(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
2022年12月29日(29.12.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/270228 A1

(51) 国際特許分類:
H04W 76/12 (2018.01) *H04W 12/033* (2021.01)

(21) 国際出願番号： PCT/JP2022/021655

(22) 国際出願日： 2022年5月26日(26.05.2022)

(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 2021-103687 2021年6月22日(22.06.2021) JP

(71) 出願人：株式会社ソラコム(**SORACOM, INC.**) [JP/JP]；〒1580094 東京都世田谷区玉川四丁目５番６号尾嶋ビル３階 Tokyo (JP).

(72) 発明者：川 上 大 喜 (**KAWAKAMI Taiki**)；〒1070052 東京都港区赤坂一丁目９番１３号三会堂ビル８階 株式会社ソラコム内 Tokyo (JP).
松井 基勝(**MATSUI Motokatsu**)；〒1070052 東京都港区赤坂一丁目９番１３号三会堂ビル８階 株式会社ソラコム内 Tokyo (JP).

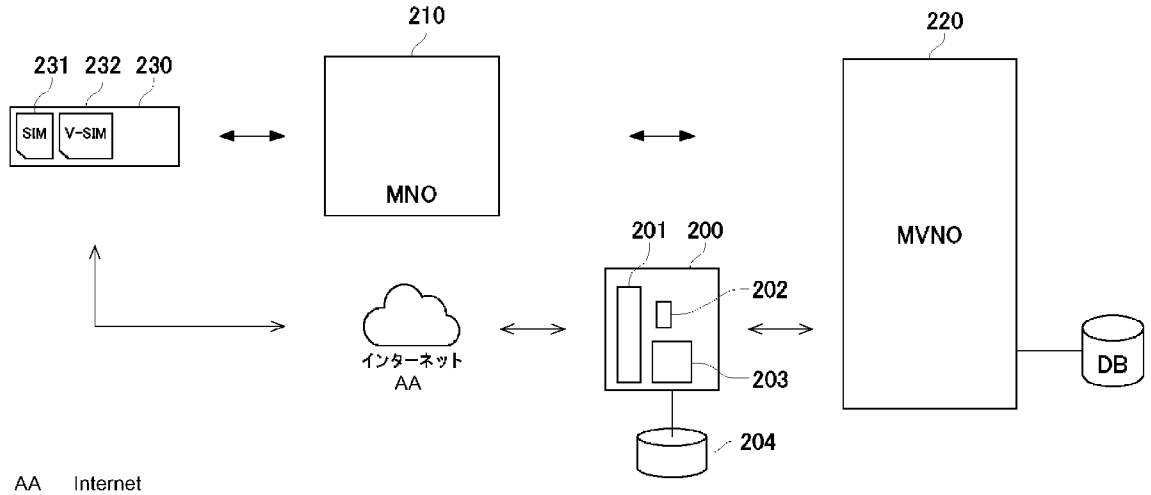
(74) 代理人：弁理士法人大塚国際特許事務所 (**OHTSUKA PATENT OFFICE, P.C.**)；〒1020094 東京都千代田区紀尾井町３番６号紀尾井町パークビル７Ｆ Tokyo (JP).

(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, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,

(54) Title: DEVICE AND METHOD FOR PROVIDING COMMUNICATION SERVICE FOR ACCESSING IP NETWORK, AND PROGRAM THEREFOR

(54) 発明の名称：ＩＰネットワークにアクセスするための通信サービスを提供するための装置、方法及びそのためのプログラム

[図2]



(57) Abstract: In the present invention, in a communication service for enabling an IoT device to access an IP network, a communication infrastructure connected to an MNO communication infrastructure is used to enable the access without going through a wireless access network for cellular communications. A device receives, from an IoT device, a session generation request including a communication service subscriber identifier, and transmits a provisioning call for a GTP tunnel between a first and a second instance included in a cloud communication infrastructure connected to the MNO communication infrastructure. An ID associated with the subscriber identifier and a transmission origin address serving as the transmission origin of a GTP-U session are received from the first or the second instance. A provisioning call including the transmission origin address and a public key is transmitted to the first instance, the provisioning call being

WO 2022/270228 A1

[続葉有]

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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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))

for a VPN tunnel between an IoT device and the first instance. Connection information is transmitted to an IoT device storing a private key corresponding to the public key.

(57) 要約:IoT機器がIPネットワークにアクセスするための通信サービスにおいて、MNOの通信インフラに接続される通信インフラを用いて、セルラー通信のための無線アクセスネットワークを介さずに当該アクセスを可能とする。装置が、IoT機器から、通信サービスの加入者識別子を含むセッション生成要求を受信し、MNOの通信インフラに接続されるクラウド上の通信インフラに含まれる第1及び第2のインスタンスの間のGTPトンネルのためのプロビジョニングコールを送信する。第1又は第2のインスタンスから、加入者識別子に関連づけられたID及びGTP-Uセッションの送信元となる送信元アドレスを受信する。第1のインスタンスにIoT機器と第1のインスタンスとの間のVPNトンネルのためのプロビジョニングコールであって、送信元アドレス及び公開鍵を含むプロビジョニングコールを送信する。公開鍵に対応する秘密鍵を記憶したIoT機器に接続情報を送信する。

明　細　書

発明の名称 ：

ＩＰネットワークにアクセスするための通信サービスを提供するための装置、方法及びそのためのプログラム

技術分野

[0001] 本発明は、IPネットワークにアクセスするための通信サービスを提供するための装置、方法及びそのためのプログラムに関する。

背景技術

[0002] セルラーネットワークを用いた無線通信サービスは、従来MNO（移動体通信事業者）により提供され、利用者はMNOと契約して当該MNOからSIMカードを受け取り、それを機器に装着することで利用を開始することができる。

[0003] 近年、MVNO（仮想移動体通信事業者）の登場により無線通信回線の小売が進んでおり、この場合、利用者はMNOではなくMVNOからSIMカードを受け取る。MVNOには、自社で一切通信インフラを有しない形態と、自社でも通信インフラを有し、その通信インフラをMNOの通信インフラに接続して無線通信サービスを提供する形態に大別することができる。後者（図１参照）は前者と比較して、自社でも通信インフラを有することから、一例として、通信速度、通信容量等の通信品質に応じた価格設定が可能であり、さまざまなニーズに応えることが試みられている。

[0004] 無線通信サービスに対するニーズとして近年顕著に増加しているのが、あらゆるモノに通信機能を加えてインターネットにつなげるIoTの動きである。以下、インターネットを含めてコンピュータネットワークに接続可能な機器を「IoT機器」と呼ぶ。SIMカードを装着することによって、IoT機器はセルラー通信を用いてIPネットワークにアクセス可能となる。

[0005] なお、MNOとMVNOの間に、MVNOが円滑な事業を行うための支援サービスを提供するMVNE（仮想移動体通信サービス提供者）が介在し、MVNEがMNOからSIMカードの提供を受けて、それをさらにMVNOに提供する場合もある。たとえば

、MVNEの通信インフラをMNOの通信インフラに接続して無線通信サービスを実現し、自社の通信インフラを有しないMVNOが小売を担うことが考えられる。

発明の概要

発明が解決しようとする課題

[0006] しかしながら、セルラー通信を用いずに、より具体的にはセルラー通信のための無線アクセスネットワークを用いずにIoT機器にIPネットワークへのアクセスを可能とすることも併用したい場合に、上述のようなMVNO又はMVNEにより提供される無線通信サービスとは別個の通信サービスを利用して各々を管理するか、複数の通信サービスを管理するための通信システムを自社で開発することが必要となり、これは管理コスト、開発コスト等のコスト増大を招く。

[0007] 本発明は、このような問題点に鑑みてなされたものであり、その目的は、MNOの通信インフラに接続される通信インフラを用いて、IoT機器に、IPネットワークにアクセスするための通信サービスを提供するための装置、方法及びそのためのプログラムにおいて、セルラー通信のための無線アクセスネットワークを介さずに当該アクセスを可能とすることにある。

[0008] また、本発明のより一般的な目的は、IoT機器がIPネットワークにアクセスするための通信サービスにおいて、MNOの通信インフラに接続される通信インフラを用いて、セルラー通信のための無線アクセスネットワークを介さずに当該アクセスを可能とすることにある。

