるので、ＳＳＬ３００２に対して、ＴＣＰ２００３とのＴＣＰセッション接続完了を通知する。この際、ＴＣＰ３００３は、応答パケットが、ＴＣＰ２００３から届いたものであると認識する。これは、実際の応答は中間ドライバ３００６内のＴＣＰから送信されたものであるが、中間ドライバ３００６内のＴＣＰは、ＴＣＰ２００３を騙ってＴＣＰ３００３にセッション確立に対しての応答を行った為、ＴＣＰ３００３は、恰も、ＴＣＰ２００３から応答があったと認識する。

【０５７２】

ＴＣＰ３００３は応答パケットを受信すると、この応答パケットに対してＡＣＫパケットを生成してＴＣＰ２００３宛に送信する。このＡＣＫパケットは、中間ドライバ３００

６のＴＣＰが、ＩＰルーティング２００４及びＩＰスタック２００５を介して受信し、ＴＣＰ処理を終端させる。

【０５７３】

ＳＳＬ３００２は、ＴＣＰ３００３からの接続完了通知を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為、ＳＳＬプロトコルに従い、セッション確立要求の為のパケット（ＳＳＬセッション確立要求パケット）を送信する。

【０５７４】

ＳＳＬセッション確立要求パケットは、ＴＣＰ３００３で受信されると、ＴＣＰ３００３と中間ドライバ３００６内のＴＣＰとの間で設定されたＴＣＰセッションを通り、中間ドライバ３００６に到着する。

【０５７５】

中間ドライバ３００６は、ＳＳＬセッション確立要求パケットを受信してＴＣＰセッションを終端させ、ＵＤＰ等の輻輳制御の掛からないヘッダを付け、パケットを中間ドライバ２００６に向け送信する。パケットはＮＩＣ３０１、ＨＵＢ３２，Ｆｉｒｅｗａｌｌ３３、ＨＵＢ２２、ＮＩＣ２０１を経由して、中間ドライバ２００６に到着する。この際、ＮＩＣ２０１内の高速化エンジン２０１４は、ＰＨＹ２０１２から受信したパケットを、そのまま、ＭＡＣ２０１１に転送する。

【０５７６】

中間ドライバ２００６は、ＳＳＬセッション確立要求パケットを受信すると、中間ドライバ２００６内のＴＣＰとＴＣＰ２００３との間で設定されたＴＣＰセッションを通り、ＴＣＰ２００３に到着する。

【０５７７】

ＴＣＰ２００３は、ＳＳＬセッション確立要求パケットをＳＳＬ２００２に転送する。

【０５７８】

ＳＳＬ２００２は、ＳＳＬセッション確立要求の内容を検証し、問題が無ければ、ゲートウェイアプリケーション２００１Ａに対して、ＳＳＬ３００２とのセッション確立を通知すると同時に、ＳＳＬプロトコルに従い、ＳＳＬ３００２に対してＳＳＬセッション確立応答パケットを送信する。

【０５７９】

ＳＳＬセッション確立応答パケットは、ＳＳＬセッション確立要求パケットとは逆の経路、即ち、ＴＣＰ２００３と中間ドライバ２００６との間のＴＣＰセッションを経由して中間ドライバ２００６に到達し、中間ドライバ２００６と中間ドライバ３００６の間のＵＤＰ等の輻輳制御の無いセッションを経由して中間ドライバ３００６に到達する。更に、中間ドライバ３００６とＴＣＰ３００３との間のＴＣＰセッションを経由して、ＳＳＬ３００２に到達する。

【０５８０】

ＳＳＬ３００２は、ＳＳＬセッション確立応答の内容をＳＳＬプロトコルに従い検証し、問題が無ければ、ゲートウェイアプリケーション３００１Ａに対して、ＳＳＬ３００２とＳＳＬ２００２との間のＳＳＬセッション確立を通知する。

【０５８１】

以上のようにして、中間ドライバ２００６と中間ドライバ３００６の間で、フレーム転送の為のＵＤＰ等の輻輳制御の無いセッションが確立される。又、ＳＳＬ２００２とＳＳＬ３００２との間で、ＳＳＬセッションが確立される。

【０５８２】

以上により、第４の実施の形態において、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合の動作が完了する。

【０５８３】

［端末２１からサーバ３１へのフレーム転送動作］

図２０を用いて、第４の実施の形態において、端末２１からサーバ３１へフレームを送

信する場合を例に挙げて、動作の説明を行う。

【０５８４】

この際、ブリッジ２００８，ブリッジ３００８，ＨＵＢ２２、ＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。

【０５８５】

又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。

【０５８６】

更に、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）が、上述の動作例により既に設定されているものとする。

【０５８７】

又、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション（アプリケーション３１０１）との間で、既に、ＴＣＰセッションが構築されているとする。

【０５８８】

端末２１内のアプリケーション２１０１が、サーバ３１内のアプリケーション３１０１宛のデータを、ＴＣＰ２１０２に渡す。

【０５８９】

ＴＣＰ２１０２は、アプリケーション２１０１からデータを受け取り、ＴＣＰプロトコルに従ってＴＣＰヘッダ（図２におけるＦ２３）やＩＰヘッダ（図２におけるＦ２２）を付けてＩＰパケットとし、ＩＰルーティング２１０３に渡す。この時、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定される。

【０５９０】

ＩＰルーティング２１０３は、ＴＣＰ２１０２から受信したパケットの宛先ＩＰアドレス（サーバ３１宛て）及び宛先ポート（ＴＣＰ３１０２宛て）を参照し、データを、そのまま、ＩＰスタック２１０４に転送する。

【０５９１】

ＩＰスタック２１０４は、ＩＰルーティング２１０３からパケットを受信し、ＭＡＣヘッダ（図２におけるＦ２１）を付けてＥｔｈｅｒｎｅｔフレームを作成し、ドライバ２１０５に渡す。このフレームはＥｔｈｅｒｎｅｔフレームＦ２０のフォーマットを有する。この時、ＩＰスタック２１０４は、ＡＲＰの結果を参照して、フレームのＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスを設定し、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスを設定する。

【０５９２】

ドライバ２１０５は、ＩＰスタック２１０５より上記フレームを受け取り、ＮＩＣ２１１に転送する。

【０５９３】

ＮＩＣ２１１は、ドライバ２１０５よりフレームを受け取り、ＭＡＣ２１１１，ＰＨＹ２１１２，ポート２１１３を経由して、ＨＵＢ２２にフレームを転送する。

【０５９４】

ＨＵＢ２２は、端末２１のＮＩＣ２１１側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０側のポートに出力する。

【０５９５】

ゲートウェイ装置２０は、ＨＵＢ２２からのフレームをポート２０１３において受け取り、ＰＨＹ２０１２、ＭＡＣ２０１１、ドライバ２００７を経由して、ブリッジ２００８に渡す。

【０５９６】
ブリッジ２００８は、ドライバ２００７から受信したフレーム（フレームフォーマットＦ２０形式）内のヘッダＦ２１内に存在するＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のＭＡＣアドレスであり、ゲートウェイ装置２０のＭＡＣアドレスでは無いことから、フレームをドライバ２００９に転送する。
【０５９７】
ブリッジ２００８から送信されたフレームは、ドライバ２００９、仮想ＮＩＣ２０１０を経由し、ゲートウェイアプリケーション２００１Ａに転送される。
【０５９８】
ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したフレームを、ゲートウェイアプリケーション２００１Ａとゲートウェイアプリケーション３００１Ａの間に設定したＳＳＬセッションに流す。すなわち、ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したＥｔｈｅｒｎｅｔフレーム（フレームフォーマットＦ２０）をデータとしてＳＳＬ２００２に渡す。
【０５９９】
ＳＳＬ２００２は、ゲートウェイアプリケーション２００１Ａからデータ（Ｆ２１～Ｆ２４）を受け取ると、これを暗号化してデータＦ１４を生成し、ＴＣＰ２００３に渡す。
【０６００】
ＴＣＰ２００３は、ＳＳＬ２００２よりデータＦ１４を受け取り、ＴＣＰヘッダＦ１３、及びＩＰヘッダＦ１２を付けて、ＩＰルーティング２００４に渡す。
【０６０１】
ここで、Ｆ１２内のＩＰ　ＤＡには、ゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡには、ゲートウェイ装置２０のＩＰアドレスが設定される。又、宛先ポートにはＴＣＰ３００３のポートが設定され、送信元ポートにはＴＣＰ２００３のポートが指定される。
【０６０２】
ＩＰルーティング２００４は、ＴＣＰ２００３より受信したデータのＩＰヘッダＦ１２内のＩＰアドレス等を参照し、フレームをＩＰスタック２００５に渡す。
【０６０３】
ＩＰスタック２００５は、ＩＰルーティング２００４よりフレームを受信し、フレームにＭＡＣヘッダＦ１１をつけて、Ｅｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームフォーマットＦ１０の形式にして、中間ドライバ２００６に渡す。
【０６０４】
ここで、Ｆ１１内のＭＡＣ　ＤＡには、ＡＲＰの結果よりＦｉｒｅｗａｌｌ　３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡには、ゲートウェイ装置２０のＭＡＣアドレスが設定される。
【０６０５】
中間ドライバ２００６は、ＩＰスタック２００５よりフレームを受信し、フレーム解析２００６Ｈにおいてフレーム解析を行う。すると解析の結果、フレームが、予め、ゲートウェイアプリケーション２００１Ａより通知された、ゲートウェイ装置３０との間のＳＳＬセッションのフレームであることから、カプセル化解除２００６Ｆにおいて、このフレームのＭＡＣヘッダＦ１１を削除して保存し、ＴＣＰ２００６Ａに渡す。
【０６０６】
中間ドライバ２００６内のＴＣＰ２００６Ａは、ＴＣＰ２００３Ａを終端する。すなわち、フレームのＩＰヘッダＦ１２とＭＡＣヘッダＦ１３を削除してＦ１４のみを残し、データＦ１４をフラグメント分割２００６Ｂに送る。更に、ＴＣＰ２００３に対してＡＣＫフレームを送信する。
【０６０７】
中間ドライバ２００６内のフラグメント分割２００６Ｂは，ＴＣＰ２００６Ａから受信したデータＦ１４のサイズを確認し、フラグメントの必要が無いことから、そのまま、デ

ータを再カプセル化２００６Ｄに送る。

【０６０８】

中間ドライバ２００６内の再カプセル化２００６Ｄは、フラグメント分割２００６Ｂより受信したデータＦ１４に、ＭＡＣヘッダＦ１１、ＩＰヘッダＦ１２、ＭＡＣヘッダＦ１３を付け、フレームフォーマットＦ１０の形式にして、ブリッジ２００８に送信する。この際、Ｆ１１内のＭＡＣ　ＤＡにはＦｉｒｅｗａｌｌ　３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡには、ゲートウェイ装置２０のＭＡＣアドレスが設定される。又、Ｆ１２内のＩＰ　ＤＡには、ゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡには、ゲートウェイ装置２０のＩＰアドレスが設定される。又、宛先ポートにはＴＣＰ３００３のポートが設定され、送信元ポートにはＴＣＰ２００３のポートが指定される。これらのヘッダは、カプセル化解除２００６Ｆによって保存されたものである。

【０６０９】

中間ドライバより送信されたフレームは、ブリッジ２００８、ドライバ２００７，ＮＩＣ２０１を経由して、ＨＵＢ２２に送られる。

【０６１０】

ＨＵＢ２２は、ゲートウェイ装置２２側のポートからフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＷＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３に出力する。

【０６１１】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からのフレームを受信し、ＩＰ　ＤＡを参照してＭＡＣヘッダＦ１１を変更し、受信フレームをフレームフォーマットＦ１０の形のまま、ＨＵＢ３２に転送する。

【０６１２】

ここで、Ｆ１１内のＭＡＣ　ＤＡにはゲートウェイ装置３０のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＬＡＮ側のＭＡＣアドレスが設定される。

【０６１３】

ＨＵＢ３２は、Ｆｉｒｅｗａｌｌ３３からのフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがゲートウェイ装置３０のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置３０側のポートに出力する。

【０６１４】

ゲートウェイ装置３０は、ＨＵＢ３２からのフレームをポート３０１３より受信すると、ＰＨＹ３０１２、ＭＡＣ３０１１、ドライバ３００７、ブリッジ３００８を経由して、中間ドライバ３００６に転送する。

【０６１５】

中間ドライバ３００６は、ブリッジ３００８よりフレームを受信する。このフレームは、受信時にはフレームフォーマットＦ１０の形をしているが、カプセル化解除３００６Ｇにおいてヘッダ Ｆ１１、ヘッダＦ１２、ヘッダＦ１３を削除し、暗号化されたデータＦ１４のみを残す。そして、データＦ１４をＴＣＰ３００６Ａに渡し、予め、ＴＣＰ３００３と中間ドライバ内のＴＣＰ３００６Ａとの間で設定されたＴＣＰセッションに流す。中間ドライバ３００６内のＴＣＰ３００６Ａは、受信したデータＦ１４に、ＴＣＰ３００３とのＴＣＰ通信に必要なＴＣＰヘッダＦ１３と、ＩＰヘッダＦ１２を付けて、再カプセル化３００６Ｅに送る。Ｆ１２内のＩＰ　ＤＡにはゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡにはゲートウェイ装置２０のＩＰアドレスが設定される。

【０６１６】

中間ドライバ３００６内の再カプセル化３００６Ｅは、ＴＣＰ３００６Ａよりデータを受信すると、これにヘッダＦ１１を付けて、ＩＰスタック３００５に送る。ここで、Ｆ１

１内のＭＡＣ　ＤＡにはゲートウェイ装置３０のＭＡＣアドレスを設定し、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＷＡＮ側のＭＡＣアドレスを設定する。このようにして、ＴＣＰ３００６Ａからの受信フレームをフレームフォーマットＦ１０の形にして、ＩＰスタック３００５に転送する。

【０６１７】

ＩＰスタック３００５は、中間ドライバ３００６から受信したフレームのＭＡＣヘッダＦ１１を取り外して、ＩＰルーティング３００４に送る。

【０６１８】

ＩＰルーティング３００４は、受信したフレームのヘッダＦ１２内のＩＰ　ＤＡと、Ｆ１３内の宛先ポート番号を参照し、フレームをＴＣＰ３００３に転送する。

【０６１９】

ＴＣＰ３００３は、ＩＰルーティング３００４からフレームを受信すると、ＴＣＰプロトコルに従ってＡＣＫパケットを返送するなどの処理を行う。そして、受信したフレームから、ＴＣＰヘッダＦ１３とＩＰヘッダＦ１２を取り外し、データＦ１４をＳＳＬ３００２に転送する。

【０６２０】

ＳＳＬ３００２は、ＴＣＰ３００３からデータＦ１４を受信すると、復号化処理により暗号化を解除し、データＦ１４からＥｔｈｅｒｎｅｔフレームＦ２０、即ち、Ｆ２１～Ｆ２４を取り出し、ゲートウェイアプリケーション３００１Ａに転送する。

【０６２１】

ゲートウェイアプリケーション３００１Ａは、ＳＳＬ３００２からフレームＦ２０を受信すると、このフレームを、そのまま、仮想ＮＩＣ３０１０に流す。

【０６２２】

このフレームは、端末２１からＨＵＢ２２に送信された時の状態そのままに保たれており、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスが設定されている。又、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定されている。

【０６２３】

ゲートウェイアプリケーション３００１Ａより仮想ＮＩＣ３０１０に渡されたフレームは、ドライバ３００９、ブリッジ３００８、ＮＩＣ３０１を経由して、ＨＵＢ３２に転送される。

【０６２４】

ＨＵＢ３２は、ゲートウェイ装置３０側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、サーバ３１側のポートに出力する。

【０６２５】

サーバ３１は、ＨＵＢ３２から送信されたフレームを受信し、ドライバ３１０５，ＩＰスタック３１０４、ＩＰルーティング３１０３、ＴＣＰ３１０２を経由して、フレーム内のデータＦ２４をアプリケーション３１０１に渡す。

【０６２６】

以上のようにして、端末２１内のアプリケーション２１０１からサーバ３１内のアプリケーション３１０１への一連のフレーム転送が完了する。

【０６２７】

上記の例とは逆の経路を辿ることで、サーバ３１内のアプリケーション３１０１から端末２１内のアプリケーション２１０１への一連のフレーム転送も、同様に実現可能である。

【０６２８】

尚、本実施の形態でも、第１の実施の形態におけるセッション中継装置１０内のソフトウェア処理と同様に、ゲートウェイ装置３０内のソフトウェアと、ゲートウェイ装置２０内のソフトウェアにおいて、中間ドライバ３００６とＴＣＰ３００３の間、及び中間ドライバ２００６とＴＣＰ２００３との間で、一時的にＴＣＰ　ｏｖｅｒ　ＴＣＰ形式の処理になる。しかしながら、中間ドライバとＴＣＰの間では、パケットが欠落する可能性が殆ど無い為、ＴＣＰ　ｏｖｅｒ　ＴＣＰによる速度低下が発生する可能性は極めて低い。これは、ＴＣＰ　ｏｖｅｒ　ＴＣＰ問題とは、パケットロスが発生した時に著しい速度低下が発生する問題であり、仮に、パケットロスが発生しなければ、ＴＣＰ　ｏｖｅｒ　ＴＣＰ形式の処理を行っても、ヘッダＦ１３側のＴＣＰのウインドウサイズは常に大きくなり、速度低下などの問題は発生しないからである。

【０６２９】

上記の方法でヘッダＦ１３側のＴＣＰの輻輳制御と再送制御を事実上停止させても、ヘッダＦ２３側のＴＣＰの輻輳制御と再送制御は通常通り機能する為、端末２１とサーバ３１の各々のアプリケーションから見た場合、端末２１内のＴＣＰとサーバ３１内のＴＣＰの働きにより、輻輳制御、再送制御ともに問題なく行われる。

【０６３０】

尚、本実施の形態では、サーバ３１と端末２１の設置場所を入れ替えることも出来る。

【０６３１】

［発明の効果］

次に、本実施の形態の効果について説明する。

【０６３２】

本実施の形態に挙げた発明を利用すると、端末２１とサーバ３１との間で、フレームの高速転送が可能になる。

【０６３３】

これは、ゲートウェイ装置２０とゲートウェイ装置３０との間の通信において、ヘッダＦ１３の位置のＴＣＰによる輻輳制御と再送制御が発生しないよう、ゲートウェイ装置３０内の中間ドライバと、ゲートウェイ装置２０内の中間ドライバにおいて、ゲートウェイ装置２０内のＴＣＰと、ゲートウェイ装置３０内のＴＣＰを終端し、ＴＣＰ　ｏｖｅｒ　ＴＣＰ問題の発生を回避しているからである。

【０６３４】

［第５の実施の形態］

本発明の第５の実施の形態は、第４の実施の形態に対して、ゲートウェイ装置２０内の中間ドライバ２００６と、ゲートウェイ装置３０内の中間ドライバ３００６が無くなり、代わりに端末２１内の中間ドライバ２１０６と、サーバ３１内の中間ドライバ３１０６が、各々、設置されている点において異なる。

【０６３５】

第５の実施の形態におけるＨＵＢ２２，ＨＵＢ３２、イントラネット２、イントラネット３の構成および動作は、第４の実施の形態と同じである。

【０６３６】

第５の実施の形態においては、イントラネット２は、閉域ＬＡＮだけで無く、インターネット等のオープンなＷＡＮを用いても構わない。

【０６３７】

［構成の説明］

図２１は、第５の実施の形態における各機器の構成とフレームの転送経路を詳細に示したブロック図である。

【０６３８】

ゲートウェイ装置２０は、第４の実施の形態におけるゲートウェイ装置２０に対して、中間ドライバ２００６が無くなっている点、及びゲートウェイアプリケーション２００１Ａが中間ドライバ２００６に対して、ＳＳＬセッションに関する情報（ゲートウェイアプリケーションのポート番号等）を伝達しなくなっている点において異なる。

【０６３９】
ゲートウェイ装置３０は、第４の実施の形態におけるゲートウェイ装置３０に対して、中間ドライバ３００６が無くなっている点、及びゲートウェイアプリケーション３００１Ａが中間ドライバ３００６に対して、ＳＳＬセッションに関する情報（ゲートウェイアプリケーションのポート番号等）を伝達しなくなっている点において異なる。
【０６４０】
端末２１は、第４の実施の形態における端末２１に対して、中間ドライバ２１０６が設置されている点において異なる。
【０６４１】
中間ドライバ２１０６は、第４の実施の形態における中間ドライバ２００６や、図７に示す第１の実施の形態における中間ドライバ１００８と、同様の構成を有し、同様の動作を行う。但し、予め、全てのアプリケーションからのＴＣＰパケットを、一旦、終端するように設定されている。その為、第４の実施の形態における、ゲートウェイアプリケーション２００１Ａから中間ドライバ２００６への、ゲートウェイアプリケーション２００１Ａのポート番号の伝達のような動作は不要である。
【０６４２】
サーバ３１は、第４の実施の形態におけるサーバ３１に対して、中間ドライバ３１０６が設置されている点において異なる。
【０６４３】
中間ドライバ３１０６は、第４の実施の形態における中間ドライバ３００６や、図７に示す第１の実施の形態における中間ドライバ１００８と、同様の構成を有し、同様の動作を行う。但し、予め、全てのアプリケーションからのＴＣＰパケットを、一旦、終端するように設定されている。その為、第４の実施の形態における、ゲートウェイアプリケーション３００１Ａから中間ドライバ３００６への、ゲートウェイアプリケーション３００１Ａのポート番号の伝達のような動作は不要である。
【０６４４】
ＨＵＢ２２、ＨＵＢ３２に関しては、第４の実施の形態と同様の構成を有し、同様の動作を行う。
【０６４５】
Ｆｉｒｅｗａｌｌ３３は、第４の実施の形態のＦｉｒｅｗａｌｌ３３と同様の構成を有し、同様の動作を行う。但し、本実施の形態においては、Ｆｉｒｅｗａｌｌ３３の代わりに、ＮＡＴルータやＰｒｏｘｙサーバを用いても良い。
【０６４６】
第５の実施の形態でも、他の実施の形態と同様に、ゲートウェイ装置２０とゲートウェイ装置３０との間で、予め、ＳＳＬセッションを設定している場合のみ、イントラネット２内の機器からイントラネット３内の機器へのアクセスが可能になる。
【０６４７】
［動作の説明］
［ＳＳＬセッションの確立動作］
図２１を用いて、第５の実施の形態において、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合を例に挙げて、動作の説明を行う。
【０６４８】
この際、ブリッジ２００８，ブリッジ３００８、ＨＵＢ２２やＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３のＬＡＮ側，Ｆｉｒｅｗａｌｌ３３のＷＡＮ側、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。
【０６４９】
又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ゲートウェイ装置２０やゲート

ウェイ装置３０を介さない直接の通信は双方向で遮断するとする。

【０６５０】

ゲートウェイ装置３０内のゲートウェイアプリケーション３００１Ａは、ユーザからのゲートウェイ装置２０内のゲートウェイアプリケーション２００１Ａへの接続要求を受け、ＳＳＬ３００２にゲートウェイ装置２０内のゲートウェイアプリケーション２００１Ａへの通信開始を指示する。

【０６５１】

ＳＳＬ３００２は、ゲートウェイアプリケーション３００１Ａからの通信開始指示を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為に、ＴＣＰ３００３にゲートウェイ装置２０内のゲートウェイアプリケーション２００１Ａへの通信開始を指示する。

【０６５２】

ＴＣＰ３００３は、ＳＳＬ３００２からの通信開始指示を受け、ＴＣＰ２００３との間でＴＣＰセッションを確立する為に、ＩＰルーティング３００４に対して、ＴＣＰ２００３とのセッション確立要求パケット（ＳＹＮ）を送信する。このパケットはＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにゲートウェイ装置２０宛、宛先ポート番号にＴＣＰ２００３が設定されている。このパケットはＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにセッション中継装置１０宛、宛先ポート番号にＴＣＰ１００３が設定されている。このＴＣＰセッション確立要求パケットとは、ＴＣＰセッションの確立時に、スリーウェイハンドシェーク（ｔｈｒｅｅ　ｗａｙ　ｈａｎｄｓｈａｋｅ）の為に送信される、ＳＹＮパケットのことである。本明細書においては、ＴＣＰセッション確立動作の説明を簡略化するため、スリーウェイハンドシェークで送受信されるパケットうち、ＳＹＮパケットをＴＣＰセッション確立要求パケットと呼び、ＳＹＮパケット＋ＡＣＫパケットを応答パケットと呼んでいる。また実際にはＡＣＫパケットも送信されるが、ＡＣＫパケットについてはＳＹＮパケットと同様に転送されるため、本動作の説明では説明を省略する。

【０６５３】

ＩＰルーティング３００４は、ＴＣＰ３００３から受信したパケットの宛先ＩＰアドレスと宛先ポート番号を参照し、パケットをＩＰスタック３００５に転送する。

【０６５４】

ＩＰスタック３００５は、ＩＰルーティング３００４より受信したパケットに、Ｆｉｒｅｗａｌｌ３３内のイントラネット３側のＭＡＣアドレスを宛先ＭＡＣアドレスとして付加し、更に送信元ＭＡＣアドレスに自ノードのＭＡＣアドレスを設定してフレームを生成し、ブリッジ３００８を経由してドライバ３００７に転送する。

【０６５５】

ドライバ３００７は、ＩＰスタック３００５からフレームを受信し、ＭＡＣ３０１１に転送する。

【０６５６】

ＭＡＣ３０１１はドライバ３００７からフレームを受信し、ＰＨＹ３０１２に転送する。

【０６５７】

ＰＨＹ３０１２は、ＭＡＣ３０１１からフレームを受信し、ポート３０１３に転送する。

【０６５８】

ポート３０１３は、ＰＨＹ３０１２からフレームを受信し、イーサネットケーブルを経由してＨＵＢ３２に転送する。

【０６５９】

ＨＵＢ３２は、フレームを受信すると、ＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＬＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３側のポートに出力する。

【０６６０】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からフレームを受信し、ゲートウェイ装置３０か

らゲートウェイ装置２０への通信の為、これを許可し、ＨＵＢ２２に転送する。
【０６６１】
ＨＵＢ２２は、Ｆｉｒｅｗａｌｌ３３からフレームを受信し、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０に転送する。
【０６６２】
ゲートウェイ装置２０は、ＨＵＢ２２内からフレームを受信し、ポート２０１３、ＰＨＹ２０１２、ＭＡＣ２０１１、ドライバ２００７、ブリッジ２００８の経路で転送し、ＩＰスタック２００５に転送する。
【０６６３】
ＩＰスタック２００５は、ブリッジ２００８からフレームを受信し、ＭＡＣヘッダを外してパケットにしてＩＰルーティング２００４に転送する。
【０６６４】
ＩＰルーティング２００４は、ＩＰスタック２００５より受信したパケットの宛先ポート番号を参照し、ＴＣＰ２００３側のポート番号が付加されていることから、ＴＣＰ２００３に転送する。
【０６６５】
ＴＣＰ２００３は、ＩＰルーティング２００４よりパケットを受信する。このパケットはＴＣＰセッション確立要求パケット（ＳＹＮ＋ＡＣＫ）であるので、ＴＣＰプロトコルに従い、セッション確立要求に対して応答パケット（ＳＹＮ＋ＡＣＫ）をＴＣＰ３００３宛てに送信する。すなわち、応答パケットの宛先ＩＰはゲートウェイ装置３０のＩＰアドレスが設定され、応答パケットの宛先ポートは、ＴＣＰ３００３のポート番号が設定される。
【０６６６】
応答パケットは、ＩＰルーティング２００４、ＩＰスタック２００５、ブリッジ２００８，ドライバ２００７，ＮＩＣ２０１，ＨＵＢ２２，Ｆｉｒｅｗａｌｌ３３、ＨＵＢ３２，ＮＩＣ３０１を経由して、ＣＰＵ３００に到達し、更に、ドライバ３００７、ブリッジ３００８，ＩＰスタック３００５、ＩＰルーティング３００４を経由し、ＴＣＰ３００３に到達する。
【０６６７】
ＴＣＰ３００３は、ＩＰルーティング３００４よりパケットを受信する。このパケットはＴＣＰセッションの確立要求に対する応答パケットであるので、ＳＳＬ３００２に対して、ＴＣＰ２００３とのＴＣＰセッション接続完了を通知する。
【０６６８】
ＳＳＬ３００２は、ＴＣＰ３００３からの接続完了通知を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為、ＳＳＬプロトコルに従い、セッション確立要求の為のパケット（ＳＳＬセッション確立要求パケット）を送信する。
【０６６９】
ＳＳＬセッション確立要求パケットは、ＴＣＰ３００３で受信されると、ＴＣＰ３００３とＴＣＰ２００３との間で設定されたＴＣＰセッションを通り、ＮＩＣ３０１、ＨＵＢ３２，Ｆｉｒｅｗａｌｌ３３、ＨＵＢ２２、ＮＩＣ２０１を経由して、ＴＣＰ２００３に到着する。
【０６７０】
ＴＣＰ２００３は、パケットをＳＳＬ２００２に転送する。
【０６７１】
ＳＳＬ２００２は、ＳＳＬセッション確立要求の内容を検証し、問題が無ければ、ゲートウェイアプリケーション２００１Ａに対して、ＳＳＬ３００２とのセッション確立を通知すると同時に、ＳＳＬプロトコルに従い、ＳＳＬ３００２に対してＳＳＬセッション確立応答パケットを送信する。
【０６７２】
ＳＳＬセッション確立応答パケットは、ＳＳＬセッション確立要求パケットとは逆の経

路、即ち、ＴＣＰ２００３とＴＣＰ３００３との間のＴＣＰセッションを経由して、ＳＳＬ３００２に到達する。

【０６７３】

ＳＳＬ３００２は、ＳＳＬセッション確立応答の内容をＳＳＬプロトコルに従い検証し、問題が無ければ、ゲートウェイアプリケーション３００１Ａに対して、ＳＳＬ３００２とＳＳＬ２００２との間のＳＳＬセッション確立を通知する。

【０６７４】

以上のようにして、ＳＳＬ２００２とＳＳＬ３００２との間で、ＳＳＬセッションが確立される。

【０６７５】

以上により、第４の実施の形態において、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合の動作が完了する。

【０６７６】

［アプリケーション２１０１からアプリケーション３１０１へのセッション構築動作］

図２１を用いて、第５の実施の形態において、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション３１０１との間の、セッション確立動作について説明を行う。

【０６７７】

この際、ブリッジ２００８，ブリッジ３００８，ＨＵＢ２２、ＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。

【０６７８】

又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。

【０６７９】

更に、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）が、上述の動作例により既に設定されているものとする。

【０６８０】

中間ドライバ２１０６及び中間ドライバ３１０６は、自ノード内の全てのアプリケーションのＴＣＰを終端するよう、予め、設定されているものとする。

【０６８１】

端末２１内のアプリケーション２１０１は、ユーザからのサーバ３１内のアプリケーション３１０１への接続要求を受け、ＴＣＰ２１０２にサーバ３１内のアプリケーション３１０１への通信開始を指示する。

【０６８２】

ＴＣＰ２１０２は、アプリケーション２１０１からの通信開始指示を受け、ＴＣＰ３１０２との間でＴＣＰセッションを確立する為に、ＩＰルーティング２１０３に対して、ＴＣＰ３１０２とのセッション確立に必要なパケットを送信する。このパケットはＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにサーバ３１宛、宛先ポート番号にＴＣＰ３１０２が設定されている。このＴＣＰセッション確立要求パケットとは、ＴＣＰセッションの確立時に、スリーウェイハンドシェーク（ｔｈｒｅｅ　ｗａｙ　ｈａｎｄｓｈａｋｅ）の為に送信される、ＳＹＮパケットのことである。本明細書においては、ＳＳＬセッション確立動作の説明を簡略化するため、スリーウェイハンドシェークで送受信されるパケットうち、ＳＹＮパケットをＴＣＰセッション確立要求パケットと呼び、ＳＹＮパケット＋ＡＣＫパケットを応答パケットと呼んでいる。また実際にはＡＣＫパケットも送信されるが、ＡＣＫパケットについてはＳＹＮパケットと同様に転送されるため、説明を省略する。

【０６８３】
ＩＰルーティング２１０４は、ＴＣＰ２１０２から受信したパケットの宛先ＩＰアドレスと宛先ポート番号を参照し、パケットをＩＰスタック２１０４に転送する。
【０６８４】
ＩＰスタック２１０４は、ＩＰルーティング２１０３より受信したパケットに、サーバ３１のＭＡＣアドレスを宛先ＭＡＣアドレスとして付加し、更に送信元ＭＡＣアドレスに端末２１のＭＡＣアドレスを設定し、中間ドライバ２１０６に転送する。
【０６８５】
中間ドライバ２１０６は、ＩＰスタック２１０４からパケットを受信し、フレーム解析を行う。解析の結果、パケットは、ＴＣＰパケットであるので、ＭＡＣヘッダを取り外し、中間ドライバ２１０６のＴＣＰ部でＴＣＰ３１０２への接続要求を終端させる。すなわち、ＴＣＰ２１０２は、もともとはＴＣＰ３１０２に対して接続要求を行ったが、実際は、この要求に対して中間ドライバ２１０６内のＴＣＰが受信して保留し、ＴＣＰ２１０２と中間ドライバ２１０６内のＴＣＰとの間で、ＴＣＰセッションの確立処理を行って終端させる。
【０６８６】
中間ドライバ２１０６は、終端処理を行う際、中間ドライバ３１０６に対して、ＴＣＰ３１０２との間でＴＣＰセッションを確立するよう要求する為、ドライバ２１０５に接続要求の為のパケットを送る。この接続要求パケットは、ＴＣＰの規格に沿ったパケットではなく、独自のパケットである。このパケットは、宛先ＩＰアドレスにサーバ３１が、宛先ポート番号にはＴＣＰ３１０２が設定されてフレームが生成される。
【０６８７】
ドライバ２１０５は、中間ドライバ２１０６から接続要求フレームを受信し、ＭＡＣ２１１１に転送する。
【０６８８】
ＭＡＣ２１１１は、ドライバ２１０５からフレームを受信し、ＰＨＹ２１１２に転送する。
【０６８９】
ＰＨＹ２１１２は、ＭＡＣ２１１１からフレームを受信し、ポート２１１３に転送する。
【０６９０】
ポート２１１３は、ＰＨＹ２１１２からフレームを受信し、イーサネットケーブルを経由してＨＵＢ２２に転送する。
【０６９１】
ＨＵＢ２２は、端末２１のＮＩＣ２１１側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０側のポートに出力する。
【０６９２】
ゲートウェイ装置２０は、ＨＵＢ２２からのフレームをポート２０１３において受け取り、ＰＨＹ２０１２、ＭＡＣ２０１１、ドライバ２００７を経由して、ブリッジ２００８に渡す。
【０６９３】
ブリッジ２００８は、ドライバ２００７から受信したフレーム（フレームフォーマットＦ２０形式）内のヘッダＦ２１内に存在するＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のＭＡＣアドレスであり、ゲートウェイ装置２０のＭＡＣアドレスではないことから、フレームをドライバ２００９に転送する。
【０６９４】
ブリッジ２００８から送信されたフレームは、ドライバ２００９、仮想ＮＩＣ２０１０を経由し、ゲートウェイアプリケーション２００１Ａに転送される。

【０６９５】
ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したフレームを、ゲートウェイアプリケーション２００１Ａとゲートウェイアプリケーション３００１Ａの間に設定したＳＳＬセッションに流す。すなわち、ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したＥｔｈｅｒｎｅｔフレーム（フレームフォーマットＦ２０）をデータとしてＳＳＬ２００２に渡す。
【０６９６】
ＳＳＬ２００２は、ゲートウェイアプリケーション２００１Ａからデータ（Ｆ２１～Ｆ２４）を受け取ると、これを暗号化してデータＦ１４を生成し、ＴＣＰ２００３に渡す。
【０６９７】
ＴＣＰ２００３は、ＳＳＬ２００２よりデータＦ１４を受け取り、ＴＣＰヘッダＦ１３、およびＩＰヘッダＦ１２をつけて、ＩＰルーティング２００４に渡す。
【０６９８】
ここで、Ｆ１２内のＩＰ　ＤＡには、ゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡには、ゲートウェイ装置２０のＩＰアドレスが設定される。又、宛先ポートにはＴＣＰ３００３のポートが設定され、送信元ポートにはＴＣＰ２００３のポートが指定される。
【０６９９】
ＩＰルーティング２００４は、ＴＣＰ２００３より受信したデータのＩＰヘッダＦ１２内のＩＰアドレス等を参照し、フレームをＩＰスタック２００５に渡す。
【０７００】
ＩＰスタック２００５は、ＩＰルーティング２００４よりフレームを受信し、フレームにＭＡＣヘッダＦ１１をつけて、Ｅｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームフォーマットＦ１０の形式にして、ブリッジ２００８に渡す。
【０７０１】
ここで、Ｆ１１内のＭＡＣ　ＤＡには、ＡＲＰの結果よりＦｉｒｅｗａｌｌ　３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡには、ゲートウェイ装置２０のＭＡＣアドレスが設定される。
【０７０２】
ＩＰスタック２００５より送信されたフレームは、ブリッジ２００８、ドライバ２００７，ＮＩＣ２０１を経由して、ＨＵＢ２２に送られる。
【０７０３】
ＨＵＢ２２は、ゲートウェイ装置２２側のポートからフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＷＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３に出力する。
【０７０４】
Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からのフレームを受信し、ＩＰ　ＤＡを参照してＭＡＣヘッダＦ１１を変更し、受信フレームをフレームフォーマットＦ１０の形のまま、ＨＵＢ３２に転送する。
【０７０５】
ここで、Ｆ１１内のＭＡＣ　ＤＡにはゲートウェイ装置３０のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＬＡＮ側のＭＡＣアドレスが設定される。
【０７０６】
ＨＵＢ３２は、Ｆｉｒｅｗａｌｌ３３からのフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがゲートウェイ装置３０のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置３０側のポートに出力する。
【０７０７】

ゲートウェイ装置３０は、ＨＵＢ３２からのフレームをポート３０１３より受信すると、ＰＨＹ３０１２、ＭＡＣ３０１１、ドライバ３００７、ブリッジ３００８を経由して、ＩＰスタック３００５に転送する。

