

(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3月26日(26.03.2020)



(10) 国際公開番号

WO 2020/059212 A1

- (51) 国際特許分類:
H04L 12/903 (2013.01) H04L 12/70 (2013.01)
- (21) 国際出願番号: PCT/JP2019/021061
- (22) 国際出願日: 2019年5月28日(28.05.2019)
- (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 2018-176630 2018年9月20日(20.09.2018) JP
- (71) 出願人: エヌ・ティ・ティ・コミュニケーションズ株式会社(NTT COMMUNICATIONS CORPORATION) [JP/JP]; 〒1008019 東京都千代田区大手町二丁目3番1号 Tokyo (JP).
- (72) 発明者: 沈 文裕(SHEN, Wenyu); 〒1008019 東京都千代田区大手町二丁目3番1号 エヌ・ティ・ティ・コミュニケーションズ株式会社内 Tokyo (JP). 新井 研二(ARAI, Kenji); 〒1008019 東京都千代田区大手町二丁目3番1

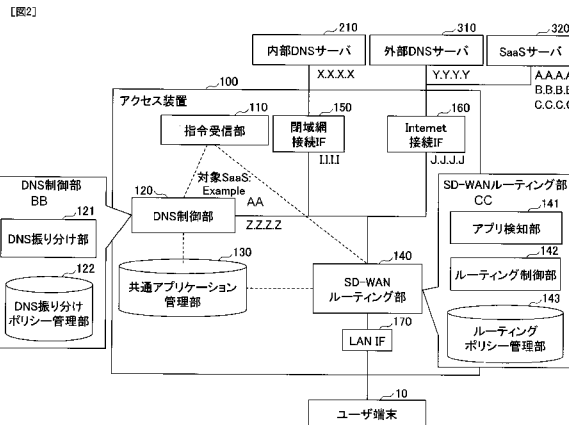
号 エヌ・ティ・ティ・コミュニケーションズ株式会社内 Tokyo (JP). 可児島 隆(KANISHIMA, Ryu); 〒1008019 東京都千代田区大手町二丁目3番1号 エヌ・ティ・ティ・コミュニケーションズ株式会社内 Tokyo (JP). 嵯峨 毅郎(SAGA, Takeo); 〒1008019 東京都千代田区大手町二丁目3番1号 エヌ・ティ・ティ・コミュニケーションズ株式会社内 Tokyo (JP).

(74) 代理人: 伊東 忠重, 外(ITO, Tadashige et al.); 〒1000005 東京都千代田区丸の内二丁目1番1号 丸の内 M Y P L A Z A (明治安田生命ビル) 16階 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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,

(54) Title: CONTROL DEVICE, CONTROL METHOD, AND PROGRAM

(54) 発明の名称: 制御装置、制御方法、及びプログラム



10 User terminal
100 Access device
110 Command reception unit
120 BB DNS control unit
121 DNS assignment unit
122 DNS assignment policy management unit
130 Common application management unit
140 CC SD-WAN routing unit
141 Application detection unit
142 Routing control unit
143 Routing policy management unit
150 Closed network connecting interface
160 Internet connecting interface
210 Internal DNS server
310 External DNS server
320 SaaS server
AA Available SaaS: Example

(57) Abstract: A control device connected to a plurality of networks, the control device assigning a packet received from a user terminal to one of the plurality of networks, wherein the control device is provided with: a DNS control unit for receiving a DNS inquiry packet transmitted from the user terminal and assigning the DNS inquiry packet to one of the plurality of networks on the basis of a subject of inquiry in the DNS inquiry; and a routing unit for receiving a packet, determining the destination of the packet on the basis of the destination address of the packet, and transmitting the packet to the determined destination.

(57) 要約: 複数の網に接続され、ユーザ端末から受信したパケットを当該複数の網のうちのいずれかの網に振り分ける制御装置において、前記ユーザ端末から送信されたDNS問い合わせパケットを受信し、当該DNS問い合わせパケットの問い合わせ対象に基づいて、当該DNS問い合わせパケットを前記複数の網のうちのいずれかの網に振り分けるDNS制御部と、パケットを受信し、当該パケットの宛先アドレスに基づいて当該パケットの送信先を決定し、決定された送信先に当該パケットを送信するルーティング部とを備える。

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))

明 細 書

発明の名称： 制御装置、制御方法、及びプログラム

技術分野

[0001] 本発明は、ユーザ端末からネットワーク上のサーバなどへのアクセスを高速化する技術に関連するものである。

背景技術

[0002] 近年、Software-as-a-Service (SaaS) の利用が爆発的に普及してきた。一方、SaaSでは、元々LAN環境での利用を想定して設計されていたアプリケーションがCloud上で提供されるため、そのパフォーマンスはネットワークの遅延や品質に左右され、特に企業がグローバル展開するほどネットワークの遅延や品質の影響が大きくなる。

[0003] 現状では、閉域網である企業ネットワークはSaaS利用に向けて設計されていない。例えば、多くの企業ネットワークではインターネットへの接続点は限られているので、インターネットを経由するSaaS接続が遠回りになってしまう。

[0004] また、企業ネットワーク内の通信である拠点間の通信とSaaS向けの通信とを同一回線に重畳する場合、拠点間などで回線の帯域が圧迫される。2020年ごろには半分以上の企業がネットワークに関連するSaaS利用上の問題を抱えるという予測もある。

[0005] 北米の大手金融／流通／小売りなどの企業のIT責任者を中心に立ち上げたONUG (Open Networking User Group) という団体でSD-WAN (Software-defined WAN) の技術が提唱されてきた。現在のWANコストの削減、運用の簡略化、品質の向上などを狙い、多くの企業が市販のSD-WANソリューションを導入し始めた。SD-WANの利用において、一番有望視されているユースケースがSaaSアクセスを中心としたLocal Breakoutと言われている。

[0006] Local Breakoutとは、ブランチ拠点において、SaaSにアクセスする際に、特定のデータフローをDeep Packet Inspection (DPI) エンジンを用いて識別し、識別された該当データフローをブランチ拠点からインターネットに直接流すようにルーティングを制御する仕組みである。

[0007] SD-WAN Customer Premises Equipment (CPE) の利用により、Local Breakoutを実現し、SaaS向けのトラフィックをブランチ拠点からインターネットに直接流すことによって、上記の様々な問題の解決が期待されている。

先行技術文献

特許文献

[0008] 特許文献1：特許第5832970号

発明の概要

発明が解決しようとする課題

[0009] しかし、従来のSD-WAN技術を用いたSaaSアクセス方法は実際の利用シーンに最適化されていない場合が多いため、ユーザ端末からSaaSサーバへのアクセスに遅延が生じるなどの課題がある。

[0010] 本発明は上記の点に鑑みてなされたものであり、閉域網を介した通信を行うユーザ端末が、インターネット上の所定のサーバに高速にアクセスすることを可能とする技術を提供することを目的とする。

課題を解決するための手段

[0011] 開示の技術によれば、複数の網に接続され、ユーザ端末から受信したパケットを当該複数の網のうちのいずれかの網に振り分ける制御装置であって、前記ユーザ端末から送信されたDNS問い合わせパケットを受信し、当該DNS問い合わせパケットの問い合わせ対象に基づいて、当該DNS問い合わせパケットを前記複数の網のうちのいずれかの網に振り分けるDNS制御部と、

パケットを受信し、当該パケットの宛先アドレスに基づいて当該パケットの送信先を決定し、決定された送信先に当該パケットを送信するルーティング部と

を備える制御装置が提供される。

発明の効果

[0012] 開示の技術によれば、閉域網を介した通信を行うユーザ端末が、インターネット上の所定のサーバに高速にアクセスすることを可能とする技術が提供される。

図面の簡単な説明

[0013] [図1]本発明の実施の形態におけるシステムの全体構成図である。

[図2]第1の実施の形態におけるアクセス装置100の機能構成図である。

[図3]アクセス装置100のハードウェア構成図である。

[図4]アプリケーション管理DBに格納される情報の例を示す図である。

[図5]アプリケーションキャッシュに格納される情報の例を示す図である。

[図6]DNS振り分けポリシー管理DBに格納される情報の例を示す図である。

[図7]IPルーティングポリシー管理DB及びアプリルーティングポリシー管理DBに格納される情報の例を示す図である。

[図8]第1の実施の形態におけるマネジメントフロー制御のフローチャートである。

[図9]第1の実施の形態におけるデータフロー制御のフローチャートである。

[図10]DNSの問い合わせの宛先を書き換える場合のDNS制御部の構成図である。

[図11]DNSの問い合わせの宛先を書き換える場合のアプリルーティングポリシー管理DBに格納される情報の例を示す図である。

[図12]DNSの問い合わせの宛先を書き換える場合におけるデータフロー制御のフローチャートである。

[図13]DNSの問い合わせ結果を用いてアプリケーションキャッシュを随時

更新する場合のフローチャートである。

[図14]DNSの問い合わせ結果を用いてアプリケーションキャッシュを随時更新する場合のアプリケーションキャッシュを示す図である。

[図15]第2の実施の形態におけるアクセス装置100の機能構成図である。

[図16]IPルーティングポリシー管理DB及びアプリルーティングポリシー管理DBに格納される情報の例を示す図である。

[図17]プロキシ振り分けポリシー管理DBに格納される情報の例を示す図である。

[図18]第2の実施の形態におけるマネジメントフロー制御のフローチャートである。

[図19]第2の実施の形態におけるデータフロー制御のフローチャートである。

[図20]アプリケーションキャッシュを利用する場合におけるプロキシ振り分けポリシー管理DBに格納される情報の例を示す図である。

[図21]アプリケーション管理DBの定期的更新を説明するための図である。

[図22]アプリケーション管理DBの定期的更新のフローチャートである。

[図23]アプリケーションキャッシュに格納される情報の例を示す図である。

発明を実施するための形態

[0014] 以下、図面を参照して本発明の実施形態を説明する。以下で説明する実施形態は一例に過ぎず、本発明が適用される実施の形態は、以下の実施形態に限られるわけではない。

[0015] (課題について)

まず、実施の形態で説明するアクセス装置100により解決される課題について説明する。なお、以下の3つの課題は例であり、アクセス装置100により解決される課題は下記の課題に限られない。

[0016] (1) DNSについての課題

多くのSaaSはどの地域のユーザにも最大限のパフォーマンスでサービスを提供するため、GeoDNS技術を採用している。GeoDNSの利用

により、DNSサーバに問い合わせたクライアントの物理的な位置に応じて、最寄りのSaaSのサーバのIPアドレスを応答することができる。なお、DNSはDomain Name Systemの略である。

[0017] ただし、企業ユーザがデータセンタなどの主要拠点に内部DNSサーバを設置し、外部DNSサーバへの問い合わせを当該主要拠点からブレイクアウトさせている設計が多い。そのため、SaaSアクセスに関するDNSトラフィックは、データセンタなどの主要拠点からインターネットに出るの対し、データフローはブランチ拠点（例：データセンタと異なる国に設置された拠点）からインターネットに出ることになり、両者の出口が合致していない。その結果、せっかくSaaSに関する特定のデータフローをブランチ拠点にてブレイクアウトしているのに、主要拠点からDNS問い合わせをした結果、主要拠点の最寄りのSaaSサーバにアクセスしてしまい、期待されている遅延の改善効果が見られない場合がある。

[0018] （２）プロキシについての課題

ユーザ端末とSaaSサーバとの間にプロキシ（プロキシ装置、プロキシサーバなどと称してもよい）を設置して、プロキシを経由して通信を行うことが多い。しかし、SaaSの種類によって、利用時にTCPセッションを大量に消費する場合もあるため、セッション増によるプロキシの処理限界により、SaaSが快適に利用できないことがある。

[0019] そこで、既存のプロキシをバイパスし、処理負荷を軽減することが求められている。従来方式では、SaaSトラフィックに対して、プロキシをバイパスさせるために、SD-WAN装置とは別に、既存のプロキシにおいて、SaaS向けの通信の宛先を定期的にチェックしなければならず、その結果をプロキシ自動設定（PAC）ファイルに反映し、当該PACファイルをまたすべてのエンドユーザに配布しなければならない。従って、運用負荷が増加する場合がある。

