

御社のネットワークは、IPv6導入進んでいますか？
～ 企業ネットのIPv6導入動向と、課題～

NTTコミュニケーションズ 宍倉弘祐

NTTコミュニケーションズ 新井研二

発表者について:

- 穴倉
 - 法人向けインターネット常時接続サービス(OCN)の設計開発に従事
- 新井
 - 法人向けIP-VPNサービス (Arcstar IP-VPN)の設計・開発に従事

目的:本セッションの目的

- 企業ネットのIPv6導入検討事例を紹介
- 直面した課題について共有
- 今後の議論の材料となることを想定しています

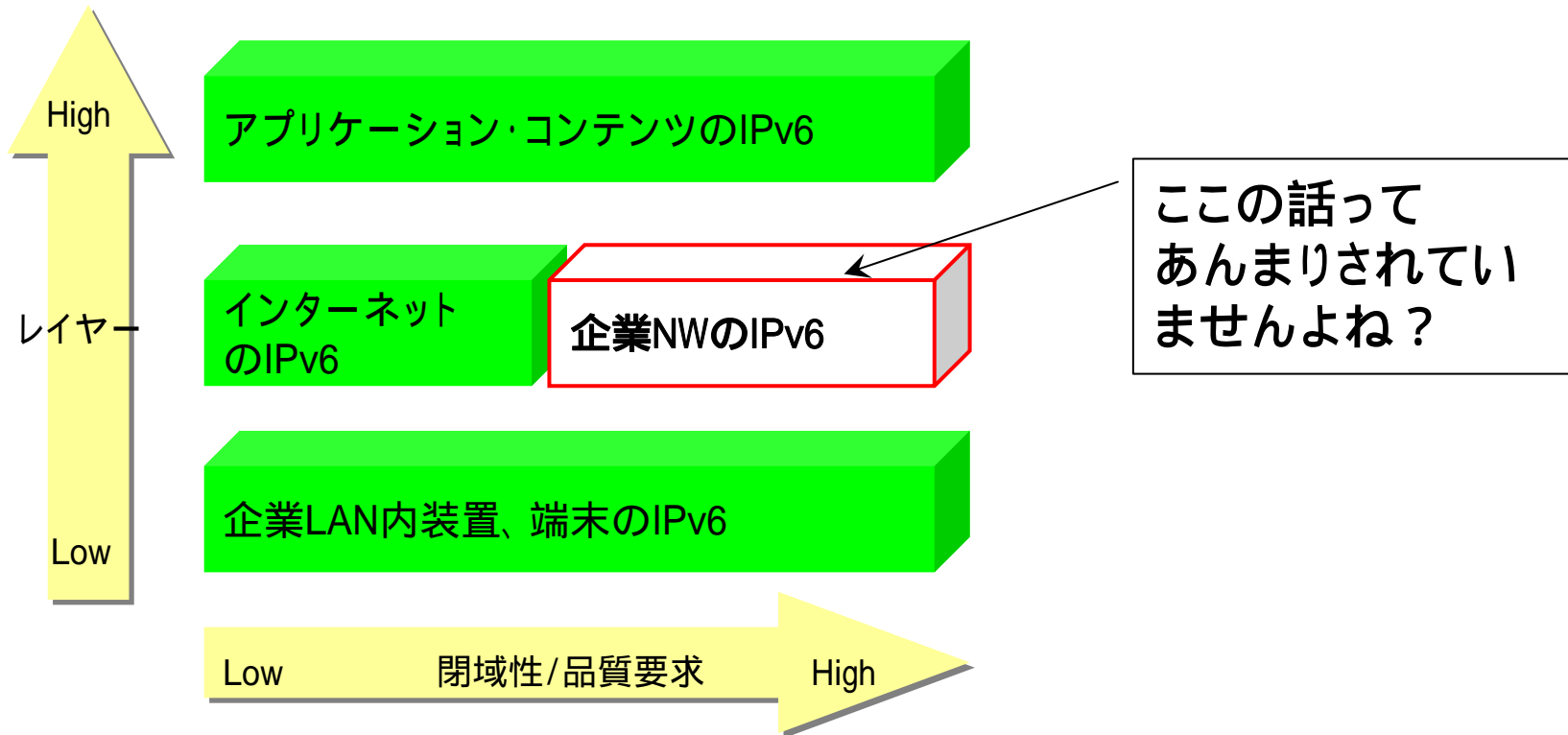
JANOG:これまでのIPv4枯渇/IPv6関連セッション

- JANOG20
 - 「IPv4アドレス枯渇を世界各地で、そして帯広で考える」
 - 「IPv6 filter recommendations 活動報告」
- JANOG21
 - 「つぶらな瞳で会場に聞いてみる～あなたの環境はIPv6に移行できる？」
 - 「IPv4アドレス枯渇に向けて～オペレーターが取り組むべき解決策を一緒に考えよう！～」
- JANOG22
 - 「IPv4アドレス 販売終了のお知らせ？～ISPによるNATで起きること～」
 - 「忘れがちなIPv6のアドレス構成」
 - 「IPv4枯渇、あなたがお使いのWebサービスは生き残れますか？」
- JANOG23
 - 「IPv6ネットワークデザイン」
 - 「IPv4/IPv6 共存環境におけるサービス移行 私たちは今何をすべきか」

などなど

JANOG: 企業NWへフォーカス

過去のJANOG Meetingを振り返ってみると...



