

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号
特開2006-352500
(P2006-352500A)

(43) 公開日 平成18年12月28日(2006.12.28)

(51) Int.Cl.
H04L 9/36 (2006.01)

F I
H04L 9/00 685

テーマコード (参考)
5 J 1 0 4

審査請求 未請求 請求項の数 17 O L (全 33 頁)

(21) 出願番号	特願2005-175880 (P2005-175880)	(71) 出願人	000005821
(22) 出願日	平成17年6月16日 (2005.6.16)		松下電器産業株式会社
			大阪府門真市大字門真1006番地
		(74) 代理人	100094145
			弁理士 小野 由己男
		(74) 代理人	100106367
			弁理士 稲積 朋子
		(74) 代理人	100121120
			弁理士 渡辺 尚
		(74) 代理人	100130340
			弁理士 木村 健二
		(72) 発明者	大須賀 恭輔
			大阪府門真市大字門真1006番地 松下電器産業株式会社内

最終頁に続く

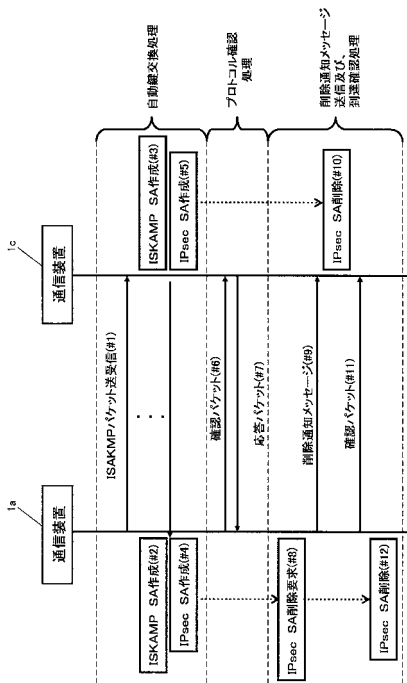
(54) 【発明の名称】 自動鍵交換処理装置および自動鍵交換処理方法

(57) 【要約】

【課題】 自動鍵交換処理によって確立されたIPsec SAの不一致発生の防止。

【解決手段】 IPsec SAに対する削除通知メッセージを送信後、相手側通信装置が削除対象のIPsec SA情報の削除を実施したかを確認する。すなわち、該当IPsec SAを利用した“確認パケット”を送信し、相手側通信装置の応答を確認する（到達確認処理）。相手側通信装置からの応答パケットが返ってきた場合、IPsec SAが削除されていないことがわかるので、再度削除通知メッセージ及び“確認パケット”を送信することにより、相手側通信装置の状況を確認する。

【選択図】 図2



【特許請求の範囲】

【請求項 1】

I P s e c (I Pセキュリティプロトコル) 及び I K E (Internet Key Exchange) に基づいて I S A K M P S A (Internet Security Association and Key Management Protocol) 及び I P s e c S A (Security Association) を確立し、暗号通信を行う通信装置であって、

前記暗号通信の相手である相手通信装置の識別子と、その相手通信装置との間で確立している I P s e c S A に関する情報と、その I P s e c S A の確立に用いた I S A K M P S A の識別子と、を記憶する管理手段と、

前記管理手段で記憶されている I P s e c S A 情報に対する削除通知メッセージを作成し、前記削除通知メッセージを前記相手通信装置に送信する削除通知メッセージ送信手段と、

前記削除通知メッセージの送信を、所定の終了条件が満たされるまで繰り返す終了条件判定手段と、

を備えることを特徴とする通信装置。

【請求項 2】

前記管理手段で記憶されている I P s e c S A 情報は、I P s e c S A の有効期限を含んでおり、

前記終了条件判定手段は、前記 I P s e c S A の有効期限が過ぎた場合、終了条件が満たされたと判断することを特徴とする、請求項 1 に記載の通信装置。

【請求項 3】

前記削除通知メッセージの削除対象である I P s e c S A 情報を用いたパケットを、前記削除通知メッセージを送信後の所定時間以内に受信したか否かを判断するパケット受信判定手段をさらに備え、

前記終了条件判定手段は、前記パケット受信判定手段の判断に基づいて前記終了条件が満たされたか否かを判断することを特徴とする、請求項 1 に記載の通信装置。

【請求項 4】

前記相手通信装置に削除通知メッセージが到達したか否かを判断する確認手段をさらに備えることを特徴とする、請求項 1 に記載の通信装置。

【請求項 5】

前記終了条件判定手段は、前記確認手段の判断に基づいて前記終了条件が満たされたか否かを判断することを特徴とする、請求項 4 に記載の通信装置。

【請求項 6】

所定の終了条件が満たされるまで前記削除通知メッセージを送信しても、前記相手通信装置に前記削除通知メッセージが到達していないと前記確認手段が判断した場合、前記終了条件判定手段は、前記相手通信装置が前記削除対象の I P s e c S A 情報を削除していない旨を、ユーザに通知することを特徴とする、請求項 4 に記載の通信装置。

【請求項 7】

前記確認手段は、

送信したパケットに対する応答パケットの一部もしくは全てが規定されている確認用プロトコルと、前記削除対象の I P s e c S A 情報と、を用いて確認パケットを作成し、前記確認パケットを送信する確認パケット送信手段と、

受信したパケットが前記削除対象の I P s e c S A 情報を用いている、かつ前記確認パケットに対する応答パケットであるか否かを判断する応答パケット判定手段と、を有しており、

前記確認手段は、前記応答パケット判定手段の判断結果に基づいて、前記削除通知メッセージが前記相手通信装置に到達しているか否かを判断することを特徴とする、請求項 4 に記載の通信装置。

【請求項 8】

前記確認パケット送信手段は、前記削除対象の I P s e c S A 情報を用いて暗号化さ

れたデータを含む確認パケットを送信し、

前記応答パケット判定手段は、前記削除対象の I P s e c S A 情報を用いて前記応答パケット中のデータを復号化可能か否かを判断し、

前記確認手段は、前記応答パケット判定手段が復号化可能と判断した場合、前記削除通知メッセージが前記相手通信装置に到達していないと判断することを特徴とする、請求項 7 に記載の通信装置。

【請求項 9】

前記 I P s e c S A 情報には、I P s e c S A を識別する I P s e c S A 識別子が含まれており、

前記応答パケット判定手段は、前記削除対象の I P s e c S A 識別子に基づいて、前記確認データに対する応答パケットであるか否かを判断することを特徴とする、請求項 7 に記載の通信装置。 10

【請求項 10】

前記管理手段は、I P s e c S A 情報と、前記相手通信装置との間で使用可能な確認用プロトコルに関する情報と、を対応づけてさらに記憶し、

前記確認パケット送信手段は、前記削除通知メッセージの 1 回目の送信に先立って 1 回目の確認パケットを前記相手通信装置に送信し、

前記確認手段は、前記 1 回目の確認パケットに関する応答パケット判定手段の判断結果に基づいて、前記管理手段に記憶されている確認用プロトコルに関する情報を更新する状況確認手段をさらに有することを特徴とする、請求項 7 に記載の通信装置。 20

【請求項 11】

前記確認用プロトコルは、T C P であることを特徴とする、請求項 7 に記載の通信装置。

【請求項 12】

前記管理手段は、I P s e c S A の有効期限を前記 I P s e c S A 情報と対応づけてさらに記憶し、

前記確認パケット送信手段は、前記確認パケットを繰り返し送信し、

前記確認手段は、前記 I P s e c S A の有効期限が満了すると、前記確認パケット送信手段による確認パケットの送信を停止させることを特徴とする、請求項 7 に記載の通信装置。 30

【請求項 13】

前記確認パケット送信手段は、前記確認パケットを繰り返し送信し、前記相手通信装置から自動鍵交換処理の開始を意図する I S A K M P パケットを受信した場合、前記確認パケットの送信を停止することを特徴とする、請求項 7 に記載の通信装置。

【請求項 14】

前記確認パケット送信手段は、確認パケットの作成において、パケットの送信元アドレスを前記自通信装置に設定されているアドレスとは異なるアドレスに書き換えることを特徴とする請求項 7 に記載の通信装置。

【請求項 15】

ネットワークで接続された請求項 1 に記載の通信装置を複数含むことを特徴とする通信システム。 40

【請求項 16】

I P s e c (I P セキュリティプロトコル) 及び I K E (Internet Key Exchange) に基づいて I S A K M P S A (Internet Security Association and Key Management Protocol) 及び I P s e c S A (Security Association) を確立し、暗号通信を行う通信方法であって、

前記暗号通信の相手である相手通信装置の識別子と、その相手通信装置との間で確立している I P s e c S A に関する情報と、その I P s e c S A の確立に用いた I S A K M P S A の識別子と、を記憶する管理ステップと、

前記ステップで記憶されている I P s e c S A 情報に対する削除通知メッセージを作 50

成し、前記削除通知メッセージを前記相手通信装置に送信する削除通知メッセージ送信ステップと、

前記削除通知メッセージの送信を、所定の終了条件が満たされるまで繰り返す終了条件判定ステップと、

を備えることを特徴とする通信方法。

【請求項 17】

I P s e c (I Pセキュリティプロトコル) 及び I K E (Internet Key Exchange) に基づいて I S A K M P S A (Internet Security Association and Key Management Protocol) 及び I P s e c S A (Security Association) を確立し、暗号通信を行うコンピュータ端末が実行する通信プログラムであって、

10

前記暗号通信の相手である相手通信装置の識別子と、その相手通信装置との間で確立している I P s e c S A に関する情報と、その I P s e c S A の確立に用いた I S A K M P S A の識別子と、を記憶する管理手段、

前記管理手段で記憶されている I P s e c S A 情報に対する削除通知メッセージを作成し、前記削除通知メッセージを前記相手通信装置に送信する削除通知メッセージ送信手段、及び

前記削除通知メッセージの送信を、所定の終了条件が満たされるまで繰り返す終了条件判定手段、

として前記コンピュータ端末を機能させることを特徴とする通信プログラム。

【発明の詳細な説明】

20

【技術分野】

【0001】

本発明は、暗号通信システムに関する。さらに詳しくは、I Pセキュリティプロトコル (I P s e c) による暗号機能を内蔵した通信技術に関する。

【背景技術】

【0002】

R F C 2 4 0 1 ~ R F C 2 4 1 2 (R F C : R e q u e s t F o r C o m m e n t s) には、1) I P (I n t e r n e t P r o t o c o l) における暗号通信、2) I P パケットの認証を行うプロトコルである I Pセキュリティプロトコル (I P s e c) 、3) そのための情報を折衝する自動鍵交換 (I K E : I n t e r n e t K e y E x c h a n g e) が、規定されている。以下、特に断らない限り、暗号通信には、I P s e c の通信データに対する認証機能を含むこととする。

30

【0003】

I P s e c による暗号機能を内蔵した通信装置は、セキュリティアソシエーション (暗号通信路: S A) と呼ぶ論理的な通信路上で暗号通信を行う。セキュリティアソシエーションでは、暗号通信で用いられる鍵情報 (暗号鍵、認証鍵) や、適用する暗号アルゴリズム及び認証アルゴリズム情報などが管理される。特に、I P s e c による暗号通信で使用されるセキュリティアソシエーション (暗号通信路) を I P s e c S A と呼ぶ。

【0004】

暗号通信を行う 2 者間において、I P s e c S A を確立する方法としては、両者において手動で I P s e c S A の諸情報を設定する手動鍵設定方法がある。このほか、両者間で互いに暗号通信を行う正当な相手か否かを確認し、I P s e c S A の諸情報を 2 者間で折衝して決定し、確立する自動鍵交換 (I K E) 方法もある。

40

【0005】

I K E は特に、R F C 2 4 0 7 ~ R F C 2 4 0 9 で規定されている。I K E では、I P s e c S A を確立するために折衝を行うが、この折衝を行うための制御用通信路を I S A K M P S A と呼ぶ。この I S A K M P S A は、I P s e c S A を確立するためだけではなく、I P s e c S A の更新や、切断 (S A 情報の削除) を行うためにも使用される。I P s e c S A を切断するときには、削除通知メッセージを一方の通信装置から他方に送る。送信側は、削除通知メッセージを送信した後に、自端末内の S A 情報を削除

50

する。他方の通信装置は、削除通知メッセージを受信すると、メッセージに従ってSA情報を削除する。なお、ISAKMPは、Internet Security Association and Key Management Protocolの略であり、IKEの通信プロトコルを規定する名称である。

【非特許文献1】標準仕様書「RFC2407」、IETF、[平成16年11月29日検索]、インターネット<URL:http://www.ietf.org/rfc/rfc2407.txt>

【非特許文献2】標準仕様書「RFC2408」、IETF、[平成16年11月29日検索]、インターネット<URL:http://www.ietf.org/rfc/rfc2408.txt>

【非特許文献3】標準仕様書「RFC2409」、IETF、[平成16年11月29日検索]、インターネット<URL:http://www.ietf.org/rfc/rfc2409.txt>

【発明の開示】

【発明が解決しようとする課題】

【0006】

しかし、上記IKEプロトコルを用いたIPsecによる暗号通信では、アプリケーション（あるいはそのユーザ）によりIPsec SAを切断しようとしても、削除通知メッセージが相手の通信装置に到達しない場合がある。この場合、一定期間、両方の通信装置間で暗号通信が成立しなくなる問題がある。

