(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
2017 年 1 月 26 日(26.01.2017)

WIPO | PCT

(10) 国際公開番号
WO 2017/014164 A1

(51) 国際特許分類:
H04L 12/66 (2006.01) *H04L 12/70* (2013.01)

(21) 国際出願番号: PCT/JP2016/070907

(22) 国際出願日: 2016 年 7 月 14 日(14.07.2016)

(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 2015-143405 2015 年 7 月 17 日(17.07.2015) JP

(71) 出願人: 日本電気株式会社(NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者: 石井　理(ISHII, Satoru); 〒1088001 東京都港区芝五丁目７番１号　日本電気株式会社内 Tokyo (JP). 長谷川　英男(HASEGAWA, Hideo); 〒1088001 東京都港区芝五丁目７番１号　日本電気株式会社内 Tokyo (JP). 中野　慎太郎(NAKANO, Shintaro); 〒1088001 東京都港区芝五丁目７番１号　日本電気株式会社内 Tokyo (JP).

(74) 代理人: 加藤　朝道(KATO, Asamichi); 〒2220033 神奈川県横浜市港北区新横浜３丁目２０番１２号加藤内外特許事務所内 Kanagawa (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, BN, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

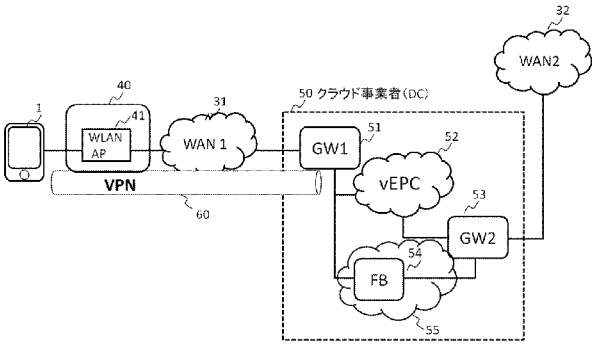
添付公開書類:

— 国際調査報告（条約第 21 条(3)）

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

(54) 発明の名称 : 通信システム、通信装置、通信方法、端末、プログラム

[図2]



50 Cloud operator (DC)

(57) **Abstract**: The present invention provides the necessary protection to a terminal that is connected to a data center via a wireless LAN and a wide area network and makes it possible to provide secure communication. In a communication system according to the present invention, a data center is provided with: a first gateway by which the data center and a terminal are connected via a wireless LAN through a VPN for a first wide area network; a second gateway that is connected to a second wide area network (WAN2); a virtual network that is connected to the first gateway and the second gateway; and a function block that carries out filtering of at least packets input from the second wide area network (WAN2) side to the second gateway.

(57) 要約: 本発明は、無線 LAN、広域ネットワークを介してデータセンタに接続する端末に対して必要な保護を提供するとともに、セキュアな通信を提供可能とする。データセンタが、端末との間を無線 LAN を介し第１の広域ネットワーク経由の VPN で接続する第１のゲートウェイと、第２の広域ネットワーク（WAN2)に接続する第２のゲートウェイと、前記第１のゲートウェイと前記第２のゲートウェイに接続された仮想ネットワークと、少なくとも、前記第２の広域ネットワーク（WAN2)側から前記第２のゲートウェイに入力されたパケットのフィルタリングを行う機能ブロックと、を備える。

WO 2017/014164 A1

明　細　書

発明の名称 ：

通信システム、通信装置、通信方法、端末、プログラム

技術分野

[0001] （関連出願についての記載）

本発明は、日本国特許出願：特願２０１５－１４３４０５号（２０１５年７月１７日出願）の優先権主張に基づくものであり、同出願の全記載内容は引用をもって本書に組み込み記載されているものとする。

本発明は通信システム、装置、方法、端末、プログラムに関する。

背景技術

[0002] 発展型パケットシステム（Evolved Packet System: EPS）は、3GPP（3rd Generation Partnership Project）アクセスネットワークのほか、非3GPPアクセスネットワークを含む。3GPPアクセスネットワークはUTRAN(UMTS(Universal Mobile Telecommunications System) Terrestrial Radio Access Network)、E-UTRAN(Evolved UTRAN)、GERAN(GSM（登録商標）(Global system for mobile communications) EDGE Radio Access Network)等を含む。

[0003] 非3GPPアクセスネットワークは、3GPPの範囲外の仕様のアクセス技術を用いたIP(Internet Protocol)アクセスネットワークであり、IEEE（The Institute of Electrical and Electronics Engineers, Inc.）802.11仕様で規定されるWi-Fi(登録商標: Wireless Fidelity)やIEEE802.16仕様で規定されるWiMAX(Worldwide Interoperability for Microwave Access)等の無線LAN（Wireless Local Area Network：WLAN）を含む。非3GPPアクセスについては例えば3GPP TS23.402: Architecture enhancements for non-3GPP accesses等を参照してもよい。

[0004] Wi-Fi（登録商標）-Callingは、通信キャリアによって提供されるサービスであるこのサービスは、当該通信キャリアのSIM(Subscriber Identity Module)が挿入された端末（User Equipment :UE）でWi-Fi（登録商標）を経由して

音声通話やショートメッセージサービス（Short Message Service: SMS）等を利用可能とする（非特許文献１参照）。端末がUMA（Unlicensed Mobile Access）技術を使ってWi-Fi（登録商標）経由で通信キャリアのセキュリティ・ゲートウェイに接続しSIM認証で認証されると、通信キャリアのコア網の交換機に接続し通話相手（固定電話、別の通信キャリアの加入端末等であってもよい）に接続される。また、端末がWi-Fi（登録商標）に接続しており且つWi-Fi（登録商標）-Callingがオンに設定されていれば、当該端末に対する着信を受けたセキュリティ・ゲートウェイはWi-Fi（登録商標）経由で当該端末を呼び出す。

[0005] 図１は、非3GPPアクセスネットワークを含むEPSを説明する図である。スマートフォン等の端末（UE）１は、基地局（evolved NodeB：eNB）１０、発展型パケットコア（Evolved Packet Core: EPC）２０を介してパケットデータ網（Packet Data Network: PDN）３０に接続するか、あるいは、Wi-Fi（登録商標）等の無線LANアクセスポイント４１を介してインターネットに接続することができる。

[0006] EPC２０のMME（Mobility Management Entity）２３は、端末１の移動管理や認証、ユーザデータ転送経路の設定等の各種処理を行う。また、MME２３は、HSS（Home Subscriber Server：加入者プロファイルを保持）２４と連携してユーザの認証等を行う。MME２３はSGW（Serving Gateway）２１から基地局１０の区間（S1-U)のユーザデータ転送経路の設定・解放を行う。SGW２１は基地局１０との間でユーザデータの送受信を行い、PGW(Packet Data Network gateway)２２との間の通信経路の設定・解放を行う。PGW２２はIMS(IP Multimedia Subsystem)やインターネット等のパケットデータ網（PDN）３０と接続する。またPGW２２は端末１に対するIPアドレス(プライベートIPアドレス)の割当て等を行う。PCRF(Policy and Charging Rules Function)２６はQoS(Quality of Service)等のポリシ制御や課金制御ルールを決定する。PGW２２及びSGW２１はPCRF２６からの通知情報に基づき、例えばパケット単位にポリシ制御を行う。なお、図１において、各ノード間の線の符号S11等はインタフェ

ースを表しており、破線はコントロールプレーン（C-Plane）、実線はユーザプレーン（U-Plane）の信号（データ）を表している。EPCの詳細は例えば3GPP TS 23.401：GPRS Enhancements for E-UTRAN Access等を参照してもよい。

[0007] Wi-Fi（登録商標）-Calling等において、端末１からの呼要求は無線LANアクセスポイント４１経由で、Un-Trusted Access（信頼できないアクセス）として、ePDG(evolved Packet Data Gateway)２７経由でPGW２２に接続され、PDN３０（例えばIMSサービス）に接続される。

[0008] ePDG２７は、モバイルインタフェース（SWu）からのIPsec(Security Architecture for Internet Protocol)接続を終端するIPsecゲートウェイである。端末（UE）１が、セキュリティ上信頼できない非3GPPアクセスに移行するか又は非3GPPアクセスに最初に接続するときに、端末１はePDG２７を検出し、ePDG２７との間での鍵交換（IKEv2）、及び、IPsecトンネルの確立を行い、確立したIPsecトンネル越しに、PGW２２と、PDN（Packet Data Network）コネクションを確立する。端末１が、非3GPPアクセスネットワークにアクセスするには、認証を行う必要がある。ePDG２７は、端末１からのEAP(Extensible Authentication Protocol)メッセージを3GPP AAA(Authentication Authorization Accounting)サーバ２５に中継し、3GPP AAAサーバ２５は、EAP-SIM（Extensible Authentication Protocol-Subscriber Identity Module）認証又は、EAP-AKA（Extensible Authentication Protocol-Authentication and Key Agreement）認証を行う（例えば3GPP TS 33.402：Security aspects of non-3GPP accesses等を参照してもよい）。

[0009] ePDG２７は、S2bインタフェースにおいてPGW２２に向かってトンネル（プロキシモバイル(Proxy Mobile) IP 又はGTP(GPRS（General Packet Radio System） Tunneling Protocol)）を設定する（例えば3GPP TR 23.834: Study on GPRS Tunneling Protocol (GTP) based S2b等を参照してもよい）。

[0010] 非3GPPアクセスがPMIPv6(Proxy Mobile IPv6)に対応している場合、ePDG２７はPGW２２にPMIPv6を介して接続できる。PGW２２とePDG２７間でプロキシモバイルIPを使用する場合、端末１とePDG２７との間でIPsecトンネルが確立

されると、ePDG２７はプロキシバインディングアップデート（Proxy Binding Update）メッセージをPGW22に送信する。この結果、PGW２２において端末１へのデータの送信先はePDG２７に切り替えられる。なお、PMIPv6は、モビリティアンカ（LMA：Local Mobility Anchor）とモビリティアクセスゲートウェイ（MAG：Mobility Access Gateway）の間でデータ転送用のトンネル（GRE（Generic Routing Encapsulation）トンネル）を確立・解放するモビリティ制御プロトコルである（IETF(The Internet Engineering Task Force) RFC(Request For Comments) 5213等を参照してもよい）。LMAは端末が接続するMAGまでパケット転送を行う（通信経路を切り替えて端末宛てパケットを在圏エリアへ転送する）。端末があるMAGから異なるMAGに移動した場合、前にデータ転送用トンネルを確立したLMAと、端末が新たに接続するMAG間でデータ転送用のトンネルが張られる。

[0011] 3GPP AAAサーバ２５は、ユーザからのネットワークアクセスの認証、認可、及びアカウンティングサービスを提供する。非3GPPアクセスの認可は、端末１と3GPP AAAサーバ２５、HSS２４間で行われる。例えば端末１がePDG２７との間でIPsecトンネルを確立すると、EAP－AKAに基づき、端末１とネットワーク間で相互の認証が行われる。3GPP AAAサーバに関して3GPP TS 29.273：Evolved Packet System (EPS);3GPP EPS AAA interfaces等を参照してもよい。

[0012] 一方、端末１が、信頼できる（Trusted）非3GPPアクセス(図１の信頼できる無線LANアクセスポイント４２)に移行するか又は最初に接続するとき、MIP(Mobile IP)トンネル（S2a、DSMIPv6(Dual-Stack MIPv6)：IETF RFC 5555等を参照してもよい）を介して、直接、PGW２２に接続する。なお、ePDG、3GPP AAAサーバについては3GPP TS 29.273: Evolved Packet System (EPS); 3GPP EPS AAA interfaces等を参照してもよい。なお、非3GPPアクセスネットワークが信頼できるアクセスネットワークであるか、信用できないアクセスネットワークであるかは、例えばHPLMN（Home Public Land Mobile Network）の通信キャリア（オペレータ）によって決定される。

[0013] IPSecは、ネットワーク層レベルでパケットの暗号化や認証を行うプロトコルである。AH(Authentication Header)はVPN(Virtual Private Network)の接続先、パケットの改竄の有無等の認証を行う（IETF RFC 2402等を参照してもよい）。ESP（Encapsulating Security Payload）はパケットの暗号化、認証（接続先・パケットの改竄）を行う（IETF RFC 2406参照）。IPSec通信には、トランスポートモード（IPsecが実装されたホスト間のIPsec）と、トンネルモード（IPsecが実装されたルータ等VPN装置間のIPsec）がある。トランスポートモードではパケットのレイヤ４以上のデータを暗号化し（図１１（Ｂ）参照）、元のIPヘッダ（Original IP header）に基づいてパケットが転送される。トンネルモードでは、パケットの元のIPヘッダ、データ部（図１１（Ａ））は暗号化され、新たなIPヘッダ（New IP header）が追加される（図１１（Ｃ）参照）。

[0014] ESPのパケット形式は、ESPヘッダ（ESP header）、ペイロード、ESPトレイラ（ESP Trailer）、認証データ（ESP Authentication data）からなる（図１１（Ｂ）、（Ｃ）参照）。ESPヘッダ（ESP header）は、SPI(Security Parameter Index：そのデータグラムに対するSA（セキュリティアソシエーション）を一意に識別する32ビットの値)と、シーケンス番号（Sequence Number）(パケットのシーケンス番号：32ビット)を有する。ESPトレイラは、パディング（Padding）（ペイロード長調節用パディングフィールド）、パッド長（Pad length）（Paddingのバイト数）、次ヘッダ（Next Header）（ESPの後のプロトコル：TCP/UDP）からなる。認証データ（Authentication data）（HMAC (Hash-based Message Authentication Code)）は、ESP パケットから認証データを抜いたものから計算されたインテグリティチェック値（Integrity Check Value: ICV）を含む可変長フィールドである。

[0015] IPsec通信を行うためには、VPN装置間で、論理的なコネクションであるセキュリティアソシエーション（Security Association：SA)の確立が行われる。SAは一方向のトンネルであるため、パケットの送信と受信用に、２つのSAが設けられる。SAは、VPN通信を行うトラフィック毎に確立され、IPsecのパ

ラメータ（セキュリティ情報）（例えばSPI(Security Parameter Index)、モード、プロトコル、暗号アルゴリズム、鍵、認証アルゴリズム、トンネルエンドポイントのIPアドレス等）からなる。

[0016] IKE(Internet Key Exchange)は、SA設定のための鍵交換プロトコルである（IKEv2について、例えばIETF RFC 4306等を参照してもよい）。ISAKMP（Internet Security Association and Key Management Protocol）_SA（Security Association）は、IKEの制御情報を暗号化し、ピア間で送受するためのSAである。

先行技術文献

非特許文献

[0017] 非特許文献1：Next-generation Wi-Fi Calling Using IMS and 3GPP Wi-Fi Access、インターネット検索（2015年4月26日検索）＜URL：http://www.aptilo.com/wi-fi-calling/next-generation-wi-fi-calling-solution＞

発明の概要

発明が解決しようとする課題

[0018] データセンタ等と無線LAN（Local Area Network）間にはインターネット等の広域ネットワーク（Wide Area Network：WAN）が介在しているため、セキュアなコネクションを確立する必要がある。

[0019] 通信キャリアが加入者に提供するフィルタリングサービス等は、例えば、該通信キャリアのパケットコア網（EPC）上等で提供される。端末（UE）が無線LAN接続に切り替えると、通信キャリアのパケットコア網（EPC）による制御ができなくなる場合がある。このため、端末が無線LANからインターネットに接続する場合、例えばペアレンタルコントロール（子供のインターネットの使いすぎや有害サイト、有害コンテンツからの保護）やアクセス拒否などの制御が十分に行えない場合が生じる。ペアレンタルコントロールに関して、例えば、子供（児童）向け端末として予めペアレンタルコントロール機能（例えば有害サイトのブロック、利用するアプリの制限、電話やメールの相

手の制限、利用時間や通話時間を制限等）を具備した端末もあるが、具備されているペアレンタルコントロール機能以外の制限等については、保護者等が適宜、対策を講じる必要がある。また、ペアレンタルコントロール機能等を具備した、いわゆる子供向け端末以外の一般の端末を年少者が利用する場合もある。

[0020] したがって、本発明の目的は、無線LAN、インターネット等の広域ネットワーク（WAN）を介してデータセンタに接続する端末に対して必要な保護を提供するとともに、セキュアな通信を提供可能とするシステム、方法、装置、プログラムを提供することにある。

課題を解決するための手段

[0021] 本発明の１つの側面によれば、端末が接続する無線LAN（Local Area Network）との間に第１の広域ネットワーク（Wide Area Network）が介在するデータセンタを備え、