・そこで今回は

「企業NWにおけるIPv6導入」

についてフォーカスします

お題目

- 企業NWと、IPv6の必要性 穴倉
- 企業NWへのIPv6導入ポイント 新井
- 直面している課題 新井 & 穴倉

企業NWと、IPv6の必要性

～ 最近受けた問い合わせと回答例 ～

ある問い合わせ

- ある企業のNW管理者 Aさん

Q. 「IPアドレスが枯渇するから、IPv6が必要って聞いたけど、うちの企業NWは今も問題なく、使えているから特にIPv6を気にしなくていいよね？」

IPv4アドレス枯渇による企業への影響

アドレスが枯渇すると。。。

1. グローバルIPv4アドレスが入手が困難になる
2. IPv6アドレスを利用したユーザが増えてくる

企業の影響範囲例

1. IPv4アドレスが入手が困難になる

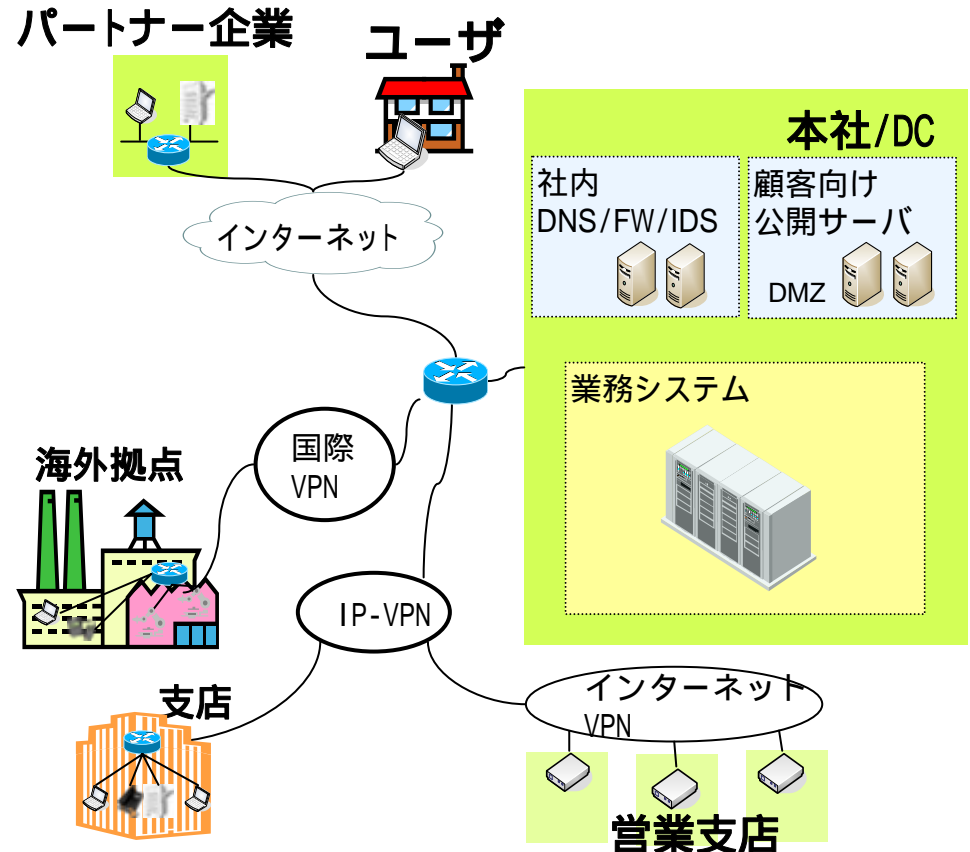
公開サーバの増設が困難

グローバルIPv4アドレスを使った
VPN(IPsec)の拠点追加が困難

2. IPv6アドレスを利用したユーザが増えてくる

IPv6のみのユーザとのアクセス不能

IPv6アドレスを前提とした市販アプリケーションが利用できない



回答例

- ある企業のNW管理者 Aさん

Q. 「IPアドレスが枯渇するから、IPv6が必要って聞いたけど、うちの企業NWは今も問題なく、使えているから特にIPv6を気にしなくていいよね？」

A. 「いいえ、IPv4グローバルアドレスの入手が困難になり、IPv6ユーザが増えてくることで、影響を受ける箇所があります。IPv6も考えてみて下さい」

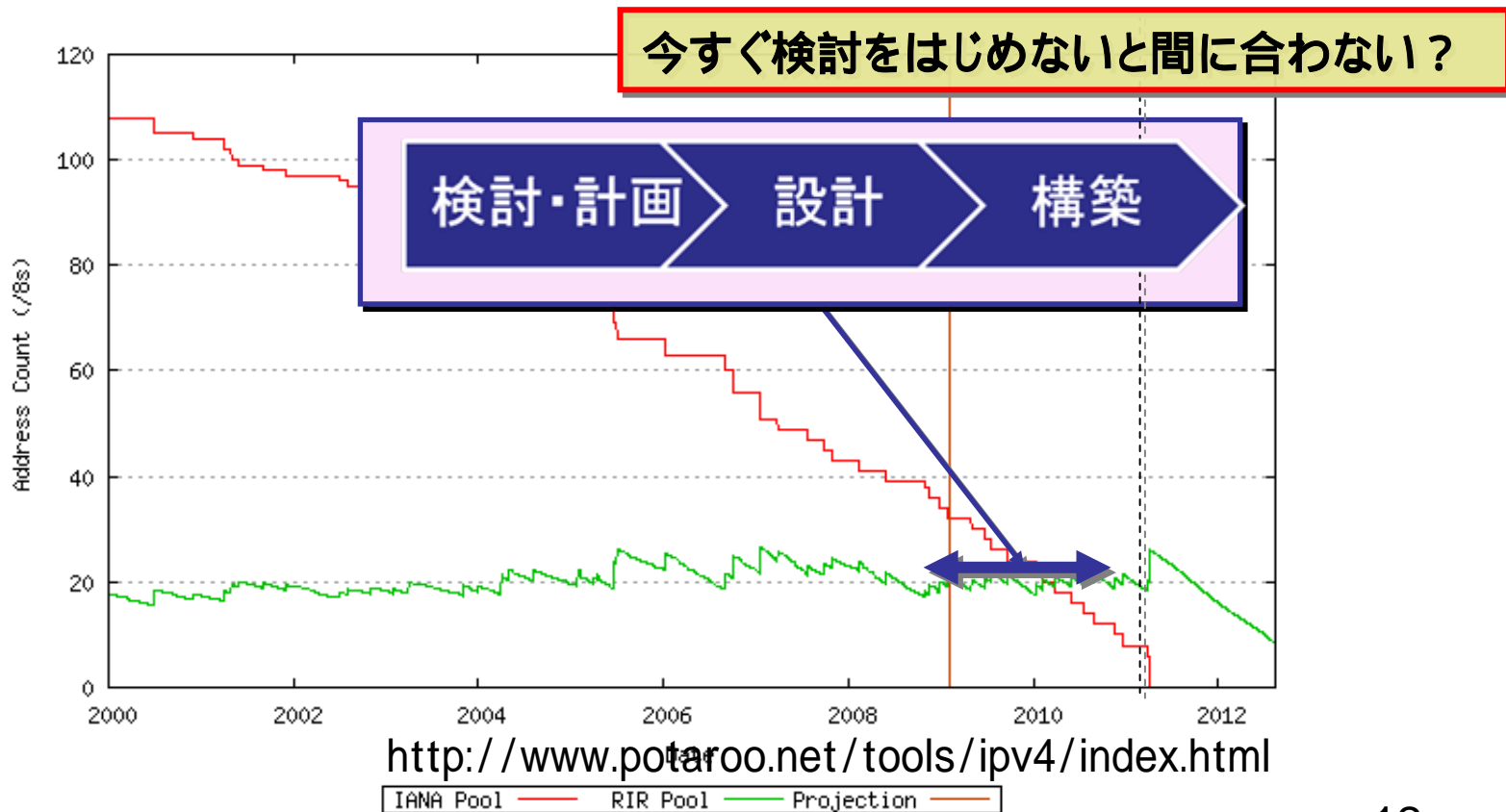
ある問い合わせ

- あるSIer勤務 Bさん

Q. 「IPアドレスが枯渇して、IPv6が必要って聞いたけどIPv6を気にするにしても、だいぶ先でしょ？」

IPv4アドレス枯渇時期の予測

- IPv4アドレスが枯渇するのは2011年頃と推測される
- 社内システムを入れ替えるには、計画・設計段階から構築までを含めると、半年から2年ぐらい？



回答例

- あるSIer勤務 Bさん

Q. 「IPアドレスが枯渇して、IPv6が必要って聞いたけどIPv6を気にするにしても、だいぶ先でしょ？」

A. 「いいえ、社内システムを入れ替えるのにどのくらいかかりますか？計画・設計段階から構築までを含めると、そろそろ検討をはじめないと間に合わなくなるかもしれません」

ある問い合わせ

- ある企業NW管理者 Cさん
- Q. 「だって、他の企業やってないよね？ やってるのって、公共事業とか、IPv6マルチキャストやりたいひとだけでしょ？ うちだけやる必要あるの？」

事例

- (最近の導入検討事例を紹介しました)

導入傾向の変化

- **今まで**
 - IPv6ならではの機能(マルチキャスト、IPsec)
 - 新規構築システム (既存システムは触らない)
 - 特定用途(通信相手が限定)

- **最近**
 - IPv4の代替 (同じことをやるのがv6になっただけ)
 - 既存システムへの導入検討
 - DMZだけでなく、内部NWの検討も

回答例

- ある企業NW管理者 Cさん
- Q. 「だって、他の企業やってないよね？ やってるのって、公共事業とか、IPv6マルチキャストやりたいひとだけでしょ？ うちだけやる必要あるの？」
- A. 「いえいえ、v4枯渇対応や、NW更改のタイミングで、v6導入の検討をはじめているところはありますよ。」

ある問い合わせ

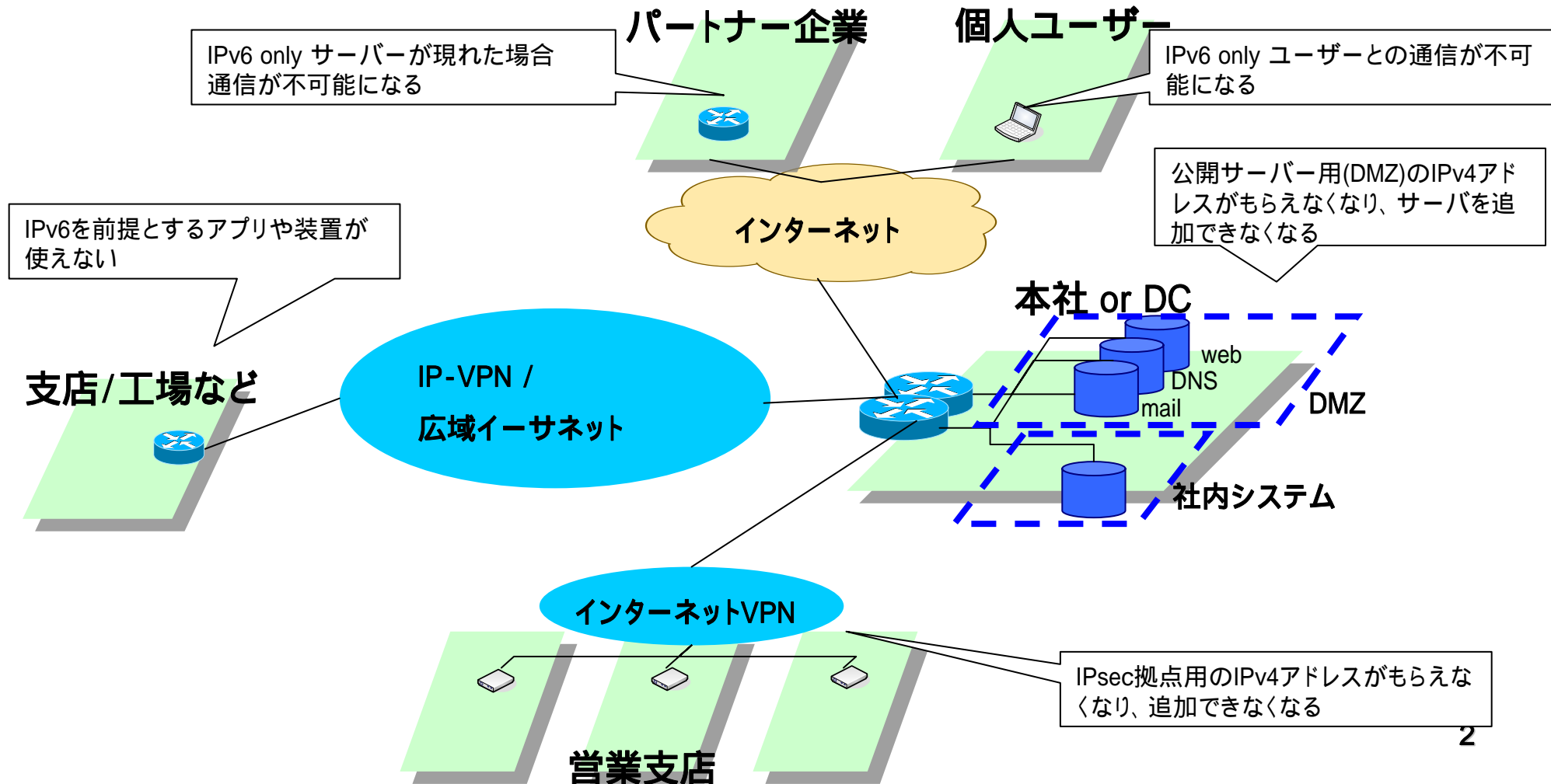
- ある企業NW管理者 Cさん
- Q. 「じゃあ、どこをどうすればいいの？」
- A. 「各箇所で考える必要がありますね」

