(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
2009 年6 月25 日 (25.06.2009)

PCT

(10) 国際公開番号
WO 2009/078103 A1

(51) 国際特許分類:
H04L 9/36 (2006.01)

(21) 国際出願番号: PCT/JP2007/074439

(22) 国際出願日: 2007 年12 月19 日 (19.12.2007)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 篠崎 敦 (SHINOZAKI, Atsushi) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 松倉 秀実, 外(MATSUKURA, Hidemi et al.); 〒1030004 東京都中央区東日本橋３丁目４番１０号 アクロポリス２１ビル６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, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, JP, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

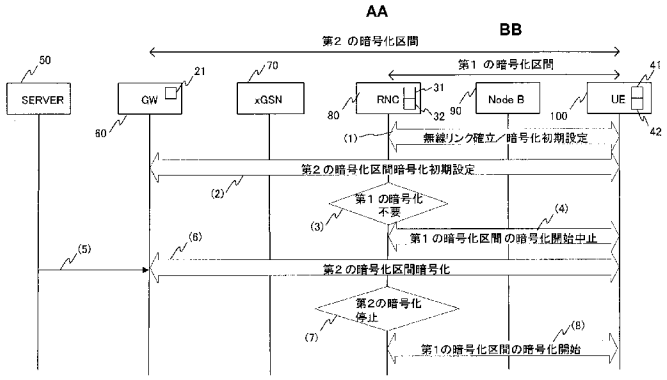
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[続葉有]

(54) **Title:** ENCRYPTION IMPLEMENTATION CONTROL SYSTEM

(54) **発明の名称:** 暗号化実施制御システム

[図10]



AA SECOND ENCRYPTION SECTION
BB FIRST ENCRYPTION SECTION
(1) WIRELESS LINK ESTABLISHMENT/ENCRYPTION INITIAL SETTING
(2) SECOND ENCRYPTION SECTION ENCRYPTION INITIAL SETTING
(3) FIRST ENCRYPTION IS NOT NECESSARY
(4) STOP STARTING ENCRYPTION IN FIRST ENCRYPTION SECTION
(6) SECOND ENCRYPTION SECTION ENCRYPTION
(7) STOP SECOND ENCRYPTION
(8) START ENCRYPTION IN FIRST ENCRYPTION SECTION

(57) **Abstract:** An encryption implementation control system comprises first encryption means for implementing the encryption of communication in a first section between a terminal device and a first relay device, second encryption means for implementing the encryption of communication in a second section including the first section, that is from the terminal device to a second relay device via the first relay device, and control means for controlling the first encryption means so as not to implement the encryption of the communication in the first section when the encryption of the communication in the second section is implemented.

[続葉有]

WO 2009/078103 A1

添付公開書類:
— 国際調査報告書

(57) 要約: 端末装置と第１中継装置との間の第１区間の通信に対する暗号化を実施する第１暗号化手段と、端末装置から第１中継装置を経由して第２中継装置に至る、第１区間を含む第２区間の通信に対する暗号化を実施する第２暗号化手段と、第２区間の暗号化が実施される場合に、第１区間の暗号化が実施されないように第１暗号化手段を制御する制御手段とを含む暗号化実施制御システムである。

明 細 書

暗号化実施制御システム

技術分野

[0001] 本発明は、無線構内交換網(無線LAN:IEEE802．11)やセルラ網(例えば3GPP)のような無線網(移動通信網)のエンドートゥーエンド(End-to-end)で実施される暗号化方法に関する。

背景技術

[0002] 代表的な無線ネットワークシステムとして、無線LAN(IEEE 802.11)を用いたネットワークシステム(無線LANシステム)や、セルラ網システム(3GPP)がある。

[0003] 無線LANシステムは、例えば、図1に示すように、メディアサーバと、メディアサーバにリンク(ネットワーク)を介して接続された無線網ゲートウェイ(GW)と、無線網ゲートウェイにIP網(例えばインターネット)を介して収容されたアクセスポイント(AP)とからなり、APに対し、端末(PC(Personal Computer)、PDA(Personal Digital Assistant)等)が無線リンク(無線伝送路)を介して接続される。APと端末との間がデータ伝送路の無線区間を構成する。

[0004] 通常、無線ネットワークでは通信のセキュリティを考慮して通信データの暗号化が実施される。図1に示したような無線LANシステムでは、図2に示すように、端末とAPとの間の無線区間において、IEEE802.11に基づく暗号化処理が行われる。無線LAN(IEEE802.11)では、暗号化方式として、例えば、WPA2(Wi-Fi Protected Access 2)による暗号化が施される(暗号化アルゴリズムは、TKIP(Temporal Key Integrity Protocol)又はAES(Advanced Encryption Standard))。

[0005] また、端末とGWとの間では、例えばIPsecによる暗号化処理が実施される。さらに、メディアサーバ(サーバ)と端末との間では、アプリケーションレベルの暗号化(例えば、SRTP(Secure Real-time Transport Protocol:RFC3771))が実施される。

[0006] セルラ網システム(携帯電話網システム)は、例えば図3に示すように、サーバと、サーバにリンクを介して接続されたゲートウェイ(GW:ルータ)と、GWにインターネットのようなIP網を介して接続される交換機(xGSN)と、交換機にリンクを介して接続される

基地局制御装置(Radio Network Controller: RNC)と、基地局制御装置にリンクを介して接続される基地局装置(Node B又はBTS(Base Transceiver System))とを備える。基地局装置に対し、移動端末(User Equipment又はMobile Node)が無線リンク(無線伝送路)を介して接続される。移動端末と基地局装置との間がデータ伝送路の無線区間を構成する。

[0007] 図3に示したようなセルラ網(3GPP)の場合には、図4に示すように、RNCと、移動端末(UE)との間において、例えばKASUMIアルゴリズムF8モードによる暗号化が実施される。UEとGWとの間、及びUEとサーバとの間では、図2に示した方式と同様の暗号化を実施することができる。

[0008] 現状、無線ネットワークにおいて適用される暗号化方式は、無線区間の構築時に一意に決定され、通信毎に変更されるものではない。

[0009] 無線ネットワークを利用した即時性を持つ(リアルタイムな)ストリーミング配信を実施する際には、一般に、通信プロトコルとしてRTP(Real-Time Transfer Protocol)が用いられる。RTPを利用する場合には、RTSP(Real-Time Transfer Streaming Protocol)による初期ネゴシエーションが実施される。加えて、通信中における受信側の情報をフィードバックするために、RTCP(RTP control protocol)が用いられる。更に、ストリーミング配信されるデータ(マルチメディアデータ:RTPパケット)に対して、SRTP／SRTCP(Secure RTP/ Secure Real-time Transport Protocol)のような暗号化処理が施される。

[0010] さらに、無線ネットワークを介して企業LANのような構内交換網内の端末装置にストリーミングデータを配信するときに、端末装置とGWとの間でセキュアな接続を提供するために、VPN(Virtual Private Network)設定を行い、IPsec(Security Architecture for Internet Protocol)による通信の秘匿化が行われることがある。

特許文献1:特開2005－347789号公報

発明の開示

発明が解決しようとする課題

[0011] 図2及び図4に示したように、無線ネットワークにおける無線区間では、IEEE802.11に基づく暗号化に加えて、SRTPによる暗号化、及び／又はIPsecによる暗号化が

実施される。このように、暗号化が重複して行われている。このため、暗号化処理が重複する。このような重複する暗号化処理は、暗号化処理を行う装置に無用の負荷を与え、また、暗号化処理のためにリソースを浪費することとなる。

[0012] 本発明の態様の目的は、暗号化処理が冗長になる場合に、不要な暗号化処理が実施されないようにする技術を提供することである。

課題を解決するための手段

[0013] 本発明の態様は、上述した目的を達成するために以下の手段を採用する。

[0014] 第1の態様は、端末装置と第1中継装置との間の第1区間の通信に対する暗号化を実施する第1暗号化手段と、

端末装置から第1中継装置を経由して第2中継装置に至る、前記第1区間を含む第2区間の通信に対する暗号化を実施する第2暗号化手段と、

前記第2区間の暗号化が実施される場合に、前記第1区間の暗号化が実施されないように前記第1暗号化手段を制御する制御手段と

を含む暗号化実施制御システムである。

[0015] 第1の態様は、前記制御手段が、前記第2区間のトラフィックを監視し、前記第2区間の暗号化を実施するためのトラフィックを検知した場合に、前記第2区間の暗号化が実施されると判定するように構成することができる。

[0016] 第1の態様は、前記第1の暗号化手段は、前記第2区間の暗号化が実施される場合に前記制御手段から通知される指示に従って前記第1区間の暗号化の開始を待機する状態となるように構成することができる。

[0017] 第1の態様は、前記制御手段が、前記第2区間で実施されていた暗号化の停止を検知した場合に、前記第1暗号化手段に前記第1区間の暗号化の開始指示を通知するように構成することができる。

[0018] 第1の態様は、前記制御手段が、前記第1中継装置に備えられるように構成することができる。

[0019] 第1の態様は、前記制御手段が、前記端末装置に備えられるように構成することができる。

[0020] 第1の態様において、第1区間に対する暗号化方式は、例えばKASUMI暗号化を

適用できる。第2区間に対する暗号化方式は、IPsecやSRTPを適用することができる。

[0021] 第1の態様は、前記第1暗号化手段が、前記第1区間におけるユーザデータ用通信路及び制御データ用通信路を対象とする暗号化を行い、

前記第2暗号化手段は、前記第2区間を転送されるユーザデータに対する暗号化を行い、

前記第1暗号化手段は、前記第2区間の暗号化が実施される場合に、前記制御手段からの指示に従って、前記ユーザデータ用通信路に対する暗号化の開始を待機する一方で、前記制御データ用通信路に対する暗号化を実施するように構成することができる。

[0022] 第2の態様は、データを中継する中継装置であって、

自装置と端末装置との間の第1区間の通信の暗号化を行う暗号化処理部と、

前記端末装置から自装置を経由して他の中継装置に至る、前記第1区間を含む第2区間の通信の暗号化が実施されるか否かを判定し、前記第2区間の暗号化が実施される場合に、前記暗号化部を前記第1区間の暗号化を実施しない状態にする制御部と

を含む中継装置である。

[0023] 第3の態様は、2以上の中継装置を介して他の装置と通信する端末装置であって、

自装置と第1中継装置との間の第1区間について、前記第1中継装置との間で通信の暗号化を行う第1暗号化処理部と、

自装置から前記第1中継装置を経由して第2中継装置に至る前記第1区間を含む第2区間について前記第2中継装置との間で暗号化を行う第2暗号化処理部と、

前記第2区間の暗号化が実施される場合に、前記第1暗号化処理部を前記第1区間の暗号化を実施しない状態にする制御部と

を含む端末装置である。

[0024] 第1の態様で採用可能な構成は、第2及び第3の態様においても適用が可能である。また、本発明は、第1～第3の態様と同様の特徴を有する方法の発明として実現可能である。