前記データセンタが、

前記端末との間を、前記無線LANを介し前記第１の広域ネットワーク経由のVPN(Virtual Private Network)で接続する第１のゲートウェイと、

第２の広域ネットワークに接続する第２のゲートウェイと、

前記第１のゲートウェイと前記第２のゲートウェイに接続された仮想ネットワークと、

前記第１のゲートウェイと前記第２のゲートウェイ間に設けられ、前記第１の広域ネットワーク側から入力されるパケット、及び、前記第２の広域ネットワーク側から入力されるパケットのうち少なくとも一方のパケットのフィルタリングを行う機能ブロックと、

を備えた通信システムが提供される。

[0022] 本発明の他の側面によれば、端末が接続する無線LAN（Local Area Network）との間に第１の広域ネットワーク（Wide Area Network）が介在する通信装置であって、

前記端末との間を、前記無線LANを介し前記第１の広域ネットワーク経由の

VPN(Virtual Private Network)で接続する第１のゲートウェイと、

第２の広域ネットワークに接続する第２のゲートウェイと、

前記第１のゲートウェイと前記第２のゲートウェイに接続された仮想ネットワークと、

前記第１のゲートウェイと前記第２のゲートウェイ間に設けられ、前記第１の広域ネットワーク側から入力されるパケット、及び、前記第２の広域ネットワーク側から入力されるパケットのうちの少なくとも一方のパケットのフィルタリング制御を行う機能ブロックと、を備えた通信装置が提供される。

[0023] 本発明の他の側面によれば、端末が接続する無線LAN（Local Area Network）との間に第１の広域ネットワーク（Wide Area Network）が介在するデータセンタの第１のゲートウェイと前記端末との間を、前記無線LANを介し前記広域ネットワーク経由のVPN(Virtual Private Network)で接続し、

前記端末から前記VPNを介して、前記データセンタに設けられた、仮想ネットワークから第２のゲートウェイを介して第２の広域ネットワークに接続し、

前記第１のゲートウェイと前記第２のゲートウェイ間に設けられた機能ブロックにて、前記第１の広域ネットワーク側から入力されるパケット、及び、前記第２の広域ネットワーク側から入力されるパケットのうちの少なくとも一方のパケットのフィルタリングする、通信方法が提供される。

[0024] 本発明のさらに別の側面によれば、

無線LANと第１の広域ネットワーク（WAN1)とを介してデータセンタに接続する端末であって、

前記データセンタとの間を、前記無線LAN及び前記広域ネットワーク経由のVPNで接続するVPN装置を備え、

前記VPNを介して、前記データセンタに設けられており、パケットコアネットワークの機能の少なくとも一部を仮想化した仮想ネットワークを介して第２の広域ネットワーク（WAN2)に接続し、

前記第２の広域ネットワーク（WAN2)側から前記データセンタ内に入力された前記端末への着呼又は前記端末宛てのデータのうち、前記データセンタ内でフィルタリングされた着呼又はデータを、前記VPNを介して、受信する機能を備えた端末が提供される。

[0025] 本発明の他の側面によれば、端末が接続する無線LAN（Local Area Network）との間に第１の広域ネットワーク（Wide Area Network）が介在するデータセンタに配置されるコンピュータに、

前記端末と前記データセンタとの間に、前記無線LANを介し前記広域ネットワーク経由のVPN(Virtual Private Network)を開設する処理と、

前記端末から前記VPNを介して、前記データセンタに設けられており、コアネットワークの構成要素の少なくとも一部を仮想化した仮想ネットワークを介して第２の広域ネットワークに接続する処理と、

前記第１の広域ネットワーク側から入力されるパケット、及び、前記第２の広域ネットワーク側から入力されるパケットのうちの少なくとも一方のパケットのフィルタリングを行う処理と、を実行させるプログラムが提供される。

[0026] 本発明のまたさらに他の側面によれば、無線LANと第１の広域ネットワーク（WAN１）を介してデータセンタに接続する端末に含まれるコンピュータに、

前記データセンタと前記端末との間に、前記無線LANを介し前記広域ネットワーク経由のVPNを開設する処理と、

前記VPNを介して、前記データセンタに設けられており、パケットコアネットワークの機能の少なくとも一部を仮想化した仮想ネットワークを介して第２の広域ネットワーク（WAN2)に接続する処理と、

前記第２の広域ネットワーク（WAN2)側から前記データセンタ内に入力された前記端末への着呼又は前記端末宛てのデータのうち、前記データセンタ内でフィルタリングされた着呼又はデータを、前記VPNを介して、受信する処理と、

を実行させるプログラムが提供される。

[0027] 本発明によれば、前記プログラムを記録したコンピュータ読み出し可能な記録媒体（半導体メモリやCD（Compact Disk）/DVD(Digital Versatile Disk)等のストレージ）が提供される。

発明の効果

[0028] 本発明によれば、無線LAN、インターネット等の広域ネットワーク（WAN）を介してデータセンタに接続する端末に対して必要な保護を提供するとともに、セキュアな通信を提供可能としている。

図面の簡単な説明

[0029] [図1]関連技術を例示する図である。

[図2]本発明の一実施形態を例示する図である。

[図3]（Ａ）は本発明の一実施形態を例示する図である。（Ｂ）はゲートウェイのVPN情報記憶部を例示する図である。（Ｃ）は、端末のVPN情報記憶部を例示する図である。

[図4]本発明の一実施形態の動作を例示する図である。

[図5]（Ａ）、（Ｂ）は、本発明の一実施形態の機能ブロックを例示する図である。

[図6]本発明の一実施形態を例示する図である。

[図7]図６の一実施形態の動作を例示する図である。

[図8]本発明の他の実施形態を例示する図である。

[図9]本発明の他の実施形態を例示する図である。

[図10]仮想化装置の構成を例示する図である。

[図11]（Ａ）はIPパケット、（Ｂ）はトランスモードのESPパケット、（Ｃ）はトンネルモードのESPパケット、（Ｄ）はUDPカプセル化、（Ｅ）はL2TP/IPsecのパケットを例示する図である。

発明を実施するための形態

[0030] 本発明の例示的な実施形態について説明する。本発明によれば、クラウド事業者のデータセンタに仮想化コア網を配置した通信システムにおいて、例えば無線LAN等、非3GPPアクセスネットワークからのアクセスによりデータセ

ンタに接続する端末に対して必要な保護を提供するとともに、セキュアなコネクションを実現する。

[0031] ネットワーク機能をソフトウェア的に実現する手法が各種提案されている。例えばSDN(Software Defined Network)/NFV(Network Function Virtualization)等では、個別に筐体を必要とする複数のネットワーク機器を、仮想化技術を利用してサーバ上に統合している。なお、NFVについては、ETSI GS NFV-MAN 001 V1.1.1 (2014-12)等を参照してもよい。通信事業者のコア網である発展型パケットコア（EPC）等の仮想化が進んでいる。

[0032] 仮想化EPC（Virtualized EPC：vEPC）では、例えばSGW、PGW、MME、HSS、PCRF等のノードの少なくとも１つ又は全ての機能を仮想マシン上で動作するアプリケーションでソフトウェア的に実現している。例えば、クライアントにクラウドサービス（あるいはデータセンタサービス）を提供するクラウド事業者のデータセンタ(Data Center: DC)内に配設されている汎用サーバ等の上に仮想化EPC（Virtualized EPC）を実現することができる。

[0033] 図２は、本発明の例示的な一実施形態を説明する図である。データセンタ５０内の仮想化EPC（vEPC）５２は、図１のEPC２０の少なくとも一部を仮想化したものである。vEPC５２は図１のEPC２０のePDG27、PGW２２、PCRF２６等、EPC２０の一部のノードの機能を仮想化したものであってもよい。

[0034] 第１のゲートウェイ５１(GW1)は、インターネット等の広域ネットワーク（Wide Area Network；WAN）１（３１）とvEPC５２を接続する。第２のゲートウェイ（GW2）５３は、インターネットやIMS等のWAN２（３２）と、vEPC５２とを接続する。

[0035] 本実施形態においては、データセンタ５０において、第１のゲートウェイ５１と第２のゲートウェイ５３間のネットワーク（仮想ネットワーク）５５上に、パケットフィルタリング又はデータ圧縮等を行う機能ブロック（Function Block: FB）５４を備えている。

[0036] 機能ブロック（Function Block: FB）５４は、ユーザ（端末１：加入者）毎に割り振りが可能とされている。特に制限されるものではないが、例えば

、vEPC５２のPCRF（不図示）がSPR（Subscriber Profile Repository）（不図示）等から取得した端末１のサービス契約情報等や、vEPC５２のPGW（不図示）等で当該端末１に割り当てたプライベートIPアドレス等に基づき、データセンタ５０にアクセスしてきた端末１に対して、端末１毎に、機能ブロック（FB）５４を割り振るようにしてもよい。

[0037] また、特に制限されるものではないが、機能ブロック（FB）５４は、第１のゲートウェイ（GW1）５１と第２のゲートウェイ（GW2）５３間に接続されたサーバ上で稼働する仮想マシン（Virtual Machine）として実装するようにしてもよい。この場合、例えば、端末１（加入者）からの接続要求等により、端末１の加入者情報やサービス契約情報等に基づき、端末１（加入者）に割り振られた機能ブロック（FB）５４が起動され、端末１（加入者）からの接続終了等に応答して、機能ブロック（FB）５４が終了する構成としてもよい。

[0038] 端末１に対応して起動された機能ブロック（FB）５４は、WAN２（３２）側から第２のゲートウェイ（GW2）５３に入力されたパケット（ダウンリンク）のフィルタリング制御を行う。また、機能ブロック（FB）５４は、端末１からWAN１（３１）を介してデータセンタ５０に入力され、WAN２（３２）側へのパケット（アップリンク）のフィルタリング制御を行うようにしてもよい。なお、機能ブロック（FB）５４は、第１のゲートウェイ（GW1）５１と第２のゲートウェイ（GW2）５３の中間に配置される構成に限定されるものでなく、例えば、第１のゲートウェイ（GW1）５１と第２のゲートウェイ（GW2）５３の少なくとも一方を構成するサーバ等の上に実装するようにしてもよい。

[0039] 端末１は、WLAN４０を経由して、WAN１（３１）、データセンタ５０の第１のゲートウェイ５１、vEPC５２、第２のゲートウェイ５３からWAN２（３２）に接続する。なお、図２において、WLAN４０は、家庭内無線LAN又は公衆無線LANであってよい。WLAN４０は、無線LANアクセスポイント（WLAN AP）４１と、NAT（Network Address Transformation）/NAPT(Network Address Port Translation)を備えた無線LANルータ（不図示）等を含み、モデム（不図示）等

を介してWAN１（３１）に接続する。

[0040] なお、本実施形態では、端末１が無線LAN４０、WAN１（３１）を介してデータセンタ５０に接続する接続形態を説明するために、端末１の接続先を無線LANアクセスポイント（WLAN AP）４１としているが、端末１は、接続先を3GPPアクセスネットワーク（例えば図１のeNB１０）に切り替え、パケットコア網（図１のEPC２０）を介して、WAN１（３１）に接続しデータセンタ５０に接続するようにしてもよいことは勿論である。

[0041] データセンタ５０のゲートウェイ装置（GW）（例えば５１）と、端末１間に、VPNトンネルを張る。ゲートウェイ５１には、VPN装置（VPNルータ）が実装され、VPNゲートウェイとして機能する。端末１には、VPN装置が実装され、VPNクライアントとして機能する。端末１では、WLAN４０を介してのデータセンタ５０との間のVPN接続の設定が行われる。VPN接続はトンネリングと暗号化を含む。WAN1（３１）がインターネットの場合、このVPNはいわゆるインターネットVPNである。

[0042] 図２において、端末１に音声通話、SMS等のサービスを提供する場合には、データセンタ５０において、例えば、第１のゲートウェイ（GW1）５１、vEPC５２、と第２のゲートウェイ（GW2）５３を経由としてWAN２（３２）を介して、音声通話やSMSのメッセージ通信の相手端末と接続する。一方、端末１とWAN２（３２）間のデータ通信用のパケット（トラフィック）は、データセンタ５０において、vEPC５２を経由せずに、第１のゲートウェイ（GW1）５１と第２のゲートウェイ（GW2）５３間の仮想ネットワーク５５にオフロードするようにしてもよい。

[0043] また、図２において、データセンタ５０の第１のゲートウェイ（GW1）５１と第２のゲートウェイ（GW2）５３間の仮想ネットワーク５５上に、例えば音声パケットを転送するようにしてもよいことは勿論である。また、端末１とWAN２（３２）間のデータパケット（データ通信）を、データセンタ５０のvEPC５２を経由して、転送するようにしてもよいことは勿論である。

[0044] データセンタ５０内の機能ブロック５４は、パケットのヘッダ情報（アド

レス、ポート番号、プロトコル等）で許可／拒否するパケットフィルタ型のファイアウォールとして構成してもよい。ただし、かかる構成に限定されるものでなく、HTTP（Hypertext Transfer Protocol）やFTP（File Transfer Protocol）など、アプリケーション層（第７層）でのフィルタリングを行うアプリケーションゲートウェイ（端末からの接続はプロキシ（＝ファイアウォール）で確立されプロキシと目的の接続先へ再度、コネクションが確立される）、パケットのヘッダ情報（アドレス、ポート番号・プロトコル等）をもとにセッションテーブルを作成し、通信の方向と状態（ステート）に基づき通信を制御するステートフルインスペクション機能を備えてもよいことは勿論である。アプリケーションゲートウェイ型では、特定のWebサイトでWebの閲覧を制限できる。

[0045] なお、無線LAN/3GPPアクセスネットワークに接続する端末１には、プライベートIPアドレスが付与され、NAT/NAPTでアドレス/ポート番号が変換されるため、WAN（WAN２）には、プライベートIPアドレスをヘッダの宛先、送信元とするパケットは流れない。IPアドレス スプーフィング（なりすまし）を遮断するため、機能ブロック５４は、プライベートIPアドレスを宛先とするパケットを拒否する設定を行うようにしてもよい。

[0046] WAN２（３２）がIMS（IP（Internet Protocol）Multimedia Sub-system）の場合、例えば端末１から発信されたSIP（Session Initiation Protocol）メッセージは、第２のゲートウェイ５３に接続するプロキシセッション制御機能P-CSCF（Proxy Call Session Control Function）から、IMSのホーム網側のサービングセッション制御機能S-CSCF（Serving Call Session Control Function）に送信されて分析され、着信側のS-CSCF又はメディアゲートウェイ制御機能MGCF（Media Gateway Control Function）にSIPメッセージを送信し、着信側のS-CSCFからインターネット又は他のIMS、あるいは、IP網と既存の電話網の間のMGW（Media Gateway）、回線交換（Circuit Switched: CS）網とIP網間にあり、SS7共通線信号網からの呼制御信号を終端し、IP網上の呼制御信号に変換するSignaling Gatewayから、回線交換（CS）ドメイン等に通

信サービスを提供する。

[0047] あるいは、データセンタ５０において、IMS機能の少なくとも一部を、仮想化ネットワーク５５上に実装してもよい。例えばSIPサーバ（例えばP-CSCF）等の機能を仮想ネットワーク５５上に実装し、機能ブロック（FB）５４を、仮想マシン上で動作させ、音声の内容を解析して遮断するコンテンツフィルタリングや、不適当な番号からの着信を禁止する着信拒否リストを備えた構成としてもよい。なお、コンテンツフィルタリングや、不適当な番号からの着信を禁止する着信拒否リストを備えた制御装置を、仮想マシンとしてではなく、実機として、第１のゲートウェイ（GW1）５１と第２のゲートウェイ（GW2）５３との間に接続する構成としてもよいことは勿論である。

[0048] 第１のゲートウェイ（GW1）５１は、VPNゲートウェイとして、特に制限されるものではないが、例えば、

・端末１との間で、無線LAN、WAN1を経由したVPNトンネルの確立、

・セキュリティパラメータのネゴシエーション、

・ユーザの認証、

・プライベートIPアドレスの割り当て、

・データの暗号化と復号化、

・セキュリティキーの管理、

・VPNトンネルを経由するデータ転送の管理、

・VPNトンネルのエンドポイントまたはルータとしての送受信データ伝送の管理、

等を行う。

[0049] なお、プライベートIPアドレスの割り当て等は、第１のゲートウェイ（GW1）５１で行わず、vEPC５２内のPGW等で行うようにしてもよい。

[0050] VPNのトンネリングプロトコルは、PPTP（Point-to-Point Tunneling Protocol）、L2TP（Layer 2 Tunneling Protocol）、IPsec、GRE（Generic Route Encapsulation）があるが、暗号化を行うプロトコルはIPsecである。VPNトンネリングプロトコルとしてIPsecを用いる場合、前述したように、ESPプロト