【0007】

図22は、この問題の発生を示す説明図である。一方の通信装置Aで切断処理が行われると、この装置は保持しているSA情報を削除し、相手方の通信装置Bに削除通知メッセージを送信する。しかし、削除通知メッセージは、ネットワーク上で破棄される可能性がある。ここで、削除通知メッセージは、UDPプロトコルを使用したISAKMPメッセージの一つである。そのため、これがネットワーク上で破棄されたとしても、通信装置Bは削除通知メッセージを検知することができない。そのため、通信装置Bでは、該当するIPsec SA情報が存在したままとなる。なお、IPsec通信では、その通信方向毎にIPsec SAの情報を管理しており、IKEを用いた場合は、双方向通信を実現するIPsec SAを確立するため、各通信装置で管理されるIPsec SA情報としては入力用と出力用の計2つが存在する。しかし、図22では、双方向通信を前提とし、これらをまとめて一本のIPsec SAとして図示している。

【0008】

前述のような、片方の通信装置にのみIPsec SA情報があり、他方の通信装置にはその情報が存在しない状態を、IPsec SA不一致の状態という。この状態において、SA情報を保持している通信装置Bは、既に保持しているIPsec SAを用いて、該当パケットを暗号化して送信する。これに対し、他方の通信装置Aでは、該当するIPsec SAを既に削除しているため、受信したパケットを廃棄し、暗号通信が成立しない。

【0009】

この暗号通信不能の状態からの復帰は、次の方法で行うことができる。第1の方法は、不一致が発生しているIPsec SAの寿命が尽きるのを待って、再度IPsec SAを確立する方法である。第2の方法は、アプリケーションまたはそのユーザが、所定期間待って暗号通信が成立しないことを確認した後、保持しているIPsec SAを明示的に削除することによって、再度IPsec SAを確立する方法である。しかし、いずれにしても、一方の通信装置において、IPsec SAの切断処理を行ってから、再度IPsec SAの確立を開始できるまでに時間を要してしまう。

【0010】

以上のように、アプリケーションまたはそのユーザによるIPsec SAの明示的な切断では、一方の通信装置から送信する削除通知メッセージが、相手側通信装置に到達し

10

20

30

40

50

ないことにより、IPsec SA不一致の状態が発生し、一定時間暗号通信が成立しなくなる。また、暗号通信の復帰までに時間を要する。

【0011】

そこで、本発明は、上述したIKEにおける削除通知メッセージをサポートする通信装置間において、IPsec SA不一致の状態の発生を防止する技術を提供することを目的とする。

【課題を解決するための手段】

【0012】

前記課題を解決するために、発明1は、IPsec (IPセキュリティプロトコル) 及びIKE (Internet Key Exchange)に基づいてISAKMP SA (Internet Security Association and Key Management Protocol) 及びIPsec SA (Security Association) を確立し、暗号通信を行う通信装置を提供する。この通信装置は、以下の手段を備えている。

- ・前記暗号通信の相手である相手通信装置の識別子と、その相手通信装置との間で確立しているIPsec SAに関する情報と、そのIPsec SAの確立に用いたISAKMP SAの識別子と、を記憶する管理手段、
- ・前記管理手段で記憶されているIPsec SA情報に対する削除通知メッセージを作成し、前記削除通知メッセージを前記相手通信装置に送信する削除通知メッセージ送信手段、
- ・前記削除通知メッセージの送信を、所定の終了条件が満たされるまで繰り返す終了条件判定手段。

【0013】

アプリケーションやそのユーザによりIPsec SAを切断する場合に、削除通知メッセージを複数回送信するため、削除通知メッセージが相手に到達しない可能性を低減することができる。従って、通信装置間でのIPsec SA不一致の状態の発生を防止することができる。

【0014】

発明2は、前記発明1において、前記管理手段で記憶されているIPsec SA情報は、IPsec SAの有効期限を含んでいる通信装置を提供する。この装置において、前記終了条件判定手段は、前記IPsec SAの有効期限が過ぎた場合、終了条件が満たされたと判断する。

【0015】

IPsec SAの寿命が切れるとき、通信中の相手側通信装置において同じタイミングで寿命切れによるIPsec SAの削除が発生する。そのため、削除通知メッセージ送信の終了条件をIPsec SAの寿命切れとすることにより、削除通知メッセージの送信を終了することができ、かつIPsec SA不一致の状態の発生を免れるという効果が得られる。

【0016】

発明3は、前記発明1において、前記削除通知メッセージの削除対象であるIPsec SA情報を用いたパケットを、前記削除通知メッセージを送信後の所定時間以内に受信したか否かを判断するパケット受信判定手段をさらに備える通信装置を提供する。この通信装置において、前記終了条件判定手段は、前記パケット受信判定手段の判断に基づいて前記終了条件が満たされたか否かを判断する。

【0017】

終了条件判定手段は、削除通知メッセージを送信後の一定期間の間に、削除しようとしているIPsec SAを用いたIPsecパケットを受信しない場合、終了条件が満たされたと判断する。これにより、相手側通信装置が削除通知メッセージに応じて該当IPsec SA情報を削除済みの場合、必要以上に削除通知メッセージを再送せずに済み、通信装置やネットワークの負荷を軽減することができる。

【0018】

発明 4 は、前記発明 1 において、前記相手通信装置に削除通知メッセージが到達したか否かを判断する確認手段をさらに備える通信装置を提供する。

【0019】

削除通知メッセージが相手側通信装置に到達したか否かを判断することにより、相手側通信装置が該当 I P s e c S A 情報を削除しているか否かを確認することができる。そのため、終了条件が「所定回数及び／または所定期間、削除通知メッセージを送信する」である場合、終了条件を満足しても、削除通知メッセージが相手側通信装置に到達したのか、それとも到達しなかったのか、を把握することができる。

【0020】

発明 5 は、発明 4 において、前記終了条件判定手段は、前記確認手段の判断に基づいて 10 前記終了条件が満たされたか否かを判断する通信装置を提供する。

【0021】

「削除通知メッセージの相手側への到達」を終了条件にすれば、無駄な削除通知メッセージを送信しなくて済み、通信装置やネットワークの負荷を軽減することができる。

【0022】

発明 6 は、前記発明 4 において、所定の終了条件が満たされるまで前記削除通知メッセージを送信しても、前記相手通信装置に前記削除通知メッセージが到達していないと前記確認手段が判断した場合、前記終了条件判定手段は、前記相手通信装置が前記削除対象の I P s e c S A 情報を削除していない旨を、ユーザに通知する通信装置を提供する。

【0023】

削除通知メッセージを終了条件が満たされるまで再送した結果、その削除通知メッセージが相手側通信装置に到達しなかったことをユーザに通知することにより、I P s e c S A 不一致の状態を解消するために、そのユーザが何らかの措置をとることができる。例えば、そのユーザは、別の通信手段により、相手側通信装置のユーザに対し、I P s e c S A 情報を削除することを要求してもよい。

【0024】

発明 7 は、前記発明 4 において、前記確認手段が以下の手段を有している通信装置を提供する。

- ・送信したパケットに対する応答パケットの一部もしくは全てが規定されている確認用プロトコルと、前記削除対象の I P s e c S A 情報と、を用いて確認パケットを作成し、 30 前記確認パケットを送信する確認パケット送信手段、
- ・受信したパケットが前記削除対象の I P s e c S A 情報を用いている、かつ前記確認パケットに対する応答パケットであるか否かを判断する応答パケット判定手段。

【0025】

この通信装置において、前記確認手段は、前記応答パケット判定手段の判断結果に基づいて、前記削除通知メッセージが前記相手通信装置に到達しているか否かを判断する。

【0026】

例えば、1) T C P の S Y N パケットに対する A C K パケット、2) U D P の t f t p (W R Q) パケットに対する t f t p (A C K) パケット、3) I C M P の E c h o R e q u e s t パケットに対する E c h o R e p l y を、確認パケットに対する応答パ 40 ケットの一例としてあげることができる。削除対象の I P s e c S A 情報を用いた確認パケットを送受信することにより、相手側通信装置が該当 I P s e c S A 情報を削除しているか否かを確認することができる。ひいては、通信装置は、削除通知メッセージの再送の可否を知ることができる。応答パケットが帰ってくるということは、相手側通信装置が削除対象の I P s e c S A 情報を削除していないことを示しているからである。

【0027】

発明 8 は、前記発明 7 において、前記確認パケット送信手段は、前記削除対象の I P s e c S A 情報を用いて暗号化されたデータを含む確認パケットを送信する通信装置を提供する。この通信装置において、前記応答パケット判定手段は、前記削除対象の I P s e c S A 情報を用いて前記応答パケット中のデータを復号化可能か否かを判断する。また 50

、前記確認手段は、前記応答パケット判定手段が復号化可能と判断した場合、前記削除通知メッセージが前記相手通信装置に到達していないと判断する。

【0028】

削除対象の I P s e c S A 情報を用いた暗号化・復号化が、通信相手との間で成立する場合、その I P s e c S A 情報は両方で削除されていないことを示す。従って、確認パケット中のデータ及び応答パケット中のデータを削除対象の I P s e c S A 情報で暗号化・復号化することにより、削除通知メッセージの再送の要否を知ることができる。

【0029】

発明 9 は、前記発明 7 において、前記 I P s e c S A 情報には、I P s e c S A を識別する I P s e c S A 識別子が含まれている通信装置を提供する。この通信装置において、前記応答パケット判定手段は、前記削除対象の I P s e c S A 識別子に基づいて、前記確認データに対する応答パケットであるか否かを判断する。 10

【0030】

送信した確認データを含むパケットに受信した I P s e c パケットの I P s e c S A の識別子を、応答パケットであるかを判定する情報として使用することにより、I P s e c S A の識別子のみを記憶しておけば、I P s e c S A の情報を削除することができるため、通信装置内のメモリを効率的に利用することができるという効果が得られる。

【0031】

発明 10 は、前記発明 7 において、前記管理手段は、I P s e c S A 情報と、前記相手通信装置との間で使用可能な確認用プロトコルに関する情報と、を対応づけてさらに記憶している通信装置を提供する。この通信装置において、前記確認パケット送信手段は、前記削除通知メッセージの 1 回目の送信に先立って 1 回目の確認パケットを前記相手通信装置に送信する。前記確認手段は、前記 1 回目の確認パケットに関する応答パケット判定手段の判断結果に基づいて、前記管理手段に記憶されている確認用プロトコルに関する情報を更新する状況確認手段をさらに有している。 20

【0032】

プロトコルに関する情報とは、プロトコルを特定できる情報であればよい。最初の削除通知メッセージを送信する前に、相手側通信装置との間で使用可能な確認用プロトコルを確認し、これを管理手段に登録しておく。これにより、削除通知メッセージ送信後の確認パケットに対する応答パケットの信憑性を高めることができる。言い換えれば、I P s e c S A 情報が相手側通信装置に残っている限り応答パケットが帰ってくるはずであり、応答パケットがない場合は I P s e c S A 情報が相手側通信装置で削除されているはずである、という状態を作り出すことができる。 30

【0033】

発明 11 は、前記発明 7 において、前記確認用プロトコルは T C P である通信装置を提供する。

【0034】

T C P を用いれば、相手側通信装置から送信される応答パケットが再送される。そのため、ネットワーク上で応答パケットが廃棄された結果、削除通知メッセージを送信した通信装置に応答パケットが到達しない、という現象の発生を抑制することができる。 40

【0035】

発明 12 は、前記発明 7 において、前記管理手段は、I P s e c S A の有効期限を前記 I P s e c S A 情報と対応づけてさらに記憶している通信装置を提供する。この通信装置において、前記確認パケット送信手段は、前記確認パケットを繰り返し送信する。前記確認手段は、前記 I P s e c S A の有効期限が満了すると、前記確認パケット送信手段による確認パケットの送信を停止させる。

【0036】

削除通知メッセージと同様に確認パケットを繰り返し送信することで、再送された削除通知メッセージの有効／無効を判断することができる。確認パケットの送信を I P s e c S A の寿命満了まで繰り返すことにより、相手側通信装置が確認用プロトコルに対応し 50

ていない場合でも、確認パケットの送信を永遠に繰り返さずに済む。

【0037】

発明13は、前記発明7において、前記確認パケット送信手段は、前記確認パケットを繰り返し送信し、前記相手通信装置から自動鍵交換処理の開始を意図するISAKMPパケットを受信した場合、前記確認パケットの送信を停止する通信装置を提供する。

【0038】

発明10と同様、確認パケットを繰り返し送信することで、再送された削除通知メッセージの有効／無効を判断することができる。新規IPsec SA確立のためのISAKMPパケットを受信するまで、確認パケットの送信を繰り返すことにより、相手側通信装置が確認用プロトコルに対応していない場合でも、確認パケットの送信を永遠に繰り返さずに済む。特に、対応するIPsec SAを保持していない場合に、自動鍵交換処理の開始を意図するISAKMPパケットを送信する実装に対して有用である。 10

【0039】

発明14は、発明7において、前記確認パケット送信手段は、確認パケットの作成において、パケットの送信元アドレスを前記自通信装置に設定されているアドレスとは異なるアドレスに書き換える通信装置を提供する。

【0040】

本通信装置がIP通信を中継する中継装置である場合、IP通信を開始した通信装置から送信されるパケットを、本通信装置において擬似的に作成する。これにより、トンネルモードのためのIPsec SA情報を削除する場合も、確認パケットを用いて、相手側通信装置におけるIPsec SA情報の有無を判断することができる。 20

【0041】

発明15は、ネットワークで接続された発明1に記載の通信装置を複数含む通信システムを提供する。

【0042】

この通信システムを構成する各通信装置は、前記発明1と同様の作用効果を奏する。

【0043】

発明16は、IPsec (IPセキュリティプロトコル) 及びIKE (Internet Key Exchange) に基づいてISAKMP SA (Internet Security Association and Key Management Protocol) 及びIPsec SA (Security Association) を確立し、暗号通信を行う通信方法を提供する。この方法は、以下のステップを含んでいる。 30