発明の効果

[0025] 本発明の態様によれば、暗号化処理が冗長になる場合に、不要な暗号化処理が実施されないようにすることができる。

図面の簡単な説明

[0026] [図1]無線LAN(IEEE802.11)システムの構成例を示す。

[図2]無線LANシステムにおける暗号化処理の例を示す。

[図3]セルラ網(3GPP)システムの構成例を示す。

[図4]セルラ網システムにおける暗号化処理の例を示す。

[図5]無線LANシステムにおいて、無線区間の暗号化処理が回避された状態を示す。

[図6]セルラ網システムにおいて、無線区間の暗号化処理が回避された状態を示す。

[図7]本実施形態におけるネットワークシステム(暗号化処理制御システム)の構成例を示す。

[図8]IPsecの概要を示す。

[図9]ESPブロックのデータ構造を示す。

[図10]具体例に係るネットワークシステム構成を示すとともに、網側の判断による第1の暗号化区間の暗号化処理制御の説明を示す。

[図11]RNCの暗号化処理部による処理例を示すフローチャートである。

[図12]RNCの判断部による処理例を示すフローチャートである。

[図13]第2の暗号化区間での暗号化処理の実施の有無を端末装置で判断する場合における第1の暗号化区間の暗号化処理制御の説明を示す。

[図14]第1の暗号化区間であるRNCとUEとの間にユーザチャネルとしてのDTCHと制御チャネルとしてのDCCHとが設けられている場合における、暗号化処理の概要を示す。

符号の説明

[0027] 10・・・送信装置

20・・・通信装置(第2中継装置)

21・・・第2の暗号化区間の暗号化／復号化処理部

30・・・通信装置(第1中継装置)

31・・・第1の暗号化区間の暗号化／復号化処理部

32・・・第1の暗号化区間の暗号化／復号化処理の実施有無の判断部

40・・・端末装置

41・・・第1暗号化処理部

42・・・第2暗号化処理部

50・・・サーバ

60・・・ゲートウェイ(GW)

70・・・交換機(xGSN)

80・・・基地局制御装置(RNC)

90・・・基地局装置(Node B)

100・・・端末装置(UE)

発明を実施するための最良の形態

[0028] 以下、図面を参照して本発明の実施形態を説明する。実施形態の構成は例示であり、本発明は実施形態の構成に限定されない。

[0029] 〔概要〕

上述したように、現状の無線ネットワークシステムでは、重複した暗号化が実施されていた。このような状況に鑑み、本発明の実施形態として、例えば、図1に示したような無線LANシステムにおけるアクセスポイント(AP)や、無線ネットワークゲートウェイ(GW)が、RTSP(Real Time Streaming Protocol)に従って、エンドートゥーエンド(End-to-End:例えば、メディアサーバと移動端末)でのSRTPネゴシエーションを観測することができる装置を備える。このとき、SRTPによる暗号化処理が或るRTPセッションについて実施される場合には、無線LAN(無線区間)での暗号化処理をそのRTPセッションについて実施しない。

[0030] 但し、当該処理は、上記したRTPセッションと同時に発生している他のセッションやその他のメディアに関する通信から独立して実施される。例えば、移動端末(端末装置)が、ストリーミング配信と並列にWebアクセスを行う場合がある。このとき、このWebアクセスに関するセッションについて無線区間での暗号化処理が要求される場合に

は、無線区間での暗号化処理が実施される。

[0031] また、実施形態では、或るRTPセッションに係る通信についてIPsecが実施されるかどうかを監視し、実施される場合には、無線区間での暗号化処理を回避する。

[0032] 図5は、図1に示したような無線LANシステムにおいて、無線区間の暗号化処理が回避された状態を示し、図6は、図3に示したようなセルラ網システムにおいて、無線区間の暗号化処理が回避された状態を示す。

[0033] 図7は、本実施形態におけるネットワークシステム(暗号化処理制御システム)の構成例を示す図である。図7に示すネットワークシステムは、送受信装置10と、第2中継装置としての通信装置20と、第1中継装置としての通信装置30と、端末装置40とを備える。

[0034] 端末装置40は、データの送受信機能を有しており、端末装置40と送受信装置10との間で送受信されるデータは、所定の通信経路を通る。この通信経路の一方の端点が端末装置40であり、他方が送受信装置10である。通信装置20及び通信装置30は、通信経路上に配置され、送受信装置10と端末装置40との間で送受信されるデータの中継装置として機能する。

[0035] このような通信経路に関して、端末装置40と通信装置30との間の区間は、この区間で送受信されるデータが暗号化される第1の暗号化区間(第1区間に相当)として定義されている。一方、端末装置40と通信装置20との間の区間は、この区間でデータが暗号化される第2の暗号化区間(第2区間に相当)として定義されている。

[0036] このように、第1の暗号化区間は、第2の暗号化区間に含まれている(重なっている)。従って、第1の暗号化区間と第2の暗号化区間との双方で並列に暗号化通信が実施される場合には、第1の暗号化区間を流れるデータは、第2の暗号化区間について適用される暗号化方式で暗号化された暗号化データが、さらに第1の暗号化区間について適用される暗号化方式で暗号化された状態となる。すなわち、第1の暗号化区間では、冗長な暗号化処理が実施される。

[0037] 通常、第1の暗号化区間及び第2の暗号化区間の夫々には、異なるタイプの暗号化方式が適用される。但し、第1及び第2の暗号化区間に関して、同種類の暗号化方式が適用されることは妨げられない。

[0038] 端末装置40は、第1の暗号化区間で暗号化通信を実施するための第1暗号化処理部41と、第2の暗号化区間で暗号化通信を実施するための第2暗号化処理部42とを備えている。

[0039] 通信装置30は、第1暗号化区間で暗号化通信を行うための暗号化処理部31を備える。暗号化処理部31は、端末装置40の第1暗号化処理部41との間で、第1の暗号化区間について適用される暗号化方式(第1の暗号化方式)に関するネゴシエーション及び初期設定を行い、通信装置30を端末装置40との間(第1の暗号化区間)で第1の暗号化方式に基づく暗号化通信を実施可能な状態にする。

[0040] 第1の暗号化区間での暗号化通信が実施される場合には、通信装置30と端末装置40との一方からは、第1の暗号化方式で暗号化された暗号化データが送信され、他方で暗号化データの復号化が実施される。

[0041] このように、暗号化処理部31及び第1暗号化処理部41は、第1の暗号化区間を流れるデータの暗号化を行う第1暗号化手段として機能する。

[0042] 通信装置20は、第2暗号化区間で暗号化通信を実施するための暗号化処理部21を備えている。暗号化処理部21は、端末装置40の第2暗号化処理部42との間で、第2の暗号化方式に関するネゴシエーション及び初期設定を行い、第2の暗号化区間で適用される暗号化方式(第2の暗号化方式)に基づく暗号化通信を実施可能な状態にする。

[0043] 第2の暗号化区間での暗号化通信が実施される場合には、通信装置20と端末装置40との一方からは、第2の暗号化方式で暗号化された暗号化データが送信され、他方で暗号化データの復号化が実施される。

[0044] また、暗号化処理部21及び第2暗号化処理部42は、第2の暗号化区間を対象とする暗号化及び復号化処理を行う第2暗号化／復号化手段として機能する。

[0045] 通信装置30は、第2暗号化区間の暗号化実施有無の判断部32をさらに備える。判断部32は、第2の暗号化区間での暗号化の実施の有無に応じて第1の暗号化区間での暗号化の実施を制御する制御手段として機能する。

[0046] 判断部32は、通信装置20と端末装置40との間(第2の暗号化区間)の通信(トラフィック)を監視し、第2の暗号化区間での暗号化が実施されるか否かを決定(判定)する。

[0047] 第2の暗号化区間で暗号化が実施されない場合には、暗号化処理部31に対して特になにもしない。この場合、暗号化処理部31では、第1の暗号化区間の暗号化に関するネゴシエーション及び初期設定が実施され、第1の暗号化区間を送受信されるデータの暗号化／復号化処理が実施される。

[0048] これに対し、第2の暗号化方式による暗号化が実施される場合には、判断部32は、暗号化処理部31による暗号化処理(データの暗号化／復号化)を停止(中止)させることができる。

[0049] また、判断部32は、第2の暗号化区間の監視において、第2の暗号化区間の暗号化が停止されたことを検知したときに、暗号化処理部31による第1の暗号化区間の暗号化が中止状態であれば、暗号化処理部31に対して暗号化処理を開始させることができる。

[0050] このように、第1の暗号化区間に対する暗号化は、第2の暗号化区間の暗号化が実施されるか否かの判断結果に基づいて実施される。このため、通信装置30の判断部32にて、第2の暗号化区間に対する暗号化が行われるか否かがチェックされる。

[0051] 第2の暗号化区間に対する暗号化が行われる場合には、第1の暗号化区間に対する暗号化を実施せず、第2の暗号化区間の暗号化が実施されない場合には、第1の暗号化区間の暗号化が実施される。さらに、第1の暗号化区間に対する暗号化が停止された後、第2の暗号化区間の暗号化が行われなくなったことが検知(検出)された場合には、第1の暗号化区間に対する暗号化が開始(再開)される。

[0052] ここで、第1の暗号化区間に対する暗号化に関して、第2の暗号化区間に対する暗号化が行われるか否かに関わらず、第1の暗号化区間の暗号化に関して必要な設定のすべてが実施され、第1の暗号化区間に対する暗号化の開始を保留させる。

[0053] また、第1の暗号化区間が、第2の暗号化区間から独立した通信路を持つ場合、例えば3GPPシステムにおいて、ユーザデータを取り扱うDTCH(Dedicated Traffic CHannel)とは独立した制御チャネルとしてのDCCH(Dedicated Control CHannel)が存在するような場合には、DTCHのみが暗号化を実施するか否かの制御対象とされ、DCCHは制御対象に含まれない(第2の暗号化区間とは無関係に暗号化が行われる)ようにすることができる。

[0054] なお、図7では、暗号化処理部31と判断部32とを通信装置30が備える例が示されている。但し、判断部32は、暗号化処理部31と物理的に離れた位置(例えば、通信装置30と異なる装置)に位置していても良い。すなわち、暗号化処理部31には、判断部32における判断結果に基づく暗号化処理の開始／停止指示が伝達され、暗号化処理部31が開始／停止指示に従って、制御対象の通信に係るデータに対する暗号化処理を実施するように構成されていれば良い。

[0055] 〔具体例〕

〈IPsecの概要〉

図8は、IPsecの概要を示す。IPsecでは、通信開始前に暗号化方法に関するネゴシエーションがIKE(Internet Key Exchange:RFC2409)の手順で実施される。

[0056] フェーズ1では、通信を行うホスト(装置)間で、フェーズ2で利用する暗号方式を決定するとともに、暗号化のための暗号鍵を生成する。フェーズ1で生成された暗号鍵は装置間で共有される。

[0057] フェーズ2では、共有された鍵を用いてIPsecで使用する暗号方式や暗号鍵など(SA:security association)を決定する。この手順は特定のパケットを用いて行われる。例えば、ISAKMP(Internet Security Association and Key Management Protocol:RFC2408)のパケットがこのフェーズ2で利用される。

[0058] このため、図7に示したネットワークシステムにおいて、例えば、通信装置20と端末装置40との間で実施されるISAKMPパケットを用いたIKEシーケンスを確認することは、これらの中間に位置する通信装置30(の判断部32)で可能である。

