データセンター屋さんの IPv4アドレス枯渇対策

さくらインターネット（株）
研究所　大久保修一
<ohkubo@sakura.ad.jp>

本発表の趣旨

- ISP屋さん(アクセスユーザ側)のIPv4アドレス枯渇対策は、過去JANOG等でも活発に議論されてきた。
- しかし、データセンター屋さん(サーバ側)についてはあまり議論されていない。
- なぜか？
- データセンターのIPv4アドレス枯渇問題は、実質「解がない」からだろう。
- 今回は、目をそらすことなくそんな厳しい現実を直視してみようと思います。

Agenda

- 自己紹介
- 弊社の紹介
- 弊社におけるIPv4枯渇対策について
- IPv4アドレス確保について
- トランスレータについて
- IPv4枯渇時代のホスティングサービス
- まとめ

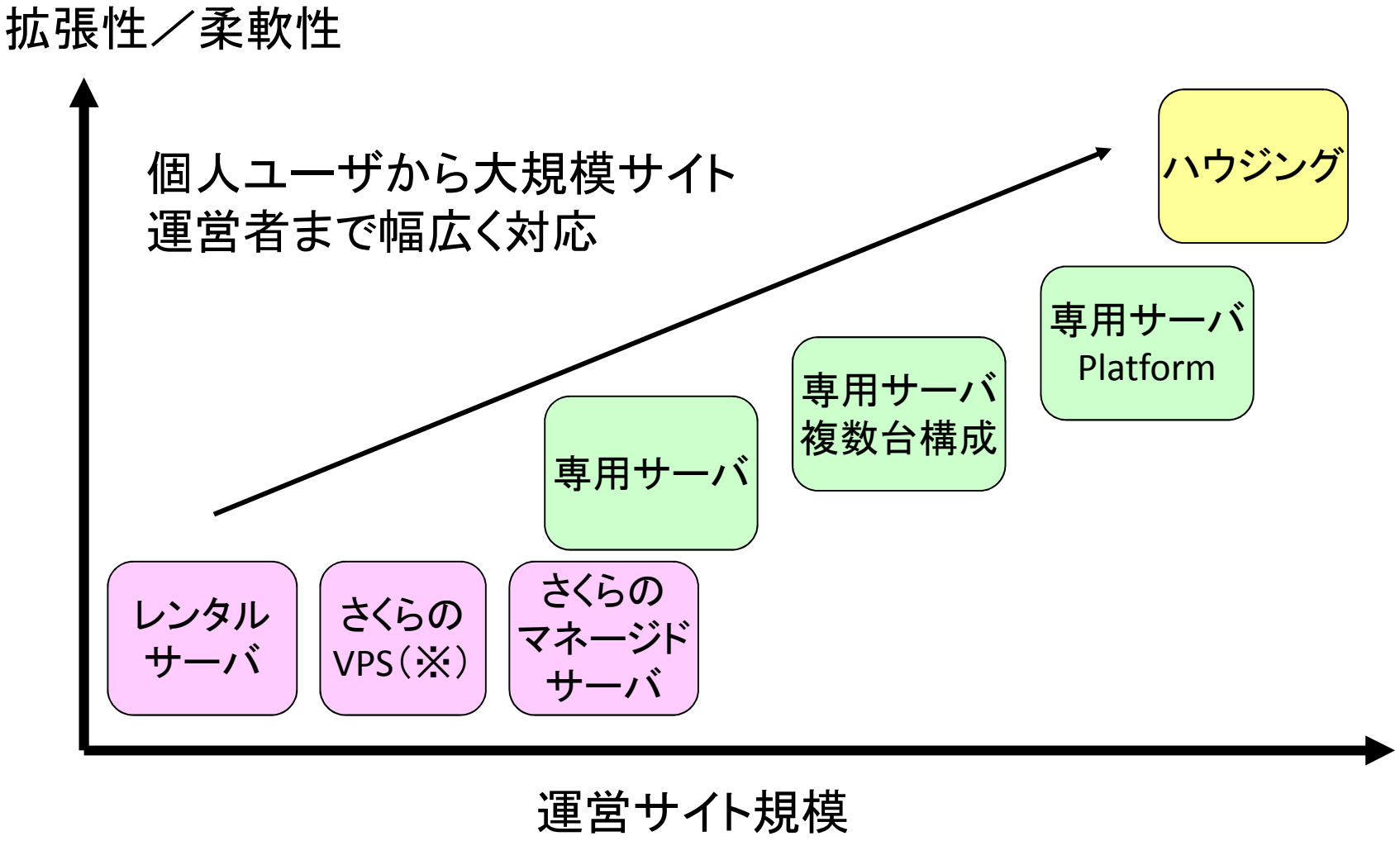
自己紹介

- 大久保 修一 ohkubo@sakura.ad.jp
- さくらインターネット研究所　所属
  - 研究所の目的：インターネット技術に関する基礎研究および応用研究を行い、成果の発信と利用に努めることにより、会社とその事業の発展に寄与する。
  - 数年後のサービスのネタになりそうな技術の評価等
  - キーワード