[0020] （３）パケット識別遅延の課題

また、従来のSD-WAN装置のDPIエンジンにおいて、HTTP/H

T T P s のハンドシェイクのやり取りを解析し、その中で抽出した S a a S のドメインネームを用いてアクセス先の S a a S を判別する方法が採用されている。しかし、この方法では最初に到着したパケット (F i r s t P a c k e t) にて S a a S を識別することが困難であるため、該当 S a a S の最初のフローが主要拠点から出てしまう場合がある。

[0021] 以下、本発明の実施の形態として、上記課題を解決する技術について詳細に説明する。なお、本実施の形態では、アクセス装置 1 0 0 が閉域網 2 0、及びインターネット 3 0 に接続されるが、この形態は一例に過ぎない。閉域網 2 0 及びインターネット 3 0 以外の 2 網間で同様の制御がされてもよい。また、アクセス装置 1 0 0 は 3 つ以上の複数の網に接続されて、パケットを当該複数の網のうちのいずれかの網に振り分けることとしてもよい。

[0022] (システム構成)

図 1 に本発明の実施の形態におけるシステムの全体構成を示す。図 1 に示すとおり、ユーザ端末 1 0、閉域網 2 0、及びインターネット 3 0 と接続されるアクセス装置 1 0 0 が備えられる。アクセス装置 1 0 0 は、ユーザ端末 1 0 からのアクセスを受けて、ユーザ端末 1 0 を、閉域網 2 0 上の装置、あるいは、インターネット 3 0 上の装置に接続させ、通信を行う装置である。なお、アクセス装置 1 0 0 を、S a a S アクセス高速化装置と称してもよい。また、アクセス装置 1 0 0 は、データフローに対する種々の制御を実施する装置なので、これを制御装置と称してもよい。

[0023] 閉域網 2 0 は、例えば企業の複数拠点を接続する企業内の網である。アクセス装置 1 0 0 は、例えば、グローバル企業の企業ネットワークにおけるブランチ拠点毎に設置される装置である。

[0024] 以下、アクセス装置 1 0 0 の構成と動作を詳細に説明する。以下では、アクセス装置 1 0 0 の基本的な構成を第 1 の実施の形態として説明し、第 1 の実施の形態のアクセス装置 1 0 0 にプロキシ制御部が追加された構成を第 2 の実施の形態として説明する。

[0025] (第 1 の実施の形態)

＜装置構成＞

図2に、第1の実施の形態におけるアクセス装置100の機能構成図を示す。図2に示すように、アクセス装置100は、指令受信部110、DNS制御部120、共通アプリケーション管理部130、SD-WANルーティング部140、複数のIF（インタフェース）を有する。

[0026] 複数のIFの例として、図2には、閉域網に接続するための閉域網接続IF150、インターネットに接続するためのInternet接続IF160、LANに接続するためのLAN-IF170が示されている。閉域網接続IF150及びInternet接続IF160には図示のとおりIPアドレスが割り当てられている。

[0027] 図示のとおり、閉域網接続IF150には内部DNSサーバ210が接続され、Internet接続IF160には、外部DNSサーバ310及びSaaSサーバ320が接続され、LAN-IF170にはユーザ端末10が接続されている。また、各サーバには図示のとおりIPアドレスが割り当てられている。本実施の形態におけるSaaSサーバ320に関して、IPアドレスは固定ではなく、随時IPアドレスが変わる。

[0028] なお、IFは、物理ポートに限らず、IPsecなどのトンネルを終端する論理ポートであってもよい。また、本実施の形態では、例として、共通アプリケーション管理部130を各アクセス装置に備えることとしているが、これに代えて、共通アプリケーション管理部130を、アクセス装置100の外部に備え、複数のアクセス装置が共通に利用可能なものとして設置してもよい。アクセス装置100の各部の詳細については後述する。

[0029] アクセス装置100は、複数のコンピュータ（通信装置なども含む）により構成されるシステムであってもよいし、1つのコンピュータで実現される装置であってもよい。また、当該コンピュータは物理マシンであってもよいし仮想マシンであってもよい。また、アクセス装置100が、本実施の形態で説明する処理を実行する専用ハードウェア回路で実現されてもよい。

[0030] アクセス装置100がコンピュータで実現される場合において、アクセス

装置１００は、コンピュータに内蔵されるＣＰＵやメモリ等のハードウェア資源を用いて、アクセス装置１００で実施される処理に対応するプログラムを実行することによって実現することが可能である。上記プログラムは、コンピュータが読み取り可能な記録媒体（可搬メモリ等）に記録して、保存したり、配布したりすることが可能である。また、上記プログラムをインターネットや電子メール等、ネットワークを通して提供することも可能である。

[0031] 図３は、上記コンピュータのハードウェア構成例を示す図である。図３のコンピュータは、それぞれバスＢで相互に接続されているドライブ装置１０００、補助記憶装置１００２、メモリ装置１００３、ＣＰＵ１００４、インタフェース装置１００５、表示装置１００６、及び入力装置１００７等を有する。

[0032] 当該コンピュータでの処理を実現するプログラムは、例えば、ＣＤ－ＲＯＭ又はメモリカード等の記録媒体１００１によって提供される。プログラムを記憶した記録媒体１００１がドライブ装置１０００にセットされると、プログラムが記録媒体１００１からドライブ装置１０００を介して補助記憶装置１００２にインストールされる。但し、プログラムのインストールは必ずしも記録媒体１００１より行う必要はなく、ネットワークを介して他のコンピュータよりダウンロードするようにしてもよい。補助記憶装置１００２は、インストールされたプログラムを格納すると共に、必要なファイルやデータ等を格納する。

[0033] メモリ装置１００３は、プログラムの起動指示があった場合に、補助記憶装置１００２からプログラムを読み出して格納する。ＣＰＵ１００４は、メモリ装置１００３に格納されたプログラムに従って、アクセス装置１００に係る機能を実現する。インタフェース装置１００５は、ネットワークに接続するためのインタフェースとして用いられ、ネットワークを介した入力手段及び出力手段として機能する。表示装置１００６はプログラムによるＧＵＩ（Graphical User Interface）等を表示する。入力装置１５７はキーボード及びマウス、ボタン、又はタッチパネル等で構成

され、様々な操作指示を入力させるために用いられる。

[0034] 以下、アクセス装置 100 の各部の構成、動作を詳細に説明する。

[0035] <共通アプリケーション管理部 130>

共通アプリケーション管理部 130 は、アプリケーション管理 DB とアプリケーションキャッシュ（アプリケーションテーブルと称してもよい）を有する。図 4 に、アプリケーション管理 DB に格納される情報の例を示し、図 5 に、アプリケーションキャッシュに格納される情報の例を示す。

[0036] アプリケーション管理 DB は様々な SaaS の通信パターンを管理する DB であり、図 4 に示す例では、アプリケーション管理 DB のカラムとして、アプリケーション名、FQDN、宛先 IP アドレスなどを有する。図 4 は例であり、アプリケーション管理 DB の構成は図 4 に示すものに限られない。例えば、図 4 のアプリケーション名、FQDN、宛先 IP アドレスに加えて、宛先ポート番号を含めてもよい。また、SaaS アプリを特定するその他のパラメータを含めてもよい。

[0037] 図 4 に示す情報は、アプリケーション名が「Example」の SaaS に関しては、宛先の FQDN が Example.com もしくは、Example365.com もしくは、宛先 IP アドレスが B.B.B.B/B の 3 種類の通信パターンがあることを示す。

[0038] アプリケーションキャッシュは、現時点においてアクセス装置 100 が把握している SaaS の宛先サーバの IP アドレスを記録する。図 5 に示すように、アプリケーションキャッシュのカラムとしては、例えば、アプリケーション名と宛先 IP アドレスを有するが、これに限られるわけではない。また、図 5 (a) は、アプリケーション名が「Example」の宛先 IP アドレスが B.B.B.B として把握された場合を示している。図 5 (b) は、例えば、アプリケーション名が「Example」の宛先 IP アドレスが B.B.B.B として把握された後、「Example」の宛先 IP アドレスとして A.A.A.A が検知された場合を示している。

[0039] <DNS 制御部 120>

図2に示したように、DNS制御部120は、DNS振り分け部121とDNS振り分けポリシー管理部122を有する。

[0040] DNS振り分け部121は、DNS振り分けポリシー管理部122が管理するDNS振り分けポリシーに従って、DNS問い合わせ（DNS問い合わせパケットと称してもよい）を振り分ける。つまり、当該DNS振り分けポリシーに従って、DNS問い合わせの送信先を決定し、その送信先に向けてDNS問い合わせを送信する。

[0041] DNS振り分けポリシー管理部122は、図6に示すDNS振り分けポリシー管理DBを有する。DNS振り分けポリシー管理DBは、DNS問い合わせに対して、実行する動作を定義する情報を格納するDBである。図6に示す例では、Example.comあるいはExample365.comのFQDNが含まれるDNS問い合わせに対して、IPアドレスがY.Y.Yの外部DNSサーバ310にForwardし、その他の問い合わせは、Defaultとして内部DNSサーバ210にForwardする動作を定義している。

[0042] <SD-WANルーティング部140>

図2に示したように、SD-WANルーティング部140は、アプリ検知部141、ルーティング制御部142、ルーティングポリシー管理部143を有する。

[0043] アプリ検知141は、SD-WANルーティング部140によりルーティングされるデータフロー（より詳細にはデータフローを構成するパケット）を調べることにより、そのデータフローの宛先あるいは送信元のアプリケーションを検知する。ルーティング制御部142は、ルーティングポリシー管理部143に管理されているルーティングポリシーに従ってパケットのルーティングを実行する。

[0044] ルーティングポリシー管理部143は、IPルーティングポリシー管理DBとアプリルーティングポリシー管理DBとを有する。図7（a）に、IPルーティングポリシー管理DBに格納される情報の例を示し、図7（b）に

、アプリルーティングポリシー管理DBに格納される情報の例を示す。

[0045] IPルーティングポリシー管理DBは、通常のルータのルーティングテーブルに相当し、図7（a）に示すとおり、宛先IPアドレスとNext Hopを格納している。

[0046] アプリルーティングポリシー管理DBは対象アプリに対するルーティング制御方法を定義する情報を格納するDBである。図7（b）には、一例として対象アプリ「Example」のSaaSフローをローカルにあるNext hop（Internet接続IF（J. J. J. J））に転送するルーティング動作を定義する情報が示されている。

[0047] 図7（a）はIPルーティングポリシー管理DBが宛先IPアドレスとNext hopのカラムを有することを示し、図7（b）はアプリルーティングポリシー管理DBが対象アプリと、Next hopのカラムを有することを示しているが、これらは一例である。IPルーティングポリシー管理DBとアプリルーティングポリシー管理DBのそれぞれにおいて、通信元のIPアドレスや、ポート番号などを含めてもよい。

[0048] 以下、アクセス装置100の基本的な動作として、DBの設定／更新などのための動作（マネジメントフローの制御と呼ぶ）と、ユーザ端末10が通信を行う際の動作（データフローの制御と呼ぶ）について説明する。

[0049] <マネジメントフローの制御>

図8に示すフローチャートの手順に沿ってマネジメントフローの制御におけるアクセス装置100の動作について説明する。

[0050] S101）対象指定

指示受信部110は、ユーザからLocal breakoutさせる対象SaaSの指定を受信し、受信内容に基づいてDNS制御部120と、SD-WANルーティング部140にそれぞれ指示をする。

[0051] S102）DNS振り分けポリシー管理DB更新

DNS制御部120は、共通アプリケーション管理部130から、対象SaaSに対するLocal breakoutのために必要な情報を収集し

、DNS振り分けポリシー管理DB（例：図6）を更新する。

[0052] 対象SaaSに対するLocal breakoutのために必要な情報は、例えば、対象SaaSに対応する1つ又は複数のFQDN（FQDN一覧）である。DNS制御部120は、取得したFQDN一覧におけるFQDNを想定される動作と紐付け、DNS振り分けポリシー管理DBに格納する。

