(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2010 年 3 月 4 日(04.03.2010)

PCT

(10) 国際公開番号
WO 2010/023951 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2009/004239

(22) 国際出願日: 2009 年 8 月 28 日(28.08.2009)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2008-222554 2008 年 8 月 29 日(29.08.2008) JP

(71) 出願人 (米国を除く全ての指定国について): パナソニック株式会社 (PANASONIC CORPORATION) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 山田　一成 (YAMADA, Kazushige). 千賀　諭(SENGA, Satoshi).

(74) 代理人: 鷲田　公一 (WASHIDA, Kimihito); 〒2060034 東京都多摩市鶴牧１丁目２４－１新都市センタービル５階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

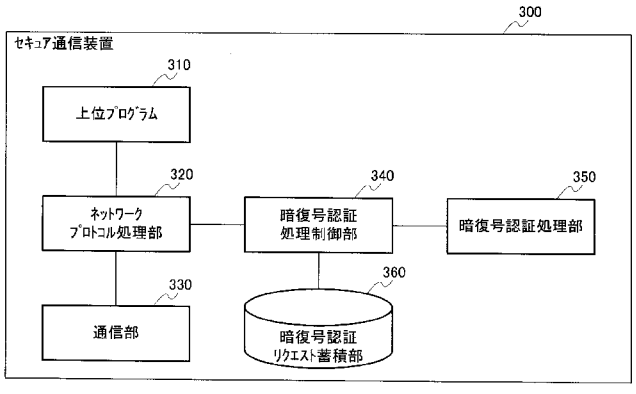
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告（条約第 21 条(3)）
— 補正された請求の範囲（条約第 19 条(1)）

(54) **Title**: SECURE COMMUNICATION DEVICE, SECURE COMMUNICATION METHOD, AND PROGRAM

(54) 発明の名称 : セキュア通信装置、セキュア通信方法及びプログラム

[図9]



300 SECURE COMMUNICATION DEVICE
310 HIGHER-LEVEL PROGRAM
320 NETWORK PROTOCOL PROCESSING UNIT
330 COMMUNICATION UNIT
340 ENCRYPTION/DECRYPTION AUTHENTICATION CONTROL UNIT
360 ENCRYPTION/DECRYPTION AUTHENTICATION REQUEST STORAGE UNIT
350 ENCRYPTION/DECRYPTION AUTHENTICATION UNIT

(57) **Abstract**: A secure communication device for high-speed encryption/decryption authentication including network stack processing. An encryption/decryption authentication control unit (340) of the secure communication device (300) acquires the result of processing of the encrypted/decrypted or authenticated previous packet from an encryption/decryption authentication unit (350) and controls a network protocol processing unit (320) so that the second half of the processing of the network protocols of the previous packet and the first half of the processing of the network protocols of the current packet are continuously performed.

(57) 要約: ネットワークスタック処理を含む高速暗復号認証処理を行うことができるセキュア通信装置。このセキュア通信装置３００の暗復号認証処理制御部３４０は、暗復号認証処理部３５０から、暗復号処理又は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、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ネットワークプロトコル処理部３２０を制御する。

WO 2010/023951 A1

明　細　書

発明の名称 ：

セキュア通信装置、セキュア通信方法及びプログラム

技術分野

[0001] 本発明は、セキュア通信装置、セキュア通信方法及びプログラムに関する。

背景技術

[0002] ネットワーク上を流れる情報を暗号化するための手段としてＩＰセキュア通信が一般的である。ＩＰｖ６においては暗号化通信を行うＩＰｓｅｃが標準機能としてＲＦＣ（Request For Comment）において規格化されている。

[0003] ＩＰセキュア通信を行うには高負荷処理である暗復号認証処理をリアルタイムに実行する必要がある。このため、ＩＰセキュア通信では、サーバやルータ等のように特別に高速化が求められる場合や、組み込み機器のように非力なマシンで実現する場合、暗号認証処理を行う特別なハードウェア（以後、ＨＷエンジンと呼ぶ）を用いて実現することがある（例えば、特許文献１参照）。なお、以後ハードウェアのことをＨＷと略記する場合がある。

[0004] 通常、ＨＷエンジンが暗復号認証処理を行うためには、ソフトウェアによるＨＷエンジンへのセットアップなどの事前処理と、ＨＷエンジンから演算結果などを取得する事後処理が必要である。したがって、あらかじめ１つめのパケットの事後処理を済まさなければ、２つめのパケットの事前処理を行えないことが一般的である。

[0005] 特許文献２には、暗復号認証エンジン内に、暗復号ユニットと複数の認証ユニットとを搭載し、それらのユニットをパイプライン処理で動作させることで、１つめのパケットに対する、暗復号ユニットもしくは認証ユニットのどちらか一方における処理が完了した時点で、２つめに対するパケットの事前処理を行えるようにする方法が提案されている。

[0006] 図１は、ＨＷ暗号認証を行う場合の通信スタック処理を説明する図であり

、図１Ａは通常の通信スタック処理を示し、図１ＢはＨＷ暗号認証を行う場合の通信スタック処理を示す。

[0007] 図１において、セキュア通信装置１０は、レイヤ処理１及びレイヤ処理２を実行する通信スタック部１１と、受信／送信情報を一時的に格納するバッファ１２と、ＨＷエンジンにＨＷ処理リクエストを発行して暗号認証処理を実行する暗号認証処理部１３とを備えて構成される。

[0008] 図１Ａに示すように、通常の通信スタック処理では、通信スタック部１１は、送信指示又は受信割込みによりバッファ１２を介してレイヤ処理１及びレイヤ処理２を実行する。

[0009] 図１Ｂに示すように、ＨＷ暗号認証を行う場合には、通信スタック部１１は、送信指示又は受信割込みを受けると、レイヤ処理１で暗号認証処理部１３に処理を指示し、暗号認証処理部１３は後述するＨＷ暗復号認証処理部１４（図２参照）にＨＷ処理リクエストを発行する。ＨＷ暗復号認証処理部１４（図２参照）は、このＨＷ処理リクエストを受け取り、ＨＷによる暗復号認証処理を行って暗号認証処理完了の遅延処理を、暗号認証処理部１３を介して通信スタック部１１に返す。通信スタック部１１は、暗号認証処理部１３による暗号認証処理結果を受け取り、バッファ１２を介してレイヤ処理２を実行する。

[0010] 通信スタック部１１は、レイヤ処理１及びレイヤ処理２による送受信処理中、ＨＷ暗復号認証処理部１４（図２参照）による暗復号認証処理を行う場合、前半処理と後半処理を非同期に処理する。通信スタック部１１は、前半処理と後半処理とを非同期に処理することで、ＨＷ暗復号認証処理部１４（図２参照）や図示しないネットワークデバイスの利用効率を高めることができる。

[0011] 図２は、上記暗号認証処理部１３の詳細な構成を示す図である。図３は、上記暗号認証処理部１３及びＨＷ暗復号認証処理部１４の動作タイミングを示すタイミングチャートである。図２及び図３中、番号(1)－(7)は処理の流れを説明するための符号である。

[0012] 図２において、セキュア通信装置１０は、通信スタック部１１と、暗号認証処理部１３と、ＨＷエンジンにより暗復号認証処理を実行するＨＷ暗復号認証処理部１４とを備えて構成される。また、暗号認証処理部１３は、リクエスト制御部２１、ＨＷ前処理部２２、ＨＷ後処理部２３、及びキュー２４を備える。

[0013] リクエスト制御部２１は、通信スタック部１１のレイヤ処理１により暗号認証処理が指示されると、そのリクエストをキュー２４に積む（(1)参照）。リクエスト制御部２１は、ＨＷビジーでない場合にはＨＷ前処理部２２にＨＷ前処理を指示する（(2)参照）。

[0014] ＨＷ前処理部２２は、キュー２４からリクエストを取得し（(3)参照）、取得したリクエストに従ってＨＷ暗復号認証処理部１４にＨＷ処理リクエストを発行する（(4)参照）。

[0015] ＨＷ暗復号認証処理部１４は、暗号認証処理部１３からのＨＷ処理リクエストに従ってＨＷによる暗復号認証処理を行う。ＨＷ暗復号認証処理部１４は、該当ＨＷ処理リクエストによる暗復号認証処理が終わると、ＨＷ割込み信号を発生し（図３参照）、このＨＷ割込み信号に基づく遅延処理開始指示をＨＷ後処理部２３に出力する（(5)参照）。

[0016] 暗号認証処理部１３は、ＨＷ暗復号認証処理部１４からの遅延処理開始指示を受けてＨＷ後処理を開始する。図３に示すように、レイヤ処理１から見て、ＨＷ前処理部２２によるＨＷ前処理が終了してＨＷ後処理部２３がＨＷ後処理を起動するまでの時間は、ＨＷ後処理部２３がＨＷ後処理を行えない、利用できない時間となる。暗号認証処理部１３は、ＨＷ暗復号認証処理部１４からＨＷ処理結果を取得して（(6)参照）ＨＷ後処理を実行する。暗号認証処理部１３は、ＨＷ後処理を終了すると、レイヤ処理２に後半処理を指示する。暗号認証処理部１３は、レイヤ処理２を実行する。これにより、図３に示すように、キュー２４から取得したリクエストによる暗号認証処理が終わり、同様にして次のＨＷ前処理が実行される。

先行技術文献

特許文献

[0017] 特許文献1：特表２００５－５０３６９９号公報

特許文献2：米国特許第６，９８３，３６６号明細書

発明の概要

発明が解決しようとする課題

[0018] しかしながら、このような従来のＨＷ暗号認証方法にあっては、通信スタック部１１が、前半処理と後半処理とを非同期に処理することで、ＨＷ暗復号認証処理部１４やネットワークデバイスの利用効率を高めることができるものの、事前処理の前に行うべきネットワークスタック処理（以下、スタック前半処理という）と、事後処理の後に行うべきネットワークスタック処理（以下、スタック後半処理という）とが、暗復号認証処理（事前処理、ＨＷエンジン処理、及び事後処理）で分断されるため、２つの処理は不連続で実行される。

[0019] ２つの処理が不連続で実行されると、パケットのバースト受信時に、優先度の高いスタック前半処理のみが連続実行されて後半処理がいつまでも実行されなくなってしまうことがある。このため、ＣＰＵやＨＷエンジンの負荷に偏りが生じ、結果的にパケット伝送のスループットが低下してしまう問題がある。

[0020] また、事後処理やスタック後半処理を実行するためのソフトウェア遅延割り込みを起床する必要があるので、余計なオーバーヘッドが発生するという問題もある。

[0021] 例えば、図２及び図３に示すように、ＨＷによるＩＰＳｅｃ処理では、レイヤ処理１とレイヤ処理２のコンテキストが分断されているため、レイヤ処理１のコンテキストが終了してからレイヤ処理２のコンテキストが開始されるまで間が開き、パフォーマンスが低下してしまう。また、図３に示すように、遅延処理開始指示（(5)参照）によってＨＷ後処理部２３が起動するまで次のパケットのリクエストを送信することができず、ＨＷ暗復号認証処理部１４の利用効率が下がってパフォーマンスが低下したり、キューがあふれて

しまう問題がある。

[0022] 本発明は、上記に鑑みてなされたものであり、処理分断によるオーバーヘッドなしに、ＣＰＵやＨＷエンジンの負荷の偏りが起こりにくい暗復号処理又は認証処理を行うことができ、ネットワークスタック処理を含む高速暗復号認証処理を行うことができるセキュア通信装置、セキュア通信方法及びプログラム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

[0023] 本発明のセキュア通信装置は、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、暗復号処理又は認証処理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、暗復号処理又は認証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、を備える構成を採る。

[0024] 本発明の暗号化情報通信方法は、通信パケットを送受信するステップと、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ステップと、暗復号処理又は認証処理を行う暗復号認証処理ステップと、暗復号処理又は認証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制御する制御ステップとを有する。

[0025] また他の観点から、本発明は、上記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である。

発明の効果

[0026] 本発明によれば、同じコンテキストで上位レイヤまでの処理を実現することにより、処理分断によるオーバーヘッドなしに、ＣＰＵやＨＷエンジンの負荷の偏りが起こりにくい暗復号処理又は認証処理を行うことができ、セキ

ュア通信における、ネットワークプロトコル処理も含めた暗復号処理又は認証処理の高速化を実現することができる。

図面の簡単な説明

[0027] [図1]従来のＨＷ暗号認証を行う場合の通信スタック処理を説明する図

[図2]従来のセキュア通信装置の暗号認証処理部の詳細な構成を示す図

[図3]従来のセキュア通信装置の暗号認証処理部及びＨＷ暗復号認証処理部の動作タイミングを示すタイミング図

[図4]本発明の基本的な考え方を説明するプロトコルレベルで記述した全体構成図

[図5]本発明の基本的な考え方を説明する負荷の平準化を示す図

[図6]本発明の基本的な考え方を説明する負荷の平準化を用いた高速制御方式を示す図

[図7]本発明の実施の形態１に係るセキュア通信装置の構成を示す図

[図8]上記実施の形態１に係るセキュア通信装置の暗号認証処理部及びＨＷ暗復号認証処理部の動作タイミングを示すタイミング図

[図9]本発明の実施の形態２に係るセキュア通信装置の構成を示すブロック図

[図10]上記実施の形態２に係るセキュア通信装置が受信側として機能する場合のセキュア通信処理時の動作を説明する制御シーケンス図

[図11]上記実施の形態２に係るセキュア通信装置によるセキュア通信処理時の動作を説明する制御シーケンス図

[図12]本発明の実施の形態３に係るセキュア通信装置が受信側として機能する場合のセキュア通信処理時の動作を説明する制御シーケンス図

[図13]上記実施の形態３に係るセキュア通信装置によるセキュア通信処理時の動作を説明する制御シーケンス図

発明を実施するための形態

[0028] 以下、本発明の実施の形態について図面を参照して詳細に説明する。

[0029] （原理説明）

まず、本発明の基本的な考え方について説明する。

[0030] 図４乃至図６は、本発明の基本的な考え方を説明する図であり、図４はプロトコルレベルで記述した全体構成を、図５は負荷の平準化を、図６は負荷の平準化を用いた高速制御方式をそれぞれ示す。

[0031] 図４において、セキュア通信装置１００は、ＩＰセキュアプロトコル１１０、クリプトマネージャ（Crypto Manager）１２０、及びHW暗復号認証エンジン１３０を備えて構成される。

[0032] ＩＰセキュアプロトコル１１０は、アプリケーション／ミドルソフトウェア（application／middle software）を実行するＩＰ層以上の処理（例えばレイヤ処理１）と、ネットワークデバイスに接続されＩＰ層以下の処理（例えばレイヤ処理２）とを有する。