    IPv4枯渇対策（IPv6、トランスレータ）

    クラウド（仮想化、NoSQL、分散ストレージ）

弊社のサービスランナップ



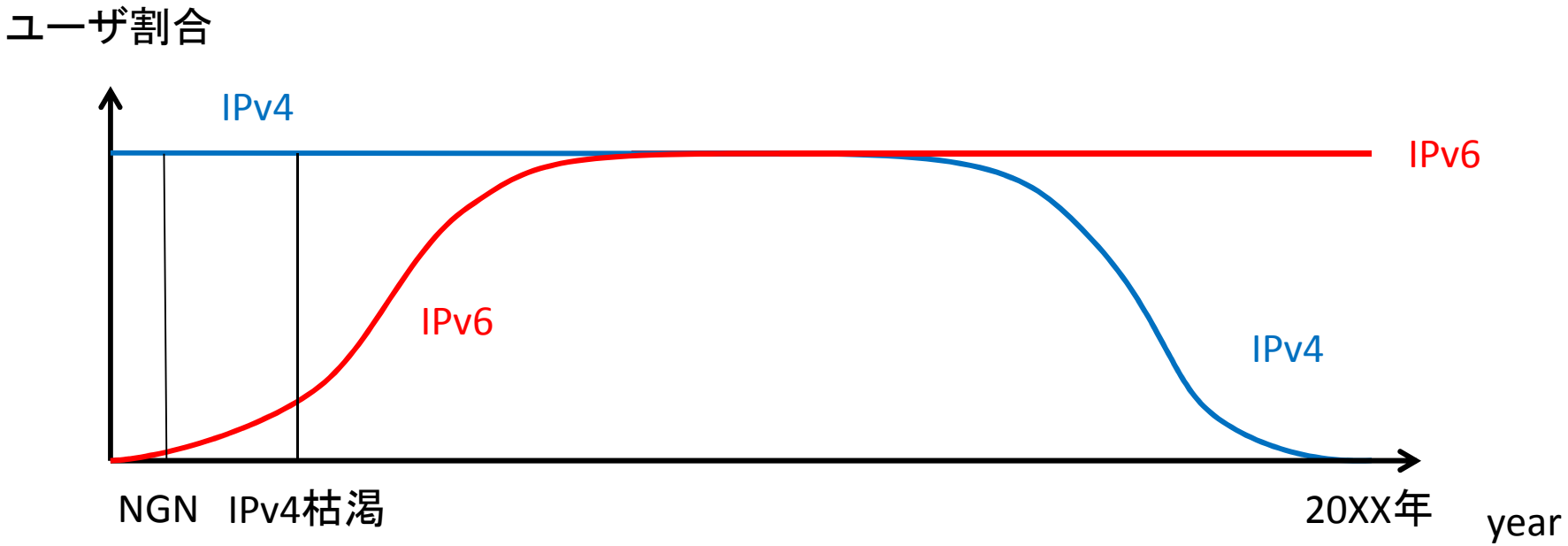
※ 昨日(2010/9/1)から正式サービスとなりました。

弊社におけるIPv4枯渇対策

- サービスのIPv6対応
- 枯渇後のIPv4アドレス確保
- プロトコルトランスレーションサービスの提供

→ 今回はこちらに限ってお話します。

インターネットのIPv6への移行



サービスのIPv6対応

IPv4アドレス確保

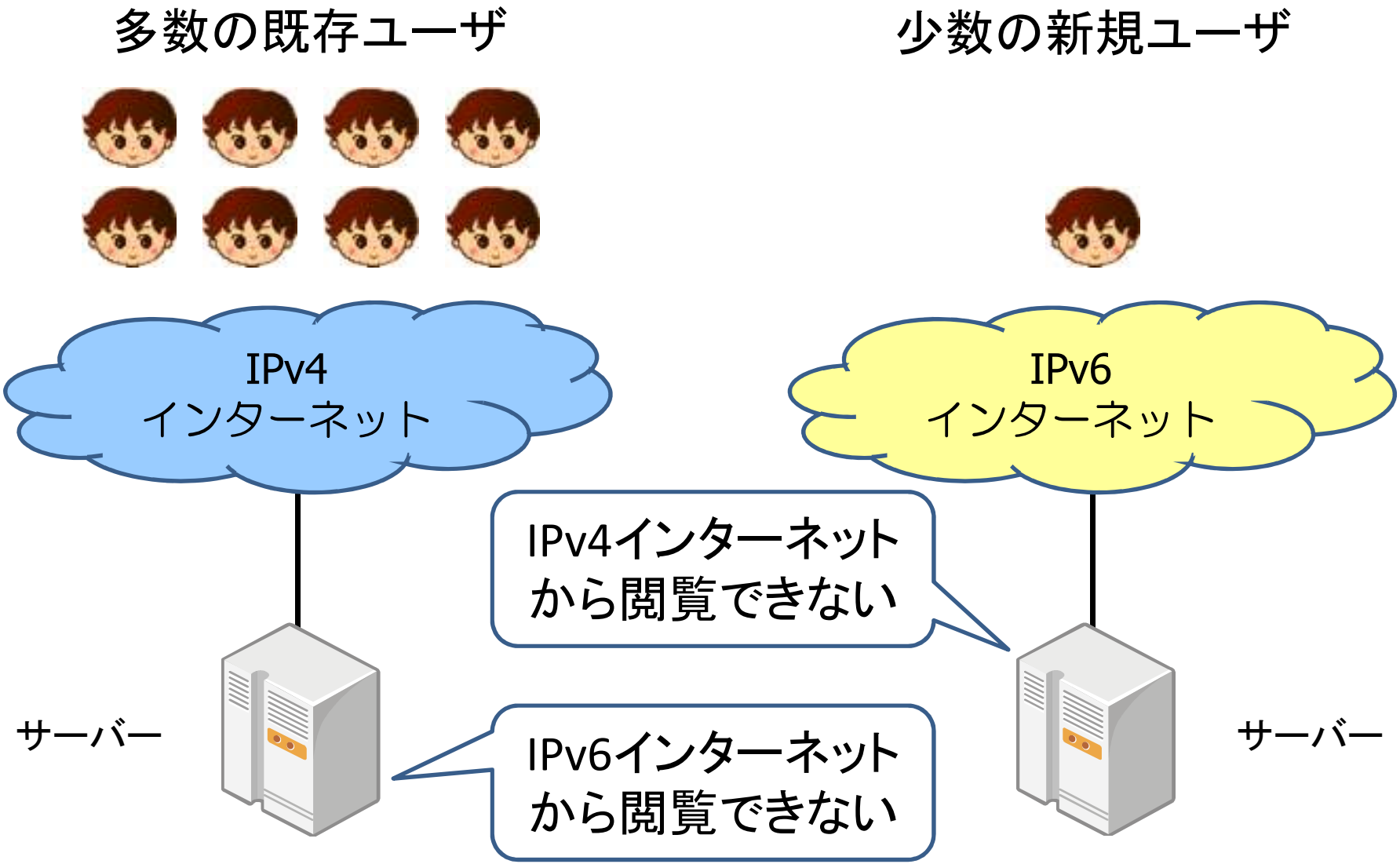
トランスレーションサービス

枯渇後のIPv4アドレス確保について

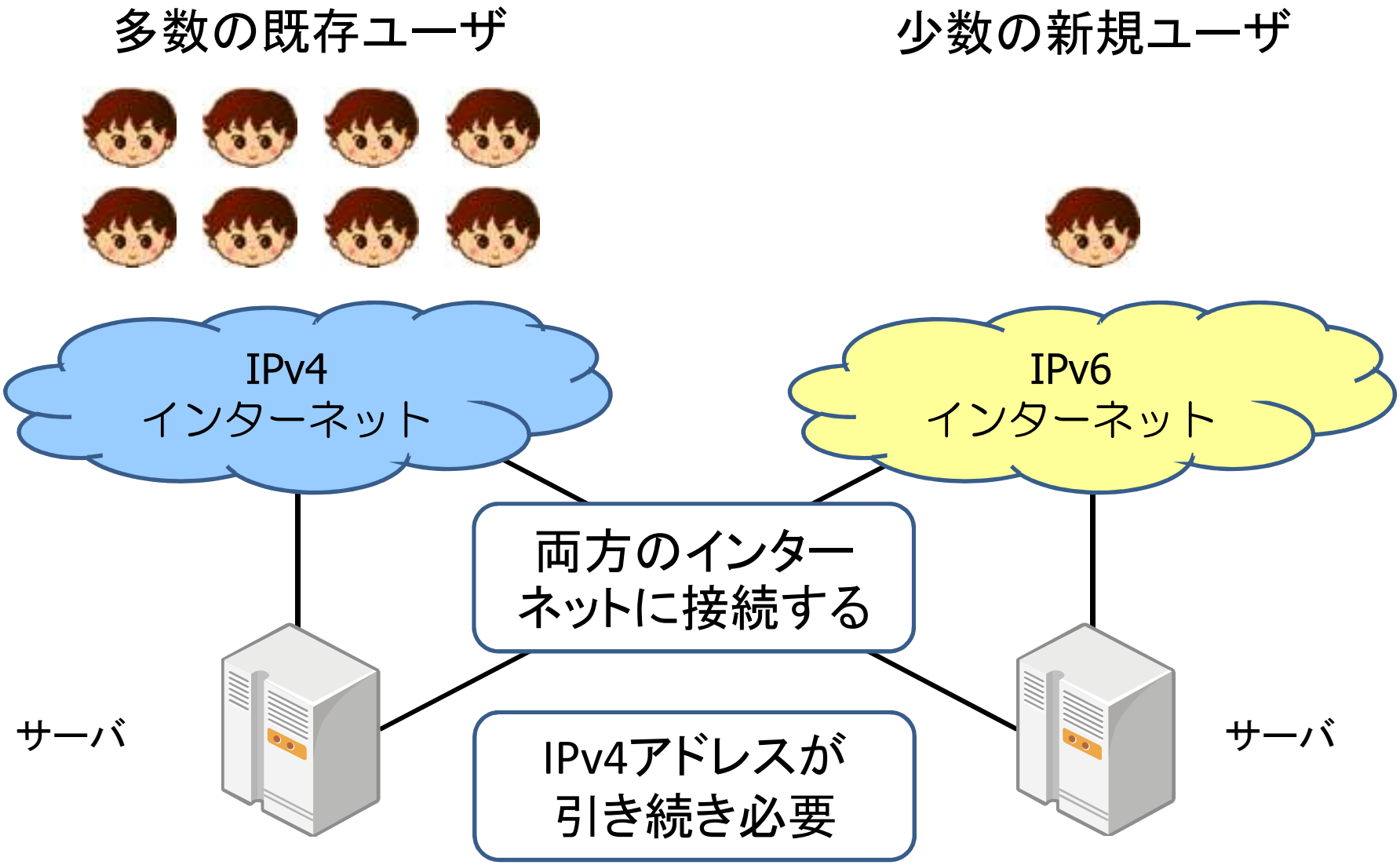
IPv4アドレス確保の必要性

- IPv6 Onlyのサービスは売れない。
  - まだインターネットのほとんどのユーザはIPv4
  - IPv6 Onlyでは、ほとんどのユーザからの参照ができない。
- インターネットが完全にIPv6に移行するまで、引き続きIPv4もサービスする必要がある。
- 枯渇した後もなんらかの手段でIPv4アドレスを確保しなければ、事業範囲の拡大ができない。

