(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6112874号
(P6112874)
(45)発行日　平成29年4月12日(2017.4.12)　(24)登録日　平成29年3月24日(2017.3.24)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601C
H04L 9/14 (2006.01)　H04L 9/00 641

請求項の数 16　(全 19 頁)

(21)出願番号　特願2013-8621(P2013-8621)
(22)出願日　平成25年1月21日(2013.1.21)
(65)公開番号　特開2014-140132(P2014-140132A)
(43)公開日　平成26年7月31日(2014.7.31)
審査請求日　平成28年1月20日(2016.1.20)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100126240
弁理士　阿部　琢磨
(74)代理人　100124442
弁理士　黒岩　創吾
(72)発明者　深田　昌敬
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

審査官　中里　裕正

最終頁に続く

(54)【発明の名称】通信装置、通信装置の制御方法、および、プログラム

(57)【特許請求の範囲】
【請求項１】
通信装置であって、
他の通信装置との間で通信されるパケットの復号または認証に用いる第１の鍵を記憶部に記憶させる記憶手段と、
前記第１の鍵の有効期限に応じて、前記第１の鍵とは異なる第２の鍵を取得する取得手段と、
前記第２の鍵を用いて復号または認証されるパケットを前記他の通信装置から受信したことを判定する判定手段と、
前記判定手段により前記第２の鍵を用いて復号または認証されるパケットを前記他の通信装置から受信したと判定されたことに応じたタイミングにおいて、当該パケットが前記記憶部から前記第１の鍵を削除することを前記他の通信装置が指示するパケットとは異なるパケットである場合であっても、前記第１の鍵を前記記憶部から削除する削除手段と、
を有することを特徴とする通信装置。
【請求項２】
前記第１の鍵および前記第２の鍵は、ＩＰＳｅｃ（Ｓｅｃｕｒｉｔｙ　Ａｒｃｈｉｔｅｃｔｕｒｅ　ｆｏｒ　Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）に準拠したＩＰパケットの復号または認証に用いられる鍵であ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】
前記更新手段は、ＩＫＥ（Ｉｎｔｅｒｎｅｔ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ）により前記

第２の鍵に更新することを特徴とする請求項１または２に記載の通信装置。
【請求項４】
前記パケットは、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）に準拠したパケットであることを特徴とする請求項１乃至３のいずれか１項に記載の通信装置。
【請求項５】
前記第１の鍵および前記第２の鍵は、ＩＰＳｅｃ（Ｓｅｃｕｒｉｔｙ　Ａｒｃｈｉｔｅｃｔｕｒｅ　ｆｏｒ　Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）に準拠したＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）で用いられる鍵であることを特徴とする請求項１乃至４のいずれか１項に記載の通信装置。
【請求項６】
前記判定手段は、ＳＰＩ（Ｓｅｃｕｒｉｔｙ　Ｐｏｉｎｔｅｒ　Ｉｎｄｅｘ）に基づいて、前記第２の鍵を用いて復号または認証されるパケットを前記他の通信装置から受信したことを判定することを特徴とする請求項１乃至５のいずれか１項に記載の通信装置。
【請求項７】
前記第１の鍵の有効期限、および、前記第２の鍵の有効期限は、前記通信装置と前記他の通信装置との間の通信結果に基づいて設定されることを特徴とする請求項１乃至６のいずれか１項に記載の通信装置。
【請求項８】
前記記憶手段は、前記第１の鍵と関連付けて前記第２の鍵を前記記憶部に記憶させ、
前記削除手段は、前記判定手段により前記第２の鍵を用いて復号または認証されるパケットを前記他の通信装置から受信したと判定されたことに応じて、当該第２の鍵に関連付けられた前記第１の鍵を前記記憶部から削除することを特徴とする請求項１乃至７のいずれか１項に記載の通信装置。
【請求項９】
前記記憶手段は、前記他の通信装置に対して送信するパケットの暗号化に用いる第３の鍵を前記記憶部に記憶させ、
前記更新手段は、前記第３の鍵の有効期限が切れた場合に、前記第３の鍵から第４の鍵に更新し、
前記判定手段は、前記第４の鍵を用いて暗号化されたパケットを前記他の通信装置に送信することを判定し、
前記削除手段は、前記判定手段により前記第４の鍵を用いて暗号化されたパケットを前記他の通信装置に送信すると判定されたことに応じて、前記第３の鍵を前記記憶部から削除する
ことを特徴とする請求項１乃至８のいずれか１項に記載の通信装置。
【請求項１０】
前記記憶手段は、前記他の通信装置に対して送信するパケットの暗号化に用いる第３の鍵を前記記憶部に記憶させ、
前記更新手段は、前記第３の鍵の有効期限が切れた場合に、前記第３の鍵から第４の鍵に更新し、
前記削除手段は、前記更新手段により前記第４の鍵に更新されたことに応じて、前記第３の鍵を前記記憶部から削除する
ことを特徴とする請求項１乃至９のいずれか１項に記載の通信装置。
【請求項１１】
前記第１の鍵および前記第２の鍵は、前記他の通信装置との間で通信されるパケットの復号に用いる暗号鍵であることを特徴とする請求項１乃至１０のいずれか１項に記載の通信装置。
【請求項１２】
前記第１の鍵および前記第２の鍵は、前記他の通信装置との間で通信されるパケットの認証に用いる認証鍵であることを特徴とする請求項１乃至１０のいずれか１項に記載の通信装置。

【請求項１３】
前記削除手段は、前記判定手段により前記第２の鍵を用いて復号または認証されるパケットを前記他の通信装置から受信したと判定されたことに応答して、前記第１の鍵を前記記憶部から削除することを特徴とする請求項１乃至１２のいずれか１項に記載の通信装置。
【請求項１４】
前記削除手段は、前記判定手段により前記第２の鍵を用いて復号または認証されるパケットを前記他の通信装置から受信したと判定されてから第１の所定時間が経過すると、前記第１の鍵を前記記憶部から削除することを特徴とする請求項１乃至１２のいずれか１項に記載の通信装置。
【請求項１５】
通信装置の制御方法であって、
他の通信装置との間で通信されるパケットの復号または認証に用いる第１の鍵を記憶部に記憶させる記憶工程と、
前記第１の鍵の有効期限に応じて、前記第１の鍵とは異なる第２の鍵を取得する取得工程と、
前記第２の鍵を用いて復号または認証されるパケットを前記他の通信装置から受信したことを判定する判定工程と、
前記判定工程において前記第２の鍵を用いて復号または認証されるパケットを前記他の通信装置から受信したと判定されたことに応じたタイミングにおいて、当該パケットが前記記憶部から前記第１の鍵を削除することを前記他の通信装置が指示するパケットとは異なるパケットである場合であっても、前記第１の鍵を前記記憶部から削除する削除工程と、
を有することを特徴とする制御方法。
【請求項１６】
コンピュータを、請求項１から１４のいずれか１項に記載の通信装置として動作させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、他の通信装置との間で通信されるパケットの復号または認証に用いる鍵を更新する通信装置に関する。
【背景技術】
【０００２】
近年、ネットワークを介したデータの送受信における、セキュリティ確保の必要性が高まっている。ＩＰネットワーク上を流れるＩＰパケットのセキュリティを確保するためのプロトコルとして、ＩＰＳｅｃ（ＩＰ　Ｓｅｃｕｒｉｔｙ　Ｐｒｏｔｏｃｏｌ）がある（特許文献１）。
【０００３】
ＩＰＳｅｃで用いられる暗号鍵や認証鍵等はＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）として管理される。ＩＰＳｅｃに準拠したパケットは、ＳＡによって管理されている暗号鍵や認証鍵等を用いて、暗号化や復号、認証等が行われる。
【０００４】
ＳＡはソフト有効期限（更新期限）ごとに定期的に旧ＳＡから新ＳＡに更新される。一方、更新前に利用されていた旧ＳＡは、通信相手からＳＡの削除指示を受信するか、ハード有効期限（削除期限）が来るまで保持される。ハード有効期限を設けることで、旧ＳＡを利用したパケットが遅延して届く場合や、通信相手が旧ＳＡから新ＳＡに移行するのに時間がかかった場合であっても、パケットの受信に失敗する可能性を低減させている。
【先行技術文献】
【特許文献】

