(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4766574号
(P4766574)
(45)発行日　平成23年9月7日(2011.9.7)　(24)登録日　平成23年6月24日(2011.6.24)

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

請求項の数 14　(全 16 頁)

(21)出願番号　特願2008-505871 (P2008-505871)
(86)(22)出願日　平成18年4月7日(2006.4.7)
(65)公表番号　特表2009-532919 (P2009-532919A)
(43)公表日　平成21年9月10日(2009.9.10)
(86)国際出願番号　PCT/EP2006/061433
(87)国際公開番号　WO2006/108805
(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)

(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】
アプリケーションを識別するためにネットワーク・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）サーバでパケットを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（ＮＡＰＴ）によって変換されており且つＩＰｓｅｃカプセル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且つＩＰｓｅｃカプセル化されたパケットを含むことに応じて、前記パケットの送信者に関する元の接続情報を取得するために前記パケットを処理し、そしてＮＡＰＴによって変換された接続情報と前記元の接続情報との間のアソシエーションのためのソース・ポート・マッピング・テーブル（ＳＰＭＴ）を検索するステップと、
ｄ）ステップｃ）の結果が重複ソースであることを表すことに応じて、前記パケットを拒絶するステップであって、前記元の接続情報が、前記ＳＰＭＴにおいて合致し且つ前記パケット中に含まれる前記ＮＡＰＴによって変換された前記接続情報に前記ＳＰＭＴにおいて関連付けられていないことに応じて、前記重複ソースであることが表される、前記拒絶するステップと
を含む、前記方法。

【請求項２】
前記ソース・ポート・マッピング・テーブルは、
クライアントとサーバとの間のセキュリティ・アソシエーションが交渉される場合に作成されるＮＡＰＴホスト・エントリと、
非重複ソース・パケットとして生成されるソース・ポート・エントリであって、前記非重複ソース・パケットは、重複ソースを検出するために使用される前記ソース・ポート・エントリと前記ＮＡＰＴホスト・エントリとの間のマッピングを備える既存のエントリがない場所から到着する、前記ソース・ポート・エントリと
を含む、請求項１に記載の方法。
【請求項３】
前記ソース・ポート・マッピング・テーブル内にＮＯ　ＩＰＳＥＣ／ＮＡＰＴホスト・エントリを確立して、請求項１のステップｂ）を失敗したすべての受信パケットを示して、ソース・ポート・エントリを有しないすべての受信パケットを表して、ソース・ポート・エントリを有しないすべての受信パケットについてのソース・ポート・エントリを作成し、
前記ソース・ポート・エントリをＮＯ　ＩＰＳＥＣ／ＮＡＰＴホスト・エントリにマッピングし、
前記ＮＯ　ＩＰＳＥＣ／ＮＡＰＴホスト・エントリにマッピングされていない前記ソース・ポート・マッピング・テーブル内にソース・ポート・エントリを既に有する受信パケットのいずれかを拒絶するステップと
をさらに含む、請求項２に記載の方法。
【請求項４】
アプリケーションを識別するためにネットワーク・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）サーバでパケットを受信するステップと、
ｂ）前記パケットがＩＰｓｅｃカプセル化されたパケットかどうかを判断するステップと、
ｃ）前記パケットがＩＰｓｅｃカプセル化されたパケットであることに応じて、前記パケットの送信パスがネットワーク・アドレス・ポート変換器（ＮＡＰＴ）を含むかどうかを判断するステップと、
ｄ）前記送信パスがＮＡＰＴを含むことに応じて、前記ＩＰｓｅｃカプセル化されたパケットを復号化して、前記パケットの送信者に関する元のソース・ポート番号及び元のパケット・プロトコルを取得するステップと、
ｅ）ＮＡＰＴによって変換されたソース・アドレス及びソース・ポート番号を有するＮＡＰＴホスト・エントリと、ＮＡＰＴによって変換されたソース・アドレス、元のソース・ポート番号及びパケット・プロトコルを有するソース・ポート・エントリとの間のアソシエーションを見つけるためのソース・ポート・マッピング・テーブル（ＳＰＭＴ）を使用して、アソシエーションを検索するステップと、
ｆ）前記ステップｅ）において検索されたアソシエーションのソース・ポート・エントリが前記パケット内に含まれる元のソース・ポート番号と異なる元のソース・ポート番号を有する場合に、前記ＩＰｓｅｃカプセル化されたパケットを拒絶するステップと
を含む、前記方法。
【請求項５】
ステップｂ）は、ユーザ・データグラム・プロトコル（ＵＤＰ）ヘッダによってカプセル化されたカプセル化セキュリティ・ペイロード（ＥＳＰ）を含むかどうかを判断するステップをさらに含む、請求項４に記載の方法。
【請求項６】
前記カプセル化されたＵＤＰヘッダは、４５００以外のソース・ポート・番号と、４５０に等しい宛先ポート番号を含むかどうかを判断するステップをさらに含む、請求項４に