【０７０８】

ＩＰスタック３００５は、ブリッジ３００８から受信したフレームのＭＡＣヘッダＦ１１を取り外して、ＩＰルーティング３００４に送る。

【０７０９】

ＩＰルーティング３００４は、受信したフレームのヘッダＦ１２内のＩＰ　ＤＡと、Ｆ１３内の宛先ポート番号を参照し、フレームをＴＣＰ３００３に転送する。

【０７１０】

ＴＣＰ３００３は、ＩＰルーティング３００４からフレームを受信すると、ＴＣＰプロトコルに従ってＴＣＰ２００３に対してＡＣＫパケットを返送するなどの処理を行う。そして、受信したフレームから、ＴＣＰヘッダＦ１３とＩＰヘッダＦ１２を取り外し、データＦ１４をＳＳＬ３００２に転送する。

【０７１１】

ＳＳＬ３００２は、ＴＣＰ３００３からデータＦ１４を受信すると、復号化処理により暗号化を解除し、データＦ１４からＥｔｈｅｒｎｅｔフレームＦ２０、即ち、Ｆ２１～Ｆ２４を取り出し、ゲートウェイアプリケーション３００１Ａに転送する。

【０７１２】

ゲートウェイアプリケーション３００１Ａは、ＳＳＬ３００２からフレームＦ２０を受信すると、このフレームを、そのまま、仮想ＮＩＣ３０１０に流す。このフレームは、端末２１からＨＵＢ２２に送信された時の状態そのままに保たれており、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスが設定されている。又、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定されている。

【０７１３】

ゲートウェイアプリケーション３００１Ａより仮想ＮＩＣ３０１０に渡されたフレームは、ドライバ３００９、ブリッジ３００８、ＮＩＣ３０１を経由して、ＨＵＢ３２に転送される。

【０７１４】

ＨＵＢ３２は、ゲートウェイ装置３０側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、サーバ３１側のポートに出力する。

【０７１５】

サーバ３１は、ＨＵＢ３２内からパケットを受信し、ポート３１１３、ＰＨＹ３１１２、ＭＡＣ３１１１、ドライバ３１０５の経路でパケットを転送し、中間ドライバ３１０６に転送する。

【０７１６】

中間ドライバ３１０６は、ドライバ３１０５からパケットを受信し、フレーム解析を行う。解析の結果、パケットは、自ノード内のアプリケーションに向けたＴＣＰパケットであるので、このパケットを受信する。パケットは、中間ドライバ２１０６から中間ドライバ３１０６に向けて送信されたＴＣＰ３１０２への接続要求パケットである為、中間ドライバ３１０６内のＴＣＰは、ＴＣＰ３１０２との間でＴＣＰセッションを確立する為に、ＩＰスタック３１０４に対して、ＴＣＰ３１０２とのセッション確立に必要なパケットを送信する。このパケットは、ＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにサーバ３１宛、宛先ポート番号にＴＣＰ３１０２が設定され、更に送信元ＩＰアドレスには端末２１のＩＰアドレスが設定され、送信元ポート番号にはＴＣＰ２１０２のポート番号が設定される。

【０７１７】
すなわち、中間ドライバ３１０６内のＴＣＰは、ＴＣＰ２１０２の名前を騙ってＴＣＰ３１０２に対してセッション確立要求を行う。従って、ＴＣＰ３１０２は、恰も、ＴＣＰ２１０２と通信しているかのように認識し、更にＴＣＰ２１０２は、恰も、ＴＣＰ３１０２と通信しているかのように認識する。しかしながら、実際のＴＣＰ処理は、ＴＣＰ２１０２と中間ドライバ２１０６内のＴＣＰとの間、及び中間ドライバ３１０６とＴＣＰ３１０２との間で行われ、更に中間ドライバ２１０６と中間ドライバ３１０６との間は、ＵＤＰ等の輻輳制御の無い方法で、別途に通信が行われる。そして、ＴＣＰ２１０２と中間ドライバ２１０６間のＴＣＰセッションと、中間ドライバ２１０６と中間ドライバ３１０６の間のＵＤＰ等何らかの通信セッション、更に中間ドライバ３１０６とＴＣＰ３１０２の間のＴＣＰセッションが、中間ドライバ２１０６及び中間ドライバ３１０６によって相互に接続・中継されることにより、恰も、ＴＣＰ３００３とＴＣＰ２００３との間でＴＣＰセッションが確立しているかのように通信が行われる。

【０７１８】
ＩＰスタック３１０４は、中間ドライバ３１０６からパケットを受信し、ＭＡＣヘッダを外してＩＰルーティング３１０３に転送する。

【０７１９】
ＩＰルーティング３１０３は、ＩＰスタック３１０４より受信したパケットの宛先ポート番号を参照し、ＴＣＰ３１０２側のポート番号が付加されていることから、このパケットをＴＣＰ３１０２に転送する。

【０７２０】
ＴＣＰ３１０２は、ＩＰルーティング３１０３よりパケットを受信する。このパケットは、ＴＣＰセッション確立要求パケットであるので、ＴＣＰプロトコルに従い、ＴＣＰセッション確立要求に対して応答パケットを返送する。この際、ＴＣＰ３１０２は、ＴＣＰセッション確立要求は、ＴＣＰ２１０２から届いたものであると認識する。これは、実際の確立要求は中間ドライバ３１０６内のＴＣＰから送信されたものであるが、中間ドライバ３１０６内のＴＣＰは、ＴＣＰ２１０２を騙ってＴＣＰ３１０２にセッション確立要求を行った為、ＴＣＰ３１０２は、恰も、ＴＣＰ２１０２とセッションを確立すると認識する。

【０７２１】
従って、ＴＣＰ３１０２は、応答パケットを、ＴＣＰ２１０２宛てに送信する。すなわち、応答パケットの宛先ＩＰは端末２１のＩＰアドレスが設定され、応答パケットの宛先ポートは、ＴＣＰ２１０２のポート番号が設定される。

【０７２２】
応答パケットは、ＩＰルーティング３１０３、ＩＰスタック３１０４を経由して、中間ドライバ３１０６に届く。

【０７２３】
中間ドライバ３１０６は、応答パケットを受信すると、中間ドライバ３１０６内のＴＣＰで受信してこの応答パケットに対してＡＣＫパケットを送信してＴＣＰ処理を終端させる。そして、中間ドライバ２１０６に対して、接続完了通知の為のパケットを送信する。この接続完了通知パケットはＴＣＰの規格に沿ったパケットではなく、独自のパケットである。このパケットは、宛先ＩＰアドレスに端末２１が、宛先ポート番号にＴＣＰ２１０２が、送信元ＩＰアドレスにサーバ３１が、送信元ポート番号にＴＣＰ３１０２が設定されてフレームが生成される。

【０７２４】
接続完了通知フレームは、接続要求フレームとは逆の経路、即ち、ドライバ３１０５，ＮＩＣ３１１，ＨＵＢ３２，ＮＩＣ３０１、ＣＰＵ３００，ＮＩＣ３０１、Ｆｉｒｅｗａｌｌ３３、ＨＵＢ３２，ＮＩＣ２０１、ＣＰＵ２００、ＮＩＣ２０１、ＨＵＢ２２、ＮＩＣ２１１を経由して、ＣＰＵ２１０内の中間ドライバ２１０６に届く。

【０７２５】

中間ドライバ２１０６は、接続完了通知フレームを受信し、フレーム解析を行う。解析の結果、受信したフレームは、自ノード内のアプリケーション宛のパケットであるので受信する。受信したパケットは、中間ドライバ３１０６から中間ドライバ２１０６に向けて送信されたＴＣＰ３１０２と中間ドライバ３１０６との間の接続完了通知である為、中間ドライバ２１０６内のＴＣＰは、ＴＣＰプロトコルに従い、セッション確立要求に対する応答パケットをＴＣＰ２１０３に送る為、ＩＰスタック２１０４に対して、ＴＣＰプロトコルに従って応答パケットを生成して送信する。

【０７２６】

応答パケットは、ＩＰスタック２１０４、ＩＰルーティング２１０３を経由し、ＴＣＰ２１０２に到達する。

【０７２７】

ＴＣＰ２１０２は、ＩＰルーティング２１０３よりパケットを受信する。このパケットはＴＣＰセッションの確立要求に対する応答パケットであるので、アプリケーション２１０１に対して、ＴＣＰ３１０２とのＴＣＰセッション接続完了を通知する。この際、ＴＣＰ２１０２は、応答パケットが、ＴＣＰ３１０２から届いたものであると認識する。これは、実際の応答は中間ドライバ２１０６内のＴＣＰから送信されたものであるが、中間ドライバ２１０６内のＴＣＰは、ＴＣＰ３１０２を騙ってＴＣＰ２１０２にセッション確立応答を行った為、ＴＣＰ２１０２は、恰も、ＴＣＰ３１０２から応答があったと認識する。

【０７２８】

ＴＣＰ２１０２は応答パケットを受信すると、この応答パケットに対してＡＣＫパケットを生成してＴＣＰ３１０２宛に設定する。このＡＣＫパケットは、中間ドライバ２１０６のＴＣＰがＩＰルーティング２１０３及びＩＰスタック２１０４を介して受信し、ＴＣＰ処理を終端させる。

【０７２９】

以上のようにして、第５の実施の形態において、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション３１０１との間の、セッション確立動作が完了する。

【０７３０】

［端末２１からサーバ３１へのフレーム転送動作］

図２１を用いて、第５の実施の形態において、端末２１からサーバ３１へフレームを送信する場合を例に挙げて、動作の説明を行う。

【０７３１】

この際、ブリッジ２００８，ブリッジ３００８，ＨＵＢ２２、ＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。

【０７３２】

又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。

【０７３３】

更に、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）が、上述の動作例により既に設定されているものとする。

【０７３４】

又、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション（アプリケーション３１０１）との間で、既に、ＴＣＰセッションが構築されているとする。

【０７３５】

端末２１内のアプリケーション２１０１が、サーバ３１内のアプリケーション３１０１宛のデータを、ＴＣＰ２１０２に渡す。

【０７３６】

ＴＣＰ２１０２は、アプリケーション２１０１からデータを受け取り、ＴＣＰプロトコルに従ってＴＣＰヘッダ（図２におけるＦ２３）やＩＰヘッダ（図２におけるＦ２２）を付けてＩＰパケットとし、ＩＰルーティング２１０３に渡す。この時、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定される。

【０７３７】

ＩＰルーティング２１０３は、ＴＣＰ２１０２から受信したパケットの宛先ＩＰアドレス（サーバ３１宛て）および宛先ポート（ＴＣＰ３１０２宛て）を参照し、データを、そのまま、ＩＰスタック２１０４に転送する。

【０７３８】

ＩＰスタック２１０４は、ＩＰルーティング２１０３からパケットを受信し、ＭＡＣヘッダ（図２におけるＦ２１）をつけてＥｔｈｅｒｎｅｔフレームを作成し、中間ドライバ２１０６に渡す。このフレームはＥｔｈｅｒｎｅｔフレームＦ２０のフォーマットを有する。この時、ＩＰスタック２１０４は、ＡＲＰの結果を参照して、フレームのＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスを設定し、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスを設定する。

【０７３９】

中間ドライバ２１０６は、ＩＰスタック２１０４よりフレームを受信し、フレーム解析２１０６Ｈにおいてフレーム解析を行う。解析の結果、フレームが、先にセッション確立を行ったＴＣＰ２１０２とＴＣＰ３１０２の間のセッションのフレームであることから、カプセル化解除２１０６Ｆにおいて、このフレームのＭＡＣヘッダＦ２１を削除して保存し、ＴＣＰ２１０６Ａに渡す。

【０７４０】

中間ドライバ２１０６内のＴＣＰ２１０６Ａは、ＴＣＰ２１０３Ａを終端する。すなわち、フレームのＩＰヘッダＦ２２とＭＡＣヘッダＦ２３を削除してＦ２４のみを残し、データＦ２４をフラグメント分割２１０６Ｂに送る。更に、ＴＣＰ２１０２に対してＡＣＫフレームを送信する。

【０７４１】

中間ドライバ２１０６内のフラグメント分割２１０６Ｂは、ＴＣＰ２１０６Ａから受信したデータＦ２４のサイズを確認し、フラグメントの必要が無いことから、そのまま、データを再カプセル化２１０６Ｄに送る。

【０７４２】

中間ドライバ２１０６内の再カプセル化２１０６Ｄは、フラグメント分割２１０６Ｂより受信したデータＦ２４に、ＭＡＣヘッダＦ２１、ＩＰヘッダＦ２２、ＭＡＣヘッダＦ２３を付け、フレームフォーマットＦ２０の形式にして、ドライバ２１０５に送信する。この際、Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、Ｆ２１内のＭＡＣ　ＳＡには、端末２１のＭＡＣアドレスが設定される。又、Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定される。又、宛先ポートにはＴＣＰ３１０２のポートが設定され、送信元ポートにはＴＣＰ２１０２のポートが指定される。これらヘッダは、カプセル化解除２１０６Ｆによって保存されたものである。

【０７４３】

ドライバ２１０５は、中間ドライバ２１０６より上記フレームを受け取り、ＮＩＣ２１１に転送する。

【０７４４】

ＮＩＣ２１１は、ドライバ２１０５よりフレームを受け取り、ＭＡＣ２１１１，ＰＨＹ２１１２，ポート２１１３を経由して、ＨＵＢ２２にフレームを転送する。

【０７４５】

ＨＵＢ２２は、端末２１のＮＩＣ２１１側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のル

ーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０側のポートに出力する。

【０７４６】

ゲートウェイ装置２０は、ＨＵＢ２２からのフレームをポート２０１３において受け取り、ＰＨＹ２０１２、ＭＡＣ２０１１、ドライバ２００７を経由して、ブリッジ２００８に渡す。

【０７４７】

ブリッジ２００８は、ドライバ２００７から受信したフレーム（フレームフォーマットＦ２０形式）内のヘッダＦ２１内に存在するＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のＭＡＣアドレスであり、ゲートウェイ装置２０のＭＡＣアドレスでは無いことから、フレームをドライバ２００９に転送する。

【０７４８】

ブリッジ２００８から送信されたフレームは、ドライバ２００９、仮想ＮＩＣ２０１０を経由し、ゲートウェイアプリケーション２００１Ａに転送される。

【０７４９】

ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したフレームを、ゲートウェイアプリケーション２００１Ａとゲートウェイアプリケーション３００１Ａの間に設定したＳＳＬセッションに流す。すなわち、ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したＥｔｈｅｒｎｅｔフレーム（フレームフォーマットＦ２０）をデータとしてＳＳＬ２００２に渡す。

【０７５０】

ＳＳＬ２００２は、ゲートウェイアプリケーション２００１Ａからデータ（Ｆ２１～Ｆ２４）を受け取ると、これを暗号化してデータＦ１４を生成し、ＴＣＰ２００３に渡す。

【０７５１】

ＴＣＰ２００３は、ＳＳＬ２００２よりデータＦ１４を受け取り、ＴＣＰヘッダＦ１３、及びＩＰヘッダＦ１２を付けて、ＩＰルーティング２００４に渡す。ここで、Ｆ１２内のＩＰ　ＤＡには、ゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡには、ゲートウェイ装置２０のＩＰアドレスが設定される。又、宛先ポートにはＴＣＰ３００３のポートが設定され、送信元ポートにはＴＣＰ２００３のポートが指定される。

【０７５２】

ＩＰルーティング２００４は、ＴＣＰ２００３より受信したデータのＩＰヘッダＦ１２内のＩＰアドレス等を参照し、フレームをＩＰスタック２００５に渡す。

【０７５３】

ＩＰスタック２００５は、ＩＰルーティング２００４よりフレームを受信し、フレームにＭＡＣヘッダＦ１１をつけて、Ｅｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームフォーマットＦ１０の形式にして、ブリッジ２００８に渡す。ここで、Ｆ１１内のＭＡＣ　ＤＡには、ＡＲＰの結果よりＦｉｒｅｗａｌｌ　３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡには、ゲートウェイ装置２０のＭＡＣアドレスが設定される。

【０７５４】

ＩＰスタック２００５より送信されたフレームは、ブリッジ２００８、ドライバ２００７，ＮＩＣ２０１を経由して、ＨＵＢ２２に送られる。

【０７５５】

ＨＵＢ２２は、ゲートウェイ装置２２側のポートからフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＷＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３に出力する。

【０７５６】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からのフレームを受信し、ＩＰ　ＤＡを参照してＭＡＣヘッダＦ１１を変更し、受信フレームをフレームフォーマットＦ１０の形のまま、

ＨＵＢ３２に転送する。
【０７５７】
ここで、Ｆ１１内のＭＡＣ　ＤＡにはゲートウェイ装置３０のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＬＡＮ側のＭＡＣアドレスが設定される。
【０７５８】
ＨＵＢ３２は、Ｆｉｒｅｗａｌｌ３３からのフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがゲートウェイ装置３０のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置３０側のポートに出力する。
【０７５９】
ゲートウェイ装置３０は、ＨＵＢ３２からのフレームをポート３０１３より受信すると、ＰＨＹ３０１２、ＭＡＣ３０１１、ドライバ３００７、ブリッジ３００８を経由して、ＩＰスタック３００５に転送する。
【０７６０】
ＩＰスタック３００５は、ブリッジ３００８から受信したフレームのＭＡＣヘッダＦ１１を取り外して、ＩＰルーティング３００４に送る。
【０７６１】
ＩＰルーティング３００４は、受信したフレームのヘッダＦ１２内のＩＰ　ＤＡと、Ｆ１３内の宛先ポート番号を参照し、フレームをＴＣＰ３００３に転送する。
【０７６２】
ＴＣＰ３００３は、ＩＰルーティング３００４からフレームを受信すると、ＴＣＰプロトコルに従ってＡＣＫパケットを返送するなどの処理を行う。そして、受信したフレームから、ＴＣＰヘッダＦ１３とＩＰヘッダＦ１２を取り外し、データＦ１４をＳＳＬ３００２に転送する。
【０７６３】
ＳＳＬ３００２は、ＴＣＰ３００３からデータＦ１４を受信すると、復号化処理により暗号化を解除し、データＦ１４からＥｔｈｅｒｎｅｔフレームＦ２０、即ち、Ｆ２１～Ｆ２４を取り出し、ゲートウェイアプリケーション３００１Ａに転送する。
【０７６４】
ゲートウェイアプリケーション３００１Ａは、ＳＳＬ３００２からフレームＦ２０を受信すると、このフレームを、そのまま、仮想ＮＩＣ３０１０に流す。このフレームは、端末２１からＨＵＢ２２に送信された時の状態そのままに保たれており、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスが設定されている。又、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定されている。
【０７６５】
ゲートウェイアプリケーション３００１Ａより仮想ＮＩＣ３０１０に渡されたフレームは、ドライバ３００９、ブリッジ３００８、ＮＩＣ３０１を経由して、ＨＵＢ３２に転送される。
【０７６６】
ＨＵＢ３２は、ゲートウェイ装置３０側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、サーバ３１側のポートに出力する。
【０７６７】
ＨＵＢ３２から送信されたフレームは、サーバ３１内のＮＩＣ３１１、ドライバ３１０５を経由して中間ドライバ３１０６に転送される。
【０７６８】

中間ドライバ３１０６は、ドライバ３１０５よりフレームを受信する。このフレームは、受信時には、フレームフォーマットＦ２０の形をしているが、カプセル化解除３１０６Ｇにおいて、ヘッダＦ２１、ヘッダＦ２２、ヘッダＦ２３を削除し、データＦ２４のみを残す。そして、データＦ２４をＴＣＰ３１０６Ａに渡し、予め、ＴＣＰ３１０２と中間ドライバ内のＴＣＰ３１０６Ａとの間で設定されたＴＣＰセッションに流す。

【０７６９】

中間ドライバ３１０６内のＴＣＰ３１０６Ａは、受信したデータＦ２４に、ＴＣＰ３１０２とのＴＣＰ通信に必要なＴＣＰヘッダＦ２３と、ＩＰヘッダＦ２２を付けて、再カプセル化３１０６Ｅに送る。Ｆ２２内のＩＰ　ＤＡにはサーバ３１のＩＰアドレスが設定され、Ｆ２２内のＩＰ　ＳＡには端末２１のＩＰアドレスが設定される。

【０７７０】

中間ドライバ３１０６内の再カプセル化３１０６Ｅは、ＴＣＰ３１０６Ａよりデータを受信すると、これにヘッダＦ２１を付けて、ＩＰスタック３１０４に送る。ここで、Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスを設定し、Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスを設定する。このようにして、ＴＣＰ３１０６Ａからの受信フレームをフレームフォーマットＦ２０の形にして、ＩＰスタック３１０４に転送する。

【０７７１】

中間ドライバ３１０６を出たフレームは、ＩＰスタック３１０４、ＩＰルーティング３１０３、ＴＣＰ３１０２を経由して、フレーム内のデータＦ２４をアプリケーション３１０１に渡される。

【０７７２】

以上のようにして、端末２１内のアプリケーション２１０１からサーバ３１内のアプリケーション３１０１への一連のフレーム転送が完了する。

【０７７３】

上記の例とは逆の経路を辿ることで、サーバ３１内のアプリケーション３１０１から端末２１内のアプリケーション２１０１への一連のフレーム転送も、同様に実現可能である。

【０７７４】

尚、本実施の形態では、ＴＣＰセッションはＴＣＰ２１０２と中間ドライバ２１０６の間、及びＴＣＰ２００３とＴＣＰ３００３の間、及び中間ドライバ３１０６とＴＣＰ３１０２の間において設定される。従って、中間ドライバ２１０６からＴＣＰ２００３の間、及びＴＣＰ３００３から中間ドライバ３１０６の間の転送には、ＴＣＰの輻輳制御および再送制御が機能しなくなる。

【０７７５】

しかしながら、一般的に、イントラネット内でパケットの損失が発生したり、輻輳が発生したりすることは稀であり、Ｆｉｒｅｗａｌｌを跨ぐ接続、即ち、ＷＡＮを介す接続の場合に、損失や輻輳への対応が必要となる。本実施の形態では、ゲートウェイ装置２０とゲートウェイ装置３０の間は、ＴＣＰが機能している為、この区間における再送制御や輻輳制御があれば、アプリケーション２１０１とアプリケーション３１０１の間の通信における影響は殆ど発生しない。

【０７７６】

尚、本実施の形態では、サーバ３１と端末２１の設置場所を入れ替えることも出来る。

【０７７７】

［発明の効果］

次に、本実施の形態の効果について説明する。

【０７７８】

本実施の形態に挙げた発明を利用すると、端末２１とサーバ３１との間で、フレームの高速転送が可能になる。

【０７７９】

これは、端末２１とサーバ３１との間の通信において、ヘッダＦ２３の位置のＴＣＰによる輻輳制御と再送制御が発生しないよう、端末２１内の中間ドライバと、サーバ３１内の中間ドライバにおいて、端末２１内のＴＣＰと、サーバ３１内のＴＣＰを終端し、ＴＣＰ　ｏｖｅｒ　ＴＣＰ問題の発生を回避しているからである。

【０７８０】

［第６の実施の形態］

本発明の第６の実施の形態は、第５の実施の形態に対して、ゲートウェイ装置３０内のブリッジ３００８と、ドライバ３００９と、仮想ＮＩＣ３０１０と、サーバ３１内の中間ドライバ３１０６が無くなり、代わりにゲートウェイ装置３０内に、カプセル化処理３００１Ｂと、ＴＣＰ３００３Ｂが、各々、設置されている点において異なる。

【０７８１】

第６の実施の形態におけるＨＵＢ２２，ＨＵＢ３２、端末２１，ゲートウェイ装置２０，イントラネット２、イントラネット３の構成および動作は、第５の実施の形態と同じである。

【０７８２】

第６の実施の形態においては、イントラネット２は、閉域ＬＡＮだけで無く、インターネット等のオープンなＷＡＮを用いても構わない。

【０７８３】

［構成の説明］

図２２は、第６の実施の形態における各機器の構成とフレームの転送経路を詳細に示したブロック図である。

【０７８４】

ゲートウェイ装置３０は、第５の実施の形態におけるゲートウェイ装置３０に対して、ブリッジ３００８と、ドライバ３００９と、仮想ＮＩＣ３０１０が無くなり、代わりに、カプセル化処理３００１Ｂと、ＴＣＰ３００３Ｂが、各々、設置されている点において異なる。

【０７８５】

カプセル化処理３００１Ｂは、ゲートウェイアプリケーション３００１ＡからフォーマットＦ２０のフレームを受信し、ヘッダＦ２１、ヘッダＦ２２、ヘッダＦ２３を、各々、削除して、データＦ２４のみをＴＣＰ３００３Ｂに渡す。又、ＴＣＰ３００３ＢからデータＦ２４を受信し、ヘッダＦ２１、ヘッダＦ２２、ヘッダＦ２３を、各々、付加して、ゲートウェイアプリケーション３００１Ａに渡す。又、接続要求を受信すると、ＴＣＰ３００３Ｂに対して、ＴＣＰセッション確立要求する。更に、ＴＣＰ３００３ＢからのＴＣＰセッション確立応答を受信し、接続完了通知フレームを作成して、ゲートウェイアプリケーション３００１Ａに渡す。

【０７８６】

ＴＣＰ３００３Ｂは、ＴＣＰ２００３やＴＣＰ３００３と同様の構成を有し、同様の動作を行う。

【０７８７】

サーバ３１は、第５の実施の形態におけるサーバ３１に対して、中間ドライバ３１０６が設置されている点において異なる。すなわち、第１～第４の実施の形態におけるサーバ３１と同様の構成を有し、同様の動作を行う。

【０７８８】

ＨＵＢ２２，ＨＵＢ３２、端末２１，ゲートウェイ装置２０，イントラネット２、イントラネット３の構成および動作は、第５の実施の形態と同じである。

【０７８９】

Ｆｉｒｅｗａｌｌ３３は、第５の実施の形態のＦｉｒｅｗａｌｌ３３と同様の構成を有し、同様の動作を行う。但し、本実施の形態においては、Ｆｉｒｅｗａｌｌ３３の代わりに、ＮＡＴルータやＰｒｏｘｙサーバを用いても良い。

【０７９０】

第６の実施の形態でも、他の実施の形態と同様に、ゲートウェイ装置２０とゲートウェイ装置３０との間で、予め、ＳＳＬセッションを設定している場合のみ、イントラネット２内の機器からイントラネット３内の機器へのアクセスが可能になる。

【０７９１】

［動作の説明］

［ＳＳＬセッションの確立動作］

第６の実施の形態におけるゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）の確立動作は、第５の実施の形態と同様である為、ここでは省略する。

【０７９２】

［アプリケーション２１０１からアプリケーション３１０１へのセッション構築動作］

図２２を用いて、第６の実施の形態において、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション３１０１との間の、セッション確立動作について説明を行う。

【０７９３】

この際、ブリッジ２００８，ＨＵＢ２２、ＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。

【０７９４】

又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。

【０７９５】

更に、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）が、上述の動作例により既に設定されているものとする。

【０７９６】

中間ドライバ２１０６は、自ノード内の全てのアプリケーションにおけるＴＣＰの処理を終端するよう予め設定されているものとする。

【０７９７】

端末２１内のアプリケーション２１０１は、ユーザからのサーバ３１内のアプリケーション３１０１への接続要求を受け、ＴＣＰ２１０２にサーバ３１内のアプリケーション３１０１への通信開始を指示する。

【０７９８】

ＴＣＰ２１０２は、アプリケーション２１０１からの通信開始指示を受け、ＴＣＰ３１０２との間でＴＣＰセッションを確立する為に、ＩＰルーティング２１０３に対して、ＴＣＰ３１０２とのＴＣＰセッション確立要求パケットを送信する。このパケットは、ＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにサーバ３１宛、宛先ポート番号にＴＣＰ３１０２が設定されている。セッション確立に必要なパケットとは、ＴＣＰセッションの確立時に、スリーウェイハンドシェーク（ｔｈｒｅｅ　ｗａｙ　ｈａｎｄｓｈａｋｅ）の為に送信される、ＳＹＮパケットパケットのことである。本明細書においては、ＴＣＰセッション確立動作の説明を簡略化するため、スリーウェイハンドシェークで送受信されるパケットうち、ＳＹＮパケットをＴＣＰセッション確立要求パケットと呼び、ＳＹＮ＋ＡＣＫパケットを応答パケットと呼んでいる。また実際にはＡＣＫパケットも送信されるが、ＡＣＫパケットについてはＳＹＮパケットと同様に転送されるため、本動作の説明では説明を省略する。

【０７９９】

ＩＰルーティング２１０４は、ＴＣＰ２１０２から受信したパケットの宛先ＩＰアドレスと宛先ポート番号を参照し、パケットをＩＰスタック２１０４に転送する。

【０８００】

ＩＰスタック２１０４は、ＩＰルーティング２１０３より受信したパケットに、サーバ

３１のＭＡＣアドレスを宛先ＭＡＣアドレスとして付加し、更に送信元ＭＡＣアドレスに端末２１のＭＡＣアドレスを設定してフレームを生成し、中間ドライバ２１０６に転送する。

【０８０１】

中間ドライバ２１０６は、ＩＰスタック２１０４からＴＣＰセッション確立要求フレームを受信し、フレーム解析を行う。解析の結果、受信したフレームは、ＴＣＰフレームであるので、カプセル化解除においてＭＡＣヘッダを取り外してパケットにする。そして、中間ドライブ２１０６のＴＣＰ部でＴＣＰ２１０２からＴＣＰ３１０２へのＴＣＰの処理を終端させる。すなわち、ＴＣＰ２１０２は、元々は、ＴＣＰ３１０２に対して接続要求を行ったが、実際は、この要求に対して中間ドライバ２１０６内のＴＣＰで受信して保留にし、ＴＣＰ２１０２と中間ドライバ２１０６内のＴＣＰとの間で、ＴＣＰセッションの確立処理を行って終端させる。

【０８０２】

中間ドライバ２１０６は、終端処理を行う際、カプセル化処理３００１Ｂに対して、ＴＣＰ３１０２との間でＴＣＰセッションを確立するよう要求する為、ドライバ２１０５に接続要求のためのパケットを送る。この接続要求パケットはＴＣＰの規格に沿ったパケットではなく、独自のパケットである。このパケットは、宛先ＩＰアドレスにサーバ３１が、宛先ポート番号にＴＣＰ３１０２が設定される。そしてこのパケットに宛先ＭＡＣアドレスを付加し、更に送信元ＭＡＣアドレスに自ノードのＭＡＣアドレスを設定して接続要求フレームが生成される。

【０８０３】

ドライバ２１０５は、中間ドライバ２１０６から接続要求のフレームを受信し、ＭＡＣ２１１１に転送する。

【０８０４】

ＭＡＣ２１１１は、ドライバ２１０５からフレームを受信し、ＰＨＹ２１１２に転送する。

【０８０５】

ＰＨＹ２１１２は、ＭＡＣ２１１１からフレームを受信し、ポート２１１３に転送する。

【０８０６】

ポート２１１３は、ＰＨＹ２１１２からフレームを受信し、イーサネットケーブルを経由してＨＵＢ２２に転送する。

【０８０７】

ＨＵＢ２２は、端末２１のＮＩＣ２１１側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０側のポートに出力する。

【０８０８】

ゲートウェイ装置２０は、ＨＵＢ２２からのフレームをポート２０１３において受け取り、ＰＨＹ２０１２、ＭＡＣ２０１１、ドライバ２００７を経由して、ブリッジ２００８に渡す。

【０８０９】

ブリッジ２００８は、ドライバ２００７から受信したフレーム（フレームフォーマットＦ２０形式）内のヘッダＦ２１内に存在するＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のＭＡＣアドレスであり、ゲートウェイ装置２０のＭＡＣアドレスではないことから、フレームをドライバ２００９に転送する。

【０８１０】

ブリッジ２００８から送信されたフレームは、ドライバ２００９、仮想ＮＩＣ２０１０を経由し、ゲートウェイアプリケーション２００１Ａに転送される。

【０８１１】

ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したフレームを、ゲートウェイアプリケーション２００１Ａとゲートウェイアプリケーション３００１Ａの間に設定したＳＳＬセッションに流す。すなわち、ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したＥｔｈｅｒｎｅｔフレーム（フレームフォーマットＦ２０）をデータとしてＳＳＬ２００２に渡す。

【０８１２】

ＳＳＬ２００２は、ゲートウェイアプリケーション２００１Ａからデータ（Ｆ２１～Ｆ２４）を受け取ると、これを暗号化してデータＦ１４を生成し、ＴＣＰ２００３に渡す。

【０８１３】

ＴＣＰ２００３は、ＳＳＬ２００２よりデータＦ１４を受け取り、ＴＣＰヘッダＦ１３、及びＩＰヘッダＦ１２を付けて、ＩＰルーティング２００４に渡す。ここで、Ｆ１２内のＩＰ　ＤＡには、ゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡには、ゲートウェイ装置２０のＩＰアドレスが設定される。又、宛先ポートにはＴＣＰ３００３のポートが設定され、送信元ポートにはＴＣＰ２００３のポートが指定される。

【０８１４】

ＩＰルーティング２００４は、ＴＣＰ２００３より受信したデータのＩＰヘッダＦ１２内のＩＰアドレス等を参照し、フレームをＩＰスタック２００５に渡す。

【０８１５】

ＩＰスタック２００５は、ＩＰルーティング２００４よりフレームを受信し、フレームにＭＡＣヘッダＦ１１を付けて、Ｅｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームフォーマットＦ１０の形式にして、ブリッジ２００８に渡す。

【０８１６】

ここで、Ｆ１１内のＭＡＣ　ＤＡには、ＡＲＰの結果よりＦｉｒｅｗａｌｌ　３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡには、ゲートウェイ装置２０のＭＡＣアドレスが設定される。

【０８１７】

ＩＰスタック２００５より送信されたフレームは、ブリッジ２００８、ドライバ２００７，ＮＩＣ２０１を経由して、ＨＵＢ２２に送られる。

【０８１８】

ＨＵＢ２２は、ゲートウェイ装置２２側のポートからフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＷＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３に出力する。

【０８１９】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からのフレームを受信し、ＩＰ　ＤＡを参照してＭＡＣヘッダＦ１１を変更し、受信フレームをフレームフォーマットＦ１０の形のまま、ＨＵＢ３２に転送する。

【０８２０】

ここで、Ｆ１１内のＭＡＣ　ＤＡにはゲートウェイ装置３０のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＬＡＮ側のＭＡＣアドレスが設定される。

【０８２１】

ＨＵＢ３２は、Ｆｉｒｅｗａｌｌ３３からのフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがゲートウェイ装置３０のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置３０側のポートに出力する。

【０８２２】

ゲートウェイ装置３０は、ＨＵＢ３２からのフレームをポート３０１３より受信すると、ＰＨＹ３０１２、ＭＡＣ３０１１、ドライバ３００７を経由して、ＩＰスタック３００

５に転送する。
【０８２３】
ＩＰスタック３００５は、ドライバ３００７から受信したフレームのＭＡＣヘッダＦ１１を取り外して、パケットにしてＩＰルーティング３００４に送る。
【０８２４】
ＩＰルーティング３００４は、ＩＰスタック３００５からのパケットのヘッダＦ１２内のＩＰ　ＤＡと、Ｆ１３内の宛先ポート番号を参照し、このパケットをＴＣＰ３００３に転送する。
【０８２５】
ＴＣＰ３００３は、ＩＰルーティング３００４からパケットを受信すると、ＴＣＰプロトコルに従ってＴＣＰ２００３に対してＡＣＫパケットを返送する等の処理を行う。そして、受信したパケットから、ＴＣＰヘッダＦ１３とＩＰヘッダＦ１２を取り外し、データＦ１４をＳＳＬ３００２に転送する。
【０８２６】
ＳＳＬ３００２は、ＴＣＰ３００３からデータＦ１４を受信すると、復号化処理により暗号化を解除し、データＦ１４からＥｔｈｅｒｎｅｔフレームＦ２０、即ち、Ｆ２１～Ｆ２４を取り出し、ゲートウェイアプリケーション３００１Ａに転送する。
【０８２７】
ゲートウェイアプリケーション３００１Ａは、ＳＳＬ３００２からフレームＦ２０を受信すると、このフレームを、そのまま、カプセル化処理３００１Ｂに流す。このフレームは、端末２１からＨＵＢ２２に送信された時の状態そのままに保たれており、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスが設定されている。又、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定されている。
【０８２８】
カプセル化処理３００１Ｂは、ゲートウェイアプリケーション３００１Ａよりフレームを受信し、フレーム解析を行う。解析の結果、このフレームは中間ドライバ２１０６から送信されたＴＣＰ３１０２への接続要求である為、ＴＣＰ３００３Ｂに対して、ＴＣＰ３１０２との間でＴＣＰセッションを確立するよう命令する。
【０８２９】
ＴＣＰ３００３Ｂは、ＴＣＰ３１０２との間でＴＣＰセッションを確立する為に、ＩＰルーティング３００４に対して、ＴＣＰ３１０２とのＴＣＰセッション確立要求パケットを送信する。このパケットは、ＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにサーバ３１宛、宛先ポート番号にＴＣＰ３１０２が設定され、更に送信元ＩＰアドレスにはゲートウェイ装置３０のＩＰアドレスが設定され、送信元ポート番号にはＴＣＰ３００３Ｂのポート番号が設定される。ＴＣＰ３００３Ｂのポート番号については、ＴＣＰ２１０２のポート番号と同一にする事も、異なるように設定する事も、どちらも可能である。尚、ＴＣＰセッション確立要求パケットとは、ＴＣＰセッションの確立時に、スリーウェイハンドシェーク（ｔｈｒｅｅ　ｗａｙ　ｈａｎｄｓｈａｋｅ）の為に送信される、ＳＹＮパケットパケットのことである。本明細書においては、ＳＳＬセッション確立動作の説明を簡略化するため、スリーウェイハンドシェークで送受信されるパケットうち、ＳＹＮパケットをＴＣＰセッション確立要求パケットと呼び、ＳＹＮ＋ＡＣＫパケットを応答パケットと呼んでいる。また実際にはＡＣＫパケットも送信されるが、ＡＣＫパケットについてはＳＹＮパケットと同様に転送されるため、本動作の説明では説明を省略する。
【０８３０】
ＩＰルーティング３００４に渡されたパケットは、ＩＰスタック３００５にて宛先ＭＡＣアドレスが付加され、更に送信元ＭＡＣアドレスに自ノードのＭＡＣアドレスを設定してフレームを作成し、ドライバ３００７、ＮＩＣ３０１を経由して、ＨＵＢ３２に転送される。