IPv4アドレス確保の必要性



IPv4アドレス確保の必要性



IPv4アドレスに関する弊社の事情

- 月間消費ペース：約4C（≒1024個）
- 弊社ではJPNIC殿よりIPアドレスの割り振りを受けている。
- 一回のおかわりで、６か月～１年分消費量の割り振りを受ける。（64C、/18くらい）
- JPNIC(APNIC)プールが枯渇すると最大でも1年以内には、IPv4アドレスの提供ができなくなる。

石狩データセンター（仮）

2011年秋竣工予定

最終的には60万台以上のサーバを稼働可能！

60万個のIPv4アドレス！？（え

このまま何もしないとどうなるか？

2011年6月頃　　IANA IPv4アドレスプール枯渇

2012年9月頃　　RIR IPv4アドレスプール枯渇

～2013年9月頃　　自社IPv4アドレスプール枯渇

事業範囲の拡大ができず・・・・

死亡

枯渇後のIPv4アドレス確保の手段

- IPアドレス移転（後ページにて補足）
  - 他の組織から購入する。
- 既存セグメントからの回収
  - アドレス利用率の低いセグメントをシュリンクし、回収、転用する。
- バックボーンからの回収
  - プライベートアドレスにリナンバし、回収、転用する。
- フレッツプールアドレスからの回収
  - LSNを導入し、フレッツプールアドレスをプライベート化する。

枯渇後のIPv4アドレス確保の手段

- ISPからの割り当て
  - アドレスが余っているISPと契約し、割り当てを受ける。
  - BGPによるグローバルルーティングはできず、上位ISPの回線品質に依存する。（パンチングホールするという荒業もあるが・・・）
- 企業買収
  - IPv4アドレスを持っている企業を買収する。
- 今のうちに確保しておく（埋蔵金計画）
- 経路ハイジャック

補足：IPアドレス移転について

- 事業者同士の合意のみでアドレスの譲渡が可能になる。
- APNIC
  - APNIC28(2009/8)にてポリシーのコンセンサス成立、ECの承認(2009/11)、APNICの正式なポリシーに
  - http://www.apnic.net/policy/transfer-policy
- JPNIC
  - 第17回JPNICオープンポリシーミーティングでコンセンサス成立
  - ポリシーWGチェアからJPNICに対しての実装勧告
  - JPNIC理事会で検討中

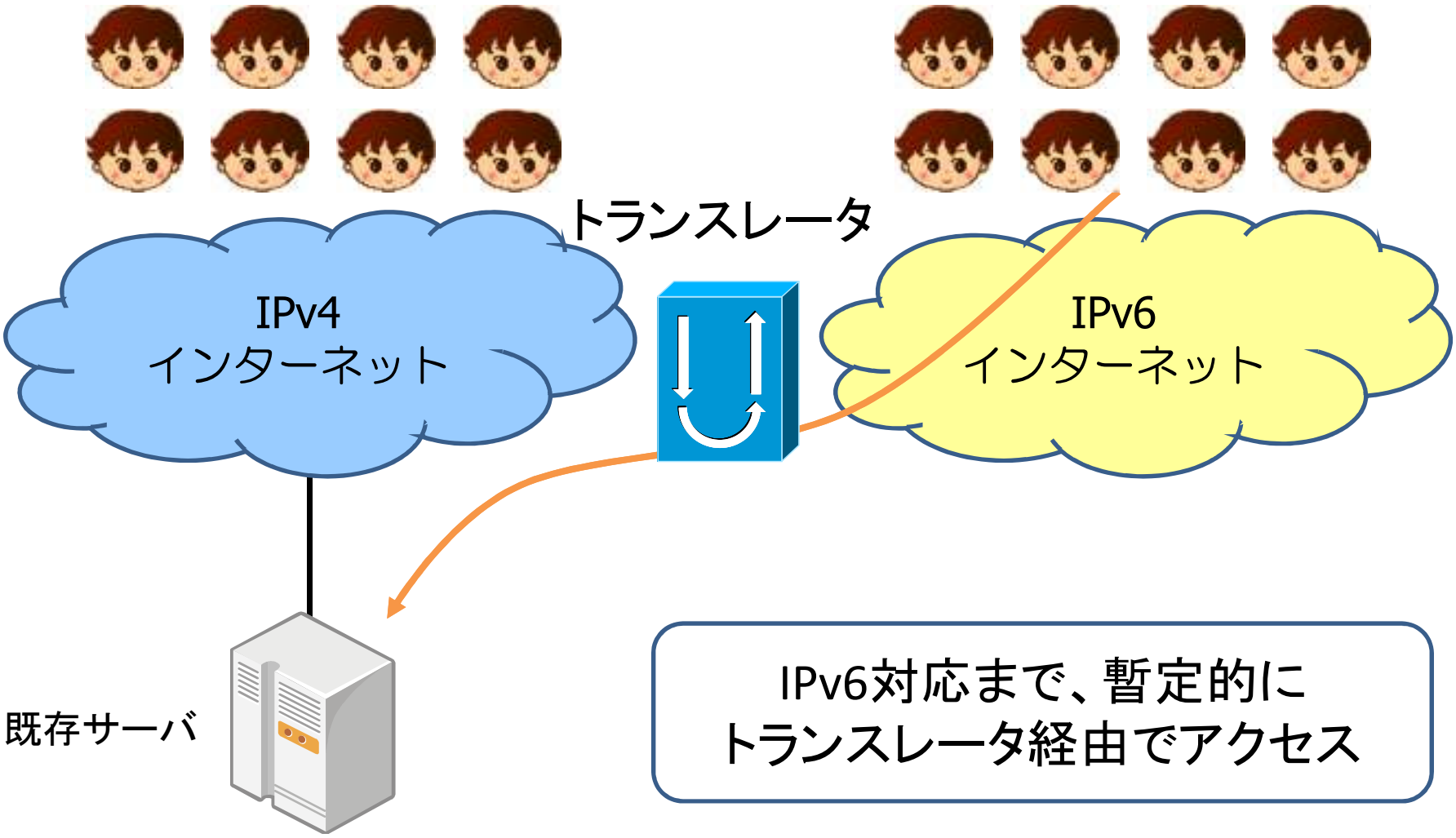
トランスレーションサービスについて

トランスレーションサービスの必要性

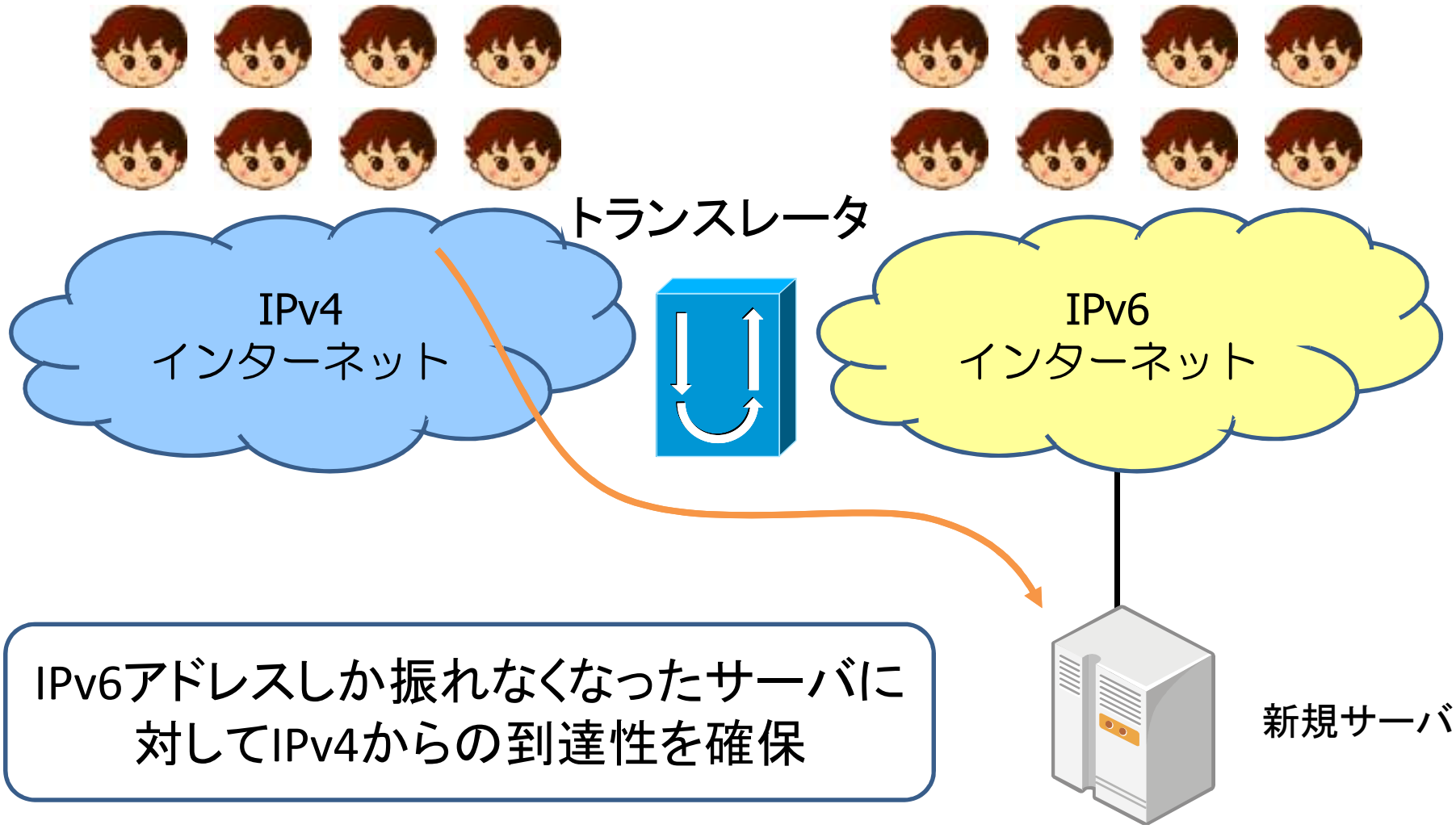
- ２つのインターネット間の通信の橋渡しが必要。
- 既存のサーバをすぐにIPv6対応できるわけではない。