企業NWへのIPv6導入ポイント

IPv4アドレスが枯渇した際の企業ネットワークへの影響例

アドレスが枯渇すると。。。

- 1. グローバルIPv4アドレスが入手が困難になる
- 2. IPv6アドレスを利用したユーザが増えてくる



IPv4アドレス枯渇対策の緊急性が高いポイント

インターネットに接続する部分

パートナー企業

個人ユーザー

インターネット

1. インターネット接続回線

2. 外部公開サーバー

支店/工場など

IP-VPN /
広域イーサネット

本社 or DC

web
DNS
mail
社内システム

3. インターネットGW

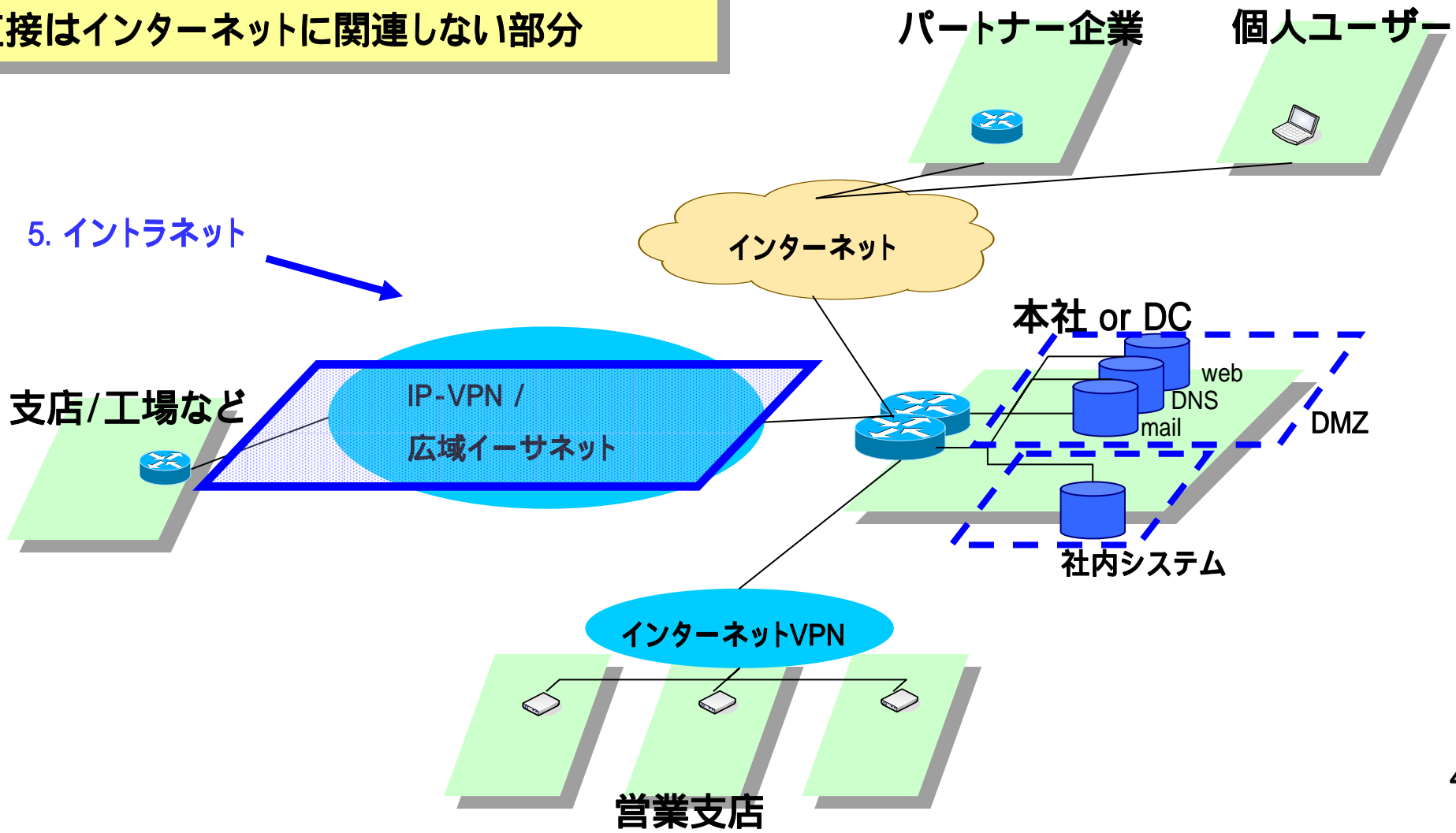
4. IPsecによる拠点間のVPN接続

インターネットVPN

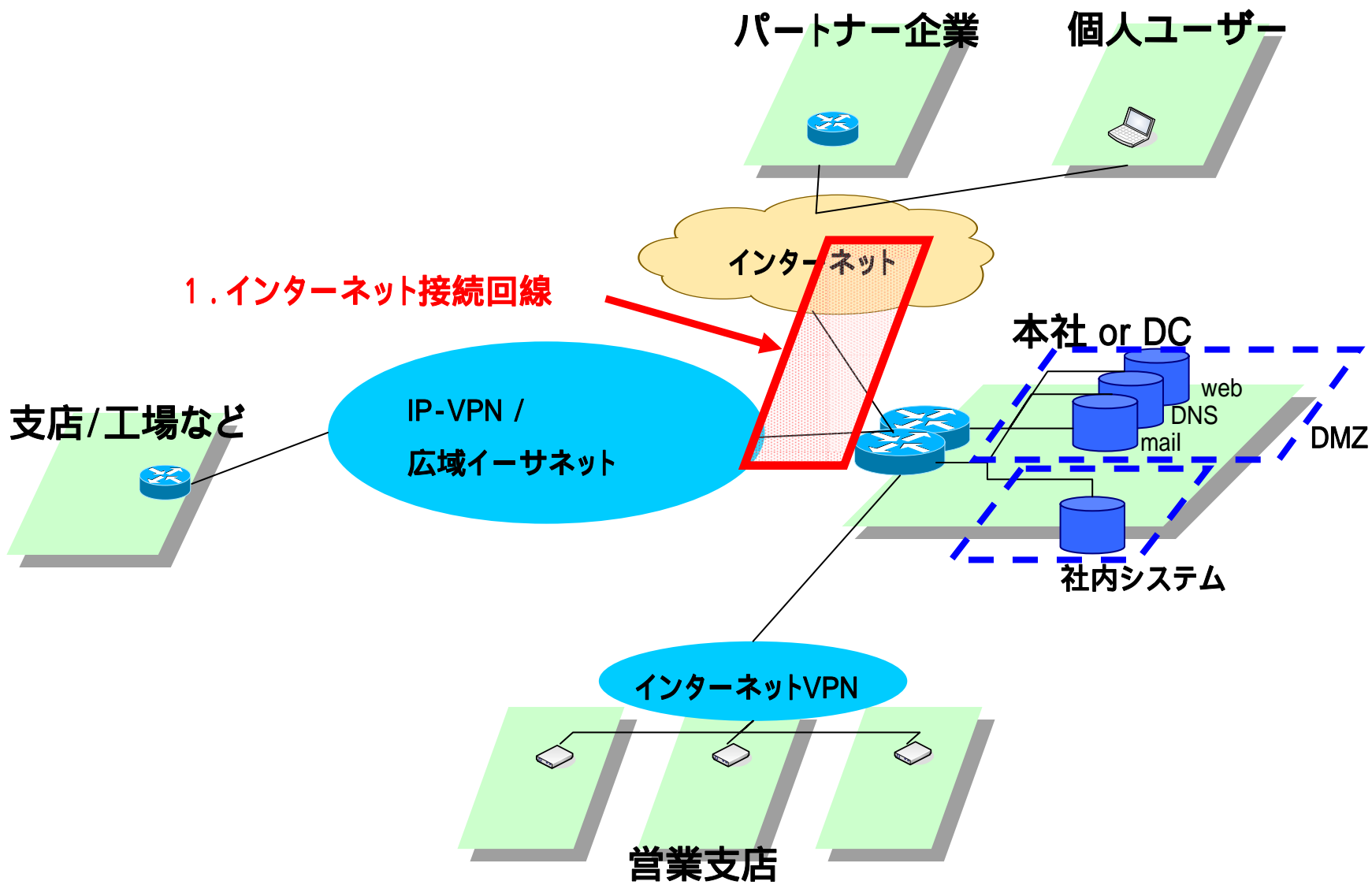
営業支店

順次対応していくポイント

直接はインターネットに関連しない部分



各ポイントの対応例



インターネット接続回線

IPv6 Internet接続必要な回線の確保

ISPのIPv6接続サービスなどを使う

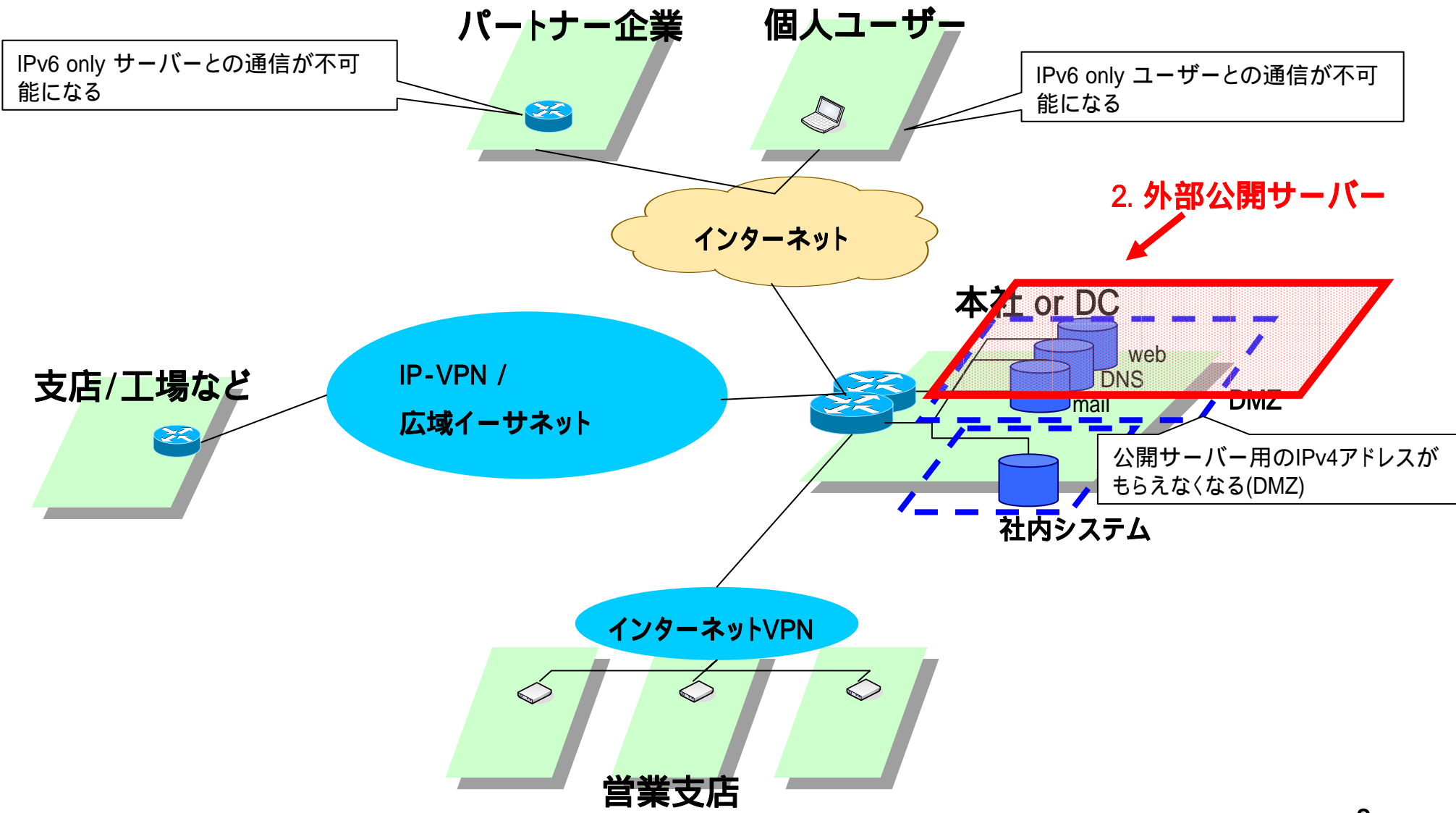
- ・大きく分けて3種類
- ・大手ISPは対応済
- ・企業向けのサービスとしてはおおむね出揃ったといえる。

接続形態	トンネル接続	ネイティブ接続	デュアル接続
スループット	カプセルングオーバーヘッドによる低下	IPv4並	IPv4並
信頼性	IPv4回線の論理障害の影響を受ける	IPv6で物理・論理ともに独立のため、IPv4回線の影響は受けない	IPv4の論理障害の影響は受けない。 物理障害の影響は受ける
コスト	安価	高価	高価

