【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23年7月7日(2011.7.7)

【公開番号】特開2010-57122(P2010-57122A)
【公開日】平成22年3月11日(2010.3.11)
【年通号数】公開・登録公報2010-010
【出願番号】特願2008-222554(P2008-222554)
【国際特許分類】
Ｈ０４Ｌ　9/36　(2006.01)
Ｈ０４Ｌ　12/22　(2006.01)
Ｈ０４Ｌ　29/06　(2006.01)
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６８５
Ｈ０４Ｌ　12/22
Ｈ０４Ｌ　13/00　３０５Ａ
Ｈ０４Ｌ　9/00　６７５Ａ

【手続補正書】
【提出日】平成23年5月24日(2011.5.24)
【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】
通信パケットを送受信する通信手段と、
ネットワークプロトコルの前半処理及び後半処理を行うネットワークプロトコル処理手段と、
暗号化処理、復号化処理、又は認証処理のうち少なくとも一つを行う暗復号認証処理手段と、
前記暗復号認証処理手段から、暗号化処理、復号化処理、又は認証処理のうち一つの処理が完了しているパケットの処理結果を取得し、前記パケットのネットワークプロトコルの後半処理と次のパケットのネットワークプロトコルの前半処理とを連続して行うように前記ネットワークプロトコル処理手段を制御する暗復号認証処理制御手段と、
を備えるセキュア通信装置。
【請求項２】
前記暗復号認証処理制御手段は、前記ネットワークプロトコル処理手段から、ネットワークプロトコルの前半処理を終えた次のパケットの暗復号認証処理を依頼された際、同じＣＰＵコンテキストにより、直前に暗復号認証処理が完了している１つ前のパケットの処理結果を前記暗復号認証処理手段から取得し、１つ前のパケットのネットワークプロトコルの後半処理を前記ネットワークプロトコル処理手段が処理するように制御する請求項１記載のセキュア通信装置。
【請求項３】
前記暗復号認証処理制御手段は、１つ前のパケットの処理結果を前記暗復号認証処理手段から取得した後、１つ前のパケットのネットワークプロトコル後半処理を前記ネットワークプロトコル処理手段において処理する前に、同じＣＰＵコンテキストにより、次のパケットの暗復号認証処理を前記暗復号認証処理手段に対して依頼する請求項１記載のセキ

