(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4482601号
(P4482601)

(45)発行日　平成22年6月16日(2010.6.16)　(24)登録日　平成22年3月26日(2010.3.26)

(51)Int.Cl.		F I		
H04L 12/56	(2006.01)	H04L	12/56	B
H04L 12/66	(2006.01)	H04L	12/66	B

請求項の数 12　(全 15 頁)

(21)出願番号	特願2008-505873 (P2008-505873)
(86)(22)出願日	平成18年4月7日 (2006.4.7)
(65)公表番号	特表2008-536418 (P2008-536418A)
(43)公表日	平成20年9月4日 (2008.9.4)
(86)国際出願番号	PCT/EP2006/061443
(87)国際公開番号	WO2006/108808
(87)国際公開日	平成18年10月19日 (2006.10.19)
審査請求日	平成21年1月22日 (2009.1.22)
(31)優先権主張番号	10/907,659
(32)優先日	平成17年4月11日 (2005.4.11)
(33)優先権主張国	米国(US)

早期審査対象出願

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100108501
弁理士　上野　剛史
(74)代理人　100112690
弁理士　太佐　種一
(74)代理人　100091568
弁理士　市位　嘉宏

最終頁に続く

(54)【発明の名称】ネットワーク・アドレス・ポート変換器によって扱われるクライアントからの重複ソースの防止

(57)【特許請求の範囲】

【請求項１】

接続を識別するためのネットワーク・アドレス、プロトコル、およびポート番号を使用するネットワーク・プロトコルにおける重複ソースの衝突を防止する方法であって、遠隔ソース・クライアントからの宛先ホストにおける接続上の受信パケットに応答して、前記接続を司るセキュリティ・アソシエーションに従うポート番号の範囲内でポート番号が利用可能であるかどうかを判断するステップと、利用可能なポート番号を前記接続に割り当てることによって、重複ソースの可能性を回避するステップと、前記接続を司るポート番号の前記範囲内で利用可能なポート番号がない場合に、前記パケットを拒絶するステップとを含む、方法。

【請求項２】

遠隔ソース・クライアント毎に割り当て可能なポート番号のリストと、前記リスト内の各ポート番号の前記割り当ておよび非割り当て状態とを保持するステップをさらに含む、請求項１に記載の方法。

【請求項３】

割り当て可能なポート番号の各リストは、ビット・ベクトルであって、ビット位置は、ポート番号を識別し、前記ビットの状態は、前記ポート番号の前記割り当ておよび非割り当て状態を表す、請求項２に記載の方法。

【請求項４】

各クライアント側の接続を変換されたポート番号に関連付けるソース・ポート変換テー

ブルを保持するステップをさらに含む、請求項１に記載の方法。
【請求項５】
前記ソース・ポート変換テーブルは、ソース・ポート・エントリと、変換されたソース・ポート・エントリとを含み、各ソース・ポート・エントリは、変換されたソース・ポート・エントリに固有に関連付けられ、各ソース・ポート・エントリは、インターネット・ソース・アドレスと、ＮＡＰＴによって割り当てられたＵＤＰソース・ポート番号と、クライアント・ソース・ポート番号と、クライアント・プロトコル識別子とを含み、各変換されたソース・ポート・エントリは、インターネット・ソース・アドレスと、変換されたクライアント・ソース・ポート番号と、クライアント・プロトコル識別子とを含み、ソース・ポート・エントリは、受信パケット上で検索されて、遠隔クライアント接続に以前に割り当てられたポート番号を識別し、変換されたソース・ポート・エントリは、送信パケット上で検索されて、以前に割り当てられた変換されたポート番号からクライアント・ポート番号を識別する、請求項４に記載の方法。
【請求項６】
接続を識別するためのネットワーク・アドレス、プロトコル、およびポート番号を使用するネットワーク・プロトコルにおける重複ソースを防止する方法であって、
ａ）パケットをサーバにおいて受信するステップと、
ｂ）前記パケットがネットワーク・アドレス・ポート変換器によって変換されており、カプセル化および暗号化されたパケットを含むかどうかを判断するステップと、
ｃ）前記パケットが変換されており、カプセル化および暗号化されたパケットを含む場合には、前記カプセル化されたパケットを復号化して、元の接続情報を得るステップと、
ｄ）前記接続を司るセキュリティ・アソシエーションに適合するポート番号の範囲内でポート番号が利用可能かどうかを判断するステップと、
ｅ）利用可能なポート番号を前記接続に割り当てることによって、重複ソースの可能性を回避するステップと、
ｆ）前記接続を司るポート番号の前記範囲内でポート番号が利用可能でない場合に、前記パケットを拒絶するステップと
を含む、方法。
【請求項７】
接続毎に割り当て可能なポート番号のリストと、前記リスト内の各ポート番号の割り当ておよび非割り当て状態とを保持するステップをさらに含む、請求項６に記載の方法。
【請求項８】
割り当て可能なポート番号の各リストは、ビット・ベクトルであって、ビット位置は、ポート番号を識別し、前記ビットの状態は、前記ポート番号の前記割り当ておよび非割り当て状態を表す、請求項７に記載の方法。
【請求項９】
接続を識別するためのネットワーク・アドレス、プロトコル、およびポート番号を使用するネットワーク・プロトコルにおける重複ソースの衝突を防止するための装置であって、遠隔ソース・クライアントからの宛先ホストにおける接続上の受信パケットに応答して、前記接続を司るセキュリティ・アソシエーションに従うポート番号の範囲内でポート番号が利用可能であるかどうかを判断するための手段と、利用可能なポート番号を前記接続に割り当てることによって、重複ソースの可能性を回避するための手段と、前記接続を司るポート番号の前記範囲内で利用可能なポート番号がない場合に、前記パケットを拒絶するための手段とを備える、装置。
【請求項１０】
接続を識別するためのネットワーク・アドレス、プロトコル、およびポート番号を使用するネットワーク・プロトコルにおける重複ソースを防止するための装置であって、
ａ）パケットをサーバにおいて受信するための手段と、
ｂ）前記パケットがネットワーク・アドレス・ポート変換器によって変換されており、カプセル化および暗号化されたパケットを含むかどうかを判断するための手段と、

