(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2015-515210
(P2015-515210A)
(43)公表日　平成27年5月21日(2015.5.21)

(51)Int.Cl.		F I			テーマコード（参考）
H04K 1/04	(2006.01)	H04K	1/04		5J104
G06F 21/60	(2013.01)	G06F	21/60	360	

審査請求 有　予備審査請求 未請求　（全 33 頁）

(21)出願番号	特願2015-503587 (P2015-503587)
(86)(22)出願日	平成25年3月28日 (2013.3.28)
(85)翻訳文提出日	平成26年11月7日 (2014.11.7)
(86)国際出願番号	PCT/US2013/034415
(87)国際公開番号	WO2013/149041
(87)国際公開日	平成25年10月3日 (2013.10.3)
(31)優先権主張番号	61/618,359
(32)優先日	平成24年3月30日 (2012.3.30)
(33)優先権主張国	米国 (US)

(71)出願人　504161984
ホアウェイ・テクノロジーズ・カンパニー・リミテッド
中華人民共和国・５１８１２９・グァンドン・シェンツェン・ロンガン・ディストリクト・バンティアン・（番地なし）・ホアウェイ・アドミニストレーション・ビルディング
(74)代理人　100146835
弁理士　佐伯　義文
(74)代理人　100140534
弁理士　木内　敬二

最終頁に続く

(54)【発明の名称】盗聴に対するＩＰｓｅｃ通信のパフォーマンス及びセキュリティの向上

(57)【要約】
本開示は、ネットワーク要素（ＮＥ）を提供し、このＮＥは、命令を格納するように構成されたメモリデバイスと、命令を実行することによって、データフロー中の複数の第１データパケットを複数の第１サブフローに分割し、ネットワークを介して複数の第１サブフローを第２のＮＥに伝送するように構成されたプロセッサとを具備する。複数の第１サブフローは、複数のパラレルサブセキュリティアソシエーション（ＳＡ）からなる第１のＩＰｓｅｃ　ＳＡクラスタを使用して伝送される。また、本開示は、インターネット鍵交換（ＩＫＥ）又はＩＫＥｖ２を使用して、ＮＥと第２のＮＥとの間に、複数の第１サブＳＡからなるＩＰｓｅｃ　ＳＡクラスタを作成するように構成されたプロセッサを具備したＮＥを提供する。複数の第１サブＳＡは、単方向性を有する。複数の第１サブＳＡは、複数の第１データパケットを共通の方向に伝送するように構成される。

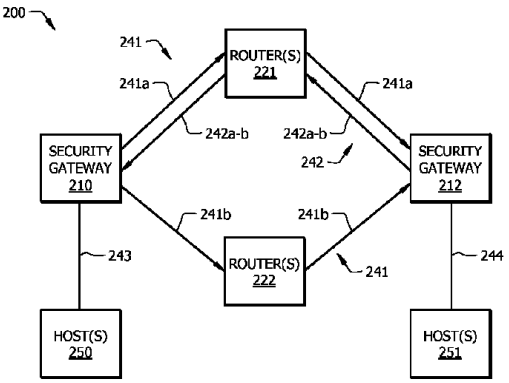


FIG. 2

【特許請求の範囲】
【請求項１】
ネットワーク要素（ＮＥ）であって、
命令を格納するように構成されたメモリデバイスと、
前記命令を実行することにより、
データフロー中の複数の第１データパケットを複数の第１サブフローに分割し、
ネットワークを介して前記複数の第１サブフローを第２のネットワーク要素に送信するように構成されたプロセッサと
を具備し、
前記複数の第１サブフローは、複数のパラレルサブセキュリティアソシエーション（ＳＡ）を含む第１のインターネットプロトコルセキュリティ（ＩＰｓｅｃ）ＳＡクラスタを使用して伝送されることを特徴とするネットワーク要素。
【請求項２】
前記複数のサブＳＡのうちの第１サブＳＡは、前記複数のサブＳＡのうちの第２サブＳＡとは異なるネットワークパスを通過することを特徴とする請求項１に記載のネットワーク要素。
【請求項３】
前記複数のサブＳＡのうちの第１サブＳＡは、前記複数のサブＳＡのうちの第２サブＳＡと共通のネットワークパスを通過することを特徴とする請求項１に記載のネットワーク要素。
【請求項４】
前記複数のサブＳＡが、ネストされないことを特徴とする請求項１に記載のネットワーク要素。
【請求項５】
前記データフロー中のデータパケットは、選択アルゴリズムを使用することによって、複数の第１サブＳＡに分散されることを特徴とする請求項１に記載のネットワーク要素。
【請求項６】
前記選択アルゴリズムが、ラウンドロビン選択アルゴリズム、ランダム選択アルゴリズム、又はラウンドロビン選択アルゴリズムとランダム選択アルゴリズムとの組合せを含むことを特徴とする請求項５に記載のネットワーク要素。
【請求項７】
前記複数のサブＳＡの各々が、セキュリティパラメータインデックス（ＳＰＩ）を含み、
各サブＳＡのＳＰＩは、他のサブＳＡのＳＰＩとは異なる値を有することを特徴とする請求項１に記載のネットワーク要素。
【請求項８】
前記プロセッサが、前記命令を実行することにより、
第２のＩＰｓｅｃ ＳＡクラスタを介して前記第２のネットワーク要素から複数の第２サブフローを受信するようにさらに構成されることを特徴とする請求項１に記載のネットワーク要素。
【請求項９】
前記複数の第２サブフローが、複数の第２データパケットを含み、
前記プロセッサが、前記命令を実行することにより、
アンチリプレイビットマップを使用することによって、前記複数の第２データパケットにアンチリプレイ機能を実行するようにさらに構成されることを特徴とする請求項８に記載のネットワーク要素。
【請求項１０】
前記複数の第１データパケットの各々が、シーケンス番号を有し、
前記シーケンス番号は、データパケットが関連付けられるサブフローに基づいて決定されるのであって、データフローに基づいては決定されないことを特徴とする請求項１に記

載のネットワーク要素。
【請求項１１】
ネットワーク要素（ＮＥ）であって、
インターネット鍵交換（ＩＫＥ）又はＩＫＥバージョン２（ＩＫＥｖ２）を使用して、ネットワーク要素と第２のネットワーク要素との間に、複数の第１サブセキュリティアソシエーション（ＳＡ）を含むインターネットプロトコルセキュリティ（ＩＰｓｅｃ）ＳＡクラスタを作成するように構成されたプロセッサを具備し、
前記複数の第１サブＳＡは、単方向性を有し、
前記複数の第１サブＳＡは、複数の第１データパケットを共通の方向に伝送するように構成されることを特徴とするネットワーク要素。
【請求項１２】
前記プロセッサが、前記複数の第１サブＳＡを使用して、通信セッションの間にネットワークを介して、複数の第１データパケットを前記第２のネットワーク要素に伝送するようにさらに構成されることを特徴とする請求項１１に記載のネットワーク要素。
【請求項１３】
前記プロセッサが、前記通信セッションの間に前記ネットワークを介して、前記第２のネットワーク要素から複数の第２データパケットを受信するようにさらに構成され、
前記複数の第２データパケットは、複数の第２サブＳＡを含む第２のＩＰｓｅｃ ＳＡクラスタを介して受信されることを特徴とする請求項１２に記載のネットワーク要素。
【請求項１４】
前記複数の第２サブＳＡが、単方向性を有し、
前記複数の第２サブＳＡが、データパケットを共通の方向に伝送するように構成され、
前記複数の第２サブＳＡが、前記複数の第１サブＳＡとは反対の方向にデータパケットを伝送するようにさらに構成されることを特徴とする請求項１３に記載のネットワーク要素。
【請求項１５】
データベース中の前記複数の第１サブＳＡのルックアップが並列して実行されるか、
前記複数の第１データパケットのシーケンス番号が並列して生成されるか、
前記複数の第２データパケットのアンチリプレイチェックが並列して実行されるか、又は、
これらが組み合わされて実行されることを特徴とする請求項１３に記載のネットワーク要素。
【請求項１６】
前記プロセッサが、ｓａＣｏｕｎｔ属性を処理することによって、前記ＳＡクラスタを作成するようにさらに構成され、
前記ｓａＣｏｕｎｔ属性に関連付けられた値は、前記ＳＡクラスタ中の第１サブＳＡの数を示すことを特徴とする請求項１１に記載のネットワーク要素。
【請求項１７】
前記プロセッサが、ｓｅｌｅｃｔＳＡ属性を処理することによって、前記ＳＡクラスタを作成するようにさらに構成され、
前記ｓｅｌｅｃｔＳＡ属性に関連付けられた値は、前記複数の第１データパケットに関連したサブフローの伝送のためのサブＳＡを選択するための選択アルゴリズムを示すことを特徴とする請求項１１に記載のネットワーク要素。
【請求項１８】
複数のインターネットプロトコルセキュリティ（ＩＰｓｅｃ）セキュリティアソシエーション（ＳＡ）サブトンネルを設定するステップと、
前記複数のＳＡサブトンネルを一緒にクラスタ化して、ＳＡクラスタを形成するステップと
を有することを特徴とする方法。
【請求項１９】

前記複数のＳＡサブトンネルが、独立して設定されて、１つずつ前記ＳＡクラスタに追加されることを特徴とする請求項１８に記載の方法。
【請求項２０】
前記複数のＳＡサブトンネルを介するように、ＩＰｓｅｃトラフィックを分割するか又は交番させるステップをさらに有することを特徴とする請求項１９に記載の方法。
【請求項２１】
前記ＳＡクラスタが、存続期間を有さないことを特徴とする請求項２０に記載の方法。
【請求項２２】
前記複数のＳＡサブトンネルが、受信エンティティにおいて共有のアンチリプレイビットマップを使用することを特徴とする請求項２１に記載の方法。
【請求項２３】
前記複数のＳＡサブトンネルの各々が、別個のアンチリプレイビットマップを使用することを特徴とする請求項２１に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、Xiangyang Zhangによって２０１２年３月３０日に出願された「Multiple Path IP Layer Security」と題する米国仮特許出願第６１／６１８３５９号の優先権を主張するものである。引用により、上記仮特許出願の全内容が本出願に援用される。
【背景技術】
【０００２】
ネットワークに接続されたデバイスは、さまざまなネットワークを経由して通信を行うことを要求される。デバイスによっては、そのような通信においても安全性（セキュリティ）を求められることがある。保護されたネットワーク（セキュアなネットワーク）を介して相互に接続されたデバイスは、いかなるネットワークを介した通信にもそのような安全性が提供されるように、保護されたネットワークに固有のセキュリティ対策手段に頼る。また、これらのデバイスは、保護されていないネットワークを経由して通信を行うことを要求されることがある。例えば、ホストコンピュータは、保護が部分的な、不均一な、及び／又はまったく保護されていないインターネットを介して、他のホスト、クライアント、ネットワーク等と通信を行うことがある。通信のセキュリティレベルは、送信側と受信側との間のあらゆる地点で通信に提供されるセキュリティレベルのうちで最も脆弱なレベルにしかなり得ない。保護されていないネットワークを通過する通信に対してセキュリティを維持するために、ネットワークデバイスは、さまざまなセキュリティプロトコルを使用し得る。例えば、発信元ネットワークデバイスは、発信元ネットワークデバイスと宛先ネットワークデバイスとの双方が（複数の）同一のセキュリティプロトコルを使用するように構成されていれば、宛先ネットワークデバイスと保護された接続及び／又は通信をネゴシエートし得る。
【先行技術文献】
【非特許文献】
【０００３】
【非特許文献１】Internet Engineering Task Force (IETF) document request for comment (RFC) 4301
【非特許文献２】IETF document draft-zhang-ipsecme-multi-path-ipsec-02
【非特許文献３】IETF document RFC 4302
【非特許文献４】IETF document RFC 4303
【発明の概要】
【課題を解決するための手段】
【０００４】
一態様において、本開示は、ネットワーク要素（Network Element, ＮＥ）を含み、このネットワーク要素は、命令を格納するように構成されたメモリデバイスと、命令を実行

することによって、データフロー中の複数の第１データパケットを複数の第１サブフローに分割し、ネットワークを介して複数の第１サブフローを第２のネットワーク要素に伝送するように構成されたプロセッサとを具備する。複数の第１サブフローは、複数のパラレルサブセキュリティアソシエーション（Security Association, ＳＡ）を含む第１のインターネットプロトコルセキュリティ（Internet Protocol Security, ＩＰｓｅｃ）ＳＡクラスタを使用して伝送される。

【０００５】

別の態様において、本開示は、インターネット鍵交換（Internet Key Exchange, ＩＫＥ）又はＩＫＥバージョン２（Internet Key Exchange version 2, ＩＫＥｖ２）を使用して、ネットワーク要素と第２のネットワーク要素との間に、複数の第１サブＳＡを含むＩＰｓｅｃ ＳＡクラスタを作成するように構成されたプロセッサを具備したネットワーク要素を含む。複数の第１サブＳＡは、単方向性を有する。複数の第１サブＳＡは、複数の第１データパケットを共通の方向に伝送するように構成される。

【０００６】

別の態様において、本開示は、複数のＩＰｓｅｃ ＳＡサブトンネルを設定するステップと、複数のＩＰｓｅｃ ＳＡサブトンネルを一緒にクラスタ化して、ＳＡクラスタを形成するステップとを有した方法を含む。

【０００７】

これらの及びその他の特徴は、添付の図面及び特許請求の範囲の記載と併せて、以下の発明の詳細な説明の記載からより明確に理解されよう。

【０００８】

以下では、本開示のより完全な理解のために、添付の図面及び発明の詳細な説明に関連して、簡単な説明を行う。同様の参照符号は、同様の部分を表す。

【図面の簡単な説明】

【０００９】

【図１】ＩＰｓｅｃセキュリティアーキテクチャの一実施形態を示す概略図である。

【図２】ＩＰｓｅｃセキュリティアーキテクチャの別の実施形態を示す概略図である。

【図３】ＳＡクラスタを作成する方法の一実施形態を示すフロー図である。

【図４】データサブフローに対するサブＳＡを選択する方法の一実施形態を示すフロー図である。

【図５】ＳＡクラスタを介してデータを受信する方法の一実施形態を示すフロー図である。

【図６】ネットワーク要素の一実施形態を示す概略図である。

【発明を実施するための形態】

【００１０】

ＩＰｓｅｃは、引用によって本出願に援用される、インターネット技術タスクフォース（Internet Engineering Task Force, ＩＥＴＦ）文書ＲＦＣ ４３０１（非特許文献１）で説明されるように、さまざまなネットワークを経由するインターネットプロトコル（Internet Protocol, ＩＰ）通信を保護するためのセキュリティプロトコル群を含むセキュリティプロトコルスイートである。ＩＰｓｅｃは、ＩＰ層（例えば、開放型システム間相互接続（Open Systems Interconnection, ＯＳＩ）参照モデルの第３層及び／又はネットワーク層）での通信を保護し得る。ＩＰｓｅｃは、セキュリティゲートウェイ間のデータフロー（例えば、通信）を保護するエンドツーエンドのセキュリティスキームとなり得る。ＩＰｓｅｃは、単方向性のＳＡ対を使用して、複数のデータパケットを含むデータフローを保護し得る。例えば、ローカルセキュリティゲートウェイは、リモートセキュリティゲートウェイに伝送する通信を保護するための第１のＳＡと、リモートセキュリティゲートウェイから受信する通信を保護するための第２のＳＡとを使用し得る。また、ＩＰｓｅｃは、ＳＡ内にＳＡがネストされる（例えば、トンネル内にトンネルを通す）ことを含むＳＡバンドルを許容してよい。ＩＰｓｅｃは、ＳＡ対及び／又はＳＡバンドル対を使用するように制限されてよい。ＩＰｓｅｃは、順次にＳＡを経由してパケットを伝送してよい