[0059] ISAKMPは、IANA(Internet Assigned Number Authority)によってTCP／UDP(Transfer Control Protocol/User Datagram Protocol)のポート番号“500”が割り当てられている。

[0060] 図9は、ESPブロックのデータ構造を示す。IKEによるネゴシエーションが完了したら、IPsecでは、ESP(Encapsulating Security Payload)と呼ばれるブロックに転送対象のデータブロック(図9の例では、TCP／UDPパケット)がカプセル化される。すなわち、カプセル化されるデータブロックがESP中のペイロードデータ格納領域にマッピングされる。

[0061] ESPブロックはIPヘッダが付与されて転送される(IPヘッダが付与されたESPブロックを「ESPパケット」と称する)。ESPパケットのペイロード、すなわちESPブロックはIPsecに基づき暗号化される。このため、ESPパケットは、セキュアな環境で転送される。なお、ESPブロックに付与されるIPヘッダの“Next Header field”には、ESP用に割り当てられた番号“50”が格納される。

[0062] IPsecには、トランスポート・モードと、トンネル・モードとがある。トランスポート・モードでは、送信ホストが送信対象の元データを暗号鍵で暗号化し、IPヘッダを付与して送信する。このIPパケットは、受信ホストで受信される。受信ホストは、IPパケットからヘッダを除去し、残ったデータ部分に対する復号化処理を行うことで、元データを得る。

[0063] このように、トランスポート・モードでは、送信ホストと受信ホストとの間で、暗号化されたデータ(ESPブロック)を有するIPパケットが送受信される。

[0064] トンネル・モードでは、送信ホストから送信側ゲートウェイにIPパケットが転送される。送信側ゲートウェイ(IPsec処理ゲートウェイ)は、送信ホストからのIPパケットを暗号化し、IPパケット中にカプセル化し、受信側ゲートウェイ(IPsec処理ゲートウェイ)へ転送する。受信側ゲートウェイでは、IPパケットからIPヘッダを除去し、残りのデータ部分を復号化して、元のIPパケットを得る。受信側ゲートウェイは、このIPパケットを暗号化することなく受信ホストへ転送する。このように、トンネル・モードでは、ゲートウェイ間の通信のみに暗号化が施される。

[0065] 本実施形態では、IPsecのトランスポート・モードが使用される場合を想定する。

[0066] 図10は、具体例に係るネットワークシステム構成を示すとともに、網側の判断による第1の暗号化区間の暗号化処理制御の説明を示す。

[0067] 図10に示すように、具体例に係るシステムとして、セルラ網システム(3GPP)が示されている。セルラ網システムは、データ要求に応じてストリーミングデータのようなデータ配信を行うサーバ50と、サーバにリンクを介して接続されたゲートウェイ(GW)60と、GW60にIP網(例:インターネット)を介して接続される交換機(xGSN)70と、xGSN70にリンクを介して接続される基地局制御装置(RNC)80と、RNC80にリンクを介して接続される基地局装置(Node B)90とを備え、基地局装置90に対して端末装置(

UE)100が無線リンク(無線伝送路)を介して接続される。

[0068] 図10において、サーバ50とUE100とが通信経路の二つの端点となる。この通信経路上において、UE100とRNC80との間の区間が、図7を用いて説明した第1の暗号化区間に相当し、UE100とGW80との間の区間が、第1の暗号化区間を含む第2の暗号化区間に相当する。

[0069] UE100は、図7に示したような、第1暗号化処理部41及び第2暗号化処理部42を備えた端末装置40に相当する。また、RNC80が、暗号化処理部31及び判断部32を備えた通信装置30に相当する。また、GW60が、暗号化処理部21を備えた通信装置20に相当する。そして、サーバ50が、図7における送信装置10に相当する。

[0070] 第1の暗号化区間では、RNC80とUE100との間で、例えば、KASUMIアルゴリズムF8モード(KASUMI暗号化:第1の暗号化方式)による暗号化通信を実施可能である。このため、第1の暗号化区間では、RNC80とUE100との間で通信コネクション(無線リンクを含む)の確立処理が行われる。さらに、第1の暗号化区間での暗号化を行うために、RNC80の暗号化処理部31とUE100の第1暗号化処理部41との間で行われるネゴシエーション(メッセージ交換)が実施され、このネゴシエーションの結果に応じた暗号化の初期設定がRNC80の暗号化処理部31及びUE100の第1暗号化処理部41の夫々において行われる。これによって、第1の暗号化区間において、暗号化通信が可能な状態となる(図10(1))。

[0071] 第2の暗号化区間では、GW60とUE100との間で、IPsec(トランスポート・モード:第2の暗号化方式)による暗号化通信を実施可能である。この第2の暗号化方式による暗号化通信を開始するために事前に実行される初期設定は、GW60の暗号化処理部21とUE100の第2暗号化処理部42との間で行われるネゴシエーション(メッセージ交換:IKE)を通じて実施される。

[0072] RNC80における判断部32は、第2の暗号化区間の暗号化に関わるネゴシエーションを実施しているトラフィックを観測することができる。この観測結果を元に、第2の暗号化区間に対する暗号化が行われるか否かを判断することができる。

[0073] 例えば、判断部32は、RNC80を通過するIPパケットのIPアドレス及びポート番号から、GW60とUE100との間の暗号化ネゴシエーションに関するトラフィックを検出

することができる。トラフィックを識別するための情報(IPアドレス等)に関して、GW80のIPアドレスが予めRNC80の判断部32に設定される。また、RNC80は、例えば、UE100とのコネクション確立手順の際に、UE100からそのIPアドレスを取得することができる。

[0074] 上述したように、ISAKMPには、IANAによってTCP／UDPのポート番号“500”が割り当てられている。このため、判断部32は、ポート番号“500”を有するGW60とUE100との間のトラフィック(パケット)の有無をチェックすることで、IPsecのネゴシエーションが行われているか否かを判断することができる。

[0075] また、IPsecによって暗号化されたパケットには、IPヘッダの“Next Header Field”に“50番”が割り当てられる。このため、判断部32は、GW60とUE100との間を転送されるIPパケットが上記した“50番”を有するか否かを判断することで、両者間で通信中のパケットが暗号化されているか否かを確認することができる。

[0076] 判断部32は、上記トラフィック観測を通じて、GW60の暗号化処理部21とUE100の第2暗号化処理部42との間で実施されるIPsecネゴシエーション(図10(2))を確認した場合には、第1の暗号化区間の暗号化は不要と判断する(図10(3))。このような判断時における、第1の暗号化区間の状況に応じて、判断部32は以下のような処理を行う。

[0077] すなわち、第1の暗号化区間に関する暗号化が不要と判断した場合において、暗号化処理の初期設定が完了済みであるが、暗号化処理が開始されていない状況(暗号化開始待機状態)の下では、判断部32は、暗号化処理部31に対してその待機状態を維持するための指示を与える。暗号化処理部31は、指示に従って待機状態を維持する。

[0078] これに対し、暗号化処理部31が既に暗号化を開始していた場合には、判断部32は、暗号化処理部31に対して暗号化の停止指示を与える。暗号化処理部31は、停止指示に従って、暗号化／復号化処理を停止(中止)する。

[0079] また、暗号化処理部31における暗号化の初期設定が完了していない場合には、判断部32は、暗号化処理部31に対して初期設定完了後における暗号化開始を停止するための指示を与える。この場合、暗号化処理部31は、指示に従って、暗号化開

始の停止状態(開始指示待ち状態)となる。

[0080] 上記したいずれの場合においても、判断部32は、暗号化処理部31に対して、暗号化処理部31が暗号化の開始待機状態となるための指示(待機指示と呼ぶ)を与える。これによって、第1の暗号化区間に関する暗号化が中止された状態となる(図10(4))。暗号化処理部31で暗号化が中止される場合には、この中止がUE100に通知され、UE100の第1暗号化処理部41でも、暗号化／復号化処理が中止される。

[0081] これに対し、第2の暗号化区間では、この区間に関する初期設定完了後、GW60の暗号化処理部21とUE100の第2暗号化処理部42との間で、IPsecによる暗号化通信が実施される。例えば、UE100がサーバ50からダウンロードするストリーミングデータ(図10(5))に対し、IPsecによる暗号化処理が施される(図10(6))。暗号化処理部21で実施された暗号化は、UE100の第2暗号化処理部42で復号される。このため、無線リンクを含む第1の暗号化区間でも、IPsecによるセキュリティが確保される。このようにして、第1の暗号化区間で冗長な暗号化が実施されないようにすることができる。

[0082] その後、判断部32は、第2の暗号化区間の暗号化を監視し、暗号化が停止されたと判断すると(図10(7))、暗号化処理部31に暗号化の開始指示を与え、第1の暗号化区間の暗号化を開始(再開を含む)させることができる。このとき、暗号化の開始がUE100の第1暗号化処理部41に通知される。これによって、無線リンクを含む第1の暗号化区間でのセキュリティが確保される。

[0083] 第2の暗号化区間における暗号化の停止は、例えば、UE100と網(GW60)との間における仮想閉域網(VPN)接続の終了に伴って行われる。判断部32は、GW60とUE100とのトラフィックから両者間のネゴシエーションを監視し、仮想閉域網(VPN)の解除を認識することが可能である。或いは、固定であるVPN接続に関して宛先が変更された場合でも認識が可能である。

[0084] 図11は、RNC80の暗号化処理部31による処理例を示すフローチャートであり、図12は、RNC80の判断部32による処理例を示すフローチャートである。

[0085] 図11に示す処理は、RNC80とUE100との間で、基地局90を介したコネクションの確立を契機に開始される。暗号化処理部31は、UE100の第1暗号化処理部41と

の間で、第1の暗号化区間に対する暗号化に関するネゴシエーション及び初期設定を行う(OP01)。

[0086] このネゴシエーション及び初期設定中において、暗号化処理部31は、判断部32から待機指示を受信したか否かを判定する(OP02)。待機指示が受信された場合には、暗号化処理部31は、ネゴシエーション及びネゴシエーション結果に基づく初期設定の終了後、暗号化開始を待機する状態となる(OP03)。

[0087] これに対し、待機指示がない場合には、暗号化処理部31は、ネゴシエーション及び初期設定が終了したか否かを判定し(OP04)、ネゴシエーション及び初期設定が終了していない場合には、処理をOP01に戻す。ネゴシエーション及び初期設定が終了している場合には、暗号化処理部31は、暗号化を開始するまでの間に、待機指示を判断部32から受信したか否かを判定する(OP05)。

[0088] このとき、判断部32からの待機指示を受信した場合には、暗号化処理部31は、暗号化開始の待機状態となる(OP06)。暗号化開始までに待機指示がない場合には、暗号化処理部31は、暗号化を開始する(OP07)。

[0089] 暗号化の開始後、暗号化処理(暗号化／復号化)が行われている際に、判断部32から待機指示が与えられた場合には(OP08;YES)、暗号化処理部31は、暗号化処理を停止して、暗号化の開始を待機する状態となる(OP09)。

[0090] 待機指示がない場合(OP08;NO)には、暗号化処理部31は、通信終了か否かを判定し(OP10)、通信終了であれば、所定の終了処理を行い、図11の処理を終了する。これに対し、通信終了でなければ、処理をOP08に戻す。