【０８３１】
ＨＵＢ３２は、ゲートウェイ装置３０側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、サーバ３１側のポートに出力する。
【０８３２】
サーバ３１は、ＨＵＢ３２内からフレームを受信し、ポート３１１３、ＰＨＹ３１１２、ＭＡＣ３１１１、ドライバ３１０５の経路でパケットを転送し、ＩＰスタック３１０４に転送する。
【０８３３】
ＩＰスタック３１０４は、ドライバ３１０５からフレームを受信してＭＡＣヘッダを外してパケットにし、ＩＰルーティング３１０３に転送する。
【０８３４】
ＩＰルーティング３１０３は、ＩＰスタック３１０４より受信したパケットの宛先ポート番号を参照し、ＴＣＰ３１０２側のポート番号が付加されていることから、このパケットをＴＣＰ３１０２に転送する。
【０８３５】
ＴＣＰ３１０２は、ＩＰルーティング３１０３よりパケットを受信する。このパケットは、ＴＣＰセッション確立要求パケット（ＳＹＮ）であるので、ＴＣＰプロトコルに従い、このＴＣＰセッション確立要求パケットに対して応答パケット（ＳＹＮ＋ＡＣＫ）を返送する。
【０８３６】
ＴＣＰ３１０２は、応答パケットを、ＴＣＰ３００３Ｂ宛てに送信する。すなわち、応答パケットの宛先ＩＰはゲートウェイ装置３０のＩＰアドレスが設定され、応答パケットの宛先ポートは、ＴＣＰ３００３Ｂのポート番号が設定される。
【０８３７】
応答パケットは、ＴＣＰセッション確立要求パケットとは逆の経路、即ち、ＩＰルーティング３１０３、ＩＰスタック３１０４、ドライバ３１０５，ＮＩＣ３１１，ＨＵＢ３２，ＮＩＣ３０１を経由して、ＴＣＰ３００３Ｂに届く。
【０８３８】
ＴＣＰ３００３Ｂは、応答パケットを受信すると応答パケットに対するＡＣＫパケットをＴＣＰ３１０２に送信し、応答パケットをカプセル化処理３００１Ｂに渡す。
【０８３９】
カプセル化処理３００１Ｂは、端末２１内の中間ドライバ２１０６に対して、接続完了通知の為のパケットを送信する。この接続完了通知パケットはＴＣＰの規格に沿ったパケットではなく、独自のパケットである。このパケットは、宛先ＩＰアドレスに端末２１が、宛先ポート番号にＴＣＰ２１０２が、送信元ＩＰアドレスにサーバ３１が、送信元ポート番号にはＴＣＰ３１０２が設定されてフレームが生成される。
【０８４０】
接続完了通知フレームは、接続要求フレームとは逆の経路、即ち、ゲートウェイアプリケーション３００１Ａ、ＳＳＬ３００２，ＴＣＰ３００３，ＩＰルーティング３００４，ＩＰスタック３００５、ドライバ３００７、ＮＩＣ３０１、ＨＵＢ３３，Ｆｉｒｅｗａｌｌ３３、ＨＵＢ３２，ＮＩＣ２０１、ＣＰＵ２００、ＮＩＣ２０１、ＨＵＢ２２、ＮＩＣ２１１を経由して、ＣＰＵ２１０内の中間ドライバ２１０６に届く。
【０８４１】
中間ドライバ２１０６は、接続完了通知フレームを受信し、フレーム解析を行う。解析の結果、自ノード内のアプリケーション宛であるので、このフレームを受信し、カプセル化解除においてＭＡＣヘッダを取り外してパケットにする。このパケットは、カプセル化処理３００１Ｂから中間ドライバ２１０６に向けて送信された、カプセル化処理３００１ＢとＴＣＰ３１０２との間の接続完了通知パケットである為、中間ドライバ２１０６内の

ＴＣＰは、ＴＣＰセッション確立要求に対する応答パケット（ＳＹＮ＋ＡＣＫ）をＴＣＰ２１０３に送る為にＴＣＰプロトコルに従って生成し、ＩＰスタック２１０４に対して、応答パケットを送信する。

【０８４２】

応答パケットは、ＩＰスタック２１０４、ＩＰルーティング２１０３を経由し、ＴＣＰ２１０２に到達する。

【０８４３】

ＴＣＰ２１０２は、ＩＰルーティング２１０３よりパケットを受信する。このパケットはＴＣＰセッションの確立要求に対する応答パケットであるので、アプリケーション２１０１に対して、ＴＣＰ３１０２とのＴＣＰセッション接続完了を通知する。この際、ＴＣＰ２１０２は、応答パケットが、ＴＣＰ３１０２から届いたものであると認識する。これは、実際の応答は中間ドライバ２１０６内のＴＣＰから送信されたものであるが、中間ドライバ２１０６内のＴＣＰは、ＴＣＰ３１０２をかたってＴＣＰ２１０２にセッション確立応答を行った為、ＴＣＰ２１０２は、恰も、ＴＣＰ３１０２から応答があったと認識する。

【０８４４】

ＴＣＰ２１０２は応答パケットを受信すると、この応答パケットに対してＡＣＫパケットを生成してＴＣＰ３１０２宛に送信する。このＡＣＫパケットは、中間ドライバ２１０６のＴＣＰが、ＩＰルーティング２１０３及びＩＰスタック２１０４を介して受信し、ＴＣＰ処理を終端させる。

【０８４５】

以上のようにして、第５の実施の形態において、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション３１０１との間の、セッション確立動作が完了する。

【０８４６】

［端末２１からサーバ３１へのフレーム転送動作］

図２２を用いて、第６の実施の形態において、端末２１からサーバ３１へフレームを送信する場合を例に挙げて、動作の説明を行う。

【０８４７】

この際、ブリッジ２００８，ＨＵＢ２２、ＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。

【０８４８】

又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。

【０８４９】

更に、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）が、上述の動作例により既に設定されているものとする。

【０８５０】

又、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション（アプリケーション３１０１）との間で、既に、ＴＣＰセッションが構築されているとする。

【０８５１】

端末２１内のアプリケーション２１０１が、サーバ３１内のアプリケーション３１０１宛のデータを、ＴＣＰ２１０２に渡す。

【０８５２】

ＴＣＰ２１０２は、アプリケーション２１０１からデータを受け取り、ＴＣＰプロトコルに従ってＴＣＰヘッダ（図２におけるＦ２３）やＩＰヘッダ（図２におけるＦ２２）を付けてＩＰパケットとし、ＩＰルーティング２１０３に渡す。この時、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２

内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定される。

【０８５３】

ＩＰルーティング２１０３は、ＴＣＰ２１０２から受信したパケットの宛先ＩＰアドレス（サーバ３１宛て）及び宛先ポート（ＴＣＰ３１０２宛て）を参照し、データを、そのまま、ＩＰスタック２１０４に転送する。

【０８５４】

ＩＰスタック２１０４は、ＩＰルーティング２１０３からパケットを受信し、ＭＡＣヘッダ（図２におけるＦ２１）を付けてＥｔｈｅｒｎｅｔフレームを作成し、中間ドライバ２１０６に渡す。このフレームは、ＥｔｈｅｒｎｅｔフレームＦ２０のフォーマットを有する。この時、ＩＰスタック２１０４は、ＡＲＰの結果を参照して、フレームのＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスを設定し、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスを設定する。

【０８５５】

中間ドライバ２１０６は、ＩＰスタック２１０４よりフレームを受信し、フレーム解析２１０６Ｈにおいてフレーム解析を行う。解析の結果、フレームが、先にセッション確立を行ったＴＣＰ２１０２とＴＣＰ３１０２の間のセッションのフレームであることから、カプセル化解除２１０６Ｆにおいて、このフレームのＭＡＣヘッダＦ２１を削除して保存し、ＴＣＰ２１０６Ａに渡す。

【０８５６】

中間ドライバ２１０６内のＴＣＰ２１０６Ａは、ＴＣＰ２１０３Ａを終端する。すなわち、フレームのＩＰヘッダＦ２２とＭＡＣヘッダＦ２３を削除してＦ２４のみを残し、データＦ２４をフラグメント分割２１０６Ｂに送る。更に、ＴＣＰ２１０２に対してＡＣＫフレームを送信する。

【０８５７】

中間ドライバ２１０６内のフラグメント分割２１０６Ｂは、ＴＣＰ２１０６Ａから受信したデータＦ２４のサイズを確認し、フラグメントの必要が無いことから、そのまま、データを再カプセル化２１０６Ｄに送る。

【０８５８】

中間ドライバ２１０６内の再カプセル化２１０６Ｄは、フラグメント分割２１０６Ｂより受信したデータＦ２４に、ＭＡＣヘッダＦ２１、ＩＰヘッダＦ２２、ＭＡＣヘッダＦ２３を付け、フレームフォーマットＦ２０の形式にして、ドライバ２１０５に送信する。この際、Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、Ｆ２１内のＭＡＣ　ＳＡには、端末２１のＭＡＣアドレスが設定される。又、Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定される。又、宛先ポートにはＴＣＰ３１０２のポートが設定され、送信元ポートにはＴＣＰ２１０２のポートが指定される。これらのヘッダは、カプセル化解除２１０６Ｆによって保存されたものである。

【０８５９】

ドライバ２１０５は、中間ドライバ２１０６より上記フレームを受け取り、ＮＩＣ２１１に転送する。

【０８６０】

ＮＩＣ２１１は、ドライバ２１０５よりフレームを受け取り、ＭＡＣ２１１１，ＰＨＹ２１１２，ポート２１１３を経由して、ＨＵＢ２２にフレームを転送する。

【０８６１】

ＨＵＢ２２は、端末２１のＮＩＣ２１１側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０側のポートに出力する。

【０８６２】

ゲートウェイ装置２０は、ＨＵＢ２２からのフレームをポート２０１３において受け取

り、ＰＨＹ２０１２、ＭＡＣ２０１１、ドライバ２００７を経由して、ブリッジ２００８に渡す。

【０８６３】

ブリッジ２００８は、ドライバ２００７から受信したフレーム（フレームフォーマットＦ２０形式）内のヘッダＦ２１内に存在するＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のＭＡＣアドレスであり、ゲートウェイ装置２０のＭＡＣアドレスでは無いとから、フレームをドライバ２００９に転送する。

【０８６４】

ブリッジ２００８から送信されたフレームは、ドライバ２００９、仮想ＮＩＣ２０１０を経由し、ゲートウェイアプリケーション２００１Ａに転送される。

【０８６５】

ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したフレームを、ゲートウェイアプリケーション２００１Ａとゲートウェイアプリケーション３００１Ａの間に設定したＳＳＬセッションに流す。

【０８６６】

すなわち、ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したＥｔｈｅｒｎｅｔフレーム（フレームフォーマットＦ２０）をデータとしてＳＳＬ２００２に渡す。

【０８６７】

ＳＳＬ２００２は、ゲートウェイアプリケーション２００１Ａからデータ（Ｆ２１～Ｆ２４）を受け取ると、これを暗号化してデータＦ１４を生成し、ＴＣＰ２００３に渡す。

【０８６８】

ＴＣＰ２００３は、ＳＳＬ２００２よりデータＦ１４を受け取り、ＴＣＰヘッダＦ１３、及びＩＰヘッダＦ１２を付けて、ＩＰルーティング２００４に渡す。ここで、Ｆ１２内のＩＰ　ＤＡには、ゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡには、ゲートウェイ装置２０のＩＰアドレスが設定される。又、宛先ポートにはＴＣＰ３００３のポートが設定され、送信元ポートにはＴＣＰ２００３のポートが指定される。

【０８６９】

ＩＰルーティング２００４は、ＴＣＰ２００３より受信したデータのＩＰヘッダＦ１２内のＩＰアドレス等を参照し、フレームをＩＰスタック２００５に渡す。

【０８７０】

ＩＰスタック２００５は、ＩＰルーティング２００４よりフレームを受信し、フレームにＭＡＣヘッダＦ１１を付けて、Ｅｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームフォーマットＦ１０の形式にして、ブリッジ２００８に渡す。

【０８７１】

ここで、Ｆ１１内のＭＡＣ　ＤＡには、ＡＲＰの結果よりＦｉｒｅｗａｌｌ　３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡには、ゲートウェイ装置２０のＭＡＣアドレスが設定される。

【０８７２】

ＩＰスタック２００５より送信されたフレームは、ブリッジ２００８、ドライバ２００７，ＮＩＣ２０１を経由して、ＨＵＢ２２に送られる。

【０８７３】

ＨＵＢ２２は、ゲートウェイ装置２２側のポートからフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＷＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３に出力する。

【０８７４】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からのフレームを受信し、ＩＰ　ＤＡを参照してＭＡＣヘッダＦ１１を変更し、受信フレームをフレームフォーマットＦ１０の形のまま、

ＨＵＢ３２に転送する。

【０８７５】

ここで、Ｆ１１内のＭＡＣ　ＤＡにはゲートウェイ装置３０のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＬＡＮ側のＭＡＣアドレスが設定される。

【０８７６】

ＨＵＢ３２は、Ｆｉｒｅｗａｌｌ３３からのフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがゲートウェイ装置３０のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置３０側のポートに出力する。

【０８７７】

ゲートウェイ装置３０は、ＨＵＢ３２からのフレームをポート３０１３より受信すると、ＰＨＹ３０１２、ＭＡＣ３０１１、ドライバ３００７を経由して、ＩＰスタック３００５に転送する。

【０８７８】

ＩＰスタック３００５は、ドライバ３００７から受信したフレームのＭＡＣヘッダＦ１１を取り外して、ＩＰルーティング３００４に送る。

【０８７９】

ＩＰルーティング３００４は、受信したフレームのヘッダＦ１２内のＩＰ　ＤＡと、Ｆ１３内の宛先ポート番号を参照し、フレームをＴＣＰ３００３に転送する。

【０８８０】

ＴＣＰ３００３は、ＩＰルーティング３００４からフレームを受信すると、ＴＣＰプロトコルに従ってＡＣＫパケットを返送する等の処理を行う。そして、受信したフレームから、ＴＣＰヘッダＦ１３とＩＰヘッダＦ１２を取り外し、データＦ１４をＳＳＬ３００２に転送する。

【０８８１】

ＳＳＬ３００２は、ＴＣＰ３００３からデータＦ１４を受信すると、復号化処理により暗号化を解除し、データＦ１４からＥｔｈｅｒｎｅｔフレームＦ２０、即ち、Ｆ２１～Ｆ２４を取り出し、ゲートウェイアプリケーション３００１Ａに転送する。

【０８８２】

このフレームは、端末２１からＨＵＢ２２に送信された時の状態そのままに保たれており、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスが設定されている。又、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定されている。

【０８８３】

ゲートウェイアプリケーション３００１Ａは、ＳＳＬ３００２からフレームＦ２０を受信すると、このフレームを、そのまま、カプセル化処理３００１Ｂに流す。

【０８８４】

カプセル化処理３００１Ｂは、ゲートウェイアプリケーション３００１Ａよりフレームを受信すると、ヘッダＦ２１、ヘッダＦ２２、ヘッダＦ２３を取り外し、これらヘッダに記載のＩＰアドレス及びポートに対して、改めて、フレームを送信する。すなわち、サーバ３１のＩＰアドレスの、ＴＣＰ３１０２のポートに対して、データＦ２４を送るようＴＣＰ３００３Ｂに伝える。

【０８８５】

ＴＣＰ３００３Ｂは、カプセル化３００１Ｂよりデータ２４を受け取り、予め、ＴＣＰ３１０２とＴＣＰ３００３Ｂとの間で設定されたＴＣＰセッションに流す。すなわち、ＴＣＰ３００３Ｂは、データＦ２４にＩＰヘッダＦ２２及びＴＣＰヘッダＦ２３を取り付け、ＩＰルーティング３００４に転送する。ここで、ＩＰヘッダＦ２２のＩＰ　ＤＡには

、サーバ３１のＩＰアドレスが記載され、ＩＰヘッダＦ２２のＩＰ　ＳＡには、ゲートウェイ装置３０のＩＰアドレスが記載される。又、宛先ポートにはＴＣＰ３１０２のポートが記載され、送信元ポートには、ＴＣＰ３００３Ｂのポートが記載される。

【０８８６】

ＩＰルーティング３００４は、ＴＣＰ３００３Ｂからパケットを受け取り、ＩＰ　ＤＡやポート等を参照して、ＩＰスタック３００５Ｂにフレームを転送する。

【０８８７】

ＩＰスタック３００５Ｂは、ＩＰルーティング３００４よりデータを受信すると、これにヘッダＦ２１を付けて、ドライバ３００７に送る。ここで、Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスを設定し、Ｆ２１内のＭＡＣ　ＳＡにはゲートウェイ装置３０のＭＡＣアドレスを設定する。このようにして、ＴＣＰ３００３Ｂからの受信フレームをフレームフォーマットＦ２０の形にして、ドライバ３００７に転送する。

【０８８８】

ＩＰスタック３００５Ｂより出力されたフレームは、ブリッジ３００８、ドライバ３００７、ＮＩＣ３０１を経由して、ＨＵＢ３２に転送される。

【０８８９】

ＨＵＢ３２は、ゲートウェイ装置３０側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、サーバ３１側のポートに出力する。

【０８９０】

ＨＵＢ３２から送信されたフレームは、サーバ３１内のＮＩＣ３１１、ドライバ３１０５、ＩＰスタック３１０４、ＩＰルーティング３１０３、ＴＣＰ３１０２を経由して転送され、フレーム内のデータＦ２４がアプリケーション３１０１に渡される。

【０８９１】

以上のようにして、端末２１内のアプリケーション２１０１からサーバ３１内のアプリケーション３１０１への一連のフレーム転送が完了する。

【０８９２】

上記の例とは逆の経路を辿ることで、サーバ３１内のアプリケーション３１０１から端末２１内のアプリケーション２１０１への一連のフレーム転送も、同様に実現可能である。

【０８９３】

尚、本実施の形態では、ＴＣＰセッションはＴＣＰ２１０２と中間ドライバ２１０６の間、及びＴＣＰ２００３とＴＣＰ３００３の間、及びＴＣＰ３００３ＢとＴＣＰ３１０２の間において設定される。従って、中間ドライバ２１０６からＴＣＰ２００３の間、及びＴＣＰ３００３からＴＣＰ３００３Ｂの間の転送には、ＴＣＰの輻輳制御および再送制御が機能しなくなる。

【０８９４】

しかしながら、一般的に、イントラネット内でパケットの損失が発生したり、輻輳が発生したりすることは稀であり、Ｆｉｒｅｗａｌｌを跨ぐ接続、即ち、ＷＡＮを介す接続の場合に、損失や輻輳への対応が必要となる。本実施の形態では、ゲートウェイ装置２０とゲートウェイ装置３０の間は、ＴＣＰが機能している為、この区間における再送制御や輻輳制御があれば、アプリケーション２１０１とアプリケーション３１０１の間の通信における影響は殆ど発生しない。

【０８９５】

本実施の形態では、ゲートウェイ装置３０側にカプセル化処理等を実装し、端末２１側に中間ドライバを実装する例を示したが、これとは逆に、ゲートウェイ装置２０側にカプセル化処理等を実装し、サーバ３１側に中間ドライバを実装することも可能である。

【０８９６】

［発明の効果］

次に、本実施の形態の効果について説明する。

【０８９７】

本実施の形態に挙げた発明を利用すると、端末２１とサーバ３１との間で、フレームの高速転送が可能になる。

【０８９８】

これは、端末２１とサーバ３１との間の通信において、ヘッダＦ２３の位置のＴＣＰによる輻輳制御と再送制御が発生しないよう、端末２１内の中間ドライバと、ゲートウェイ装置３０内のカプセル化処理３００１Ｂにおいて、端末２１内のＴＣＰと、サーバ３１内のＴＣＰを終端し、ＴＣＰ　ｏｖｅｒ　ＴＣＰ問題の発生を回避しているからである。

【０８９９】

［第７の実施の形態］

本発明の第７の実施の形態は、第６の実施の形態に対して、ゲートウェイ装置３０内に、ブリッジ３００８と、ＩＰスタック３００５Ｂが追加設置されている点において異なる。

【０９００】

第７の実施の形態におけるＨＵＢ２２，ＨＵＢ３２、端末２１，ゲートウェイ装置２０，イントラネット２、イントラネット３の構成および動作は、第６の実施の形態と同じである。

【０９０１】

第７の実施の形態においては、イントラネット２は、閉域ＬＡＮだけで無く、インターネット等のオープンなＷＡＮを用いても構わない。

【０９０２】

第６の実施の形態では、サーバ３１側のアプリケーションが、実際に、端末２１内のアプリケーション２１０１から通信しているものの、ゲートウェイ装置３０からアクセスを受けていると認識してしまう問題があった。

【０９０３】

第７の実施の形態では、ゲートウェイ装置にＩＰスタックを追加で設置することで、サーバ３１側のアプリケーションが、端末２１からアクセスを受けていると認識される環境を作っている。

【０９０４】

［構成の説明］

図２３は、第７の実施の形態におけ、各機器の構成とフレームの転送経路を詳細に示したブロック図である。

【０９０５】

ゲートウェイ装置３０は、第６の実施の形態におけるゲートウェイ装置３０に対して、ブリッジ３００８と、ＩＰスタック３００５Ｂが各々、追加されている点において異なる。

【０９０６】

ブリッジ３００８は、第３～第５の実施の形態におけるブリッジ３００８と同様である。すなわち、ＭＡＣ　ＤＡをもとに、転送先となるドライバ若しくはＩＰスタックを決定する。

【０９０７】

ＩＰスタック３００５Ｂは、ＩＰスタック３００５と同様の構成をもち、同様の動作を行う。但し、付加するＭＡＣ　ＳＡ及びＩＰ　ＳＡに関しては、カプセル化解除３００１Ｂより指定されたアドレスを用いる。

【０９０８】

ＨＵＢ２２、ＨＵＢ３２、端末２１，ゲートウェイ装置２０，イントラネット２、イントラネット３の構成および動作は、第６の実施の形態と同じである。

【０９０９】

Ｆｉｒｅｗａｌｌ３３は、第６の実施の形態のＦｉｒｅｗａｌｌ３３と同様の構成を有

し、同様の動作を行う。但し、本実施の形態においては、Ｆｉｒｅｗａｌｌ３３の代わりに、ＮＡＴルータやＰｒｏｘｙサーバを用いても良い。

【０９１０】

第７の実施の形態でも、他の実施の形態と同様に、ゲートウェイ装置２０とゲートウェイ装置３０との間で、予め、ＳＳＬセッションを設定している場合のみ、イントラネット２内の機器からイントラネット３内の機器へのアクセスが可能になる。

【０９１１】

［動作の説明］

［ＳＳＬセッションの確立動作］

第６の実施の形態における、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）の確立動作は、第５の実施の形態、及び第６の実施の形態と同様である為、ここでは省略する。

【０９１２】

［アプリケーション２１０１からアプリケーション３１０１へのセッション構築動作］

図２３を用いて、第７の実施の形態において、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション３１０１との間の、セッション確立動作について説明を行う。

【０９１３】

この際、ブリッジ２００８，ＨＵＢ２２、ＨＵＢ３２がすでに端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。

【０９１４】

又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。

【０９１５】

更に、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）が、上述の動作例により、既に、設定されているものとする。

【０９１６】

中間ドライバ２１０６は、自ノード内の全てのアプリケーションにおけるＴＣＰの処理を終端するよう、予め、設定されているものとする。

【０９１７】

端末２１内のアプリケーション２１０１は、ユーザからのサーバ３１内のアプリケーション３１０１への接続要求を受け、ＴＣＰ２１０２にサーバ３１内のアプリケーション３１０１への通信開始を指示する。

【０９１８】

ＴＣＰ２１０２は、アプリケーション２１０１からの通信開始指示を受け、ＴＣＰ３１０２との間でＴＣＰセッションを確立する為に、ＩＰルーティング２１０３に対して、ＴＣＰ３１０２とのＴＣＰセッション確立要求パケット（ＹＮ）を送信する。このパケットは、ＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにサーバ３１宛、宛先ポート番号にＴＣＰ３１０２が設定されている。このＴＣＰセッション確立要求パケットとは、ＴＣＰセッションの確立時に、スリーウェイハンドシェーク（ｔｈｒｅｅ　ｗａｙ　ｈａｎｄｓｈａｋｅ）の為に送信される、ＳＹＮパケットのことである。本明細書においては、ＳＳＬセッション確立動作の説明を簡略化するため、スリーウェイハンドシェークで送受信されるパケットうち、ＳＹＮパケットをＴＣＰセッション確立要求パケットと呼び、ＳＹＮパケット＋ＡＣＫパケットを応答パケットと呼んでいる。また実際にはＡＣＫパケットも送信されるが、ＡＣＫパケットについてはＳＹＮパケットと同様に転送されるため、本動作の説明では説明を省略する。

【０９１９】

ＩＰルーティング２１０４は、ＴＣＰ２１０２から受信したセッション確立要求パケッ

トの宛先ＩＰアドレスと宛先ポート番号を参照し、パケットをＩＰスタック２１０４に転送する。

【０９２０】

ＩＰスタック２１０４は、ＩＰルーティング２１０３より受信したパケットに、サーバ３１のＭＡＣアドレスを宛先ＭＡＣアドレスとして付加し、更に送信元ＭＡＣアドレスに端末２１のＭＡＣアドレスを設定してＴＣＰセッション確立フレームを生成し、中間ドライバ２１０６に転送する。

【０９２１】

中間ドライバ２１０６は、ＩＰスタック２１０４からフレームを受信し、フレーム解析を行う。解析の結果、フレームはＴＣＰセッション確立フレームであるので、中間ドライバ２１０６カプセル化解除においてＭＡＣヘッダを取り外し、中間ドライバ２１０６ＴＣＰ部でＴＣＰ２１０２からＴＣＰ３１０２へのセッション確立要求を終端させる。すなわち、ＴＣＰ２１０２は、元々は、ＴＣＰ３１０２に対してＴＣＰセッション確立要求を行ったが、実際は、この要求に対して中間ドライバ２１０６内のＴＣＰが受信して保留し、ＴＣＰ２１０２と中間ドライバ２１０６内のＴＣＰとの間で、ＴＣＰセッションの確立処理を行ってＴＣＰセッション確立処理を終端させる。

【０９２２】

中間ドライバ２１０６は、ＴＣＰセッション確立処理を終端させる際、カプセル化処理３００１Ｂに対して、ＴＣＰ３１０２との間でＴＣＰセッションを確立するよう要求する為、ドライバ２１０５に接続要求のパケットを送る。この接続要求パケットはＴＣＰの規格に沿ったパケットではなく、独自のパケットである。この接続要求パケットには、宛先ＩＰアドレスにサーバ３１が、宛先ポート番号にＴＣＰ３１０２が設定される。そして、このパケットに宛先ＭＡＣアドレスが付加され、更に送信元ＭＡＣアドレスに自ノードのＭＡＣアドレスを設定されてフレームが生成される。

【０９２３】

ドライバ２１０５は、中間ドライバ２１０６から接続要求フレームを受信し、ＭＡＣ２１１１に転送する。

【０９２４】

ＭＡＣ２１１１は、ドライバ２１０５からフレームを受信し、ＰＨＹ２１１２に転送する。

【０９２５】

ＰＨＹ２１１２は、ＭＡＣ２１１１からフレームを受信し、ポート２１１３に転送する。

【０９２６】

ポート２１１３は、ＰＨＹ２１１２からフレームを受信し、イーサネットケーブルを経由してＨＵＢ２２に転送する。

【０９２７】

ＨＵＢ２２は、端末２１のＮＩＣ２１１側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０側のポートに出力する。

【０９２８】

ゲートウェイ装置２０は、ＨＵＢ２２からのフレームをポート２０１３において受け取り、ＰＨＹ２０１２、ＭＡＣ２０１１、ドライバ２００７を経由して、ブリッジ２００８に渡す。

【０９２９】

ブリッジ２００８は、ドライバ２００７から受信したフレーム（フレームフォーマットＦ２０形式）内のヘッダＦ２１内に存在するＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のＭＡＣアドレスであり、ゲートウェイ装置２０のＭＡＣアドレスではないことから、フレームをドライバ２００９に転送する。

【０９３０】
ブリッジ２００８から送信されたフレームは、ドライバ２００９、仮想ＮＩＣ２０１０を経由し、ゲートウェイアプリケーション２００１Ａに転送される。
【０９３１】
ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したフレームを、ゲートウェイアプリケーション２００１Ａとゲートウェイアプリケーション３００１Ａの間に設定したＳＳＬセッションに流す。
【０９３２】
すなわち、ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したＥｔｈｅｒｎｅｔフレーム（フレームフォーマットＦ２０）をデータとしてＳＳＬ２００２に渡す。
【０９３３】
ＳＳＬ２００２は、ゲートウェイアプリケーション２００１Ａからデータ（Ｆ２１～Ｆ２４）を受け取ると、これを暗号化してデータＦ１４を生成し、ＴＣＰ２００３に渡す。
【０９３４】
ＴＣＰ２００３は、ＳＳＬ２００２よりデータＦ１４を受け取り、ＴＣＰヘッダＦ１３及びＩＰヘッダＦ１２を付けて、ＩＰルーティング２００４に渡す。
【０９３５】
ここで、Ｆ１２内のＩＰ　ＤＡには、ゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡには、ゲートウェイ装置２０のＩＰアドレスが設定される。又、宛先ポートにはＴＣＰ３００３のポートが設定され、送信元ポートにはＴＣＰ２００３のポートが指定される。
【０９３６】
ＩＰルーティング２００４は、ＴＣＰ２００３より受信したデータのＩＰヘッダＦ１２内のＩＰアドレス等を参照し、フレームをＩＰスタック２００５に渡す。
【０９３７】
ＩＰスタック２００５は、ＩＰルーティング２００４よりフレームを受信し、フレームにＭＡＣヘッダＦ１１をつけて、Ｅｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームフォーマットＦ１０の形式にして、ブリッジ２００８に渡す。
【０９３８】
ここで、Ｆ１１内のＭＡＣ　ＤＡには、ＡＲＰの結果よりＦｉｒｅｗａｌｌ　３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡには、ゲートウェイ装置２０のＭＡＣアドレスが設定される。
【０９３９】
ＩＰスタック２００５より送信されたフレームは、ブリッジ２００８、ドライバ２００７，ＮＩＣ２０１を経由して、ＨＵＢ２２に送られる。
【０９４０】
ＨＵＢ２２は、ゲートウェイ装置２２側のポートからフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＷＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３に出力する。
【０９４１】
Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からのフレームを受信し、ＩＰ　ＤＡを参照してＭＡＣヘッダＦ１１を変更し、受信フレームをフレームフォーマットＦ１０の形のままＨＵＢ３２に転送する。
【０９４２】
ここで、Ｆ１１内のＭＡＣ　ＤＡにはゲートウェイ装置３０のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＬＡＮ側のＭＡＣアドレスが設定される。
【０９４３】

ＨＵＢ３２は、Ｆｉｒｅｗａｌｌ３３からのフレームを受信すると、Ｆ１１内のＭＡＣ ＤＡを参照し、ＭＡＣ ＤＡがゲートウェイ装置３０のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置３０側のポートに出力する。

【０９４４】

ゲートウェイ装置３０は、ＨＵＢ３２からのフレームをポート３０１３より受信すると、ＰＨＹ３０１２、ＭＡＣ３０１１、ドライバ３００７、ブリッジ３００８を経由して、ＩＰスタック３００５に転送する。

【０９４５】

ＩＰスタック３００５は、ブリッジ３００８から受信したフレームのＭＡＣヘッダＦ１１を取り外してパケットにして、ＩＰルーティング３００４に送る。

【０９４６】

ＩＰルーティング３００４は、ＩＰスタック３００５より受信したパケットのヘッダＦ１２内のＩＰ ＤＡと、Ｆ１３内の宛先ポート番号を参照し、パケットをＴＣＰ３００３に転送する。

【０９４７】

ＴＣＰ３００３は、ＩＰルーティング３００４からパケットを受信すると、ＴＣＰプロトコルに従ってＴＣＰ２００３に対してＡＣＫパケットを返送するなどの処理を行う。そして、受信したパケットから、ＴＣＰヘッダＦ１３とＩＰヘッダＦ１２を取り外し、データＦ１４をＳＳＬ３００２に転送する。

【０９４８】

ＳＳＬ３００２は、ＴＣＰ３００３からデータＦ１４を受信すると、復号化処理により暗号化を解除し、データＦ１４からＥｔｈｅｒｎｅｔフレームＦ２０、即ち、Ｆ２１～Ｆ２４を取り出し、ゲートウェイアプリケーション３００１Ａに転送する。

【０９４９】

ゲートウェイアプリケーション３００１Ａは、ＳＳＬ３００２からフレームＦ２０を受信すると、このフレームを、そのまま、カプセル化処理３００１Ｂに流す。このフレームは、端末２１からＨＵＢ２２に送信された時の状態のままに保たれており、ＬＡＮ ＭＡＣ Ｆ２１内のＭＡＣ ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ ＭＡＣ Ｆ２１内のＭＡＣ ＳＡには端末２１のＭＡＣアドレスが設定されている。又、ＬＡＮ ＩＰ Ｆ２２内のＩＰ ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ ＩＰ Ｆ２２内のＩＰ ＳＡには、端末２１のＩＰアドレスが設定されている。

【０９５０】

カプセル化処理３００１Ｂは、ゲートウェイアプリケーション３００１Ａよりフレームを受信し、フレーム解析を行う。解析の結果、パケットは、中間ドライバ２１０６から送信されたＴＣＰ３１０２への接続要求パケットである為、ＴＣＰ３００３Ｂに対して、ＴＣＰ３１０２との間でＴＣＰセッションを確立するよう命令する。同時に、ＩＰスタック３００５Ｂに対して、ＩＰアドレスとして端末２１のＩＰアドレスを持ち、ＭＡＣアドレスとして端末２１のＭＡＣアドレスを持つよう設定する。

【０９５１】

ＴＣＰ３００３Ｂは、ＴＣＰ３１０２との間でＴＣＰセッションを確立する為に、ＩＰルーティング３００４に対して、ＴＣＰ３１０２とのＴＣＰセッション確立要求パケット（ＳＹＮ）を送信する。このパケットはＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにサーバ３１宛、宛先ポート番号にＴＣＰ３１０２が設定され、更に送信元ＩＰアドレスには端末２１のＩＰアドレスが設定され、送信元ポート番号にはＴＣＰ２１０２のポート番号が設定されてＴＣＰセッション確立要求のフレームが生成される。

【０９５２】

ＩＰルーティング３００５Ｂに渡されたフレームは、ＩＰスタック３００５，ドライバ３００７、ＮＩＣ３０１を経由して、ＨＵＢ３２に転送される。

【０９５３】

ＨＵＢ３２は、ゲートウェイ装置３０側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、サーバ３１側のポートに出力する。

【０９５４】

サーバ３１は、ＨＵＢ３２内からフレームを受信し、ポート３１１３、ＰＨＹ３１１２、ＭＡＣ３１１１、ドライバ３１０５の経路で転送し、ＩＰスタック３１０４に転送する。

【０９５５】

ＩＰスタック３１０４は、ドライバ３１０５からフレームを受信し、ＭＡＣヘッダを外してＴＣＰセッション確立要求パケットＩＰルーティング３１０３に転送する。

【０９５６】

ＩＰルーティング３１０３は、ＩＰスタック３１０４より受信したパケットの宛先ポート番号を参照し、ＴＣＰ３１０２側のポート番号が付加されていることから、このパケットをＴＣＰ３１０２に転送する。

【０９５７】

ＴＣＰ３１０２は、ＩＰルーティング３１０３よりパケットを受信する。このパケットはＴＣＰセッション確立要求パケットであるので、ＴＣＰプロトコルに従い、セッション確立に対して応答パケットを返送する。

【０９５８】

ＴＣＰ３１０２は、応答パケットを、ＴＣＰ２１０２宛てに送信する。すなわち、応答パケットの宛先ＩＰは端末２１のＩＰアドレスが設定され、応答パケットの宛先ポートは、ＴＣＰ２１０２のポート番号が設定される。これは、ＴＣＰ３００３Ｂが、恰も、ＴＣＰ２１０２で有るかのように振る舞い、ＩＰスタック３００５Ｂが、恰も、端末２１のＩＰスタック２１０４であるかのように振る舞っているからである。

【０９５９】

応答パケットは、セッション確立要求パケットとは逆の経路、即ち、ＩＰルーティング３１０３、ＩＰスタック３１０４、ドライバ３１０５，ＮＩＣ３１１，ＨＵＢ３２，ＮＩＣ３０１、ブリッジ３００８，ＩＰスタック３００５Ｂを経由して、ＴＣＰ３００３Ｂに届く。

【０９６０】

ＴＣＰ３００３Ｂは、応答パケットを受信すると、この応答パケットに対するＡＣＫパケットをＴＣＰ３１０２に送信してＴＣＰの処理を終端させ、データをカプセル化処理３００１Ｂに渡す。

【０９６１】

カプセル化処理３００１Ｂは、端末２１内の中間ドライバ２１０６に対して、接続完了通知の為のパケットを送信する。この接続完了通知のパケットは、ＴＣＰの規格に沿ったパケットではなく、独自のパケットである。このパケットは、宛先ＩＰアドレスとして端末２１が、宛先ポート番号としてＴＣＰ２１０２が、送信元ＩＰアドレスとしてサーバ３１が、送信元ポート番号としてＴＣＰ３１０２が設定されフレームが生成される。

【０９６２】

接続完了通知フレームは、接続要求フレームとは逆の経路、即ち、ゲートウェイアプリケーション３００１Ａ、ＳＳＬ３００２，ＴＣＰ３００３，ＩＰルーティング３００４，ＩＰスタック３００５、ドライバ３００７、ＮＩＣ３０１、ＨＵＢ３３，Ｆｉｒｅｗａｌｌ３３、ＨＵＢ３２，ＮＩＣ２０１、ＣＰＵ２００、ＮＩＣ２０１、ＨＵＢ２２、ＮＩＣ２１１を経由して、ＣＰＵ２１０内の中間ドライバ２１０６に届く。

【０９６３】

中間ドライバ２１０６は、接続完了通知フレームを受信し、フレーム解析を行う。解析の結果、自ノード内のアプリケーション宛のパケットであるので受信する。受信したパケットは、カプセル化処理３００１Ｂから中間ドライバ２１０６に向けて送信された、カプ

セル化処理３００１ＢとＴＣＰ３１０２との間の接続完了通知パケットである為、中間ドライバ２１０６内のＴＣＰは、ＴＣＰプロトコルに従い、ＴＣＰセッション確立に対する応答パケットをＴＣＰ２１０３に送る為、ＩＰスタック２１０４に対して、応答パケットを送信する。

