(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
2020年2月13日(13.02.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/031752 A1

(51) 国際特許分類:
H04L 12/923 (2013.01) *H04L 12/70* (2013.01)

(21) 国際出願番号： PCT/JP2019/029423

(22) 国際出願日： 2019年7月26日(26.07.2019)

(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 2018-148840 2018年8月7日(07.08.2018) JP

(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 宮本 克真 (**MIYAMOTO, Katsuma**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 岡田 昭宏(**OKADA, Akihiro**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 土屋 英雄(**TSUCHIYA, Hideo**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP).

(74) 代理人: 特許業務法人酒井国際特許事務所 (**SAKAI INTERNATIONAL PATENT OFFICE**); 〒1000013 東京都千代田区霞が関３丁目８番１号 虎の門三井ビルディング Tokyo (JP).

(54) **Title:** MANAGEMENT DEVICE AND MANAGEMENT METHOD

(54) 発明の名称： 管理装置および管理方法

［図1］

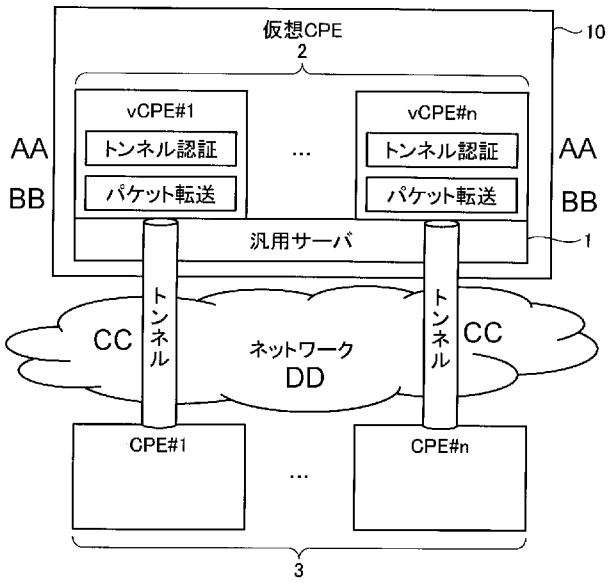


FIG. 1:
1 General-purpose server
2 Virtual CPE
AA Tunnel authentication
BB Packet transfer
CC Tunnel
DD Network

(57) **Abstract:** An acquisition unit (11a) acquires the state of a server where a plurality of virtual CPEs are constructed, and an instruction unit (11b) gives instructions to CPEs which have been connected to the virtual CPEs regarding control on a communication band in accordance with the state of the server. The instruction unit (11b) gives instructions to the CPEs which have been connected to the virtual CPEs so as to limit the communication band to a prescribed value or lower when the CPU use rate acquired by the acquisition unit (11a) exceeds a prescribed threshold value. The instruction unit

WO 2020/031752 A1

［続葉有］

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, 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：

一　国際調査報告（条約第21条(3)）

(11b) gives instructions to the CPEs which have been connected to the virtual CPEs so as to limit the communication band to the prescribed value or lower when the number of connections of the CPEs which have been connected to the virtual CPEs, the number being acquired by the acquisition unit (11a), decreases below a prescribed threshold value. The acquisition unit (11a) acquires the presence of CPEs not being connected to the virtual CPEs, and when there are CPEs that are not connected, the instruction unit (11b) give instructions to the CPEs which have been connected to the virtual CPEs so as to disable communication of a communication type other than a prescribed communication type.

(57) 要約：取得部（１１ａ）が、複数の仮想ＣＰＥが構築されたサーバの状態を取得し、指示部（１１ｂ）が、仮想ＣＰＥと接続済のＣＰＥに、サーバの状態に応じて、通信帯域の制御を指示する。指示部（１１ｂ）は、取得部（１１ａ）が取得したＣＰＵ使用率が所定の閾値を超えた場合に、仮想ＣＰＥと接続済のＣＰＥに、通信帯域を所定値以下に制限することを指示する。指示部（１１ｂ）は、取得部（１１ａ）が取得した仮想ＣＰＥと接続済のＣＰＥのコネクション数が所定の閾値を下回った場合に、仮想ＣＰＥと接続済のＣＰＥに、通信帯域を所定値以下に制限することを指示する。取得部（１１ａ）が仮想ＣＰＥと未接続のＣＰＥの有無を取得し、指示部（１１ｂ）が、未接続のＣＰＥが有る場合に、仮想ＣＰＥと接続済のＣＰＥに、所定の通信種別以外の通信種別の通信の遮断を指示する。

明　細　書

発明の名称 ： 管理装置および管理方法

技術分野

[0001] 本発明は、管理装置および管理方法に関する。

背景技術

[0002] 従来、顧客宅内設備（ＣＰＥ、Customer Premises Equipment）の機能を、仮想ＣＰＥ（ｖＣＰＥ）としてコアネットワークの仮想化基盤で集約する技術が知られている（非特許文献１参照）。各仮想ＣＰＥは、ユーザ宅内のＣＰＥと、ＩＰｓｅｃ（ＩＰ SECurity Architecture、非特許文献２参照）等の通信方式で構築されるトンネルによって接続される。

[0003] ＩＰｓｅｃでは、通信開始時には「トンネル認証処理」が行われ、通信中には「パケット転送処理」が行われる。これらの処理は、ルータではそれぞれの専用ハードウェアによって実行され、汎用サーバ等ではＣＰＵ（Central Processing Unit）等のサーバ上のリソースによって実行される。

先行技術文献

非特許文献

[0004] 非特許文献1：“ETSI GS NFV 001 V1.1.1(2013-10) Network Functions Virtualization (NFV); Use Cases”、[online]、ETSI、[平成30年7月11日検索]、インターネット＜URL：http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf＞

非特許文献2：“IPsecの概要”、[online]、YAMAHA Corporation、[平成30年7月11日検索]、インターネット＜URL：http://www.rtpro.yamaha.co.jp/RT/docs/ipsec/abst.html＞

発明の概要

発明が解決しようとする課題

[0005] しかしながら、従来の技術では、複数の仮想ＣＰＥが構築されたサーバにおいてトンネル接続要求が集中した場合には、トンネル確立が遅延する場合

があった。例えば、大規模停電からの復旧時等に多数のＣＰＥが同一のサーバ上のｖＣＰＥに一斉に再接続を要求すると、サーバでは、各ｖＣＰＥとの間で一斉に「トンネル認証処理」が行われる。

[0006] その場合に、多数の接続済のＣＰＥが通信を行うと、ｖＣＰＥが構築されているサーバでは、「パケット転送処理」によって処理負荷が高くなり、再接続を要求している他のＣＰＥの「トンネル認証処理」の実行が遅くなるので、トンネル確立が遅延する。トンネル確立が遅延するとタイムアウトしてしまうので、サーバ全体として復旧に時間がかかることになる。