[0033] クリプトマネージャ１２０は、上記ＩＰ層以下の処理によりHWエンジンを初期化するためのリクエストを生成するリクエスト生成HW初期化部１２１と、HW暗復号認証結果を取得・格納し、上記ＩＰ層以上の処理に渡すHW後処理結果格納部１２２とを備えている。クリプトマネージャ１２０は、後述する負荷の平準化と、この負荷の平準化を用いた高速制御方式を用いることにより、事前処理の前に行うべきネットワークスタック処理（スタック前半処理）と、事後処理の後に行うべきネットワークスタック処理（スタック後半処理）とを、暗復号認証処理（事前処理、HWエンジン処理、及び事後処理）で分断することなく、２つの処理を連続して実行する。すなわち、クリプトマネージャ１２０は、ＩＰセキュアプロトコル１１０のＩＰ層以上の処理（例えばレイヤ処理１）とＩＰ層以下の処理（例えばレイヤ処理２）に対して、前記図２の従来例の暗号認証処理部１３のように、HW前処理部２２とHW後処理部２３とを非同期で動作させる構成ではなく、２つの処理を連続して実行する。

[0034] HW暗復号認証エンジン１３０は、クリプトマネージャ１２０のリクエスト生成HW初期化部１２１からのHW処理リクエストに従って、通信相手に送信する平文パケットを、ＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）、３ＤＥＳ（Ｔｒｉｐｌｅ Ｄａｔａ Ｅｎｃｒｙｐｔｉ

ｏｎ Ｓｔａｎｄａｒｄ）等の暗号アルゴリズムで暗号化するか、ＳＨＡ－１（Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ－１）等のアルゴリズムを用いて認証情報の付与をするか、暗号化と認証情報の付与の両方をおこなう。同様に、通信相手から受信した暗号パケットを、付与された認証情報を元に改ざんチェックをおこなうか、暗号化されたパケットを復号化するか、改ざんチェックと復号化の両方をおこなう。HW暗復号認証エンジン１３０は、該当HW処理リクエストによるHW暗復号認証処理が終わると、暗復号認証結果をクリプトマネージャ１２０のHW後処理結果格納部１２２に出力する。

[0035] 以下、上述のように構成されたセキュア通信装置１００の動作について説明する。

[0036] 図４中、番号(1)－(3)で示される矢印は処理の流れを示す。

[0037] 図４に示すように、クリプトマネージャ１２０は、ＩＰセキュアプロトコル１１０のＩＰ層以上の処理（例えばレイヤ処理１）とＩＰ層以下の処理（例えばレイヤ処理２）に対して、スタック前半処理とスタック後半処理とを、暗復号認証処理（事前処理、HWエンジン処理、事後処理）で分断することなく連続して実行する。

[0038] 具体的には、ＩＰセキュアプロトコル１１０は、ＩＰ層以下の処理がネットワークデバイスからの優先度の高い処理をクリプトマネージャ１２０のリクエスト生成HW初期化部１２１に渡す。リクエスト生成HW初期化部１２１は、ＩＰ層以下の処理から渡された優先度の高い要求を基に、HWエンジンを初期化するためのリクエストを生成する。ここまでの処理が、(1)ネットワークプロトコルの前半処理（以下、前半処理という）に相当する。

[0039] HW暗復号認証エンジン１３０は、クリプトマネージャ１２０のリクエスト生成HW初期化部１２１からのHW処理リクエストに従ってHWによる暗復号認証処理を行い、暗復号認証結果をクリプトマネージャ１２０のHW後処理結果格納部１２２に出力する。ここでの処理が、(2)HW暗復号認証処理に相当する。

[0040] ＨＷ後処理結果格納部１２２は、ＨＷ暗復号認証結果を取得・格納し、ＩＰセキュアプロトコル１１０のＩＰ層以上の処理に渡し、このＩＰ層以上の処理はアプリケーション／ミドルソフトウェアの要求に基づくＩＰ層以上の処理を実行する。ここまでの処理が、(3)ネットワークプロトコルの後半処理（以下、後半処理という）に相当する。

[0041] 図５は、負荷の平準化を説明する図であり、図５Ａは特別な制御を行わない場合の図４の(1)前半処理、(2)ＨＷ暗復号認証処理、(3)後半処理を示し、図５Ｂは負荷の平準化を行った場合の図４の(1)前半処理、(2)ＨＷ暗復号認証処理、(3)の後半処理を示す。また図５中、「」内の数字は、パケットの到着順序を示す。また、番号１５０の破線矢印は、ネットワークプロトコルの前半処理のタイミングを、番号１５１の破線矢印は、ＨＷ割込みコンテキストに基づく遅延処理開始指示をそれぞれ示す。

[0042] まず、図５Ａの特別な制御を行わない場合には、リクエスト生成ＨＷ初期化部１２１は、(1)前半処理でパケット「１」－「４」について優先度の高い前半処理を行い、パケット「１」－「４」のリクエストをＨＷ暗復号認証エンジン１３０に発行する。ＨＷ暗復号認証エンジン１３０は、(2)ＨＷ暗復号認証処理で、発行されたパケット「１」－「４」のリクエストのうちパケット「１」についてのリクエストのＨＷ暗復号認証処理を行う。ＨＷ後処理結果格納部１２２は、(3)ネットワークプロトコルの後半処理でパケット「１」についてＨＷ暗復号認証結果を取得・格納し、ＩＰ層以上の処理に渡す。図示は省略しているが、その後、ＨＷ暗復号認証エンジン１３０は、(2)ＨＷ暗復号認証処理で、パケット「２」－「４」についてのリクエストのＨＷ暗復号認証処理を順次行い、ＨＷ後処理結果格納部１２２は、(3)後半処理でパケット「２」－「４」についてＨＷ暗復号認証結果を取得・格納する。図５Ａに示すように、パケット「１」－「４」についてここまでの処理が終了してはじめて、リクエスト生成ＨＷ初期化部１２１は、(1)前半処理で次のパケット「５」－「７」のリクエストをＨＷ暗復号認証エンジン１３０に発行することができる。

[0043] このように、図４の構成を採ったとしても図５Ａのように特別な制御を行わない場合には、ビットレート低下や負荷上昇による再生品質低下が考えられる。

[0044] そこで、図４の構成に加え図５Ｂに示す負荷の平準化を行う。

[0045] 図５Ｂの負荷の平準化では、まず、ＩＰセキュアプロトコル１１０とリクエスト生成ＨＷ初期化部１２１は、(1)前半処理でパケット「１」のネットワークプロトコルの前半処理（ＩＰ層以下の処理）を行い、パケット「１」のリクエストをＨＷ暗復号認証エンジン１３０に発行する。ＨＷ暗復号認証エンジン１３０は、(2)ＨＷ暗復号認証処理で、発行されたパケット「１」のリクエストのＨＷ暗復号認証処理を行う。ＩＰセキュアプロトコル１１０とＨＷ後処理結果格納部１２２は、(3)後半処理でパケット「１」のＨＷ暗復号認証結果を取得・格納し、ネットワークプロトコルの後半処理（ＩＰ層以上の処理）を行う。次いで、ＩＰセキュアプロトコル１１０とリクエスト生成ＨＷ初期化部１２１は、(1)前半処理でパケット「２」のネットワークプロトコルの前半処理（ＩＰ層以下の処理）を行い、パケット「２」のリクエストをＨＷ暗復号認証エンジン１３０に発行する。ＨＷ暗復号認証エンジン１３０は、(2)ＨＷ暗復号認証処理で、発行されたパケット「２」のリクエストのＨＷ暗復号認証処理を行う。ＩＰセキュアプロトコル１１０とＨＷ後処理結果格納部１２２は、(3)後半処理でパケット「２」のＨＷ暗復号認証結果を取得・格納し、ネットワークプロトコルの後半処理（ＩＰ層以上の処理）を行う。次いで、ＩＰセキュアプロトコル１１０とリクエスト生成ＨＷ初期化部１２１は、(1)前半処理でパケット「３」のネットワークプロトコルの前半処理（ＩＰ層以下の処理）を行い、パケット「３」のリクエストをＨＷ暗復号認証エンジン１３０に発行する。ＨＷ暗復号認証エンジン１３０は、(2)ＨＷ暗復号認証処理で、発行されたパケット「３」についてのリクエストのＨＷ暗復号認証処理を行う。ＩＰセキュアプロトコル１１０とＨＷ後処理結果格納部１２２は、(3)後半処理でパケット「３」のＨＷ暗復号認証結果を取得・格納し、ネットワークプロトコルの後半処理（ＩＰ層以上の処理）を行う。

[0046] このように、図５Ｂの負荷の平準化を行うと、図５Ａの特別な制御を行わない場合に比べ、(1)前半処理でリクエストが滞留することがなくなるため、処理の均質化及びビットレート低下抑制を図ることができる。

[0047] しかし、上述した負荷の平準化では、番号１５０の破線矢印に示すようにネットワークプロトコルの前半処理のタイミングで暗復号認証処理を動作させるため、順序維持のためにＨＷ／ＳＷを並列処理できない。本発明は、合成・細分化・並び替えにより、処理順序を維持しつつ、ＨＷ／ＳＷの並列処理を実現するものである。

[0048] 図６Ａは、図５Ｂの負荷の平準化をより詳細に説明する図である。

[0049] 図６Ａの負荷の平準化では、ＩＰセキュアプロトコル１１０とリクエスト生成ＨＷ初期化部１２１は、(1)前半処理でパケット「２」について「ネットワークプロトコルの前半処理（ＩＰ層以下の処理）」を行うとともに、「暗復号認証前半処理（リクエスト生成とHW初期化）」を行う。HW暗復号認証エンジン１３０は、(2)ＨW暗復号認証処理で、発行されたパケット「２」のリクエストのＨW暗復号認証処理を行う。ＩＰセキュアプロトコル１１０とＨW後処理結果格納部１２２は、(3)後半処理でパケット「２」について「暗復号認証後半処理（HW後処理と結果格納）」を行うとともに、「ネットワークプロトコルの後半処理（ＩＰ層以上の処理）」を行う。

[0050] 図６ＢＣは、本高速制御方式を説明する図である。図６Ｂは、負荷平準化後に高速制御を行うための高速制御方式の方式Ａを、図６Ｃは、方式Ａを更に細分化した高速制御方式の方式Ｂをそれぞれ示す。

[0051] 本高速制御方式は、前半処理と後半処理を一連のコンテキストで行う。すなわち、直前のパケットの後半処理（レイヤ２以降の処理）と次のパケットの処理（レイヤ１の処理）とを合体させることで、関数の時間として待ち時間なしでパケットの処理を行う。

[0052] 図６Ｂの高速制御方式の方式Ａでは、１つ前のパケットの(3)ネットワークプロトコルの後半処理と次のパケットの(1)ネットワークプロトコルの前半処理を合体した、(1)(3)前半処理／後半処理を実現する。図６Ｂの場合、(1)(3

)前半処理／後半処理で１つ前のパケット「１」の(3)後半処理と次のパケット「２」の(1)前半処理を合体する。(2)ＨＷ暗復号認証処理はそのままである。このため、方式Ａの(1)(3)前半処理／後半処理では、 図６Ａの番号１５１の破線矢印に示すＨＷ割込みコンテキストに基づく遅延処理開始指示よりも先に、図６Ｂの番号１５２の破線矢印に示すネットワークプロトコルの前半処理開始のタイミングで(1)(3)前半処理／後半処理を開始できることになる。このため、方式Ａは、図６Ｂの番号１５２の破線矢印に示すネットワークプロトコルの前半処理開始のタイミングか、図６Ａの番号１５１の破線矢印に示すＨＷ割込みコンテキストに基づく遅延処理開始指示のうち、いずれか早い方で処理を開始することができ、処理時間を短縮することができる。ここで、(1)前半処理と(3)後半処理の優先度が異なる場合であっても処理が滞ることなくスムーズな処理を実現することができる。

[0053] 図６Ｃの方式Ｂは、方式Ａの各処理を並び替えることで、ＨＷ／ＳＷの並行処理を実現し、より高速制御を図るものである。各処理の並び替えは以下(i)－(iv)の通りである。

[0054] (i)ネットワークプロトコルの前半処理

(ii)暗復号認証後半処理

(iii)暗復号認証前半処理

(iv)ネットワークプロトコルの後半処理

上記各処理の並べ替えを具体的に説明すると、図６Ｃの場合、図６Ｂのパケット「１」とパケット「２」は以下の並べ替え処理となる。

[0055] (i)２番目のパケット「２」の前半処理

(ii)１番目のパケット「１」のＨＷ後半処理

(iii)２番目のパケット「２」のＨＷ前半処理

(iv)１番目のパケット「１」のレイヤ２以降の処理

ＨＷ暗復号処理が終わってから実際に後半処理が開始されるまでには若干のロス（余分な処理）がある。なにか別の処理が入ってきたり、またカーネルの処理が含まれる。図６Ｃの方式Ｂは、各処理の並び替えにより１つのシ

ーケンスで、上記(i)ネットワークプロトコル前半処理の直後に、上記(ii)暗復号認証後半処理を行う。続いて、上記上記(iii)暗復号認証前半処理の直後に、上記(iv)ネットワークプロトコルの後半処理を連続して行うことで、番号１５１のHW割込みコンテキストに基づく遅延処理開始指示が削減される。すなわち、上位プログラムによる関数呼び出しがあると、上記(i)－(iv)をロスなしで連続で実行するので、番号１５１の遅延処理開始指示が必要なくなる。図６Ａの負荷の平準化では、HW割り込みが発生して後半処理を開始するために、番号１５１の遅延処理開始指示が出される。しかし実際には、それよりも前に次のパケットが到着することも有りうる。このような場合、図６Ｃの方式Ｂでは、開始指示を待つ前に開始できるようになるので、その分速度改善につながる。パケットの送信指示が先かHW処理完了（割り込みHW割り込み）が先かの競争が行われ、早い方で処理を開始するものである。このように、各処理を並び替えることで、HW／SWの並行処理を実現することができる。

[0056] （実施の形態１）

図７は、上記基本的な考え方に基づく本発明の実施の形態１に係る暗号化情報通信システムのセキュア通信装置の構成を示す図である。

[0057] 図７において、セキュア通信装置２００は、レイヤ処理１及びレイヤ処理２を実行する通信スタック部２１０と、受信／送信情報を一時的に格納するバッファ２２０と、HWエンジンにHW処理リクエストを発行して暗号認証処理を実行する暗号認証処理部２３０と、HWエンジンにより暗復号認証処理を実行するHW暗復号認証処理部２４０とを備えて構成される。また、暗号認証処理部２３０は、リクエスト制御部２３１、HW前後処理部２３２、及びキュー２３３を備える。

[0058] HW前後処理部２３２は、図６Ｂの方式Ａ又は図６Ｃの方式Ｂにより前半処理と後半処理を一連のコンテキストで行う。HW前後処理部２３２は、図６Ｃの方式Ｂを採用した場合、(i)ネットワークプロトコル前半処理、(ii)暗復号認証後半処理、(iii)暗復号認証前半処理、乃至(iv)ネットワークプロト