初期導入には既存回線への影響とコストを考慮し、トンネル接続

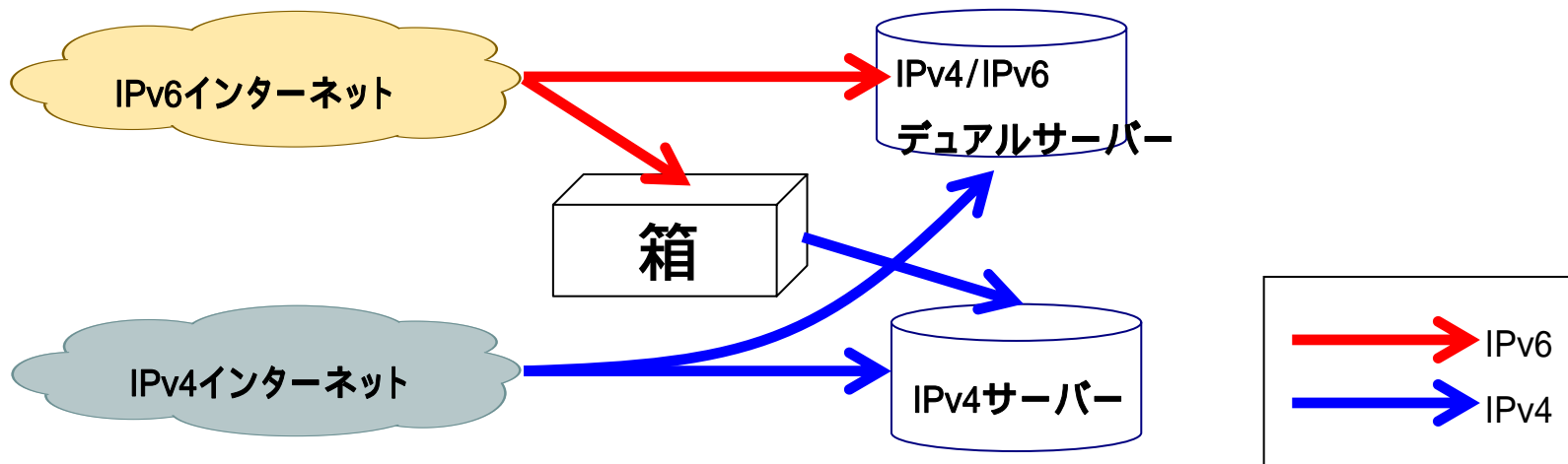
もしくは帯域を限定した別線を用意する手法がある。

その後にデュアル接続に移行するパターンが一般的。



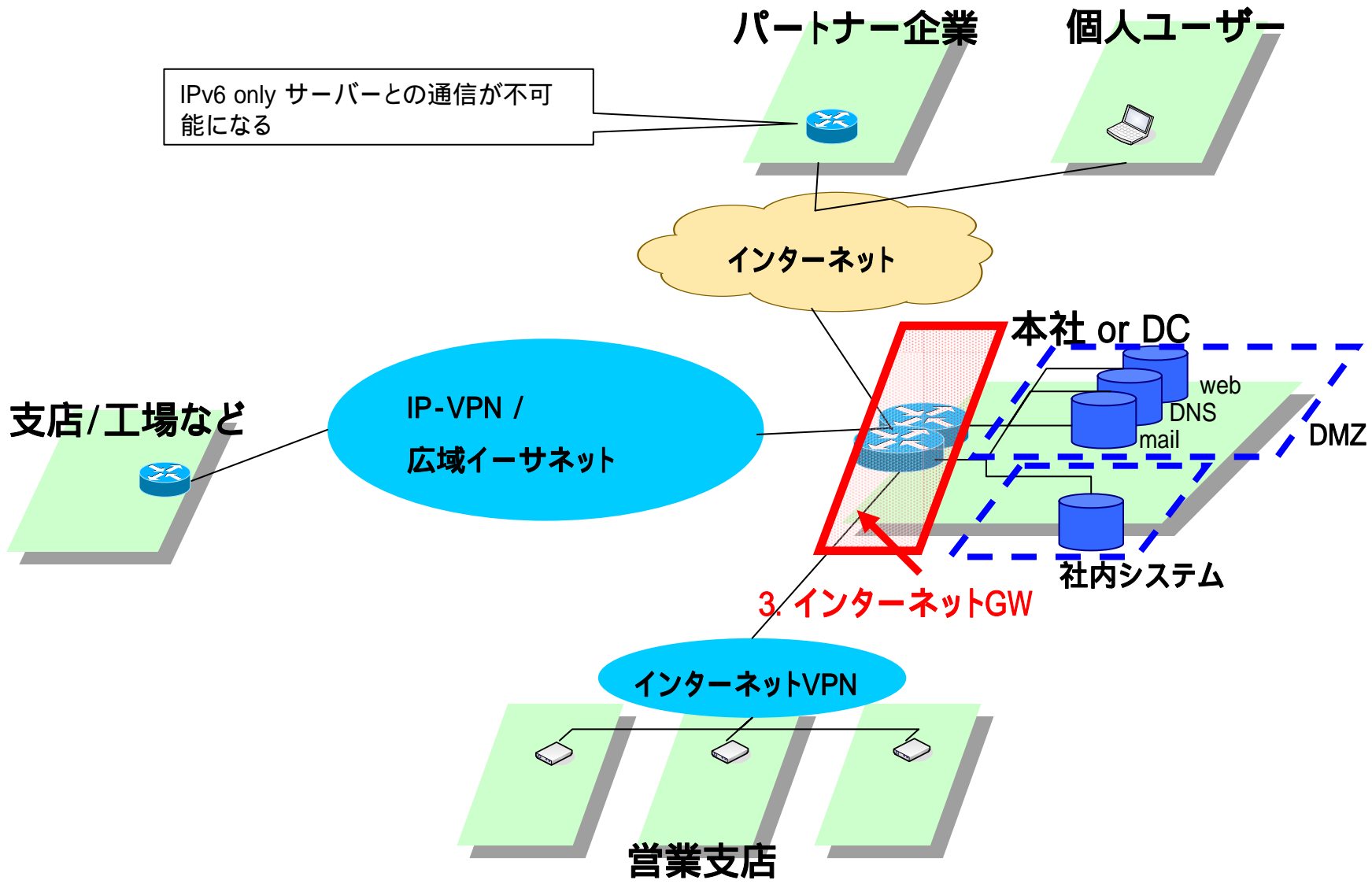
外部公開サーバー

外部のIPv6ユーザーからの到達性を確保する
リバースプロキシ、64SLBなどの”変換箱”で対応可能なケースがある



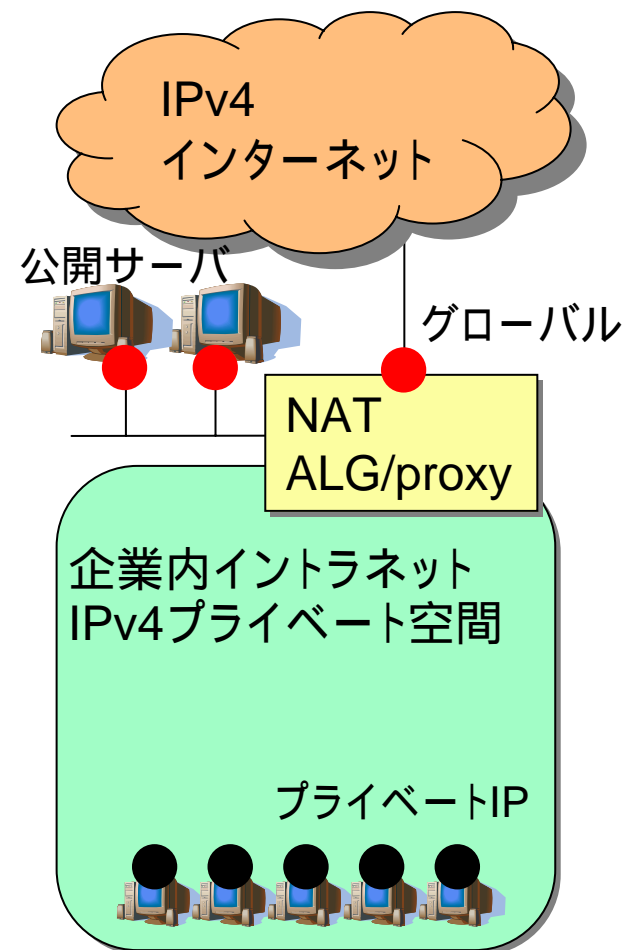
サーバーの種類や、ログ対応、運用負荷、コストを検討した結果
サーバー自体をIPv6対応することが望ましいケースもある

一日目のセッション、JANOG 24「IPv4枯渇に向けて ~コンテンツ提供者はどうすればよい? ~」でも議論されました。

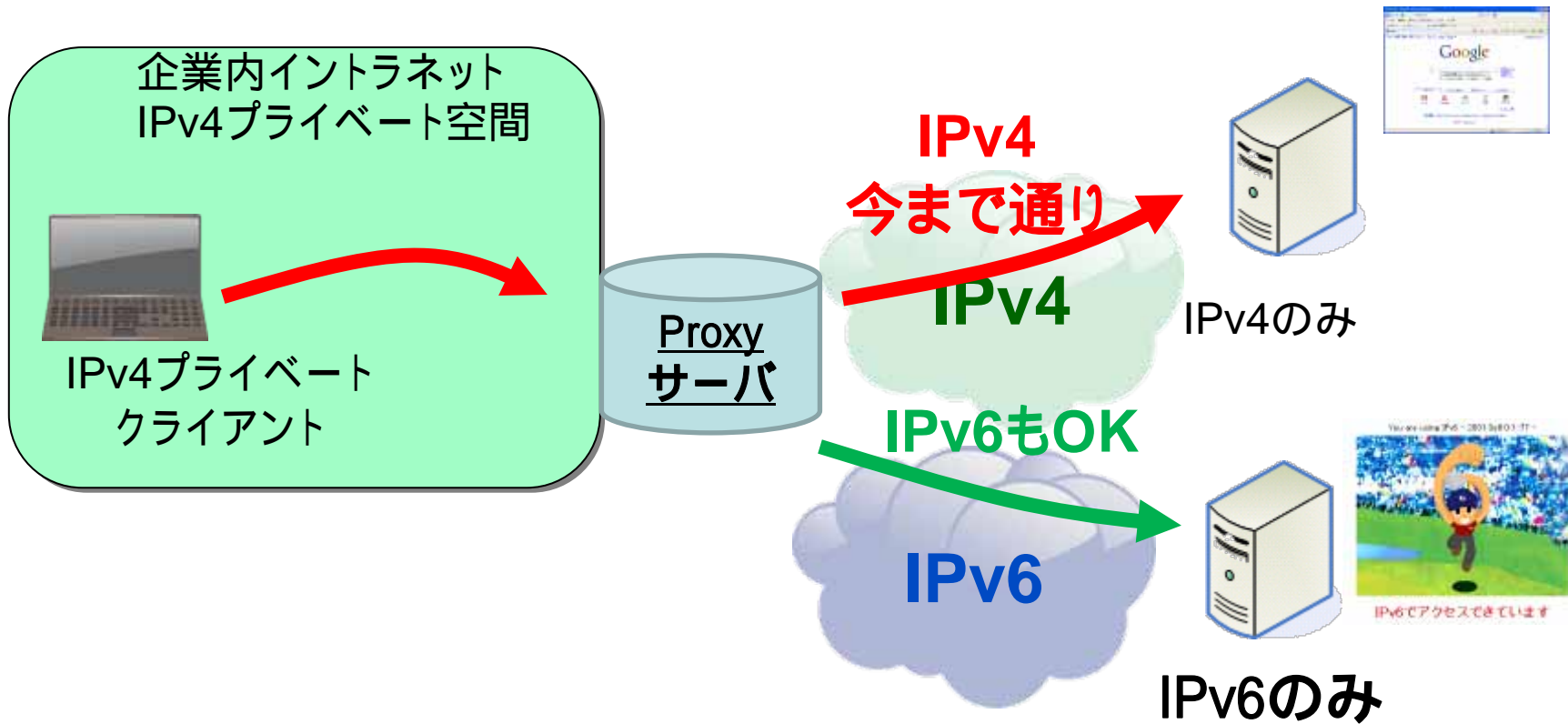


企業ネットワークの現状

- 外部接続・DMZ
少数のIPv4グローバルアドレス
で運用
NAT/ALG/proxyが一般
- 企業内イントラネット
IPv4プライベート利用が中心



インターネットGW



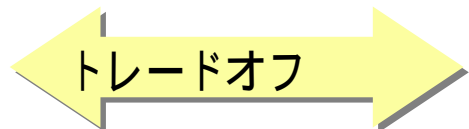
IPv4/IPv6デュアルプロキシーで中継してIPv4 / IPv6 へ接続

イントラネットとIPv6インターネット接続の関係

A . イントラネットはIPv4プライベート。IPv6インターネットに出る際は変換

既存モデル(NAT/ALG/proxy)との親和性は高く、導入自体は比較的容易

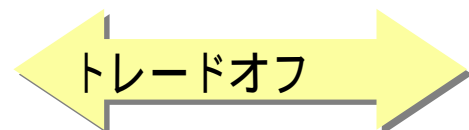
変換機器(トランスレータ、IPv6 proxy)の機器コスト/運用コストが追加になる



