ユビキタス社会に必要となるネットワーク技術

－NAT越えと移動透過性－

平成20年10月24日

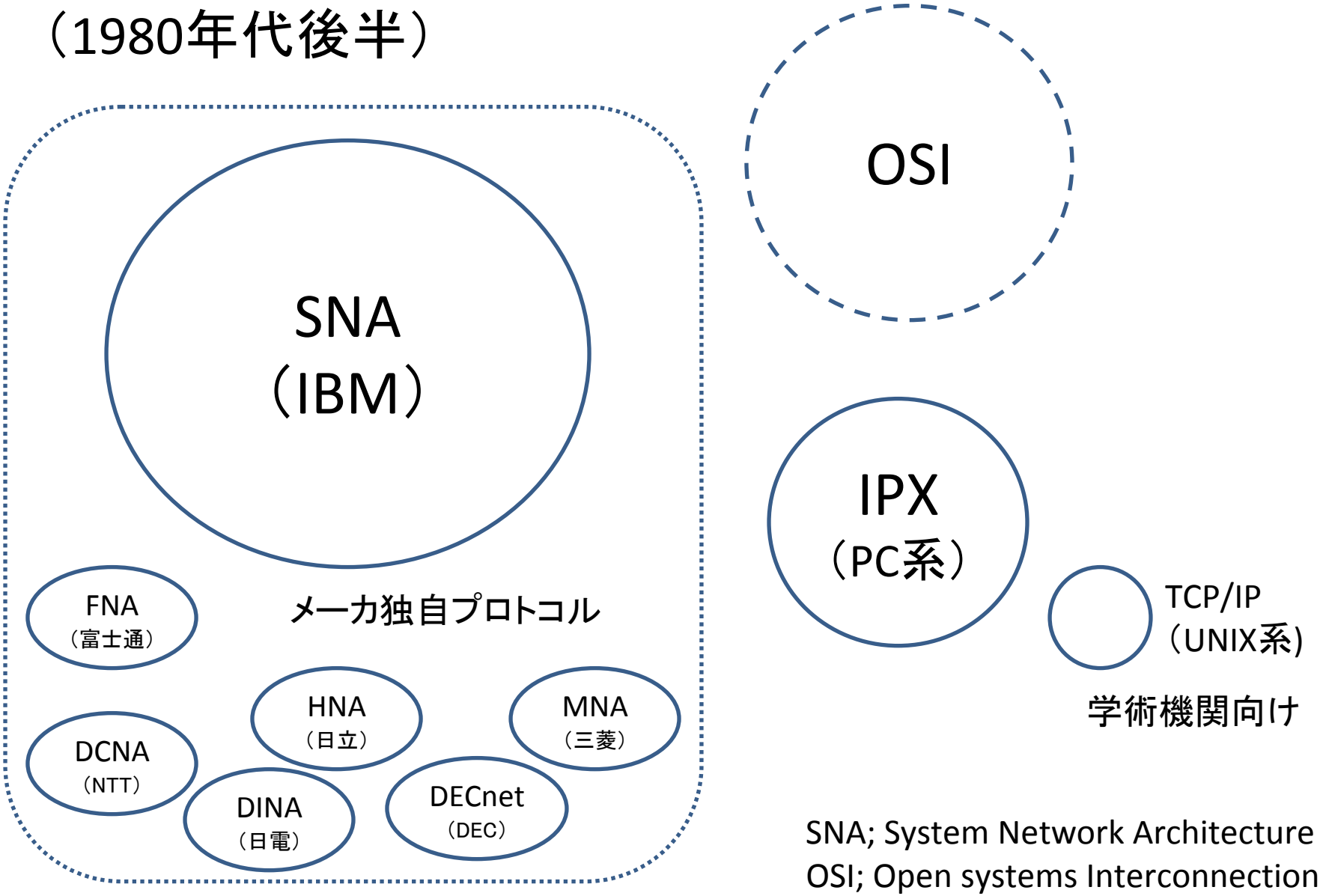
名城大学　理工学部情報工学科
渡邊　晃

目次

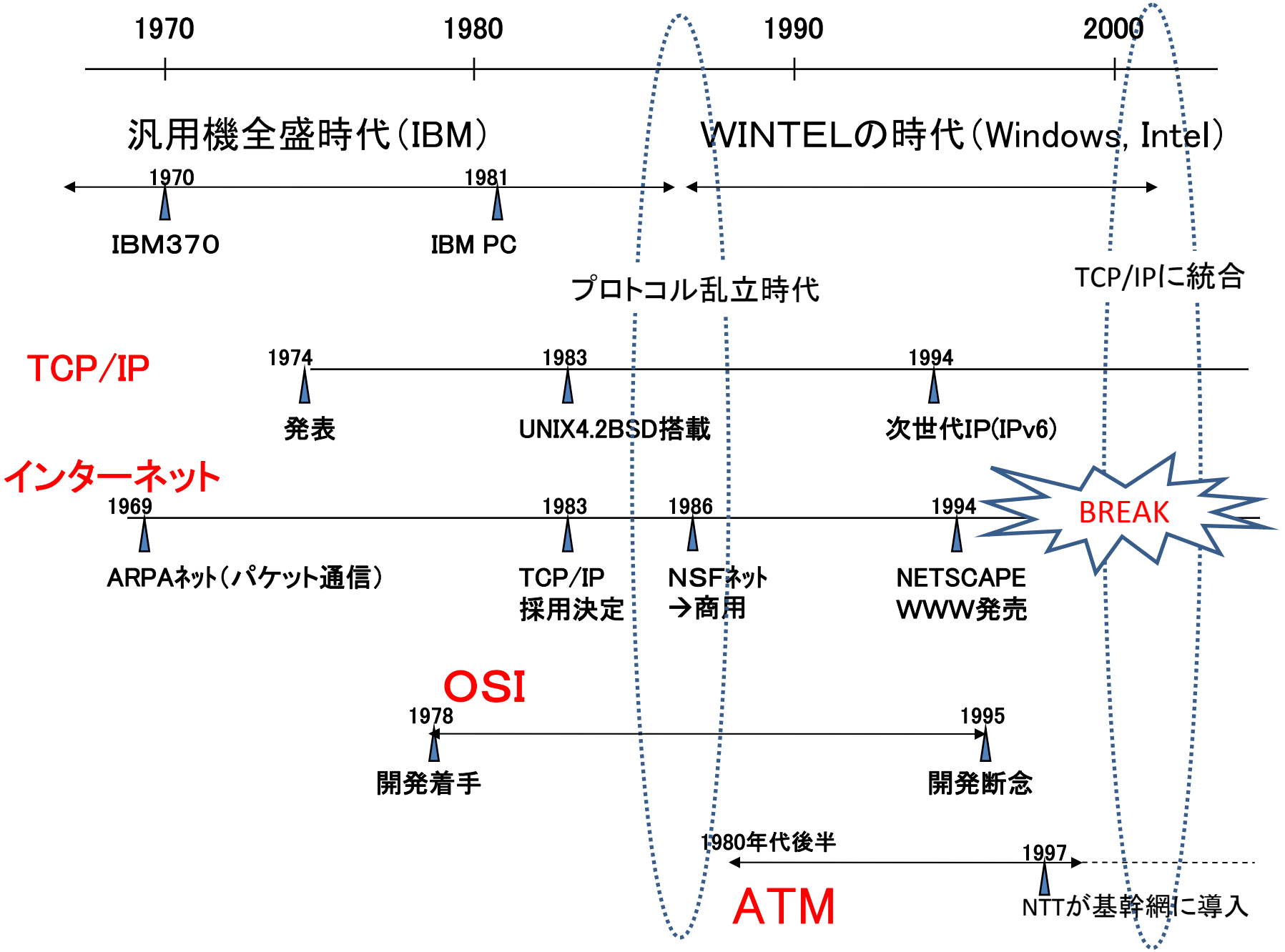
- TCP/IPが市場を制覇するまで
- TCP/IPが直面する課題
- 提案内容
  ーNAT越えと移動透過性

TCP/IPが市場を制覇するまで

プロトコル乱立時代のイメージ（1980年代後半）



SNA; System Network Architecture
OSI; Open systems Interconnection

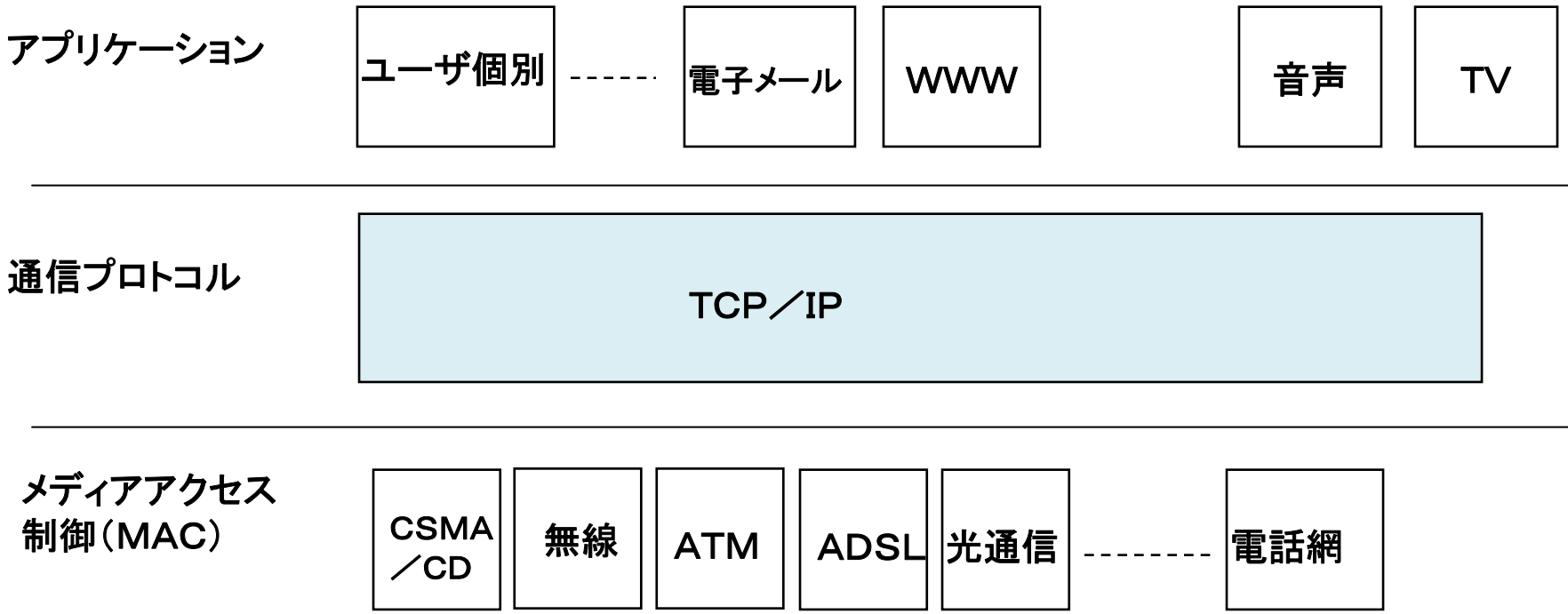


OSIは欧日のコンピュータ・ネットワークの発展を阻害したと言われている

TCP／IPが通信プロトコルを制覇したことによる効用

Everything over IP.

IP over everything.