ｃ）カプセル化されたパケットを復号化して、元の接続情報を得るための手段と、
ｄ）前記接続を司るセキュリティ・アソシエーションに適合するポート番号の範囲内でポート番号が利用可能かどうかを判断するための手段と、
ｅ）利用可能なポート番号を前記接続に割り当てることによって、重複ソースの可能性を回避するための手段と、
ｆ）前記接続を司るポート番号の前記範囲内でポート番号が利用可能でない場合に、前記パケットを拒絶するための手段と
を含む、装置。
【請求項１１】
コンピュータにロードされると、前記コンピュータに対して、接続を識別するためのネットワーク・アドレス、プロトコル、およびポート番号を使用するネットワーク・プロトコルにおける重複ソースの衝突を防止する方法を行わせるプログラム命令を記憶するための記憶媒体であって、前記命令は、遠隔ソース・クライアントからの宛先ホストにおける接続上の受信パケットに応答して、前記接続を司るセキュリティ・アソシエーションに従うポート番号の範囲内でポート番号が利用可能であるかどうかを判断するための命令と、利用可能なポート番号を前記接続に割り当てることによって、重複ソースの可能性を回避するための命令と、前記接続を司るポート番号の前記範囲内で利用可能なポート番号がない場合に、前記パケットを拒絶するための命令とを備える、記憶媒体。
【請求項１２】
請求項１～８のいずれか１つに記載の方法の各ステップをコンピュータに実行させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般的には、インターネット・ネットワーキングに関し、特定的には、ネットワーク・アドレスおよびポート変換によって生じる衝突に対する対応に関する。
【背景技術】
【０００２】
本明細書において、インターネットとインターネット通信の基礎を形成するＴＣＰ／ＩＰプロトコルとの観点から、問題と解決策とを説明する。しかしながら、本発明は、プロトコルの詳細によっては、他の通信プロトコルにも同様に提供可能である。
【０００３】
インターネット・ネットワーク・アドレス変換を使用する理由はいくつかある。主な理由は、公開アドレスの使用を節約することである。ネットワーク・アドレス変換器（ＮＡＴ）のインターネット・プロトコル（ＩＰ）アドレスは、一般的には公開アドレスである。すなわち、ＮＡＴ　ＩＰアドレスは、外部世界に知られているが、ＮＡＴの背後にあるサーバまたはクライアントのすべては、プライベート・アドレスであり、外部世界には知られていない。そのような場合、外部世界は、ＮＡＴと通信を行い、ＮＡＴは、その背後にある適切なサーバおよびクライアントとの通信を制御する。これは、ＮＡＴの背後にある装置のＩＰアドレスは当該ファミリー内で固有であればよいが、世界のその他におけるＩＰアドレスは重複している可能性がある。ＮＡＴは、ＩＰアドレスの変換のみに関与する。さらに、ネットワーク・アドレス・ポート変換（ＮＡＰＴ）として知られる種類の変換があり、ここでは、ＩＰアドレスおよびポート番号の両方が変換される。ネットワーク・アドレス変換（ＮＡＴ）およびネットワーク・アドレス・ポート変換（ＮＡＰＴ）のための規格は、インターネット技術標準化委員会（ＩＥＴＦ）の、「Ｔｒａｄｉｔｉｏｎａｌ　ＩＰ　Ｎｅｔｗｏｒｋ　Ａｄｄｒｅｓｓ　Ｔｒａｎｓｌａｔｉｏｎ」という名称のＲＦＣ３０２２に記載されている。
【０００４】
元来のインターネットは、セキュリティを主要な要素として設計されていない。実際、インターネットは、科学的および教育的通信に対する支援として、意図的に比較的オープ

ンに作られた。しかしながら、ウェブの出現とその商用によって、安全なインターネット通信に対する必要性が増している。一般的にはＩＰｓｅｃとして知られるインターネット・セキュリティ・プロトコルは、これらの問題に対処するために定義されていた。例えば、ＩＰｓｅｃは、ネットワーク装置の認証または送信データの暗号化もしくはその両方を提供する。ソース・アドレスと宛先アドレスとの間のＩＰｓｅｃ通信は、セキュリティ・アソシエーション（ＳＡ）に従って管理される。ＳＡは、通信に適用されるＩＰｓｅｃ処理を定義する１つ以上の規則である。ＩＰｓｅｃは、ＲＦＣ２４０１および他のＲＦＣに定義されている。パケットが拒否されるか、ＩＰｓｅｃ処理なしで許可されるか、またはＩＰｓｅｃ処理ありで許可されるかどうかは、必要に応じて動的にセキュリティ・ポリシー・データベース（ＳＰＤ）内のセキュリティ規則を有するパケットの属性を照合することによって判断される。この判断を行うために、既知の技術は、送信および受信パケットの両方に関する最も特定性の高い属性から最も特定性の低い属性の順で、静的および動的規則を検索する。静的規則のセットが、実質的にはセキュリティ規則である。静的規則は、予め定義付けられており、一般的にはあまり頻繁に変化しない。動的規則は、ＩＫＥ（インターネット鍵交換）処理中に必要に応じてノード間で交渉され、セキュリティ・ポリシー・データベースに追加される規則である。ＩＢＭ社の米国特許第６３４７３７６号は、ＳＰＤの動的規則を検索する好ましい一方法を記載する。

【０００５】

ネットワーク・アドレスまたはポート変換とＩＰｓｅｃ処理との間には、固有の不適合性が存在する。このような不適合性が、ＩＰｓｅｃの配置には障壁となる。ＲＦＣ３７１５は、このような不適合性のいくつかを認識し説明しているが、一般的な解決策は提供していない。例えば、ＲＦＣ３７１５の第４．１節は、ＲＦＣ３４５６「Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ（ＤＨＣＰｖ４，Ｃｏｎｆｉｇｕｒａｔｉｏｎ ｏｆ ＩＰｓｅｃ Ｔｕｎｎｅｌ Ｍｏｄｅ）」に提案された限定的な解決策を示しているが、より一般的な解決策が必要とされていることを述べている。加えて、ＩＥＴＦのＩＰｓｅｃワーキング・グループからの「ＵＤＰ Ｅｎｃａｐｓｕｌａｔｉｏｎ ｏｆ ＩＰｓｅｃ パケット」という名称のＲＦＣ３９４８の第５節も、不適合性のいくつかの問題に対処している。特に、ＲＦＣ３９４８の第５．２節は、ＮＡＰＴによって扱われるクライアントへの接続上でどんなＩＰｓｅｃセキュリティ・アソシエーションを使用するかを判断する問題について簡単に説明している。また、この節は、ＮＡＰＴがＩＰｓｅｃトラフィックも扱う場合にＮＡＰＴの背後のクライアントへのクリア・テキスト接続を可能にする他の問題について述べている。

【発明の開示】

【発明が解決しようとする課題】

【０００６】

よって、クライアントがＮＡＰＴで扱われる場合には、重複ソースを回避するという問題に対処する必要性がある。この問題に対しては、どの関連のＩＥＴＦ ＲＦＣも解決策を提供していない。本明細書の目的のために、重複ソースは、同一のソース・アドレス（例えば、ＩＰｓｅｃカプセル化された元のパケットに割り当てられたＮＡＰＴのＩＰアドレス）、同一のトランスポート・プロトコル、および同一の元ソース・ポート番号（すなわち、ＩＰｓｅｃカプセル化されたパケットのトランスポート・ヘッダにおけるポート番号）を有するパケットとして定義される。

【０００７】

重複ソースは、ネットワークの整合性を破る重複接続という結果をもたらす。例えば、パケットが誤った宛先に送られる可能性がある。

【０００８】

「Ｎｅｇｏｔｉａｔｉｏｎ ｏｆ ＮＡＴ‐Ｔｒａｖｅｒｓａｌ ｉｎ ｔｈｅ ＩＫＥ」という名称のＲＦＣ３９４７は、ＮＡＴトラバーサル・サポートためのＩＫＥ（インターネット鍵交換）のフェーズ１およびフェーズ２において必要とされるものを記述している。これには、パケット通信における両端がＮＡＴトラバーサルをサポートしているか

どうかを検出することと、ホストからホストへのパスに沿って１つ以上のＮＡＴがあるかどうかを検出することを含まれる。また、ＩＫＥクイック・モードにおけるユーザ・データグラム・プロトコル（ＵＤＰ）のカプセル化されたＩＰｓｅｃパケットの使用を交渉するやり方も含まれており、元ソースＩＰアドレスを他端に必要に応じて送信するやり方を記載している。ＵＤＰは、ＲＦＣ７６８に定義されている。ＲＦＣ３９４８である「ＵＤＰ　Ｅｎｃａｐｓｕｌａｔｉｏｎ　ｏｆ　ＩＰｓｅｃ　Ｐａｃｋｅｔｓ」は、ＮＡＴをトラバースするために、ＵＤＰパケット内部のＥＳＰ（カプセル化セキュリティ・ペイロード）パケットをカプセル化およびカプセル開放するための方法を定義している。ＥＳＰは、ＲＦＣ２４０６に定義されている。ＥＳＰは、ＩＰｖ４およびＩＰｖ６における混合セキュリティ・サービスを提供するように設計されている。