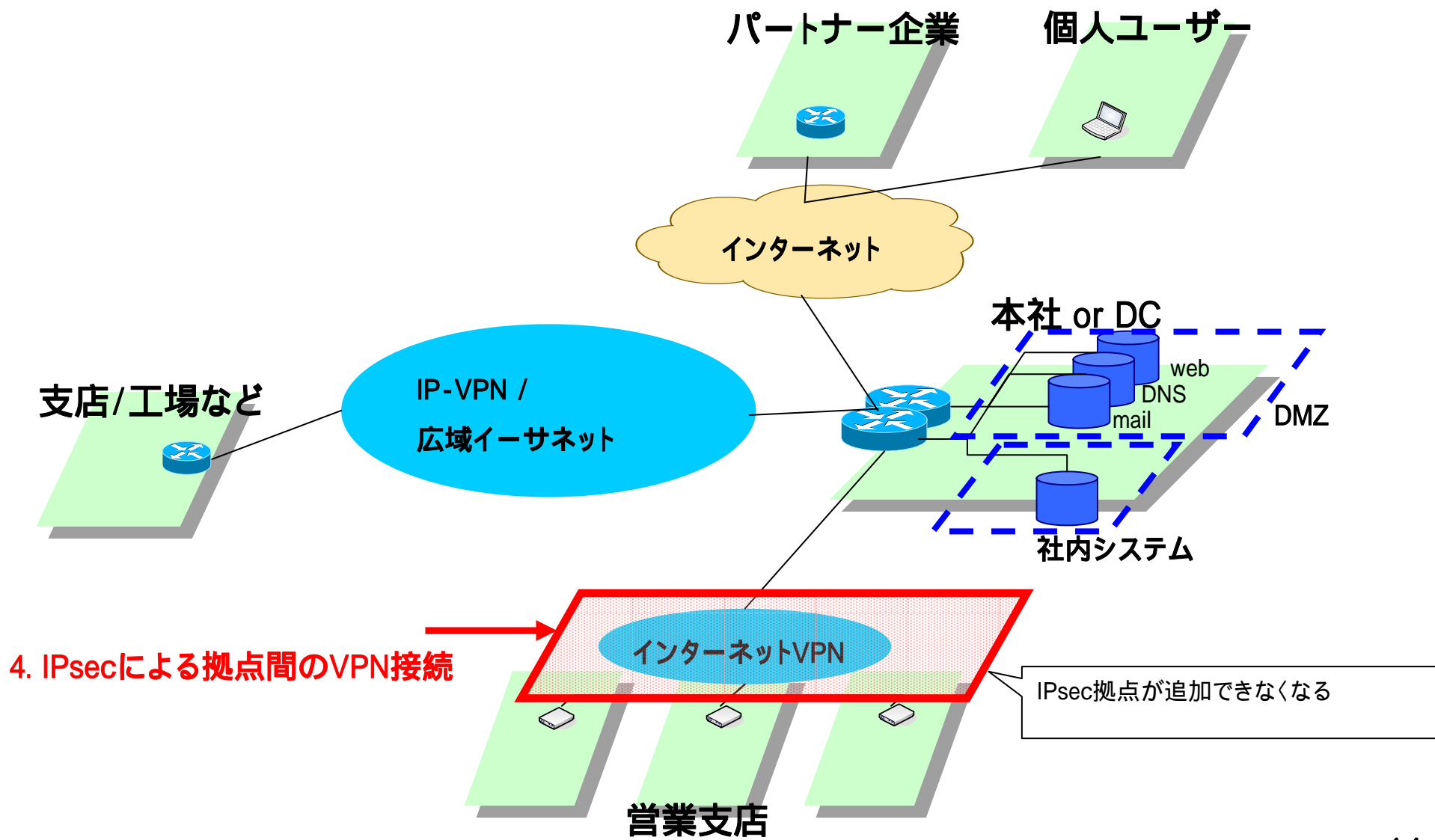
B . イントラネットにIPv6導入

新規構築や既存の網との併用による追加コストの発生

フラットな通信やマルチキャストなどIPv6の特徴を生かした新アプリの導入

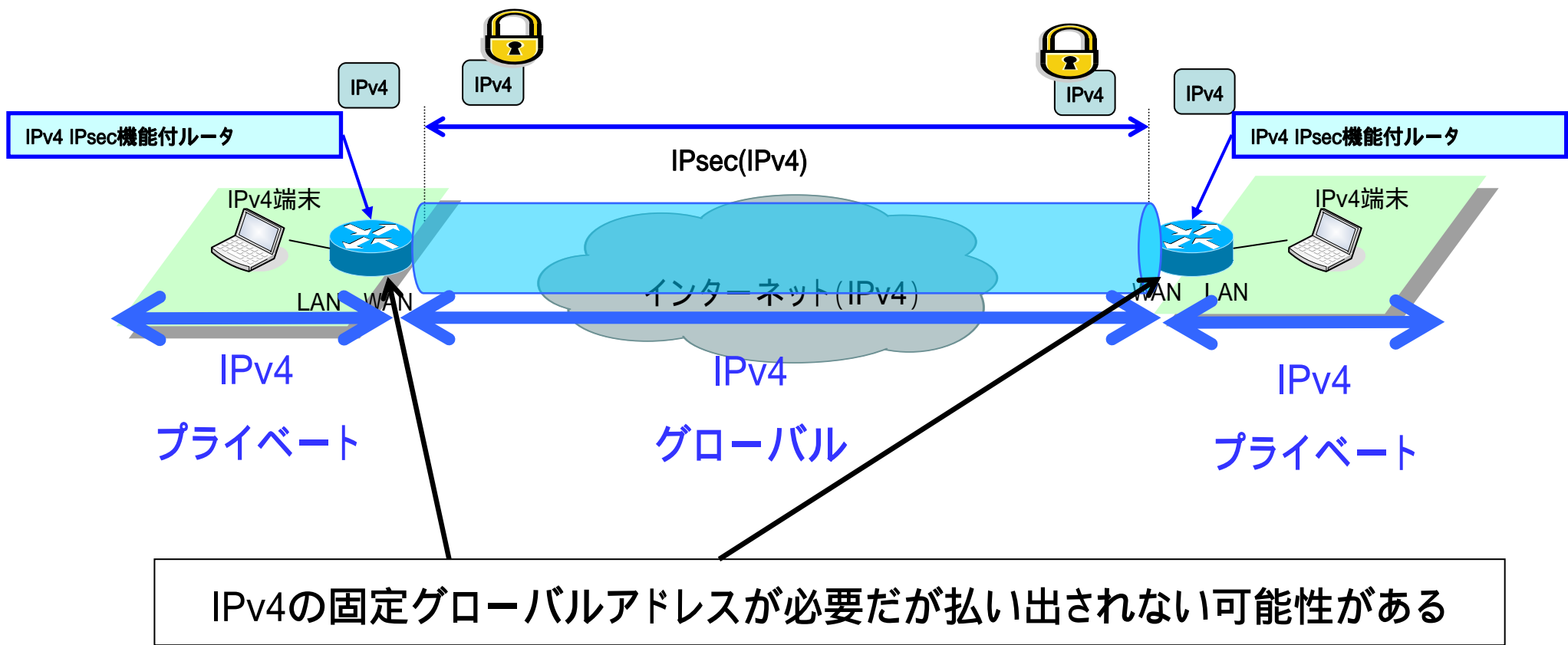


企業としては、AとBの両方を視野に入れて検討することが有効
ある企業にとってはA。ある企業にとってはB、または両方という企業もありえる。



IPsecによる拠点間の接続

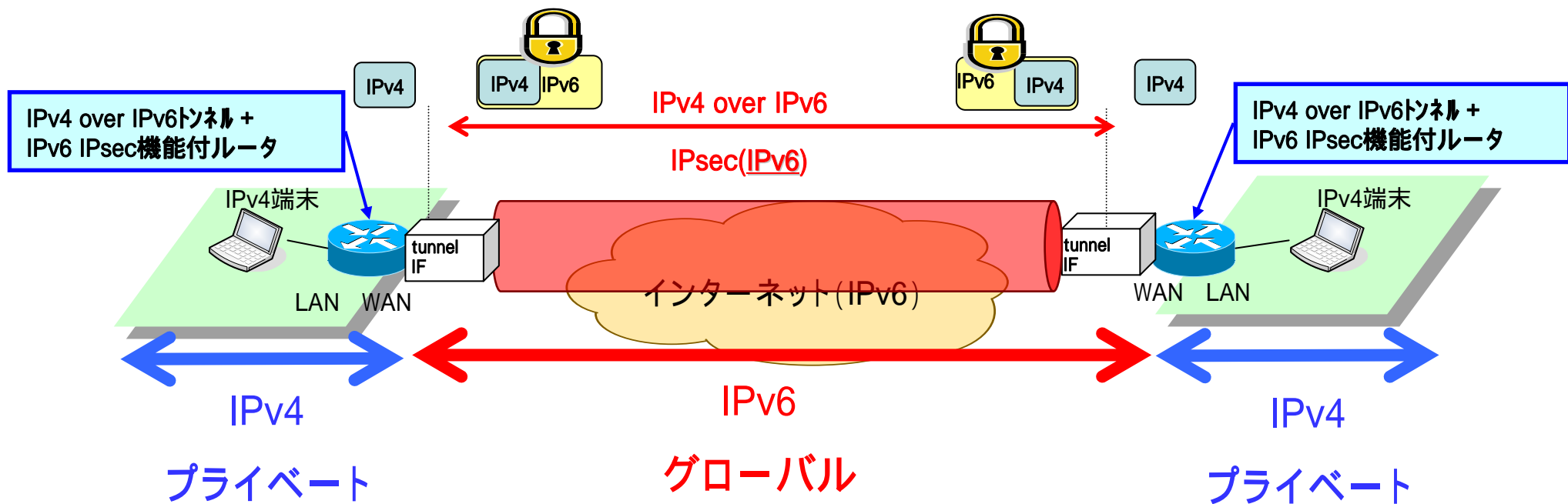
IPv4グローバルアドレスがもらえない場合に、新たにIPsec VPN拠点を追加したい



IPsecによる拠点間の接続

トンネリング(IPv4 over IPv6) + IPv6 IPsec

の機能を持つルーターで対応する手法がある



IPv4パケットをIPv6でカプセル化し、
IPv6のIPsecで暗号化して転送する

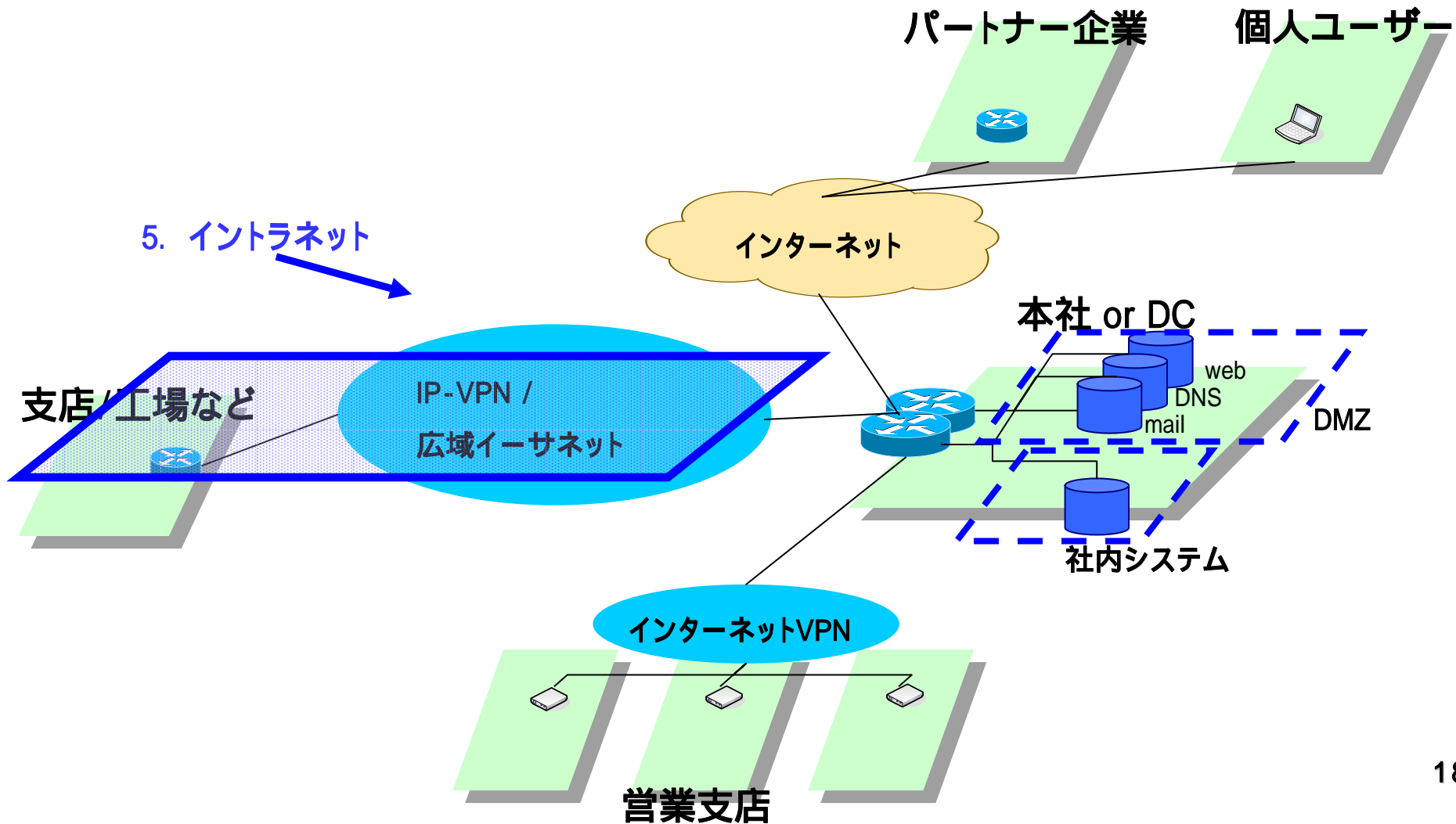
トンネリング(IPv4 over IPv6) + IPv6 IPsecの性能

最近は10万円くらいのルーターでも実用に問題ない程度に動作する

某ルータースループット試験結果

(100Mbps, 暗号化方式 AES 256bit, 双方向通信)