記載の方法。
【請求項７】
インターネット・ホストからのインターネット鍵交換（ＩＫＥ）メッセージに応答して、前記サーバにおける前記ＳＰＭＴ内に、ＮＡＰＴによって変換されたソース・アドレス及びソース・ポート番号をそれぞれ含む複数のＮＡＰＴホスト・エントリを動的に構築するステップをさらに含む、請求項４に記載の方法。
【請求項８】
ＩＰｓｅｃパケットが到着して処理されると、前記ＳＰＭＴ内に、ＮＡＰＴによって変換されたソース・アドレス、元のソース・ポート番号及びパケット・プロトコルをそれぞれ含む複数のソース・ポート・エントリを動的に構築するステップと、前記構築されたＮＡＰＴホスト・エントリと前記構築されたソース・ポート・エントリとの間のアソシエーションを確立するステップとをさらに含む、請求項７に記載の方法。
【請求項９】
前記アソシエーションを確立するステップは、アソシエーションがないＩＰｓｅｃパケットが到着することに応じて、各アソシエーションを動的に確立するステップをさらに含む、請求項８に記載の方法。
【請求項１０】
単一のホスト「ＮＯ　ＩＰＳＥＣ／ＮＡＰＴ」エントリを前記ＳＰＭＴに追加して、ＥＳＰヘッダを含まないかまたはＮＡＰＴを通過していないすべてのパケットを関連付けるステップと、
ＥＳＰヘッダを含まないかまたはＮＡＰＴを通過しておらず、且つアソシエーションを有しないパケットが到着することに応じて、前記ＳＰＭＴのソース・ポート・エントリと、前記「ＮＯ　ＩＰＳＥＣ／ＮＡＰＴ」エントリとの間のアソシエーションを形成するステップと、
前記「ＮＯ　ＩＰＳＥＣ／ＮＡＰＴ」エントリをポイントしない前記合致ソース・ポート・エントリについて確立されたアソシエーションが既にあることに応じて、ＥＳＰヘッダを含まないかまたはＮＡＰＴを通過していないパケットを拒絶するステップと
をさらに含む、請求項９に記載の方法。
【請求項１１】
到着パケットの送信パスがＮＡＰＴを含まないか、前記到着パケットがＩＰｓｅｃパケットでないことに応じて、規則のセキュリティ・テーブルを検索して、前記パケットの拒絶または受け入れを司る合致規則を見つけるステップと、
前記パケットがＩＰｓｅｃパケットであって前記合致規則がＩＰｓｅｃ処理を必要としないことに応じて、前記パケットを拒絶するステップと、
前記パケットがＩＰｓｅｃパケットでなく且つ前記合致規則がＩＰｓｅｃ処理を必要とすることに応じて、前記パケットを拒絶するステップと
をさらに含む、請求項４に記載の方法。
【請求項１２】
コンピュータに、請求項１～１１のいずれか１項に記載の方法の各ステップを実行させるコンピュータ・プログラム。
【請求項１３】
アプリケーションを識別するためにネットワーク・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）サーバでパケットを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（ＮＡＰＴ）によって変換されており且つＩＰｓｅｃカプセル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）前記パケットが変換されており且つＩＰｓｅｃカプセル化されたパケットを含むことに応じて、前記パケットの送信者に関する元の接続情報を取得するために前記パケット

を処理し、そしてＮＡＰＴによって変換された接続情報と前記元の接続情報との間のアソシエーションのためのソース・ポート・マッピング・テーブル（ＳＰＭＴ）を検索する手段と、