コルでカプセル化される。また、IPSec-SA設定のため、IKEプロトコルで鍵交換が行われる（IKEでは、UDP(User Datagram Protocol)のポート500番を利用する）。

[0051] 例えば無線ＬＡＮルータ等は、複数の端末（VPNクライアント）が接続することから、端末のプライベートIPアドレスとグローバルIPアドレス、及びTCP(Transmission Control Protocol)/UDPヘッダのポート番号の変換を行うNAPT機能を備えている。

[0052] IPSecのトンネル・モードでは、IPヘッダとデータ部分(図１１（Ａ）)をまとめて暗号化し、新たにIPヘッダ（図１１（Ｃ）のNew IP Header）を再度つけ直して送信を行う(IETF RFC 4303)。NAPTでは、IPヘッダのIPアドレス欄とTCP/UDPヘッダのポート番号を変更する。ESPプロトコルでは、図１１（Ｃ）のように、IPヘッダの次にESPヘッダ（SPI、Serial Number）が配置され、ESPヘッダにはポート番号欄が存在しない。このため、アドレス変換のNAPTが機能しない。すなわち、図２の端末１と第１のゲートウェイ（GW1）５１間にNAPTが存在すると、IPsecを用いたVPNはNAPTによって成立しなくなる。

[0053] この場合、IPsec VPNを、NAPTに対応させるため、図１１（Ｄ）に示すように、ESPパケットにUDPヘッダを付加することで、NAT/NAPTを通過できるようにするUDPカプセル化（UDP Encapsulation of IPsec Packets）手法を用いてもよい。UDPカプセルの場合、図１１（Ｄ）において、最初のIPヘッダは転送用のIPヘッダであり、付加されたUDPヘッダの送信元、宛先ポート番号は、IKEで使用しているのと同じポート番号５００を使い、NAT/NAPTで変更されている場合、変更された番号をそのまま使用する。付加されたUDPヘッダチェックサム欄（checksum）は０とする。UDPヘッダに続くNon-IKE markerはIKEパケットと区別するための設定情報である（０が入る）。これは、追加されたUDPヘッダのポート番号はIKEパケットのポート番号と同じポート番号を使うため、IKEパケットでないことを示すためである。なお、IKEパケットでは、この部分に、ISAKMP_SAのネゴシエーションの開始側が生成するクッキー値とISAKMP_SAのネゴシエーションの応答側が生成するクッキー値が入る。

[0054] L2TPは、PPP(Point-to-Point Protocol)フレームをUDPでカプセル化することによってIPネットワーク上での交換を可能としLAC（L2TP Access Concentrator）とLNS(L2TP Network Server)の2拠点間でのVPNを実現させる。L2TP/IPsecは暗号化の仕組みを持たないＬ２TPにおいてIPsecにより暗号化を行うプロトコルである。L2TP/IPsecでは、最初IPSecによるコネクション（SA）を確立する 。図１１（Ｅ）は、L2TP/IPsecのパケット形式を例示した図である。

[0055] なお、VPNトンネルを、NAT/NAPTに対応させるには、UDPカプセル化以外にも、IPアドレスやポート番号の変化を検出して自動的にNATを検出するNATトラバーサル手法を用いてもよい。

[0056] 次に、VPNクライアント（端末１）とVPNゲートウェイ（GW５１）間でのIPsecを用いたVPNトンネルの設定の手順について説明する。

[0057] （１）IPsec通信による通信相手との間で設定した事前共通鍵（Pre-shared Key）から鍵作成情報を生成して交換し、IKE SA（ISAKMP SA）を確立し、鍵作成情報から鍵を作成する（IKEフェーズ１）。なお、VPNクライアント（端末１）とVPNゲートウェイ（GW５１）間で認証アルゴリズム、暗号アルゴリズム、事前共通鍵は同一とする。

[0058] （２）次に、データ通信用のIPsecトンネルを設定する。IKE SA上で通信を行い、データ通信用のSAを確立する。接続先と同じ認証アルゴリズムと鍵であれば、IPsec SAが確立する。IPsec SAで通信するための鍵を作成する（IKEフェーズ2）。なお、IPsecは一定時間で消滅する。IKE SAは、IPsec SAと比べ長時間保持される。

[0059] （３）次に、暗号化対象のデータに対して、暗号アルゴリズムとIPsec SAで作成した鍵を用いて暗号化、復号化を行う。暗号化されたデータはIPsec SAを転送される。なお、暗号アルゴリズムはDES（Data Encryption Standard）、３DES（Triple Data Encryption Standard）等が用いられ、認証アルゴリズムはMD5（Message Digest Five）や、SHA-1(Secure Hash Algorithm)。

[0060] 図３（Ａ）は、端末１と、データセンタ５０の第１のゲートウェイ（GW1）５１のVPN装置に関する構成を例示した図である。第１のゲートウェイ５１の

VPN装置５１１のVPN設定部５１２は、VPNの設定を制御し、設定情報をVPN情報記憶部５１３に記憶する。VPN通信制御部５１４はVPNトンネルの接続の制御（IKEフェーズ１、２）、暗号化、復号化によるVPNトンネル経由でのデータ通信の通信制御を行う。端末１も同様の構成とされる。

[0061] IPsecVPNの場合、第１のゲートウェイ５１においてVPNトンネルの設定を行う場合、VPN設定部５１２は、VPNを識別するVPN識別子（VPNトンネル識別子）、事前共通鍵（pre-shared key）、通信相手の識別（名前等）、認証アルゴリズム、暗号アルゴリズム、IKEのキープアライブ（VPN切断時、再接続する）の有無を設定する。さらに、経路情報として経路のネットワークアドレス（IPアドレス＋ネットマスク）を設定する。さらに、XAUTH（eXtended AUTHentication）によるユーザ認証の有無や、NATトラバーサルの有無を設定する。XAUTHはIKEフェーズ1（機器の認証）の後、VPNリモートクライアントとサーバ間でユーザ名、パスワードを暗号化して交換しユーザ認証を行う。

[0062] 端末１のVPN装置１０１のVPN設定部１０２においても、VPNクライアントの設定として設定名、事前共通鍵（pre-shared key）、クライアント名、接続先ゲートウェイ（IPアドレス、又は名前）、認証アルゴリズム、暗号アルゴリズム、接続先ネットワーク、NATトラバーサルの有無等を設定する。

[0063] VPN情報記憶部５１３には、例えば、

・IKEの暗号アルゴリズム(3DES-CBC（Cipher Block Chaining Mode）、 DES-CBC、 AES（Advanced Encryption Standard）-CBC)、

・IKEのハッシュアルゴリズム（MD5、SHA-1）、

・ESPのカプセル化（NATによるESPを通過できない環境化でIPsec通信を可能とするため、UDPでカプセル化して送信・受信する）、

・事前共有鍵（pre-shared-key）、

・SAのポリシ（例えば、ポリシ識別子（Policy_ID）、VPNゲートウェイの識別子（gatewaｙ）、認証ヘッダ（AH）、認証アルゴリズム、自装置側のネットワーク識別子、相手側のネットワーク識別子等）、

・トランスポートモードの定義（送信元ポートリスト、宛先ポートリスト）

、

・NATトラバーサルの有無

等の少なくともいずれかが記憶される（ただし、上記に限定されない）。これらの情報は、VPN設定部が入力するコマンドで設定するようにしてもよい。

[0064] 図３（Ｂ）は、VPN設定部５１２で設定されVPN情報記憶部５１３に保存されたVPNの管理情報の一例を例示する図である。VPNには、VPN識別子が付与され、端末（ユーザ）毎に管理される。図３（Ｂ）において、接続相手IPアドレスは第１のゲートウェイ５１等（DHCPサーバ）で払い出したVPNクライアント（端末１）のプライベートIPアドレス（ローカルIPアドレス）である。端末ID/接続先の名前は、端末１のID（例えばIMSI(International Mobile Subscriber Identity)）やユーザIDであってもよい。装置アドレスは第１のゲートウェイ５１（ルータ）のVPNトンネル側のIPアドレスである。接続ネットワークはVPN通信の送信先のネットワークであり、VPNトンネル側のネットワークアドレスである。図３（Ｂ）の例では、図３（Ａ）の端末１に割り当てられたIPアドレスを100.1.100.1とし、接続ネットワークを端末１に割り当てられたIPアドレスを100.1.100.1としている（ネットマスク：32）。データセンタ５０から端末１宛てのパケットはWAN1（３１）に接続する無線LANルータで経路探索され、該当するポートに接続する無線LANアクセスポイントを介して端末１に向けてVPNで送信される。VPNの管理情報として、端末１のIPアドレス、端末ID等以外に、例えば１つのWLANに複数の無線LANアクセスポイントが含まれる場合、端末１の接続先の無線LANアクセスポイントの名前（Access Point Name: APN）、あるいは当該無線LANアクセスポイントが接続する無線LANルータのポート情報等を備えてもよい。なお、図３（Ｂ）に示したVPN情報は一例を示すものであり、かかる構成に制限されるものでないことは勿論である。

[0065] 図３（Ｃ）は、VPNクライアントである端末１のVPN設定部１０２で設定されVPN情報記憶部１０３に保存されたVPNの管理情報の一例を例示する図である。接続先は、拠点のホスト名で指定してもよい（例えばデータセンタ５０

のFDNQ（Fully Qualified Domain Name）等）。接続ネットワークは、VPNクライアント（端末１）からのVPN通信の送信先のネットワークであり、第１のゲートウェイ５１のVPNトンネル側のネットワークアドレスである。接続ネットワークを第１のゲートウェイ５１のVPN側のアドレス：100.1.1.0/24としている（ネットマスク：24）。

[0066] VPN通信制御部５１４、１０４は、VPNトンネルを終端し、セキュリティキーの管理やVPNトンネルを経由するデータ転送の管理、VPNトンネルのエンドポイントまたはルータとしての送受信データ伝送を制御し、データの暗号化とカプセル化によるパケット転送や、パケットのデカプセル化と復号化を行う。

[0067] なお、図３（Ｂ）、図３（Ｃ）では、IPv4（Internet Protocol Version 4）の例で説明しているが、IPV4に制限されるものでないことは勿論である。また、図３（Ｂ）、図３（Ｃ）のIPアドレスは架空のアドレスである。

[0068] なお、図３では、VPNトンネルとしてIPsecトンネルを用いた例を説明したが、L2TP/IPsecを用いる場合、IPsecトンネル内にL2TPトンネルが配設される。L2TPトンネルの確立には、コネクション制御メッセージ及びセッション制御メッセージが用いられる。L2TP/IPsecによるVPNを構築する場合には、コネクション制御メッセージによってトンネルを作成したのち、セッション制御メッセージによってセッションを確立される。

[0069] 上記したように、VPNは、端末単位（端末ID、共通アカウント）で割り振られる。図３(B)において、端末ID/名前の欄は、ユーザIDのほか、データセンタ５０のクライド事業者がユーザに提供するユーザアカウント(例えば：”aaa@example.com”)であってもよい。すなわち、第１のゲートウェイ５１において、VPNの管理は、端末１（VPNクライアント）のIPアドレス以外にも、ユーザ固有の情報（ユーザアカウントあるいはWebメールアドレス等）を用いてもよい。

[0070] 端末１が無線LANアクセスポイント４１に最初にアクセスすると、無線LANアクセスポイント４１は、端末１からのアクセス要求パケットを、メインと

なるデータセンタ５０にWAN１（３１）を介して転送する。データセンタ５０の第１のゲートウェイ（GW1)５１は、端末１にIPアドレス（プライベートIPアドレス）を割り当て、VPNトンネル６０を張る。VPNトンネル６０をIPsecトンネルとする場合、前述したように、IKE SAの確立（IKEフェーズ）１、IPsec SAの確立（IKEフェーズ２）、IPsec SA上での暗号化通信が行われる。

[0071] 図４は、図２を参照して説明した例示的な一実施形態のシステムにおいて、端末１の初期アタッチ処理とWAN2（３２）に接続する接続先３３に接続するシーケンスの一例を説明する図である。図４には、図２の端末１、WLAN４０、第１のゲートウェイ５１（GW1）、vEPC５２、第２のゲートウェイ（GW２）５３、WAN2（３２）における動作シーケンスの一例が模式的に例示されている。各シーケンス動作に付した番号は説明のためのシーケンス番号である。

[0072] １． 端末１は、無線LAN（WLAN）４０との間で接続を確立し、例えばvEPC５２内の不図示のHSS/AAAにより認証・認可（Authentication & Authorization）を行う。なお、図４の例では、第１のゲートウェイ５１（GW1）は、セキュリティ上信頼できない非3GPP無線アクセス（Untrusted Non-3GPP IP Access）である無線LAN４０を収容する場合に、端末１が接続するゲートウェイとして設定されているものとする。

[0073] ２． 端末１側から、第１のゲートウェイ（GW1）５１との間のIKE認証・トンネルセットアップ手順を実行する。これは、前述したIKEフェーズ１、２に対応する。IKEv2認証トンネルセットアップであってよい。

[0074] ３． vEPC５２がSGWとPGWを含み、ベアラの設定が必要な場合、第１のゲートウェイ（GW1）５１は、vEPC５２に対して例えばベアラ設定要求（Create Session Request）を送信する。この場合、接続先のパケットデータ網に接続するPGWが選択され、SGWとPGW間のS８インタフェースにGTP（GPRS(General Packet Radio System) Tunneling Protocol）トンネルが張られる。

[0075] ４． vEPC５２から第１のゲートウェイ（GW1）５１にベアラ設定応答（Create Session Response）が送信される。

[0076] ５．　以上で、IPsec VPNトンネルのセットアップが完了する。

[0077] ６．　第１のゲートウェイ（GW1）から、IKEv2メッセージで端末１に払い出されたIPアドレスが通知される。

[0078] ７．　端末１から第１のゲートウェイ（GW1）へのＩＰ接続はこの時点で設定される。以上がアタッチ処理のシーケンスに対応する。

[0079] ８．　端末１側からのWAN２（３２）側に接続先３３への接続要求を受けると、第１のゲートウェイ（GW1）５１から接続先（WAN2側）３３へのIPルーチングが行われる。

[0080] ９．　以上で、端末１からVPN、データセンタ５０のvEPC５２を介し、WAN２側の接続先３３との間の接続の設定が完了する。なお、WAN２（３２）側から端末１へのダウンリンク方向のパケットは、vEPC５２内のPGWが、PCRF等のポリシに応じて、第１のゲートウェイ５１（GW1）に転送し、第１のゲートウェイ５１（GW1）からVPNトンネル６０を介して端末１に転送される。

[0081] 図５（Ａ）は、図２の機能ブロック５４の構成の一例を示す図である。図５（Ａ）を参照すると、機能ブロック５４は、

・パケットを受信し、転送制御部５４２からの制御のもと、許可されたパケットを通話させる通信部５４１と、

・パケットの廃棄、通過を制御するフィルタ情報を記憶するフィルタ情報記憶部５４３と、

・通信部５４１で受信したパケットのヘッダからアドレス、ポート、プロトコルを抽出し、フィルタ情報記憶部５４３の条件と照合し、当該パケットの拒否、許可を判定し、判定結果を通信部５４１に通知する転送制御部５４２と、

・フィルタ情報記憶部５４３に、フィルタ情報を設定するフィルタ情報設定部５４４と、

を備えている。

[0082] フィルタ情報設定部５４４は、図２のデータセンタ５０内の管理端末（不図示）、あるいは端末１からのベアラリソース修正要求等により、フィルタ

情報記憶部５４３のフィルタ情報を設定するようにしてもよい。フィルタ情報設定部５４４からの端末１毎のフィルタ情報の設定により、機能ブロック５４は、等価的に、端末１毎に設けられることになる。

[0083] 図５（Ｂ）は、図５（Ａ）のフィルタ情報記憶部５４３の構成として、パケットフィルタ情報の一例を示す。図５（Ｂ）を参照すると、種別（フィルタの条件に一致したパケットの扱い：通過、又は廃棄）、方向（フィルタの評価の方向：無線LANからWAN２をUP、WAN2から無線LANをDOWNとしている）、プロトコル（フィルタ対象とするパケットのIPプロトコル）、送信元アドレス（フィルタ対象とするパケットの送信元IPプロトコル）、送信ポート（フィルタ対象とするパケットの送信元ポート）、宛先アドレス（フィルタ対象とするパケットの宛先IPプロトコル）、宛先ポート（フィルタ対象とするパケットの宛先ポート）等を含む。