【０００５】
【特許文献１】特開２００６－３５２５００号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、通信相手からのＳＡの削除指示がネットワークにおいて消失してしまうと、通信装置は当該削除指示を受信することができず、ハード有効期限が来るまで削除できなくなってしまう。
また、ハード有効期限は、ユーザが任意の値を設定できるので、更新された後、長時間にわたり旧ＳＡが削除されずにメモリに残ってしまう場合がある。
旧ＳＡが削除されずに長時間メモリに残ってしまうと、メモリ空間を圧迫し、また、ＳＡを検索する際の処理負荷が高まってしまうという課題がある。
上記課題を鑑み、パケットの復号または認証に用いる鍵を記憶するメモリを有効利用できるようすることを目的とする。
【課題を解決するための手段】
【０００７】
上記課題を鑑み、本発明の通信装置は、他の通信装置との間で通信されるパケットの復号または認証に用いる第１の鍵を記憶部に記憶させる記憶手段と、前記第１の鍵の有効期限に応じて、前記第１の鍵とは異なる第２の鍵を取得する取得手段と、前記第２の鍵を用いて復号または認証されるパケットを前記他の通信装置から受信したことを判定する判定手段と、前記判定手段により前記第２の鍵を用いて復号または認証されるパケットを前記他の通信装置から受信したと判定されたことに応じたタイミングにおいて、当該パケットが前記記憶部から前記第１の鍵を削除することを前記他の通信装置が指示するパケットとは異なるパケットである場合であっても、前記第１の鍵を前記記憶部から削除する削除手段と、を有する。
【発明の効果】
【０００８】
本発明によれば、パケットの復号または認証に用いる鍵を第１の鍵から第２の鍵に更新する際に、第２の鍵を用いて復号または認証されるパケットであって、前記第１の鍵の削除指示とは異なるパケットを受信した場合であっても、当該パケットの受信に応じたタイミングにおいて第１の鍵を削除するので、メモリを有効利用できると共に、処理負荷を軽減させることができる。
【図面の簡単な説明】
【０００９】
【図１】通信装置１０１のハードウェア構成図。
【図２】通信装置１０１のソフトウェアブロック図。
【図３】通信装置１０１が実現するフローチャート。
【図４】通信装置１０１が実現するフローチャート。
【図５】通信装置１０１が実現するフローチャート。
【図６】通信装置１０１のソフトウェアブロック図。
【図７】通信装置１０１が実現するフローチャート。
【図８】通信装置１０１が実現するフローチャート。
【図９】通信装置１０１が実現するフローチャート。
【図１０】通信装置１０１が実現するフローチャート。
【図１１】通信装置１０１が実現するフローチャート。
【発明を実施するための形態】
【００１０】
＜実施形態１＞
本実施形態では、通信装置１０１が不図示の他の通信装置とＩＰＳｅｃにより暗号化されたデータパケット（以下、パケット）を通信する場合について説明する。ここで、ＩＰ

Ｓｅｃとは、Ｓｅｃｕｒｉｔｙ Ａｒｃｈｉｔｅｃｔｕｒｅ ｆｏｒ Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌの略である。

【００１１】

図１に、通信装置１０１のハードウェア構成を示す。主プロセッサ１１１はデータの表示（投影を含む）や印刷等のアプリケーション処理を行う。主プロセッサ１１１は、後述するサブプロセッサ１２１に対して、不図示の他の通信装置へのデータ送信指示も行う。主メモリ１１２はアプリケーション処理に用いるためのデータや、他の通信装置とのデータ通信に用いる各種パラメータ、および、後述する各種フローチャートを実現するためのプログラム等を記憶する。ＴＯＥ（ＴＣＰ／ＩＰオフロードエンジン）１１３は、他の通信装置とデータ通信するためのプロトコル処理を行う。主プロセッサ１１１、主メモリ１１２、および、ＴＯＥ１１３は、バス１１４により接続されている。

【００１２】

次に、ＴＯＥ１１３の内部構成について説明する。サブプロセッサ１２１は他の通信装置とのデータ通信のための各種プロトコル処理を行う。検索装置１２２は共有メモリ１２３の中から、他の通信装置とのデータ通信に必要な各種情報を検索する。検索装置１２２の動作については後述する。

【００１３】

共有メモリ１２３は、他の通信装置とのデータ通信に必要な各種情報や、通信するデータを記憶する。鍵管理部１２４は、他の通信装置とのデータ通信に用いる暗号鍵を管理する。なお、暗号鍵は共有メモリ１２３に記憶（格納）されているものとする。暗号・復号器１２５は、鍵管理部１２４により管理されている暗号鍵を用いて、他の通信装置との間で通信されるデータの暗号化および復号化を行う。

【００１４】

データパス制御部１２６は、共有メモリ１２３とＭＡＣ部１２７との間のデータ転送（ＤＭＡ転送）を制御する。ＭＡＣ部１２７は、ＯＳＩ参照モデルのデータリンク層（第２層）の下位副層に相当するＭＡＣ層のプロトコル処理を行う。ＰＨＹ部１２８は、ＯＳＩ参照モデルの第１層に位置するＰＨＹ（物理）層のプロトコル処理と電気信号の処理を行う。

【００１５】

バス１２９は、ＴＯＥ１１３内部の各種ハードウェアを接続している。バスブリッジ１３０は、バス１１４およびバス１２９を接続している。ネットワーク１３１は、通信装置１０１と不図示の他の通信装置とを接続している。なお、ネットワーク１３１は有線でも無線でもよい。

【００１６】

図２に、主メモリ１１２により記憶されたプログラムを主プロセッサ１１１もしくはサブプロセッサ１２１が読み出すことで実現されるソフトウェアブロックを示す。なお、図２に示された複数のソフトウェアブロックを１つのソフトウェアブロックとして構成してもよいし、１つのソフトウェアブロックを複数のソフトウェアブロックとして構成してもよい。また、図２に示すソフトウェアブロックの一部または全部をハードウェアとして構成してもよい。

【００１７】

検索部２０１は、パケット（送信パケットもしくは受信パケット）に対応するＳＡ（Ｓｅｃｕｒｉｔｙ Ａｓｓｏｃｉａｔｉｏｎ）を検索する。ここで、検索部２０１は、当該受信パケットの送信元である他の通信装置のＩＰアドレスとポート番号、通信装置１０１自身のＩＰアドレスとポート番号、プロトコル種別、ＳＰＩ等を検索キーとして、共有メモリ１２３の中から対応ＳＡを検索する。ここで、プロトコル種別とは他の通信装置とＴＣＰに準拠した通信を行っているか、ＵＤＰに準拠した通信を行っているかを示す情報である。また、ＳＰＩとはＳｅｃｕｒｉｔｙ Ｐｏｉｎｔｅｒ Ｉｎｄｅｘの略であり、ＳＡで用いられる暗号鍵や認証鍵を識別するための情報である。また、ＳＡでは、他の通信装置との暗号通信で用いる暗号鍵情報や暗号化アルゴリズム、認証鍵や認証アルゴリズム

などの暗号化通信パラメータが管理されている。ただし、ＳＡに暗号鍵と暗号化アルゴリズムの情報を含まないようにしてもよいし、認証鍵と認証アルゴリズムの情報を含まないようにしてもよい。

【００１８】

破棄部２０２はパケット（送信パケットもしくは受信パケット）を破棄する。判定部２０３は、検索部２０１により検出されたＳＡに旧ＳＡの情報が関連付けられているか否かを判定する。なお、旧ＳＡについての説明は後述する。削除部２０４は、ＳＡを共有メモリ１２３から削除する。

【００１９】

ＩＰＳｅｃ処理部２０５は受信パケットに対して所定のＩＰＳｅｃ処理を施す。具体的には、ＩＰＳｅｃ処理部２０５は対応ＳＡにおいて管理されている暗号鍵情報および暗号化アルゴリズムに従って受信パケットの復号を行う。また、ＩＰＳｅｃ処理部２０５は対応ＳＡにおいて管理されている認証鍵および認証アルゴリズムに従って受信パケットの認証を行う。これにより、受信パケットの復号に失敗した場合や、受信パケットの認証に失敗した場合には、破棄部２０２は当該受信パケットを破棄する。なお、復号もしくは認証のいずれか一方のみを行うようにしてもよい。

【００２０】

更に、ＩＰＳｅｃ処理部２０５は対応ＳＡにおいて管理されている暗号鍵情報および暗号化アルゴリズムに従って送信パケットを暗号化する。また、ＩＰＳｅｃ処理部２０５は対応ＳＡにおいて管理されている認証鍵および認証アルゴリズムに従って送信パケットの認証情報を作成して当該送信パケットに付加する。なお、暗号化もしくは認証情報の付加のいずれか一方のみを行うようにしてもよい。

【００２１】

期限管理部２０６は、対応ＳＡのソフト有効期限（更新期限）、および、ハード有効期限（削除期限）が切れているか否かを判定する。なお、ここでは、ソフト有効期限およびハード有効期限は通信装置１０１において予め定められている所定の値とする。しかし、これに限らず、通信装置１０１の通信相手である他の通信装置において予め定められている所定の値としてもよい。また、通信装置１０１および他の通信装置の各々において定められている値のうち小さい方、または、大きい方を有効期限としてもよい。

【００２２】

処理判定部２１１は、新しいＳＡの要求処理を既に実行中か否かを判定する。フラグ部２１２は、新しいＳＡの要求処理を既に実行していることを示すフラグの管理を行う。ＩＫＥ部２１３は、Ｉｎｔｅｒｎｅｔ　Ｋｅｙ　Ｅｘｃｈａｎｇｅプロトコルに従って、新たなＳＡを取得するための処理を他の通信装置との間で行う。ＳＡ判定部２１４は新たなＳＡに対応する旧ＳＡ、即ち、ソフト有効期限が切れたＳＡが共有メモリ１２３に記憶されているかを判定する。記憶部２１５はＩＫＥ部２１３により新たに取得されたＳＡを共有メモリ１２３に記憶する。