ｄ）前記ＳＰＭＴが重複ソースであることを表すことに応じて、前記パケットを拒絶するための手段あって、前記元の接続情報が、前記ＳＰＭＴにおいて合致し且つ前記パケット中に含まれる前記ＮＡＰＴによって変換された前記接続情報に前記ＳＰＭＴにおいて関連付けられていないことに応じて、前記重複ソースであることが表される、前記拒絶するための手段と

を備える、前記装置。

【請求項１４】

アプリケーションを識別するためにネットワーク・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）サーバでパケットを受信するための手段と、

ｂ）前記パケットがＩＰｓｅｃカプセル化されたパケットかどうかを判断するための手段と、

ｃ）前記パケットがＩＰｓｅｃカプセル化されたパケットであることに応じて、前記パケットの送信パスがネットワーク・アドレス・ポート変換器（ＮＡＰＴ）を含むかどうかを判断するための手段と、

ｄ）前記送信パスがＮＡＰＴを含むことに応じて、前記ＩＰｓｅｃカプセル化されたパケットを復号化して、前記パケットの送信者に関する元のソース・ポート番号及び元のパケット・プロトコルを取得するための手段と、

ｅ）ＮＡＰＴによって変換されたソース・アドレス及びソース・ポート番号を有するＮＡＰＴホスト・エントリと、ＮＡＰＴによって変換されたソース・アドレス、元のソース・ポート番号及びパケット・プロトコルを有するソース・ポート・エントリとの間のアソシエーションを見つけるためのソース・ポート・マッピング・テーブル（ＳＰＭＴ）を使用して、アソシエーションを検索するための手段と、

ｆ）前記検索されたアソシエーションのソース・ポート・エントリが前記パケット内に含まれる元のソース・ポート番号と異なる元のソース・ポート番号を有する場合に、前記ＩＰｓｅｃカプセル化されたパケットを拒絶するための手段と

を備える、前記装置。

【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、本技術は、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、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、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、ＮＡＴ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文献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 ＥＳＰ 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、元ソース・ポート番号と、元トランスポート・プロトコルとを取得する。ソース・ポート・マッピング・テーブル（ＳＰＭＴ）を検索して、ＮＡＰＴソースＩＰアドレスと、元ソース・ポート番号と、ＮＡＰＴソースＩＰアドレスおよび変換されたソース・ポート番号に関連した元トランスポート・プロトコルとの間のアソシエーションを求める。不正確なアソシエーションが見つかると、パケットは、不正な重複ソース、すなわち、同一のソースＩＰアドレス、ソース・ポート番号およびプロトコルを使用しているＮＡＰＴによって扱われる異なるホストからの第２のパケットを表すものとして拒絶される。

【００１０】

好ましい実施形態において、サーバにおけるＳＰＭＴ内のネットワーク・アドレス・ポート変換器（ＮＡＰＴ）ホスト・エントリが、インターネット・ホストからのインターネット鍵交換（ＩＫＥ）メッセージに応答して動的に構築される。各ＮＡＰＴホスト・エントリは、ＮＡＰＴのソースＩＰアドレスと、ＮＡＰＴによって割り当てられたソース・ポートとを含む。ＳＰＭＴ内のソース・ポート・エントリは、暗号化されたパケットが到着して復号化されるにつれて動的に構築され、ソース・ポート・エントリとＳＰＭＴのＮＡＰＴホスト・エントリとの間でアソシエーションが確立される。各ソース・ポート・エントリは、ＮＡＰＴのソースＩＰアドレスと、元ソース・ポート番号と、元プロトコルとを含む。

【００１１】

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】

【００１２】

本発明の実施形態によって対処される問題は、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、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。

【００１３】

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の組み合わせにおいて実施することができる。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。

【００１４】

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、または伝播媒体であることが可能であるが、これらに限定されない。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。

【００１５】

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。

【００１６】

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。

【００１７】

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。

【００１８】

図１は、クライアント１０．１．１．１からＮＡＰＴ２１０．１．１．１とＮＡＰＴ２１１．１．１．１を通って宛先ホスト１１．１．１．１へのパケット進行と、パケット進行に伴うパケット・ヘッダおよび内容の変化とを示す。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進行を示す。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。注意すべきなのは、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によって特定されるように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他のセキュリティ・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。

【００１９】

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・ポート番号は、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。