[0084] フィルタID＝１では、ポート２３（telnet）（TCPポート番号＝２３）からの第１のゲートウェイ（GW1）５１に対するパケットを廃棄する。フィルタID＝２では、端末１のプライベートIPアドレスを宛先とするパケットを廃棄する。フィルタID＝3では、端末１からの特定の宛先アドレスへパケットを廃棄する。なお、図５（Ｂ）の記号＊は、任意（any）を表している。

[0085] 図５（Ｂ）において、フィルタID＝２、３等のフィルタ情報が、端末１（加入者）に固有の情報である。なお、図５（Ｂ）のフィルタID＝１のフィルタ情報（宛先がGW１、送信ポート＝２３のパケット）も、端末１（加入者）に対応するフィルタ情報に含めるようにしてもよいことは勿論である。

[0086] 図５（Ｂ）の機能ブロック５４を端末（加入者）毎に機能ブロック５４を割り振る場合、図５（Ｂ）のフィルタ情報を、フィルタ情報設定部５４４から、端末（加入者）毎にフィルタ情報記憶部５４３に設定し、該フィルタ情報を、端末１に紐付けて管理し、他の転送制御部５４２、通信部５４１、フィルタ情報設定部５４４は、複数の端末に対して、共通のコードで実現するようにしてもよい。なお、データセンタ５０において、端末１（加入者）の管理は、端末１のユーザに対して、データセンタ５０側で割り当てたユーザ

アカウントを用いてもよい。

[0087] 図６は、前述した実施形態の一例を例示する図である。図６を参照すると、データセンタ５０のvEPC５２のePDG５２７と端末１間にIPsecトンネルが設定される。ePDG５２７は、VPNゲートウェイとして機能し、VPNトンネルを終端する。

[0088] ePDG５２７は、VPNゲートウェイとして機能し、

・端末１との間での、無線LAN４０、WAN１（３１）を介してのVPN(IPsec)トンネルの確立、

・セキュリティパラメータのネゴシエーション、

・ユーザの認証、

・端末１へのプライベートIPアドレスの割り当て、

・データの暗号化と復号化、

・セキュリティキーの管理、

・VPNトンネルを経由するデータ転送の管理、

・VPNトンネルのエンドポイントとしての送受信データ伝送の管理を行う。なお、端末１へのプライベートIPアドレスの割り当ては、vEPC５２のPGW５２２で行うようにしてもよい。

[0089] 端末１からIKEV2でEAPメッセージをePDG５２７に送信し、vEPC５２の3GPP AAAサーバ５２５に中継し、EAP-SIM/EAP-AKA認証を行う。vEPC５２のePDG５２７とPGW５２２間は、GTP又はPMIPv6トンネルで接続される。

[0090] vEPC５２において、PGW２２とePDG２７間でプロキシモバイルIP(PMIPv6トンネル)を使用する場合、端末１とvEPC５２のePDG２７との間でIPsecトンネルが確立されると、ePDG２７は、プロキシバインディングアップデート（Proxy Binding Update）をPGW22に送信する。この結果、vEPC５２のPGW２２では、端末１への着信の送信先を、vEPC５２のePDG２７に切り替え、VPNトンネル６０を介し、WLAN４０経由で、着信が端末１に通知される。

[0091] PGW５２２には、例えばEPSベアラに関するTFT（Traffic Flow Template）を有するパケットフィルタ５２９が接続されている。なお、パケットフィル

タ５２９は、図２の機能ブロック５４として機能し、端末１毎に設けられる。すなわち、パケットフィルタ５２９におけるフィルタ情報（パケットの廃棄等）は、前述したように、端末１（加入者）毎に設けられる。パケットフィルタ５２９は、PGW５２２内に配置してもよいことは勿論である。

[0092] パケットフィルタ５２９において、WAN2から端末１側への下り方向や端末１からWAN2への上り方向のフィルタ情報の設定（追加、修正、削除等）は、上記したように、端末１からのベアラリソース修正手順のRequest Bearer Resource Modificationメッセージ（3GPP TS 23.401等を参照してもよい）で行うようにしてもよい。

[0093] あるいは、パケットフィルタ５２９におけるフィルタ情報の設定は、端末１からAttach Request等の接続要求処理や、その他、所定のイベント発生時等に行ってもよい。なお、パケットフィルタ５２９は、アプリケーション層でのフィルタリングを行う機能、あるいはステートフルインスペクション機能を備えた構成としてもよいことは勿論である。あるいは、パケットフィルタ５２９に、WAN２（３２）からの着信を拒否する着信拒否リストを備えた構成としてもよい。

[0094] WAN２（３２）をIMSで構成した場合、vEPC52と接続するP-CSCF(Proxy-Call Session Control Function)や、Serving-CSCFに、音声の内容を解析して遮断するコンテンツフィルタリングや、不適当な番号からの着信を禁止する着信拒否リストを備えた構成としてもよい。なお、SGW５２１は、不図示3GPPアクセスネットワークからのデータセンタ５０のアクセスに接続される。なお、図６において、パケットフィルタ５２９以外にも、さらに別の機能ブロック５４を備えた構成としてもよい。図６の例では、機能ブロック５４として、データ圧縮器５３０をePDG５２７に接続し、当該データ圧縮器５３０において、端末１の能力情報あるいは機種情報等に応じて、端末１向けに転送されるパケットのペイロード部のデータの圧縮率を可変させるようにしてもよい。あるいは、データ圧縮器５３０を、PGW５２２に接続し、WAN２（３２）に送信するデータの圧縮率を可変に制御するようにしてもよい。

[0095] 図６では、ePDG５２７、PGW５２２をvEPC５２で実装しているが、クラウド事業者がMVNO（Mobile Virtual Network Operator）として、例えばMNO（Mobile Network Operator）のePDG２７、PGW２２（図１）を借り受けたものであってもよい。

[0096] 例えば端末１からのWi-Fi（登録商標）-Callingについては、端末１とePDG５２７との間で、WLAN４０、WAN1（３１）を経由したVPN６０（IPsecトンネル）が張られ、ePDG５２７とPGW５２２間にGTP/PMIPv6のトンネルが張られ、PGW５２２から、例えばIMSからなるWAN２（３２）を介して、接続先に接続される。すなわち、Wi-Fi（登録商標）-Callingは、クラウド事業者（MVNO）による通信サービスとして制御され、セキュアなコネクションが提供されるとともに、パケットフィルタ５２９により、不等な着信や有害サイト等からの保護が提供される。なお、PGW５２２は、図２の第２のゲートウェイ（GW2）５３としての機能と、機能ブロック５４の機能を併せ持つようにしてもよい。

[0097] 図７は、図６のシステムにおいて、端末１の初期アタッチ処理とWAN2（３２）に接続する接続先３３に通信接続するシーケンスを模式的に説明する図である。図７には、図６の端末１、WLAN４０（WLAN AP）、ePDG５２７、PGW５２２、HSS５２４/AAAサーバ５２５、PCRF５２６、WAN2（３２）側の接続先３３における動作シーケンスの一例が例示されている。各シーケンス動作に付した番号は説明のためのシーケンス番号である。図７において、例えばePDG５２７を第１のゲートウェイ（GW1）、PGW５２２を第２のゲートウェイ（GW２）に置き換えると、図４を参照して説明した動作に、一部対応させることができる。

[0098] １． 端末１は、無線LAN（WLAN）４０との間で接続を確立し、例えばvEPC５２内ののHSS524/AAA５２５により認証・認可（Authentication & Authorization）を行う。

[0099] ２． 端末１側から、ePDG５２７の間のIKEv2認証・トンネルセットアップ手順（IKEv2のフェーズ１、２等）を実行する。

[0100] ３．　ePDG５２７は、PGW５２２に対してProxy Binding Update（モバイルノードのホームネットワークプレフィクスと、モバイルノードが接続されているMAG（Mobile Access Gateway）との間のバインディングを確立するために、MAGによってLMA（Local Mobility Anchor）に送信される要求メッセージ）を送信する。

[0101] ４．　PGW５２２は、PCRF５２６と連携して、IP接続アクセスネットワーク（IP－CAN（Connection Access Network））セッションの確立手順を行う。

[0102] ５．　PGW５２２は、AAAサーバ５２５にPGWの識別情報（PGW ID）を通知し、AAAサーバ５２５は、HSS５２４に、PGW５２２のIDと、端末１に対応したAPN（Access Point Name）を通知して登録する。

[0103] ６．　PGW５２２はプロキシバインディングアップデート処理を行い、端末１に対応したバインディング・キャッシュ・エントリを作成する。これにより、PGW５２２において、端末１宛てのパケットは、バインディング・キャッシュ・エントリに保持された内容に従い、ePDG５２７に向けて送信されることになる。PGW５２２は、ePDG５２７に対してプロキシバインディング応答（Proxy Binding Ack）を送信する。

[0104] ７．　以上で、IPsec VPNトンネルのセットアップが完了する。

[0105] ８．　ePDG５２から端末１に対してIKEv2メッセージで、IPアドレスが通知される。

[0106] ９．　端末１からのIP接続のセットアップが完了する。端末１とePDG５２７間はIPsecトンネル、ePDG５２７とPGW５２２間は、PMIP（Proxy Mobile Internet Protocol）等のトンネルが張られる。以上がアタッチ処理のシーケンスに対応する。

[0107] １０．　端末１側からのWAN２（３２）側に接続先３３への接続要求をePDG５２７からPMIPトンネルを介して受けると、PGW５２２から接続先（WAN2側）へのIPルーチングが行われる。この場合、端末１からのSIPメッセージが第２のゲートウェイ（GW2）５３を介してIMSのP-CSCFに送信され、S-CSCF、MGCF、あるいはMGW等を介して例えばPSTN（Public Switched Telephone Networks）

の接続先３３に接続するようにしてもよい。あるいは、S-CSCFからインターネット又は他のIMSに接続する接続先３３に接続するようにしてもよい。なお、図６では、端末１はIMSに対して登録済みであるものとする。IMSのP-CSCFとPGW５２２（SGiインタフェース）はIPsec（VPN）で通信を行う。

[0108] １１．　以上で、端末１からVPN、データセンタ５０のvEPC５２を介し、WAN２側の接続先３３との間の接続の設定が完了する。なお、WAN２（３２）側から端末１へのダウンリンク方向のパケットは、vEPC５２内のPGW５２２がバインディング・キャッシュ・エントリに基づきePDG５２７にPIMPトンネルを介して転送し、ePDG５２７からVPNトンネル６０を介して端末１に転送される。

[0109] 次に、図１０を参照して、vEPC５２のノードの構成について説明する。データセンタ５０内のサーバ５７上の仮想マシン（Virtual Machine: VM）５７１は仮想ネットワークインタフェースコントローラ（vNIC）５７５を介して仮想スイッチ（vSwitch）５７６の仮想ポート：Ａに接続し、仮想スイッチ（vSwitch）５７６の仮想ポート：Ｂから物理ＮＩＣ（pNIC）５７７を介して物理スイッチ（Physical Switch）５８の物理ポート：Ｃに接続され、物理スイッチ（Physical Switch）５８の物理ポート：Ｄを介して、データセンタ５０内のLAN等のネットワーク５５に接続される。仮想マシン５７１は、ゲストOS（Operating System）５７３と、アプリケーション５７２を備え、EPCのネットワークノードの機能の一部又は全て（例えば図６のePDG５２７の機能、あるいは他のノードの機能）を実現する。仮想ネットワーク５９は例えば図６のルータ５６に接続される。なお、前述したように、図２の機能ブロック５４を、図１０の仮想マシン（Virtual Machine: VM）５７１で構成してもよい。

[0110] 仮想NIC（vNIC）、仮想スイッチ（vSwitch）等は、サーバ５７上の仮想化機構であるハイパーバイザ（Hypervisor）５７４によって提供される。なお、物理スイッチ５８をL2（Layer 2）スイッチで構成し、ネットワーク５９をVLAN（Virtual LAN）等の仮想ネットワークで構成してもよい。

[0111] 同様に、図１０の仮想マシン５７１で、図２の機能ブロック５４を実装し

、VLAN等のネットワーク５９で、図２の仮想ネットワーク５５を構成してもよい。なお、図９では、ネットワーク機能の仮想化を管理統合するマネージャ等、NFV(Network Functions Virtualization)の管理ユニット(NFV Orchestrator (NFVO)、VNF (Virtualized Network Function) Manager等)は省略されている。

[0112] 図８は、別の実施形態を説明する図である。図８に示す実施形態では、一つの無線LANアクセスポイント４１に、クラウド事業者のデータセンタ５０のvEPC５２に、端末１－１、１－２、１－３がアクセスしている。

[0113] データセンタ５０では、複数の端末１－１～１－３について、端末毎、あるいは当該端末のユーザのアカウント毎に、VPNを管理し、同時に複数のVPNトンネル６０－１～６０－３を収容するようにしてもよい。なお、端末１－１～１－３の各々の構成、及び動作等については、前記実施形態と同様である。

[0114] データセンタ５０は、VPN６０－１～６０－３に第１のゲートウェイ（GW1）５１を介してそれぞれ接続する複数の機能ブロック５４－１～５４－３と、複数の機能ブロック５４－１～５４－３と、第２のゲートウェイ（GW2）５３間に接続する機能ブロック５４－４を備えている。

[0115] 機能ブロック５４－１～５４－３は、ユーザ側からフィルタ対象のパケット（ペアレンタルコントロールやアクセス拒否等）の設定を行うようにしてもよい。機能ブロック５４－４は、データセンタ５０のクラウド事業者の保守端末又は制御装置（不図示）等からフィルタ対象のパケット（例えば特定の地域、サイト等からのパケット）を設定するようにしてもよい。ユーザ側から機能ブロック５４－１～５４－３を設定する場合、端末１側から、データセンタ５０に対する要求メッセージにより設定するようにしてもよい。あるいは、端末１のユーザと、データセンタ５０でvEPC５２を提供するクラウド事業者との契約情報に基づき、データセンタ５０を所持するクラウド事業者側の保守端末又は制御装置（不図示）等から、機能ブロック５４－１～５４－３に対して、フィルタ対象の設定を行うようにしてもよい。

[0116] なお、１つの無線LANアクセスポイント４１に複数の端末が接続すると、複数の端末は電波を共有して通信することになり、複数（多数）の端末が１つの無線LANアクセスポイント４１にアクセスすると、各端末のスループット（単位時間あたりのデータ転送量等）が低下する。そこで、１つの無線LANアクセスポイント４１に複数の端末が接続し、アクセスが集中している場合、複数の端末の接続先を、アクセスが集中している無線アクセスポイントとは別の無線アクセスポイントに振り分け、負荷を分散させる制御を行う無線LANコントローラ（不図示）等を備えた構成としてもよい。

[0117] 図９は、本発明のさらに別の実施形態を説明する図である。図９を参照すると、本実施形態では、第１のゲートウェイ（GW1）と第２のゲートウェイ（GW2）間の仮想ネットワーク５５上の機能ブロック５４－１に加えて、vEPC５２内に機能ブロック５４－２を備えている。例えば機能ブロック５４－１は、データ通信用のパケットのフィルタリングを行う。vEPC５２内の機能ブロック５４－２は、例えばユーザ側の指定した電話番号番号からの着信拒否や、ユーザ側の指定した電話番号が登録されているSMSや着信を許可する。機能ブロック５４－１と機能ブロック５４－２は、等価的に、端末１毎に、フィルタ情報等が設定され、等価的に、端末１毎に設けられる構成とされる。

[0118] 機能ブロック５４－２は、IMSのSIPサーバの機能の少なくとも一部を仮想化して、例えばPGWに接続し、着信拒否や許可の制御を実現するようにしてもよい。あるいは、図６を参照して説明したように、vEPC５２のPGWでTFTを管理するパケットフィルタ（図６の５２９）に、機能ブロック５４－２の機能を付加してもよいことは勿論である。

[0119] 第１のゲートウェイ（GW1）と第２のゲートウェイ（GW2）間の機能ブロック５４－１は、WAN2（３２）から端末１側へのパケットのデータを、端末１の能力情報等（SDP（Session Description Protocol）による能力交換等）に基づき、圧縮符号化の圧縮率を、端末１側の能力や機種等に適応するように変更した上で、第１のゲートウェイから端末１に転送するようにしてもよい。この場合、機能ブロック５４－１は、WAN２（３２）から第２のゲートウェ

イで受信したパケットのデータ（圧縮符号化データ）を、一旦復号した上で再符号化し、圧縮率を変更するというトランスコード処理を行うようにしてもよい。トランスコード処理において、ビットレート、フレームレート、解像度等を変更してもよい。例えば端末１にダウンロードされるデータサイズを圧縮し、ネットワーク負荷の低減、転送効率の向上、帯域の有効利用を図ることができる。