Packet長(byte)	64	214	512	1024	1300	1500
スループット(Mbps)	10.0	29.8	63.6	76.2	88.9	29.8



拠点間WANサービスのIPv6対応

IP-VPN

- IPレベルでのルーティングなので対応が必要
- 既存利用サービスがIPv6に対応している場合はオプション申し込みなどで継続利用可能
- 対応していない場合はIP-VPN網内での ”IPv6 over IPv4トンネリング” で対応

専用線

- 終端端末がIPv6に対応すれば特に意識せず利用可能

広域イーサネット

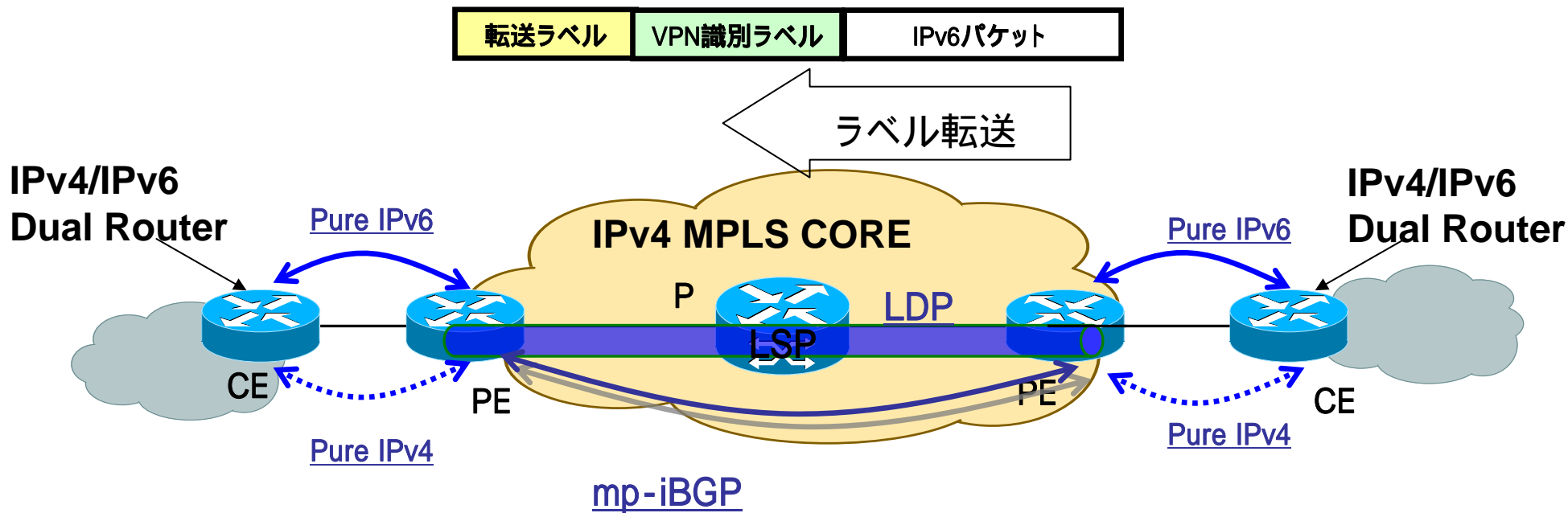
- イーサフレーム処理のため、終端端末がIPv6に対応していれば利用可能

ただし、監視機能等にIPv4を利用している場合もあるので、念のため確認が必要

(参考) IP-VPNのIPv6化の方式

6VPE方式

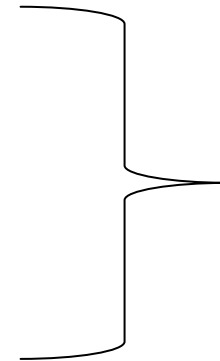
- ・RFC 4659 (2006年)
- ・MPLSを利用しているキャリアはエッジルータのみの対応でIPv6化可能
- ・単純なトンネリングと異なりスループット劣化無し
- ・FRRなどMPLS網内の技術はそのまま利用可能





直面している課題

- ・閉域網の実現に関して
 - ・簡易マルチホームに関して
 - ・端末のアドレス管理に関して
 - ・ファイアーウォールに関して
- などなど



本日はこの2つをお話します

これまでのIPv4の場合は

- グローバルアドレスで構成するが外部に経路を広告しない

もしくは

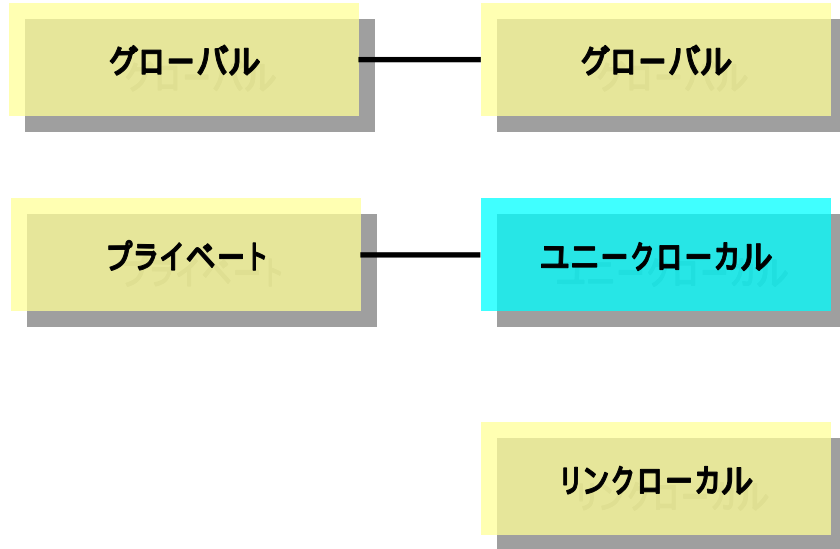
- 大半はそもそも ”ローカルな” アドレスで設計する

閉域網でのアドレス設計

通常IPv4 イン트라ネットはプライベートアドレスで構成されていますが、
代わりに何を使用します？

IPv4

IPv6



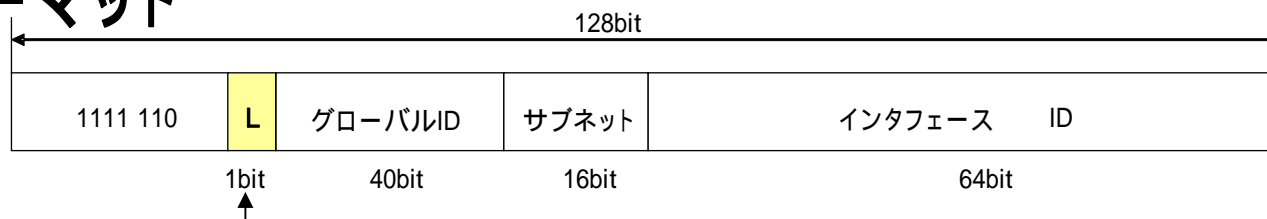
これなんだっけ？

- ・リンク内のみのためイン트라ネットでは使用不可
- ・JANOG 23 “IPv6ネットワークデザイン” 参照
 - リンクローカルアドレスの登場するプロトコル
 - 運用上の注意点

ユニークローカルアドレス(ULA)

- ・RFC4193 (2005年)
- ・社内ネットワークやVPNなどのGlobal Internetに広告しない
限定されたサイトでの使用が目的

フォーマット



L=1 (FD00::/8): 独自割り当て領域(ランダムなグローバル識別子を使用)

- グローバルIDをランダムに生成する、
完全には一意でないアドレス
- 使用に際し申請は不要

L=0 (FC00::/8): 将来定義

- 完全な一意性を保障する、管理されたアドレス
- 管理団体が配布
- 割当方法・条件・必要性が議論となり、現在未定義

OK!

グローバルID



グローバルID生成方法(RFC記載のアルゴリズム例)



数学的に厳密に一意ではないが、重複確率は極めて低い

N個のアドレスブロックで

N= 1,000	約0.00005%
N= 10,000	約0.005%
N=150,000	約1% 程度重複

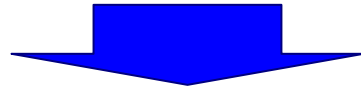
作成されるプレフィックス長は/48、サブネット16bitと合わせると/64であり、一般的なグローバルアドレスのプレフィックス長(/48-/64)と親和性は高い。それ以上(/40など)使いたい場合は複数作る必要有

実際の見たい目

作ってみると

EUI-64 =021120fffe0DC530

NTP date=cdfec4ab88d90468



fd8a:2826:0bee::/48

参照URL

<http://www.kame.net/~suz/gen-ula.html>

Q. 見た目わかりにくいから
もっとわかりやすい他のじゃだめなの？

A. **認められないとの記述あり** (fd00:dead:beaf::48などは不可)

Locally assigned Global IDs MUST be generated with a pseudo-random algorithm consistent with RFC4086

-RFC4193抜粋-

(RFC4086 "Randomness Requirements for Security")

閉域網におけるULAとGUAの比較

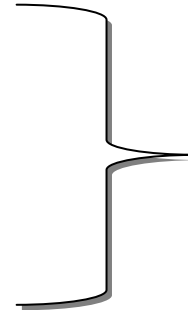
	ULA(Unique Local Address)	GUA(Global Unicast Address)
アドレス取得申請の必要有無	無	有 (/48-/64ならISPに申請)
管理・運用	ランダムイズされているため/48が多数の場合、非常に面倒	ULAに比べれば容易
外部への広告	外部への広告は不可	もちろんOK
リナンバの可能性	ランダムで作っていれば限りなく衝突の可能性が低い ランダムで作らなければ衝突の可能性もあるかもしれない	ISPの契約変更時に発生する可能性はあり
想定されるシチュエーション 意見1	<ul style="list-style-type: none"> ・試験導入 ・小規模ネットワーク ・完全に閉じたネットワーク 	<ul style="list-style-type: none"> ・大企業社内ネットワークの本格導入 ・外部接続を前提としたネットワーク
想定されるシチュエーション 意見2	<ul style="list-style-type: none"> ・閉域網にはやっぱりULAを使用した 	<ul style="list-style-type: none"> ・グローバルはインターネットに流す経路として使いたい

ULA使用時の注意点

- IPv4のプライベートアドレスと同様に外部に経路がリークしないようにする
- DNSのリークにも注意
(正引きしたら、ULAがとれてしまったりしないように)
(インターネットのルートDNSサーバに、0.0.d.f.ip6.arpa.へのクエリーを出したりしないように)
- ランダムイズされたPrefixを必ず使用しなければならない
(RFCに反して作成した場合、ネットワーク結合時のアドレス重複に伴うリナンバーが発生することがある)

課題

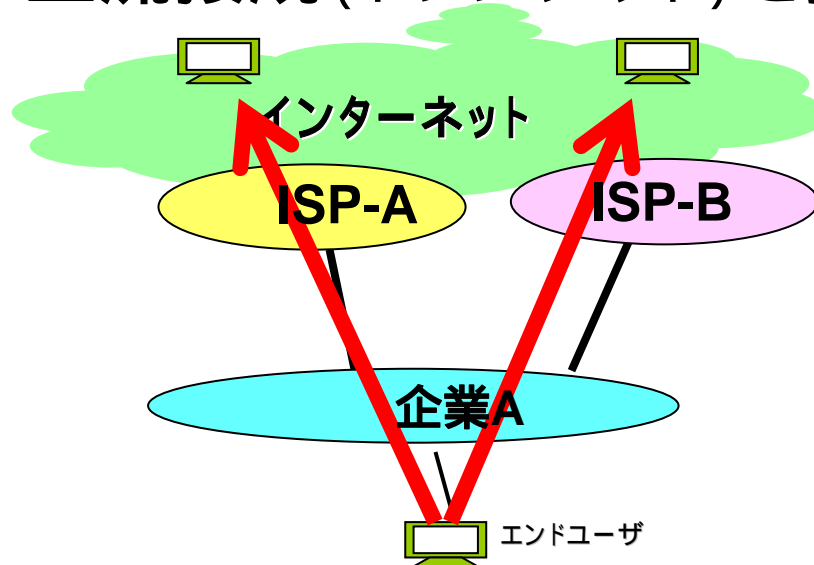
- ・閉域網の実現に関して
 - ・簡易マルチホームに関して
 - ・端末のアドレス管理に関して
 - ・ファイヤーウォールに関して
- などなど