【００２０】

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。

【００２１】

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。

【００２２】

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ある。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。

【００２３】

宛先ホストにおけるソース・ポート・マッピング・テーブル（ＳＰＭＴ）を使用して、ＮＡＰＴによって扱われるクライアントまたはサーバからパケットが受信される重複ソースを検出する。ＳＰＭＴの例示を図３の３００に示す。このテーブルは、ＩＰｓｅｃセキュリティ・アソシエーションが確立される場合にインターネット鍵交換（ＩＫＥ）パケットがサーバで受信されるときに動的に構築される。図３を参照して、ＩＫＥが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交渉する場合、ＴＣＰ／ＩＰスタックは、３０２などのＮＡＰＴホスト・エントリを作成して、ＮＡＰＴによって表される遠隔クライアントを表すように通知される。このエントリは、ＮＡＰＴのソースＩＰアドレス（本例においては、２１０．１．１．１）と、ＮＡＰＴによってこのクライアントに対して割り当てられたソース・ポート（本例においては、４５０１）とを含む。図３は、同一のＮＡＰＴ　ＩＰソース・アドレス２１０．１．１．１と、ＮＡＰＴによって割り当てられた異なるソース・ポート４５０２とを有する、第２の例示的なＮＡＰＴクライアント３０４を示す。ＳＰＭＴ３００の右側は、ソース・ポート・エントリである。これらのエントリは、既存のエントリのないＩＰｓｅｃの暗号化されたパケットが到着するにつれて作成される。ソース・ポートエントリを追加する処理は、ＩＰｓｅｃ復号化が生じた後に生じる。ソース・ポート・エントリをＮＡＰＴホスト・エントリにマッピングするアソシエーション３０６は、ソース・ポート・エントリが作成されるにつれて作成される。ＮＡＰＴホスト・エントリは、当該エントリに関する最終セキュリティ・アソシエーションが削除されると除去される。パケットが到着して復号化されると、ソースＮＡＰＴアドレスと、元パケットのソース・ポートと、元パケットのプロトコルとが利用可能である。これらの属性の合致を見つけるために、ＳＰＭＴのソース・ポート・エントリが検索される。合致が見つかると、ＮＡＰＴソース・アドレスと、ＮＡＰＴによって割り当てられたソース・ポートとの合致を見つけるために、関連したＮＡＰＴホスト・エントリがチェックされる。これらの後者の属性が不一致の場合、ソースＮＡＰＴの背後の２つのクライアントは同一のソース・ポート番号を使用しようとしているということを意味する。これは、重複ソースを表し、第２のパケットは拒絶される。これらの後者の属性が一致すると、パケットは許可される。

【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４５０１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、宛先ホ

スト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、（パケット・フィールド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、フィールド５０６から利用可能である。これらの属性を使用して、ＳＰＭＴ３００のソース・ポート・エントリが検索される。この例において、３０８において合致が見つかる。対応のアソシエーション３０６は、ＮＡＰＴホスト・エントリ３０２をポイントする。ソースＮＡＰＴアドレス２１０．１．１．１およびＮＡＰＴソース・ポート４５０１は、このパケットと合致する（ＮＡＰＴソース・ポート４５０１は、受信パケットのフィールド４０２からクリアで利用可能である）。よって、このパケットは、正確な接続に関連付けられて、受け付けられる。

【００２５】

図６および図７は、２番目に到着する「重複」ソース・パケットを表し、これは拒絶されることになる。なぜならば、フィールド７００からのＮＡＰＴソース・アドレス２１０．１．１．１と、７０６からのプロトコルと、ソース・クライアント・ポート４０９６は、ＳＰＭＴ３００のソース・ポート・エントリである３０８と合致するが、関連ＮＡＰＴエントリ３０２は、受信パケットのフィールド６０２からの４５０２のＮＡＰＴ割り当てポート番号と合致しないからである。

【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ＳＰＭＴ３００のＮＡＰＴホスト・エントリの初期化を示す。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、ＳＰＭＴ３００における関連ＮＡＰＴホスト・エントリを作成するためにＴＣＰ／ＩＰスタックへ通知を送信する。この通知は、ＩＫＥフローから取り出されたＮＡＰＴソース・アドレスとポート番号とを含む。

