

問4 NAT (ネットワーク)

(R1秋・FE 午後問4)

【解答】

【設問1】 エ

【設問2】 a-エ, b-ウ, c-イ, d-カ

【解説】

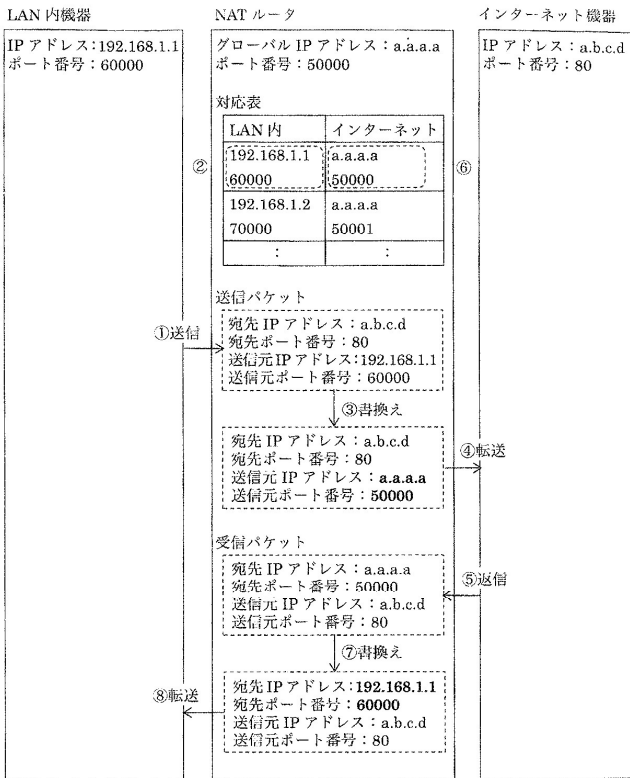
NAT と、NAT の拡張である NAT64 を用いることで、IPv6 ネットワーク内の機器から、IPv4 ネットワーク内の機器への通信を可能にする仕組みについての問題である。設問1は、静的 NAT と動的 NAT のそれぞれの特徴を理解し、どのようなケースに向いているかを問う問題であり、設問2は、NAT64 と DNS64 の組合せによって、IPv6 機器から IPv4 機器へアクセスする際の流れを問う問題である。問題文や設問文に手順が説明されているので、落ち着いて読み、各機能の仕組みを確認しながら解答する。

【設問1】

まず、静的 NAT の仕組みについて、説明する。

図Aは静的 NAT での IP アドレスの書換え例である。①～⑧は、図Aの①～⑧に対応している。

- ① LAN 内機器が NAT ルータ (以下、ルータという) にパケットを送信する。
- ② ルータは、送信パケットの送信元 IP アドレスとポート番号の組みが、ルータ内の対応表に定義されているかどうかを確認する。
- ③ 定義されていれば、送信パケットの送信元 IP アドレスとポート番号が、書き換えられる。
- ④ ルータは、インターネット機器へパケットを転送する。
- ⑤ ルータがインターネット機器からの返信パケットを受信する。
- ⑥ ルータは、受信パケットの宛先 IP アドレスとポート番号の組みが、定義されているかどうかを確認する。
- ⑦ 定義されていれば、受信パケットの宛先 IP アドレスとポート番号が、書き換えられる。
- ⑧ ルータが受信パケットを LAN 内機器に転送する。



注記 ここで a.a.a.a や a.b.c.d はあるグローバル IP アドレスの一つを指しているものとする。網掛け部分は NAT ルータによって書き換えられた箇所を示す。