・アプリケーションと伝送媒体が切り離された。

→独立した発展が可能となった。

なぜOSIは失敗したのか

・あらゆる仕様を盛り込み膨大な仕様
・トップダウンで机上の理論に注力、実践軽視
・政治主義的な標準化活動（各国の利権）
・仕様書を共有。ソースコードは企業秘密
・電話回線中心の発想（課金、リアルタイム性）

－＞ 開発期間の増大
解釈の違いで相互接続困難
メモリ食う
性能が出ない

なぜTCP／IPが生き残ったのか

・シンプルな仕様（データ通信に特化，リアルタイム性は考慮せず）
・実践重視(*)
・迅速な標準化活動（メーリングリストの活用）
・センスのあるリーダの存在(**)
・ソースを公開（UNIX）

－＞ 短期開発
　　相互接続容易
　　そこそこの性能

(*)IETFにおける標準化の条件：2つ以上の独立した組織が実装を完了していること
(**)ビント・サーフ，ロバート・カーン

シンプルであるため，技術進歩に伴いリアルタイム性が出てきた
　　→IP電話の実現，電話網のオールIP化

なぜインターネットは急速に普及したのか

・圧倒的な安さ　→　理由は次スライド
・キラーアプリケーションの出現　　WWW（1994年）
・検索エンジンの技術　→　リアルタイムでの情報収集
・ホームページによる情報発信
・豊富なアプリケーション（メール、WWW、地図、ショッピング、ニュース、電話）
・TCP/IPがインターネットの普及に耐えられるものであったこと

インターネットはなぜ安いのか？　⇔　電話網と比べて

① パケット交換　⇔　回線交換

伝送路を有効に使用できる。技術の進歩とともに効率が向上する。

② ベストエフォート型　⇔　ギャランティ型

できるだけの努力はするが、帯域を保証することはしない。

③ 部分的な二重化　⇔　完全二重化

故障に対して、できるだけのことをするが完全な保証はしない。

④ エンドエンドの原則　⇔　ネットワークが頑張る

複雑な処理はすべて端末で行う。ネットワークは何もしない。

⑤ 加入者線の流用　⇔　加入者線の整備

電話網ですでに整備されていた加入者線を使うことができた。

電話屋；電話こそ社会のインフラ、高品質維持
インターネット屋；電話は数あるアプリケーションの一つ
NATがきらい

TCP/IPが直面する課題

インターネットの課題は何か
（TCP/IP）

①IPv4グローバルアドレスの枯渇
②移動透過性（通信しながらの移動）
③セキュリティ（認証と暗号化）

課題①IPv4グローバルアドレスの枯渇

IPv4アドレス長・・・32ビット　　全て使い切ったとして40億個

階層構造のため無駄が避けられない

短期解決策；

1．アドレスの配布を細分化

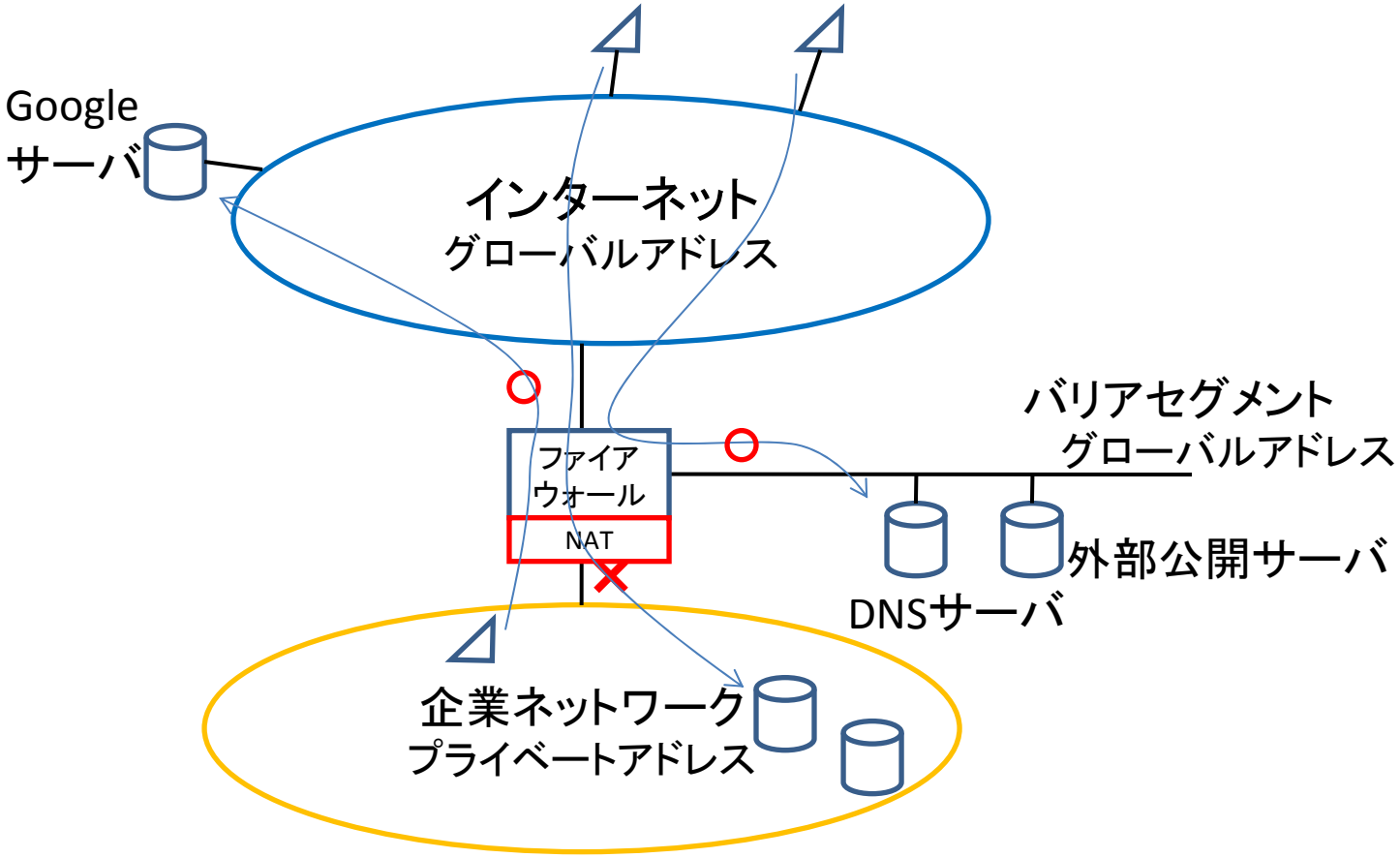
2．組織内で自由に使えるアドレス範囲を定義

ーー＞プライベートアドレス

長期解決策；

IPv6　→IPアドレス長128ビット

プライベートアドレスの利用方法



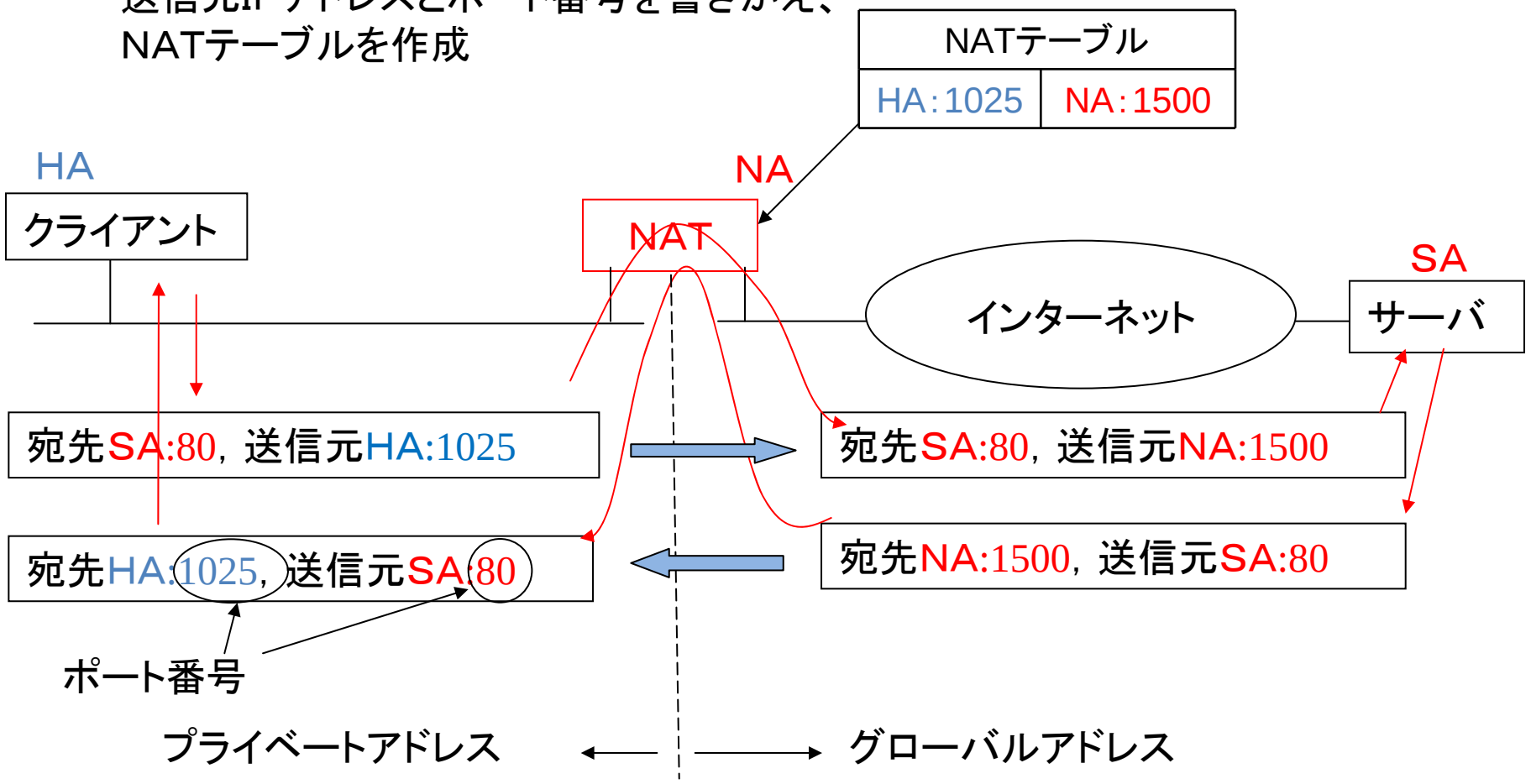
NATはファイアウォールの影に隠れていた

NAT; Network Address Translation

NATのしくみとNAT越え問題

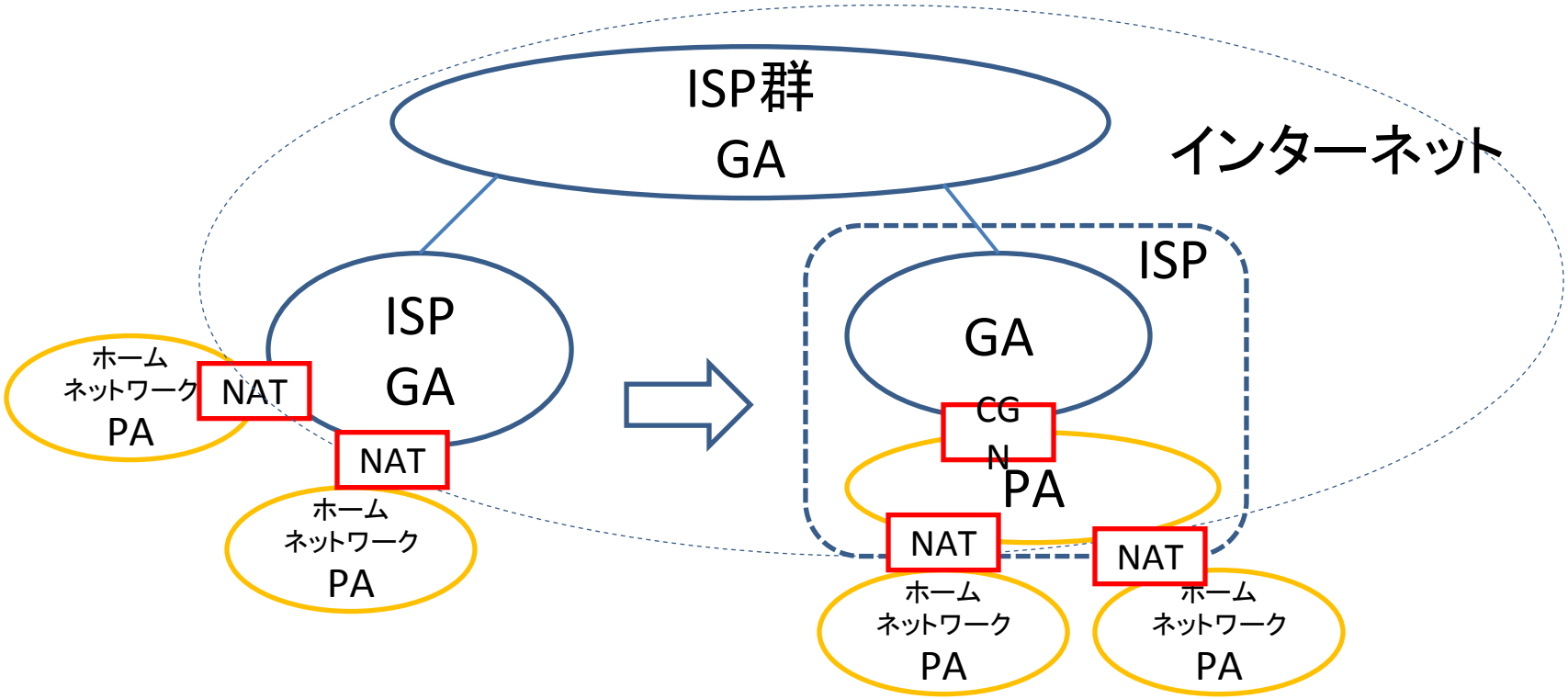
ポート番号：上位ｱﾌﾟﾘｹｰｼｮﾝを識別する番号

送信元IPアドレスとポート番号を書きかえ、
NATテーブルを作成



インターネット側（グローバルアドレス側）からの通信開始ができない

NAT越え問題はホームネットワークで表面化する可能性がある
サービス低下の恐れ（PA内にサーバを設置できない）



PA; Private Address
GA; Global Address

- CGN; Carrier Grade NATによるIPv4の延命
- いずれはIPv6に移行
- IPv6推進論者は、IPv6ではNATが不要であることを主張