【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。ステップ９０２におけ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。９０２における答えがハイであると仮定すると、９０８は図１０のＡと続く。図１０において、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、ＮＡＰＴソース・アドレスと、元クライアント・ソース・ポート番号と、プロトコルとが、上述のようにクリアで取得される。ステップ１００４は、これらの属性についてＳＰＭＴ３００のソース・ポート・エントリを検索する。１００６において、合致が見つからない場合には、ステップ１００８においてソース・ポート・エントリが作成され、パケットの受信処理は通常通り継続する。ステップ１００６において合致が見つかると、ステップ１０１０は、対応のアソシエーション３０６を使用して、ＮＡＰＴ割り当てソース・アドレスと、復号化されたパケットからの同一の属性への対応ＮＡＰＴホスト・エントリからのポート番号とを比較する。この比較が失敗すると、パケットは１０１１において拒絶される。合致が取得されると、パケット処理は、通常通り１０１２において継続する。

【００２９】

図９からのオプション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。しかしながら、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、そのような重複パケットを回避する。オプション１の処理は、図１１のＢで開始する。このオプションは、ＳＰＭＴテーブル３００を通じてすべてのデータ・パケットを処理する。これは、「ＮＯ　ＩＰＳＥＣ／ＮＡＰＴ」として指定された他の単一のＮＡＰＴホスト・エントリを追加することによって行われる。ＳＰＭＴ３００のパケットが到着すると、ソース・ポート・エントリを上述のように検索する。合致が見つからない場合には、ソース・ポート・エントリが１１０６において作成されて、「ＮＯ　ＩＰＳＥＣ／ＮＡＰＴ」ＮＡＰＴホスト・エントリに関連付けられる。合致するソース・ポート・エントリが１１０４で見つかると、ステップ１１１０は、対応アソシエーション３０６が「ＮＯ　ＩＰＳＥＣ／ＮＡＰＴ」ＮＡＰＴホスト・エントリをポイントしているかどうかを判断する。ポイントしている場合には、パケットは１１０８で許可される。そうでなければ、パケットは１１１２で拒絶される。このオプション１の利点は、簡略性である。その利点は、すべてのデータ・トラフィックがＳＰＭＴテーブル３００を通じて処理されるということである。

【００３０】

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・パケットを拒絶する。ＩＰｓｅｃがいったんホストに設定されると、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、支配的な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暗号化されていない場合には、１２１２において、支配的な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。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。ＳＰＭＴ３００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ＳＰＭＴ３００のソース・ポート・エントリ（例えば、３０８）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。内部ソースＩＰアドレスは、ステップ１００８の一部として、ソース・ポート・エントリに追加される。トンネル・モード・パケットが到着すると、ステップ１００４において上述したようなＳＰＭＴのソース・ポート・エントリを検索して、ＮＡＰＴホスト・エントリに対するアソシエーションを見つけ、ステップ１０１０において、上記説明に加えて、復号化されたパケットから取得した内部ソース・クライアントＩＰアドレスがソース・ポート・エントリ内のクライアントＩＰアドレスと同一であることを検証する。この検証が失敗す

ると、当該パケットは拒絶される。

【００３１】

好ましい実施形態が数多くの軽微の変形を有しうることは、当業者にとって明らかだろう。例えば、ＩＣＭＰプロトコルは、ポート番号を使用せず、むしろクエリ識別子を使用する。開示され請求された本発明に関して、クエリ識別子は、ポート番号と等価である。

【図面の簡単な説明】

【００３２】

【図１】クライアントからＮＡＰＴ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・マッピング・テーブル（ＳＰＭＴ）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ソース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】ＳＰＭＴ内のＮＡＰＴホスト・エントリの作成のフローチャートである。