[0120] なお、上記の非特許文献１の開示を、本書に引用をもって繰り込むものとする。本発明の全開示（請求の範囲を含む）の枠内において、さらにその基本的技術思想に基づいて、実施形態ないし実施例の変更・調整が可能である。また、本発明の請求の範囲の枠内において種々の開示要素（各請求項の各要素、各実施例の各要素、各図面の各要素等を含む）の多様な組み合わせ乃至選択が可能である。すなわち、本発明は、請求の範囲を含む全開示、技術的思想にしたがって当業者であればなし得るであろう各種変形、修正を含むことは勿論である。

[0121] 上記した実施形態は以下のように付記される（ただし、以下に制限されない）。

[0122]（付記１）

端末が接続する無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）との間に第１の広域ネットワーク（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）が介在するデータセンタを備え、

前記データセンタが、

前記端末との間を、前記無線ＬＡＮを介し前記第１の広域ネットワーク経由のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）で接続する第１のゲートウェイと、

第２の広域ネットワークに接続する第２のゲートウェイと、

前記第１のゲートウェイと前記第２のゲートウェイに接続された仮想ネットワークと、

前記第１のゲートウェイと前記第２のゲートウェイ間に設けられ、前記第

１の広域ネットワーク側から入力されるパケット、及び、前記第２の広域ネットワーク側から入力されるパケットのうち少なくとも一方のパケットのフィルタリングを行う機能ブロックと、

を備えた、通信システム。

[0123]（付記２）

前記データセンタにおいて、

前記仮想ネットワークが、パケットコアネットワークの機能の少なくとも一部を仮想化した仮想パケットコアネットワークを含む、付記１記載の通信システム。

[0124]（付記３）

前記データセンタにおいて、

前記機能ブロックが、

前記第１のゲートウェイと前記第２のゲートウェイ間に接続された第１の機能ブロックと、

前記仮想パケットコアネットワークに接続された第２の機能ブロックと、

のうち少なくとも一つを含む、付記２記載の通信システム。

[0125]（付記４）

前記データセンタにおいて、

前記機能ブロックが、

パケットの遮断、通過を制御するパケットフィルタに加えて、

前記端末への着信やテキストメッセージのアクセス拒否、許可を制御する機能ブロックを有する、付記１乃至３のいずれか一に記載の通信システム。

[0126]（付記５）

前記データセンタにおいて、

前記機能ブロックが、

前記第２の広域ネットワーク側から入力されたパケット、及び、前記端末側から前記第１の広域ネットワークを介して入力されたパケットのうち少なくとも一方のパケットのペイロード部のデータの圧縮を制御する機能ブロッ

クを、さらに備えた、付記１乃至３のいずれか一に記載の通信システム。

[0127]（付記６）

前記データセンタにおいて、

前記機能ブロックが、

前記端末に対応させて設けられ、前記端末毎に、前記端末に対するパケットのフィルタリング、及び／又は、前記端末への着信やメッセージのアクセスの拒否、許可が設定される機能ブロックを有する付記１乃至５のいずれか一に記載の通信システム。

[0128]（付記７）

前記端末に対して前記無線ＬＡＮを介して提供される音声通話又はテキストメッセージのサービスにおいて、

前記端末は、前記ＶＰＮから前記データセンタの前記仮想パケットコアネットワーク、前記第２の広域ネットワークを介して接続先と通信し、

前記第２の広域ネットワーク側からの前記端末への着呼又はメッセージのうち、前記データセンタの前記仮想パケットコアネットワークに接続された前記第２の機能ブロックで許可された着呼又はメッセージが、前記ＶＰＮを介して、前記端末に送信される、付記３記載の通信システム。

[0129]（付記８）

前記端末に対して前記無線ＬＡＮを介して提供されるデータ通信サービスにおいて、

前記端末は、前記ＶＰＮから前記データセンタの前記仮想ネットワークを介して前記第２の広域ネットワークに接続し、

前記第２の広域ネットワーク側からの前記端末へのデータは、前記データセンタの前記第１のゲートウェイと前記第２のゲートウェイ間に接続された前記第１の機能ブロックでフィルタリングされ、許可されたパケットが前記ＶＰＮを介して、前記端末に送信される、付記３又は７記載の通信システム。

[0130]（付記９）

一つの無線ＬＡＮアクセスポイントに接続する第１乃至第Ｎ（Ｎは２以上の整数）の端末と、前記データセンタの前記第１のゲートウェイ間を第１乃至第ＮのＶＰＮで接続し、

前記データセンタにおいて、

前記機能ブロックが、

前記第１のゲートウェイで終端される前記第１乃至第ＮのＶＰＮにそれぞれ接続される第１乃至第Ｎの機能ブロックを備え、さらに、

前記第１乃至第Ｎの機能ブロックに一端で接続され、前記第２のゲートウェイに他端が接続された第Ｎ＋１の機能ブロックを備え、

前記第１乃至第Ｎの機能ブロックの設定は、前記第１乃至第Ｎの端末のユーザ側から行われ、

前記第Ｎ＋１の機能ブロックの設定は、前記データセンタ側で行われる、付記１又は２記載の通信システム。

[0131]（付記１０）

前記データセンタにおいて、

前記第１のゲートウェイは、端末単位又は前記端末のユーザ単位に、前記端末との間の前記ＶＰＮを管理する、付記１乃至９のいずれか一に記載の通信システム。

[0132]（付記１１）

端末が接続する無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）との間に第１の広域ネットワーク（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）が介在する通信装置であって、

前記端末との間を、前記無線ＬＡＮを介し前記第１の広域ネットワーク経由のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）で接続する第１のゲートウェイと、

第２の広域ネットワークに接続する第２のゲートウェイと、

前記第１のゲートウェイと前記第２のゲートウェイに接続された仮想ネットワークと、

前記第１のゲートウェイと前記第２のゲートウェイ間に設けられ、前記第１の広域ネットワーク側から入力されるパケット、及び、前記第２の広域ネットワーク側から入力されるパケットのうちの少なくとも一方のパケットのフィルタリング制御を行う機能ブロックと、

を備えた、通信装置。

[0133]（付記１２）

前記仮想ネットワークが、パケットコアネットワークの機能の少なくとも一部を仮想化した仮想パケットコアネットワークを含む、付記１１記載の通信装置。

[0134]（付記１３）

前記機能ブロックが、

前記第１のゲートウェイと前記第２のゲートウェイ間に接続された第１の機能ブロックと、

前記仮想パケットコアネットワークに接続された第２の機能ブロックと、

のうち少なくとも一つを含む、付記１２記載の通信装置。

[0135]（付記１４）

前記機能ブロックが、パケットの遮断、通過を制御するパケットフィルタに加えて、

前記端末への着信やテキストメッセージのアクセス拒否、許可を制御する機能ブロックを有する、付記１１乃至１３のいずれか一に記載の通信装置。

[0136]（付記１５）

前記データセンタにおいて、

前記機能ブロックが、

前記第２の広域ネットワーク側から入力されたパケット、及び、前記端末側から前記第１の広域ネットワークを介して入力されたパケットのうち少なくとも一方のパケットのペイロード部のデータの圧縮を制御する機能ブロックを、さらに備えた、付記１１乃至１３のいずれか一に記載の通信装置。

[0137]（付記１６）

前記機能ブロックが、

前記端末に対応させて設けられ、前記端末毎に、前記端末に対するパケットのフィルタリング、及び／又は、前記端末への着信やメッセージのアクセスの拒否、許可が設定される機能ブロックを有する付記１１乃至１５のいずれか一に記載の通信装置。

[0138]（付記１７）

前記端末に対して前記無線ＬＡＮを介して提供される音声通話又はテキストメッセージのサービスにおいて、

前記端末は、前記ＶＰＮから前記通信装置の前記仮想パケットコアネットワーク、前記第２の広域ネットワークを介して接続先と通信し、

前記第２の広域ネットワーク側からの前記端末への着呼又はメッセージのうち、前記通信装置の前記仮想パケットコアネットワークに接続された前記第２の機能ブロックで許可された着呼又はメッセージが、前記ＶＰＮを介して、前記端末に送信される、付記１３記載の通信装置。

[0139]（付記１８）

前記端末に対して前記無線ＬＡＮを介して提供されるデータ通信サービスにおいて、

前記端末は、前記ＶＰＮから前記データセンタの前記仮想ネットワークを介して前記第２の広域ネットワークに接続し、

前記第２の広域ネットワーク側からの前記端末へのデータは、前記通信装置の前記第１のゲートウェイと前記第２のゲートウェイ間に接続された前記第１の機能ブロックでフィルタリングされ、許可されたパケットが前記ＶＰＮを介して、前記端末に送信される、付記１３又は１７記載の通信装置。

[0140]（付記１９）

一つの無線ＬＡＮアクセスポイントに接続する第１乃至第Ｎ（Ｎは２以上の整数）の端末と、前記通信装置の前記第１のゲートウェイ間を第１乃至第ＮのＶＰＮで接続し、

前記機能ブロックが、

前記第１のゲートウェイで終端される前記第１乃至第ＮのＶＰＮにそれぞれ接続される第１乃至第Ｎの機能ブロックを備え、さらに、

前記第１乃至第Ｎの機能ブロックに一端で接続され、前記第２のゲートウェイに他端が接続された第Ｎ＋１の機能ブロックを備え、

前記第１乃至第Ｎの機能ブロックの設定は、前記第１乃至第Ｎの端末のユーザ側から行われ、

前記第Ｎ＋１の機能ブロックの設定は、前記通信装置側で行われる、付記１１又は１２記載の通信装置。

[0141]（付記２０）

前記第１のゲートウェイは、端末単位又は前記端末のユーザ単位に、前記端末との間の前記ＶＰＮを管理する、付記１１乃至１９のいずれか一に記載の通信装置。

[0142]（付記２１）

端末が接続する無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）との間に第１の広域ネットワーク（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）が介在するデータセンタの第１のゲートウェイと前記端末との間を、前記無線ＬＡＮを介し前記広域ネットワーク経由のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）で接続し、

前記端末から前記ＶＰＮを介して、前記データセンタに設けられた、仮想ネットワークから第２のゲートウェイを介して第２の広域ネットワークに接続し、

前記第１のゲートウェイと前記第２のゲートウェイ間に設けられた機能ブロックにて、前記第１の広域ネットワーク側から入力されるパケット、及び、前記第２の広域ネットワーク側から入力されるパケットのうちの少なくとも一方のパケットのフィルタリングを行う、通信方法。

[0143]（付記２２）

前記データセンタにおいて、

前記仮想ネットワークが、パケットコアネットワークの機能の少なくとも

一部を仮想化した仮想パケットコアネットワークを含む、付記２１記載の通信方法。

[0144]（付記２３）

前記データセンタは、前記第２の広域ネットワーク側から入力されたパケットと、前記端末側から入力されたパケットのうち、少なくとも一方のパケットのペイロード部のデータの圧縮を制御する、付記２１又は２２記載の通信方法。

[0145]（付記２４）

前記データセンタにおいて、前記機能ブロックは、前記端末に対応させて設けられ、

前記端末毎に、前記端末に対するパケットのフィルタリング、及び／又は、前記端末への着信やメッセージのアクセスの拒否、許可が設定される付記２１乃至２３のいずれか一に記載の通信方法。

[0146]（付記２５）

無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）と第１の広域ネットワーク（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）とを介してデータセンタに接続する端末であって、

前記データセンタとの間を、前記無線ＬＡＮ及び前記広域ネットワーク経由のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）で接続するＶＰＮ装置を備え、

前記ＶＰＮを介して、前記データセンタに設けられており、パケットコアネットワークの機能の少なくとも一部を仮想化した仮想ネットワークを介して第２の広域ネットワークに接続する手段と、

前記第２の広域ネットワーク側から前記データセンタ内に入力された前記端末への着呼又は前記端末宛てのデータのうち、前記データセンタ内の機能ブロックでフィルタリングされた着呼又はデータを、前記ＶＰＮを介して、受信する手段を備えた、端末。

[0147]（付記２６）

前記データセンタ内の前記機能ブロックにおけるフィルタリングの設定を行う機能を備えた付記２５記載の端末。

[0148]（付記２７）

端末が接続する無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）との間に第１の広域ネットワーク（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）が介在するデータセンタに配置されるコンピュータに、

前記端末と前記データセンタとの間に、前記無線ＬＡＮを介し前記広域ネットワーク経由のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）を開設する処理と、

前記端末から前記ＶＰＮを介して、前記データセンタに設けられており、コアネットワークの構成要素の少なくとも一部を仮想化した仮想ネットワークを介して第２の広域ネットワークに接続する処理と、

前記第１の広域ネットワーク側から入力されるパケット、及び、前記第２の広域ネットワーク側から入力されるパケットのうちの少なくとも一方のパケットのフィルタリングを行う処理と、

を実行させるプログラム。

[0149]（付記２８）

無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）と第１の広域ネットワーク（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）を介してデータセンタに接続する端末に含まれるコンピュータに、

前記データセンタと前記端末との間に、前記無線ＬＡＮを介し前記広域ネットワーク経由のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）を開設する処理と、

前記ＶＰＮを介して、前記データセンタに設けられており、パケットコアネットワークの機能の少なくとも一部を仮想化した仮想ネットワークを介して第２の広域ネットワークに接続する処理と、

前記第２の広域ネットワーク側から前記データセンタ内に入力された前記端末への着呼又は前記端末宛てのデータのうち、前記データセンタ内でフィ

ルタリングされた着呼又はデータを、前記ＶＰＮを介して、受信する処理と

、

を実行させるプログラム。

符号の説明

[0150] １、１－１～１－３　端末（UE）

１０　基地局（eNB）

２０　EPC

２１　SGW

２２　PGW

２３　MME

２４　HSS

２５　3GPP　AAA

２６　PCRF

２７　ePDG

３０　PDN

３１　WAN1

３２　WAN2

４０　WLAN

４１、４２　無線LANアクセスポイント（WLAN AP）

５０　データセンタ（DC）

５１　第１のゲートウェイ（GW1）

５２　仮想化EPC（vEPC）

５３　第２のゲートウェイ（GW2）

５４、５４－１～５４－４　機能ブロック

５５　仮想ネットワーク

５６　ルータ

５７　サーバ

５８　物理スイッチ

５９　ネットワーク（仮想ネットワーク）

６０、６０－１～６０－３　VPNトンネル

１０１　VPN装置

１０２　VPN設定部

１０３　VPN情報記憶部

１０４　VPN通信制御部

５１１　VPN装置

５１２　VPN設定部

５１３　VPN情報記憶部

５１４　VPN通信制御部

５２１　SGW

５２２　PGW

５２４　HSS

５２５　AAA

５２６　PCRF

５２７　ePDG

５２８　S2b (GTP/PMIPv6)

５２９　パケットフィルタ

５３０　データ圧縮器

５４１　通信部

５４２　転送制御部

５４３　フィルタ情報記憶部

５４４　フィルタ情報設定部

５７１　仮想マシン

５７２　アプリケーション

５７３　OS

５７４　ハイパーバイザ

５７５　仮想NIC

５７６　仮想スイッチ

５７７　物理NIC

請求の範囲

[請求項1] 端末が接続する無線LAN（Local Area Network）との間に第１の広域ネットワーク（Wide Area Network）が介在するデータセンタを備え、

前記データセンタが、

前記端末との間を、前記無線LANを介し前記第１の広域ネットワーク経由のVPN(Virtual Private Network)で接続する第１のゲートウェイと、

第２の広域ネットワークに接続する第２のゲートウェイと、

前記第１のゲートウェイと前記第２のゲートウェイに接続された仮想ネットワークと、

前記第１のゲートウェイと前記第２のゲートウェイ間に設けられ、前記第１の広域ネットワーク側から入力されるパケット、及び、前記第２の広域ネットワーク側から入力されるパケットのうち少なくとも一方のパケットのフィルタリングを行う機能ブロックと、

を備えた、通信システム。

[請求項2] 前記データセンタにおいて、

前記仮想ネットワークが、パケットコアネットワークの機能の少なくとも一部を仮想化した仮想パケットコアネットワークを含む、請求項１記載の通信システム。

[請求項3] 前記データセンタにおいて、

前記機能ブロックが、

前記第１のゲートウェイと前記第２のゲートウェイ間に接続された第１の機能ブロックと、

前記仮想パケットコアネットワークに接続された第２の機能ブロックと、

のうち少なくとも一つを含む、請求項２記載の通信システム。

[請求項4] 前記データセンタにおいて、

前記機能ブロックが、

前記端末への着信やテキストメッセージのアクセス拒否、許可を制御する機能ブロックをさらに有する、請求項１乃至３のいずれか１項に記載の通信システム。

[請求項5] 前記データセンタにおいて、

前記機能ブロックが、

前記第２の広域ネットワーク側から入力されたパケット、及び、前記端末側から前記第１の広域ネットワークを介して入力されたパケットのうち少なくとも一方のパケットのペイロード部のデータの圧縮を制御する機能ブロックを、さらに備えた、請求項１乃至４のいずれか１項に記載の通信システム。