[0091] 上述したOP03、OP06及びOP09の処理により、暗号化処理部31は、待機指示に従って、暗号化の開始を待機する状態(暗号化実施のサスペンド状態)となる。この場合、暗号化処理部31は、判断部32からの暗号化の開始(再開を含む)の指示を待ち受ける状態となる(OP12)。

[0092] 判断部32から開始指示が与えられた場合には、処理がOP07へ進み、サスペンド状態が解除され、暗号化処理が開始される。開始指示がない場合には、通信終了か否かが判定される(OP12)。このとき、通信終了でなければ、処理がOP11に戻り、通信終了であれば、所定の終了処理が行われ、図11の処理が終了する。

[0093] 図12に示す処理は、例えば、RNC80とUE100との間で、基地局90を介したコネクションの確立を契機に開始される。判断部32は、GW60とUE100との間のトラフィックを監視し(OP21)、第2の暗号化区間に関する暗号化処理が実施されるか否かを判定する(OP22)。

[0094] 第2の暗号化区間に関する暗号化処理が実施される場合には、判断部32は、暗号化処理部31に対して待機指示を送信する(OP23)。これにより、暗号化処理部31が第1の暗号化区間の暗号化開始の待機状態となる。

[0095] その後、判断部32は、トラフィックの監視を継続し(OP24)、第2の暗号化区間の暗号化が停止されたか否かを判定する(OP25)。暗号化が停止された場合には、判断部32は、第1の暗号化区間に対する暗号化の開始(再開を含む)指示を暗号化処理部31に送信する(OP26)。これによって、第1の暗号化区間での暗号化処理が開始される。このような暗号化の中止は、UE100の第1暗号化処理部41にも通知される。

[0096] その後、通信終了か否かが判定され(OP27)、通信終了でなければ、処理がOP21に戻る。通信終了であれば、判断部32は、必要に応じて終了処理を行い、図12の処理を終了する。

[0097] 図10～図12に示した例では、RCE80が判断部32を備える。これに対し、判断部32は、端末装置(UE)が備えるように構成することもできる。即ち、端末装置側で、IPsecによる網との通信を実施する場合に、網側に対して第2の暗号化区間での暗号化を実施するため第1の暗号化区間での暗号化は不要である旨を通知することでも実現可能である。例えば、セルラ網システム(3GPP)の場合では、端末装置は、網側との制御リンク(制御チャネル:DCCH)を有する。この制御チャネルを用いて、第1の暗号化区間の暗号化(例えばKASUMI暗号化)を停止することを通知することが可能である。第1の暗号化処理を制御する網側装置(図7の通信装置30)に対して、第1の暗号化区間の暗号化処理を停止(中止)することを通知する手段(機構)を別途設けても良い。

[0098] 図13は、第2の暗号化区間での暗号化処理の実施の有無を端末装置としてのUE100で判断する場合における第1の暗号化区間の暗号化処理制御の説明を示す。

[0099] 図13におけるセルラ網システムは、図10に示したシステムとほぼ同様の構成を備

える。但し、この例では、UE100が、第2の暗号化区間に関する暗号化の実施有無を判断する判断部32を備えている。

[0100] 図13において、UE100は、第1の暗号化区間に関する暗号化処理を行う網側装置であるRNC80との間で、無線リンクを含むコネクションの確立処理、及び第1の暗号化区間に対する暗号化処理の初期設定が実施される(図13(1))。

[0101] その後、GW60とUE100との間で、第2の暗号化区間に対する暗号化処理(IPsec)のネゴシエーション及び初期設定が実施されたと仮定する(図13(2))。

[0102] このような初期設定は、GW60の暗号化処理部21とUE100の第2暗号化処理部42との間で実施される。このため、判断部32は、例えば、第2暗号化処理部42から、第2の暗号化区間に対する暗号化初期設定の実施の通知を受け取ることで、第2の暗号化区間の暗号化が実施されることを認識(判断)することができる(図13(3))。

[0103] すると、UE100は、RNC80に対して、第1の暗号化区間に対する暗号化開始の待機指示(暗号化処理が不要である旨)を通知する。このとき、例えば、両者間を接続する制御チャネル(DCCH)を用いることができる。これによって、第1の暗号化区間の暗号化の開始が中止される(図13(4))。

[0104] その後、例えば、UE100がサーバ50からストリーミングデータのようなデータをダウンロードする場合には、サーバ50からUE100へ転送されるデータ(図13(5))に対し、GW60の暗号化処理部21でIPsecに基づく暗号化処理が行われ、UE100まで転送される。UE100では、第2暗号化処理部42がデータの復号を行う。このような処理は、図10の例と同様である。

[0105] その後、UE100が、例えばGW60との間でのVPN解除を行うことによって、UE100の判断部32は、第2の暗号化区間に対する暗号化が停止されると認識(判断)することができる(図13(7))。

[0106] この場合、UE100は、RNC80の暗号化処理部31に対して、第1の暗号化区間に対する暗号化の開始(再開)指示を、例えば制御チャネルを介して通知することができる。これによって、第1の暗号化区間での暗号化処理が開始される(図13(8))。

[0107] このように、端末装置で第2の暗号化区間の暗号化の実施の有無が判断される場合には、端末装置(ここではUE100)は、第1の暗号化区間の暗号化処理を実施する

装置(ここではRNC80)に対して、暗号化処理開始の待機指示(中止指示)や、暗号化処理の開始(再開)指示を通知する通知手段を備えた装置として機能する。

[0108] 図13に示す例における、RNC80の暗号化処理部31の処理は、図11に示した処理と同様である。但し、待機指示や開始(再開)指示は、UE100からRNC80へ通知されたものを受信する。

[0109] 一方、UE100における判断部32の処理は、図12に示した処理と同様である。即ち、UE100における判断部32は、OP21やOP24において、第2暗号化処理部42による第2の暗号化区間の暗号化に関するネゴシエーション(トラフィック)を監視して、第2の暗号化区間の暗号化の実施及び停止を判定することができる。

[0110] 判断部32は、第2の暗号化区間の暗号化の実施を判定(検知)した場合には、第1の暗号化区間の暗号化開始の待機指示をRNC80へ送信(通知)する(OP23)。また、第2の暗号化区間の暗号化の停止を判定(検知)した場合には、第1の暗号化区間に対する暗号化開始(再開)指示をRNC80へ送信(通知)する(OP25)。これらの指示は、UE100とRNC80との間を結ぶ制御リンクを用いて通知することができる。

[0111] なお、上記の説明では、サーバ50からUE100へのデータ転送方向(下り方向)に関して説明したが、UE100からサーバ50へのデータ転送方向(上り方向)についても、同様の処理が行われる。

[0112] ところで、第1の暗号化区間における通信経路として、ユーザデータ用の通信路(DTCHのようなユーザチャネル)と制御データ用の通信路(DCCHのような制御チャネル)とが独立に存在する場合には、第1の暗号化区間に対する暗号化の中止(開始の待機)は、ユーザデータ用の通信路(DCCH)のみを対象とする。

[0113] 第1の暗号化区間の暗号化(例えばKASUMI暗号化)は、DTCHとDCCHとの双方を対象として行われる。これに対し、第2の暗号化区間に対して実施されるIPsecの暗号化は、ユーザデータのみを対象とする。よって、DCCHに対する暗号化が停止されないようにすることで、DCCHのトラフィックに対するセキュリティを確保することができる。

[0114] 図14は、第1の暗号化区間であるRNC80とUE100との間にユーザチャネルとしてのDTCHと制御チャネルとしてのDCCHとが設けられている場合における、暗号

化処理の概要を示す。

[0115] 図14に示すように、第1の暗号化区間に対する暗号化処理が実施される場合には、DTCH及びDCCHの双方のトラフィックを対象とした暗号化処理が実施される。これに対し、待機指示によって第1の暗号化区間に対する暗号化処理が中止(停止)される場合には、DTCHのみが停止の対象となり、DCCHに対する暗号化処理は停止されない。よって、図10(4)及び図13(4)の動作、及び図11に示したOP、図11のOP03、OP06及びOP09の処理は、ユーザチャネルであるDTCHのみを対象として実施される。

[0116] なお、上記した具体例では、第2の暗号化区間で実施される暗号化方式がIPsecである場合について説明したが、他の暗号化方式(例えばSRTP)であっても良い。また、第1の暗号化区間で実施される暗号化方式もKASUMI暗号化に限られない。

[0117] また、無線網制御装置と第1の暗号化区間に対する暗号化処理を行う装置とが物理的に分離されている場合で、第2の暗号化処理が行われているか否かを無線ネットワーク制御装置が観測する態様も採用することができる。例えば、RNC80が判定部32を有し、基地局装置90が暗号化処理部31を備える場合である。

[0118] この場合、RNC80は、第2の暗号化区間のトラフィックを監視することによって第1の暗号化区間の暗号化を行わないと判断した場合に、基地局装置90に、暗号化を行わないことを通知する。この場合、基地局装置90は、第1の暗号化区間の暗号化を行わないために、対向する端末装置(UE100)に対して第1の暗号化区間の暗号化を行わないように制御する。また、基地局装置90が備える暗号化処理部31は、自らの暗号化処理を実施しない。

[0119] 〈実施形態の効果〉

本発明の実施形態によれば、第2の暗号化区間の暗号化の実施に応じて、第2の暗号化区間と重複する第1の暗号化区間での暗号化を中止することができる。また、第2の暗号化区間の暗号化の停止に応じて、第1の暗号化区間における暗号化を開始(再開)することもできる。

[0120] 従って、第1の暗号化区間に対して不要な暗号化処理を行わずにすむ。このため、ネットワークの処理能力に対する影響を抑えることができ、システムの容量向上に繋

がる。例えばセルラ網(3GPP)システムの場合において、暗号化処理を行わないことは、処理可能なコネクション数を倍増させることが可能である。また、第1の暗号化区間中の無線区間に係る暗号化処理上で暗号化の同期外れが発生して暗号化や復号化が失敗することや、この失敗に基づく通信障害を回避することが可能となる。さらに、暗号化処理を実施しないことで、暗号化処理を行う装置での消費電力低減を図ることができる。

請求の範囲

[1] 端末装置と第1中継装置との間の第1区間の通信に対する暗号化を実施する第1暗号化手段と、

端末装置から第1中継装置を経由して第2中継装置に至る、前記第1区間を含む第2区間の通信に対する暗号化を実施する第2暗号化手段と、

前記第2区間の暗号化が実施される場合に、前記第1区間の暗号化が実施されないように前記第1暗号化手段を制御する制御手段と

を含む暗号化実施制御システム。

[2] 前記制御手段は、前記第2区間のトラフィックを監視し、前記第2区間の暗号化を実施するためのトラフィックを検知した場合に、前記第2区間の暗号化が実施されると判定する