  →トランスレータで暫定的に対応
- ただ、トランスレーションは万能ではない。

トランスレータが必要なシチュエーション



トランスレータが必要なシチュエーション



IPv6アドレスしか振れなくなったサーバに
対してIPv4からの到達性を確保

トランスレータの動向

- 現在いくつかの実装がなされている
  SIIT(RFC2765)、NAT-PT(RFC2766)はHistorical Statusとなっており有効でない。
- IETF BEHAVE WGにて再定義の働きがなされている。
- https://datatracker.ietf.org/wg/behave/

トランスレータの技術

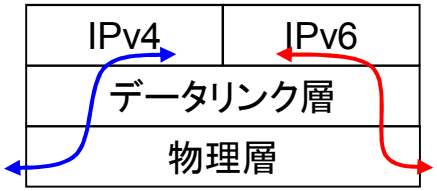
- IPv4とIPv6のプロトコル変換を行う。
- 3つの方式が存在する
  - NAT-PT(将来NAT64,DNS64等に置き換わる予定)

    Network Address Translation - Protocol Translation
  - TRT

    Transport Relay Translator
  - Proxy

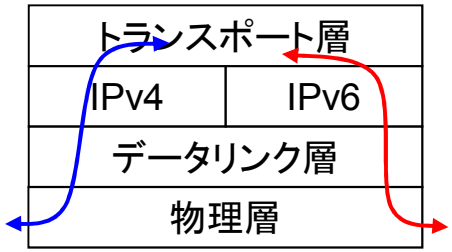
トランスレータの技術

NAT-PT



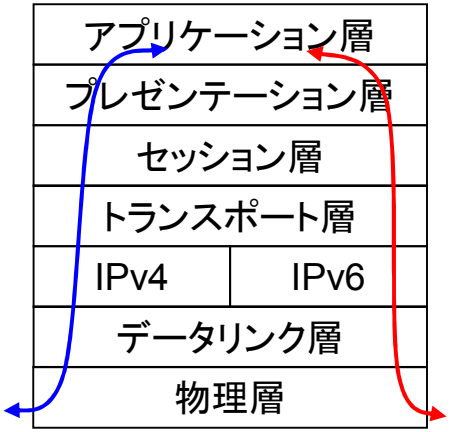
- IPヘッダ、ICMPの変換のみ。
- 一部ALG機能により、ペイロードの変換も行う。
- MTUの問題が大きい。

TRT



- 一旦TCPのコネクションを終端する。
- セッション毎にソケットを開く。
- トランスレータが輻輳・再送制御、PMTUDを行う。

Proxy



- ペイロードの中身をinspectionし、書き換えもできる。
- 通信のコンテキストによって、動作を柔軟に変更可能。

NAT-PTの実装

- 横河電機TTBシリーズ（販売終了）
- D-Link DFL-1600IT
  - 横河電機TTBを実装したアプライアンス
- ALAXALA AXシリーズ（ルータのおまけ機能）
- セイコープレシジョン SX-3640 IPTranslator
- A10ネットワークス AXシリーズ
  - NAT-PT機能実装予定（2010年末～2011年初頭）
- Ecdysis（OpenBSD、Linux）（NAT64、DNS64）

TRT方式の実装

- FreeBSD faith
  - OS標準の機能として実装されている。
- Linux pTRTd

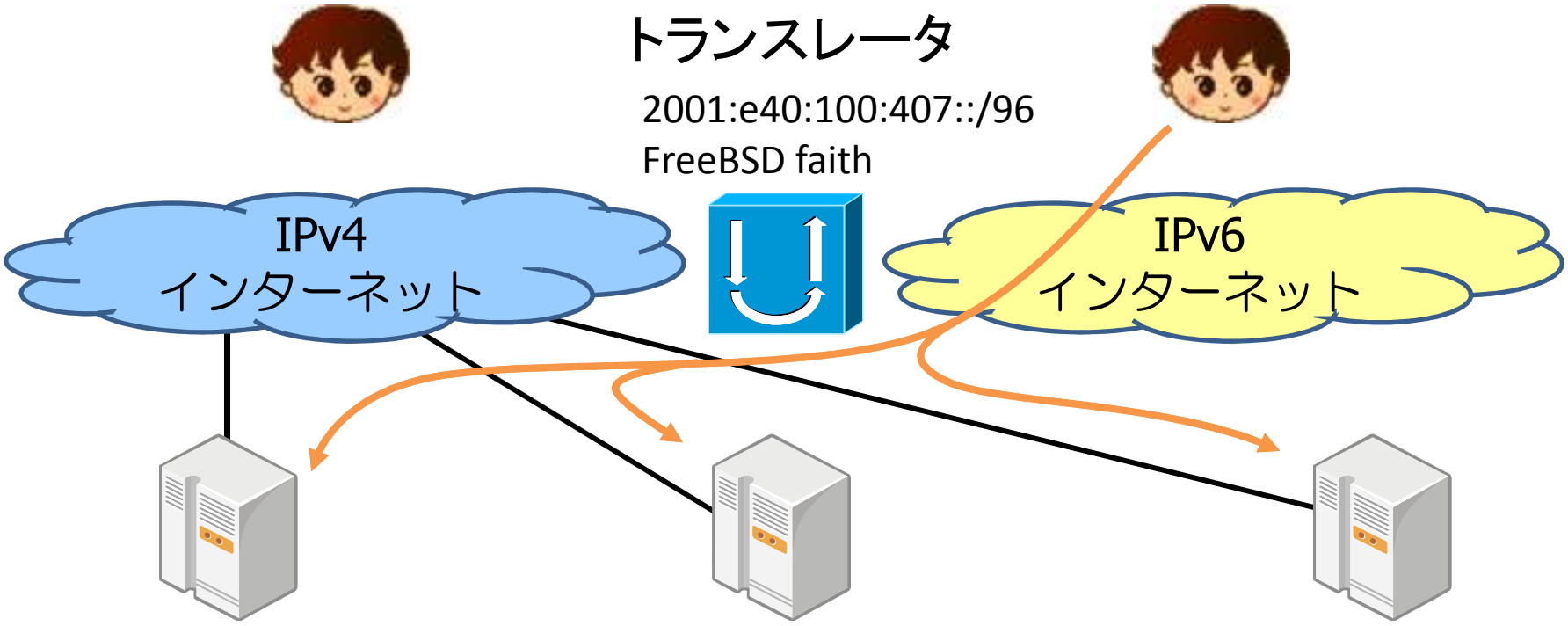
Proxy方式の実装

- F5ネットワークス BIG-IP
  - IPv4,IPv6 SLBを実装
- A10ネットワークス AXシリーズ
  - IPv4,IPv6 SLBを実装
- オープンソース系
  - Apache mod_proxy
  - lighttpd mod_proxy
  - Squid
  - Stone
  - delegate
  - inetd + netcat、その他たくさん