[0053] 本実施の形態では、Local breakoutの際のNext-hopは事前に設定された外部DNSサーバ310のIPアドレス（Y．Y．Y．Y）を想定する。それ以外のFQDNに関する問い合わせは内部DNSサーバ210のIPアドレス（X．X．X．X）を想定する。

[0054] 例えば、図6の最初のレコードには、DNS問い合わせにおける対象SaaSのFQDNがExample．comである場合において、当該DNS問い合わせをIPアドレス（Y．Y．Y．Y）にForwardする動作に対応する情報が記録される。

[0055] S103）アプリルーティングポリシー管理DB更新

SD-WANルーティング部140は、アプリルーティングポリシー管理DB（例：図7（b））を更新する。具体的には、図7（b）に示すように、対象SaaSと事前に定義されているNext hopアドレスとを紐付けた情報を記録する。

[0056] ＜データフローの制御例1＞

次に、データフローの制御例1におけるアクセス装置100の動作について、図9のフローチャートの手順に沿って説明する。データフローの制御例1では、ユーザ端末10でのDNSサーバのアドレスがアクセス装置100のDNS制御部120（Z．Z．Z．Z）に設定されている。

[0057] S201）DNS問い合わせ受信／転送

ルーティング制御部142は、ユーザ端末10から送信されたDNS問い合わせを受信し、IPルーティングポリシー管理DB（例：図7（a））に従って、通常のルータと同様にして、該当問い合わせをDNS制御部120

に転送する。DNS制御部120のDNS振り分け部121がDNS問い合わせを受信する。

[0058] S202) DNS問い合わせ再転送

DNS制御部120におけるDNS振り分け部121は、受信したDNS問い合わせをDNS振り分けポリシー管理DB（例：図6）に従って再転送する。

[0059] 例えば、該当DNS問い合わせに含まれるFQDNが、対象SaaSのExample.comである場合において、DNS振り分け部121は、DNS振り分けポリシー管理DB（図6）に従って、当該DNS問い合わせを外部DNSサーバ310（Y.Y.Y.Y）に転送される。その他のDNS問い合わせはDefaultに従って、内部DNSサーバ210に転送される。なお、データフローの制御例1においても、後述する問い合わせ先変更部123を備えることで、DNS問い合わせの宛先を転送先のIPアドレスに変更してもよい。

[0060] その後、ユーザ端末10は、該当DNSサーバから送出されたIPアドレスを受信し、当該IPアドレスを宛先とするデータ通信を開始する。

[0061] S203) データフロー検知

DNSの問い合わせ実施後、ユーザ端末10によるデータ通信が開始されると、対象SaaSのデータフローがLAN-IF170により受信され、SD-WANルーティング部140に送信される。

[0062] SD-WANルーティング部140のアプリ検知部141は特定のSaaSのデータフローを検知し、該当フローの宛先IPアドレスを用いて、アプリケーションキャッシュ（例：図5）を更新する。アプリ検知部141によるSaaSデータフローの検知方法として、例えばHTTP/HTTPSのHeaderから抽出する方法があるが、それに限らない。

[0063] S204) ルーティング制御

ルーティング制御部142は、アプリルーティングポリシー管理DB（例：図7（b））と、アプリケーションキャッシュ（例：図5）を用いて、S

aaSデータフローのルーティングを制御する。例えば、対象aaSがExample.comの場合、アプリケーションキャッシュにExample.comに対する宛先アドレスとしてA.A.A.Aが記録された後、ルーティング制御部142は、宛先がA.A.A.Aであるパケットを受信すると、アプリケーションキャッシュを参照することで、対象aaSがExampleであることを把握し、アプリルーティングポリシー管理DBを参照することで、当該パケットをInternet接続IF160(J.J.J.J)に転送する。

[0064] S205) ルーティング制御

その後、同じデータフローが発生した場合、アプリ検知部141を経由することなく、アプリケーションキャッシュを用いることでルーティングの制御を実行することが可能となる。

[0065] <データフローの制御例2>

次に、データフローの制御例2として、ユーザ端末10でのDNSサーバのアドレスが内部DNSサーバ210(X.X.X.X)と設定されるケースについて、データフローの制御例1と異なる点を説明する。

[0066] データフローの制御例2では、図10に示すように、DNS制御部120は、DNS振り分け部121とDNS振り分けポリシー管理部122に加えて、問い合わせ先変更部123を有する。

[0067] また、図11に示すように、アプリルーティングポリシー管理DBにDNS問い合わせに対するルーティングポリシーを新たに追加する。このルーティングポリシーは、ポート番号(例:53)でDNS問い合わせトラフィックを特定し、Next hopをDNS制御部120(Z.Z.Z.Z)とするポリシーである。

[0068] この場合のデータフローの制御を図12のフローチャートの手順に沿って説明する。

[0069] S301) DNS問い合わせ受信/転送

ルーティング制御部142は、DNS問い合わせを受信すると、アプリル

ーティングポリシー管理DB（図11）におけるDNSに関するポリシーに従って、当該DNS問い合わせをDNS制御部120（Z，Z，Z，Z）に転送する。

[0070] S302) DNS問い合わせ再転送

DNS制御部120におけるDNS振り分け部121は、受信したDNS問い合わせをDNS振り分けポリシー管理部122に従って再転送する。対象SaaS以外の問い合わせはDefaultに従って、内部DNSサーバ210（X，X，X，X）に再転送される。

[0071] S303) 宛先アドレス変更

一方、対象SaaSのDNS問い合わせは、宛先を問い合わせ先変更部123によって変更した上で再転送する。変更先となるDNS問い合わせの宛先アドレスは事前に設定されるものとし、例として外部DNSサーバ310のIPアドレス（Y，Y，Y，Y）が変更先として設定される。以降の処理はデータフローの制御例1と同様である。

[0072] <DNSの問い合わせの結果を用いたアプリケーションキャッシュの更新>

上述した例では、アプリ検知部141がパケットを解析することにより当該パケットに係るデータフローに対応するSaaSアプリケーションを識別し、アプリケーションキャッシュ（例：図5）を更新していた。この方法に代えて（あるいはこの方法に加えて）、DNSの問い合わせ結果を用いてアプリケーションキャッシュを更新してもよい。

[0073] DNSの問い合わせの結果を用いて、アプリケーションキャッシュを随時更新する機能を持たせることで、First packetでSaaSアプリケーションの識別が可能となる。

[0074] この場合のアクセス装置100の動作を図13のフローチャートの手順に沿って説明する。

[0075] S401) アプリケーションキャッシュ更新

例えば、DNS問い合わせが外部DNSサーバ310に転送され、外部D

NSサーバ310から送出される問い合わせ結果（FQDNに対応するIPアドレス）をルーティング制御部142が受信する。ルーティング制御部142は、当該問い合わせ結果を用いてアプリケーションキャッシュを更新する。

[0076] 例えば、Example.comの問い合わせ結果がA、A、A、Aであり、Example365.comの問い合わせ結果がC、C、C、Cであるとし、ルーティング制御部142がそれぞれの問い合わせ結果を受信した場合、図14に示すように、アプリケーションキャッシュが更新される。つまり、A、A、A、Aのレコードと、C、C、C、Cのレコードが追加される。なお、本実施の形態におけるExample.comとExample365.comのアプリケーション名はいずれも「Example」として識別される。

[0077] S402) ルーティング制御

その後、ルーティング制御部142が、該当SaaSのデータフローを受信した場合、アプリルーティングポリシー管理DB（例：図7（b））と、アプリケーションキャッシュ（例：図14）を用いて、該当フローのルーティングを制御する。

[0078] 具体的には、ルーティング制御部142は、データフローの宛先IPアドレスでアプリケーションキャッシュを検索し、ヒットするレコードがある場合、当該レコードのアプリケーション名（対象SaaS名）を用いてアプリルーティングポリシー管理DBで当該対象SaaSのNext hopを検索する。その結果、ルーティング制御部142はNext hopに記載されているIPアドレスに該当フローを転送する。

[0079] （第2の実施の形態）

次に、第2の実施の形態を説明する。ここでは、第1の実施の形態と異なる点を主に説明する。

[0080] <装置構成>

図15に、第2の実施の形態におけるアクセス装置100の機能構成図を

示す。図15に示すように、第2の実施の形態におけるアクセス装置100は、第1の実施の形態におけるアクセス装置100に対してプロキシ制御部180が追加された構成である。また、図15には、内部プロキシサーバ220が示されている。図示するように、ここではプロキシ制御部180のIPアドレスはZ'、Z'、Z'、Z'であり、内部プロキシサーバ220のIPアドレスはZ1、Z1、Z1、Z1である。

[0081] 図15に示すとおり、プロキシ制御部180は、プロキシ振り分け部181とプロキシ振り分けポリシー管理部182を有する。

[0082] 第2の実施の形態では、プロキシ制御部180までトラフィックをルーティングさせるため、図16(a)に示すように、ルーティングポリシー管理部143におけるIPルーティングポリシー管理DBに新たにZ'、Z'、Z'、Z'に関するポリシーを追加する。

[0083] また、プロキシ振り分けポリシー管理部182はプロキシ振り分けポリシー管理DBを有する。図17に、プロキシ振り分けポリシー管理DBに格納される情報の例を示す。図17に示すように、プロキシ振り分けポリシー管理DBは、各FQDNと、IPアドレスに対するプロキシの制御動作を定義する情報を格納したDBである。

[0084] プロキシ振り分け部181は、プロキシ振り分けポリシー管理DBの情報に従って、トラフィックの振り分け制御を実行する。例えば、プロキシ振り分け部181は、宛先のFQDNがExample.comであるパケットを受信した場合、当該パケットをプロキシパススルーとさせる。Defaultの場合、内部プロキシ(Z1、Z1、Z1、Z1)とプロキシチェーニングを実施する。

[0085] <マネジメントフローの制御>

図18に示すフローチャートの手順に沿って、プロキシ制御部180の追加に伴って追加される制御フローについて説明する。

[0086] S501) 対象指定

まず、指示受信部110は、ユーザからLocal breakoutさ

せる対象SaaSの指定を受信し、受信内容に基づいてプロキシ制御部180に指示をする。

[0087] S502) プロキシ振り分けポリシー管理DB更新

プロキシ制御部180は、共通アプリケーション管理部130のアプリケーション管理DBから、対象SaaSに対するLocal breakoutのために必要な情報を収集し、プロキシ振り分けポリシー管理DBを更新する。

[0088] 対象SaaSに対するLocal breakoutのために必要な情報は、例えば、対象SaaSに対応する1つ又は複数のFQDN（FQDN一覧）と1つ又は複数のIPアドレス（IPアドレス一覧）である。プロキシ制御部180は、取得したFQDN一覧とIPアドレス一覧を、想定される動作と紐付け、プロキシ振り分けポリシー管理DBに格納する。

[0089] 図17に示すように、パススルーしない場合（Defaultの場合）におけるNext-hopは、事前に設定されたプロキシチェーニングの先となる内部DNSサーバ220のIPアドレス（Z1, Z1, Z1, Z1）としている。

[0090] <データフローの制御>

次に、データフローの制御におけるアクセス装置100の動作について、図19のフローチャートの手順に沿って説明する。

[0091] S601) トラフィック受信／転送

ルーティング制御部142は、プロキシ制御部180向けのトラフィック（ここでは、SaaSアクセス要求とする）を受信し、ルーティングポリシー管理部143のIPルーティングポリシー管理DB（例：図16（a））に従って、トラフィックをプロキシ制御部180（Z', Z', Z', Z'）に転送する。プロキシ制御部180におけるプロキシ振り分け部181がトラフィック（SaaSアクセス要求）を受信する。