NATの思わぬ効用

無視できない情報システム部の使命感

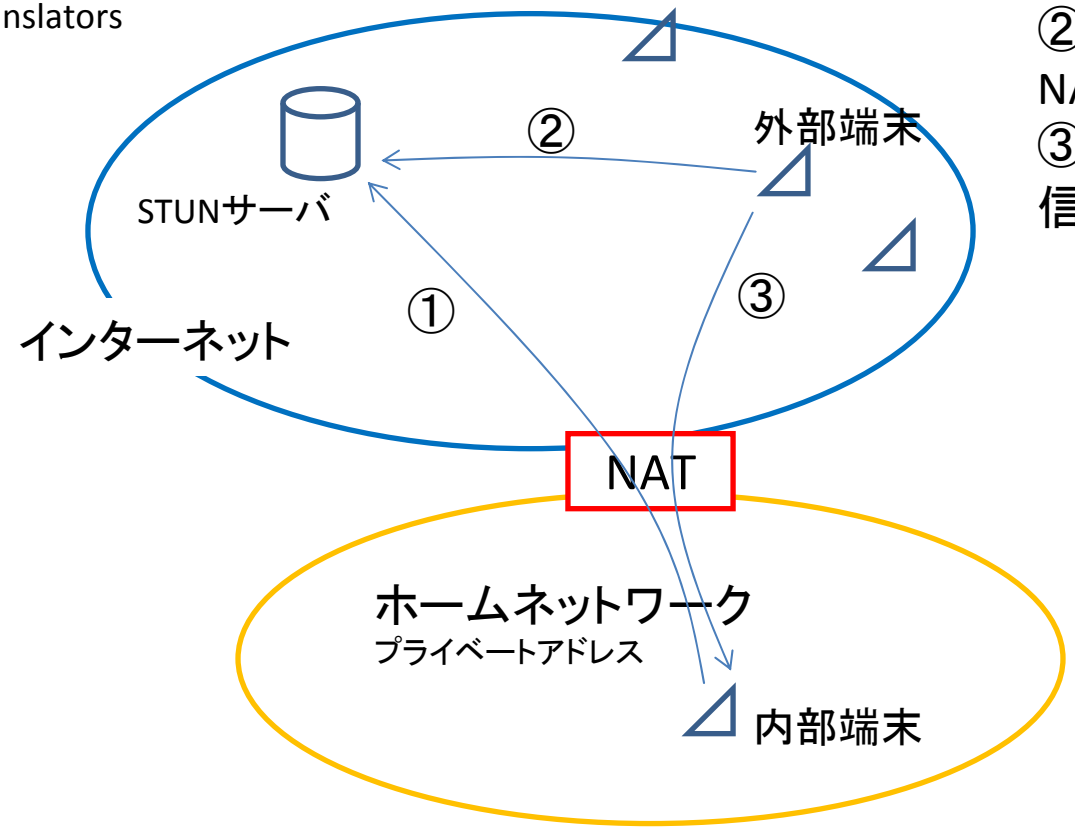
・組織内のアドレスが見えなくなる
→ ネットワーク管理者の安心感

IPv6の普及に係る予想：
・家庭ネットワークにはIPv4グローバルアドレスが提供できなくなる（2014年頃から）
・新規ユーザはIPv6
・多くの企業はIPv4のまま残る。NATが使えるから
・大手ISPはIPv6へ移行する
・中小ISPはIPv4のまま取り残される可能性あり。CGNによるIPv4の延命。NAT越え技術との併用
・IPv6への移行は徐々に進むものの、IPv4は永久に使われ続ける

NAT越えの既存技術とその課題

STUN

Simple Traversal of User Datagram Protocol [UDP] through Network Address Translators



①内部端末からSTUNサーバにアクセスしてNATテーブルを生成する
②外部装置がSTUNサーバにNATの情報を問い合わせる
③NATテーブルに合わせて送信する

課題:
- Cone型NATにしか使えない。世の中の7割がCone型NAT
- 特殊なサーバが必要
- 内部端末と外部端末のアプリケーションがSTUN機能をサポートする必要がある