[0009] なお、MNO、MVNO及びMVNEという用語は、その定義が異なることがある。本明細書においては、MNOは3GのSGSN、LTEのS-GWを通信インフラとして保有し、MVNO又はMVNEについては区別せず、MNOの通信インフラに接続される通信インフラを有する事業者と包括的に呼称することがある。当該事業者が保有する通信インフラとしては、3GのGGSN、LTEのP-GWが例として挙げられる。

[0010] また、上述の説明ではSIMカードがIoT機器に装着されることを例としているが、物理的なSIMカードに限らず、IoT機器に組み込まれた半導体チップ、IoT機器のモジュール内のセキュアなエリアに搭載されたソフトウェア等によ

り実装してよく、以下ではこれらを包含して「SIM」と呼ぶ。SIMは、当該SIMを識別するSIM識別子を記憶している。SIM識別子の例としては、IMSI、ICCID、MSISDN等が挙げられる。

課題を解決するための手段

[0011] 本発明は、このような問題点に鑑みてなされたものであり、その目的は、MNOの通信インフラに接続されるクラウド上の通信インフラが備える設備を用いて、IoT機器に、IPネットワークにアクセスするための通信サービスを提供するための方法であって、前記通信サービスの加入者を識別するための加入者識別子を含むセッション生成要求を受信するステップと、前記加入者識別子に関連づけてIDを記憶するステップと、前記設備に含まれる第１のインスタンス及び第２のインスタンスに、前記第１のインスタンスと前記第２のインスタンスとの間のGTP-Uセッションを生成するための第１のプロビジョニングコールであって、前記IDを含む第１のプロビジョニングコールを送信するステップと、前記第１のインスタンス又は前記第２のインスタンスから、前記第１のプロビジョニングコールの応答として、前記GTP-Uセッションの送信元となる送信元アドレスを受信するステップと、前記第１のインスタンスに、前記IoT機器と前記第１のインスタンスとの間のVPNセッションを生成するための第２のプロビジョニングコールであって、前記送信元アドレス及び第１のクレデンシャルを含む第２のプロビジョニングコールを送信するステップと、前記第１のクレデンシャル又は前記第１のクレデンシャルに対応する第２のクレデンシャルを記憶した前記IoT機器に向けて、前記送信元アドレス及び前記第１のインスタンスの宛先アドレスを含む接続情報を送信するステップと

を含む。

[0012] また、本発明の第２の態様は、第１の態様の方法であって、前記接続情報は、前記第１のインスタンスのポート番号を含む。

[0013] また、本発明の第３の態様は、第１の態様の方法であって、前記第１のクレデンシャルは、公開鍵であり、前記第２のクレデンシャルは、前記公開鍵

に対応する秘密鍵である。

[0014] また、本発明の第４の態様は、第１の態様の方法であって、前記セッション生成要求は、前記IoT機器から受信する。

[0015] また、本発明の第５の態様は、第１から第４のいずれかの態様の方法であって、前記第１のインスタンス及び前記第２のインスタンスは、クラウド又はパブリッククラウド上のインスタンスである。

[0016] また、本発明の第６の態様は、装置に、MNOの通信インフラに接続されるクラウド上の通信インフラが備える設備を用いて、IoT機器に、IPネットワークにアクセスするための通信サービスを提供するための方法を実行させるためのプログラムであって、前記方法は、前記通信サービスの加入者を識別するための加入者識別子を含むセッション生成要求を受信するステップと、前記加入者識別子に関連づけてIDを記憶するステップと、前記設備に含まれる第１のインスタンス及び第２のインスタンスに、前記第１のインスタンスと前記第２のインスタンスとの間のGTP-Uセッションを生成するための第１のプロビジョニングコールであって、前記IDを含む第１のプロビジョニングコールを送信するステップと、前記第１のインスタンス又は前記第２のインスタンスから、前記第１のプロビジョニングコールの応答として、前記GTP-Uセッションの送信元となる送信元アドレスを受信するステップと、前記第１のインスタンスに、前記IoT機器と前記第１のインスタンスとの間のVPNセッションを生成するための第２のプロビジョニングコールであって、前記送信元アドレス及び第１のクレデンシャルを含む第２のプロビジョニングコールを送信するステップと、前記第１のクレデンシャル又は前記第１のクレデンシャルに対応する第２のクレデンシャルを記憶した前記IoT機器に向けて、前記送信元アドレス及び前記第１のインスタンスの宛先アドレスを含む接続情報を送信するステップとを含む。

[0017] また、本発明の第７の態様は、MNOの通信インフラに接続されるクラウド上の通信インフラが備える設備を用いて、IoT機器に、IPネットワークにアクセスするための通信サービスを提供するための装置であって、前記通信サービ

スの加入者を識別するための加入者識別子を含むセッション生成要求を受信して、前記加入者識別子に関連づけてIDを記憶し、前記設備に含まれる第１のインスタンス及び第２のインスタンスに、前記第１のインスタンスと前記第２のインスタンスとの間のGTP-Uセッションを生成するための第１のプロビジョニングコールであって、前記IDを含む第１のプロビジョニングコールを送信して、前記第１のインスタンス又は前記第２のインスタンスから、前記第１のプロビジョニングコールの応答として、前記GTP-Uセッションの送信元となる送信元アドレスを受信し、前記第１のインスタンスに、前記IoT機器と前記第１のインスタンスとの間のVPNセッションを生成するための第２のプロビジョニングコールであって、前記送信元アドレス及び第１のクレデンシャルを含む第２のプロビジョニングコールを送信し、前記第１のクレデンシャル又は前記第１のクレデンシャルに対応する第２のクレデンシャルを記憶した前記IoT機器に向けて、前記送信元アドレス及び前記第１のインスタンスの宛先アドレスを含む接続情報を送信する。

[0018] また、本発明の第８の態様は、その間にGTP-Uセッションが生成された第１のインスタンス及び第２のインスタンスを有するクラウド上の通信インフラを用いて、IoT機器がIPネットワークにアクセスするための通信サービスを提供する方法であって、前記第１のインスタンスが、前記IoT機器から、前記IoT機器に格納されたクレデンシャル又は一時的なクレデンシャルによって暗号化されたIPパケットをカプセル化したVPNパケットを受信するステップと、前記第１のインスタンスが、前記VPNパケットに含まれる送信元アドレス又は一時的なキーに対応するクレデンシャル又は一時的なクレデンシャルを取得して、暗号化された前記IPパケットを復号化するステップと、前記第１のインスタンスが、復号化された前記IPパケットのヘッダに含まれる送信元アドレスに基づいて、前記第１のインスタンスに保持された、１又は複数の送信元アドレスと各送信元アドレスが割り当てられたGTPセッションの送信先との対応づけを参照して、前記第２のインスタンスを判定するステップと、前記第１のインスタンスが、前記第２のインスタンスに対して、復号化された前記I

PパケットをGTPペイロードとするGTPパケットを送信するステップと、前記第２のインスタンスが、前記GTPパケットからGTPヘッダを取り除いて、前記GTPペイロードであるIPパケットを前記通信インフラの外部又は内部のIPネットワークに送信するステップとを含む。

[0019] また、本発明の第９の態様は、その間にGTP-Uセッションが生成された、クラウド上の通信インフラに、IoT機器がIPネットワークにアクセスするための通信サービスを提供する方法を実行させるためのプログラムであって、前記方法は、前記通信インフラが有する第１のインスタンスが、前記IoT機器から、前記IoT機器に格納されたクレデンシャル又は一時的なクレデンシャルによって暗号化されたIPパケットをカプセル化したVPNパケットを受信するステップと、前記第１のインスタンスが、前記VPNパケットに含まれる送信元アドレス又は一時的なキーに対応するクレデンシャル又は一時的なクレデンシャルを取得して、暗号化された前記IPパケットを復号化するステップと、前記第１のインスタンスが、復号化された前記IPパケットのヘッダに含まれる送信元アドレスに基づいて、前記第１のインスタンスに保持された、１又は複数の送信元アドレスと各送信元アドレスが割り当てられたGTPセッションの送信先との対応づけを参照して、前記通信インフラが有する第２のインスタンスであって、前記通信インフラの外部又は内部のIPネットワークにIPパケットを送信可能な第２のインスタンスを判定するステップと、前記第１のインスタンスが、前記第２のインスタンスに対して、復号化された前記IPパケットをGTPペイロードとするGTPパケットを送信するステップとを含む。