本日はこの2つをお話
します

マルチホーム

- マルチホームおさらい
 - 冗長性確保や負荷分散などのため、2つ以上の上流接続(トランジット)を持つこと

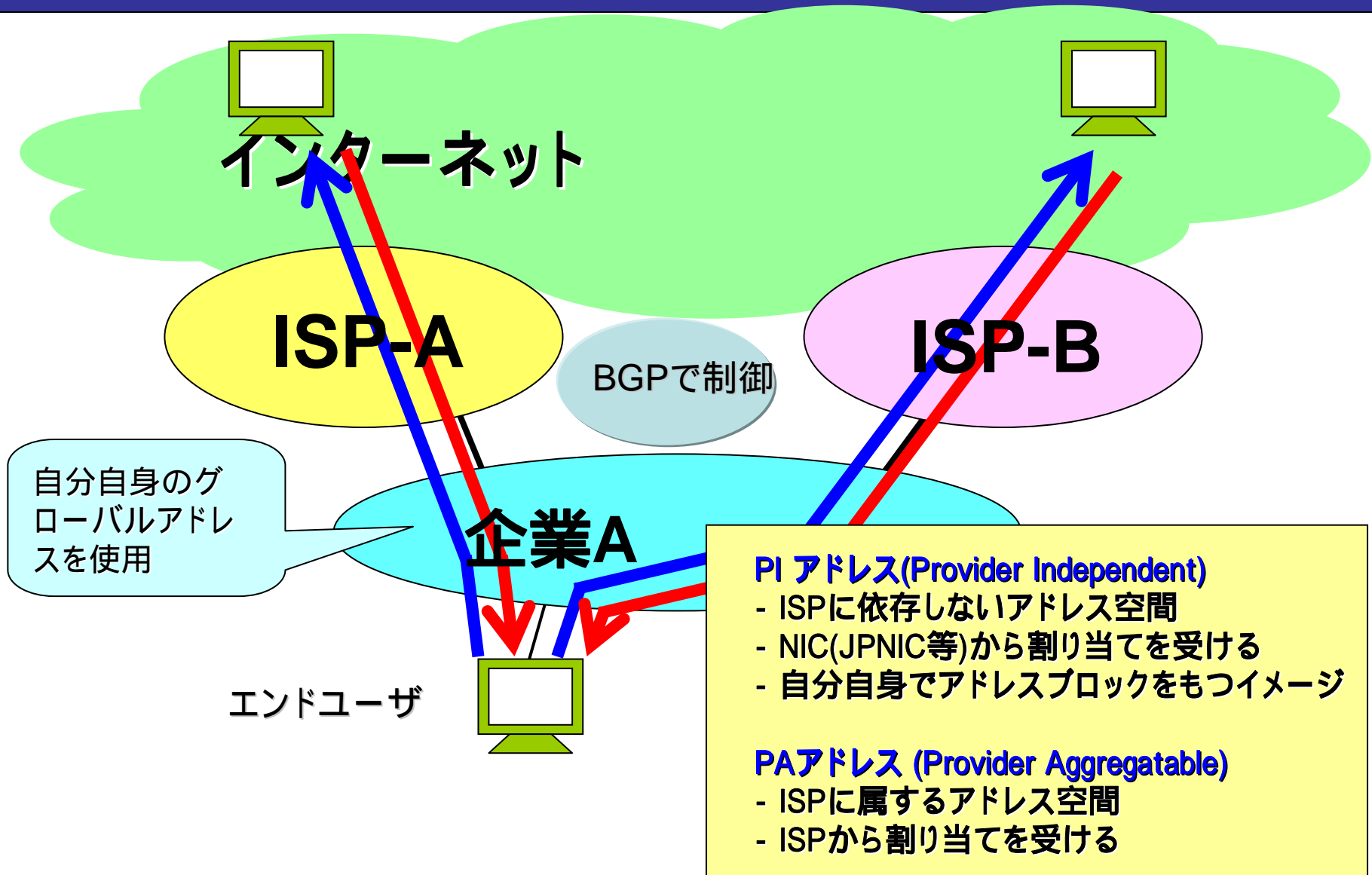


- これだけで1時間セッション
 - JANOG5「マルチホーム解剖学-実例とその分析」
 - JANOG6「NATによる準マルチホーム化技法」など

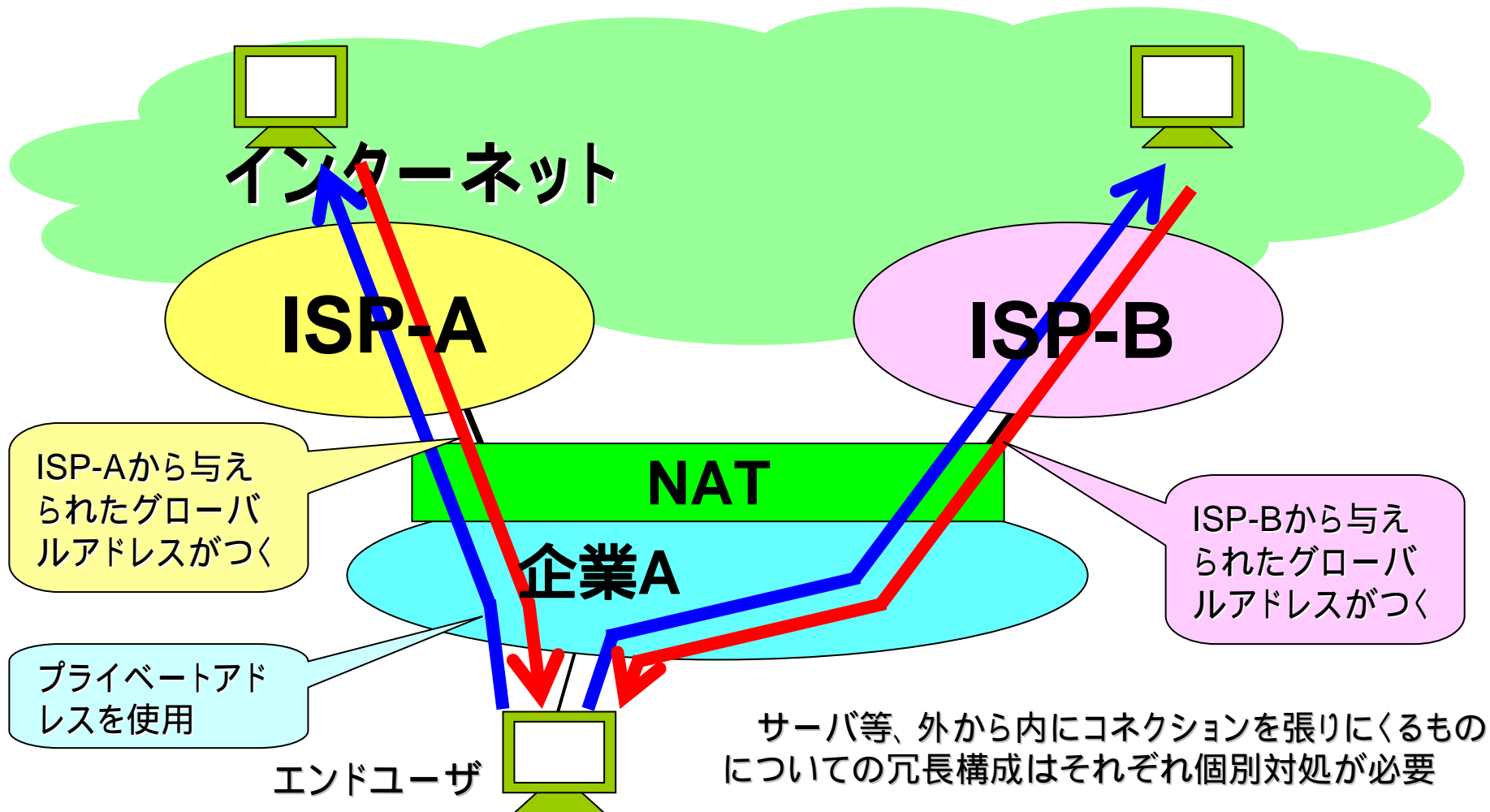
IPv4のマルチホームでよく見かける手法

- 1. BGPで制御
 - グローバルASとPIアドレスが必要
 - 細かなトラフィック制御が可能
 - ISPや大規模な企業に多い
 - 高いルータ(経路を持つメモリ、計算するCPU)
 - 大変な運用(AS運用、フルルート保持、バランス見直し)
- 2. NATで制御
 - フレッツと専用線等でも、簡易に冗長化できる
 - inbound等の細かなトラフィック制御はDNSと連携が必要
 - 中小規模の企業などに多い
 - マルチホームのための専用装置が有名(linkproof, isurf, etc)

BGPで制御



NATで制御



IPv6のマルチホームは？

- 1. グローバルASとPIアドレスを取得し、BGPで制御
 - IPv4と同様
 - AS番号はIPv4と同じでOK
- 2. プライベートアドレス相当とNATで制御
 - IPv6なのにNAT?? IPv6の設計思想の1つでNATなし？
 - 実はIETFで議論中
- 3. IPv6ならではの手法
 - マルチプレフィックス環境で、端末が制御
 - shim6

(参考) IPv6 PIアドレス

- IPv4同様、マルチホームのために必要
- 設立は実はわりと最近
 - IPv6策定当初は経路集約優先で認められていなかった
 - 2005年に日本からAPNICへ提案「マルチホームネットワークへのIPv6 PIアドレス新設について」
 - 日本からIMF外山さん等9名のボランティアメンバーからなるIPv6 PIワーキンググループにて検討した成果

IETF BEHAVE-WGと、NAT66

- BEHAVE WG(Behavior Engineering for Hindrance Avoidance)とは
 - IPv4 NATの挙動を定義するワーキンググループ
 - 標準仕様が定義されないまま普及したNATはさまざまな実装があり、NATトラバーサル処理が複雑化しEnd-to-End通信を阻害
 - NATの実装をBCP(Best Current Practices)として文書化
- NAT66の出自
 - IPv6でもNATを必要とするケースが存在
 - 企業NWでネットワーク間を接続する際のトポロジーの隠ぺい、など
 - 実装し利用する人々が出てきたらIPv4 NATのような標準仕様のない混沌とした状況へ
 - IPv6 NATの標準仕様を策定する必要

NAT66の中身

- 最新ドラフトより(2008.11頃から活発化)
 - <http://tools.ietf.org/html/draft-mrw-behave-nat66-02>
 - Prefix変換
 - ポート変換はしない
 - incomingもoutgoingの通信のいずれもいつでも許可 (透過)
 - セキュリティに対して懸念がある場合はNAT66にファイアウォール機能を具備してもよい