[0007] 本発明は、上記に鑑みてなされたものであって、複数の仮想ＣＰＥが構築されたサーバにおいてトンネル接続要求が集中した場合に、トンネル確立の遅延を抑止することを目的とする。

課題を解決するための手段

[0008] 上述した課題を解決し、目的を達成するために、本発明に係る管理装置は、複数の仮想ＣＰＥが構築されたサーバの状態を取得する取得部と、前記仮想ＣＰＥと接続済のＣＰＥに、前記サーバの状態に応じて、通信帯域の制御を指示する指示部と、を備えることを特徴とする。

発明の効果

[0009] 本発明によれば、複数の仮想ＣＰＥが構築されたサーバにおいてトンネル接続要求が集中した場合にも、トンネル確立の遅延を抑止することができる。

図面の簡単な説明

[0010] [図1]図１は、本実施形態に係る管理装置の処理対象のシステムの構成を例示する模式図である。

[図2]図２は、管理装置の処理対象のシステムを説明するための説明図である。

[図3]図３は、管理装置の処理対象のシステムを説明するための説明図である。

[図4]図４は、管理装置の概略構成を例示する模式図である。

[図5]図５は、管理装置の処理を説明するための説明図である。

[図6]図６は、管理処理手順を例示するフローチャートである。

[図7]図７は、管理プログラムを実行するコンピュータの一例を示す図である。

発明を実施するための形態

[0011] 以下、図面を参照して、本発明の実施形態を詳細に説明する。なお、この実施形態により本発明が限定されるものではない。また、図面の記載において、同一部分には同一の符号を付して示している。

[0012] ［システム構成］

まず、図１は、本実施形態に係る管理装置の処理対象のシステムの構成を例示する模式図である。図１に示すように、管理装置の処理対象のシステムは、汎用サーバ１上に構築された複数の仮想ＣＰＥ２（ｖＣＰＥ＃１、…、ｖＣＰＥ＃ｎ）と、ユーザ宅内のＣＰＥ３（ＣＰＥ＃１、…、ＣＰＥ＃ｎ）とを含む。汎用サーバ１上の各仮想ＣＰＥ２は、各ＣＰＥ３に対応して構築される。

[0013] ユーザ宅内のＣＰＥ３と、これに対応する仮想ＣＰＥ２とは、ＩＰｓｅｃ等によってネットワーク内に作成されたトンネルで接続される。図１に示した例では、ｖＣＰＥ＃１とＣＰＥ＃１とがトンネルで接続され、ｖＣＰＥ＃ｎとＣＰＥ＃ｎとがトンネルで接続される。

[0014] ここで、図２および図３は、管理装置の処理対象のシステムを説明するための説明図である。まず、図２に示すように、ＩＰｓｅｃでは、トンネル認証処理とパケット転送処理を経て通信が行われる。

[0015] トンネル認証処理は、ＩＫＥ（Internet Key Exchange）と呼ばれる鍵交換プロトコルで実行される。このトンネル認証処理には、ＩＰｓｅｃの通信に用いる鍵情報を安全に運ぶための制御用トンネルを作成するフェーズ１と、制御用トンネル内で通信に用いる通信用トンネルを作成するフェーズ２とが含まれる。

[0016] また、パケット転送処理では、トンネル認証処理で作成された通信用トン

ネルを用いて通信が行われる。通信用トンネルは、上り通信用と下り通信用との２つのトンネルが対になったトンネルである。また、ＩＰｓｅｃの通信では、トンネル認証処理で交換された鍵を用いた暗号通信が行われる。

[0017] また、図３に示すように、複数の仮想ＣＰＥ２が構築された汎用サーバ１は、仮想ＣＰＥ２と未接続のＣＰＥ３（ＣＰＥ＃ｎ）に対してはトンネル認証処理を行ってトンネルで接続し、通信可能な接続済の状態にする。また、汎用サーバ１は、トンネル認証処理を経て接続済となったＣＰＥ３（ＣＰＥ＃１）との間では、パケット転送処理によって通信が行われる。

[0018] 管理装置１０は、複数の仮想ＣＰＥ２が構築された汎用サーバ１に実装される。ただし、本発明は汎用サーバ１に実装される場合に限定されず、例えば、汎用サーバ１と通信可能に構成された異なるハードウェアに実装されてもよい。

[0019] 管理装置１０は、例えば、複数のＣＰＥ３が一斉に切断された場合、複数のＣＰＥ３が一斉にトンネル接続を要求した場合、あるいはオペレータの判断により手動で、後述する管理処理を実行する。具体的には、管理装置１０は、接続済のＣＰＥ３に対して汎用サーバ１の状態に応じた通信帯域の制御を指示する。管理装置１０は、これにより、汎用サーバ１の状態に応じて動的に、接続済のＣＰＥ３（ＣＰＥ＃１）との間のパケット転送処理の帯域を制限し、未接続のＣＰＥ３（ＣＰＥ＃ｎ）に対するトンネル認証処理を優先的に行えるようにする。

[0020] ［管理装置の構成］

次に、図４は、本実施形態の管理装置の概略構成を例示する模式図である。図４に示すように、本実施形態に係る管理装置１０は、ＣＰＵ（Central Processing Unit）やＦＰＧＡ（Field Programmable Gate Array）等で実現され、メモリに記憶された処理プログラムを実行して、制御部１１として機能する。また、管理装置１０は、ＲＡＭ、フラッシュメモリ等の半導体メモリ素子で実現される記憶部１２を備える。

[0021] 記憶部１２は、帯域情報１２ａを記憶する。帯域情報１２ａは、汎用サー

バ１の状態と通信帯域とを対応づけた情報であり、後述する管理処理において、指示部１１ｂが参照する。帯域情報１２ａは、例えば、不図示のキーボード等の入力部を介して、予め記憶部１２に記憶される。

[0022] 制御部１１は、図４に例示するように、取得部１１ａおよび指示部１１ｂとして機能する。なお、これらの機能部は、それぞれが異なるハードウェアに実装されてもよい。

[0023] 取得部１１ａは、複数の仮想ＣＰＥ２が構築された汎用サーバ１の状態を取得する。例えば、取得部１１ａは、汎用サーバ１の状態として、汎用サーバ１のＣＰＵ使用率、トラヒック量、汎用サーバ１に構築された仮想ＣＰＥ２と接続済のＣＰＥ３のコネクション数、または、汎用サーバ１に構築された仮想ＣＰＥ２と未接続のＣＰＥ３の有無等を取得する。

[0024] 指示部１１ｂは、仮想ＣＰＥ２と接続済のＣＰＥ３に、汎用サーバ１の状態に応じて、通信帯域の制御を指示する。具体的には、指示部１１ｂは、取得部１１ａが取得した汎用サーバ１の状態と帯域情報１２ａとを対比して、仮想ＣＰＥ２と、これと接続済みのＣＰＥ３とに対し、通信帯域の制御（帯域制御）を指示する。