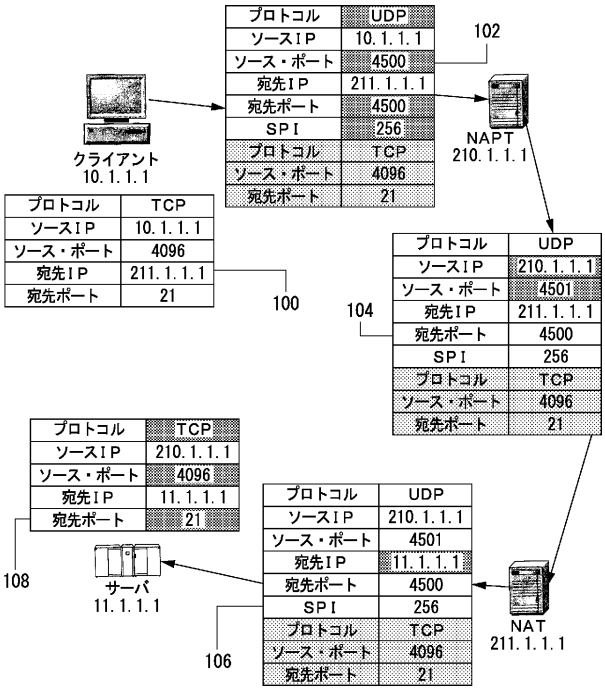
【図９】受信パケットが最初に宛先ホストに到着した場合に利用可能なオプションを示すフローチャートである。

【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処理を示すフローチャートである。

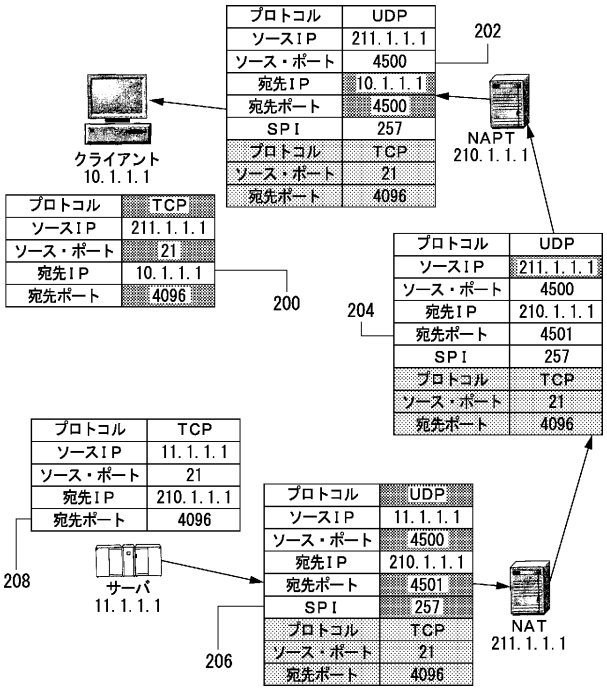
【図１１】カプセル化およびＮＡＰＴ通過という両条件を満足しない受信パケットを処理する一代替方法を示すフローチャートである。

【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。

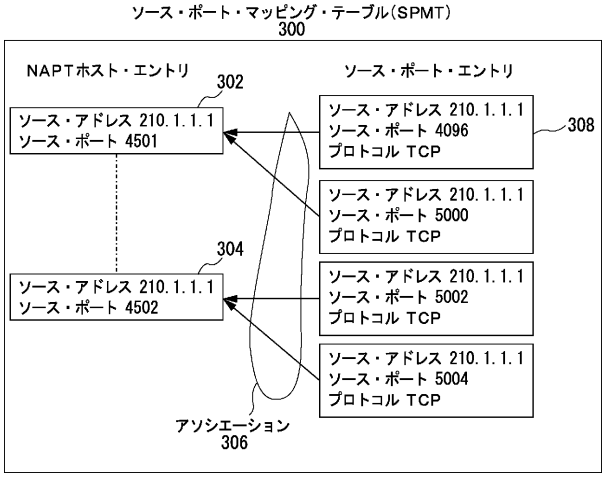
【図１】



【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		406		
IPヘッダ	UDPヘッダ	404	プロトコルTCP	408	410
ソース 210.1.1.1	ソース・ポート 4501	ESPヘッダ	ソース・ポート 4096	ペイロード	ESPトレーラ
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	
IPヘッダ	プロトコルTCP	508
ソース 210.1.1.1	ソース・ポート 4096	ペイロード
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