【００２３】

図３に、通信装置１０１が不図示の他の通信装置からＩＰＳｅｃに準拠したパケットを受信する際に、主メモリ１１２により記憶されたプログラムを主プロセッサ１１１もしくはサブプロセッサ１２１が読み出すことで実現されるフローチャートを示す。

【００２４】

まず、検索部２０１は、他の通信装置から受信したパケット（以下、受信パケット）に対応するＳＡを検索する（Ｓ３０１）。ここでは、ＳＰＩを参照することで新ＳＡと旧ＳＡとを区別して検索する。即ち、新ＳＡで管理されている暗号鍵や認証鍵を用いて復号や認証をすべきパケットを受信したのか、旧ＳＡで管理されている暗号鍵や認証鍵を用いて復号や認証をすべきパケットを受信したのか、を判別することができる。なお、受信パケットを新ＳＡで管理されている暗号鍵や認証鍵を用いて復号や認証を行って成功すれば新ＳＡ、旧ＳＡで管理されている暗号鍵や認証鍵を用いて復号や認証を行って成功すれば旧ＳＡとして検索するようにしてもよい。

【００２５】
そして、対応ＳＡが検出されなかった場合（Ｓ３０２のＮｏ）、破棄部２０２は受信パケットを破棄する（Ｓ３０３）。一方、対応ＳＡが検出された場合（Ｓ３０２のＹｅｓ）、判定部２０３は、検出された対応ＳＡに旧ＳＡの情報が関連付けられているか否かを判定する（Ｓ３０３）。
【００２６】
旧ＳＡの情報が関連付けられていない場合（Ｓ３０４のＮｏ）、Ｓ３０６に進む。一方、旧ＳＡの情報が関連付けられている場合（Ｓ３０４のＹｅｓ）、削除部２０４は当該旧ＳＡを共有メモリ１２３から削除して（Ｓ３０５）、Ｓ３０６に進む。
【００２７】
Ｓ３０６において、ＩＰＳｅｃ処理部２０５は受信パケットに対して所定のＩＰＳｅｃ処理を施す。具体的には、ＩＰＳｅｃ処理部２０５は対応ＳＡにおいて管理されている暗号鍵情報および暗号化アルゴリズムに従って受信パケットの復号を行う。また、ＩＰＳｅｃ処理部２０５は対応ＳＡにおいて管理されている認証鍵および認証アルゴリズムに従って受信パケットの認証を行う。これにより、受信パケットの復号に失敗した場合や、受信パケットの認証に失敗した場合には、破棄部２０２は当該受信パケットを破棄する。なお、復号もしくは認証のいずれか一方のみを行うようにしてもよい。
【００２８】
次に、期限管理部２０６は、対応ＳＡのソフト有効期限（更新期限）が切れているか否かを判定する（Ｓ３０７）。ソフト有効期限が切れている場合（Ｓ３０７のＹｅｓ）、対応ＳＡの更新処理が行われる（Ｓ３０８）。具体的には、新たなＳＡの要求処理が行われる。なお、要求処理については、後述する。
【００２９】
ここで、有効期限は時間で設定してもよいし、バイト数で設定してもよい。時間により有効期限が設定される場合、ＳＡが取得されてからの時間をタイマで計測し、予め設定された有効期限よりも長い時間が計測された場合に有効期限が切れたものと判定する。また、バイト数により有効期限が設定される場合、当該ＳＡにより通信したパケットのバイト数を加算していき、所定バイト数に達した場合に有効期限が切れたものと判定する。
【００３０】
続いて、期限管理部２０６は、対応ＳＡのハード有効期限（削除期限）が切れているか否かを判定する（Ｓ３０９）。ハード有効期限が切れている場合（Ｓ３０９のＹｅｓ）、削除部２０４は対応ＳＡを共有メモリ１２３から削除する（Ｓ３１０）。
【００３１】
次に、Ｓ３０８で行われるＳＡ要求処理について、図４を用いて説明する。
【００３２】
処理判定部２１１は、ソフト有効期限の切れたＳＡの代わりとなる新しいＳＡの要求処理を既に実行中か否かを判定する（Ｓ４０１）。実行中である場合（Ｓ４０１のＹｅｓ）、図４に示す処理を終了する。一方、実行中ではない場合（Ｓ４０１のＮｏ）、フラグ部２１２は、新しいＳＡの要求処理を既に実行していることを示すフラグを立てる（Ｓ４０２）。ここでは、当該フラグとして仮ＳＡを共有メモリ１２３に記憶させるものとする。また、Ｓ４０１の判定は仮ＳＡが共有メモリ１２３に記憶されているか否かで判定を行うものとする。
【００３３】
そして、ＩＫＥ部２１３は、所定プロトコルに従って新たなＳＡを取得するための処理を他の通信装置との間で行う（Ｓ４０３）。ＩＫＥ部２１３により新たなＳＡが取得されると、ＳＡ判定部２１４は新たなＳＡに対応する旧ＳＡ、即ち、ソフト有効期限が切れたＳＡが共有メモリ１２３に記憶されているかを判定する。判定の結果、旧ＳＡが記憶されている場合には（Ｓ４０４のＹｅｓ）、記憶部２１５はＳ４０３において新たに取得したＳＡに旧ＳＡの情報を関連付けて共有メモリ１２３に記憶する。また、旧ＳＡが記憶されていない場合には（Ｓ４０４のＮｏ）、記憶部２１５はＳ４０３において新たに取得した

ＳＡを共有メモリ１２３に記憶する。この場合、新たに取得したＳＡに対応する旧ＳＡが存在しないので、関連付けは行われない。

【００３４】

その後、フラグ部２１２は、新しいＳＡの要求処理を既に実行していることを示すフラグを削除する（Ｓ４０７）。ここでは、共有メモリ１２３に記憶させていた仮ＳＡを削除する。

【００３５】

このようにして、新たなＳＡと旧ＳＡとが関連付けられて共有メモリ１２３に記憶され、図３におけるＳ３０３の判定に用いられることになる。

【００３６】

図５に、通信装置１０１が不図示の他の通信装置にＩＰＳｅｃに準拠したパケットを送信する際に、主メモリ１１２により記憶されたプログラムを主プロセッサ１１１もしくはサブプロセッサ１２１が読み出すことで実現されるフローチャートを示す。

【００３７】

まず、検索部２０１は、他の通信装置に送信するパケット（以下、送信パケット）に対応するＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）を検索する（Ｓ５０１）。

【００３８】

対応ＳＡが検出されなかった場合（Ｓ５０２のＮｏ）、図４に示す新たなＳＡの要求処理が行われる（Ｓ５０３）。更に、破棄部２０２は送信パケットを破棄して（Ｓ５０４）、図５に示す処理を終了する。

【００３９】

一方、対応ＳＡが検出された場合（Ｓ５０２のＹｅｓ）、判定部２０３は、検出された対応ＳＡに旧ＳＡの情報が関連付けられているか否かを判定する（Ｓ５０５）。旧ＳＡの情報が関連付けられていない場合（Ｓ５０５のＮｏ）、Ｓ５０７に進む。一方、旧ＳＡの情報が関連付けられている場合（Ｓ５０５のＹｅｓ）、削除部２０４は当該旧ＳＡを共有メモリ１２３から削除して（Ｓ５０６）、Ｓ５０７に進む。

【００４０】

Ｓ５０７において、ＩＰＳｅｃ処理部２０５は送信パケットに対して所定のＩＰＳｅｃ処理を施す。具体的には、ＩＰＳｅｃ処理部２０５は対応ＳＡにおいて管理されている暗号鍵情報および暗号化アルゴリズムに従って送信パケットを暗号化する。また、ＩＰＳｅｃ処理部２０５は対応ＳＡにおいて管理されている認証鍵および認証アルゴリズムに従って送信パケットの認証情報を作成して当該送信パケットに付加する。なお、暗号化もしくは認証情報の付加のいずれか一方のみを行うようにしてもよい。

【００４１】

次に、期限管理部２０６は、対応ＳＡのソフト有効期限（更新期限）が切れているか否かを判定する（Ｓ５０８）。ソフト有効期限が切れている場合（Ｓ５０８のＹｅｓ）、対応ＳＡの更新処理が行われる（Ｓ５０９）。具体的には、新たなＳＡの要求処理が行われる。

【００４２】

続いて、期限管理部２０６は、対応ＳＡのハード有効期限（削除期限）が切れているか否かを判定する（Ｓ５１０）。ハード有効期限が切れている場合（Ｓ５１０のＹｅｓ）、削除部２０４は対応ＳＡを共有メモリ１２３から削除する（Ｓ５１１）。