- ・前記暗号通信の相手である相手通信装置の識別子と、その相手通信装置との間で確立しているIPsec SAに関する情報と、そのIPsec SAの確立に用いたISAKMP SAの識別子と、を記憶する管理ステップ、
- ・前記ステップで記憶されているIPsec SA情報に対する削除通知メッセージを作成し、前記削除通知メッセージを前記相手通信装置に送信する削除通知メッセージ送信ステップ、
- ・前記削除通知メッセージの送信を、所定の終了条件が満たされるまで繰り返す終了条件判定ステップ。

【0044】

この方法は、前記発明1の通信装置が実行する方法であり、発明1と同様の作用効果を奏する。 40

【0045】

発明17は、IPsec (IPセキュリティプロトコル) 及びIKE (Internet Key Exchange) に基づいてISAKMP SA (Internet Security Association and Key Management Protocol) 及びIPsec SA (Security Association) を確立し、暗号通信を行うコンピュータ端末が実行する通信プログラムを提供する。この通信プログラムは、前記コンピュータ端末を、以下の手段として機能させる。

- ・前記暗号通信の相手である相手通信装置の識別子と、その相手通信装置との間で確立しているIPsec SAに関する情報と、そのIPsec SAの確立に用いたISAK 50

MP SAの識別子と、を記憶する管理手段、

- ・前記管理手段で記憶されているIPsec SA情報に対する削除通知メッセージを作成し、前記削除通知メッセージを前記相手通信装置に送信する削除通知メッセージ送信手段、
- ・前記削除通知メッセージの送信を、所定の終了条件が満たされるまで繰り返す終了条件判定手。

【0046】

この方法は、前記発明1の通信装置が実行するプログラムであり、発明1と同様の作用効果を奏する。なお、このプログラムを記録したコンピュータ読み取り可能な記録媒体も、本発明の範囲に含まれる。ここで記録媒体としては、コンピュータが読み書き可能なフレキシブルディスク、ハードディスク、半導体メモリ、CD-ROM、DVD、光磁気ディスク(MO)、その他のものが挙げられる。

10

【発明の効果】

【0047】

本発明を用いれば、アプリケーションやそのユーザによりIPsec SAを切断する場合に、削除通知メッセージを複数回送信するため、削除通知メッセージが相手に到達しない可能性が低減する。また、削除通知メッセージが通信相手に到達したか否かの確認を行う。従って、通信装置間でのIPsec SA不一致の状態の発生を防止することができる。

【発明を実施するための最良の形態】

20

【0048】

<第1実施形態>

〔通信システムの構成〕

図1は、本発明の通信装置を用いた通信システムの構成例を示す説明図である。この通信システムは、複数の通信装置1a～1fが、通信ネットワーク2で接続されて構成されている。通信装置1e、fは、他の通信装置1a、b、c、d間の通信を中継するルータである。以下、通信装置1e、fを他の通信装置1a～dと区別する場合、ルータ1e、fという。暗号通信を行う形態には、トランスポートモード及びトンネルモードの2つがある。トランスポートモードは、2者間で暗号通信路(IPsec SA)を確立して暗号通信を行う形態である。例えば、通信装置1a、c間で通信を行う場合、通信装置1a、cの2者でIPsec SAを確立して暗号通信を行う。一方、トンネルモードは、主にパケットを中継する機器間でIPsec SAを確立して、暗号通信を行う。例えば、通信装置1a、c間で通信を行う場合に、ルータ1e、fの2者間でIPsec SAを確立し、両者間を経由する通信を両ルータ1e、f間で暗号化する。なお、ルータ1e、fにおいて暗号通信を行う条件次第では、ルータ1e、f間が中継する通信であっても、暗号通信を行わない場合もある。以後、単に通信装置1というときには、IPsec SAを確立することのできるルータ1e、f及び通信装置1a～dを含む。

30

【0049】

〔削除通知メッセージ〕

次に、IKEを用いた場合のIPsec SAの切断に用いられる削除通知メッセージについて説明する。

40

【0050】

IKEでは、ISAKMP SAの確立及びIPsec SAの確立に、ISAKMP メッセージと呼ばれるメッセージフォーマットを用いたIPパケットの通信を行う。ISAKMP SAの確立には、例えばメインモードと呼ばれる折衝手順(トランザクション)があり、IPsec SAの確立には、例えばクイックモードと呼ばれる折衝手順がある。ISAKMP SAは、IPsec SAの確立・切断などに使用される制御用通信路である。

【0051】

ISAKMP SA及びIPsec SAが確立している状態において、IPsecに

50

よる暗号通信が可能となる。暗号通信は、主として通信する情報の機密性及び完全性を保証するために使用される。暗号化・復号化を行うためには、鍵を必要とする。この鍵が第三者に知れると、第三者は容易にその暗号化された情報を復号化することができる。このため、鍵の管理は重要である。また、鍵は、暗号化された多くの時間を費やせば類推可能であり、さらに、同じ鍵を用いて暗号化された多く情報を集めれば、それだけ類推が容易となる。このため、IKEでは、IPsec SAが不要となった場合に削除し、必要なときには、再度IPsec SAを確立するための仕組みが提供されている。

【0052】

その仕組みとして、ISAKMP SA及びIPsec SAの削除通知メッセージが、ISAKMPメッセージの一つとして規定されている。削除通知メッセージは、一方の通信装置におけるアプリケーションまたはユーザによる明示的なIPsec SAの切断時に、もう一方の通信装置に対し、IPsec SAの削除を通知するメッセージである。このメッセージは、削除ペイロード (Delete Payload) を含む通知メッセージ (Informational Exchange) として規定されている。このメッセージを受信した通信装置は、削除通知メッセージに該当するIPsec SAに関する情報を削除する。これにより、暗号通信を行っていた通信装置の両者において、不要となったIPsec SA情報を削除することができる。

【0053】

〔発明の概要〕

図2は、図1の通信装置が行う処理の概要を示す説明図である。図1の通信システムにおける通信装置は、前述の削除通知メッセージが相手側通信装置に届かずにIPsec SA不一致の状態が発生するのを防ぐために、以下の処理を行う。以下では、説明を容易にするために、図1の通信装置1a、1cが通信する場合の通信装置1aの処理を例にとるが、どの通信装置であっても処理は同様に行われる。

【0054】

通信装置の処理は、(i)プロトコル確認処理、(ii)削除通知メッセージ送信処理、(iii)到達確認処理、に大別される。このうち、削除通知メッセージ送信処理は本発明に必須の処理である。これらの処理を行うに先立ち、通信装置1は、RFCに規定された自動鍵交換処理を行い、ISAKMP SAを確立し(#1、#2、#3)、確立したISAKMP SAを用いてIPsec SAを確立する(#4、#5)。

【0055】

(i)プロトコル確認処理では、通信装置1aは、相手側通信装置1cが使用可能な通信プロトコルを確認する。双方に使用可能なプロトコルを用いて、後述する確認パケットを送信するためである。確認パケットとは、削除通知メッセージが相手側通信装置1cに到達しているか否かを確認するために送信するパケットである。具体的には、通信装置1aは、通信装置1cに対してある通信プロトコルを用いて“事前確認パケット”を送信し(#6)、それに対する応答パケットを受信した場合(#7)、通信装置1cはその通信プロトコルを使用可能と判断する。事前確認パケット及び応答パケットには、確立したIPsec SAが用いられる。これにより、通信装置1aは、IPsec SA及び所定の通信プロトコルを用いた“確認パケット”が使用可能であるか、を判断する。

【0056】

(ii)削除通知メッセージ送信処理では、通信装置1aにおいて、アプリケーションやユーザからのIPsec SA切断要求が発生した場合(#8)、削除通知メッセージを送信する(#9)。削除通知メッセージが通信装置1cに到達すれば、通信装置1cは削除対象のIPsec SA情報を、記憶領域から削除する(#10)。何らかの原因で削除通知メッセージが通信装置1cに到達しない場合、削除対象のIPsec SA情報は通信装置1cにそのまま残される。通信装置1aは、削除通知メッセージを終了条件が満たされるまで、繰り返し送信する。

【0057】

(iii)到達確認処理では、通信装置1aは、相手側通信装置1cがIPsec SAを

10

20

30

40

50

削除しているか否かを確認する。すなわち、削除通知メッセージ送信後、削除要求元の通信装置 1 a は、前記プロトコル確認処理で使用可能であることを確認した通信プロトコルを用い、“確認パケット”を送信する（＃11）。確認パケットに対する応答パケットがなければ、相手側通信装置 1 c が I P s e c S A 情報を削除したと判断し、自端末の I P s e c S A 情報を削除する（＃12）。ここでの“確認パケット”は、I P s e c パケットである。確認パケットは、所定の条件を満たすまで繰り返し送信される。

【0058】

以上の処理により、削除通知メッセージが相手側通信装置 1 c に到達したか否かを確認し、確認結果に応じて自端末の I P s e c S A 情報を削除する。そのため、削除通知メッセージが相手側通信装置 1 c に到達せず、その結果 I P s e c S A 情報が通信装置 1 a, 1 c 間で不一致の状態になることを防止できる。しかも、最初の削除通知メッセージ送信に先立ち、確認パケットを送信するためのプロトコルが使用可能か否かを確認することで、確認パケットに対する応答パケットの信頼度を高めることができる。

【0059】

〔通信装置の構成〕

（1）全体構成

図 3 は、図 1 に示す通信装置 1 の機能ブロック図である。前述したように、通信装置 1 は、I P s e c S A を確立することのできるルータ 1 e, f 及び通信装置 1 a ~ d を含む。通信装置 1 は、I K E 処理部 20 と、アプリケーション部 30 と、I P 処理部 40 と、通信部 50 と、を備えている。I P 処理部 40 は、I P s e c 処理部 60 を備えている。なお、アプリケーション部 30 は、図 3 において一つのみ図示しているが、複数であってもよい。このような機能を有する通信装置 10 は、C P U、R O M、R A M、ハードディスクなどを有するコンピュータにより実現される。C P U は、I K E 処理部 20、アプリケーション部 30、I P 処理部 40 及び通信部 50 として機能する。

【0060】

I K E 処理部 20 及び I P 処理部 40 には、相手通信装置との間で暗号通信を適用する条件が設定されている。この条件設定は、例えば、通信装置の初期設定としてなされてもよいし、アプリケーション部 30 からの設定としてなされてもよい。I K E 処理部 20 は、アプリケーション部 30 または I P 処理部 40 からの要求に従い、自動鍵交換処理を行なう。アプリケーション部 30 は、アプリケーションのアルゴリズムに応じた所定の通信処理を相手通信装置との間で行ない、関連する送受信処理を I P 処理部 40 に要求する。I P 処理部 40 は、I P パケットの送受信に係る処理を行なう。通信部 50 は、通信媒体に特有の送受信処理を行なう。

【0061】

上記構成を有する通信装置 10 は、次のように動作する。アプリケーション部 30 は、相手装置との通信を開始すると、相手装置に対して I P パケットの送信を試みる。I P 処理部 40 では、I P s e c 処理部 60 を必要に応じて使用し、該当 I P パケットが暗号通信の対象であるか否かを判定する。暗号通信の対象である場合は、I P 処理部 40 は I P s e c S A 情報の存在を確認し、存在していれば該当 I P パケットを暗号化して通信部 50 に送信要求を行なう。一方、I P s e c S A 情報が存在していない場合、I P 処理部 40 は、I K E 処理部 20 に対し、暗号化しようとする I P パケットの情報と共に、I P s e c S A の確立を要求する。I K E 処理部 20 は、受け取った I P s e c S A 確立要求に従い、予め設定された条件に適合した相手装置との間で自動鍵交換処理（I K E 折衝処理）を開始する。自動鍵交換処理におけるデータは、I P パケット上の U D P（U s e r D a t a g r a m P r o t o c o l）を使用して送受信される。このため、自動鍵交換処理におけるデータの送受信には、I P 処理部 40 が用いられる。

【0062】

なお、アプリケーション部 30 は、その通信に先立ち、予め I K E 処理部 20 に対し、相手側通信装置との間に I S A K M P S A、および I P s e c S A の確立を指示することもできる。

【0063】

(2) IKE 処理部

図4は、IKE処理部20の機能構成を示す説明図である。IKE処理部20は、要求受付部21と、SA管理部22（管理手段に相当）と、SA確立部23と、ISAKMPメッセージ処理部24（削除通知メッセージ送信手段に相当）と、確認プロセス管理部25（パケット受信判定手段、確認手段、確認パケット送信手段、応答パケット判定手段に相当）と、を含む。

【0064】

(2-1) 要求受付部

要求受付部21は、アプリケーション部30やIP処理部40からのIPsec SA 10 確立要求を受け付け、IKE折衝処理の開始をSA管理部22に指示する。また、要求受付部21は、相手通信装置との間で暗号通信を適用する条件の設定をSA管理部22に指示する。IKE折衝処理には、ISAKMP SAの確立・切断や、IPsec SAの確立・切断が含まれる。

【0065】

(2-2) SA管理部

SA管理部22は、ISAKMP SA及びIPsec SA（以下、まとめてSAと 20 いうことがある）の確立・切断・更新を管理する。SAの管理のために、SA管理部22は管理テーブル22aを保持している。管理テーブル22aは、各ISAKMP SA及びIPsec SAに関する情報（以下、SA情報という）を記憶している。SA情報は、SAの確立・切断・更新に従い、登録・削除・更新される。また、SA管理部22は、ISAKMP SAが全くなかった場合または全くなくなるに先立ち、新たなISAKMP SAをSA確立部23に再度、確立要求することができる。