。また、各ＳＡには、一意に定まるセキュリティパラメータインデックス（Security Parameter Index, ＳＰＩ）が割り当てられてよい。このことから、盗聴ノードは、単一のネットワークノードを監視することによって、ＳＡによって保護されたトンネルを通過するすべてのパケットを受信し、ＳＰＩを使用してパケットを互いに関連付けし得る。盗聴ノードがＳＡセキュリティ対策手段を突破した場合、その盗聴ノードは、データフロー全体への完全なアクセスを行えるようになり得る。

【００１１】

本明細書で開示されるものは、保護されていないネットワークを経由して伝送されるデータトラフィックのための強化された保護機能を備えた方法及び／又はシステムである。ＩＰｓｅｃのデータ保護は、データフローを複数のサブフローに分割し、複数のサブフローを（例えば、複数のサブトンネル及び／又は複数のトランスポート通信を介して、）並行して伝送することによって強化され得る。サブＳＡは、サブフロー毎に独立して設定されてよい。複数のサブＳＡが組み合わされて、ＳＡクラスタが形成されてよい。各サブＳＡは、一意に定まるＳＰＩを含んでよい。ＳＡクラスタ中のサブＳＡは、ローカルセキュリティゲートウェイとリモートセキュリティゲートウェイとの間で異なるネットワークパスを使用してよく、又は使用しなくてもよい。このことから、盗聴ノードは、ネットワークパスの途中で単一のノードを監視することによっては、すべてのサブフローへのアクセスを行えず、他のネットワークパスの存在、数、又はルートを把握し得ない。また、各サブＳＡが一意に定まるＳＰＩを含み得るので、複数のサブフローからパケットを取得する盗聴ノードであっても、データパケットを互いに関連付けて、それらが同一のフローに関係していると判断し得ない。また、複数のサブフローのパラレル伝送は、シリアル伝送を超えて伝送効率を向上させることを可能にし得る。ＳＡクラスタについては、引用によって本出願に援用される、ＩＥＴＦ文書draft-zhang-ipsecme-multi-path-ipsec-02（非特許文献２）に詳しい。

【００１２】

方法及び／又はシステムは、複数のパスにデータトラフィックを分散させることによって、セキュリティサービスを向上させ得る。例えば、そのような分散は、異なる経路が使用されてよいので、攻撃者がすべてのパケットの傍受に成功するための難易度を高め得る。同一の経路が使用される場合であっても、攻撃者／盗聴者は、ＳＡのセットが特定のクラスタ化されたＳＡの一部分であると判断することが困難となり、これは、傍受されたパケットの復号化の難易度を増加させ得る。また、複数のパスの選択は、（例えば、リンク障害発生時の）信頼性の向上を提供し得る。また、複数のＳＡの使用は、最適化されたパフォーマンス及び最適化されたネットワークコントロールのための追加のオプションを提供し得る。これらの技術は、ＩＰｓｅｃによって提供されるセキュリティサービスを向上させ得る。ＳＡクラスタは、異なるパケットに異なる暗号変換を実行するオプションを提供してよい。さらにまた、ＳＡクラスタは、異なるパスに沿ってパケットを伝送するオプションを提供してよい。

【００１３】

図１は、ＩＰｓｅｃセキュリティアーキテクチャ１００の一実施形態を示す概略図である。ＩＰｓｅｃセキュリティアーキテクチャ１００は、ホスト１５０と、ホスト１５１とを具備し、これらは、保護されていないネットワーク１３０に位置するルータ１２０を経由して、セキュリティゲートウェイ１１０，１１２を介して通信を行い得る。ホスト１５０，１５１は、それぞれ、保護された接続１４３，１４４を介してセキュリティゲートウェイ１００，１１２に接続され得る。ホスト１５０，１５１は、保護されていないネットワーク１３０を経由する通信を希望し得る。セキュリティゲートウェイ１１０は、セキュリティゲートウェイ１１２への伝送のために、例えば、ＩＫＥ及び／又はＩＫＥｖ２を使用して、単方向性のＳＡ １４１を設定してよい。同様に、セキュリティゲートウェイ１１２は、セキュリティゲートウェイ１１０への伝送のために、単方向性のＳＡ １４２を設定してよく、その結果、ＳＡ対が作成され得る。ホスト１５０は、保護された接続１４３を介してセキュリティゲートウェイ１１０と通信を行うことによって、ホスト１５１に

データを伝送し得る。セキュリティゲートウェイ１１０は、ＳＡ １４１を使用して、ルータ１２０を介して保護されていないネットワーク１３０を経由してセキュリティゲートウェイ１１２に通信を伝送し得る。次いで、そのような通信は、保護された接続１４４を介してホスト１５１にルーティングされて、伝送された通信に対するエンドツーエンドセキュリティが達成され得る。ホスト１５１は、実質的に同一の手法で、ただし、ＳＡ １４１の代わりにＳＡ １４２を使用して、ホスト１５２にデータパケットを伝送し得る。

【００１４】

ホスト１５０，１５１などのホストは、ネットワークを介して他のホストと通信を行う任意のデバイスであってよい。例えば、ホスト１５０及び／又はホスト１５１は、サーバ、クライアント端末、又はそれらの組合せを含んでよい。ホスト１５０，１５１は、サービスリクエスト、アプリケーションホスティング等に応答して、リソースの共有を目的とするデータ通信を行うように構成されてよい。一例として、ホスト１５０は、クライアント端末を含んでよく、ホスト１５１は、サーバを含んでよく、かつホスト１５１は、アプリケーションをホストし、ホスト１５０からのアプリケーションリクエストに応答し得る。別の例では、ホスト１５０，１５１は、それぞれ、仮想マシン（Virtual Machine，ＶＭ）、記憶スペース、処理リソースなどのリソースを含んでよく、ネットワーク接続を介して、データ、アプリケーション等のリロケートを動的に行い得る。

【００１５】

セキュリティゲートウェイ１１０，１１２などのセキュリティゲートウェイは、保護されたネットワークのエッジに位置する任意のネットワーク要素（Network Element，ＮＥ）であってよい。保護されたネットワークは、保護された接続１４３，１４４などの保護された接続を含んでよい。セキュリティゲートウェイ１１０，１１２は、その内部に位置する任意のデバイス及び／又は保護されたネットワークを通過する通信に対してセキュリティを提供し得る。セキュリティゲートウェイ１１０，１１２は、保護されたネットワークに許可なくアクセスすることを防止してよく（例えば、ファイアウォールとして）、かつ保護されたネットワークを離れる通信のためのセキュリティプロトコルを実装してもよい。例えば、ホスト１５０，１５１が、それぞれ、データセンターに配置されている場合、セキュリティゲートウェイ１１０，１１２は、保護されたネットワークを離れるすべてのトラフィックがゲートウェイ１１０及び／又はゲートウェイ１１２を通過するように、データセンターネットワークのエッジに配置されてよい。セキュリティゲートウェイ１１０，１１２は、それぞれ、ホスト１５０，１５１からデータを受信し、保護されていないネットワーク１３０（例えば、インターネット）を経由するＩＰｓｅｃ ＳＡ １４１，１４２を作成することによって、通信セッションを開始してよい。セキュリティゲートウェイ１１０，１１２は、そのようなＳＡの作成を目的として、例えば、ＩＫＥ及び／又はＩＫＥｖ２を使用することによって、セキュリティ鍵を交換してよい。

【００１６】

ＳＡ １４１，１４２などのＩＰｓｅｃ ＳＡは、トランスポートモード又はトンネルモードで動作し得る。トランスポートモードでは、データパケットのペイロード（例えば、伝送される実際のデータ）が暗号化されてよく、一方、データパケットルーティング情報を含むデータパケットのヘッダは暗号化されずともよい。トンネルモードでは、データパケット全体が暗号化されてよい。また、ＳＡは、認証ヘッダ（Authentication Header，ＡＨ）及び／又はカプセル化セキュリティペイロード（Encapsulating Security Payload，ＥＳＰ）動作をサポートするためのデータ及び／又はアルゴリズムを含んでよい。ＡＨは、データフローに対するコネクションレス整合性及びデータ発信元認証を提供し得る。ＥＳＰは、データパケット秘匿性（例えば、カプセル化）、データ発信元認証、コネクションレス整合性、アンチリプレイサービス、及びフロー秘匿性を提供し得る。ＳＡ １４１，１４２は、それぞれ、単方向性を有してよい。このことから、ＳＡ １４１，１４２の対は、セキュリティゲートウェイ１１０，１１２間でデータパケットをやりとりするために必要とされ得る。一実施形態では、ＳＡ １４１，１４２は、それぞれ、ＳＡバンドルを含んでよい。ＳＡバンドルは、ネストされた２つのＳＡ（例えば、トンネル内のトン

ネル）を含み得る。例えば、ＳＡバンドルは、ＥＳＰ ＳＡ内のＡＨ ＳＡを含んでよい。ＩＰｓｅｃセキュリティアーキテクチャ１００は、セキュリティゲートウェイ１１０，１１２間の保護された通信毎に、単一のＳＡ対及び／又は単一のＳＡ対バンドル（例えば、ＳＡ １４１及びＳＡ １４２）を提供するように制限されてよい。各ＳＡは、別個のＳＰＩを含んでよく、別個のＳＰＩは、ＳＡデータベース（Security Association Database，ＳＡＤ）でインデックスとして使用されてよく、かつＳＡ宛先アドレスと組み合わされて、ＳＡを一意に識別し、ＳＡに関連付けられた暗号化鍵及びプロトコルを決定するために使用されてもよい。

【００１７】

ルータ１２０は、保護されていないネットワーク１３０に位置する任意のＮＥ又は複数のＮＥからなるグループであってよい。ルータは、セキュリティゲートウェイ１１０からデータパケットを受信し、セキュリティゲートウェイ１１２にデータパケットを転送してよく、また、その逆を行ってもよい。ルータ１２０は、ＯＳＩ参照モデルの第２層、第２．５層、及び／又は第３層の技術を使用して、パケットをルーティングし得る。ルータ１２０は、データパケットのヘッダに基づいてルーティング決定を行ってよい。データパケットがカプセル化されている場合（例えば、ＥＳＰの場合）、ルータ１２０は、データパケットのヘッダ及び／又はペイロードに格納されたデータを意識することなく、カプセル化されたパケットのヘッダに基づいてルーティング決定を行ってよい。ルータ１２０は、セキュリティゲートウェイ１１０とセキュリティゲートウェイ１１２との間のエンドツーエンド接続可能性を提供し得る。ルータ１２０は、ＳＡ １４１のための単一のネットワークパスと、ＳＡ １４２のための単一のネットワークパスとを用意してよい。ＳＡ １４１のためのネットワークパスは、ＳＡ １４２のためのネットワークパスと同一のパスであってもよく、又は同一のパスでなくてもよい。

【００１８】

ＩＰｓｅｃプロトコルスイートは、ＩＰｓｅｃに準拠するシステムのための基本アーキテクチャ１００の一例を指定するものである。ＩＰｓｅｃプロトコルスイートは、例えば、ＩＰ層において、ＩＰバージョン４（ＩＰｖ４）環境とＩＰバージョン６（ＩＰｖ６）環境との両方で、セキュリティサービスのセットがトラフィックに対してどのように提供されるかを説明するものである。先に記載したように、ＩＰｓｅｃプロトコルスイートは、ＩＰｓｅｃの概念としてＳＡを定義している。ＳＡ（例えば、ＳＡ １４１，１４２）は、接続によって搬送されるトラフィックにセキュリティサービスを付与し得る単純な接続を定義し得る。セキュリティサービスは、ＡＨ又はＥＳＰの使用によってＳＡに付与されてよく、それら両方によって単一のＳＡに提供されなくてもよい。ＡＨ及びＥＳＰは、引用によって本出願に援用される、ＩＥＴＦ文書ＲＦＣ ４３０２（非特許文献３）及びＲＦＣ ４３０３（非特許文献４）でさらに説明される。ＡＨ及びＥＳＰ保護の両方がトラフィックストリームに適用される場合、２つのＳＡが作成されて、セキュリティプロトコルの反復適用（例えば、ネストされたＳＡ）を介して保護が達成されるように調整されてよい。ユニキャストトラフィックを搬送するために１つのＳＡが使用され得るので、ＳＡの対（例えば、ＳＡ １４１及びＳＡ １４２）は、ポイントツーポイント通信として確立され得る。２つのＳＡ １４１，１４２は、２つのセキュリティゲートウェイ１１０，１１２間に１つのユニキャストＩＰｓｅｃトンネルを作成し得る。異なるＳＡ同士を区別するためには、３２ビットの値を含み得るＳＰＩが、到着データパケットが結び付けられるべきＳＡを識別するために受信側によって使用されてよい。ＳＰＩの割り当ては、ＳＡの作成者によって完了されてよく、それは受信側であってもよい。送信側では、任意のＳＰＩの競合を解決するために、追加的な宛先ＩＰアドレス情報が使用されてよい。このようにして、送信側は、その配下でＩＰパケットが処理される適切なＳＡを選択し得る。別の実施形態では、各セキュリティゲートウェイ１１０，１１２は、ローカルＳＰＩを割り当てるとともに、それぞれ、相手側ＳＰＩの知識を保持してもよい。パケットの送信時、各当事者（例えば、それぞれ、ゲートウェイ１１０又はゲートウェイ１１２）は、データパケットヘッダ中の他の当事者（例えば、それぞれ、ゲートウェイ１１２又はゲートウェ

イ１１０）のＳＰＩを使用してよい。

【００１９】

図１は、セキュリティゲートウェイ１１０，１１２間にＳＡが位置することだけを示しているが、ホスト１５０及び／又はホスト１５１などのホストは、ある実施形態では、ＳＡを介してゲートウェイ１１０及び／又はゲートウェイ１１２などのゲートウェイと直接に通信を行ってもよい。例えば、ホストとして機能するクライアント端末は、保護されたネットワーク上に配置されなくてよい。その場合、クライアント端末は、ＳＡを使用して、保護されていないネットワーク１３０を経由してセキュリティゲートウェイと直接に通信を行い得る。

【００２０】

図２は、ＩＰｓｅｃセキュリティアーキテクチャ２００の別の実施形態を示す概略図である。アーキテクチャ２００は、ホスト２５０，２５１、保護された接続２４３，２４４、セキュリティゲートウェイ２１０，２１２、及びルータ２２１，２２２を含んでよく、これらは、それぞれ、ホスト１５０，１５１、保護された接続１４３，１４４、セキュリティゲートウェイ１１０，１１２、及びルータ１２０と実質的に同一であってよい。セキュリティゲートウェイ２１０，２１２は、ＳＡクラスタ２４１及びＳＡクラスタ２４２を介して通信を行い得る。