[0025] ここで、図５は、管理装置の処理を説明するための説明図である。図５には、大規模停電が復旧した場合に、停電が復旧したエリアに設置された多数のＣＰＥ３（ＣＰＥ＃１、…、ＣＰＥ＃ｎ）から、同一の汎用サーバ１の仮想ＣＰＥ２（ｖＣＰＥ＃１、…、ｖＣＰＥ＃ｎ）に、一斉に再接続の要求があった場合が例示されている。

[0026] 管理装置１０では、例えば、取得部１１ａが、汎用サーバ１のＣＰＵ使用率を取得したときには、指示部１１ｂは、汎用サーバ１のＣＰＵ使用率が所定の閾値を超えた場合に、仮想ＣＰＥ２（ｖＣＰＥ＃１）と、これと接続済のＣＰＥ３（ＣＰＥ＃１）とに、通信帯域を所定値以下に制限することを指示する。

[0027] この場合には、帯域情報１２ａには、例えば、ＣＰＵ使用率が高いほど、通信帯域の所定値が小さくなるように、複数段階に分類したＣＰＵ使用率の

段階ごとに、異なる通信帯域の所定値を設定しておく。指示部１１ｂは、帯域情報１２ａを参照し、取得部１１ａが取得したＣＰＵ使用率に対応する通信帯域の所定値を、仮想ＣＰＥ２（ｖＣＰＥ＃１）と、これと接続済のＣＰＥ３（ＣＰＥ＃１）とに通知する。

[0028] 帯域制御を指示された場合に、ユーザ宅内のＣＰＥ３（ＣＰＥ＃１）が、上りパケットの通信帯域を指示された所定値に制限する。また、仮想ＣＰＥ２（ｖＣＰＥ＃１）が、下りパケットの通信帯域を指示された所定値に制限する。

[0029] これにより、汎用サーバ１では、ＣＰＵ使用率が高い場合に、接続済のＣＰＥ３との間の「パケット転送処理」が制限される。そのため、未接続のＣＰＥ３との間の「トンネル認証処理」を優先して行える。したがって、トンネル確立の遅延によるタイムアウトを抑止できるので、汎用サーバ１全体として、停電からの復旧が早くなる。

[0030] なお、汎用サーバ１の状態として、汎用サーバ１のＣＰＵ使用率の代わりに汎用サーバ１のトラヒック量を用いてもよい。すなわち、取得部１１ａが、汎用サーバ１のトラヒック量を、汎用サーバ１の状態として取得して、指示部１１ｂが、トラヒック量が所定の閾値を超えた場合に、仮想ＣＰＥと接続済のＣＰＥに、通信帯域を所定値以下に制限することを指示する。この場合には、帯域情報１２ａには、例えば、トラヒック量が多いほど、通信帯域の所定値が小さくなるように、複数段階に分類したトラヒック量の段階ごとに、異なる通信帯域の所定値を設定しておけばよい。

[0031] また、取得部１１ａが、汎用サーバ１に構築された仮想ＣＰＥ２と接続済のＣＰＥ３の数（コネクション数）を取得したときには、指示部１１ｂは、コネクション数が所定の閾値を下回った場合に、仮想ＣＰＥ２と接続済のＣＰＥ３（ＣＰＥ＃１）に、通信帯域を所定値以下に制限することを指示する。

[0032] この場合には、帯域情報１２ａには、例えば、コネクション数が少ないほど、通信帯域の所定値が小さくなるように、複数段階に分類したコネクショ

ン数の段階ごとに、異なる通信帯域の所定値を設定しておく。指示部１１ｂは、帯域情報１２ａを参照し、取得部１１ａが取得したコネクション数に対応する通信帯域の所定値を、仮想ＣＰＥ２（ｖＣＰＥ＃１）と接続済のＣＰＥ３（ＣＰＥ＃１）とに通知する。これにより、汎用サーバ１では、ＣＰＥ３のコネクション数が少ない場合に、接続済のＣＰＥ３との間の「パケット転送処理」が制限され、未接続のＣＰＥ３との間の「トンネル認証処理」を優先して行える。

[0033] また、取得部１１ａが、汎用サーバ１に構築された仮想ＣＰＥ２と未接続のＣＰＥ３の有無を取得したときには、指示部１１ｂは、仮想ＣＰＥ２と未接続のＣＰＥ３が有る場合に、仮想ＣＰＥ２と接続済のＣＰＥ３（ＣＰＥ＃１）に、所定の通信種別以外の通信種別の通信の遮断を指示する。

[0034] すなわち、例えば、停電が復旧して再接続中のＣＰＥ３（ＣＰＥ＃ｎ）がある間には、指示部１１ｂは、接続済のＣＰＥ３（ＣＰＥ＃１）には、ＶｏＩＰ等の特定の通信種別の通信のみを許可し、それ以外の通信種別の通信は遮断させる。また、指示部１１ｂは、全ＣＰＥ３のトンネル認証処理が完了して停電復旧した場合には、全ての通信種別の通信を許可する。

[0035] この場合には、帯域情報１２ａには、例えば、特定の通信種別以外の通信の通信帯域を０に設定しておく。指示部１１ｂは、取得部１１ａが仮想ＣＰＥ２と未接続のＣＰＥ３が有るとの情報を取得した場合に、帯域情報１２ａを参照し、仮想ＣＰＥ２（ｖＣＰＥ＃１）と接続済のＣＰＥ３（ＣＰＥ＃１）とに、通信を許可する通信種別と、それ以外の通信種別の通信の帯域を０にする指示とを通知する。これにより、汎用サーバ１では、未接続のＣＰＥ３が有る場合に、特定の通信種別以外の通信を遮断して、未接続のＣＰＥ３との間の「トンネル認証処理」を優先して行える。

[0036] ［管理処理］

次に、図６は、管理処理手順を例示するフローチャートである。図６に示すフローチャートは、例えば、所定の間隔で定期的に、あるいは、オペレータが指示したタイミングで開始される。

[0037] まず、取得部１１ａが、複数の仮想ＣＰＥ２が構築された汎用サーバ１の状態を取得する（ステップＳ１）。例えば、取得部１１ａは、汎用サーバ１のＣＰＵ使用率、トラヒック量、汎用サーバ１に構築された仮想ＣＰＥ２と接続済のユーザ宅内のＣＰＥ３のコネクション数、または汎用サーバ１に構築された仮想ＣＰＥ２と未接続のＣＰＥ３の有無等を取得する。

[0038] 次に、指示部１１ｂが、仮想ＣＰＥ２と接続済のＣＰＥ３に、汎用サーバ１の状態に応じて、通信帯域の制御を指示する（ステップＳ２）。具体的には、指示部１１ｂは、取得部１１ａが取得した汎用サーバ１の状態と帯域情報１２ａと対比して、仮想ＣＰＥ２と、これと接続済みのＣＰＥ３とに対し、帯域制御を指示する。