弊社での事例紹介

- 弊社Webサーバが IPv4にしか対応していない。
- 暫定的なIPv6対応にトランスレータを使用。
- TRT方式(FreeBSD faith)を使用。

ネットワーク構成



www.sakura.ad.jp
support.sakura.ad.jp
server.sakura.ad.jp
www.sakura.ne.jp

faq.sakura.ad.jp

sakura.teamlab-search.jp

外部のASPを使用

トランスレータの運用

- TRT方式は、TCPを終端する。
- トランスレート先のIPv4サーバがダウンしても、IPv6側からTCPのコネクションが張れる。
- 監視はTCPコネクションだけでなく、コンテンツの中身のチェックが必要。
- HTTPだと、ステータスコードなど。
- IPv4アクセス元がトランスレータのアドレスになる。
- 本来のアクセス元(IPv6)を調べるには、トランスレータのログと突き合わせる必要がある。

トランスレータの問題点

- 一般的なアドレス共有の問題点
  http://tools.ietf.org/html/draft-ietf-intarea-shared-addressing-issues-01

  - ポート割り当て
  - ICMPパケットの扱い
  - 分割されたパケットの扱い
  - マルチキャスト
  - モバイルIP
  - 単一障害点
  - ロギング
  - spamブラックリスト
  - IPSEC
  - 認証
  - トレーサビリティ
  - 地理的な位置情報

トランスレータへの付加機能検討

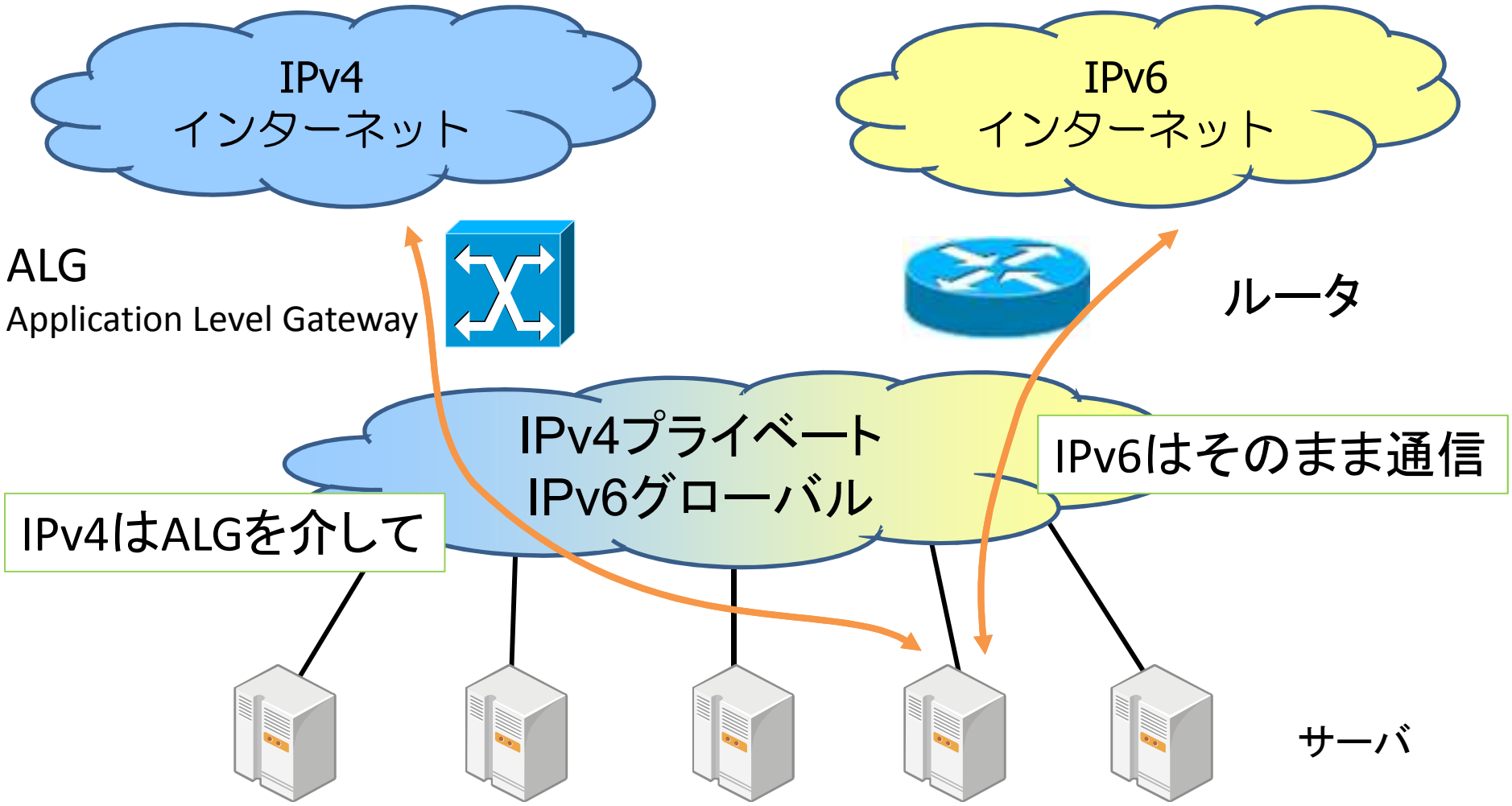
- ロギング機能
- FireWall機能
  - パケットフィルタ
  - DoS攻撃によるセッション溢れ対策
  - TCP SYN Cookie
- ロードバランシング機能
  - 中継先のサーバのHealthCheckをして、負荷分散
- コンテンツキャッシュ機能
- その他