【0066】

図5は、SA管理部22が保持する管理テーブル22aに蓄積されるSA情報の概念説明図である。管理テーブル22aは、「ISAKMP SA ID」、「IPsec終端 30 点」の通信装置の識別子及び「SPI」を少なくとも1レコードに含む。「ISAKMP SA ID」は、通信装置内に管理するISAKMP SAの識別子であり、Initiator Cookie、もしくは、Responder Cookieなどを用いる。通信装置の識別子としては、この例ではIPアドレスを用いているが、その他の通信アドレスやMACアドレス等の装置固有情報を用いることもできる。「SPI (Security Parameter Index)」は、IPsec SAの識別子である。ISAKMP SA ID及びSPIは、異なる相手通信装置に対してであれば、同じ値を取ることもあり得る。

【0067】

前述の情報に加え、この例では、「IPsec SAの状態」、「確認用プロトコル」及び「IPsec SAの有効期限」が、1レコード中にさらに含まれる。本実施形態では、IPsec SAの状態として、「使用可能」と、「使用不可」の二つの状態を管理している。「使用可能」の状態は、IPsec SA確立後の正常な状態であり、アプリケーション処理部30から要求される通信においてIPsec SAを使用可能であること 40 を示す。一方、「使用不可」の状態は、ユーザまたはアプリケーションからIPsec SAの削除要求を受けた場合に遷移する状態であり、アプリケーション処理部30から要求される通信においてIPsec SAを使用できないことを示す。なお、SAの状態として、「使用可能」及び「使用不可」を含んでいれば、他の状態を含んでいてもよい。また、本実施の形態では、ISAKMP SAとIPsec SAが1対1で管理されているが、ISAKMP SA1つに対し、複数のIPsec SAが対応づけられている可能性もあるため、異なるレコードにおいて、ISAKMP SA IDが同じものが存在してもよい。

【0068】

「確認用プロトコル」をIPsec SA毎に管理することで、各IPsec SA毎 50

に確認パケットを送信するプロトコルを制御可能になる。プロトコル確認処理は、IPsec SAが確立している状態において実施する。「IPsec SAの有効期限」を管理することで、IPsec SAの寿命が尽きた時点を契機として、そのIPsec SAの削除通知メッセージやその確認パケットを送信することが可能となる。

【0069】

この他に、各IPsec SA毎に、暗号アルゴリズム、暗号用鍵、認証アルゴリズム、認証用鍵など他の情報を管理していても構わない。

【0070】

(2-3) SA確立部

SA確立部23は、SA管理部22からの要求に従ってSA確立のためのIKE折衝処理を行ない、ISAKMPメッセージ処理部24に対して対応するISAKMPメッセージの構築処理を要求する。また、SA管理部22は、相手通信装置からIKE折衝処理要求を受け取り、IKE折衝処理を行い、SA管理部22に対してSA情報の更新要求を行なう。SA確立及びIKE折衝処理そのものについては、RFCに規定されており、本発明はその範囲を逸脱しないので、説明は省略する。

【0071】

(2-4) ISAKMPメッセージ処理部

ISAKMPメッセージ処理部24は、SA確立部23からの要求及びSA管理部22からの要求に対して該当するISAKMPメッセージの構築を行ない、IP処理部40に構築したメッセージを送信依頼する。また、ISAKMPメッセージ処理部24は、IP処理部40から受信したISAKMPメッセージをRFCの規定に従って解析する。受信したISAKMPメッセージが相手通信装置からのIKE折衝処理要求である場合は、SA確立部23にその処理を指示する。ISAKMPメッセージが削除通知であった場合、ISAKMPメッセージ処理部24はその削除通知に含まれる削除ペイロードを抽出し、SA管理部22にその処理を指示する。なお、ISAKMPメッセージ処理部24は、ISAKMPメッセージの送受信の際に、RFC2407～RFC2409で規定されている所定の暗号化・復号化、認証情報の付加・認証情報の認証などを行なう。

【0072】

(2-5) 確認プロセス管理部

確認プロセス管理部25は、SA管理部22からの削除通知メッセージ送信要求を受け付け、削除通知メッセージの送信前及び後に、“事前確認パケット”や“確認パケット”の送信をIP処理部40に要求する。また、確認プロセス管理部25は、ISAKMPメッセージ処理部24に対し、削除通知メッセージ送信要求を行う。確認プロセス管理部25は、前記到達確認処理において、IP処理部40に対し、IPsec SAを適用する条件の問い合わせを行う。確認プロセス管理部25は、確認パケット送信及び応答パケット受信のために、IPsec処理部60に対し、IPsec暗号化・復号化処理及び認証処理を要求する。さらに、確認プロセス管理部25は、到達確認処理終了後、IPsec SA情報の更新または削除を、IP処理部40に要求する。確認プロセス管理部25の構成については、詳細を後述する。

【0073】

〔確認プロセス管理部〕

(1) 全体構成

図6は、確認プロセス管理部25の機能構成を示すブロック図である。確認プロセス管理部25は、確認プロセス実行部251（終了条件判定手段、確認手段及び状況確認手段に相当）、プロトコル記憶部252、確認パケット送信部253及びパケット受信判定部254（パケット受信判定手段に相当）を有している。

【0074】

確認プロセス実行部251は、SA管理部22から削除通知メッセージ送信要求を受信し、削除通知メッセージの送信及び到達確認処理を行う。具体的には、確認プロセス実行部251は、確認パケット送信部253へ“事前確認パケット”及び“確認パケット”の

10

20

30

40

50

送信を要求し、パケット受信判定部 254 に“応答パケット”の受信要求を行い、パケット受信判定結果を取得する。確認プロセス実行部 251 については、詳細を後述する。

【0075】

プロトコル記憶部 252 は、通信装置自身が使用可能な通信プロトコルと、通信相手の応答の仕方と、を記憶している。

【0076】

確認パケット送信部 253 は、確認プロセス実行部 251 から事前確認パケット及び確認パケットの送信要求を受け、暗号認証処理を I P s e c 処理部 60 に要求し、パケットの送信を I P 処理部 40 に要求する。

【0077】

パケット受信判定部 254 は、I P 処理部 40 から受信パケットを取得し、そのパケットがどのようなパケットであるかを判定し、判定結果を確認プロセス実行部 251 へ渡す。パケット受信判定部 254 については、詳細を後述する。

【0078】

(2) プロトコル記憶部

図 7 は、プロトコル記憶部 252 に記憶される情報の概念説明図である。プロトコル記憶部 252 には、通信装置自身が使用可能なプロトコルと、送信パケットと、応答パケットと、が対応づけられて記憶されている。例えば、プロトコルとして T C P を用いる場合、S Y N パケットに対しては、A C K パケットまたは R S T パケットが応答パケットである。S Y N パケットとは、R F C 7 9 3 に規定されているコードビットの S Y N フラグを立てた T C P ヘッダを含むパケットである。A C K パケットとは、前記コードビットの A C K の制御ビットを立てた T C P ヘッダを含むパケットである。R S T パケットとは、前記コードビットの R S T の制御ビットを立てた T C P ヘッダを含むパケットである。

【0079】

同様に、U D P の t f t p (W R Q) パケットに対しては、t f t p (A C K) または I C M P (Port Unreachable) が応答パケットである。t f t p (W R Q) パケットとは、I E N 1 3 3 に規定された W R Q (W r i t e R e q u e s t) のペイロードを有するパケットである。t f t p (A C K) パケットとは、I E N 1 3 3 に規定された A C K (A c k n o w l e d g e m e n t) のペイロードを有するパケットである。I C M P (Port Unreachable) パケットとは、R F C 7 9 2 に記載のコードフィールドにおいて、P o r t U n r e a c h a b l e であるペイロードを有するパケットである。

【0080】

また、I C M P を用いる場合、E c h o R e q u e s t パケットに対して E c h o R e p l y が応答パケットである。また、E c h o パケットとは、R F C 7 9 2 に記載されている E c h o のペイロードを有するパケットである。

【0081】

なお、図 7 は 3 つのプロトコルを一例として示しているが、I C M P v 6 E c h o R e q u e s t、E c h o R e p l y など、送信パケットに対する応答パケットが規定されているプロトコルを用いてもよい。さらに、本実施形態では、各確認用プロトコルをあらかじめ記憶しているが、アプリケーション処理部 30 などを用いて、プロトコルを動的に追加・削除してもよい。

【0082】

(3) 確認プロセス実行部

図 8 は、確認プロセス実行部 251 の機能ブロック図である。確認プロセス実行部 251 は、削除通知終了判定部 510 (終了条件判定手段に相当)、削除通知到達確認部 520 (確認手段に相当) 及びプロトコル確認部 530 (状況確認手段に相当) を含む。

【0083】

削除通知終了判定部 510 は、削除通知到達確認部 520 に対して到達確認処理要求を行う。また、削除通知終了判定部 510 は、所定の終了条件を満たすまで、繰り返し、I S A K M P メッセージ処理部 24 に対し、削除通知メッセージの送信要求を行う (発明 1

10

20

30

40

50

に対応)。所定の終了条件とは、例えば I P s e c S A や I S A K M P S A の有効期限の満了（発明 2 に対応）、削除通知メッセージの送信回数の上限値の超過、削除通知メッセージの到達の確認である。この他、削除通知メッセージの再送を終了するための条件は、必要に応じ、適宜設定可能である。

【0084】

削除通知到達確認部 520 は、削除通知終了判定部 510 からの到達確認処理要求に応じ、到達確認処理を行う（発明 4 に対応）。到達確認処理は、確認パケット送信部 253 に対し、確認パケットの送信要求を行い、パケット受信判定部 254 から、パケット受信判定結果を取得する処理である。到達確認処理終了後、削除通知到達確認部 520 は、その結果を削除通知終了判定部 510 に通知する（発明 5 に対応）。 10

【0085】

プロトコル確認部 530 は、確認パケットを送信するために使用可能なプロトコルを確認パケット送信前に確認し、使用可能なプロトコルを S A 管理部 22 に通知する。

【0086】

（4）パケット受信判定部

図 9 は、パケット受信判定部 254 の機能ブロック図である。パケット受信判定部 254 は、I S A K M P パケット解析部 540、応答パケット判定部 550 及び I P s e c 受信部 560 を含む。I S A K M P パケット解析部 540 は、自動鍵交換処理の開始を意図する I S A K M P パケットであるか、否かを解析する。I P s e c 受信部 560 は、I P s e c S A を用いて送信されたパケットを解析する。パケット受信判定部 254 内では、受信したパケットについて各部がそれぞれ解析した結果を、確認プロセス実行部 251 20 に通知する。

【0087】

〔通信装置が行う処理〕

次に、通信装置 1 が行うプロトコル確認処理、削除通知メッセージ送信処理、到達確認処理について、具体的に説明する。以下の説明において、プロトコルを確認するための確認パケットを事前確認パケットと呼び、削除通知メッセージ後の確認パケットと区別する。

【0088】

（1）プロトコル確認処理 30

（1-1）メインルーチン

図 10 は、プロトコル確認処理のメインルーチンの流れの一例を示すフローチャートである。

【0089】

ステップ S1：まず、自動鍵交換処理が完了し、I P s e c S A が「使用可能」状態となったら、S A 管理部 22 は、確認プロセス管理部 25 内の確認プロセス実行部 251 に対して、I P s e c S A が確立済みとなったことを通知する。

【0090】

ステップ S2：通知を受けた確認プロセス実行部 251 は、プロトコル確認部 530 の機能により、各確認用プロトコルが使用可能であることを確認する処理を開始する。 40

【0091】

ステップ S3～S4：プロトコル確認部 530 は、プロトコル記憶部 252 の先頭のエントリにセットし（S3）、先頭のエントリから送信パケットのペイロード及び応答パケットのペイロードを読み出す。さらに、プロトコル確認部 530 は、送信パケットのペイロードを確認パケット送信部 253 に、応答パケットのペイロードをパケット受信判定部 254 に、それぞれ確立済みの I P s e c S A 情報とともに渡す（S4）。確認プロセス実行部 251 は、プロトコル確認部 530 の機能により、確認パケット送信部 253 に対し、事前確認パケットの送信要求を行う（S4）。例えば、先頭のエントリが T C P プロトコルであれば、事前確認パケットは S Y N フラグが有効となっている T C P ヘッダを含む（前記図 7 参照）（発明 11 に対応）。 50

【0092】

なお、実際に送信するときには、相手通信装置のアドレス、相手通信装置、および、自通信装置のポート情報の設定、チェックサム値の計算を行う必要がある。また、同時に送信パケットに対して相手側通信装置1からの送信が期待される応答パケットのペイロードを獲得する。このペイロードはACKフラグもしくはRSTフラグが有効となっているTCPヘッダを含むペイロードである。また、実際に利用する場合には相手通信装置のアドレス、相手通信装置、および、自通信装置のポート情報の設定を行う必要がある。

【0093】

ステップS5：確認パケット送信部253は、事前確認パケット送信処理を行う。この処理では、確認パケット送信部253は、事前確認パケットを相手側通信装置1に送信する。 10

【0094】

ステップS6：プロトコル確認部530は、確認パケット送信部253から事前確認パケットの送信結果を待機する。

【0095】

ステップS7：プロトコル確認部530は、送信成功の通知を受けた場合、パケット受信判定部254にパケット受信要求を行う。要求を受けたパケット受信判定部254は、相手側通信装置1cからの応答パケットを待機し、応答パケットの有無をプロトコル確認部530に通知する。