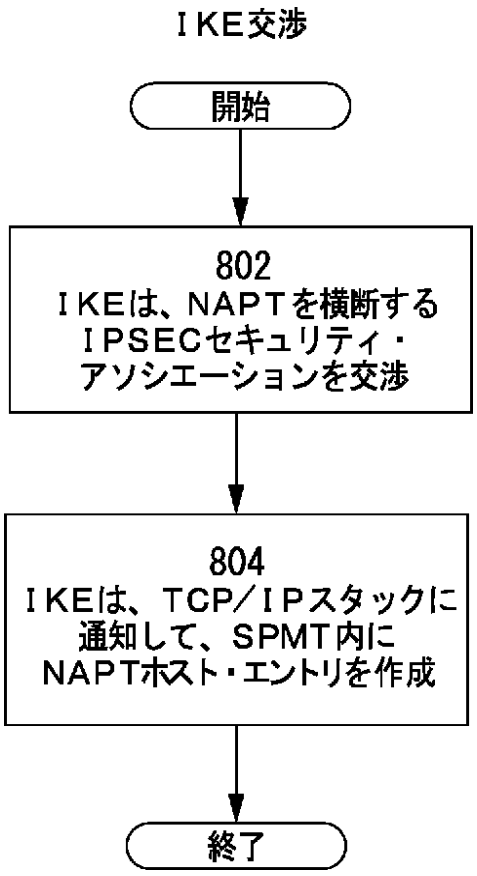
600	602		606		
IPヘッダ	UDPヘッダ	604	プロトコルTCP	608	610
ソース 210.1.1.1	ソース・ポート 4502	ESPヘッダ	ソース・ポート 4096	ペイロード	ESPトレーラ
宛先 11.1.1.1	宛先ポート 4500		宛先ポート 21		

【図７】

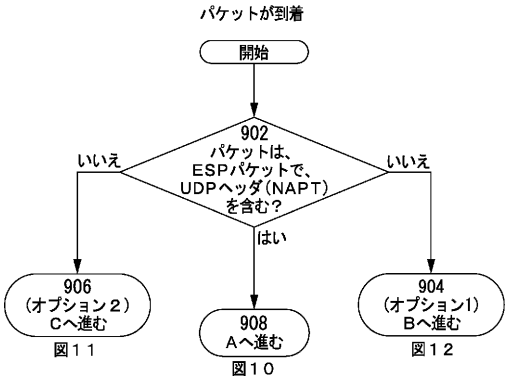
ホストにおけるIPSEC処理後の図５からのパケット

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

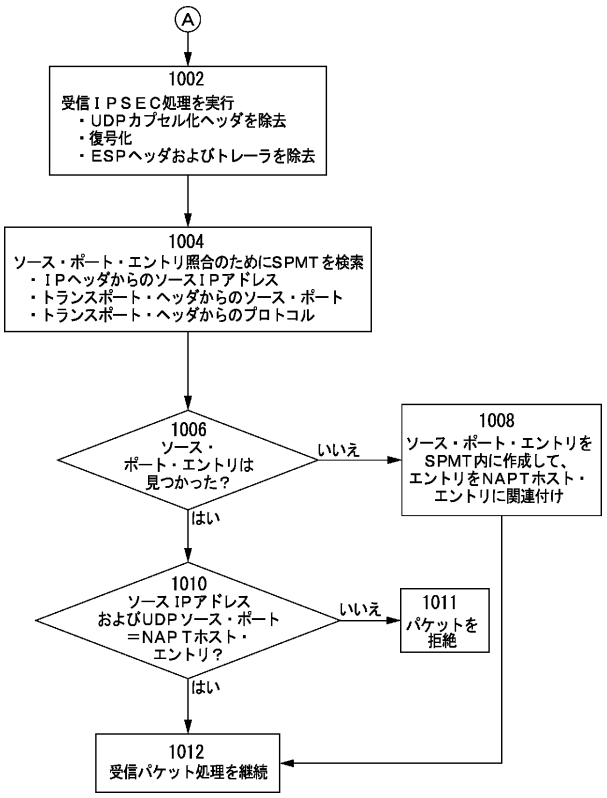
【図８】


ＩKE交渉
開始
802
ＩKEは、NAPTを横断する
ＩPSECセキュリティ・
アソシエーションを交渉
804
ＩKEは、TCP／ＩPスタックに
通知して、SPMT内に
NAPTホスト・エントリを作成
終了

