

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2020-99097

(P2020-99097A)

(43) 公開日 令和2年6月25日 (2020.6.25)

(51) Int.Cl.	F I	テーマコード (参考)
H04W 4/50 (2018.01)	H04W 4/50	5K067
H04W 4/24 (2009.01)	H04W 4/24	5K201
H04W 84/12 (2009.01)	H04W 84/12	
H04W 48/18 (2009.01)	H04W 48/18 113	
H04M 3/00 (2006.01)	H04M 3/00 C	

審査請求 有 請求項の数 14 O L (全 34 頁)

(21) 出願番号	特願2020-36059 (P2020-36059)	(71) 出願人	000004237
(22) 出願日	令和2年3月3日 (2020.3.3)		日本電気株式会社
(62) 分割の表示	特願2017-533105 (P2017-533105) の分割	(74) 代理人	100080816
原出願日	平成28年8月3日 (2016.8.3)		弁理士 加藤 朝道
(31) 優先権主張番号	特願2015-154492 (P2015-154492)	(74) 代理人	100098648
(32) 優先日	平成27年8月4日 (2015.8.4)		弁理士 内田 深人
(33) 優先権主張国・地域又は機関	日本国 (JP)	(72) 発明者	石井 理
			東京都港区芝五丁目7番1号 日本電気株 式会社内
		(72) 発明者	長谷川 英男
			東京都港区芝五丁目7番1号 日本電気株 式会社内

最終頁に続く

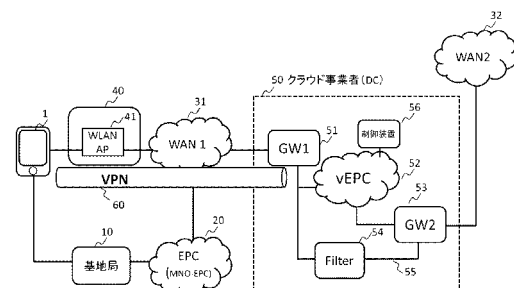
(54) 【発明の名称】 通信システム、通信装置、通信方法、端末、プログラム

(57) 【要約】 (修正有)

【課題】 端末の接続先のネットワークに応じた通信サービスを提供可能とするシステム、装置、方法を提供する。

【解決手段】 基地局に接続されたコアネットワークと、無線LANとに第1の広域ネットワークを介して接続するデータセンタは、無線LAN又は基地局への接続が選択自在とされ、データセンタに接続する端末が、第1の広域ネットワークとの間で接続しているネットワークに応じて、データセンタの仮想コアネットワークでのサービスを可変に制御する。

【選択図】 図2



【特許請求の範囲】**【請求項 1】**

仮想通信事業者によって提供され、無線LAN (Local Area Network) または通信事業者が提供する無線アクセスネットワークに接続する端末からの通信を受信する仮想モバイルコアネットワークと、

前記仮想モバイルコアネットワークを制御する制御装置と、

を含み、

前記制御装置は、

前記端末が接続するネットワークの種別に応じて、前記端末からの通信に対して、前記仮想モバイルコアネットワークを介して前記仮想通信事業者が提供する通信サービスに関する制御を行う

ことを特徴とするデータセンタ。

【請求項 2】

前記制御装置は、

前記端末が接続するネットワークの種別に応じて、前記端末からの通信に対して、前記仮想モバイルコアネットワークを介して提供する前記通信サービスの通信品質に関する制御を行う

ことを特徴とする請求項 1 に記載のデータセンタ。

【請求項 3】

前記制御装置は、

前記端末が接続するネットワークが、予め定められた前記無線LANであることに応じて、前記通信品質の優先度を高くする

ことを特徴とする請求項 2 に記載のデータセンタ。

【請求項 4】

前記制御装置は、

前記端末が接続するネットワークが、前記無線アクセスネットワークであることに応じて、前記通信品質の優先度を低くする

ことを特徴とする請求項 2 または 3 に記載のデータセンタ。

【請求項 5】

前記制御装置は、

前記端末が接続するネットワークの種別に応じて、前記端末からの通信に対して、前記仮想モバイルコアネットワークを介して提供する前記通信サービスの課金に関する制御を行う

ことを特徴とする請求項 1 から 4 のいずれか 1 項に記載のデータセンタ。

【請求項 6】

前記制御装置は、

前記端末が接続するネットワークが、前記無線LANであることに応じて、前記通信サービスに対する課金を行わないように制御する

ことを特徴とする請求項 5 に記載のデータセンタ。

【請求項 7】

前記制御装置は、

前記端末が接続するネットワークが、前記無線アクセスネットワークであることに応じて、前記通信サービスに対する課金を行うように制御する

ことを特徴とする請求項 5 または 6 に記載のデータセンタ。

【請求項 8】

仮想通信事業者によって提供されるデータセンタにおいて、

無線LAN (Local Area Network) または通信事業者が提供する無線アクセスネットワークに接続する端末からの通信を、前記仮想通信事業者によって提供される仮想モバイルコアネットワークで受信し、

前記端末が接続するネットワークの種別に応じて、前記端末からの通信に対して、前記

10

20

30

40

50

仮想モバイルコアネットワークを介して前記仮想通信事業者が提供する通信サービスに関する制御を行う

ことを特徴とする通信方法。

【請求項 9】

前記端末が接続するネットワークの種別に応じて、前記端末からの通信に対して、前記仮想モバイルコアネットワークを介して提供する前記通信サービスの通信品質に関する制御を行う

ことを特徴とする請求項 8 に記載の通信方法。

【請求項 10】

前記端末が接続するネットワークが、予め定められた前記無線LANであることに応じて、前記通信品質の優先度を高くする

10

ことを特徴とする請求項 9 に記載の通信方法。

【請求項 11】

前記端末が接続するネットワークが、前記無線アクセスネットワークであることに応じて、前記通信品質の優先度を低くする

ことを特徴とする請求項 9 または 10 に記載の通信方法。

【請求項 12】

前記端末が接続するネットワークの種別に応じて、前記端末からの通信に対して、前記仮想モバイルコアネットワークを介して提供する前記通信サービスの課金に関する制御を行う

20

ことを特徴とする請求項 8 から 11 のいずれか 1 項に記載の通信方法。

【請求項 13】

前記端末が接続するネットワークが、前記無線LANであることに応じて、前記通信サービスに対する課金を行わないように制御する

ことを特徴とする請求項 12 に記載の通信方法。

【請求項 14】

前記端末が接続するネットワークが、前記無線アクセスネットワークであることに応じて、前記通信サービスに対する課金を行うように制御する

ことを特徴とする請求項 12 または 13 に記載の通信方法。

【発明の詳細な説明】

30

【技術分野】

【0001】

本発明は通信システム、通信装置、通信方法、端末、プログラムに関する。

【背景技術】

【0002】

(関連出願についての記載)

本発明は、日本国特許出願：特願 2015-154492 号（2015 年 8 月 4 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。

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。

40

【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.) 802.11x 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

50

Access)等の無線LAN (Wireless Local Area Network: WLAN) を含む。非 3 GPPアクセスについては、例えば3GPP TS23.402: Architecture enhancements for non-3GPP accesses等が参照される。

【0004】

Wi-Fi (登録商標) -Callingは、通信キャリア (オペレータ) によりWi-Fi (登録商標) ネットワーク上で提供されるVoIP (Voice over IP) サービスである。例えば、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) ネットワークを経由し、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、当該通信キャリアのコアネットワーク (Evolved Packet Core: EPC) の交換機に接続し、通信キャリアの電話番号による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)。また、端末がWi-Fi (登録商標) に接続しておりWi-Fi (登録商標) -Callingがオンであれば、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) ネットワーク経由で端末を呼び出す。

10

【0005】

図1は、非 3 GPP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、通信キャリアの基地局 (evolved NodeB: eNB) 10、EPC 20を介して、パケットデータネットワーク (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。

20

【0006】

EPC 20のMME (Mobility Management Entity) 23は、例えば端末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、MME 23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。MME 23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。SGW 21は、例えば基地局10との間でユーザデータの送受信を行い、PGW (PDN (Packet Data Network) Gateway) 22との間の通信経路の設定・解放を行う。

【0007】

PGW 22は、例えばIMS (Internet Multimedia Subsystem) やインターネット等のパケットデータネットワーク (PDN) 30と接続する。

30

【0008】

また、PGW 22は、例えば端末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、ユーザに対するパケットフィルタリング、課金サポート、合法的傍受及びパケットスクリーニング等を行う。

【0009】

PCRF (Policy and Charging Rules Function) 26は、例えばQoS (Quality of Service) 等のポリシー制御や課金制御ルールを決定する。PGW 22及びSGW 21は、PCRF 26からの通知情報に基づき、例えばパケット単位にポリシー制御を行う。

【0010】

PCRF 26とGxインタフェースで接続され、通信ネットワークにおけるポリシー及び課金実施機能ノードである不図示のPCEF (Policy and Charging Enforcement Function) は、例えばPGW 22に配置される。

40

【0011】

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。なお、EPCの詳細は、例えば3GPP TS 23.401: GPRS Enhancements for E-UTRAN Access等が参照される。

【0012】

PGW 22でのパケットフィルタに関して、端末 (UE) 1 は、例えばベアラリソース修正

50

手順 (UE requester bearer resource modification procedure) にて、PGW 2 2 が管理する EPS ベアラのトラフィックフローテンプレート (Traffic Flow Templates : TFT) を設定する。PGW 2 2 において、パケットフィルタは、例えばアップリンク (UL) 用とダウンリンク (DL) 用と区別して管理される。

