

# NTMobileの開発 -NAT Traversal with Mobile-

インターネットの課題と現状  
提案の概要  
2010.9.24

名城大学  
渡邊

# 研究背景

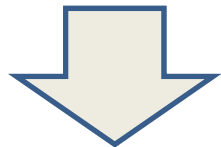
ネットワークのあるべき姿は、自由な通信＋セキュリティ  
IPv4には、様々な通信の制約がある

- ・NAT越え問題
- ・移動透過性
- ・エンドエンドのセキュリティ

IPv6への移行が、思ったように進んでいない

# IPv6は普及するのか

- ・IPv4が広く普及済みである
- ・IPv4とIPv6の互換性がない
- ・IPv6でなければいけないアプリケーションが今のところ存在しない
- ・IPv4で動作していたアプリケーションがIPv6で動かないことがある
- ・2011年にIANAの持つIPv4グローバルアドレスが枯渇する
  - 末端のISPへの影響が出るのは2014年ごろ
  - アドレス枯渇後の新規ユーザはIPv6アドレスしか取得できなくなる



- ・IPv6はやむを得ず徐々に導入されていく。
- ・旧来のユーザはIPv4のまま残る(積極的に移行する理由がない)
  - ーIPv4で蓄積したノウハウがある
  - ーNATにもよい点がある(アドレスの隠蔽)
- ・IPv4/v6混在環境が今後長く続く