請求項1に記載の暗号化実施制御システム。

[3] 前記第1の暗号化手段は、前記第2区間の暗号化が実施される場合に前記制御手段から通知される指示に従って前記第1区間の暗号化の開始を待機する状態となる

請求項1に記載の暗号化実施制御システム。

[4] 前記制御手段は、前記第2区間で実施されていた暗号化の停止を検知した場合に、前記第1暗号化手段に前記第1区間の暗号化の開始指示を通知する

請求項1に記載の暗号化実施制御システム。

[5] 前記制御手段は、前記第1中継装置に、あるいは前記端末装置に備えられる

請求項1に記載の暗号化実施制御システム。

[6] 前記第2暗号化手段はIPsecによる、あるいはSRTPによる暗号化処理を実施する

請求項1に記載の暗号化実施制御システム。

[7] 前記第1暗号化手段は、前記第1区間におけるユーザデータ用通信路及び制御データ用通信路を対象とする暗号化を行い、

前記第2暗号化手段は、前記第2区間を転送されるユーザデータに対する暗号化を行い、

前記第1暗号化手段は、前記第2区間の暗号化が実施される場合に、前記制御手段からの指示に従って、前記ユーザデータ用通信路に対する暗号化の開始を待機

する一方で、前記制御データ用通信路に対する暗号化を実施する

請求項1に記載の暗号化実施制御システム。

[8] データを中継する中継装置であって、

自装置と端末装置との間の第1区間の通信の暗号化を行う暗号化処理部と、

前記端末装置から自装置を経由して他の中継装置に至る、前記第1区間を含む第2区間の通信の暗号化が実施されるか否かを判定し、前記第2区間の暗号化が実施される場合に、前記暗号化部を前記第1区間の暗号化を実施しない状態にする制御部と

を含む中継装置。

[9] 2以上の中継装置を介して他の装置と通信する端末装置であって、

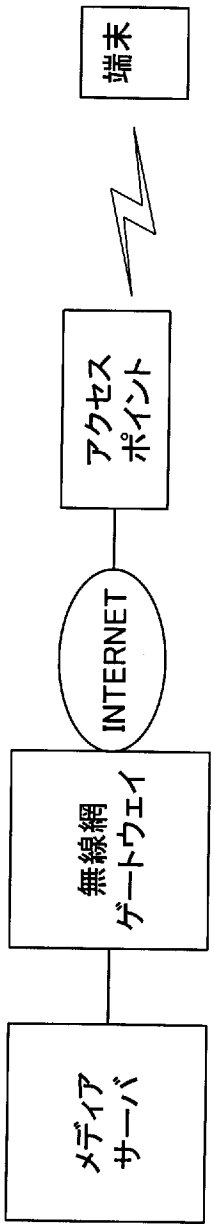
自装置と第1中継装置との間の第1区間について、前記第1中継装置との間で通信の暗号化を行う第1暗号化処理部と、

自装置から前記第1中継装置を経由して第2中継装置に至る前記第1区間を含む第2区間について前記第2中継装置との間で暗号化を行う第2暗号化処理部と、

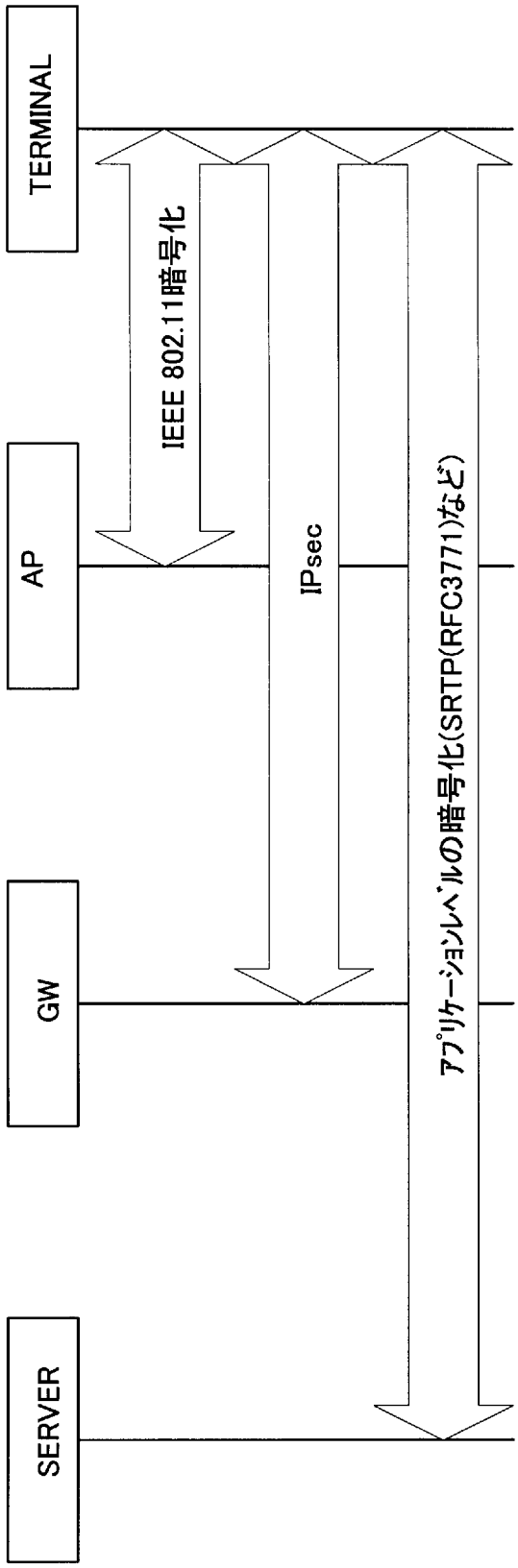
前記第2区間の暗号化が実施される場合に、前記第1暗号化処理部を前記第1区間の暗号化を実施しない状態にする制御部と

を含む端末装置。

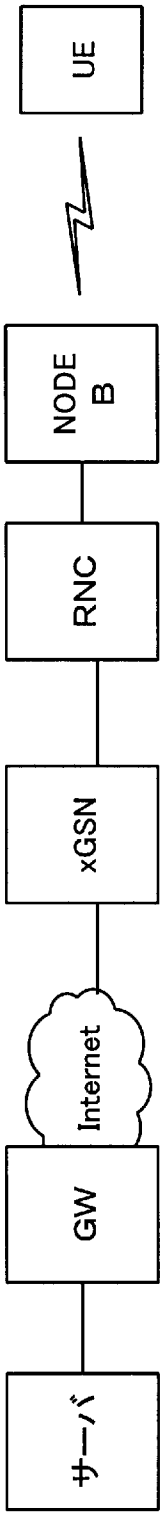
[図1]



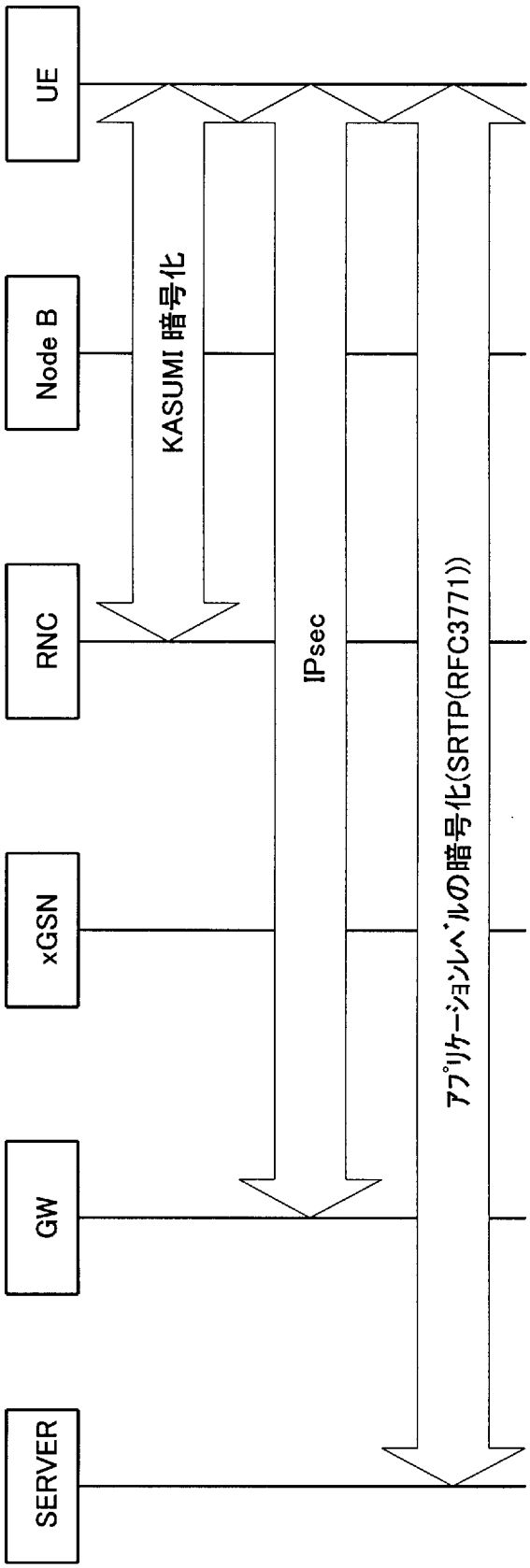
[図2]


TERMINAL
AP
GW
SERVER
IEEE 802.11暗号化
IPsec
アプリケーションレベルの暗号化(SRTP(RFC3771)など)

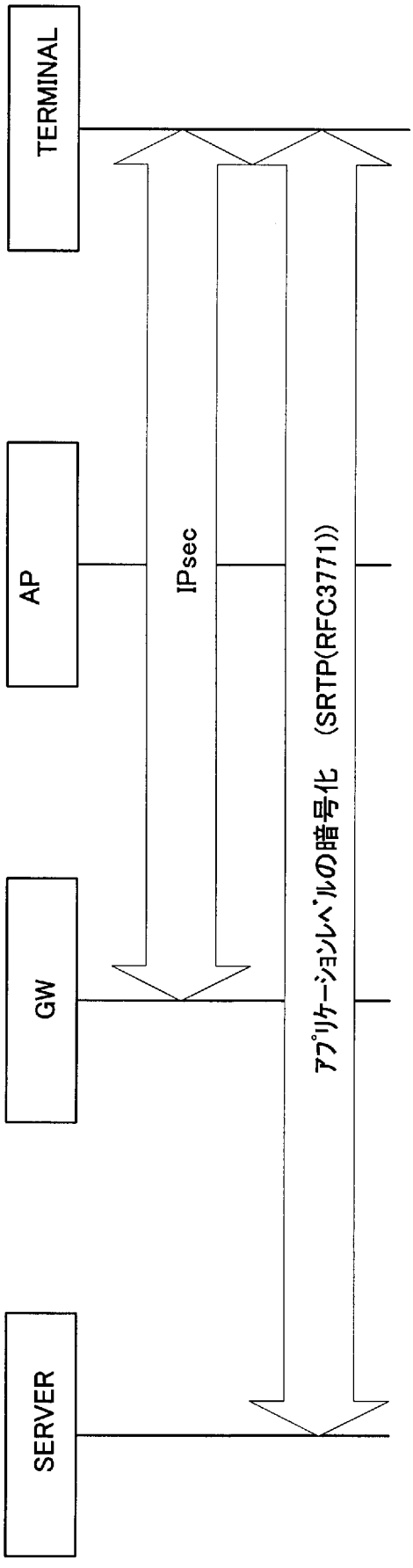
[図3]



