【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成28年3月10日(2016.3.10)

【公開番号】特開2014-140132(P2014-140132A)
【公開日】平成26年7月31日(2014.7.31)
【年通号数】公開・登録公報2014-041
【出願番号】特願2013-8621(P2013-8621)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ

【手続補正書】
【提出日】平成28年1月20日(2016.1.20)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【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、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に用いる第１の暗号鍵を記憶部に記憶させる記憶手段と、
前記第１の暗号鍵の有効期限に応じて、前記第１の暗号鍵から第２の暗号鍵に更新する更新手段と、
前記更新手段により前記第２の暗号鍵に更新されてから第１の所定時間より前に前記第１の暗号鍵を削除する設定ではないことを判定する判定手段と、
前記判定手段により前記第１の所定時間より前に前記第１の暗号鍵を削除する設定ではないと判定された場合、前記第２の暗号鍵に更新されてから前記第１の所定時間よりも短い第２の所定時間が経過すると前記第１の暗号鍵を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１６】
前記第２の暗号鍵に更新されてから前記第２の所定時間が経過するまでを計測するタイマを更に有し、
前記タイマにより前記第２の所定時間が計測されると、前記削除手段は前記第１の暗号鍵を削除する
ことを特徴とする請求項１５に記載の通信装置。
【請求項１７】
前記他の通信装置との間のラウンドトリップタイム（ＲＴＴ）を計測する計測手段を更に有し、
前記第２の所定時間は、前記計測手段により計測されたＲＴＴであることを特徴とする請求項１５または１６に記載の通信装置。
【請求項１８】
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、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１９】
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に用いる第１の暗号鍵を記憶部に記憶させる記憶工程と、
前記第１の暗号鍵の有効期限に応じて、前記第１の暗号鍵から第２の暗号鍵に更新する更新工程と、
前記更新工程において前記第２の暗号鍵に更新されてから第１の所定時間より前に前記第１の暗号鍵を削除する設定ではない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１の所定時間より前に前記第１の暗号鍵を削除する設定ではないと判定された場合、前記第２の暗号鍵に更新されてから前記第１の所定時間よりも短い第２の所定時間が経過すると前記第１の暗号鍵を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２０】
コンピュータを、請求項１から１７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。
【手続補正２】

【補正対象書類名】明細書
【補正対象項目名】０００６
【補正方法】変更
【補正の内容】
【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。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００７
【補正方法】変更
【補正の内容】
【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、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。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０００８
【補正方法】変更
【補正の内容】
【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記憶するメモリを有効利用することができる。