# 研究の目的

IPv4における通信の制約を除去する

NAT越え問題の解決

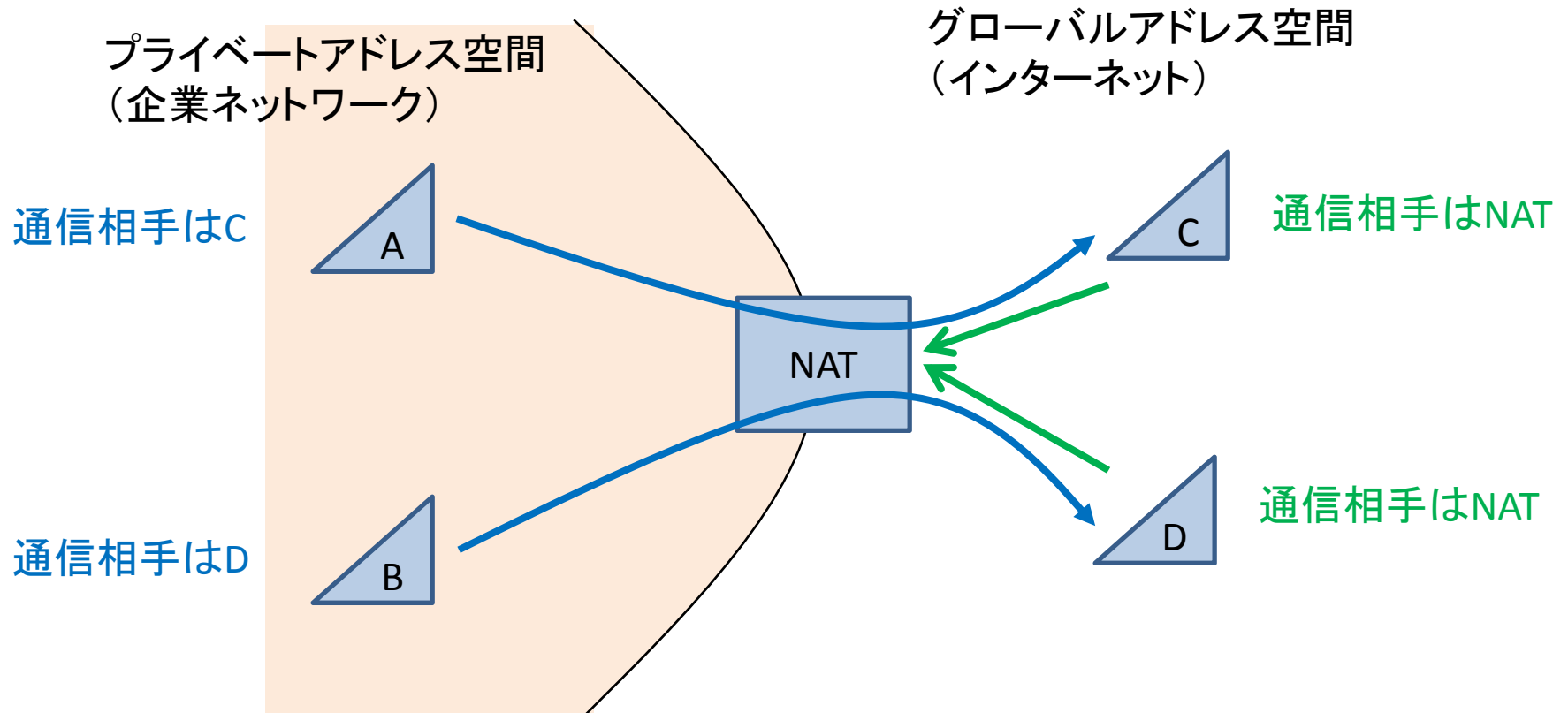
通信中の自由な移動

そのうえで、エンドエンドのセキュリティを確保する

## 条件：

- ・現状のネットワーク環境を変えない(ルータ/NATはそのまま)
- ・スケーラビリティがある
- ・一般端末との混在が可能 → 段階的な普及
- ・IPv6との共存に向けた発展性がある
- ・性能が劣化しない

## インターネット側（NATの外側）からの通信開始ができない



IPv6になればNATは不要になるという考え

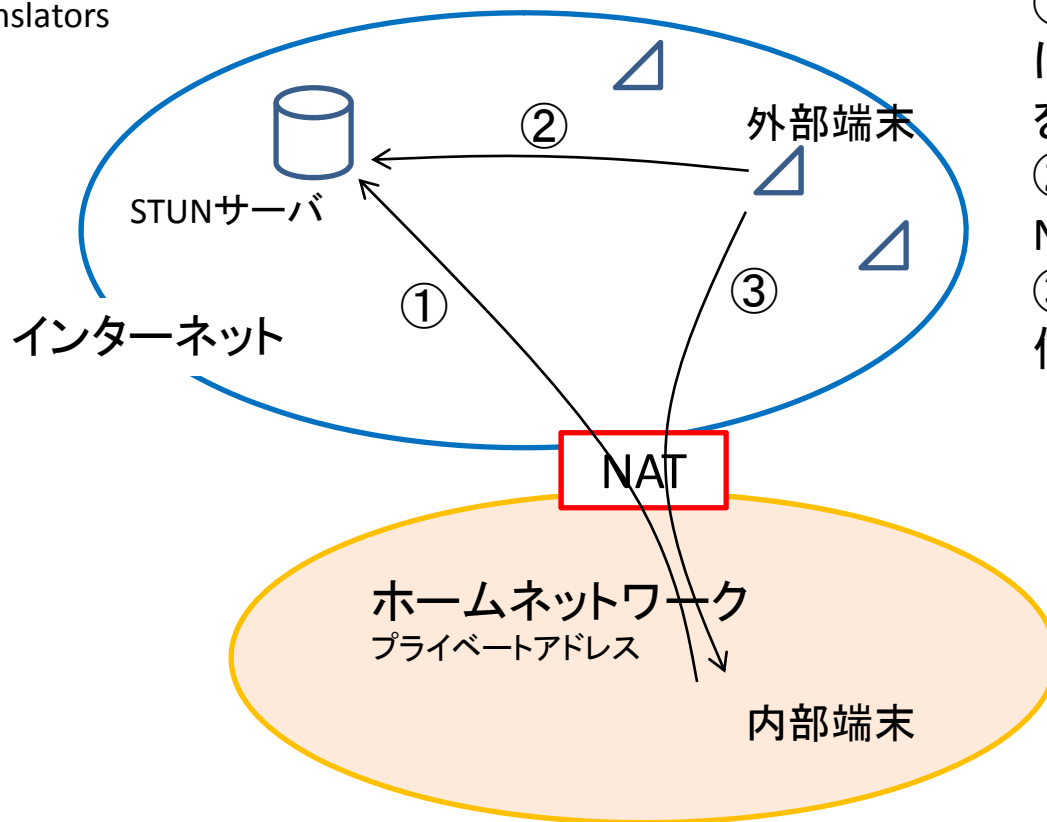
→ NAT越えに関する研究は少ない(特に国内では)