課題②移動透過性

インターネットでは通信中に移動できない

携帯電話

・電話番号は携帯電話を識別する情報である

→　移動しても電話番号は変わらない　→　移動しても通信を継続できる

インターネット

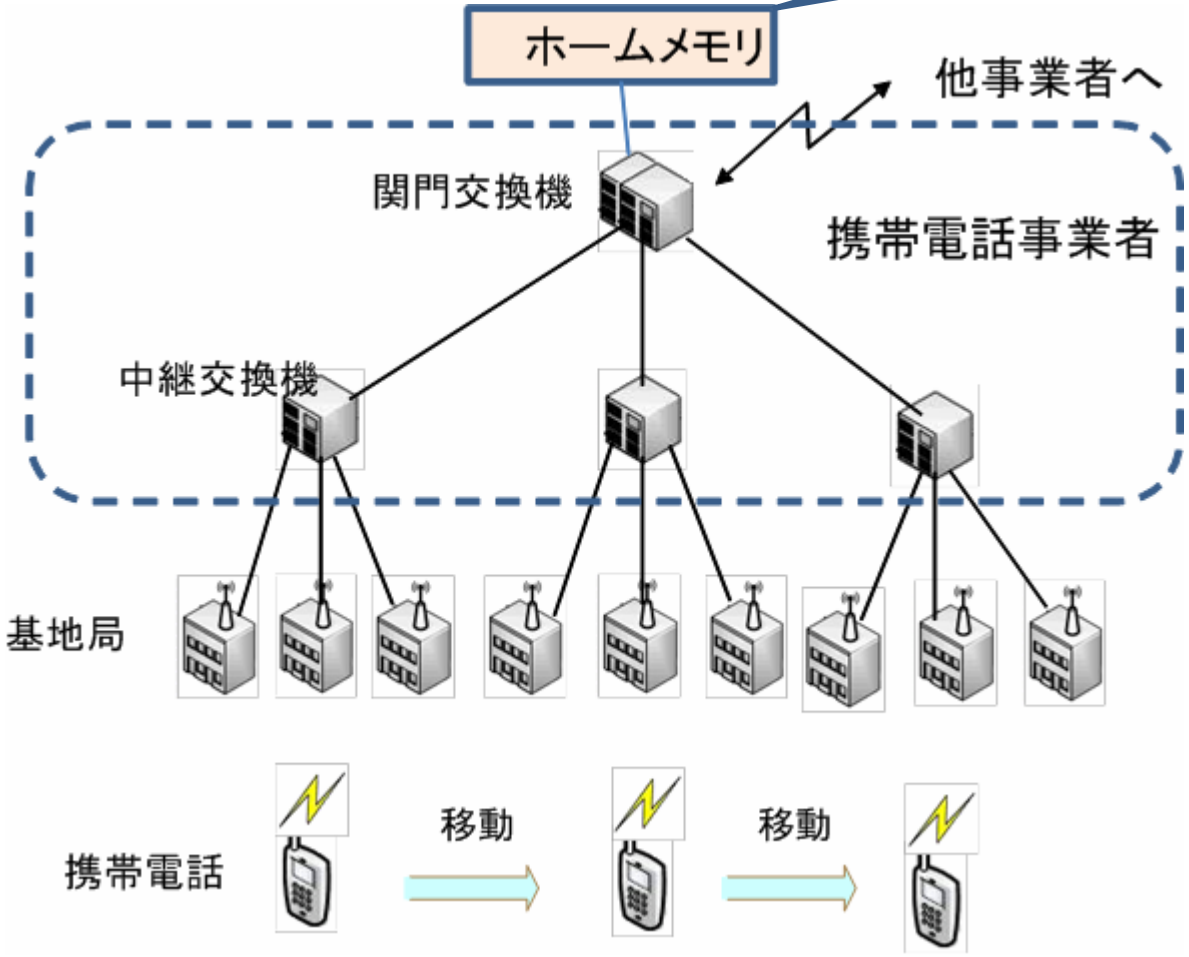
・IPアドレスは端末を識別するとともに場所に依存した情報である

→　移動するとIPアドレスが変わる　→　移動すると通信を継続できない

現在のIP電話は移動できないため、携帯電話の代替にはならない

携帯電話のしくみ

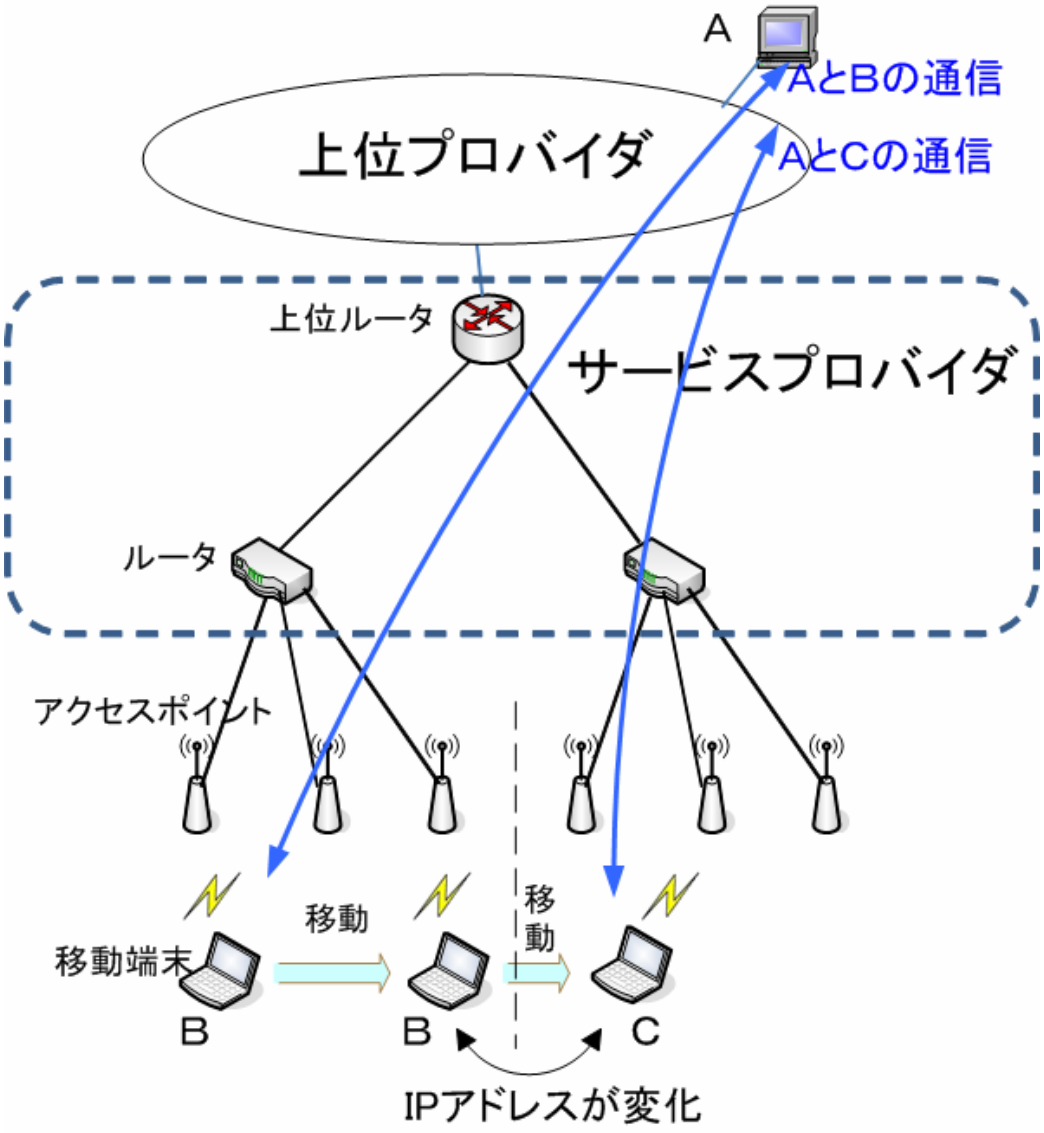
携帯電話の場所を記憶するメモリ



電話番号は変わらない

・ネットワークの頑張り
・事業者ごとに異なる方式

インターネットのしくみ



IPアドレス/ポート番号は通信の識別子

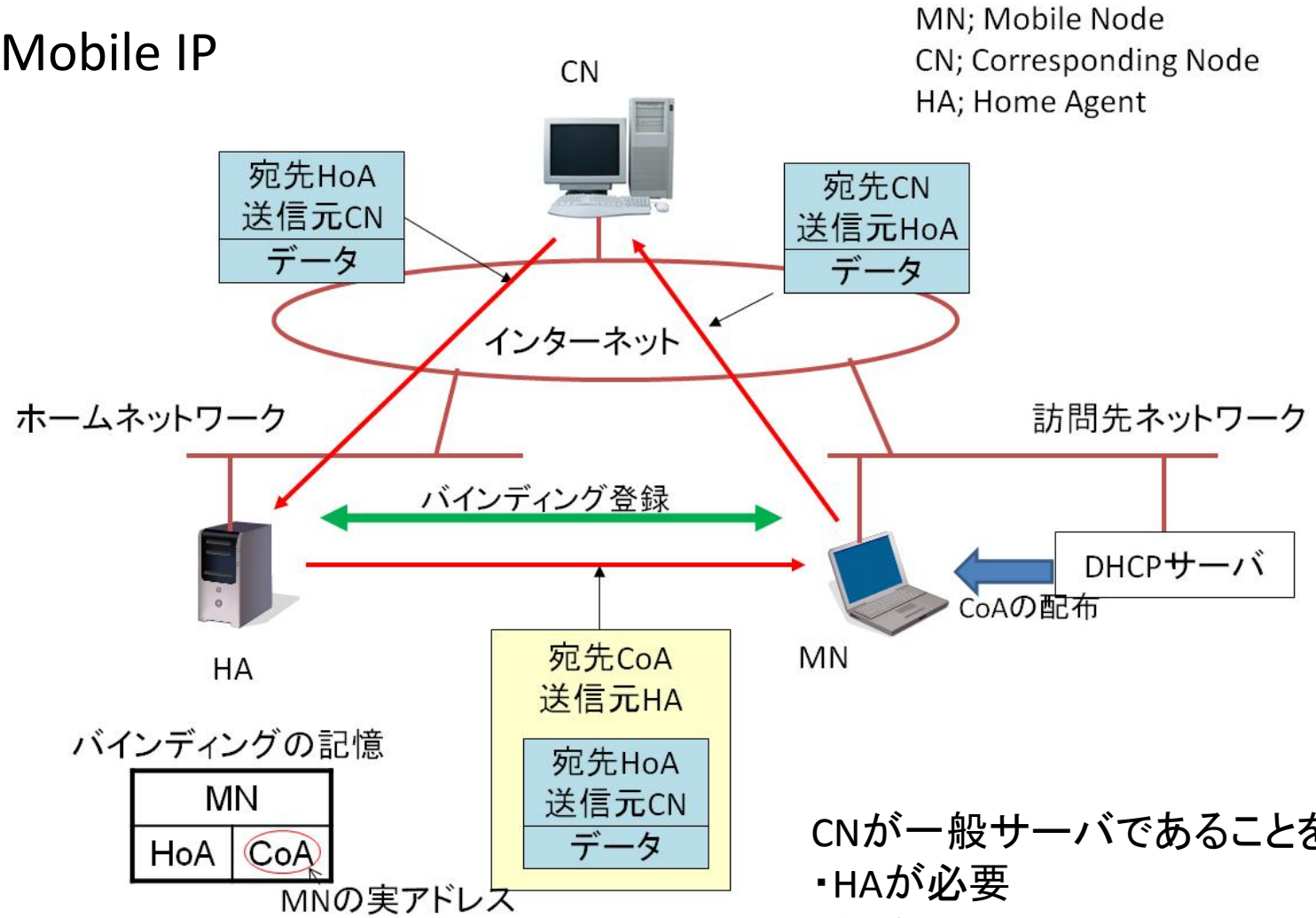
↓

アドレスが異なると違う通信とみなされる

・ネットワークは何もしてくれない
・プロバイダによる違いはない

移動透過性の既存技術とその課題（IPv4）

Mobile IP



CNが一般サーバであることを想定した技術

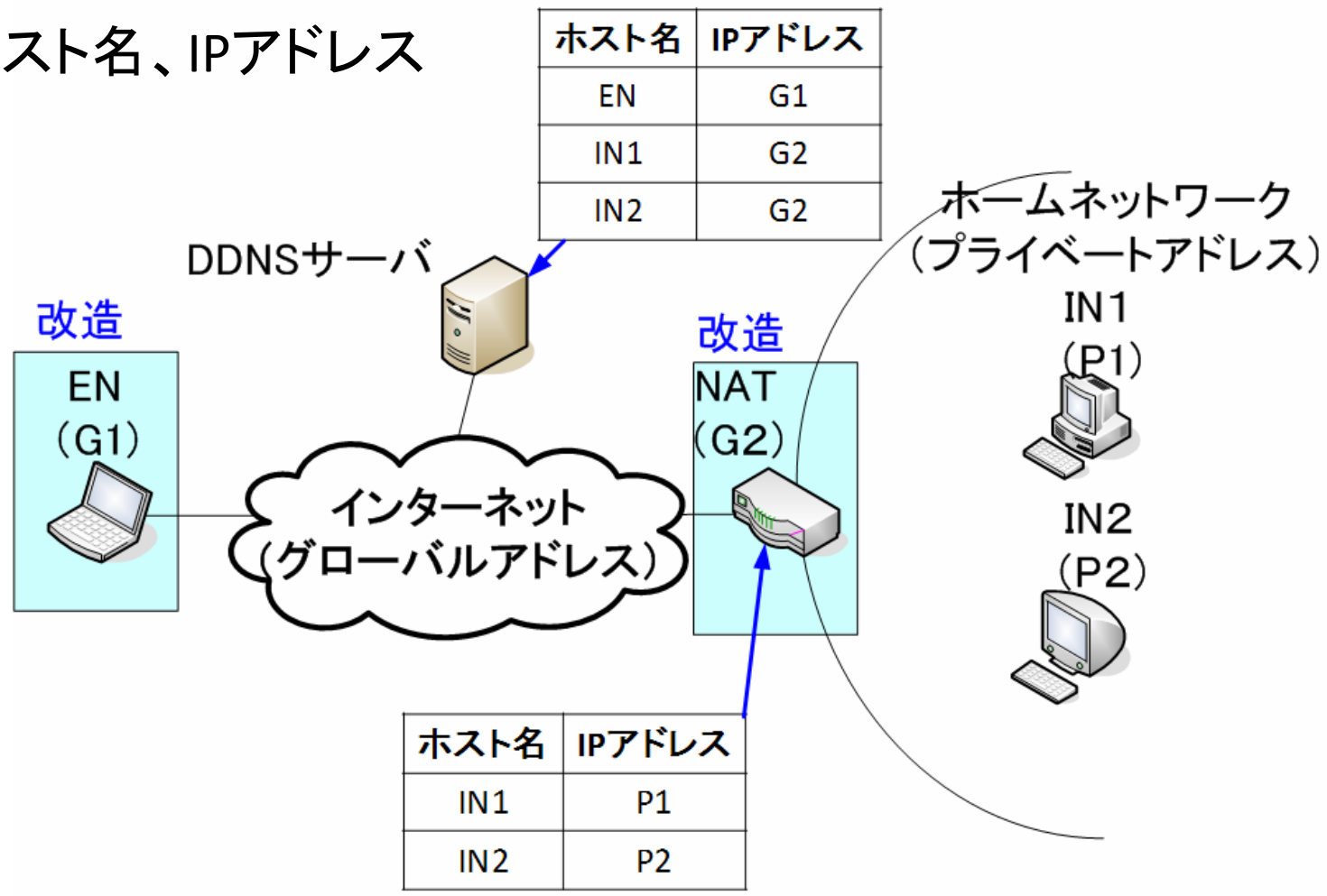
- HAが必要
- 経路の冗長
- トンネル転送によるオーバヘッド
- 不正パケットとして廃棄される可能性
- CNが動く場合は別のHAが必要

提案内容

NAT越えと移動透過性

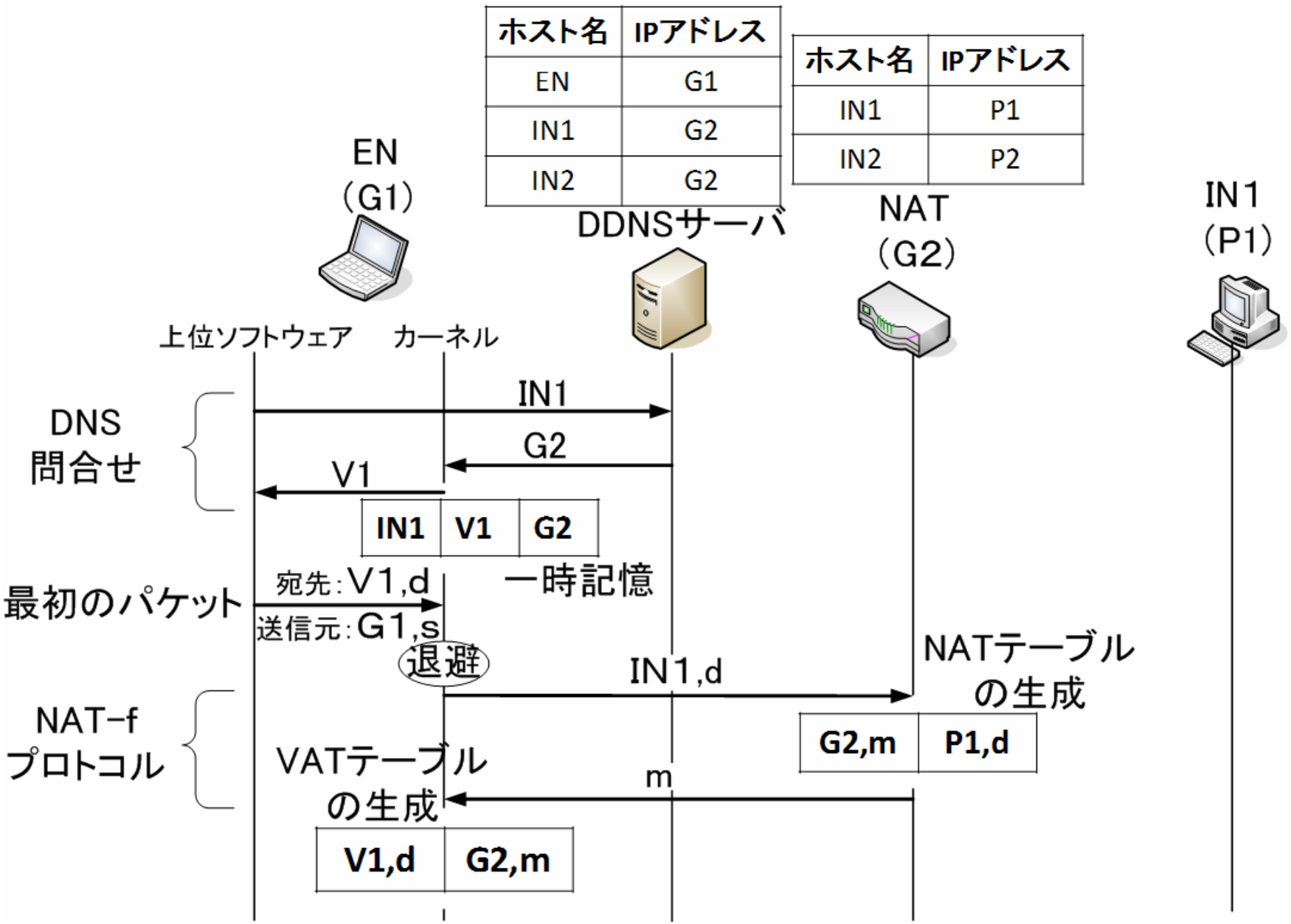
NAT越えを実現するNAT-f
(NAT-free protocol)