[請求項6] 前記データセンタにおいて、

前記機能ブロックが、

前記端末に対応させて設けられ、前記端末毎に、前記端末に対するパケットのフィルタリング、及び／又は、前記端末への着信やメッセージのアクセスの拒否、許可が設定される機能ブロックを有する、請求項１乃至４のいずれか１項に記載の通信システム。

[請求項7] 前記端末に対して前記無線LANを介して提供される音声通話又はテキストメッセージのサービスにおいて、

前記端末は、前記VPNから前記データセンタの前記仮想パケットコアネットワーク、前記第２の広域ネットワークを介して接続先と通信し、

前記第２の広域ネットワーク側からの前記端末への着呼又はメッセージのうち、前記データセンタの前記仮想パケットコアネットワークに接続された前記第２の機能ブロックで許可された着呼又はメッセージが、前記VPNを介して、前記端末に送信される、請求項３記載の通信システム。

[請求項8] 前記端末に対して前記無線LANを介して提供されるデータ通信サー

ビスにおいて、

前記端末は、前記VPNから前記データセンタの前記仮想ネットワークを介して前記第２の広域ネットワークに接続し、

前記第２の広域ネットワーク側からの前記端末へのデータは、前記データセンタの前記第１のゲートウェイと前記第２のゲートウェイ間に接続された前記第１の機能ブロックでフィルタリングされ、許可されたパケットが前記VPNを介して、前記端末に送信される、請求項３又は７記載の通信システム。

[請求項9] 一つの無線LANアクセスポイントに接続する第１乃至第Ｎ（Ｎは２以上の整数）の端末と、前記データセンタの前記第１のゲートウェイ間を第１乃至第ＮのVPNで接続し、

前記データセンタにおいて、

前記機能ブロックが、

前記第１のゲートウェイで終端される前記第１乃至第ＮのVPNにそれぞれ接続される第１乃至第Ｎの機能ブロックを備え、さらに、

前記第１乃至第Ｎの機能ブロックに一端で接続され、前記第２のゲートウェイに他端が接続された第Ｎ＋１の機能ブロックを備え、

前記第１乃至第Ｎの機能ブロックの設定は、前記第１乃至第Ｎの端末のユーザ側から行われ、

前記第Ｎ＋１の機能ブロックの設定は、前記データセンタ側で行われる、請求項１又は２記載の通信システム。

[請求項10] 前記データセンタにおいて、

前記第１のゲートウェイは、端末単位又は前記端末のユーザ単位に、前記端末との間の前記VPNを管理する、請求項１乃至９のいずれか１項に記載の通信システム。

[請求項11] 端末が接続する無線LAN（Local Area Network）との間に第１の広域ネットワーク（Wide Area Network）が介在する通信装置であって、

前記端末との間を、前記無線LANを介し前記第１の広域ネットワーク経由のVPN(Virtual Private Network)で接続する第１のゲートウェイと、

第２の広域ネットワークに接続する第２のゲートウェイと、

前記第１のゲートウェイと前記第２のゲートウェイに接続された仮想ネットワークと、

前記第１のゲートウェイと前記第２のゲートウェイ間に設けられ、前記第１の広域ネットワーク側から入力されるパケット、及び、前記第２の広域ネットワーク側から入力されるパケットのうちの少なくとも一方のパケットのフィルタリング制御を行う機能ブロックと、

を備えた、通信装置。

[請求項12] 前記仮想ネットワークが、パケットコアネットワークの機能の少なくとも一部を仮想化した仮想パケットコアネットワークを含む、請求項１１記載の通信装置。

[請求項13] 前記機能ブロックが、

前記第１のゲートウェイと前記第２のゲートウェイ間に接続された第１の機能ブロックと、

前記仮想パケットコアネットワークに接続された第２の機能ブロックと、

のうち少なくとも一つを含む、請求項１２記載の通信装置。

[請求項14] 前記機能ブロックが、

前記端末への着信やテキストメッセージのアクセス拒否、許可を制御する機能ブロックを含む、請求項１１乃至１３のいずれか１項に記載の通信装置。

[請求項15] 前記データセンタにおいて、

前記機能ブロックが、

前記第２の広域ネットワーク側から入力されたパケット、及び、前記端末側から前記第１の広域ネットワークを介して入力されたパケッ

トのうち少なくとも一方のパケットのペイロード部のデータの圧縮を制御する機能ブロックを、さらに備えた、請求項１１乃至１３のいずれか１項に記載の通信装置。

[請求項16] 前記機能ブロックが、

前記端末に対応させて設けられ、前記端末毎に、前記端末に対するパケットのフィルタリング、及び／又は、前記端末への着信やメッセージのアクセスの拒否、許可が設定される機能ブロックを有する、請求項１１乃至１５のいずれか１項に記載の通信装置。

[請求項17] 前記端末に対して前記無線LANを介して提供される音声通話又はテキストメッセージのサービスにおいて、

前記端末は、前記VPNから前記通信装置の前記仮想パケットコアネットワーク、前記第２の広域ネットワークを介して接続先と通信し、

前記第２の広域ネットワーク側からの前記端末への着呼又はメッセージのうち、前記通信装置の前記仮想パケットコアネットワークに接続された前記第２の機能ブロックで許可された着呼又はメッセージが、前記VPNを介して、前記端末に送信される、請求項１３記載の通信装置。

[請求項18] 前記端末に対して前記無線LANを介して提供されるデータ通信サービスにおいて、

前記端末は、前記VPNから前記データセンタの前記仮想ネットワークを介して前記第２の広域ネットワークに接続し、

前記第２の広域ネットワーク側からの前記端末へのデータは、前記通信装置の前記第１のゲートウェイと前記第２のゲートウェイ間に接続された前記第１の機能ブロックでフィルタリングされ、許可されたパケットが前記VPNを介して、前記端末に送信される、請求項１３又は１７記載の通信装置。

[請求項19] 一つの無線LANアクセスポイントに接続する第１乃至第Ｎ（Ｎは２以上の整数）の端末と、前記通信装置の前記第１のゲートウェイ間を

第１乃至第ＮのVPNで接続し、

前記機能ブロックが、

前記第１のゲートウェイで終端される前記第１乃至第ＮのVPNにそれぞれ接続される第１乃至第Ｎの機能ブロックを備え、さらに、

前記第１乃至第Ｎの機能ブロックに一端で接続され、前記第２のゲートウェイに他端が接続された第Ｎ＋１の機能ブロックを備え、

前記第１乃至第Ｎの機能ブロックの設定は、前記第１乃至第Ｎの端末のユーザ側から行われ、

前記第Ｎ＋１の機能ブロックの設定は、前記通信装置側で行われる、請求項１１又は１２記載の通信装置。

[請求項20] 前記第１のゲートウェイは、端末単位又は前記端末のユーザ単位に、前記端末との間の前記VPNを管理する、請求項１１乃至１９のいずれか１項に記載の通信装置。

[請求項21] 端末が接続する無線LAN（Local Area Network）との間に第１の広域ネットワーク（Wide Area Network）が介在するデータセンタの第１のゲートウェイと前記端末との間を、前記無線LANを介し前記広域ネットワーク経由のVPN(Virtual Private Network)で接続し、

前記端末から前記VPNを介して、前記データセンタに設けられた、仮想ネットワークから第２のゲートウェイを介して第２の広域ネットワークに接続し、

前記第１のゲートウェイと前記第２のゲートウェイ間に設けられた機能ブロックにて、前記第１の広域ネットワーク側から入力されるパケット、及び、前記第２の広域ネットワーク側から入力されるパケットのうちの少なくとも一方のパケットのフィルタリングを行う、通信方法。

[請求項22] 前記データセンタにおいて、

前記仮想ネットワークが、パケットコアネットワークの機能の少なくとも一部を仮想化した仮想パケットコアネットワークを含む、請求

項２１記載の通信方法。

[請求項23] 前記データセンタは、前記第２の広域ネットワーク側から入力されたパケットと、前記端末側から入力されたパケットのうち、少なくとも一方のパケットのペイロード部のデータの圧縮を制御する、請求項２１又は２２記載の通信方法。

[請求項24] 前記データセンタにおいて、前記機能ブロックは、前記端末に対応させて設けられ、前記端末毎に、前記端末に対するパケットのフィルタリング、及び／又は、前記端末への着信やメッセージのアクセスの拒否、許可が設定される、請求項２１乃至２３のいずれか１項に記載の通信方法。

[請求項25] 無線LAN（Local Area Network）と第１の広域ネットワーク（Wide Area Network）とを介してデータセンタに接続する端末であって、

前記データセンタとの間を、前記無線LAN及び前記広域ネットワーク経由のVPN(Virtual Private Network)で接続するVPN装置を備え、

前記VPNを介して、前記データセンタに設けられており、パケットコアネットワークの機能の少なくとも一部を仮想化した仮想ネットワークを介して第２の広域ネットワークに接続し、

前記第２の広域ネットワーク側から前記データセンタ内に入力された前記端末への着呼又は前記端末宛てのデータのうち、前記データセンタ内の機能ブロックでフィルタリングされた着呼又はデータを、前記VPNを介して、受信する機能を備えた、端末。

[請求項26] 前記データセンタ内の前記機能ブロックにおけるフィルタリングの設定を行う機能を備えた請求項２５記載の端末。

[請求項27] 端末が接続する無線LAN（Local Area Network）との間に第１の広域ネットワーク（Wide Area Network）が介在するデータセンタに配置されるコンピュータに、

前記端末と前記データセンタとの間に、前記無線LANを介し前記広域ネットワーク経由のVPN(Virtual Private Network)を開設する処理

と、

前記端末から前記VPNを介して、前記データセンタに設けられており、コアネットワークの構成要素の少なくとも一部を仮想化した仮想ネットワークを介して第２の広域ネットワークに接続する処理と、

前記第１の広域ネットワーク側から入力されるパケット、及び、前記第２の広域ネットワーク側から入力されるパケットのうちの少なくとも一方のパケットのフィルタリングを行う処理と、

を実行させるプログラム。

[請求項28] 無線LAN（Local Area Network）と第１の広域ネットワーク（Wide Area Network）を介してデータセンタに接続する端末に含まれるコンピュータに、

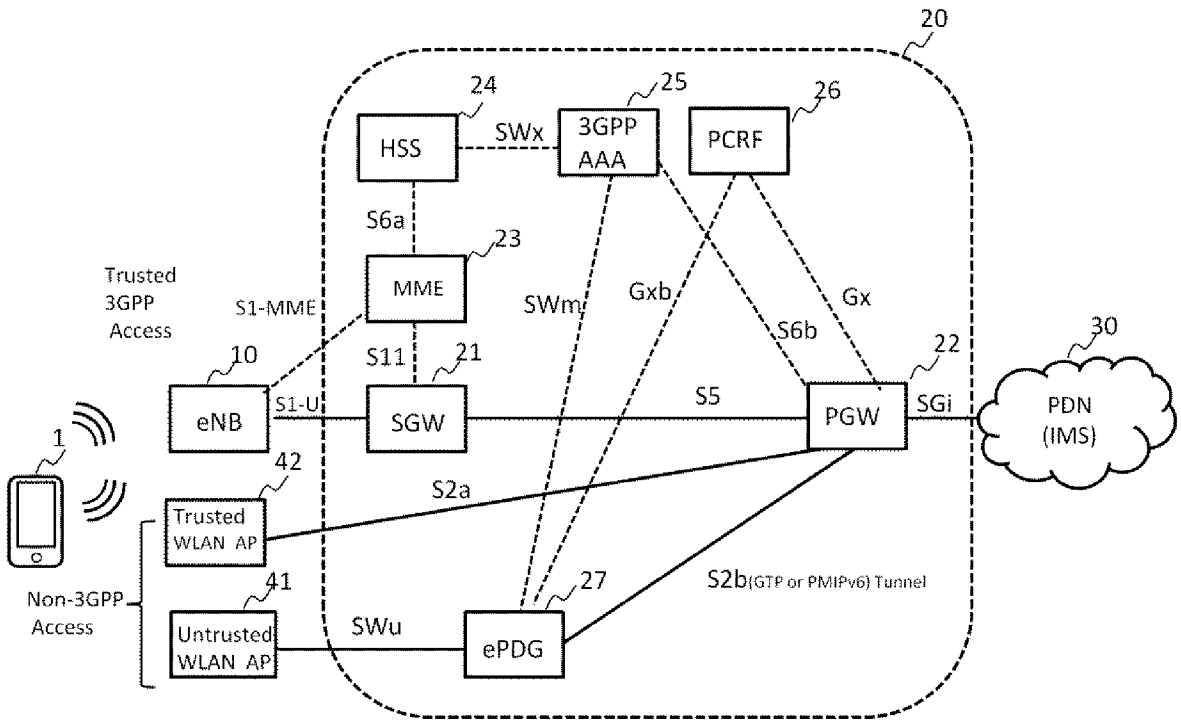
前記データセンタと前記端末との間に、前記無線LANを介し前記広域ネットワーク経由のVPN(Virtual Private Network)を開設する処理と、

前記VPNを介して、前記データセンタに設けられており、パケットコアネットワークの機能の少なくとも一部を仮想化した仮想ネットワークを介して第２の広域ネットワークに接続する処理と、

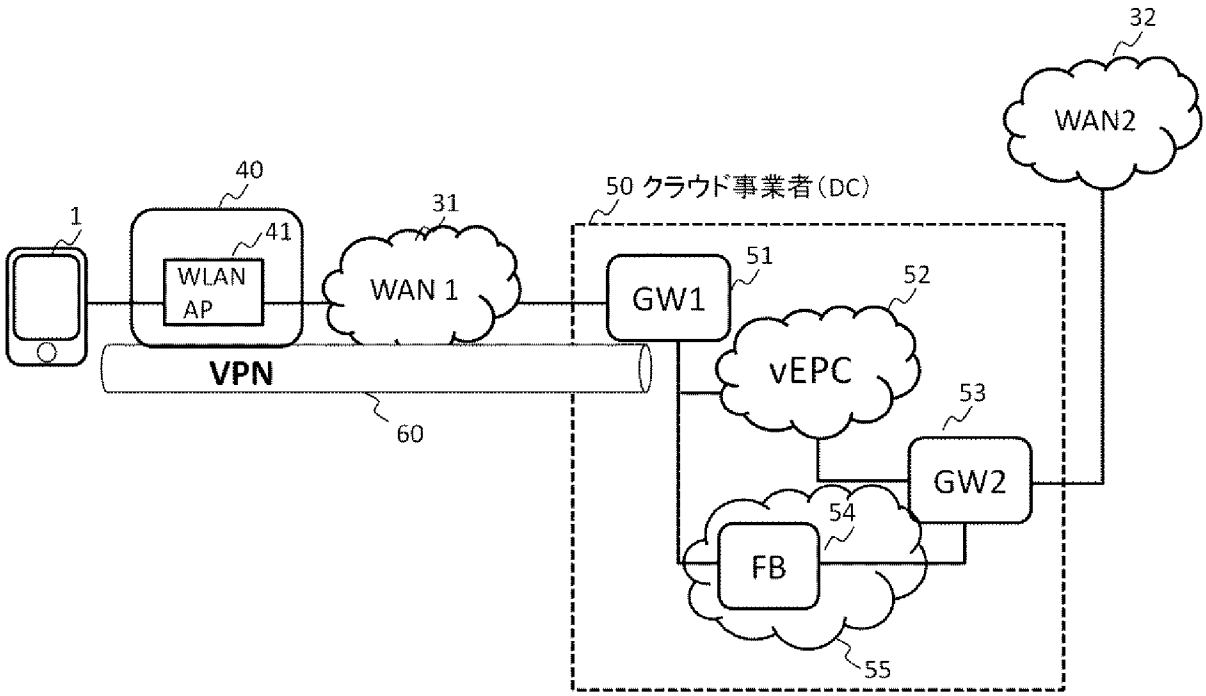
前記第２の広域ネットワーク側から前記データセンタ内に入力された前記端末への着呼又は前記端末宛てのデータのうち、前記データセンタ内でフィルタリングされた着呼又はデータを、前記VPNを介して、受信する処理と、

を実行させるプログラム。

[図1]