IPv4枯渇時代のホスティングサービス

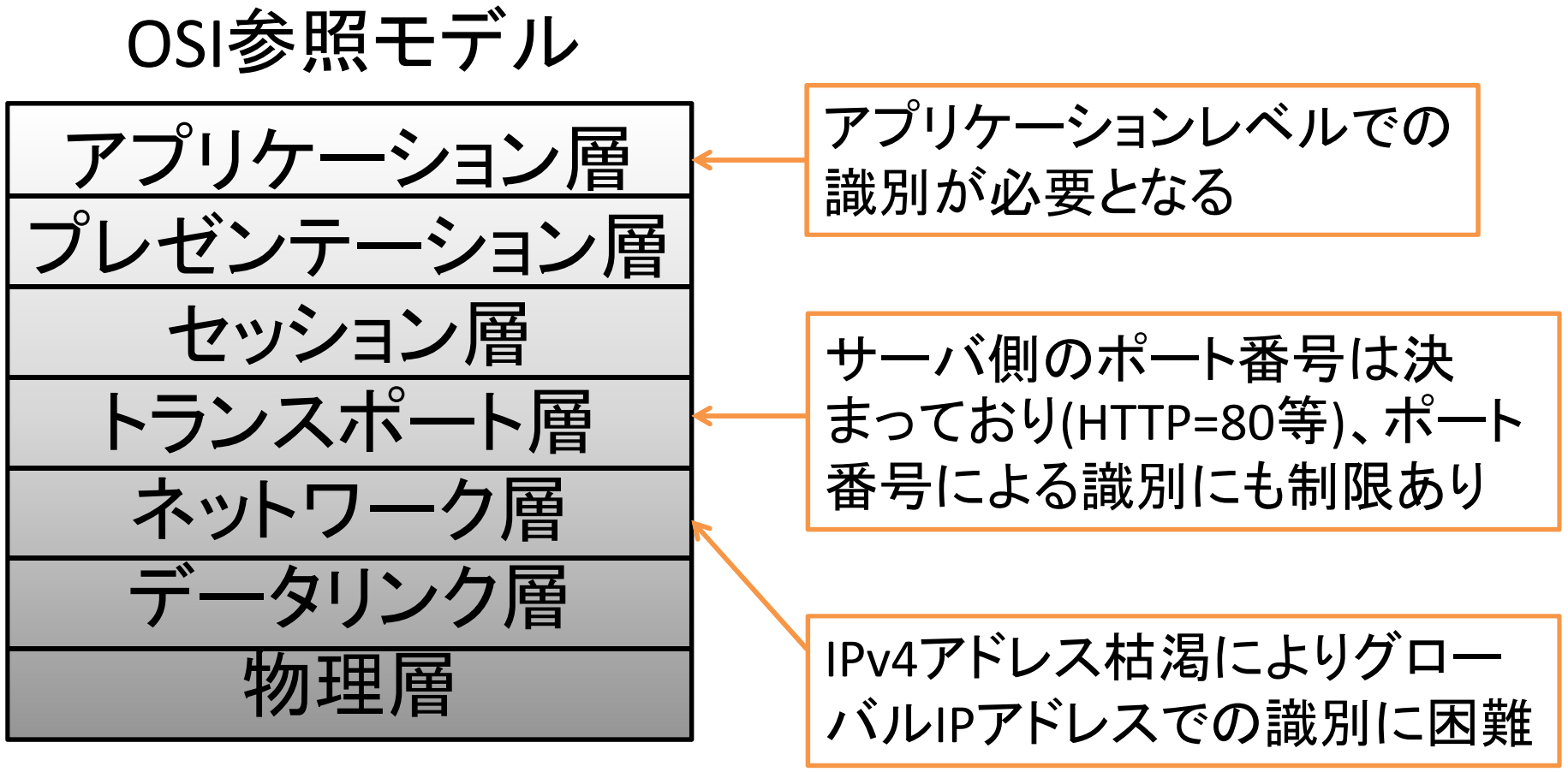
IPv4アドレスが枯渇すると？

- サーバにIPv4グローバルアドレスが振れなくなる可能性もある。
  - できるだけ避けたいが、不可避な状況も想定される。
  - IPv6グローバルアドレスと、IPv4プライベートアドレスを割り当てる。
- IPv4グローバルアドレスはオプション扱いになる。
- 場合によっては、ポート番号単位での販売も。
- IPv4インターネットからのアプリケーションの到達性を提供する。

IPv4枯渇時代のホスティングサービス



なぜALGが必要か？


OSI参照モデル
アプリケーション層
プレゼンテーション層
セッション層
トランスポート層
ネットワーク層
データリンク層
物理層
アプリケーションレベルでの識別が必要となる
サーバ側のポート番号は決まっており(HTTP=80等)、ポート番号による識別にも制限あり
IPv4アドレス枯渇によりグローバルIPアドレスでの識別に困難

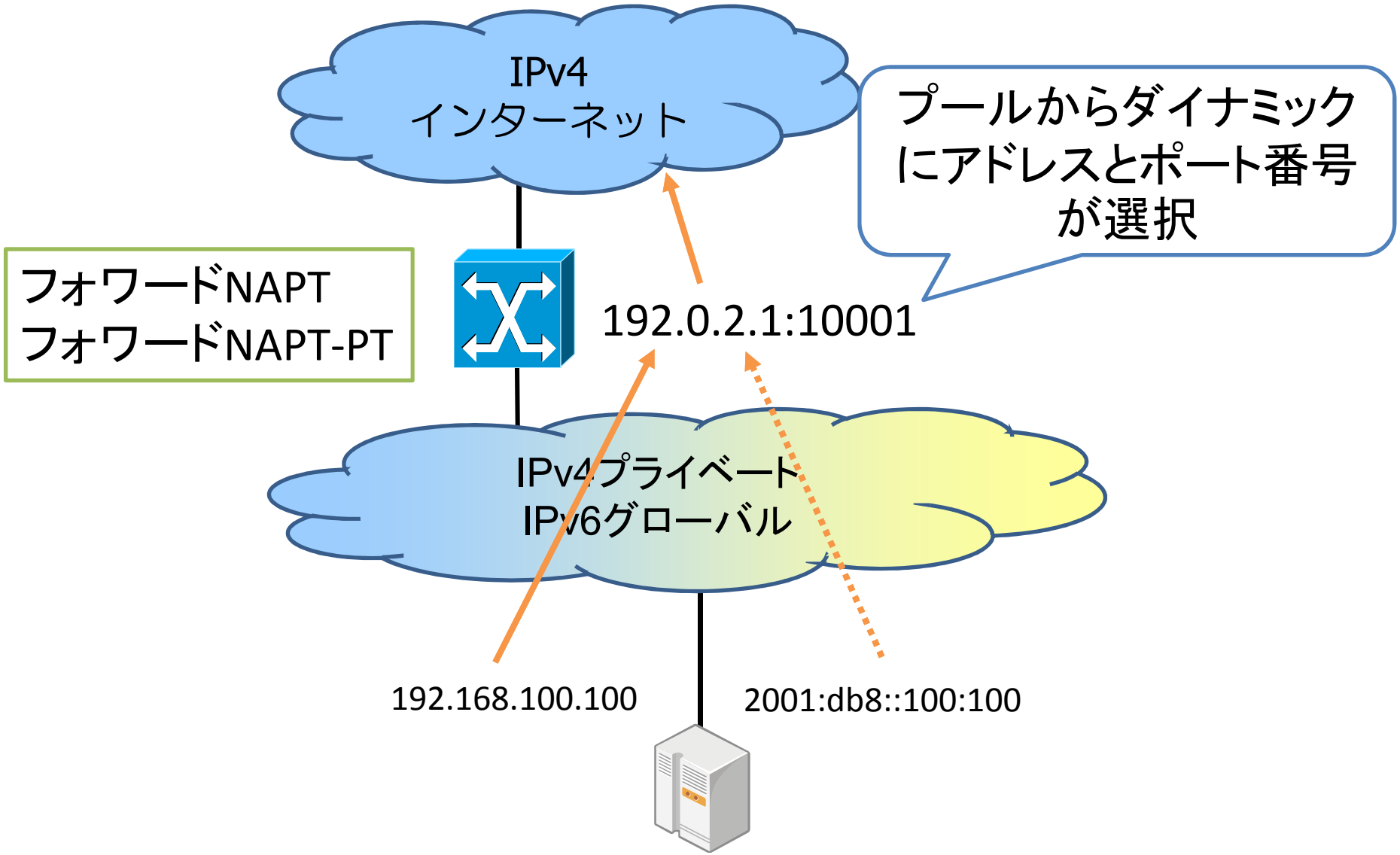
ALGの機能

- IPv4インターネットからのアプリケーション到達性を提供。LSN、トランスレータの機能を併せ持つ。
- IPレイヤ
  - IPv4グローバル⇔IPv4プライベート変換
  - IPv4グローバル⇔IPv6グローバル変換
  - フォワードNAT（NAPT、NAPT-PT）
  - 1:1NAT（フォワード、リバース双方向）
  - リバースNAT（ポートフォワード）