【 0 0 1 3 】

端末 (UE) 1 の要求によるベアラ修正 (UE requested bearer resource modification) では、端末 1 は、例えばベアラリソース修正要求 (Request Bearer Resource Modification) を、基地局 (eNB) 1 0 を介して MME 2 3 に送信する。ベアラリソース修正要求には、例えば、PGW22 におけるパケットフィルタの追加、修正、削除等の要求 (TAD (Traffic Aggregate Description)) が含まれる。追加の場合、ベアラリソース修正要求には、追加されるパケットフィルタ情報が含まれる。MME23 は、SGW 2 1 を介して、ベアラリソースコマンドを PGW 2 2 に送信し、PGW 2 2 では、例えば PCRF 2 6 と相互作用して PCC (Policy and Charging Control) を決定する (PCEF Initiated IP-CAN (IP Connectivity Access Network) Session Modification) (例えば 3GPP TS 23.203 : Policy and charging control architecture 等が参照される)。

【 0 0 1 4 】

PGW 2 2 は、例えば当該 TAD の内容や当該 TAD に含まれるパケットフィルタ情報に関連した GBR (Guaranteed Bit Rate) 変更を PCRF 2 6 に提供する。要求が受理されると、PGW 2 2 は、TAD に対応した EPS ベアラの TFT において、1 つ又は複数のパケットフィルタの挿入、修正、削除を行う。

【 0 0 1 5 】

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 4 1 経由で、Un-Trusted Access (信頼できないアクセス) として、通信キャリアの ePDG (evolved Packet Data Gateway) 2 7 経由で PGW 2 2 に接続され、PDN 3 0 (例えば IMS サービス) に接続される。

【 0 0 1 6 】

ePDG 2 7 は、モバイルインタフェース (Swt) 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 ePDG 2 7 を検出し、ePDG 2 7 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、PGW 2 2 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。ePDG 2 7 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 2 5 に中継し、3GPP AAA サーバ 2 5 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 等が参照される)。

【 0 0 1 7 】

ePDG 2 7 は、S2b インタフェースにおいて PGW 2 2 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 等参照が参照される)。

【 0 0 1 8 】

非 3GPP アクセスが PMIPv6 (Proxy Mobile IPv6) に対応している場合、PGW 2 2 に PMIPv6 を介して接続できる。PGW 2 2 と ePDG 2 7 間でプロキシモバイル IP を使用する場合、端末 1 と ePDG 2 7 との間で IPsec トンネルが確立されると、ePDG 2 7 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、PGW 2 2 において端末 1 へのデータの送信先は ePDG 2 7 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 参照)。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 から別の 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。

【0019】

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、及びアカウントリ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、HSS 24 間で行われる。例えば端末 1 が ePDG 27 との間で IPsec トンネルを確立すると、例えば 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。

【0020】

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 参照) を介して、直接、PGW 22 に接続する。なお、ePDG、3GPP AAA サーバについては、例えば 3GPP TS 29.273: Evolved Packet System (EPS); 3GPP EPS AAA interfaces 等が参照される。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、例えば加入者が登録されている 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。

【0021】

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 参照)。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 13 (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 13 (A)) は暗号化され、新たな IP ヘッダ (New IP header) が追加される (図 13 (C) 参照)。

【0022】

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 13 (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 (Transmission Control Protocol)/UDP (User Datagram Protocol)) 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。

【0023】

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。

【0024】

IKE(Internet Key Exchange)は、SA設定のための鍵交換プロトコルである（例えばIETF RFC 4306参照）。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（例えばIETF RFC 4306参照）。

【0025】

近時、通信事業の形態として、無線通信設備やコアネットワーク等の通信インフラを保有する通信事業者（キャリア）であるMNO(Mobile Network Operator)から必要なインフラを借り受け、通信サービスを提供するMVNO (Mobile Virtual Network Operator) が広ま

10

っている。本明細書では、MVNOの通信事業者をMVNOキャリアという。MVNOキャリアに契約した端末は、例えばSIM (Subscriber Identity Module) フリー端末からなる。なお、本明細書では、MNOをMNOキャリアともいう。

【先行技術文献】

【非特許文献】

【0026】

【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】

20

【発明が解決しようとする課題】

【0027】

データセンタ等において、端末の接続先アクセスネットワークの種別（例えば非3GPPアクセスネットワーク、3GPPアクセスネットワーク）等に対応した通信サービスを提供するための機構が望まれる。

【0028】

したがって、本発明は、上記課題に鑑みて創案されたものであって、その目的の一つは端末の接続先のネットワークに応じた通信サービス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】

30

【0029】

本発明の1つの側面によれば、基地局に接続されたコアネットワークと、無線LANとに第1の広域ネットワーク(WAN1)を介して接続するデータセンタを備え、前記データセンタが、コアネットワークの機能の少なくとも一部を仮想化し、前記第1の広域ネットワークに接続される仮想コアネットワークと、

前記無線LAN又は前記基地局への接続が選択自在とされ、前記データセンタに接続する端末が前記第1の広域ネットワークとの間で接続しているネットワークに応じて、前記仮想コアネットワークでのサービスを可変に制御する制御装置と、を備えた、通信システムが提供される。

【0030】

40

本発明の他の側面によれば、基地局に接続されたコアネットワークと、無線LANとに第1の広域ネットワーク(WAN1)を介して接続する装置（手段）と、

コアネットワークの機能の少なくとも一部を仮想化し、前記第1の広域ネットワークに接続される仮想コアネットワークと、

前記無線LAN又は前記基地局への接続が選択自在とされ、前記通信装置に接続する端末が、前記第1の広域ネットワークとの間で接続しているネットワークに応じて、前記仮想コアネットワークでのサービスを可変に制御する制御装置と、を備えた、通信装置が提供される。

【0031】

本発明の他の側面によれば、基地局に接続されたコアネットワークと、無線LANとに第

50

1の広域ネットワーク(WAN1)を介して接続するデータセンタでは、前記第1の広域ネットワークに接続され、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コアネットワークを有し、前記無線LAN又は前記基地局への接続が選択自在とされ、前記データセンタに接続する端末が、前記第1の広域ネットワークとの間で接続しているネットワークに応じて、前記仮想コアネットワークでのサービスを可変に制御する、通信方法が提供される。

【0032】

本発明のさらに別の側面によれば、モバイルネットワークの基地局又は無線LAN(Local Area Network)と通信を行う手段と、通話発信時に、前記モバイルネットワークの基地局を経由して通話するか、前記無線LANを経由して通話するかを選択可能な手段と、を有する端末が提供される。

10

【0033】

本発明の他の側面によれば、無線LANと、基地局に接続するコアネットワークとに第1の広域ネットワーク(WAN1)を介して接続するデータセンタに配置されるコンピュータに、コアネットワークの機能の少なくとも一部を仮想化し、前記第1の広域ネットワークに接続される仮想コアネットワークの処理と、

前記無線LAN又は前記基地局への接続が選択自在とされ、前記データセンタに接続する端末が、前記第1の広域ネットワークとの間で接続しているネットワークに応じて、前記仮想コアネットワークでのサービスを可変に制御する処理と、を実行させるプログラムが提供される。

20

【0034】

本発明のまたさらに他の側面によれば、モバイルネットワークの基地局又は無線LAN(Local Area Network)と通信を行う処理と、

通話発信時に、前記モバイルネットワークの基地局を経由して通話するか、前記無線LANを経由して通話するかを選択可能とする処理を、端末のコンピュータに実行させるプログラムが提供される。

【0035】

本発明によれば、モバイルネットワークの基地局又は無線LAN(Local Area Network)との通信を行う処理と、セットアップ時に、前記モバイルネットワークの基地局を経由して通話するか、前記無線LANを経由して通話するかを選択可能とする処理を、端末のコンピュータに実行させるプログラムが提供される。

30

【0036】

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】

【0037】

本発明によれば、端末の接続先のネットワークに応じた通信サービスを提供可能としている。

【図面の簡単な説明】

40

【0038】

【図1】関連技術を例示する図である。

【図2】本発明の例示的な一実施形態を例示する図である。

【図3】(A)は本発明の例示的な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シーケンスを例示する図である。

【図5】(A)、(B)は、本発明の例示的な一実施形態のフィルタを例示する図である。

【図6】本発明の例示的な一実施形態の制御装置を例示する図である。

【図7】本発明の他の例示的な実施形態を例示する図である。

50

【図 8】本発明の他の実施形態の動作シーケンスを例示する図である。

【図 9】本発明の他の例示的な実施形態を例示する図である。

【図 10】(A)、(B)、(C)は本発明の例示的な一実施形態の端末画面を例示する図である。

【図 11】(A)、(B)は本発明の例示的な一実施形態の端末を例示する図である。

【図 12】仮想化装置の構成を例示する図である。

【図 13】(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】

10

【0039】

本発明の実施形態について説明する。本発明の実施形態によれば、端末が、基地局及びコア網、又は、無線LAN (Local Area Network) の一方を介して第1の広域ネットワーク (Wide Area Network) 経由で接続するデータセンタでは、前記端末が前記第1の広域ネットワーク (Wide Area Network) との間で接続しているネットワークに応じて、前記データセンタの仮想ネットワークで提供する通信サービス等を可変に制御する。

【0040】

特に制限されないが、本実施形態では、データセンタの仮想ネットワークとして、例えば仮想化EPC (Virtualized EPC: vEPC) を備えた構成としてもよい。仮想化EPC (vEPC) 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等によりソフトウェア的に実現することで構成してもよい。例えば、図12を参照して後に説明するように、仮想化EPC (vEPC) は、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実現するようにしてもよい。

20

【0041】

図2は、本発明の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EPC 20の少なくとも一部を仮想化したものである。すなわち、vEPC 52は図1のEPC 20のePDG 27、PGW 22、PCRF 26等、EPC 20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。

30

【0042】

第1のゲートウェイ (GW1) 51 (Ingress gateway) 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、vEPC 52とを接続する。第2のゲートウェイ 53 (Egress gateway) は、インターネットやIMS等のWAN 2 (32) と、vEPC 52とを接続する。