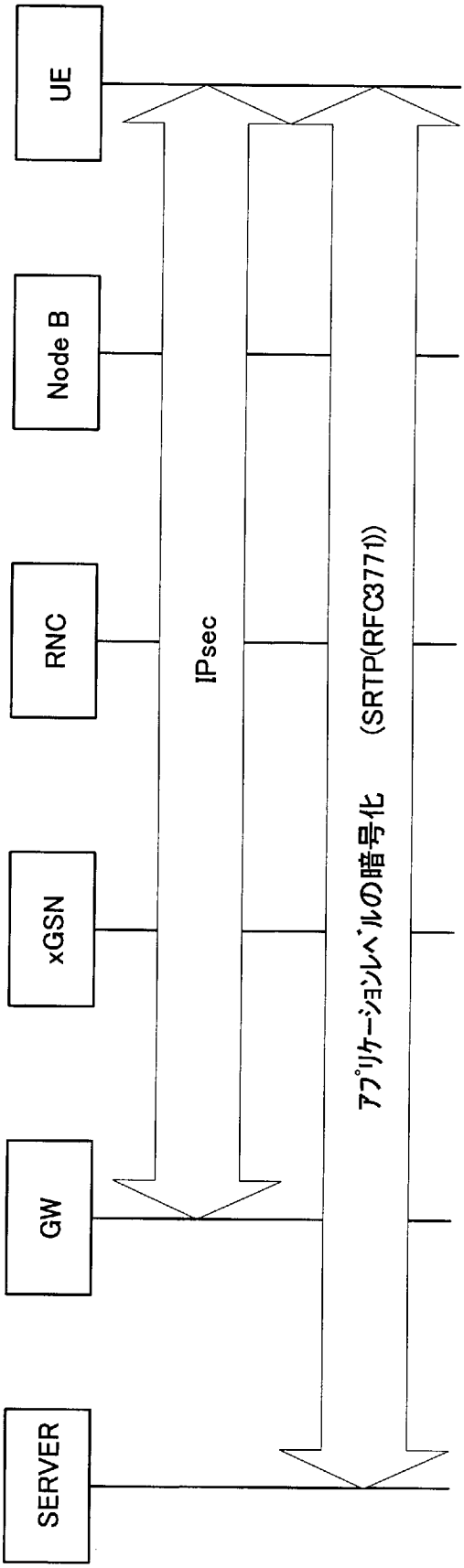
[図4]


UE
Node B
RNC
xGSN
GW
SERVER
KASUMI 暗号化
IPsec
アプリケーションレベルの暗号化(SRTP(RFC3771))

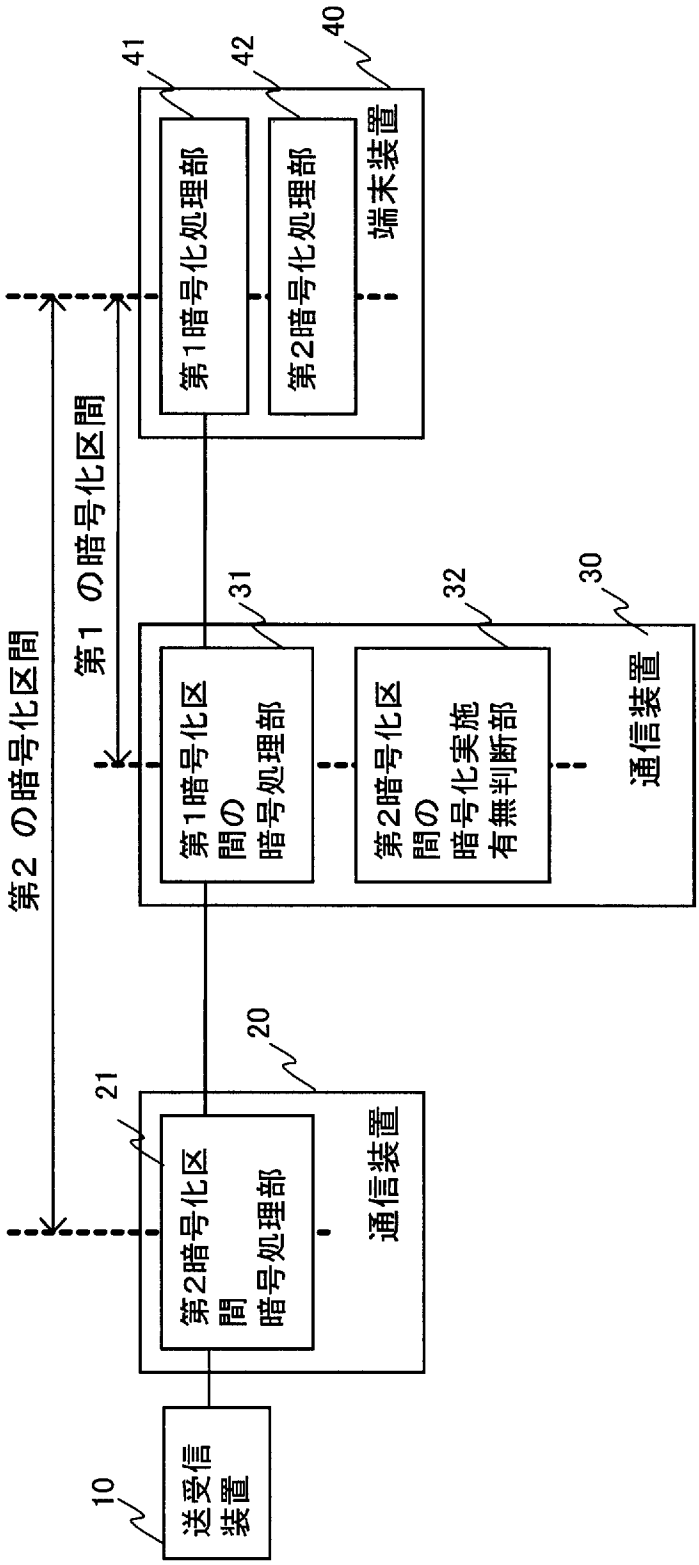
[図5]



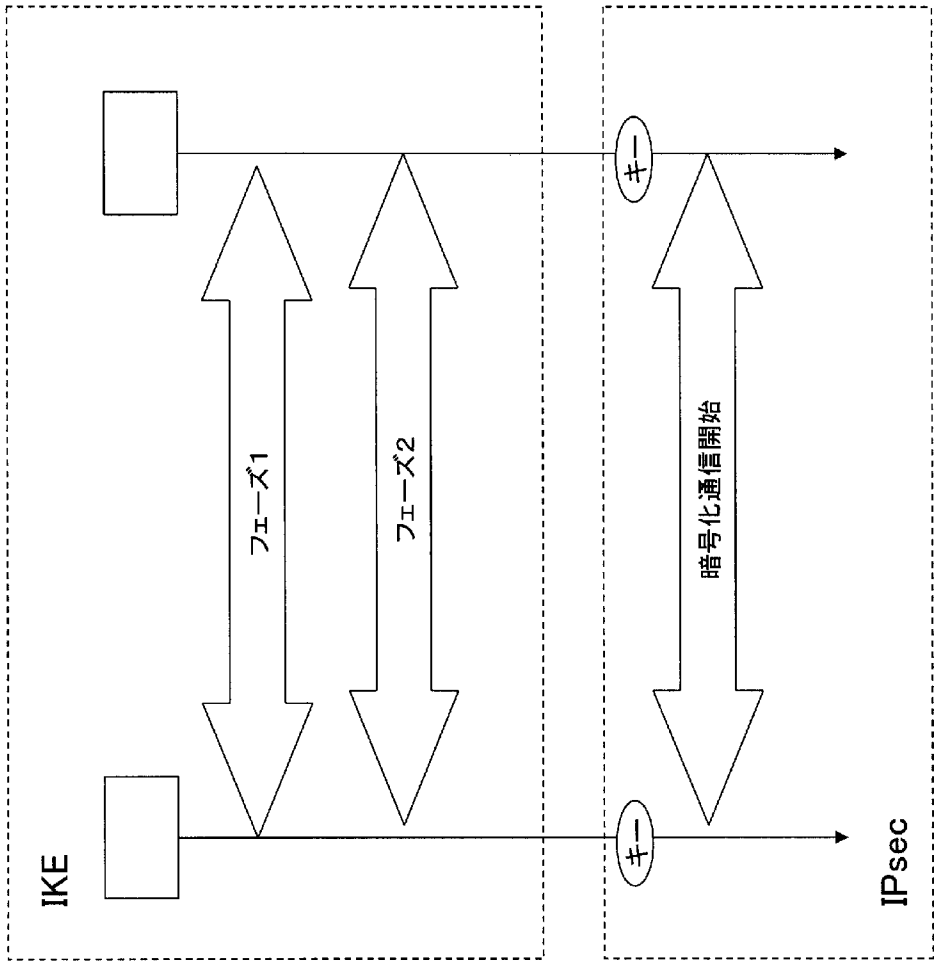
[図6]


UE
Node B
RNC
xGSN
GW
SERVER
IPsec
アプリケーションレベルの暗号化 (SRTP(RFC3711))

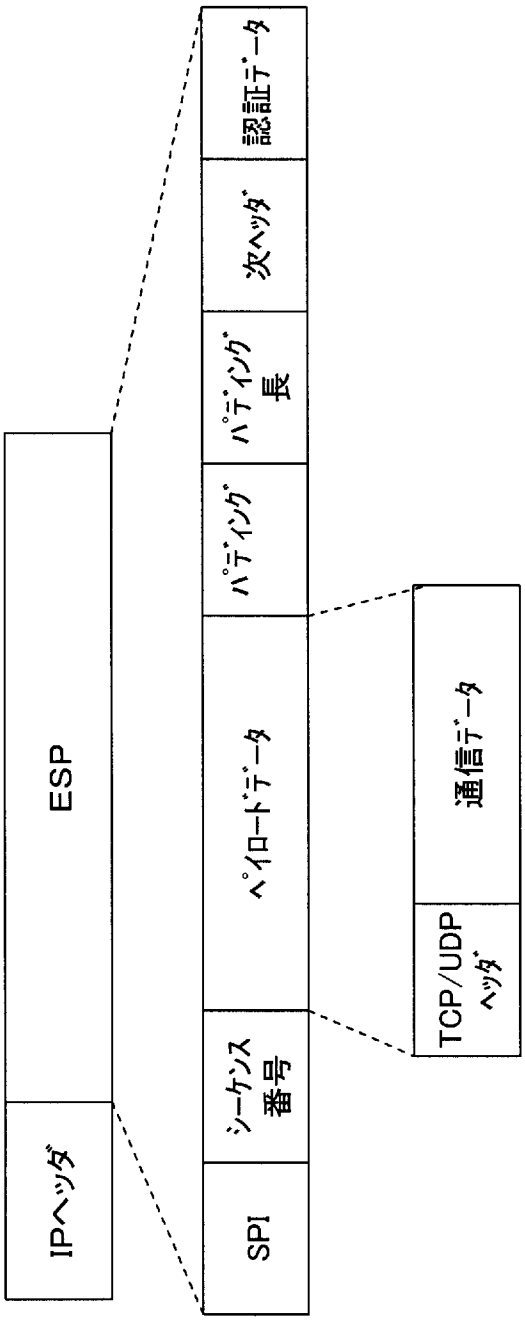
[図7]