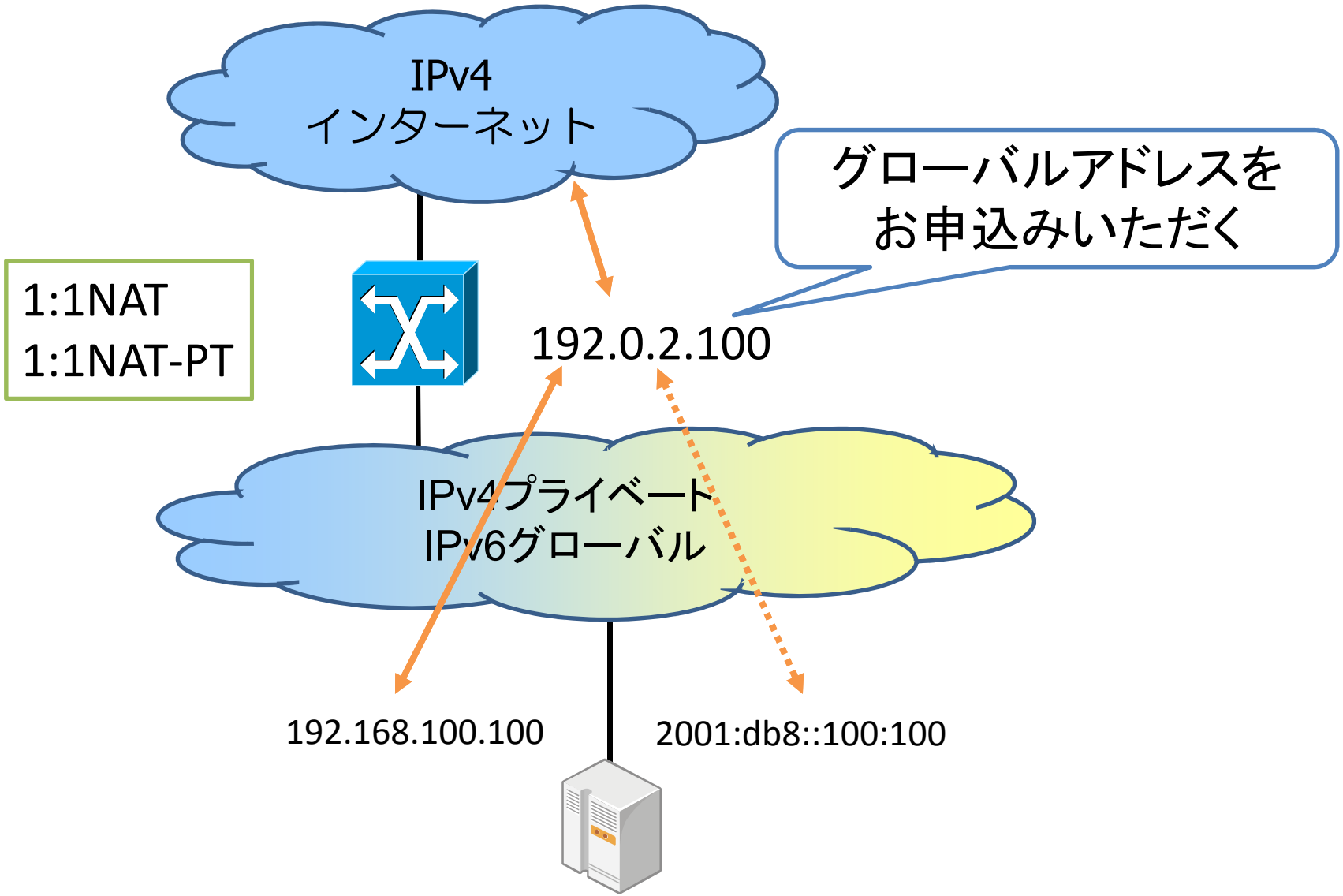
ALGの機能

- アプリケーションレイヤ
  - HTTP Name Base Virtual Host
  - SMTPゲートウェイ
  - SIPプロキシ
  - その他アプリケーションごとに対応

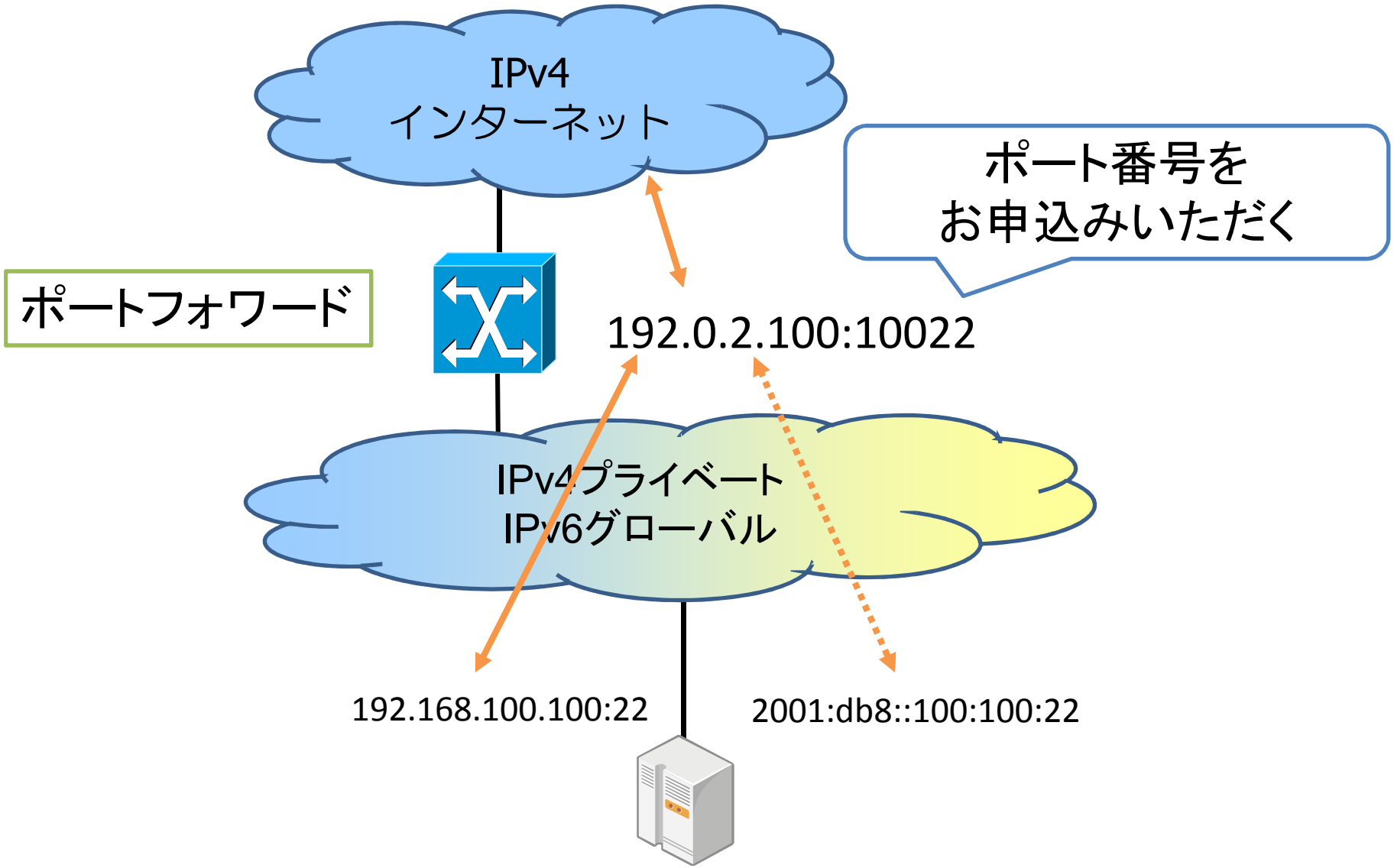
ALGの機能


IPv4
インターネット
プールからダイナミック
にアドレスとポート番号
が選択
フォワードNAPT
フォワードNAPT-PT
192.0.2.1:10001
IPv4プライベート
IPv6グローバル
192.168.100.100
2001:db8::100:100