[0020] また、本発明の第１０の態様は、IoT機器がIPネットワークにアクセスするための通信サービスを提供するためのクラウド上の通信インフラであって、その間にGTP-Uセッションが生成された第１のインスタンス及び第２のインスタンスを有し、前記第１のインスタンスが、前記IoT機器から、前記IoT機器に格納されたクレデンシャル又は一時的なクレデンシャルによって暗号化されたIPパケットをカプセル化したVPNパケットを受信し、前記VPNパケットに含まれる送信元アドレス又は一時的なキーに対応するクレデンシャル又は一

時的なクレデンシャルを取得して、暗号化された前記IPパケットを復号化し、前記第１のインスタンスが、復号化された前記IPパケットのヘッダに含まれる送信元アドレスに基づいて、前記第１のインスタンスに保持された、１又は複数の送信元アドレスと各送信元アドレスが割り当てられたGTPセッションの送信先との対応づけを参照して、前記第２のインスタンスを判定して、前記第２のインスタンスに対して、復号化された前記IPパケットをGTPペイロードとするGTPパケットを送信し、前記第２のインスタンスが、前記GTPパケットからGTPヘッダを取り除いて、前記GTPペイロードであるIPパケットを前記通信インフラの外部又は内部のIPネットワークに送信する。

[0021] 本発明の一態様によれば、VPNトンネルによってインターネット等のIPネットワーク上で秘匿回線が与えられ、ＩｏＴ機器は、当該秘匿回線を通じて、MNOの通信インフラに接続される通信インフラであって、GTPトンネルを通じてIPネットワークにデータを送信し、IPネットワークからデータを受信することのできる通信インフラに、無線アクセスネットワークを介さずに接続可能となる。

図面の簡単な説明

[0022] [図1]自社の通信インフラをMNOの通信インフラに接続して無線通信サービスを提供するMVNOを模式的に示す図である。

[図2]本発明の一実施形態にかかるIPネットワークにアクセスするための通信サービスを提供するための装置を示す図である。

[図3A]本発明の一実施形態にかかるIPネットワークにアクセスするための通信サービスを提供するための方法の流れを示す図である。

[図3B]本発明の一実施形態にかかるIPネットワークにアクセスするための通信サービスを提供するための方法の流れを示す図である。

[図4]本発明の一実施形態にかかるIoT機器がIPネットワークにアクセスするための通信サービスにおけるデータ送信の流れを示す図である。

発明を実施するための形態

[0023] 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。

[0024] 図２に、本発明の一実施形態にかかるIPネットワークにアクセスするための通信サービスを提供するための装置を示す。装置２００は、MNOの通信インフラ２１０に接続されるMVNOの通信インフラ２２０及びIoT機器２３０とIPネットワーク上で通信する。装置２００は、IoT機器２３０がIPネットワークにアクセスするための接続を確立するためのものであるため、接続装置とも呼ぶ。MVNOの通信インフラ２２０は、クラウド又はパブリッククラウド上の複数のインスタンスにより構成される。

[0025] ここで、本明細書において「クラウド」とは、ネットワーク上で需要に応じてCPU、メモリ、ストレージ、ネットワーク帯域などのコンピューティングリソースを動的にプロビジョニングし、提供できるシステムを言う。たとえば、AWS等によりクラウドを利用することができる。また、本明細書において「パブリッククラウド」とは、複数のテナントがコンピューティングリソースの提供を受けることが可能なクラウドを言う。

[0026] 装置２００は、通信インターフェースなどの通信部２０１と、プロセッサ、CPU等の処理部２０２と、メモリ、ハードディスク等の記憶装置又は記憶媒体を含む記憶部２０３とを備え、各処理を行うためのプログラムを実行することによって構成することができる。装置２００は、１又は複数の装置、コンピュータないしサーバを含むことがある。また、当該プログラムは、１又は複数のプログラムを含むことがあり、また、コンピュータ読み取り可能な記憶媒体に記録して非一過性のプログラムプロダクトとすることができる。当該プログラムは、記憶部２０３又は装置２００からＩＰネットワークを介してアクセス可能なデータベース２０４等の記憶装置又は記憶媒体に記憶しておき、処理部２０２において実行することができる。以下で記憶部２０３に記憶されるものとして記述されるデータはデータベース２０４に記憶してもよく、またその逆も同様である。

[0027] 装置２００は、クラウド又はパブリッククラウド上の１又は複数のインスタンスとすることができ、MVNOの通信インフラ２２０と同一のクラウド上の１又は複数のインスタンスとしてもよい。MVNOの通信インフラ２２０が有す

る各インスタンスは、図示していないが、接続装置２００と同様のハードウェア構成とすることができる。

[0028] 以下では、まず、通信サービスに必要なセッションの生成につき説明し、その後に、生成されたセッションを用いたIPネットワークへのデータの送信について説明する。

[0029] セッションの生成

図３Ａ及び３Ｂに、本発明の一実施形態にかかるIPネットワークにアクセスするための通信サービスを提供するための方法の流れを示す。まず、装置２００は、IoT機器２３０から、当該通信サービスの加入者を識別するための加入者識別子を含むセッション生成要求を受信する（Ｓ３０１）。当該セッション生成要求は、セルラー回線以外のインターネット通信回線によって送信可能であり、一例として、固定インターネット回線によって送信してもよく、セルラー回線を経て送信してもよい。

[0030] 図２では、IoT機器２３０には、MVNOの通信インフラ２２０を用いて、無線アクセスネットワークを介して提供されるIPネットワークにアクセスするための通信サービスを利用するためのSIMを識別するSIM識別子２３１が格納されていることに加えて、無線アクセスネットワークを介さずに提供されるIPネットワークにアクセスするための通信サービスを利用するための加入者識別子２３２が格納されている。図２において、加入者識別子２３２はこれを用いて接続が確立された際に仮想的なSIM識別子と考えられることから、「V-SIM (Virtual SIM)」と便宜上示している。また、IoT機器２３０には、セッション生成要求を正当に行うためのトークンが格納されていてもよい。IoT機器２３０には、必ずしもSIM識別子２３１が格納されていなくてもよい。

[0031] 接続装置２００は、受信したセッション生成要求に含まれるトークンを必要に応じて検証した後に、当該セッション生成要求に含まれる加入者識別子２３２に関連づけてIDを生成して記憶する（Ｓ３０２）。なお、セッション生成要求は、IoT機器２３０のために、加入者識別子２３２に正当にアクセス可能なIoT機器２３０以外の装置から接続装置２００に送信することも考えら

れる。

[0032] IoT機器２３０以外の装置としては、一例として、IoT機器２３０を管理する管理者が用いるコンピュータが挙げられる。当該管理者は、加入者識別子２３２にアクセス可能であり、接続装置２００に対してセッション生成要求を行うために必要なトークンが付与されていれば、当該トークンを用いて、加入者識別子２３２を含むセッション生成要求を、IoT機器２３０のために行うことができる。また、別の例として、IoT機器２３０以外の装置としては、IoT機器２３０に格納されたSIM識別子２３１を用いてIoT機器２３０を認証してIoT機器２３０との間で秘匿回線を確立可能な認証サーバが挙げられる。確立された秘匿回線を通じてIoT機器２３０から加入者識別子２３２を受信した当該認証サーバは、加入者識別子２３２に正当にアクセスしていると言える。SIM識別子２３１により識別されるSIMが、MNOの通信インフラ２１０に接続される通信インフラ２２０を有する事業者により発行されている場合、当該認証サーバは通信インフラ２２０が有する設備に含まれる１又は複数のインスタンスとすることができる。

[0033] 次に、接続装置２００は、通信インフラ２２０が有する第１のインスタンス及び第２のインスタンスを採択し（Ｓ３０３）、当該第２のインスタンスに対して、当該第１のインスタンスと前記第２のインスタンスとの間のGTP-Uセッションを生成するためのプロビジョニングコールを送信する（Ｓ３０４）。このプロビジョニングコールは、接続装置２００に記憶された当該ID及び接続装置２００が採択した当該第１のインスタンスのIPアドレス、ホスト名等の第１の宛先アドレスを含むことができる。

[0034] 当該第１のインスタンスは、第１のノード群から採択し、当該第２のインスタンスは、第２のノード群から採択することができる。各インスタンスは、複数のサーバを含み、各インスタンスがデータを受信するサーバと、そこからデータを送信するサーバが異なってもよい。MVNOの通信インフラ２２０がIoT機器２３０に無線アクセスネットワークを介したIPネットワークへのアクセスを提供する際には、MNOの通信インフラ２１０に接続される第１のサー

バ群から採択された第１のサーバと、当該第１のサーバと接続される、第２のサーバ群から採択された第２のサーバが用いられる。第２のノード群の少なくとも一部は、第２のサーバ群の少なくとも一部と同一とすることができる。