【００２１】

ＳＡクラスタ２４１，２４２は、それぞれ、複数のパラレルサブＳＡを含んでよい。パラレルサブＳＡは、同一の発信元ノード（例えば、セキュリティゲートウェイ２１０）と、同一の宛先ノード（例えば、セキュリティゲートウェイ２１２）とを備えた複数の単方向性サブＳＡであってよく、それぞれ、同一のデータフローの一部分を搬送してよい。例えば、ＳＡクラスタ２４１は、パラレルサブＳＡ ２４１ａ，２４１ｂを含んでよく、ＳＡクラスタ２４２は、パラレルサブＳＡ ２４２ａ，２４２ｂを含んでよい。ＳＡクラスタは、サブＳＡがネストされ得るＳＡバンドルとは異なり得る。しかしながら、ある実施形態では、サブＳＡは、ＳＡバンドルを含んでもよい。ＳＡクラスタ毎に２つのサブＳＡだけが示されているが、ＳＡクラスタ２４１，２４２は、特定の通信のために望まれる分だけより多くのサブＳＡを含んでもよい。サブＳＡ ２４１ａ，２４１ｂは、それぞれ、ＳＡ １４１と同様のものであってよく、サブＳＡ ２４２ａ，２４２ｂは、それぞれ、ＳＡ １４２と同様のものであってよい。しかしながら、各サブＳＡは、データフローの一部分の搬送及び／又はカプセル化だけを行い得る。例えば、セキュリティゲートウェイ２１０は、複数のデータパケットを含むデータフローを、ＳＡクラスタ２４１を介してセキュリティゲートウェイ２１２に伝送することを希望し得る。セキュリティゲートウェイ２１０は、サブＳＡ ２４１ａ，２４１ｂ間でパケットを交番させ、サブＳＡ ２４１ｂよりも多くのパケットをサブＳＡ ２４１ａで送信し、フローを別個のデータパケットブロックに分割し、サブＳＡ ２４１ａ，２４１ｂ間のブロックに交番させる等を行い得る。サブＳＡは、それぞれ、異なるＳＰＩを有してよく、したがって、ＳＡクラスタ２４１及び／又はＳＡクラスタ２４２は、複数のＳＰＩを有し得る。ＳＡクラスタ中の複数のサブＳＡは、セキュリティゲート間で同一の経路又は異なる経路を使用してよい。例えば、ＳＡクラスタ２４１は、それぞれ、ルータ２２１を介する経路を使用するサブＳＡ ２４１ａと、ルータ２２２を介する経路を使用するサブＳＡ ２４１ｂとを含んでよい。別の例として、ＳＡクラスタ２４２は、そのどちらもルータ２２１を介する経路を使用するサブＳＡ ２４２ａ及びサブＳＡ ２４２ｂを含んでもよい。

【００２２】

アーキテクチャ２００は、データフローが分割され、盗聴ノードによって予測し得ない方法でルーティングされるようにし得る。各ＳＡクラスタが未知数のサブＳＡを含み得るので、盗聴ノードは、特定のデータフローに関係するデータパケットの正確な数を把握し得ない。さらに、各ＳＡクラスタが複数のＳＰＩを含み得るので、盗聴ノードは、取得した任意のデータパケットを互いに関連付けることができず、複数のデータパケットが同一のデータフローに関連することを判断できない。さらに、あるサブＳＡは他のサブＳＡと

は異なるネットワーク経路を通過し得るので、盗聴ノードは、単一のネットワークノードを監視することによっては、フローのデータパケットのすべてを取得できず、残りのデータパケットを取得するために他のどのデータパケットを監視すべきかを判断できない。このように、ＳＡクラスタ２４１及び／又はＳＡクラスタ２４２の使用は、盗聴及び／又はハッキングプロセスに重大な不確実性を付与し得、したがって、保護されていないネットワーク上のセキュリティを強化し得る。また、パラレルサブＳＡでデータパケットを送信する機能は、伝送を最適化し得る。例えば、ルータ２２１が輻輳状態となった場合、発信データパケットは、通信セッションを終了することなく、サブＳＡ ２４１ａからサブＳＡ２４１ｂに移されてよい。さらに、データフローパケットのパラレル伝送は、アーキテクチャ１００によって必要とされるデータフローパケットのシリアル処理と比較して、並列プロセッサの処理効率を増大させ得る。例えば、ＳＡルックアップ、シーケンス番号の生成、及び／又はアンチリプレイチェックは、データフローパケットが並列に伝送される場合には、並列に実行されてよい。

【００２３】

アーキテクチャ２００は、ＳＡクラスタの作成及び使用を実現するために、抽象構文記法１（Abstract Syntax Notation one, ＡＳＮ．１）を使用してよい。以下のＡＳＮ．１定義は、サブＳＡ（例えば、それぞれ、サブＳＡ ２４１ａ，２４１ｂ又はサブＳＡ ２４２ａ，２４２ｂ）の数に基づいて、ＳＡクラスタ（例えば、ＳＡクラスタ２４１及び／又はＳＡクラスタ２４２）を作成するためのものであってよく、また、サブフロー伝送のための適切なサブＳＡを選択するためのものであってもよい。

【００２４】

```
Processing ::= SEQUENCE {
extSeqNum     BOOLEAN, -- TRUE 64 bit counter, FALSE 32 bit
seqOverflow   BOOLEAN, -- TRUE rekey, FALSE terminate & audit
fragCheck     BOOLEAN, -- TRUE stateful fragment checking,
                       -- FALSE no stateful fragment checking
lifetime      SALifetime,
spi           ManualSPI,
algorithms    ProcessingAlgs,
tunnel        TunnelOptions  OPTIONAL, -- if absent, use transport mode
saCount       INTEGER  OPTIONAL,       -- if absent, use 1
selectSA      SASelAlgoType  OPTIONAL  -- ignored if saCount is 1,
                                       -- if absent, use round-robin
}
SASelAlgoType ::= INTEGER {
round-robin   (0),
random        (1),
others        (2)
}
```

【００２５】

上記のＡＳＮ．１定義では、ｅｘｔＳｅｑＮｕｍ、ｓｅｑＯｖｅｒｆｌｏｗ、及びｆｒａｇＣｈｅｃｋ属性は、論理値であってよく（例えば、真（true）又は偽（false）の値を含み得）、ＳＡクラスタを作成するエンティティが、６４ビットカウンタか又は３２ビットカウンタか、シーケンス番号がオーバーフローした場合に、クラスタに鍵を再発行（rekey）するか又は終了するか、フローの断片化に対してステートフルチェックを行うか又は行わないかについて、それぞれどのように設定すべきか指示するように設定され得る。ｌｉｆｅｔｉｍｅ属性は、ＳＡクラスタ及び／又は特定のサブＳＡの存続期間（lifetime）を指示してよく、ここで、存続期間は、ＳＡクラスタ及び／又はサブＳＡがデータを受信及び／又は送信することなくアクティブでいられる時間であってよい。ＳＡクラスタは、タイムアウトしないように設定されてもよい。ｓｐｉ属性は、ＳＰＩ値を手作業で設

定するために、管理者によって使用されてよく、ＳＰＩ値が自動的に生成される場合には、無視されてもよい。ａｌｇｏｒｉｔｈｍｓ属性は、ＳＡクラスタ及び／又はサブＳＡを作成及び／又は使用するために使用される他の処理アルゴリズムを指示し得る。ｔｕｎｎｅｌ属性は、ＳＡクラスタ及び／又はサブＳＡがトンネルモード及び／又はトランスポートモードを使用する否かと、トンネルモードに関連した任意のオプションとを指示するために使用され得る。ｓａＣｏｕｎｔ属性は、変数であってよく、ＳＡクラスタに対して作成されるサブＳＡの数を示す整数又は他の値に設定されてよい。ｓｅｌｅｃｔＳＡ属性は、変数であってよく、ＳＡＳｅｌＡｌｇｏＴｙｐｅに対応する整数又は他の値に設定されてよい。ｓｅｌｅｃｔＳＡは、特定のサブフローの伝送のためのサブＳＡを選択するために、送信者によって使用されてよい。ＳＡＳｅｌＡｌｇｏＴｙｐｅは、変数であってよく、特定の選択アルゴリズムを指示するために、整数又は他の値に設定されてよい。例えば、ＳＡＳｅｌＡｌｇｏＴｙｐｅは、ラウンドロビン選択アルゴリズムを示す値「０」、ランダム選択アルゴリズムを示す値「１」、他の選択アルゴリズム（例えば、ユーザ定義、ＳＡパスの遅延に基づく配分（apportion）、サービス品質が保証されたＳＡパスに基づく配分）を示す他の値に設定されてもよい。ラウンドロビンは、各サブＳＡにデータフロー中の等しい部分を割り当てる選択アルゴリズムであってよい。

【００２６】

データの機密性は、送信されたデータを盗聴などの受動的攻撃から保護し得る。ＩＰｓｅｃの実装形態（例えば、アーキテクチャ１００）において、すべてのＩＰデータグラムは、１つのＩＰｓｅｃトンネル内を伝送されてよく、１つのＳＡによる保護が提供され得る。機密セキュリティサービスを向上させるためには、ＳＡのセット（例えば、サブＳＡ　２４１ａ、サブＳＡ　２４１ｂ、サブＳＡ　２４２ａ、及び／又はサブＳＡ　２４２ｂ）がトラフィックを保護するために使用されてよい。複数のトンネルは、２つのエンティティ間にセットアップされ、次いで、一緒にクラスタ化されて、１つのクラスタ化トンネル（例えば、ＳＡクラスタ２４１及び／又はＳＡクラスタ２４２）を形成し得る。１つのＩＰパケットは、なお、単一のＳＡによって保護され得る。送信エンティティは、トラフィックをこれらすべてのサブＳＡに分割してよい。受信エンティティは、複数のＩＰｓｅｃトンネルからのトラフィックを多重化し得る。一緒にクラスタ化されたトンネルは、サブトンネルと称されてよい。サブトンネルに対するＳＡは、サブＳＡと称されてよい。１つのクラスタ化トンネル内で保護され得るＩＰトラフィックは、すべてのサブトンネルに分割されてよい。ＳＡクラスタという用語は、トラフィックがセキュリティポリシを満たすように処理されなければならないＳＡの組合せを説明するために使用されてよい。複数のサブトンネルが２つの保護されたエンティティ間のトラフィックの同一のフローに設定されるので、物理パスは異なり得る。これらのクラスタ化ＳＡの処理順序は、これらすべてのＳＡがＳＡにネストされてよく、又はネストされなくてもよいので、ローカルの問題となり得る。

【００２７】

ＳＡクラスタリングが送信者によって実行されてよいこと、及び受信エンティティがＩＰ層でのＳＡクラスタの存在を認識し得ることに留意されたい。例えば、トラフィックの多重化は、受信機がＩＰ層で複数のサブＳＡを経由するＳＡクラスタトラフィックを互いに関連付けるメカニズムを有し得ないので、上位層プロセスによって実行され、ＩＰｓｅｃプロセスによって直接に実行され得ない。しかしながら、上位層プロセスは、多重化トラフィックを収集する他の方法（例えば、上位層プロセスに関連するシーケンス番号を相互に関連付けること等）を使用してもよい。

【００２８】

サブＳＡは、ＩＫＥネゴシエーションを介してネゴシエートされている場合、自身のソフト及びハードの存続期間を有し得る。しかしながら、ＳＡクラスタに対する存続期間はなくともよい。アーキテクチャ２００は、各サブＳＡの維持性を変更し得ない。１つのサブＳＡが（例えば、タイムアウトにより）無効となった場合、そのようなサブＳＡは、さらなるパケット処理に使用され得ない。ＳＡクラスタが有効なサブＳＡを保持しなくなっ

た場合、そのＳＡクラスタは無効となってよい。

【００２９】

図３は、ＳＡクラスタを作成する方法３００の一実施形態を示すフロー図である。方法３００において、セキュリティゲートウェイ２１０及び／又はセキュリティゲートウェイ２１２などのＮＥは、ステップ３１０で、（例えば、ホスト２４０からの）リクエストを受信し、セキュリティゲートウェイ２１２などの別のＮＥとＳＡを確立し得る。ステップ３１２で、方法３００は、ＳＡに対するセキュリティポリシを検索し得る。セキュリティポリシは、ＮＥ上に配置されてよい及び／又は管理ＮＥなどの他のＮＥからアクセスされてよいセキュリティポリシデータベース（Security Policy Database, ＳＰＤ）に格納されてよい。セキュリティポリシは、ＳＡに関連付けられることとなる処理パラメータ及び／又は暗号鍵素材を決定するために使用されてよい。ステップ３１４で、方法３００は、セキュリティポリシをチェックして、ｓａＣｏｕｎｔ変数が存在するか決定し得る。方法３００は、ｓａＣｏｕｎｔ変数が存在しない場合はステップ３１６へ進み、ＳＡＣｏｕｎｔ変数が存在する場合はステップ３２０に進み得る。

【００３０】

ステップ３１６では、ｓａＣｏｕｎｔ変数が存在せず、これは、単一のＳＡ（例えば、ＳＡ １４１）がセキュリティポリシによって指定されていることを意味し得る。このことから、方法３００は、例えば、ＩＫＥ及び／又はＩＫＥｖ２を使用することによって、ＳＡを作成し、ステップ３１８に進んで動作を終了し得る。

【００３１】

ステップ３２０では、ｓａＣｏｕｎｔ変数が存在しており、これは、ＳＡクラスタ化がセキュリティポリシで指定されていることを意味し得る。ｓａＣｏｕｎｔ変数の値は、ＳＡクラスタ中のサブＳＡの数を示してよい。ｓａＣｏｕｎｔ変数の値が１以上でない場合、方法３００は、ステップ３２２に進み、クラスタは少なくとも１つのサブＳＡを必要とするので、エラーを返し得る。ｓａＣｏｕｎｔの値が１以上である場合、方法３００は、ステップ３２４に進み得る。ステップ３２４で、方法は、カウント変数を作成し、ｓａＣｏｕｎｔ変数の値に等しくなるように、カウント変数の値を設定し得る。ステップ３２６で、方法３００は、（例えば、ＩＫＥ及び／又はＩＫＥｖ２を使用することによって、）サブＳＡを作成し得る。ステップ３２８で、カウント変数の値は、１だけデクリメントされ得る。ステップ３３０で、方法３００は、カウント変数の値がゼロよりも大きいか否かを決定し得る。カウント変数の値がゼロよりも大きいままである場合、方法３００は、ステップ３２６に戻って、カウント変数の値によって指示されるように、追加のＳＡを作成し得る。カウント変数の値がステップ３３０でゼロに達した場合、方法３００は、ステップ３１８へ進んで動作を終了し得る。このように、サブＳＡは、セキュリティポリシに基づいて作成されて、ＳＡクラスタに追加されてよい。