【００４３】

このようにして、ソフト有効期限が切れた旧ＳＡに対応する新たなＳＡが取得されてから、新たなＳＡを利用したパケットを他の通信装置から受信するまで記憶部に記憶しておく。従って、新たなＳＡが取得した後に、他の通信装置から旧ＳＡを利用したパケットを受信した場合であっても、当該パケットを正常に受信することができる。即ち、他の通信装置が旧ＳＡを利用したパケット送信から、新たなＳＡを利用したパケット送信までの切替えに時間がかかったとしても、パケットをロストする可能性を低下させることができる。

【００４４】
また、上記実施形態では、ＩＰＳｅｃに対応したパケットを送信する際に、当該パケット送信に利用するＳＡに関連付けられた旧ＳＡが存在するか否かを判定し、存在している場合には当該旧ＳＡを削除した。これに限らず、通信装置１０１が送信時に用いる新たなＳＡを取得したことに応じて、当該新ＳＡに対応する旧ＳＡを削除するようにしてもよい。これにより、旧ＳＡを早く削除することができるので、メモリをより有効に活用することができる。
【００４５】
＜実施形態２＞
次に、実施形態２について説明する。通信装置１０１のハードウェア構成は実施形態１と同様である。
【００４６】
図６に、主メモリ１１２により記憶されたプログラムを主プロセッサ１１１もしくはサブプロセッサ１２１が読み出すことで実現されるソフトウェアブロックを示す。なお、図６に示された複数のソフトウェアブロックを１つのソフトウェアブロックとして構成してもよいし、１つのソフトウェアブロックを複数のソフトウェアブロックとして構成してもよい。また、図６に示すソフトウェアブロックの一部または全部をハードウェアとして構成してもよい。
【００４７】
ネットワークプロトコル処理部６０４はＴＣＰ、ＵＤＰ、ＩＰ等のネットワークプロトコルを処理する。ネットワークインタフェース部６０３を介して受信したパケットはネットワークプロトコル処理部６０４でＭＡＣ、ＩＰプロトコル処理を行い、ＩＰＳＥＣ処理部６０７でＩＰｓｅｃ受信処理を行う。ＩＰＳＥＣ処理部６０７でＩＰｓｅｃ受信処理が完了すると再びネットワークプロトコル処理部６０４でＴＣＰ、ＵＤＰ等のプロトコル処理を行う。その後、アプリケーション処理部６０５でアプリケーション処理を行う。またＩＫＥパケットであった場合はＩＫＥ処理部６０６でＩＫＥ処理を行う。
【００４８】
アプリケーション処理部６０５及びＩＫＥ処理部６０６が通信相手へパケットを送信する場合は、ネットワークプロトコル処理部６０４に送信要求を行い、ＴＣＰ、ＵＤＰ、ＩＰ等のプロトコル処理を行う。その後、ＩＰｓｅｃ処理部６０７でＩＰｓｅｃ処理を行い、ネットワークプロトコル処理部６０４でＩＰ、ＭＡＣプロトコル処理を行い、ネットワークインタフェース部６０３を介してパケットを送信する。
【００４９】
ＩＰｓｅｃプロトコル処理部６１２はパケットの送受信におけるＩＰｓｅｃプロトコル処理を行い、ＥＳＰ、ＡＨといったＩＰｓｅｃプロトコル処理を行う。また送受信パケットのポリシーを特定するためＳＰ管理部６０９に登録されたＳＰの検索要求を行う。ここで、ＳＰとはＳｅｃｕｒｉｔｙ　Ｐｏｌｉｃｙの略である。
【００５０】
また暗号・認証処理で必要となるＳＡを特定するためＳＡ管理部６１０に登録されたＳＡの検索要求を行う。またバイト数による有効期限のカウントを行い、ＳＡ管理部６１０に有効期限カウントの更新要求を行う。暗号・認証処理部６０８はＳＡの暗号化アルゴリズム、暗号鍵、認証アルゴリズム、認証鍵等に基づいて暗号、認証処理を行う。ＳＰ、ＳＡテーブル更新管理部はＩＫＥ処理部からのＳＰ、ＳＡの登録、更新、削除、参照処理を制御し、ＳＡ管理部、ＳＰ管理部に対して処理要求を行う。またパケット送信時、ＩＰｓｅｃプロトコル処理部６１２がＳＡ管理部６１０にＳＡ検索要求を行った結果、該当するＳＡがなかった場合はＩＰｓｅｃプロトコル処理部６１２からＳＡ折衝要求を受付、ＩＫＥ処理部６０６に対して通知を行う。またソフト有効期限切れの通知を受けてＳＡ折衝要求を受付、ＩＫＥ処理部６０６に対して通知を行う。タイマ部はＳＡ管理部６１０、ＳＰ、ＳＡテーブル更新管理部６１１からの設定により指定された時間が経過したこと通知する。ＳＡ管理部６１０はＳＡＤを保持し、要求された処理に基づいてＳＡＤに対する操作

を行い、処理結果を返す。またＳＰ管理部６０９はＳＰＤを保持し、要求された処理に基づいて操作を行い、処理結果を返す。

【００５１】

ここで、ＳＡＤとは、Ｓｅｃｕｒｉｔｙ Ａｓｓｏｃｉａｔｉｏｎ Ｄａｔａｂｅｓｅの略であり、ＳＡを管理・保持するデータベースのことである。また、ＳＰＤとは、Ｓｅｃｕｒｉｔｙ Ｐｏｌｉｃｙ Ｄａｔａｂａｓｅの略であり、ＳＰを管理・保持するデータベースのことである。

【００５２】

次に、通信装置１０１のＩＰｓｅｃパケット送信処理フローについて説明する。図７におけるステップＳ７０１において、アプリケーション処理部６０５は通信相手へのパケット送信処理を行い、ネットワークプロトコル処理部６０４に対して送信要求を行う。なお、ＩＫＥ処理部６０６がＩＫＥパケットを送信する際はＩＫＥ処理部６０６からネットワークプロトコル処理部６０４に対して送信要求を行う。

【００５３】

ステップＳ７０２において、ネットワークプロトコル処理部６０４はアプリケーション処理部６０５よりデータの送信要求を受け付ける。すると、アプリケーション処理部６０５が指定したＴＣＰまたはＵＤＰのトランスポート層プロトコル処理およびＩＰプロトコル処理を行う。次に作成したＩＰパケットをＩＰｓｅｃ処理部６０７へ通知する。

【００５４】

ステップＳ７０３において、ＩＰｓｅｃ処理部６０７は送信するＩＰパケットを受け取る。すると、ＩＰｓｅｃプロトコル処理部６１２がＩＰパケットのＩＰアドレスやトランスポート層プロトコル種別、ポート番号等のパケット情報からＳＰ管理部６０９に対してＳＰ検索処理要求を行う。ＳＰ検索処理要求を受け付けたＳＰ管理部６０９はＳＰＤに指定パケット情報に該当するＳＰが登録されているかを検索し、検索結果をＩＰｓｅｃプロトコル処理部６１２に通知する。

【００５５】

ステップＳ７０４において、ＩＰｓｅｃプロトコル処理部６１２はＳＰ管理部６０９から通知された検索結果を判定する。該当するＳＰがありかつ、該ＳＰに指定されたポリシーがＩＰｓｅｃ適用（Ａｐｐｌｙ ＩＰｓｅｃ）であった場合はステップＳ７０５へ進む。該当するＳＰがなかった場合もしくは、該当するＳＰに指定されたポリシーがＩＰｓｅｃ適用以外であった場合はステップＳ２１６へ進む。

【００５６】

ステップＳ７１６において、ステップＳ７０３でＳＰが見つからなかった場合、ＳＰが見つからなかった場合の暗号通信処理装置のポリシーを確認し、ポリシーが破棄（Ｄｉｓｃａｒｄ）であればパケットを破棄して終了する。ポリシーが通過（Ｂｙｐａｓｓ ＩＰｓｅｃ）であった場合はステップＳ７１８へ進む。またステップＳ７０３でＳＰが見つかった場合は該ＳＰのポリシーを確認し、ポリシーが破棄であった場合はパケットを破棄して終了する。またポリシーが通過であった場合はステップＳ７１８へ進む。

【００５７】

ステップＳ７０５において、ＩＰｓｅｃプロトコル処理部６１２はＳＰに関連づけられたＳＡの情報とパケット情報からＳＡ管理部６１０に対してＳＡ検索処理要求を行う。ＳＡ検索処理要求を受け付けたＳＡ管理部６１０はＳＡＤに、指定されたＳＰに関連付けられたＳＡ情報とパケット情報に該当するＳＡが登録されているかを検索し、検索結果をＩＰｓｅｃプロトコル処理部６１２に通知する。

【００５８】

ステップＳ７０６において、ＩＰｓｅｃプロトコル処理部６１２はＳＡ管理部６１０から通知された検索結果を判定する。該当するＳＡがあった場合はステップＳ７０７へ進む。該当するＳＡがなかった場合はステップＳ７１７へ進む。