【0096】

“事前確認パケット”を受信した相手側通信装置1cは、TCPクライアント機能のみしかサポートしていない場合、またはTCPサーバ機能をサポートしていても、“事前確認パケット”のペイロードで要求されたTCPポートをbindしていない場合、対応するIPsec SAを利用してRSTを示す応答パケットを暗号化・認証処理を行い、通信装置1aに対して送信する。逆に、“事前確認パケット”のペイロードに指定されたTCPポートをbindしていれば、相手側通信装置1cは、ACKを示す応答パケットを通信装置1aに送信する。ACKを示す応答パケットにおいても、IPsec SAを利用して、暗号化・認証処理を行われたパケットが送信される。また、相手側通信装置1cがRSTを返さない実装の場合、応答パケットは送信されない。 20

【0097】

ステップS8～S9：応答パケット判定部550は、応答パケットを受信したか否かを、パケット受信判定部254からの通知に基づいて判断する（S8）。パケット受信判定処理の詳細は後述する。応答パケットを受信した場合、応答パケット判定部550は、プロトコル管理部530に通知し、プロトコル確認部530は、使用可能であることが確認されたプロトコルを、対応するIPsec SAのレコードに追加するよう、SA管理部22に要求する（S9）（発明10に対応）。応答パケットを受信しなかった場合、後述するステップS10に移行する。 30

【0098】

ステップS10～S11：前記ステップS6において、確認パケット送信部253から送信失敗の通知を受けた場合、プロトコル確認部530は、プロトコル記憶部252に登録されている全てのプロトコルについて事前確認パケットの送信を試みたか否かを確認する（S10）。事前確認パケットに対する応答パケットを受信できなかった場合も同様である。全てのプロトコルについて試みていれば、本処理を終了する。まだ送信を試みていないプロトコルがあれば、プロトコル記憶部252から次の確認用プロトコルを取得し（S11）、そのプロトコルを用いて事前確認パケットの送信を試みる（S4）。 40

【0099】

以上の処理により、削除通知メッセージの後に送信する確認パケットを、どのプロトコルを用いて送信すればよいかを決定することができる。従って、確認パケットの信頼度を高め、ひいては削除通知メッセージの到達確認処理の信頼度を高めることができる。

【0100】

(1-2) 事前確認パケット送信処理サブルーチン

図11は、事前確認パケット送信処理サブルーチンの処理の流れの一例を示すフローチャートである。前記プロトコル確認処理のメインルーチンにおいてステップS5に移行すると、以下の処理が開始される。

【0101】

ステップS501～S502：確認パケット送信部253は、獲得した送信ペイロードがIPsec SAを適用する条件に適合するかを、IP処理部40に問い合わせる（S501）。もし、適合しないのであれば、確認パケット送信部253は、事前確認パケットの送信を行わず、プロトコル確認部530に送信失敗を通知する（S502）。適合する場合、ステップS503に移行する。

10

【0102】

ステップS503：確認パケット送信部253は、事前確認パケットのペイロードに対してIPsec処理を行うために、事前確認パケットのペイロードとIPsec SA情報とをIPsec処理部60に渡し、暗号化・認証処理要求を行う。要求を受けたIPsec処理部60は、暗号化・認証処理を行い、確認パケット送信部253に暗号化・認証処理後の事前確認パケットのペイロードを渡す。IPsec処理部60における暗号化・認証処理については、RFC2401などに記載の処理を逸脱せず、その説明を省略する。

【0103】

ステップS504～S506：さらに、確認パケット送信部253は、そのペイロードにIPヘッダを追加することにより“事前確認パケット”を作成し（S504）、IP処理部40に対して送信要求を行う（S505）。さらに、確認パケット送信部253は、プロトコル確認部530に送信成功を通知する（S506）。送信要求を受けたIP処理部40は、通信部50を介して、構築した“事前確認パケット”を送信する。

20

【0104】

(1-3) パケット受信判定処理サブルーチン

図12は、パケット受信判定処理サブルーチンの処理の流れの一例を示すフローチャートである。前記プロトコル確認処理のメインルーチンにおいてステップS7に移行すると、以下の処理が開始される。

【0105】

ステップS701～S702：パケット受信判定部254は、事前確認パケットの送信後、応答パケットの受信待ちを開始する。一定期間経過しても相手側通信装置1cからの応答がなければ（S701）、パケット受信判定部254は、応答パケット受信失敗をプロトコル確認部530に通知する（S702）。応答が返ってこない理由としては、ネットワーク上でパケットがロスした場合や、前述したように端末102がRSTを返さない実装の場合などがある。

30

【0106】

ステップS703：一方、通信部50を介して相手側通信装置1cからパケットを受信した場合、パケット受信判定部254は、以下の処理により受信パケットが期待している応答パケットであるか否かを判定する。

40

【0107】

ステップS704～S706：まず、パケット受信判定部254は、受信したパケットがIPsecパケットでなければ、再度端末102からのパケットの受信待ちを一定期間行う（S704）。受信したパケットがIPsecパケットであれば、IPsec復号化処理を行うために、IPsec処理部60に、受信パケットと、送信した削除通知メッセージに対応するIPsec SAの情報とを渡し、復号化処理・認証処理を要求する。そして、復号化処理後のパケットが、期待している応答パケットであることを確認する（S705）。応答パケットであれば、プロトコル確認部530に応答パケット受信成功を通知する（S706）。応答パケットでない場合は、再度、端末102からのパケットの受信待ちを一定期間行う（S701）。

50

【0108】

本実施形態において、受信パケットの確認対象フィールドとしては、1) 送信元ポート、宛先ポートが一致していること、2) コードビットフィールドにおいて、RSTまたはACKの制御ビットが立っていること、などが挙げられる。なお、上記確認対象フィールド以外に、TCPヘッダ内の各フィールド及びTCPペイロードの各フィールドを確認対象としてもよい。

【0109】

なお、TCPプロトコルについて説明を行ったが、UDPプロトコル、ICMPプロトコルなど、送信するパケットに対して、応答パケットの一部もしくは全てが規定されている通信においても、同様の処理により確認することができる。

10

【0110】

以上のように、パケット受信判定部254は、応答パケットの受信成功または失敗を、プロトコル確認部530に通知する。

【0111】

なお、本実施形態では、SA管理部505における、確認用プロトコルのフィールドを「使用可能」、「使用不可」と示したが、応答パケットを記載することにより、代替してもよい。なお、その場合、プロトコル記憶部252にて、応答パケットとして、二つのペイロードを記憶している場合、確認用プロトコルの使用可能状況の確認処理にて、受信したペイロードのみをSA管理部505に記憶してもよいし、二つのペイロードを記憶してもよい。

20

【0112】

また、応答パケットとして規定したデータをあらかじめ記憶せず、パケット受信判定処理において受信したパケットを応答パケットとして規定してもよい。

【0113】

さらに、IPsec SAが確立した直後に、使用可能状況の確認処理を実施したが、通信装置相互において、IPsec SAが確立した状態であれば、プロトコル確認処理を実行するタイミング及び実施回数はこれに限定されない。事前確認パケットを複数回送信する場合、応答パケットも複数受信する可能性があるが、1つでも応答パケットとして判断できるパケットが受信できれば、それ以降のパケットは破棄してもよい。

【0114】

さらに、プロトコル記憶部252に記憶したプロトコルをプロトコル確認処理にて使用したが、実際にIPsec SAを適用するアプリケーションによる通信の送受信パケットを記憶しておき、それを確認用プロトコルとして使用してもよい。

30

【0115】

以上のように、プロトコル確認処理を行うことにより、IPsec SAが確立した状態において、対向通信装置からの応答パケットが確認できるため、より正確な到達確認処理が実施可能となる。

【0116】

(2) 削除通知メッセージ送信処理及び到達確認処理

(2-1) 削除通知メッセージ送信要求処理

40

図13は、削除通知メッセージ送信要求処理の流れの一例を示すフローチャートである。

【0117】

ステップS21～S22：要求受付部21は、通信装置相互にIPsec SAが「使用可能」として確立している状態において、ユーザまたはアプリケーションによる削除要求を待機する。削除要求が発生すると、要求受付部21にて受け付けられ、SA管理部22に通知される(S22)。通知を受けたSA管理部22は、該当するIPsec SAの状態を「使用不可」とし、確認プロセス管理部25に削除通知メッセージ送信処理の実行を要求する。

【0118】

50

ステップ S 2 3 : 確認プロセス管理部 2 5 は、後述する削除通知メッセージ送信処理を実行し、削除対象の I P s e c S A について削除通知メッセージを送信する。

【 0 1 1 9 】

確認プロセス管理部 2 5 内では、削除通知終了判定部 5 1 0 に到達確認処理の実行回数をあらかじめ規定しておく。削除通知終了判定部 5 1 0 は、I S A K M P メッセージ処理部 2 4 に削除通知メッセージ送信要求を行う。その後、所定の終了条件を満たさない間、削除通知メッセージ送信要求及び到達確認処理は繰り返される。以下では、説明を容易にするために、送信回数が規定した上限値を超えたとき、終了条件を満たすものとする。終了条件を満たす場合は、到達確認処理を終了する。また、規定した実行回数を超えても終了条件を満たさなければ、終了条件を満たさない場合の処理を行う。なお、規定する実行回数は、特に限定しないが、ネットワーク上でパケットが破棄されることも考慮し、本実施形態では 2 回と規定する。

10

【 0 1 2 0 】

(2 - 2) 削除通知メッセージ送信処理

図 1 4 は、削除通知メッセージ送信処理の流れの一例を示すフローチャートである。前記図 1 3 の処理においてステップ S 2 3 に移行すると、以下の処理が開始される。

【 0 1 2 1 】

ステップ S 3 1 ~ S 3 2 : 確認プロセス実行部 2 5 1 は、削除通知メッセージの送信を要求されると、削除通知終了判定部 5 1 0 に通知する。削除通知終了判定部 5 1 0 は、少なくとも 1 つの確認用プロトコルが使用可能であるかを確認するために、S A 管理部 2 2 に使用可能な確認用プロトコルがあるか、問い合わせる (S 3 1) 。問い合わせた結果、使用可能な確認用プロトコルが存在しない場合、確認用プロトコルなしの処理を行う (S 3 2) 。この処理については、後述する第 3 実施形態で詳述する。

20

【 0 1 2 2 】

ステップ S 3 3 : 一方、使用可能な確認用プロトコルが存在する場合、確認プロセス実行部 2 5 1 は、削除対象の I P s e c S A に対する削除通知メッセージの送信を、I S K A M P メッセージ処理部 5 0 4 に要求する。I S A K M P メッセージ処理部 2 4 は、削除通知メッセージを作成し、I P 処理部 4 0 に送信を要求する。なお、削除通知メッセージは R F C 2 4 0 7 ~ R F C 2 4 0 9 に規定されている範囲を逸脱しないものとし、説明を省略する。

30

【 0 1 2 3 】

ステップ S 3 4 ~ S 3 7 : 次に、削除通知終了判定部 5 1 0 は、S A 管理部 2 2 に対し、削除対象の I P s e c S A の有効期限が満了しているか否かを問い合わせる (S 3 4) 。寿命切れであれば、本処理を終了し、削除通知終了判定部 5 1 0 は S A 管理部 2 2 に I P s e c S A の削除要求を行う (後述する S 3 7) 。一方、I P s e c S A が寿命切れでない場合、削除通知終了判定部 5 1 0 は、削除通知到達確認部 5 2 0 に到達確認処理要求を行う (発明 5 に対応) 。削除通知到達確認部 5 2 0 は、到達確認処理を行い (S 3 5) 、削除通知メッセージの再送の終了条件を満たすか否かを判定する (S 3 6) 。終了条件を満たす場合、削除通知終了判定部 5 1 0 は S A 管理部 2 2 に I P s e c S A の削除要求を行い、削除通知メッセージ送信及び到達確認処理を終了する (S 3 7) 。終了条件を満たさない場合、ステップ S 3 8 に移行する。

40

【 0 1 2 4 】

ステップ S 3 8 ~ S 4 0 : 削除通知終了判定部 5 1 0 は、削除通知メッセージの送信回数をインクリメントする (S 3 8) 。インクリメントした送信回数が規定の上限値 (この場合は “ 2 ”) を超えていたら (S 3 9) 、終了条件を満たさない場合の処理を行う (S 4 0) (発明 6 に対応) 。規定の上限値を超えていなければ、再度削除通知メッセージ送信を行う (S 3 3) 。

【 0 1 2 5 】

終了条件を満たさない場合の処理としては、ユーザに相手側通信装置 1 c における I P s e c S A が削除されていないことを通知するなどが挙げられる (発明 6 に対応) 。こ

50

のとき、自端末1aにおいて、SA管理部22に、該当するIPsec SA情報の削除を要求してもよいし、IPsec SAの状態を「使用不可能」とする要求をしてもよい。

【0126】

なお、削除通知メッセージは、IPsec SAのための削除通知メッセージ、ISAKMP SAのための削除通知メッセージのどちらであってもよい。

【0127】

以上の処理により、所定の終了条件を満たすまで、削除通知メッセージを繰り返し送信する。従って、削除通知メッセージを1回しか送信しない場合に比して、相手側通信装置に到達する確実性が増し、IPsec SA不一致の状態の発生確率を抑制することができる。 10