NAT66の中身 その2

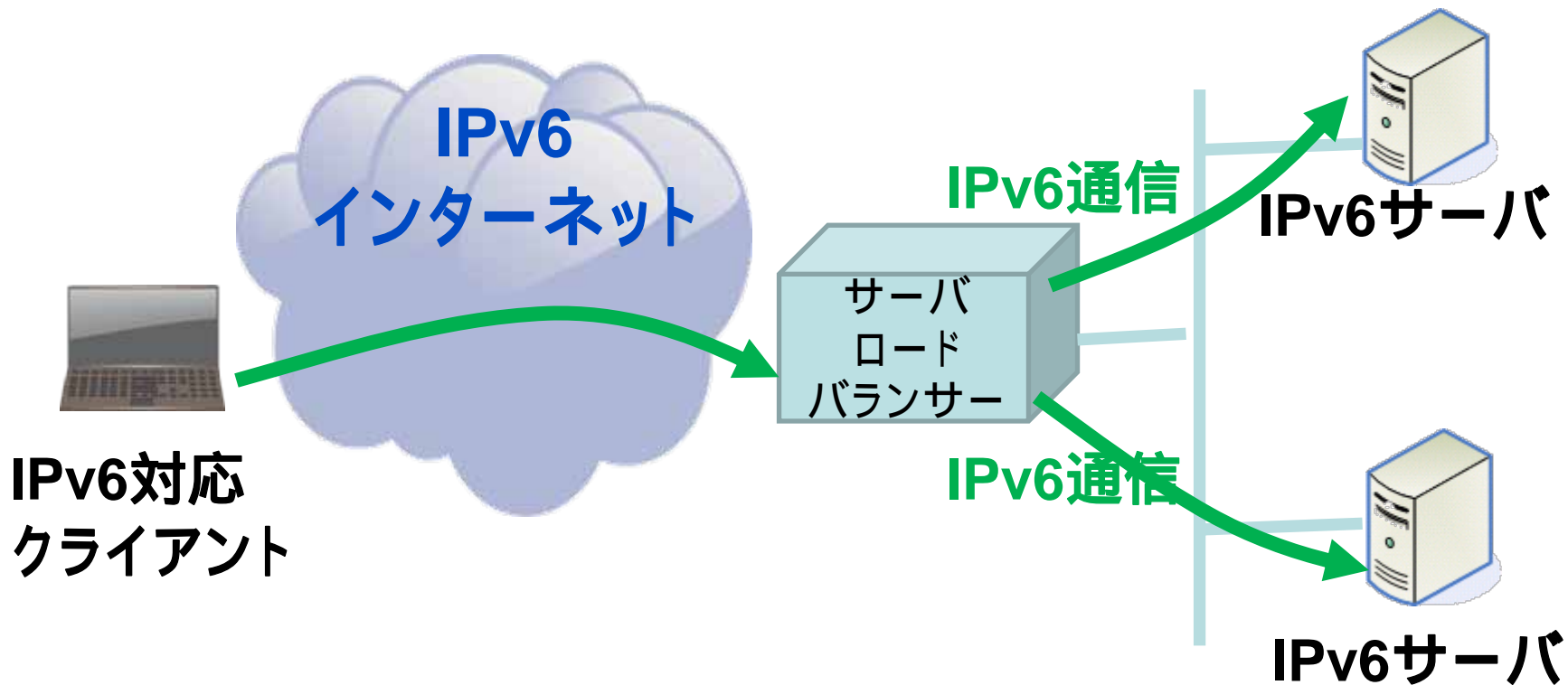
– Checksum-Neutral Mapping

- チェックサム再計算を不要に
- Internal /48 to external /48 mappingで浮いてる16bit分をうまくいじって、アドレス変換後のチェックサムが等しくなるように
- IPv4のNATはTCP/UDP/ICMP以外のトランスポートプロトコル、たとえばSCTP/DCCPが通らない
- IPv6はEnd-to-Endの透過性を保持、という試みの模様

NAT66のその後

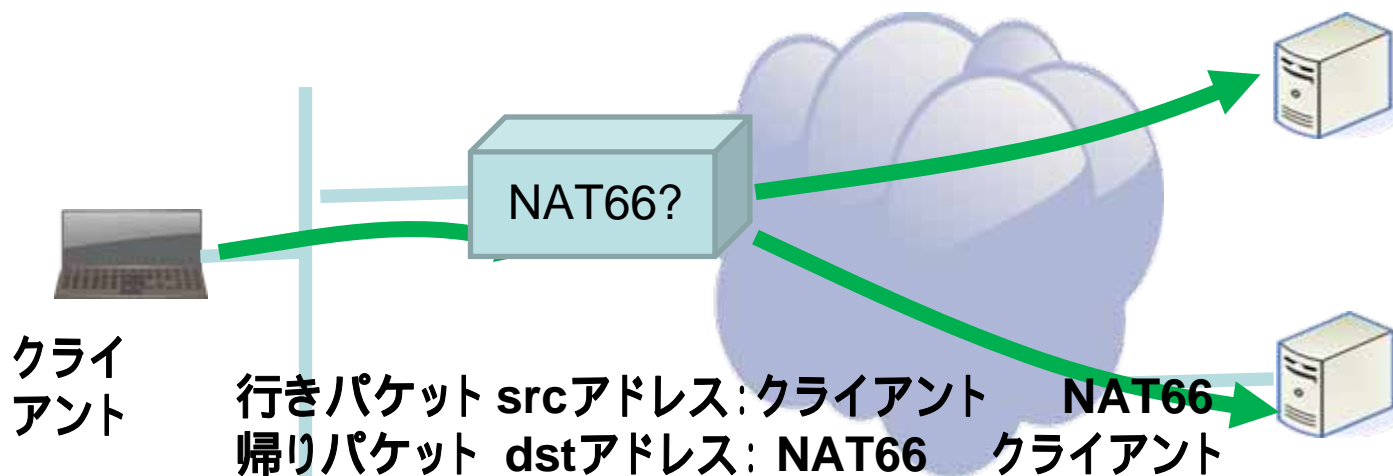
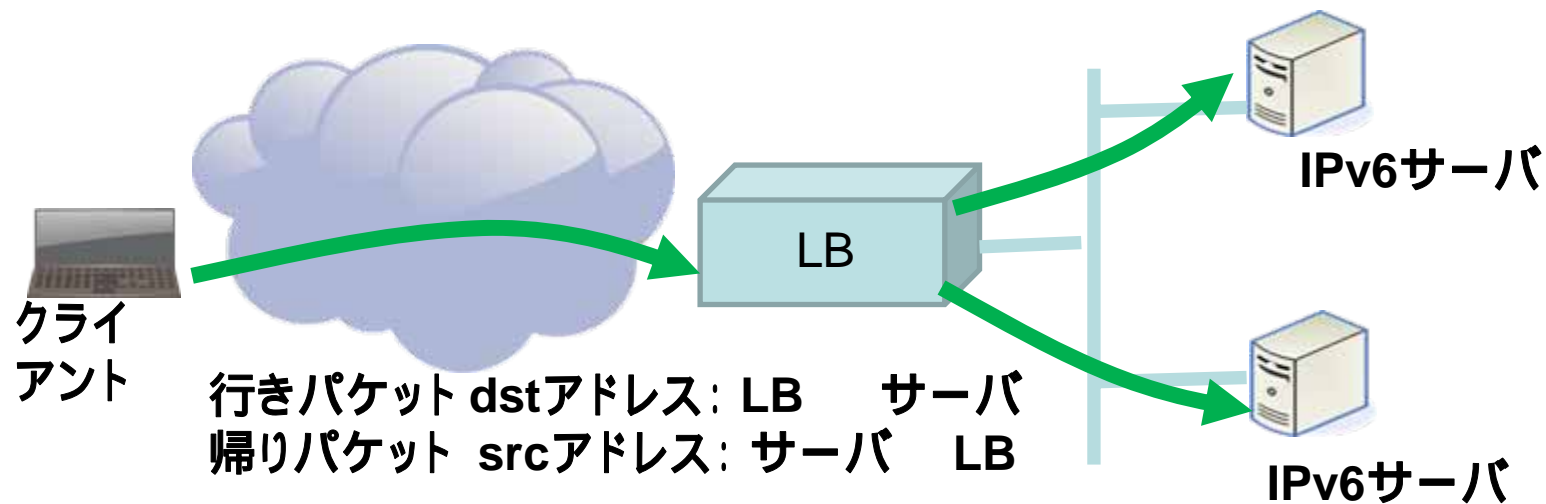
- 6AI BoF (IPv6 Address Independence BoF)
 - 3月に、BEHAVE WGから切り離されWG化 標準化を狙ったものだったが。。。
 - アドレスの独立性を提供するという側面を焦点
 - ISPから付与されるアドレスが変わってもサイト内のアドレスを付け替える必要がない
 - マルチホームが単純になる
 - これがNATを導入するデメリットを上回るか？

ロードバランサーでのv6変換はNAT66?



ロードバランサーもIPv6通信をNATしてる

ロードバランサーでの変換との違い



マルチホームまとめ

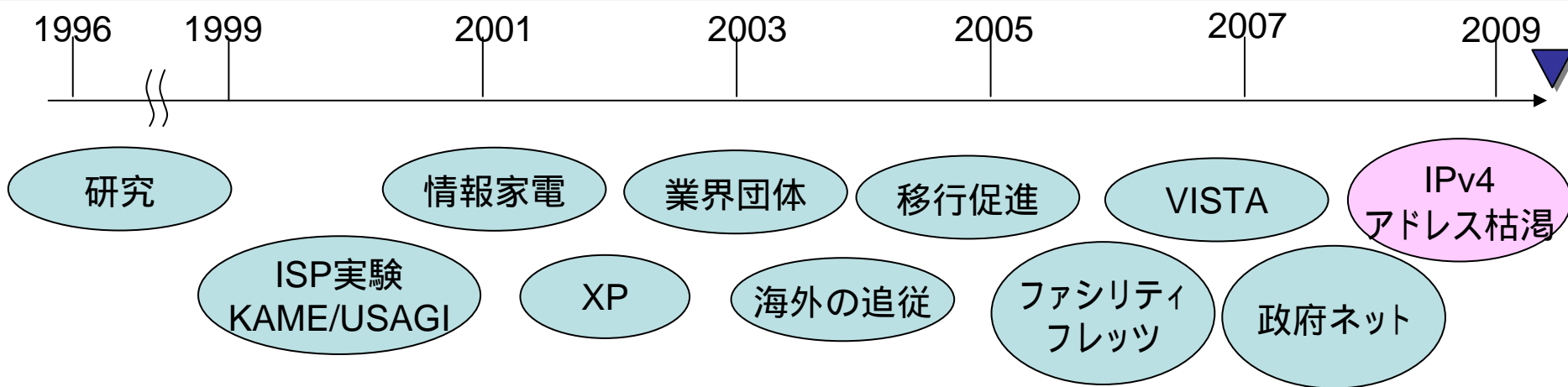
- いくつか手法はあるが、IPv6ならではの手法は不安で使えない。。。
 - 運用経験
 - 機器の実装
- IPv4でよくあるプライベートアドレス+NATで制御する方式は今後かな？
 - NAT66(ベース)を実装した機器
 - マルチホーミング専用装置

質疑応答

- 企業NWのIPv6導入のために
- 他にもこんな悩ましいポイントがあるよ
- こんな解決方法があるのでは？
- などなど大募集

ありがとうございました

(参考) NTT ComのIPv6への取り組み



- NTTコミュニケーションズの主な取り組み**
- ・IETFにてIPv6策定メンバー(1995)
 - ・IPv6実験NET運用 (1996)
 - ・sTLAアドレス取得(1999)
 - ・OCN実験開始(1999)
 - ・NTT MCL米国にてIX運用(2000)
 - ・NTTヨーロッパ実験 (2000)
 - ・IPv6商用サービス(2001)
 - ・情報家電プロジェクト(2001) (VPN, コントローラ, ホットスポット)
 - ・アジアでサービス(2002)
 - ・World Com Award受賞(2002)
 - ・バックボーンIPv4/IPv6デュアル化(2003)
 - ・IPv6移行実験(2006)
 - ・アジアブロードバンド(2006)
 - ・RFID実験
 - ・緊急地震速報(2007)
 - ・マルチポリシーVPN(2007)
 - ・IP-VPNデュアル(2009)
 - ・ネット家電接続、m2m-x実験(2004)
 - ・World Com Award 受賞(2004)
 - ・個人向けIPv6サービス(2005)
 - ・IPv6対応ホスティング:VPS(2005)
 - ・IPv6サービスにSLA適用(2005)
 - ・モバイルIPv6実験(2005)