[0092] S602) トラフィック受信／転送

プロキシ振り分け部181は、受信したSaaSアクセス要求を一旦終端

し、プロキシ振り分けポリシー管理DB（図17）に従って、該当SaaSにアクセスするためのプロキシ制御を行う。

[0093] 一例として、Example.comにアクセスする要求に関して、図17の動作定義に従って、パススルーとさせる。パススルーの場合、プロキシ制御部180が起点となって、DNSの問い合わせを実施する。DNSの問い合わせ動作や、その後の一連の動作はこれまでの説明と同様である。なお、この場合のDNS問い合わせは、プロキシ制御部180からルーティング制御部142に送られ、ルーティング制御部140からDNS制御部120に送られる。

[0094] 一方、対象SaaSアクセス以外のデータフローに関しては、Defaultに該当し、内部プロキシサーバ220とチェーニングさせるために、プロキシ制御部180は、内部プロキシサーバ220に該当データフローのアクセスを要求する。要求の中身の一例として以下の様式が考えられる。

[0095] [IP header (抜粋)]

Src IP: Z', Z', Z', Z'

Dst IP: Z1, Z1, Z1, Z1

[TCP header (抜粋)]

Src port: 26001

Dst port: 443

[Http request (抜粋)]

GET https://www.example.com

上記の要求によって、該当のデータフローについては、内部プロキシサーバ220がユーザ端末10に対するプロキシとなって動作を行う。

[0096] <情報収集方法の他の例>

上記のマネジメントフローの例では、プロキシ制御部180が共通アプリケーション管理部130のアプリケーション管理DBから必要な情報を収集するとしたが、それに加えて（又はそれに代えて）、アプリケーションキャッシュから情報を収集することとしてもよい。図20に、アプリケーション

キャッシュから収集した情報も利用して更新したプロキシ振り分けポリシー管理DB 182の例を示す。

[0097] この場合、プロキシ制御部180は、アプリケーション管理DBから対象SaaSに対応するFQDN一覧とIPアドレスに加えて、アプリケーションキャッシュから既にキャッシングされているIPアドレスも収集し、それらのIPアドレスをプロキシ振り分けポリシー管理DBにおいて想定される動作と紐付ける。また、プロキシ振り分けポリシー管理部182は定期的に共通アプリケーション管理部130と同期し、常にアプリケーション管理DBと、アプリケーションキャッシュの最新情報を保持する。

[0098] SaaSサーバのIPアドレスが随時変更されることから、上記のようにアプリケーションキャッシュの最新情報を保持することで、正確なIPアドレスに基づいた動作を実行できる。

[0099] <アプリケーション管理DB、アプリケーションキャッシュの定期更新について>

第1の実施の形態と第2の実施の形態に共通の動作として、図21に示すように、外部アプリケーション管理サーバ400から情報を取得することにより、共通アプリケーション管理部130が、アプリケーション管理DBを定期的に更新することとしてもよい。この場合の動作を図22のフローチャートを参照して説明する。なお、外部アプリケーション管理サーバ400には最新の情報が格納されているものとする。

[0100] S701) ポーリング

共通アプリケーション管理部130は、定期的に外部アプリケーション管理サーバ400にDBのアップデートがあるかどうかの問い合わせ（ポーリング）を行う。

[0101] S702) 更新

共通アプリケーション管理部130は、アップデートがあったことを検知すると、最新のデータを受信し、アプリケーション管理DBを更新する。

[0102] また、共通アプリケーション管理部130は、アプリケーションキャッシ

ュを定期的に更新してもよい。この場合、図23に示すように、アプリケーションキャッシュはレコード毎にタイマー値を保持する。共通アプリケーション管理部130は、アプリケーションキャッシュを監視し、レコードのデータが設定された時点から更新されずにタイマー値の期間が経過した時点で当該レコードを自動的に削除する。

[0103] SaaSサーバのIPアドレスは固定されておらず、随時変更されることから、上記のように更新機構を設けることで、正確なIPアドレスに基づいた動作を実行できる。

[0104] (実施の形態の効果等)

以上説明したように、本発明の実施の形態に係るアクセス装置100においては、SD-WANルーティング部140に加えて、共通アプリケーション管理部130と、DNS制御部120と、プロキシ制御部180を設けることとした。

[0105] DNS制御部120は共通アプリケーション管理部130を参照しながら、特定SaaSのデータフローの制御に追随し、それに関するDNSトラフィックの最適出口を判断・制御する。同様に、プロキシ制御部180は、共通アプリケーション管理部130を参照しながら、特定SaaSのデータフロー対し、既存プロキシを迂回させるようにルーティング制御を行う。さらに、DNS制御部120を経由して行われたDNSの問い合わせ結果であるSaaSサーバのIPアドレスをアプリケーションキャッシュに随時反映し、アクセス先のSaaSサーバIPを用いて、特定SaaSを識別することができる。

[0106] 上記のような構成を備えるアクセス装置100により、特定SaaSのデータフローをブランチ拠点から直接にブレイクアウトさせる際に、該当SaaSアクセスに関するDNSトラフィックや、プロキシへのルーティングをそれに合わせて連動的に制御することが可能となり、該当SaaSへの最適アクセスが実現される。

[0107] すなわち、DNSフローとデータフローの出口を一致させることによって

、ブランチ拠点の最寄りのSaaSサーバへアクセスすることが可能となる。また、既存プロキシをバイパスすることによって、該当SaaSアクセスに起因するプロキシ処理負荷を軽減することが期待できる。さらに、最新のDNSの問い合わせ結果を用いて、First Packetで特定SaaSを識別できる。

[0108] (実施の形態のまとめ)

以上、説明したとおり、本実施の形態により、少なくとも下記の制御装置、制御方法、及びプログラムが提供される。

(第1項)

複数の網に接続され、ユーザ端末から受信したパケットを当該複数の網のうちのいずれかの網に振り分ける制御装置であって、

前記ユーザ端末から送信されたDNS問い合わせパケットを受信し、当該DNS問い合わせパケットの問い合わせ対象に基づいて、当該DNS問い合わせパケットを前記複数の網のうちのいずれかの網に振り分けるDNS制御部と、

パケットを受信し、当該パケットの宛先アドレスに基づいて当該パケットの送信先を決定し、決定された送信先に当該パケットを送信するルーティング部と

を備える制御装置。

(第2項)

前記制御装置は、パケットの宛先アドレスと当該パケットの宛先のアプリケーションとを対応付けた情報を格納するアプリケーションテーブルを備え、

前記ルーティング部は、前記アプリケーションテーブルを参照することにより、受信したパケットの宛先アドレスに対応するアプリケーションを把握し、当該アプリケーションに対して予め定められたポリシーに従って当該パケットを前記複数の網のうちのいずれかの網に振り分ける

第1項に記載の制御装置。

(第3項)

前記ルーティング部は、前記DNS問い合わせパケットの問い合わせ対象と、問い合わせの応答として受信したアドレスとを用いて前記アプリケーションテーブルを更新する

第2項に記載の制御装置。

(第4項)

前記アプリケーションテーブルは、レコード毎にタイマー値を有し、当該タイマー値の期間が経過したレコードを削除する

第2項又は第3項の制御装置。

(第5項)

前記DNS制御部は、前記DNS問い合わせパケットの宛先アドレスを、当該DNS問い合わせパケットの振り分け先に応じて書き換える

第1項ないし第4項のうちいずれか1項に記載の制御装置。

(第6項)

前記制御装置は所定のプロキシ装置に接続されており、前記制御装置は、受信したパケットのアクセス先のアプリケーションに基づいて、当該パケットを前記プロキシ装置に送信するか否かを決定するプロキシ制御部

を更に備える第1項ないし第5項のうちいずれか1項に記載の制御装置。

(第7項)

前記プロキシ制御部は、

アプリケーション毎の宛先アドレスと動作とを記録したプロキシ振り分けテーブルを備え、当該プロキシ振り分けテーブルを参照することにより、パケットを前記プロキシ装置に送信するか否かの決定を行い、

前記アプリケーションテーブルを利用して前記プロキシ振り分けテーブルを更新する

第2項ないし第4項のうちいずれか1項に従属する第6項に記載の制御装置。

(第8項)

前記制御装置は、

アプリケーションの情報を管理するアプリケーション管理データベースと

、

外部のアプリケーション管理サーバに定期的にアクセスすることにより、

前記アプリケーション管理データベースを更新する管理部と

を備える第１項ないし第７項のうちいずれか１項に記載の制御装置。

(第９項)

複数の網に接続され、ユーザ端末から受信したパケットを当該複数の網のうちのいずれかの網に振り分ける制御装置が実行する制御方法であって、

前記ユーザ端末から送信されたDNS問い合わせパケットを受信し、当該DNS問い合わせパケットの問い合わせ対象に基づいて、当該DNS問い合わせパケットを前記複数の網のうちのいずれかの網に振り分けるステップと

、

パケットを受信し、当該パケットの宛先アドレスに基づいて当該パケットの送信先を決定し、決定された送信先に当該パケットを送信するステップとを備える制御方法。

(第１０項)

コンピュータを、第１項ないし第８項のうちいずれか１項に記載の制御装置における各部として機能させるためのプログラム。

[0109] 以上、本実施の形態について説明したが、本発明はかかる特定の実施形態に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

[0110] 本特許出願は２０１８年９月２０日に出願した日本国特許出願第２０１８－１７６６３０号に基づきその優先権を主張するものであり、日本国特許出願第２０１８－１７６６３０号の全内容を本願に援用する。

符号の説明

[0111] １０ ユーザ端末

２０ 閉域網

- 3 0 インターネット
 - 1 0 0 アクセス装置
 - 1 1 0 指令受信部
 - 1 2 0 D N S 制御部
 - 1 2 1 D N S 振り分け部
 - 1 2 2 D N S 振り分けポリシー管理部
 - 1 2 3 問い合わせ先変更部
 - 1 3 0 共通アプリケーション管理部
 - 1 4 0 S D - W A N ルーティング部
 - 1 4 1 アプリ検知部
 - 1 4 2 ルーティング制御部
 - 1 4 3 ルーティングポリシー管理部
 - 1 5 0 閉域網接続 I F
 - 1 6 0 I n t e r n e t 接続 I F
 - 1 7 0 L A N - I F
 - 1 8 0 プロキシ制御部
 - 1 8 1 プロキシ振り分け部
 - 1 8 2 プロキシ振り分けポリシー管理部
 - 2 1 0 内部 D N S サーバ
 - 2 2 0 内部プロキシサーバ
 - 3 1 0 外部 D N S サーバ
 - 3 2 0 S a a S サーバ
 - 4 0 0 外部アプリケーション管理サーバ
- 1 0 0 0 ドライブ装置
 - 1 0 0 1 記録媒体
 - 1 0 0 2 補助記憶装置
 - 1 0 0 3 メモリ装置
 - 1 0 0 4 C P U

1 0 0 5 インターフェース装置

1 0 0 6 表示装置

1 0 0 7 入力装置

請求の範囲

- [請求項1] 複数の網に接続され、ユーザ端末から受信したパケットを当該複数の網のうちのいずれかの網に振り分ける制御装置であって、
- 前記ユーザ端末から送信されたDNS問い合わせパケットを受信し、当該DNS問い合わせパケットの問い合わせ対象に基づいて、当該DNS問い合わせパケットを前記複数の網のうちのいずれかの網に振り分けるDNS制御部と、
- パケットを受信し、当該パケットの宛先アドレスに基づいて当該パケットの送信先を決定し、決定された送信先に当該パケットを送信するルーティング部と
- を備える制御装置。
- [請求項2] 前記制御装置は、パケットの宛先アドレスと当該パケットの宛先のアプリケーションとを対応付けた情報を格納するアプリケーションテーブルを備え、
- 前記ルーティング部は、前記アプリケーションテーブルを参照することにより、受信したパケットの宛先アドレスに対応するアプリケーションを把握し、当該アプリケーションに対して予め定められたポリシーに従って当該パケットを前記複数の網のうちのいずれかの網に振り分ける
- 請求項1に記載の制御装置。
- [請求項3] 前記ルーティング部は、前記DNS問い合わせパケットの問い合わせ対象と、問い合わせの応答として受信したアドレスとを用いて前記アプリケーションテーブルを更新する
- 請求項2に記載の制御装置。
- [請求項4] 前記アプリケーションテーブルは、レコード毎にタイマー値を有し、当該タイマー値の期間が経過したレコードを削除する
- 請求項2又は3の制御装置。
- [請求項5] 前記DNS制御部は、前記DNS問い合わせパケットの宛先アドレ