【0043】

図2において、無線LAN 40は、家庭内無線LAN又は公衆無線LANであってよい。無線LAN 40は、無線LANアクセスポイント (WLAN AP)、NAT (Network Address Transformation) /NAPT (Network Address Port Translation) を備えた無線LANルータ等を含み、モデム等を介してWAN 1 (31) に接続する。

40

【0044】

また、端末1は設定切り替え等により、Wi-Fi (登録商標) 等の無線LAN 40を介して、データセンタ50にアクセスするようにしてもよい。その場合、端末1は、無線LAN 40を経由して、WAN 1 (31)、データセンタ50の第1のゲートウェイ 51、vEPC 52、第2のゲートウェイ 53からWAN 2 (32) に接続する。

【0045】

図2において、端末1が接続する基地局10、EPC 20の一部は、クラウド事業者がMVNO (Mobile Virtual Network Operator) キャリアとして通信キャリア (MNOキャリア) から借り上げたものであってもよい。データセンタ50内の仮想化EPC 52を介して、MVNOキャリアとして、クライアントに各種通信サービスを提供することができる。

50

【0046】

基地局（eNB）10に接続されたMNOキャリアのEPC（MNO-EPC）20と、無線LAN40に、WAN1（31）を介して接続するクラウド事業者のデータセンタ（DC）50を備えている。データセンタ50は、無線LAN40への接続又は基地局10への接続が選択自在な端末1が、無線LAN40を介して接続する場合、端末1との間を、無線LAN40及びWAN1（31）経由のVPNで接続するVPN装置を備えた第1のゲートウェイ51と、EPCの機能の少なくとも一部を仮想化した仮想化EPC（vEPC）52と、を備えている。VPNは、第1のゲートウェイ51で終端し、仮想化EPC（vEPC）52、第2のゲートウェイ53を介してWAN2に接続される。さらに、少なくともWAN2（32）側から第2のゲートウェイ53に入力されたパケットのフィルタリングを行うフィルタ54を備えている。フィルタ54は、第2のゲートウェイ（GW）53に入力されたパケットのフィルタリングとともに、WAN1（31）側から第1のゲートウェイ51に入力されたパケットのフィルタリングを行うようにしてもよいことは勿論である。

10

【0047】

さらに、WAN1（31）との間で、端末1がどのネットワークに接続しているか、接続先のネットワークの種別（無線LANであるか、基地局・EPCであるか等）に応じて、vEPC52での通信サービス（例えば課金方式あるいはQoSポリシー）を可変に制御し、端末1が接続するネットワーク間で差を付ける制御を行う制御装置56を備えている。なお、図2では、単に説明のために、制御装置56は、vEPC52に接続するノードとして示されているが、制御装置56を、vEPC52内に備えた構成、vEPC52のアプライアンス内に実装した構成としてもよいことは勿論である。

20

【0048】

LTE（Long Term Evolution）では、QoS制御は、端末と基地局の間の無線アクセスネットワーク（Radio Access Network）区間とコアネットワーク（EPC）の双方で行われるが、ここでは、vEPC52において、例えばWAN1及び／又はWAN2の帯域保証等を行うようにしてもよい。

【0049】

データセンタ50のvEPC52において、例えば、端末1が基地局10・EPC20を介してWAN1（31）経由でアクセスしてきた場合（3G/LTE接続時）には、vEPC52のポリシー／課金実施機能PCEF（Policy Charging Enforcement Function）等における課金実施をアクティブとする（すなわち、PCRFからの課金ポリシーにしたがって課金を実施する）。一方、端末1が、無線LANアクセスポイント41を介しWAN1（31）経由でアクセスしてきた場合（例えば信頼できない非3GPPアクセスネットワーク接続時）、vEPC52内のPCEF等による端末1に対する課金を行わないようにしてもよい。

30

【0050】

vEPC52で端末1に対する課金を行わない場合として、例えば、端末1が、EPC20を介さずに、無線LANアクセスポイント41から、WAN1（31）を介してデータセンタ50に接続する無線LAN IP電話VoWLAN（Voice over Wireless LAN）を含む。また、端末1が無線LANアクセスポイント41を介しWAN1（31）経由でWi-Fi（登録商標）-callingを行う場合、MNO又はMVNOのePDGから、EPC20又はvEPC52のPGWに接続されるが、この場合も、vEPC52のPCEFでの課金は行わないようにしてもよい（無料）。

40

【0051】

なお、例示的な実施形態において、MNO-EPC20のアプライアンス（図1のEPC20参照）とvEPC52のアプライアンスとの振り分け（例えばSGWはMNO-EPC20、PGWはvEPC52等）については任意である。

【0052】

ただし、後述するように、データセンタ50のvEPC52に、ePDG、PGW、PCRF等を具備し、クラウド事業者が通信キャリア（MVNO）として、Wi-Fi（登録商標）-callingサービスを端末1に提供し、当該サービスに対する課金、QoS制御を行うようにしてもよい。

【0053】

50

また、

- ・端末1が、Wi-Fi（登録商標）-callingにより、無線LAN、WAN1（31）経由で、データセンタ50のvEPC52に接続し、このvEPC52内のePDGをセキュリティ・ゲートウェイとする場合と、
- ・端末1が、基地局10、MNO-EPC20、WAN1（31）経由で、データセンタ50のvEPC52に接続する場合と、

では、データセンタ50でのEPSベアラが異なる。仮想ネットワーク機能（Virtual Network Function：VNF）のインスタンス（仮想マシン：Virtual Machine：VM）の生成・起動等の管理・制御は、例えばvEPC52における仮想ネットワーク機能を管理・制御する制御装置（不図示）で行うようにしてもよい。

10

【0054】

端末1が接続する無線LANアクセスポイント41との間にWAN1（31）が介在するデータセンタ50において、第1のゲートウェイ51と、端末1間に、VPNトンネル60を張る。第1のゲートウェイ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。無線LANアクセスポイント41は、図示されない無線LANルータ、モデム等を介して、WAN1（31）に接続される。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、無線LAN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。

【0055】

20

本実施形態によれば、クラウド事業者のデータセンタ50において、無線LAN40、広域ネットワークWAN1（31）経由のアクセスに対して、データセンタ50との間でセキュアなコネクション（音声通話/SMSやデータ通信）を実現している。

【0056】

また、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等を行うフィルタ54を備えている。

【0057】

フィルタ54は、WAN2（32）側から第2のゲートウェイ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。フィルタ54は、端末1から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。フィルタ54は、第1のゲートウェイ51と第2のゲートウェイ53間に接続され、セキュリティポリシーを管理するサーバ等を実装するようにしてもよい。フィルタ54は、当該サーバ上で仮想マシン上で稼働するようにしてもよい。

30

【0058】

端末1が、無線LAN40、WAN1（31）を介してデータセンタ50にアクセスする場合、通信キャリアのコア網（EPC）で提供される制御（パケットフィルタ等）は行われなくなるが、本実施形態によれば、データセンタ50内のフィルタ54がパケットフィルタリング機能等を提供している。

【0059】

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51、vEPC52、第2のゲートウェイ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）間のデータ通信の packets（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にオフロードを行うようにしてもよい。

40

【0060】

ただし、図2において、データセンタ50の第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55上に、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

50

センタ 5 0 の vEPC 5 2 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。

【 0 0 6 1 】

なお、データセンタ 5 0 のフィルタ 5 4 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不適切なWebサイトの閲覧等を制限することができる。

【 0 0 6 2 】

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 2（3 2）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、フィルタ 5 4 は、プライベートIPアドレスを宛先とするWAN 2（3 2）からのパケットを拒否する設定を行うようにしてもよい。

【 0 0 6 3 】

WAN 2（3 2）がIMS（IP Multimedia Subsystem）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 5 3 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SGW（Signaling Gateway）から、回線交換ドメイン等に通信サービスを提供する。

【 0 0 6 4 】

あるいは、データセンタ 5 0 において、IMS機能の少なくとも一部を、仮想ネットワーク 5 5 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 5 5 上に実装し、フィルタ 5 4 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、第 2 のゲートウェイ 5 1、5 3 間に接続する構成としてもよいことは勿論である。

【 0 0 6 5 】

第 1 のゲートウェイ 5 1 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。

【0066】

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

【0067】

VPNのトンネリングプロトコルとして、例えばPPTP(Point-to-Point Tunneling Protocol)、L2TP(Layer 2 Tunneling Protocol)、IPsec、GRE(Generic Route Encapsulation)等がある。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)。

10

【0068】

例えば無線LANに設置されるルータ等は、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(User Datagram Protocol)ヘッダのポート番号の変換を行うNAPT機能を備えている。

【0069】

IPsecのトンネル・モードでは、IPヘッダとデータ部分(図13(A))をまとめて暗号化し、新たにIPヘッダ(図13(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13(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3の端末1と第1のゲートウェイ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。

20

【0070】

この場合、IPsec VPNをNAPTに対応させるため、図13(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13(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、クッキー(Cookie)値、例えば、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。

30

【0071】

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13(E)は、L2TP/IPsecのパケット形式を例示した図である。

40

【0072】

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トラバース手法を用いてもよい。

【0073】

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。

50

【0074】

(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。

【0075】

(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。

10

【0076】

(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) 等が用いられる。

【0077】

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。

20

【0078】

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。

30

【0079】

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。

【0080】

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が含まれる。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。

40

50

【0081】

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で送信されるが、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。

10

【0082】

20

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FQDN(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)。

【0083】

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。

30

【0084】

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。

【0085】

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。

40

【0086】

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/名前欄は、ユーザIDのほか、データセンタ50のクラウ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。

【0087】

50

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。

【0088】

図4は、図2の一実施形態のシステムにおいて、端末1のアタッチ処理とWAN2(32)に接続する接続先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(WLAN AP)、第1のゲートウェイ51、vEPC52、第2のゲートウェイ53(GW2)、WAN2(32)側の接続先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。