[0035] 当該第２のインスタンスは、当該第２のインスタンスに対するプロビジョニングコールの応答を接続装置２００に送信する（Ｓ３０５）。そして、当該第２のインスタンスは、GTP-Uセッションの待ち受け状態となる（Ｓ３０６）。当該応答には、当該ID及び当該GTP-Uセッションに対する送信元となるIPアドレス等の送信元アドレスを含むことができ、当該送信元アドレスは、当該第２のインスタンスが採択することができる。また、ここでは、応答を送信した後に待ち受け状態となるものとして記述したが、この順序は逆でもよい。送信元アドレスは、当該第２のインスタンスではなく、接続装置２００において割り当ててもよい。この場合には、第２のインスタンスへのプロビジョニングコールに送信元アドレスを含めてもよい。いずれにしても、当該第２のインスタンスは、当該IDに関連づけて当該送信元アドレスを記憶することができる。また、装置２００においては、加入者識別子２３２に関連づけて当該送信元アドレスを記憶することができる。

[0036] 次いで、接続装置２００は、当該第１のインスタンスに対して、当該第１のインスタンスと当該第２のインスタンスとの間のGTP-Uセッションを生成するためのプロビジョニングコールを送信する（Ｓ３０７）。このプロビジョニングコールは、接続装置２００に記憶された当該ID、送信元アドレス及び接続装置２００が採択した当該第２のインスタンスの第２の宛先アドレスを含むことができる。

[0037] その後、当該第１のインスタンスは、GTP-Uセッションの待ち受け状態となる（Ｓ３０８）。

ここで、当該第１のインスタンスと当該第２のインスタンスとの間でGTP-Uセッションが生成され、いわゆるGTPトンネルが確立した状態となる。接続装置２００は、当該第１のインスタンスに対するプロビジョニングコールの応答

を受信する（Ｓ３０９）。当該第１のインスタンスは、応答を送信した後に待ち受け状態となることも考えられるが、接続できない時間が発生しないように、待ち受け状態となった後に応答を送信することが好ましい。

[0038] そして、接続装置２００は、当該第１のインスタンスに対して、IoT機器２３０と当該第１のインスタンスとの間のVPNセッションを生成するためのプロビジョニングコールを送信する（Ｓ３１０）。このプロビジョニングコールは、当該送信元アドレス、及びIoT機器２３０に関連づけられたクレデンシャルを含む。当該クレデンシャルは、データベース２０４に加入者識別子２３２と関連づけて記憶しておいてもよく、またはIoT機器２３０からのセッション生成要求に含まれていてもよい。

[0039] 当該クレデンシャルは、たとえば、公開鍵とすることができる。この場合、IoT機器２３０には、当該公開鍵に対応する秘密鍵が格納されている。VPNセッションには、公開鍵暗号化方式以外の暗号化方式を用いてもよく、より一般的に、暗号化方式に合わせて必要な第１のクレデンシャルが当該第１のインスタンスに送信され、当該第１のクレデンシャル又はこれに対応する第２のクレデンシャルがIoT機器２３０に格納されていればよい。

[0040] VPNセッションを生成するためのプロビジョニングコールを受信した後に、当該第１のインスタンスは、当該送信元アドレス及び当該クレデンシャルを記憶して、VPNセッションの待ち受け状態となる（Ｓ３１１）。また、接続装置２００は、当該第１のインスタンスから、当該プロビジョニングコールに対する応答を受信する（Ｓ３１２）。当該応答には、一例において、当該送信元アドレス及び当該第１のインスタンスの第１の宛先アドレスを含むことができる。当該第１のインスタンスは、応答を送信した後に待ち受け状態となることも考えられるが、接続できない時間が発生しないように、待ち受け状態となった後に応答を送信することが好ましい。

[0041] 当該応答を受信した接続装置２００は、当該応答に含まれる当該送信元アドレス及び当該第１の宛先アドレスにポート番号を必要に応じて加えた接続情報をIoT機器２３０に送信する（Ｓ３１３）。当該第１のインスタンスから

の応答にポート番号が含まれる場合には、受信した接続情報をIoT機器２３０に送信すればよい。IoT機器２３０では、当該接続情報に基づいて、デバイスプロビジョニングが行われ、当該第１のインスタンスへの接続が試行される（Ｓ３１４）。ここで、IoT機器２３０と当該第１のインスタンスとの間に介在する装置が存在してもよい。当該第１のインスタンスからIoT機器２３０に対して成功の応答が送信されれば（Ｓ３１５）、ハンドシェイクに成功し、VPNトンネルが確立した状態になる。当該試行を受信したことに応じて、当該試行に対する成功の応答を送信したことに応じて、又はより一般に当該試行を受信した後に、第１のインスタンスがGTP-Uセッションの待ち受け状態となり、GTPトンネルが確立されるようにしてもよい。

[0042] 当該第１のインスタンスが、当該成功の応答を送信した後に、接続装置２００にオンラインとなったこと、すなわち、加入者識別子２３２を用いた通信のための接続が確立したことを通知してもよい（Ｓ３１６）。かかる通知を受信した接続装置２００は、たとえば、加入者識別子２３２を用いた通信が可能であることを表すためのオンライン表示情報をIoT機器２３０、又はIoT機器２３０を管理する管理者が用いるコンピュータ等のIoT機器２３０以外の装置に送信してもよい（Ｓ３１７）。ここで、接続装置２００は、当該試行が成功したことの応答を受信したことを受けて、加入者識別子２３２がオンラインとなったことを自ら判定し、記憶してもよい。また、当該第１のインスタンスが、所定期間が経過したか否かを判定し（Ｓ３１８）、経過した場合に接続装置２００にオフラインとなったこと、すなわち、加入者識別子２３２を用いた通信のための接続が失われたことを通知してもよい（Ｓ３１９）。かかる通知を受信した接続装置２００は、たとえば、加入者識別子２３２を用いた通信が可能でないことを表すためのオフライン表示情報を、又はIoT機器２３０を管理する管理者が用いるコンピュータ等のIoT機器２３０以外の装置に送信してもよい（Ｓ３２０）。ＶＰＮトンネルの生存確認を行うためにいかに上記所定期間の起算時点及び期間を定義するかは、ＶＰＮ技術の個別の仕様に応じて定めればよい。起算時点としては、たとえば、VPNト

ンネルが切断された時点が挙げられる。

[0043] 上述の説明では、GTPトンネルの確立に当たって、第２のインスタンスに対してプロビジョニングコールをし、その後に第１のインスタンスに対してプロビジョニングコールをしたが、逆の順序とする実装も考えられる。より一般的には、MNOの通信インフラ２１０に接続されるクラウド上の通信インフラ２２０が備える設備に含まれる第１のインスタンス及び第２のインスタンスに、当該第１のインスタンスと当該第２のインスタンスとの間のGTP-Uセッションを生成するための第１のプロビジョニングコールを送信して、当該第１及び第２のインスタンスを待ち受け状態にし、当該第１のインスタンス又は当該第２のインスタンスから、GTP-Uセッションの送信元アドレスを受信することができればよい。

[0044] セッション生成要求がIoT機器２３０以外の装置から接続装置２００に送信される場合、当該要求に対する応答は、IoT機器２３０以外の装置に対して送信される。IoT機器２３０以外の装置とIoT機器２３０との間に秘匿回線が確立されていれば、接続情報を当該秘匿回線を通じてIoT機器２３０に送信して、デバイスプロビジョニングを行うことができるので、接続情報が接続装置２００からIoT機器２３０に向けて送信されると言える。

[0045] また、ハンドシェイク時に、当該第１のインスタンスに記憶されたクレデンシャル又はこれに対応するクレデンシャルを用いて一時的なクレデンシャルを生成し、当該第１のインスタンスに記憶してもよい。この場合、当該第１のインスタンスにおいては、当該送信元アドレスに当該一時的なクレデンシャルを関連づけておく。同様に、IoT機器２３０にも一時的なクレデンシャルが記憶される。また、たとえば、初回ハンドシェイク時に、一時的なキーを生成してもよく、当該第１のインスタンスにおいては、当該送信元アドレスに当該キーを関連づけておくことに加えて、当該キーに当該一時的なクレデンシャルを関連づけておく。