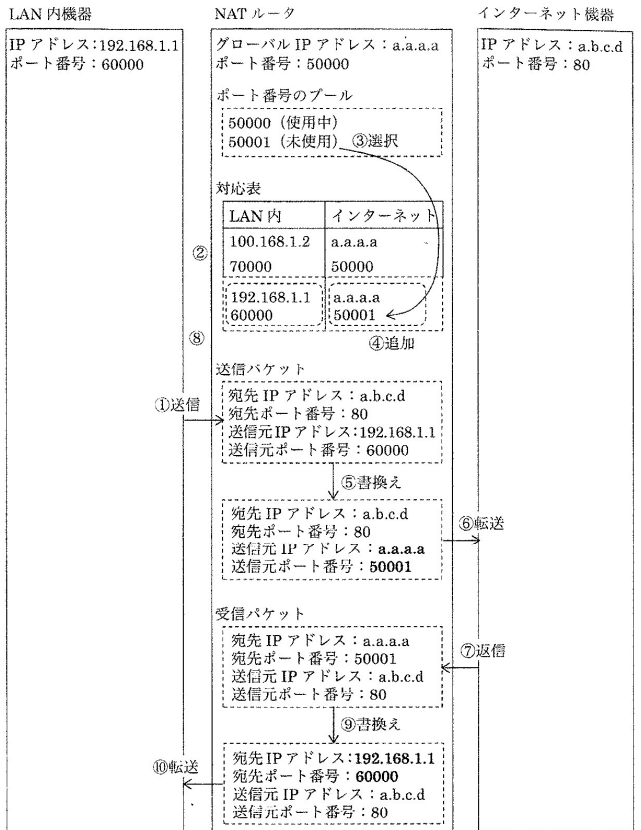
図A 静的 NAT での IP アドレスとポート番号の書換え例

次に、動的 NAT の仕組みについて説明する。動的 NAT は、LAN 内機器がインターネット機器にアクセスしている一定期間内だけ、グローバル IP アドレスとポート番号を対応づける方法である。図Bは、動的 NAT での IP アドレスの書換え例である。①～⑩は、図Bの①～⑩に対応している。

- ① LAN 内機器がルータにパケットを送信する。
- ② ルータは、送信パケットの送信元 IP アドレスとポート番号の組みが、既に対応表に記憶されているかどうかを確認する (この例では、この時点で記憶されていないものとする)。
- ③ 記憶されていない場合、ルータは、プールしているポート番号から、使用していないものを選び、追加して記憶する。
- ④ 送信パケットの宛先 IP アドレスとポート番号を書き換える。
- ⑤ 送信パケットの送信元 IP アドレスとポート番号を書き換える。
- ⑥ ルータは、インターネット機器へパケットを転送する。
- ⑦ ルータが、インターネット機器からの返信パケットを受信する。
- ⑧ ルータは、受信パケットの宛先 IP アドレスとポート番号の組みが、対応表に記憶されているかどうかを確認する (この例では、この時点で記憶されているものとする)。

⑨ 記憶されていれば、受信パケットの宛先 IP アドレスとポート番号が、書き換えられる。

⑩ ルータが受信パケットを LAN 内機器に転送する。



注記 ここで a.a.a.a や a.b.c.d はあるグローバル IP アドレスの一つを指しているものとする。網掛け部分は NAT ルータによって書き換えられた箇所を示す。

図B 動的 NAT での IP アドレスとポート番号の書換え例

静的 NAT では、LAN 内機器がインターネット機器にアクセスする際のポート番号が、常に同じ値で確保済みである。そのため固定されたポート番号を確実に利用できる。しかし、割り当てるポート番号を事前に定義しなければならないため、管理の負荷も高い。それに対して、動的 NAT では、複数の LAN 内機器が使用するグローバル IP アドレスとポート番号を共有するため、同時に使用する数の分だけあればよく、用意するグローバル IP アドレスの数を節約することができる。これらの特徴を踏まえて、設問1の(1)～(3)のケースについて確認する。

- ・ケース(1): 外部のインターネット機器からアクセスする際には、パケットの宛先 IP アドレスに、グローバル IP アドレスが使用される。このパケットの宛先 IP アドレスが、常に内部に設置された特定の LAN 内機器のプライベート IP アドレスに固定的に書き換えられなければならない。そのため、静的 NAT が適している。
- ・ケース(2): LAN 内機器から、インターネット機器にアクセスする場合は、動的 NAT を利用することで、ポート番号の割当てや管理の手間を省くことができる。動的 NAT が適している。
- ・ケース(3): あらかじめ決まった固定のポート番号を使う場合には、ポート番号が定義されていなければならない。そのため、静的 NAT が適している。

動的 NAT が適しているのは、ケース「(2)だけ」であり、(エ)が正解である

【設問2】

現在のインターネット環境は、従来から普及している IPv4 と後継の IPv6 が混在しており、IPv6 アドレスだけをもつ機器 (IPv6 機器) と IPv4 アドレスだけをもつ機器 (IPv4 機器)、IPv6 と IPv4 の両方に対応した機器 (デュアルスタック) が存在する。この環境下で、IPv6 機器から IPv4 機器にアクセスする方法として、DNS64 と NAT64 を連携させる方法がある。まず、DNS64 が IPv4 機器の IP アドレスを IPv6 用に変換し、NAT64 が受け取ったパケットの宛先 IP アドレスを元の IPv4 アドレスに戻して、IPv4 機器へ届ける。