10

【0089】

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。

【0090】

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もよい。

20

【0091】

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、MMEとして機能し、vEPC52のS11インタフェースを介して、例えばベアラ設定要求(Create Session Request)をSGWに送信するようにしてもよい。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。

【0092】

4. vEPC52のSGWから、MMEとして機能する第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。

30

【0093】

5. 以上で、IPsec VPNトンネルのセットアップが完了する。

【0094】

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。

【0095】

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。

【0096】

40

8. 端末1側からのWAN2(32)側に接続先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)へのIPルーチングが行われる。

【0097】

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等のポリシーに応じて、第1のゲートウェイ51に転送し、第1のゲートウェイ51からVPNトンネル60を介して端末1に転送される。

【0098】

図5(A)は、図2のフィルタ54の構成の一例を示す図である。図5(A)を参照すると、フィルタ54は、

50

- ・パケットを受信し、転送制御部 5 4 2 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 5 4 1 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 5 4 3 と、
- ・通信部 5 4 1 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 5 4 3 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 5 4 1 に通知する転送制御部 5 4 2 と、
- ・フィルタ情報記憶部 5 4 3 に、フィルタ情報を設定するフィルタ情報設定部 5 4 4 と、を備えている。フィルタ情報設定部 5 4 4 は、図 2 のデータセンタ 5 0 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 5 4 3 のフィルタ情報を設定するようにしてもよい。

10

【0099】

図 5 (B) は、図 5 (A) のフィルタ情報記憶部 5 4 3 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WAN 2 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。

20

【0100】

フィルタID=1では、ポート23（telnet）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ようにしてもよい（telnetポート（23番）を封鎖）。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。

【0101】

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。

30

【0102】

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）毎に設定し、フィルタ情報を、端末に紐付けて管理し、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。

【0103】

図6は、図2において、端末1が接続するネットワークが無線LANであるか、基地局10・EPC20であるか等に応じて、データセンタ50のvECP52で行われる課金方式、通信品質（QoS）等を制御する制御装置56の構成を例示する図である。

40

【0104】

図6を参照すると、制御装置56は、端末の接続先のネットワークを判別する接続先ネットワーク判別部561と、接続先ネットワーク判別部561で判別されたネットワーク種別（無線LAN、3G/LTE等）に応じて、必要なサービスの設定と制御を行うサービス制御部562と、サービス制御部562からの設定情報（課金ポリシー）に基づき、パケット単位で課金を実施する課金実施部563と、サービス制御部562からの設定情報（QoSポリシー）に基づき、パケット単位で通信品質を制御する通信品質制御部564と、課金実施部563にキャプチャしたパケットを受け渡し、通信品質制御部564から制御を受ける

50

通信部 5 6 5 を備えている。

【0105】

接続先ネットワーク判別部 5 6 1 は、端末の接続先が非3GPPアクセスネットワーク（無線LANアクセスポイント）であるか、3GPPアクセスネットワーク（基地局）であるかを、例えば端末の接続確立時等に端末から取得するようにしてもよい。あるいは、接続先ネットワーク判別部 5 6 1 は、MMEで管理する無線ベアラ情報、あるいは、端末の接続確立時のHSS、3GPP AAAサーバ等での認証結果情報から、端末の接続先ネットワーク情報を取得するようにしてもよい。通信部 5 6 5 は、受信したパケットを不図示の受信バッファに蓄積し、通信品質制御部 5 6 4 からの制御のもと、優先度の高いパケットから順に取り出して送信する等の優先制御や、WAN 1 及び／又はWAN2等の帯域保証等に必要な帯域制御を行う。

10

【0106】

図 7 は、前述した実施形態の一例を例示する図である。図 7 を参照すると、データセンタ 5 0 のvEPC 5 2 のePDG 5 2 7 と端末 1 間にIPsecトンネルが設定される。ePDG 5 2 7 は、VPNゲートウェイとして機能し、VPNトンネルを終端する。

【0107】

ePDG 5 2 7 は、VPNゲートウェイとして機能し、

- ・ 端末 1 との間での、無線LAN 4 0、WAN 1 （3 1）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、vEPC 5 2 のPGW 5 2 2 で行うようにしてもよい。

20

【0108】

端末 1 からIKEV2でEAPメッセージをePDG 5 2 7 に送信し、vEPC 5 2 の3GPP AAAサーバ 5 2 5 に中継し、EAP-SIM/EAP-AKA認証を行う。vEPC 5 2 のePDG 5 2 7 とPGW 5 2 2 間は、GTP又はPMIPv6トンネルで接続される。

30

【0109】

vEPC 5 2 において、PGW 5 2 2 とePDG 5 2 7 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vEPC 5 2 のePDG 5 2 7 との間でIPsecトンネルが確立されると、ePDG 5 2 7 は、プロキシバインディングアップデート（Proxy Binding Update）をPGW 5 2 2 に送信する。この結果、vEPC 5 2 のPGW 5 2 2 では、端末 1 への着信の送信先を、vEPC 5 2 のePDG 5 2 7 に切り替え、VPNトンネル 6 0 を介し、無線LAN 4 0 経由で、着信が端末 1 に通知される。

【0110】

PGW 5 2 2 は、例えばEPSベアラに関するTFT (Traffic Flow Template) を有するフィルタ 5 2 9 を備えている。フィルタ 5 2 9 において、WAN2から端末 1 側への下り方向のパケットフィルタの設定（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メッセージで行うようにしてもよい。あるいは、端末 1 からAttach Requestメッセージ等の接続処理や、その他、所定のイベント発生時等に行ってもよい。なお、フィルタ 5 2 9 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、フィルタ 5 2 9 に、WAN 2 （3 2）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。

40

【0111】

50

WAN2(32)をIMSで構成した場合、vEPC 5 2 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。

【0112】

制御装置 5 6 は、図 6 を参照して説明した制御装置 5 6 からなる。この実施形態では、制御装置 5 6 は、PCRF 5 2 6 に接続され、該PCRF 5 2 6 から通知される課金情報やQoSポリシー情報に基づき、端末 1 が接続するネットワークに応じて、課金制御、QoSポリシーに差を付ける制御を行う。制御装置 5 6 は、PCEFノードとして実装してもよい。あるいは、制御装置 5 6 は、PGW 5 2 2 内に実装してもよい。制御装置 5 6 のサービス制御部 5 6 2 (図 6) は、PCRF 5 2 6 からGxインタフェースで通知される課金情報、QoSポリシー情報に基づき、端末 1 が接続するネットワーク種別に応じて、課金、QoSポリシーを設定するようにしてもよい。図 6 の接続先ネットワーク判別部 5 6 1 は、ePDG 5 2 7、HSS 5 2 4 及び 3GPP AAA 5 2 5 でのSIM認証の結果から、端末 1 からの経路が無線LAN 4 0 を含むことを判別するようにしてもよい。なお、第 1、第 2 のゲートウェイ 5 1、5 3 はルータ (エッジルータ) で構成してもよい。

【0113】

図 7 では、ePDG 5 2 7、PGW 5 2 2 をvEPC 5 2 として実装しているが、クラウド事業者がMVNO (Mobile Virtual Network Operator) として、MNO (Mobile Network Operator) のePDG 2 7、PGW 2 2 (図 1) を借り受けたものであってもよい。

【0114】

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ePDG 5 2 7 との間で、無線LAN 4 0、WAN1 (3 1) を経由したVPN 6 0 (IPsecトンネル) が張られ、ePDG 5 2 7 とPGW 5 2 2 間にGTP/PMIPv6のトンネルが張られ、PGW 5 2 2 から、例えばIMSからなるWAN 2 (3 2) 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、フィルタ 5 2 9 により、不当な着信や有害サイト等からの保護が提供される。なお、PGW 5 2 2 は、図 3 の第 2 のゲートウェイ 5 3 の機能を備えている。

【0115】

図 7 のフィルタ 5 4 は、図 2 を参照して説明したフィルタ 5 4 と同一であるため、説明は省略する。

【0116】

なお、図 7 において、vEPC 5 2 の各ネットワーク機能を仮想化したノード (仮想マシン)、制御装置 5 6 のほか、フィルタ 5 4 等も、サーバ等のコンピュータ上で実行されるプログラムでその機能・処理を実現するようにしてもよいことは勿論である。

【0117】

図 8 は、図 7 のシステムにおいて、端末 1 のアタッチ処理とWAN2 (3 2) に接続する接続先に通信接続するシーケンスを説明する図である。図 7 には、図 6 の端末 1、WLAN 4 0 (WLAN AP)、ePDG 5 2 7、PGW 5 2 2、HSS 5 2 4 / AAAサーバ 5 2 5、PCRF 5 2 6、WAN 2 (3 2) 側の接続先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 8 において、例えばePDG 5 2 7 を第 1 のゲートウェイ (GW1)、PGW 5 2 2 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。

【0118】

1. 端末 1 は、無線LAN (WLAN) 4 0 との間で接続を確立し、例えばvEPC 5 2 内のHSS 5 2 4 / AAA 5 2 5 により認証・認可 (Authentication & Authorization) を行う。

【0119】

2. 端末 1 側から、ePDG 5 2 7 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。

【0120】

3. ePDG 5 2 7 は、PGW 5 2 2 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。

【0 1 2 1】

4. PGW 5 2 2 は、PCRF 5 2 6 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。

【0 1 2 2】

5. PGW 5 2 2 は、AAAサーバ 5 2 5 にPGWの識別情報（PGW ID）を通知し、AAAサーバ 5 2 5 は、HSS 5 2 4 に、PGW 5 2 2 のIDと、端末 1 に対応したAPN（Access Point Name）を通知して登録する。

10

【0 1 2 3】

6. PGW 5 2 2 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、PGW 5 2 2 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、ePDG 5 2 7 に向けて送信されることになる。PGW 5 2 2 は、ePDG 5 2 7 に対してProxy Binding Ackを送信する。