登場人物、ホスト名、IPアドレス
前提条件

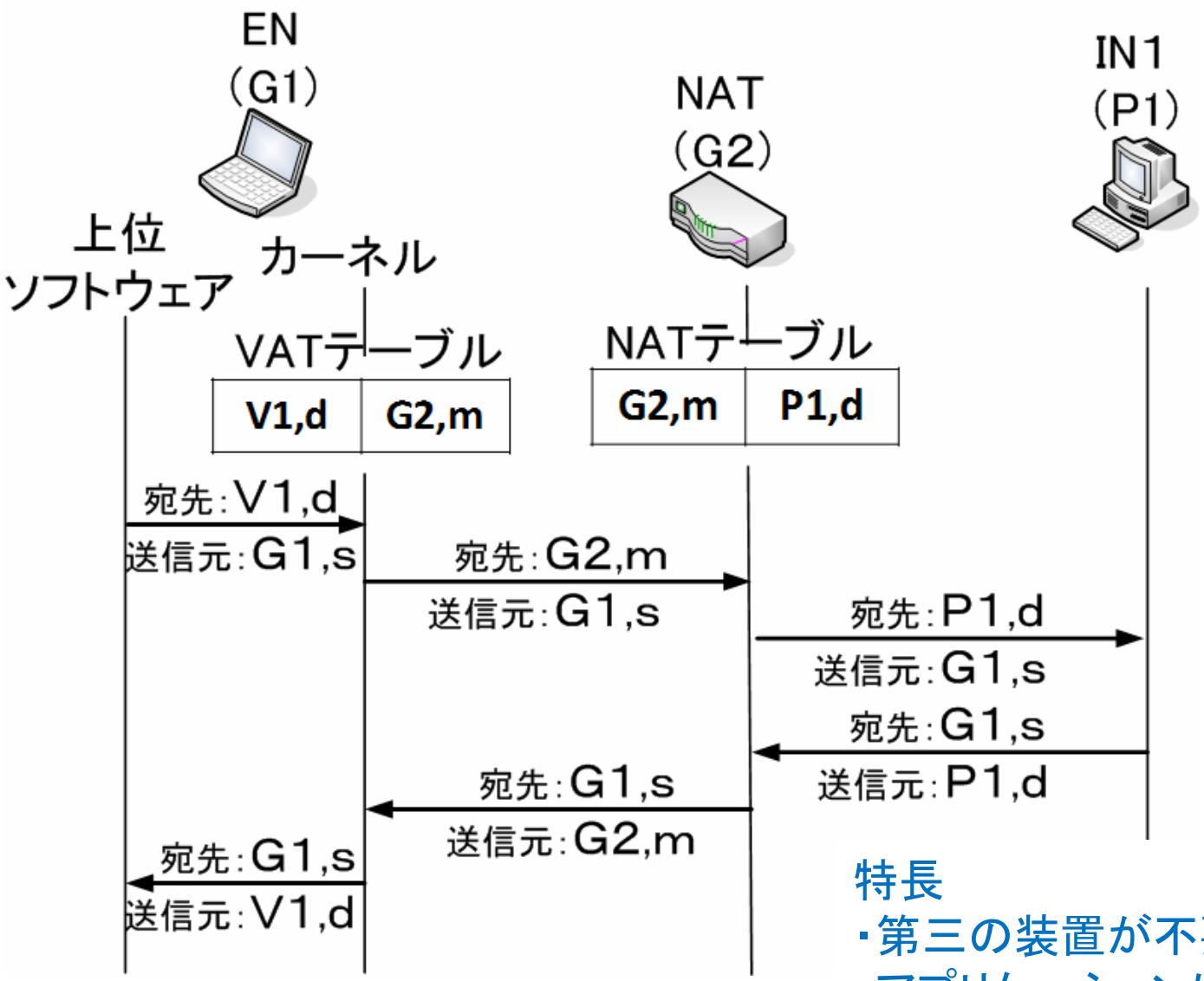


鈴木，宇佐見，渡邊，“外部動的マッピングによりNAT越え通信を実現するNAT-f の提案と実装”情報処理学会論文誌，Vol.48，No.12，pp.3949-3961，Dec.2007.

通信前のネゴシェーション



通信時のアドレス変換の様子

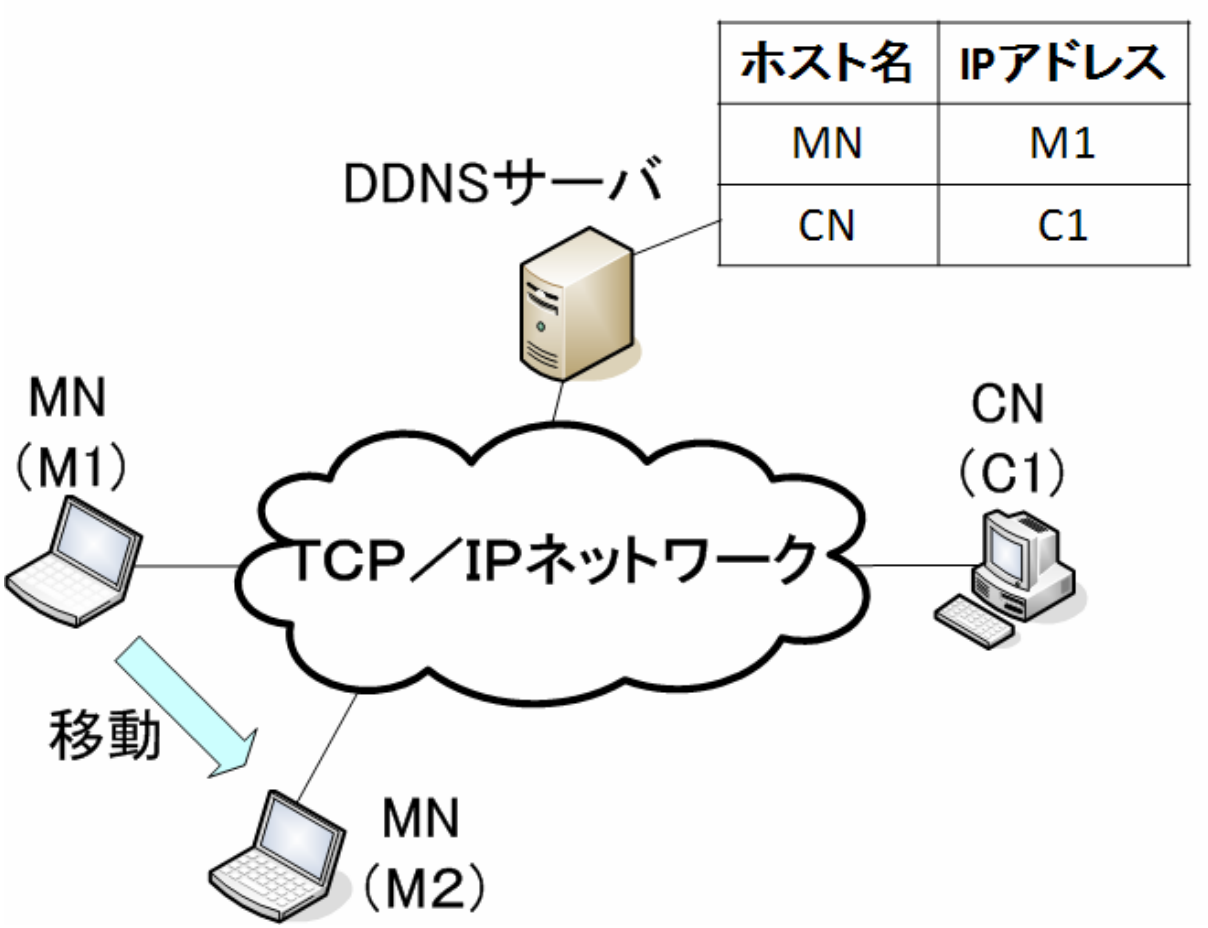


特長

- 第三の装置が不要
- アプリケーションに影響がない
- 高スループット
- NATの効用を損なわない

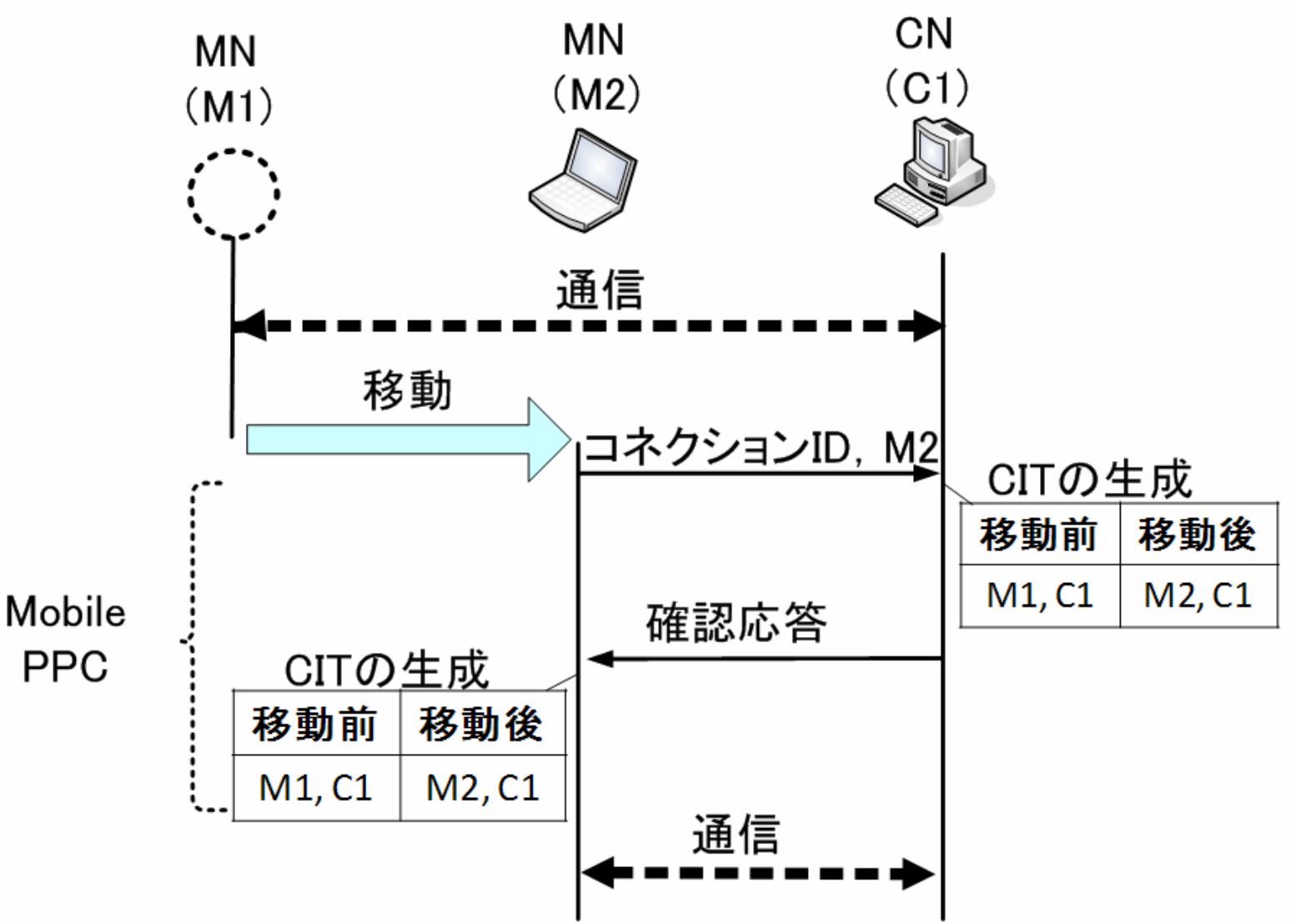
移動透過性を実現するMobilePPC
(Mobile Peer to Peer Communication)