【００３２】

先に記載したように、ＳＡクラスタのセットアップは、複数のサブＳＡのセットアップを含んでよい。サブトンネルは、独立して設定されてよい。セットアップの後、サブトンネルは、クラスタに１つずつ追加されることができる。ＳＡクラスタにサブＳＡを追加する正確な方法は、ローカルの問題であり得る。協働するすべてのサブトンネルは、異なるＳＰＩ値を含んでよい。１つのクラスタ化トンネルのためにいくつのサブトンネルが使用されるかの制限はなくてよい。送信エンティティと受信エンティティとの双方は、任意のＩＰｓｅｃトラフィックがサブトンネルのいずれかを介して送信される前に、ＳＡクラスタ仕様に合意し得る。新しいサブＳＡは、トラフィックがクラスタ化されたトンネル内に流れ始めた後にも、セットアップされ、ＳＡクラスタに参加し得る。サブトンネルが独立であっても、それらは１つのシーケンス番号ソースを共有してよい。クラスタ化されたトンネル内を搬送される各ＩＰｓｅｃパケットは、一意に定まるシーケンス番号を有してよい。

【００３３】

すべてのサブトンネルは、独立してセットアップされてよい。異なるサブトンネルを介

するトラフィックが同一の経路を使用してもよい。また、トラフィックは、ルーティングポリシに基づいて、例えば、コストが等しい複数の経路を使用することによって、異なる経路を使用してよい。ＳＡクラスタが１つのサブＳＡしか含まない場合には、ＳＡクラスタは、アーキテクチャ１００用に設計されたデバイスがＳＡクラスタをサポートしていない場合のアーキテクチャ１００の下で、ＩＰｓｅｃ実装と完全に相互運用可能であってよい。

【００３４】

図４は、データサブフローのためのサブＳＡを選択する方法４００の一実施形態を示すフロー図である。ステップ４１０で、発信パケットは、例えば、セキュリティゲートウェイ２１０及び／又はセキュリティゲートウェイ２１２によって、受信され得る。ステップ４１２で、方法４００は、ＳＰＤに問い合わせを行って、ステップ４１０からのパケットが属するフローに一致するＳＰＤエントリを見つけ出し得る。ステップ４１４で、方法４００は、ＳＰＤエントリに格納されたｓａＣｏｕｎｔ値が１よりも大きいか否かを決定し得る。方法は、ｓａＣｏｕｎｔ値が１よりも大きくない場合はステップ４１８に進み、ｓａＣｏｕｎｔ値が１よりも大きい場合はステップ４１６に進み得る。ステップ４１８で、方法４００は、ＳＡのＳＰＩとフロー情報とを使用してＳＡデータベース（ＳＡＤ）に問い合わせを行って、ＳＡのカプセル化及び／又は伝送を行うためのデータを見つけ出し得る。カウント値が１以下である場合、１つのＳＡだけが存在してよく、ＳＡ選択は必要とされなくてよい。カウント値が１よりも大きい場合、ステップ４１６で、方法４００は、サブＳＡ選択アルゴリズム（例えば、ｓｅｌｅｃｔＳＡ及び／又はＳＡＳｅｌＡｌｇｏＴｙｐｅ）に従って、サブフローのためのサブＳＡを選択し得る。サブＳＡが選択されると、方法は、ステップ４１８へ進み、選択されたサブＳＡのＳＰＩを使用してＳＡＤに問い合わせを行い得る。この方法では、フローのデータパケットは、選択アルゴリズムを使用することによって、サブＳＡ間に分配されてよい。先に記載したように、選択アルゴリズムは、データトラフィックの効率とセキュリティ上の理由との両方のために、サブＳＡ間でパケットを交番させてよい。

【００３５】

先に記載したように、送信エンティティは、ＩＰｓｅｃトラフィックを複数のサブトンネルを介するように分割及び／又は交番させ得る。ＳＡクラスタがセキュリティポリシ設定に基づいてトラフィック処理のために選択された場合、１つのサブＳＡは、指定されたパケットの発信ＩＰｓｅｃ処理のために選択され得る。ローカル実装は、指定されたＩＰパケットにどのＳＡが適用されるべきかを決定し得る。シーケンス番号がすべてのサブＳＡに共有され得ることを除いて、アーキテクチャ１００に関連する他の処理手順は、変更されずともよい。送信エンティティにおけるローカル実装は、パケットのシーケンス番号を取得するための任意の方法を選択してよく、サブＳＡの選択とは独立していてよい。代替実施形態では、各サブＳＡは、独自のシーケンス番号を生成してよく、サブＳＡ間のシーケンス番号の共有を必要としなくともよい。

【００３６】

図５は、ＳＡクラスタを介してデータを受信する方法５００の一実施形態を示すフロー図である。アンチリプレイは、ＩＰｓｅｃの機能であり、受信ＮＥが同一のパケットを複数回処理することを防止するために使用されてよい。単一のＳＡが使用される場合、パケットは、順番通りに受信されてよく、受信ＮＥは、最後に受信したパケットのシーケンス番号よりも小さいシーケンス番号を有する新たに受信したパケットを破棄することを許可され得る。ＳＡクラスタが使用される場合、パケットは、並行して送信されてよい。このことから、データパケットは、共有されるシーケンス番号が使用される場合には、順番通りには受信され得ない。方法５００は、アンチリプレイビットマップの使用を介してＳＡクラスタを使用するとき、アンチリプレイ機能を実現するために使用されてよい。

【００３７】

ステップ５１０で、受信パケットは、例えば、セキュリティゲートウェイ２１０及び／又はセキュリティゲートウェイ２１２によって、受信され得る。ステップ５１２で、方法

は、例えば、ＳＰＩを使用してＳＰＤに問い合わせを行うことによって、アンチリプレイがＳＡによって使用されるか否かを決定し得る。アンチリプレイがＳＡに使用されていない場合、方法５００は、ステップ５１４へ進み、パケットを処理し得る。アンチリプレイが使用される場合、方法５００は、ステップ５１６へ進み得る。ステップ５１６で、方法５００は、データパケットのシーケンス番号を取得し、そのシーケンス番号をアンチリプレイビットマップと比較し得る。例えば、アンチリプレイビットマップは、シーケンス番号に対応するパケットが受信されているか否かを示すための対応する値（例えば、それぞれ、値「０」、値「１」、又はそれらの組合せに設定される）を有する使用可能なすべてのシーケンス番号を含んでよい。ステップ５１８で、方法５００は、シーケンス番号がリプレイビットマップに設定されているか否かを決定し得る。シーケンス番号が（例えば、値「１」に）設定されている場合、方法は、そのシーケンス番号を有するパケットが既に受信されたと決定し、ステップ５２０へ進んで、パケットを破棄し得る。シーケンス番号が（例えば、値「１」に）設定されていない場合、方法は、そのシーケンス番号を有するパケットが受信されていないと決定し、ステップ５２２へ進み得る。ステップ５２２で、方法は、当該シーケンス番号に関連付けられたパケットが受信されていることを示すように、アンチリプレイビットマップを（例えば、対応する値を値「０」に設定することによって）更新し得る。次いで、方法５００は、ステップ５１４へ進み、パケットを処理し得る。

【００３８】

先に記載したように、受信側のサブＳＡの選択は、単一のＳＡの選択と同様のプロセスで行われよく、そのどちらも、ＳＰＩ及びＩＰアドレス情報に基づいてよい。シーケンス番号の処理への変更を除いて、他の態様は変更されずともよい。複数のサブトンネルの使用は、２つのエンティティ間の保護された通信チャネルに対して、ＩＰｓｅｃパケットの配信順序の乱れを生じさせ得る。対処法としては、受信エンティティが送信順序の維持を必要とする場合に、データパケットのＩＰｓｅｃヘッダ中のシーケンス番号を使用できる。アンチリプレイが有効になっている場合、すべてのサブトンネルは、受信エンティティで１つの共有アンチリプレイビットマップを使用してよい。アンチリプレイのチェックは、特定のサブＳＡの代わりに、ＳＡクラスタを対象として完了されてよい。

【００３９】

マルチパスソリューションが配信順序の乱れの問題をもたらすのであるが、この順序の乱れの問題は、単一のＳＡにも発生することがある。再順序付け（リオーダー）プロセスは、ＴＣＰリオーダー及び／又はＩＰリアセンブリと同様の手法で、特定のネットワークのトポロジーに基づいて、アグリゲートノード及び／又はエンドホスト（例えば、ホスト２４０及び／又はホスト２４１）において完了されてよい。

【００４０】

図６は、セキュリティゲートウェイ１１０、セキュリティゲートウェイ１１２、セキュリティゲートウェイ２１０、及び／若しくはセキュリティゲートウェイ２１２、ホスト１４０、ホスト１４１、ホスト２４０、及び／若しくはホスト２４１、並びに／又はルータ１２０、ルータ２２１、及び／若しくはルータ２２２を含み得るネットワーク要素（ＮＥ）６００の一実施形態を示す概略図である。当業者には、用語ＮＥに、ＮＥ ６００が一例に過ぎないデバイスの広い範囲が包含されることが認識されよう。ＮＥ ６００は、説明の明確化を目的として記載されるのであって、本開示の用途を特定のＮＥの実施形態又は実施形態のクラスに限定することを意味しない。本明細書に記載される特徴／方法のうちの少なくともいくつか、例えば、ＳＡクラスタを作成するための方法３００、サブフローのためのサブＳＡを選択するための方法４００、及び／又はＳＡクラスタからデータを受信するための方法５００は、ＮＥ ６００などのネットワーク装置又は構成要素の全体又は一部分として実装されてよい。例えば、本開示の特徴／方法は、ハードウェア、ファームウェア、及び／又はハードウェア上で動作するようインストールされたソフトウェアを使用して実施されてよい。ＮＥ ６００は、ネットワークを介してフレームを搬送する任意の装置、例えば、スイッチ、ルータ、ブリッジ、サーバ、クライアント等であってよ

い。図６に示すように、ＮＥ ６００は、送信機、受信機、又はそれらの組合せであり得るトランシーバ（Ｔｘ／Ｒｘ）６１０を含んでよい。Ｔｘ／Ｒｘ ６１０は、他のノードからのフレームを送信及び／又は受信するための複数のダウンストリームポート６２０に接続されてよく、かつＴｘ／Ｒｘ ６１０は、他のノードからのフレームを送信及び／又は受信するための複数のアップストリームポート６５０に接続されてよい。プロセッサ６３０は、フレームを処理するために及び／又はフレームを送信するノードを決定するために、Ｔｘ／Ｒｘ ６１０に接続されてよい。プロセッサ６３０は、１つ又は複数のマルチコアプロセッサ、及び／又は、データ格納部、バッファ等として機能し得るメモリデバイス６３２を含んでよい。プロセッサ６３０は、汎用プロセッサとして実装されてよく、あるいは、１つ以上の特定用途向け集積回路（Application Specific Integrated Circuit，ＡＳＩＣ）及び／又はデジタル信号プロセッサ（Digital Signal Processor，ＤＳＰ）の一部分であってもよい。ダウンストリームポート６２０及び／又はアップストリームポート６５０は、電気的な及び／又は光学的な送信及び／又は受信コンポーネントを含んでよい。ＮＥ ６００は、ルーティング決定を行うルーティングコンポーネントであってよく、又はなくてもよい。

【００４１】

ＮＥ ６００に実行可能な命令をプログラム及び／又はロードすることによって、プロセッサ６３０、ダウンストリームポート６２０、Ｔｘ／Ｒｘ ６１０、メモリ６３２、及び／又はアップストリームポート６５０のうちの少なくとも１つが変更され、本開示によって示唆される新規な機能を含む特定の機械又は装置、例えば、マルチコア転送アーキテクチャへとＮＥ ６００を部分的に変更するということに留意されたい。実行可能なソフトウェアをコンピュータにロードすることによって実施可能な機能性が既知の設計ルールによってハードウェア実施形態に変換可能であることは、電気工学及びソフトウェア工学の分野における基本的事項である。典型的に、ソフトウェアとして実装するか、ハードウェアとして実装するかの決定は、ソフトウェア領域からハードウェア領域への変換によって生じる何らかの問題というよりは、生産されるユニットの設計の安定性及び数量を考慮してなされる。一般に、ハードウェア実装の変更はソフトウェア設計の変更よりも高額となるので、頻繁に変更される設計は、ソフトウェアとして実装されることが好ましい。一般に、大規模生産に対しては、ハードウェア実装がソフトウェア実装よりも安価となり得るので、大量に生産されることが決まっている設計は、ハードウェア、例えば、ＡＳＩＣとして実装されることが好ましい。多くの場合、設計は、ソフトウェア形態で開発され、テストされた後に、既知の設計ルールによって、ソフトウェアの命令を配線回路（hardwire）として備える、特定用途向け集積回路の均等な配線回路実装へと変換される。新たなＡＳＩＣによってコントロールされる機械が特定の機械又は装置であることと同様に、実行可能な命令をプログラム及び／又はロードされたコンピュータもまた、特定の機械又は装置とみなされ得る。

【００４２】

少なくとも１つの実施形態が開示され、当技術分野で通常の知識を有する者によってなされる（複数の）実施形態の変形、組合せ、及び／若しくは修正、並びに／又は（複数の）実施形態の特徴は、本開示の範囲内にある。（複数の）実施形態の特徴の組合せ、統合、及び／又は省略の結果である変形形態もまた、本開示の範囲内にある。数値の範囲又は限定が明確に示されている場合、そのような明示的な範囲又は限定は、明確に示された範囲又は限定内に納まる大きさの反復的範囲又は限定を含む（例えば、約１から約１０は、２，３，４等を含み、０．１０を超えることは、０．１１，０．１２，０．１３等を含む）ものと理解されたい。例えば、下限Ｒ１、上限Ｒ２の数値範囲が開示されている場合、厳密に言えば、その範囲内に納まるあらゆる数値が開示されている。より詳細には、Ｒ＝Ｒ１＋ｋ＊（Ｒｕ－Ｒ１）の範囲内の数が明確に開示される。ここで、ｋは、１パーセント刻みで、１パーセントから１００パーセントの範囲内にある変数であり、すなわち、ｋは、１パーセント、２パーセント、３パーセント、４パーセント、５パーセント、…、７０パーセント、７１パーセント、７２パーセント、…、９５パーセント、９６パーセント

、９７パーセント、９８パーセント、９９パーセント、又は１００パーセントである。さらに、先に記載したように２つの数Ｒによって定義される任意の数値範囲もまた、明確に開示される。「約」という語の使用は、特に明記されない限り、後に続く数の±１０％を意味する。請求項中の任意の要素に対する「選択的に（optionally）」という語の使用は、その要素が必要とされること又はその要素が必要とされないことを意味し、その両方の選択肢が特許請求の範囲内にある。具備する、含む、及び有する（comprise, include, and having）といったより広い語の使用は、からなる（consisting of）、本質的に含む（consisting essentially of）、及び実質的に含む（comprised substantially of）といったより狭い語を包含するものと理解されたい。したがって、保護の範囲は、先に記載された内容によって限定されるのではなく、添付の特許請求の範囲によって規定されるのであって、特許請求の範囲の主題のすべての均等物を含む。各々の及びすべての請求項は、本明細書へのさらなる開示として援用され、かつ特許請求の範囲は、本開示の（複数の）実施形態でもある。開示中の参考文献についての記載は、それが従来技術であること、特に、本出願の優先日後の発行日を有する任意の参考文献であることを認めるものではない。本開示において引用したすべての特許、特許出願、及び刊行物の開示は、それらが本開示への例示的な、手続き的な、又はその他詳細な補足を提供するものであるとして、引用によって本開示に援用される。