【００５９】

ステップＳ７１７において、ＩＰｓｅｃ処理部６０７はＳＡ折衝要求処理を行う。

【００６０】
ここで図８を用いてステップＳ７１７のＳＡ折衝要求処理について説明する。
【００６１】
ＩＰｓｅｃプロトコル処理部６１２はＳＡ折衝要求をＳＰ、ＳＡテーブル更新管理部６１１に対して行う。ＳＰ、ＳＡテーブル更新管理部６１１はＳＡ折衝要求を受け付けると、ステップＳ８０１において、すでにＳＡ要求を行っているかを確認するため仮ＳＡを検索する。なお、仮ＳＡはＳＡ要求を行う際に作成して保持し、ＳＡ折衝が完了した際に削除する。また一定時間経過してもＳＡ要求が完了しない場合はタイムアウトし仮ＳＡを削除する。
【００６２】
ステップＳ８０２において該当する仮ＳＡが検索の結果登録されていた場合はＳＡ要求がすでに行われていると判断し、ＳＡ要求を破棄して終了する。仮ＳＡが登録されていなかった場合はステップＳ８０３へ進む。
【００６３】
ステップＳ８０３においてＳＰ、ＳＡテーブル更新管理部６１１は、仮ＳＡを作成して保持する。
【００６４】
ステップＳ８０４において、ＳＰ、ＳＡテーブル更新管理部６１１はＩＫＥ処理部６０６に対してＳＡ要求を通知する。ＳＡ要求を受け取るとＩＫＥ処理部６０６はＩＫＥプロトコルに基づいてＳＡ折衝を通信相手と行う。
【００６５】
ステップＳ８０５において、ＳＰ、ＳＡテーブル更新管理部６１１はＳＡ要求をした仮ＳＡのタイマとなるタイマ処理要求をタイマ部６１３に対して行い処理を終了する。
【００６６】
なおタイマ部６１３は仮ＳＡタイマがタイムアウトするとＳＰ、ＳＡテーブル更新管理部に対して通知する。通知を受けたＳＰ、ＳＡテーブル更新管理部６１１は仮ＳＡを削除する。
【００６７】
ステップＳ７１８において要求された送信パケットを破棄して処理を終了する。
【００６８】
ステップＳ７０７において、ＩＰｓｅｃプロトコル処理部６１２は特定されたＳＡを用いて、ＳＡに指定されたＥＳＰまたはＡＨのＩＰｓｅｃプロトコル処理を行う。ステップＳ７０８において、ＩＰｓｅｃプロトコル処理部６１２はＩＰｓｅｃプロトコル処理の中での暗号、認証処理を暗号・認証処理部６０８へ要求する。暗号・認証処理部６０８は要求を受け付けると暗号鍵、暗号アルゴリズム及び認証鍵、認証アルゴリズム等のＳＡ情報に基づいて暗号、認証処理を行う。
【００６９】
ステップＳ７０９においてＩＰｓｅｃプロトコル処理部６１２は使用したＳＡのバイト数による有効期限のカウント値を更新し、ＳＡ管理部６１０にカウント値の更新要求を行う。ＳＡ管理部６１０はカウント値の更新要求を受け付けると該当するＳＡのバイト数カウンタを更新する。
【００７０】
ステップＳ７１０においてソフト有効期限が切れたかを確認する。ソフト有効期限が切れた場合はステップＳ７１１へ進む。ソフト有効期限が切れていないかもしくは、すでに切れていた場合はステップＳ７１２へ進む。
【００７１】
ステップＳ７１１においてＩＰｓｅｃ処理部６０７はＳＡ折衝要求処理を行う。ステップＳ７１１におけるＳＡ折衝要求処理はステップＳ７１７のＳＡ折衝要求処理と共通の処理である。
【００７２】

ステップＳ７１２においてハード有効期限が切れたかを確認する。ハード有効期限が切れた場合はステップＳ７１３へ進む。ハード有効期限が切れていない場合はステップＳ７１４へ進む。

【００７３】

ステップＳ７１３においてＩＰｓｅｃプロトコル処理部はハード有効期限が切れたことをＳＰ、ＳＡテーブル更新管理部６１１に対し通知する。ハード有効期限切れの通知を受けたＳＰ、ＳＡテーブル更新管理部６１１はＩＫＥ処理部６０６にハード有効期限切れを通知し、ＳＡ管理部６１０に対して該当ＳＡの削除要求を行い、ＳＡ管理部６１０はＳＡＤから該当ＳＡを削除する。

【００７４】

ステップＳ７１４において、ＩＰｓｅｃ処理部６０７によってＩＰｓｅｃ処理されたＩＰｓｅｃパケットはネットワークプロトコル処理部６０４でフラグメント処理等のＩＰプロトコル処理、ＭＡＣヘッダ処理を行う。その後、ネットワークインタフェース部６０３にパケットの送信要求を行う。

【００７５】

ステップＳ７１５においてネットワークインタフェース部６０３はネットワークへパケットを送信して処理を終了する。

【００７６】

次に通信装置１０１のＩＰｓｅｃパケット受信処理フローについて説明する。図９におけるステップＳ９０１において、ネットワークインタフェース部６０３はネットワークから受信パケットを検知すると、受信パケットを取得してネットワークプロトコル処理部６０４へ通知する。

【００７７】

ステップＳ９０２においてネットワークプロトコル処理部６０４は受信パケットのヘッダ解析を行い、ＭＡＣ、ＩＰプロトコル処理を行う。ステップＳ９０３において、ネットワークプロトコル処理部６０４は受信パケットをＩＰｓｅｃ処理部６０７へと通知する。ＩＰｓｅｃ処理部６０７は受信パケットを受け取ると、ＩＰｓｅｃプロトコル処理部６１２はヘッダ解析を行い、ＩＰｓｅｃパケットであるか判断する。ＩＰｓｅｃパケットであった場合はステップＳ９０４へ進む。ＩＰｓｅｃパケットでなかった場合はステップＳ９１３へ進む。

【００７８】

ステップＳ９０４において、受信したＩＰｓｅｃパケットのＩＰアドレスやＩＰｓｅｃプロトコル種別、ＩＰｓｅｃヘッダ等のパケット情報から、ＳＡ管理部６１０にＳＡ検索処理要求を行う。ＳＡ検索処理要求を受け付けたＳＡ管理部６１０はＳＡＤに指定したパケット情報に該当するＳＡが登録されているかを検索し、検索結果をＩＰｓｅｃプロトコル処理部６１２に通知する。

【００７９】

ステップＳ９０５において、ＩＰｓｅｃプロトコル処理部６１２は検索結果を判定する。該当するＳＡが見つからなかった場合、ステップＳ９１９へ進み、該当するＳＡが見つかった場合はステップＳ９０６へ進む。

【００８０】

ステップＳ９０６において、ＩＰｓｅｃプロトコル処理部６１２は検索の結果得られたＳＡを用いてＥＳＰまたはＡＨのＩＰｓｅｃプロトコル処理を行う。ステップＳ９０７において、ＩＰＳＥＣプロトコル処理部６１２はＩＰｓｅｃプロトコル処理の中での暗号（復号）、認証処理を暗号・認証処理部６０８に要求する。暗号・認証処理部６０８は要求を受け付けると暗号鍵、暗号アルゴリズム及び認証鍵、認証アルゴリズム等のＳＡ情報に基づいて暗号、認証処理を行う。

【００８１】

ステップＳ９０８においてＩＰｓｅｃプロトコル処理部６１２は使用したＳＡのバイト数による有効期限のカウント値を更新し、ＳＡ管理部６１０にカウント値の更新要求を行

う。ＳＡ管理部６１０はカウント値の更新要求を受け付けると該当するＳＡのバイト数カウンタを更新する。

【００８２】

ステップＳ９０９においてソフト有効期限が切れたかを確認する。ソフト有効期限が切れた場合はステップＳ９１０へ進む。ソフト有効期限が切れていないかもしくは、すでに切れていた場合はステップＳ９１１へ進む。

【００８３】

ステップＳ９１０においてＩＰｓｅｃ処理部６０７はＳＡ折衝要求処理を行う。ステップＳ９１０におけるＳＡ折衝要求処理はステップＳ７１７のＳＡ折衝要求処理と共通の処理である。

【００８４】

ステップＳ９１１においてハード有効期限が切れたかを確認する。ハード有効期限が切れた場合はステップＳ９１２へ進む。ハード有効期限が切れていない場合はステップＳ９１３へ進む。

【００８５】

ステップＳ９１２においてＩＰｓｅｃプロトコル処理部はハード有効期限が切れたことをＳＰ、ＳＡテーブル更新管理部６１１に対し通知する。ハード有効期限切れの通知を受けたＳＰ、ＳＡテーブル更新管理部６１１はＩＫＥ処理部６０６にハード有効期限切れを通知し、ＳＡ管理部６１０に対して該当ＳＡの削除要求を行い、ＳＡ管理部６１０はＳＡＤから該当ＳＡを削除する。