登場人物、ホスト名、IPアドレス
前提条件

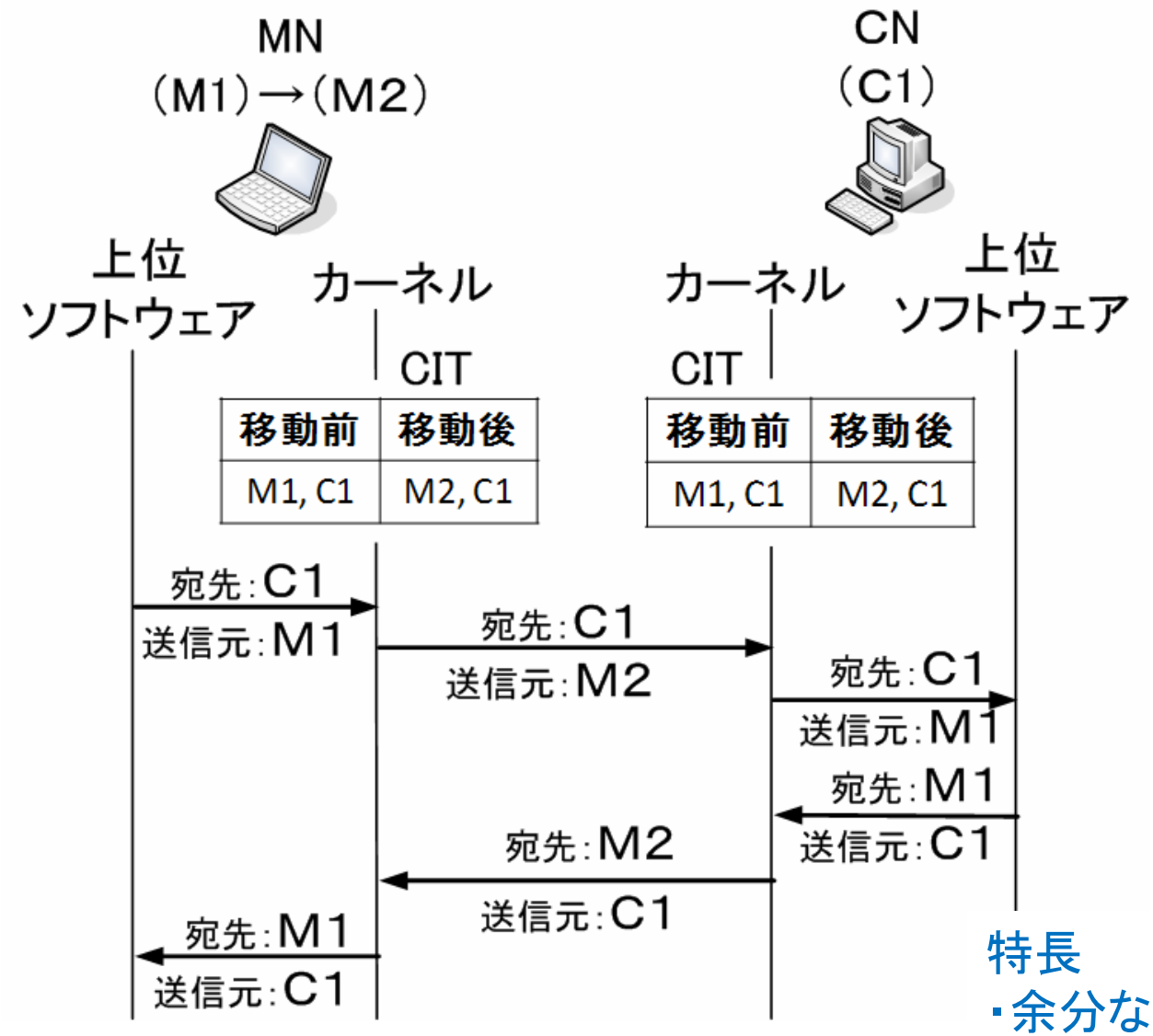


竹内，鈴木，渡邊，“エンドエンドで移動透過性を実現するMobile PPCの提案と実装”
情報処理学会論文誌，Vol.47，No.12，pp.3244-3257，Dec.2006.