【0 1 2 4】

7. 以上で、IPsec VPNトンネルのセットアップが完了する。

【0 1 2 5】

20

8. ePDG 5 2 7 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。

【0 1 2 6】

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ePDG 5 2 7 間はIPsecトンネル、ePDG 5 2 7 とPGW 5 2 2 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。

【0 1 2 7】

10. 端末 1 側からのWAN 2（3 2）側に接続先への接続要求をePDG 5 2 7 からPMIPトンネルを介して受けると、PGW 5 2 2 から接続先（WAN2側）へのIPルーティングが行われる。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 5 3 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に接続する接続先に接続するようにしてもよい。なお、図 8 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PGW 5 2 2（SGiインタフェース）はIPsec（VPN）で通信を行う。

30

【0 1 2 8】

11. 以上で、端末 1 からVPN、データセンタ 5 0 のvEPC 5 2 を介し、WAN 2 側の接続先との間の接続の設定が完了する。なお、WAN 2（3 2）側から端末 1 へのダウンリンク方向のパケットは、vEPC 5 2 内のPGW 5 2 2 がバインディングキャッシュエントリに基づきePDG 5 2 7 にPIMPトンネルを介して転送し、ePDG 5 2 7 からVPNトンネル 6 0 を介して端末 1 に転送される。

40

【0 1 2 9】

次に、図 1 2 を参照して、vEPC 5 2 のノードの構成について説明する。データセンタ 5 0 内のサーバ 5 7 上の仮想マシン（Virtual Machine: VM）5 7 1 は仮想ネットワークインタフェースコントローラ（vNIC）5 7 5 を介して仮想スイッチ（vSwitch）5 7 6 の仮想ポート：Aに接続し、仮想スイッチ（vSwitch）5 7 6 の仮想ポート：Bから物理NIC（pNIC）5 7 7 を介して物理スイッチ（Physical Switch）5 8 の物理ポート：Cに接続され、物理スイッチ（Physical Switch）5 8 の物理ポート：Dを介して、データセンタ 5 0 内のLAN等のネットワーク（仮想ネットワーク）5 9 に接続される。仮想マシン 5 7 1 は、ゲストOS（Operating System）5 7 3 と、アプリケーション 5 7 2 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 7 のePDG 5 2 7 の機能、あるいは

50

他のノードの機能)を実現する。ネットワーク59は例えば図7の第1のゲートウェイ(ルータ)51に接続される。

【0130】

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。同様に、図12の仮想マシン571によって、図2のフィルタ54を実装し、VLAN等の仮想ネットワーク59によって、図2のネットワーク55を構成してもよい。なお、図12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。 10

【0131】

図9は、本発明の別の例示的な実施形態を説明する図である。図9に示す実施形態では、端末1は、データセンタ50を所持するクラウド事業者が提供する無線LANアクセスポイント41、クラウド事業者とは他の事業者(他キャリア)が提供する無線LANアクセスポイント43、他のキャリアの基地局10及び該基地局10に接続するEPC20のいずれかを介しWAN1経由でデータセンタ50に接続する。

【0132】

データセンタ50において不図示の制御装置(図6の56)は、
端末1が接続するネットワークが、 20
・データセンタ50を所持する事業者に提供された無線LANアクセスポイント41、
・データセンタ50のクラウド事業者と異なる他のキャリアによって提供された無線LANアクセスポイント43、
・通信キャリア(クラウド事業者と異なる他のキャリア)の基地局10及びEPC20
のうちのいずれであるかによって、vEPC52における課金方式やQoS制御に差を付ける制御を行う。QoS制御のパラメータとしてQCI(QoS Class Identifier)が用いられ、LTEでは、音声通話(VoIP)のQCIは2と高い値(優先度)に設定される。

【0133】

特に制限されるものではないが、端末1が接続するネットワークに応じて、例えば以下のようなサービスに差を設けるようにしてもよい。 30

【0134】

端末1が、クラウド事業者の無線LANアクセスポイント41に接続してデータセンタ50のvEPC52に接続した場合、vEPC52の利用に対して課金は行わない(無料)。

【0135】

端末1が、他のキャリアの無線LANアクセスポイント43に接続してデータセンタ50のvEPC52に接続した場合、vEPC52の利用に対して、例えば単位時間当たりX円等の設定による所定の課金を行う。

【0136】

端末1が、別のキャリアの基地局20に接続してデータセンタ50のvEPC52に接続した場合、例えば単位時間当たりY円($Y>X$)等の設定による所定の課金を行う。 40

【0137】

また、データセンタ50のvEPC52でQoS制御として、端末1が、クラウド事業者の無線LANアクセスポイント41に接続してデータセンタ50のvEPC52に接続した場合、高品質とする。端末1が、他のキャリアの無線LANアクセスポイント43に接続してデータセンタ50のvEPC52に接続した場合、低品質とする。

【0138】

端末1が、別のキャリアの基地局20に接続してデータセンタ50のvEPC52に接続した場合、低品質又は中程度の品質とする。

【0139】

図10(A)乃至図10(C)は、本発明のさらに別の例示的な実施形態を説明する図で 50

ある。図10(A)を参照すると、本実施形態では、端末1は、スマートフォンやタブレット端末等スマートデバイスとして説明する。なお、端末1は、その他の種別の端末であっても良い。例えば、スマートフォンでない従来型の携帯電話（フィーチャーフォン）であっても良い。表示部11は、表示装置とタッチパッドのような位置入力装置を組み合わせたタッチパネルである。図10(A)の表示部11のホーム画面に表示された受話器（電話機）マークのアイコン111をユーザがタップすると、アプリケーション画面が表示され、電話帳アイコンをユーザがタップすると、名簿が表示される。名簿の中から電話をかけたい相手：日電太郎112をユーザがタップすると、図10(B)に示すように、その電話番号113が表示され、電話番号113をユーザがタップすると、受話器（電話をかける）114と、Wi-Fi（登録商標）電話115が表示される。

10

【0140】

ユーザは受話器（電話をかける）114と、Wi-Fi（登録商標）電話115のいずれかを選択して相手に電話をかける。

【0141】

受話器（電話をかける）114をタップすると、端末1は、基地局に接続し、通話相手に接続する。

【0142】

Wi-Fi（登録商標）電話115を選択すると、端末1は、Wi-Fi（登録商標）アクセスポイントに接続し、Wi-Fi（登録商標）-Calling（無線LANからセキュリティ・ゲートウェイを介してキャリアの交換機に接続する）により、通話相手に接続する。

20

【0143】

図10(A)、(B)の例では、Wi-Fi（登録商標）の電話を通話時に選択しているが、図10(C)に示すように、表示部11においてネットワーク設定画面116上で、Wi-Fi（登録商標）通信のオンとオフ117、Wi-Fi（登録商標）電話のオン、オフ118を設定する。オン、オフの設定は、タッチ式、あるいはスライド式であってもよい。

【0144】

なお、図10(B)において、Wi-Fi（登録商標）-CallingによるSMSを選択項目の一つとして表示するようにしてもよい。

【0145】

また、図10(B)において、Wi-Fi（登録商標）電話115のマークは、Wi-Fi（登録商標）アクセスポイントからの受信電波強度（電界強度）を表すように可変としてもよい。Wi-Fi（登録商標）アクセスポイントからの受信電波強度（電界強度）が大であると、電波を表す弧（波）の本数が増加し、受信電波強度（電界強度）が小であると、電波を表す弧（波）の本数が減少する等、表示を変えるようにしてもよい。

30

【0146】

ネットワーク設定画面116上で、予め設定する場合、端末の接続先のネットワークの種別による優先度や条件等を設定するようにしてもよい。

【0147】

図11(A)は、図10(A)乃至図(C)を参照して説明した端末1の構成を模式的に例示した図である。図11(A)を参照すると、端末1は、図10(A)乃至図10(C)等の画面を表示するタッチパネル1001と、タッチパネル1001へのデータや画像の出力と、ユーザからのタッチパネル1001への入力の位置検知等を行うタッチパネル入力・出力部1002と、受話器アイコン111（図10(A)）のタップで起動され、電話をかける処理を実行するアプリケーション（アプリケーションプログラム）1003と、アプリケーション1003での処理結果に基づき、無線LAN、又は基地局との接続を確立する制御部1004と、基地局と通信する通信モジュール（3G/LTE通信モジュール）1006及びアンテナ1007と、Wi-Fi（登録商標）通信モジュール（IEEE802.11a/b/h/nインタフェース）1008及びアンテナ1009を備えている。なお、アプリケーション1003及び制御部1004等の処理は、端末1の不図示のCPU(Central Processing Unit)で実行されるプログラムで実現される。

40

50

【0148】

図10(A)、図10(B)に例示したように、通話開始時に、端末1からの接続先ネットワークの変更等に応じて、通信モジュール1006又は通信モジュール1008を選択するようにしてもよい。すなわち、アプリケーション1003は、記憶部1005に設定情報が格納されていない場合、ユーザがタッチパネル1001上で、電話(3GPPアクセスネットワークによる電話、又は、Wi-Fi(登録商標)電話)のいずれを選択したかに応じて、制御部1004は、通信モジュール1006又は通信モジュール1008を選択し、基地局又はWi-Fi(登録商標)アクセスポイントと通信接続する。

【0149】

一方、図11(B)のような設定情報が、記憶部1005に予め設定されている場合、アプリケーション1003は、ユーザが電話をかける相手の電話番号(図10(B)の113)をタップすると、Wi-Fi(登録商標)電話を選択して、制御部1004を介して、Wi-Fi(登録商標)通信モジュール1008、アンテナ1009からWi-Fi(登録商標)アクセスポイント(無線LANアクセスポイント)との接続を行う。なお、図11(A)において、制御部1004は、図10(C)の設定画面116から入力された設定情報(図10(B))を記憶部1005に記憶する。Wi-Fi(登録商標)電話のオン・オフを、常に図10(C)の設定画面116から行うようにしてもよい。