【００８６】

ステップＳ９１３においてＩＰｓｅｃプロトコル処理部６１２は受信したＩＰパケットのＩＰアドレスやトランスポート層プロトコル種別、ポート番号等のパケット情報からＳＰ管理部６０９に対してＳＰ検索処理要求を行う。ＳＰ検索処理要求を受け付けたＳＰ管理部６０９はＳＰＤに指定パケット情報に該当するＳＰが登録されているかを検索し、検索結果をＩＰｓｅｃプロトコル処理部６１２に通知する。

【００８７】

ステップＳ９１４において、ＩＰｓｅｃプロトコル処理部６１２はＳＰ管理部６０９から通知された検索結果を判定する。該当するＳＰがありかつ、該ＳＰに指定されたポリシーがＩＰｓｅｃ適用であった場合はステップＳ９１６へ進む。該当するＳＰがなかった場合もしくは、該当するＳＰに指定されたポリシーがＩＰｓｅｃ適用以外であった場合はステップＳ９１５へ進む。

【００８８】

ステップＳ９１５において、ステップＳ３１３でＳＰが見つからなかった場合、暗号通信処理装置のポリシーを確認し、ポリシーが破棄（Ｄｉｓｃａｒｄ）であればステップＳ９１９へ進み、ステップＳ９１９においてパケットを破棄して終了する。ポリシーが通過（Ｂｙｐａｓｓ　ＩＰｓｅｃ）であった場合はステップＳ９１７へ進む。またステップＳ９１３でＳＰが見つかった場合は該ＳＰのポリシーを確認し、ポリシーが破棄であった場合はステップＳ９１９へ進み、パケットを破棄して終了する。またポリシーが通過であった場合はステップＳ９１７へ進む。

【００８９】

ステップＳ９１６において、ＳＰに指定されたポリシーにおいて使用されるＳＡがＩＰｓｅｃプロトコル処理において使用したＳＡをマッチしているかを判定する。使用したＳＡがポリシーにマッチしていなければステップＳ９１９へ進み、パケットを破棄して終了する。マッチしている場合はステップＳ９１７へ進む。

【００９０】

ステップＳ９１７においてＩＰｓｅｃ処理が完了したＩＰパケットのヘッダ解析を行い、ＩＰプロトコルの処理を行う。その後ＩＰ上位プロトコルヘッダを解析してＴＣＰやＵＤＰといったトランスポート層プロトコルの処理を行う。トランスポート層プロトコル処理を終えたパケットデータはアプリケーションへ通知する。

【００９１】
ステップＳ９１８において、アプリケーション処理部６０５は受信したデータからアプリケーション処理を行う。なお、受信したパケットがＩＫＥパケットであった場合、ネットワークプロトコル処理部６０４はＩＫＥ処理部６０６へと通知を行い、ＩＫＥプロトコル処理を行う。
【００９２】
次にＩＰｓｅｃ処理部６０７におけるＳＡ登録処理フローについて説明する。図１０におけるステップＳ１００１において、ＳＰ、ＳＡテーブル更新管理部６１１は登録を行うＳＡに該当する仮ＳＡがあるかを検索する。該当する仮ＳＡが有った場合は該当仮ＳＡタイマを停止する要求をタイマ部６１３に対して行う。その後該当仮ＳＡを削除する。該当仮ＳＡがなかった場合は何もしない。
【００９３】
次に、ステップＳ１００２において不要ＳＡ削除設定処理を行う。
【００９４】
ここで図１１を用いてステップＳ１００２の不要ＳＡ削除設定処理について説明する。
【００９５】
ステップＳ１１０１において、ＳＰ、ＳＡテーブル更新管理部６１１は新規に登録するＳＡのセレクタと同一のＳＡが登録されているかを調べるためＳＡ検索要求を行う。ＳＡ管理部６１０は新規に追加するＳＡのセレクタ等をキーとしてＳＡＤを検索し、結果をＳＰ、ＳＡ管理部６１０に通知する。この際キーとしては、動作モード及び、自局ＩＰアドレス及び、宛先ＩＰアドレス及び、セキュリティプロトコル及び、ＳＡの状態を用いる。ＳＡの状態以外のパラメータは新規に登録するＳＡと同一のセレクタ値である。またＳＡの状態はソフト有効期限切れなのか、ソフト有効期限切れでないのかといった状態である。また動作モードとはＩＰｓｅｃで利用されるトランスポートモード、もしくはトンネルモードのいずれかである。検索の結果、新規に登録するＳＡのセレクタ等と一致するＳＡが登録されていない場合は処理を終了する。登録されている場合はステップＳ１１０２へ進む。
【００９６】
ステップＳ１１０２において検索の結果見つかった該当ＳＡのハード有効期限時間が設定されているか確認する。ハード有効期限時間が設定されていない場合はステップＳ１１０４へ進む。ハード有効期限時間が設定されている場合はステップＳ１１０３へ進む。なお、ステップＳ１１０２の判定処理を行わず、ステップＳ１１０４へ進んでもよい。この場合はハード有効期限時間が設定されているかどうかにかかわらず強制的にハード有効期限時間を設定することとなる。
【００９７】
ステップＳ１１０３において、設定されているハード有効期限時間が閾値以下であるかを判断し、閾値以下である場合は不要ＳＡ削除設定処理を終了する。閾値以下ではない場合はステップＳ１１０４へ進む。なお、閾値はシステムであらかじめ定めた所定の値（所定時間）である。または、ＴＣＰやＩＣＭＰ等を利用して別途計測したＲＴＴ（ラウンドトリップタイム）であってもよい。さらにはＳＡのソフト有効期限が切れてからリキーされたＳＡが登録されるまでの時間であってもよい。その他、ハード有効期限時間と比較するにあたっての適切な任意の値であればよい。
【００９８】
またステップＳ１１０３の判定処理を行わず、ハード有効期限時間が設定されていた場合にはそのまま不要ＳＡ削除設定処理を終了してもよい。
【００９９】
ステップＳ１１０４において、該当するソフト有効期限切れのＳＡのハード有効期限を更新して不要ＳＡ削除設定処理を終了する。更新する際の値はステップＳ１１０３において閾値として示したいずれかの値を用いる。また本値はステップＳ１１０３において比較した値と同一の値であってもよいし、異なっていてもよい。ハード有効期限時間の設定さ

れたＳＡはＳＡ管理部６１０及び、タイマ部６１３の処理によってハード有効期限切れとなる。その後ＳＰ、ＳＡテーブル更新管理部６１１へと通知される。ＳＰ、ＳＡテーブル更新管理部６１１はＳＡ管理部６１０へＳＡ削除要求を行い、ＳＡ管理部６１０はＳＡＤから該当ＳＡを削除する。ステップＳ１１０４の処理では、ハード有効期限時間を設定することによりＳＡ管理部６１０及びタイマ部６１３の処理によってハード有効期限切れを検知しているが、ＳＰ、ＳＡテーブル更新管理部６１１が不要ＳＡ削除タイマをセットし削除要求を行ってもよい。

【０１００】

ステップＳ１１０３においてＳＰ、ＳＡテーブル更新管理部６１１はＳＡ管理部６１０に対して新規ＳＡの追加要求を行う。ＳＡ管理部６１０は新規ＳＡ追加要求を受け付けるとＳＡＤに新規ＳＡを登録して処理を終了する。

【０１０１】

本実施形態によれば、ＳＡを登録する際にソフト有効期限が切れた同一セレクタのＳＡがあるかを判定し、不要ＳＡ削除設定処理を行うことにより、ソフト有効期限の切れたＳＡを削除することが可能となる。これにより、不要なＳＡによってメモリリソースを圧迫することを防ぐことが可能となる。また、一定期間ソフト有効期限切れのＳＡを保持することで、ソフト有効期限切れのＳＡを使用したパケットを破棄せず、本来受信可能なパケットをロストすることを防ぐことが可能となる。またユーザの設定ミスによってソフト有効期限切れのＳＡが残り続けることを防ぐことができる。さらには通信相手のＳＡ削除メッセージによらずソフト有効期限切れのＳＡを削除することができ、例えＩＫＥパケットがネットワーク上でロストした場合であっても適切にＳＡを削除することが可能となる。また不要ＳＡを適切に削除することができるためＩＰｓｅｃパケット送受信時のＳＡＤの検索処理負荷を低減することも可能となる。

【０１０２】

また、上記実施形態を組み合わせてもよい。例えば、旧ＳＡのハード有効期限の時間を第２の実施形態のように設定するとともに、第１の実施形態に用に相手から新たなＳＡを利用したパケットを受信した場合には当該ＳＡに関連付けられた旧ＳＡを削除するようにしてもよい。