【０９６４】

応答パケットは、ＩＰスタック２１０４、ＩＰルーティング２１０３を経由し、ＴＣＰ２１０２に到達する。

【０９６５】

ＴＣＰ２１０２は、ＩＰルーティング２１０３よりパケットを受信する。このパケットはＴＣＰセッションの確立要求に対する応答パケットであるので、アプリケーション２１０１に対して、ＴＣＰ３１０２とのＴＣＰセッション接続完了を通知する。この際、ＴＣＰ２１０２は、応答パケットが、ＴＣＰ３１０２から届いたものであると認識する。これは、実際の応答は中間ドライバ２１０６内のＴＣＰから送信されたものであるが、中間ドライバ２１０６内のＴＣＰは、ＴＣＰ３１０２を騙ってＴＣＰ２１０２にセッション確立応答を行った為、ＴＣＰ２１０２は、恰も、ＴＣＰ３１０２から応答があったと認識する。

【０９６６】

ＴＣＰ２１０２は応答パケットを受信すると、この応答パケットに対してＡＣＫパケットを生成してＴＣＰ３１０２宛に送信する。このＡＣＫパケットは、中間ドライバ２１０６のＴＣＰが、ＩＰルーティング２００４及びＩＰスタック２００５を介して受信し、ＴＣＰ処理を終端させる。

【０９６７】

以上のようにして、第５の実施の形態において、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション３１０１との間の、セッション確立動作が完了する。

【０９６８】

［端末２１からサーバ３１へのフレーム転送動作］

図２３を用いて、第７の実施の形態において、端末２１からサーバ３１へフレームを送信する場合を例に挙げて、動作の説明を行う。

【０９６９】

この際、ブリッジ２００８，ブリッジ３００８，ＨＵＢ２２、ＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。

【０９７０】

又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。

【０９７１】

更に、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）が、上述の動作例により既に設定されているものとする。

【０９７２】

又、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション（アプリケーション３１０１）との間で、既に、ＴＣＰセッションが構築されているとする。

【０９７３】

端末２１内のアプリケーション２１０１が、サーバ３１内のアプリケーション３１０１宛のデータを、ＴＣＰ２１０２に渡す。

【０９７４】

ＴＣＰ２１０２は、アプリケーション２１０１からデータを受け取り、ＴＣＰプロトコルに従ってＴＣＰヘッダ（図２におけるＦ２３）やＩＰヘッダ（図２におけるＦ２２）を付けてＩＰパケットとし、ＩＰルーティング２１０３に渡す。この時、ＬＡＮ　ＩＰ　Ｆ

２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定される。

【０９７５】

ＩＰルーティング２１０３は、ＴＣＰ２１０２から受信したパケットの宛先ＩＰアドレス（サーバ３１宛て）及び宛先ポート（ＴＣＰ３１０２宛て）を参照し、データを、そのまま、ＩＰスタック２１０４に転送する。

【０９７６】

ＩＰスタック２１０４は、ＩＰルーティング２１０３からパケットを受信し、ＭＡＣヘッダ（図２におけるＦ２１）を付けてＥｔｈｅｒｎｅｔフレームを作成し、中間ドライバ２１０６に渡す。このフレームはＥｔｈｅｒｎｅｔフレームＦ２０のフォーマットを有する。この時、ＩＰスタック２１０４は、ＡＲＰの結果を参照して、フレームのＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスを設定し、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスを設定する。

【０９７７】

中間ドライバ２１０６は、ＩＰスタック２１０４よりフレームを受信し、フレーム解析２１０６Ｈにおいてフレーム解析を行う。解析の結果、フレームが、先に、セッション確立を行った、ＴＣＰ２１０２とＴＣＰ３１０２の間のセッションのフレームであることから、カプセル化解除２１０６Ｆにおいて、このフレームのＭＡＣヘッダＦ２１を削除して保存し、ＴＣＰ２１０６Ａに渡す。

【０９７８】

中間ドライバ２１０６内のＴＣＰ２１０６Ａは、ＴＣＰ２１０３Ａを終端する。すなわち、フレームのＩＰヘッダＦ２２とＭＡＣヘッダＦ２３を削除してＦ２４のみを残し、データＦ２４をフラグメント分割２１０６Ｂに送る。更に、ＴＣＰ２１０２に対してＡＣＫフレームを送信する。

【０９７９】

中間ドライバ２１０６内のフラグメント分割２１０６Ｂは，ＴＣＰ２１０６Ａから受信したデータＦ２４のサイズを確認し、フラグメントの必要がないことから、そのまま、データを再カプセル化２１０６Ｄに送る。

【０９８０】

中間ドライバ２１０６内の再カプセル化２１０６Ｄは、フラグメント分割２１０６Ｂより受信したデータＦ２４に、ＭＡＣヘッダＦ２１、ＩＰヘッダＦ２２、ＭＡＣヘッダＦ２３を付け、フレームフォーマットＦ２０の形式にして、ドライバ２１０５に送信する。この際、Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、Ｆ２１内のＭＡＣ　ＳＡには、端末２１のＭＡＣアドレスが設定される。又、Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定される。又、宛先ポートにはＴＣＰ３１０２のポートが設定され、送信元ポートにはＴＣＰ２１０２のポートが指定される。これらヘッダは、カプセル化解除２１０６Ｆによって保存されたものである。

【０９８１】

ドライバ２１０５は、中間ドライバ２１０６より上記フレームを受け取り、ＮＩＣ２１１に転送する。

【０９８２】

ＮＩＣ２１１は、ドライバ２１０５よりフレームを受け取り、ＭＡＣ２１１１，ＰＨＹ２１１２，ポート２１１３を経由して、ＨＵＢ２２にフレームを転送する。

【０９８３】

ＨＵＢ２２は、端末２１のＮＩＣ２１１側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０側のポートに出力する。

【０９８４】

ゲートウェイ装置２０は、ＨＵＢ２２からのフレームをポート２０１３において受け取り、ＰＨＹ２０１２、ＭＡＣ２０１１、ドライバ２００７を経由して、ブリッジ２００８に渡す。

【０９８５】

ブリッジ２００８は、ドライバ２００７から受信したフレーム（フレームフォーマットＦ２０形式）内のヘッダＦ２１内に存在するＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のＭＡＣアドレスであり、ゲートウェイ装置２０のＭＡＣアドレスではないことから、フレームをドライバ２００９に転送する。

【０９８６】

ブリッジ２００８から送信されたフレームは、ドライバ２００９、仮想ＮＩＣ２０１０を経由し、ゲートウェイアプリケーション２００１Ａに転送される。

【０９８７】

ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したフレームを、ゲートウェイアプリケーション２００１Ａとゲートウェイアプリケーション３００１Ａの間に設定したＳＳＬセッションに流す。すなわち、ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したＥｔｈｅｒｎｅｔフレーム（フレームフォーマットＦ２０）をデータとしてＳＳＬ２００２に渡す。

【０９８８】

ＳＳＬ２００２は、ゲートウェイアプリケーション２００１Ａからデータ（Ｆ２１～Ｆ２４）を受け取ると、これを暗号化してデータＦ１４を生成し、ＴＣＰ２００３に渡す。

【０９８９】

ＴＣＰ２００３は、ＳＳＬ２００２よりデータＦ１４を受け取り、ＴＣＰヘッダＦ１３、及びＩＰヘッダＦ１２を付けて、ＩＰルーティング２００４に渡す。

【０９９０】

ここで、Ｆ１２内のＩＰ　ＤＡには、ゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡには、ゲートウェイ装置２０のＩＰアドレスが設定される。又、宛先ポートにはＴＣＰ３００３のポートが設定され、送信元ポートにはＴＣＰ２００３のポートが指定される。

【０９９１】

ＩＰルーティング２００４は、ＴＣＰ２００３より受信したデータのＩＰヘッダＦ１２内のＩＰアドレス等を参照し、フレームをＩＰスタック２００５に渡す。

【０９９２】

ＩＰスタック２００５は、ＩＰルーティング２００４よりフレームを受信し、フレームにＭＡＣヘッダＦ１１を付けて、Ｅｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームフォーマットＦ１０の形式にして、ブリッジ２００８に渡す。

【０９９３】

ここで、Ｆ１１内のＭＡＣ　ＤＡには、ＡＲＰの結果よりＦｉｒｅｗａｌｌ　３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡには、ゲートウェイ装置２０のＭＡＣアドレスが設定される。

【０９９４】

ＩＰスタック２００５より送信されたフレームは、ブリッジ２００８、ドライバ２００７，ＮＩＣ２０１を経由して、ＨＵＢ２２に送られる。

【０９９５】

ＨＵＢ２２は、ゲートウェイ装置２２側のポートからフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＷＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３に出力する。

【０９９６】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からのフレームを受信し、ＩＰ　ＤＡを参照してＭＡＣヘッダＦ１１を変更し、受信フレームをフレームフォーマットＦ１０の形のままＨ

ＵＢ３２に転送する。

【０９９７】

ここで、Ｆ１１内のＭＡＣ　ＤＡにはゲートウェイ装置３０のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＬＡＮ側のＭＡＣアドレスが設定される。

【０９９８】

ＨＵＢ３２は、Ｆｉｒｅｗａｌｌ３３からのフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがゲートウェイ装置３０のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置３０側のポートに出力する。

【０９９９】

ゲートウェイ装置３０は、ＨＵＢ３２からのフレームをポート３０１３より受信すると、ＰＨＹ３０１２、ＭＡＣ３０１１、ドライバ３００７、ブリッジ３００８を経由して、ＩＰスタック３００５に転送する。

【１０００】

ＩＰスタック３００５は、ブリッジ３００８から受信したフレームのＭＡＣヘッダＦ１１を取り外して、ＩＰルーティング３００４に送る。

【１００１】

ＩＰルーティング３００４は、受信したフレームのヘッダＦ１２内のＩＰ　ＤＡと、Ｆ１３内の宛先ポート番号を参照し、フレームをＴＣＰ３００３に転送する。

【１００２】

ＴＣＰ３００３は、ＩＰルーティング３００４からフレームを受信すると、ＴＣＰプロトコルに従ってＡＣＫパケットを返送する等の処理を行う。そして、受信したフレームから、ＴＣＰヘッダＦ１３とＩＰヘッダＦ１２を取り外し、データＦ１４をＳＳＬ３００２に転送する。

【１００３】

ＳＳＬ３００２は、ＴＣＰ３００３からデータＦ１４を受信すると、復号化処理により暗号化を解除し、データＦ１４からＥｔｈｅｒｎｅｔフレームＦ２０、即ち、Ｆ２１～Ｆ２４を取り出し、ゲートウェイアプリケーション３００１Ａに転送する。

【１００４】

このフレームは、端末２１からＨＵＢ２２に送信された時の状態のままに保たれており、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスが設定されている。又、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定されている。

【１００５】

ゲートウェイアプリケーション３００１Ａは、ＳＳＬ３００２からフレームＦ２０を受信すると、このフレームを、そのまま、カプセル化処理３００１Ｂに流す。

【１００６】

カプセル化処理３００１Ｂは、ゲートウェイアプリケーション３００１Ａよりフレームを受信すると、ヘッダＦ２１、ヘッダＦ２２、ヘッダＦ２３を取り外し、これらヘッダに記載のＩＰアドレスおよびポートに対して、改めてフレームを送信する。すなわち、サーバ３１のＩＰアドレスの、ＴＣＰ３１０２のポートに対して、データＦ２４を送るよう、ＴＣＰ３００３Ｂに伝える。同時に、フレームのヘッダＦ２１のＭＡＣ　ＳＡに端末２１のＭＡＣアドレスを設定し、ヘッダＦ２２のＩＰ　ＳＡに端末２１のＩＰアドレスが設定されるよう、ＩＰスタック３００５Ｂを設定する。

【１００７】

ＴＣＰ３００３Ｂは、カプセル化３００１Ｂよりデータ２４を受け取り、予め、ＴＣＰ３１０２とＴＣＰ３００３Ｂとの間で設定されたＴＣＰセッションに流す。すなわち、

ＴＣＰ３００３Ｂは、データＦ２４にＩＰヘッダＦ２２及びＴＣＰヘッダＦ２３を取り付け、ＩＰルーティング３００４に転送する。ここで、ＩＰヘッダＦ２２のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが記載され、ＩＰヘッダＦ２２のＩＰ　ＳＡには、端末２１のＩＰアドレスが記載される。又、宛先ポートにはＴＣＰ３１０２のポートが記載され、送信元ポートには、ＴＣＰ２１０２のポートが記載される。

【１００８】

ＩＰルーティング３００４は、ＴＣＰ３００３Ｂからパケットを受け取り、ＩＰ　ＤＡやポート等を参照して、ＩＰスタック３００５Ｂにフレームを転送する。

【１００９】

ＩＰスタック３００５Ｂは、ＩＰルーティング３００４よりデータを受信すると、これにヘッダＦ２１を付けて、ドライバ３００７に送る。ここで、Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスを設定し、Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスを設定する。このようにして、ＴＣＰ３００３Ｂからの受信フレームをフレームフォーマットＦ２０の形にして、ブリッジ３００８を経由してドライバ３００７に転送する。

【１０１０】

ＩＰスタック３００５Ｂより出力されたフレームは、ブリッジ３００８、ドライバ３００７、ＮＩＣ３０１を経由して、ＨＵＢ３２に転送される。

【１０１１】

ＨＵＢ３２は、ゲートウェイ装置３０側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、サーバ３１側のポートに出力する。

【１０１２】

ＨＵＢ３２から送信されたフレームは、サーバ３１内のＮＩＣ３１１、ドライバ３１０５、ＩＰスタック３１０４、ＩＰルーティング３１０３、ＴＣＰ３１０２を経由して転送され、フレーム内のデータＦ２４がアプリケーション３１０１に渡される。

【１０１３】

以上のようにして、端末２１内のアプリケーション２１０１からサーバ３１内のアプリケーション３１０１への一連のフレーム転送が完了する。

【１０１４】

上記の例とは逆の経路を辿ることで、サーバ３１内のアプリケーション３１０１から端末２１内のアプリケーション２１０１への一連のフレーム転送も、同様に実現可能である。

【１０１５】

尚、本実施の形態では、ＴＣＰセッションはＴＣＰ２１０２と中間ドライバ２１０６の間、及びＴＣＰ２００３とＴＣＰ３００３の間、及びＴＣＰ３００３ＢとＴＣＰ３１０２の間において設定される。従って、中間ドライバ２１０６からＴＣＰ２００３の間、及びＴＣＰ３００３からＴＣＰ３００３Ｂの間の転送には、ＴＣＰの輻輳制御および再送制御が機能しなくなる。

【１０１６】

しかしながら、一般的に、イントラネット内でパケットの損失が発生したり、輻輳が発生したりすることは稀であり、Ｆｉｒｅｗａｌｌを跨ぐ接続、即ち、ＷＡＮを介す接続の場合に、損失や輻輳への対応が必要となる。本実施の形態では、ゲートウェイ装置２０とゲートウェイ装置３０の間は、ＴＣＰが機能している為、この区間における再送制御や輻輳制御があれば、アプリケーション２１０１とアプリケーション３１０１の間の通信における影響は殆ど発生しない。

【１０１７】

本実施の形態では、ゲートウェイ装置３０側にカプセル化処理等を実装し、端末２１側に中間ドライバを実装する例を示したが、これとは逆に、ゲートウェイ装置２０側にカプ

セル化処理等を実装し、サーバ３１側に中間ドライバを実装することも可能である。

【１０１８】

［発明の効果］

次に、本実施の形態の効果について説明する。

【１０１９】

本実施の形態に挙げた発明を利用すると、端末２１とサーバ３１との間で、フレームの高速転送が可能になる。

【１０２０】

これは、端末２１とサーバ３１との間の通信において、ヘッダＦ２３の位置のＴＣＰによる輻輳制御と再送制御が発生しないよう、端末２１内の中間ドライバと、ゲートウェイ装置３０内のカプセル化処理３００１Ｂにおいて、端末２１内のＴＣＰと、サーバ３１内のＴＣＰを終端し、ＴＣＰ　ｏｖｅｒ　ＴＣＰ問題の発生を回避しているからである。

【１０２１】

［第８の実施の形態］

本発明の第８の実施の形態は、第５の実施の形態に対して、端末２１内の中間ドライバ２１０６と、サーバ３１内の中間ドライバ３１０６が、各々、無くなり、ゲートウェイ装置２０内に高速化エンジンＸ２０１４が設置されて、ＳＳＬ２００２の暗号化および復号化処理が、高速化エンジンＸ２０１４において行われている点において異なる。

【１０２２】

又、第８の実施の形態は、第５の実施の形態において、ＴＣＰ　ｏｖｅｒ　ＴＣＰに対する対策を行わず、ＳＳＬセッションにおける暗号化および復号化処理の高速化に特化した構成になっている。

【１０２３】

第８の実施の形態におけるＨＵＢ２２，ＨＵＢ３２、イントラネット２、イントラネット３、ゲートウェイ装置３０の構成および動作は、第５の実施の形態と同じである。

【１０２４】

第８の実施の形態においては、イントラネット２は、閉域ＬＡＮだけでなく、インターネット等のオープンなＷＡＮを用いても構わない。

【１０２５】

［構成の説明］

図２４は、第８の実施の形態における各機器の構成とフレームの転送経路を詳細に示したブロック図である。

【１０２６】

ゲートウェイ装置２０は、第５の実施の形態におけるゲートウェイ装置２０に対して、高速化エンジンＸ２０１４が設置され、ＳＳＬ２００２の暗号化および復号化処理が、高速化エンジンＸ２０１４において行われる点において異なる。

【１０２７】

端末２１は、第５の実施の形態における端末２１に対して、中間ドライバ２１０６がなくなっている点において異なる。すなわち、第１～第４の実施の形態における端末２１と同様の構成を有し、同様の動作を行う。

【１０２８】

サーバ３１は、第５の実施の形態におけるサーバ３１に対して、中間ドライバ３１０６が無くなっている点において異なる。すなわち、第１～第４、第６、第７の実施の形態におけるサーバ３１と同様の構成を有し、同様の動作を行う。

【１０２９】

ＨＵＢ２２、ＨＵＢ３２、ゲートウェイ装置３０に関しては、第５の実施の形態と同様の構成を有し、同様の動作を行う。

【１０３０】

Ｆｉｒｅｗａｌｌ１３３は、第７の実施の形態のＦｉｒｅｗａｌｌ１３３と同様の構成を有し、同様の動作を行う。但し、本実施の形態においては、Ｆｉｒｅｗａｌｌ１３３の代わり

に、ＮＡＴルータやＰｒｏｘｙサーバを用いても良い。

【１０３１】

第８の実施の形態でも他の実施の形態と同様に、予め、ゲートウェイ装置２０とゲートウェイ装置３０との間でＳＳＬセッションを設定している場合のみ、イントラネット２内の機器からイントラネット３内の機器へのアクセスが可能になる。

【１０３２】

図２５は、第８の実施の形態における高速化エンジンＸ２０１４の構成を詳細に示したブロック図である。

【１０３３】

第８の実施の形態における高速化エンジンＸ２０１４は、図１２に示す第１の実施の形態における高速化エンジン２０１４に対して、フレーム解析２０１４Ｂ、及びマルチプレクサ２０１４Ｆの位置および動作が異なり、フラグメント分割２０１４Ｈ、カプセル化２０１４Ｉ、カプセル化解除２０１４Ｊ、フラグメント解除２０１４Ｋ、制御フレーム解析２０１４Ｄ、及びマルチプレクサ２０１４Ｅが存在しない点において異なる。

【１０３４】

第１の実施の形態における高速化エンジン２０１４では、暗号化および復号化を行うフレームが、インタフェース２０１４Ａから入力されたが、第８の実施の形態における高速化エンジンＸ２０１４では、暗号化および復号化を行うフレームが、インタフェース２０１４Ｃより入力される。

【１０３５】

第８の実施の形態における高速化エンジンＸ２０１４では、インタフェース２０１４Ａ，インタフェース２０１４Ｃ、暗号化２０１４Ｇ、復号化２０１４Ｌ、制御フレーム送受信部２０１４Ｍは、第１の実施の形態における高速化エンジン２０１４におけるインタフェース２０１４Ａ，インタフェース２０１４Ｃ、暗号化２０１４Ｇ、復号化２０１４Ｌ、制御フレーム送受信部２０１４Ｍと、各々、同様の構成を有し、同様の動作を行う。

【１０３６】

フレーム解析２０１４Ｂは、インタフェース２０１４Ｃからフレームを受信し、以下に示す（１）～（４）の順序で宛先を決定して転送する。

（１）　受信したフレームが高速化エンジンの制御に関わる特殊なフレームであるか否か判断し、特殊フレームで無い場合は、インタフェース２０１４Ａに転送する。

（２）　受信したフレームが特殊フレーム、かつ、高速化エンジンＸ２０１４の制御設定に関わるもの（制御フレーム）であれば、制御フレーム送受信部２０１４Ｍに転送する。

（３）　受信したフレームが特殊フレーム、かつ、暗号化に関わるもの（被暗号化フレーム）であれば、暗号化２０１４Ｇに転送する。

（４）　受信したフレームが特殊フレーム、かつ、復号化に関わるもの（被復号化フレーム）であれば、復号化２０１４Ｌに転送する。

【１０３７】

フレーム解析２０１４Ｂは、受信したフレームが特殊フレームであるか否かの判断は、通常はＭＡＣ　ＤＡとＭＡＣ　ＳＡに基づいて判断する。ＭＡＣ　ＤＡ若しくはＭＡＣ　ＳＡの何れかに、予め、規定したアドレス範囲のＭＡＣアドレス（制御用ＭＡＣアドレスと呼ぶ。例えば０００００４Ｃ０００００００～ＦＦ）が記載されている場合は、受信したフレームを制御フレームと判断する。

【１０３８】

制御フレーム、被暗号化フレーム、及び被復号化フレームの判断も、各々、ＭＡＣアドレスに基づいて判別する。例えば、被暗号化フレームのＭＡＣ　ＤＡは００：００：４Ｃ：００：００：０Ａに設定され、被復号化フレームのＭＡＣ　ＤＡは００：００：４Ｃ：００：００：０Ｂに設定される。

【１０３９】

マルチプレクサ２０１４Ｆは、暗号化２０１４Ｇ、復号化２０１４Ｌ、制御フレーム送受信部２０１４Ｍ、更にインタフェース２０１４Ａよりフレームを受信し、必要であれば

、キューに保存して送信タイミングを調整し、インタフェース２０１４Ｃに送信する。キューに保存するのは、暗号化２０１４Ｇ、復号化２０１４Ｌ、制御フレーム送受信部２０１４Ｍ、更にインタフェース２０１４Ａの各々から到着するフレームの衝突を避ける為である。

【１０４０】

[動作の説明]

[ＳＳＬセッションの確立動作]

図２４を用いて、第８の実施の形態において、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合を例に挙げて、動作の説明を行う。

【１０４１】

この際、ブリッジ２００８、ブリッジ３００８、ＨＵＢ２２やＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３のＬＡＮ側、Ｆｉｒｅｗａｌｌ３３のＷＡＮ側、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。

【１０４２】

又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０との間の通信は双方向で許可するが、端末２１とサーバ３１との間のゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。

【１０４３】

ゲートウェイ装置３０内のゲートウェイアプリケーション３００１Ａは、ユーザからのゲートウェイ装置２０内のゲートウェイアプリケーション２００１Ａへの接続要求を受け、ＳＳＬ３００２にゲートウェイ装置２０内のゲートウェイアプリケーション２００１Ａへの通信開始を指示する。

【１０４４】

ＳＳＬ３００２は、ゲートウェイアプリケーション３００１Ａからの通信開始指示を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為に、ＴＣＰ３００３にゲートウェイ装置２０内のゲートウェイアプリケーション２００１Ａへの通信開始を指示する。

【１０４５】

ＴＣＰ３００３は、ＳＳＬ３００２からの通信開始指示を受け、ＴＣＰ２００３との間でＴＣＰセッションを確立する為に、ＩＰルーティング３００４に対して、ＴＣＰ２００３とのＴＣＰセッション確立要求パケット（ＳＹＮ）を送信する。このＴＣＰセッション確立要求パケットは、ＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにゲートウェイ装置２０宛、宛先ポート番号にＴＣＰ２００３が設定されている。

【１０４６】

ＩＰルーティング３００４は、ＴＣＰ３００３から受信したパケットの宛先ＩＰアドレスと宛先ポート番号を参照し、パケットをＩＰスタック３００５に転送する。

【１０４７】

ＩＰスタック３００５は、ＩＰルーティング３００４より受信したパケットに、Ｆｉｒｅｗａｌｌ３３内のイントラネット３側のＭＡＣアドレスを宛先ＭＡＣアドレスとして付加し、更に送信元ＭＡＣアドレスに自ノードのＭＡＣアドレスを設定してＴＣＰセッション確立要求フレームにし、ブリッジ３００８を経由してドライバ３００７に転送する。

【１０４８】

ドライバ３００７は、ＩＰスタック３００５からフレームを受信し、ＭＡＣ３０１１に転送する。

【１０４９】

ＭＡＣ３０１１は、ドライバ３００７からフレームを受信し、ＰＨＹ３０１２に転送する。

【１０５０】

ＰＨＹ３０１２は、ＭＡＣ３０１１からフレームを受信し、ポート３０１３に転送する

。

【１０５１】

ポート３０１３は、ＰＨＹ３０１２からフレームを受信し、イーサネットケーブルを経由してＨＵＢ３２に転送する。

【１０５２】

ＨＵＢ３２は、フレームを受信すると、ＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＬＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３側のポートに出力する。

【１０５３】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からフレームを受信し、ゲートウェイ装置３０からゲートウェイ装置２０への通信の為、これを許可し、ＨＵＢ２２に転送する。

【１０５４】

ＨＵＢ２２は、Ｆｉｒｅｗａｌｌ３３からパケットを受信し、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０に転送する。

【１０５５】

ゲートウェイ装置２０は、ＨＵＢ２２内からパケットを受信し、ポート２０１３、ＰＨＹ２０１２、ＭＡＣ２０１１、ドライバ２００７、ブリッジ２００８の経路でパケットを転送し、ＩＰスタック２００５に転送する。

【１０５６】

ＩＰスタック２００５は、ブリッジ２００８からパケットを受信し、ＭＡＣヘッダを外してパケットにしてＩＰルーティング２００４に転送する。

【１０５７】

ＩＰルーティング２００４は、ＩＰスタック２００５より受信したパケットの宛先ポート番号を参照し、ＴＣＰ２００３側のポート番号が付加されていることから、このパケットをＴＣＰ２００３に転送する。

【１０５８】

ＴＣＰ２００３は、ＩＰルーティング２００４よりパケットを受信する。このパケットは、ＴＣＰセッション確立要求パケット（ＳＹＮ）であるので、ＴＣＰプロトコルに従い、セッション確立要求に対して、セッション確立の為に必要な応答パケット（ＳＹＮ＋ＡＣＫ）をＴＣＰ３００３宛てに送信する。すなわち、応答パケットの宛先ＩＰはゲートウェイ装置３０のＩＰアドレスが設定され、応答パケットの宛先ポートはＴＣＰ３００３のポート番号が設定される。

【１０５９】

応答パケットは、ＩＰルーティング２００４、ＩＰスタック２００５、ブリッジ２００８、ドライバ２００７、ＮＩＣ２０１、ＨＵＢ２２、Ｆｉｒｅｗａｌｌ３３、ＨＵＢ３２、ＮＩＣ３０１を経由して、ＣＰＵ３００に到達し、更にドライバ３００７、ブリッジ３００８、ＩＰスタック３００５、ＩＰルーティング３００４を経由し、ＴＣＰ３００３に到達する。

【１０６０】

ＴＣＰ３００３は、ＩＰルーティング３００４より応答パケットを受信する。このパケットは、ＴＣＰセッションの確立要求に対する応答パケットであるので、ＴＣＰ２００３に対してＡＣＫパケットを送信する。ＴＣＰ２００３は、ＡＣＫパケットを受信するとＳＳＬ３００２に対してＴＣＰ３００３とのＴＣＰセッション接続完了を通知する。

【１０６１】

ＳＳＬ３００２は、ＴＣＰ３００３との接続完了通知を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為、ＳＳＬプロトコルに従い、セッション確立要求の為のパケット（ＳＳＬセッション確立要求パケット）を送信する。

【１０６２】

ＳＳＬセッション確立要求パケットは、ＴＣＰ３００３で受信されると、ＴＣＰ３００３とＴＣＰ２００３との間で設定されたＴＣＰセッションを通り、ＮＩＣ３０１、ＨＵＢ

３２、Ｆｉｒｅｗａｌｌ３３、ＨＵＢ２２、ＮＩＣ２０１を経由して、ＴＣＰ２００３に到着する。

【１０６３】

ＴＣＰ２００３は、ＳＳＬセッション確立要求パケットをＳＳＬ２００２に転送する。

【１０６４】

ＳＳＬ２００２は、ＳＳＬセッション確立要求の内容を検証し、問題が無ければ、ゲートウェイアプリケーション２００１Ａに対して、ＳＳＬ３００２とのセッション確立を通知すると同時に、ＳＳＬプロトコルに従い、ＳＳＬ３００２に対してＳＳＬセッション確立応答パケットを送信する。

【１０６５】

ＳＳＬセッション確立応答パケットは、ＳＳＬセッション確立要求パケットとは逆の経路、即ち、ＴＣＰ２００３とＴＣＰ３００３との間のＴＣＰセッションを経由して、ＳＳＬ３００２に到達する。

【１０６６】

ＳＳＬ２００２は、ＳＳＬ２００２の秘密鍵、ＳＳＬ３００２の公開鍵、ＳＳＬ２００２とＳＳＬ３００２の間の共通鍵、ＳＳＬセッションの相手方機器のＩＰアドレス（ゲートウェイ装置３０のＩＰアドレス）、ＳＳＬセッションの相手方機器の宛先ポート（ＴＣＰ３００３のポート）、自ノード側のＳＳＬセッションの送信元ポート番号（ＴＣＰ２００３のポート）、送信元ＩＰアドレス（ゲートウェイ装置２０のＩＰアドレス）、及び開始命令を制御フレームに載せ、仮想ＮＩＣ２０１０に制御フレームを送信する。

【１０６７】

制御フレームは、ＳＳＬ２００２を出ると、仮想ＮＩＣ２０１０、ドライバ２００９、ブリッジ２００８、ドライバ２００７、ＭＡＣ２１１１を経由して、高速化エンジンＸ２０１４に到着する。

【１０６８】

高速化エンジンＸ２０１４は、ＭＡＣアドレス等に基づいて受信したフレームが制御フレームであることを判別し、制御フレーム送受信部で受信する。そして、公開鍵、秘密鍵および共通鍵を、各々、復号化および暗号化に使用する為に保存し、ＩＰアドレスやポート番号をフレーム解析の為に保存する。そして、高速化処理開始命令を受け、フレーム解析、暗号化、及び複号化の処理を開始する。

【１０６９】

ＳＳＬ３００２は、ＳＳＬセッション確立応答の内容をＳＳＬプロトコルに従い検証し、問題が無ければ、ゲートウェイアプリケーション３００１Ａに対して、ＳＳＬ３００２とＳＳＬ２００２との間のＳＳＬセッション確立を通知する。

【１０７０】

以上のようにして、ＳＳＬ２００２とＳＳＬ３００２との間で、ＳＳＬセッションが確立される。

【１０７１】

以上により、第８の実施の形態において、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合の動作が完了する。

【１０７２】

[端末２１からサーバ３１へのフレーム転送動作]

図２４を用いて、第８の実施の形態において、端末２１からサーバ３１へフレームを送信する場合を例に挙げて、動作の説明を行う。

【１０７３】

この際、ブリッジ２００８、ブリッジ３００８、ＨＵＢ２２、ＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。

【１０７４】

又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１との間のゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。

【１０７５】

更に、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）が、上述の動作例により、既に、設定されているものとする。

【１０７６】

又、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション３１０１との間で、既に、ＴＣＰセッションが構築されているとする。

【１０７７】

端末２１内のアプリケーション２１０１が、サーバ３１内のアプリケーション３１０１宛のデータを、ＴＣＰ２１０２に渡す。

【１０７８】

ＴＣＰ２１０２は、アプリケーション２１０１からデータを受け取り、ＴＣＰプロトコルに従ってＴＣＰヘッダ（図２におけるＦ２３）やＩＰヘッダ（図２におけるＦ２２）を付けてＩＰパケットとし、ＩＰルーティング２１０３に渡す。この時、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡにはサーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには端末２１のＩＰアドレスが設定される。

【１０７９】

ＩＰルーティング２１０３は、ＴＣＰ２１０２から受信したパケットの宛先ＩＰアドレス（サーバ３１宛て）及び宛先ポート（ＴＣＰ３１０２宛て）を参照し、データを、そのまま、ＩＰスタック２１０４に転送する。

【１０８０】

ＩＰスタック２１０４は、ＩＰルーティング２１０３からパケットを受信し、ＭＡＣヘッダ（図２におけるＦ２１）を付けてＥｔｈｅｒｎｅｔフレームを作成し、ドライバ２１０５に渡す。このフレームはＥｔｈｅｒｎｅｔフレームＦ２０のフォーマットを有する。この時、ＩＰスタック２１０４は、ＡＲＰの結果を参照して、フレームのＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスを設定し、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスを設定する。

【１０８１】

ドライバ２１０５は、ＩＰスタック２１０５より上記フレームを受け取り、ＮＩＣ２１１に転送する。

【１０８２】

ＮＩＣ２１１は、ドライバ２１０５よりフレームを受け取り、ＭＡＣ２１１１、ＰＨＹ２１１２、ポート２１１３を経由して、ＨＵＢ２２にフレームを転送する。

【１０８３】

ＨＵＢ２２は、端末２１のＮＩＣ２１１側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０側のポートに出力する。

【１０８４】

ゲートウェイ装置２０は、ＨＵＢ２２からのフレームをポート２０１３において受け取り、ＰＨＹ２０１２、ＭＡＣ２０１１、ドライバ２００７を経由して、ブリッジ２００８に渡す。

【１０８５】

ブリッジ２００８は、ドライバ２００７から受信したフレーム（フレームフォーマットＦ２０形式）内のヘッダＦ２１内に存在するＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のＭＡＣアドレスであり、ゲートウェイ装置２０のＭＡＣアドレスでは無いことから、フレームをドライバ２００９に転送する。

【１０８６】

ブリッジ２００８から送信されたフレームは、ドライバ２００９、仮想ＮＩＣ２０１０を経由し、ゲートウェイアプリケーション２００１Ａに転送される。

【１０８７】

ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したフレームを、ゲートウェイアプリケーション２００１Ａとゲートウェイアプリケーション３００１Ａの間に設定したＳＳＬセッションに流す。

【１０８８】

すなわち、ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したＥｔｈｅｒｎｅｔフレーム（フレームフォーマットＦ２０）をデータとしてＳＳＬ２００２に渡す。

【１０８９】

ＳＳＬ２００２は、ゲートウェイアプリケーション２００１Ａから未暗号化のデータＦ１４（Ｆ２１～Ｆ２４）を受け取ると、ヘッダＦ１１をつけて、被暗号化フレームを作り、仮想ＮＩＣ２０１０に渡す。ここで、ヘッダＦ１１内のＭＡＣ　ＤＡには暗号化を命令する為の特殊ＭＡＣ（例えば００：００：４Ｃ：００：００：０Ａ等）を設定し、ＭＡＣ　ＳＡには仮想ＮＩＣ２０１０のＭＡＣアドレス等を設定する。このフレームは、ＳＳＬ２００２から仮想ＮＩＣ２０１０に、直接、渡すことは勿論、ゲートウェイアプリケーション２００１Ａを経由して、仮想ＮＩＣ２０１０に渡しても良い。

【１０９０】

被暗号化フレームは、仮想ＮＩＣ２０１０、ドライバ２００９、ブリッジ２００８、ドライバ２００７、ＭＡＣ２０１１を経由して、高速化エンジンＸ２０１４に到着する。

【１０９１】

高速化エンジンＸ２０１４は、インタフェース２０１４Ｃにおいて被暗号化フレームを受け取り、フレーム解析２０１４Ｂで受信フレームを被暗号化フレームだと判別し、ヘッダＦ１１ＭＡＣ　ＤＡとＭＡＣ　ＳＡの値を反転させ、暗号化２０１４Ｇに送る。高速化２０１４Ｇは、受信したフレームのデータＦ１４、即ち、Ｆ２１,Ｆ２２，Ｆ２３，Ｆ２４の部分を暗号化して、暗号化されたデータＦ１４を作成し、マルチプレクサ２０１４Ｆに渡す。マルチプレクサ２０１４Ｆは、暗号化より受信したフレームを、必要であれば、バッファリングし、インタフェース２０１４Ｃに送る。

【１０９２】

高速化エンジンＸ２０１４を出たフレームは、ＭＡＣ２０１１、ドライバ２００７、ブリッジ２００８、ドライバ２００９、仮想ＮＩＣ２０１０を経由して、ＳＳＬ２００２に戻る。このフレームのＭＡＣ　ＤＡには仮想ＮＩＣ２０１０のＭＡＣアドレス等が設定され、ＭＡＣ　ＳＡには暗号化を命令する為の特殊ＭＡＣ（例えば００：００：４Ｃ：００：００：０Ａ等）が設定されている。

【１０９３】

ＳＳＬ２００２は、仮想ＮＩＣより受信したフレームのヘッダＦ１１（ＭＡＣヘッダ）を削除し、データＦ１４のみをＴＣＰ２００３に渡す。

【１０９４】

ＴＣＰ２００３は、ＳＳＬ２００２よりデータＦ１４を受け取り、ＴＣＰヘッダＦ１３、及びＩＰヘッダＦ１２を付けて、ＩＰルーティング２００４に渡す。

【１０９５】

ここで、Ｆ１２内のＩＰ　ＤＡにはゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡにはゲートウェイ装置２０のＩＰアドレスが設定される。又、宛先ポートにはＴＣＰ３００３のポートが設定され、送信元ポートにはＴＣＰ２００３のポートが指定される。

【１０９６】

ＩＰルーティング２００４は、ＴＣＰ２００３より受信したデータのＩＰヘッダＦ１２内のＩＰアドレス等を参照し、フレームをＩＰスタック２００５に渡す。

【１０９７】

ＩＰスタック２００５は、ＩＰルーティング２００４よりフレームを受信し、フレームにＭＡＣヘッダＦ１１を付けて、Ｅｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームフォーマットＦ１０の形式にして、ブリッジ２００８に渡す。