【0128】

(2-3) 到達確認処理サブルーチン

図15は、到達確認処理サブルーチンの処理の流れの一例を示すフローチャートである(発明4に対応)。この処理では、IPsecパケットである確認パケットを、繰り返し送信し、相手側通信装置1cからの応答パケットの有無を確認する。確認パケットの再送終了条件は、この例では、ISAKMPパケットを受信した場合及び再送回数が規定の上限値を超える場合である。確認パケットの再送終了条件は、これに限定されず、例えばIPsec SAの有効期限が満了した場合であっても良い(発明12に対応)。一方、該当のIPsec SAを用いて、暗号化された応答パケットを受信した場合、終了条件を 20

【0129】

前記図14の処理でステップS35に移行すると、以下の処理が開始される。

【0130】

ステップS51：削除通知到達確認部520は、確認パケット送信用に使用可能である確認用プロトコルをSA管理部22に問い合わせる。確認用プロトコルがある場合、SA管理部22は、管理テーブル22aから送信パケットのペイロード及び応答パケットのペイロードを読み出し、削除通知到達確認部520に渡す。削除通知到達確認部520は、送信パケットのペイロードを確認パケット送信部253に、応答パケットのペイロードを 30

パケット受信判定部254に、それぞれ削除対象のIPsec SA情報とともに渡す。次に、削除通知到達確認部520は、確認パケット送信部253に対し、確認パケットの送信を要求する(発明7に対応)。確認パケット送信要求に対する確認パケット送信処理は、図11の事前確認パケット送信処理と同様である。

【0131】

ステップS52：削除通知到達確認部520は、確認パケット送信失敗の通知を確認パケット送信部253から受信した場合は、SA管理部22に使用可能である確認用プロトコルの問い合わせを行い、失敗したプロトコル以外のプロトコルがあれば、それを使用して、再度確認パケットの送信要求を行う。もし、他のプロトコルが存在しなければ、終了条件を満たさないとして、到達確認処理を終了する(後述するS55)。 40

【0132】

ステップS53：確認パケット送信成功の通知を確認パケット送信部253から受信した場合、削除通知到達確認部520は、パケット受信判定部254に受信判断処理サブルーチンの実行を要求し、相手側通信装置1cからの応答パケットを一定期間待機する。

【0133】

ステップS54～S55：削除通知到達確認部520は、応答パケット受信成功の通知を受信した場合(S54)、削除通知メッセージの送信終了条件を満たさないこととする(S55)(発明7に対応)。

【0134】

ステップS56～S58：削除通知到達確認部520は、応答パケット受信失敗の通知 50

を受信した場合（S 5 4）、その真偽を確認するために、確認パケットの再送を確認パケット送信部 2 5 3 に要求する。まず、削除通知到達確認部 5 2 0 は、確認パケットの再送終了条件が満たされているかを判断する。この例では、削除通知到達確認部 5 2 0 は、再送回数が規定の上限回数を超えているかを確認する（S 5 6）。再送回数が規定の回数を超えていなければ、削除通知到達確認部 5 2 0 は、再送回数をインクリメントし（S 5 7）、再度確認パケットの送信を確認パケット送信部 2 5 3 に対して要求する（S 5 1）（発明 1 2 に対応）。再送回数が規定の上限回数を超えている場合、削除通知メッセージの終了条件を満たしていることとする（S 5 8）（発明 7 に対応）。

【0 1 3 5】

なお、削除通知メッセージの送信は、1 回につき 1 つとして説明したが、複数個同一の削除通知メッセージを送信しても構わない。同様に、到達確認処理を 1 つの“確認パケット”により実施するとして説明したが、複数の“確認パケット”により実施してもよい。

【0 1 3 6】

このように、本実施の形態によれば、到達確認処理を実施することにより、相手側通信装置において I P s e c S A が残っていることを確認することができ、必要以上にネットワーク負荷を上げずに、対向通信装置に対して、削除通知メッセージを送信することができる。

【0 1 3 7】

また、事前に確認用プロトコルの使用可能状況を確認することにより、より正確に到達確認処理を実施することができる。

【0 1 3 8】

また、確認用プロトコルとして T C P プロトコルを利用することにより、ネットワーク上でパケットロスした場合においても、再送制御により、パケットが相手側通信装置 1 c に到達しやすくなる。

【0 1 3 9】

（2-4）受信判断処理サブルーチン

図 1 6 は、受信判断処理サブルーチンにおける処理の流れの一例を示すフローチャートである（発明 7 に対応）。前記図 1 5 の処理でステップ S 5 3 に移行すると、以下の処理が開始される。

【0 1 4 0】

ステップ S 6 1：パケット受信判定部 2 5 4 は、相手側通信装置 1 c からのパケットを一定期間待機する（S 6 1）。相手側通信装置 1 c からのパケットを一定期間内に受信しない場合、削除通知到達確認部 5 2 0 に対して応答パケット受信失敗を通知する（S 6 2）。受信しなかった理由として、次の 2 つが考えられる。第 1 の理由は、通信装置 1 c が削除通知メッセージを受信し、削除対象の I P s e c S A 情報を削除したため、通信装置 1 a から送信した I P s e c 化された確認パケットを復号化処理できず、応答を返さない場合である。第 2 の理由は、相手側通信装置 1 c には、I P s e c S A 情報が残っており、応答パケットとして I P s e c パケットを送信したが、ネットワーク上のなんらかの問題により破棄される場合である。

【0 1 4 1】

ステップ S 6 3～S 6 5：パケット受信判定部 2 5 4 は、何らかのパケットを通信装置 1 c から受信した場合、そのパケットが I S A K M P パケットであるか否かを確認する（S 6 4）。受信したパケットが自動鍵交換処理開始のための I S K A M P パケットと判断された場合、パケット受信判定部 2 5 4 は応答パケット受信失敗を削除通知到達確認部 5 2 0 に通知する（S 6 5）（発明 1 3 に対応）。これにより、確認パケットの再送は停止し、終了条件が満たしていなければ削除通知メッセージが再送される。I S A K M P パケットを受信する理由として次の要因が考えられる。その要因は、通信装置 1 c が、I P s e c パケットを受信したが該当する I P s e c S A 情報が存在しない場合、自動的に自動鍵交換処理を実行し、I P s e c S A を確立しようとする実装である場合である。

【0 1 4 2】

ステップ S 6 6 ~ S 6 8 : 受信したパケットが I S A K M P パケットではない場合、パケット受信判定部 2 5 4 は、受信したパケットが I P s e c 化されたパケットであるか否かを判断する (S 6 6) 。 I P s e c 化されたパケットであれば、パケット受信判定部 2 5 4 は、応答パケット判定部 5 5 0 に I P s e c 処理部 6 0 に復号処理を要求し、復号化されたパケットを取得し、確認パケットに対する応答パケットであるか否かの判断を要求する (S 6 7) 。 応答パケットであった場合、応答パケット判定部 5 5 0 は、応答パケット受信成功を削除通知到達確認部 5 2 0 に通知する (S 6 8) 。 (発明 8 に対応) 逆に、受信したパケットが応答パケットではない場合や、 I P s e c 化されたパケットでない場合、パケット受信判定部 2 5 4 は再度パケットの受信待ちを行う (S 6 1) 。

【 0 1 4 3 】

10

本実施形態では、受信したパケットが期待している応答パケットであるか否かの判断を、復号後のパケットに基づいて行うが、応答パケットの S P I 値が確認パケットの S P I 値と一致した場合に応答パケットであると判断してもよい (発明 9 に対応) 。 この場合、 S P I 値及び確認用プロトコルの使用可能状況フィールド以外の情報を S A 管理部 2 2 に残しておく必要がないために、メモリの枯渇を防ぐことができる。

【 0 1 4 4 】

以上のように、パケット受信判定部 2 5 4 は、確認パケットに対する応答パケットの受信成功または失敗を、削除通知到達確認部 5 2 0 に通知する。

【 0 1 4 5 】

< 第 2 実施形態 >

20

本実施形態において、通信システムの構成及び通信装置の機能構成は、前記第 1 実施形態と同様である。本実施形態において、 I P 通信の送信元及び宛先は通信装置 1 a 及び 1 c とし、自動鍵交換処理をルータ 1 e , f 間にて行うトンネルモードの場合の処理について説明する。このときのルータとしての通信装置 1 e , f の機能について説明を行う。

【 0 1 4 6 】

(1) トンネルモードのパケット構成

図 1 7 は、 I P s e c トンネルモードのパケット構成の説明図である。 I P s e c トンネルモードは、 I P パケット全体に対してセキュリティ機能を適用し、ルータが新たにトンネル配送用の外側 I P ヘッダ及び E S P ヘッダを追加したパケットによる通信である。第 1 実施形態にて説明したように、トンネルモードは主にパケットを中継する機器間で I P s e c S A を確立して、暗号通信を行う。例えば、通信装置 1 a , c 間で I P 通信を行い、ルータ 1 e , f 間で暗号通信を行う。この場合、内側 I P ヘッダの宛先、送信元は、通信装置 1 a , c であり、外側 I P ヘッダの宛先、送信元は、ルータ 1 e , f であり、内側 I P ヘッダと、外側 I P ヘッダの宛先、送信元は異なる。

30

【 0 1 4 7 】

このため、到達確認処理における確認パケット (事前確認パケットを含む) を作成する場合、第 1 実施形態とは異なる処理が必要となる。以下に、第 1 実施形態とは異なる箇所のみを説明する。

【 0 1 4 8 】

(2) 管理テーブル

40

図 1 8 は、本実施形態の管理テーブル 2 2 b を示す図である。この管理テーブルは、第 1 実施形態における管理テーブル 2 2 a に、 I P 通信の送信元及び宛先を示すフィールドを追加した構成となっている。トンネルモードは、上記で説明の通り、 I P s e c による通信の端点と I P による通信の端点異なる。そのため、確認パケットを作成するためには、 I P s e c 通信の端点のみだけでは不十分であり、 I P 通信の送信元及び宛先が必要となる。それ以外のフィールドについては、前記管理テーブル 2 2 a と同様である。

【 0 1 4 9 】

(3) I P 端点の取得

次に、前記第 1 実施形態と異なる処理について説明する。前記第 1 実施形態と本実施の形態の処理が異なる点は、自動鍵交換処理が完了し、 I P s e c S A 確立後、 I P s e

50

c S Aが確立済みを通ずるまでの処理である。図19は、S A管理部22におけるIPsec S A確立後の処理の流れを示すフローチャートである。この処理では、S A管理部22は、IPsec S Aの確立済通知に先立ってIPsec S Aが使用されるのを待ち、使用されたときのIPパケットによりIP通信の端点の情報を得る。確認パケットの作成において、トンネルモードでは、IP通信の端点を送信元及び宛先とするIPヘッダを持つIPパケット全体を、暗号化処理・認証処理の対象とする。しかし、トンネルモードでは、暗号通信の端点とIP通信の端点異なり、暗号通信の端点同士で自動鍵交換処理を行うため、IPsec S Aを確立する過程（自動鍵交換処理）及びIPsec S A確立後、通信が発生しない場合において、S A管理部22は、IP通信の端点を得ることができない。本処理は、S A管理部22がIP通信の端点を得るために行う処理である。 10

【0150】

ステップS71～S74：S A管理部22は、IPsec S Aが確立された状態において（S71）、IP処理部40から中継処理を行うパケットの送信要求が生じるのを待機する（S72）。送信要求が生じると、送信パケットのペイロードがIPsec S Aを適用する条件に適合するか否かを、IP処理部40に問い合わせる（S73）。S A管理部22は、IPsecが適用される条件のパケットであり、かつ、そのためのIPsec S Aが存在しているかを判断する（S74）。IPsec S Aが存在しなければ、S A管理部22は、自動鍵交換の実行をS A確立部23に要求し、IPsec S Aを確立する。 20

【0151】

ステップS75～S77：一方、IPsec S Aが存在すれば、対応するIPsec S Aに対するIP通信の端点が記憶されているかを、S A管理部22は判断する（S75）。IP通信の端点が既に記憶されていれば、通常のIPsecパケットと同様に処理し、再度IP処理部からのIPsec適用問い合わせを待つ（S72）。記憶されていなければ、IPsec適用問い合わせを受けたパケットのIPヘッダから送信元及び宛先を読み出し、該当するIPsec S AのIP通信端点の送信元・宛先として管理テーブル22bに書き込む（S76）。書き込みが完了したら、S A管理部22は確認プロセス管理部25に対し、IPsec S A確立を通知する（S77）。 30

【0152】

このように、S A管理部22において、トンネルモード時のIP通信端点を保持しておくことにより、確認パケット作成及び応答パケットの判断に活用できる。

【0153】

（4）確認パケット及び応答パケットの作成

確認パケットの作成は、前記図10に示すプロトコル確認処理及び図15の到達確認処理サブルーチンにて行われる。これらの処理では、確認プロセス管理部25が暗号化・認証処理要求を行うと、IPsec処理部60では、IP通信のパケットを構築し、暗号化・認証処理対象をIPパケット全体として処理を行う（発明14に対応）。

【0154】

また、応答パケットの判断は、図12に示すパケット受信判定処理及び図16に示す受信判断処理サブルーチンにて行う。これらの処理では、ペイロードの確認に加えて、復号後のIPパケットにおける送信元及び宛先が期待すべき結果であることを確認してもよい。 40

【0155】

これ以外の処理に関しては、第1の実施の形態と同様に処理を行う。

【0156】

本実施形態によれば、トンネルモード用のIPsec S Aの削除通知メッセージに対しても、到達確認処理を行うことができる。

【0157】

<第3実施形態>

図20は、第3実施形態の通信装置1における確認プロセス管理部25の機能ブロック図である。本実施形態において、通信システムの構成及び通信装置の機能構成は、確認プロセス管理部25にプロトコル記憶部252がないことを除き、前記第1実施形態と同様である。本実施形態における通信システムでは、第1実施形態と同様に、通信装置1a、1c間でIP通信及びIPsec通信を行う。