コル後半処理を連続して行う。具体的には、HW前後処理部２３２は、取得したリクエストに従ってHW暗復号認証処理部２４０にHW処理リクエストを発行する（(5)参照）一方で、HW暗復号認証処理部２４０からHW割込みコンテキストに基づく遅延処理開始指示を受け取り、さらに、HW暗復号認証処理部２４０からHW処理結果を取得して（(6)参照）HW後処理を実行する。ここで、レイヤ処理１及びレイヤ処理２は、図６Ｂの各処理の並べ替え処理となる。例えば、(i)２番目のパケット「２」の前半処理、(ii)１番目のパケット「１」のHW後半処理、(iii)２番目のパケット「２」のHW前半処理、乃至(iv)１番目のパケット「１」のレイヤ２以降の処理である。

[0059] 以下、上述のように構成されたセキュア通信装置２００の動作について説明する。

[0060] 図８は、上記暗号認証処理部２３０及びHW暗復号認証処理部２４０の動作タイミングを示すタイミングチャートである。図７及び図８中、番号(1)－(6)は処理の流れを説明するための符号である。

[0061] 通信スタック部２１０は、通常の通信スタック処理では、送信指示又は受信割込みによりバッファ１２０を介してレイヤ処理１及びレイヤ処理２を実行する。レイヤ処理１は、ネットワークプロトコルの前半処理であり、ＴＣＰプロトコル処理及びＩＰプロトコル処理の一部を含む優先度の高い上位レイヤ処理である。レイヤ処理２は、ネットワークプロトコルの後半処理であり、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る。

[0062] 通信スタック部２１０は、HW暗号認証を行う場合には、送信指示又は受信割込みを受けると、レイヤ処理１で暗号認証処理部２３０に処理を指示し、暗号認証処理部２３０はHW暗復号認証処理部２４０に対しHW処理リクエストを発行する。

[0063] HW暗復号認証処理部２４０は、このHW処理リクエストを受け取り、HWによる暗復号認証処理を行って暗号認証処理完了の遅延処理を、暗号認証処理部２３０を介して通信スタック部２１０に返す。通信スタック部２１０

は、暗号認証処理部２３０による暗号認証処理結果を受け取り、バッファ２２０を介してレイヤ処理２を実行する。

[0064] 具体的には、暗号認証処理部２３０は、以下の動作を行う。

[0065] リクエスト制御部２３１は、通信スタック部２１０のレイヤ処理１により暗号認証処理が指示されると、そのリクエストをキュー２３３に積む（(1)参照）。リクエスト制御部２３１は、ＨＷビジーでない場合にはＨＷ前後処理部２３２にＨＷ前処理を指示する（(2)参照）。

[0066] ＨＷ前後処理部２３２は、処理済みのリクエストがあればＨＷ暗復号認証処理部２４０からＨＷ処理結果を取得して（(3)参照）ＨＷ後処理を実行する。ＨＷ前後処理部２３２は、ＨＷ後処理を終了すると、レイヤ処理２に後半処理を指示する（(6)参照）。

[0067] また、ＨＷ前後処理部２３２は、キュー２３３にリクエストが積まれていれば、キュー２３３からリクエストを取得し（(4)参照）、取得したリクエストに従ってＨＷ暗復号認証処理部２４０にＨＷ処理リクエストを発行する（(5)参照）。

[0068] ＨＷ暗復号認証処理部２４０は、ＨＷ前後処理部２３２からのＨＷ処理リクエスト（(5)参照）に従ってＨＷによる暗復号認証処理を行う。ＨＷ暗復号認証処理部２４０は、該当ＨＷ処理リクエストによる暗復号認証処理が終わると、ＨＷ割込みコンテキストを発生し（図８参照）、このＨＷ割込みコンテキストに基づく遅延処理開始指示をＨＷ前後処理部２３２に出力する（(0)参照）。

[0069] 図８の符号ａ．で示すように、ＨＷ前後処理部２３２は、ＨＷ暗復号認証処理部２４０からの遅延処理開始指示（(0)参照）、又はレイヤ処理１からの指示のうち、いずれか早い方で処理を開始する。ＨＷ前後処理部２３２は、いずれかの指示によりＨＷ前後処理をすぐに実行できるため、レイヤ処理１から見た場合、レイヤ処理１が利用できない時間はなくなる。

[0070] ＨＷ前後処理部２３２は、ＨＷ暗復号認証処理部２４０からＨＷ処理結果を取得して（(3)参照）ＨＷ後処理を実行する。ＨＷ前後処理部２３２は、Ｈ

W後処理を終了すると、レイヤ処理２に後半処理を指示する。通信スタック部２１０は、レイヤ処理２を実行する。

[0071] 図８の符号ｂ．で示すように、暗号認証処理部２３０は、HW処理待ち時間なしに、レイヤ処理１とレイヤ２を同じコンテキストで実行する。

[0072] このように、暗号認証処理部２３０のHW前後処理部２３２は、処理済みのリクエストがある場合はHW処理結果取得（(3)参照）と後半処理指示（(6)参照）を行う。キュー２３３にリクエストが積まれていれば、HW前処理（(4)(5)参照）を行う。また、HW前後処理部２３２は、HW暗復号認証処理部２４０からの遅延処理開始指示時（(0)参照）も、キュー２３３を見て同様の処理を行う。

[0073] したがって、暗号認証処理部２３０は、レイヤ処理２以降をレイヤ処理１と同じシーケンスで実行できるので、利用できない時間が減り、パフォーマンスが向上する。従来例では、図３に示すようにHW前処理部２２によるHW前処理が終了してHW後処理部２３がHW後処理を起動するまでの時間は、HW後処理部２３がHW後処理を行えない、利用できない時間となっていた。これに対して、暗号認証処理部２３０は、遅延処理開始依頼によってHW後処理部２３（図２の従来例）を起動するよりも早くHW後処理、次のHW処理リクエストを実行することができ、HW暗復号認証処理部２４０の利用効率を高めることができる。

[0074] （実施の形態２）

図９は、本発明の実施の形態２に係る暗号化情報通信システムのセキュア通信装置の構成を示すブロック図である。

[0075] 図９において、セキュア通信装置３００は、上位プログラム３１０、ネットワークプロトコル処理部３２０、通信部３３０、暗復号認証処理制御部３４０、暗復号認証処理部３５０、及び暗復号認証リクエスト蓄積部３６０を備えて構成される。

[0076] 上記上位プログラム３１０、ネットワークプロトコル処理部３２０及び暗復号認証処理制御部３４０は、ＣＰＵにより実行される。

[0077] セキュア通信装置３００は、セキュア通信を行う相手側セキュア通信装置と、通信部３３０により接続され、セキュア通信装置間で通信可能になっている。

[0078] 上位プログラム３１０は、実際に暗号化されたデータの送受信を行おうとしているアプリケーション、もしくは、その他のプログラムである。

[0079] ネットワークプロトコル処理部３２０は、トランスポート層やネットワーク層などのネットワークプロトコル処理を行う。より具体的には、ネットワークプロトコル処理部３２０は、上位プログラム３１０の指示によって、任意のデータのネットワークプロトコルの上位レイヤ処理（ＴＣＰプロトコル処理やＩＰプロトコル処理の一部等）を行い、処理が完了した平文パケットを、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、暗復号認証処理制御部３４０に依頼して暗号認証処理を行う。

[0080] また、ネットワークプロトコル処理部３２０は、暗復号認証処理制御部３４０からの指示で、暗号認証処理が完了した暗号化パケットのネットワークプロトコルの下位レイヤ処理（ＩＰプロトコル処理の一部やそれ以下の処理等）を行い、通信部３３０に処理が完了した暗号化パケットの送信処理を指示する。

[0081] また、ネットワークプロトコル処理部３２０は、通信部３３０で受信した暗号化パケットを受け取り、ネットワークプロトコルの下位レイヤ処理を行い、処理が完了した暗号化パケットを、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、暗復号認証処理制御部３４０に依頼して暗号認証処理を行う。

[0082] また、ネットワークプロトコル処理部３２０は、暗復号認証処理制御部３４０からの指示で、暗号認証処理が完了した平文パケットのネットワークプロトコルの上位レイヤ処理を行い、上位プログラム３１０の受信バッファに処理が完了した平文パケットを格納する。

[0083] 通信部３３０は、ネットワークプロトコル処理部３２０の指示で任意のパケットの送信処理を行う。また、通信部３３０は、対向のセキュア通信装置

が送信したデータを受信し、ネットワークプロトコル処理部３２０に転送する。具体的には、有線ＬＡＮや無線ＬＡＮなどの、ＩＰ通信が行えるネットワークデバイスが望ましい。

[0084] 暗復号認証処理制御部３４０は、ネットワークプロトコル処理部３２０からの暗復号認証指示に基づき、暗復号認証リクエストに格納されている平文・暗号化データを、暗復号認証処理部３５０に指示して暗復号認証処理を行う。

[0085] また、暗復号認証処理制御部３４０は、暗復号認証リクエスト蓄積部３６０に暗復号認証リクエストが格納されている場合には、先に格納されている暗復号認証リクエストの暗復号認証処理を暗復号認証処理部３５０に依頼し、ネットワークプロトコル処理部３２０から依頼された暗復号認証リクエストについては暗復号認証リクエスト蓄積部３６０に格納する。

[0086] また、暗復号認証処理制御部３４０は、暗復号認証処理部３５０が処理中の場合には、暗復号認証リクエストを暗復号認証リクエスト蓄積部３６０に格納して処理を終了する。

[0087] 特に、暗復号認証処理制御部３４０は、暗復号認証処理部３５０から、暗復号処理又は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、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ネットワークプロトコル処理部３２０を制御する。

[0088] また、暗復号認証処理制御部３４０は、暗復号認証処理部３５０において既に処理が完了した暗復号認証リクエストが存在する場合には、既に処理が完了している暗復号認証リクエストの暗復号認証完了処理を先に行い、次に新たに指示を受けた暗復号認証リクエストの暗復号認証処理要求を暗復号認証処理部３５０に対して行う。その後、暗復号認証完了処理を行った暗号データのネットワークプロトコル後半処理（上位レイヤ処理から指示を受けている場合は下位レイヤ処理、下位レイヤ処理から指示を受けている場合は上位レイヤ処理）を同じＣＰＵコンテキストで行うよう、ネットワークプロト

コル処理部３２０に指示し、ネットワークプロトコル後半処理が完了すると、暗復号認証処理制御部３４０の処理を終了する。処理の詳細については後述する。

[0089] 暗復号認証処理部３５０は、暗復号認証処理制御部３４０の、暗復号認証開始指示によって暗復号認証処理を開始し、暗復号認証処理が完了した時点で暗復号認証処理制御部３４０に処理完了通知を行う。具体的には、ハードウェア割り込み処理にて起床されたソフトウェア割り込みによって処理完了通知をすることが望ましい。その後、暗復号認証処理制御部３４０の、暗復号認証完了処理指示によって、結果や付随データを取得するための完了処理を行う。

[0090] 暗復号認証リクエスト蓄積部３６０は、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、暗復号処理又は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部３５０に受け渡す。暗復号認証リクエスト蓄積部３６０は、暗復号認証リクエストを出し入れするためのキュー構造である。通常ＦＩＦＯ（First-In First-Out）で構成されるが、例えばパケットのＴＯＳ（Type of Service）フィールドや、送受信アドレス、送受信ポート、プロトコルなどの情報を元に、デキューする暗復号認証リクエストに優先度をつけるようにするなど、その他の構成であってもよい。なお、ＴＯＳフィールドは、ＩＰヘッダに含まれる長さ８ビットの情報であり、上位３ビットが優先度を表示するＩＰプレシデンスである。

[0091] 以下、上述のように構成されたセキュア通信装置３００の動作について説明する。

[0092] まず、セキュア通信装置３００が暗号化パケットの受信側として機能する場合について説明する。

[0093] 図１０は、セキュア通信装置３００が受信側として機能する場合のセキュア通信処理時の動作を説明する制御シーケンス図である。図１０において、上位プログラム３１０、ネットワークプロトコル処理部３２０及び暗復号認

証処理制御部３４０は、ＣＰＵにより実行される。

[0094] ステップＳ１０１では、上位プログラム３１０は、ソケットを生成し、対向のセキュア通信装置のアドレス情報やポート番号をバインドする。

[0095] ステップＳ１０２では、上位プログラム３１０は、暗号化したい平文データを、ソケットを通してネットワークプロトコル処理部３２０に処理を依頼する。

[0096] ステップＳ１０３では、ネットワークプロトコル処理部３２０は、受け取った平文データを最大送信単位ごとに平文パケットとして再構成し、ネットワークプロトコルの上位レイヤ処理（ＴＣＰプロトコル処理やＩＰプロトコル処理の一部等）を行う。

[0097] ステップＳ１０４では、ネットワークプロトコル処理部３２０は、平文パケットを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暗復号認証リクエスト蓄積部３６０に格納し、暗復号認証処理制御部３４０に暗号認証処理を指示する。ＣＰＵにより実行されるここまでの処理が、例えば図６Ｂの(i)２番目のパケット「２」についてのネットワークプロトコルの前半処理に相当する。

[0098] ステップＳ１０５では、暗復号認証処理制御部３４０は、暗復号認証処理部３５０が処理中でないかを判別する。暗復号認証処理部３５０が処理中であった場合は、処理を終了する。

[0099] ステップＳ１０６では、暗復号認証処理制御部３４０は、暗復号認証処理部３５０において既に暗復号認証処理が終了している暗復号認証リクエストがないか否かを判別する。

[0100] ステップＳ１０７では、暗復号認証処理制御部３４０は、暗復号認証処理部３５０において既に暗復号認証処理が終了している暗復号認証リクエストの暗復号認証完了処理を行う。ＣＰＵにより実行されるステップＳ１０５乃至ステップＳ１０７までの処理が、例えば図６Ｂの(ii)１番目のパケット「１」のＨＷ後半処理に相当する。

[0101] ステップＳ１０８では、暗復号認証処理制御部３４０は、暗復号認証リク

エスト蓄積部３６０に暗復号認証リクエストが格納されているか否かを判別する。

[0102] 暗復号認証リクエスト蓄積部３６０に暗復号認証リクエストが存在する場合、ステップＳ１０９で暗復号認証処理制御部３４０は、暗復号認証処理部３５０のセットアップを行う。具体的には、暗復号認証処理制御部３４０は、暗復号認証リクエストに格納されている平文・暗号化データと暗復号認証処理に必要なパラメータを用いて、暗復号認証処理を暗復号認証処理部３５０に指示する。ＣＰＵにより実行されるステップＳ１０８及びステップＳ１０９の処理が、例えば図６Ｂの(iii)２番目のパケット「２」のHW前半処理に相当する。

[0103] ステップＳ１１０では、暗復号認証処理部３５０は、暗復号認証処理制御部３４０の指示に基づき、暗復号認証処理を開始する。ここで、暗復号認証処理は非同期に実行され、処理の完了を待ち合わせることはしない。

[0104] ステップＳ１１１では、暗復号認証処理制御部３４０は、上記ステップＳ１０７において暗復号認証完了処理を行った暗復号認証リクエストがあれば、ネットワークプロトコル処理部３２０に対して、ネットワークプロトコル後半処理（上位レイヤ処理から指示を受けている場合は下位レイヤ処理、下位レイヤ処理から指示を受けている場合は上位レイヤ処理）を同じＣＰＵコンテキストで行うように指示する。