【０１０３】

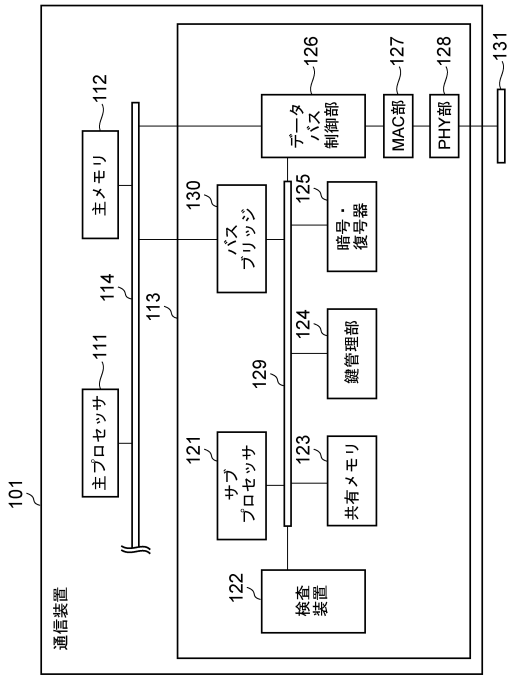
また、上述のフローチャートをコンピュータに実現させるためのプログラムや、当該プログラムを記憶した記憶媒体であっても、同様の作用効果を得ることができる。

【符号の説明】

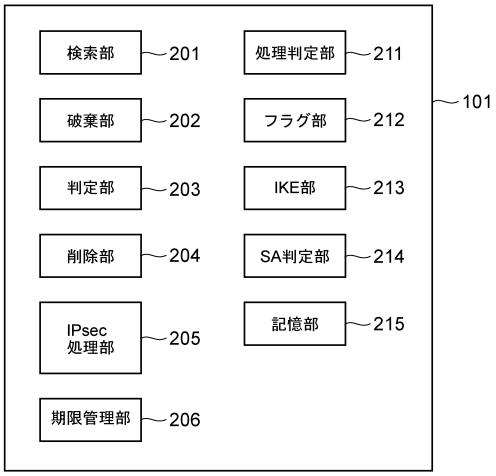
【０１０４】

１０１　通信装置
１１１　主プロセッサ
１１２　主メモリ
１１３　ＴＯＥ
１１４　バス
１２１　サブプロセッサ
１２２　検索装置
１２３　共有メモリ
１２４　鍵管理部
１２５　暗号・復号器
１２６　データバス制御部
１２７　ＭＡＣ部
１２８　ＰＨＹ部
１２９　バス
１３０　バスブリッジ
１３１　ネットワーク

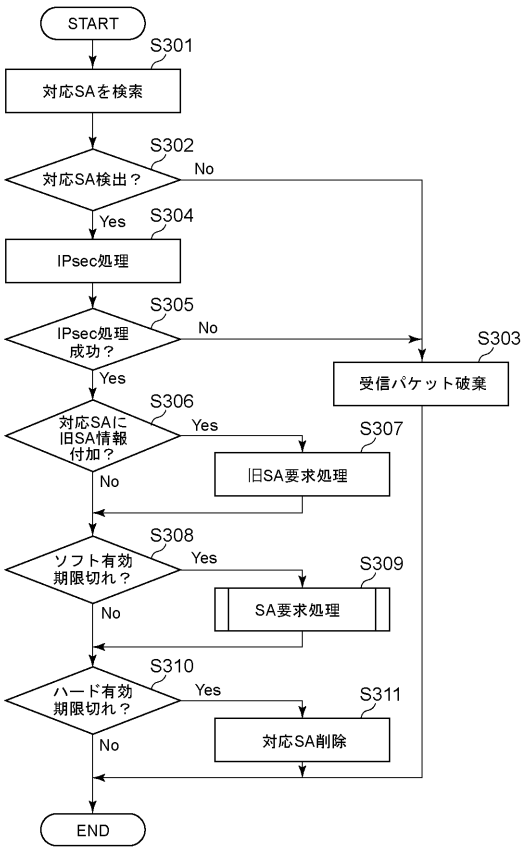
【図１】


通信装置
101
主プロセッサ
111
主メモリ
112
114
113
サブプロセッサ
121
バスブリッジ
130
129
データバス制御部
126
MAC部
127
PHY部
128
131
暗号・復号器
125
鍵管理部
124
共有メモリ
123
検査装置
122

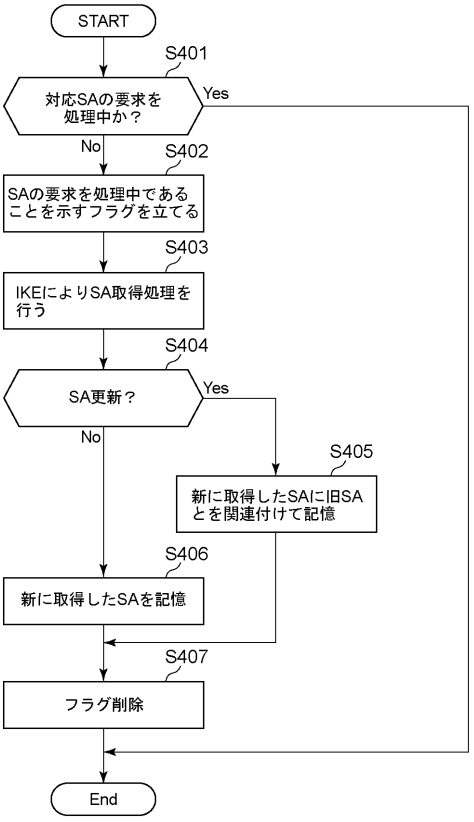
【図２】


検索部 201
破棄部 202
判定部 203
削除部 204
IPsec処理部 205
期限管理部 206
処理判定部 211
フラグ部 212
IKE部 213
SA判定部 214
記憶部 215
101

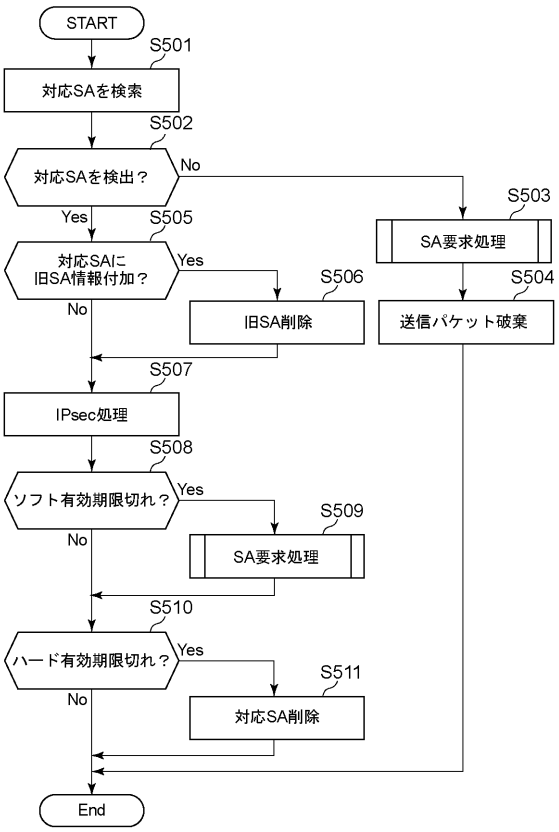
【図３】


START
S301
対応SAを検索
S302
対応SA検出？
No
Yes
S304
IPsec処理
S305
IPsec処理成功？
No
Yes
S303
受信パケット破棄
S306
対応SAに旧SA情報付加？
Yes
No
S307
旧SA要求処理
S308
ソフト有効期限切れ？
Yes
No
S309
SA要求処理
S310
ハード有効期限切れ？
Yes
No
S311
対応SA削除
END

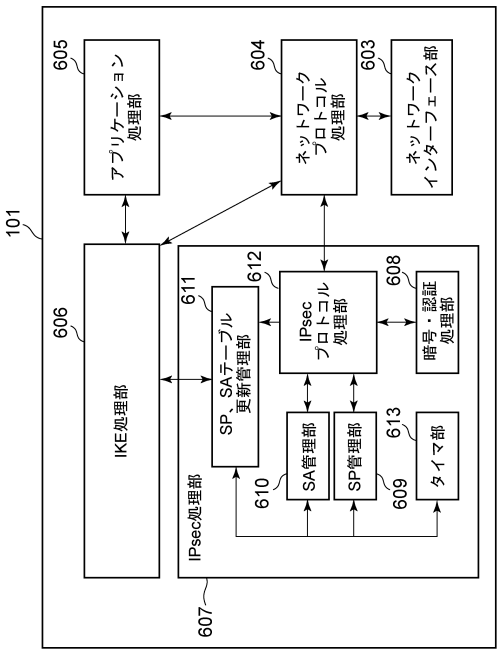
【図４】


START
S401
対応SAの要求を処理中か？
Yes
No
S402
SAの要求を処理中であることを示すフラグを立てる
S403
IKEによりSA取得処理を行う
S404
SA更新？
Yes
No
S405
新に取得したSAに旧SAとを関連付けて記憶
S406
新に取得したSAを記憶
S407
フラグ削除
End