【0158】

本実施形態では、削除通知メッセージの到達確認処理を実行しない。その代わり、所定時間、この例ではIPsec SAの有効期限が切れるまで、削除通知メッセージを繰り返し送信する（発明3に対応）。なお、到達確認処理を行わないため、プロトコル確認処理も行わない。

10

【0159】

図21は、本実施形態における削除通知メッセージ送信処理の流れの一例を示すフローチャートである。本実施形態では、前記図14の削除通知メッセージ送信処理に代えて以下の処理により削除通知メッセージを送信する。

【0160】

ステップS81～S83：削除通知終了判定部510は、対応する削除通知メッセージの送信を、ISAKMPメッセージ処理部24に要求する（S81）。その後、削除通知終了判定部510は、SA管理部22にIPsec SAの有効期限が切れているかを問い合わせる（S82）。有効期限が切れている場合、削除通知終了判定部510は本処理を終了し、SA管理部22にIPsec SAの削除要求を行う（S83）。

20

【0161】

ステップS84～S86：一方、有効期限が切れていないか、寿命切れの通知を受ける前にパケット受信判定部254がIPsec化されたパケットを受信した場合（S84）、パケット受信判定部254は、そのIPsec化されたパケットを復号するIPsec SAの状態をSA管理部22に問い合わせる（S85）。該当するIPsec SAの状態が「使用不可」であった場合は、削除通知終了判定部510は再度削除通知メッセージを送信要求する（S81）。逆に「使用可能」であった場合は、寿命切れの通知またはIPsec化されたパケットの受信を待つ（S82、S84）。

【0162】

これ以外の処理に関しては、第1実施形態と同様の処理のため、その説明を省略する。

30

【0163】

なお、IPsec化されたパケットの受信待ちを終了するタイミングとして、IPsec SAの寿命切れを一例に挙げたが、そのタイミングはこれに限定されない。また、IPsec化されたパケットの受信後に、削除通知メッセージを送信する場合を例にとったが、IPsec化されたパケットの受信とは無関係に削除通知メッセージを送信してもよい。

【0164】

このように、本実施形態によれば、「使用不可」のIPsec SAを使用したパケットを受信した場合に、相手側通信装置1cにIPsec SAが存在していることがわかり、その場合に、削除通知メッセージを送信することができる。

40

【0165】

また、受信待ちを終了するタイミングをIPsec SAとすることで、相手側通信装置においてIPsec SAが削除された以降は、他の通信装置からの受信待ちしていたパケットを偽装したパケットを用いての攻撃に対して、削除通知メッセージを送信せずに済む。

【0166】

<その他の実施形態>

前述した方法及びこの方法を実行するプログラム並びにこのプログラムを記録したコンピュータ読み取り可能な記録媒体も、本発明の範囲に含まれる。ここで記録媒体としては、コンピュータが読み書き可能なフレキシブルディスク、ハードディスク、半導体メモリ

50

、C D－R O M、D V D、光磁気ディスク（M O）、その他のものが挙げられる。

【産業上の利用可能性】

【0 1 6 7】

本発明にかかる削除通知メッセージを送信する装置及び方法は、I P s e cを用いた暗号通信を行う全ての通信装置に適用可能である。このような通信装置としては、例えばI P通信機能を有する家電機器や各種中継器を挙げることができる。

【図面の簡単な説明】

【0 1 6 8】

【図 1】本発明の通信装置を用いた通信システムの構成例を示す説明図

【図 2】図 1 の通信装置が行う処理の概要を示す説明図

10

【図 3】図 1 に示す通信装置の機能ブロック図

【図 4】I K E処理部の機能構成を示す説明図

【図 5】S A管理部が保持する管理テーブル 2 2 aに蓄積されるS A情報の概念説明図

【図 6】確認プロセス管理部の機能構成を示すブロック図

【図 7】プロトコル記憶部に記憶される情報の概念説明図

【図 8】確認プロセス実行部 2 5 1 の機能ブロック図

【図 9】パケット受信判定部の機能ブロック図

【図 1 0】プロトコル確認処理のメインルーチンの流れの一例を示すフローチャート

【図 1 1】事前確認パケット送信処理サブルーチンの処理の流れの一例を示すフローチャート

20

【図 1 2】事前確認パケット送信処理サブルーチンの処理の流れの一例を示すフローチャート

【図 1 3】削除通知メッセージ送信要求処理の流れの一例を示すフローチャート

【図 1 4】削除通知メッセージ送信処理の流れの一例を示すフローチャート

【図 1 5】到達確認処理サブルーチンの処理の流れの一例を示すフローチャート

【図 1 6】受信判断処理サブルーチンにおける処理の流れの一例を示すフローチャート

【図 1 7】I P s e cトンネルモードのパケット構成の説明図

【図 1 8】第 2 実施形態のS A管理部が有する管理テーブルに蓄積された情報の概念説明図

【図 1 9】S A管理部 2 2 におけるI P s e c S A確立後の処理の流れを示すフローチャート

30

【図 2 0】第 2 実施形態の通信装置における確認プロセス管理部の機能ブロック図

【図 2 1】削除通知メッセージ送信処理の流れの一例を示すフローチャート

【図 2 2】従来の通信システムの説明図

【符号の説明】

【0 1 6 9】

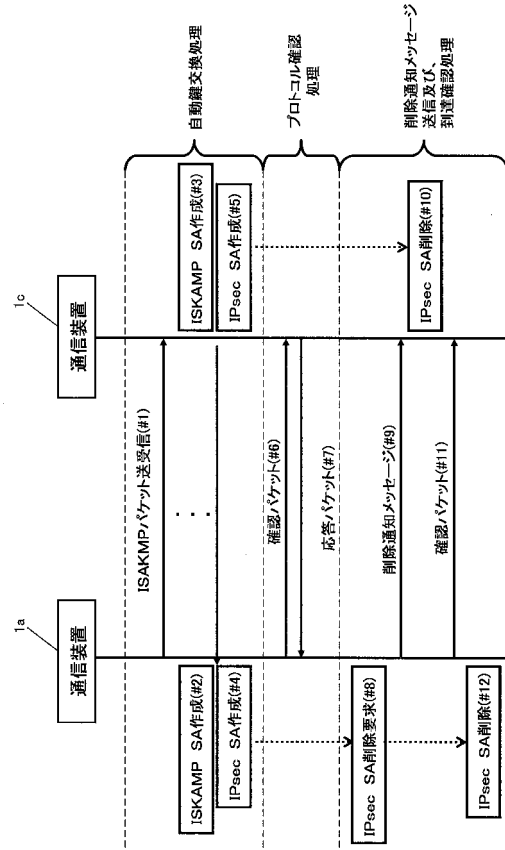
1 a～f：通信装置

2：通信ネットワーク

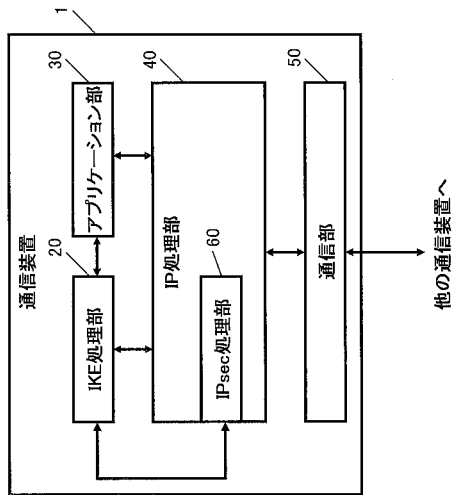
【図 1】



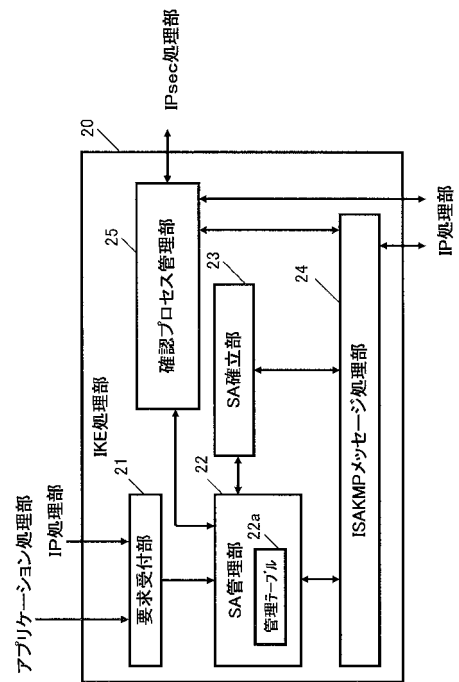
【図 2】



【図 3】



【図 4】



【図 5】

22a

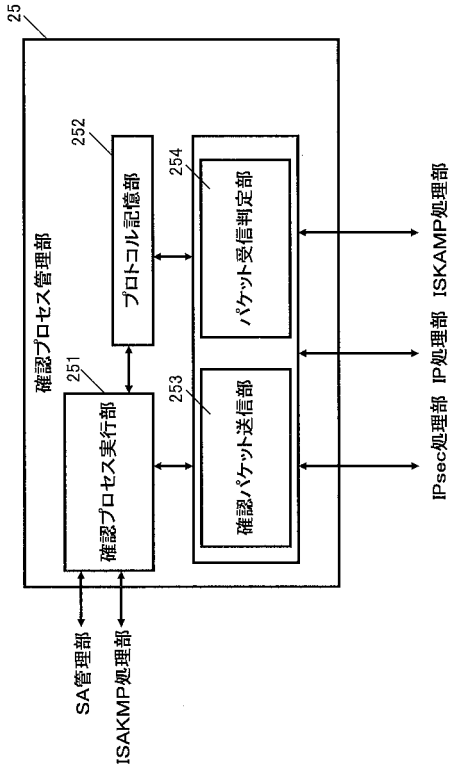
管理テーブル

No.	ISAKMP SA	IPsec終端点 送信元	宛先	SPI	IPsec SA状態	確認用プロトコル			IPsec SAの有効期限
						TCP	UDP	ICMP	
1	100	1.1.1.1	1.1.1.2	11112	使用可能	○	×	×	28800
2	200	1.1.1.1	1.1.1.3	11113	使用不可	○	×	○	500

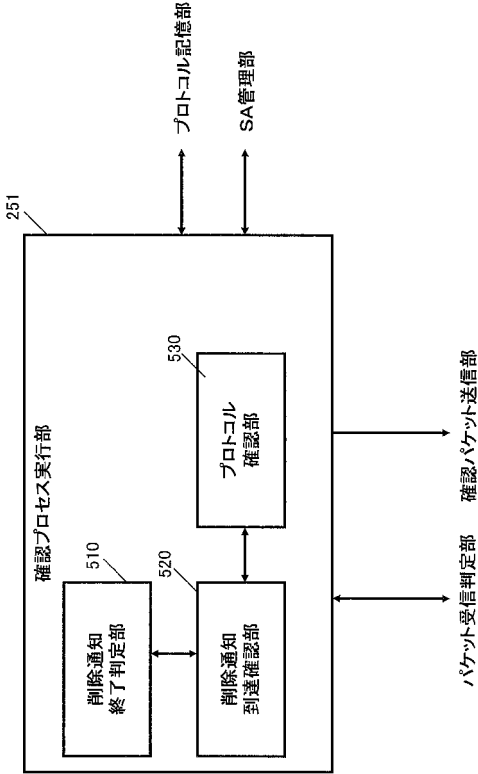
【図 7】

プロトコル記憶部 252		
プロトコル	送信パケット	応答パケット
TCP	SYN	ACK
		RST
UDP	tftp (WRQ)	tftp (ACK)
		ICMP (Port Unreachable)
ICMP	Echo Request	Echo Reply