[0105] ステップＳ１１２では、ネットワークプロトコル処理部３２０は、ネットワークプロトコルの下位レイヤ処理を行い、処理が完了した暗号化パケットを送信するように通信部３３０に指示する。ＣＰＵにより実行されるステップＳ１１１及びステップＳ１１２の処理が、例えば図６Ｂの(iv)１番目のパケット「１」のレイヤ２以降の処理に相当する。

[0106] ステップＳ１１３では、通信部３３０は、ネットワークプロトコル処理部３２０から受け取った暗号化パケットを対向のセキュア通信装置（相手側セキュア通信装置）に送信する。

[0107] このように、ステップＳ１０１からステップＳ１１２に至るまで、前半処

理と後半処理を一連のＣＰＵコンテキストで行う。直前のパケットの後半処理（レイヤ２以降の処理）と次のパケットの処理（レイヤ１の処理）をシームレスに連続させることで、関数の時間としては待ち時間なしでパケットの処理が行えることになる。すなわち、暗復号認証処理制御部３４０は、リクエストの通知だけで関数をリターンせずにレイヤ２以降の処理を実行して（換言すれば、同じＣＰＵコンテキストにて）、その後に関数をリターンする。暗復号認証処理制御部３４０が、途中で関数をリターンしないことで１つのシーケンスで実行される。したがって、受信したパケットをネットワークプロトコル処理する際、暗復号認証処理による処理の分断なしに、同じコンテキストで上位レイヤまでの処理を実現することができる。

[0108] 次に、セキュア通信装置３００が、送信側の暗号化情報通信装置である場合を例に動作を説明する。この場合は、暗復号認証処理部３５０で暗復号認証処理が終了した際の動作に対応する。

[0109] 図１１は、セキュア通信装置３００によるセキュア通信処理時の動作を説明する制御シーケンス図である。

[0110] ステップＳ２０１では、暗復号認証処理部３５０は、暗復号認証処理制御部３４０に対してステップＳ２０２以降の処理を開始するようソフトウェア遅延割り込み処理の開始を指示する。

[0111] ステップＳ２０２では、暗復号認証処理制御部３４０は、暗復号認証処理部３５０が処理中でないかを判別する。暗復号認証処理部３５０が処理中であった場合は、処理を終了する。

[0112] ステップＳ２０３では、暗復号認証処理制御部３４０は、暗復号認証処理部３５０において既に暗復号認証処理が終了している暗復号認証リクエストがないか否かを判別する。

[0113] ステップＳ２０４では、暗復号認証処理制御部３４０は、暗復号認証処理部３５０において既に暗復号認証処理が終了している暗復号認証リクエストの暗復号認証完了処理を行う。

[0114] ステップＳ２０５では、暗復号認証処理制御部３４０は、暗復号認証リク

エスト蓄積部３６０に暗復号認証リクエストが格納されているか否かを判別する。

[0115] 暗復号認証リクエスト蓄積部３６０に暗復号認証リクエストが存在する場合、ステップＳ２０６で暗復号認証処理制御部３４０は、暗復号認証処理部３５０のセットアップを行う。具体的には、暗復号認証処理制御部３４０は、暗復号認証リクエストに格納されている平文・暗号化データと暗復号認証処理に必要なパラメータを用いて、暗復号認証処理を暗復号認証処理部３５０に指示する。

[0116] ステップＳ２０７では、暗復号認証処理部３５０は、暗復号認証処理制御部３４０の指示に基づき、暗復号認証処理を開始する。ここで、暗復号認証処理は非同期に実行され、処理の完了を待ち合わせることはしない。

[0117] ステップＳ２０８では、暗復号認証処理制御部３４０は、上記ステップＳ２０７において暗復号認証完了処理を行った暗復号認証リクエストがあれば、ネットワークプロトコル処理部３２０に対して、ネットワークプロトコル後半処理（上位レイヤ処理から指示を受けている場合は下位レイヤ処理、下位レイヤ処理から指示を受けている場合は上位レイヤ処理）を同じＣＰＵコンテキストで行うように指示する。

[0118] ステップＳ２０９では、ネットワークプロトコル処理部３２０は、ネットワークプロトコルの下位レイヤ処理を行い、処理が完了した暗号化パケットを送信するように通信部３３０に指示する。

[0119] ステップＳ２１０では、通信部３３０は、ネットワークプロトコル処理部３２０から受け取った暗号化パケットを対向のセキュア通信装置（相手側セキュア通信装置）に送信する。

[0120] 以上詳細に説明したように、本実施の形態によれば、セキュア通信装置３００の暗復号認証処理制御部３４０は、暗復号認証処理部３５０から、暗復号処理又は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、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ネットワークプロ

トコル処理部３２０を制御する。例えば、暗復号認証処理制御部３４０は、ネットワークプロトコル処理部３２０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処理又は認証処理を依頼された際、同じＣＰＵコンテキストにより、直前に暗復号処理又は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暗復号認証処理部３５０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ネットワークプロトコル処理部３２０が処理するように制御する。これにより、受信したパケットをネットワークプロトコル処理する際、暗復号認証処理による処理の分断なしに、同じコンテキストで上位レイヤまでの処理を実現することができる。その結果、処理分断によるオーバーヘッドなしに、ＣＰＵやＨＷエンジンの負荷の偏りが起こりにくい暗復号処理又は認証処理を行うことができる。したがって、ルータやゲートウェイなど、特別に高速化が求められる機器や、組み込み機器など非力なリソースしか持たない端末同士であっても、高速なセキュア送信処理を実現することができる。

[0121] また、本実施の形態では、暗復号認証処理制御部３４０は、１つ前のパケットの処理結果を暗復号認証処理部３５０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ネットワークプロトコル処理部３２０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処理又は認証処理を暗復号認証処理部３５０に対して依頼する。この構成により、ＣＰＵコンテキストの切り替えを行うことなく、１つ目のパケット処理完了後に２つ目のパケットの暗復号処理又は認証処理の依頼を行うことができ、暗復号処理又は認証処理の高速化を図ることができる。また、暗復号認証処理部３５０が動作していない時間を最小にすることができ、暗復号処理又は認証処理の高速化や、暗復号認証処理手段の効率的な利用を図ることができる。

[0122] また、本実施の形態では、暗復号認証処理制御部３４０は、暗復号認証処理部３５０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

処理結果を暗復号認証処理部３５０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処理又は認証処理を暗復号認証処理部３５０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ネットワークプロトコル処理部３２０が処理するように制御する。この構成により、ネットワークプロトコルの前半処理、完了ハードウェア割り込み（又はソフトウェア遅延割り込み）のうち、いずれか早いタイミングで暗復号認証処理制御部３４０を動作させることができ、暗復号処理又は認証処理の高速化を図ることができる。

[0123] また、本実施の形態では、暗復号認証処理制御部３４０は、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、の順に並び替えてネットワークプロトコル処理部３２０と暗復号認証処理部３５０とを並列処理させるので、合成・細分化・並び替えにより、処理順序を維持しつつ、ＨＷ／ＳＷの並行処理を実現することができる。

[0124] さらに、本実施の形態では、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、暗復号処理又は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、暗復号認証リクエストを優先度順に暗復号認証処理部３５０に受け渡す暗復号認証リクエスト蓄積部３６０を備えているので、例えばＡＶストリーミングのように、高い優先度で処理を行わなければならない送受信パケットの高速化を図ることができる。

[0125] （実施の形態３）

実施の形態３は、セキュア通信装置の別の動作例について説明する。

[0126] 本発明の実施の形態３に係るセキュア通信装置のハード的構成は、図９に示すセキュア通信装置３００と同一構成であるため説明を省略する。

[0127] 図１２は、セキュア通信装置３００が受信側として機能する場合のセキュ

ア通信処理時の動作を説明する制御シーケンス図である。図１０に示すフローと同一処理を行うステップには同一ステップ番号を付して説明を省略する。

[0128] ステップＳ３０１では、通信部３３０は、対向のセキュア通信装置から受信した暗号化パケットを処理するため、ステップＳ３０２以降の処理を行うためのソフトウェア遅延割り込み処理の開始指示を行う。

[0129] ステップＳ３０２では、ネットワークプロトコル処理部３２０は、受け取った暗号化パケットの、ネットワークプロトコルの下位レイヤ処理（ＩＰプロトコル処理の一部とそれ以下のレイヤ処理）を行う。

[0130] ステップＳ１０４からステップＳ１１１までの処理は図１０の対応する処理と同じである。

[0131] ステップＳ３０３では、ネットワークプロトコル処理部３２０は、ネットワークプロトコルの上位レイヤ処理（ＴＣＰプロトコル処理やＩＰプロトコル処理の一部等）を行い、処理が完了した平文パケットを上位プログラム３１０の受信バッファに格納する。

[0132] 次に、セキュア通信装置３００が、送信側の暗号化情報通信装置である場合を例に動作を説明する。この場合は、暗復号認証処理部３５０で暗復号認証処理が終了した際の動作に対応する。

[0133] 図１３は、セキュア通信装置３００によるセキュア通信処理時の動作を説明する制御シーケンス図である。図１１に示すフローと同一処理を行うステップには同一ステップ番号を付して説明を省略する。

[0134] ステップＳ２０１では、暗復号認証処理部３５０は、暗復号認証処理制御部３４０に対してステップＳ２０２以降の処理を開始するようソフトウェア遅延割り込み処理の開始を指示する。

[0135] ステップＳ２０２からステップＳ２０８までの処理は図１１の対応する処理と同じである。

[0136] ステップＳ４０１では、ネットワークプロトコル処理部３２０は、ネットワークプロトコルの上位レイヤ処理（ＴＣＰプロトコル処理やＩＰプロトコ

ル処理の一部等）を行い、処理が完了した平文パケットを上位プログラム３１０の受信バッファに格納する。

[0137] このように、本実施の形態のセキュア通信装置によれば、実施の形態２と同様の効果、すなわち受信したパケットをネットワークプロトコル処理する際、暗復号認証処理による処理の分断なしに、同じコンテキストで上位レイヤまでの処理を実現することができ、ルータやゲートウェイなど、特別に高速化が求められる機器や、組み込み機器など非力なリソースしか持たない端末同士であっても、高速なセキュア受信処理を実現することができる。

[0138] 以上の説明は本発明の好適な実施の形態の例証であり、本発明の範囲はこれに限定されることはない。例えば、ＩＰｖ６ネットワークを介してＩＰｓｅｃプロトコルにより暗号化通信を行う暗号化情報通信システムに適用可能であるが、ＩＰｖネットワークであればよく、ＩＰｖ６ネットワークの機能を含む上位バージョンが策定された場合はこれも包含するものである。

[0139] また、ネットワークプロトコル処理部３２０、暗復号認証処理制御部３４０等の各機能ブロックは典型的には集積回路であるＬＳＩとして実現される。これらは個別に１チップ化されてもよいし、一部又は全てを含むように１チップ化されてもよい。集積度の違いにより、ＩＣ、システムＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。

[0140] また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Field Programmable Gate Array）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用してもよい。

[0141] さらには、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

[0142] また、本実施の形態ではセキュア通信装置及びセキュア通信方法という名称を用いたが、これは説明の便宜上であり、暗号化情報通信装置、暗号化情

報通信システム、セキュリティアソシエーション方法等であってもよいことは勿論である。

[0143] さらに、上記セキュア通信装置を構成する各部、例えばネットワークプロトコル処理部の種類、その数及び接続方法などはどのようなものでもよい。

[0144] 以上説明したセキュア通信方法は、このセキュア通信方法を機能させるためのプログラムでも実現される。このプログラムはコンピュータで読み取り可能な記録媒体に格納されている。

[0145] ２００８年８月２９日出願の特願２００８－２２２５５４の日本出願に含まれる明細書、図面および要約書の開示内容は、すべて本願に援用される。

産業上の利用可能性

[0146] 以上のように、本発明に係るセキュア通信装置、セキュア通信方法及びプログラムは、ソフトウェア処理、又は、ハードウェア処理によって高速なＩＰセキュア通信処理を行うことができる効果を有し、セキュア通信機器及びセキュア通信方法等に有用である。

符号の説明

[0147] １００，２００，３００　セキュア通信装置

１１０　ＩＰセキュアプロトコル

１２０　クリプトマネージャ

１３０　HW暗復号認証エンジン

２１０　通信スタック部

２２０　バッファ

２３０　暗号認証処理部

２３１　リクエスト制御部

２３２　HW前後処理部

２３３　キュー

２４０　HW暗復号認証処理部

３１０　上位プログラム

３２０　ネットワークプロトコル処理部

３３０　通信部

３４０　暗復号認証処理制御部

３５０　暗復号認証処理部

３６０　暗復号認証リクエスト蓄積部

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、

暗復号処理又は認証処理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、暗復号処理又は認証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処理又は認証処理を依頼された際、同じＣＰＵコンテキストにより、直前に暗復号処理又は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処理又は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処理又は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、暗復号処理又は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] 通信パケットを送受信するステップと、

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ステップと、

暗復号処理又は認証処理を行う暗復号認証処理ステップと、

暗復号処理又は認証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、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処理又は認証処理を依頼された際、同じＣＰＵコンテキストにより、直前に暗復号処理又は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、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ステップにおいて処理する請求項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、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処理又は認証処理を前記暗復号認証処理ステップ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処理又は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ステップにおいて処理する請求項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] 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、暗復号処理又は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。

補正された請求の範囲

[2009年12月25日(25.12.2009)国際事務局受理]

[1] (補正後) 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。

[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。

[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。

[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。

[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。

[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。

[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。

[8] (補正後) 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。

[9] (補正後) 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C

PU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。

[10] (補正後) 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。

[11] (補正後) 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。

[12] (補正後) 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。

[13] (補正後) 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。

[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。

[図1]