【１０９８】

ここで、ＡＲＰの結果より、Ｆ１１内のＭＡＣ　ＤＡには、Ｆｉｒｅｗａｌｌ　３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡには、ゲートウェイ装置２０のＭＡＣアドレスが設定される。

【１０９９】

ＩＰスタック２００５より送信されたフレームは、ブリッジ２００８、ドライバ２００７、ＭＡＣ２０１１、高速化エンジンＸ２０１４、ＰＨＹ２０１２、ＭＡＣ２０１３を経由して、ＨＵＢ２２に送られる。この時、高速化エンジンＸ２０１４は、ＭＡＣから受信したフレームを、そのまま、ＰＨＹ２０１２に転送する。

【１１００】

ＨＵＢ２２は、ゲートウェイ装置２２側のポートからフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＷＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３に出力する。

【１１０１】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からのフレームを受信し、ＩＰ　ＤＡを参照してＭＡＣヘッダＦ１１を変更し、受信フレームをフレームフォーマットＦ１０の形のままＨＵＢ３２に転送する。

【１１０２】

ここで、Ｆ１１内のＭＡＣ　ＤＡにはゲートウェイ装置３０のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＬＡＮ側のＭＡＣアドレスが設定される。

【１１０３】

ＨＵＢ３２は、Ｆｉｒｅｗａｌｌ３３からのフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがゲートウェイ装置３０のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置３０側のポートに出力する。

【１１０４】

ゲートウェイ装置３０は、ＨＵＢ３２からのフレームをポート３０１３より受信すると、ＰＨＹ３０１２、ＭＡＣ３０１１、ドライバ３００７、ブリッジ３００８を経由して、ＩＰスタック３００５に転送する。

【１１０５】

ＩＰスタック３００５は、ブリッジ３００８から受信したフレームのＭＡＣヘッダＦ１１を取り外して、ＩＰルーティング３００４に送る。

【１１０６】

ＩＰルーティング３００４は、受信したフレームのヘッダＦ１２内のＩＰ　ＤＡと、Ｆ１３内の宛先ポート番号を参照し、フレームをＴＣＰ３００３に転送する。

【１１０７】

ＴＣＰ３００３は、ＩＰルーティング３００４からフレームを受信すると、ＴＣＰプロトコルに従ってＴＣＰ２００３にＡＣＫパケットを返送する等の処理を行う。そして、受信したフレームから、ＴＣＰヘッダＦ１３とＩＰヘッダＦ１２を取り外し、データＦ１４をＳＳＬ３００２に転送する。

【１１０８】

ＳＳＬ３００２は、ＴＣＰ３００３からデータＦ１４を受信すると、復号化処理により暗号化を解除し、データＦ１４からＥｔｈｅｒｎｅｔフレームＦ２０、即ち、Ｆ２１～Ｆ２４を取り出し、ゲートウェイアプリケーション３００１Ａに転送する。

【１１０９】

ゲートウェイアプリケーション３００１Ａは、ＳＳＬ３００２からフレームＦ２０を受信すると、このフレームを、そのまま、仮想ＮＩＣ３０１０に流す。

【１１１０】

このフレームは、端末２１からＨＵＢ２２に送信された時の状態のままに保たれており、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスが設定されている。又、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定されている。

【１１１１】

ゲートウェイアプリケーション３００１Ａより仮想ＮＩＣ３０１０に渡されたフレームは、ドライバ３００９、ブリッジ３００８、ＮＩＣ３０１を経由して、ＨＵＢ３２に転送される。

【１１１２】

ＨＵＢ３２は、ゲートウェイ装置３０側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、サーバ３１側のポートに出力する。

【１１１３】

サーバ３１はＨＵＢ３２から送信されたフレームを受信し、ドライバ３１０５、ＩＰスタック３１０４、ＩＰルーティング３１０３、ＴＣＰ３１０２を経由して、フレーム内のデータＦ２４をアプリケーション３１０１に渡す。

【１１１４】

以上のようにして、端末２１内のアプリケーション２１０１からサーバ３１内のアプリケーション３１０１への一連のフレーム転送が完了する。

【１１１５】

上記の例とは逆の経路を辿ることで、サーバ３１内のアプリケーション３１０１から端末２１内のアプリケーション２１０１への一連のフレーム転送も、同様に実現可能である。

【１１１６】

本実施の形態では、ゲートウェイ装置２０側に高速化エンジンを実装する例を示したが、これとは逆に、ゲートウェイ装置３０側に高速化エンジンを実装することも可能である。又、ゲートウェイ装置２０側と、ゲートウェイ装置３０側の両方に、高速化エンジンを実装することも出来る。更に、本実施の形態では、サーバ３１と端末２１の設置場所を入れ替えることも出来る。

【１１１７】

[発明の効果]

次に、本実施の形態の効果について説明する。

本実施の形態に挙げた発明を利用すると、端末２１とサーバ３１との間で、フレームの高速転送が可能になる。

【１１１８】

これは、ゲートウェイ装置２０において、暗号化および復号化の処理をハードウェア化し、ＳＳＬの処理を高速化しているからである。

【１１１９】

[第９の実施の形態]

本発明の第９の実施の形態は、第８の実施の形態に対して、ゲートウェイ装置３０内に中間ドライバＹ３００６が設置され、ゲートウェイ装置２０内の高速化エンジンＸ２０１４が高速化エンジンＹ２０１４に変更され、ゲートウェイ装置２０内のＳＳＬ２００２、及びゲートウェイ装置３０内のＳＳＬ３００２において、暗号化および復号化を行わず、これら処理を高速化エンジンＹ２０１４、及び中間ドライバＹ３００６にて行う点におい

て異なる。

【１１２０】

又、第９の実施の形態も、第８の実施の形態と同様に、ＴＣＰ　ｏｖｅｒ　ＴＣＰに対する対策を行わず、暗号化および復号化処理の高速化に特化した構成になっている。

【１１２１】

第９の実施の形態におけるＨＵＢ２２、ＨＵＢ３２、イントラネット２、イントラネット３、ゲートウェイ装置３０、端末２１、サーバ３１の構成および動作は、第８の実施の形態と同じである。

【１１２２】

第９の実施の形態においては、イントラネット２は、閉域ＬＡＮだけで無く、インターネット等のオープンなＷＡＮを用いても構わない。

【１１２３】

[構成の説明]

図２６は、第９の実施の形態における各機器の構成とフレームの転送経路を詳細に示したブロック図である。

【１１２４】

ゲートウェイ装置２０は、第８の実施の形態におけるゲートウェイ装置２０に対して、高速化エンジンＸ２０１４が高速化エンジンＹ２０１４に変更され、ＳＳＬ２００２が暗号化および復号化を行わずに証明書の交換のみに関与し、ＳＳＬセッションの確立完了後も、ゲートウェイアプリケーション２００１Ａから受信したデータを暗号化せず、そのまま、ＴＣＰ２００３に渡し、又、ＴＣＰ２００３から受信したデータを復号化せず、そのまま、ゲートウェイアプリケーション２００１Ａに渡す点において異なる。

【１１２５】

ゲートウェイ装置３０は、第８の実施の形態におけるゲートウェイ装置３０に対して、中間ドライバＹ３００６が設置され、ＳＳＬ３００２が暗号化および復号化を行わずに証明書の交換のみに関与し、ＳＳＬセッションの確立完了後も、ゲートウェイアプリケーション３００１Ａから受信したデータを暗号化せず、そのまま、ＴＣＰ３００３に渡し、又、ＴＣＰ３００３から受信したデータを復号化せず、そのまま、ゲートウェイアプリケーション３００１Ａに渡す点において異なる。

【１１２６】

端末２１、サーバ３１、ＨＵＢ２２、ＨＵＢ３２、ゲートウェイ装置３０に関しては、第８の実施の形態と同様の構成を有し、同様の動作を行う。

【１１２７】

Ｆｉｒｅｗａｌｌ３３は、第８の実施の形態のＦｉｒｅｗａｌｌ３３と同様の構成を有し、同様の動作を行う。但し、本実施の形態においては、Ｆｉｒｅｗａｌｌ３３の代わりに、ＮＡＴルータやＰｒｏｘｙサーバを用いても良い。

【１１２８】

第９の実施の形態でも、他の実施の形態と同様に、ゲートウェイ装置２０とゲートウェイ装置３０との間で、予め、ＳＳＬセッションを設定している場合のみ、イントラネット２内の機器からイントラネット３内の機器へのアクセスが可能になる。

【１１２９】

図２７は、第９の実施の形態における高速化エンジンＹ２０１４の構成を詳細に示したブロック図である。

【１１３０】

第９の実施の形態における高速化エンジンＹ２０１４は、図１２に示す第１の実施の形態における高速化エンジン２０１４に対して、フラグメント分割２０１４Ｈ、カプセル化２０１４Ｉ、カプセル化解除２０１４Ｊ、フラグメント解除２０１４Ｋが存在しない点において異なる。

【１１３１】

第１の実施の形態における高速化エンジン２０１４では、暗号化および復号化を行うフ

レームが、インタフェース２０１４Ａから入力され、第８の実施の形態における高速化エンジンＸ２０１４では暗号化および復号化を行うフレームがインタフェース２０１４Ｃより入力された。しかしながら、第９の実施の形態における高速化エンジンＹ２０１４では、暗号化を行うフレームはインタフェース２０１４Ｃから入力され、復号化を行うフレームはインタフェース２０１４Ａより入力される。

【１１３２】

第９の実施の形態における高速化エンジンＹ２０１４では、インタフェース２０１４Ａ、インタフェース２０１４Ｃ、暗号化２０１４Ｇ、復号化２０１４Ｌ、制御フレーム送受信部２０１４Ｍは、第１の実施の形態における高速化エンジン２０１４におけるインタフェース２０１４Ａ、インタフェース２０１４Ｃ、暗号化２０１４Ｇ、復号化２０１４Ｌ、制御フレーム送受信部２０１４Ｍと、各々、同様の構成を有し、同様の動作を行う。

【１１３３】

フレーム解析２０１４Ｂは、インタフェース２０１４Ａからフレームを受信し、以下に示す順序で宛先を決定して転送する。

（１） 自ノード宛て、かつ、予め設定されたＳＳＬセッションのフレームであれば、ゲートウェイ装置３０で暗号化されたフレームであれば、フレームを復号化２０１４Ｌに転送する。

（２） （１）以外のフレームであれば、フレームをマルチプレクサ２０１４Ｅに転送する。

【１１３４】

フレーム解析２０１４Ｄは、インタフェース２０１４Ｃからフレームを受信し、以下に示す順序で宛先を決定して転送する。

（１） 高速化エンジンの制御に関わる特殊なフレーム（以降、制御フレームと呼ぶ）である場合は、フレームを制御フレーム送受信部２０１４Ｍに転送する。

（２） 自ノードのＭＡＣ ＳＡが付加されており、かつ、予め設定されたＳＳＬセッションのフレームであれば、フレームを暗号化２０１４Ｇに転送する。

（３） （１）～（２）以外のフレームであれば、マルチプレクサ２０１４Ｆに転送する。

【１１３５】

フレーム解析２０１４Ｄは、特殊フレームであるか否かの判断を、通常はＭＡＣ ＤＡとＭＡＣ ＳＡに基づいて判断する。ＭＡＣ ＤＡ若しくはＭＡＣ ＳＡの何れかに、予め規定したアドレス範囲のＭＡＣアドレス（制御用ＭＡＣアドレスと呼ぶ。例えば、００００４Ｃ０００００００～ＦＦ）が記載されている場合は、フレームを制御フレームと判断する。

【１１３６】

マルチプレクサ２０１４Ｅは、フレーム解析２０１４Ｂおよび制御フレーム送受信部２０１４Ｍ、若しくは復号化２０１４Ｌよりフレームを受信し、必要であれば、キューに保存して送信タイミングを調整し、インタフェース２０１４Ｃに送信する。

【１１３７】

キューに保存するのは、フレーム解析２０１４Ｂ側、復号化２０１４Ｌ、制御フレーム送受信部２０１４Ｍ側の各々から到着するフレームの衝突を避ける為である。

【１１３８】

マルチプレクサ２０１４Ｆは、フレーム解析２０１４Ｄ及び暗号化２０１４Ｇよりフレームを受信し、必要であれば、キューに保存して送信タイミングを調整し、インタフェース２０１４Ａに送信する。キューに保存するのは、制御フレーム解析２０１４Ｄ、更に暗号化２０１４Ｇの各々から到着するフレームの衝突を避ける為である。

【１１３９】

尚、高速化エンジンＹ２０１４は、複数のＳＳＬセッションの暗号化及び復号化を行うこともできる。その為、上記ＩＰアドレス、ポート、公開鍵、秘密鍵および共通鍵などのセッション情報を複数持つことも可能である。

【１１４０】
図２８は、第９の実施の形態における中間ドライバＹ３００６の構成を詳細に示したブロック図である。
【１１４１】
第９の実施の形態における中間ドライバＹ３００６は、図７に示す第１の実施の形態における中間ドライバ１００８に対して、制御フレーム送受信部１００８Ｍ、フラグメント分割１００８Ｂ、フラグメント組立１００８Ｃ、再カプセル化１００８Ｄ、カプセル化解除１００８Ｆ、再カプセル化１００８Ｅ、カプセル化解除１００８Ｇが存在せず、代わりに暗号化Ｙ３００６Ａ及び復号化Ｙ３０６Ｂが設置されている点において異なる。
【１１４２】
第９の実施の形態における中間ドライバＹ３００６は、暗号化Ｙ３００６Ａ、復号化Ｙ３００６Ｂ、フレーム解析Ｙ３００６Ｃ、フレームＹ３００６Ｄ、マルチプレクサＹ３００６Ｅ、マルチプレクサＹ３００６Ｆ、設定管理部Ｙ３００６Ｇで構成される。
【１１４３】
暗号化Ｙ３００６Ａは、フレーム解析Ｙ３００６Ｃよりフレームを受信し、３ＤＥＳ等の方法で暗号化を行い、マルチプレクサＹ３００６Ｅに転送する。暗号化に用いる公開鍵と共通鍵は、設定管理部Ｙ３００６Ｇより通知を受けたものを利用する。
【１１４４】
復号化Ｙ３００６Ｂは、フレーム解析Ｙ３００６Ｄよりフレームを受信し、３ＤＥＳ等の方法で復号化を行い、マルチプレクサＹ３００６Ｆに転送する。復号化に用いる秘密鍵と共通鍵は、設定管理部Ｙ３００６Ｇより通知を受けたものを利用する。
【１１４５】
フレーム解析Ｙ３００６Ｃは、インタフェースＩＰスタック３００５からフレームを受信し、以下に示す（１）～（２）の順序で宛先を決定して転送する。
（１）　自ノードのＭＡＣ　ＳＡが付加されており、かつ、予め設定されたＳＳＬセッションのフレームであれば、フレームを暗号化Ｙ３００６Ａに転送する。
（２）　（１）以外のフレームであれば、マルチプレクサＹ３００６Ｅに転送する。
【１１４６】
フレーム解析Ｙ３００６Ｄは、ブリッジ３００８からフレームを受信し、以下に示す順序で宛先を決定して転送する。
（１）　自ノード宛て、かつ、予め設定されたＳＳＬセッションのフレームであれば、フレームを復号化Ｙ３００６Ｂに転送する。
（２）　（１）以外のフレームであれば、フレームをマルチプレクサＹ３００６Ｆに転送する。
【１１４７】
マルチプレクサＹ３００６Ｅは、フレーム解析Ｙ３００６Ｃと、暗号化Ｙ３００６Ａからフレームを受信し、ブリッジ３００８に転送する。この際、フレームの同時到着により欠落が発生しないよう、バッファ動作を行う。
【１１４８】
マルチプレクサＹ３００６Ｆは、フレーム解析Ｙ３００６Ｄ及び復号化Ｙ３００６Ｂよりフレームを受信し、必要であれば、キューに保存して送信タイミングを調整し、ＩＰスタック３００５に送信する。キューに保存するのは、フレーム解析Ｙ３００６Ｄ、復号化Ｙ３００６Ｂ側の各々から到着するフレームの衝突を避ける為である。
【１１４９】
設定管理部Ｙ３００６Ｇは、ゲートウェイアプリケーション３００１Ａより、高速化処理に関連するセッションの情報（ＩＰアドレス、ポート番号等）の通知を受けてフレーム解析Ｙ３００６Ｃ及びフレーム解析Ｙ３００６Ｄの設定を行い、又、ゲートウェイアプリケーション３００１Ａ若しくはＳＳＬ３００２より暗号化用の公開鍵と復号化用の秘密鍵、さらには共通鍵の通知を受けて、暗号化Ｙ３００６Ａ及び復号化Ｙ３００６Ｂの設定を行う。

【１１５０】
尚、中間ドライバＹ３００６は複数のＳＳＬセッションの暗号化及び復号化を行うことも出来る。その為、上記ＩＰアドレス、ポート、公開鍵、秘密鍵および共通鍵などのセッション情報を複数持つことも可能である。
【１１５１】
[動作の説明]
[ＳＳＬセッションの確立動作]
図２６を用いて、第９の実施の形態において、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合を例に挙げて、動作の説明を行う。
【１１５２】
この際、ブリッジ２００８、ブリッジ３００８、ＨＵＢ２２やＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３のＬＡＮ側、Ｆｉｒｅｗａｌｌ３３のＷＡＮ側、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。
【１１５３】
又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間のゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。
【１１５４】
ゲートウェイ装置３０内のゲートウェイアプリケーション３００１Ａは、ユーザからのゲートウェイ装置２０内のゲートウェイアプリケーション２００１Ａへの接続要求を受け、ＳＳＬ３００２にゲートウェイ装置２０内のゲートウェイアプリケーション２００１Ａへの通信開始を指示する。
【１１５５】
ＳＳＬ３００２は、ゲートウェイアプリケーション３００１Ａからの通信開始指示を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為に、ＴＣＰ３００３にゲートウェイ装置２０内のゲートウェイアプリケーション２００１Ａへの通信開始を指示する。
【１１５６】
ＴＣＰ３００３は、ＳＳＬ３００２からの通信開始指示を受け、ＴＣＰ２００３との間でＴＣＰセッションを確立する為に、ＩＰルーティング３００４に対して、ＴＣＰ２００３とのＴＣＰセッション確立要求パケット（ＳＹＮ）を送信する。このＴＣＰセッション確立要求パケットはＴＣＰ規格に沿ったものであり、宛先ＩＰアドレスにゲートウェイ装置２０宛、宛先ポート番号にＴＣＰ２００３が設定される。
【１１５７】
ＩＰルーティング３００４は、ＴＣＰ３００３から受信したパケットの宛先ＩＰアドレスと宛先ポート番号を参照し、パケットをＩＰスタック３００５に転送する。
【１１５８】
ＩＰスタック３００５は、ＩＰルーティング３００４より受信したパケットに、Ｆｉｒｅｗａｌｌ３３内のイントラネット３側のＭＡＣアドレスを宛先ＭＡＣアドレスとして付加し、更に送信元ＭＡＣアドレスに自ノードのＭＡＣアドレスを設定してフレームが生成され、中間ドライバＹ３００６に転送する。
【１１５９】
中間ドライバＹ３００６は、ＩＰスタックからＴＣＰセッション確立要求フレームを受信してヘッダ解析を行う。解析の結果、暗号化が必要なフレームではない為、このフレームを、そのまま、ブリッジ３００８を経由してドライバ３００７に転送する。
【１１６０】
ドライバ３００７は、ＩＰスタック３００５からフレームを受信し、ＭＡＣ３０１１に転送する。
【１１６１】

ＭＡＣ３０１１は、ドライバ３００７からフレームを受信し、ＰＨＹ３０１２に転送する。

【１１６２】

ＰＨＹ３０１２は、ＭＡＣ３０１１からフレームを受信し、ポート３０１３に転送する。

【１１６３】

ポート３０１３は、ＰＨＹ３０１２からフレームを受信し、イーサネットケーブルを経由してＨＵＢ３２に転送する。

【１１６４】

ＨＵＢ３２は、フレームを受信すると、ＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＬＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３側のポートに出力する。

【１１６５】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からフレームを受信し、ゲートウェイ装置３０からゲートウェイ装置２０への通信の為、これを許可し、ＨＵＢ２２に転送する。

【１１６６】

ＨＵＢ２２は、Ｆｉｒｅｗａｌｌ３３からフレームを受信し、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０に転送する。

【１１６７】

ゲートウェイ装置２０は、ＨＵＢ２２内からフレームを受信し、ポート２０１３、ＰＨＹ２０１２、ＭＡＣ２０１１、ドライバ２００７、ブリッジ２００８の経路で転送し、ＩＰスタック２００５に転送する。

【１１６８】

ＩＰスタック２００５は、ブリッジ２００８からフレームを受信し、ＭＡＣヘッダを外してパケットにしてＩＰルーティング２００４に転送する。

【１１６９】

ＩＰルーティング２００４は、ＩＰスタック２００５より受信したパケットの宛先ポート番号を参照し、ＴＣＰ２００３側のポート番号が付加されていることから、このパケットをＴＣＰ２００３に転送する。

【１１７０】

ＴＣＰ２００３は、ＩＰルーティング２００４よりパケットを受信する。このパケットは、ＴＣＰセッション確立要求パケット（ＳＹＮ）であるので、ＴＣＰプロトコルに従い、セッション確立要求に対して、セッション確立の為に必要な応答パケット（ＳＹＮ＋ＡＣＫ）をＴＣＰ３００３宛てに送信する。すなわち、応答パケットの宛先ＩＰはゲートウェイ装置３０のＩＰアドレスが設定され、応答パケットの宛先ポートはＴＣＰ３００３のポート番号が設定される。

【１１７１】

応答パケットは、ＩＰルーティング２００４、ＩＰスタック２００５、ブリッジ２００８、ドライバ２００７、ＮＩＣ２０１、ＨＵＢ２２、Ｆｉｒｅｗａｌｌ３３、ＨＵＢ３２、ＮＩＣ３０１を経由して、ＣＰＵ３００に到達し、更に、ドライバ３００７、ブリッジ３００８、ＩＰスタック３００５、ＩＰルーティング３００４を経由し、ＴＣＰ３００３に到達する。

【１１７２】

ＴＣＰ３００３は、ＩＰルーティング３００４よりパケットを受信する。このパケットは、ＴＣＰセッションの確立要求に対する応答パケットであるので、この応答パケットに対するＡＣＫパケットをＴＣＰ２００３を宛先に設定して送信する。更に、ＳＳＬ３００２に対して、ＴＣＰ２００３とのＴＣＰセッション接続完了を通知する。

【１１７３】

ＳＳＬ３００２は、ＴＣＰ３００３からの接続完了通知を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為、ＳＳＬプロトコルに従い、セッション確立要求の為の

パケット（ＳＳＬセッション確立要求パケット）を送信する。

【１１７４】

ＳＳＬセッション確立要求パケットは、ＴＣＰ３００３で受信されると、ＴＣＰ３００３とＴＣＰ２００３との間で設定されたＴＣＰセッションを通り、ＮＩＣ３０１、ＨＵＢ３２、Ｆｉｒｅｗａｌｌ３３、ＨＵＢ２２、ＮＩＣ２０１を経由して、ＴＣＰ２００３に到着する。

【１１７５】

ＴＣＰ２００３は、パケットをＳＳＬ２００２に転送する。

【１１７６】

ＳＳＬ２００２は、ＳＳＬセッション確立要求の内容を検証し、問題が無ければ、ゲートウェイアプリケーション２００１Ａに対して、ＳＳＬ３００２とのセッション確立を通知すると同時に、ＳＳＬプロトコルに従い、ＳＳＬ３００２に対してＳＳＬセッション確立応答パケットを送信する。

【１１７７】

ＳＳＬセッション確立応答パケットは、ＳＳＬセッション確立要求パケットとは逆の経路、即ち、ＴＣＰ２００３とＴＣＰ３００３との間のＴＣＰセッションを経由して、ＳＳＬ３００２に到達する。

【１１７８】

ＳＳＬ２００２は、ＳＳＬ２００２の秘密鍵、ＳＳＬ３００２の公開鍵、ＳＳＬ２００２とＳＳＬ３００２の共通鍵、ＳＳＬセッションの相手方機器のＩＰアドレス（ゲートウェイ装置３０のＩＰアドレス）、ＳＳＬセッションの相手方機器の宛先ポート（ＴＣＰ３００３のポート）、自ノード側のＳＳＬセッションの送信元ポート番号（ＴＣＰ２００３のポート）、送信元ＩＰアドレス（ゲートウェイ装置２０のＩＰアドレス）、及び開始命令を制御フレームに載せ、仮想ＮＩＣ２０１０に制御フレームを送信する。

【１１７９】

制御フレームは、ＳＳＬ２００２を出ると、仮想ＮＩＣ２０１０、ドライバ２００９、ブリッジ２００８、ドライバ２００７、ＭＡＣ２１１１を経由して、高速化エンジンＹ２０１４に到着する。

【１１８０】

高速化エンジンＹ２０１４は、ＭＡＣアドレス等により制御フレームを判別し、制御フレーム送受信部で受信する。そして、公開鍵、秘密鍵および共通鍵を、各々、復号化および暗号化に使用する為に保存し、ＩＰアドレスやポート番号をフレーム解析の為に保存する。そして、高速化処理開始命令を受け、フレーム解析、暗号化、及び複号化の処理を開始する。

【１１８１】

ＳＳＬ３００２は、ＳＳＬセッション確立応答の内容をＳＳＬプロトコルに従い検証し、問題が無ければ、ゲートウェイアプリケーション３００１Ａに対して、ＳＳＬ３００２とＳＳＬ２００２との間のＳＳＬセッション確立を通知する。

【１１８２】

ＳＳＬ３００２は、ＳＳＬ３００２の秘密鍵、ＳＳＬ２００２の公開鍵、ＳＳＬ３００２とＳＳＬ２００２の間の共通鍵、ＳＳＬセッションの相手方機器のＩＰアドレス（ゲートウェイ装置２０のＩＰアドレス）、ＳＳＬセッションの相手方機器の宛先ポート（ＴＣＰ２００３のポート）、自ノード側のＳＳＬセッションの送信元ポート番号（ＴＣＰ３００３のポート）、送信元ＩＰアドレス（ゲートウェイ装置３０のＩＰアドレス）、及び開始命令を、中間ドライバＹ３００６に通知する。

【１１８３】

中間ドライバＹ３００６は、ＳＳＬ３００２から通知を受けた公開鍵、秘密鍵および共通鍵を、各々、復号化および暗号化に使用するため保存し、ＩＰアドレスやポート番号をフレーム解析の為に保存する。そして、高速化処理開始命令を受け、フレーム解析、暗号化および複号化の処理を開始する。

【１１８４】
以上のようにして、ＳＳＬ２００２とＳＳＬ３００２との間で、ＳＳＬセッションが確立される。
【１１８５】
以上により、第９の実施の形態において、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合の動作が完了する。
【１１８６】
[端末２１からサーバ３１へのフレーム転送動作]
図２６を用いて、第９の実施の形態において、端末２１からサーバ３１へフレームを送信する場合を例に挙げて、動作の説明を行う。
【１１８７】
この際、ブリッジ２００８、ブリッジ３００８、ＨＵＢ２２、ＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。
【１１８８】
又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０との間の通信は双方向で許可するが、端末２１とサーバ３１との間のゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。
【１１８９】
更に、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）が、上述の動作例により、既に、設定されているものとする。
【１１９０】
又、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション３１０１との間で、既にＴＣＰセッションが構築されているとする。
【１１９１】
端末２１内のアプリケーション２１０１が、サーバ３１内のアプリケーション３１０１宛のデータを、ＴＣＰ２１０２に渡す。
【１１９２】
ＴＣＰ２１０２は、アプリケーション２１０１からデータを受け取り、ＴＣＰプロトコルに従ってＴＣＰヘッダ（図２におけるＦ２３）やＩＰヘッダ（図２におけるＦ２２）を付けてＩＰパケットとし、ＩＰルーティング２１０３に渡す。この時、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡにはサーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには端末２１のＩＰアドレスが設定される。
【１１９３】
ＩＰルーティング２１０３は、ＴＣＰ２１０２から受信したパケットの宛先ＩＰアドレス（サーバ３１宛て）および宛先ポート（ＴＣＰ３１０２宛て）を参照し、データを、そのまま、ＩＰスタック２１０４に転送する。
【１１９４】
ＩＰスタック２１０４は、ＩＰルーティング２１０３からパケットを受信し、ＭＡＣヘッダ（図２におけるＦ２１）を付けてＥｔｈｅｒｎｅｔフレームを作成し、ドライバ２１０５に渡す。このフレームはＥｔｈｅｒｎｅｔフレームＦ２０のフォーマットを有する。この時、ＩＰスタック２１０４は、ＡＲＰの結果を参照して、フレームのＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスを設定し、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスを設定する。
【１１９５】
ドライバ２１０５は、ＩＰスタック２１０５より上記フレームを受け取り、ＮＩＣ２１１に転送する。
【１１９６】
ＮＩＣ２１１は、ドライバ２１０５よりフレームを受け取り、ＭＡＣ２１１１、ＰＨＹ

２１１２、ポート２１１３を経由して、ＨＵＢ２２にフレームを転送する。

【１１９７】

ＨＵＢ２２は、端末２１のＮＩＣ２１１側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０側のポートに出力する。

【１１９８】

ゲートウェイ装置２０は、ＨＵＢ２２からのフレームをポート２０１３において受け取り、ＰＨＹ２０１２、ＭＡＣ２０１１、ドライバ２００７を経由して、ブリッジ２００８に渡す。

【１１９９】

ブリッジ２００８は、ドライバ２００７から受信したフレーム（フレームフォーマットＦ２０形式）内のヘッダＦ２１内に存在するＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のＭＡＣアドレスであり、ゲートウェイ装置２０のＭＡＣアドレスでは無いことから、フレームをドライバ２００９に転送する。

【１２００】

ブリッジ２００８から送信されたフレームは、ドライバ２００９、仮想ＮＩＣ２０１０を経由し、ゲートウェイアプリケーション２００１Ａに転送される。

【１２０１】

ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したフレームを、ゲートウェイアプリケーション２００１Ａとゲートウェイアプリケーション３００１Ａとの間に設定したＳＳＬセッションに流す。

【１２０２】

すなわち、ゲートウェイアプリケーション２００１Ａは、仮想ＮＩＣ２０１０から受信したＥｔｈｅｒｎｅｔフレーム（フレームフォーマットＦ２０）をデータとしてＳＳＬ２００２に渡す。

【１２０３】

ＳＳＬ２００２は、ゲートウェイアプリケーション２００１Ａから未暗号化のデータＦ１４（Ｆ２１～Ｆ２４）を受け取ると、暗号化処理を行わず、そのまま、ＴＣＰ２００３に転送する。

【１２０４】

ＴＣＰ２００３は、ＳＳＬ２００２よりデータＦ１４を受け取り、ＴＣＰヘッダＦ１３、及びＩＰヘッダＦ１２を付けて、ＩＰルーティング２００４に渡す。

【１２０５】

ここで、Ｆ１２内のＩＰ　ＤＡにはゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡにはゲートウェイ装置２０のＩＰアドレスが設定される。又、宛先ポートにはＴＣＰ３００３のポートが設定され、送信元ポートにはＴＣＰ２００３のポートが指定される。

【１２０６】

ＩＰルーティング２００４は、ＴＣＰ２００３より受信したデータのＩＰヘッダＦ１２内のＩＰアドレス等を参照し、フレームをＩＰスタック２００５に渡す。

【１２０７】

ＩＰスタック２００５は、ＩＰルーティング２００４よりフレームを受信し、フレームにＭＡＣヘッダＦ１１を付けて、Ｅｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームフォーマットＦ１０の形式にして、ブリッジ２００８に渡す。

【１２０８】

ここで、ＡＲＰの結果より、Ｆ１１内のＭＡＣ　ＤＡにはＦｉｒｅｗａｌｌ　３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはゲートウェイ装置２０のＭＡＣアドレスが設定される。

【１２０９】

ＩＰスタック２００５より送信されたフレームは、ブリッジ２００８、ドライバ２００７、ＭＡＣ２０１１を経由して、高速化エンジンＹ２０１４に送られる。

【１２１０】

高速化エンジンＹ２０１４は、インタフェース２０１４Ｃにおいてフレームを受け取り、フレーム解析Ｙ２０１４Ｄで受信フレームが、予め、ＳＳＬ２００２より通知されたＳＳＬセッションのフレームだと判別し、データＦ１４の暗号化を行う。そして、マルチプレクサ２０１４Ｆを経由して、ＰＨＹ２０１２に転送する。この時、フレームのヘッダＦ１１～Ｆ１３には変更を加えない。

【１２１１】

高速化エンジンＹ２０１４を出たフレームは、ＰＨＹ２０１２、ポート２０１３を経由して、ＨＵＢ２２に送られる。

【１２１２】

ＨＵＢ２２は、ゲートウェイ装置２２側のポートからフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＷＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３に出力する。

【１２１３】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からのフレームを受信し、ＩＰ　ＤＡを参照してＭＡＣヘッダＦ１１を変更し、受信フレームをフレームフォーマットＦ１０の形のままＨＵＢ３２に転送する。

【１２１４】

ここで、Ｆ１１内のＭＡＣ　ＤＡにはゲートウェイ装置３０のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＬＡＮ側のＭＡＣアドレスが設定される。

【１２１５】

ＨＵＢ３２は、Ｆｉｒｅｗａｌｌ３３からのフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがゲートウェイ装置３０のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置３０側のポートに出力する。

【１２１６】

ゲートウェイ装置３０は、ＨＵＢ３２からのフレームをポート３０１３より受信すると、ＰＨＹ３０１２、ＭＡＣ３０１１、ドライバ３００７、ブリッジ３００８を経由して、中間ドライバＹ３００６に転送する。

【１２１７】

中間ドライバＹ３００６は、ブリッジ３００８よりフレームを受け取り、フレーム解析Ｙ３００６Ｄで受信フレームが、予め、ＳＳＬ３００２より通知されたＳＳＬセッションのフレームだと判別し、データＦ１４の復号化を行う。そして、復号化処理によりデータＦ１４の暗号化を解除した後、マルチプレクサＹ３００６Ｆを経由して、ＩＰスタック３００５に転送する。この時、フレームのヘッダＦ１１～Ｆ１３には変更を加えない。

【１２１８】

ＩＰスタック３００５は、中間ドライバＹ３００６から受信したフレームのＭＡＣヘッダＦ１１を取り外して、ＩＰルーティング３００４に送る。

【１２１９】

ＩＰルーティング３００４は、受信したフレームのヘッダＦ１２内のＩＰ　ＤＡと、Ｆ１３内の宛先ポート番号を参照し、フレームをＴＣＰ３００３に転送する。

【１２２０】

ＴＣＰ３００３は、ＩＰルーティング３００４からフレームを受信すると、ＴＣＰプロトコルに従ってＡＣＫパケットを返送する等の処理を行う。そして、受信したフレームから、ＴＣＰヘッダＦ１３とＩＰヘッダＦ１２を取り外し、データＦ１４をＳＳＬ３００２に転送する。

【１２２１】
ＳＳＬ３００２は、ＴＣＰ３００３からデータＦ１４を受信すると、復号化などの処理をせず、そのまま、ゲートウェイアプリケーション３００１Ａに転送する。
【１２２２】
ゲートウェイアプリケーション３００１Ａは、ＳＳＬ３００２からフレームＦ２０を受信すると、このフレームを、そのまま、仮想ＮＩＣ３０１０に流す。
【１２２３】
このフレームは、端末２１からＨＵＢ２２に送信された時の状態のままに保たれており、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスが設定されている。又、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡにはサーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには端末２１のＩＰアドレスが設定されている。
【１２２４】
ゲートウェイアプリケーション３００１Ａより仮想ＮＩＣ３０１０に渡されたフレームは、ドライバ３００９、ブリッジ３００８、ＮＩＣ３０１を経由して、ＨＵＢ３２に転送される。
【１２２５】
ＨＵＢ３２は、ゲートウェイ装置３０側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、サーバ３１側のポートに出力する。
【１２２６】
サーバ３１はＨＵＢ３２から送信されたフレームを受信し、ドライバ３１０５、ＩＰスタック３１０４、ＩＰルーティング３１０３、ＴＣＰ３１０２を経由して、フレーム内のデータＦ２４をアプリケーション３１０１に渡す。
【１２２７】
以上のようにして、端末２１内のアプリケーション２１０１からサーバ３１内のアプリケーション３１０１への一連のフレーム転送が完了する。
【１２２８】
上記の例とは逆の経路を辿ることで、サーバ３１内のアプリケーション３１０１から端末２１内のアプリケーション２１０１への一連のフレーム転送も、同様に、実現可能である。
【１２２９】
本実施の形態では、ゲートウェイ装置２０側に高速化エンジンを実装し、ゲートウェイ装置３０側に中間ドライバを実装する例を示したが、これとは逆に、ゲートウェイ装置３０側に高速化エンジンを実装し、ゲートウェイ装置２０側に中間ドライバを実装することも可能である。又、ゲートウェイ装置２０側と、ゲートウェイ装置３０側の両方に、高速化エンジンを実装し、中間ドライバを一切使用しないようにすることも出来る。更に、ゲートウェイ装置２０側とゲートウェイ装置３０側の両方に中間ドライバを実装し、高速化エンジンを使用しないようにすることも出来る。更に、本実施の形態では、サーバ３１と端末２１の設置場所を入れ替えることも出来る。
【１２３０】
[発明の効果]
次に、本実施の形態の効果について説明する。
実施の形態に挙げた発明を利用すると、端末２１とサーバ３１との間で、フレームの高速転送が可能になる。
【１２３１】
これは、ゲートウェイ装置２０において、ＳＳＬセッションを用いて通信する際のデータの暗号化および復号化の処理をハードウェア化し、ＳＳＬの処理を高速化しているから

である。

【１２３２】

又、本実施の形態に挙げた発明を利用すると、高速化処理の為のハードウェア（高速化エンジン）の開発費用や部材費用を、比較的低く抑えることが出来る。

【１２３３】

これは、比較的安価なＭＡＣとＰＨＹとの間のインタフェースに、高速化処理の為のハードウェア（高速化エンジン）を実装することが出来るからである。

【１２３４】

又、これは、ハードウェアへの実装が難しいＴＣＰ処理をソフトウェアに残し、ハードウェアへの実装が比較的容易で、かつ、高速化処理の効果が大きな、暗号化／復号化のみをハードウェア処理できるからである。