【課題を解決するための手段】

【０００９】

本発明は、ＮＡＰＴによって扱われるソース・アプリケーションを識別するためのソース・アドレス、プロトコル、およびソース・ポート番号を使用する接続におけるパケットの複製ソースを防止することに向けられている。パケットがサーバで受信されると、当該パケットが、ネットワーク・アドレス・ポート変換器（ＮＡＰＴ）を含む送信路のＥＳＰパケットをカプセル化するＵＤＰパケットかどうかについて判断する。この判断が合致すると、元パケットはカプセル開放されて、元のソース・ポート番号と、元のトランスポート・プロトコルとを取得する。接続を管理するセキュリティ・アソシエーションに適合するポート番号の範囲内でポート番号が利用可能どうかについて判断する。利用可能なポート番号が見つかると、当該接続に割り当てることによって、重複ソースの可能性を回避する。利用可能なポート番号が接続を管理するポート番号の範囲内になければ、当該パケットは拒絶される。

【００１０】

本発明の好ましい一実施形態を、以下の図面を参照して一例として説明する。

【発明を実施するための最良の形態】

【００１１】

しかしながら、本発明は、数多くの異なる形式で実施されてもよく、本明細書に記載された実施形態に限定されるものとして解釈すべきではない。むしろ、これらの実施形態は、本開示が徹底的かつ完全となり、本発明の範囲を当業者に対して完全に伝えるものとなるように提供される。対処される問題は、インターネット送信におけるトランスポート・モードおよびトンネル・モードの両方について存在するが、開示された実施形態は、主にトランスポート・モードに向けられている。説明する軽微な変形によって、トランスポート・モードに関する開示をトンネル・モードにおける動作のために適合させる。

【００１２】

本発明の実施形態は、ソフトウェア、ハードウェア、またはハードウェアおよびソフトウェアにおいて実施することができる。当業者によって理解されるように、本発明の実施形態は、完全にハードウェア実施形態、完全にソフトウェア（ファームウェア、常駐ソフトウェア、マイクロコードなどを含む）実施形態、またはソフトウェアおよびハードウェア局面を含む実施形態という形態を取ることができる。さらに、本発明の実施形態は、コンピュータまたは任意の命令実行システムによってまたはそれに関連して使用される媒体で実施されるプログラム・コード手段を有する、コンピュータ使用可能またはコンピュータ読み取り可能な記憶媒体上のコンピュータ・プログラム製品の形態を取ることができる。本明細書の場合、コンピュータ使用可能またはコンピュータ読み取り可能な媒体は、命令実行システム、装置、または機器によってまたはそれに関連して使用される、プログラムを包含、記憶、通信、伝播、または搬送することができる任意の手段でありうる。しかしながら、媒体は、例えば、電子的、磁気的、光学的、電磁的、赤外線、または半導体のシステム、装置、機器、または伝播媒体に限定されない。コンピュータ読み取り可能な媒体のより特定的な例（網羅したリストではない）には、１つ以上の線を有する電気接続、着脱可能なコンピュータ・ディスケット、ランダム・アクセス・メモリ（ＲＡＭ）、読み

出し専用メモリ（ＲＯＭ）、消去可能プログラム可能読み出し専用メモリ（ＥＰＲＯＭまたはフラッシュ・メモリ）、光ファイバ、携帯型コンパクト・ディスク読み出し専用メモリ（ＣＤ‐ＲＯＭ）が含まれるだろう。注意すべきは、コンピュータ使用可能またはコンピュータ読み取り可能な媒体は、プログラムを印刷可能な用紙または他の適した媒体であってさえよく、なぜならば、プログラムを例えば用紙または他の媒体の光走査を介して電子的に取り込んでから、コンパイル、解釈、または、そうでない場合には必要があれば適切なやり方での処理の後、コンピュータ・メモリに記憶することができるからである。

【００１３】

本説明において、同様の番号は、全体に渡って同様の構成要素を示す。

【００１４】

ＩＰｓｅｃ処理を使用して、パケットの内容をセキュリティ目的のために認証または暗号化することができる。認証および暗号化は、共にパケットに適用できるか、または、別個に適用できる。この説明を簡略化すると、ＩＰｓｅｃ処理の説明は、暗号化および復号化の観点でのパケットのカプセル化およびカプセル開放について述べている。説明の処理は、認証が単独に適用されていても、暗号化と共に適用されていても、等しく有効である。

【００１５】

ＩＰｓｅｃ処理がソース・クライアントからの送信パケットに適用されると、当該処理は、元ソースおよび宛先ポートならびにプロトコル・フィールドを暗号化し、この暗号化されたものをＵＤＰパケットにカプセル化する。元クライアント・ソースＩＰアドレスがＵＤＰパケットに保持されるが、ソース・ポート番号は、ＲＦＣ３９４８「ＵＤＰ Ｅｎｃａｐｓｕｌａｔｉｏｎ ｏｆ ＩＰｓｅｃ ＥＳＰ Ｐａｃｋｅｔｓ」に規定されているような４５００に設定される。ＵＤＰパケットはその後ＮＡＰＴへ送られ、ＮＡＰＴは、さらなる変換を行う。これらの変換は、図１および図２に対して以下に詳細に説明する。特に、ＮＡＰＴは、その自身のＩＰアドレスをクライアント・ソースＩＰアドレスの代わりに使用し、ＵＤＰヘッダに対する新規の固有のポート番号を割り当て、戻りパケットが元ソースに対してマッピングされるようにこれらの変換を追跡する。ＲＦＣ３９４８が説明する手法では、ＴＣＰまたはＵＤＰパケット内の元ソース・ポート番号は、ＮＡＰＴ装置によって変更されない。なぜならば、これは、ＩＰｓｅｃ ＥＳＰペイロードの一部として暗号化されている元トランスポート・ヘッダの一部だからである。その代わりに、上述のように、ＵＤＰカプセル化のために追加されたＵＤＰヘッダ内のポート番号が変更される。そのようなＩＰｓｅｃパケットがサーバによって受信されて暗号化されると、元ソースおよびパケットの宛先ポートを明らかにする。ＩＰｓｅｃを通じて処理されなかったパケットについては、ＮＡＰＴ装置は、元ソースＩＰアドレスおよびソース・ポートを変換する。暗号化されないパケットについては、ＮＡＰＴは、重複接続（重複ソース）がないことを保証する。

【００１６】

図１は、クライアントからサーバへ送られるようにネットワーク・パスに沿ったＩＰｓｅｃパケットの変換を示す。図２は、サーバからクライアントへの逆方向の戻りパケットの変換を示す。図１を参照して、ＩＰアドレス１０．１．１．１のクライアントは、ＩＰアドレス１１．１．１．１のサーバ宛の暗号化されたパケットを送出する。ＩＰｓｅｃによる処理以前のパケットの元の内容を１００に示す。１００の左欄はパケットのフィールド型を記述し、右欄はフィールド内容を示す。１００の宛先ＩＰアドレスは、２１１．１．１．１であり、実際の宛先サーバ１１．１．１．１の前のＮＡＴの公開アドレスである。ＮＡＴ２１１．１．１．１の役割は、パケットを１１．１．１．１のようなバックエンド・サーバにマッピングすることである。１００において、ソースおよび宛先ポートは、例示的にそれぞれ４０９６および２１に設定されている。ＩＰｓｅｃ処理後のパケットの内容を１０２に示す。パケット１０２の底部にある薄く網掛けされた部分は、ＩＰｓｅｃによって暗号化された部分を示す。１０２の濃く網掛けされた部分（および送信路の他の点におけるパケット内容）は、送信の当該点において変化または追加されたフィールドで