図Cは、IPv6 機器から IPv4 機器にアクセスするときの流れである。

- ① IPv6 機器は、DNS64 に送信先のホスト名に対応する IP アドレスを問い合わせる。
- ② DNS64 は、ホスト名と IP アドレスの対応表で、ホスト名に対応する IPv6 アドレスがあればそれを返し、対応する IPv6 アドレスがなく、IPv4 アドレスがあれば、それを IPv6 形式のアドレスに変換して回答する。
- ③ IPv6 機器は、DNS64 から入手した IP アドレスを使って、パケットを送信する。
- ④ NAT64 の機能をもつルータ (以下、NAT64 ルータという) が、パケットを IPv4 形式に変換して、IPv4 機器に転送する。

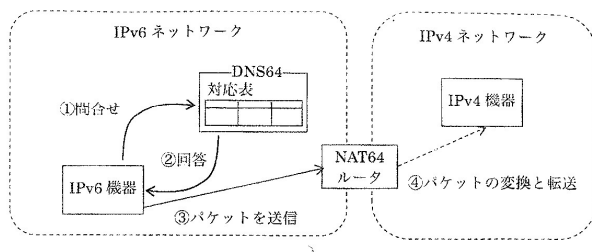


図 C IPv6 から IPv4 へのアクセスの流れ

- ・空欄 a1：DNS64 の役割は、IPv6 機器からの名前解決の問合せに対応することである。そのため、IPv6 機器からアクセス可能な IPv6 ネットワーク内に存在する。これは、(1)に「IPv6 機器は、アクセス先の機器の IP アドレスを、DNS64 から入手する」とあり、IPv6 機器から直接通信できる場所にあることが判断できる。したがって、「IPv6」が入る。
 - ・空欄 a2：DNS64 は、名前解決の問合せに対し、IPv6 アドレスがあれば、これを返し、IPv6 アドレスがなく、IPv4 アドレスだけであれば、IPv4 アドレスを返す。また、(2)に着目すると、「IPv6 機器は、入手した IP アドレスに宛てて IPv6 のパケットを送信する」とあり、ここで入手されている IP アドレスは IPv6 であると推測できることから、「IPv6」であることが分かる。
 - ・空欄 a3：(1)に「対応する a2 (IPv6) アドレスがあればそれを返し、対応する a2 (IPv6) アドレスがなく、a3 アドレスがあれば、それを a2 (IPv6) に変換して返す」とあるため、空欄 a3 は、「IPv4」であると推測できる。
- これらから、(エ)が正解である。
- ・空欄 b：IPv6 機器から送信された IPv6 パケットを IPv4 機器に転送するためには、宛先 IP アドレスを IPv4 機器の IP アドレスに変換する必要がある。したがって、IPv4 機器の IP アドレスである「192.168.0.2」となる。(ウ)が正解である。
 - ・空欄 c：IPv4 機器から返信される IPv4 パケットを NAT64 ルータが受信するためには、IPv4 パケットの宛先 IP アドレスが NAT64 ルータの IPv4 アドレスでなければならない。したがって、IPv4 の IP アドレスである「192.168.0.1」となる。(イ)が正解である。
 - ・空欄 d：IPv6 機器に転送される IPv6 パケットの送信元 IP アドレスは、NAT64 ルータによって、IPv4 の IP アドレスから、IPv6 機器の IP アドレスに変換される。このときの IPv6 アドレス表現は、設問文の(1)のように、「当該 IPv4 アドレスを示す 4 バイトの前に、あらかじめ決められた 12 バイトのプレフィックスが付加したもの」である。ここでは、図 1 の注記にある「64:ff9b:0:0:0:0」がプレフィックスとして使われる。したがって、変換後の IPv6 パケットの送信元 IP アドレスは、前方の 12 バイトがプレフィックスの「64:ff9b:0:0:0:0」、後方の 4 バイトが「192.168.0.2」の 16 進表現である「c0a8:0002」となる。結合すると「64:ff9b:0:0:0:0:c0a8:0002」となり、これを省略した表現である(カ)の「64:ff9b::c0a8:2」が正解である。

IPv6 での IP アドレスの表記について補足する。IPv6 での IP アドレスは、128 ビット (16 バイト) である。2 進数で表現すると長くなるため、16 進数に変換し、4 桁ごとに「:」で区切って表記する。また、「0」が続く場合は、省略して表記することができる。図 D に、IPv6 アドレスの表記例をばす。

fc00:0000:0000:0000:0000:0000:0000:0002

区切り内の「0000」が複数回続く場合は「::」と表記することができる

fc00::2

区切り内の前方が「0」のときは、省略して表記することができる

図 D IPv6 アドレスの表記例