ュア通信装置。
【請求項４】
前記暗復号認証処理制御手段は、前記暗復号認証処理手段からの完了ハードウェア割り込みコンテキスト、又は、ソフトウェア遅延割り込みコンテキストにより、処理が完了した１つ前のパケットの処理結果を前記暗復号認証処理手段から取得する暗復号認証後半処理を行い、ネットワークプロトコルの前半処理が完了した次のパケットがある場合は、同じＣＰＵコンテキストにより、次のパケットの暗復号認証処理を前記暗復号認証処理手段に依頼する暗復号認証前半処理を行い、１つ前のパケットのネットワークプロトコル後半処理を前記ネットワークプロトコル処理手段が処理するように制御する請求項１記載のセキュア通信装置。
【請求項５】
前記暗復号認証処理制御手段は、前記各処理を、(i)次のパケットのネットワークプロトコルの前半処理、(ii)１つ前のパケットの暗復号認証後半処理、(iii)次のパケットの暗復号認証前半処理、及び(iv)１つ前のパケットのネットワークプロトコルの後半処理、の順に並び替えて前記ネットワークプロトコル処理手段と前記暗復号認証処理手段とを並列処理させる請求項４記載のセキュア通信装置。
【請求項６】
ネットワークプロトコルの前半処理が完了したパケットを、パケット毎に優先度を設定し、暗復号認証処理に必要なパラメータとともに暗復号認証リクエストとして蓄積し、該暗復号認証リクエストを優先度順に前記暗復号認証処理手段に受け渡す暗復号認証リクエスト蓄積手段をさらに備える請求項１記載のセキュア通信装置。
【請求項７】
前記ネットワークプロトコルの前半処理は、ＩＰプロトコル処理の一部やそれ以下のレイヤ処理を含む下位レイヤ処理であり、前記ネットワークプロトコルの後半処理は、ＴＣＰプロトコル処理及びＩＰプロトコル処理の一部を含む上位レイヤ処理である請求項１記載のセキュア通信装置。
【請求項８】
通信手段が、送受信パケットをネットワークデバイス、または上位レイヤから取得するステップと、
ネットワークプロトコル処理手段が、前記取得したパケットに対してネットワークプロトコルの前半処理を行うネットワークプロトコル処理ステップと、
暗復号認証処理手段が、前記ネットワークプロトコル処理されたパケットに対して、暗号化処理、復号化処理、又は認証処理のうち少なくとも一つを行う暗復号認証処理ステップと、
暗復号認証処理制御手段が、前記暗復号認証処理の処理結果パケットを取得し、処理結果パケットに対して前記パケットのネットワークプロトコルの後半処理と次のパケットのネットワークプロトコルの前半処理とを連続して行うように制御する制御ステップとを有するセキュア通信方法。
【請求項９】
前記制御ステップでは、前記暗復号認証処理制御手段が、ネットワークプロトコルの前半処理を終えた次のパケットの暗復号認証処理を依頼された際、同じＣＰＵコンテキストにより、直前に暗復号認証処理が完了している１つ前のパケットの処理結果を取得し、前記ネットワークプロトコル処理ステップでは、ネットワークプロトコル処理手段が、１つ前のパケットのネットワークプロトコルの後半処理を処理する請求項８記載のセキュア通信方法。
【請求項１０】
前記制御ステップでは、前記暗復号認証処理制御手段が、１つ前のパケットの処理結果を取得した後、１つ前のパケットのネットワークプロトコル後半処理を前記ネットワークプロトコル処理ステップにおいて処理する前に、同じＣＰＵコンテキストにより、次のパケットの暗復号認証処理を前記暗復号認証処理手段に対して依頼する請求項８記載のセキ

ュア通信方法。
【請求項１１】
前記制御ステップでは、前記暗復号認証処理制御手段が、前記暗復号認証処理ステップからの完了ハードウェア割り込みコンテキスト、又は、ソフトウェア遅延割り込みコンテキストにより、処理が完了した１つ前のパケットの処理結果を前記暗復号認証処理ステップから取得する暗復号認証後半処理を行い、ネットワークプロトコルの前半処理が完了した次のパケットがある場合は、同じＣＰＵコンテキストにより、次のパケットの暗復号認証処理を前記暗復号認証処理手段に依頼する暗復号認証前半処理を行い、
前記ネットワークプロトコル処理ステップでは、前記ネットワークプロトコル処理手段が、１つ前のパケットのネットワークプロトコル後半処理を処理する請求項８記載のセキュア通信方法。
【請求項１２】
前記制御ステップでは、前記暗復号認証処理制御手段が、前記各処理を、(i)次のパケットのネットワークプロトコルの前半処理、(ii)１つ前のパケットの暗復号認証後半処理、(iii)次のパケットの暗復号認証前半処理、及び(iv)１つ前のパケットのネットワークプロトコルの後半処理、の順に並び替える請求項１１記載のセキュア通信方法。
【請求項１３】
暗復号認証リクエスト蓄積手段が、ネットワークプロトコルの前半処理が完了したパケットを、パケット毎に優先度を設定し、暗復号認証処理に必要なパラメータとともに暗復号認証リクエストとして蓄積し、該暗復号認証リクエストを優先度順に前記暗復号認証処理ステップに受け渡すステップをさらに備える請求項８記載のセキュア通信方法。
【請求項１４】
請求項８記載のセキュア通信方法の各ステップをコンピュータに実行させるためのプログラム。