ある。１０２において、実際のソースおよび宛先ポートは、ＩＰｓｅｃによる４０９６および２１という暗号化された値であり、この時点では読み出し可能ではない。ＩＰｓｅｃ処理は、ＵＤＰヘッダを追加して、これが元クライアント・パケットのポートおよびプロトコルをカプセル化するＩＰｓｅｃパケットである旨を示す。ＩＰｓｅｃによって追加されたクリア・テキストＵＤＰヘッダ内のソースおよび宛先ポートは、ＲＦＣ３９４８によって必要に応じて４５００に設定されている。ＳＰＩ（セキュリティ・パラメータ・インデックス）フィールドは、例示的に２５６に設定されている。ＳＰＩフィールドは、セキュリティ・プロトコル（ＥＳＰまたはＡＨ）および宛先アドレスと共に、暗号化アルゴリズムおよびこれらのエンティティ間のセキュリティ・パラメータを司るクライアント１０．１．１．１とサーバ１１．１．１．１との間のセキュリティ・アソシエーションをポイントする。

【００１７】

１０２のパケットは、ＩＰアドレス２１０．１．１．１におけるＮＡＰＴによって変換されて、１０４に示すパケットとなる。この時点で、ＮＡＰＴ２１０．１．１．１は、ソースＩＰアドレスを変更して、２１０．１．１．１という自身のアドレスを反映させている。また、ＮＡＰＴは、新規の固有のソース・ポート番号を設定する。図１において、選択されたソース・ポート番号４５００から４５０１へ例示的に変更される。ＮＡＰＴ２１０．１．１．１は、サーバ１１．１．１．１からの戻りパケットと、クライアントＩＰ１０．１．１．１およびソース・ポート４５００からの今後の送信パケットとについて、この変換を追跡する。

【００１８】

１０４のパケットは、ＮＡＴ２１１．１．１．１によって、サーバ１１．１．１．１に対する入力パケットへ再変換する。この入力パケットを１０６に示す。実質的には、パケットの宛先ＩＰアドレスが、ＮＡＴ２１１．１．１．１によって、宛先サーバの実際の宛先アドレス１１．１．１．１にマッピングされる。パケットのＩＰｓｅｃ処理は、ソース１０．１．１．１．におけるＩＰｓｅｃ処理によって追加されたＵＤＰヘッダを除去して、実際のソースおよび宛先ポート番号を復旧させる。その後、１０８に示すような復旧されたパケットは、宛先ポート（本例では２１）へ送られて、アプリケーション処理に供される。

【００１９】

完全性のために、図２は、サーバ２１１．１．１．１から元クライアント１０．１．１．１への戻りパケット・フローを示す。このパケット・フローの詳細を説明する必要がないのは、対処される重複ソースの問題は、戻りパケットには生じないからである。

【００２０】

図１を再び参照すると、１０８のパケットは、ソース・アドレスとして、ＮＡＰＴ２１０．１．１．１のアドレスと、ソース・ポート・アドレス４０９６を含む。しかしながら、ＮＡＰＴ２１０１．１．１の背後にある例えば、１０．１．１．２という他のクライアントが、ソース・ポート４０９６からホスト１１．１．１．１へパケットを送っている可能性も高い。したがって、クライアント１０．１．１．１およびホスト１１．１．１．１間のパスにおけるＮＡＰＴがあるゆえに、衝突を生じさせる不正な重複ソースの可能性がある。

【００２１】

宛先ホストにおけるソース・ポート変換テーブル（ＳＰＴＴ、図３）を使用して、ソース間の関連（図３におけるソース・ポート・エントリと称される）を定義する。これには、ＮＡＰＴと、宛先ホストによってそのような接続に割り当てられた変換されたポート番号（変換されたソース・ポート・エントリと称する）とを含む。変換されたソース・ポートが、所定のセキュリティ・アソシエーションに関連付けられる受信パケットに対する割り当てに利用可能な（まだ割り当てられていない）ポートのプールから選択される。各交渉されたセキュリティ・アソシエーションは、変換ポートの自身のプールを有することになる。所定の接続について、各変換ポートのプールは、当然ながら、元のクライアント・

ポート番号によって部分的に定義さされるように、元接続が必要とするＳＰＤにおける同一または同等のセキュリティ規則に従う。利用可能な変換ポートを受信パケットに割り当てることによって、本発明によって拒絶される「重複」パケットの数は減少するはずであり、恐らく劇的に減少するはずである。

【００２２】

ＳＰＴＴの一例を、図３の３００に示す。このテーブルは、受信パケットが宛先ホストに到着するときに必要に応じて動的に構築される。ＳＰＴＴのソース・ポート・エントリは、４つのフィールドを有する。１）接続のパスにおけるＮＡＰＴのソースＩＰアドレス（例えば、エントリ３０２は、ＮＡＰＴ　ＩＰ　アドレス２１０．１．１．１を含む）、２）ＮＡＰＴよって割り当てられたＵＤＰソース・ポート（例えば、エントリ３０２の４５０１）、３）ＮＡＰＴによって扱われる発信クライアントによって選択された元のソース・ポート番号（例えば、エントリ３０２における４０９６）、４）元のクライアント・パケットのプロトコル（例えば、エントリ３０２におけるＴＣＰ）。ＳＰＴＴの各ソース・ポート・エントリは、変換されたソース・ポート・エントリをポイントする。例えば、ソース・ポート・エントリ３０２は、図３の変換されたソース・ポート・エントリ３０８をポイントする。各変換されたソース・ポート・エントリは、３つのフィールドを含む。１）接続のパスにおけるＮＡＰＴのソースＩＰアドレス（例えば、エントリ３０８は、ＮＡＰＴ　ＩＰアドレス２１０．１．１．１を含む）。２）ＮＡＰＴによって扱われる発信クライアントの変換されたソース・ポート番号（例えば、エントリ３０２における４０９６）。３）元のクライアント・パケットによって選択されたプロトコル（例えば、エントリ３０８におけるＴＣＰ）．ソース・ポート・エントリを使用して、宛先ホストへ入るパケットについての変換されたソース・ポート・エントリを見つけ、変換されたソース・ポート・エントリを使用して、ホストから出るパケットについてのソース・ポート・エントリを見つける。