[0046] データの送受信

図４に、本発明の第１の実施形態にかかるIPネットワークにアクセスする

ための通信サービスにおけるデータ送信の流れを示す。

[0047] まず、IoT機器２３０は、第１のインスタンスに対して、IoT機器２３０に格納されたクレデンシャル又は一時的なクレデンシャルによって暗号化されたIPパケットをVPNパケットにカプセル化して送信する（Ｓ４０１）。当該VPNパケットは、暗号化されたIPパケットと、VPNセッションに関するVPNセッション情報とを含む。当該VPNセッション情報には、送信元アドレス又はこれに関連づけられた一時的なキーが含まれる。ここで、IoT機器２３０と当該第１のインスタンスとの間に介在する装置が存在してもよい。

[0048] 当該VPNパケットを受信した当該第１のインスタンスは、VPNセッション情報に含まれる送信元アドレス又はこれに関連づけられた一時的なキーに対応するクレデンシャル又は一時的なクレデンシャルを取得して、暗号化されたIPパケットの復号化を試行する（Ｓ４０２）。

[0049] セッション生成過程のデバイスプロビジョニング時に、IoT機器２３０においてルーティング情報の設定がなされてもよい。より具体的には、IoT機器２３０から送出される暗号化されたIPパケットのGTPトンネル終端後の送信先アドレスに応じて、VPNトンネルを通すか否かをIoT機器２３０において判定するようにしてもよい。

[0050] 次に、当該第１のインスタンスは、復号化されたIPパケットのヘッダに含まれる送信元アドレスに基づいて、当該第１のインスタンスに保持された１又は複数の送信元アドレスと各送信元アドレスが割り当てられたGTPセッションの送信先との対応づけを参照して、送信先となる第２のインスタンスを判定する（Ｓ４０３）。そして、当該第１のインスタンスは、判定された当該第２のインスタンスに対して、復号化されたIPパケットをGTPペイロードとするGTPパケットを送信する（Ｓ４０４）。これによって、VPNトンネルは終端される。各インスタンスは、複数のサーバを含み、各インスタンスがデータを受信するサーバと、そこからデータを送信するサーバが異なってもよい。

[0051] 当該第２のインスタンスでは、受信したGTPパケットからGTPヘッダを取り除いて、GTPペイロードであるIPパケットをMVNOの通信インフラ２２０の外部

又は内部のIPネットワークに送信する（Ｓ４０５）。GTPヘッダにはIDが含まれ、当該第２のインスタンスが記憶するIDと送信元アドレスとの対応づけを参照して、当該第２のインスタンスは送信元アドレスを同定することができ、さらに、装置２００が記憶する送信元アドレスと加入者識別子との対応づけを参照して、加入者識別子を推移的に同定可能である。

[0052] このように、VPNトンネルによってインターネット等のIPネットワーク上で秘匿回線が与えられ、ＩｏＴ機器２３０は、GTPプロトコルによるデータ通信を行うMVNOの通信インフラ２２０に、無線アクセスネットワークを介さずにIPネットワークを介して接続可能となる。

[0053] 図４においては、データの送信について示したが、MVNOの通信インフラ２２０は、IPネットワークからデータを受信する場合には以下のとおりである。第２のインスタンスに対して、IoT機器２３０宛のIPパケットが着信した際、送信先であるIoT機器２３０のアドレスに対応するGTP-Uセッションを特定し、当該IPパケットにGTPヘッダを付与して第１のインスタンスへと送信する。そして、第１のインスタンスでは、受信したGTPパケットからGTPヘッダを取り除き、IoT機器２３０宛のIPパケットを得る。当該IPパケットの送信先アドレスから対応するVPNセッションを特定して、VPNセッションに関連づけられた一時的なキーに対応するクレデンシャル又は一時的なクレデンシャルを用いて、IPパケットをVPNパケットにカプセル化し、VPNトンネルを経由してIoT機器２３０へと送信する。IoT機器２３０では、受信したVPNパケットをVPNセッション情報を元に関連づけられた一時的なキーに対応するクレデンシャル又は一時的なクレデンシャルを取得して、暗号化されたIPパケットの復号化を行い、IPパケットを処理する。

[0054] IoT機器２３０を管理する管理者が用いるコンピュータなどの加入者識別子２３２に正当にアクセス可能なIoT機器２３０以外の装置から、接続装置２００に加入者識別子２３２に関連づけられた送信元アドレス又はこれに対応するキーによって定まるVPNセッションの無効化要求を送信してもよい。この場合、当該無効化要求を受信した接続装置２００は、第１のインスタンスに対

して、当該送信元アドレス又はこれに関連づけられたキーに対応するクレデンシャル又は一時的なクレデンシャルを破棄又は無効化することを要求し、かつ、VPNセッションの無効化に応じて、加入者識別子２３２に関連づけた記憶された課金状態を更新する。

符号の説明

[0055] ２００　装置

２０１　通信部

２０２　処理部

２０３　記憶部

２０４　データベース

２１０　MNOの通信インフラ

２２０　MNOの通信インフラに接続される通信インフラ

請求の範囲

[請求項1] MNOの通信インフラに接続されるクラウド上の通信インフラが備える設備を用いて、IoT機器に、IPネットワークにアクセスするための通信サービスを提供するための方法であって、

前記通信サービスの加入者を識別するための加入者識別子を含むセッション生成要求を受信するステップと、

前記加入者識別子に関連づけてIDを記憶するステップと、

前記設備に含まれる第１のインスタンス及び第２のインスタンスに、前記第１のインスタンスと前記第２のインスタンスとの間のGTP-Uセッションを生成するための第１のプロビジョニングコールであって、前記IDを含む第１のプロビジョニングコールを送信するステップと、

前記第１のインスタンス又は前記第２のインスタンスから、前記第１のプロビジョニングコールの応答として、前記GTP-Uセッションの送信元となる送信元アドレスを受信するステップと、

前記第１のインスタンスに、前記IoT機器と前記第１のインスタンスとの間のVPNセッションを生成するための第２のプロビジョニングコールであって、前記送信元アドレス及び前記第１のクレデンシャルを含む第２のプロビジョニングコールを送信するステップと、

前記第１のクレデンシャル又は前記第１のクレデンシャルに対応する第２のクレデンシャルを記憶した前記IoT機器に向けて、前記送信元アドレス及び前記第１のインスタンスの宛先アドレスを含む接続情報を送信するステップと

を含む。

[請求項2] 請求項１に記載の方法であって、

前記接続情報は、前記第１のインスタンスのポート番号を含む。

[請求項3] 請求項１又は２に記載の方法であって、

前記第１のクレデンシャルは、公開鍵であり、

前記第２のクレデンシャルは、前記公開鍵に対応する秘密鍵である。

[請求項4] 請求項１に記載の方法であって、

前記セッション生成要求は、前記IoT機器から受信する。

[請求項5] 請求項１から４のいずれかに記載の方法であって、

前記第１のインスタンス及び前記第２のインスタンスは、クラウド又はパブリッククラウド上のインスタンスである。

[請求項6] 装置に、MNOの通信インフラに接続されるクラウド上の通信インフラが備える設備を用いて、IoT機器に、IPネットワークにアクセスするための通信サービスを提供するための方法を実行させるためのプログラムであって、前記方法は、

前記通信サービスの加入者を識別するための加入者識別子を含むセッション生成要求を受信するステップと、

前記加入者識別子に関連づけてIDを記憶するステップと、

前記設備に含まれる第１のインスタンス及び第２のインスタンスに、前記第１のインスタンスと前記第２のインスタンスとの間のGTP-Uセッションを生成するための第１のプロビジョニングコールであって、前記IDを含む第１のプロビジョニングコールを送信するステップと、

前記第１のインスタンス又は前記第２のインスタンスから、前記第１のプロビジョニングコールの応答として、前記GTP-Uセッションの送信元となる送信元アドレスを受信するステップと、

前記第１のインスタンスに、前記IoT機器と前記第１のインスタンスとの間のVPNセッションを生成するための第２のプロビジョニングコールであって、前記送信元アドレス及び前記第１のクレデンシャルを含む第２のプロビジョニングコールを送信するステップと、

前記第１のクレデンシャル又は前記第１のクレデンシャルに対応する第２のクレデンシャルを記憶した前記IoT機器に向けて、前記送信

元アドレス及び前記第１のインスタンスの宛先アドレスを含む接続情報を送信するステップと
を含む。

[請求項7] MNOの通信インフラに接続されるクラウド上の通信インフラが備える設備を用いて、IoT機器に、IPネットワークにアクセスするための通信サービスを提供するための装置であって、