移動時のネゴシェーション



通信時のアドレス変換の様子

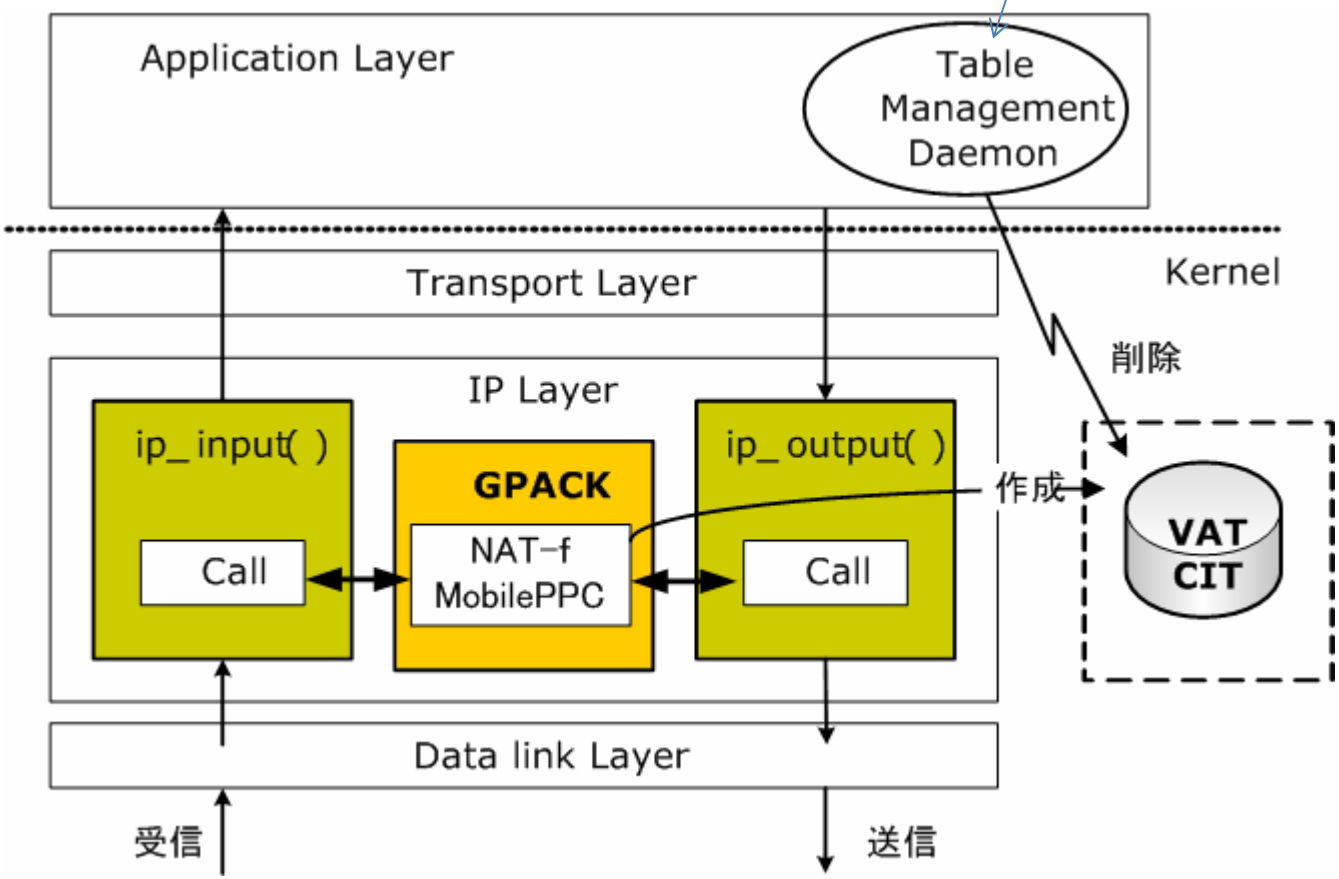


特長

- 余分な装置がない
- アプリケーションに影響がない
- 高スループット
- 既存端末と上位互換

実装方法

使用していないテーブルを削除するデーモン



・GPACKでIPアドレス/ポート番号変換

・変換テーブルがない場合はパケットをカーネル内に退避してGPACK間でネゴシェーション

イノベーションジャパン2008（大学見本市）へ出展

展示会の様子

デモの様子

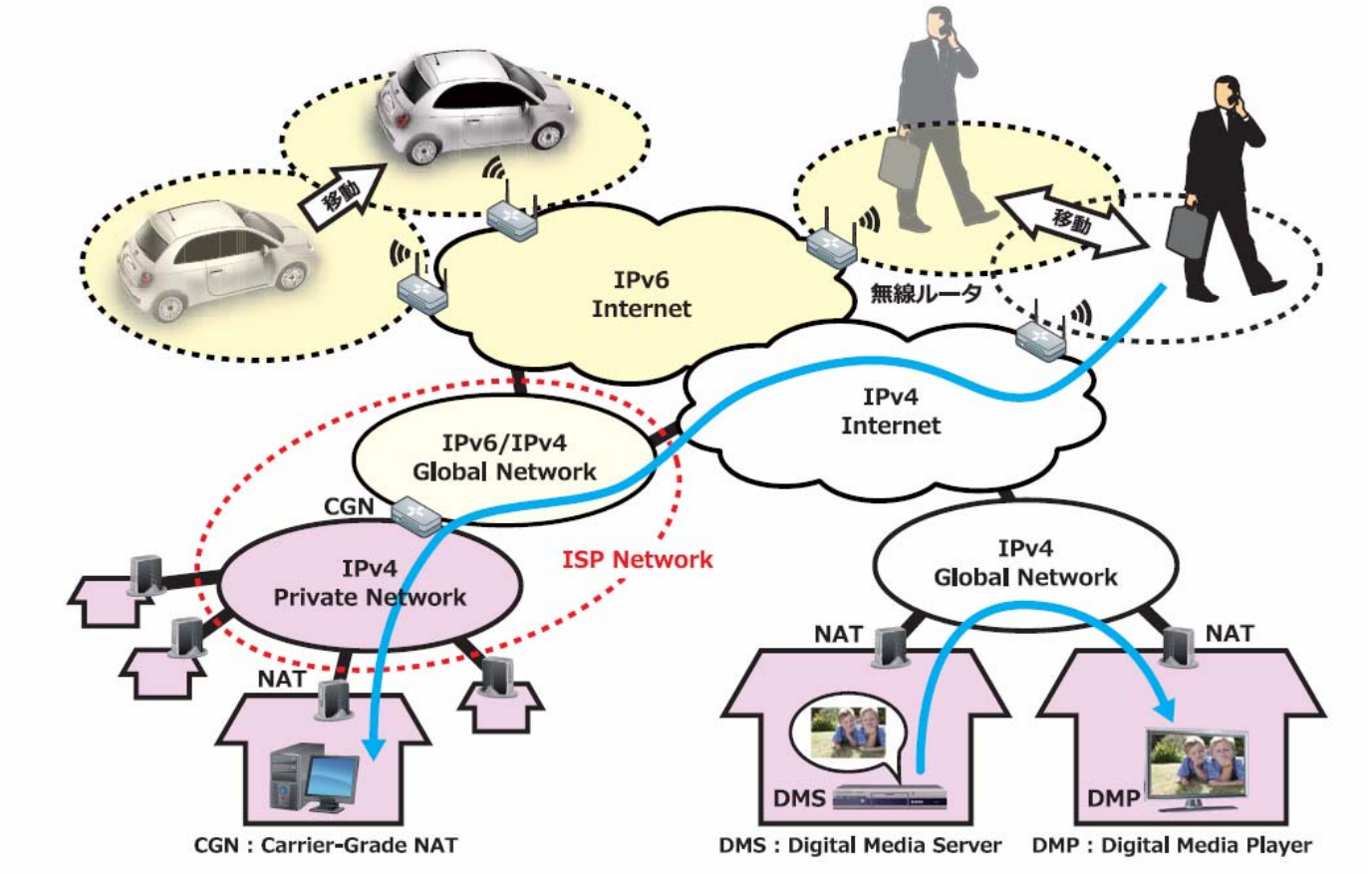
今後のネットワークのあるべき姿

アドレス空間の違い（IPv4グローバルアドレス/プライベートアドレス/IPv6アドレス）を意識することなく、

・自由に通信を開始できる

・通信中にどのような空間に移動してもよい

・ネットワークが移動してもよい



最後に

シンプル・イズ・ザ・ベスト

- 複雑なものは普及しない

TCP/IPには、いろいろな機能を追加できる

- エンドエンドの原則の効用
- NATは例外として認めるのが妥当

終わり

V6推進派の意見

・アドレスが絶対的に足りない。他に手段がない
・NATがいらなくなる（インターネット本来の姿）
・管理が容易になる（PnP機能）

V6否定派の意見

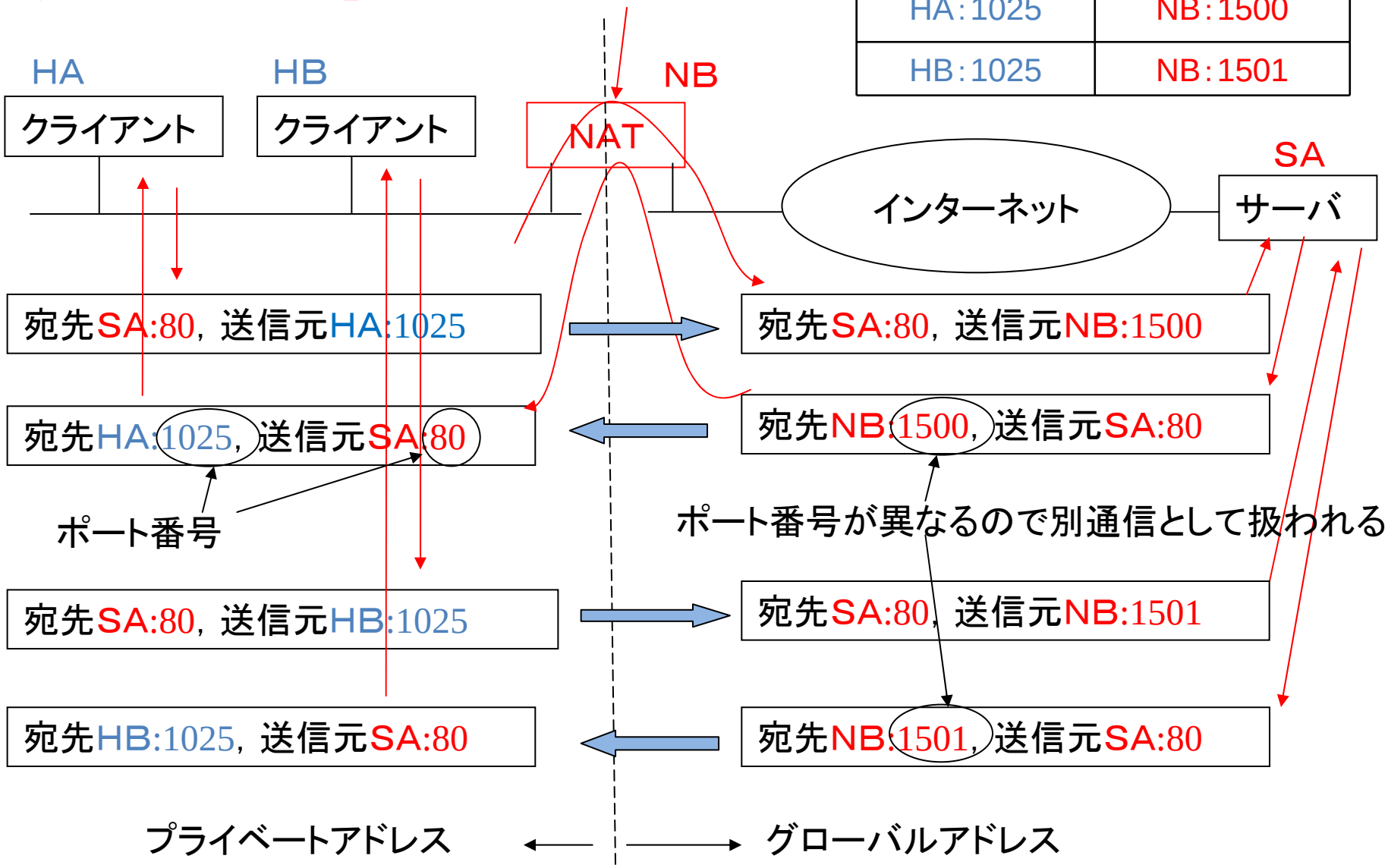
・v6でないといけない理由がない（キラーアプリケーションがない）
・現状で別に困っていない
・V4のアドレスはまだある
・V4との互換性がない。移行は大変
・DNSの整備、検索エンジンの整備などが必要