【００２３】

図１３に示す利用可能なソース・ポート・プール（ＡＳＰＰ）は、変換割り当てのために利用可能なポート数と、既に割り当てられたポート数とを追跡する。サーバにおいて新規の遠隔クライアントからパケットがまず受信されると、ＡＳＰＰ内の情報が動的に生成される。ＡＳＰＰ１３００は、ポート・ベクトルをポイントする遠隔クライアント・エントリを含む。各遠隔クライアント・エントリは、受信パケットから取られたＮＡＰＴのＩＰアドレスと、パケットのＵＤＰまたはＴＣＰという元のクライアント・プロトコルという２つのフィールドを含む。元のクライアント・プロトコルは、パケットが到着すると暗号化されて、宛先ホストにおけるＩＰｓｅｃ処理後にクリアで利用可能である。これらの各遠隔クライアント・エントリは、互いに異なるポート・ベクトルをポイントし、その各ビットは、ベクトル内のビットの位置によって定義されるポート番号の利用可能または利用不可能な状態を記述している。図１３を参照して、ＮＡＰＴをトラバースするＩＰｓｅｃセキュリティ・アソシエーションをＩＫＥが交渉する場合には、ＴＣＰ／ＩＰスタックは交渉されたセキュリティ・アソシエーションの下で受領可能なポート番号の範囲を作成する。この範囲のポート番号は、重複ソースの可能性を回避するために、受信パケットに対して任意に割り当てることができる。これがどのように行われるかは、図８から図１２までの説明で明らかになるだろう。わかるように、対応遠隔クライアント・エントリについてのセキュリティ・アソシエーションに従って割り当てることができるポートの範囲のみが、任意のベクトル内にアドレス指定される。

【００２４】

図４から図７は、上述の説明を例示する助けとなる。図４は、ソースＮＡＰＴから来るパケットを示す。例示のため、クライアント・アドレスおよびポートは、１０．１．１．１および４０９６であると仮定する。４００は、ＮＡＰＴによって更新されたＩＰヘッダである。これは、ＮＡＰＴアドレス２１０．１．１．１と、ホスト宛先アドレス１１．１．１．１とを含む。４０２は、ＩＰｓｅｃ処理によって追加されてＮＡＰＴによって更新されたカプセル化ＵＤＰヘッダである。ソース・ポート４５００は、ＮＡＰＴによって４

５０１へ変更されている。４０４は、ＩＰｓｅｃ処理によって追加されたカプセル化されたセキュリティ制御（ＥＳＰ）ヘッダを含む。ＴＣＰトランスポート・ヘッダ４０６は、元クライアント・ソースと、宛先ポートとを含み、それぞれ４０９６および２１である。４０８は、ＥＳＰトレーラが続くペイロード・データを含む。トランスポート・ヘッダ４０６およびペイロード４０８は、ＩＰｓｅｃ処理に従って暗号化される。図５は、宛先における復号化後の図４のパケットを表す。注意すべきなのは、（５００からの）ソースＮＡＰＴアドレス２１０．１．１．１と、クライアント・ソース・ポート４０９６と、プロトコル（ＴＣＰ）とが５０６から利用可能である。受信パケットについては、これらの属性を使用して、ＳＰＴＴ３００のソース・ポート・エントリ（例えば、３０２、３０４）を検索して、対応する変換されたソース・ポート・エントリがもしあればそれを見つける。送信パケットについては、変換ソース・ポート・エントリ（例えば、３０８、３１０）を検索して、対応するソース・ポート・エントリを見つける。

【００２５】

図６および図７は、２番目に到着する「重複」ソース・パケットを表す。このパケットは、パケットを司るセキュリティ・アソシエーションに従って利用可能なポート番号の範囲からパケットに割り当てるための利用可能なポート番号があることを仮定して、本発明の実施形態によって受け付けられることになる。

【００２６】

適切なフローチャートに関連して、この処理をより詳細に以下に説明する。

【００２７】

図８は、ＩＫＥ交渉中のセキュリティ・アソシエーションの初期化を示す。ＩＫＥ交渉は、ステップ８０２で表されている。交渉中に、ステップ８０４は、交渉されたセキュリティ・アソシエーションをインストールするためのＴＣＰ／ＩＰスタックへの通知を送信する。セキュリティ・アソシエーションがいったん既知となると、ＳＰＤを検索して、接続に割り当てるために利用可能な範囲があれば、ポート番号の範囲を判断する。ステップ８０６は、これらのポート番号を判断して、スタックに記憶されたセキュリティ・アソシエーションに追加する。

【００２８】

図９は、データ・パケットが宛先ホストに到着する場合の重複ソースを回避する処理を開始する。図９は、データ・パケットが宛先ホストに到着する場合の重複ソースを検出する処理を開始する。ステップ９０２は、受信パケットがＵＤＰヘッダ内にカプセル化されたＥＳＰパケットを含み、かつＵＤＰヘッダ内のソース・ポートが予め規定されたＵＤＰカプセル化ポート４５００ではないかどうかを判断する。上記が真であれば、パケットは、暗号化または認証のいずれかのためにＩＰｓｅｃを使用しており、ＮＡＰＴは送信路に含まれる。パケットが４５００の宛先ポートを伴うＵＤＰプロトコルを使用しており、最初の４バイトが非ゼロ・データを含む場合には、パケットは、ＵＤＰカプセル化されたＥＳＰパケットとして識別される。これらの質問に対する答えがいいえの場合は、９０４におけるオプション１と９０６におけるオプション２という２つの代替処理オプションがある。これらを共に以下で説明する。両質問に対する答えがはいの場合、ステップ９０８はず１０のＡに続く。図１０において、ステップ１００１は、受信パケットからＵＤＰヘッダを除去する。ステップ１００２は、パケットを復号化するために必要なＩＰｓｅｃ処理を行う。その結果、３０２における４０９６のような元クライアント・ソース・ポート番号と、３０２におけるＴＣＰのような元のクライアント・プロトコルが取得される。それぞれ３０２における、２１０．１．１．１および４５０１といったＮＡＰＴソースＩＰアドレスおよびＮＡＰＴ割り当てポート番号は、ＵＤＰヘッダからわかる。ステップ１００４は、これらの属性に対して、ＳＰＴＴ３００のソース・ポート・エントリを検索する。合致するソース・ポート・エントリがステップ１００６で見つかる場合、変換されたポート番号は既にこのセッションに割り当てられているという意味である。ステップ１００８は、既に割り当てられたポート番号を探し当てる。この例において、合致するソース・ポート・エントリは３０２である。対応する変換ソース・ポート・エントリは、３０８であ

る。エントリ３０８は、割り当てられたソース・ポート番号４０９６を含み、これは、たまたま元のクライアント・ソース・ポート番号と同一である。これは、エントリ３０８が作成されたとき、元のクライアント・ソース・ポート番号が割り当てのために利用可能であり、したがって割り当てられたポートとして使用されたことを意味する。このことは、以下でより詳細に述べる。ステップ１０１０は、パケット・トランスポート・ヘッダ内のソース・ポート番号を３０８からの変換されたソース・ポートで置換し、１０１２において従来のパケット処理を継続する。ステップ１００８において、一致する変換されたソース・ポート・エントリが３１０であった場合には、ＳＰＴＴ３００の例示内容に従って、変換されたポート番号は３８０９６であっただろう。この例で説明を続けると、ＳＰＴＴ３００におけるソース・ポート・エントリがステップ１００６で見つからない場合には、処理は、必要に応じてＡＳＰＰ１３００の単数および複数のエントリを作成することを開始する。はじめに、ステップ１０１６は、ＡＳＰＰ遠隔クライアント・エントリが既に存在するかどうかを判断する。もし存在しなければ、ステップ１０２０は、この例において、ソース・ＮＡＰＴ　ＩＰアドレス２１０．１．１．１と、復号化されたパケットからのプロトコルＴＣＰとを使用してエントリを作成する。ステップ１０２２は、対応のビット・ベクトルを作成する。はじめに、ベクトルのすべてのビットが利用可能な状態に設定される。図１１のＥにおいて、ステップ１１０２は、次に、パケット内のクライアント・ソース・ポート番号がソース・ポート・ビット・ベクトルにおいて利用可能であるとマーク付けされているかどうか判断する。もしそうであれば、１１０４において、パケット内のソース・ポート番号が割り当てられる。これは、本例の３０２および３０８に対応し、元のソース・ポート番号と割り当てられたポート番号が一致している。元のクライアント・ソース・ポート番号がベクトルで利用不可能であるとマーク付けされている場合には、ステップ１１１０は、セキュリティ・アソシエーションにしたがって割り当てることができるポートの範囲を判断する。ポート・ビット・ベクトルのこの範囲内において、ステップ１１１２は、利用可能な次のポートがもしあればそれを判断する。割り当てのために利用可能なポート番号がなければ、１１１４においてパケットは拒絶される。なぜならば、分解することができない重複ソースを表しているからである。ポートがベクトル内の許容範囲内で利用可能であれば、ステップ１１１３において、３０８および３１０のような変換されたソース・ポート・エントリを、ベクトルからの選択された利用可能なポートを使用してＳＰＴＴ内３００に作成する。ステップ１１０６は、選択されたポートをマーク付けする。ステップ１１０８は、３０４などのソース・ポート・エントリをＳＰＴＴ３００に作成して、それをステップ１１１３において作成された変換されたソース・ポート・エントリと関連付ける。処理は図１０のＦに続き、ステップ１０１０において、パケット・ポート番号が、割り当てられたポート番号に置換され、通常のパケット処理がステップ１０１２において継続する。