[0039] 例えば、指示部１１ｂは、汎用サーバ１のＣＰＵ使用率が所定の閾値を超えた場合に、仮想ＣＰＥ２と、これと接続済のＣＰＥ３とに、通信帯域を所定値以下に制限することを指示する。

[0040] または、指示部１１ｂは、汎用サーバ１のトラヒック量が所定の閾値を超えた場合に、仮想ＣＰＥと接続済のＣＰＥに、通信帯域を所定値以下に制限することを指示する。

[0041] または、指示部１１ｂは、汎用サーバ１に構築された仮想ＣＰＥ２と接続済のＣＰＥ３のコネクション数が所定の閾値を下回った場合に、仮想ＣＰＥ２と接続済のＣＰＥ３に、通信帯域を所定値以下に制限することを指示する。

[0042] または、指示部１１ｂは、仮想ＣＰＥ２と未接続のＣＰＥ３が有る場合に、仮想ＣＰＥ２と接続済のＣＰＥ３に、所定の通信種別以外の通信種別の通信の遮断を指示する。

[0043] 帯域制御を指示されたユーザ宅内のＣＰＥ３は、上りパケットの通信帯域を指示された所定値に制限する。また、仮想ＣＰＥ２（ｖＣＰＥ＃１）は、下りパケットの通信帯域を指示された所定値に制限する。これにより、一連の管理処理が終了する。

[0044] 以上、説明したように、本実施形態の管理装置１０では、取得部１１ａが

、複数の仮想ＣＰＥ２が構築された汎用サーバ１の状態を取得する。また、指示部１１ｂが、仮想ＣＰＥ２と接続済のＣＰＥ３に、汎用サーバ１の状態に応じて、通信帯域の制御を指示する。

[0045] これにより、これにより、汎用サーバ１の状態に応じて動的に、接続済のＣＰＥ３との間のパケット転送処理を制限し、未接続のＣＰＥ３に対するトンネル認証処理を優先的に行える。例えば、複数の仮想ＣＰＥが構築された汎用サーバ１においてトンネル接続要求が集中した場合に、「トンネル認証処理」を「パケット転送処理」より優先して実行することができる。したがって、トンネル確立の遅延によるタイムアウトを抑止することができるので、汎用サーバ１全体として例えば大規模停電からの復旧が早期に可能となる。

[0046] また、取得部１１ａが汎用サーバ１のＣＰＵ使用率を、汎用サーバ１の状態として取得したときには、指示部１１ｂは、帯域情報１２ａを参照し、ＣＰＵ使用率が所定の閾値を超えた場合に、仮想ＣＰＥ２と接続済のＣＰＥ３に、通信帯域を所定値以下に制限することを指示する。これにより、これにより、汎用サーバ１では、ＣＰＵ使用率が高い場合に、接続済のＣＰＥ３との間の「パケット転送処理」が制限され、未接続のＣＰＥとの間の「トンネル認証処理」を優先して行える。

[0047] また、取得部１１ａが、汎用サーバ１に構築された仮想ＣＰＥ２と接続済のＣＰＥ３のコネクション数を、汎用サーバ１の状態として取得したときには、指示部１１ｂは、コネクション数が所定の閾値を下回った場合に、仮想ＣＰＥ２と接続済のＣＰＥ３に、通信帯域を所定値以下に制限することを指示する。これにより、汎用サーバ１では、ＣＰＥ３のコネクション数が少ない場合に、接続済のＣＰＥ３との間の「パケット転送処理」が制限され、未接続のＣＰＥとの間の「トンネル認証処理」を優先して行える。

[0048] また、取得部１１ａが、汎用サーバ１に構築された仮想ＣＰＥ２と未接続のＣＰＥ３の有無を、汎用サーバ１の状態として取得したときには、指示部１１ｂは、仮想ＣＰＥ２と未接続のＣＰＥ３が有る場合に、仮想ＣＰＥ２と

接続済のＣＰＥ３に、所定の通信種別以外の通信種別の通信の遮断を指示する。これにより、汎用サーバ１では、未接続のＣＰＥ３が有る場合に、特定の通信種別以外の通信を遮断して、未接続のＣＰＥ３との間の「トンネル認証処理」を優先して行える。

[0049] ［プログラム］

上記実施形態に係る管理装置１０が実行する処理をコンピュータが実行可能な言語で記述したプログラムを作成することもできる。一実施形態として、管理装置１０は、パッケージソフトウェアやオンラインソフトウェアとして上記の管理処理を実行する管理プログラムを所望のコンピュータにインストールさせることによって実装できる。例えば、上記の管理プログラムを情報処理装置に実行させることにより、情報処理装置を管理装置１０として機能させることができる。ここで言う情報処理装置には、デスクトップ型またはノート型のパーソナルコンピュータが含まれる。また、その他にも、情報処理装置にはスマートフォン、携帯電話機等の移動体通信端末、さらには、ＰＤＡ（Personal Digital Assistants）等のスレート端末などがその範疇に含まれる。また、管理装置１０の機能を、クラウドサーバに実装してもよい。

[0050] 図７は、管理プログラムを実行するコンピュータの一例を示す図である。コンピュータ１０００は、例えば、メモリ１０１０と、ＣＰＵ１０２０と、ハードディスクドライブインタフェース１０３０と、ディスクドライブインタフェース１０４０と、シリアルポートインタフェース１０５０と、ビデオアダプタ１０６０と、ネットワークインタフェース１０７０とを有する。これらの各部は、バス１０８０によって接続される。

[0051] メモリ１０１０は、ＲＯＭ（Read Only Memory）１０１１およびＲＡＭ１０１２を含む。ＲＯＭ１０１１は、例えば、ＢＩＯＳ（Basic Input Output System）等のブートプログラムを記憶する。ハードディスクドライブインタフェース１０３０は、ハードディスクドライブ１０３１に接続される。ディスクドライブインタフェース１０４０は、ディスクドライブ１０４１に

接続される。ディスクドライブ１０４１には、例えば、磁気ディスクや光ディスク等の着脱可能な記憶媒体が挿入される。シリアルポートインタフェース１０５０には、例えば、マウス１０５１およびキーボード１０５２が接続される。ビデオアダプタ１０６０には、例えば、ディスプレイ１０６１が接続される。

[0052] ここで、ハードディスクドライブ１０３１は、例えば、ＯＳ１０９１、アプリケーションプログラム１０９２、プログラムモジュール１０９３およびプログラムデータ１０９４を記憶する。上記実施形態で説明した各情報は、例えばハードディスクドライブ１０３１やメモリ１０１０に記憶される。

[0053] また、管理プログラムは、例えば、コンピュータ１０００によって実行される指令が記述されたプログラムモジュール１０９３として、ハードディスクドライブ１０３１に記憶される。具体的には、上記実施形態で説明した管理装置１０が実行する各処理が記述されたプログラムモジュール１０９３が、ハードディスクドライブ１０３１に記憶される。