【0150】

上記した各実施形態によれば、無線LAN、WAN1を介してデータセンタにアクセスする端末に対してセキュアなネットワーク接続を提供し、さらに、端末からのWi-Fi(登録商標)-Calling等に対して、端末が接続するネットワーク種別に応じた通信サービス(課金、通信品質)を提供可能としている。さらに、有害なサイト、有害コンテンツからの保護や不当な着信等の拒否を可能としている。

【0151】

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。

【0152】

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

【0153】

(付記1)

基地局に接続されたコアネットワークと、無線LAN(Local Area Network)とに第1の広域ネットワーク(Wide Area Network)を介して接続するデータセンタを備え、

前記データセンタは、

コアネットワークの機能の少なくとも一部を仮想化し、前記第1の広域ネットワークに接続される仮想コアネットワークと、

前記無線LAN又は前記基地局への接続が選択自在とされ、前記データセンタに接続する端末が、前記第1の広域ネットワークとの間で接続しているネットワークに応じて、前記仮想コアネットワークでの前記端末に対するサービスを可変に制御する制御装置と、

を備えた、通信システム。

【0154】

(付記2)

前記データセンタにおいて、

前記制御装置は、

前記端末が前記基地局及び前記コアネットワークを介し前記第1の広域ネットワーク経

由で前記データセンタに接続しているか、あるいは、前記端末が前記無線LAN及び前記第1の広域ネットワーク経由で前記データセンタに接続しているか、という前記端末が接続するネットワークの種別に対応して、

また、前記端末が前記無線LAN及び前記第1の広域ネットワーク経由で前記データセンタに接続している場合には、前記無線LANのアクセスポイントが、前記データセンタの事業者によって提供されたものであるか、あるいは、前記データセンタの前記事業者と異なる他の事業者によって提供されたものであるか、という前記端末が接続する無線LANの種別に対応して、

前記仮想コアネットワークで前記端末に提供する課金方式と通信品質サービスの少なくとも一方を可変に制御する、付記1記載の通信システム。

10

【0155】

(付記3)

前記データセンタにおいて、

前記端末が、前記無線LANを介し前記第1の広域ネットワーク経由で前記データセンタに接続する場合、前記端末との間を、前記無線LAN及び前記第1の広域ネットワーク経由のVPN(Virtual Private Network)で接続するVPN装置を備えた、付記1又は2記載の通信システム。

【0156】

(付記4)

前記データセンタが、

20

前記第1の広域ネットワークに接続し、前記VPN装置を備えた第1のゲートウェイと、前記第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、を備え、

前記第1のゲートウェイと前記第2のゲートウェイは、前記仮想コアネットワークに接続され、

前記第1の広域ネットワークから入力されるパケットと、前記第2の広域ネットワークから入力されるパケットの少なくとも一方のパケットのフィルタリングを行うフィルタを、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備えた、付記3記載の通信システム。

【0157】

30

(付記5)

前記データセンタにおいて、

前記フィルタが、前記第2の広域ネットワーク側からの前記端末への着信やメッセージのアクセス拒否、許可を制御する、付記4記載の通信システム。

【0158】

(付記6)

前記端末が、前記VPNから前記VPN装置及び前記仮想コアネットワークを経由し、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データを、前記データセンタの前記仮想コアネットワーク及び前記VPN装置から、前記VPNを介して受信する、付記3乃至5のいずれかに記載の通信システム。

40

【0159】

(付記7)

前記データセンタの前記VPN装置は、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3乃至6のいずれかに記載の通信システム。

【0160】

(付記8)

前記端末が、前記基地局を介して通信するか、前記無線LANを介して通信するかを選択する手段を備えた、付記1乃至7のいずれかに記載の通信システム。

【0161】

50

(付記 9)

前記無線LANのアクセスポイントが、
前記データセンタの事業者によって提供されるアクセスポイントと、
他の通信キャリアによって提供されるアクセスポイントと、
の少なくとも一方を含む、付記 1 乃至 8 のいずれかに記載の通信システム。

【0162】

(付記 10)

基地局に接続されたコアネットワークと、無線LAN (Local Area Network) とに第 1 の
広域ネットワーク (Wide Area Network) を介して接続する装置 (手段) と、

コアネットワークの機能の少なくとも一部を仮想化し、前記第 1 の広域ネットワークに
接続される仮想コアネットワークと、

前記無線LAN又は前記基地局への接続が選択自在とされる端末であって、前記通信装置
に接続する前記端末が、前記第 1 の広域ネットワークとの間で接続しているネットワーク
に応じて、前記仮想コアネットワークでの前記端末に対するサービスを可変に制御する制
御装置と、

を備えた、通信装置。

【0163】

(付記 11)

前記制御装置は、

前記端末が前記基地局及び前記コアネットワークを介し前記第 1 の広域ネットワーク経
由で前記通信装置に接続しているか、あるいは、前記端末が前記無線LAN及び前記第 1 の
広域ネットワーク経由で前記通信装置に接続しているか、という前記端末が接続するネッ
トワークの種別に対応して、

また、前記端末が前記無線LAN及び前記第 1 の広域ネットワーク経由で前記通信装置に
接続している場合には、前記無線LANのアクセスポイントが、第 1 の事業者によって提供
されたものであるか、あるいは、前記第 1 の事業者と異なる他の事業者によって提供され
たものであるか、という前記端末が接続する無線LANの種別に対応して、

前記仮想コアネットワークで前記端末に提供する課金方式と通信品質サービスの少なく
とも一方を可変に制御する、付記 10 記載の通信装置。

【0164】

(付記 12)

前記端末が、前記無線LANを介し前記第 1 の広域ネットワーク経由で前記データセンタ
に接続する場合、前記端末との間を、前記無線LAN及び前記第 1 の広域ネットワーク経由
のVPN(Virtual Private Network)で接続するVPN装置を備えた、付記 10 又は 11 記載の
通信装置。

【0165】

(付記 13)

前記第 1 の広域ネットワークに接続し、前記VPN装置を備えた第 1 のゲートウェイと、
前記第 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、
を備え、

前記第 1 のゲートウェイと前記第 2 のゲートウェイは、前記仮想コアネットワークに接
続され、

前記第 1 の広域ネットワークから入力されるパケットと、前記第 2 の広域ネットワーク
から入力されるパケットの少なくとも一方のパケットのフィルタリングを行うフィルタを
、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備えた、付記 12 記載の通信装
置。

【0166】

(付記 14)

前記フィルタが、前記第 2 の広域ネットワーク側からの前記端末への着信やメッセージ
のアクセス拒否、許可を制御する、付記 13 記載の通信装置。

【0167】

(付記15)

前記端末が、前記VPNから前記VPN装置及び前記仮想コアネットワークを経由し、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データを、前記通信装置の前記仮想コアネットワーク及び前記VPN装置から前記VPNを介して受信する、付記12乃至14のいずれかに記載の通信装置。

【0168】

(付記16)

前記VPN装置は、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10乃至15のいずれかに記載の通信装置。

10

【0169】

(付記17)

基地局に接続されたコアネットワークと、無線LAN(Local Area Network)と、に第1の広域ネットワーク(Wide Area Network)を介して接続するデータセンタでは、

前記第1の広域ネットワークに接続され、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コアネットワークを有し、

前記無線LAN又は前記基地局への接続が選択自在とされ、前記データセンタに接続する端末が、前記第1の広域ネットワークとの間で接続しているネットワークに応じて、前記仮想コアネットワークでの前記端末に対するサービスを可変に制御する、通信方法。

20

【0170】

(付記18)

前記データセンタにおいて、

前記端末が前記基地局及び前記コアネットワークを介し前記第1の広域ネットワーク経由で前記データセンタに接続しているか、あるいは、前記端末が前記無線LAN及び前記第1の広域ネットワーク経由で前記データセンタに接続しているか、という前記端末が接続するネットワークの種別に対応して、

また、

前記端末が前記無線LAN及び前記第1の広域ネットワーク経由で前記データセンタに接続している場合には、前記無線LANのアクセスポイントが、前記データセンタを所持する事業者によって提供されたものであるか、あるいは、前記データセンタの前記事業者と異なる他の事業者によって提供されたものであるか、という前記端末が接続する無線LANの種別に対応して、

30

前記仮想コアネットワークで前記端末に提供する課金方式と通信品質サービスの少なくとも一方を可変に制御する、付記17記載の通信方法。

【0171】

(付記19)

前記端末が、前記無線LANを介し前記第1の広域ネットワーク経由で前記データセンタに接続する場合、前記端末と前記データセンタとの間を、前記無線LAN及び前記第1の広域ネットワーク経由のVPN(Virtual Private Network)で接続する、付記17又は18記載の通信方法。

40

【0172】

(付記20)

前記データセンタでは、

第1のゲートウェイが、前記第1の広域ネットワークに接続し、

第2のゲートウェイが、前記第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のゲートウェイは、前記仮想コアネットワークに接続され、

前記第1のゲートウェイと前記第2のゲートウェイ間のフィルタで、前記第1の広域ネットワークから入力されるパケットと、前記第2の広域ネットワークから入力されるパケ

50

ットの少なくとも一方のパケットのフィルタリングを行う、付記 19 記載の通信方法。

【0173】

(付記 21)

前記フィルタが、前記第 2 の広域ネットワーク側からの前記端末への着信やメッセージのアクセス拒否、許可を制御する、付記 20 記載の通信方法。

【0174】

(付記 22)

前記端末が、前記VPNから前記VPN装置及び前記仮想コアネットワークを経由し、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データを、前記データセンタの前記仮想コアネットワーク及び前記VPN装置から、前記VPNを介して受信する、付記 19 乃至 21 のいずれかに記載の通信方法。