第2 の暗号化区間
第1 の暗号化区間
10
送受信装置
21
第2暗号化区間 暗号処理部
20
通信装置
31
第1暗号化区間の暗号処理部
32
第2暗号化区間の暗号化実施有無判断部
30
通信装置
41
第1暗号化処理部
42
第2暗号化処理部
40
端末装置

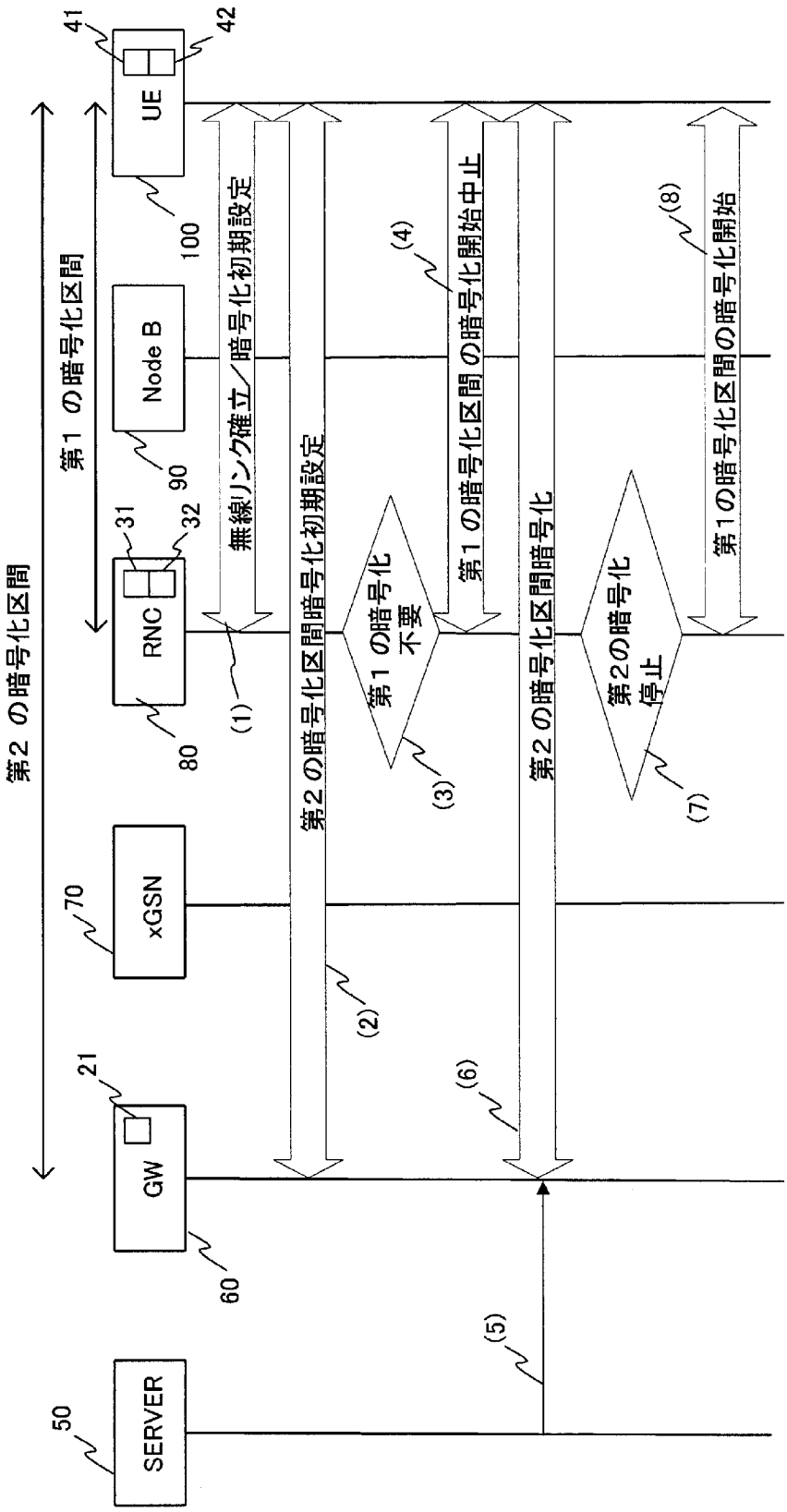
[図8]



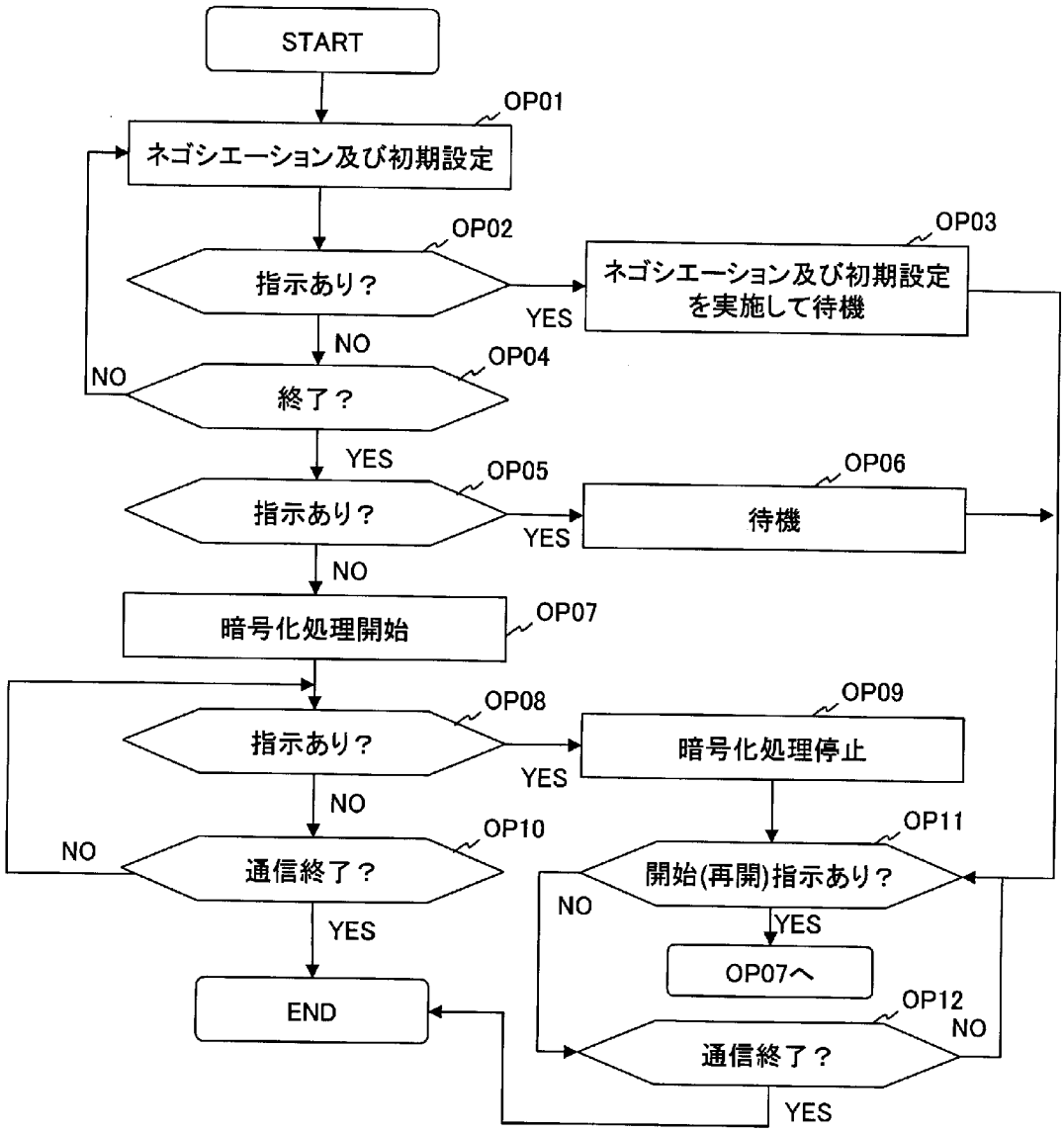
[図9]


ESP
IPヘッダ
SPI
シーケンス番号
ペイロードデータ
パディング
パディング長
次ヘッダ
認証データ
TCP/UDPヘッダ
通信データ

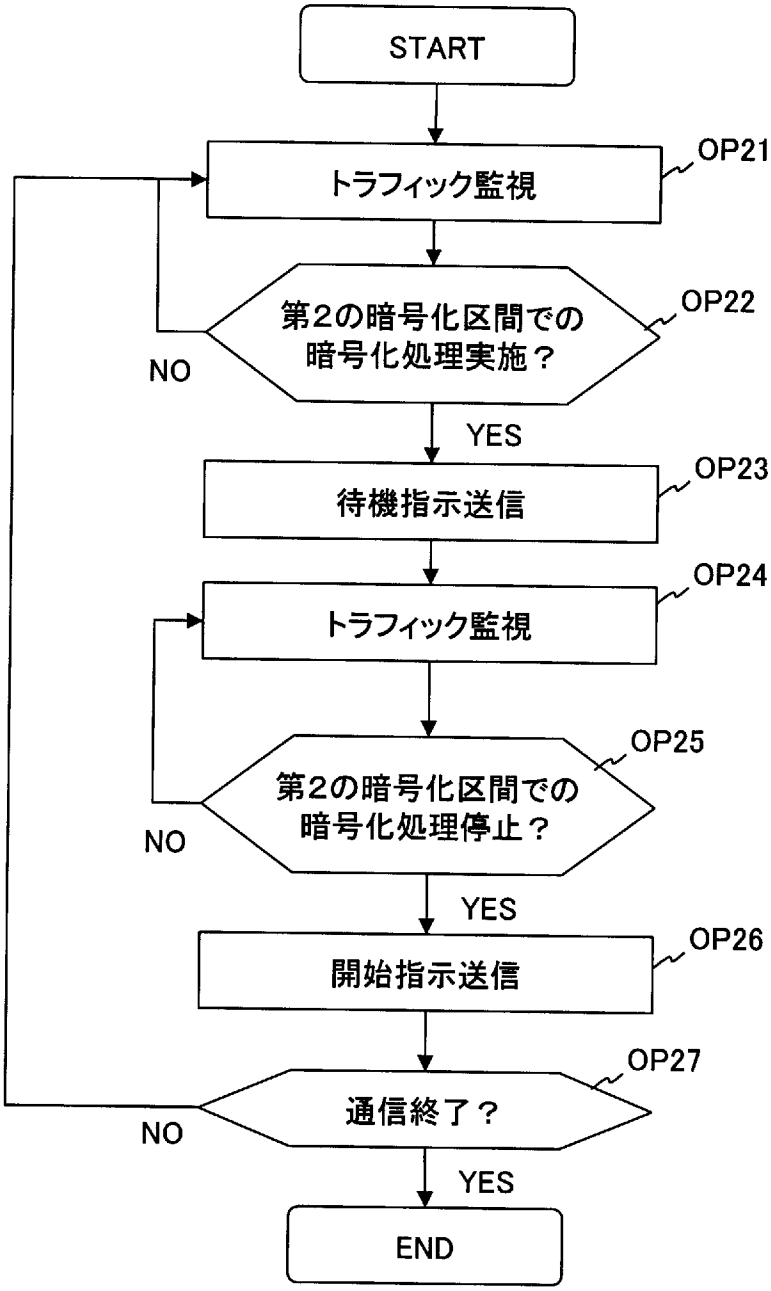
[図10]