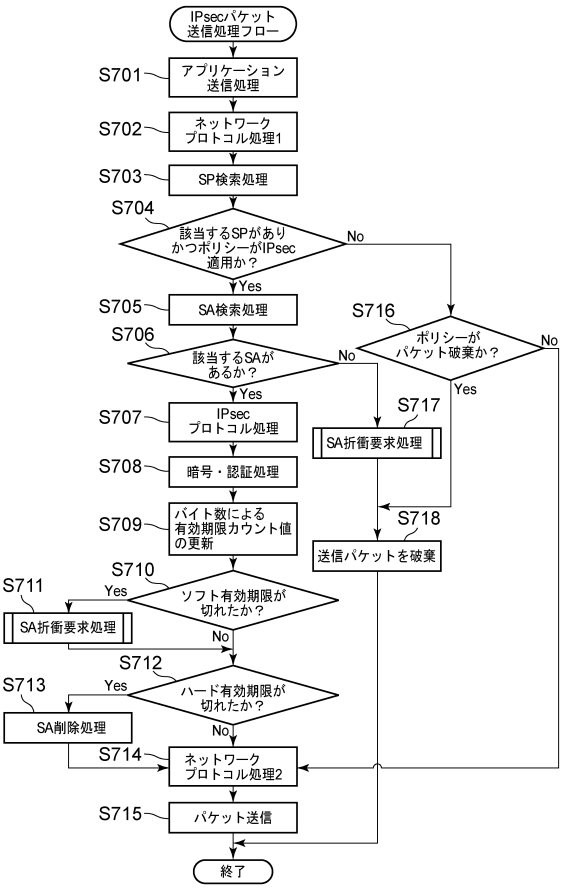
【図５】


START
S501
対応SAを検索
S502
対応SAを検出？
No
S503
SA要求処理
Yes
S505
対応SAに
旧SA情報付加？
Yes
S506
旧SA削除
No
S504
送信パケット破棄
S507
IPsec処理
S508
ソフト有効期限切れ？
Yes
S509
SA要求処理
No
S510
ハード有効期限切れ？
Yes
S511
対応SA削除
No
End

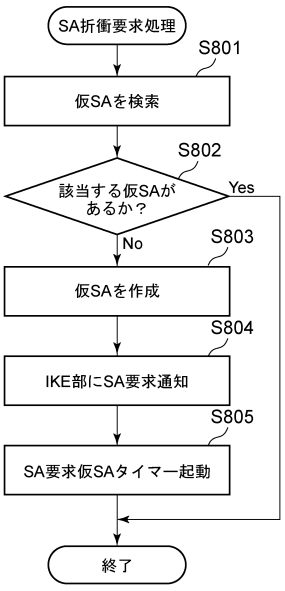
【図６】


101
605
アプリケーション
処理部
604
ネットワーク
プロトコル
処理部
603
ネットワーク
インターフェース部
606
IKE処理部
611
SP、SAテーブル
更新管理部
612
IPsec
プロトコル
処理部
608
暗号・認証
処理部
610
SA管理部
609
SP管理部
613
タイマ部
IPsec処理部
607

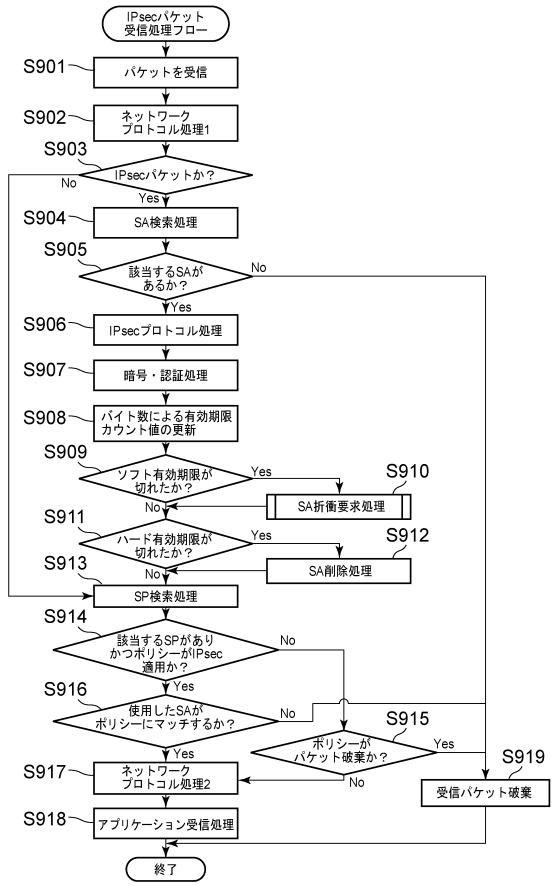
【図７】


IPsecパケット
送信処理フロー
S701
アプリケーション
送信処理
S702
ネットワーク
プロトコル処理1
S703
SP検索処理
S704
該当するSPがあり
かつポリシーがIPsec
適用か？
No
Yes
S705
SA検索処理
S716
ポリシーが
パケット破棄か？
No
S706
該当するSAが
あるか？
No
Yes
S707
IPsec
プロトコル処理
S717
SA折衝要求処理
S708
暗号・認証処理
S709
バイト数による
有効期限カウント値
の更新
S718
送信パケットを破棄
S710
ソフト有効期限が
切れたか？
Yes
S711
SA折衝要求処理
No
S712
ハード有効期限が
切れたか？
Yes
S713
SA削除処理
No
S714
ネットワーク
プロトコル処理2
S715
パケット送信
終了

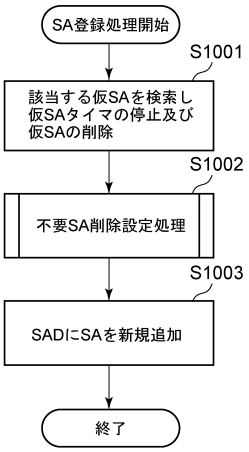
【図８】


SA折衝要求処理
S801
仮SAを検索
S802
該当する仮SAが
あるか？
Yes
No
S803
仮SAを作成
S804
IKE部にSA要求通知
S805
SA要求仮SAタイマー起動
終了

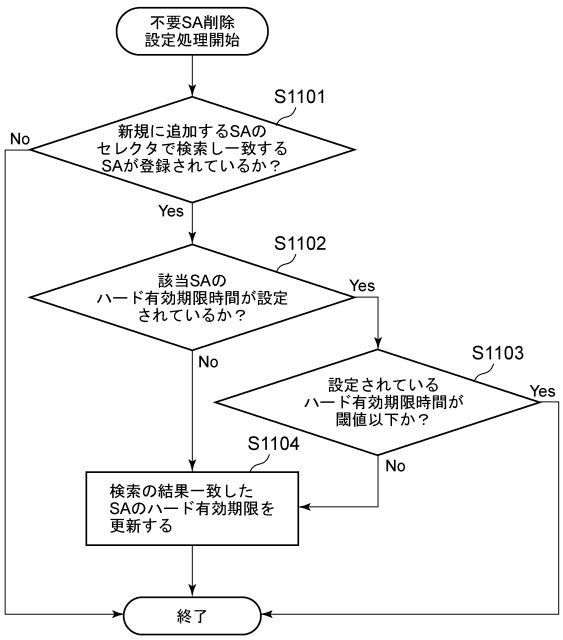
【図９】


IPsecパケット
受信処理フロー
S901
パケットを受信
S902
ネットワーク
プロトコル処理1
S903
IPsecパケットか？
No
Yes
S904
SA検索処理
S905
該当するSAが
あるか？
No
Yes
S906
IPsecプロトコル処理
S907
暗号・認証処理
S908
バイト数による有効期限
カウント値の更新
S909
ソフト有効期限が
切れたか？
Yes
S910
SA折衝要求処理
No
S911
ハード有効期限が
切れたか？
Yes
S912
SA削除処理
No
S913
SP検索処理
S914
該当するSPがあり
かつポリシーがIPsec
適用か？
No
Yes
S916
使用したSAが
ポリシーにマッチするか？
No
Yes
S915
ポリシーが
パケット破棄か？
Yes
No
S919
受信パケット破棄
S917
ネットワーク
プロトコル処理2
S918
アプリケーション受信処理
終了

【図１０】


SA登録処理開始
S1001
該当する仮SAを検索し
仮SAタイマの停止及び
仮SAの削除
S1002
不要SA削除設定処理
S1003
SADにSAを新規追加
終了

【図１１】


不要SA削除
設定処理開始
S1101
新規に追加するSAの
セレクタで検索し一致する
SAが登録されているか？
No
Yes
S1102
該当SAの
ハード有効期限時間が設定
されているか？
Yes
No
S1103
設定されている
ハード有効期限時間が
閾値以下か？
Yes
No
S1104
検索の結果一致した
SAのハード有効期限を
更新する
終了

フロントページの続き

(56)参考文献 特開２００７－１０４３１０（ＪＰ，Ａ）
特開２００２－２１７８９６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｌ　　９／１４