【００２９】

図９からのオプション１を使用する場合には、上述のステップ１１１０における変形が必要である。受信パケットがＩＰｓｅｃパケットではないとステップ９１０が判断する場合には、このパケットに関連したＳＡはない。したがって、ステップ１１１０は、好ましい実施形態におけるようなＳＡからというよりも直接ＳＰＤから、割り当てのために利用可能なポートの範囲を含むポート・ビット・ベクトルを取得しなければならない。

【００３０】

図９のオプション１およびオプション２は、パケットがクリア内に送られる（ＩＰｓｅｃ処理がない）か、パス内にアドレス変換（ＮＡＰＴ）がないかのいずれかの状況を表す。ＮＡＰＴをトラバースするなんらかのセキュリティ・アソシエーションがこのホスト内で終了している限り、この状況では重複ソースの可能性がまだある。代替オプション１および２は両方とも、このような条件でのそのような重複パケットを回避する。オプション１は、重複ソース回避のための上述と同一の原則を適用するが、パケットによる必要に応じてＩＰｓｅｃ処理を適用したり回避したりすることによって行う。オプション２は、ＳＰＤのフィルタリング規則を使用して、重複ソースを回避する。オプション１（９０４）

が選択されると、ステップ９１０は、パケットがＩＰｓｅｃ処理を必要とするかを判断する。もし必要とすれば、処理は９１２へ続き、図１０のＢのステップ１００２は、必要に応じてＩＰｓｅｃ処理を行って、処理は１００４へ続く。ステップ９１０においてパケットがＩＰｓｅｃパケットでない場合には、ステップ９１４は、図１０のＤへと続き、ＢのＩＰｓｅｃ処理を単にスキップする。この場合、図１０のステップ１００４は、ゼロ（０）のＵＤＰソース・ポートを使用する。なぜならば、パケット内にはカプセル化ＵＤＰヘッダがないからである。

【００３１】

オプション２は、受信ＩＰｓｅｃパケット・フィルタリングを使用して、重複ソースをできる限り回避する。ＩＰｓｅｃがいったん設定されると、すべてのパケットは、パケットが暗号化されているかどうかに関わらず、ＩＰｓｅｃ規則テーブルＳＰＤを介して処理される。これは、所定の接続上のクリア・パケットがＩＰｓｅｃ規則によって実際に許可されたことを検証するためのものである。オプション２の処理は、図１２のＣで開始する。ステップ１２０２において、受信パケットは、ＩＰｓｅｃ規則テーブル（図示せず）を介して処理される。好ましい一実施形態においてこれがどのように行われるかについては、上記の米国特許第６３４７３７６号から判断できる。この特許を、その全体を参照により援用するものとする。パケットが暗号化されると（ステップ１２０４）、ステップ１２０６は、ＩＰｓｅｃ規則が暗号化を要求しているかどうかを判断する。要求していると仮定すると、パケットは１２０６において許可される。そうでない場合には、１２１０において拒絶される。ステップ１２０４においてパケットがクリアである場合には、１２１２において、一致するＩＰｓｅｃ規則は暗号化されていないパケットを許可するかどうかについての判断がなされ、それに従ってパケットが許可または拒絶される。

【００３２】

トンネル・モードにおいて、ＩＰｓｅｃ　ＳＡは、必ずしもエンド・ツー・エンドではない。例えば、ＳＡは、ホストと、複数のクライアントおよびサーバを扱うゲートウェイとの間を交渉してもよい。トンネル・モードにおいて、単一のＮＡＰＴアドレス（ＵＤＰカプセル化ヘッダにおけるソースＩＰアドレス）は、複数のホストを表す場合がある。トンネル・モードにおいて、パケットのカプセル化されかつ暗号化された部分は、ソースの元のＩＰアドレスとＴＣＰトランスポート・ヘッダとの両方を含む。本明細書の目的のために、トンネル・モードにおけるソースの元のＩＰアドレスを、内部ソースＩＰアドレスと称する。内部ソースＩＰアドレスは、全体的に固有ではないので、パケット・ルーティングまたは接続のソースを表すためには使用できない。ＳＰＴＴ３００のソース・ポート・エントリ内に含まれるような元のソース・ポートと、トランスポート・モードについて上述したようなＵＤＰポートだけを伴うカプセル化ソースＩＰアドレスとは、固有でない場合もあろう。これに対処するために、内部ソースＩＰアドレスを含む追加のフィールドが、図３のＳＰＴＴ３００のソース・ポート・エントリ（例えば、３０２および３０４）に追加される。（トランスポート・モードにおいては利用可能ではない）内部ソースＩＰアドレスは、ソース・ポート・エントリの他の値と組み合わせると、トンネル・モードのＩＰｓｅｃ　ＳＡによって保護されたホストについての固有の識別子を生じさせる。

【００３３】

開示された好ましい実施形態が本教示の意図および範囲内の数多くの軽微の変形を有しうることを、当業者は理解するだろう。発明者の意図は、本発明の分野における適用可能な関連技術の状況に従って可能な程度の変形を含むということである。