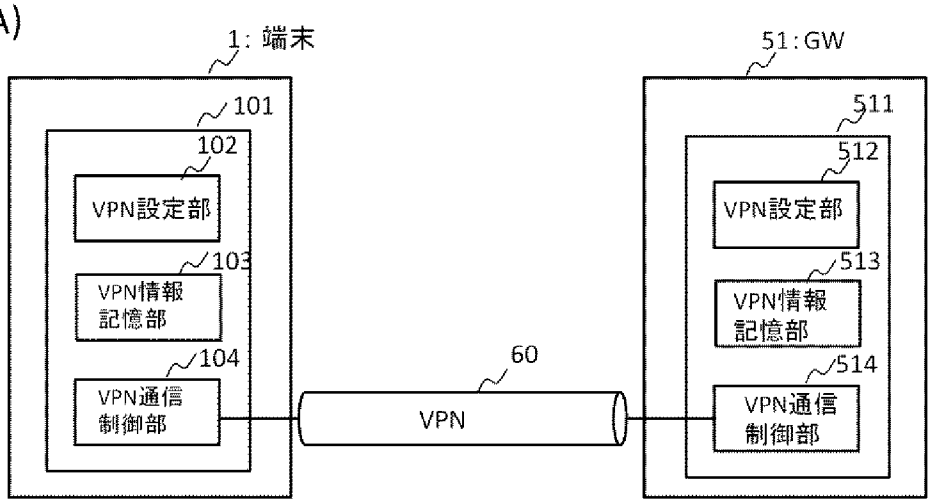

20
24
25
26
HSS
SWx
3GPP AAA
PCRF
S6a
23
MME
Trusted 3GPP Access
S1-MME
SWm
Gxb
Gx
S6b
10
S11
21
22
30
eNB
S1-U
SGW
S5
PGW
SGi
PDN (IMS)
1
42
S2a
Trusted WLAN AP
41
27
S2b(GTP or PMIPv6) Tunnel
Non-3GPP Access
SWu
Untrusted WLAN AP
ePDG

[図2]


32
WAN2
40
50 クラウド事業者(DC)
1
41
31
WLAN
AP
WAN 1
GW1
51
52
vEPC
VPN
60
53
GW2
54
FB
55

[図3]

(A)



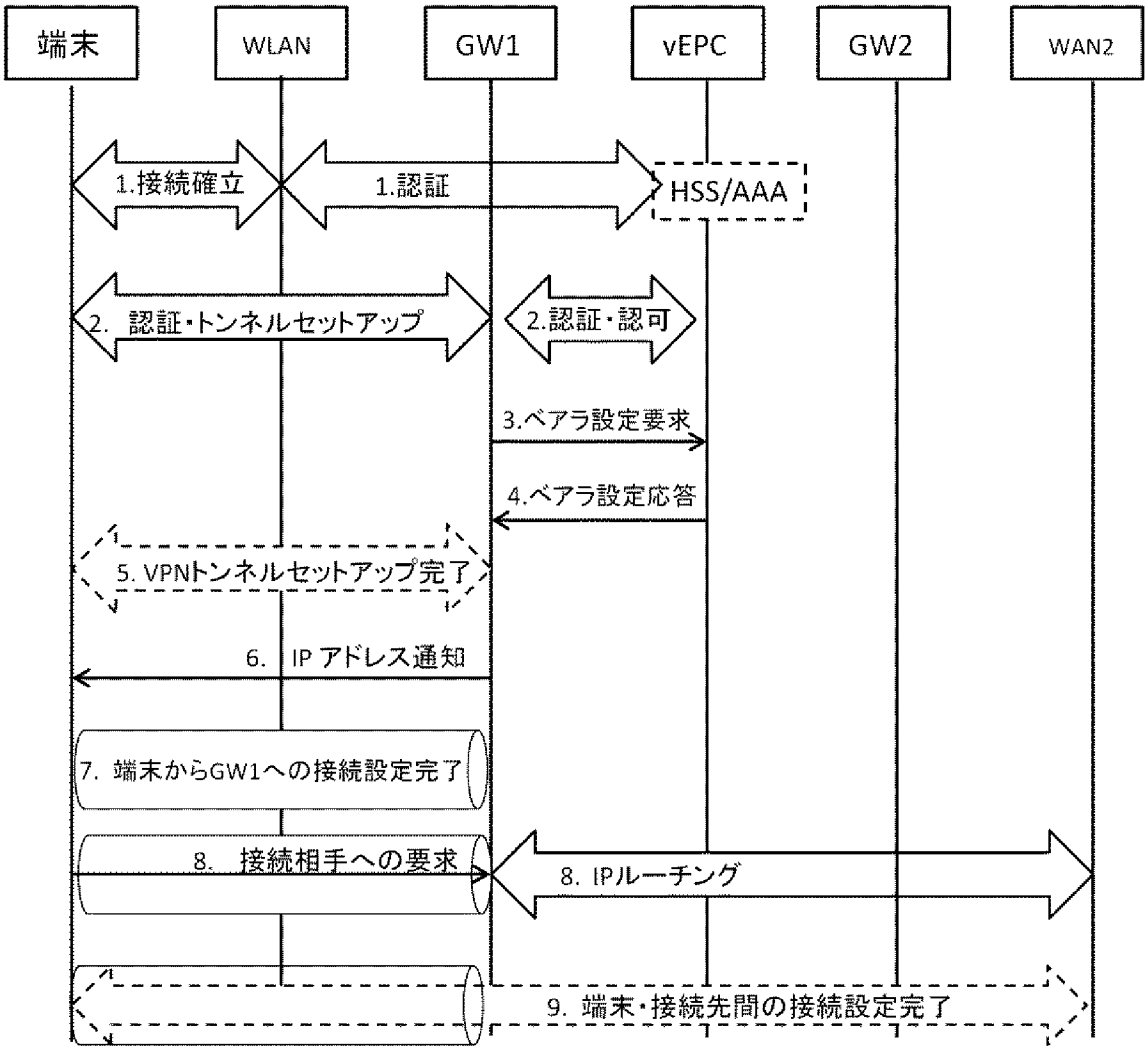
(B)

VPN識別子	接続相手アドレス	端末ID/名前	事前共通鍵	装置アドレス	認証アルゴリズム	暗号アルゴリズム	接続ネットワーク	NATトラバーサル	・・・
VPN1	100.1.100.1	smart1	secret1	100.1.1.1	SHA-1	AES	100.1.100.1/32	有	
VPN2	100.1.100.2	smart2	secret2	100.1.1.1	SHA-1	DES	100.1.100.2/32	有	
VPN3	100.1.100.3	smart3	secret3	100.1.1.1	SHA-1	3DES	100.1.100.3/32	有	
⋮									

(C)

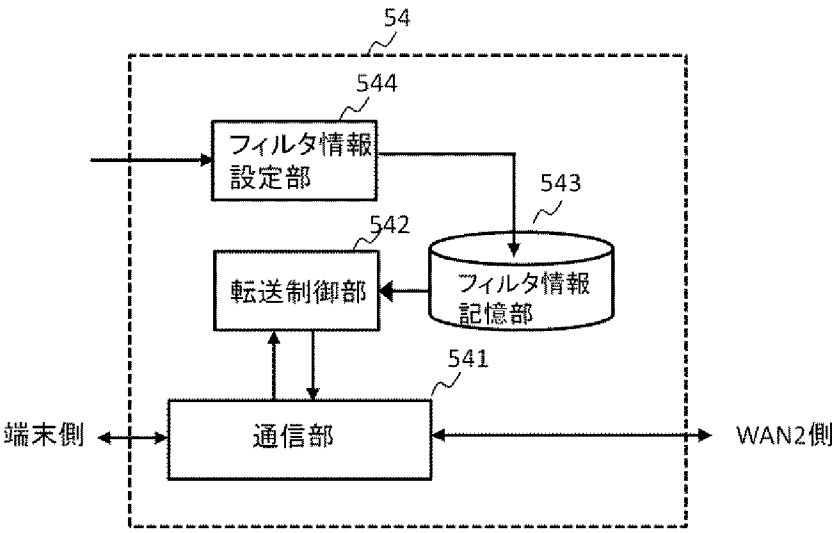
VPN識別子	接続先GWアドレス	接続先GW名前	事前共通鍵	クライアントアドレス	認証アルゴリズム	暗号アルゴリズム	接続ネットワーク	NATトラバーサル	・・・
VPN1	100.1.1.1	example.dc.com	secret1	100.1.100.1	SHA-1	DES	100.1.1.0/24	有	

[図4]


端末
WLAN
GW1
vEPC
GW2
WAN2
1.接続確立
1.認証
HSS/AAA
2. 認証・トンネルセットアップ
2.認証・認可
3.ベアラ設定要求
4.ベアラ設定応答
5. VPNトンネルセットアップ完了
6. IP アドレス通知
7. 端末からGW1への接続設定完了
8. 接続相手への要求
8. IPルーチング
9. 端末・接続先間の接続設定完了

[図5]

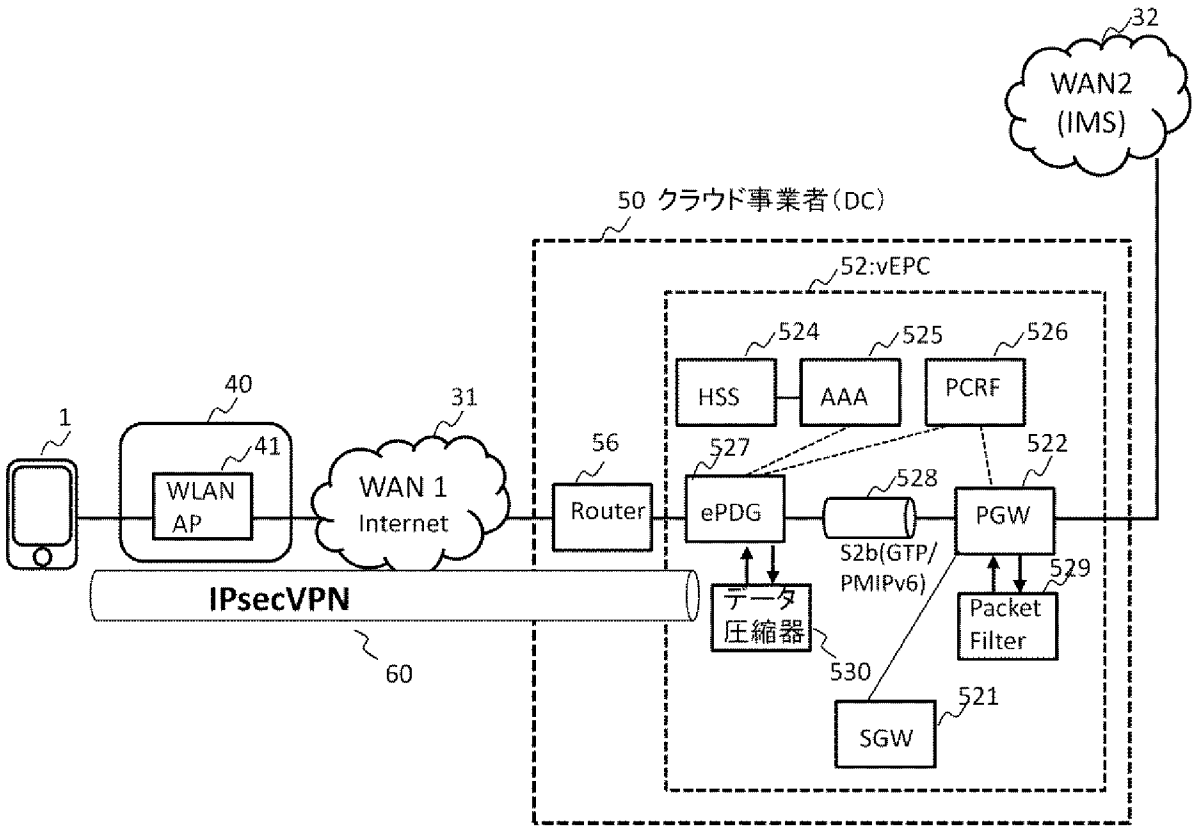
(A)



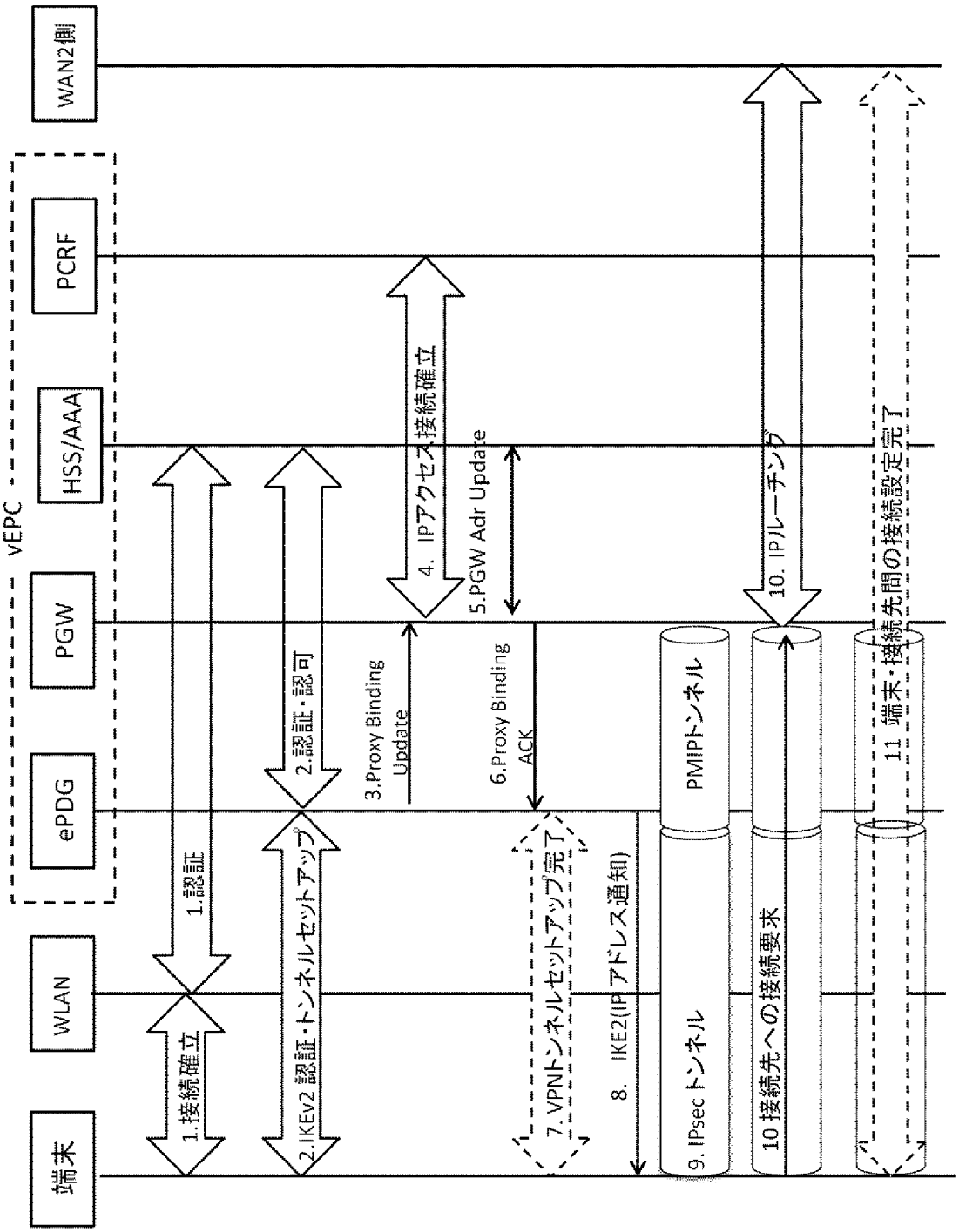
(B)

フィルタID	種別	方向	プロトコル	送信元アドレス	送信ポート	宛先アドレス	宛先ポート
1	廃棄	DOWN	TCP/UDP	*	23	GW1	*
2	廃棄	DOWN	UDP	xxx.*	*	端末1のプライベートIPアドレス	*
3	廃棄	UP	TCP/UDP	端末1のプライベートIPアドレス	*	YYY	*
⋮							