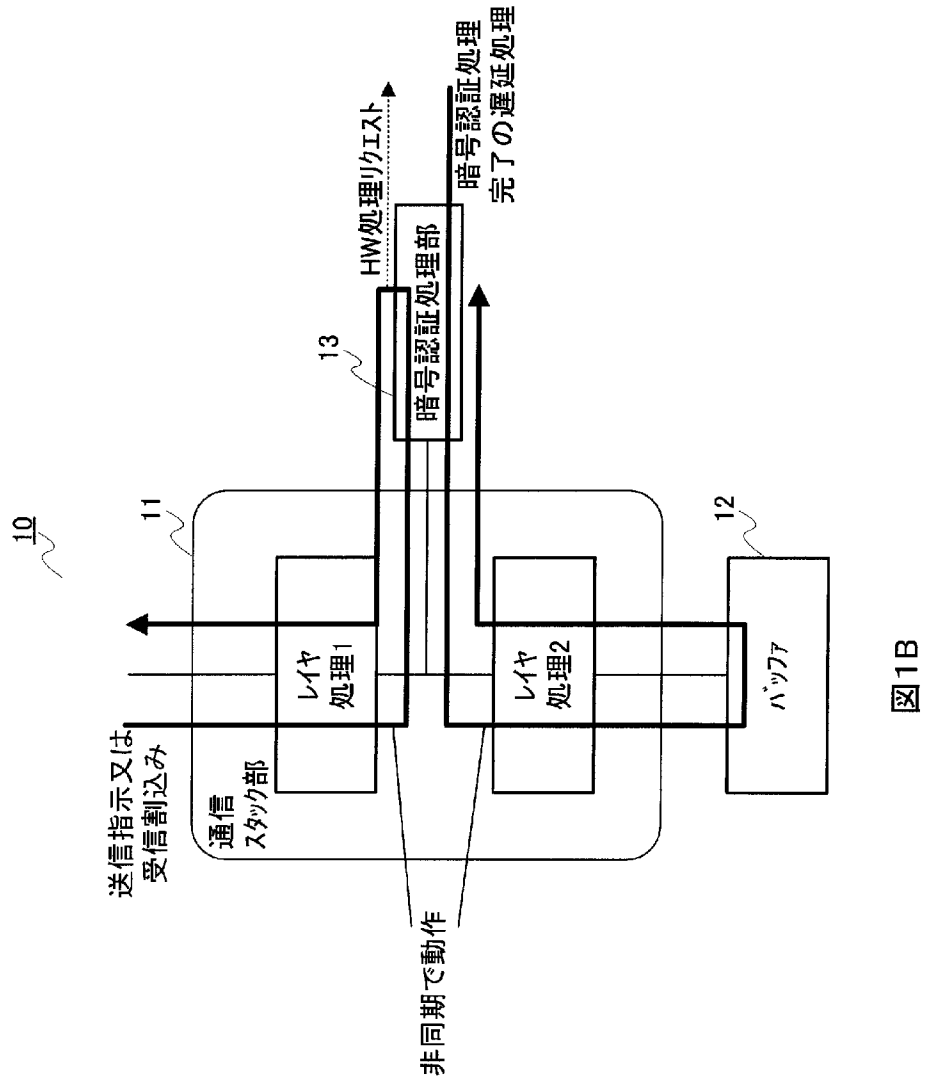

10
11
12
13
通信
スタック部
送信指示又は
受信割込み
レイヤ
処理1
レイヤ
処理2
バッファ
暗号認証処理部
HW処理リクエスト
暗号認証処理
完了の遅延処理
非同期で動作

図1B

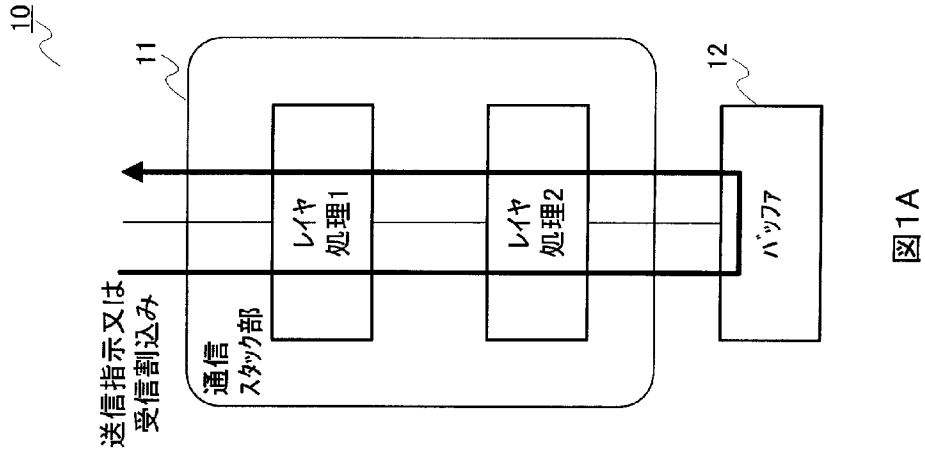
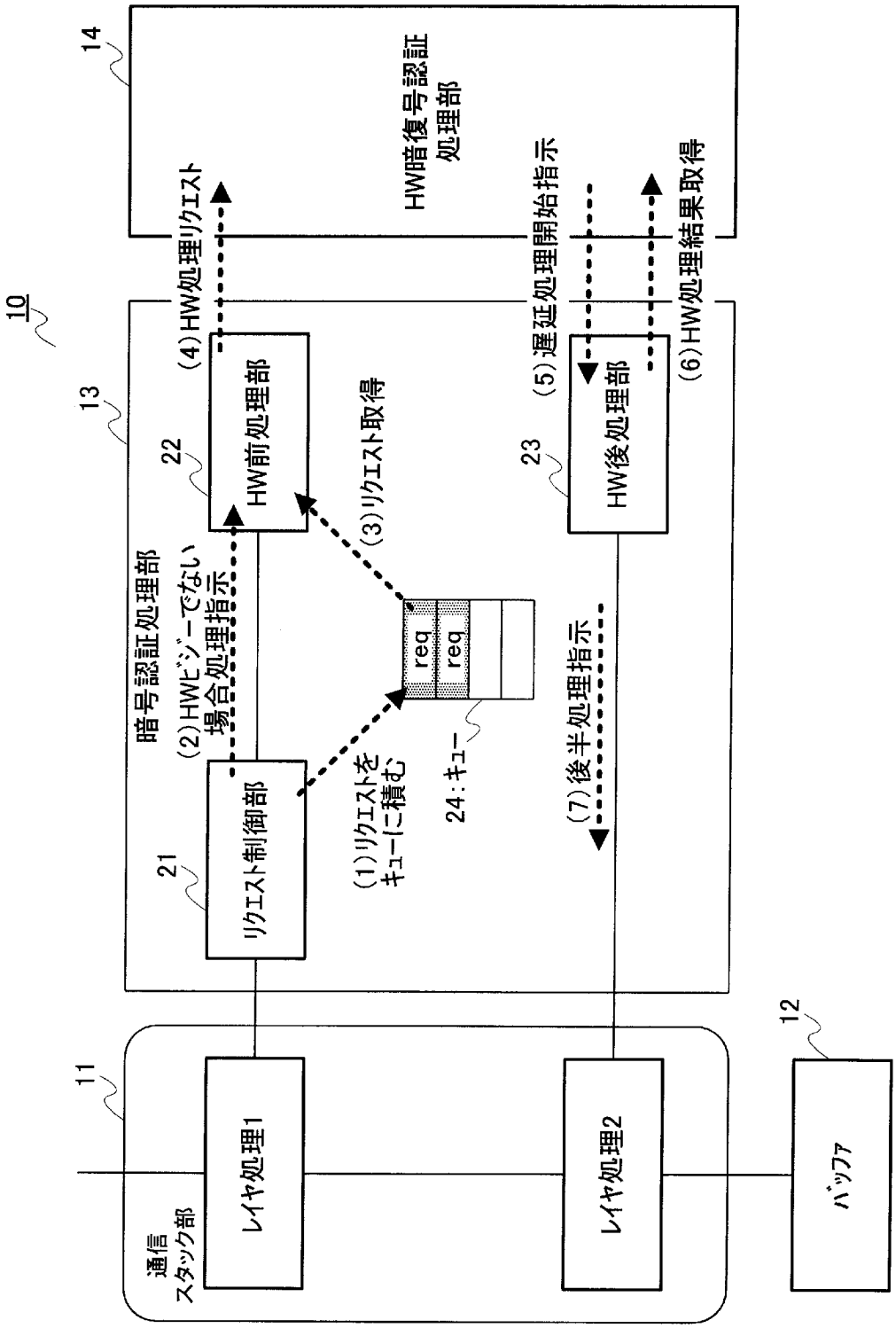
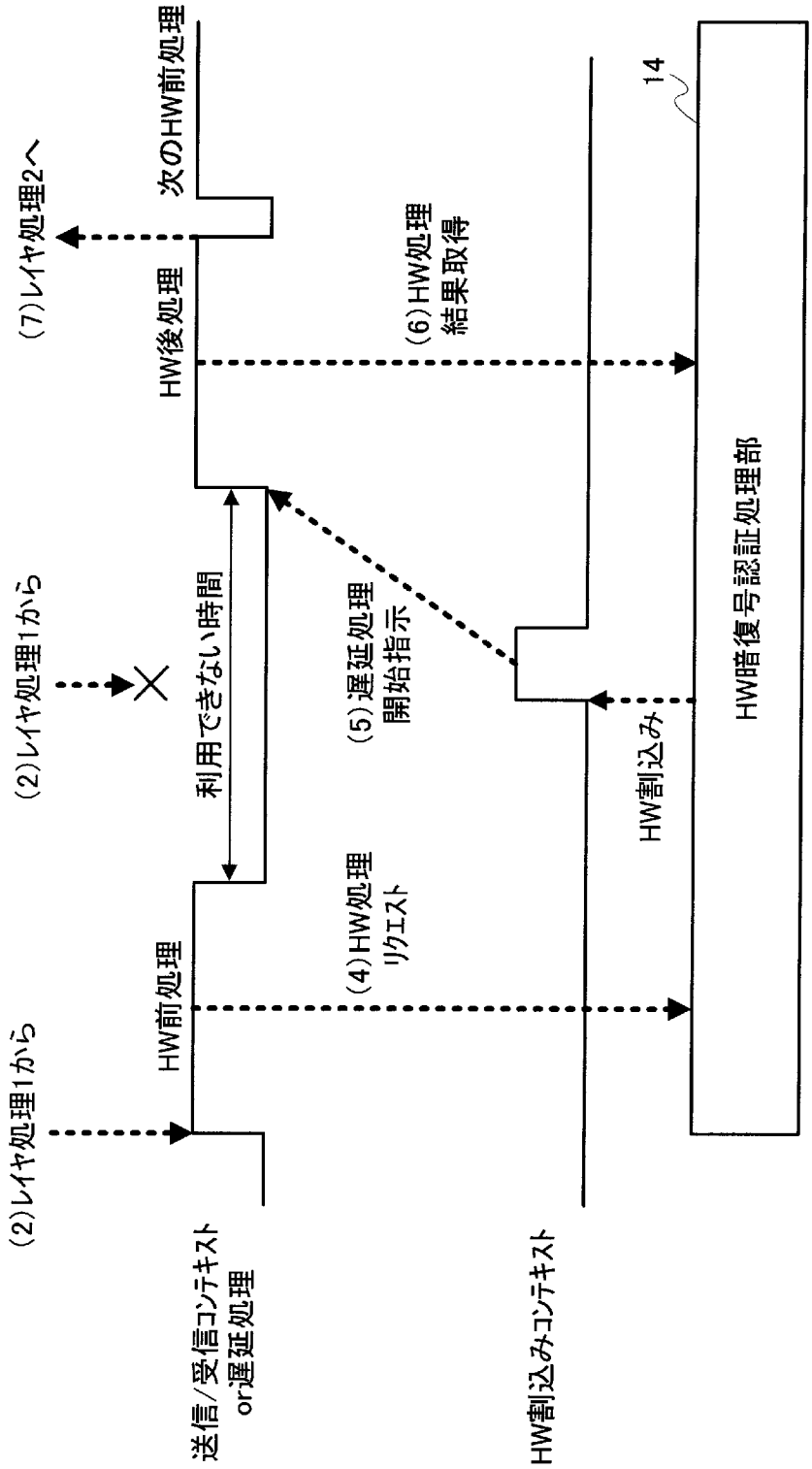

10
11
12
通信
スタック部
送信指示又は
受信割込み
レイヤ
処理1
レイヤ
処理2
バッファ

図1A

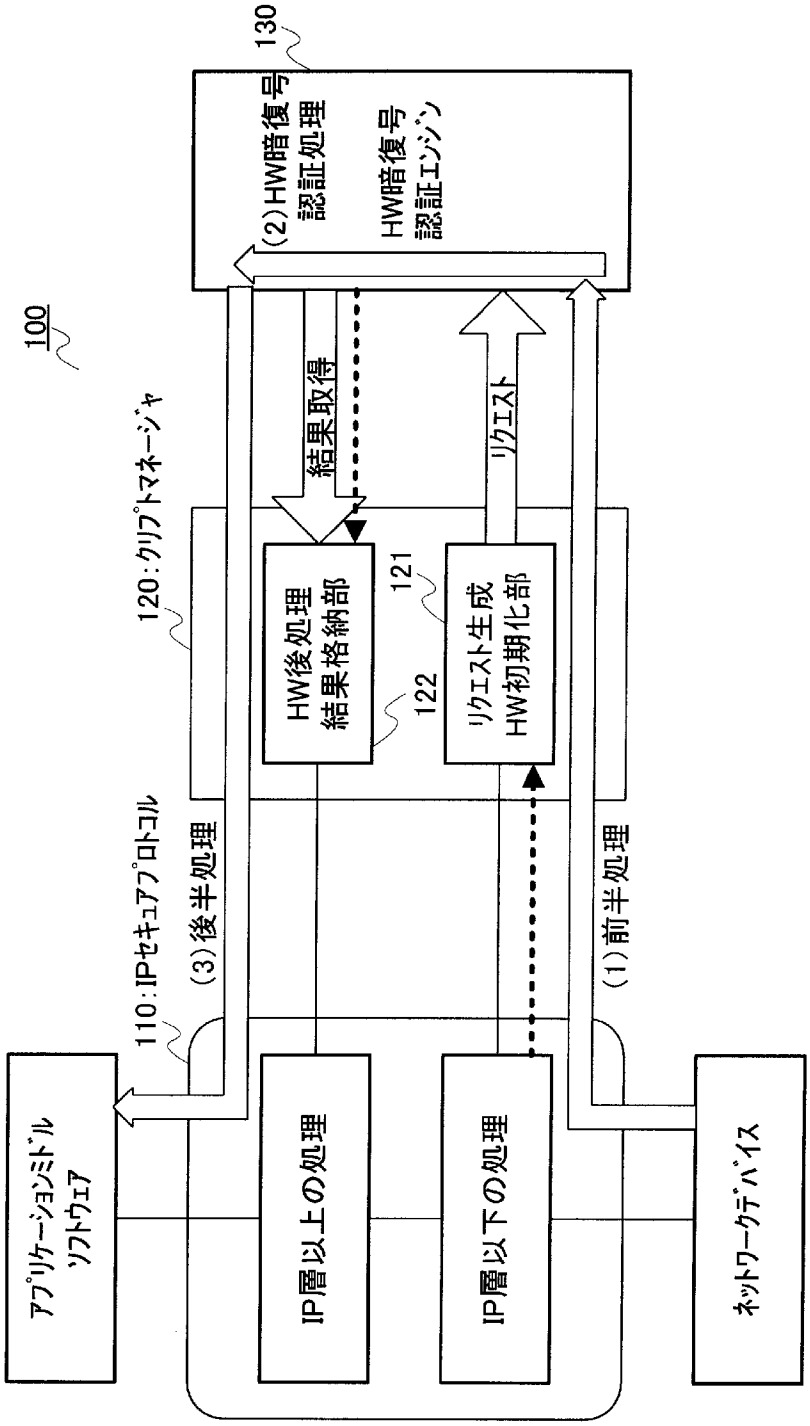
[図2]