【図面の簡単な説明】

【００３４】

【図１】クライアントからＮＡＰＴおよびＮＡＴを介して宛先ホストへのパケットの進行と、パケットの進行に伴うパケット・ヘッダおよび内容に対する変更とを示す。

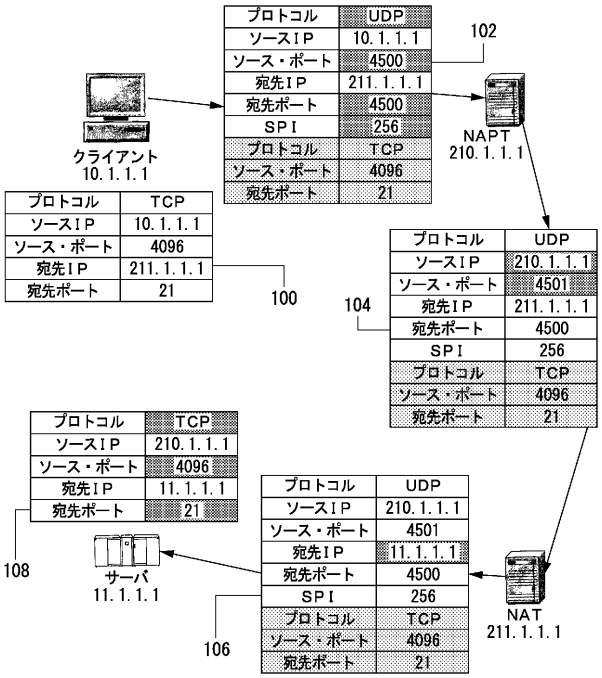
【図２】図１のパケットに応答する戻りパケットを示す。

【図３】ソース・ポート変換テーブル（ＳＰＴＴ）の一実施形態を例示する。

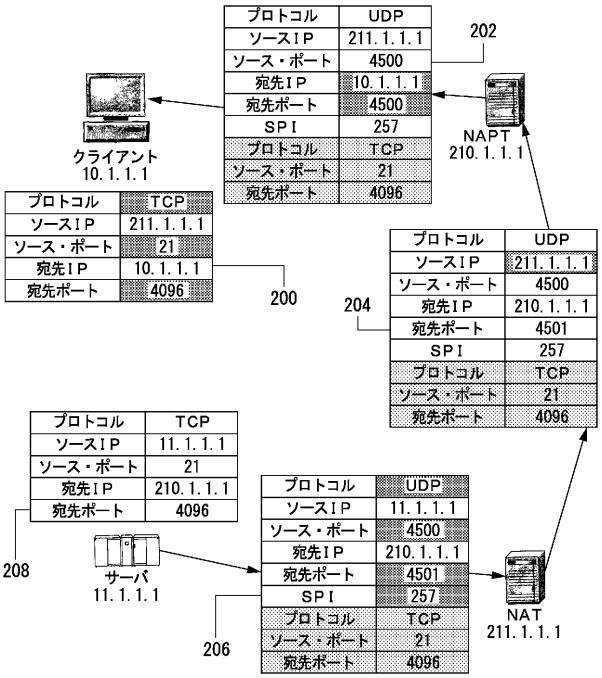
【図４】暗号化された元パケットをカプセル化するＮＡＰＴ変換パケットを示す。

【図５】復号化後の図４のパケットを示す。
【図６】図４に対応する、送信路内のＮＡＰＴを含ませることによって生じる違法な重複接続を表す先のパケットと同一のパス上の第２のパケットを示す。
【図７】図５に対応する、送信路内のＮＡＰＴを含ませることによって生じる違法な重複接続を表す先のパケットと同一のパス上の第２のパケットを示す。
【図８】セキュリティ・アソシエーションが定義されかつポート番号の範囲が決定されて、両者共にこの宛先とクライアントとの間の通信のためのプロトコル・スタックにインストールすることとなる、インターネット鍵交換のフローチャートを例示する。
【図９】受信パケットが最初に宛先ホストに到着した場合に利用可能なオプションを示すフローチャートである。
【図１０】暗号化された元パケットをカプセル化しかつＮＡＰＴを通った受信パケットのエントリＡにおける処理と、ＮＡＰＴを通っていないＩＰｓｅｃパケットのエントリＢにおける処理と、ＮＡＰＴを通っておらずかつＩＰｓｅｃパケットでもないエントリＤにおける処理とを示すフローチャートである。
【図１１】図１０からの受信パケットの処理を継続する。
【図１２】カプセル化およびＮＡＰＴ通過という両条件を満足しない受信パケットを処理する一代替方法を示すフローチャートである。
【図１３】割り当ておよび未割り当てポート・番号を追跡する利用可能なソース・ポート・プールの実施形態を例示する。

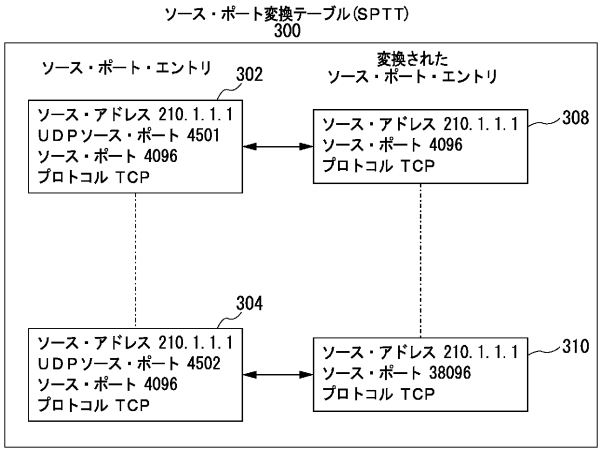
【図１】



【図２】



【図３】



【図４】

クライアント・アドレス10.1.1.1ポート4096からの
NAPTカプセル化されたパケット

400	402	404	406	408	410
IPヘッダ	UDPヘッダ	ESPヘッダ	プロトコルTCP	ペイロード	ESPトレーラ
ソース 210.1.1.1	ソース・ポート 4501		ソース・ポート 4096		
宛先 11.1.1.1	宛先ポート 4500		宛先ポート 21		

【図５】

ホストにおけるIPSEC処理後の図４からのパケット

500	506	508
IPヘッダ	プロトコルTCP	ペイロード
ソース 210.1.1.1	ソース・ポート 4096	
宛先 11.1.1.1	宛先ポート 21	

【図６】

クライアント・アドレス10.1.1.2ポート4096からの
NAPTカプセル化されたパケット

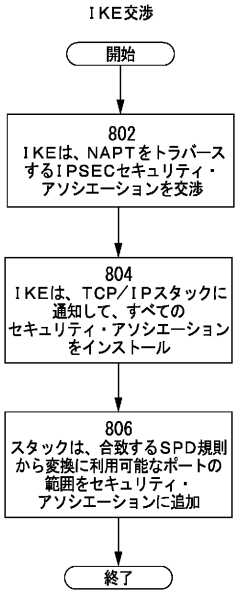
600	602	604	606	608	610
IPヘッダ	UDPヘッダ	ESPヘッダ	プロトコルTCP	ペイロード	ESPトレーラ
ソース 210.1.1.1	ソース・ポート 4502		ソース・ポート 4096		
宛先 11.1.1.1	宛先ポート 4500		宛先ポート 21		

【図７】

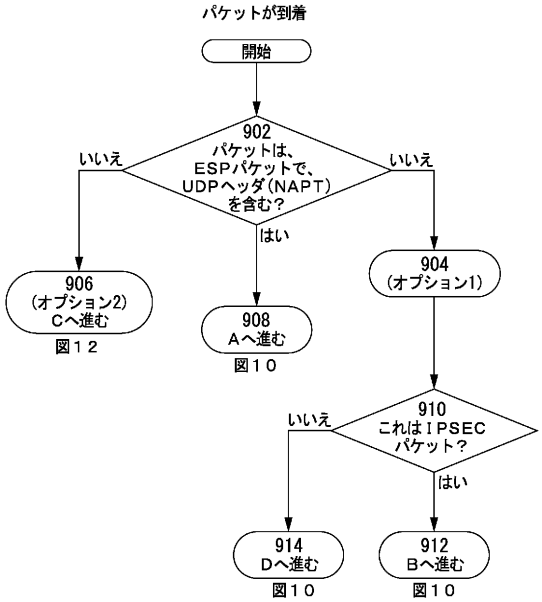
ホストにおけるIPSEC処理後の図５からのパケット

700	706	708
IPヘッダ	プロトコルTCP	ペイロード
ソース 210.1.1.1	ソース・ポート 4096	
宛先 11.1.1.1	宛先ポート 21	