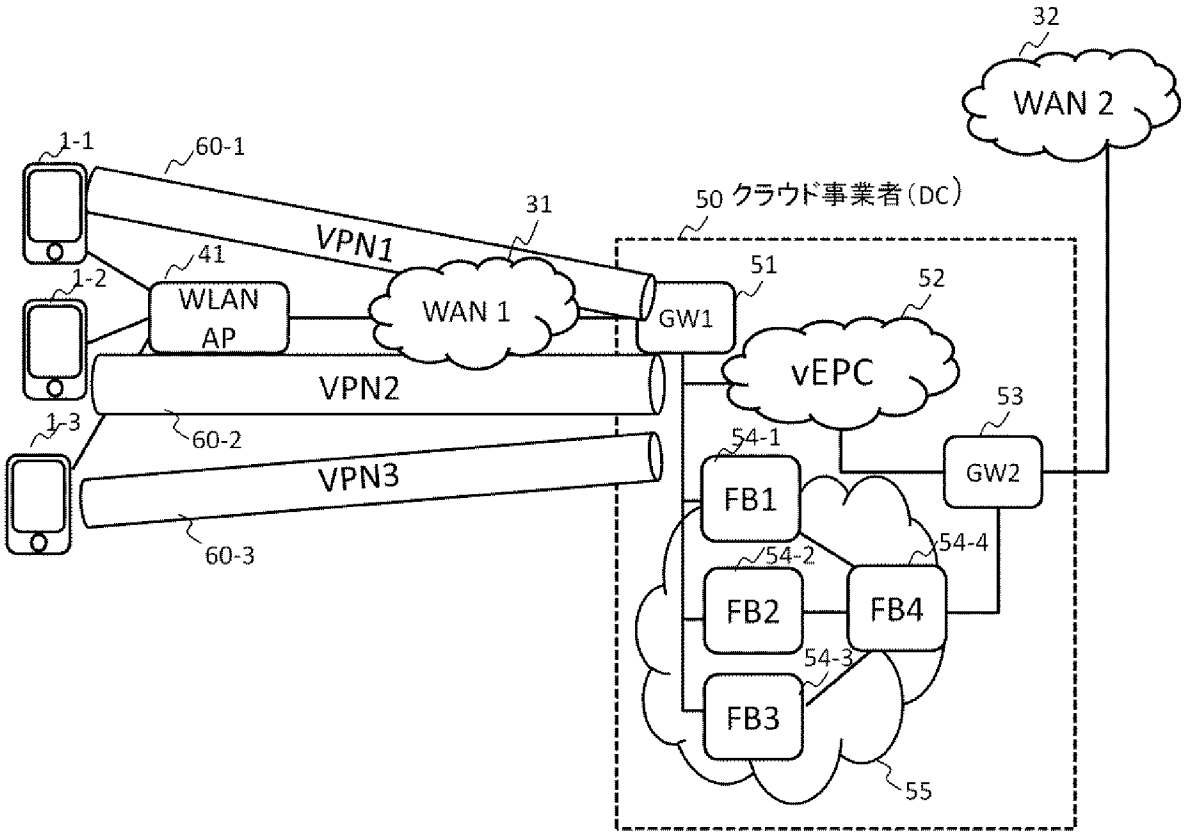
[図6]


32
WAN2
(IMS)
50 クラウド事業者(DC)
52:vEPC
524
525
526
HSS
AAA
PCRF
40
31
1
41
56
527
522
528
WLAN
AP
WAN 1
Internet
Router
ePDG
PGW
S2b(GTP/
PMIPv6)
529
IPsecVPN
データ
圧縮器
Packet
Filter
530
521
SGW
60

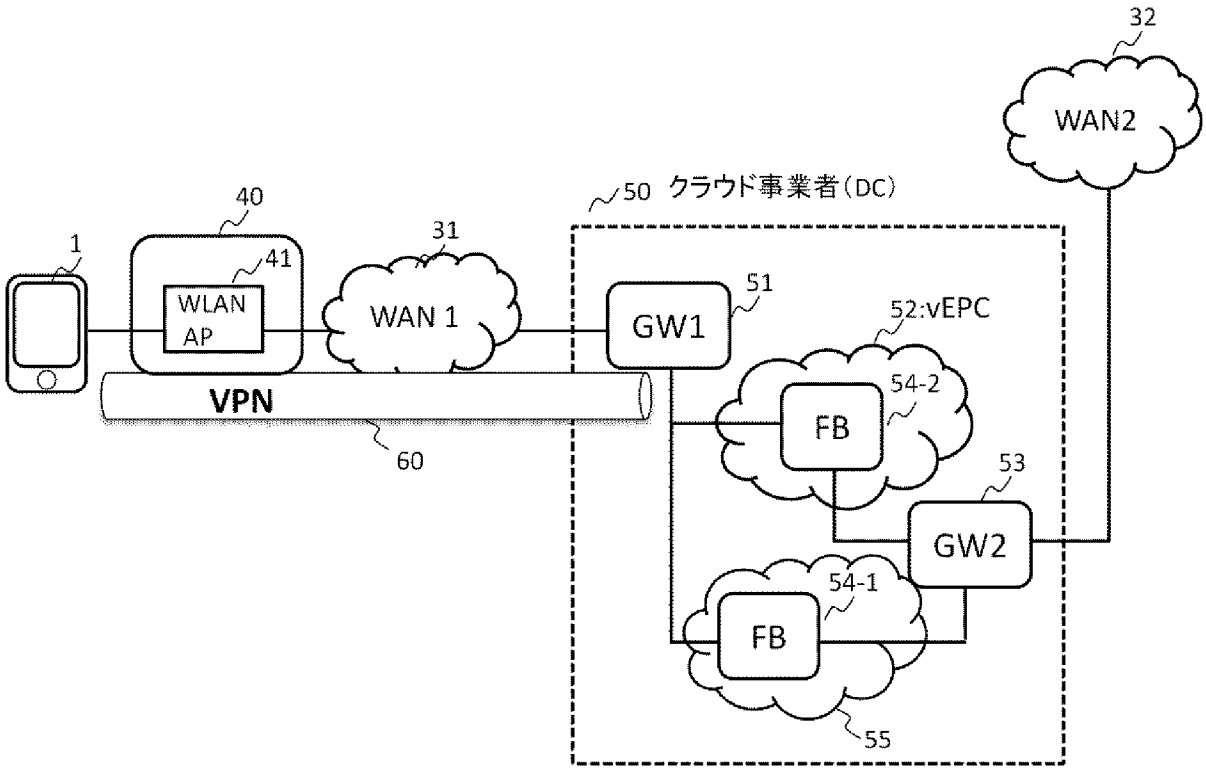
[図7]


端末
WLAN
ePDG
PGW
HSS/AAA
PCRF
WAN2側
vEPC
1.接続確立
1.認証
2.IKEv2 認証・トンネルセットアップ
2.認証・認可
3.Proxy Binding Update
4. IPアクセス接続確立
5.PGW Adr Update
6.Proxy Binding ACK
7.VPNトンネルセットアップ完了
8. IKE2(IPアドレス通知)
9. IPsecトンネル
PMIPトンネル
10 接続先への接続要求
10. IPルーチング
11 端末・接続先間の接続設定完了

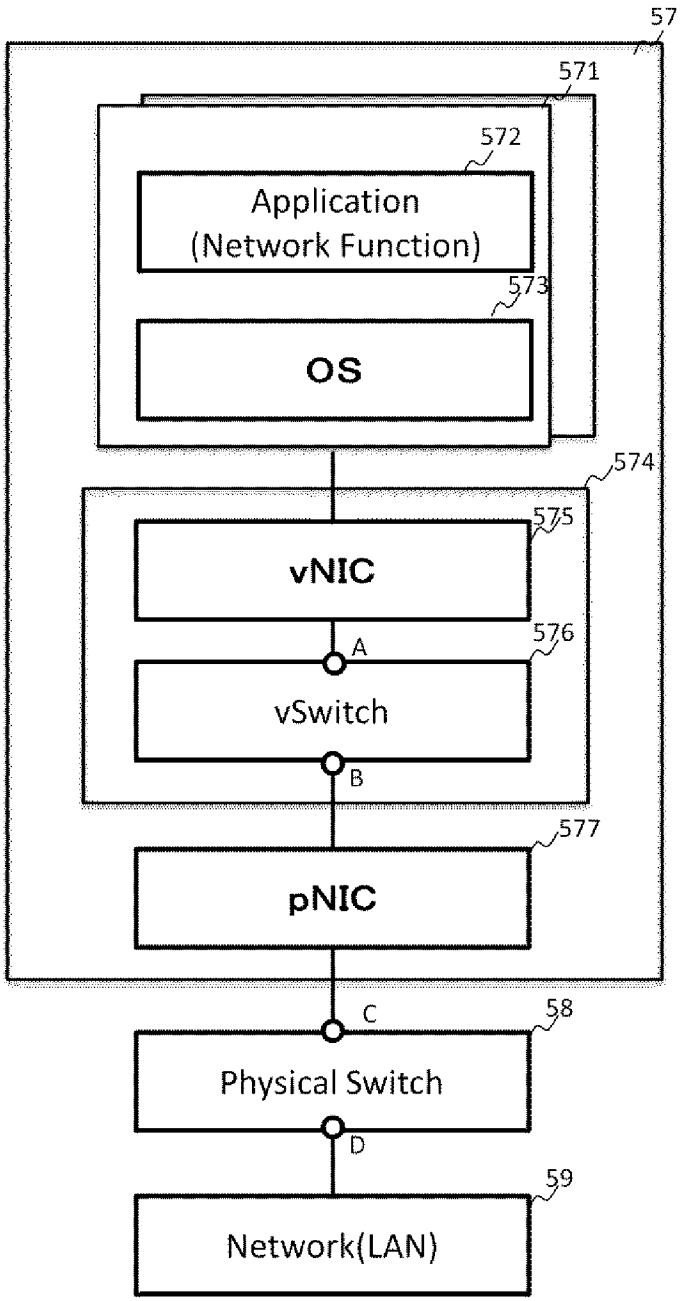
[図8]


32
WAN 2
1-1
60-1
VPN1
31
50 クラウド事業者（DC）
41
1-2
WLAN
AP
WAN 1
GW1
51
52
vEPC
VPN2
53
1-3
60-2
54-1
VPN3
GW2
FB1
60-3
54-2
54-4
FB2
FB4
54-3
FB3
55

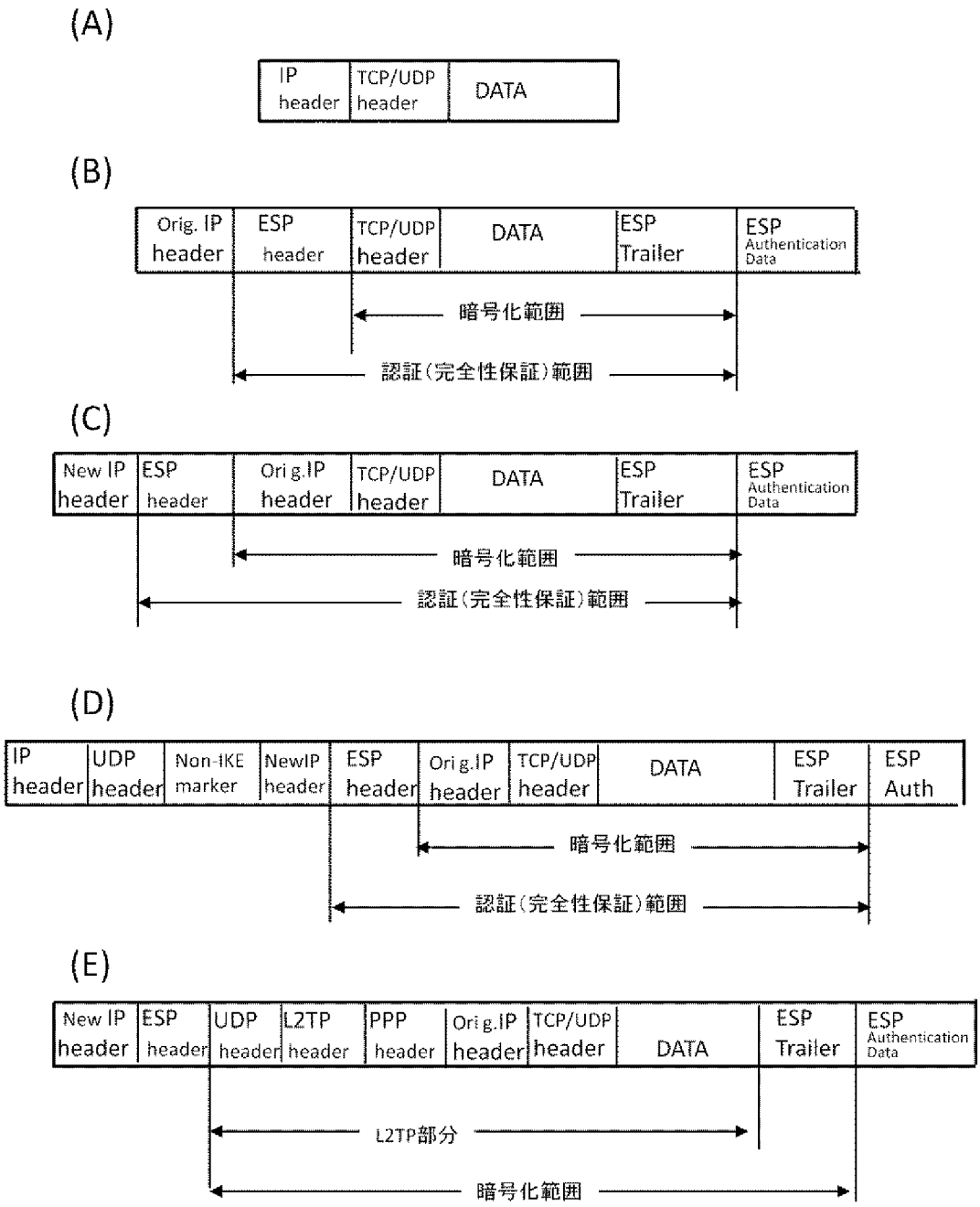
[図9]


32
WAN2
50 クラウド事業者(DC)
40
1
41
31
WLAN
AP
WAN 1
GW1
51
52:vEPC
54-2
FB
VPN
60
53
GW2
54-1
FB
55

[図10]


57
571
572
Application
(Network Function)
573
OS
574
575
vNIC
576
A
vSwitch
B
577
pNIC
C
58
Physical Switch
D
59
Network(LAN)

[図11]


(A)
IP header
TCP/UDP header
DATA
(B)
Orig. IP header
ESP header
TCP/UDP header
DATA
ESP Trailer
ESP Authentication Data
暗号化範囲
認証(完全性保証)範囲
(C)
New IP header
ESP header
Orig.IP header
TCP/UDP header
DATA
ESP Trailer
ESP Authentication Data
暗号化範囲
認証(完全性保証)範囲
(D)
IP header
UDP header
Non-IKE marker
NewIP header
ESP header
Orig.IP header
TCP/UDP header
DATA
ESP Trailer
ESP Auth
暗号化範囲
認証(完全性保証)範囲
(E)
New IP header
ESP header
UDP header
L2TP header
PPP header
Orig.IP header
TCP/UDP header
DATA
ESP Trailer
ESP Authentication Data
L2TP部分
暗号化範囲

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/070907

A. CLASSIFICATION OF SUBJECT MATTER
H04L12/66(2006.01)i, *H04L12/70*(2013.01)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)
H04L12/66, H04L12/70

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	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

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.
A	JP 2006-33443 A (NEC Fielding Ltd.), 02 February 2006 (02.02.2006), entire text; all drawings (Family: none)	1-28
A	JP 2004-135248 A (Fujitsu Ltd.), 30 April 2004 (30.04.2004), entire text; all drawings & US 2004/0037260 A1 entire text; all drawings & EP 1396964 A2	1-28
A	JP 2010-231396 A (OKI Networks Co., Ltd.), 14 October 2010 (14.10.2010), entire text; all drawings (Family: none)	1-28

☐ 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
15 September 2016 (15.09.16)	27 September 2016 (27.09.16)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１６／０７０９０７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/66(2006.01)i, H04L12/70(2013.01)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.　H04L12/66, H04L12/70

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	１９７１－２０１６年
日本国実用新案登録公報	１９９６－２０１６年
日本国登録実用新案公報	１９９４－２０１６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	関連する請求項の番号
Ａ	JP 2006-33443 A（ＮＥＣフィールディング株式会社）2006.02.02, 全文、全図（ファミリーなし）	１－２８
Ａ	JP 2004-135248 A（富士通株式会社）2004.04.30, 全文、全図 & US 2004/0037260 A1 全文,全図 & EP 1396964 A2	１－２８
Ａ	JP 2010-231396 A（株式会社ＯＫＩネットワークス）2010.10.14, 全文、全図（ファミリーなし）	１－２８

☐　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	国際調査報告の発送日
１５．０９．２０１６	２７．０９．２０１６

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）　５Ｘ　８５２３
宮島　郁美
電話番号　０３－３５８１－１１０１　内線　３５９６