10
11
12
13
14
21
22
23
24:キュー
通信スタック部
レイヤ処理1
レイヤ処理2
バッファ
暗号認証処理部
リクエスト制御部
HW前処理部
HW後処理部
HW暗復号認証処理部
req
req
(1)リクエストをキューに積む
(2)HWビジーでない場合処理指示
(3)リクエスト取得
(4)HW処理リクエスト
(5)遅延処理開始指示
(6)HW処理結果取得
(7)後半処理指示

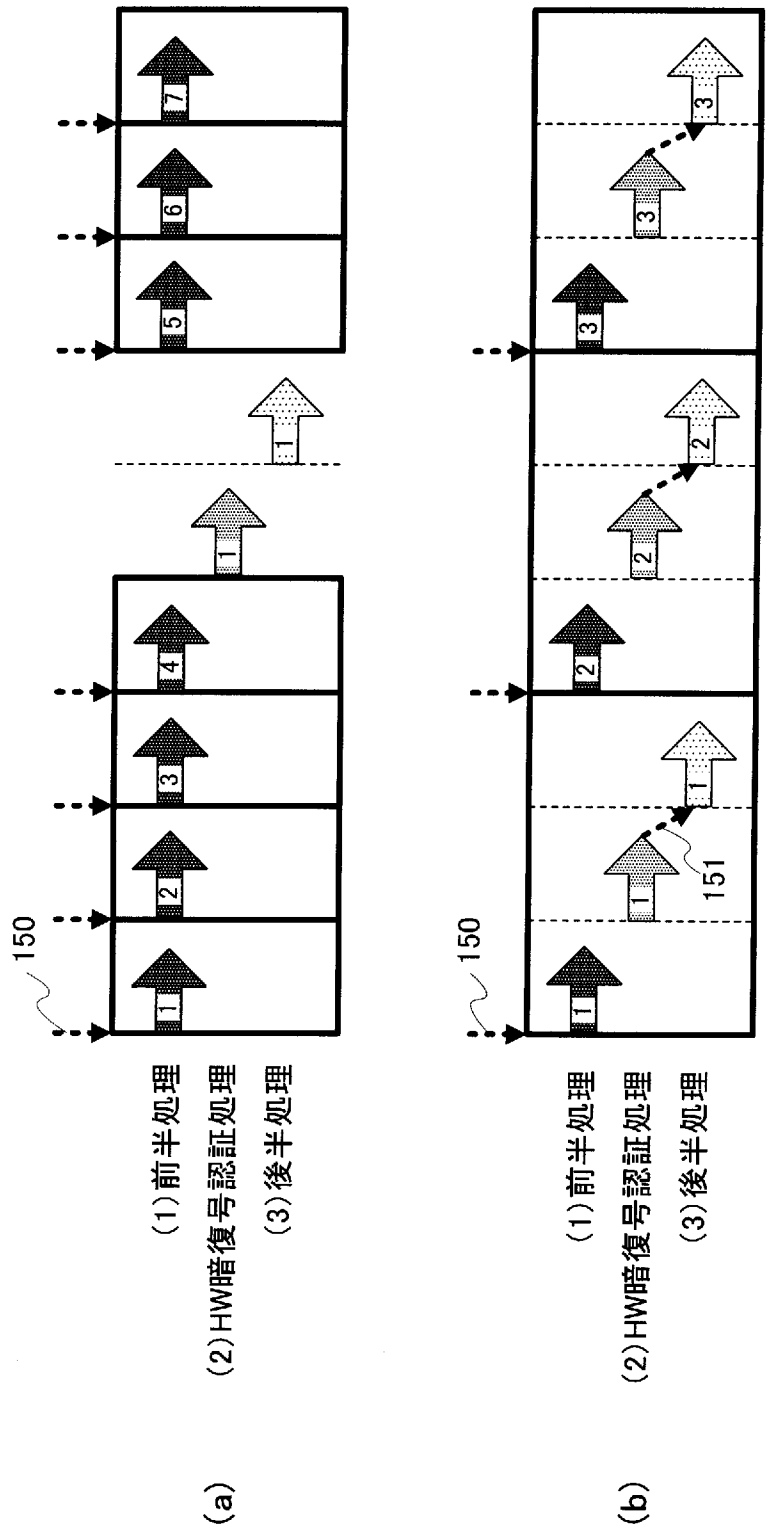
[図3]


(2)レイヤ処理1から
HW前処理
送信/受信コンテキスト
or遅延処理
(2)レイヤ処理1から
利用できない時間
(4)HW処理
リクエスト
(5)遅延処理
開始指示
HW後処理
(7)レイヤ処理2へ
次のHW前処理
(6)HW処理
結果取得
HW割込みコンテキスト
HW割込み
14
HW暗復号認証処理部

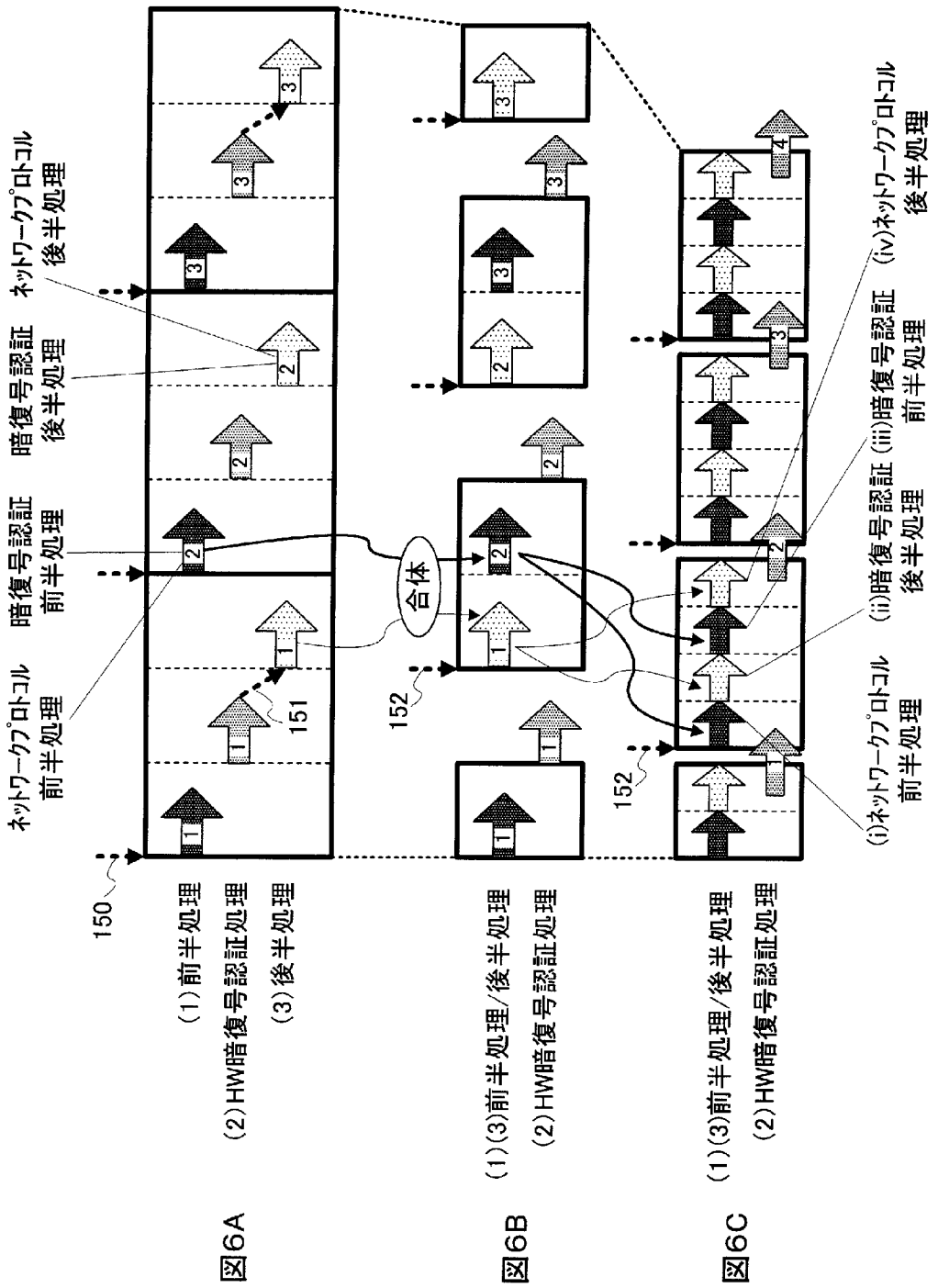
[図4]


100
130
(2)HW暗復号
認証処理
HW暗復号
認証エンジン
結果取得
リクエスト
120:クリプトマネージャ
HW後処理
結果格納部
121
122
リクエスト生成
HW初期化部
110:IPセキュアプロトコル
(3)後半処理
(1)前半処理
アプリケーションミドル
ソフトウェア
IP層以上の処理
IP層以下の処理
ネットワークデバイス

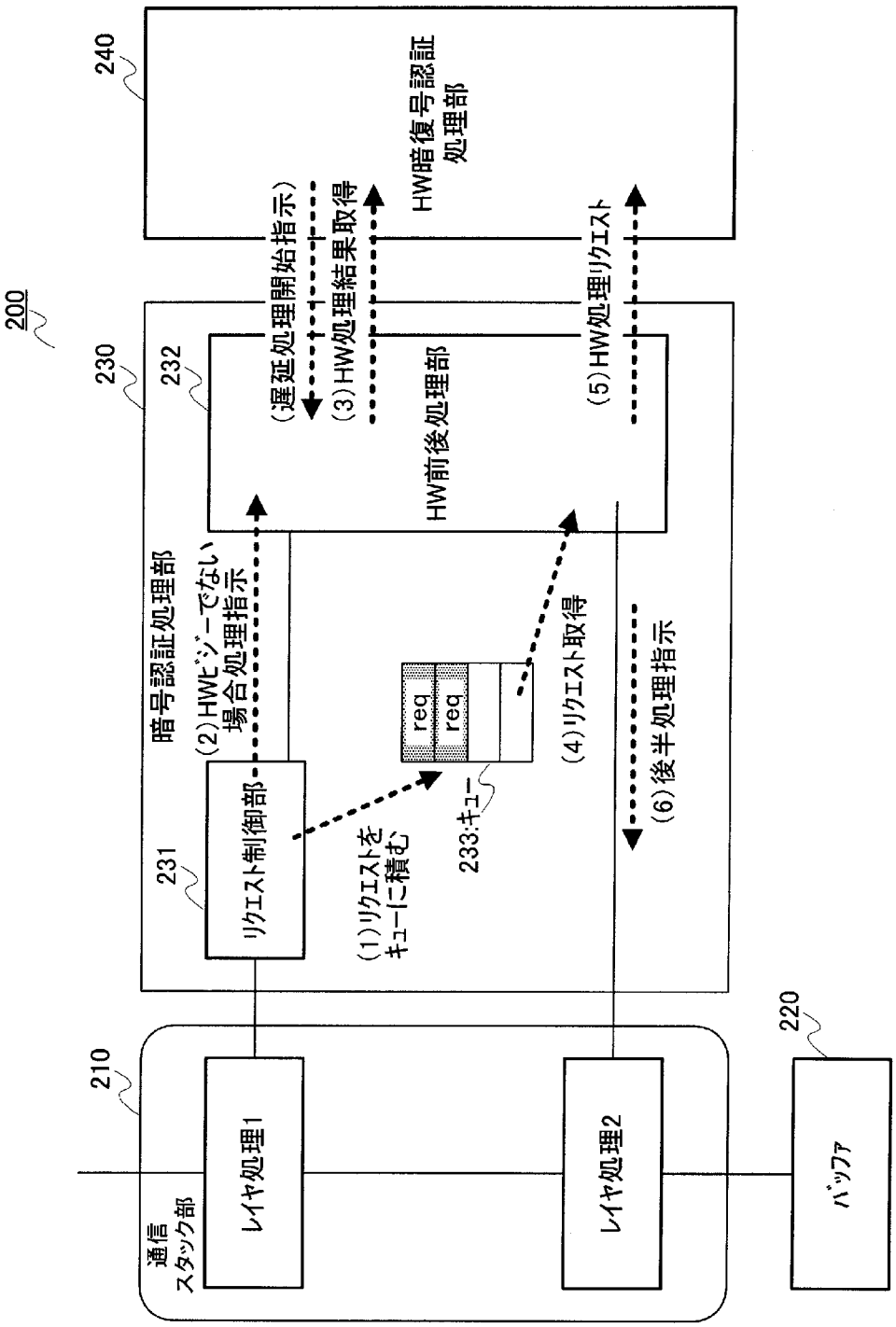
[図5]


150
1
2
3
4
1
5
6
7
(1)前半処理
(2)HW暗復号認証処理
(3)後半処理
(a)
150
1
1
151
2
2
3
3
(1)前半処理
(2)HW暗復号認証処理
(3)後半処理
(b)

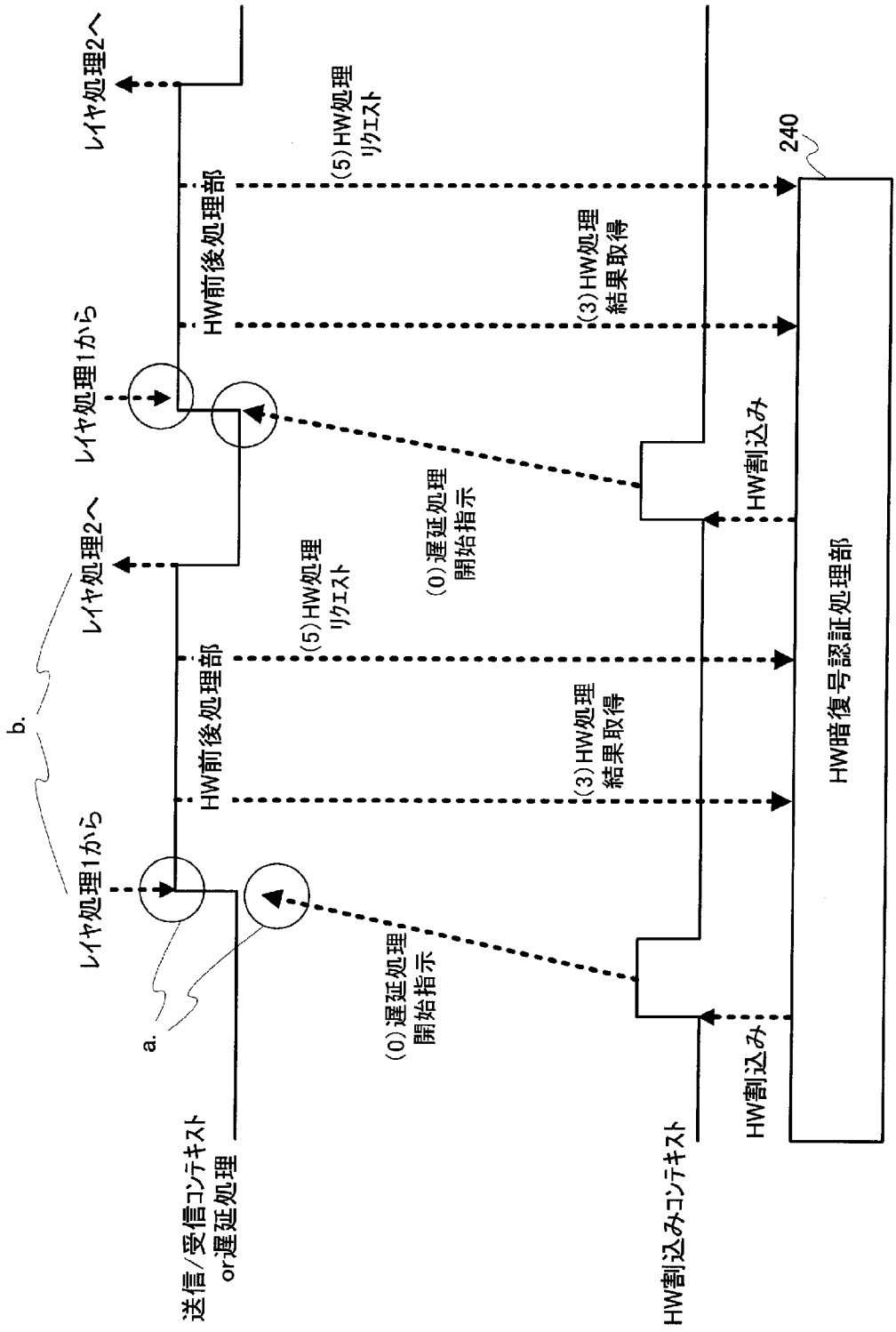
[図6]