【００４３】

本開示にはいくつかの実施形態が提供されているが、開示されたシステム及び方法は、本開示の精神又は範囲から逸脱することなく、他の多くの特定の形態で実施され得ることが理解されよう。本実施例は、例示のみを意図し、限定を意図せず、その意図は、明細書中で与えられた詳細に限定されるものではない。例えば、さまざまな要素又は構成要素は、別のシステムにおいては、組み合わされるか又は一体化されてよく、又は、ある特徴は、省略されるか又は実装されなくてよい。

【００４４】

さらに、個別に又は区別されてさまざまな実施形態として記載及び例示された、技術、システム、及び方法は、本開示の範囲から逸脱することなく、他のシステム、モジュール、技術、又は方法と組み合わせられるか又は統合されてよい。互いに接続されるか、直接接続されるか、又は通信を行うように示されるか又は説明された他の要素は、電気的、機械的、又はそれ以外であろうとなかろうと、何らかのインターフェース、デバイス、又は中間構成要素を介して、間接的に接続されるか又は通信を行ってよい。変更、代用、及び置換の他の例は、当業者によって確認可能であり、本明細書に開示される精神及び範囲から逸脱することなく行われてよい。

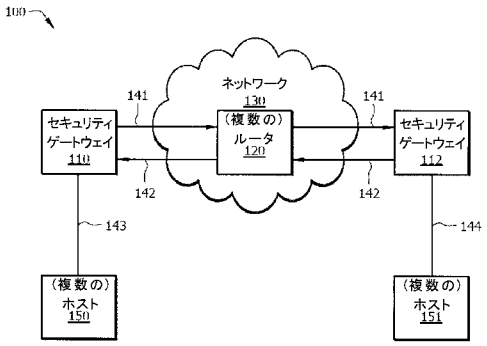
【符号の説明】

【００４５】

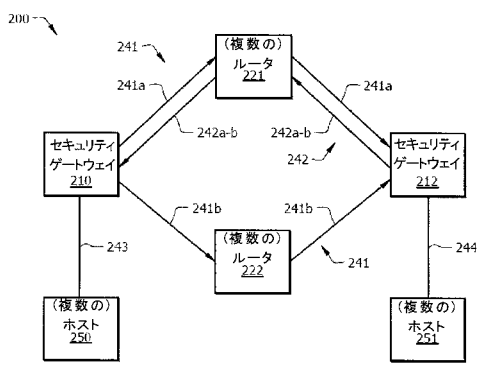
１００　ＩＰｓｅｃセキュリティアーキテクチャ
１１０，１１２，２１０，２１２　セキュリティゲートウェイ
１２０，２２１，２２２　ルータ
１３０　ネットワーク
１４１，１４２　単方向性セキュリティアソシエーション
１４３，１４４，２４３，２４４　保護された接続
１５０，１５１，２５０，２５１　ホスト
２４１，２４２　セキュリティアソシエーションクラスタ
２４１ａ，２４１ｂ，２４２ａ，２４２ｂ　パラレルサブセキュリティアソシエーション
６００　ネットワーク要素
６１０　トランシーバ
６２０　ダウンストリームポート
６３０　プロセッサ
６３２　メモリ

６５０　アップストリームポート

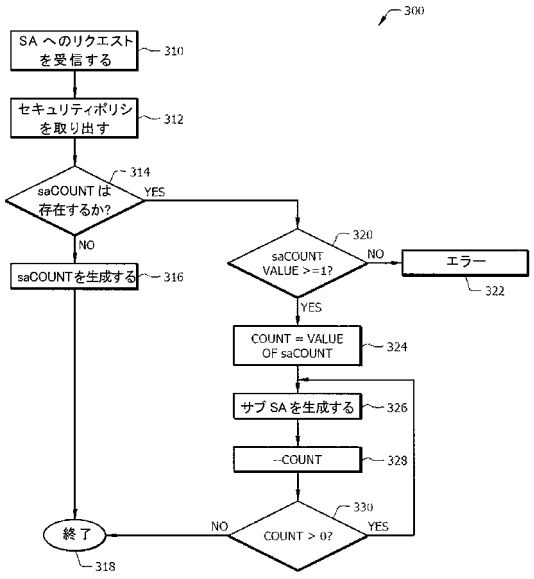
【図１】



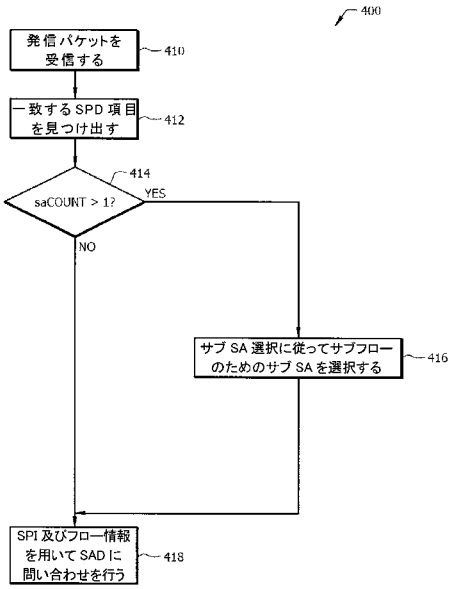
【図２】



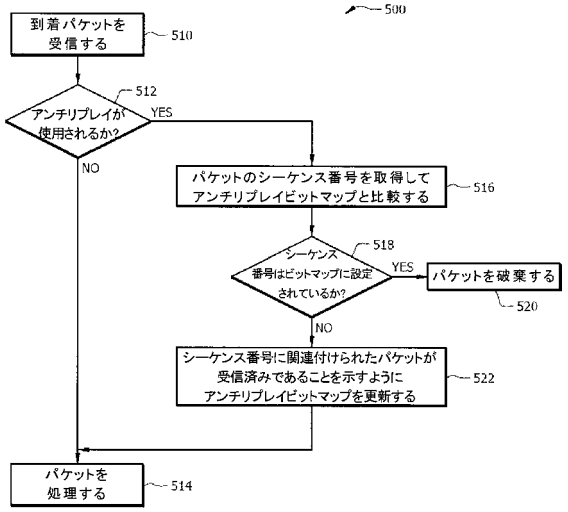
【図３】



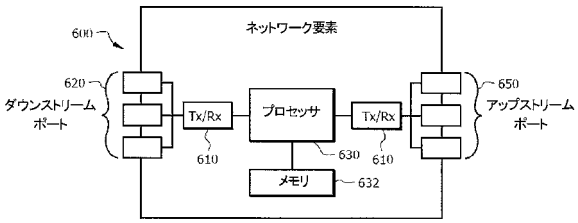
【図４】



【図５】



【図６】



【手続補正書】
【提出日】平成26年11月7日(2014.11.7)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【発明の詳細な説明】
【背景技術】
【０００１】
ネットワークに接続されたデバイスは、さまざまなネットワークを経由して通信を行うことを要求される。デバイスによっては、そのような通信においても安全性（セキュリティ）を求められることがある。保護されたネットワーク（セキュアなネットワーク）を介して相互に接続されたデバイスは、いかなるネットワークを介した通信にもそのような安全性が提供されるように、保護されたネットワークに固有のセキュリティ対策手段に頼る。また、これらのデバイスは、保護されていないネットワークを経由して通信を行うことを要求されることがある。例えば、ホストコンピュータは、保護が部分的な、不均一な、及び／又はまったく保護されていないインターネットを介して、他のホスト、クライアント、ネットワーク等と通信を行うことがある。通信のセキュリティレベルは、送信側と受信側との間のあらゆる地点で通信に提供されるセキュリティレベルのうちで最も脆弱なレベルにしかなり得ない。保護されていないネットワークを通過する通信に対してセキュリティを維持するために、ネットワークデバイスは、さまざまなセキュリティプロトコルを使用し得る。例えば、発信元ネットワークデバイスは、発信元ネットワークデバイスと宛先ネットワークデバイスとの双方が（複数の）同一のセキュリティプロトコルを使用するように構成されていれば、宛先ネットワークデバイスと保護された接続及び／又は通信を

ネゴシエートし得る。
【先行技術文献】
【非特許文献】
【０００２】
【非特許文献１】Internet Engineering Task Force (IETF) document request for comment (RFC) 4301
【非特許文献２】IETF document draft-zhang-ipsecme-multi-path-ipsec-02
【非特許文献３】IETF document RFC 4302
【非特許文献４】IETF document RFC 4303
【発明の概要】
【課題を解決するための手段】
【０００３】
一態様において、本開示は、ネットワーク要素（Network Element, ＮＥ）を含み、このネットワーク要素は、命令を格納するように構成されたメモリデバイスと、命令を実行することによって、データフロー中の複数の第１データパケットを複数の第１サブフローに分割し、ネットワークを介して複数の第１サブフローを第２のネットワーク要素に伝送するように構成されたプロセッサとを具備する。複数の第１サブフローは、複数のパラレルサブセキュリティアソシエーション（Security Association, ＳＡ）を含む第１のインターネットプロトコルセキュリティ（Internet Protocol Security, ＩＰｓｅｃ）ＳＡクラスタを使用して伝送される。
【０００４】
別の態様において、本開示は、インターネット鍵交換（Internet Key Exchange, ＩＫＥ）又はＩＫＥバージョン２（Internet Key Exchange version 2, ＩＫＥｖ２）を使用して、ネットワーク要素と第２のネットワーク要素との間に、複数の第１サブＳＡを含むＩＰｓｅｃ ＳＡクラスタを作成するように構成されたプロセッサを具備したネットワーク要素を含む。複数の第１サブＳＡは、単方向性を有する。複数の第１サブＳＡは、複数の第１データパケットを共通の方向に伝送するように構成される。
【０００５】
別の態様において、本開示は、複数のＩＰｓｅｃ ＳＡサブトンネルを設定するステップと、複数のＩＰｓｅｃ ＳＡサブトンネルを一緒にクラスタ化して、ＳＡクラスタを形成するステップとを有した方法を含む。
【０００６】
これらの及びその他の特徴は、添付の図面及び特許請求の範囲の記載と併せて、以下の発明の詳細な説明の記載からより明確に理解されよう。
【０００７】
以下では、本開示のより完全な理解のために、添付の図面及び発明の詳細な説明に関連して、簡単な説明を行う。同様の参照符号は、同様の部分を表す。
【図面の簡単な説明】
【０００８】
【図１】ＩＰｓｅｃセキュリティアーキテクチャの一実施形態を示す概略図である。
【図２】ＩＰｓｅｃセキュリティアーキテクチャの別の実施形態を示す概略図である。
【図３】ＳＡクラスタを作成する方法の一実施形態を示すフロー図である。
【図４】データサブフローに対するサブＳＡを選択する方法の一実施形態を示すフロー図である。
【図５】ＳＡクラスタを介してデータを受信する方法の一実施形態を示すフロー図である。
【図６】ネットワーク要素の一実施形態を示す概略図である。
【発明を実施するための形態】
【０００９】
ＩＰｓｅｃは、引用によって本出願に援用される、インターネット技術タスクフォース

（Internet Engineering Task Force, ＩＥＴＦ）文書ＲＦＣ ４３０１（非特許文献１）で説明されるように、さまざまなネットワークを経由するインターネットプロトコル（Internet Protocol, ＩＰ）通信を保護するためのセキュリティプロトコル群を含むセキュリティプロトコルスイートである。ＩＰｓｅｃは、ＩＰ層（例えば、開放型システム間相互接続（Open Systems Interconnection, ＯＳＩ）参照モデルの第３層及び／又はネットワーク層）での通信を保護し得る。ＩＰｓｅｃは、セキュリティゲートウェイ間のデータフロー（例えば、通信）を保護するエンドツーエンドのセキュリティスキームとなり得る。ＩＰｓｅｃは、単方向性のＳＡ対を使用して、複数のデータパケットを含むデータフローを保護し得る。例えば、ローカルセキュリティゲートウェイは、リモートセキュリティゲートウェイに伝送する通信を保護するための第１のＳＡと、リモートセキュリティゲートウェイから受信する通信を保護するための第２のＳＡとを使用し得る。また、ＩＰｓｅｃは、ＳＡ内にＳＡがネストされる（例えば、トンネル内にトンネルを通す）ことを含むＳＡバンドルを許容してよい。ＩＰｓｅｃは、ＳＡ対及び／又はＳＡバンドル対を使用するように制限されてよい。ＩＰｓｅｃは、順次にＳＡを経由してパケットを伝送してよい。また、各ＳＡには、一意に定まるセキュリティパラメータインデックス（Security Parameter Index, ＳＰＩ）が割り当てられてよい。このことから、盗聴ノードは、単一のネットワークノードを監視することによって、ＳＡによって保護されたトンネルを通過するすべてのパケットを受信し、ＳＰＩを使用してパケットを互いに関連付けし得る。盗聴ノードがＳＡセキュリティ対策手段を突破した場合、その盗聴ノードは、データフロー全体への完全なアクセスを行えるようになり得る。

【００１０】

本明細書で開示されるものは、保護されていないネットワークを経由して伝送されるデータトラフィックのための強化された保護機能を備えた方法及び／又はシステムである。ＩＰｓｅｃのデータ保護は、データフローを複数のサブフローに分割し、複数のサブフローを（例えば、複数のサブトンネル及び／又は複数のトランスポート通信を介して、）並行して伝送することによって強化され得る。サブＳＡは、サブフロー毎に独立して設定されてよい。複数のサブＳＡが組み合わされて、ＳＡクラスタが形成されてよい。各サブＳＡは、一意に定まるＳＰＩを含んでよい。ＳＡクラスタ中のサブＳＡは、ローカルセキュリティゲートウェイとリモートセキュリティゲートウェイとの間で異なるネットワークパスを使用してよく、又は使用しなくてもよい。このことから、盗聴ノードは、ネットワークパスの途中で単一のノードを監視することによっては、すべてのサブフローへのアクセスを行えず、他のネットワークパスの存在、数、又はルートを把握し得ない。また、各サブＳＡが一意に定まるＳＰＩを含み得るので、複数のサブフローからパケットを取得する盗聴ノードであっても、データパケットを互いに関連付けて、それらが同一のフローに関係していると判断し得ない。また、複数のサブフローのパラレル伝送は、シリアル伝送を超えて伝送効率を向上させることを可能にし得る。ＳＡクラスタについては、引用によって本出願に援用される、ＩＥＴＦ文書draft-zhang-ipsecme-multi-path-ipsec-02（非特許文献２）に詳しい。