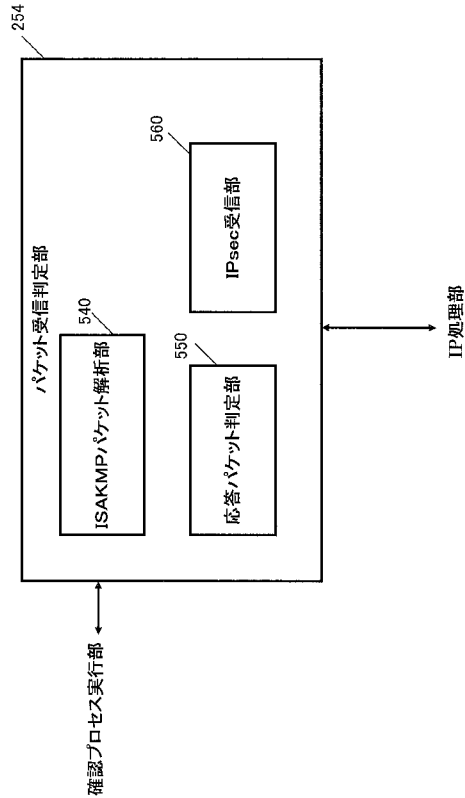
【図 6】



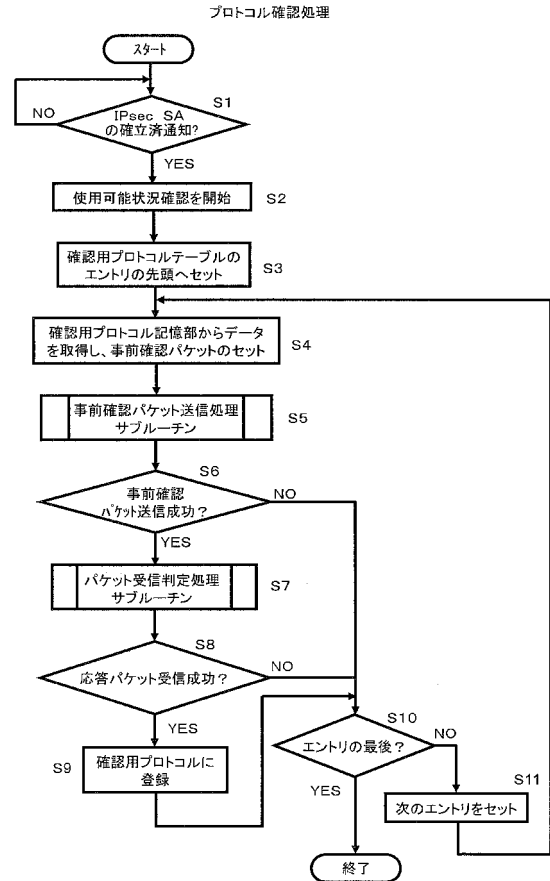
【図 8】



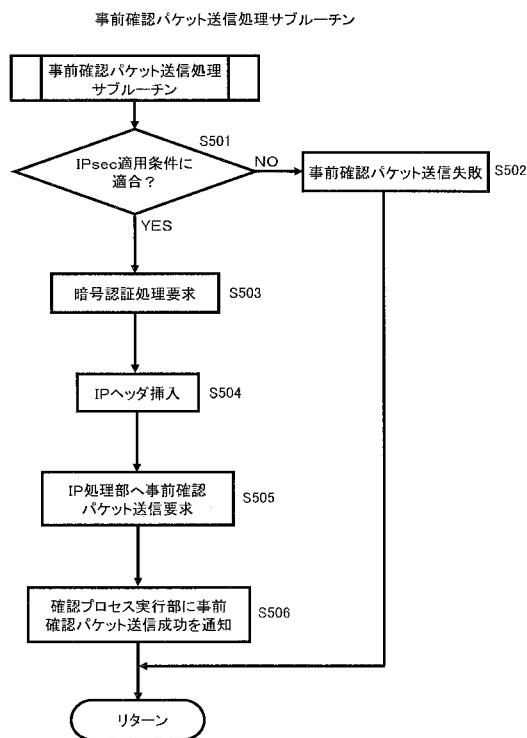
【図 9】



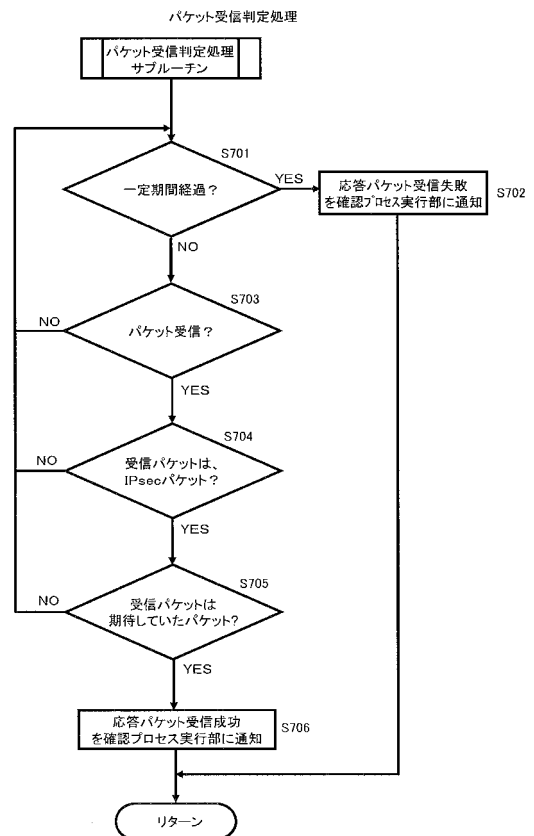
【図 10】



【図 11】

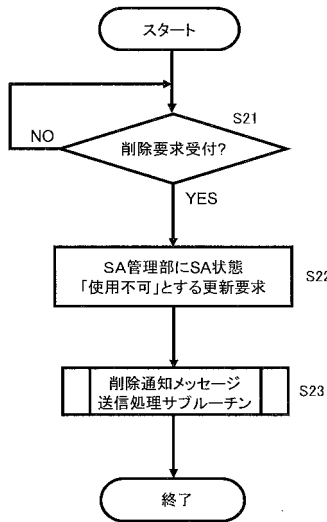


【図 12】



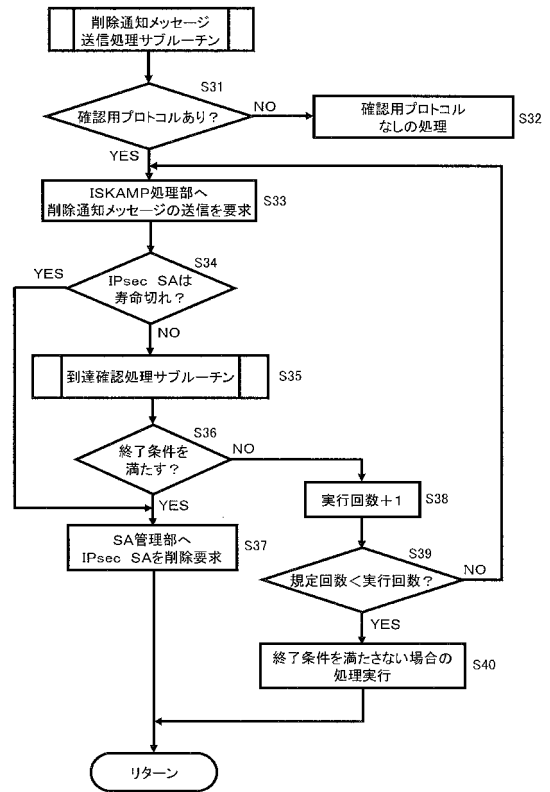
【図 13】

削除通知メッセージ送信要求処理

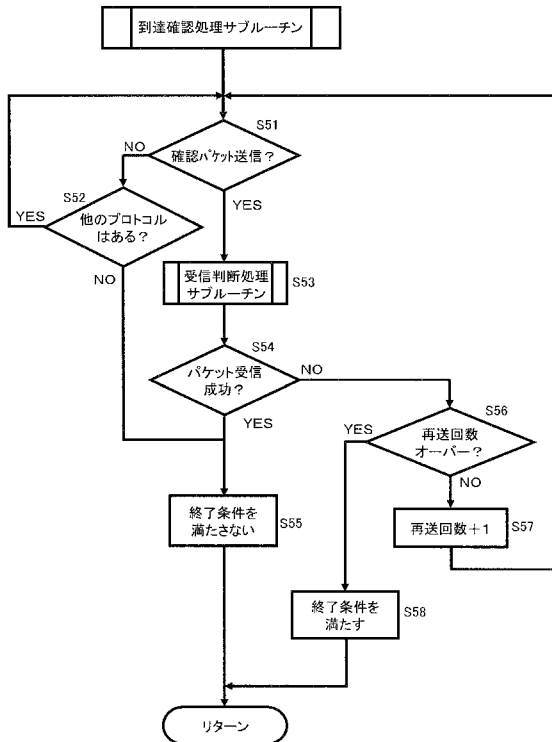


【図 14】

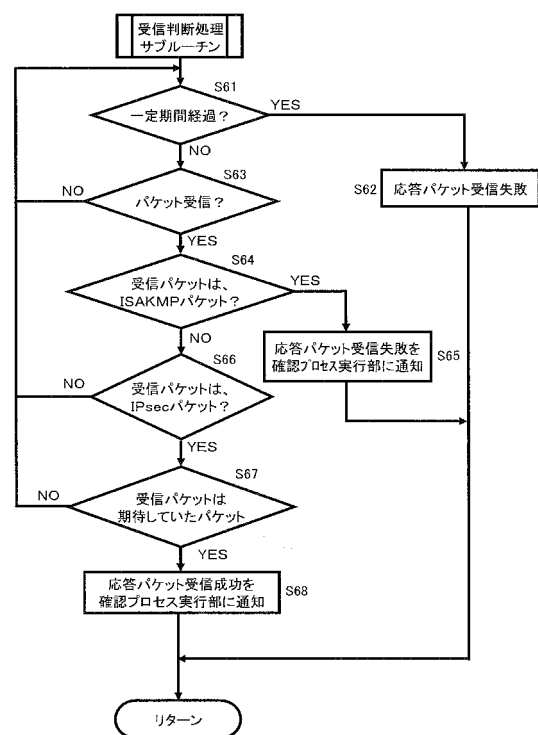
削除通知メッセージ送信処理



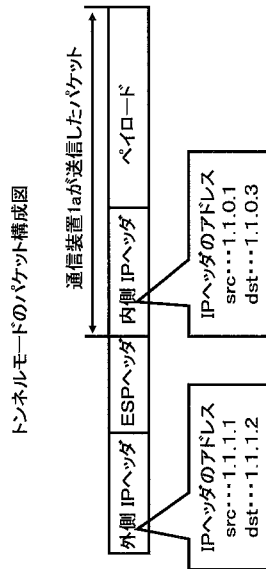
【図 15】



【図 16】



【図 17】

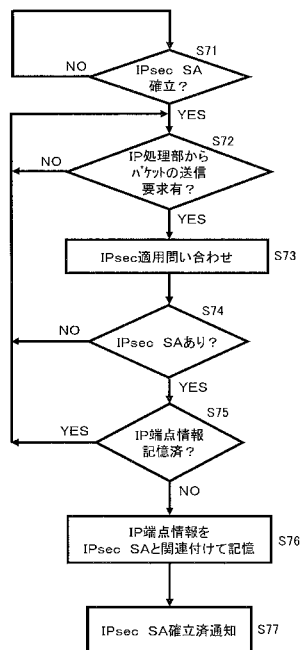


【図 18】

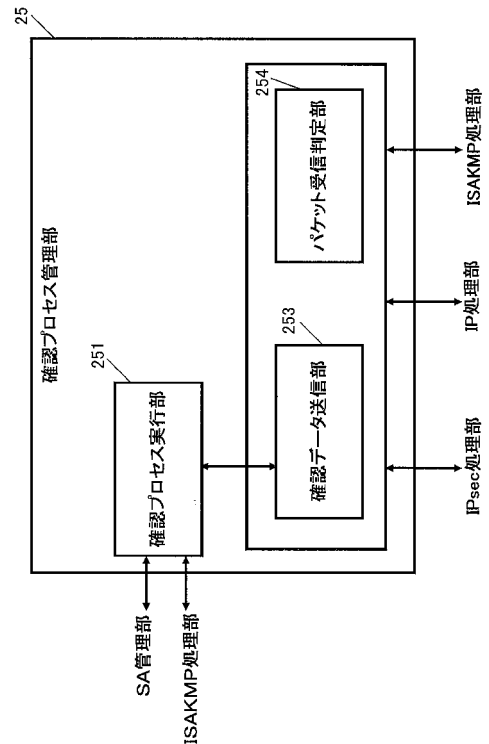
管理テーブル(第2実施形態)

No.	IPsec 終端点		IP 終端点		SPI	SA 状態	確認用プロトコル		寿命
	送信元	宛先	送信元	宛先			TCP	UDP	ICMP
1	111	112	101	103	11112	使用可能	○	×	28800
2	111	113	111	113	11113	使用不可	○	×	500

【図 19】

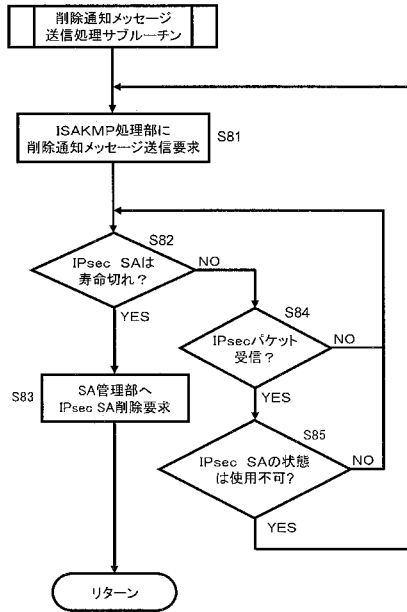


【図 20】

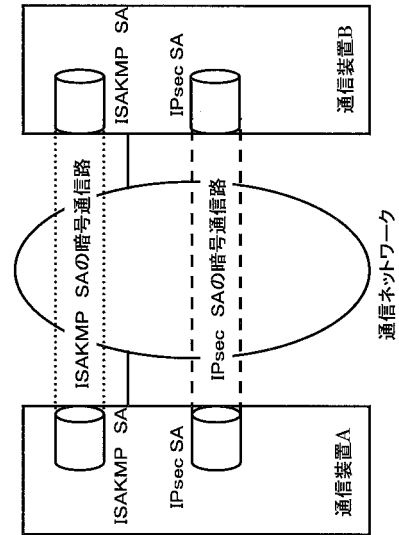


【図 2 1】

削除通知メッセージ送信処理(第3実施形態)



【図 2 2】



フロントページの続き

(72)発明者 高垣 景一

大阪府門真市大字門真１００６番地 松下電器産業株式会社内

(72)発明者 山内 実

大阪府門真市大字門真１００６番地 株式会社松下ソフトリサーチ内

Fターム(参考) 5J104 AA07 AA16 AA32 AA34 EA04 EA15 EA16 EA17 JA03 KA02
KA04 NA02 NA37 PA07