[0054] また、管理プログラムによる情報処理に用いられるデータは、プログラムデータ１０９４として、例えば、ハードディスクドライブ１０３１に記憶される。そして、ＣＰＵ１０２０が、ハードディスクドライブ１０３１に記憶されたプログラムモジュール１０９３やプログラムデータ１０９４を必要に応じてＲＡＭ１０１２に読み出して、上述した各手順を実行する。

[0055] なお、管理プログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ハードディスクドライブ１０３１に記憶される場合に限られず、例えば、着脱可能な記憶媒体に記憶されて、ディスクドライブ１０４１等を介してＣＰＵ１０２０によって読み出されてもよい。あるいは、管理プログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ＬＡＮやＷＡＮ（Wide Area Network）等のネットワークを介して接続された他のコンピュータに記憶され、ネットワークインタフェース１０７０を介してＣＰＵ１０２０によって読み出されてもよい。

[0056] 以上、本発明者によってなされた発明を適用した実施形態について説明し

たが、本実施形態による本発明の開示の一部をなす記述および図面により本発明は限定されることはない。すなわち、本実施形態に基づいて当業者等によりなされる他の実施形態、実施例および運用技術等は全て本発明の範疇に含まれる。

符号の説明

[0057] １　汎用サーバ

２　仮想ＣＰＥ

３　ＣＰＥ

１０　管理装置

１１　制御部

１１ａ　取得部

１１ｂ　指示部

１２　記憶部

１２ａ　帯域情報

請求の範囲

[請求項1] 複数の仮想ＣＰＥ（Customer Premises Equipment）が構築されたサーバの状態を取得する取得部と、