【００１１】

方法及び／又はシステムは、複数のパスにデータトラフィックを分散させることによって、セキュリティサービスを向上させ得る。例えば、そのような分散は、異なる経路が使用されてよいので、攻撃者がすべてのパケットの傍受に成功するための難易度を高め得る。同一の経路が使用される場合であっても、攻撃者／盗聴者は、ＳＡのセットが特定のクラスタ化されたＳＡの一部分であると判断することが困難となり、これは、傍受されたパケットの復号化の難易度を増加させ得る。また、複数のパスの選択は、（例えば、リンク障害発生時の）信頼性の向上を提供し得る。また、複数のＳＡの使用は、最適化されたパフォーマンス及び最適化されたネットワークコントロールのための追加のオプションを提供し得る。これらの技術は、ＩＰｓｅｃによって提供されるセキュリティサービスを向上させ得る。ＳＡクラスタは、異なるパケットに異なる暗号変換を実行するオプションを提供してよい。さらにまた、ＳＡクラスタは、異なるパスに沿ってパケットを伝送するオプ

ションを提供してよい。
【００１２】
図１は、ＩＰｓｅｃセキュリティアーキテクチャ１００の一実施形態を示す概略図である。ＩＰｓｅｃセキュリティアーキテクチャ１００は、ホスト１５０と、ホスト１５１とを具備し、これらは、保護されていないネットワーク１３０に位置するルータ１２０を経由して、セキュリティゲートウェイ１１０，１１２を介して通信を行い得る。ホスト１５０，１５１は、それぞれ、保護された接続１４３，１４４を介してセキュリティゲートウェイ１００，１１２に接続され得る。ホスト１５０，１５１は、保護されていないネットワーク１３０を経由する通信を希望し得る。セキュリティゲートウェイ１１０は、セキュリティゲートウェイ１１２への伝送のために、例えば、ＩＫＥ及び／又はＩＫＥｖ２を使用して、単方向性のＳＡ １４１を設定してよい。同様に、セキュリティゲートウェイ１１２は、セキュリティゲートウェイ１１０への伝送のために、単方向性のＳＡ １４２を設定してよく、その結果、ＳＡ対が作成され得る。ホスト１５０は、保護された接続１４３を介してセキュリティゲートウェイ１１０と通信を行うことによって、ホスト１５１にデータを伝送し得る。セキュリティゲートウェイ１１０は、ＳＡ １４１を使用して、ルータ１２０を介して保護されていないネットワーク１３０を経由してセキュリティゲートウェイ１１２に通信を伝送し得る。次いで、そのような通信は、保護された接続１４４を介してホスト１５１にルーティングされて、伝送された通信に対するエンドツーエンドセキュリティが達成され得る。ホスト１５１は、実質的に同一の手法で、ただし、ＳＡ １４１の代わりにＳＡ １４２を使用して、ホスト１５２にデータパケットを伝送し得る。
【００１３】
ホスト１５０，１５１などのホストは、ネットワークを介して他のホストと通信を行う任意のデバイスであってよい。例えば、ホスト１５０及び／又はホスト１５１は、サーバ、クライアント端末、又はそれらの組合せを含んでよい。ホスト１５０，１５１は、サービスリクエスト、アプリケーションホスティング等に応答して、リソースの共有を目的とするデータ通信を行うように構成されてよい。一例として、ホスト１５０は、クライアント端末を含んでよく、ホスト１５１は、サーバを含んでよく、かつホスト１５１は、アプリケーションをホストし、ホスト１５０からのアプリケーションリクエストに応答し得る。別の例では、ホスト１５０，１５１は、それぞれ、仮想マシン（Virtual Machine，ＶＭ）、記憶スペース、処理リソースなどのリソースを含んでよく、ネットワーク接続を介して、データ、アプリケーション等のリロケートを動的に行い得る。
【００１４】
セキュリティゲートウェイ１１０，１１２などのセキュリティゲートウェイは、保護されたネットワークのエッジに位置する任意のネットワーク要素（Network Element，ＮＥ）であってよい。保護されたネットワークは、保護された接続１４３，１４４などの保護された接続を含んでよい。セキュリティゲートウェイ１１０，１１２は、その内部に位置する任意のデバイス及び／又は保護されたネットワークを通過する通信に対してセキュリティを提供し得る。セキュリティゲートウェイ１１０，１１２は、保護されたネットワークに許可なくアクセスすることを防止してよく（例えば、ファイアウォールとして）、かつ保護されたネットワークを離れる通信のためのセキュリティプロトコルを実装してもよい。例えば、ホスト１５０，１５１が、それぞれ、データセンターに配置されている場合、セキュリティゲートウェイ１１０，１１２は、保護されたネットワークを離れるすべてのトラフィックがゲートウェイ１１０及び／又はゲートウェイ１１２を通過するように、データセンターネットワークのエッジに配置されてよい。セキュリティゲートウェイ１１０，１１２は、それぞれ、ホスト１５０，１５１からデータを受信し、保護されていないネットワーク１３０（例えば、インターネット）を経由するＩＰｓｅｃ ＳＡ １４１，１４２を作成することによって、通信セッションを開始してよい。セキュリティゲートウェイ１１０，１１２は、そのようなＳＡの作成を目的として、例えば、ＩＫＥ及び／又はＩＫＥｖ２を使用することによって、セキュリティ鍵を交換してよい。
【００１５】

ＳＡ １４１，１４２などのＩＰｓｅｃ ＳＡは、トランスポートモード又はトンネルモードで動作し得る。トランスポートモードでは、データパケットのペイロード（例えば、伝送される実際のデータ）が暗号化されてよく、一方、データパケットルーティング情報を含むデータパケットのヘッダは暗号化されずともよい。トンネルモードでは、データパケット全体が暗号化されてよい。また、ＳＡは、認証ヘッダ（Authentication Header，ＡＨ）及び／又はカプセル化セキュリティペイロード（Encapsulating Security Payload，ＥＳＰ）動作をサポートするためのデータ及び／又はアルゴリズムを含んでよい。ＡＨは、データフローに対するコネクションレス整合性及びデータ発信元認証を提供し得る。ＥＳＰは、データパケット秘匿性（例えば、カプセル化）、データ発信元認証、コネクションレス整合性、アンチリプレイサービス、及びフロー秘匿性を提供し得る。ＳＡ １４１，１４２は、それぞれ、単方向性を有してよい。このことから、ＳＡ １４１，１４２の対は、セキュリティゲートウェイ１１０，１１２間でデータパケットをやりとりするために必要とされ得る。一実施形態では、ＳＡ １４１，１４２は、それぞれ、ＳＡバンドルを含んでよい。ＳＡバンドルは、ネストされた２つのＳＡ（例えば、トンネル内のトンネル）を含み得る。例えば、ＳＡバンドルは、ＥＳＰ ＳＡ内のＡＨ ＳＡを含んでよい。ＩＰｓｅｃセキュリティアーキテクチャ１００は、セキュリティゲートウェイ１１０，１１２間の保護された通信毎に、単一のＳＡ対及び／又は単一のＳＡ対バンドル（例えば、ＳＡ １４１及びＳＡ １４２）を提供するように制限されてよい。各ＳＡは、別個のＳＰＩを含んでよく、別個のＳＰＩは、ＳＡデータベース（Security Association Database，ＳＡＤ）でインデックスとして使用されてよく、かつＳＡ宛先アドレスと組み合わされて、ＳＡを一意に識別し、ＳＡに関連付けられた暗号化鍵及びプロトコルを決定するために使用されてもよい。

【００１６】

ルータ１２０は、保護されていないネットワーク１３０に位置する任意のＮＥ又は複数のＮＥからなるグループであってよい。ルータは、セキュリティゲートウェイ１１０からデータパケットを受信し、セキュリティゲートウェイ１１２にデータパケットを転送してよく、また、その逆を行ってもよい。ルータ１２０は、ＯＳＩ参照モデルの第２層、第２．５層、及び／又は第３層の技術を使用して、パケットをルーティングし得る。ルータ１２０は、データパケットのヘッダに基づいてルーティング決定を行ってよい。データパケットがカプセル化されている場合（例えば、ＥＳＰの場合）、ルータ１２０は、データパケットのヘッダ及び／又はペイロードに格納されたデータを意識することなく、カプセル化されたパケットのヘッダに基づいてルーティング決定を行ってよい。ルータ１２０は、セキュリティゲートウェイ１１０とセキュリティゲートウェイ１１２との間のエンドツーエンド接続可能性を提供し得る。ルータ１２０は、ＳＡ １４１のための単一のネットワークパスと、ＳＡ １４２のための単一のネットワークパスとを用意してよい。ＳＡ １４１のためのネットワークパスは、ＳＡ １４２のためのネットワークパスと同一のパスであってもよく、又は同一のパスでなくてもよい。

【００１７】

ＩＰｓｅｃプロトコルスイートは、ＩＰｓｅｃに準拠するシステムのための基本アーキテクチャ１００の一例を指定するものである。ＩＰｓｅｃプロトコルスイートは、例えば、ＩＰ層において、ＩＰバージョン４（ＩＰｖ４）環境とＩＰバージョン６（ＩＰｖ６）環境との両方で、セキュリティサービスのセットがトラフィックに対してどのように提供されるかを説明するものである。先に記載したように、ＩＰｓｅｃプロトコルスイートは、ＩＰｓｅｃの概念としてＳＡを定義している。ＳＡ（例えば、ＳＡ １４１，１４２）は、接続によって搬送されるトラフィックにセキュリティサービスを付与し得る単純な接続を定義し得る。セキュリティサービスは、ＡＨ又はＥＳＰの使用によってＳＡに付与されてよく、それら両方によって単一のＳＡに提供されなくてもよい。ＡＨ及びＥＳＰは、引用によって本出願に援用される、ＩＥＴＦ文書ＲＦＣ ４３０２（非特許文献３）及びＲＦＣ ４３０３（非特許文献４）でさらに説明される。ＡＨ及びＥＳＰ保護の両方がトラフィックストリームに適用される場合、２つのＳＡが作成されて、セキュリティプロト

コルの反復適用（例えば、ネストされたＳＡ）を介して保護が達成されるように調整されてよい。ユニキャストトラフィックを搬送するために１つのＳＡが使用され得るので、ＳＡの対（例えば、ＳＡ　１４１及びＳＡ　１４２）は、ポイントツーポイント通信として確立され得る。２つのＳＡ　１４１，１４２は、２つのセキュリティゲートウェイ１１０，１１２間に１つのユニキャストＩＰｓｅｃトンネルを作成し得る。異なるＳＡ同士を区別するためには、３２ビットの値を含み得るＳＰＩが、到着データパケットが結び付けられるべきＳＡを識別するために受信側によって使用されてよい。ＳＰＩの割り当ては、ＳＡの作成者によって完了されてよく、それは受信側であってもよい。送信側では、任意のＳＰＩの競合を解決するために、追加的な宛先ＩＰアドレス情報が使用されてよい。このようにして、送信側は、その配下でＩＰパケットが処理される適切なＳＡを選択し得る。別の実施形態では、各セキュリティゲートウェイ１１０，１１２は、ローカルＳＰＩを割り当てるとともに、それぞれ、相手側ＳＰＩの知識を保持してもよい。パケットの送信時、各当事者（例えば、それぞれ、ゲートウェイ１１０又はゲートウェイ１１２）は、データパケットヘッダ中の他の当事者（例えば、それぞれ、ゲートウェイ１１２又はゲートウェイ１１０）のＳＰＩを使用してよい。

【００１８】

図１は、セキュリティゲートウェイ１１０，１１２間にＳＡが位置することだけを示しているが、ホスト１５０及び／又はホスト１５１などのホストは、ある実施形態では、ＳＡを介してゲートウェイ１１０及び／又はゲートウェイ１１２などのゲートウェイと直接に通信を行ってもよい。例えば、ホストとして機能するクライアント端末は、保護されたネットワーク上に配置されなくてよい。その場合、クライアント端末は、ＳＡを使用して、保護されていないネットワーク１３０を経由してセキュリティゲートウェイと直接に通信を行い得る。

【００１９】

図２は、ＩＰｓｅｃセキュリティアーキテクチャ２００の別の実施形態を示す概略図である。アーキテクチャ２００は、ホスト２５０，２５１、保護された接続２４３，２４４、セキュリティゲートウェイ２１０，２１２、及びルータ２２１，２２２を含んでよく、これらは、それぞれ、ホスト１５０，１５１、保護された接続１４３，１４４、セキュリティゲートウェイ１１０，１１２、及びルータ１２０と実質的に同一であってよい。セキュリティゲートウェイ２１０，２１２は、ＳＡクラスタ２４１及びＳＡクラスタ２４２を介して通信を行い得る。

【００２０】

ＳＡクラスタ２４１，２４２は、それぞれ、複数のパラレルサブＳＡを含んでよい。パラレルサブＳＡは、同一の発信元ノード（例えば、セキュリティゲートウェイ２１０）と、同一の宛先ノード（例えば、セキュリティゲートウェイ２１２）とを備えた複数の単方向性サブＳＡであってよく、それぞれ、同一のデータフローの一部分を搬送してよい。例えば、ＳＡクラスタ２４１は、パラレルサブＳＡ　２４１ａ，２４１ｂを含んでよく、ＳＡクラスタ２４２は、パラレルサブＳＡ　２４２ａ，２４２ｂを含んでよい。ＳＡクラスタは、サブＳＡがネストされ得るＳＡバンドルとは異なり得る。しかしながら、ある実施形態では、サブＳＡは、ＳＡバンドルを含んでもよい。ＳＡクラスタ毎に２つのサブＳＡだけが示されているが、ＳＡクラスタ２４１，２４２は、特定の通信のために望まれる分だけより多くのサブＳＡを含んでもよい。サブＳＡ　２４１ａ，２４１ｂは、それぞれ、ＳＡ　１４１と同様のものであってよく、サブＳＡ　２４２ａ，２４２ｂは、それぞれ、ＳＡ　１４２と同様のものであってよい。しかしながら、各サブＳＡは、データフローの一部分の搬送及び／又はカプセル化だけを行い得る。例えば、セキュリティゲートウェイ２１０は、複数のデータパケットを含むデータフローを、ＳＡクラスタ２４１を介してセキュリティゲートウェイ２１２に伝送することを希望し得る。セキュリティゲートウェイ２１０は、サブＳＡ　２４１ａ，２４１ｂ間でパケットを交番させ、サブＳＡ　２４１ｂよりも多くのパケットをサブＳＡ　２４１ａで送信し、フローを別個のデータパケットブロックに分割し、サブＳＡ　２４１ａ，２４１ｂ間のブロックに交番させる等を行い得る。サ

ブＳＡは、それぞれ、異なるＳＰＩを有してよく、したがって、ＳＡクラスタ２４１及び／又はＳＡクラスタ２４２は、複数のＳＰＩを有し得る。ＳＡクラスタ中の複数のサブＳＡは、セキュリティゲート間で同一の経路又は異なる経路を使用してよい。例えば、ＳＡクラスタ２４１は、それぞれ、ルータ２２１を介する経路を使用するサブＳＡ ２４１ａと、ルータ２２２を介する経路を使用するサブＳＡ ２４１ｂとを含んでよい。別の例として、ＳＡクラスタ２４２は、そのどちらもルータ２２１を介する経路を使用するサブＳＡ ２４２ａ及びサブＳＡ ２４２ｂを含んでもよい。