NAPT（IPマスカレード）のしくみ

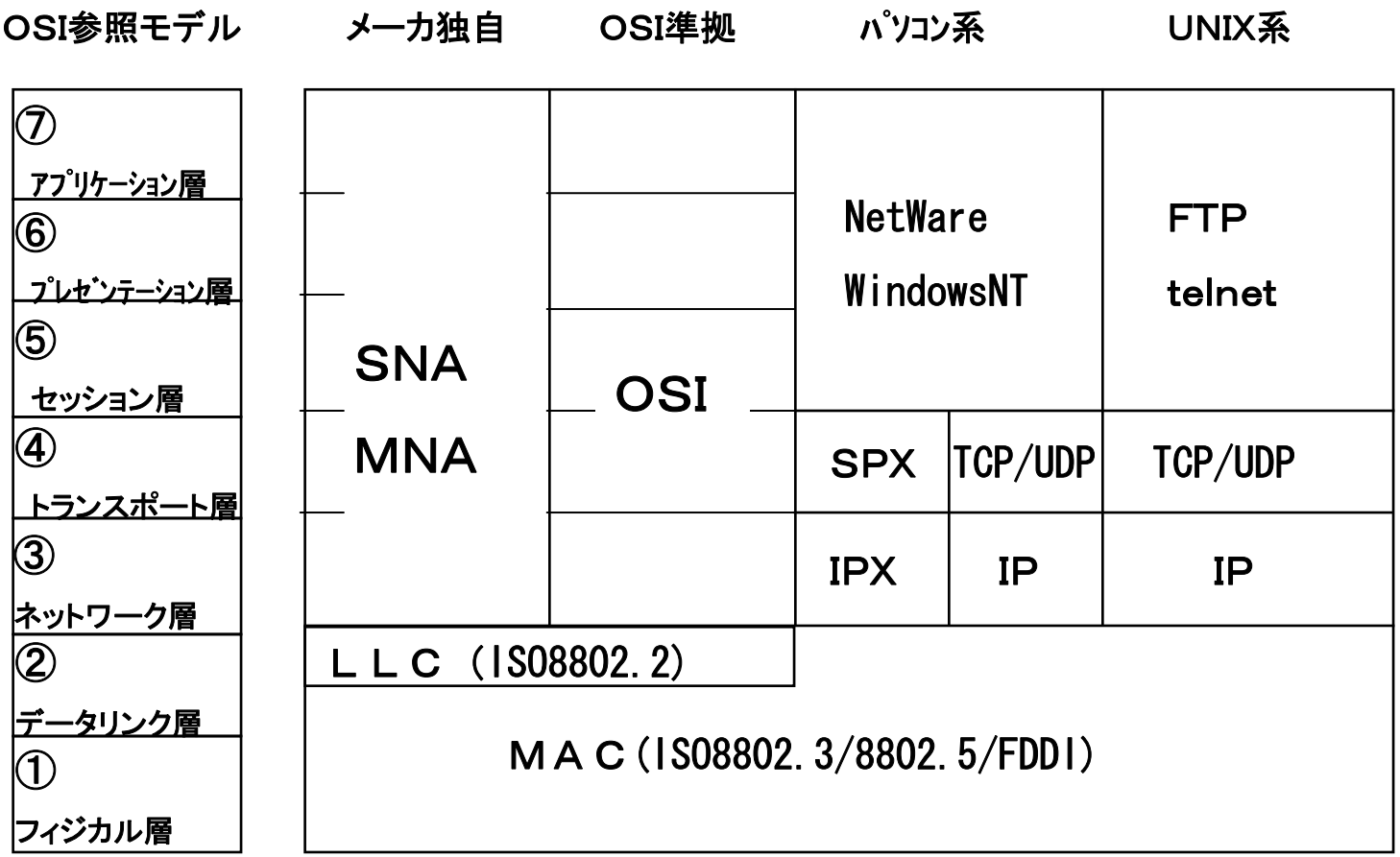
ポート番号：上位ｱﾌﾟﾘｹｰｼｮﾝを識別する番号

送信元IPアドレスとポート番号を入れ替え、対応するNAPTテーブルを作成

NAPTテーブル	
HA：1025	NB：1500
HB：1025	NB：1501



プロトコル乱立時代（1980年代後半）

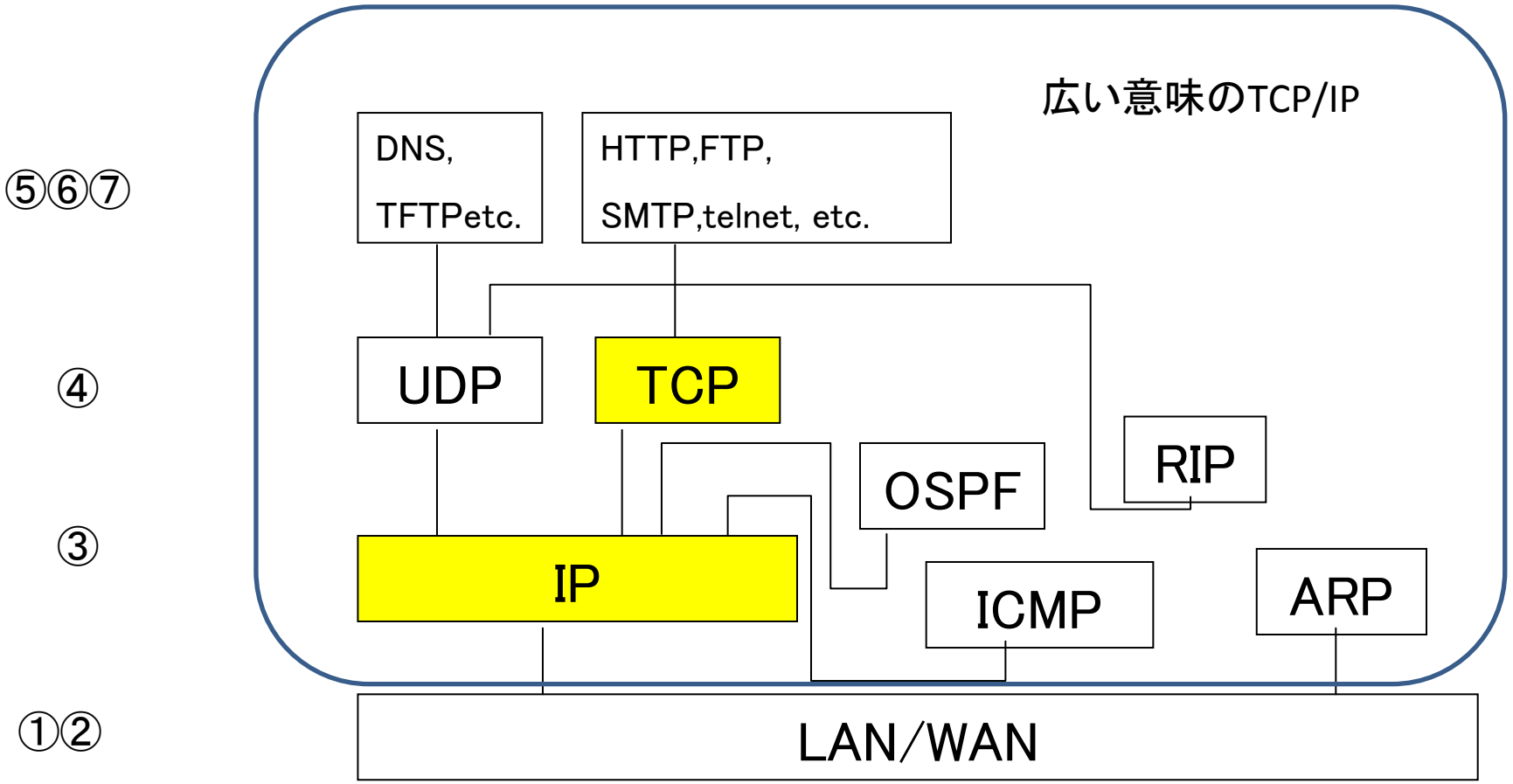


・メーカ独自ネットワークは、オープンシステムの進展に伴い衰退した。

・OSI準拠ネットワークは、仕様が重く普及しなかった。

・パソコン系／UNIX系はTCP／IPに統一され急速に普及した。

TCP/IPのプロトコルスタック・・・・・OSI　7レイヤとはきれいに対応しない



ヘッダ構造とレイヤ構造が統一されていない
TCPのチェックサムの仕様　IpsecがNATを通過できない理由
レイヤに分ける考えはTCP/IPにもあった

OSI7レイヤ；OSIの唯一の成果

成功した技術と失敗した技術

	失敗	成功
プロトコル	OSI	TCP/IP
交換方式	ATM	IP，イーサネット
LAN	FDDI	イーサネット

共通して言えることは？

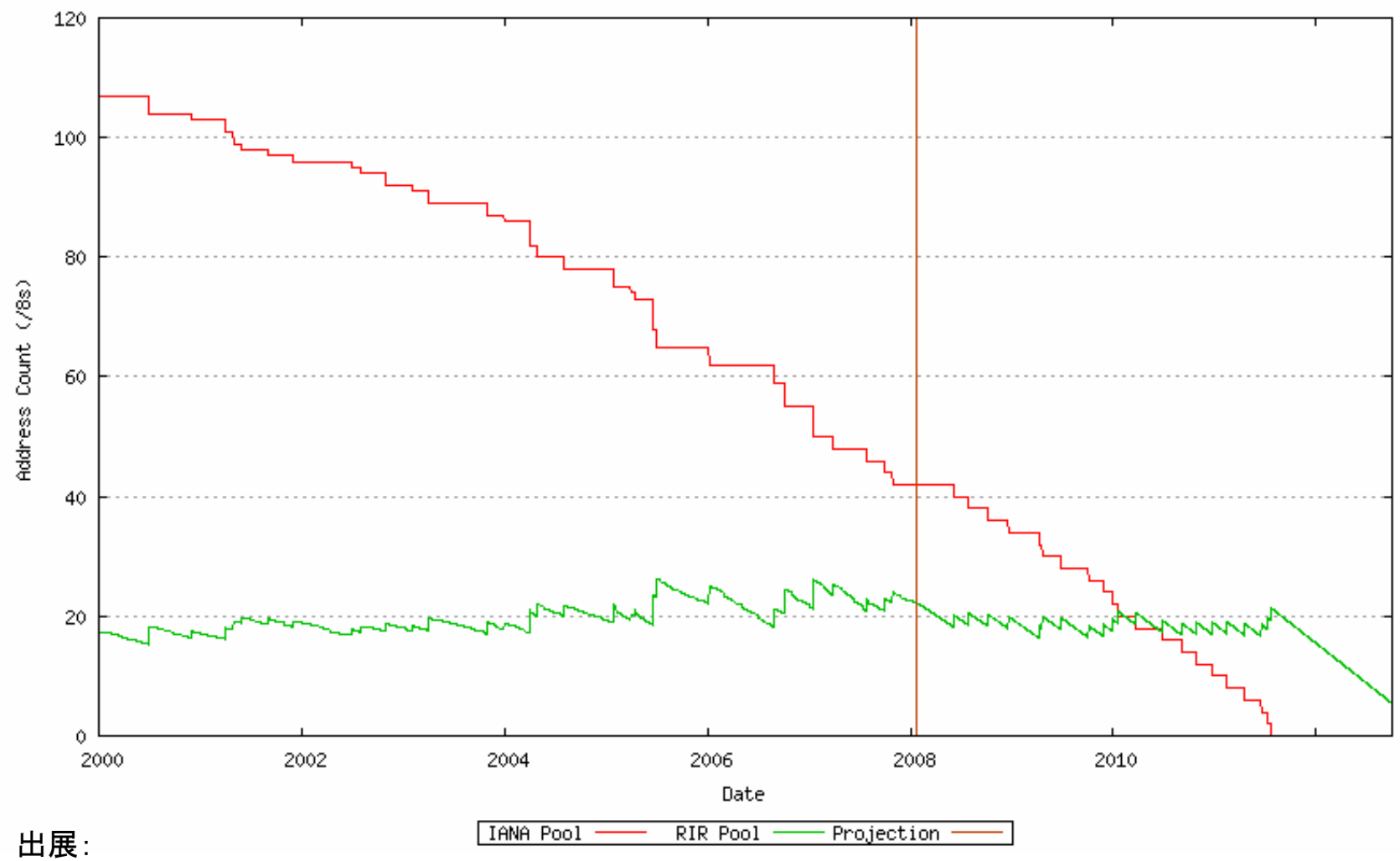
・机上の検討が先行した技術は失敗

・仕様の膨大化、複雑化　⇒　開発期間の増大、開発コストの増大、機器コストの増大

ATM; Asynchronous Transfer Mode

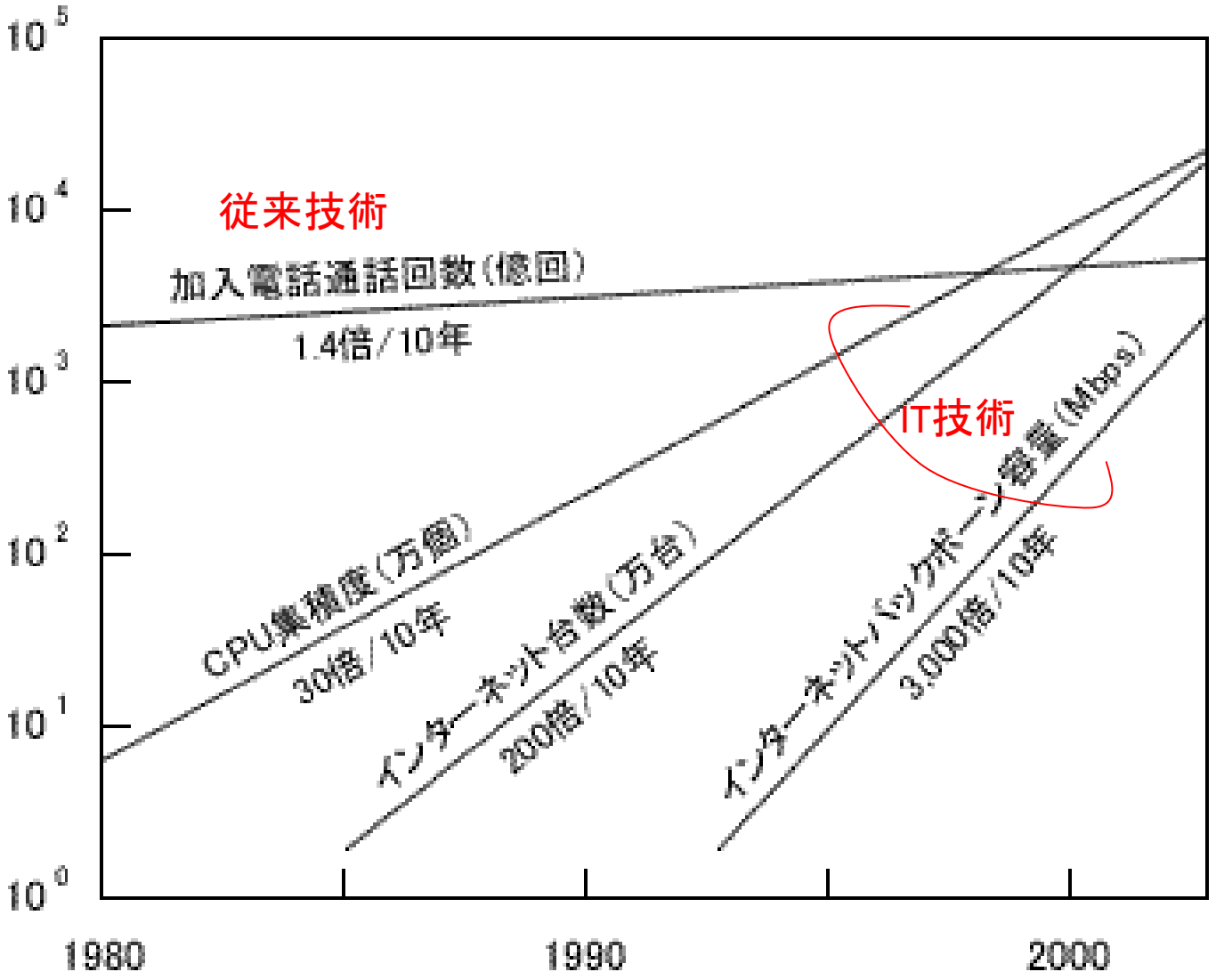
FDDI; Fiber Distributed Data Interface

グローバルアドレスのプール状況



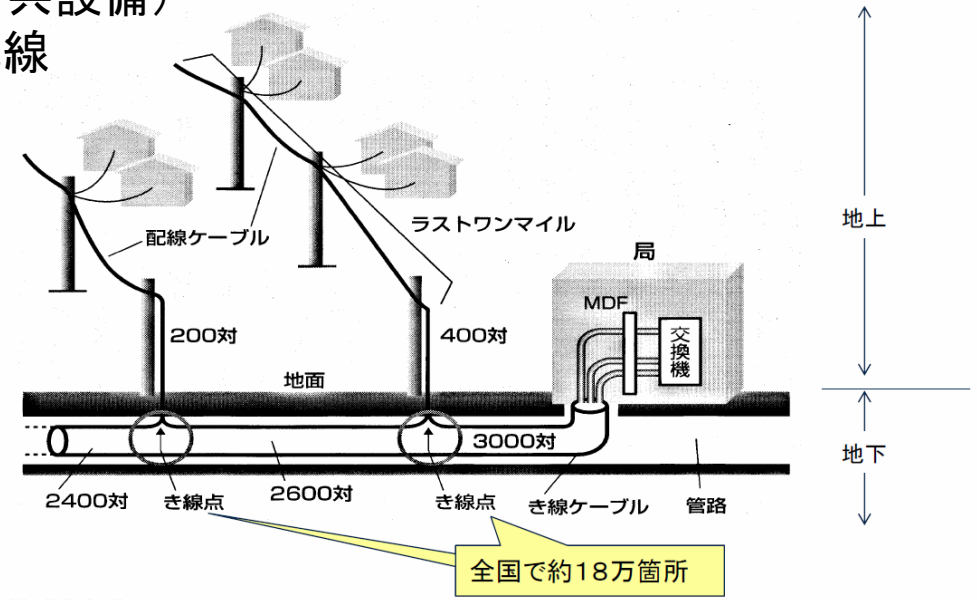
出展:
http://ipv4.potaroo.net/
By Geoff Huston of APNIC (2008/1/26).

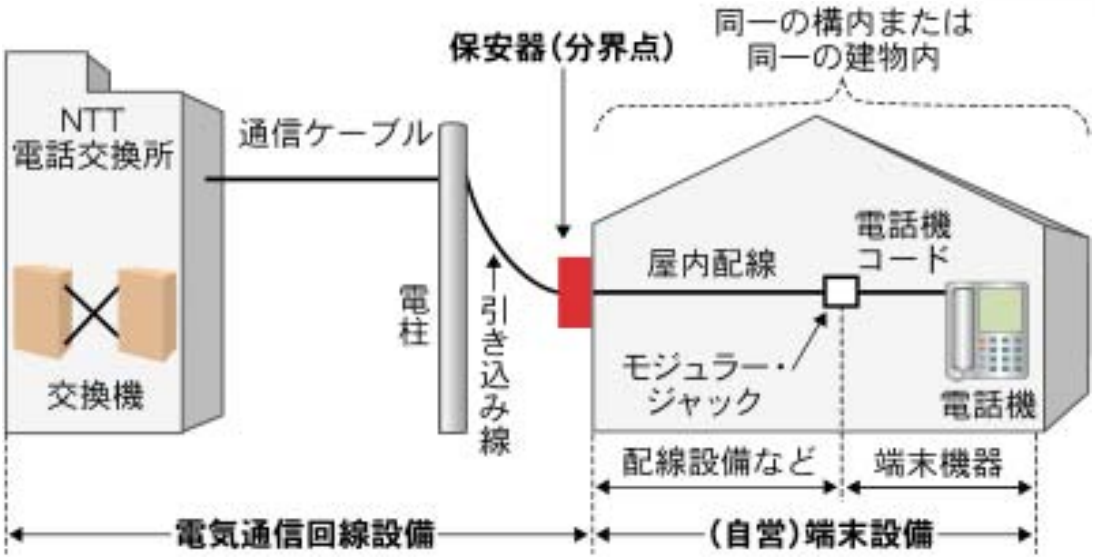
IT技術の発展


10^5
10^4
10^3
10^2
10^1
10^0
1980
1990
2000
従来技術
加入電話通話回数(億回)
1.4倍/10年
IT技術
CPU集積度(万個)
30倍/10年
インターネット台数(万台)
200倍/10年
インターネットバックボーン容量(Mbps)
3,000倍/10年

電話設備の物理構成

ユーザ宅と交換所が完全に1対1で接続されている･･･電話サービスの特徴
保安器までが通信事業者の責任範囲（公共設備）
多数の電信柱、交換機近くは地下道に配線





VPNよるNAT越え

・2段階操作となる

　NATへ接続後、Pアドレスを取得、内部サーバへ接続

・相手がどのNAT配下なのかを知っている必要がある