前記仮想ＣＰＥと接続済のＣＰＥに、前記サーバの状態に応じて、通信帯域の制御を指示する指示部と、

を備えることを特徴とする管理装置。

[請求項2] 前記取得部は、前記サーバのＣＰＵ使用率を、前記サーバの状態として取得し、

前記指示部は、前記ＣＰＵ使用率が所定の閾値を超えた場合に、前記仮想ＣＰＥと接続済のＣＰＥに、通信帯域を所定値以下に制限することを指示する

ことを特徴とする請求項１に記載の管理装置。

[請求項3] 前記取得部は、前記サーバに構築された前記仮想ＣＰＥと接続済のＣＰＥのコネクション数を、前記サーバの状態として取得し、

前記指示部は、前記コネクション数が所定の閾値を下回った場合に、前記仮想ＣＰＥと接続済のＣＰＥに、通信帯域を所定値以下に制限することを指示する

ことを特徴とする請求項１に記載の管理装置。

[請求項4] 前記取得部は、前記サーバに構築された前記仮想ＣＰＥと未接続のＣＰＥの有無を、前記サーバの状態として取得し、

前記指示部は、前記仮想ＣＰＥと未接続のＣＰＥが有る場合に、前記仮想ＣＰＥと接続済のＣＰＥに、所定の通信種別以外の通信種別の通信の遮断を指示する

ことを特徴とする請求項１に記載の管理装置。

[請求項5] 管理装置で実行される管理方法であって、

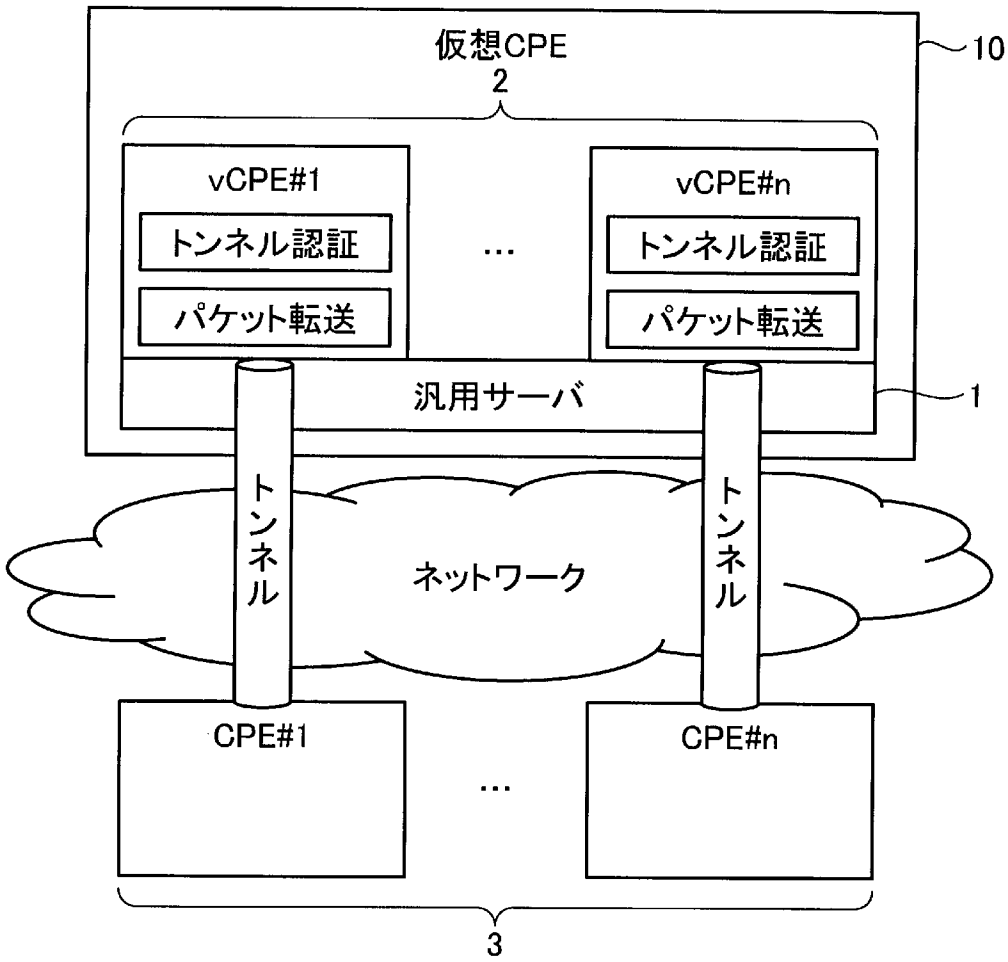
複数の仮想ＣＰＥが構築されたサーバの状態を取得する取得工程と、

前記仮想ＣＰＥと接続済のＣＰＥに、前記サーバの状態に応じて、

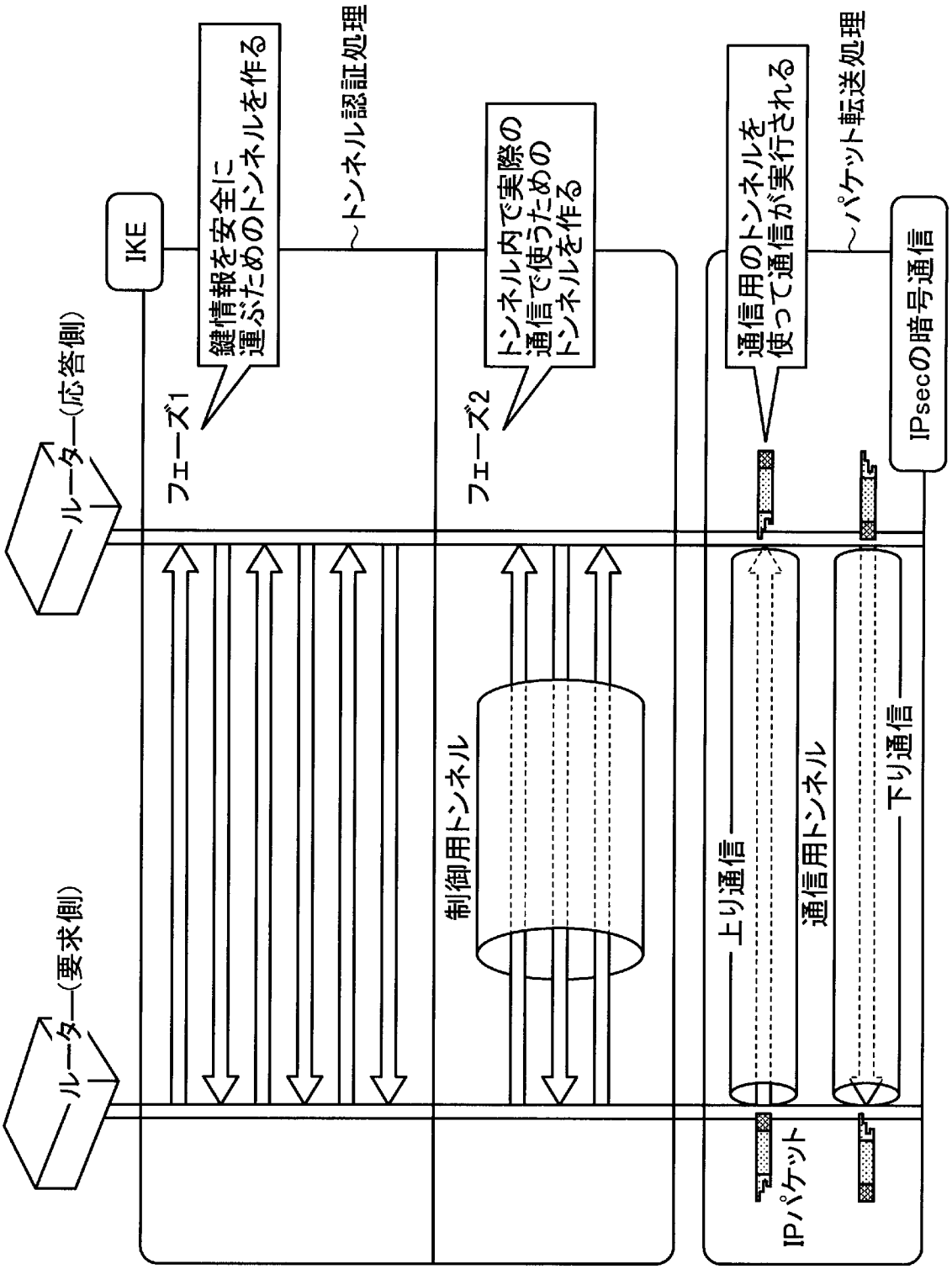
通信帯域の制御を指示する指示工程と、

を含んだことを特徴とする管理方法。

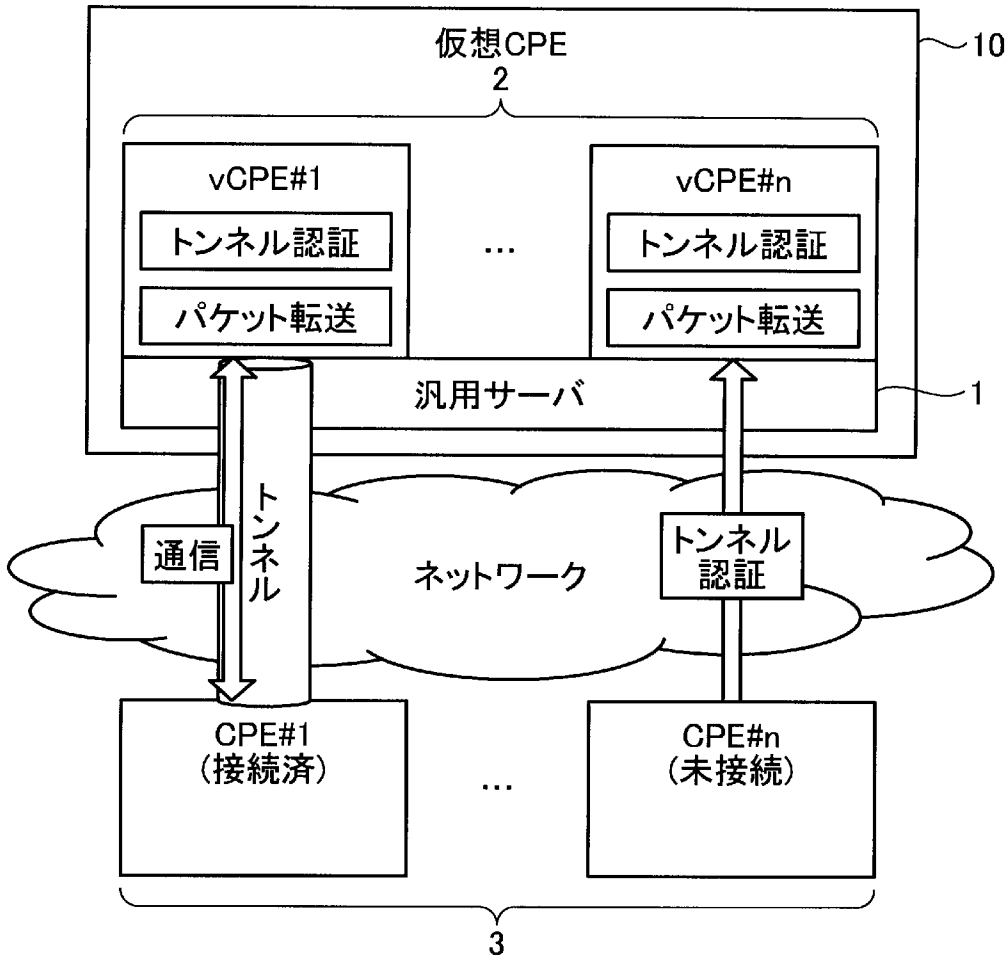
[図1]