10

【0175】

(付記 23)

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 19 乃至 22 のいずれかに記載の通信方法。

【0176】

(付記 24)

モバイルネットワークの基地局又は無線LAN (Local Area Network) と通信を行う手段と、

20

通話発信時に、前記モバイルネットワークの基地局を経由して通話するか、前記無線LANを経由して通話するかを選択可能な手段と、

を有する端末。

【0177】

(付記 25)

モバイルネットワークの基地局又は無線LAN (Local Area Network) との通信を行う手段と、

通話発信時に、前記モバイルネットワークの基地局を経由して通話するか、前記無線LANを経由して通話するかを選択可能な通話アプリケーションと、

を有する端末。

30

【0178】

(付記 26)

モバイルネットワークの基地局又は無線LANとの通信を行う手段と、

セットアップ時に、前記モバイルネットワークの基地局を経由して通話するか、前記無線LANを経由して通話するかを選択可能な手段と、

を有する端末。

【0179】

(付記 27)

前記無線LAN及び第 1 の広域ネットワークを介してデータセンタに接続する場合、前記データセンタとの間を、前記無線LAN及び前記第 1 の広域ネットワーク経由のVPN(Virtual Private Network)で接続する手段を備えた、付記 24 乃至 26 のいずれかに記載の端末。

40

【0180】

(付記 28)

無線LAN (Local Area Network) と、基地局に接続するコアネットワークとに第 1 の広域ネットワーク (Wide Area Network) を介して接続するデータセンタに配置されるコンピュータに、

コアネットワークの機能の少なくとも一部を仮想化し、前記第 1 の広域ネットワークに接続される仮想コアネットワークの処理と、

前記無線LAN又は前記基地局への接続が選択自在とされ、前記データセンタに接続する

50

端末が、前記第 1 の広域ネットワークとの間で接続しているネットワークに応じて、前記仮想コアネットワークでの記端末に対するサービスを可変に制御する処理と、
 を実行させる、プログラム。

【0181】

(付記 29)

前記端末が前記基地局及び前記コアネットワークを介し前記第 1 の広域ネットワーク経由で前記データセンタに接続しているか、あるいは、前記端末が前記無線LAN及び前記第 1 の広域ネットワーク経由で前記データセンタに接続しているか、という、前記端末が接続するネットワークの種別に対応して、

前記端末が前記無線LAN及び前記第 1 の広域ネットワーク経由で前記データセンタに接続している場合には、前記無線LANのアクセスポイントが、前記データセンタを所持する事業者によって提供されたものであるか、あるいは、前記データセンタの前記事業者と異なる他の事業者によって提供されたものであるか、という、前記端末が接続する無線LANの種別に対応して、

前記仮想コアネットワークで前記端末に提供する課金方式と通信品質サービスの少なくとも一方を可変に制御する処理を、前記コンピュータに実行させる、付記 28 記載のプログラム。

【0182】

(付記 30)

前記端末が、前記無線LANを介して前記データセンタに接続する場合、前記端末との間を、前記無線LAN及び前記第 1 の広域ネットワーク経由のVPN(Virtual Private Network)で接続する処理を、前記コンピュータに実行させる、付記 28 又は 29 記載のプログラム。

【0183】

(付記 31)

モバイルネットワークの基地局又は無線LAN (Local Area Network) と通信を行う処理と、

通話発信時に、前記モバイルネットワークの基地局を経由して通話するか、前記無線LANを経由して通話するかを選択可能とする処理を、端末のコンピュータに実行させる、プログラム。

【0184】

(付記 32)

モバイルネットワークの基地局又は無線LAN (Local Area Network) との通信を行う処理と、

セットアップ時に、前記モバイルネットワークの基地局を経由して通話するか、前記無線LANを経由して通話するかを選択可能とする処理を、端末のコンピュータに実行させるプログラム。

【符号の説明】

【0185】

1、1-1～1-3 端末 (UE)

10 基地局 (eNB)

11 表示部

20 EPC

21 SGW

22 PGW

23 MME

24 HSS

25 3GPP AAA

26 PCRF

27 ePDG

10

20

30

40

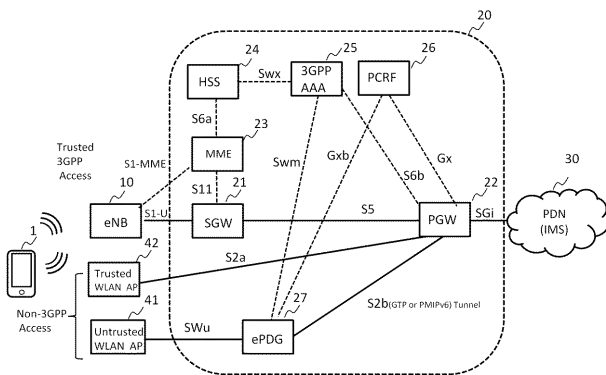
50

3 0	PDN	
3 1	WAN1	
3 2	WAN2	
4 0	WLAN	
4 1、4 2、4 3	無線LANアクセスポイント (WLAN AP)	
5 0	データセンタ (DC)	
5 1	第 1 のゲートウェイ (GW)	
5 2	仮想化EPC (vEPC)	
5 3	第 2 ゲートウェイ	
5 4	機能ブロック (フィルタ)	10
5 5	ネットワーク (仮想ネットワーク)	
5 6	制御装置	
5 7	サーバ	
5 8	物理スイッチ	
5 9	ネットワーク	
6 0	VPNトンネル	
1 0 1	VPN装置	
1 0 2	VPN設定部	
1 0 3	VPN情報記憶部	
1 0 4	VPN通信制御部	20
1 1 1	受話器マーク (アイコン)	
1 1 2	名簿 (氏名表示)	
1 1 3	電話番号	
1 1 4	電話アイコン	
1 1 5	Wi-Fi (登録商標) 電話アイコン	
1 1 6	設定画面 (ネットワーク設定画面)	
1 1 7	Wi-Fi (登録商標) 通信設定欄	
1 1 8	Wi-Fi (登録商標) 電話設定欄	
5 1 1	VPN装置	
5 1 2	VPN設定部	30
5 1 3	VPN情報記憶部	
5 1 4	VPN通信制御部	
5 2 2	PGW	
5 2 4	HSS	
5 2 5	3GPP AAA	
5 2 6	PCRF	
5 2 7	ePDG	
5 2 8	S2b (GTP/PMIPv6)	
5 2 9	フィルタ	
5 4 1	通信部	40
5 4 2	転送制御部	
5 4 3	フィルタ情報記憶部	
5 4 4	フィルタ情報設定部	
5 6 1	接続先ネットワーク判別部	
5 6 2	サービス制御部	
5 6 3	課金実施部	
5 6 4	通信品質制御部	
5 6 5	通信部	
5 7 1	仮想マシン	
5 7 2	アプリケーション	50

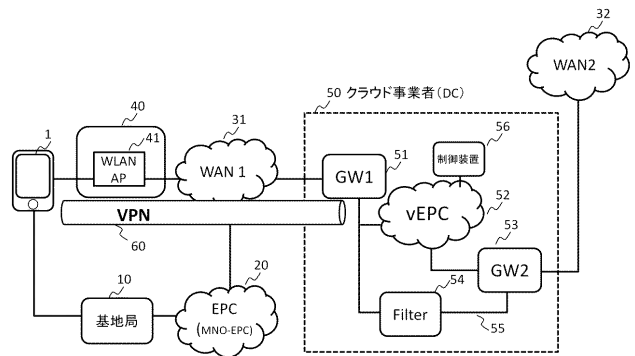
- | | |
|---------|--------------------|
| 5 7 3 | OS |
| 5 7 4 | ハイパーバイザ |
| 5 7 5 | 仮想NIC |
| 5 7 6 | 仮想スイッチ |
| 5 7 7 | 物理NIC |
| 1 0 0 1 | タッチパネル |
| 1 0 0 2 | タッチパネル入力・出力部 |
| 1 0 0 3 | アプリケーション |
| 1 0 0 4 | 制御部 |
| 1 0 0 5 | 記憶部（設定情報） |
| 1 0 0 6 | 3G/LTE通信モジュール |
| 1 0 0 7 | アンテナ |
| 1 0 0 8 | Wi-Fi（登録商標）通信モジュール |
| 1 0 0 9 | アンテナ |