# NAT越え技術の例とその課題

既存技術

## STUN (RFC3489)

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)
- ・TCPが考慮されていない
- ・端末の移動が考慮されていない

## IPv4の課題2: 移動透過性

### インターネットでは通信中に移動するのが難しい

- ・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

NATによりアドレス変換される → NATを跨る移動はさらに難しい



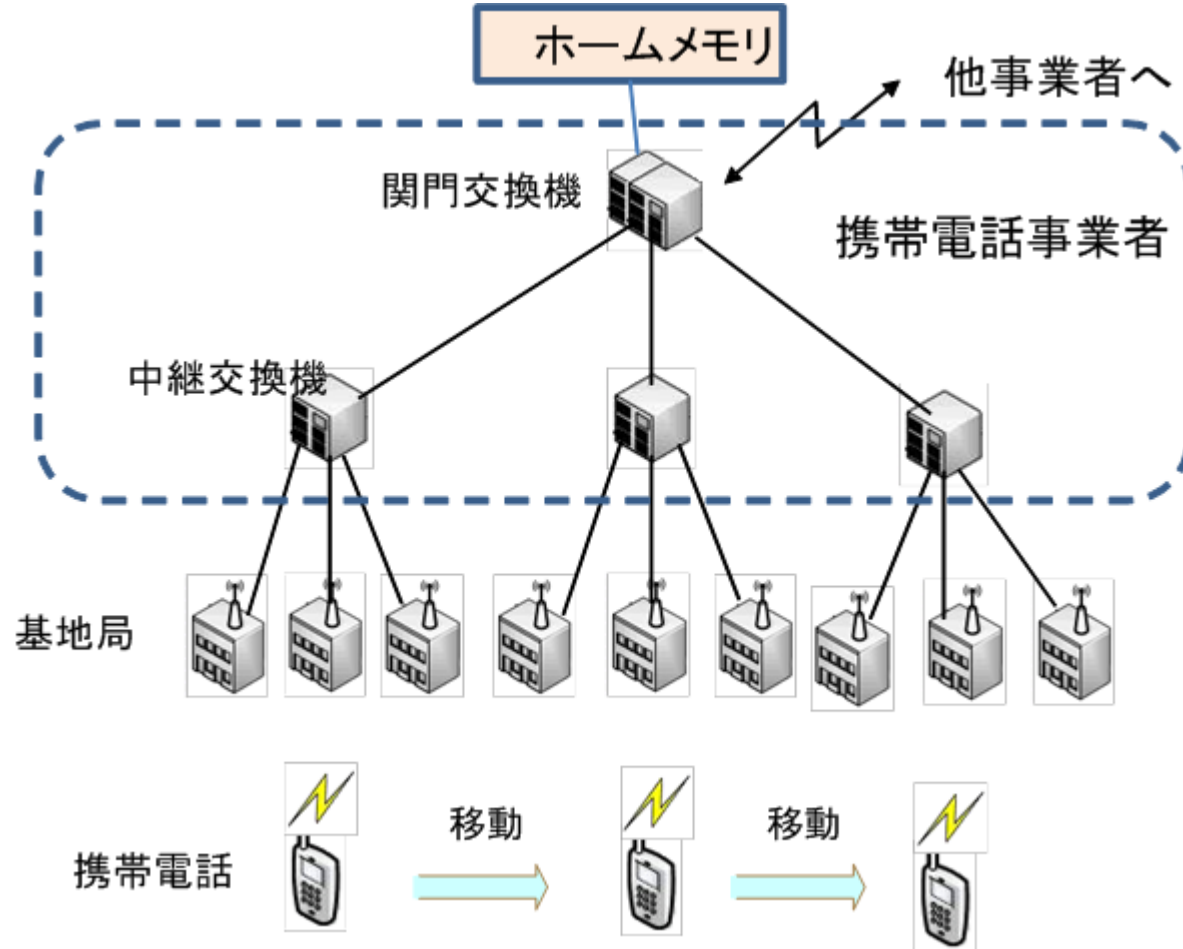
移動透過性に必要となる技術:

- ・パケットを正しくルーティングできる
- ・上位ソフトウェアはIPアドレスの変化に気付かない

# 携帯電話による移動

ネットワークの頑張り

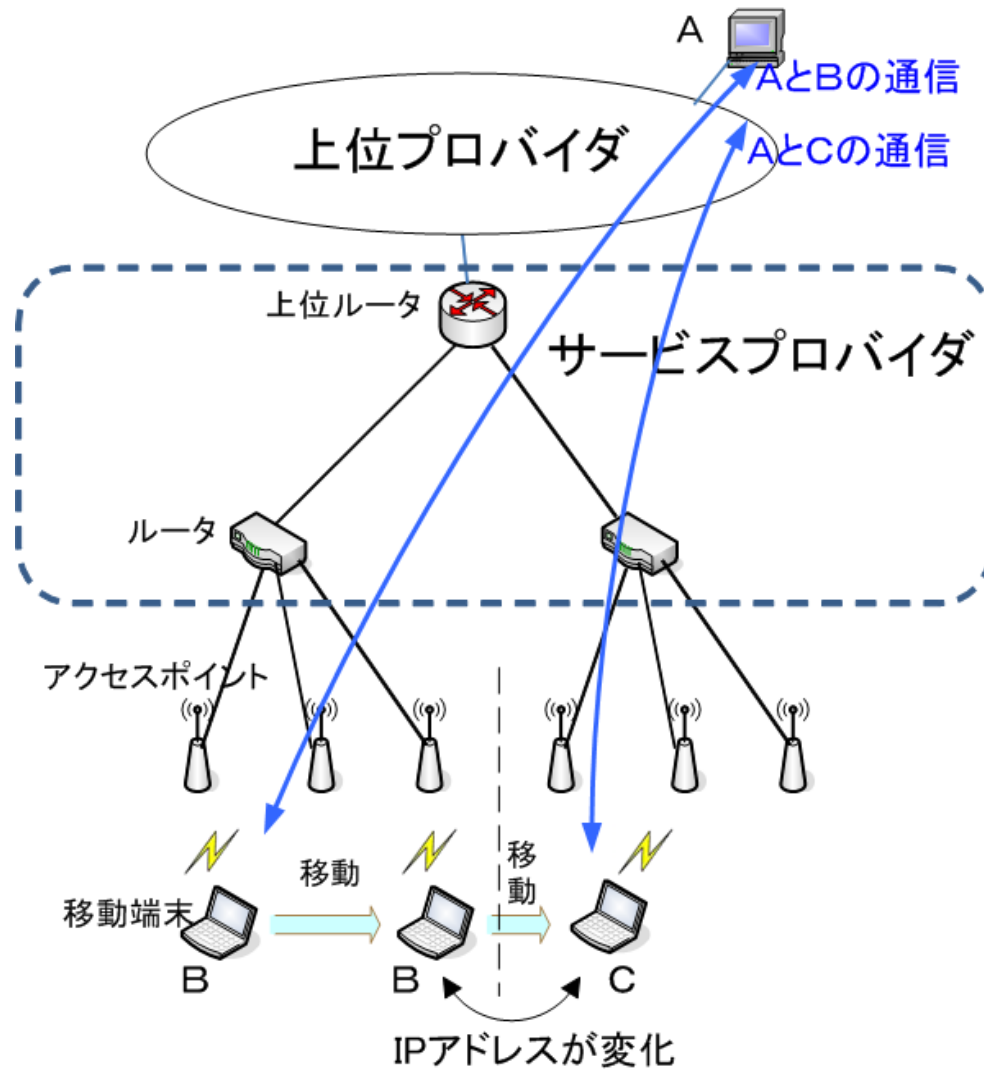
携帯電話の場所を記憶