【００２１】

アーキテクチャ２００は、データフローが分割され、盗聴ノードによって予測し得ない方法でルーティングされるようにし得る。各ＳＡクラスタが未知数のサブＳＡを含み得るので、盗聴ノードは、特定のデータフローに関係するデータパケットの正確な数を把握し得ない。さらに、各ＳＡクラスタが複数のＳＰＩを含み得るので、盗聴ノードは、取得した任意のデータパケットを互いに関連付けることができず、複数のデータパケットが同一のデータフローに関連することを判断できない。さらに、あるサブＳＡは他のサブＳＡとは異なるネットワーク経路を通過し得るので、盗聴ノードは、単一のネットワークノードを監視することによっては、フローのデータパケットのすべてを取得できず、残りのデータパケットを取得するために他のどのデータパケットを監視すべきかを判断できない。このように、ＳＡクラスタ２４１及び／又はＳＡクラスタ２４２の使用は、盗聴及び／又はハッキングプロセスに重大な不確実性を付与し得、したがって、保護されていないネットワーク上のセキュリティを強化し得る。また、パラレルサブＳＡでデータパケットを送信する機能は、伝送を最適化し得る。例えば、ルータ２２１が輻輳状態となった場合、発信データパケットは、通信セッションを終了することなく、サブＳＡ ２４１ａからサブＳＡ２４１ｂに移されてよい。さらに、データフローパケットのパラレル伝送は、アーキテクチャ１００によって必要とされるデータフローパケットのシリアル処理と比較して、並列プロセッサの処理効率を増大させ得る。例えば、ＳＡルックアップ、シーケンス番号の生成、及び／又はアンチリプレイチェックは、データフローパケットが並列に伝送される場合には、並列に実行されてよい。

【００２２】

アーキテクチャ２００は、ＳＡクラスタの作成及び使用を実現するために、抽象構文記法１（Abstract Syntax Notation one, ＡＳＮ．１）を使用してよい。以下のＡＳＮ．１定義は、サブＳＡ（例えば、それぞれ、サブＳＡ ２４１ａ，２４１ｂ又はサブＳＡ ２４２ａ，２４２ｂ）の数に基づいて、ＳＡクラスタ（例えば、ＳＡクラスタ２４１及び／又はＳＡクラスタ２４２）を作成するためのものであってよく、また、サブフロー伝送のための適切なサブＳＡを選択するためのものであってもよい。

【００２３】

```
Processing ::= SEQUENCE {
extSeqNum     BOOLEAN, -- TRUE 64 bit counter, FALSE 32 bit
seqOverflow   BOOLEAN, -- TRUE rekey, FALSE terminate & audit
fragCheck     BOOLEAN, -- TRUE stateful fragment checking,
                       -- FALSE no stateful fragment checking
lifetime      SALifetime,
spi           ManualSPI,
algorithms    ProcessingAlgs,
tunnel        TunnelOptions  OPTIONAL, -- if absent, use transport mode
saCount       INTEGER  OPTIONAL,       -- if absent, use 1
selectSA      SASelAlgoType  OPTIONAL  -- ignored if saCount is 1,
                                       -- if absent, use round-robin
}
SASelAlgoType ::= INTEGER {
round-robin   (0),
```

```
    random          (1),
    others          (2)
    }
```

【００２４】

上記のＡＳＮ．１定義では、ｅｘｔＳｅｑＮｕｍ、ｓｅｑＯｖｅｒｆｌｏｗ、及びｆｒａｇＣｈｅｃｋ属性は、論理値であってよく（例えば、真（true）又は偽（false）の値を含み得）、ＳＡクラスタを作成するエンティティが、６４ビットカウンタか又は３２ビットカウンタか、シーケンス番号がオーバーフローした場合に、クラスタに鍵を再発行（rekey）するか又は終了するか、フローの断片化に対してステートフルチェックを行うか又は行わないかについて、それぞれどのように設定すべきか指示するように設定され得る。ｌｉｆｅｔｉｍｅ属性は、ＳＡクラスタ及び／又は特定のサブＳＡの存続期間（lifetime）を指示してよく、ここで、存続期間は、ＳＡクラスタ及び／又はサブＳＡがデータを受信及び／又は送信することなくアクティブでいられる時間であってよい。ＳＡクラスタは、タイムアウトしないように設定されてもよい。ｓｐｉ属性は、ＳＰＩ値を手作業で設定するために、管理者によって使用されてよく、ＳＰＩ値が自動的に生成される場合には、無視されてもよい。ａｌｇｏｒｉｔｈｍｓ属性は、ＳＡクラスタ及び／又はサブＳＡを作成及び／又は使用するために使用される他の処理アルゴリズムを指示し得る。ｔｕｎｎｅｌ属性は、ＳＡクラスタ及び／又はサブＳＡがトンネルモード及び／又はトランスポートモードを使用する否かと、トンネルモードに関連した任意のオプションとを指示するために使用され得る。ｓａＣｏｕｎｔ属性は、変数であってよく、ＳＡクラスタに対して作成されるサブＳＡの数を示す整数又は他の値に設定されてよい。ｓｅｌｅｃｔＳＡ属性は、変数であってよく、ＳＡＳｅｌＡｌｇｏＴｙｐｅに対応する整数又は他の値に設定されてよい。ｓｅｌｅｃｔＳＡは、特定のサブフローの伝送のためのサブＳＡを選択するために、送信者によって使用されてよい。ＳＡＳｅｌＡｌｇｏＴｙｐｅは、変数であってよく、特定の選択アルゴリズムを指示するために、整数又は他の値に設定されてよい。例えば、ＳＡＳｅｌＡｌｇｏＴｙｐｅは、ラウンドロビン選択アルゴリズムを示す値「０」、ランダム選択アルゴリズムを示す値「１」、他の選択アルゴリズム（例えば、ユーザ定義、ＳＡパスの遅延に基づく配分（apportion）、サービス品質が保証されたＳＡパスに基づく配分）を示す他の値に設定されてもよい。ラウンドロビンは、各サブＳＡにデータフロー中の等しい部分を割り当てる選択アルゴリズムであってよい。

【００２５】

データの機密性は、送信されたデータを盗聴などの受動的攻撃から保護し得る。ＩＰｓｅｃの実装形態（例えば、アーキテクチャ１００）において、すべてのＩＰデータグラムは、１つのＩＰｓｅｃトンネル内を伝送されてよく、１つのＳＡによる保護が提供され得る。機密セキュリティサービスを向上させるためには、ＳＡのセット（例えば、サブＳＡ　２４１ａ、サブＳＡ　２４１ｂ、サブＳＡ　２４２ａ、及び／又はサブＳＡ　２４２ｂ）がトラフィックを保護するために使用されてよい。複数のトンネルは、２つのエンティティ間にセットアップされ、次いで、一緒にクラスタ化されて、１つのクラスタ化トンネル（例えば、ＳＡクラスタ２４１及び／又はＳＡクラスタ２４２）を形成し得る。１つのＩＰパケットは、なお、単一のＳＡによって保護され得る。送信エンティティは、トラフィックをこれらすべてのサブＳＡに分割してよい。受信エンティティは、複数のＩＰｓｅｃトンネルからのトラフィックを多重化し得る。一緒にクラスタ化されたトンネルは、サブトンネルと称されてよい。サブトンネルに対するＳＡは、サブＳＡと称されてよい。１つのクラスタ化トンネル内で保護され得るＩＰトラフィックは、すべてのサブトンネルに分割されてよい。ＳＡクラスタという用語は、トラフィックがセキュリティポリシを満たすように処理されなければならないＳＡの組合せを説明するために使用されてよい。複数のサブトンネルが２つの保護されたエンティティ間のトラフィックの同一のフローに設定されるので、物理パスは異なり得る。これらのクラスタ化ＳＡの処理順序は、これらすべてのＳＡがＳＡにネストされてよく、又はネストされなくてもよいので、ローカルの問題となり得る。

【００２６】
ＳＡクラスタリングが送信者によって実行されてよいこと、及び受信エンティティがＩＰ層でのＳＡクラスタの存在を認識し得ることに留意されたい。例えば、トラフィックの多重化は、受信機がＩＰ層で複数のサブＳＡを経由するＳＡクラスタトラフィックを互いに関連付けるメカニズムを有し得ないので、上位層プロセスによって実行され、ＩＰｓｅｃプロセスによって直接に実行され得ない。しかしながら、上位層プロセスは、多重化トラフィックを収集する他の方法（例えば、上位層プロセスに関連するシーケンス番号を相互に関連付けること等）を使用してもよい。
【００２７】
サブＳＡは、ＩＫＥネゴシエーションを介してネゴシエートされている場合、自身のソフト及びハードの存続期間を有し得る。しかしながら、ＳＡクラスタに対する存続期間はなくともよい。アーキテクチャ２００は、各サブＳＡの維持性を変更し得ない。１つのサブＳＡが（例えば、タイムアウトにより）無効となった場合、そのようなサブＳＡは、さらなるパケット処理に使用され得ない。ＳＡクラスタが有効なサブＳＡを保持しなくなった場合、そのＳＡクラスタは無効となってよい。
【００２８】
図３は、ＳＡクラスタを作成する方法３００の一実施形態を示すフロー図である。方法３００において、セキュリティゲートウェイ２１０及び／又はセキュリティゲートウェイ２１２などのＮＥは、ステップ３１０で、（例えば、ホスト２４０からの）リクエストを受信し、セキュリティゲートウェイ２１２などの別のＮＥとＳＡを確立し得る。ステップ３１２で、方法３００は、ＳＡに対するセキュリティポリシを検索し得る。セキュリティポリシは、ＮＥ上に配置されてよい及び／又は管理ＮＥなどの他のＮＥからアクセスされてよいセキュリティポリシデータベース（Security Policy Database, ＳＰＤ）に格納されてよい。セキュリティポリシは、ＳＡに関連付けられることとなる処理パラメータ及び／又は暗号鍵素材を決定するために使用されてよい。ステップ３１４で、方法３００は、セキュリティポリシをチェックして、ｓａＣｏｕｎｔ変数が存在するか決定し得る。方法３００は、ｓａＣｏｕｎｔ変数が存在しない場合はステップ３１６へ進み、ＳＡＣｏｕｎｔ変数が存在する場合はステップ３２０に進み得る。
【００２９】
ステップ３１６では、ｓａＣｏｕｎｔ変数が存在せず、これは、単一のＳＡ（例えば、ＳＡ １４１）がセキュリティポリシによって指定されていることを意味し得る。このことから、方法３００は、例えば、ＩＫＥ及び／又はＩＫＥｖ２を使用することによって、ＳＡを作成し、ステップ３１８に進んで動作を終了し得る。
【００３０】
ステップ３２０では、ｓａＣｏｕｎｔ変数が存在しており、これは、ＳＡクラスタ化がセキュリティポリシで指定されていることを意味し得る。ｓａＣｏｕｎｔ変数の値は、ＳＡクラスタ中のサブＳＡの数を示してよい。ｓａＣｏｕｎｔ変数の値が１以上でない場合、方法３００は、ステップ３２２に進み、クラスタは少なくとも１つのサブＳＡを必要とするので、エラーを返し得る。ｓａＣｏｕｎｔの値が１以上である場合、方法３００は、ステップ３２４に進み得る。ステップ３２４で、方法は、カウント変数を作成し、ｓａＣｏｕｎｔ変数の値に等しくなるように、カウント変数の値を設定し得る。ステップ３２６で、方法３００は、（例えば、ＩＫＥ及び／又はＩＫＥｖ２を使用することによって、）サブＳＡを作成し得る。ステップ３２８で、カウント変数の値は、１だけデクリメントされ得る。ステップ３３０で、方法３００は、カウント変数の値がゼロよりも大きいか否かを決定し得る。カウント変数の値がゼロよりも大きいままである場合、方法３００は、ステップ３２６に戻って、カウント変数の値によって指示されるように、追加のＳＡを作成し得る。カウント変数の値がステップ３３０でゼロに達した場合、方法３００は、ステップ３１８へ進んで動作を終了し得る。このように、サブＳＡは、セキュリティポリシに基づいて作成されて、ＳＡクラスタに追加されてよい。
【００３１】

先に記載したように、ＳＡクラスタのセットアップは、複数のサブＳＡのセットアップを含んでよい。サブトンネルは、独立して設定されてよい。セットアップの後、サブトンネルは、クラスタに１つずつ追加されることができる。ＳＡクラスタにサブＳＡを追加する正確な方法は、ローカルの問題であり得る。協働するすべてのサブトンネルは、異なるＳＰＩ値を含んでよい。１つのクラスタ化トンネルのためにいくつのサブトンネルが使用されるかの制限はなくてよい。送信エンティティと受信エンティティとの双方は、任意のＩＰｓｅｃトラフィックがサブトンネルのいずれかを介して送信される前に、ＳＡクラスタ仕様に合意し得る。新しいサブＳＡは、トラフィックがクラスタ化されたトンネル内に流れ始めた後にも、セットアップされ、ＳＡクラスタに参加し得る。サブトンネルが独立であっても、それらは１つのシーケンス番号ソースを共有してよい。クラスタ化されたトンネル内を搬送される各ＩＰｓｅｃパケットは、一意に定まるシーケンス番号を有してよい。

【００３２】

すべてのサブトンネルは、独立してセットアップされてよい。異なるサブトンネルを介するトラフィックが同一の経路を使用してもよい。また、トラフィックは、ルーティングポリシに基づいて、例えば、コストが等しい複数の経路を使用することによって、異なる経路を使用してよい。ＳＡクラスタが１つのサブＳＡしか含まない場合には、ＳＡクラスタは、アーキテクチャ１００用に設計されたデバイスがＳＡクラスタをサポートしていない場合のアーキテクチャ１００の下で、ＩＰｓｅｃ実装と完全に相互運用可能であってよい。

【００３３】

図４は、データサブフローのためのサブＳＡを選択する方法４００の一実施形態を示すフロー図である。ステップ４１０で、発信パケットは、例えば、セキュリティゲートウェイ２１０及び／又はセキュリティゲートウェイ２１２によって、受信され得る。ステップ４１２で、方法４００は、ＳＰＤに問い合わせを行って、ステップ４１０からのパケットが属するフローに一致するＳＰＤエントリを見つけ出し得る。ステップ４１４で、方法４００は、ＳＰＤエントリに格納されたｓａＣｏｕｎｔ値が１よりも大きいか否かを決定し得る。方法は、ｓａＣｏｕｎｔ値が１よりも大きくない場合はステップ４１８に進み、ｓａＣｏｕｎｔ値が１よりも大きい場合はステップ４１６に進み得る。ステップ４１８で、方法４００は、ＳＡのＳＰＩとフロー情報とを使用してＳＡデータベース（ＳＡＤ）に問い合わせを行って、ＳＡのカプセル化及び／又は伝送を行うためのデータを見つけ出し得る。カウント値が１以下である場合、１つのＳＡだけが存在してよく、ＳＡ選択は必要とされなくてよい。カウント値が１よりも大きい場合、ステップ４１６で、方法４００は、サブＳＡ選択アルゴリズム（例えば、ｓｅｌｅｃｔＳＡ及び／又はＳＡＳｅｌＡｌｇｏＴｙｐｅ）に従って、サブフローのためのサブＳＡを選択し得る。サブＳＡが選択されると、方法は、ステップ４１８へ進み、選択されたサブＳＡのＳＰＩを使用してＳＡＤに問い合わせを行い得る。この方法では、フローのデータパケットは、選択アルゴリズムを使用することによって、サブＳＡ間に分配されてよい。先に記載したように、選択アルゴリズムは、データトラフィックの効率とセキュリティ上の理由との両方のために、サブＳＡ間でパケットを交番させてよい。