第2 の暗号化区間
第1 の暗号化区間
SERVER
50
GW
21
60
xGSN
70
RNC
31
32
80
Node B
90
UE
41
42
100
無線リンク確立／暗号化初期設定
(1)
第2の暗号化区間暗号化初期設定
(2)
第1 の暗号化
不要
(3)
(4)
第1の暗号化区間の暗号化開始中止
(5)
第2の暗号化区間暗号化
(6)
第2の暗号化
停止
(7)
(8)
第1の暗号化区間の暗号化開始

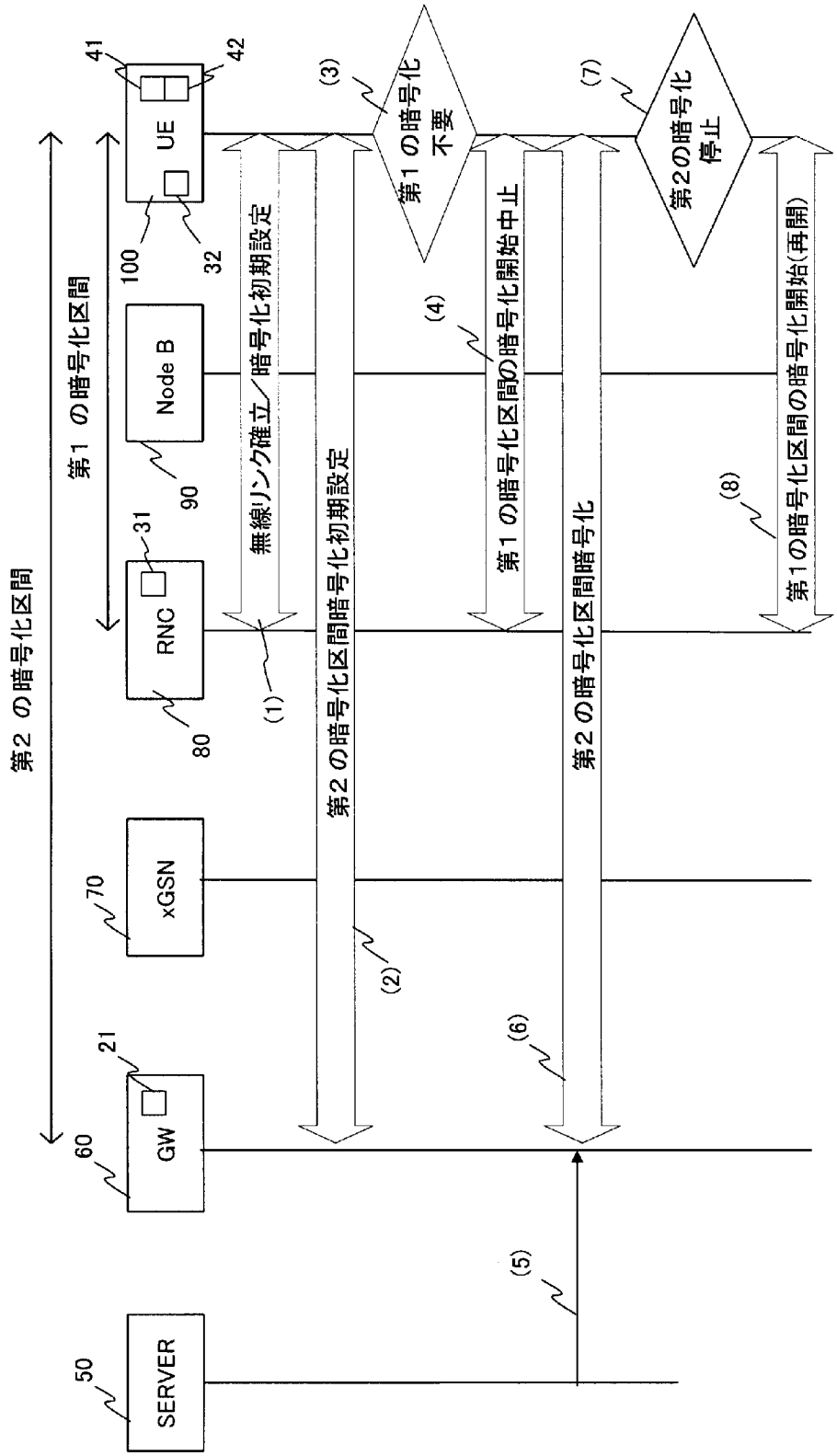
[図11]


START
OP01
ネゴシエーション及び初期設定
OP02
指示あり？
YES
OP03
ネゴシエーション及び初期設定
を実施して待機
NO
OP04
終了？
NO
YES
OP05
指示あり？
YES
OP06
待機
NO
暗号化処理開始
OP07
OP08
指示あり？
YES
OP09
暗号化処理停止
NO
OP10
通信終了？
NO
YES
END
OP11
開始(再開)指示あり？
NO
YES
OP07へ
OP12
通信終了？
NO
YES

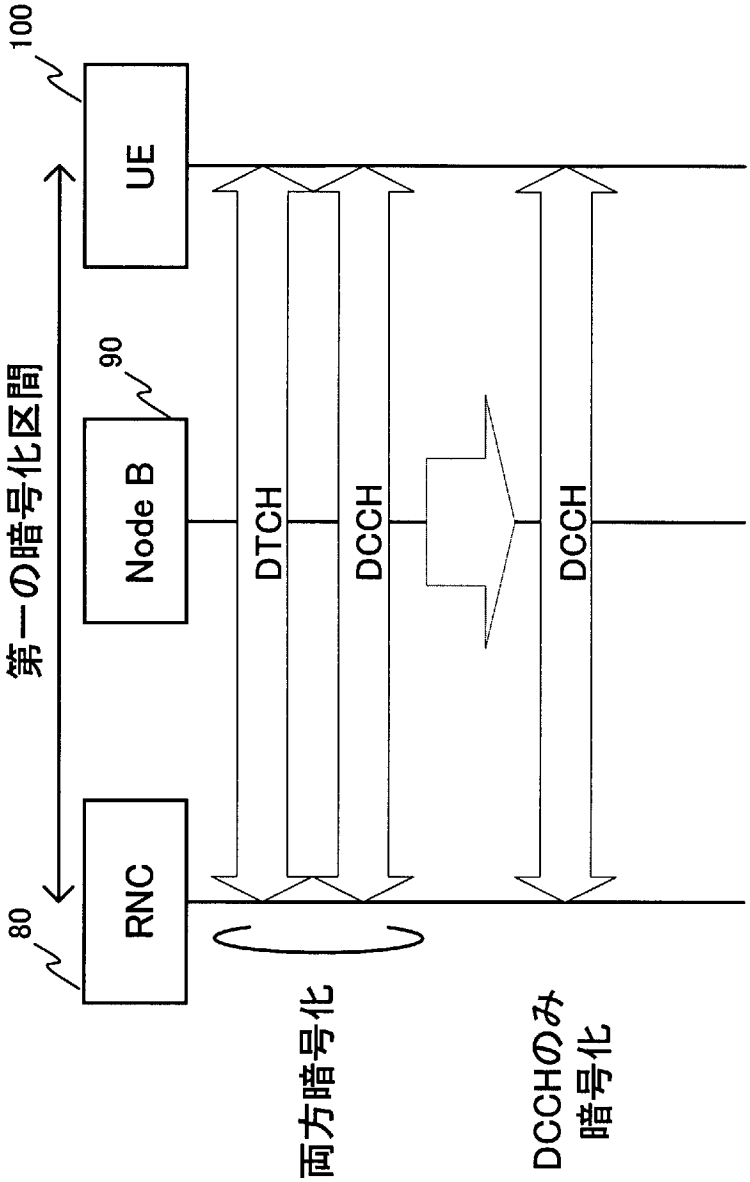
[図12]


START
トラフィック監視
OP21
第2の暗号化区間での
暗号化処理実施？
OP22
NO
YES
待機指示送信
OP23
トラフィック監視
OP24
第2の暗号化区間での
暗号化処理停止？
OP25
NO
YES
開始指示送信
OP26
通信終了？
OP27
NO
YES
END

[図13]


第2 の暗号化区間
第1 の暗号化区間
SERVER
50
GW
60
21
xGSN
70
RNC
80
31
Node B
90
UE
100
32
41
42
(1)
無線リンク確立／暗号化初期設定
(2)
第2 の暗号化区間暗号化初期設定
(3)
第1 の暗号化
不要
(4)
第1 の暗号化区間の暗号化開始中止
(5)
(6)
第2 の暗号化区間暗号化
(7)
第2の暗号化
停止
(8)
第1の暗号化区間の暗号化開始(再開)

[図14]


100
UE
90
Node B
80
RNC
第一の暗号化区間
DTCH
DCCH
DCCH
両方暗号化
DCCHのみ
暗号化

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/074439

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/36(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)
H04L9/36

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 1996-2008
Kokai Jitsuyo Shinan Koho 1971-2008 Toroku Jitsuyo Shinan Koho 1994-2008

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2000-31980 A (Kokusai Electric Co., Ltd., Nippon Telegraph And Telephone Corp.), 28 January, 2000 (28.01.00), Abstract; Par. No. [0007]; Figs. 1, 2 (Family: none)	1-9
Y	JP 2007-36834 A (Canon Inc.), 08 February, 2007 (08.02.07), Abstract (Family: none)	1-9
Y	WO 2006/093079 A1 (NEC Corp.), 08 September, 2006 (08.09.06), Par. Nos. [0451] to [0454]; Figs. 35 to 37 (Family: none)	1-9

☒ 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
11 January, 2008 (11.01.08)	22 January, 2008 (22.01.08)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/074439

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-224409 A (Oki Electric Industry Co., Ltd.), 21 August, 1998 (21.08.98), Par. No. [0334] (Family: none)	1-9
A	JP 9-214556 A (Toshiba Corp.), 15 August, 1997 (15.08.97), Par. No. [0255] & US 6092191 A	1-9

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００７／０７４４３９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/36(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.　H04L9/36

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	１９７１－２００８年
日本国実用新案登録公報	１９９６－２００８年
日本国登録実用新案公報	１９９４－２００８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）

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	関連する請求の範囲の番号
Y	JP 2000-31980 A (国際電気株式会社, 日本電信電話株式会社) 2000.01.28, 【要約】, 【0007】, 図 1,2 (ファミリーなし)	1-9
Y	JP 2007-36834 A (キヤノン株式会社) 2007.02.08, 【要約】 (ファミリーなし)	1-9
Y	WO 2006/093079 A1 (日本電気株式会社) 2006.09.08, [0451]-[0454], 図 35-37 (ファミリーなし)	1-9

☑　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 １１．０１．２００８	国際調査報告の発送日 ２２．０１．２００８
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　３３６５ 速水　雄太 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	関連する請求の範囲の番号
Y	JP 10-224409 A (沖電気工業株式会社) 1998.08.21, 【0334】 (ファミリーなし)	1-9
A	JP 9-214556 A (株式会社東芝) 1997.08.15, 【0255】 & US 6092191 A	1-9