ネットワークプロトコル 前半処理
暗復号認証 前半処理
暗復号認証 後半処理
ネットワークプロトコル 後半処理
150
151
152
152
合体
(1)前半処理
(2)HW暗復号認証処理
(3)後半処理
(1)(3)前半処理/後半処理
(2)HW暗復号認証処理
(1)(3)前半処理/後半処理
(2)HW暗復号認証処理
(i)ネットワークプロトコル 前半処理
(ii)暗復号認証 後半処理
(iii)暗復号認証 前半処理
(iv)ネットワークプロトコル 後半処理
図6A
図6B
図6C

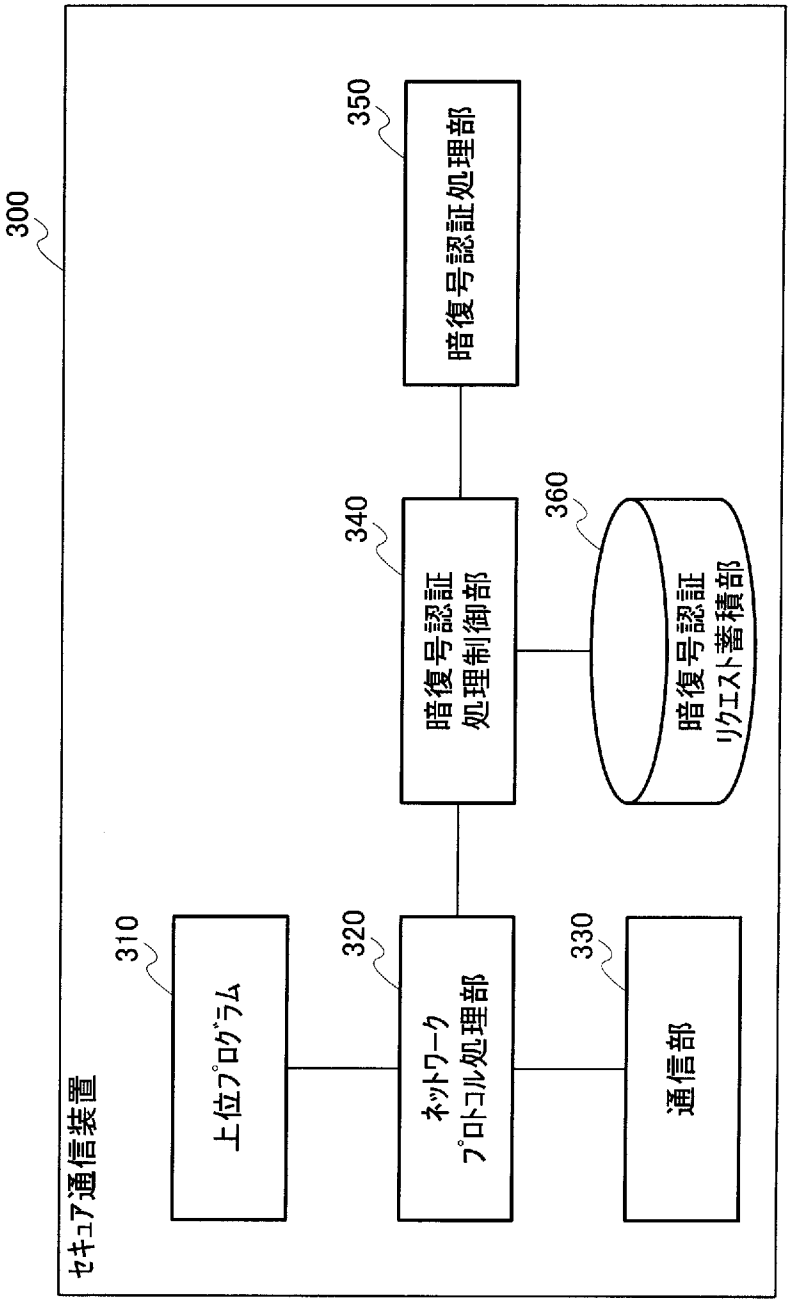
[図7]


200
240
HW暗復号認証処理部
230
232
(遅延処理開始指示)
(3)HW処理結果取得
HW前後処理部
(5)HW処理リクエスト
暗号認証処理部
(2)HWビジーでない場合処理指示
req
req
(4)リクエスト取得
(6)後半処理指示
231
リクエスト制御部
(1)リクエストをキューに積む
233:キュー
210
220
通信スタック部
レイヤ処理1
レイヤ処理2
バッファ

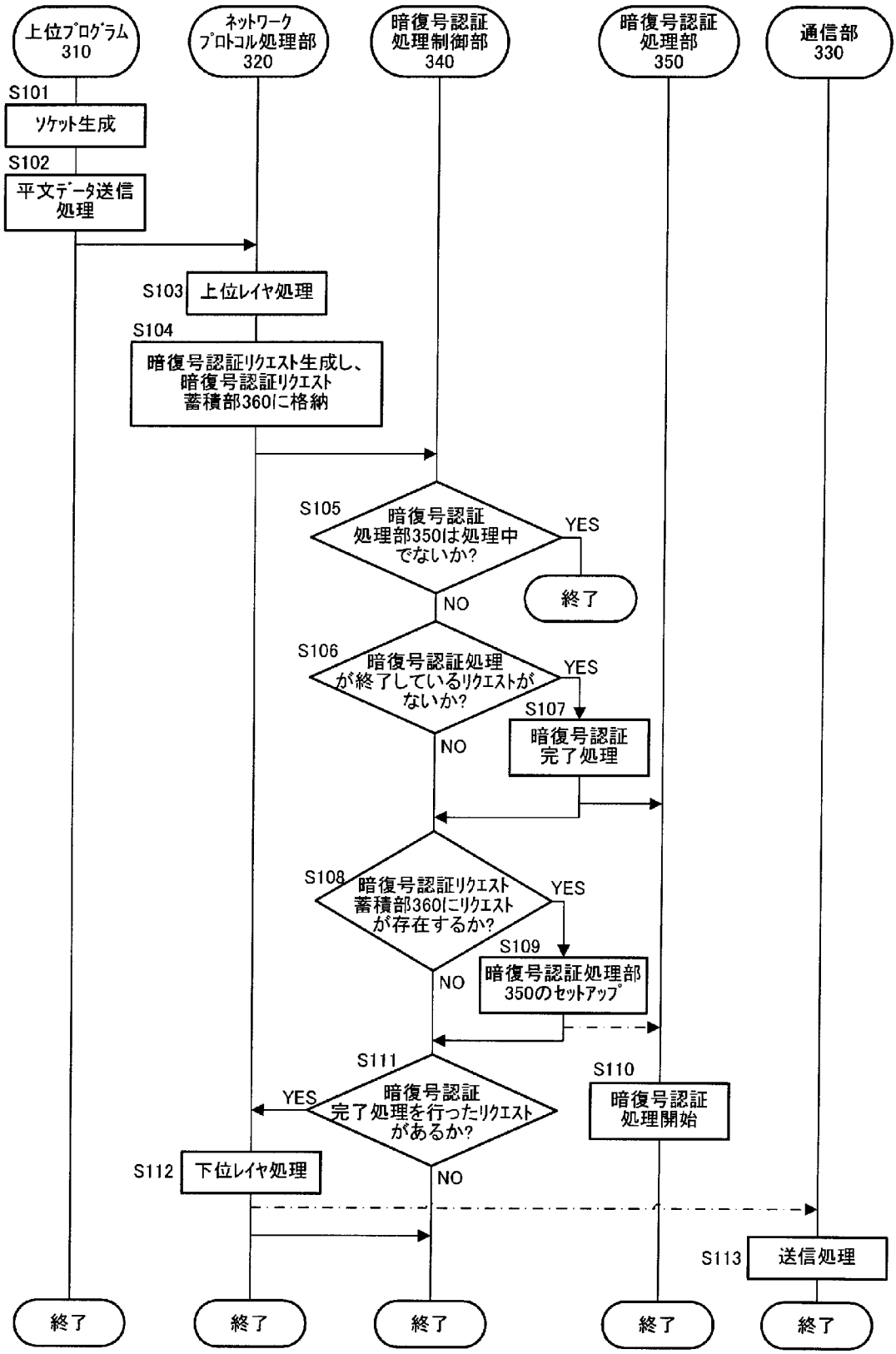
[図8]


レイヤ処理2へ
レイヤ処理1から
HW前後処理部
(5)HW処理
リクエスト
(3)HW処理
結果取得
(0)遅延処理
開始指示
HW割込み
240
HW暗復号認証処理部
送信/受信コンテキスト
or遅延処理
HW割込みコンテキスト
a.
b.

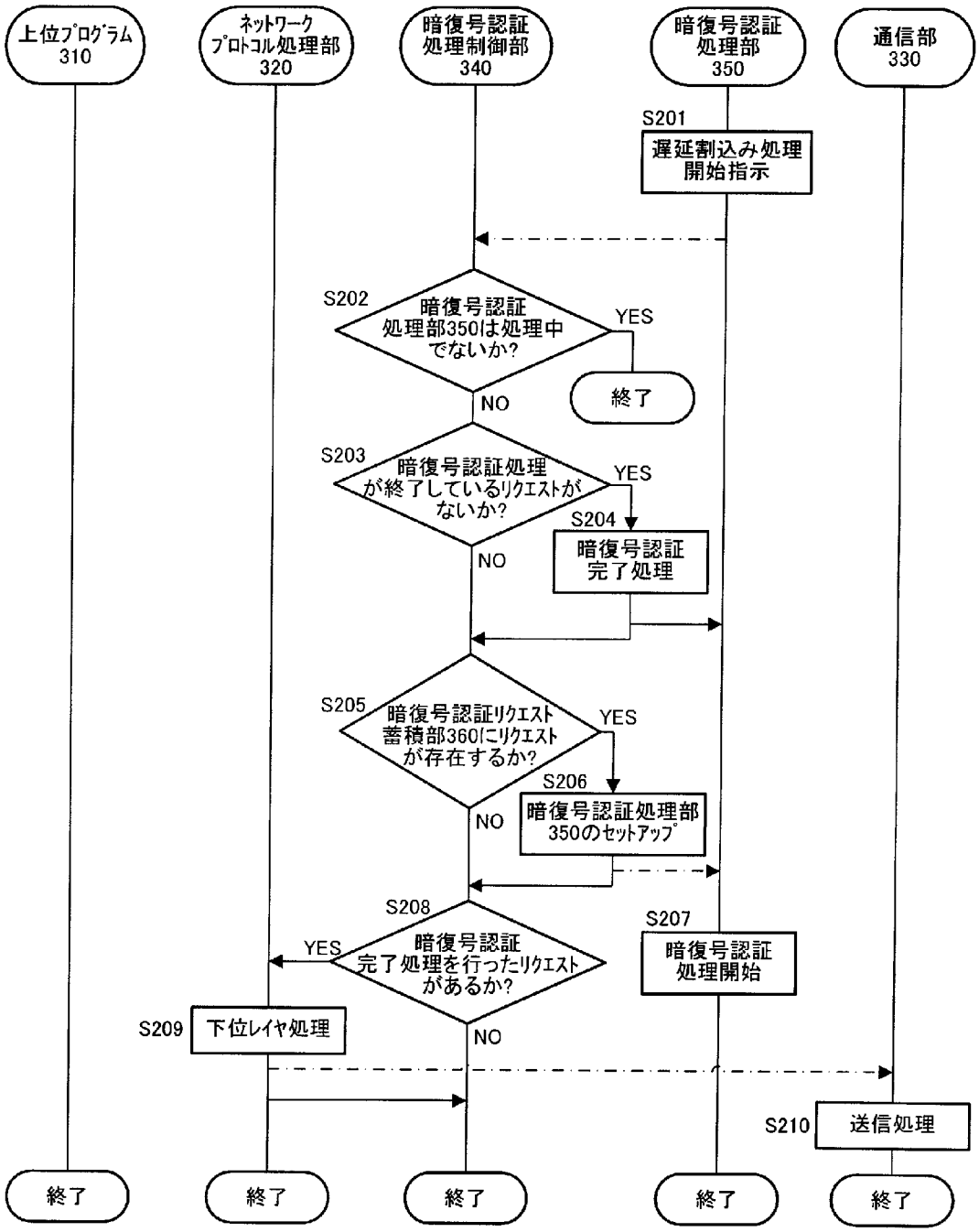
[図9]


300
セキュア通信装置
310
上位プログラム
320
ネットワーク
プロトコル処理部
330
通信部
340
暗復号認証
処理制御部
350
暗復号認証処理部
360
暗復号認証
リクエスト蓄積部