10

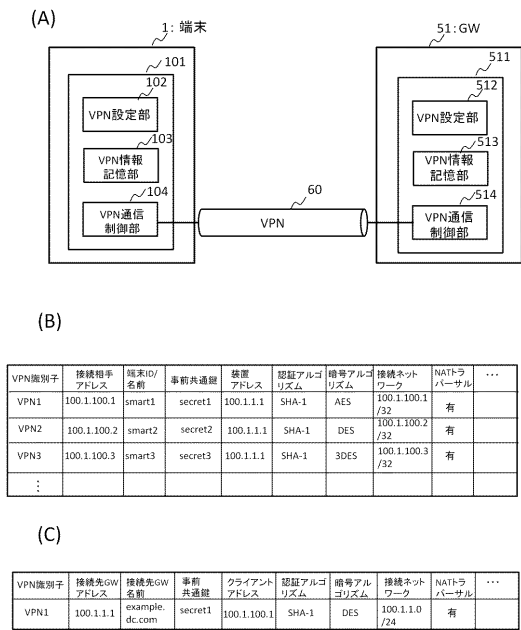
【 図 1 】



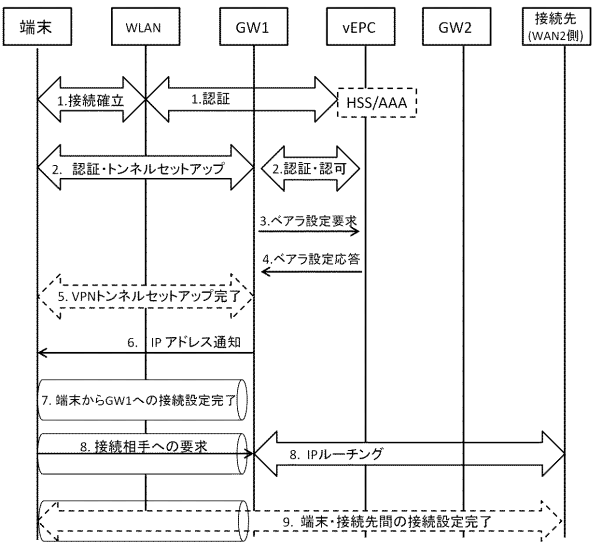
【図 2】



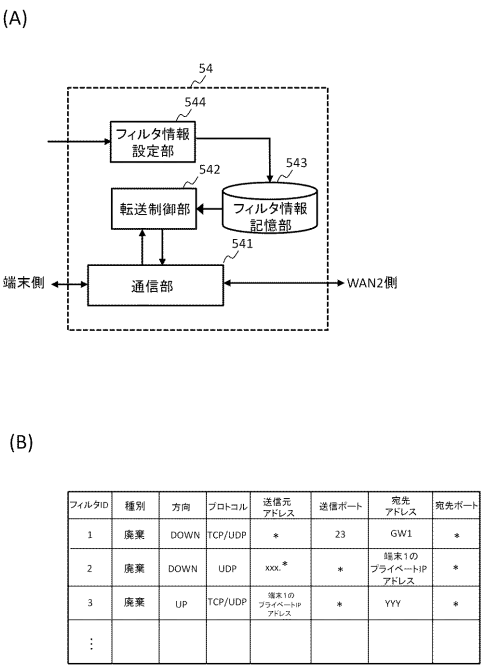
【図 3】



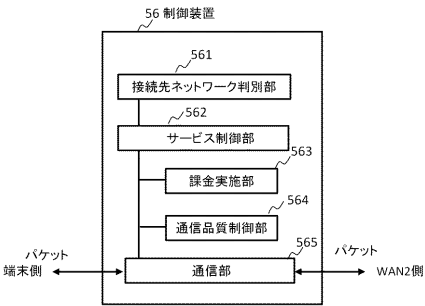
【図 4】



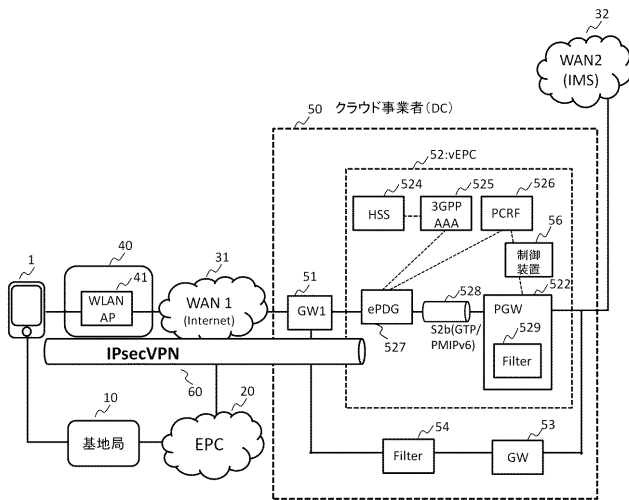
【図 5】



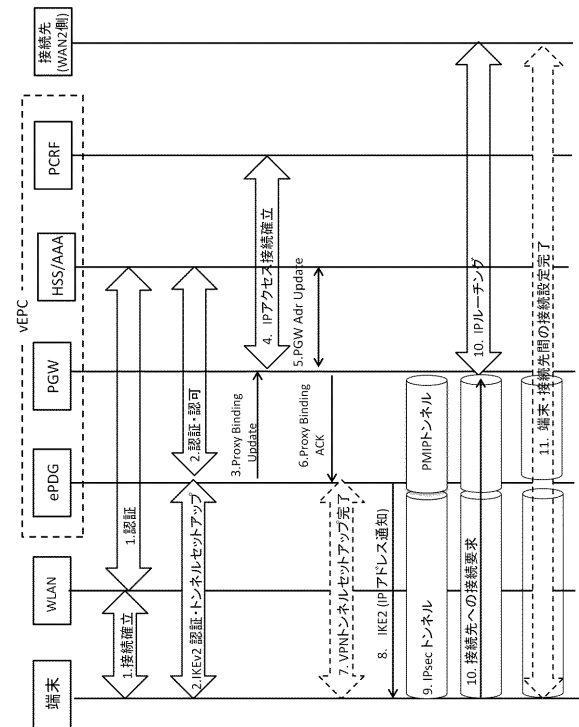
【図 6】



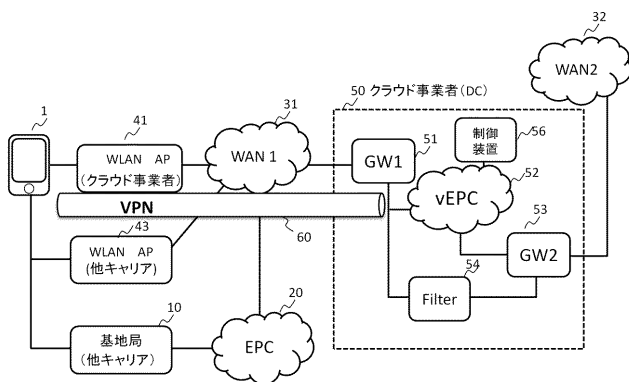
【図 7】



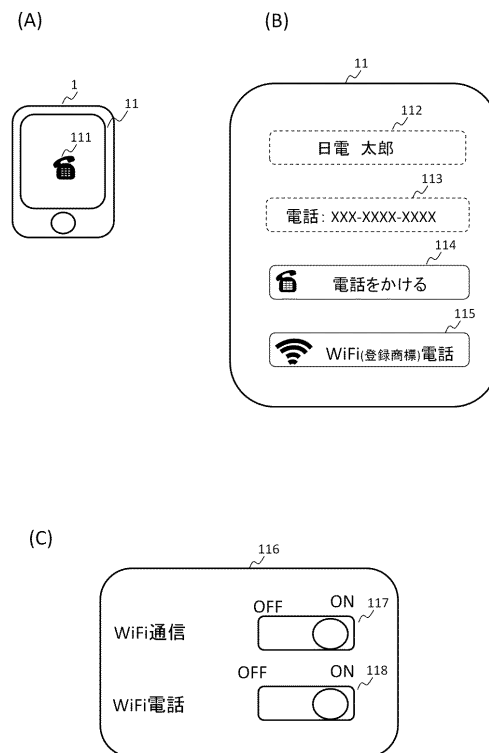
【図 8】



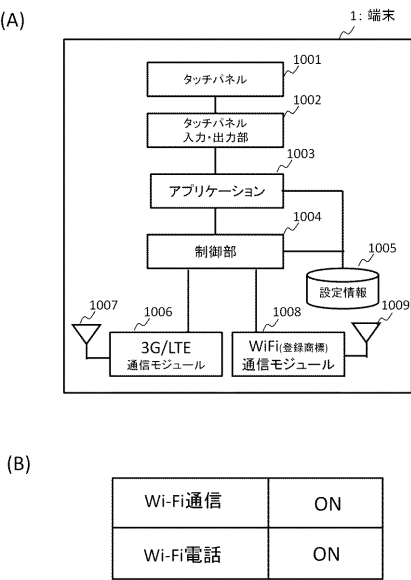
【図 9】



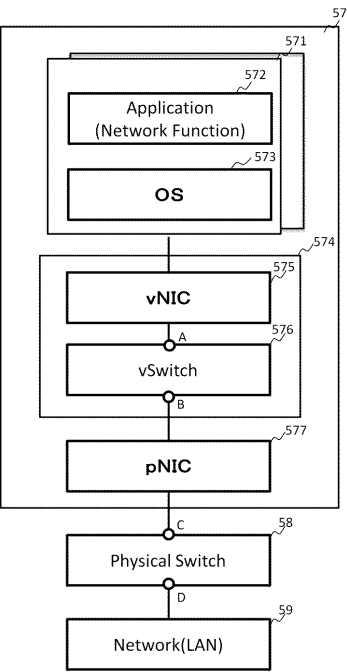
【図 10】



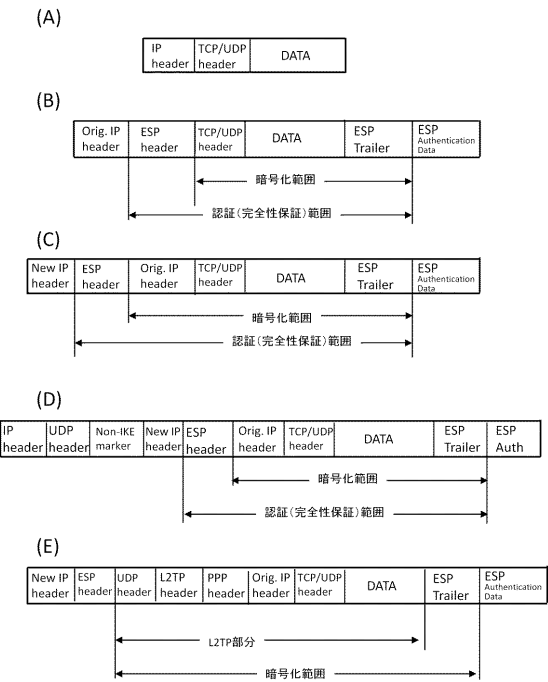
【図 1 1】



【図 1 2】



【図 1 3】



フロントページの続き

(72)発明者 中野 慎太郎

東京都港区芝五丁目7番1号 日本電気株式会社内

Fターム(参考) 5K067 DD29 EE02 EE16

5K201 AA01 BA20 DA02 EA07 EB07 EC05 EC07 ED04 FA02 FA07