スを、当該DNS問い合わせパケットの振り分け先に応じて書き換える

請求項1ないし4のうちいずれか1項に記載の制御装置。

[請求項6] 前記制御装置は所定のプロキシ装置に接続されており、前記制御装置は、

受信したパケットのアクセス先のアプリケーションに基づいて、当該パケットを前記プロキシ装置に送信するか否かを決定するプロキシ制御部

を更に備える請求項1ないし5のうちいずれか1項に記載の制御装置。

[請求項7] 前記プロキシ制御部は、

アプリケーション毎の宛先アドレスと動作とを記録したプロキシ振り分けテーブルを備え、当該プロキシ振り分けテーブルを参照することにより、パケットを前記プロキシ装置に送信するか否かの決定を行い、

前記アプリケーションテーブルを利用して前記プロキシ振り分けテーブルを更新する

請求項2ないし4のうちいずれか1項に従属する請求項6に記載の制御装置。

[請求項8] 前記制御装置は、

アプリケーションの情報を管理するアプリケーション管理データベースと、

外部のアプリケーション管理サーバに定期的にアクセスすることにより、前記アプリケーション管理データベースを更新する管理部と

を備える請求項1ないし7のうちいずれか1項に記載の制御装置。

[請求項9] 複数の網に接続され、ユーザ端末から受信したパケットを当該複数の網のうちのいずれかの網に振り分ける制御装置が実行する制御方法であって、

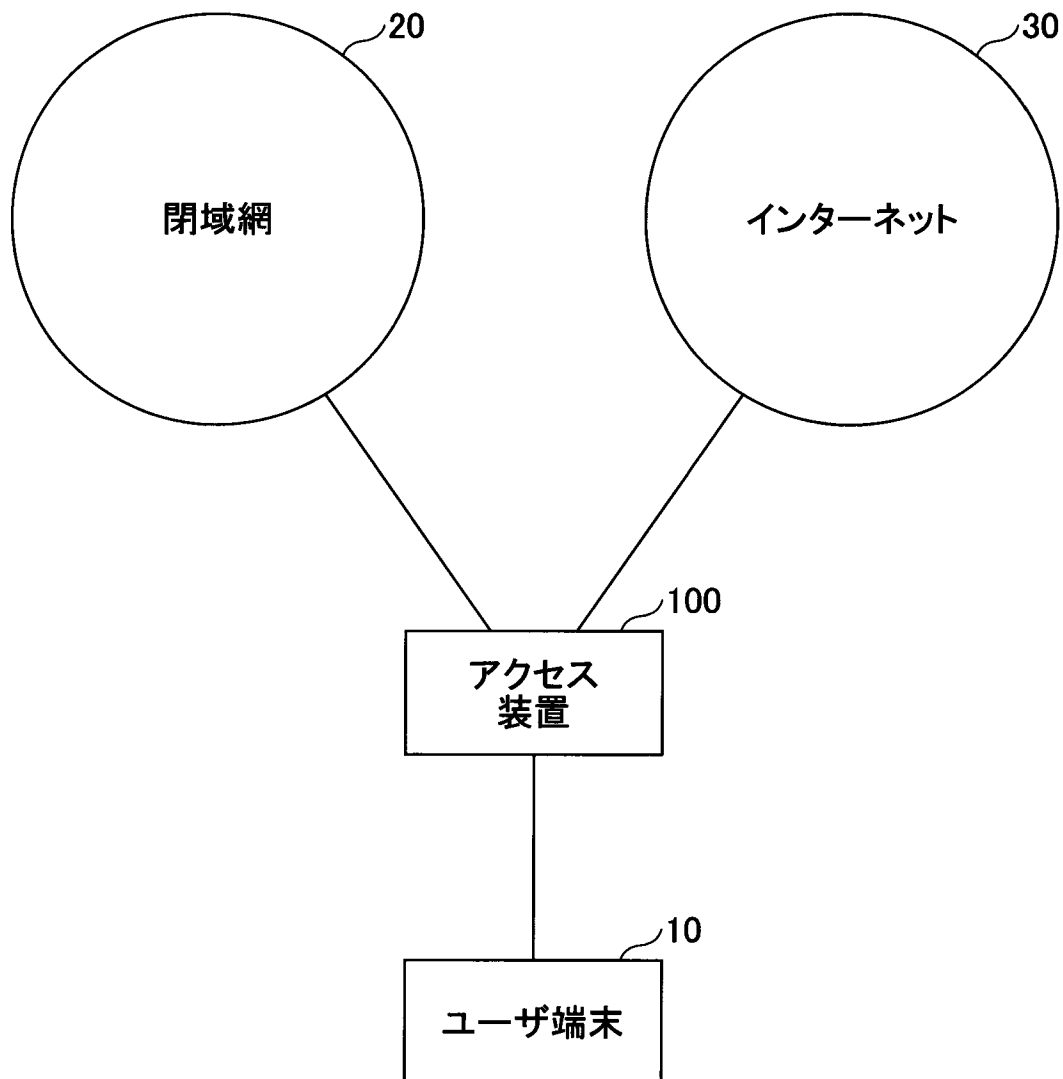
前記ユーザ端末から送信されたDNS問い合わせパケットを受信し、当該DNS問い合わせパケットの問い合わせ対象に基づいて、当該DNS問い合わせパケットを前記複数の網のうちのいずれかの網に振り分けるステップと、

パケットを受信し、当該パケットの宛先アドレスに基づいて当該パケットの送信先を決定し、決定された送信先に当該パケットを送信するステップと

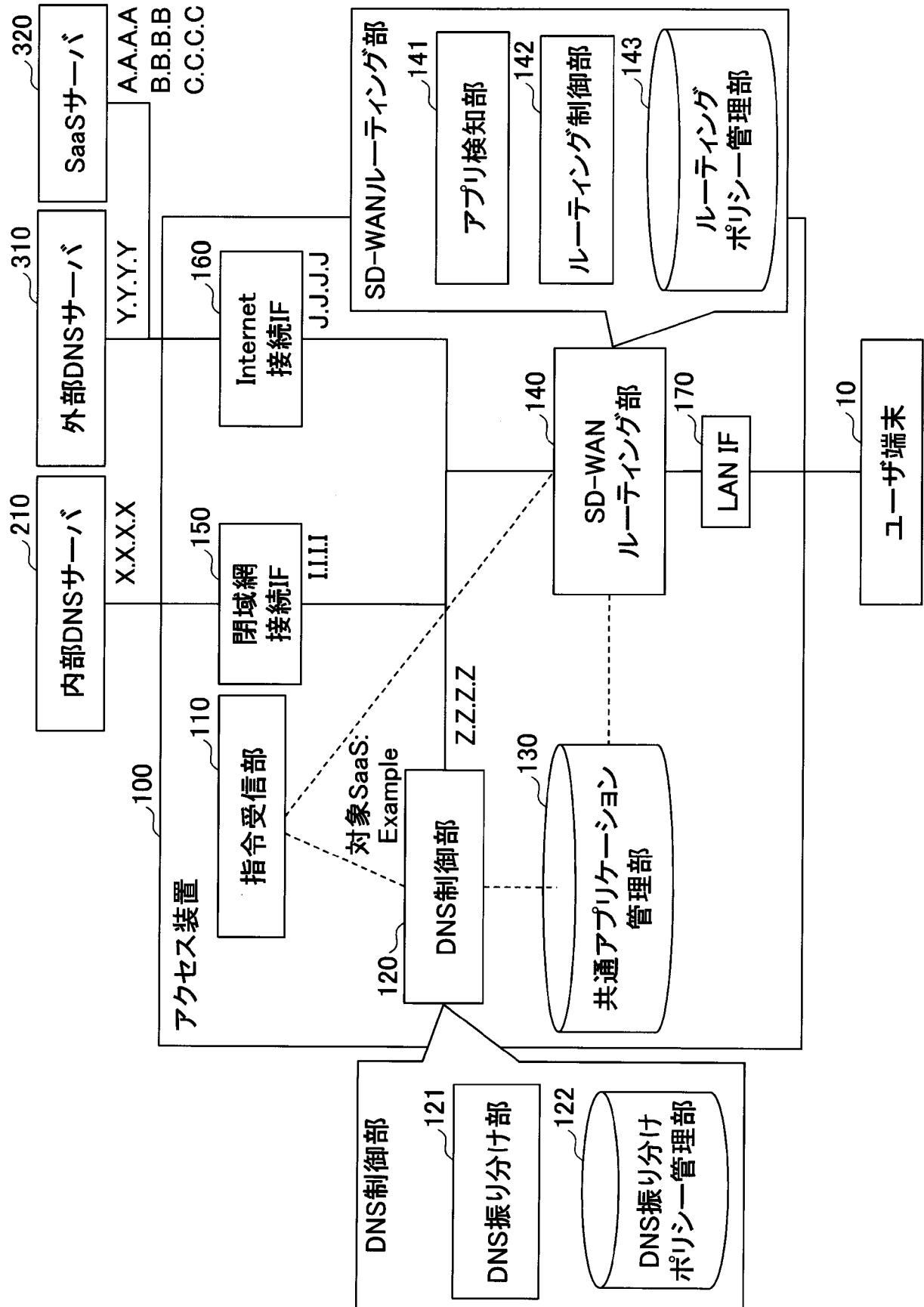
を備える制御方法。

[請求項10] コンピュータを、請求項1ないし8のうちいずれか1項に記載の制御装置における各部として機能させるためのプログラム。

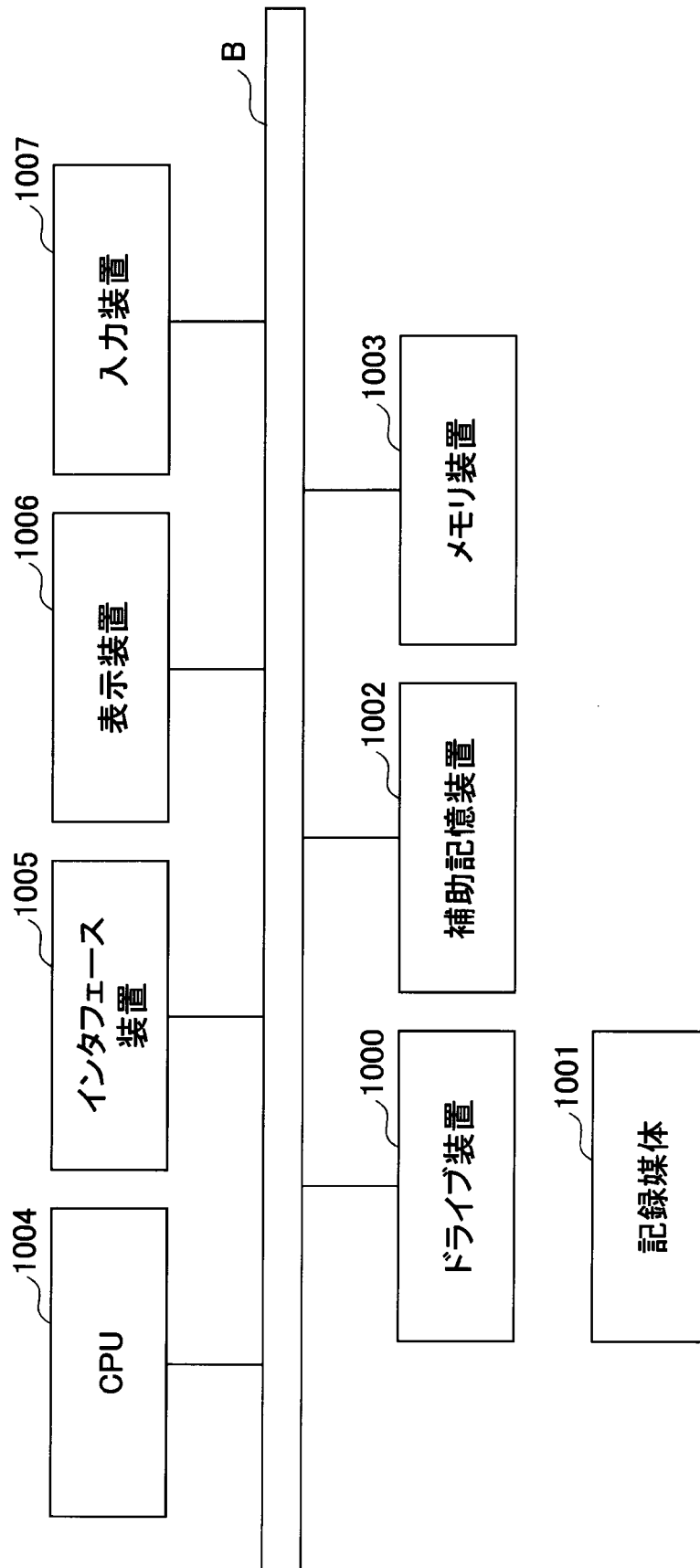
[図1]