【１２３５】

[第１０の実施の形態]

本発明の第１０の実施の形態は、第９の実施の形態に対して、ゲートウェイ装置２０内の処理を、端末２１内に設置した中間ドライバＺ２１０６において行う点で異なる。

又、ゲートウェイ装置２０およびゲートウェイ装置３０が無い為、ＨＵＢ２２およびＨＵＢ３３を廃止し、端末２１とＦｉｒｅｗａｌｌ３３のＷＡＮ側を、直接、接続し、サーバ３１とＦｉｒｅｗａｌｌ３３のＬＡＮ側も、直接、接続するようにした。

【１２３６】

又、第１０の実施の形態も、第９の実施の形態と同様に、ＴＣＰ　ｏｖｅｒ　ＴＣＰに対する対策を行わず、ＳＳＬセッションを用いて通信する際のデータの暗号化および復号化処理の高速化に特化した構成になっている。

【１２３７】

第１０の実施の形態においては、イントラネット２は、閉域ＬＡＮだけでなく、インターネット等のオープンなＷＡＮを用いても構わない。

【１２３８】

[構成の説明]

図２９は、第１０の実施の形態における各機器の構成とフレームの転送経路を詳細に示したブロック図である。

端末２１は、第９の実施の形態における端末２１に対して、中間ドライバＺ２１０６が追加されており、中間ドライバＺ２１０６内において、ゲートウェイ装置２０と同様の動作を行う。又、ＮＩＣ２１１が、第９の実施の形態におけるゲートウェイ装置２０内に存在するＮＩＣ２０１に変更されている点において異なる。

【１２３９】

中間ドライバＺ２１０６は、ゲートウェイアプリケーション２００１Ａ、ＳＳＬ２００２、ＴＣＰ２００３、ＩＰルーティング２００４、ＩＰスタック２００５で構成される。上記各部分は、第９の実施の形態のゲートウェイ装置２０内の、ゲートウェイアプリケーション２００１Ａ、ＳＳＬ２００２、ＴＣＰ２００３、ＩＰルーティング２００４、ＩＰスタック２００５と、各々、同様の構成を有し、同様の動作を行う。

【１２４０】

ＮＩＣ２０１は、第９の実施の形態のゲートウェイ装置２０内のＮＩＣ２０１と同様の構成を有し、同様の動作を行う。

【１２４１】

サーバ３１は、第９の実施の形態におけるサーバ３１に対して、中間ドライバＺ３１０６が追加されており、中間ドライバＺ３１０６内において、ゲートウェイ装置３０と同様の動作を行う。

【１２４２】

中間ドライバＺ３１０６は、ゲートウェイアプリケーション３００１Ａ、ＳＳＬ３００２、ＴＣＰ３００３、ＩＰルーティング３００４、ＩＰスタック３００５、中間ドライバＹ３００６で構成される。上記各部分は、第９の実施の形態のゲートウェイ装置３０内の

、ゲートウェイアプリケーション３００１Ａ、ＳＳＬ３００２、ＴＣＰ３００３、ＩＰルーティング３００４、ＩＰスタック３００５、中間ドライバＹ３００６と、各々、同様の構成を有し、同様の動作を行う。

【１２４３】

Ｆｉｒｅｗａｌｌ３３は、第９の実施の形態のＦｉｒｅｗａｌｌ３３と同様の構成を有し、同様の動作を行う。但し、本実施の形態においては、Ｆｉｒｅｗａｌｌ３３の代わりに、ＮＡＴルータやＰｒｏｘｙサーバを用いても良い。

【１２４４】

第１０の実施の形態でも、他の実施の形態と同様に、ゲートウェイ装置２０とゲートウェイ装置３０との間で、予めＳＳＬセッションを設定している場合のみ、イントラネット２内の機器からイントラネット３内の機器へのアクセスが可能になる。

【１２４５】

［動作の説明］

［ＳＳＬセッションの確立動作］

図２９を用いて、第１０の実施の形態において、サーバ３１から端末２１へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合を例に挙げて、動作の説明を行う。

【１２４６】

この際、Ｆｉｒｅｗａｌｌ３３は、端末２１のＩＰスタック２００５とサーバ３１のＩＰスタック３００５の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ＩＰスタック２００５やＩＰスタック３００５を介さない直接の通信は双方向で遮断するとする。

【１２４７】

サーバ３１内のゲートウェイアプリケーション３００１Ａは、ユーザからの端末２１内のゲートウェイアプリケーション２００１Ａへの接続要求を受け、ＳＳＬ３００２に端末２１内のゲートウェイアプリケーション２００１Ａへの通信開始を指示する。

【１２４８】

ＳＳＬ３００２は、ゲートウェイアプリケーション３００１Ａからの通信開始指示を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為に、ＴＣＰ３００３に端末２１内のゲートウェイアプリケーション２００１Ａへの通信開始を指示する。

【１２４９】

ＴＣＰ３００３は、ＳＳＬ３００２からの通信開始指示を受け、ＴＣＰ２００３との間でＴＣＰセッションを確立する為に、ＩＰルーティング３００４に対して、ＴＣＰ２００３とのＴＣＰセッション確立要求パケット（ＳＹＮ）を送信するために、ＴＣＰ規格に沿ったセッション確立要求パケットを生成する。このパケットは、宛先ＩＰアドレスとして端末２１のＩＰスタック２００４側宛、宛先ポート番号にＴＣＰ２００３が設定されている。

【１２５０】

ＩＰルーティング３００４は、ＴＣＰ３００３から受信したパケットの宛先ＩＰアドレスと宛先ポート番号を参照し、パケットをＩＰスタック３００５に転送する。

【１２５１】

ＩＰスタック３００５は、ＩＰルーティング３００４より受信したパケットに、Ｆｉｒｅｗａｌｌ３３内のイントラネット３側のＭＡＣアドレスを宛先ＭＡＣアドレスとして付加し、更に送信元ＭＡＣアドレスに自ノードのＭＡＣアドレスを設定してフレームを生成して、中間ドライバＹ３００６に転送する。

【１２５２】

中間ドライバＹ３００６は、ＩＰスタック３００５からフレームを受信してヘッダ解析を行う。解析の結果、暗号化が必要なフレームでは無い為、このフレームを、そのまま、ドライバ３１０５に転送する。

【１２５３】

ドライバ３１０５は、中間ドライバＹ３００６からフレームを受信し、ＭＡＣ３１１１に転送する。

【１２５４】

ＭＡＣ３１１１は、ドライバ３１０５からフレームを受信し、ＰＨＹ３１１２に転送する。

【１２５５】

ＰＨＹ３１１２は、ＭＡＣ３１１１からフレームを受信し、ポート３１１３に転送する。

【１２５６】

ポート３１１３は、ＰＨＹ３１１２からフレームを受信し、イーサネットケーブルを経由してＦｉｒｅｗａｌｌ３３に転送する。

【１２５７】

Ｆｉｒｅｗａｌｌ３３は、サーバ３１からフレームを受信し、サーバ３１から端末２１への通信の為、これを許可し、端末２１に転送する。

【１２５８】

端末２１は、Ｆｉｒｅｗａｌｌ３３からフレームを受信し、ポート２０１３、ＰＨＹ２０１２、高速化エンジンＹ２０１４、ＭＡＣ２０１１、ドライバ２１０５の経路でパ転送し、ＩＰスタック２００５に転送する。この時、高速化エンジンＹ２０１４は、ＰＨＹから受信したフレームをそのままＭＡＣに流す。

【１２５９】

ＩＰスタック２００５は、ブリッジ２００８からパケットを受信し、ＭＡＣヘッダを外してパケットにしてＩＰルーティング２００４に転送する。

【１２６０】

ＩＰルーティング２００４は、ＩＰスタック２００５より受信したパケットの宛先ポート番号を参照し、ＴＣＰ２００３側のポート番号が付加されていることから、このパケットをＴＣＰ２００３に転送する。

【１２６１】

ＴＣＰ２００３は、ＩＰルーティング２００４よりパケットを受信する。このパケットは、ＴＣＰセッション確立要求パケット（ＳＹＮ）であるので、ＴＣＰプロトコルに従い、ＴＣＰセッション確立要求に対して、応答パケット（ＳＹＮ＋ＡＣＫ）を生成してＴＣＰ３００３宛てに送信する。すなわち、応答パケットの宛先ＩＰはサーバ３１のＩＰスタック３００５のＩＰアドレスが設定され、応答パケットの宛先ポートは、ＴＣＰ３００３のポート番号が設定される。

【１２６２】

応答パケットは、ＩＰルーティング２００４、ＩＰスタック２００５、ドライバ２１０５、ＮＩＣ２０１、Ｆｉｒｅｗａｌｌ３３、ＮＩＣ３１１を経由してＣＰＵ３１０に到達し、更にドライバ３１０５、ＩＰスタック３００５、ＩＰルーティング３００４を経由し、ＴＣＰ３００３に到達する。

【１２６３】

ＴＣＰ３００３は、ＩＰルーティング３００４よりパケットを受信する。このパケットは、ＴＣＰセッションの確立要求に対する応答パケットであるので、この応答パケットに対するＡＣＫパケットをＴＣＰ２００３に送信する。更にＳＳＬ３００２に対して、ＴＣＰ２００３とのＴＣＰセッション接続完了を通知する。

【１２６４】

ＳＳＬ３００２は、ＴＣＰ３００３からの接続完了通知を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為、ＳＳＬプロトコルに従い、セッション確立要求の為のパケット（ＳＳＬセッション確立要求パケット）を送信する。

【１２６５】

ＳＳＬセッション確立要求パケットは、ＴＣＰ３００３で受信されると、ＴＣＰ３００３とＴＣＰ２００３との間で設定されたＴＣＰセッションを通り、ＮＩＣ３１１、Ｆｉｒ

ｅｗａｌｌ３３、ＮＩＣ２０１を経由して、ＴＣＰ２００３に到着する。

【１２６６】

ＴＣＰ２００３は、ＳＳＬセッション確立要求パケットをＳＳＬ２００２に転送する。

【１２６７】

ＳＳＬ２００２は、ＳＳＬセッション確立要求の内容を検証し、問題が無ければ、ゲートウェイアプリケーション２００１Ａに対して、ＳＳＬ３００２とのセッション確立を通知すると同時に、ＳＳＬプロトコルに従い、ＳＳＬ３００２に対してＳＳＬセッション確立応答パケットを送信する。

【１２６８】

ＳＳＬセッション確立応答パケットは、ＳＳＬセッション確立要求パケットとは逆の経路、即ち、ＴＣＰ２００３とＴＣＰ３００３との間のＴＣＰセッションを経由して、ＳＳＬ３００２に到達する。

【１２６９】

ＳＳＬ２００２は、ＳＳＬ２００２の秘密鍵、ＳＳＬ３００２の公開鍵、ＳＳＬ２００２とＳＳＬ３００２の間の共通鍵、ＳＳＬセッションの相手方機器のＩＰアドレス（サーバ３１のＩＰルーティング３００４側のＩＰアドレス）、ＳＳＬセッションの相手方機器の宛先ポート（ＴＣＰ３００３のポート）、自ノード側のＳＳＬセッションの送信元ポート番号（ＴＣＰ２００３のポート）、送信元ＩＰアドレス（端末２１のＩＰルーティング２００４側のＩＰアドレス）、及び開始命令を制御フレームに載せ、高速化エンジンＹ２０１４に制御フレームを送信する。

【１２７０】

制御フレームは、ＳＳＬ２００２を出ると、ドライバ２１０５、ＭＡＣ２０１１を経由して、高速化エンジンＹ２０１４に到着する。

【１２７１】

高速化エンジンＹ２０１４は、ＭＡＣアドレス等により制御フレームを判別し、制御フレーム送受信部で受信する。そして、公開鍵、秘密鍵および共通鍵を、各々、復号化および暗号化に使用する為に保存し、ＩＰアドレスやポート番号をフレーム解析の為に保存する。そして、高速化処理開始命令を受け、フレーム解析、暗号化、及び複号化の処理を開始する。

【１２７２】

ＳＳＬ３００２は、ＳＳＬセッション確立応答の内容をＳＳＬプロトコルに従い検証し、問題が無ければ、ゲートウェイアプリケーション３００１Ａに対して、ＳＳＬ３００２とＳＳＬ２００２との間のＳＳＬセッション確立を通知する。

【１２７３】

又、ＳＳＬ３００２は、ＳＳＬ３００２の秘密鍵、ＳＳＬ２００２の公開鍵、ＳＳＬ２００２とＳＳＬ３００２の間の共通鍵、ＳＳＬセッションの相手方機器のＩＰアドレス（端末２１のＩＰアドレス）、ＳＳＬセッションの相手方機器の宛先ポート（ＴＣＰ２００３のポート）、自ノード側のＳＳＬセッションの送信元ポート番号（ＴＣＰ３００３のポート）、送信元ＩＰアドレス（サーバ３１のＩＰアドレス）、及び開始命令を、中間ドライバＹ３００６に通知する。

【１２７４】

中間ドライバＹ３００６は、ＳＳＬ３００２から通知を受けた公開鍵、秘密鍵および共通鍵を、各々、復号化および暗号化に使用する為に保存し、ＩＰアドレスやポート番号をフレーム解析の為に保存する。そして、高速化処理開始命令を受け、フレーム解析、暗号化、及び複号化の処理を開始する。

【１２７５】

以上のようにして、ＳＳＬ２００２とＳＳＬ３００２との間で、ＳＳＬセッションが確立される。

【１２７６】

以上により、第１０の実施の形態において、サーバ３１から端末２１へのＳＳＬセッシ

ョン（セキュアＴＣＰセッション）を確立する場合の動作が完了する。

【１２７７】

［端末２１からサーバ３１へのフレーム転送動作］

図２９を用いて、第１０の実施の形態において、端末２１からサーバ３１へフレームを送信する場合を例に挙げて、動作の説明を行う。

【１２７８】

この際、Ｆｉｒｅｗａｌｌ３３は、端末２１のＩＰスタック２００５とサーバ３１のＩＰスタック３００５の間の通信は双方向で許可するが、端末２１とサーバ３１の間の、ＩＰスタック２００５やＩＰスタック３００５を介さない直接の通信は双方向で遮断するとする。

【１２７９】

更に、サーバ３１から端末２１へのＳＳＬセッション（セキュアＴＣＰセッション）が、上述の動作例により既に設定されているものとする。

【１２８０】

又、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション３１０１との間で、既に、ＴＣＰセッションが構築されているとする。

【１２８１】

端末２１内のアプリケーション２１０１が、サーバ３１内のアプリケーション３１０１宛のデータを、ＴＣＰ２１０２に渡す。

【１２８２】

ＴＣＰ２１０２は、アプリケーション２１０１からデータを受け取り、ＴＣＰプロトコルに従ってＴＣＰヘッダ（図２におけるＦ２３）やＩＰヘッダ（図２におけるＦ２２）を付けてＩＰパケットとし、ＩＰルーティング２１０３に渡す。この時、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡにはサーバ３１のＩＰスタック３１０４のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰスタック２１０４のＩＰアドレスが設定される。

【１２８３】

ＩＰルーティング２１０３は、ＴＣＰ２１０２から受信したパケットの宛先ＩＰアドレス（サーバ３１宛て）及び宛先ポート（ＴＣＰ３１０２宛て）を参照し、データを、そのまま、ＩＰスタック２１０４に転送する。

【１２８４】

ＩＰスタック２１０４は、ＩＰルーティング２１０３からパケットを受信し、ＭＡＣヘッダ（図２におけるＦ２１）を付けてＥｔｈｅｒｎｅｔフレームを作成し、中間ドライバＺ２１０６に渡す。このフレームはＥｔｈｅｒｎｅｔフレームＦ２０のフォーマットを有する。この時、ＩＰスタック２１０４は、ＡＲＰの結果を参照して、フレームのＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスを設定し、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスを設定する。

【１２８５】

中間ドライバＺ２１０６内のゲートウェイアプリケーション２００１Ａは、ＩＰスタック２１０４から受信したフレームを、ゲートウェイアプリケーション２００１Ａとゲートウェイアプリケーション３００１Ａの間に設定したＳＳＬセッションに流す。

【１２８６】

すなわち、ゲートウェイアプリケーション２００１Ａは、ＩＰスタック２１０４から受信したＥｔｈｅｒｎｅｔフレーム（フレームフォーマットＦ２０）をデータとしてＳＳＬ２００２に渡す。

【１２８７】

ＳＳＬ２００２は、ゲートウェイアプリケーション２００１Ａから未暗号化のデータＦ１４（Ｆ２１～Ｆ２４）を受け取ると、暗号化処理を行わず、そのまま、ＴＣＰ２００３に転送する。

【１２８８】

ＴＣＰ２００３は、ＳＳＬ２００２よりデータＦ１４を受け取り、ＴＣＰヘッダＦ１３、及びＩＰヘッダＦ１２を付けて、ＩＰルーティング２００４に渡す。

【１２８９】

ここで、Ｆ１２内のＩＰ　ＤＡにはサーバ３１のＩＰスタック３００５のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡには端末２１のＩＰスタック２００５のＩＰアドレスが設定される。又、宛先ポートにはＴＣＰ３００３のポートが設定され、送信元ポートにはＴＣＰ２００３のポートが指定される。

【１２９０】

ＩＰルーティング２００４は、ＴＣＰ２００３より受信したデータのＩＰヘッダＦ１２内のＩＰアドレス等を参照し、フレームをＩＰスタック２００５に渡す。

【１２９１】

ＩＰスタック２００５は、ＩＰルーティング２００４よりフレームを受信し、フレームにＭＡＣヘッダＦ１１を付け、Ｅｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームフォーマットＦ１０の形式にしてドライバ２１０５に渡す。

【１２９２】

ここで、ＡＲＰの結果より、Ｆ１１内のＭＡＣ　ＤＡにはＦｉｒｅｗａｌｌ　３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡには、端末２１のＭＡＣアドレスが設定される。

【１２９３】

ＩＰスタック２００５より送信されたフレームは、ドライバ２１０５、ＭＡＣ２０１１を経由して、高速化エンジンＹ２０１４に送られる。

【１２９４】

高速化エンジンＹ２０１４は、インタフェース２０１４Ｃにおいてフレームを受け取り、フレーム解析Ｙ２０１４Ｄで受信フレームが、予め、ＳＳＬ２００２より通知されたＳＳＬセッションのフレームだと判別し、データＦ１４の暗号化を行う。そして、マルチプレクサ２０１４Ｆを経由して、ＰＨＹ２０１２に転送する。この時、フレームのヘッダＦ１１～Ｆ１３には、変更を加えない。

【１２９５】

高速化エンジンＹ２０１４を出たフレームは、ＰＨＹ２０１２、ポート２０１３を経由して、Ｆｉｒｅｗａｌｌ３３に送られる。

【１２９６】

Ｆｉｒｅｗａｌｌ３３は、端末２１からのフレームを受信し、ＩＰ　ＤＡを参照してＭＡＣヘッダＦ１１を変更し、受信フレームをフレームフォーマットＦ１０の形のままサーバ３１に転送する。

【１２９７】

ここで、Ｆ１１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＬＡＮ側のＭＡＣアドレスが設定される。

【１２９８】

サーバ３１は、Ｆｉｒｅｗａｌｌ３３からのフレームをポート３１１３より受信すると、ＰＨＹ３１１２、ＭＡＣ３１１１、ドライバ３１０５を経由して、中間ドライバＺ３１０６内の中間ドライバＹ３００６に転送する。

【１２９９】

中間ドライバＹ３００６は、ドライバ３１０５よりフレームを受け取り、フレーム解析Ｙ３００６Ｄで受信フレームが、予め、ＳＳＬ３００２より通知されたＳＳＬセッションのフレームだと判別し、データＦ１４の復号化を行う。そして、復号化処理によりデータＦ１４の暗号化を解除した後、マルチプレクサＹ３００６Ｆを経由して、ＩＰスタック３００５に転送する。この時、フレームのヘッダＦ１１～Ｆ１３には変更を加えない。

【１３００】

ＩＰスタック３００５は、中間ドライバＹ３００６から受信したフレームのＭＡＣヘッダＦ１１を取り外して、ＩＰルーティング３００４に送る。

【１３０１】
ＩＰルーティング３００４は、受信したフレームのヘッダＦ１２内のＩＰ　ＤＡと、Ｆ１３内の宛先ポート番号を参照し、フレームをＴＣＰ３００３に転送する。
【１３０２】
ＴＣＰ３００３は、ＩＰルーティング３００４からフレームを受信すると、ＴＣＰプロトコルに従ってＡＣＫパケットを返送する等の処理を行う。そして、受信したフレームから、ＴＣＰヘッダＦ１３とＩＰヘッダＦ１２を取り外し、データＦ１４をＳＳＬ３００２に転送する。
【１３０３】
ＳＳＬ３００２は、ＴＣＰ３００３からデータＦ１４を受信すると、復号化などの処理をせず、そのまま、ゲートウェイアプリケーション３００１Ａに転送する。
【１３０４】
ゲートウェイアプリケーション３００１Ａは、ＳＳＬ３００２からフレームＦ２０を受信すると、このフレームを、そのまま、ＩＰスタック３１０４に流す。
【１３０５】
ゲートウェイアプリケーション３００１Ａから送出されたフレームは、ＩＰスタック３１０４、ＩＰルーティング３１０３、ＴＣＰ３１０２を経由して転送され、フレーム内のデータＦ２４がアプリケーション３１０１に渡される。
【１３０６】
以上のようにして、端末２１内のアプリケーション２１０１からサーバ３１内のアプリケーション３１０１への一連のフレーム転送が完了する。
【１３０７】
上記の例とは逆の経路を辿ることで、サーバ３１内のアプリケーション３１０１から端末２１内のアプリケーション２１０１への一連のフレーム転送も、同様に、実現可能である。
【１３０８】
本実施の形態では、端末２１側に中間ドライバと高速化エンジンを実装し、サーバ３１側に中間ドライバを実装する例を示したが、これとは逆に、サーバ３１側に高速化エンジンと中間ドライバを実装し、端末２１側に中間ドライバを実装することも可能である。
【１３０９】
又、端末２１側と、サーバ３１側の両方に、高速化エンジンを実装することも出来る。更に、端末２１側とサーバ３１側の両方に中間ドライバを実装し、高速化エンジンを使用しないようにすることも出来る。更に、本実施の形態では、サーバ３１と端末２１の設置場所を入れ替えることも出来る。
【１３１０】
［発明の効果］
次に、本実施の形態の効果について説明する。
【１３１１】
本実施の形態に挙げた発明を利用すると、端末２１とサーバ３１との間で、フレームの高速転送が可能になる。
【１３１２】
これは、端末２１において、暗号化および復号化の処理をハードウェア化し、ＳＳＬの処理を高速化しているからである。
【１３１３】
又、本実施の形態に挙げた発明を利用すると、高速化処理の為のハードウェア（高速化エンジン）の開発費用や部材費用を、比較的低く抑えることが出来る。
【１３１４】
これは、比較的安価なＭＡＣとＰＨＹと間のインタフェースに、高速化処理の為のハードウェア（高速化エンジン）を実装することが出来るからである。
【１３１５】

又、これは、ハードウェアへの実装が難しいＴＣＰ処理をソフトウェアに残し、ハードウェアへの実装が比較的容易で、かつ、高速化処理の効果が大きな暗号化／復号化のみをハードウェア処理できるからである。

【１３１６】

［第１１の実施の形態］

本発明の第１１の実施の形態は、図１９に示す第３の実施の形態に対して、ゲートウェイ装置２０において、ＴＣＰ２００３の代わりにＵＤＰ２００３を設置し、中間ドライバ２００６を廃止し、代わりにブリッジ２００８、ドライバ２００９、仮想ＮＩＣ２０１０を設置したものである。又、ゲートウェイ装置３０においても、ＴＣＰ３００３の代わりにＵＤＰ３００３を設置し、中間ドライバ３００６を廃止している。又、中間ドライバではなく制御フレームを高速化エンジンで作成し、仮想ＮＩＣとブリッジを使って送信している。

【１３１７】

第１１の実施の形態における、端末２１、サーバ３１、ＨＵＢ２２、ＨＵＢ３２、イントラネット２、イントラネット３の構成および動作は、第３の実施の形態と同じである。

【１３１８】

第１１の実施の形態においては、イントラネット２は、閉域ＬＡＮだけでなく、インターネット等のオープンなＷＡＮを用いても構わない。

【１３１９】

［構成の説明］

図３０は、第１１の実施の形態における各機器の構成とフレームの転送経路を詳細に示したブロック図である。

【１３２０】

ゲートウェイ装置２０は、第３の実施の形態におけるゲートウェイ装置２０に対して、ＴＣＰ２００３の代わりにＵＤＰ２００３を設置し、中間ドライバ２００６を廃止し、代わりにブリッジ２００８、ドライバ２００９、仮想ＮＩＣ２０１０を設置している点において異なる。

【１３２１】

ブリッジ２００８、ドライバ２００９、仮想ＮＩＣ２０１０は、各々、第３の実施の形態におけるブリッジ３０８、ドライバ３００９、仮想ＮＩＣ３０１０と同様の構成を有し、同様の動作を行う。

【１３２２】

ＵＤＰ２００３は、ＴＣＰ２００３の機能から輻輳制御および再送制御を除いたものである。

【１３２３】

高速化エンジン制御２００１は、第３の実施の形態における高速化エンジン制御２００１の機能の他、第３の実施の形態における中間ドライバ２００６内の制御フレーム送受信に関わる機能も併せ持っている。

【１３２４】

ゲートウェイ装置３０は、第３の実施の形態におけるゲートウェイ装置３０に対して、ＴＣＰ３００３の代わりにＵＤＰ３００３を設置し、中間ドライバ３００６を廃止している点において異なる。

【１３２５】

ＵＤＰ３００３は、本実施の形態におけるゲートウェイ装置２０内のＵＤＰ２００３と同様である。

【１３２６】

第１１の実施の形態では、ゲートウエイ装置２０とゲートウェイ装置３０との間で、予めＳＳＬセッションを設定している場合のみ、イントラネット２内の機器からイントラネット３内の機器へのアクセスが可能になる。

【１３２７】

［動作の説明］

［ＳＳＬセッションの確立動作］

図３０を用いて、第１１の実施の形態において、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＴＣＰセッション）を確立する場合を例に挙げて、動作の説明を行う。

【１３２８】

この際、ブリッジ２００８、ブリッジ３００８、ＨＵＢ２２やＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３のＷＡＮ側、Ｆｉｒｅｗａｌｌ３３のＬＡＮ側、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。

【１３２９】

又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間のゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。

【１３３０】

ゲートウェイ装置３０内のゲートウェイアプリケーション３００１Ａは、ユーザからのゲートウェイ装置２０内の高速化エンジン制御２００１への接続要求を受け、ＳＳＬ３００２にゲートウェイ装置２０内の高速化エンジン制御２００１への通信開始を指示する。同時に、中間ドライバ３００６に対して、ゲートウェイ装置２０内の高速化エンジン制御２００１への通信開始を通知する。この通知には、ゲートウェイ装置２０のＩＰアドレス、高速化エンジン制御２００１のポート番号、及びゲートウェイアプリケーション３００１Ａの送信元ポート番号、更にゲートウェイ装置３０のＩＰアドレスが含まれる。

【１３３１】

ＳＳＬ３００２は、ゲートウェイアプリケーション３００１Ａからの通信開始指示を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為に、ＵＤＰ３００３にゲートウェイ装置２０内の高速化エンジン制御２００１への通信開始を指示する。

【１３３２】

ＵＤＰ３００３は、ＳＳＬ３００２からの通信開始指示を受け、ＵＤＰ２００３との間でＴＣＰセッションを確立する為に、ＩＰルーティング３００４に対して、ＵＤＰ２００３とのセッション確立に必要なパケットを送信する。このパケットは、ＵＤＰ規格に沿ったものであり、宛先ＩＰアドレスにゲートウェイ装置２０宛、宛先ポート番号にＵＤＰ２００３が設定されている。

【１３３３】

ＩＰルーティング３００４は、ＵＤＰ３００３から受信したパケットの宛先ＩＰアドレスと宛先ポート番号を参照し、パケットをＩＰスタック３００５に転送する。

【１３３４】

ＩＰスタック３００５は、ＩＰルーティング３００４より受信したパケットに、Ｆｉｒｅｗａｌｌ３３内のイントラネット３側のＭＡＣアドレスを宛先ＭＡＣアドレスとして付加し、更に送信元ＭＡＣアドレスに自ノードのＭＡＣアドレスを設定してフレームを生成し、ブリッジ３００８を経由してドライバ３００７に転送する。

【１３３５】

ドライバ３００７は、ブリッジ３００８からフレームを受信し、ＭＡＣ３０１１に転送する。

【１３３６】

ＭＡＣ３０１１は、ドライバ３００７からフレームを受信し、ＰＨＹ３０１２に転送する。

【１３３７】

ＰＨＹ３０１２は、ＭＡＣ３０１１からフレームを受信し、ポート３０１３に転送する。

【１３３８】

ポート３０１３は、ＰＨＹ３０１２からフレームを受信し、イーサネットケーブルを経由してＨＵＢ３２に転送する。

【１３３９】

ＨＵＢ３２は、フレームを受信すると、ＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＬＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３側のポートに出力する。

【１３４０】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からフレームを受信し、ゲートウェイ装置３０からゲートウェイ装置２０への通信の為、これを許可し、ＨＵＢ２２に転送する。

【１３４１】

ＨＵＢ２２は、Ｆｉｒｅｗａｌｌ３３からフレームを受信し、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０に転送する。

【１３４２】

ゲートウェイ装置２０は、ＨＵＢ２２内からフレームを受信し、ポート２０１３、ＰＨＹ２０１２、高速化エンジン２０１４、ＭＡＣ２０１１、ドライバ２００７、ブリッジ２００８の経路でパケットを転送し、ＩＰスタック２００５に転送する。この時、高速化エンジン２０１４は、ＰＨＹから受信したフレームを、そのまま、ＭＡＣ　２０１１に転送する。

【１３４３】

ＩＰスタック２００５は、ブリッジ２００８からフレームを受信し、ＭＡＣヘッダを外してＩＰルーティング２００４に転送する。

【１３４４】

ＩＰルーティング２００４は、ＩＰスタック２００５より受信したパケットの宛先ポート番号を参照し、ＵＤＰ２００３側のポート番号が付加されていることから、このパケットをＵＤＰ２００３に転送する。

【１３４５】

ＵＤＰ２００３は、ＩＰルーティング２００４よりパケットを受信する。そして、セッション確立要求受信の報告をＳＳＬ２００２に伝える。その結果、ＳＳＬ２００２は、ＵＤＰ２００３に対して、ＵＤＰ２００３に対してセッションを確立するよう命令する。

【１３４６】

ＵＤＰ２００３は、セッション確立の為に必要なパケットを、ＵＤＰ３００３宛てに送信する。すなわち、セッション確立要求パケットの宛先ＩＰはゲートウェイ装置３０のＩＰアドレスが設定され、パケットの宛先ポートはＴＣＰ３００３のポート番号が設定される。

【１３４７】

接続要求パケットは、セッション確立要求パケットとは逆の経路、即ち、ＩＰルーティング２００４、ＩＰスタック２００５、ブリッジ２００８、ドライバ２００７、ＮＩＣ２０１、ＨＵＢ２２、Ｆｉｒｅｗａｌｌ３３、ＨＵＢ３２、ＮＩＣ３０１、ドライバ３００７、ブリッジ３００８、ＩＰスタック３００５、ＩＰルーティング３００４を経由し、ＵＤＰ３００３に到達する。

【１３４８】

ＵＤＰ３００３は、ＩＰルーティング３００４よりパケットを受信する。このパケットは、ＵＤＰセッションの確立要求であるので、ＳＳＬ３００２に対して、ＵＤＰ２００３とのＵＤＰセッション接続完了を通知する。

【１３４９】

ＳＳＬ３００２は、ＵＤＰ３００３からの接続完了通知を受け、ＳＳＬ２００２との間でＳＳＬセッションを確立する為、ＳＳＬプロトコルに従い、セッション確立要求の為のパケット（ＳＳＬセッション確立要求パケット）を送信する。

【１３５０】

ＳＳＬセッション確立要求パケットは、ＵＤＰ３００３で受信されると、ＵＤＰ３００

３と中間ドライバ３００６内のＵＤＰとの間で設定されたＵＤＰセッションを通り、ＮＩＣ３０１、ＨＵＢ３２、Ｆｉｒｅｗａｌｌ３３、ＨＵＢ２２、ＮＩＣ２０１を経由して、ＵＤＰ２００３に到着する。この際、ＮＩＣ２０１内の高速化エンジン２０１４は、ＰＨＹ２０１２から受信したパケットを、そのまま、ＭＡＣ２０１１に転送する。

【１３５１】

ＵＤＰ２００３は、パケットをＳＳＬ２００２に転送する。

【１３５２】

ＳＳＬ２００２は、ＳＳＬセッション確立要求の内容を検証し、問題が無ければ、高速化エンジン制御２００１に対して、ＳＳＬ３００２とのセッション確立を通知すると同時に、ＳＳＬプロトコルに従い、ＳＳＬ３００２に対してＳＳＬセッション確立応答パケットを送信する。

【１３５３】

ＳＳＬセッション確立応答パケットは、ＳＳＬセッション確立要求パケットとは逆の経路、即ち、ＵＤＰ２００３と中間ドライバ２００６との間のＵＤＰセッションを経由してＳＳＬ３００２に到達する。

【１３５４】

ＳＳＬ３００２は、ＳＳＬセッション確立応答の内容をＳＳＬプロトコルに従い検証し、問題が無ければ、ゲートウェイアプリケーション３００１Ａに対して、ＳＳＬ３００２とＳＳＬ２００２との間のＳＳＬセッション確立を通知する。

【１３５５】

高速化エンジン制御２００１は、ＳＳＬ２００２からのＳＳＬセッション確立通知を受けると、制御フレームを作成し、このフレームを仮想ＮＩＣ２０１０、ドライバ２００９、ブリッジ２００８、ドライバ２００７、ＭＡＣ２０１１の経路で転送し、高速化エンジン２０１４に送る。制御フレームには、公開鍵、秘密鍵および共通鍵、ＳＳＬセッションの相手方機器のＩＰアドレス（ゲートウェイ装置３０のＩＰアドレス）、ＳＳＬセッションの相手方機器の宛先ポート（ＵＤＰ３００３のポート）、自ノード側のＳＳＬセッションの送信元ポート番号（ＵＤＰ２００３のポート）、送信元ＩＰアドレス（ゲートウェイ装置２０のＩＰアドレス）、及び開始命令が含まれる。

【１３５６】

高速化エンジン２０１４は、ＭＡＣアドレス等により制御フレームを判別し、制御フレーム送受信部で受信する。そして、公開鍵、秘密鍵および共通鍵を、それぞれ復号化および暗号化に使用する為に保存し、ＩＰアドレスやポート番号をフレーム解析の為に保存する。そして、高速化処理開始命令を受け、フレーム解析、暗号化、及び復号化の処理を開始する。

【１３５７】

高速化エンジン２０１４は、高速化処理開始命令以前は、制御フレーム以外のＭＡＣ２０１１から受信したフレームは、全て、そのまま、ＰＨＹ２０１２に送信し、ＰＨＹ２０１２から受信したフレームは、全て、そのまま、ＭＡＣ２０１１に送信していた。しかしながら、高速化処理開始命令以降は、制御フレーム以外のＭＡＣ２０１１から受信したフレームを、全て、そのまま、ＰＨＹ２０１２に送信する動作には変わりないが、ＰＨＹ２０１２から受信したフレームについては、以下のような処理を行う。

（１）　ゲートウェイ装置２０宛て、かつ、ＳＳＬ３００２で暗号化されたフレームであれば、ＵＤＰ等のカプセル化を解除し、必要であれば、フラグメントを解除し、フレームを復号化し、ＰＨＹ２０１２側に送信する。

（２）　（１）以外の自ノード宛てフレームであれば、ＭＡＣ２０１１に転送する。

（３）　ブロードキャストフレーム、若しくはマルチキャストフレームであれば、フレームをコピーして、一方はそのままＭＡＣ２０１１に転送し、もう一方は暗号化とカプセル化を行い、ＳＳＬ３００２（ＰＨＹ２０１２側）に送信する。必要であれば、フラグメントを分割も行う。

（４）　（１）～（３）以外のフレームであれば、暗号化とカプセル化を行い、ＳＳＬ３

００２（ＰＨＹ２０１２側）に送信する。必要であれば、フラグメントを分割も行う。
【１３５８】
以上のようにして、高速化エンジン２０１４とＵＤＰ３００３との間で、フレーム転送の為のＵＤＰ等の輻輳制御の無いセッションが確立される。又、高速化エンジン２０１４とＳＳＬ３００２との間で、ＳＳＬセッションが確立される。
【１３５９】
すなわち、ＳＳＬ２００２は、セッション確立要求時のみ、ＳＳＬ３００２と遣り取りを行うが、セッション確立が終了すると、以後は、高速化エンジン２０１４とＳＳＬ３００２との間で、ＳＳＬの暗号化および復号化の遣り取りを行う。
【１３６０】
又、ＵＤＰ３００３は、セッション確立要求時のみＵＤＰ２００３とフレームの遣り取りを行うが、ＳＳＬセッションが確立した後は、高速化エンジン２０１４とＵＤＰ３００３との間でフレームの遣り取りを行う。
【１３６１】
以上により、第３の実施の形態において、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＵＤＰセッション）を確立する場合の動作が完了する。
【１３６２】
［端末２１からサーバ３１へのフレーム転送動作］
図３０を用いて、第１１の実施の形態において、端末２１からサーバ３１へフレームを送信する場合を例に挙げて、動作の説明を行う。
【１３６３】
この際、ブリッジ２００８、ブリッジ３００８、ＨＵＢ２２やＨＵＢ３２が、既に、端末２１、サーバ３１、Ｆｉｒｅｗａｌｌ３３、ゲートウェイ装置２０、ゲートウェイ装置３０のＭＡＣアドレスを学習しているものとする。
【１３６４】
又、Ｆｉｒｅｗａｌｌ３３は、ゲートウェイ装置２０とゲートウェイ装置３０の間の通信は双方向で許可するが、端末２１とサーバ３１の間のゲートウェイ装置２０やゲートウェイ装置３０を介さない直接の通信は双方向で遮断するとする。
【１３６５】
更に、ゲートウェイ装置３０からゲートウェイ装置２０へのＳＳＬセッション（セキュアＵＤＰセッション）が、上述の動作例により、既に、設定されているものとする。
【１３６６】
又、端末２１内のアプリケーション２１０１と、サーバ３１内のアプリケーション（アプリケーション３１０１）との間で、既に、ＴＣＰセッションが構築されているとする。
【１３６７】
端末２１内のアプリケーション２１０１が、サーバ３１内のアプリケーション３１０１宛のデータを、ＴＣＰ２１０２に渡す。
【１３６８】
ＴＣＰ２１０２は、アプリケーション２１０１からデータを受け取り、ＴＣＰプロトコルに従ってＴＣＰヘッダ（図２におけるＦ２３）やＩＰヘッダ（図２におけるＦ２２）を付けてＩＰパケットとし、ＩＰルーティング２１０３に渡す。この時、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡにはサーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには端末２１のＩＰアドレスが設定される。
【１３６９】
ＩＰルーティング２１０３は、ＴＣＰ２１０２から受信したパケットの宛先ＩＰアドレス（サーバ３１宛て）及び宛先ポート（ＴＣＰ３１０２宛て）を参照し、データを、そのまま、ＩＰスタック２１０４に転送する。
【１３７０】
ＩＰスタック２１０４は、ＩＰルーティング２１０３からパケットを受信し、ＭＡＣヘ