【００３４】

先に記載したように、送信エンティティは、ＩＰｓｅｃトラフィックを複数のサブトンネルを介するように分割及び／又は交番させ得る。ＳＡクラスタがセキュリティポリシ設定に基づいてトラフィック処理のために選択された場合、１つのサブＳＡは、指定されたパケットの発信ＩＰｓｅｃ処理のために選択され得る。ローカル実装は、指定されたＩＰパケットにどのＳＡが適用されるべきかを決定し得る。シーケンス番号がすべてのサブＳＡに共有され得ることを除いて、アーキテクチャ１００に関連する他の処理手順は、変更されずともよい。送信エンティティにおけるローカル実装は、パケットのシーケンス番号を取得するための任意の方法を選択してよく、サブＳＡの選択とは独立していてよい。代替実施形態では、各サブＳＡは、独自のシーケンス番号を生成してよく、サブＳＡ間のシ

ーケンス番号の共有を必要としなくともよい。
【００３５】
図５は、ＳＡクラスタを介してデータを受信する方法５００の一実施形態を示すフロー図である。アンチリプレイは、ＩＰｓｅｃの機能であり、受信ＮＥが同一のパケットを複数回処理することを防止するために使用されてよい。単一のＳＡが使用される場合、パケットは、順番通りに受信されてよく、受信ＮＥは、最後に受信したパケットのシーケンス番号よりも小さいシーケンス番号を有する新たに受信したパケットを破棄することを許可され得る。ＳＡクラスタが使用される場合、パケットは、並行して送信されてよい。このことから、データパケットは、共有されるシーケンス番号が使用される場合には、順番通りには受信され得ない。方法５００は、アンチリプレイビットマップの使用を介してＳＡクラスタを使用するとき、アンチリプレイ機能を実現するために使用されてよい。
【００３６】
ステップ５１０で、受信パケットは、例えば、セキュリティゲートウェイ２１０及び／又はセキュリティゲートウェイ２１２によって、受信され得る。ステップ５１２で、方法は、例えば、ＳＰＩを使用してＳＰＤに問い合わせを行うことによって、アンチリプレイがＳＡによって使用されるか否かを決定し得る。アンチリプレイがＳＡに使用されていない場合、方法５００は、ステップ５１４へ進み、パケットを処理し得る。アンチリプレイが使用される場合、方法５００は、ステップ５１６へ進み得る。ステップ５１６で、方法５００は、データパケットのシーケンス番号を取得し、そのシーケンス番号をアンチリプレイビットマップと比較し得る。例えば、アンチリプレイビットマップは、シーケンス番号に対応するパケットが受信されているか否かを示すための対応する値（例えば、それぞれ、値「０」、値「１」、又はそれらの組合せに設定される）を有する使用可能なすべてのシーケンス番号を含んでよい。ステップ５１８で、方法５００は、シーケンス番号がリプレイビットマップに設定されているか否かを決定し得る。シーケンス番号が（例えば、値「１」に）設定されている場合、方法は、そのシーケンス番号を有するパケットが既に受信されたと決定し、ステップ５２０へ進んで、パケットを破棄し得る。シーケンス番号が（例えば、値「１」に）設定されていない場合、方法は、そのシーケンス番号を有するパケットが受信されていないと決定し、ステップ５２２へ進み得る。ステップ５２２で、方法は、当該シーケンス番号に関連付けられたパケットが受信されていることを示すように、アンチリプレイビットマップを（例えば、対応する値を値「０」に設定することによって）更新し得る。次いで、方法５００は、ステップ５１４へ進み、パケットを処理し得る。
【００３７】
先に記載したように、受信側のサブＳＡの選択は、単一のＳＡの選択と同様のプロセスで行われよく、そのどちらも、ＳＰＩ及びＩＰアドレス情報に基づいてよい。シーケンス番号の処理への変更を除いて、他の態様は変更されずともよい。複数のサブトンネルの使用は、２つのエンティティ間の保護された通信チャネルに対して、ＩＰｓｅｃパケットの配信順序の乱れを生じさせ得る。対処法としては、受信エンティティが送信順序の維持を必要とする場合に、データパケットのＩＰｓｅｃヘッダ中のシーケンス番号を使用できる。アンチリプレイが有効になっている場合、すべてのサブトンネルは、受信エンティティで１つの共有アンチリプレイビットマップを使用してよい。アンチリプレイのチェックは、特定のサブＳＡの代わりに、ＳＡクラスタを対象として完了されてよい。
【００３８】
マルチパスソリューションが配信順序の乱れの問題をもたらすのであるが、この順序の乱れの問題は、単一のＳＡにも発生することがある。再順序付け（リオーダー）プロセスは、ＴＣＰリオーダー及び／又はＩＰリアセンブリと同様の手法で、特定のネットワークのトポロジーに基づいて、アグリゲートノード及び／又はエンドホスト（例えば、ホスト２４０及び／又はホスト２４１）において完了されてよい。
【００３９】
図６は、セキュリティゲートウェイ１１０、セキュリティゲートウェイ１１２、セキュ

リティゲートウェイ２１０、及び／若しくはセキュリティゲートウェイ２１２、ホスト１４０、ホスト１４１、ホスト２４０、及び／若しくはホスト２４１、並びに／又はルータ１２０、ルータ２２１、及び／若しくはルータ２２２を含み得るネットワーク要素（ＮＥ）６００の一実施形態を示す概略図である。当業者には、用語ＮＥに、ＮＥ ６００が一例に過ぎないデバイスの広い範囲が包含されることが認識されよう。ＮＥ ６００は、説明の明確化を目的として記載されるのであって、本開示の用途を特定のＮＥの実施形態又は実施形態のクラスに限定することを意味しない。本明細書に記載される特徴／方法のうちの少なくともいくつか、例えば、ＳＡクラスタを作成するための方法３００、サブフローのためのサブＳＡを選択するための方法４００、及び／又はＳＡクラスタからデータを受信するための方法５００は、ＮＥ ６００などのネットワーク装置又は構成要素の全体又は一部分として実装されてよい。例えば、本開示の特徴／方法は、ハードウェア、ファームウェア、及び／又はハードウェア上で動作するようインストールされたソフトウェアを使用して実施されてよい。ＮＥ ６００は、ネットワークを介してフレームを搬送する任意の装置、例えば、スイッチ、ルータ、ブリッジ、サーバ、クライアント等であってよい。図６に示すように、ＮＥ ６００は、送信機、受信機、又はそれらの組合せであり得るトランシーバ（Ｔｘ／Ｒｘ）６１０を含んでよい。Ｔｘ／Ｒｘ ６１０は、他のノードからのフレームを送信及び／又は受信するための複数のダウンストリームポート６２０に接続されてよく、かつＴｘ／Ｒｘ ６１０は、他のノードからのフレームを送信及び／又は受信するための複数のアップストリームポート６５０に接続されてよい。プロセッサ６３０は、フレームを処理するために及び／又はフレームを送信するノードを決定するために、Ｔｘ／Ｒｘ ６１０に接続されてよい。プロセッサ６３０は、１つ又は複数のマルチコアプロセッサ、及び／又は、データ格納部、バッファ等として機能し得るメモリデバイス６３２を含んでよい。プロセッサ６３０は、汎用プロセッサとして実装されてよく、あるいは、１つ以上の特定用途向け集積回路（Application Specific Integrated Circuit, ＡＳＩＣ）及び／又はデジタル信号プロセッサ（Digital Signal Processor, ＤＳＰ）の一部分であってもよい。ダウンストリームポート６２０及び／又はアップストリームポート６５０は、電気的な及び／又は光学的な送信及び／又は受信コンポーネントを含んでよい。ＮＥ ６００は、ルーティング決定を行うルーティングコンポーネントであってよく、又はなくてもよい。

【００４０】

ＮＥ ６００に実行可能な命令をプログラム及び／又はロードすることによって、プロセッサ６３０、ダウンストリームポート６２０、Ｔｘ／Ｒｘ ６１０、メモリ６３２、及び／又はアップストリームポート６５０のうちの少なくとも１つが変更され、本開示によって示唆される新規な機能を含む特定の機械又は装置、例えば、マルチコア転送アーキテクチャへとＮＥ ６００を部分的に変更するということに留意されたい。実行可能なソフトウェアをコンピュータにロードすることによって実施可能な機能性が既知の設計ルールによってハードウェア実施形態に変換可能であることは、電気工学及びソフトウェア工学の分野における基本的事項である。典型的に、ソフトウェアとして実装するか、ハードウェアとして実装するかの決定は、ソフトウェア領域からハードウェア領域への変換によって生じる何らかの問題というよりは、生産されるユニットの設計の安定性及び数量を考慮してなされる。一般に、ハードウェア実装の変更はソフトウェア設計の変更よりも高額となるので、頻繁に変更される設計は、ソフトウェアとして実装されることが好ましい。一般に、大規模生産に対しては、ハードウェア実装がソフトウェア実装よりも安価となり得るので、大量に生産されることが決まっている設計は、ハードウェア、例えば、ＡＳＩＣとして実装されることが好ましい。多くの場合、設計は、ソフトウェア形態で開発され、テストされた後に、既知の設計ルールによって、ソフトウェアの命令を配線回路（hardwire）として備える、特定用途向け集積回路の均等な配線回路実装へと変換される。新たなＡＳＩＣによってコントロールされる機械が特定の機械又は装置であることと同様に、実行可能な命令をプログラム及び／又はロードされたコンピュータもまた、特定の機械又は装置とみなされ得る。

【００４１】
少なくとも１つの実施形態が開示され、当技術分野で通常の知識を有する者によってなされる（複数の）実施形態の変形、組合せ、及び／若しくは修正、並びに／又は（複数の）実施形態の特徴は、本開示の範囲内にある。（複数の）実施形態の特徴の組合せ、統合、及び／又は省略の結果である変形形態もまた、本開示の範囲内にある。数値の範囲又は限定が明確に示されている場合、そのような明示的な範囲又は限定は、明確に示された範囲又は限定内に納まる大きさの反復的範囲又は限定を含む（例えば、約１から約１０は、２，３，４等を含み、０．１０を超えることは、０．１１，０．１２，０．１３等を含む）ものと理解されたい。例えば、下限Ｒ１、上限Ｒ２の数値範囲が開示されている場合、厳密に言えば、その範囲内に納まるあらゆる数値が開示されている。より詳細には、Ｒ＝Ｒ１＋ｋ＊（Ｒｕ－Ｒ１）の範囲内の数が明確に開示される。ここで、ｋは、１パーセント刻みで、１パーセントから１００パーセントの範囲内にある変数であり、すなわち、ｋは、１パーセント、２パーセント、３パーセント、４パーセント、５パーセント、…、７０パーセント、７１パーセント、７２パーセント、…、９５パーセント、９６パーセント、９７パーセント、９８パーセント、９９パーセント、又は１００パーセントである。さらに、先に記載したように２つの数Ｒによって定義される任意の数値範囲もまた、明確に開示される。「約」という語の使用は、特に明記されない限り、後に続く数の±１０％を意味する。請求項中の任意の要素に対する「選択的に（optionally）」という語の使用は、その要素が必要とされること又はその要素が必要とされないことを意味し、その両方の選択肢が特許請求の範囲内にある。具備する、含む、及び有する（comprise, include, and having）といったより広い語の使用は、からなる（consisting of）、本質的に含む（consisting essentially of）、及び実質的に含む（comprised substantially of）といったより狭い語を包含するものと理解されたい。したがって、保護の範囲は、先に記載された内容によって限定されるのではなく、添付の特許請求の範囲によって規定されるのであって、特許請求の範囲の主題のすべての均等物を含む。各々の及びすべての請求項は、本明細書へのさらなる開示として援用され、かつ特許請求の範囲は、本開示の（複数の）実施形態でもある。開示中の参考文献についての記載は、それが従来技術であること、特に、本出願の優先日後の発行日を有する任意の参考文献であることを認めるものではない。本開示において引用したすべての特許、特許出願、及び刊行物の開示は、それらが本開示への例示的な、手続き的な、又はその他詳細な補足を提供するものであるとして、引用によって本開示に援用される。
【００４２】
本開示にはいくつかの実施形態が提供されているが、開示されたシステム及び方法は、本開示の精神又は範囲から逸脱することなく、他の多くの特定の形態で実施され得ることが理解されよう。本実施例は、例示のみを意図し、限定を意図せず、その意図は、明細書中で与えられた詳細に限定されるものではない。例えば、さまざまな要素又は構成要素は、別のシステムにおいては、組み合わされるか又は一体化されてよく、又は、ある特徴は、省略されるか又は実装されなくてよい。
【００４３】
さらに、個別に又は区別されてさまざまな実施形態として記載及び例示された、技術、システム、及び方法は、本開示の範囲から逸脱することなく、他のシステム、モジュール、技術、又は方法と組み合わせられるか又は統合されてよい。互いに接続されるか、直接接続されるか、又は通信を行うように示されるか又は説明された他の要素は、電気的、機械的、又はそれ以外であろうとなかろうと、何らかのインターフェース、デバイス、又は中間構成要素を介して、間接的に接続されるか又は通信を行ってよい。変更、代用、及び置換の他の例は、当業者によって確認可能であり、本明細書に開示される精神及び範囲から逸脱することなく行われてよい。
【符号の説明】
【００４４】
１００　ＩＰｓｅｃセキュリティアーキテクチャ

１１０，１１２，２１０，２１２　セキュリティゲートウェイ
１２０，２２１，２２２　ルータ
１３０　ネットワーク
１４１，１４２　単方向性セキュリティアソシエーション
１４３，１４４，２４３，２４４　保護された接続
１５０，１５１，２５０，２５１　ホスト
２４１，２４２　セキュリティアソシエーションクラスタ
２４１ａ，２４１ｂ，２４２ａ，２４２ｂ　パラレルサブセキュリティアソシエーション
６００　ネットワーク要素
６１０　トランシーバ
６２０　ダウンストリームポート
６３０　プロセッサ
６３２　メモリ
６５０　アップストリームポート

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/034415

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

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)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KENT BBN CORP R ATKINSON @HOME NETWORK S: "Security Architecture for the Internet Protocol; rfc2401.txt", 19981101, 1 November 1998 (1998-11-01), XP015008185, ISSN: 0000-0003 cited in the application page 8 - page 29 -----	1-23

☐ 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
31 May 2013	10/06/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Raposo Pires, João

Form PCT/ISA/210 (second sheet) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC

(72)発明者 ジフェイ・ソン
アメリカ合衆国・カリフォルニア・９５１３１・サン・ノゼ・イーグル・ポイント・ランディング・１２９１
(72)発明者 シャオヨン・イ
アメリカ合衆国・カリフォルニア・９４５３９・フリーモント・コリエア・コート・４１０８４
(72)発明者 シャンヤン・ジャン
アメリカ合衆国・カリフォルニア・９５１２９・サン・ノゼ・ジョンソン・アヴェニュー・１１９８

Ｆターム(参考) 5J104 AA03 EA13 PA07