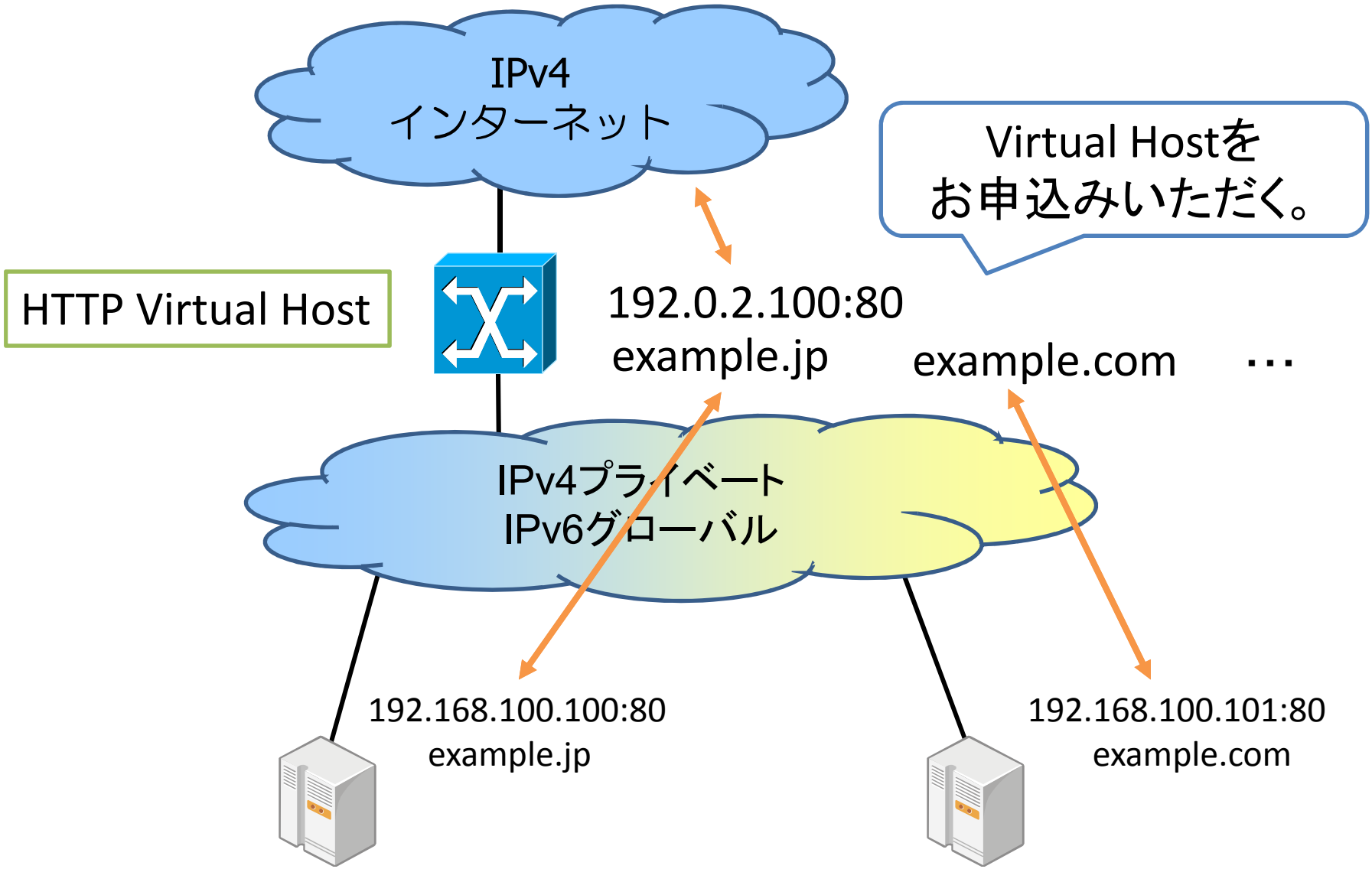
ALGの機能


IPv4
インターネット
グローバルアドレスを
お申込みいただく
1:1NAT
1:1NAT-PT
192.0.2.100
IPv4プライベート
IPv6グローバル
192.168.100.100
2001:db8::100:100

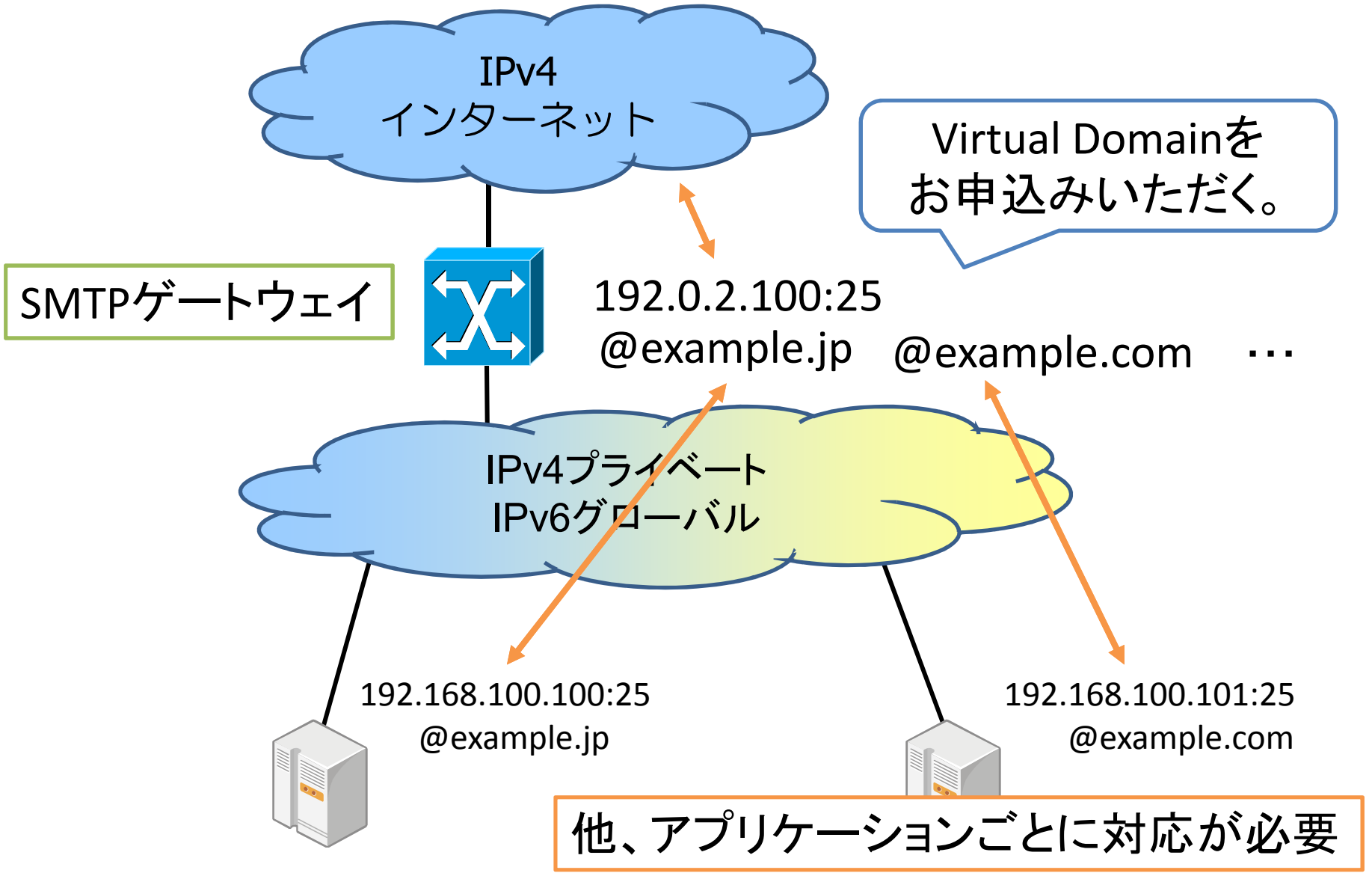
ALGの機能


IPv4
インターネット
ポート番号を
お申込みいただく
ポートフォワード
192.0.2.100:10022
IPv4プライベート
IPv6グローバル
192.168.100.100:22
2001:db8::100:100:22

ALGの機能


IPv4
インターネット
Virtual Hostを
お申込みいただく。
HTTP Virtual Host
192.0.2.100:80
example.jp
example.com
…
IPv4プライベート
IPv6グローバル
192.168.100.100:80
example.jp
192.168.100.101:80
example.com

ALGの機能


IPv4
インターネット
Virtual Domainを
お申込みいただく。
SMTPゲートウェイ
192.0.2.100:25
@example.jp
@example.com
…
IPv4プライベート
IPv6グローバル
192.168.100.100:25
@example.jp
192.168.100.101:25
@example.com
他、アプリケーションごとに対応が必要

まとめ

- データセンター屋において、IPv4枯渇対策として一番重要なのは「枯渇後のIPv4アドレス確保」
- 今後「IPv4アドレス争奪戦」が繰り広げられる。
- IPv4アドレスを持っている事業者が業界を支配し、持っていない事業者は衰退する。
- IPv4アドレス共有型の提供モデルも検討が必要。
- 一般的にIPv6対応が取り沙汰されることが多いが、「トランスレーション」「IPv4アドレス確保」と共にバランスよく進める必要がある。

議論

- 枯渇後にIPv4アドレスを確保する方法は？
- 既に確保の検討、対策を実施されている事業者さんはいらっしゃいますか？
- トランスレータに付加機能を実装するならば、どのような機能が欲しいか？
- インターネットが完全にIPv6に移行するのはいつごろでしょうか？