仮想CPE
2
10
vCPE#1
トンネル認証
パケット転送
...
vCPE#n
トンネル認証
パケット転送
汎用サーバ
1
トンネル
トンネル
ネットワーク
CPE#1
...
CPE#n
3

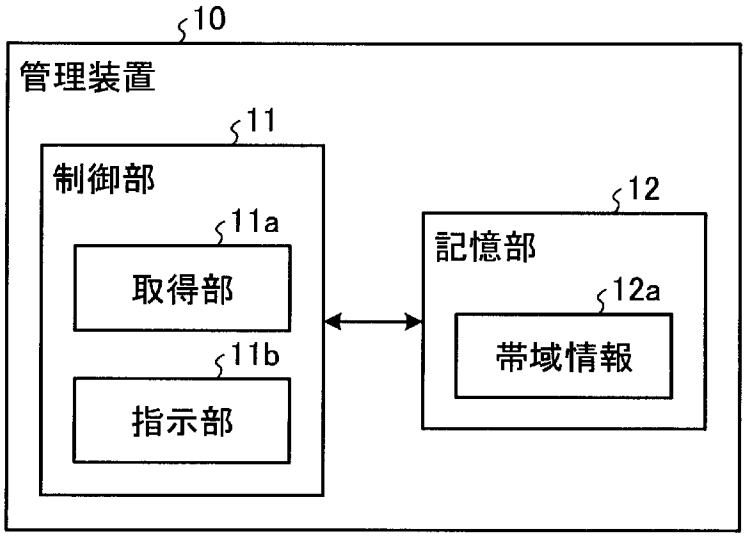
[図2]


ルータ(要求側)
ルータ(応答側)
IKE
フェーズ1
鍵情報を安全に運ぶためのトンネルを作る
トンネル認証処理
フェーズ2
トンネル内で実際の通信で使うためのトンネルを作る
通信用のトンネルを使って通信が実行される
パケット転送処理
IPsecの暗号通信
制御用トンネル
上り通信
通信用トンネル
下り通信
IPパケット

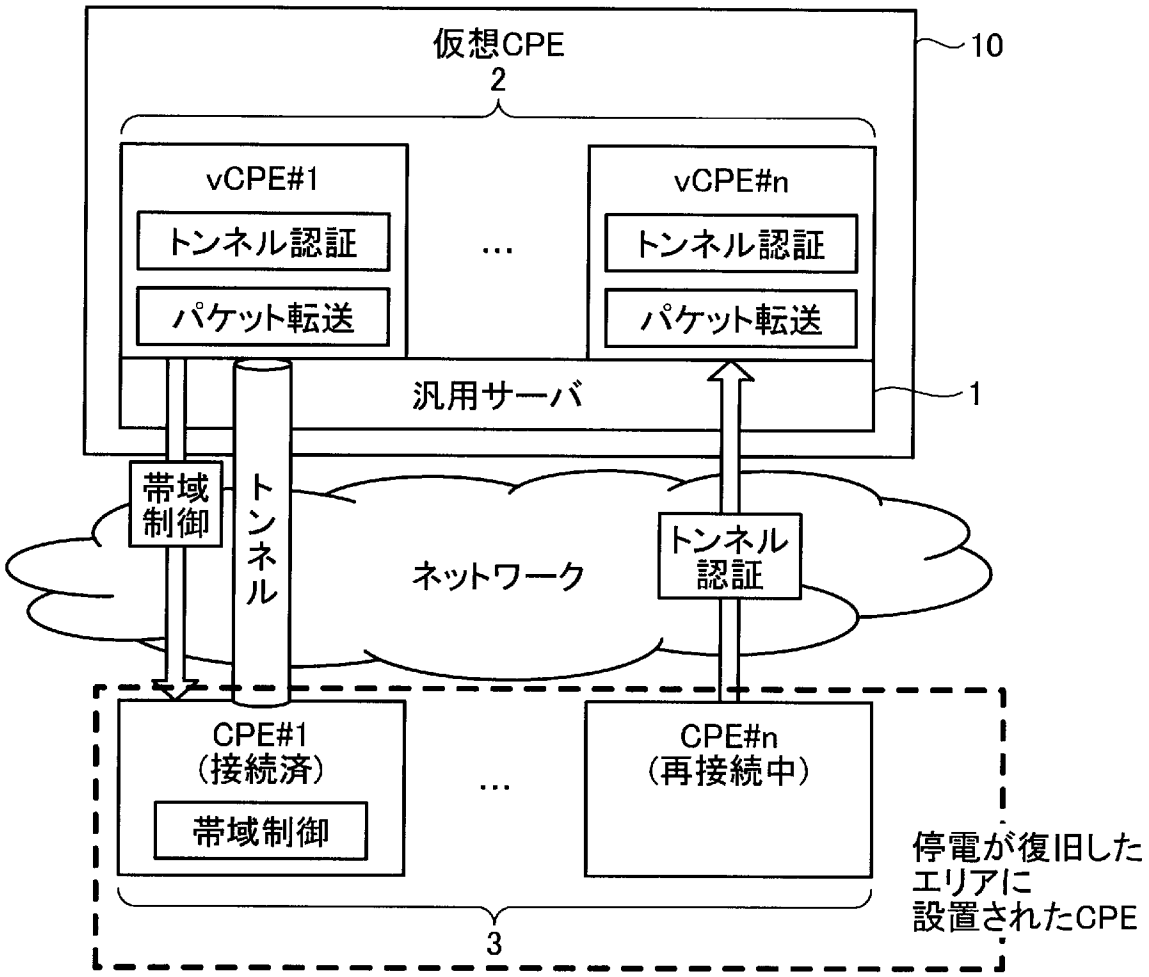
[図3]


仮想CPE
2
10
vCPE#1
トンネル認証
パケット転送
…
vCPE#n
トンネル認証
パケット転送
汎用サーバ
1
トンネル
通信
ネットワーク
トンネル
認証
CPE#1
(接続済)
…
CPE#n
(未接続)
3

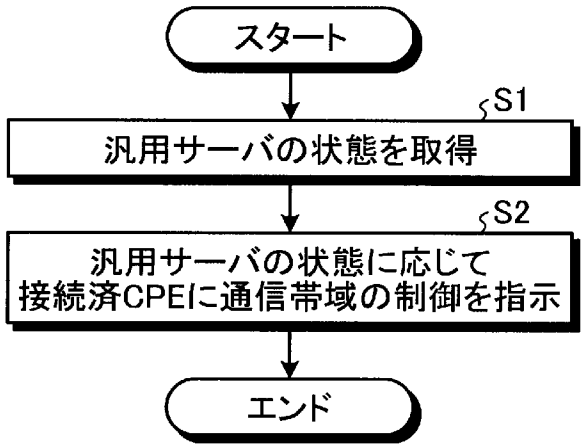
[図4]