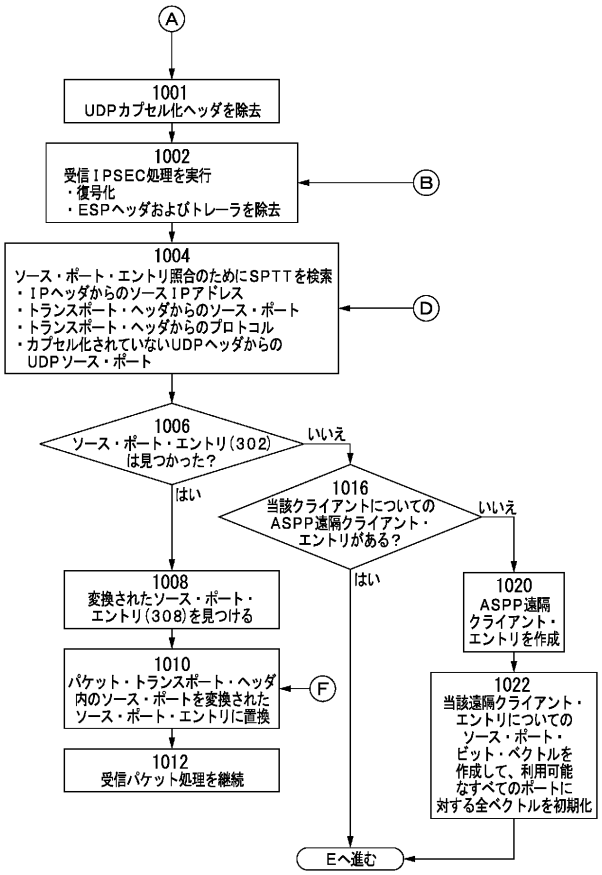
【図８】



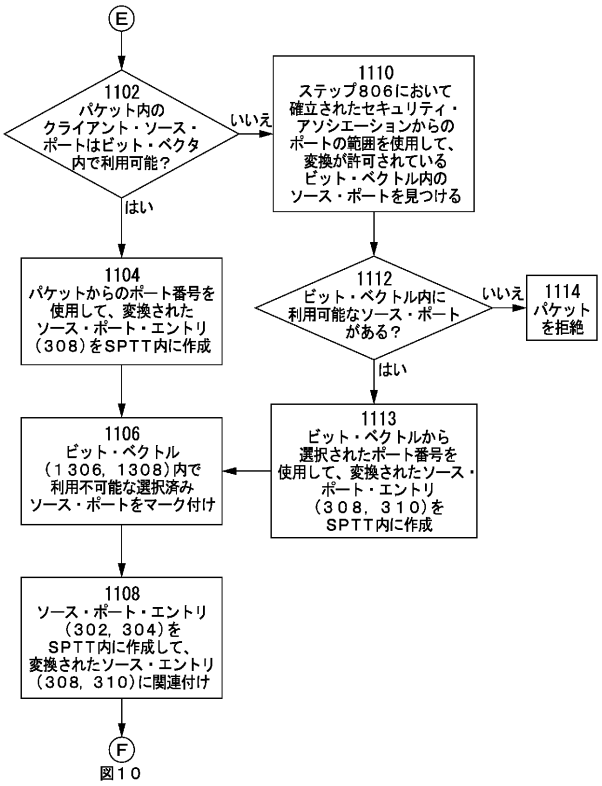
【図９】



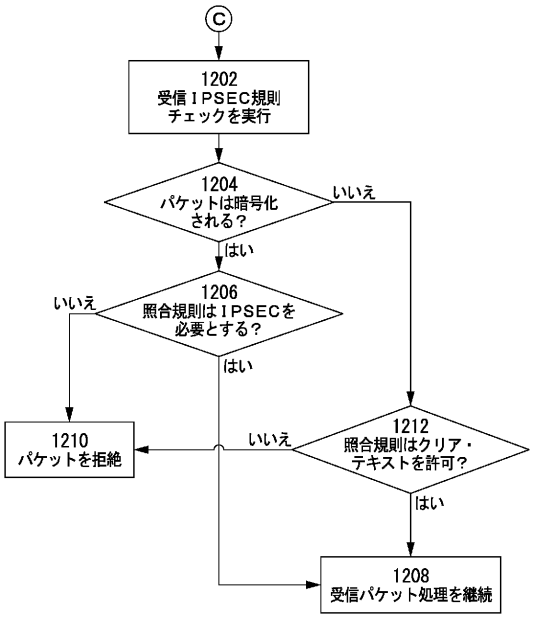
【図１０】



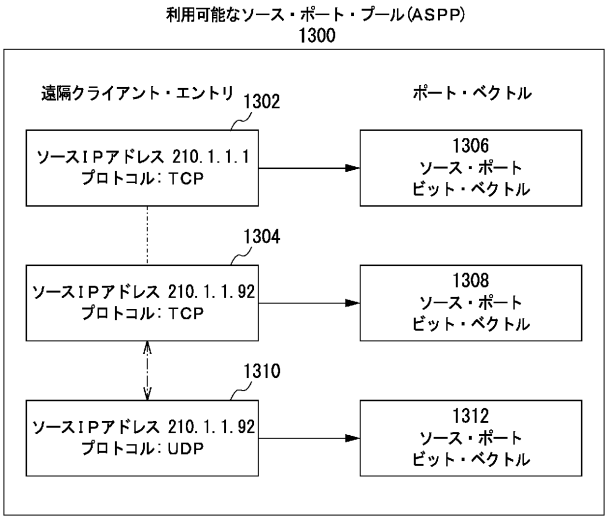
【図１１】



【図１２】



【図１３】



フロントページの続き

(74)代理人 100086243
弁理士 坂口 博
(72)発明者 ジャクビック、パトリシア
アメリカ合衆国２７６０６ ノースキャロライナ州 ラレイ クラッチフィールド・ロード ５７０４
(72)発明者 オーバービー、リンウッド、ヒュー、ジュニア
アメリカ合衆国２７６１５ ノースキャロライナ州 ラレイ メイナー・オークス・ドライブ ７２５２
(72)発明者 ポーター、ジョイス、アン
アメリカ合衆国２７５０２ ノースキャロライナ州 エイペックス ウェスト・セイント・ジュリアン・プレース １００７
(72)発明者 ウィアボウスキー、デイビッド、ジョン
アメリカ合衆国１３８２７ ニューヨーク州 オウェゴ イースト・ビーチャー・ヒル・ロード ２４８９

審査官 玉木 宏治

(56)参考文献 特開２００３－３３３０６６（ＪＰ，Ａ）
特開２００２－２３２４５０（ＪＰ，Ａ）
A.Huttumen et al., UDP Encapsulation of IPsec ESP Packets, rfc3948, ２００５年 １月, http://www.ietf.org/rfc/rfc3948.txt
M.Stenberg et al., IPsec NAT-Traversal, Internet Draft:draft-stenberg-ipsec-nat-traversal-02.txt, ２００１年 ２月, http://www.watersprings.org/pub/id/draft-stenberg-ipsec-nat-traversal-02.txt
Camelo Zaccone et al., Address reuse in the Internet, adjourning or suspending the adoption of IP next generation?, Proceedings. IEEE International Conference on Networks, 2000. (ICON 2000), ２０００年 ９月
RSIP Support for End-to-end IPsec, rfc3104, http://www.ietf.org/rfc/rfc3104.txt

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 12/00-66