[図2]



[図3]



[図4]

アプリケーション管理DB

アプリケーション名	FQDN	宛先IPアドレス
Example	Example.com	
		B.B.B.B/B
	Example365.com	

[図5]

(a)

アプリケーションキャッシュ

アプリケーション名	宛先IPアドレス
Example	B.B.B.B

(b)

アプリケーションキャッシュ(アプリ検知後)

アプリケーション名	宛先IPアドレス
Example	A.A.A.A
	B.B.B.B

[図6]

DNS振り分けポリシー管理DB

FQDN	動作	Next hop
Example.com	Forward	Y.Y.Y.Y
Example365.com	Forward	Y.Y.Y.Y
Default	Forward	X.X.X.X

[図7]

(a)

IPルーティングポリシー管理DB

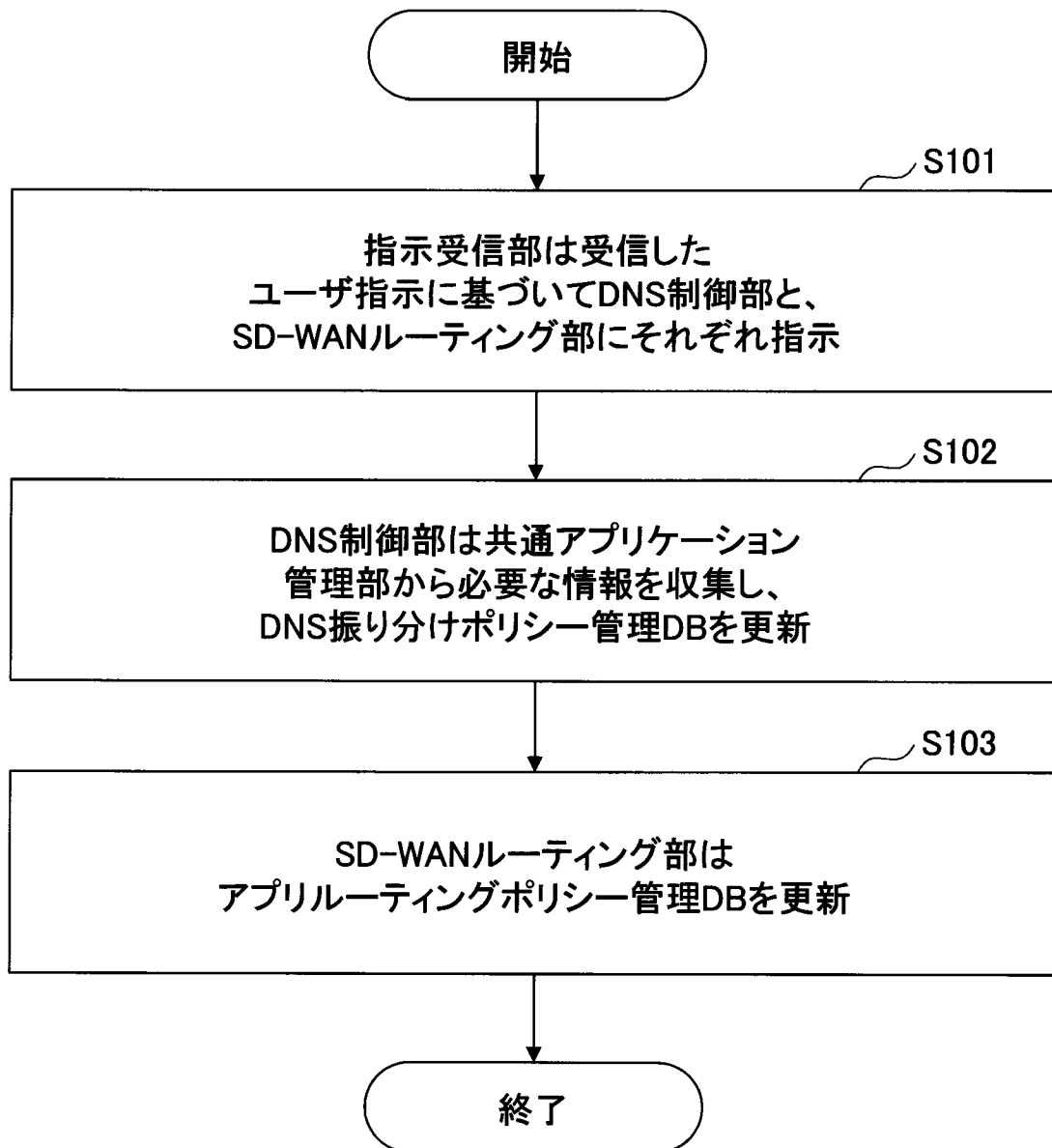
(b)

アプリケーションポリシー管理DB

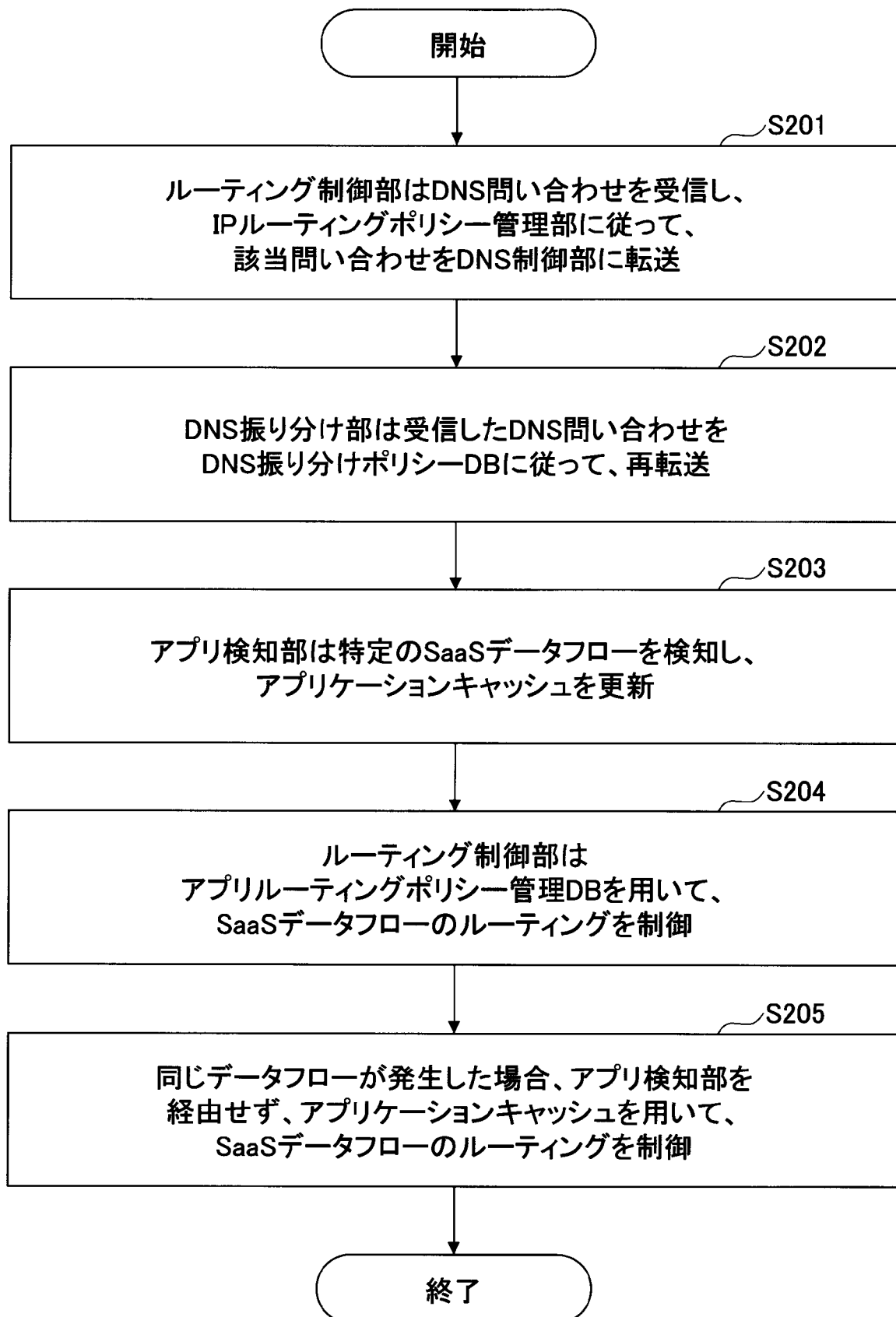
宛先IPアドレス	Next hop
X.X.X.X/X	I.I.I.I
Y.Y.Y.Y/Y	J.J.J.J
Z.Z.Z.Z/Z	Z.Z.Z.Z
Default	I.I.I.I

対象アプリ	Next hop
Example	J.J.J.J

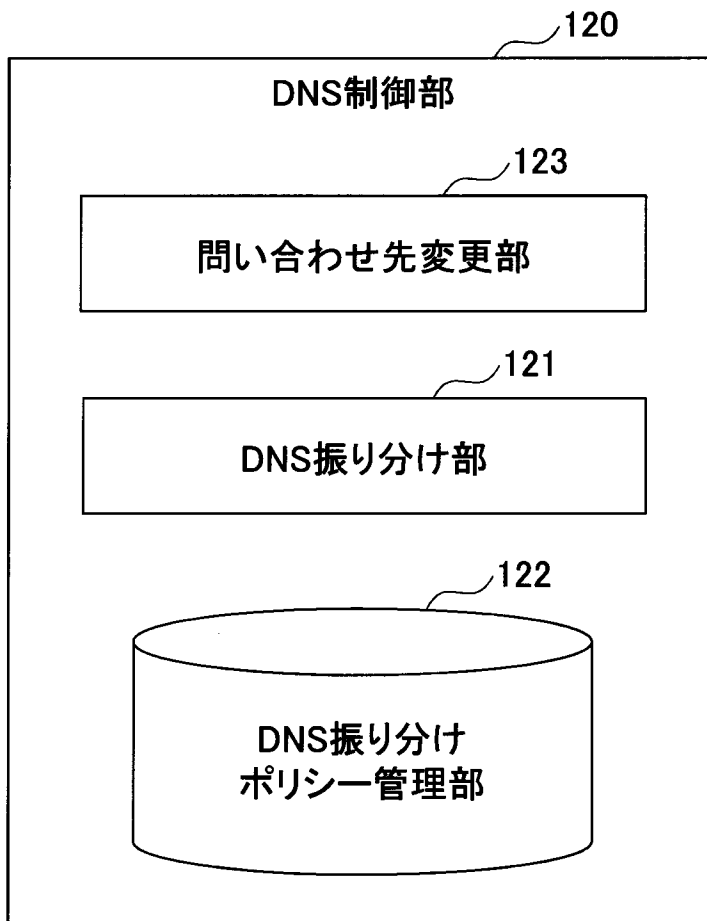
[図8]



[図9]



[図10]