ッダ（図２におけるＦ２１）を付けてＥｔｈｅｒｎｅｔフレームを作成し、ドライバ２１０５に渡す。このフレームはＥｔｈｅｒｎｅｔフレームＦ２０のフォーマットを有する。この時、ＩＰスタック２１０４は、ＡＲＰの結果を参照して、フレームのＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスを設定し、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスを設定する。

【１３７１】

ドライバ２１０５は、ＩＰスタック２１０５より上記フレームを受け取り、ＮＩＣ２１１に転送する。

【１３７２】

ＮＩＣ２１１は、ドライバ２１０５よりフレームを受け取り、ＭＡＣ２１１１、ＰＨＹ２１１２、ポート２１１３を経由して、ＨＵＢ２２にフレームを転送する。

【１３７３】

ＨＵＢ２２は、端末２１のＮＩＣ２１１側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置２０側のポートに出力する。

【１３７４】

ゲートウェイ装置２０内のＮＩＣ２０１は、ポート２０１３でＨＵＢ２２からのフレームを受信し、ＰＨＹ２０１２を経由して、高速化エンジン２０１４に渡す。

【１３７５】

高速化エンジン２０１４は、到着したフレームの宛先ＭＡＣがサーバ３１宛てであることから、高速化エンジン２０１４内の暗号化２０１４Ｇにおいてフレームを暗号化して図３におけるデータＦ１４を作成し、更にカプセル化２０１４Ｉにおいて図３におけるＦ１１～Ｆ１３の各ヘッダを付加してＥｔｈｅｒ　ｏｖｅｒ　ＳＳＬフレームＦ１０のフォーマットにして、再びＰＨＹ２０１２側に転送する。

【１３７６】

この時、ＩＮＥＴ　ＭＡＣ　Ｆ１１内のＭＡＣ　ＤＡにはＦｉｒｅｗａｌｌ３３のＷＡＮ側のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはゲートウェイ装置２０のＭＡＣアドレスが設定される。又、ＩＮＥＴ　ＩＰ　Ｆ１２内のＩＰ　ＤＡにはゲートウェイ装置３０のＩＰアドレスが設定され、Ｆ１２内のＩＰ　ＳＡにはゲートウェイ装置２０のＩＰアドレスが設定される。ＩＮＥＴ　ＴＣＰ　Ｆ１３に関しては、ＵＤＰ３００３の宛先ポートが設定され、送信元ポートにはＵＤＰ２００３を設定する。（本実施の形態では、Ｆｉｒｅｗａｌｌ３３がＵＤＰ通信を許可するものとする）

ＰＨＹ２０１２は、高速化エンジン２０１４よりフレームを受信すると、ポート２０１３を経由してＨＵＢ２２にフレームを転送する。

【１３７７】

ＨＵＢ２２は、ゲートウェイ装置２２側のポートからフレームを受信すると、Ｆ１１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがＦｉｒｅｗａｌｌ３３のＷＡＮ側のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、Ｆｉｒｅｗａｌｌ３３に出力する。

【１３７８】

Ｆｉｒｅｗａｌｌ３３は、ＨＵＢ２２からのフレームを受信し、ＩＰ　ＤＡを参照してＭＡＣヘッダＦ１１を変更し、受信フレームをフレームフォーマットＦ１０の形のままＨＵＢ３２に転送する。

【１３７９】

ここで、Ｆ１１内のＭＡＣ　ＤＡにはゲートウェイ装置３０のＭＡＣアドレスが設定され、Ｆ１１内のＭＡＣ　ＳＡにはＦｉｒｅｗａｌｌ３３のＬＡＮ側のＭＡＣアドレスが設定される。

【１３８０】

ＨＵＢ３２は、Ｆｉｒｅｗａｌｌ３３からのフレームを受信すると、Ｆ１１内のＭＡＣ

ＤＡを参照し、ＭＡＣ　ＤＡがゲートウェイ装置３０のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、ゲートウェイ装置３０側のポートに出力する。

【１３８１】

ゲートウェイ装置３０は、ＨＵＢ３２からのフレームをポート３０１３より受信すると、ＰＨＹ３０１２、ＭＡＣ３０１１、ドライバ３００７、ブリッジ３００８を経由して、ＩＰスタック３００５に転送する。

【１３８２】

ＩＰスタック３００５は、ブリッジ３００８から受信したフレームのＭＡＣヘッダＦ１１を取り外して、ＩＰルーティング３００４に送る。

【１３８３】

ＩＰルーティング３００４は、受信したフレームのヘッダＦ１２内のＩＰ　ＤＡと、Ｆ１３内の宛先ポート番号を参照し、フレームをＴＣＰ３００３に転送する。

【１３８４】

ＵＤＰ３００３は、ＩＰルーティング３００４からフレームを受信すると、受信したフレームから、ＵＤＰヘッダＦ１３とＩＰヘッダＦ１２を取り外し、データＦ１４をＳＳＬ３００２に転送する。

【１３８５】

ＳＳＬ３００２は、ＵＤＰ３００３からデータＦ１４を受信すると、復号化処理により暗号化を解除し、データＦ１４からＥｔｈｅｒｎｅｔフレームＦ２０、即ち、Ｆ２１～Ｆ２４を取り出し、ゲートウェイアプリケーション３００１Ａに転送する。

【１３８６】

ゲートウェイアプリケーション３００１Ａは、ＳＳＬ３００２からフレームＦ２０を受信すると、このフレームを、そのまま、仮想ＮＩＣ３０１０に流す。

【１３８７】

このフレームは、端末２１からＨＵＢ２２に送信された時の状態のままに保たれており、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＤＡにはサーバ３１のＭＡＣアドレスが設定され、ＬＡＮ　ＭＡＣ　Ｆ２１内のＭＡＣ　ＳＡには端末２１のＭＡＣアドレスが設定されている。又、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＤＡには、サーバ３１のＩＰアドレスが設定され、ＬＡＮ　ＩＰ　Ｆ２２内のＩＰ　ＳＡには、端末２１のＩＰアドレスが設定されている。

【１３８８】

ゲートウェイアプリケーション３００１Ａより仮想ＮＩＣ３０１０に渡されたフレームは、ドライバ３００９、ブリッジ３００８、ＮＩＣ３０１を経由して、ＨＵＢ３２に転送される。

【１３８９】

ＨＵＢ３２は、ゲートウェイ装置３０側のポートからフレームを受信すると、Ｆ２１内のＭＡＣ　ＤＡを参照し、ＭＡＣ　ＤＡがサーバ３１のものであることから、過去のルーティング学習結果に基づき、このフレームを、そのまま、サーバ３１側のポートに出力する。

【１３９０】

サーバ３１は、ＨＵＢ３２から送信されたフレームを受信し、ドライバ３１０５、ＩＰスタック３１０４、ＩＰルーティング３１０３、ＴＣＰ３１０２を経由して、フレーム内のデータＦ２４をアプリケーション３１０１に渡す。

【１３９１】

以上のようにして、端末２１内のアプリケーション２１０１からサーバ３１内のアプリケーション３１０１への一連のフレーム転送が完了する。

【１３９２】

上記の例とは逆の経路を辿ることで、サーバ３１内のアプリケーション３１０１から端末２１内のアプリケーション２１０１への一連のフレーム転送も、同様に実現可能である

。
【１３９３】
本実施の形態では、ゲートウェイ装置２０側に高速化エンジンを実装する例を示したが、これとは逆に、ゲートウェイ装置３０側に高速化エンジンを実装することも可能である。更に、本実施の形態では、サーバ３１と端末２１の設置場所を入れ替えることも出来る。
【１３９４】
［発明の効果］
次に、本実施の形態の効果について説明する。
【１３９５】
本実施の形態に挙げた発明を利用すると、端末２１とサーバ３１との間で、フレームの高速転送が可能になる。
【１３９６】
これは、高速化エンジンを利用することで、ゲートウェイ装置２０におけるＣＰＵ（ソフトウェア処理）によるカプセル化処理および暗号化／復号化処理を排除し、これら処理を全て高速化エンジン（ハードウェア）で実現できる為である。
【１３９７】
又、本実施の形態に挙げた発明を利用すると、高速化処理の為のハードウェア（高速化エンジン）の開発費用や部材費用を、比較的低く抑えることが出来る。
【１３９８】
これは、暗号化／復号化とカプセル化を同一ハードウェア（ＦＰＧＡ／ＡＳＩＣ）上で行うことが出来るからである。
【１３９９】
又、これは、比較的安価なＭＡＣとＰＨＹ間のインタフェースに、ハードウェアを実装することが出来るからである。
【１４００】
又、これは、ハードウェアへの実装が難しいＴＣＰ処理をソフトウェアに残し、ハードウェアへの実装が比較的容易で、かつ、高速化処理の効果が大きな暗号化／復号化とカプセル化のみをハードウェア処理できるからである。
【１４０１】
［第１２の実施の形態］
本発明の第１２の実施の形態は、第１の実施の形態に対して、高速化エンジン２０１４において、複数のセッション取り扱えるようにしたものである。
【１４０２】
［構成の説明］
図３１は、本実施の形態における中間ドライバ１００８の構成を示すブロック図である。本実施の形態における中間ドライバ１００８は、図７に示す第１の実施の形態における中間ドライバ１００８に対して、設定管理部１００８Ｌ内にテーブルを有し、複数のセッションの情報を保存できる点において異なる。
【１４０３】
更に、フレーム解析１００８Ｈ及びフレーム解析１００８Ｉが、設定管理部１００８Ｌ内のテーブルを参照して、受信したフレームの転送先を決定する点において異なる。
【１４０４】
フレーム解析１００８Ｈは、ＩＰスタック１００７からフレームを受信し、以下の順序でフレームのヘッダ情報をキーにして設定管理部１００８Ｌ内のテーブルを検索する。
（１）　フレームが高速化処理に関係するフレームで有るかどうか検索する。フレームが高速化処理に関係するフレームで有る場合、フレームをカプセル化解除１００８Ｆに転送する。フレームが高速化処理に関係するフレームか否かは、ＭＡＣアドレス、ＩＰアドレス、ＴＣＰヘッダ、ＵＤＰヘッダ等を基に判別される。
（２）　検索の結果、その他のフレームであれば、マルチプレクサ１００８Ｋに転送する

。
【１４０５】
フレーム解析１００８Ｉは、ドライバ１００９からフレームを受信し、以下の順序でフレームのヘッダ情報をキーにして設定管理部１００８Ｌ内のテーブルを検索する。
（１） フレームが高速化処理に関係するフレームで有るか否かを検索する。
【１４０６】
フレームが高速化処理に関係するフレームで有る場合、フレームをカプセル化解除１００８Ｇに転送する。フレームが高速化処理に関係するフレームか否かは、ＭＡＣアドレス、ＩＰアドレス、ＴＣＰヘッダ、ＵＤＰヘッダ等を基に判別される。
（２） フレームが機器や高速化エンジンの制御に関わる特殊なフレーム（以降、制御フレームと呼ぶ）であるか否かを検索する。
【１４０７】
検索の結果、フレームが制御フレームである場合、フレームを制御フレーム送受信部１００８Ｍに転送する。特殊フレームであるか否かは、通常はＭＡＣ ＤＡとＭＡＣ ＳＡにより判断される。ＭＡＣ ＤＡもしくはＭＡＣ ＳＡをキーにテーブル検索を行い、予め、テーブルに登録したアドレス範囲のＭＡＣアドレス（制御用ＭＡＣアドレスと呼ぶ。例えば０００００４Ｃ００００ｘｘ）が記載されている場合は、フレームを制御フレームと判断する。
（３） 検索の結果、その他のフレームであればマルチプレクサ１００８Ｊに転送する。
【１４０８】
設定管理部１００８Ｌは、以下の機能を有する。
（１） 中継アプリケーション１００１より、高速化処理に関連するセッションの情報（ＭＡＣアドレス、ＩＰアドレス、ポート番号等）の通知を受け、テーブルに保存する。
（２） 中継アプリケーション１００１より、特殊フレームのＭＡＣアドレスの通知を受け、テーブルに保存する。
（３） フレーム解析１００８Ｈ及びフレーム解析１００８Ｉからの要求により、テーブルの検索を行い、検索結果を知らせる。
【１４０９】
テーブルには、１セッションだけでなく、複数セッション分のＭＡＣアドレス、ＩＰアドレス、ポート番号等の情報を記憶できる。
【１４１０】
図３２は、本実施の形態における高速化エンジン２０１４の構成を示すブロック図である。本実施の形態における高速化エンジン２０１４は、図１２に示す第１の実施の形態における高速化エンジン２０１４に対して、設定管理部２０１４Ｎを有し、複数のセッションの情報を保存出来る点において異なる。
【１４１１】
更に、フレーム解析２０１４Ｂが、設定管理部２０１４Ｎ内のテーブルを参照して、受信したフレームの転送先を決定する他、暗号化２０１４Ｇ、復号化２０１４Ｌ、カプセル化２０１４Ｉも、設定管理部２０１４Ｎ内のテーブルを参照して、セッションに適した公開鍵、秘密鍵および共通鍵、ヘッダ等の情報を得る。
【１４１２】
フレーム解析２０１４Ｂは、インタフェース２０１４Ａからフレームを受信し、以下に示す（１）～（４）の順序で宛先を決定して転送する。
（１） 設定管理部２０１４Ｎ内のテーブルを検索し、自ノード宛て、かつ、検索にヒットした場合（予め設定されたＳＳＬセッションのフレームである場合、即ち、セッション中継装置１０によって暗号化されたフレームである場合）は、フレームをカプセル化解除２０１４Ｊに転送する。この時、設定管理部から受け取ったセッションＩＤ情報も一緒に渡す。
（２） （１）以外の自ノード宛てフレーム（自ノード宛て、かつ、設定管理部２０１４Ｎ内のテーブルを検索でミスヒットした場合）であれば、フレームをマルチプレクサ２０

１４Ｅに転送する。
（３） ＭＡＣ ＤＡにブロードキャストＭＡＣ、若しくはブロードキャストＭＡＣが付加された、ブロードキャストフレーム、又はマルチキャストフレームであれば、マルチプレクサ２０１４Ｅと暗号化２０１４Ｇに、フレームをコピーして転送する。仮に、複数のセッションが設定管理部２０１４Ｎに登録されている場合は、登録セッションの本数分、フレームをコピーし、設定管理部２０１４Ｎから得られるセッションＩＤと共に、暗号化２０１４Ｇに渡す。
（４） （１）～（３）以外のフレームであれば、暗号化２０１４Ｇに転送する。仮に、複数のセッションが設定管理部２０１４Ｎに登録されている場合は、登録セッションの本数分、フレームをコピーし、設定管理部２０１４Ｎから得られるセッションＩＤと共に、暗号化２０１４Ｇに渡す。
【１４１３】
制御フレーム解析２０１４Ｄは、インタフェース２０１４Ｃからフレームを受信し、フレームが高速化エンジンの制御に関わる特殊なフレーム（以後、制御フレームと呼ぶ）である場合は、フレームを制御フレーム送受信部２０１４Ｍに転送する。特殊フレームで無い場合は、マルチプレクサ２０１４Ｆに転送する。特殊フレームであるか否かは、通常はＭＡＣ ＤＡとＭＡＣ ＳＡにより判断する。ＭＡＣ ＤＡ又はＭＡＣ ＳＡの何れかに、予め規定したアドレス範囲のＭＡＣアドレス（制御用ＭＡＣアドレスと呼ぶ。例えば、０００００４Ｃ０００００００～ＦＦ）が記載されている場合は、フレームを制御フレームと判断する。
【１４１４】
暗号化２０１４Ｇは、フレーム解析２０１４Ｂよりフレームを受信し、３ＤＥＳ等の方法で暗号化を行い、フラグメント分割２０１４Ｈに転送する。暗号化に用いる公開鍵は、フレーム解析２０１４Ｂより通知を受けたセッションＩＤをキーにして、設定管理部２０１４Ｎ内のテーブルを検索し、この結果得られた公開鍵と共通鍵を利用する。
【１４１５】
カプセル化２０１４Ｉは、図７に示す中間ドライバ１００８内の再カプセル化１００８Ｄと同様の動作を行う。すなわち、フラグメント分割２０１４Ｈより送られて来るデータ（図３におけるＦ１４）に、ＩＮＥＴ ＭＡＣ Ｆ１１、ＩＮＥＴ ＩＰ Ｆ１２、ＩＮＥＴ ＴＣＰ Ｆ１３の各ヘッダを付加し、マルチプレクサ２０１４Ｆに転送する。付加するＦ１１～Ｆ１３の各ヘッダの値は、セッションＩＤをキーにして、設定管理部２０１４Ｎ内のテーブルを検索し、この結果得られたヘッダの値を利用する。尚、設定により、ＩＮＥＴ ＴＣＰ Ｆ１３の位置に、ＴＣＰヘッダでは無く、ＵＤＰヘッダを設定することも出来る。
【１４１６】
カプセル化２０１４Ｉにおいて、ＴＣＰヘッダＦ１３を付加するのは、通信経路上に存在するＦｉｒｅｗａｌｌやＮＡＴルータ等（図１の例ではＦｉｒｅｗａｌｌ２３）でパケットが遮断されることを防ぐ為である。Ｆ１３にＵＤＰヘッダを設定した場合は、通信経路上にＦｉｒｅｗａｌｌやＮＡＴルータ等が存在する場合に、通信が遮断される可能性がある。カプセル化２０１４Ｉにおいて付加したＴＣＰヘッダは、フレームフォーマットはＴＣＰの形式を有するが、実際には、ＴＣＰは付加したヘッダでは無いので、輻輳制御や再送制御には用いられない。ここで付加するヘッダＦ１３は、厭くまで、ＦｉｒｅｗａｌｌやＮＡＴを通過する為のものであり、実際の輻輳制御や再送制御は、端末２１やサーバ３１内に存在するＴＣＰ（図３のフレームフォーマットＦ１０におけるＦ２３のＴＣＰヘッダ部分）によって行われる。
【１４１７】
復号化２０１４Ｌは、フラグメント解除２０１４Ｋよりフレームを受信し、３ＤＥＳ等の方法で復号化を行い、マルチプレクサ２０１４Ｆに転送する。復号化に用いる公開鍵は、セッションＩＤをキーにして、設定管理部２０１４Ｎ内のテーブルを検索し、この結果得られた秘密鍵と共通鍵を利用する。

【１４１８】
制御フレーム送受信部２０１４Ｍは、図７に示す中間ドライバ１００８内の制御フレーム送受信部１００８Ｍとの間で、制御フレームの送受信を行う。制御フレーム送受信部２０１４Ｍは、マルチプレクサ２０１４Ｅに高速化エンジンの制御に関わる特殊なフレーム（以降、制御フレームと呼ぶ）を送り、又、制御フレーム解析２０１４Ｄより制御フレームを受信する。そして、制御フレームで受信した設定パラメータ類を、設定管理部２０１４Ｎ内のテーブルに保存する。ここで、仮に、制御フレームで高速化処理の開始、及び終了の命令を受け取った場合、フレーム解析２０１４Ｂに通知する。制御フレーム送受信部では、以下の情報が送受信される。
（１）　ＳＳＬセッションの相手方機器（セッション中継装置１０）のＩＰアドレスや宛先ポート、及び自ノード（ゲートウェイ装置２０）側のＳＳＬセッションの送信元ポート番号や送信元ＩＰアドレス、更には宛先ＭＡＣアドレスと、自ノードの送信元ＭＡＣアドレス。
（２）　公開鍵
（３）　秘密鍵
（４）　共通鍵
（５）　高速化処理の開始および終了
【１４１９】
設定管理部２０１４Ｎは、制御フレーム送受信部２０１４Ｍからの設定情報を得て、これをセッションごとにテーブル形式で保存する。又、暗号化２０１４Ｇ、復号化２０１４Ｌ、フレーム解析２０１４Ｂからの要求に対して、以下に示す（１）～（３）の方法でテーブルを検索し、結果を返答する。設定管理部２０１４Ｎは、テーブルにより複数セッション分の情報を保持し、要求により検索を行い、適切な情報を返答することが出来る。
（１）　暗号化２０１４Ｇからの検索要求に対しては、検索キー（セッションＩＤ）に対応したセッションの公開鍵と共通鍵を返答する。
（２）　復号化２０１４Ｌからの検索要求に対しては、検索キー（セッションＩＤ）に対応したセッションの秘密鍵と共通鍵を返答する。
（３）　フレーム解析２０１４Ｂからの検索要求に対しては、ヒットの場合は、検索キー（ＭＡＣアドレス、ＩＰアドレス、ポート）に対応したセッションのＩＤを返答する。ミスヒットの場合は、その旨を返答する。
【１４２０】
［動作の説明］
第１２の実施の形態における動作は、第１の実施の形態における動作とほぼ同じな為、内容については省略する。
【１４２１】
本実施の形態では、複数のセッションの設定が可能な為、受信したパケットのヘッダに応じて、動的にＳＳＬセッションを確立させ、又、これを切断することも出来る。この場合、セッションの構築先のＩＰアドレスは、ラーニングやＢＧＰ等の方法により、決定される。
【１４２２】
［発明の効果］
次に、本実施の形態の効果について説明する。
【１４２３】
本実施の形態に挙げた発明を利用すると、端末２１とサーバ３１との間で、フレームの高速転送が可能になる。
【１４２４】
これは、高速化エンジンを利用することで、ゲートウェイ装置２０やゲートウェイ装置３０におけるＣＰＵでのソフトウェア処理によるカプセル化処理および暗号化／復号化処理を排除し、これら処理を全て高速化エンジン（ハードウェア）で実現できる為である。
【１４２５】

更に、これは、ゲートウェイ装置とセッション中継装置との間の通信において、ヘッダＦ１３の位置のＴＣＰによる輻輳制御と再送制御とが発生しないよう、セッション中継装置内の中間ドライバと、ゲートウェイ装置内の中間ドライバにおいて、ＴＣＰを終端し、ＴＣＰ　ｏｖｅｒ　ＴＣＰ問題の発生を回避しているからである。

【１４２６】

又、本実施の形態に挙げた発明を利用すると、高速化処理の為のハードウェア（高速化エンジン）の開発費用や部材費用を、比較的低く抑えることが出来る。

【１４２７】

これは、暗号化／復号化とカプセル化を同一ハードウェア（ＦＰＧＡ／ＡＳＩＣ）上で行うことが出来るからである。

【１４２８】

又、これは、比較的安価なＭＡＣとＰＨＹ間のインタフェースに、ハードウェアを実装することが出来るからである。

【１４２９】

又、これは、ハードウェアへの実装が難しいＴＣＰ処理をソフトウェアに残し、ハードウェアへの実装が比較的容易で、かつ、高速化処理の効果が大きな暗号化／復号化とカプセル化のみをハードウェア処理できるからである。

【１４３０】

以上好ましい実施の形態及び実施例を挙げて本発明を説明したが、本発明は、必ずしも、上記実施の形態及び実施例に限定されるものでは無く、その技術的思想の範囲内において様々に変形して実施することが出来る。

【１４３１】

尚、上述した各実施の形態の構成において、ソフトウェアで構成される部分とハードで構成される部分とを切り分けて説明したが、ソフトウェア及びハードで構成される部分は上記実施の形態に限るものではない。

【産業上の利用可能性】

【１４３２】

本発明によれば、インターネット等のＷＡＮを介して、企業の拠点ＬＡＮ間でのイーサネットレイヤでの通信を可能にするインターネットＶＰＮ装置やインターネットＶＰＮシステムに適用できる。

【１４３３】

又、インターネット等のＷＡＮ上の端末から、企業の拠点ＬＡＮ内にイーサネットレベルでの通信を可能にする、リモートアクセス装置やリモートアクセスシステムに適用できる。

【１４３４】

上気した本発明の第１の効果は、フレームの高速転送を可能に出来ることである。

【１４３５】

これは、高速化エンジンを利用することで、ゲートウェイ装置におけるＣＰＵ（ソフトウェア処理）によるカプセル化処理および暗号化／復号化処理を排除し、これら処理をすべて高速化エンジン（ハードウェア）で実現できる為である。

【１４３６】

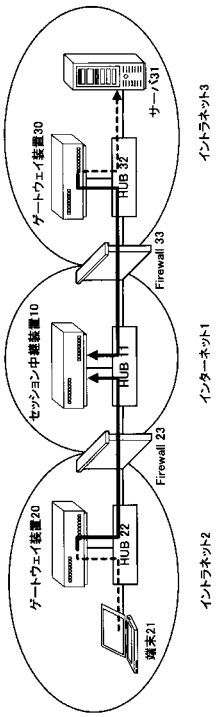
更に、これは、ゲートウェイ装置とセッション中継装置との間の通信において、ヘッダＦ１３の位置のＴＣＰによる輻輳制御と再送制御が発生しないよう、セッション中継装置内の中間ドライバと、ゲートウェイ装置内の中間ドライバにおいて、ＴＣＰを終端し、ＴＣＰ　ｏｖｅｒ　ＴＣＰ問題の発生を回避しているからである。

【１４３７】

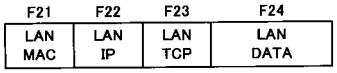
又、これは、端末２１とサーバ３１との間の通信において、ヘッダＦ２３の位置のＴＣＰによる輻輳制御と再送制御が発生しないよう、端末２１内の中間ドライバと、サーバ３１内の中間ドライバにおいて、端末２１内のＴＣＰと、サーバ３１内のＴＣＰを終端し、ＴＣＰ　ｏｖｅｒ　ＴＣＰ問題の発生を回避しているからである。

【１４３８】
又、これは、ゲートウェイ装置において、暗号化および復号化の処理をハードウェア化し、ＳＳＬの処理を高速化しているからである。
【１４３９】
本発明の第２の効果は、高速化処理の為のハードウェア（高速化エンジン）の開発コストや部材コストを、比較的低く抑えることが出来る。
【１４４０】
これは、暗号化／復号化とカプセル化を同一ハードウェア（ＦＰＧＡ／ＡＳＩＣ）上で行うことが出来るからである。
【１４４１】
又、これは、比較的安価なＭＡＣとＰＨＹ間のインタフェースに、ハードウェアを実装することが出来るからである。
【１４４２】
又、これは、ハードウェアへの実装が難しいＴＣＰ処理をソフトウェアに残し、ハードウェアへの実装が比較的容易でかつ高速化処理の効果が大きな、暗号化／復号化とカプセル化のみをハードウェア処理できるからである。

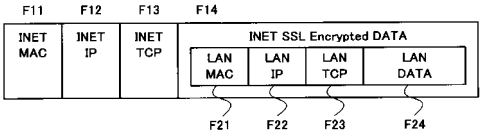
【図１】



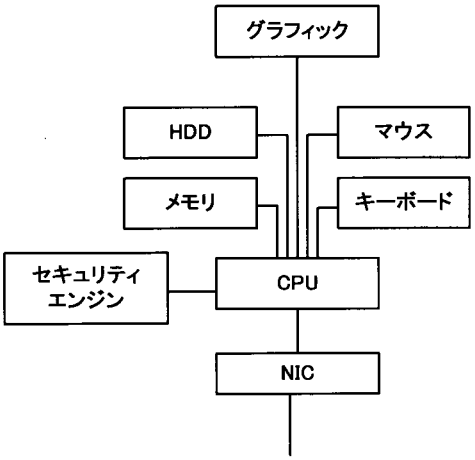
【図２】



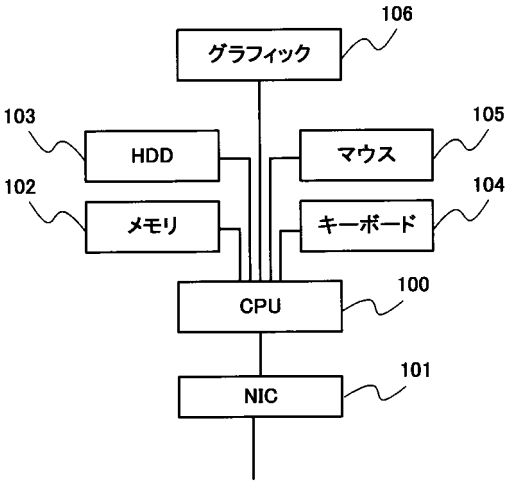
【図３】



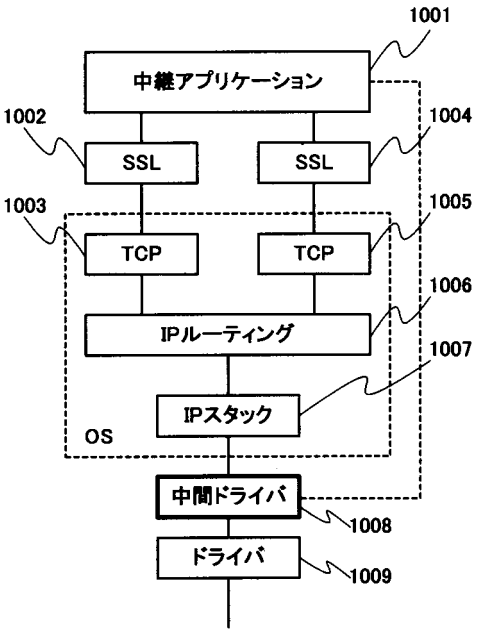
【図４】


グラフィック
HDD
マウス
メモリ
キーボード
セキュリティ
エンジン
CPU
NIC

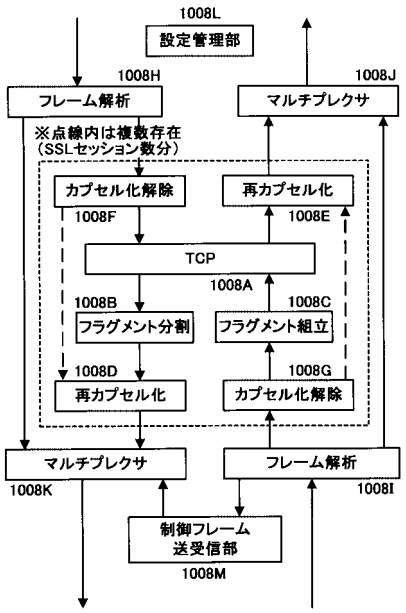
【図５】


106
グラフィック
103
HDD
105
マウス
102
メモリ
104
キーボード
CPU
100
NIC
101

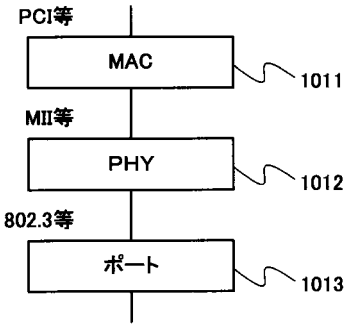
【図６】


1001
中継アプリケーション
1002
SSL
SSL
1004
1003
1005
TCP
TCP
1006
IPルーティング
1007
IPスタック
OS
中間ドライバ
1008
ドライバ
1009

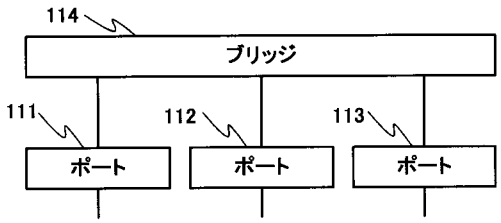
【図７】


1008L
設定管理部
1008H
フレーム解析
1008J
マルチプレクサ
※点線内は複数存在
（SSLセッション数分）
カプセル化解除
再カプセル化
1008F
1008E
TCP
1008A
1008B
1008C
フラグメント分割
フラグメント組立
1008D
1008G
再カプセル化
カプセル化解除
マルチプレクサ
フレーム解析
1008K
1008I
制御フレーム
送受信部
1008M