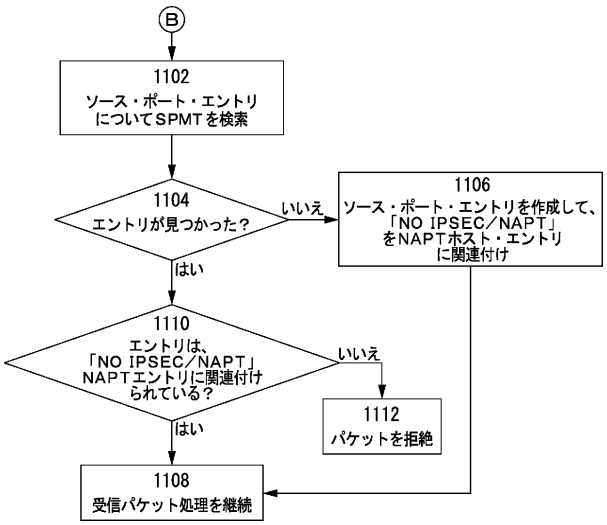
【図９】


パケットが到着
開始
902
パケットは、
ESPパケットで、
UDPヘッダ(NAPT)
を含む？
いいえ
いいえ
はい
906
(オプション２)
Cへ進む
908
Aへ進む
904
(オプション1)
Bへ進む
図１１
図１０
図１２

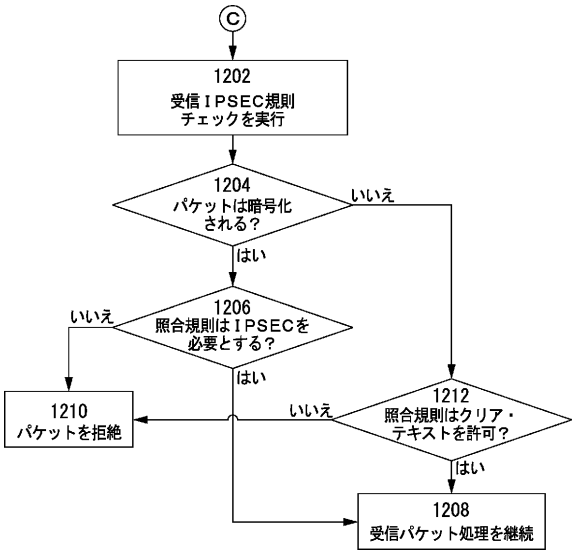
【図１０】


A
1002
受信ＩPSEC処理を実行
・UDPカプセル化ヘッダを除去
・復号化
・ESPヘッダおよびトレーラを除去
1004
ソース・ポート・エントリ照合のためにSPMTを検索
・ＩPヘッダからのソースＩPアドレス
・トランスポート・ヘッダからのソース・ポート
・トランスポート・ヘッダからのプロトコル
1006
ソース・
ポート・エントリは
見つかった？
いいえ
1008
ソース・ポート・エントリを
SPMT内に作成して、
エントリをNAPTホスト・
エントリに関連付け
はい
1010
ソース IPアドレス
およびUDPソース・ポート
＝NAP Tホスト・
エントリ？
いいえ
1011
パケットを
拒絶
はい
1012
受信パケット処理を継続

【図１１】


B
1102
ソース・ポート・エントリ
についてSPMTを検索
1104
エントリが見つかった？
いいえ
1106
ソース・ポート・エントリを作成して、
「NO IPSEC／NAPT」
をNAPTホスト・エントリ
に関連付け
はい
1110
エントリは、
「NO IPSEC／NAPT」
NAPTエントリに関連付け
られている？
いいえ
1112
パケットを拒絶
はい
1108
受信パケット処理を継続

【図１２】


Ⓒ
1202
受信ＩＰＳＥＣ規則
チェックを実行
1204
パケットは暗号化
される？
いいえ
はい
1206
照合規則はＩＰＳＥＣを
必要とする？
いいえ
はい
1210
パケットを拒絶
いいえ
1212
照合規則はクリア・
テキストを許可？
はい
1208
受信パケット処理を継続

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 永井 啓司

(56)参考文献 特開２００７－１４２６７５（ＪＰ，Ａ）
米国特許出願公開第２００４／０１４３７５８（ＵＳ，Ａ１）
A.Huttumen et al., UDP Encapsulation of IPsec ESP Packets, rfc3948, ２００５年 １月, http://www.ietf.org/rfc/rfc3948.txt

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 12/00-12/28、12/44-12/66