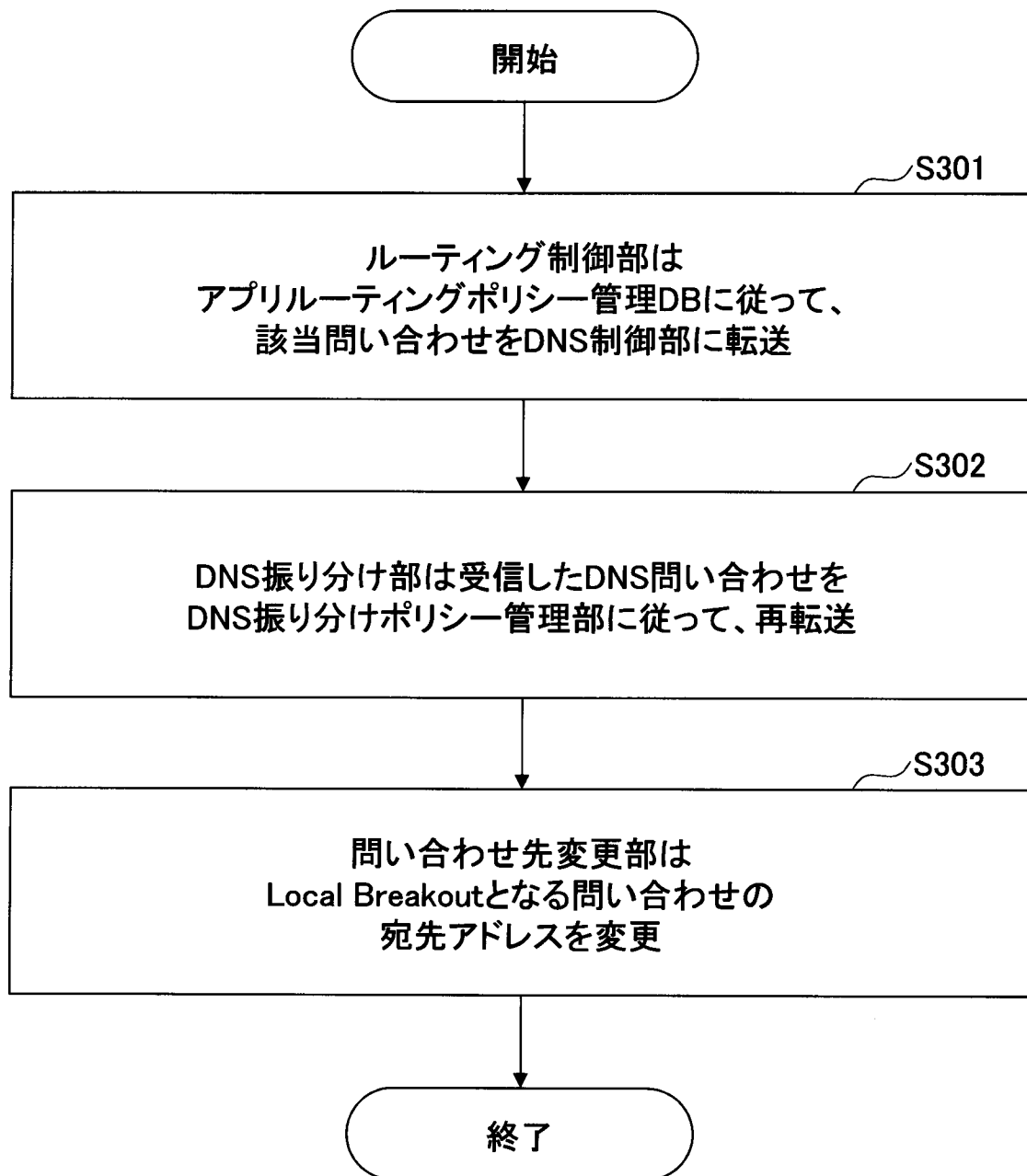


[図11]

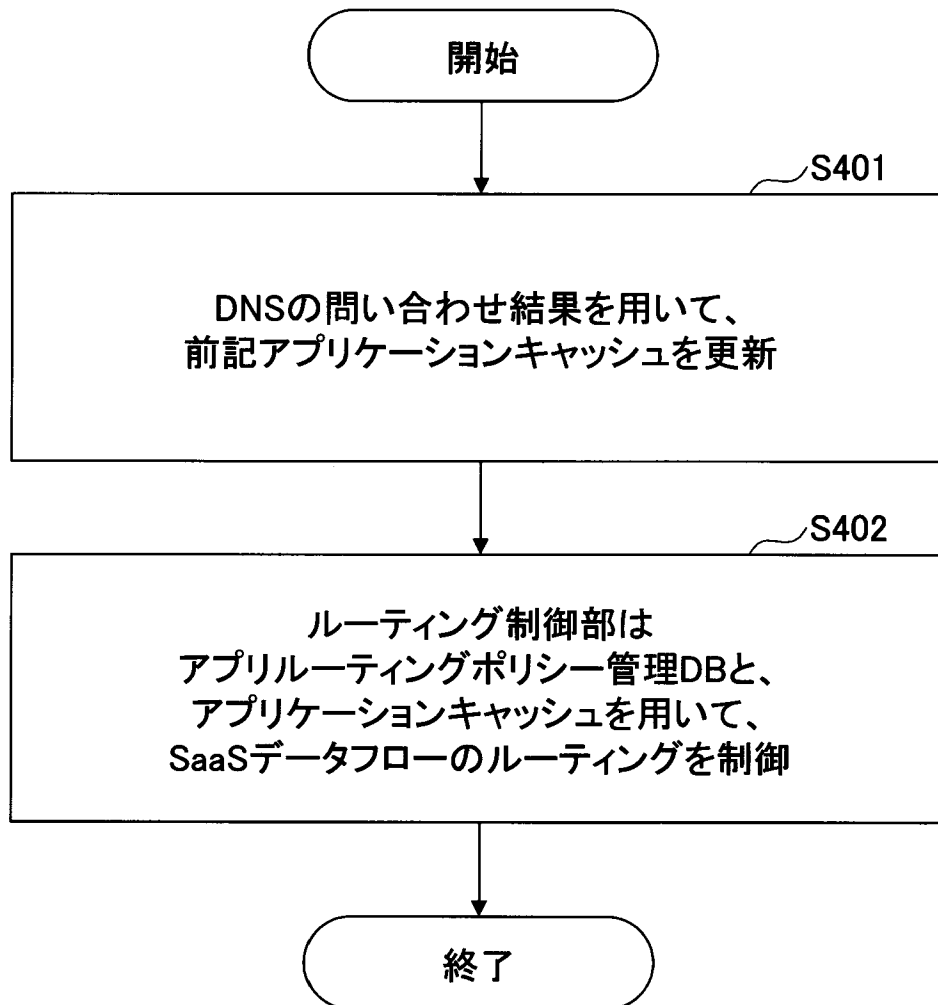
アプリケーションポリシー管理DB

対象アプリ	宛先ポート番号	Next hop
DNS	53	Z.Z.Z.Z
Example		J.J.J.J

[図12]



[図13]



[図14]

アプリケーションキヤッシュ

アプリケーション名	宛先IPアドレス
Example	A.A.A.A
	B.B.B.B
	C.C.C.C

[図16]

(a)

IPルーティングポリシー管理DB

宛先IPアドレス	Next hop
B.B.B.B/B	J.J.J.J
X.X.X.X/X	I.I.I.I
Y.Y.Y.Y/Y	J.J.J.J
Z.Z.Z.Z/Z	Z.Z.Z.Z
Z'.Z'.Z'.Z'/Z'	Z'.Z'.Z'.Z'
Default	I.I.I.I

(b)

アプリルーティングポリシー管理DB

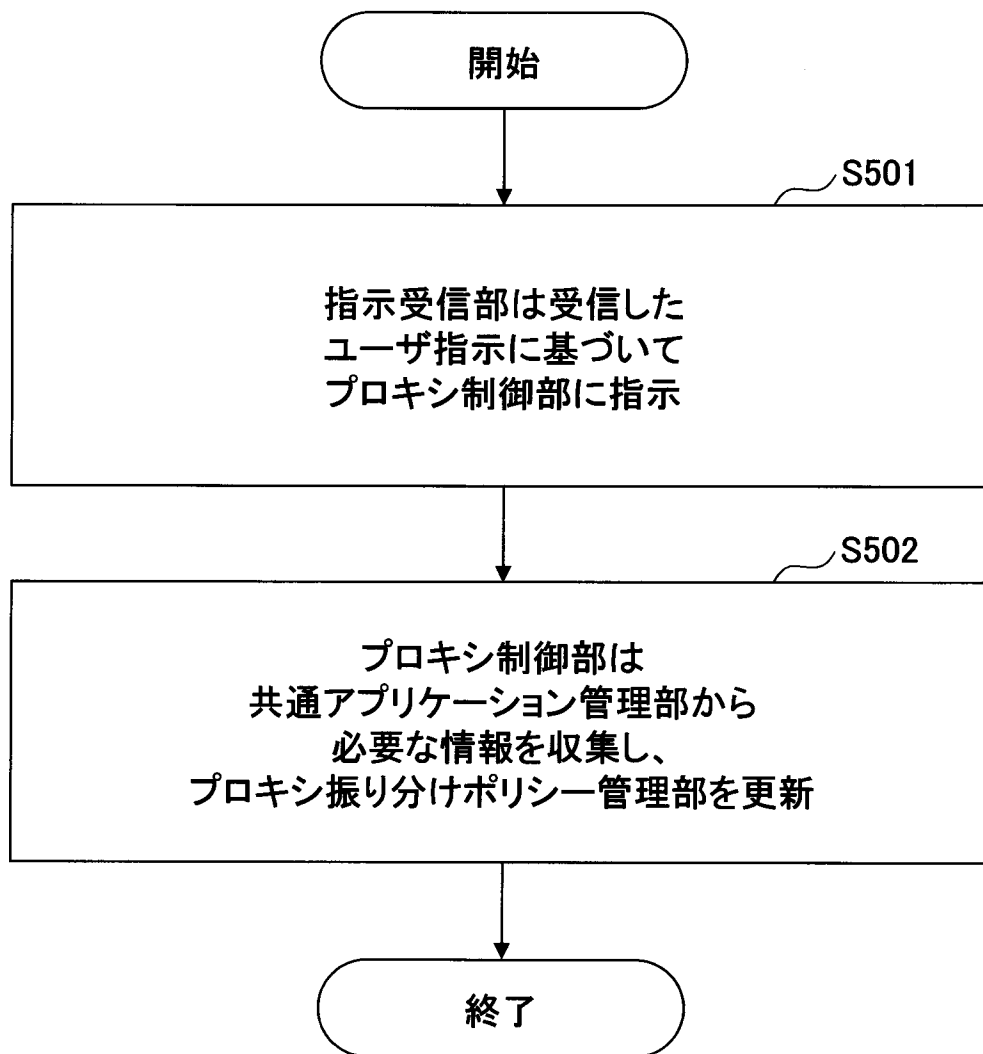
対象アプリ	Next hop
Example	J.J.J.J

[図17]