前記通信サービスの加入者を識別するための加入者識別子を含むセッション生成要求を受信して、前記加入者識別子に関連づけてIDを記憶し、

前記設備に含まれる第１のインスタンス及び第２のインスタンスに、前記第１のインスタンスと前記第２のインスタンスとの間のGTP-Uセッションを生成するための第１のプロビジョニングコールであって、前記IDを含む第１のプロビジョニングコールを送信して、前記第１のインスタンス又は前記第２のインスタンスから、前記第１のプロビジョニングコールの応答として、前記GTP-Uセッションの送信元となる送信元アドレスを受信し、

前記第１のインスタンスに、前記IoT機器と前記第１のインスタンスとの間のVPNセッションを生成するための第２のプロビジョニングコールであって、前記送信元アドレス及び前記第１のクレデンシャルを含む第２のプロビジョニングコールを送信し、

前記第１のクレデンシャル又は前記第１のクレデンシャルに対応する第２のクレデンシャルを記憶した前記IoT機器に向けて、前記送信元アドレス及び前記第１のインスタンスの宛先アドレスを含む接続情報を送信する。

[請求項8] その間にGTP-Uセッションが生成された第１のインスタンス及び第２のインスタンスを有するクラウド上の通信インフラであって、MNOの通信インフラに接続される通信インフラを用いて、IoT機器がIPネットワークにアクセスするための通信サービスを提供する方法であっ

て、

前記第１のインスタンスが、前記IoT機器から、前記IoT機器に格納されたクレデンシャル又は一時的なクレデンシャルによって暗号化されたIPパケットをカプセル化したVPNパケットを受信するステップと、

前記第１のインスタンスが、前記VPNパケットに含まれる送信元アドレス又は一時的なキーに対応するクレデンシャル又は一時的なクレデンシャルを取得して、暗号化された前記IPパケットを復号化するステップと、

前記第１のインスタンスが、復号化された前記IPパケットのヘッダに含まれる送信元アドレスに基づいて、前記第１のインスタンスに保持された、１又は複数の送信元アドレスと各送信元アドレスが割り当てられたGTPセッションの送信先との対応づけを参照して、前記第２のインスタンスを判定するステップと、

前記第１のインスタンスが、前記第２のインスタンスに対して、復号化された前記IPパケットをGTPペイロードとするGTPパケットを送信するステップと、

前記第２のインスタンスが、前記GTPパケットからGTPヘッダを取り除いて、前記GTPペイロードであるIPパケットを前記通信インフラの外部又は内部のIPネットワークに送信するステップと

を含む。

[請求項9] その間にGTP-Uセッションが生成された、MNOの通信インフラに接続されるクラウド上の通信インフラに、IoT機器がIPネットワークにアクセスするための通信サービスを提供する方法を実行させるためのプログラムであって、前記方法は、

前記通信インフラが有する第１のインスタンスが、前記IoT機器から、前記IoT機器に格納されたクレデンシャル又は一時的なクレデンシャルによって暗号化されたIPパケットをカプセル化したVPNパケッ

トを受信するステップと、

前記第１のインスタンスが、前記VPNパケットに含まれる送信元アドレス又は一時的なキーに対応するクレデンシャル又は一時的なクレデンシャルを取得して、暗号化された前記IPパケットを復号化するステップと、

前記第１のインスタンスが、復号化された前記IPパケットのヘッダに含まれる送信元アドレスに基づいて、前記第１のインスタンスに保持された、１又は複数の送信元アドレスと各送信元アドレスが割り当てられたGTPセッションの送信先との対応づけを参照して、前記通信インフラが有する第２のインスタンスであって、前記通信インフラの外部又は内部のIPネットワークにIPパケットを送信可能な第２のインスタンスを判定するステップと、

前記第１のインスタンスが、前記第２のインスタンスに対して、復号化された前記IPパケットをGTPペイロードとするGTPパケットを送信するステップと

を含む。

[請求項10] IoT機器がIPネットワークにアクセスするための通信サービスを提供するための、MNOの通信インフラに接続されるクラウド上の通信インフラであって、

その間にGTP-Uセッションが生成された第１のインスタンス及び第２のインスタンスを有し、

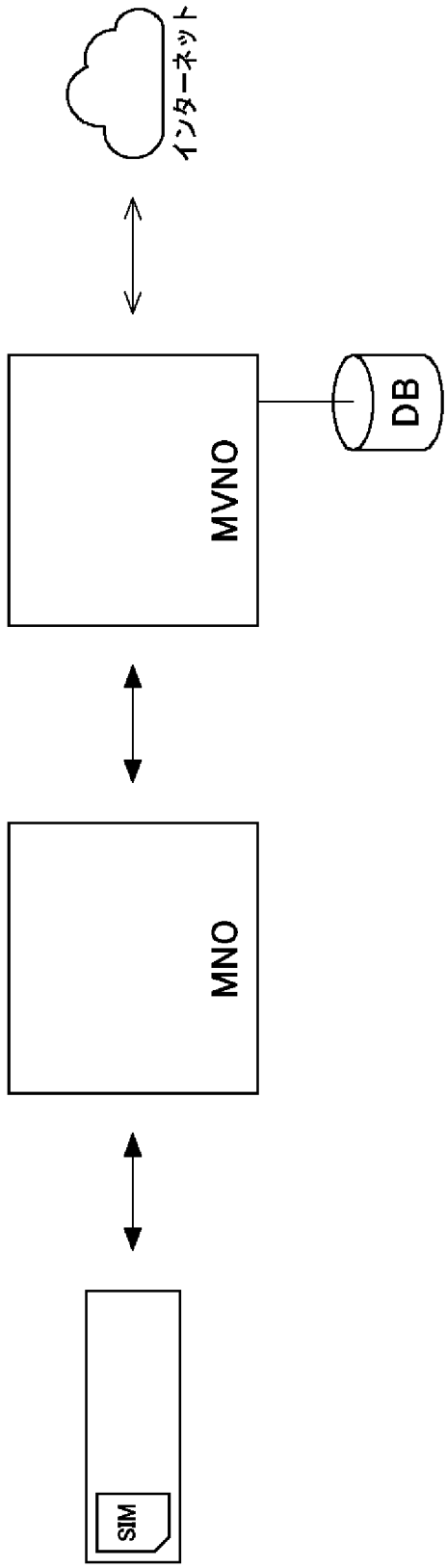
前記第１のインスタンスが、前記IoT機器から、前記IoT機器に格納されたクレデンシャル又は一時的なクレデンシャルによって暗号化されたIPパケットをカプセル化したVPNパケットを受信し、前記VPNパケットに含まれる送信元アドレス又は一時的なキーに対応するクレデンシャル又は一時的なクレデンシャルを取得して、暗号化された前記IPパケットを復号化し、