10
管理装置
11
制御部
11a
取得部
11b
指示部
12
記憶部
12a
帯域情報

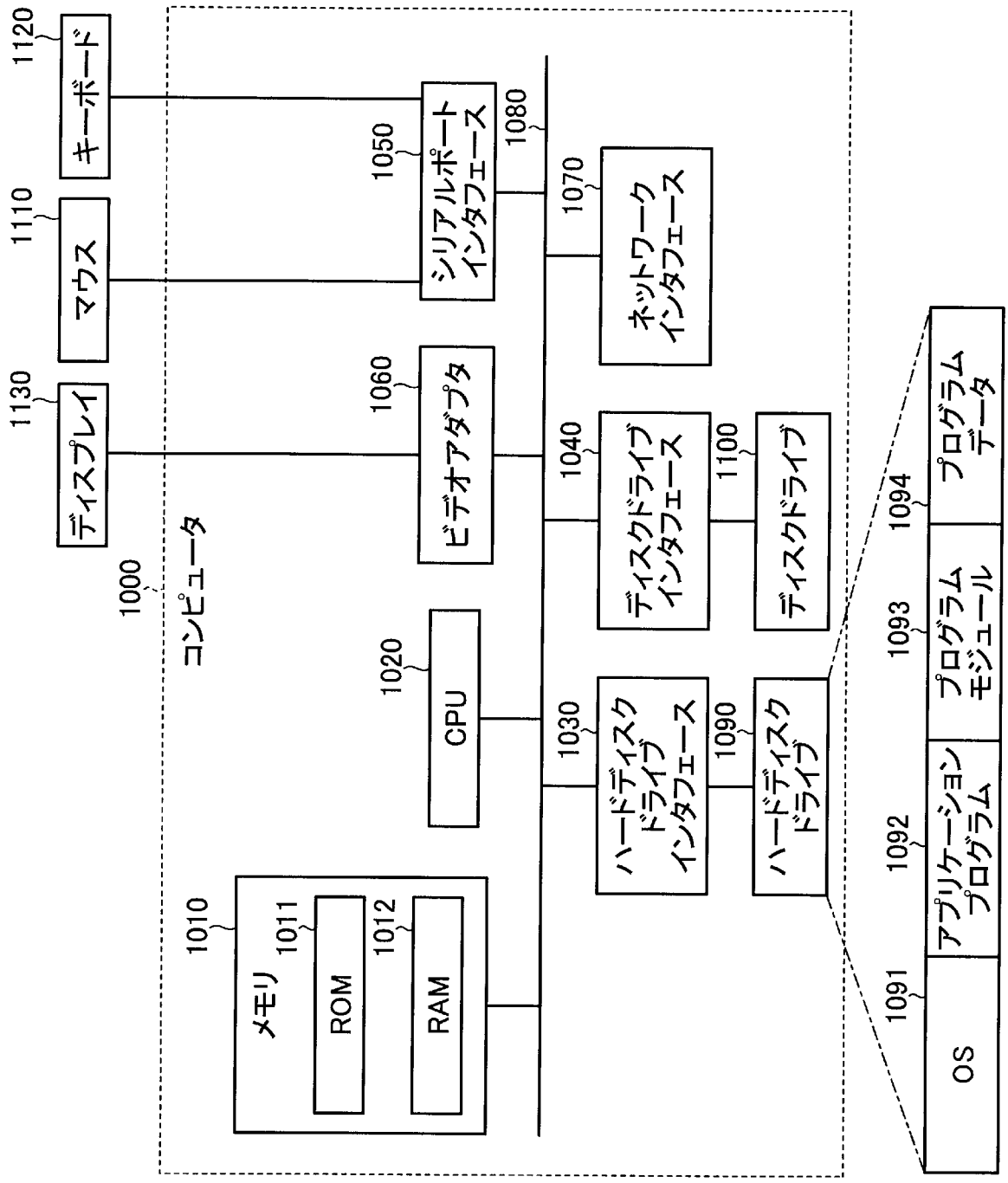
[図5]


仮想CPE
2
10
vCPE#1
トンネル認証
パケット転送
...
vCPE#n
トンネル認証
パケット転送
汎用サーバ
1
帯域制御
トンネル
ネットワーク
トンネル認証
CPE#1
(接続済)
帯域制御
...
CPE#n
(再接続中)
停電が復旧したエリアに設置されたCPE
3

[図6]


スタート
S1
汎用サーバの状態を取得
S2
汎用サーバの状態に応じて
接続済CPEに通信帯域の制御を指示
エンド

[図7]


1000
コンピュータ
1010
メモリ
1011
ROM
1012
RAM
1020
CPU
1030
ハードディスクドライブインタフェース
1040
ディスクドライブインタフェース
1050
シリアルポートインタフェース
1060
ビデオアダプタ
1070
ネットワークインタフェース
1080
1090
ハードディスクドライブ
1100
ディスクドライブ
1091
OS
1092
アプリケーションプログラム
1093
プログラムモジュール
1094
プログラムデータ
1110
マウス
1120
キーボード
1130
ディスプレイ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/029423

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. H04L12/923(2013.01)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)
Int.Cl. H04L12/923, H04L12/70

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	土屋 英雄 他 TSUCHIYA, Hideo et al., 仮想 CPE 適用時におけるセキュリティ機能配備の提案 "A proposal of allocation of security function on virtual CPE system", 電子情報通信学会 2018 年総合大会講演論文集 通信 2 PROCEEDINGS OF THE 2018 IEICE GENERAL CONFERENCE, 06 March 2018, p. 87	1,2,5 3,4
Y A	JP 2017-147526 A (NIPPON TELEGRAPH AND TELEPHONE CORP.) 24 August 2017, paragraphs [0025]-[0031] (Family: none)	1,2,5 3,4

☒ 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 08 October 2019 (08.10.2019)	Date of mailing of the international search report 15 October 2019 (15.10.2019)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/029423

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2015-156150 A (NIPPON TELEGRAPH AND TELEPHONE CORP.) 27 August 2015, entire text, all drawings (Family: none)	1-5

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０２９４２３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/923(2013.01)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.　H04L12/923, 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	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９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
Y	土屋　英雄　他　Hideo　TSUCHIYA et al., 仮想ＣＰＥ適用時におけるセキュリティ機能配備の提案　A proposal of allocation of security function on virtual CPE system, 電子情報通信学会２０１８年総合大会講演論文集　通信２　PROCEEDINGS OF THE 2018 IEICE GENERAL CONFERENCE, 2018.03.06, p.87	1, 2, 5
A		3, 4
Y	JP 2017-147526 A（日本電信電話株式会社） 2017.08.24, 段落 0025-0031（ファミリーなし）	1, 2, 5
A		3, 4

☑　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
０８．１０．２０１９	１５．１０．２０１９

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　３６５５
森田　充功
電話番号　０３－３５８１－１１０１　内線　３５９６

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2015-156150 A（日本電信電話株式会社） 2015.08.27，全文，全図（ファミリーなし）	1-5