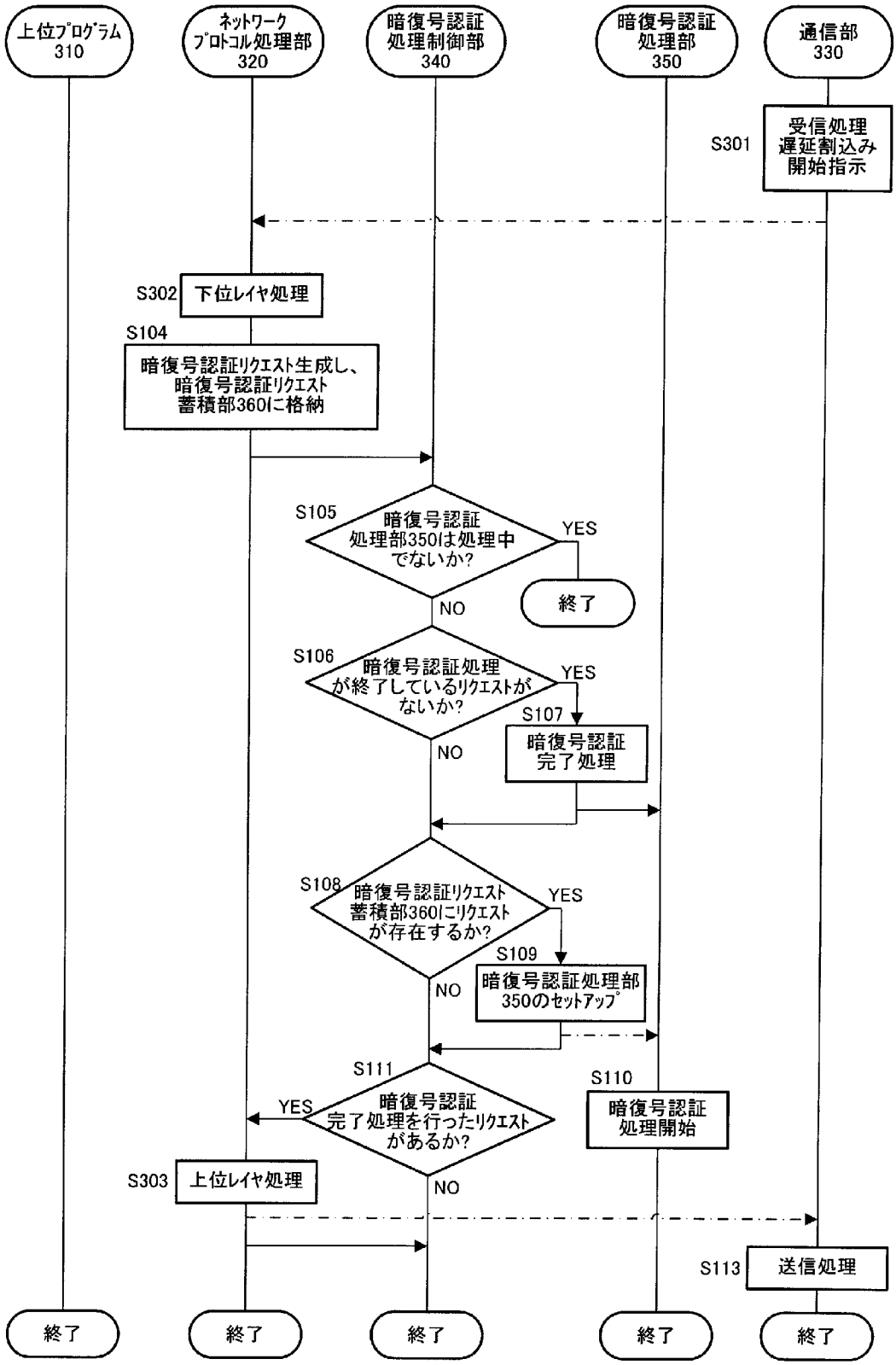
[図10]


上位ﾌﾟﾛｸﾞﾗﾑ 310
ﾈｯﾄﾜｰｸ ﾌﾟﾛﾄｺﾙ処理部 320
暗復号認証 処理制御部 340
暗復号認証 処理部 350
通信部 330
S101
ｿｹｯﾄ生成
S102
平文ﾃﾞｰﾀ送信 処理
S103
上位レイヤ処理
S104
暗復号認証リクエスト生成し、暗復号認証リクエスト蓄積部360に格納
S105
暗復号認証 処理部350は処理中でないか?
YES
終了
NO
S106
暗復号認証処理が終了しているリクエストがないか?
YES
S107
暗復号認証 完了処理
NO
S108
暗復号認証リクエスト蓄積部360にリクエストが存在するか?
YES
S109
暗復号認証処理部350のセットアップ
NO
S111
暗復号認証 完了処理を行ったリクエストがあるか?
YES
S110
暗復号認証 処理開始
S112
下位レイヤ処理
NO
S113
送信処理
終了
終了
終了
終了
終了

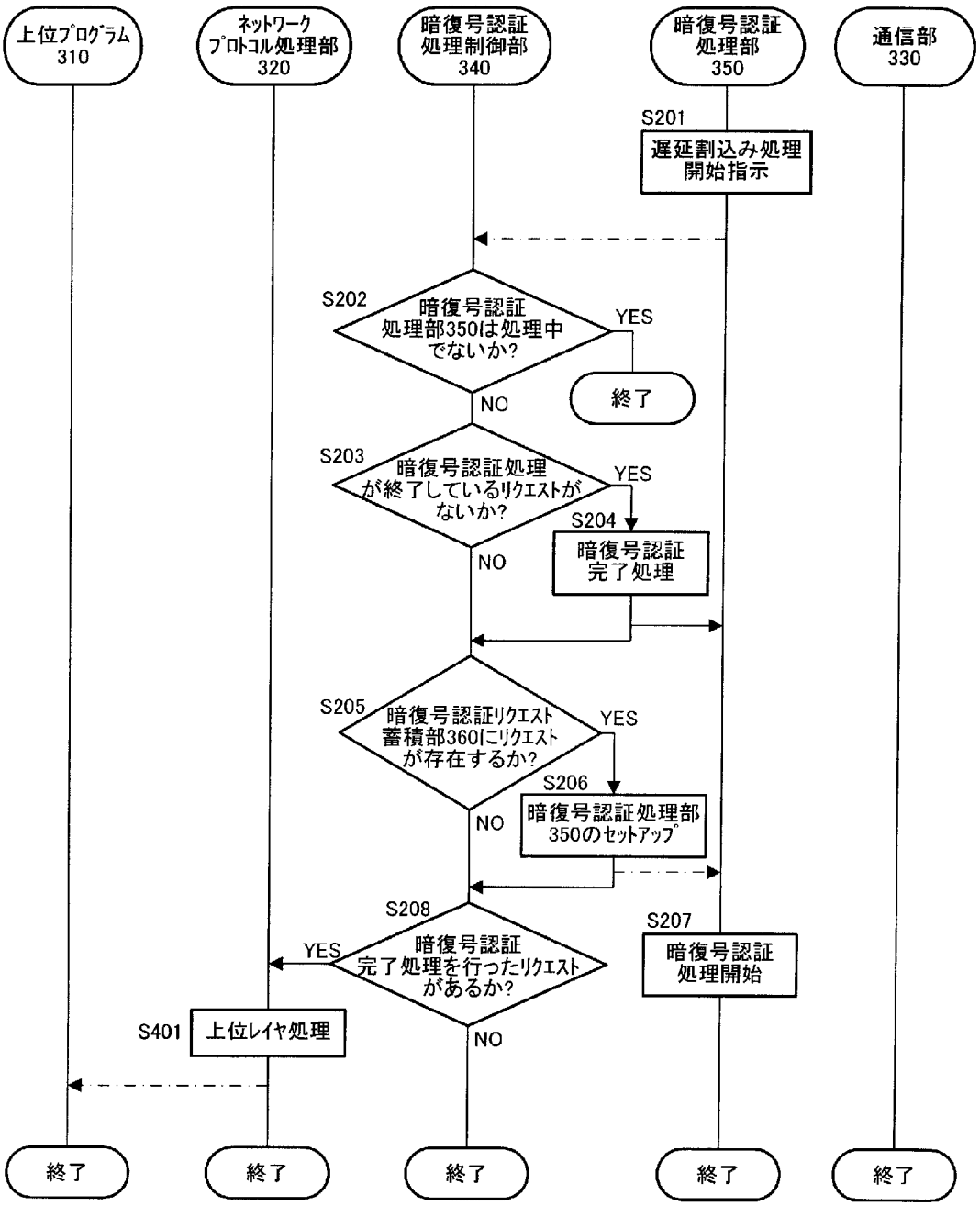
[図11]


上位プログラム
310
ネットワーク
プロトコル処理部
320
暗復号認証
処理制御部
340
暗復号認証
処理部
350
通信部
330
S201
遅延割込み処理
開始指示
S202
暗復号認証
処理部350は処理中
でないか?
YES
終了
NO
S203
暗復号認証処理
が終了しているリクエストが
ないか?
YES
S204
暗復号認証
完了処理
NO
S205
暗復号認証リクエスト
蓄積部360にリクエスト
が存在するか?
YES
S206
暗復号認証処理部
350のセットアップ
NO
S208
暗復号認証
完了処理を行ったリクエスト
があるか?
YES
S207
暗復号認証
処理開始
S209
下位レイヤ処理
NO
S210
送信処理
終了
終了
終了
終了
終了

[図12]


上位プログラム 310
ネットワークプロトコル処理部 320
暗復号認証処理制御部 340
暗復号認証処理部 350
通信部 330
S301
受信処理遅延割込み開始指示
S302
下位レイヤ処理
S104
暗復号認証リクエスト生成し、暗復号認証リクエスト蓄積部360に格納
S105
暗復号認証処理部350は処理中でないか?
YES
終了
NO
S106
暗復号認証処理が終了しているリクエストがないか?
YES
S107
暗復号認証完了処理
NO
S108
暗復号認証リクエスト蓄積部360にリクエストが存在するか?
YES
S109
暗復号認証処理部350のセットアップ
NO
S111
暗復号認証完了処理を行ったリクエストがあるか?
YES
S110
暗復号認証処理開始
S303
上位レイヤ処理
NO
S113
送信処理
終了
終了
終了
終了
終了

[図13]


上位プログラム
310
ネットワーク
プロトコル処理部
320
暗復号認証
処理制御部
340
暗復号認証
処理部
350
通信部
330
S201
遅延割込み処理
開始指示
S202
暗復号認証
処理部350は処理中
でないか?
YES
終了
NO
S203
暗復号認証処理
が終了しているリクエストが
ないか?
YES
S204
暗復号認証
完了処理
NO
S205
暗復号認証リクエスト
蓄積部360にリクエスト
が存在するか?
YES
S206
暗復号認証処理部
350のセットアップ
NO
S208
暗復号認証
完了処理を行ったリクエスト
があるか?
YES
S207
暗復号認証
処理開始
S401
上位レイヤ処理
NO
終了
終了
終了
終了
終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/004239

A. CLASSIFICATION OF SUBJECT MATTER
G09C1/00(2006.01)i

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)
G09C1/00, H04L9/06, H04L9/08, H04L9/10, H04L9/12, H04L9/14, H04L9/16, H04L9/18, H04L9/20, H04L9/22, H04L9/24, H04L9/26, H04L9/28, H04L9/30, H04L9/32, H04L9/34, H04L9/36, H04L9/38, H04L12/22, H04L29/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2009
Kokai Jitsuyo Shinan Koho 1971-2009 Toroku Jitsuyo Shinan Koho 1994-2009

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus(JDreamII)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-164924 A (NEC Access Technica, Ltd.), 07 June, 2002 (07.06.02), Par. Nos. [0010] to [0073]; Figs. 1 to 4 (Family: none)	1-7
A	JP 2002-217951 A (Sony Corp.), 02 August, 2002 (02.08.02), Par. No. [0043]; Fig. 3 & US 2002/0105956 A1	1-7
A	JP 2002-524891 A (SSH Communications Security Ltd.), 06 August, 2002 (06.08.02), Full text; all drawings & US 6253321 B1 & EP 1145520 A & WO 1999/067930 A2	1-7

☒ 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
28 September, 2009 (28.09.09)	06 October, 2009 (06.10.09)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/004239

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2008-512950 A (Cavium Networks), 24 April, 2008 (24.04.08), Full text; all drawings & US 2006/0056406 A1 & US 2007/0038798 A1 & WO 2006/031459 A1	1-7
A	JP 2008-48042 A (Matsushita Electric Industrial Co., Ltd.), 28 February, 2008 (28.02.08), Full text; all drawings & EP 2051434 A & WO 2008/018318 A1	1-7
P,A	JP 2008-310270 A (Panasonic Corp.), 25 December, 2008 (25.12.08), Full text; all drawings & WO 2008/155905 A1	1-7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/004239

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [X] Claims Nos.: 8-14
because they relate to subject matter not required to be searched by this Authority, namely:
Claims 8-14 relate to a method of performing purely mental acts, and the subject matter is not required to be searched by this International Searching Authority under PCT Rule 17(2)(a)(i) and Rule 39.1.

2. [ ] Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. [ ] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. [ ] As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

the

[ ] The additional search fees were accompanied by the applicant's protest and, where applicable, payment of a protest fee.

[ ] The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

[ ] No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００９／００４２３９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G09C1/00(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G09C1/00, H04L9/06, H04L9/08, H04L9/10, H04L9/12, H04L9/14, H04L9/16, H04L9/18, H04L9/20, H04L9/22, H04L9/24, H04L9/26, H04L9/28, H04L9/30, H04L9/32, H04L9/34, H04L9/36, H04L9/38, H04L12/22, H04L29/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００９年
日本国実用新案登録公報	１９９６－２００９年
日本国登録実用新案公報	１９９４－２００９年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlus(JDreamII)

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2002-164924 A (エヌイーシーアクセステクニカ株式会社) 2002.06.07, 段落【００１０】－【００７３】,【図１】－【図４】（ファミリーなし）	１－７
A	JP 2002-217951 A (ソニー株式会社) 2002.08.02, 段落【００４３】,【図３】 & US 2002/0105956 A1	１－７

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ２８．０９．２００９	国際調査報告の発送日 ０６．１０．２００９
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　３１４６ 松平　英 電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Ａ	JP 2002-524891 A（アスアスホー　コミュニケーションズ　セキュリティ　リミティド）2002.08.06，全文，全図 & US 6253321 B1 & EP 1145520 A & WO 1999/067930 A2	１－７
Ａ	JP 2008-512950 A（カビウム・ネットワークス）2008.04.24，全文，全図 & US 2006/0056406 A1 & US 2007/0038798 A1 & WO 2006/031459 A1	１－７
Ａ	JP 2008-48042 A（松下電器産業株式会社）2008.02.28，全文，全図 & EP 2051434 A & WO 2008/018318 A1	１－７
Ｐ，Ａ	JP 2008-310270 A（パナソニック株式会社） 2008.12.25，全文，全図 & WO 2008/155905 A1	１－７

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００９／００４２３９

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第8条第3項（ＰＣＴ17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

１．☐ 請求項　８－１４　は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、
請求項８～１４は、純粋に精神的な行為の遂行に関する方法そのものであり、PCT第17条(2)(a)(i)及びＰＣＴ規則39.1の規定により、この国際調査機関が調査することを要しない対象に係るものである。

２．☐ 請求項　　は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

３．☐ 請求項　　は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第3文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

１．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求項について作成した。

２．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求項について調査することができたので、追加調査手数料の納付を求めなかった。

３．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求項のみについて作成した。

４．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求項について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。

☐ 追加調査手数料の納付はあったが、異議申立てはなかった。