前記第１のインスタンスが、復号化された前記IPパケットのヘッダ

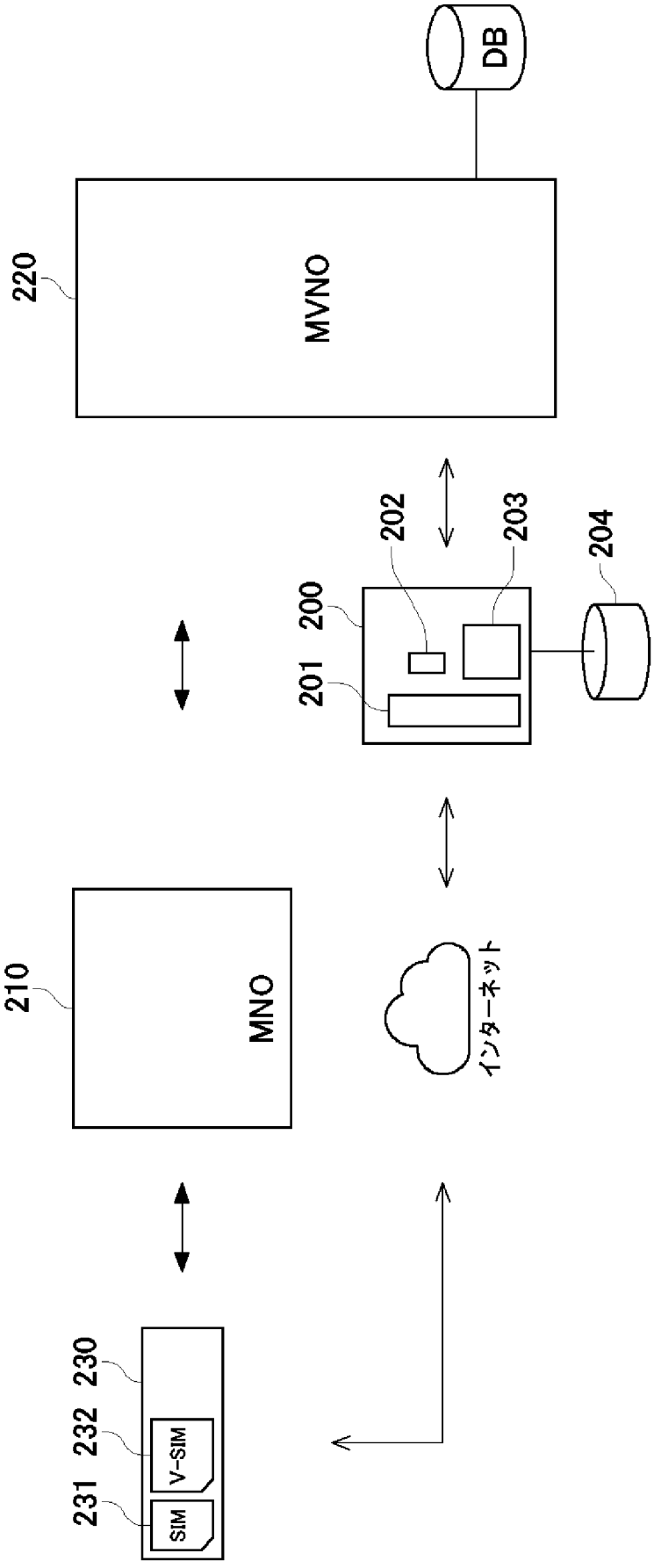
に含まれる送信元アドレスに基づいて、前記第１のインスタンスに保持された、１又は複数の送信元アドレスと各送信元アドレスが割り当てられたGTPセッションの送信先との対応づけを参照して、前記第２のインスタンスを判定して、前記第２のインスタンスに対して、復号化された前記IPパケットをGTPペイロードとするGTPパケットを送信し、

前記第２のインスタンスが、前記GTPパケットからGTPヘッダを取り除いて、前記GTPペイロードであるIPパケットを前記通信インフラの外部又は内部のIPネットワークに送信する。

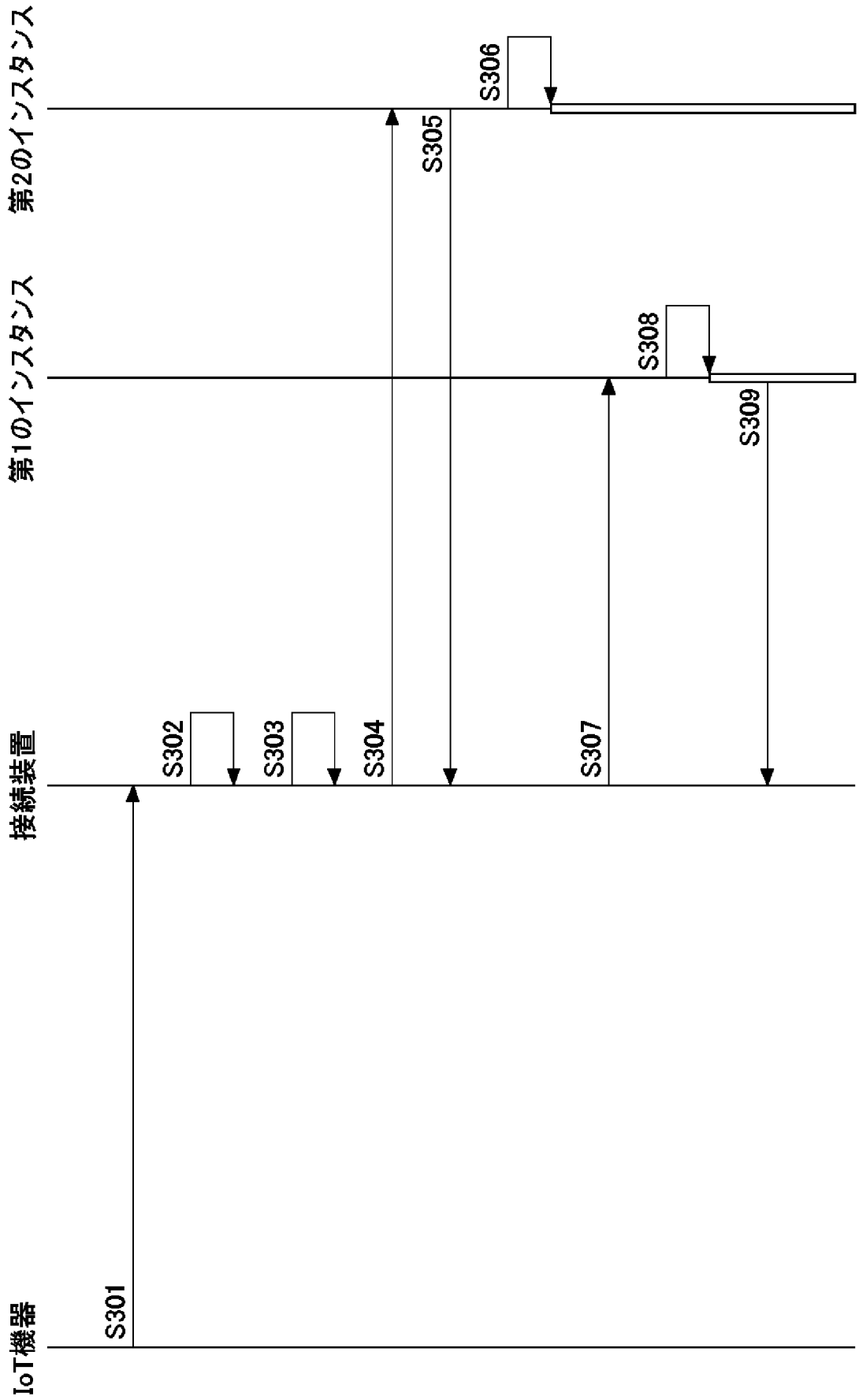
[図1]



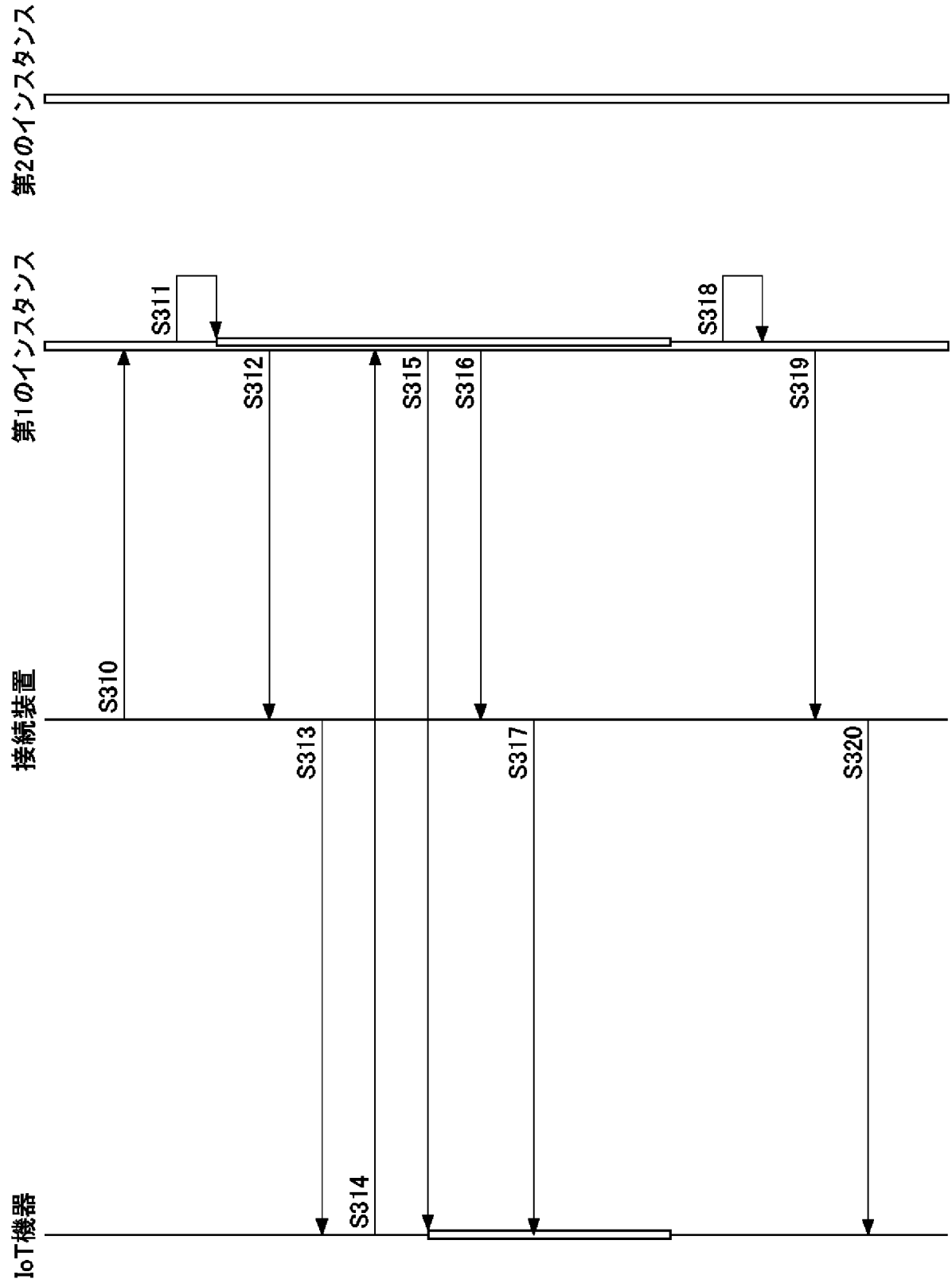
[図2]