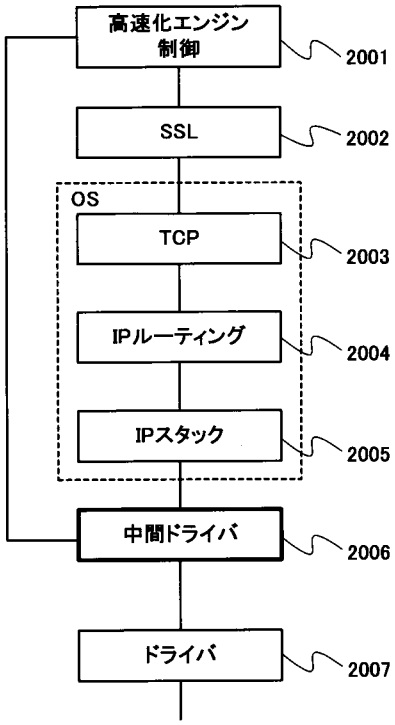
【図８】



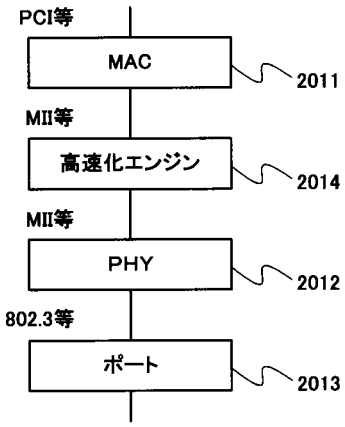
【図９】



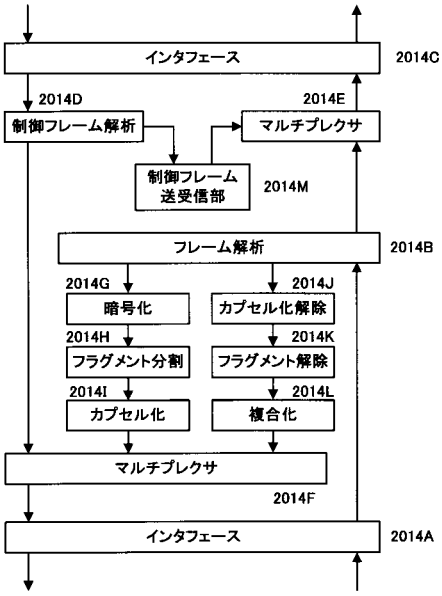
【図１０】



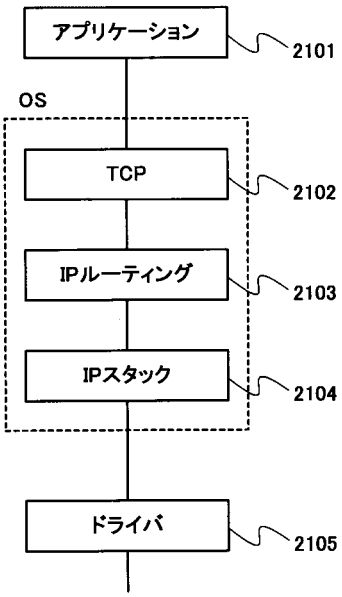
【図１１】



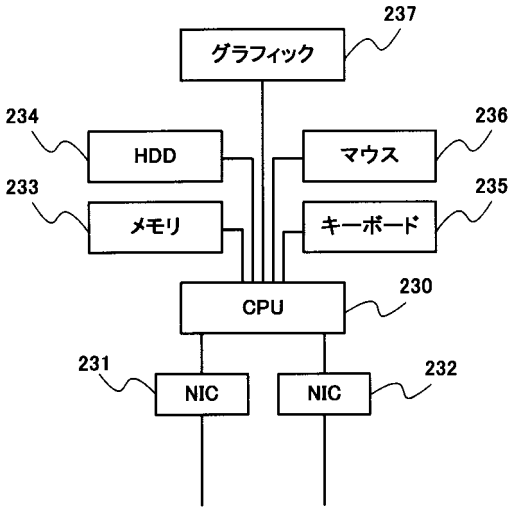
【図１２】



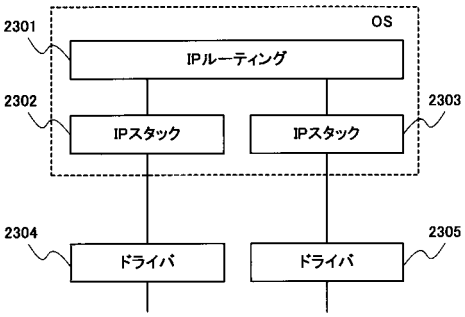
【図１３】



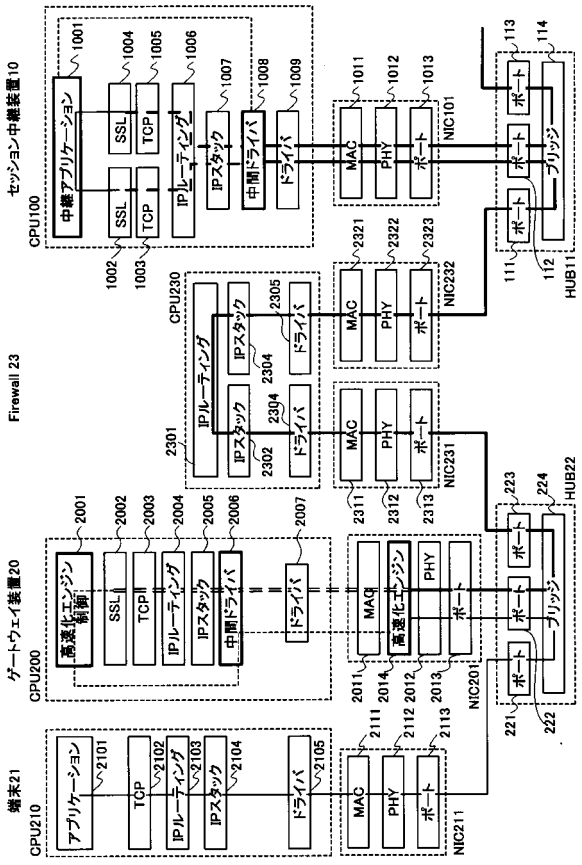
【図１４】



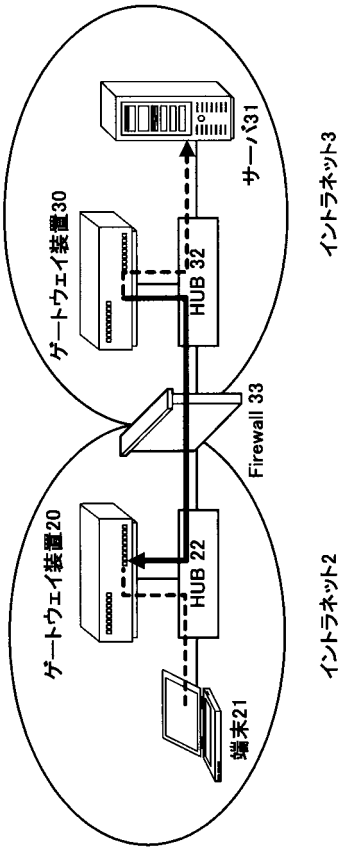
【図１５】



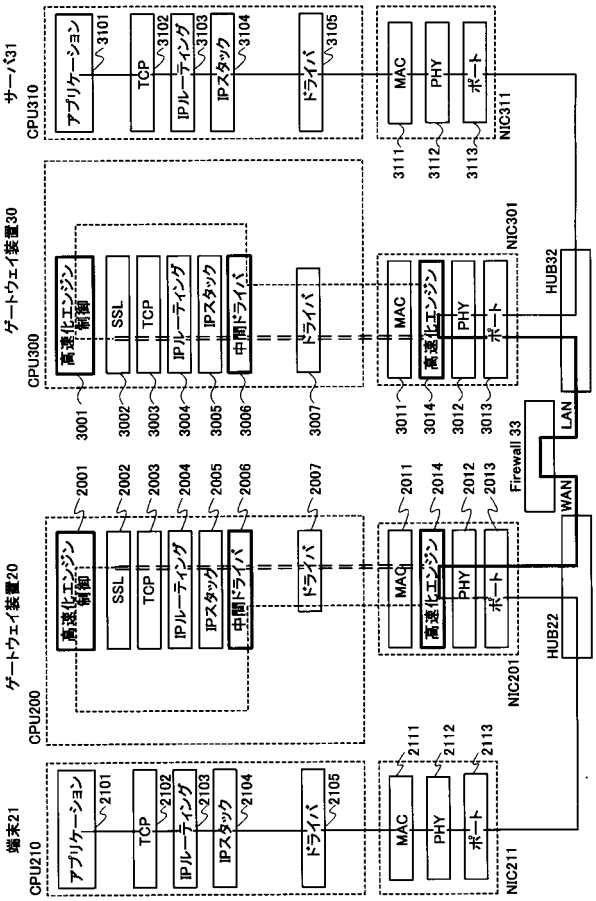
【図１６】



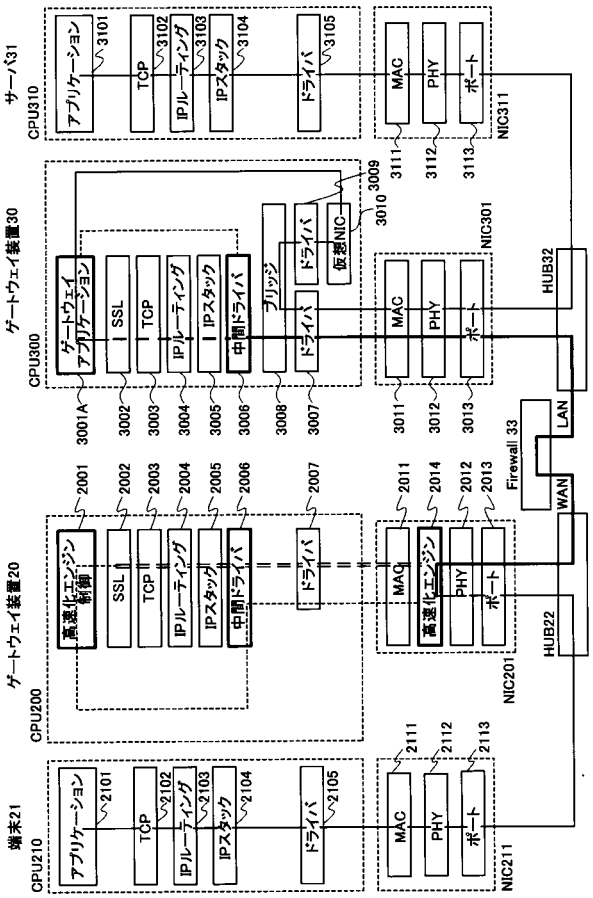
【図１７】



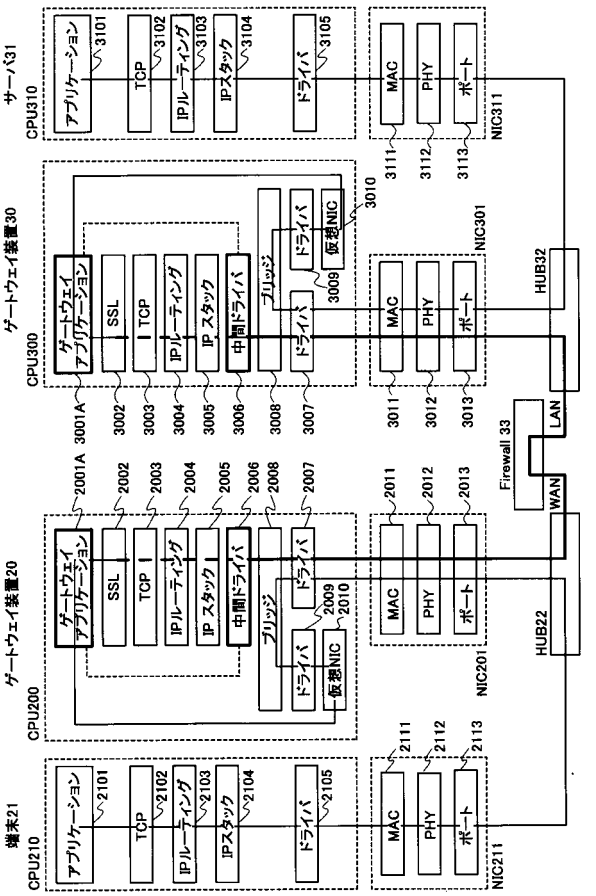
【図１８】



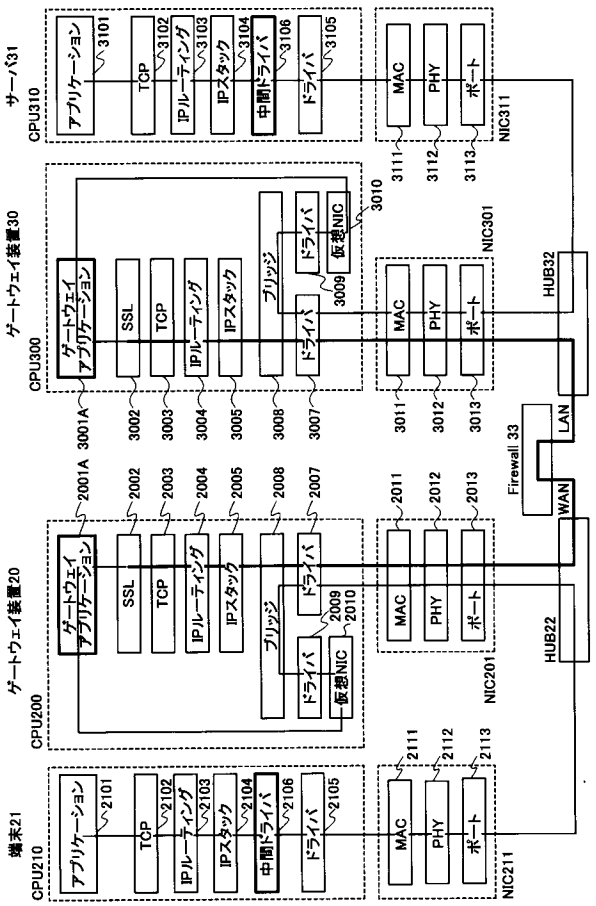
【図１９】



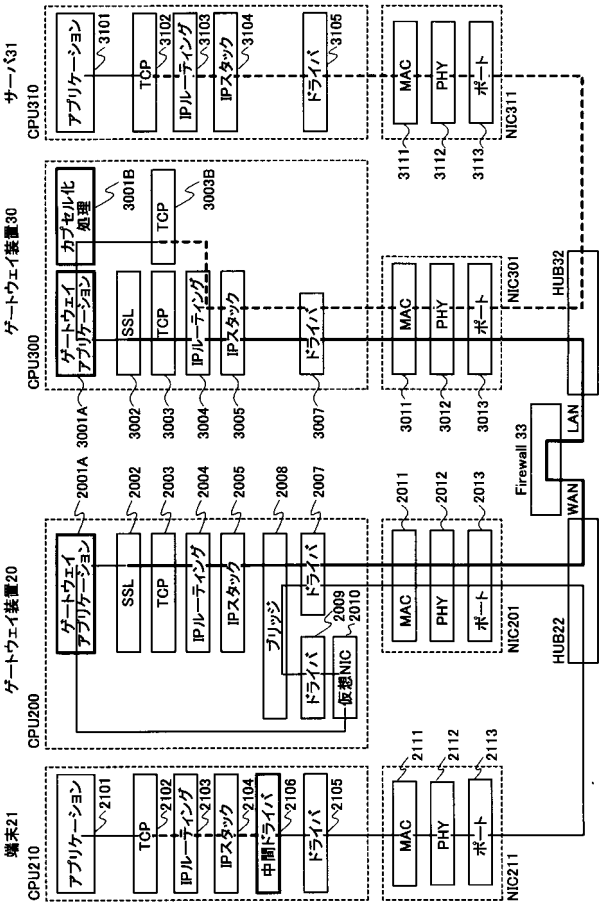
【図２０】



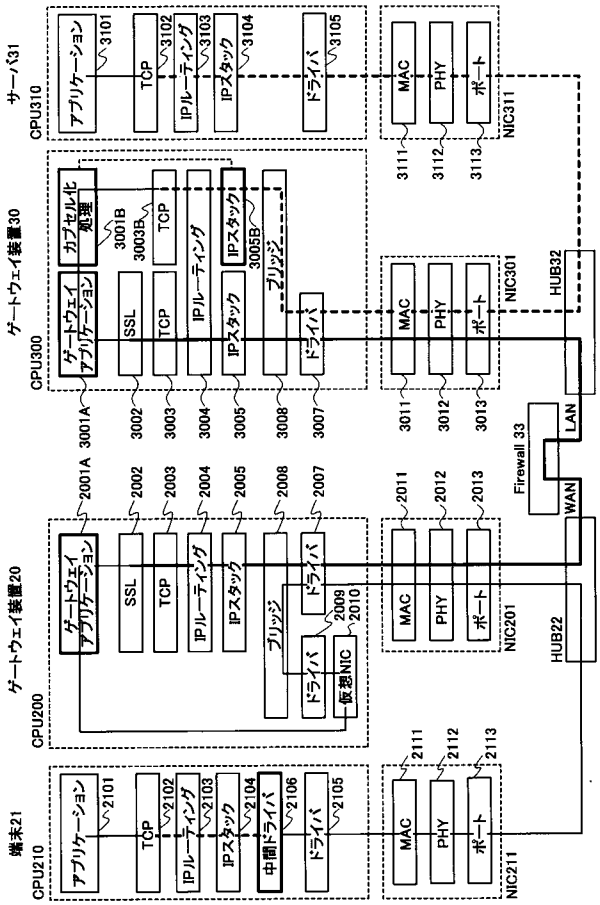
【図２１】



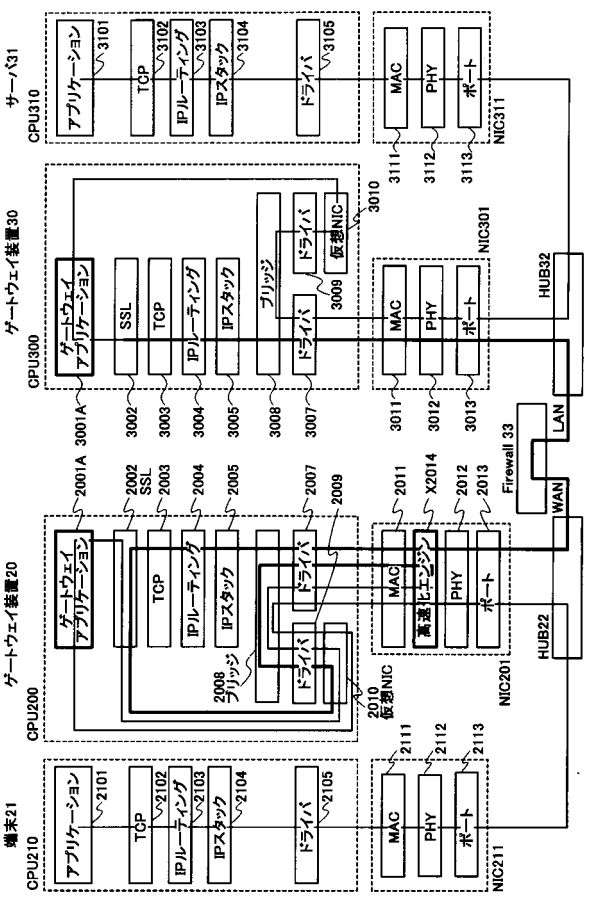
【図２２】



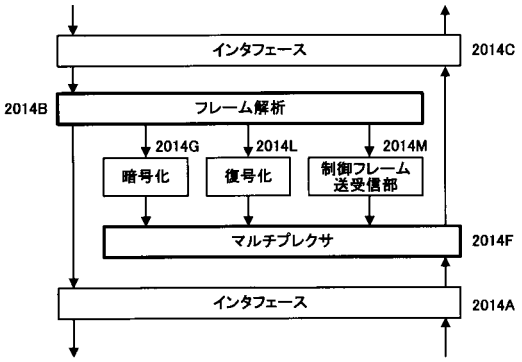
【図２３】



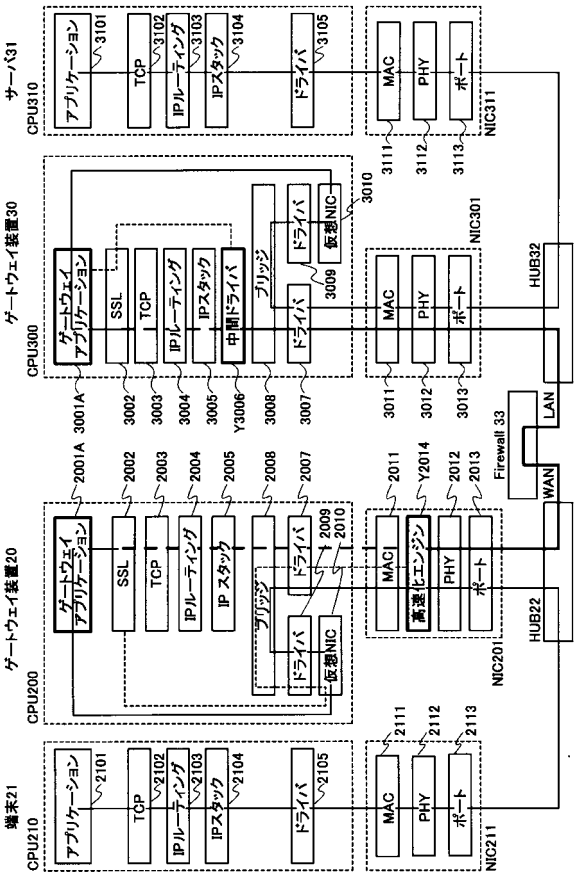
【図２４】



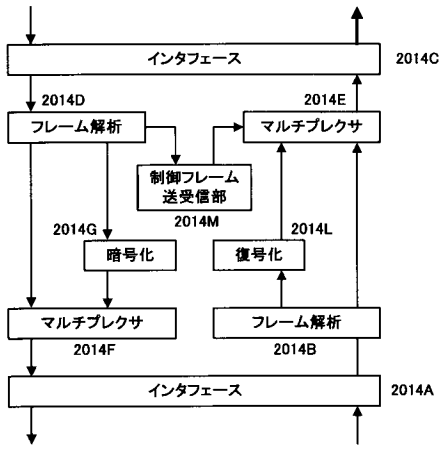
【図２５】



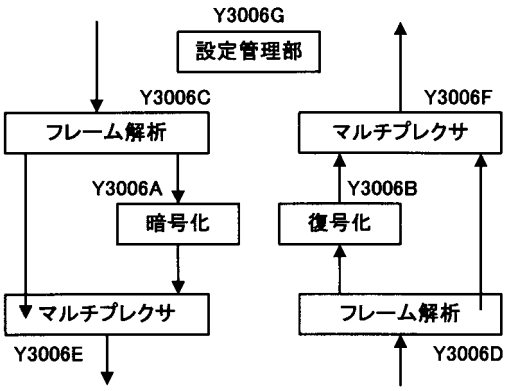
【図２６】



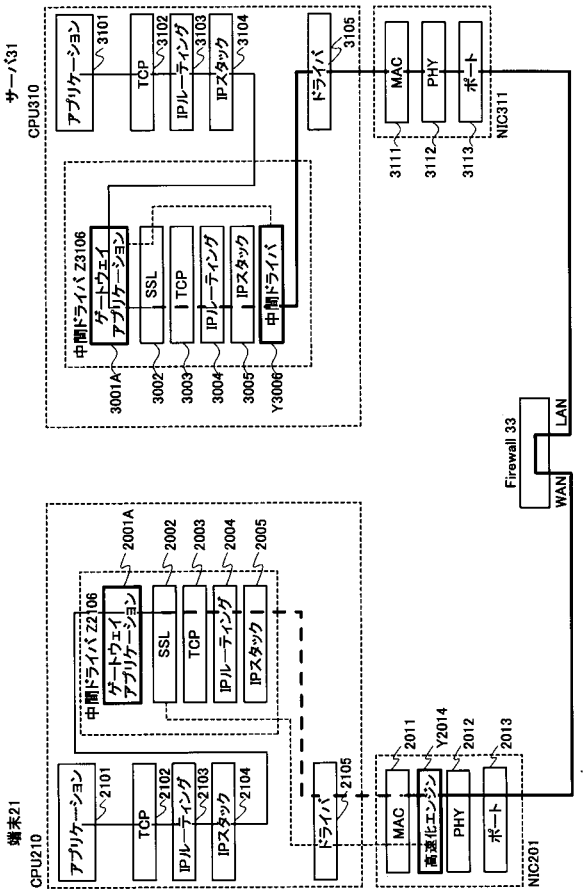
【図２７】



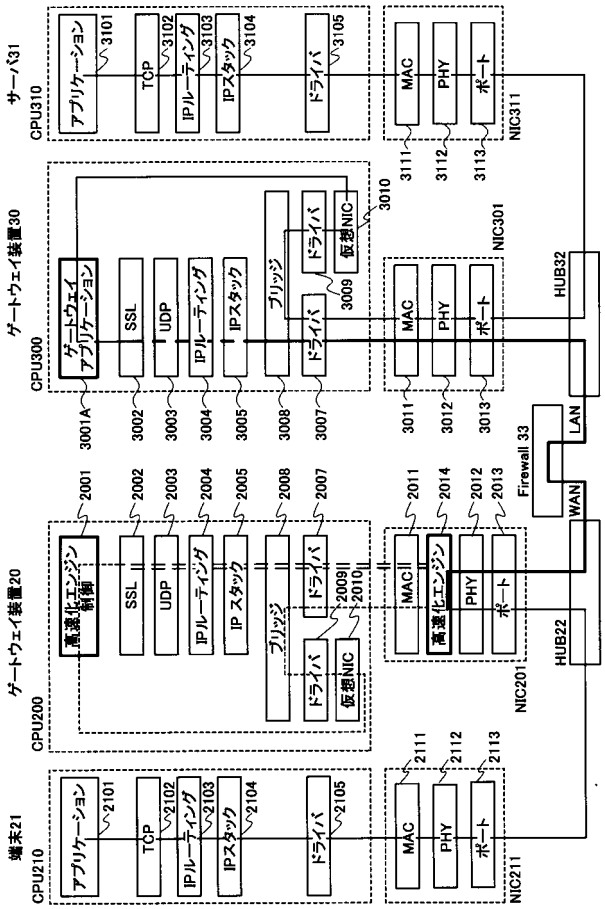
【図２８】



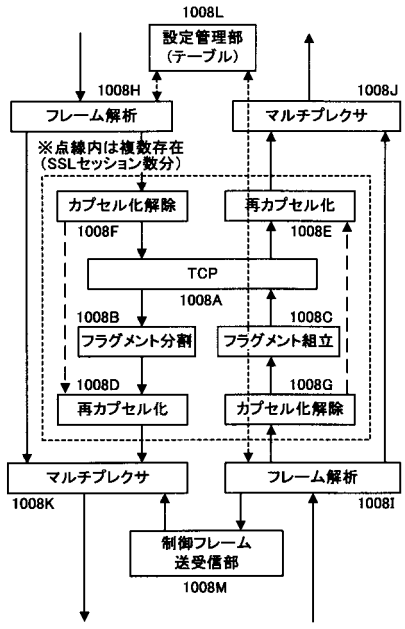
【図２９】



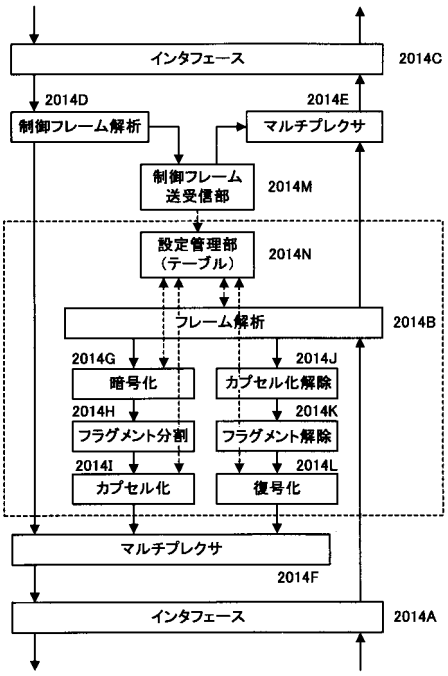
【図３０】



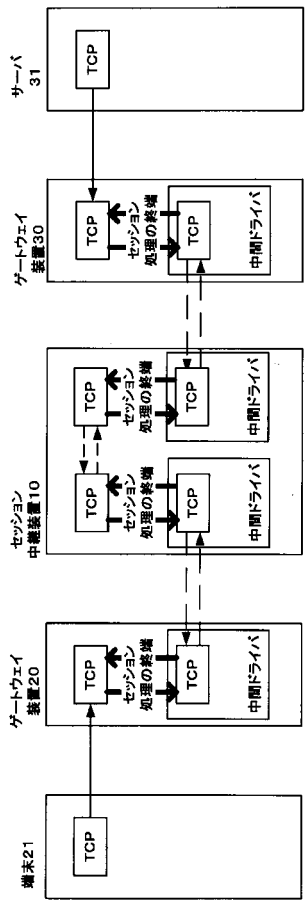
【図３１】



【図３２】



【図３３】



【手続補正書】
【提出日】平成18年12月28日(2006.12.28)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【書類名】請求の範囲
【請求項１】（削除）
【請求項２】（削除）
【請求項３】（削除）
【請求項４】（削除）
【請求項５】（削除）
【請求項６】（削除）
【請求項７】（削除）
【請求項８】（削除）
【請求項９】（削除）
【請求項１０】（削除）
【請求項１１】（削除）
【請求項１２】（削除）
【請求項１３】（削除）
【請求項１４】（削除）
【請求項１５】（削除）
【請求項１６】（削除）
【請求項１７】（削除）

【請求項１８】（削除）
【請求項１９】（削除）
【請求項２０】（削除）
【請求項２１】（削除）
【請求項２２】（削除）
【請求項２３】（削除）
【請求項２４】（削除）
【請求項２５】（削除）
【請求項２６】（削除）
【請求項２７】（削除）
【請求項２８】（削除）
【請求項２９】（削除）
【請求項３０】　通信システムであって、
　トンネル経路を確立させる一対のトンネル設定手段と、
　前記トンネル経路を介して通信する端末と
を有し、
　前記トンネル設定手段は、
　対向するトンネル設定手段宛にＴＣＰセッションを用いて前記トンネル経路を確立させるための接続要求を発呼する高速エンジン制御部と、
　前記接続要求に呼応してＴＣＰセッションを終端させ、対向するトンネル設定手段と輻輳制御の無いセッションを用いてトンネル経路を確立した後にそのトンネル経路のヘッダ情報を送信する中間ドライバと、
　前記ヘッダ情報を保持し、前記端末の送信側からのフレームに前記保持しているヘッダ情報を追加して対向となるトンネル設定手段に向けて転送する転送手段と
を有することを特徴とする通信システム。
【請求項３１】前記転送手段は、対向するトンネル設定手段からのフレームに記載された前記ヘッダ情報を削除して端末に転送することを特徴とする請求項３０に記載の通信システム。
【請求項３２】前記転送手段は、前記確立したトンネル経路を用いて暗号化通信する際の暗号鍵を保存し、高速化処理開始命令を受信すると、この保存した暗号鍵を用いて前記通信装置間で送受信されるデータの暗号化又は復号化を行う暗号化手段を有することを特徴とする請求項３０又は請求項３１に記載の通信システム。
【請求項３３】通信システムであって、
　トンネル経路を確立させる一対のトンネル設定手段と、
　前記トンネル経路を介して通信する端末と
を有し、
　前記トンネル設定手段は、
　前記トンネル経路を用いて暗号化通信する際の暗号鍵を取得する暗号鍵取得手段と、
　前記取得した暗号鍵を保存し、高速化処理開始命令を受信すると、この保存した暗号鍵を用いて前記トンネル経路を介して送信するフレームを暗号化する暗号化と、
　前記暗号化されたフレームに暗号化ヘッダ並びにカプセル化ヘッダの付加を行って対向するトンネル設定手段に送信するカプセル化部と、
　受信したフレームからカプセル化ヘッダ並びに暗号化ヘッダを削除するカプセル化解除部と、
　前記カプセル化ヘッダ並びに暗号化ヘッダが削除されたフレームを前記保存した暗号鍵を用いて復号する復号化部と
を有することを特徴とする通信システム。
【請求項３４】通信システムであって、
　トンネル経路を確立させる一対のトンネル設定手段と、
　前記トンネル経路を介して通信する端末と

を有し、
前記トンネル設定手段は、対向するトンネル設定手段とＴＣＰセッションを用いてトンネル経路を確立させた後、前記ＴＣＰセッションを用いずに前記端末間を通信させるように構成されていることを特徴とする通信システム。
【請求項３５】通信装置であって、
トンネル経路の確立先宛にＴＣＰセッションを確立させるための接続要求を発呼する高速エンジン制御部と、
前記接続要求に呼応してＴＣＰセッションを終端させ、前記トンネル経路の確立先と輻輳制御の無いセッションをもちいてトンネル経路を確立した後にそのトンネル経路のヘッダ情報を送信する中間ドライバと、
前記ヘッダ情報を保持し、送信されてきたフレームに前記保持しているヘッダ情報を追加して前記トンネル経路の確立先に向けて転送する転送手段と
を有することを特徴とする通信装置。
【請求項３６】 前記転送手段は、前記トンネル経路の確立先から送信されてきたフレームに記載された前記ヘッダ情報を削除して端末に転送することを特徴とする請求項３５に記載の通信システム。
【請求項３７】前記転送手段は、前記確立したトンネル経路を用いて暗号化通信する際の暗号鍵を保存し、高速化処理開始命令を受信すると、この保存した暗号鍵を用いて前記通信装置間で送受信されるデータの暗号化又は復号化を行う暗号化手段を有することを特徴とする請求項３５又は請求項３６に記載の通信装置。
【請求項３８】トンネル経路を介して通信する通信装置であって、
前記トンネル経路を用いて暗号化通信する際の暗号鍵を取得する暗号鍵取得手段と、
前記取得した暗号鍵を保存し、高速化処理開始命令を受信すると、この保存した暗号鍵を用いて前記トンネル経路を介して送信するフレームを暗号化する暗号化部と、
前記暗号化されたフレームに暗号化ヘッダ並びにカプセル化ヘッダを付加して、トンネル経路の確立先に送信するカプセル化部と、
トンネル経路の確立先からのフレームからカプセル化ヘッダ並びに暗号化ヘッダを削除するカプセル化解除部と、
前記カプセル化ヘッダ並びに暗号化ヘッダが削除されたフレームを前記保存した暗号鍵を用いて復号する復号化部と
を有することを特徴とする通信装置。
【請求項３９】確立されたトンネル経路を介して通信する通信装置であって、
トンネル経路の確立先とＴＣＰセッションを用いてトンネル経路を確立させた後、前記ＴＣＰセッションを用いずに前記確立されたトンネル経路を用いて通信するように構成されていることを特徴とする通信装置。
【請求項４０】確立されたトンネル経路を介して通信する通信方法であって、
トンネル経路の確立先にＴＣＰセッションを用いて前記トンネル経路を確立させるための接続要求を発呼する発呼ステップと、
前記接続要求に呼応してＴＣＰセッションを終端させる終端ステップと、
前記トンネル経路の確立先と輻輳制御の無いセッションを用いてトンネル経路を確立する確立ステップと、
前記トンネル経路のヘッダ情報を保存する保存ステップと、
端末からのフレームに前記保存したヘッダ情報を追加して、前記トンネル経路の確立先に送信する送信ステップと、
前記トンネル経路の確立先からのフレームに記載された前記ヘッダ情報を削除して端末に転送する転送ステップと
を有することを特徴とする通信方法。
【請求項４１】前記送信ステップは、
前記確立したトンネル経路を用いて暗号化通信する際の暗号鍵を保存する保存ステップと、

高速化処理開始命令を受信すると、前記保存した暗号鍵を用いて前記トンネル経路の確立先に送信するデータの暗号化を行う暗号化ステップと
を有することを特徴とする請求項４０に記載の通信方法。
【請求項４２】前記送信ステップは、
前記確立したトンネル経路を用いて暗号化通信する際の暗号鍵を保存する保存ステップと、
高速化処理開始命令を受信すると、前記保存した暗号鍵を用いて前記トンネル経路の確立先からのデータを復号化する複合化ステップと
を有することを特徴とする請求項４０又は請求項４１に記載の通信方法。
【請求項４３】確立されたトンネル経路を介して通信する通信方法であって、
前記トンネル経路を用いて暗号化通信する際の暗号鍵を取得する暗号鍵取得ステップと、
前記取得した暗号鍵を保存し、高速化処理開始命令を受信すると、この保存した暗号鍵を用いて前記トンネル経路を介して送信するフレームを暗号化する暗号化ステップと、
前記暗号化されたフレームに暗号化ヘッダ並びにカプセル化ヘッダの付加を行ってトンネル経路の確立先に送信する送信ステップと、
受信したフレームからカプセル化ヘッダ並び暗号化ヘッダを削除するカプセル化解除ステップと、
前記カプセル化ヘッダ並びに暗号化ヘッダが削除されたフレームを前記保存した暗号鍵を用いて復号する復号化ステップと
を有することを特徴とする通信方法。
【請求項４４】確立されたトンネル経路を介して通信する通信方法であって、
ＴＣＰセッションを用いて、トンネル経路を確立させる確立ステップと、
前記ＴＣＰセッションを用いずに、前期トンネル経路を介して端末間を通信させる通信ステップと
を有することを特徴とする通信方法。
【請求項４５】通信装置のプログラムであって、前記プログラムは前記通信装置を、
トンネル経路の確立先宛にＴＣＰセッションを確立させるための接続要求を発呼する高速エンジン制御部と、
前記接続要求に呼応してＴＣＰセッションを終端させ、前記トンネル経路の確立先と輻輳制御の無いセッションをもちいてトンネル経路を確立した後にそのトンネル経路のヘッダ情報を送信する中間ドライバと、
前記ヘッダ情報を保持し、送信されてきたフレームに前記保持しているヘッダ情報を追加して前記トンネル経路の確立先に向けて転送する転送手段と
して機能させることを特徴とするプログラム。
【請求項４６】トンネル経路を介して通信する通信装置のプログラムであって、前記プログラムは前記通信装置を、
前記トンネル経路を用いて暗号化通信する際の暗号鍵を取得する暗号鍵取得手段と、
前記取得した暗号鍵を保存し、高速化処理開始命令を受信すると、この保存した暗号鍵を用いて前記トンネル経路を介して送信するフレームを暗号化する暗号化部と、
前記暗号化されたフレームに暗号化ヘッダ並びにカプセル化ヘッダを付加して、トンネル経路の確立先に送信するカプセル化部と、
トンネル経路の確立先からのフレームからカプセル化ヘッダ並びに暗号化ヘッダを削除するカプセル化解除部と、
前記カプセル化ヘッダ並びに暗号化ヘッダが削除されたフレームを前記保存した暗号鍵を用いて復号する復号化部と
して機能させることを特徴とするプログラム。
【請求項４７】　トンネル経路を介して通信する通信装置のプログラムであって、前記プログラムは前記通信装置を、
トンネル経路の確立先とＴＣＰセッションを用いてトンネル経路を確立させた後、前記

ＴＣＰセッションを用いずに前記確立されたトンネル経路を用いて通信する手段として機能させることを特徴とするプログラム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/303294

A. CLASSIFICATION OF SUBJECT MATTER
H04L12/56(2006.01), ***H04L9/08***(2006.01), ***H04L29/08***(2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L12/56(2006.01), ***H04L9/08***(2006.01), ***H04L29/08***(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2006
Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2004-533138 A (Interdigital Acquisition Corp.), 28 October, 2004 (28.10.04), Abstract; Fig. 6 & US 2003/235206 A1 & EP 1397922 A & WO 2002/067599 A1 & CA 2438511 A & BR 207537 A & CN 1582583 A	1-4,6,10-13, 18-21,26-29 5,7,14,15, 22,23
X Y	JP 2004-304696 A (Matsushita Electric Industrial Co., Ltd.), 28 October, 2004 (28.10.04), Figs. 2, 26 (Family: none)	8,9,16,17, 24,25 5,7,14,15, 22,23

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 May, 2006 (09.05.06)	16 May, 2006 (16.05.06)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/303294

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-526266 A (HUGHES ELECTRONICS CORP.), 02 September, 2003 (02.09.03), Full text & EP 1232628 A & WO 2001/065805 A2 & NO 20015151 A & AU 5381301 A & CA 2356813 A & CN 1552147 A	1-29
A	Kana YAMANEGI et al., "TCP Proxy Kiko no Jitsu-network-jo deno Jisso Hyoka", IEICE Technical Report, Vol.104, No.658, 10 February, 2005 (10.02.05), pages 7 to 12	1-29

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/303294

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-7, 10-15, 18-23, 26-29 relate to a communication system having terminating means adapted for terminating the session of a TCP and provided between communication devices carrying out communication by setting up the TCP session.

The inventions of claims 8, 9, 16, 17, 24, 25 relate to a communication system having encryption key acquiring means and encrypting means both provided between communication devices carrying out encryption communication.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

the

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, payment of a protest fee..

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２００６／３０３２９４

Ａ． 発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl. *H04L12/56(2006.01), H04L9/08(2006.01), H04L29/08(2006.01)*

Ｂ． 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl. *H04L12/56(2006.01), H04L9/08(2006.01), H04L29/08(2006.01)*

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００６年
日本国実用新案登録公報	１９９６－２００６年
日本国登録実用新案公報	１９９４－２００６年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2004-533138 A (インターデジタル・アクイジション・コーポレイション) 2004.10.28, 要約, 図６ & US 2003/235206 A1 & EP 1397922 A & WO 2002/067599 A1	1-4, 6, 10-13, 18-21, 26-29
Y	& CA 2438511 A & BR 207537 A & CN 1582583 A	5, 7, 14, 15, 22, 23

☑ Ｃ欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ０９．０５．２００６	国際調査報告の発送日 １６．０５．２００６
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） ５Ｓ ３３６５ 石川 正二 電話番号 ０３－３５８１－１１０１ 内線 ３５４６

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００５年４月）

国際調査報告 | 国際出願番号 ＰＣＴ／ＪＰ２００６／３０３２９４

C（続き）． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2004-304696 A（松下電器産業株式会社）2004.10.28, 図2, 26 （ファミリーなし）	8,9,16,17, 24,25
Y		5,7,14,15, 22,23
A	JP 2003-526266 A（ヒューズ・エレクトロニクス・コーポレーション）2003.09.02, 全文 & EP 1232628 A & WO 2001/065805 A2 & NO 20015151 A & AU 5381301 A & CA 2356813 A & CN 1552147 A	1-29
A	山根木果奈ほか，ＴＣＰプロキシ機構の実ネットワーク上での実装評価，電子情報通信学会技術研究報告，Vol. 104, No. 658, 2005.02.10, 第7-12頁	1-29

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２００６／３０３２９４

第Ⅱ欄 請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第8条第3項（ＰＣＴ17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲＿＿＿＿＿＿＿＿ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲＿＿＿＿＿＿＿＿ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲＿＿＿＿＿＿＿＿ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第3文の規定に従って記載されていない。

第Ⅲ欄 発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１－７，１０－１５，１８－２３，２６－２９に係る発明は、ＴＣＰセッションを確立させて通信する通信装置間に、ＴＣＰのセッションを終端させる終端手段を有する通信システムに関するものである。

請求の範囲８，９，１６，１７，２４，２５に係る発明は、暗号化通信する通信装置間に、暗号鍵取得手段と、暗号化手段とを有する通信システムに関するものである。

1．☑ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。

☑ 追加調査手数料の納付を伴う異議申立てがなかった。

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．ＥＴＨＥＲＮＥＴ
２．イーサネット
３．フロッピー
４．Ｌｉｎｕｘ

Ｆターム(参考) 5J104 AA16 AA32 EA04 EA15 EA16 JA03 JA21 NA02 NA37 PA07
5K030 GA01 GA15 HA08 HD03 KA05 LA02 LB01 LD19 LE14
5K034 EE11 HH06 HH11 LL01

（注）この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項(実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。