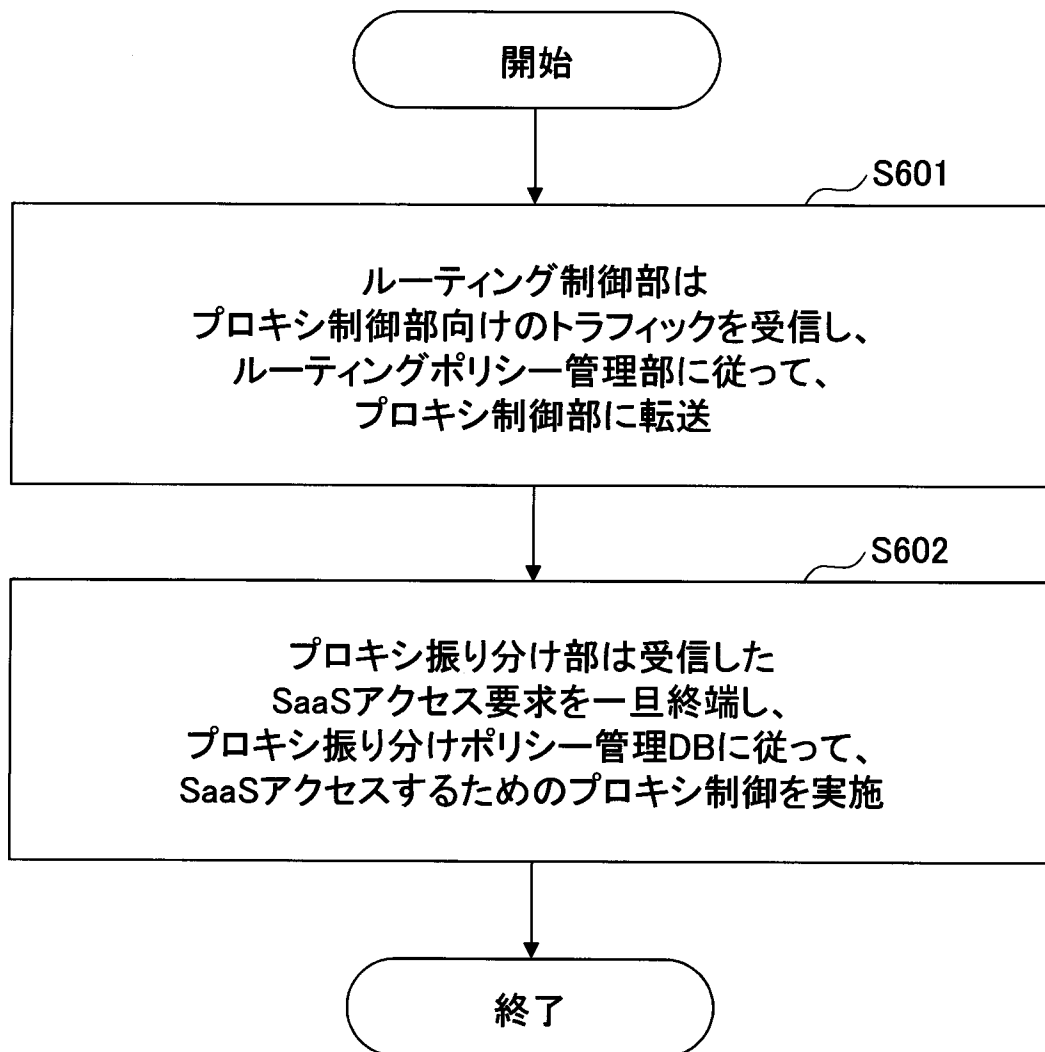
プロキシ振り分けポリシー管理DB

FQDN	IPアドレス	動作	Next hop
Example.com		パススルー	
	B.B.B.B		
Example365.com		パススルー	
Default		プロキシチェーニング	Z1.Z1.Z1.Z1

[図18]



[図19]

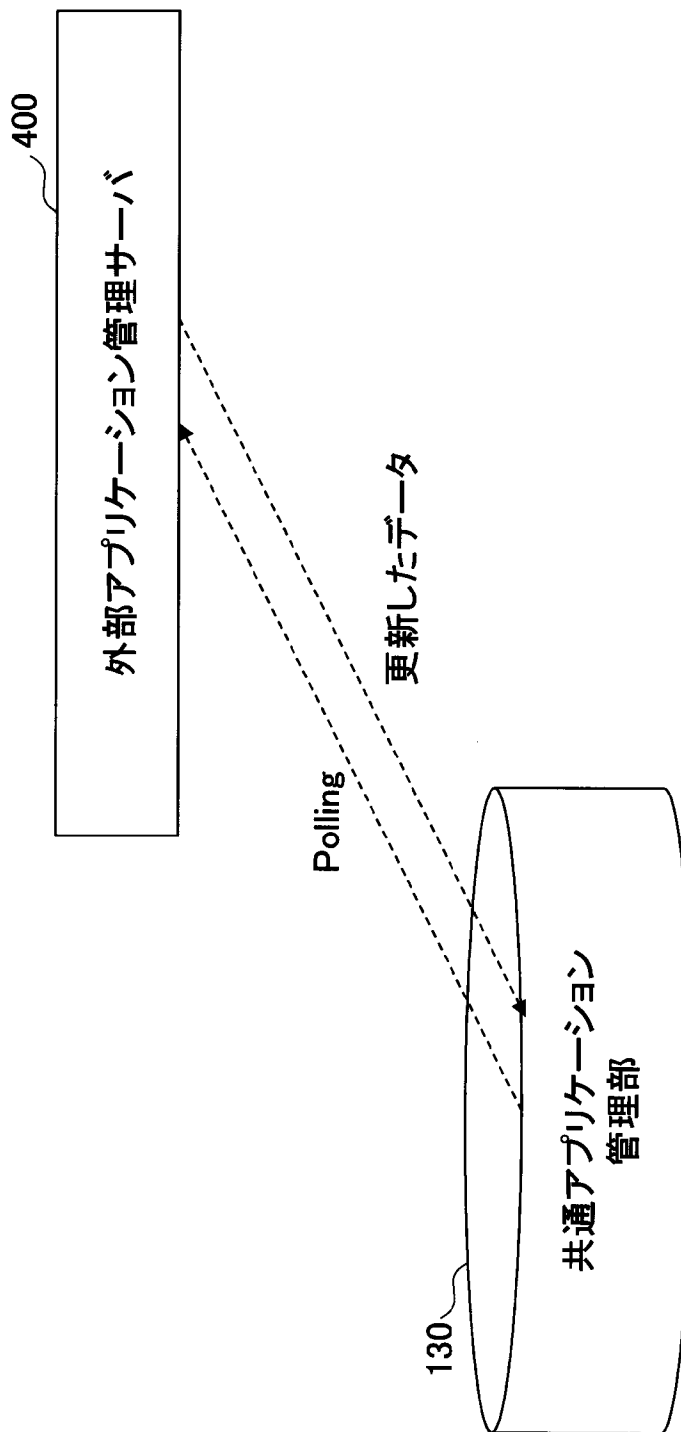


[図20]

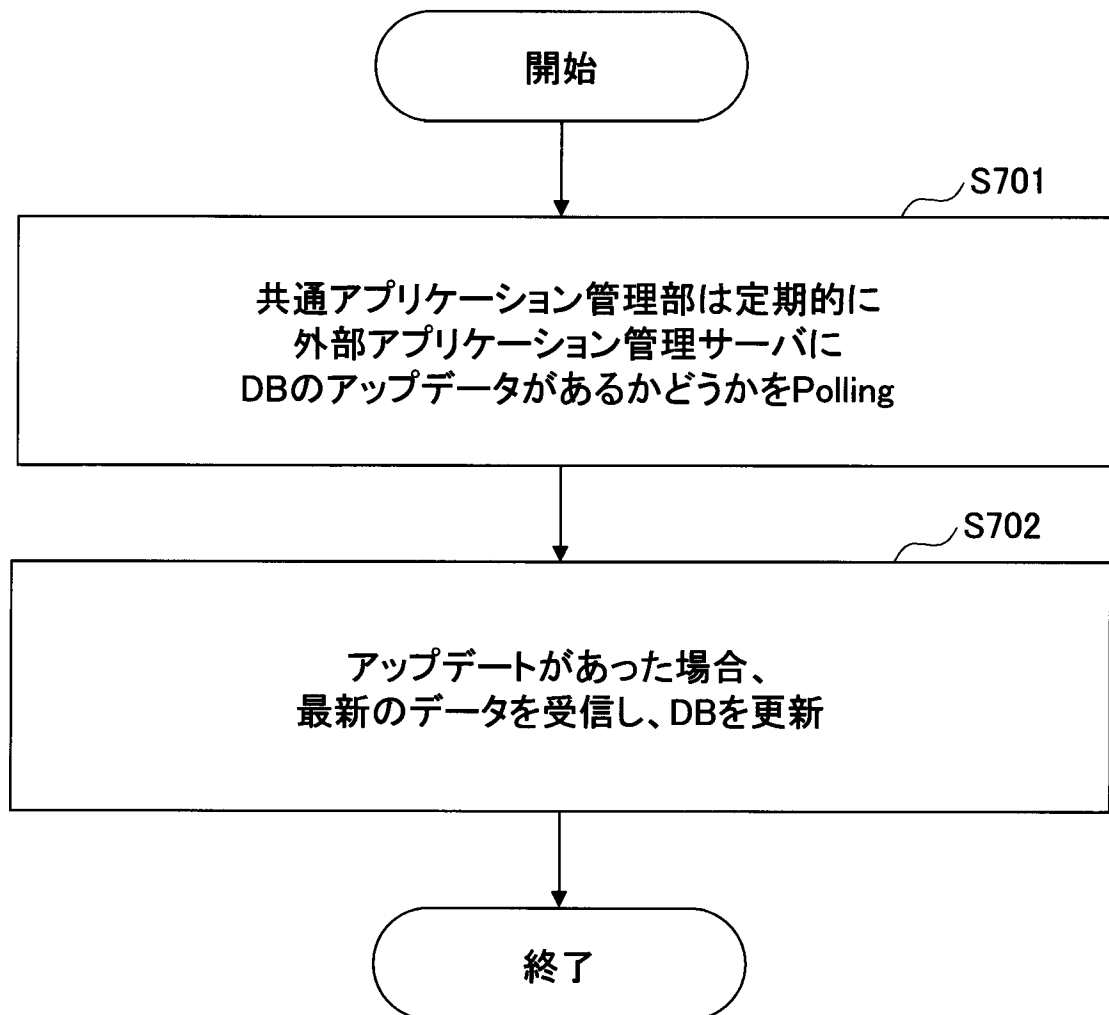
プロキシ振り分けポリシー管理DB

FQDN	IPアドレス	動作	Next hop
Example.com	A.A.A.A	パススルー	
	B.B.B.B	パススルー	
Example365.com	C.C.C.C	パススルー	
Default		プロキシチェーニング	Z1.Z1.Z1.Z1

[図21]



[図22]



[図23]

アプリケーションキャッシュ

アプリケーション名	宛先IPアドレス	Timer
Example	A.A.A.A	1 day
	B.B.B.B	無期限
	C.C.C.C	1 day

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/021061

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04L12/903 (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. H04L12/903, 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.
X A	インターネットブレイクアウトについて, [Online], 21 May 2018, [retrieved on 29 July 2019], Internet: < https://bonseed.hatenadiary.jp/entry/2018/05/21/232337 >, non-official translation (About Internet breakout)	1, 5, 6, 8-10 2-4, 7
A	JP 2005-159986 A (NEC CORPORATION) 16 June 2005 & US 2005/0117514 A1 & CN 1622545 A	1-10
A	JP 2005-229309 A (TOSHIBA CORPORATION) 25 August 2005 & US 2005/0111384 A1 & CN 1620044 A	1-10



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
29.07.2019

Date of mailing of the international search report
13.08.2019

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/JP2019/021061

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 2005-236480 A (NEC CORPORATION) 02 September 2005 (Family: none)	1-10

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04L12/903(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（I P C））

Int.Cl. H04L12/903, 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

国際調査で利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
X A	インターネットブレイクアウトについて、[オンライン], 2018.05.21, [検索日 2019.07.29], インターネット: < https://bonseed.hatenadiary.jp/entry/2018/05/21/232337 >	1, 5, 6, 8-10 2-4, 7
A	JP 2005-159986 A (日本電気株式会社) 2005.06.16, & US 2005/0117514 A1 & CN 1622545 A	1-10
A	JP 2005-229309 A (株式会社東芝) 2005.08.25, & US 2005/0111384 A1 & CN 1620044 A	1-10

☒ 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

29.07.2019

国際調査報告の発送日

13.08.2019

国際調査機関の名称及びあて先

日本国特許庁（I S A/J P）

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）

松崎 孝大

電話番号 03-3581-1101 内線 3596

5 X

4 0 6 0

C (続き) . 関連すると認められる文献		
引用文献の カテゴリ*	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 2005-236480 A (日本電気株式会社) 2005.09.02, (ファミリーなし)	1-10