DB
220
MVNO
202
203
204
200
201
210
MNO
インターネット
230
232
V-SIM
231
SIM

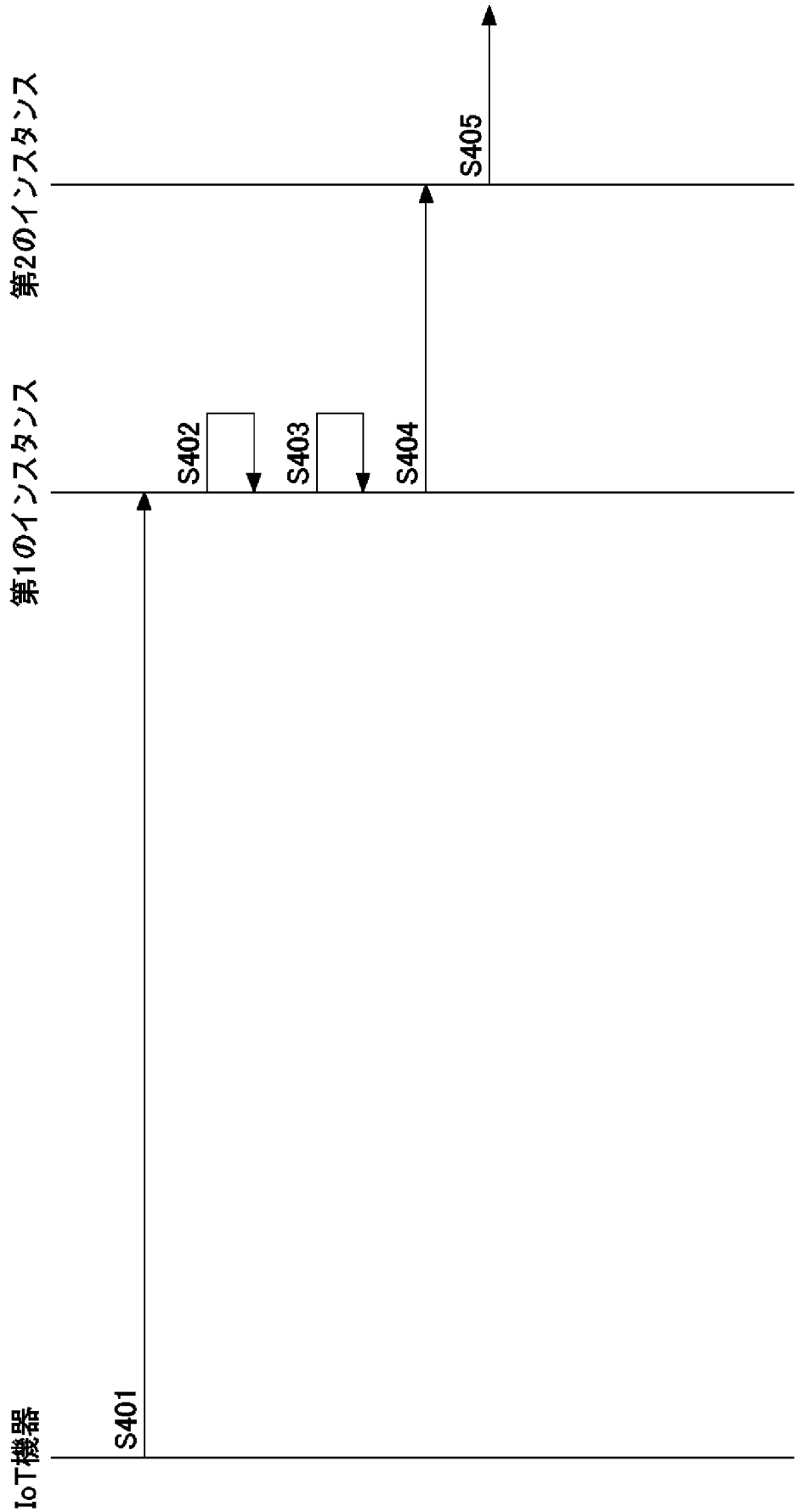
[図3A]


第2のインスタンス
第1のインスタンス
接続装置
IoT機器
S301
S302
S303
S304
S305
S306
S307
S308
S309

[図3B]


第2のインスタンス
第1のインスタンス
接続装置
IoT機器
S310
S311
S312
S313
S314
S315
S316
S317
S318
S319
S320

[図4]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2022/021655

A. CLASSIFICATION OF SUBJECT MATTER

H04W 76/12(2018.01)i; ***H04W 12/033***(2021.01)i
FI: H04W76/12; H04W12/033

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)

H04W76/12; H04W12/033

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 1971-2022
Registered utility model specifications of Japan 1996-2022
Published registered utility model applications of Japan 1994-2022

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102149133 A (GUANGZHOU KOTEL TECHNOLOGY CO LTD) 10 August 2011 (2011-08-10) paragraphs [0057], [0070]-[0073], fig. 5, 7	1-10
A	WO 2017/022791 A1 (NEC CORPORATION) 09 February 2017 (2017-02-09) paragraphs [0107]-[0108]	1-10
A	WO 2008/017709 A1 (ALCATEL LUCENT) 14 February 2008 (2008-02-14) p. 11, lines 5-20	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	Date of mailing of the international search report
05 August 2022	**16 August 2022**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2022/021655

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 102149133 A	10 August 2011	(Family: none)	
WO 2017/022791 A1	09 February 2017	US 2018/0213472 A1 paragraphs [0141]-[0142] EP 3334136 A1	
WO 2008/017709 A1	14 February 2008	US 2009/0323635 A1 paragraph [0058] CN 101523817 A	

国際調査報告

国際出願番号
PCT/JP2022/021655

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04W 76/12(2018.01)i; H04W 12/033(2021.01)i
FI: H04W76/12; H04W12/033

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））

H04W76/12; H04W12/033

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	１９７１－２０２２年
日本国実用新案登録公報	１９９６－２０２２年
日本国登録実用新案公報	１９９４－２０２２年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	CN 102149133 A (GUANGZHOU KOTEL TECHNOLOGY CO LTD) 10.08.2011 (2011-08-10) 段落[0057],[0070]-[0073],図5,7	1-10
A	WO 2017/022791 A1 (日本電気株式会社) 09.02.2017 (2017-02-09) 段落[0107]-[0108]	1-10
A	WO 2008/017709 A1 (ALCATEL LUCENT) 14.02.2008 (2008-02-14) 第11頁第5-20行	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抵触するものではなく、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
05.08.2022	16.08.2022

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
伊東　和重 5J 8839

電話番号 03-3581-1101 内線 3534

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2022/021655

引用文献	公表日	パテントファミリー文献	公表日
CN 102149133 A	10.08.2011	（ファミリーなし）	
WO 2017/022791 A1	09.02.2017	US 2018/0213472 A1 段落[0141]-[0142] EP 3334136 A1	
WO 2008/017709 A1	14.02.2008	US 2009/0323635 A1 段落[0058] CN 101523817 A	