移動しても端末のIPアドレスが変わらないようにネットワーク側が頑張る



# 一方、インターネットでは ネットワークは何もしてくれない

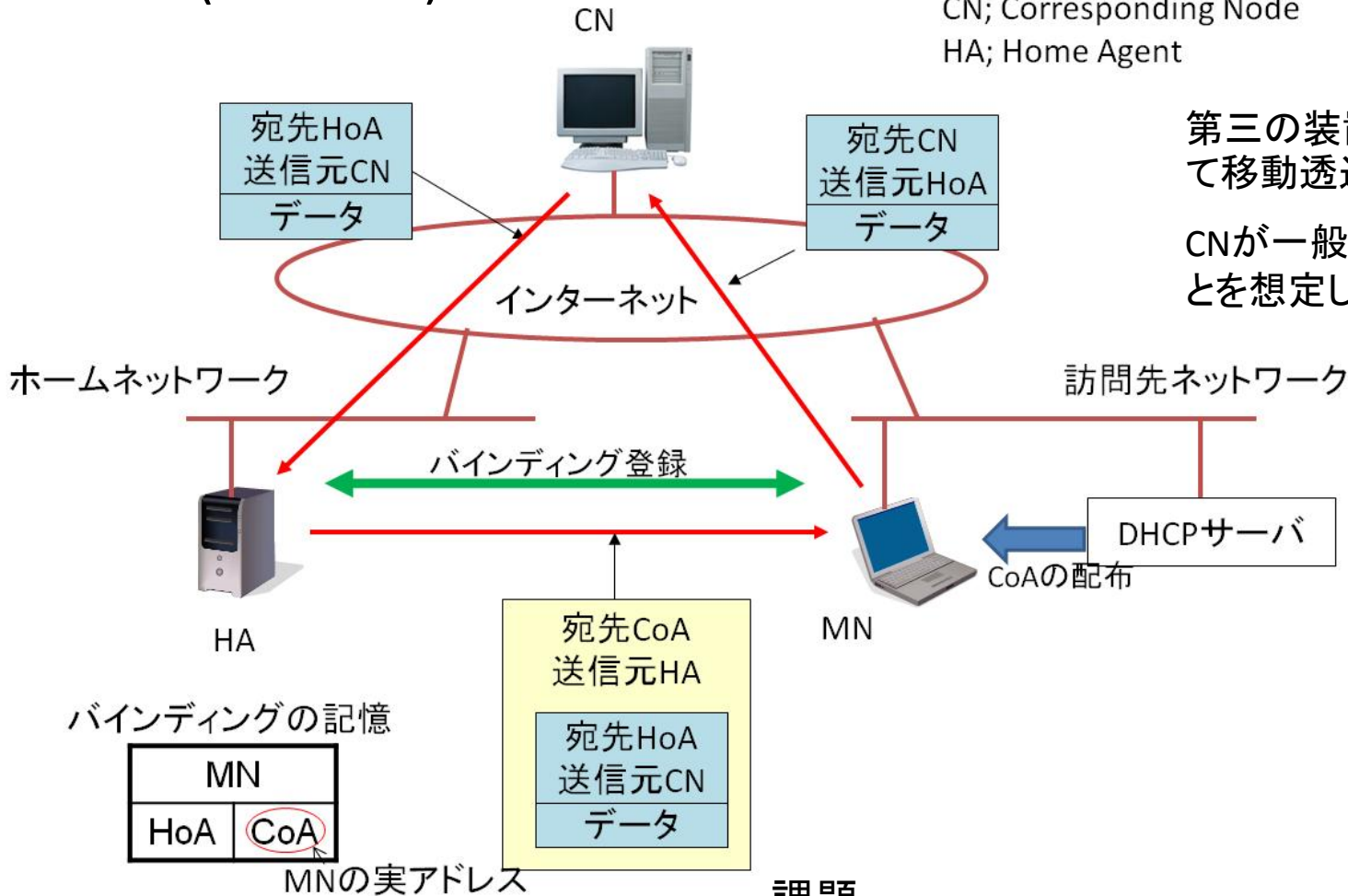


IPアドレス/ポート番号は通信の識別子  
↓  
アドレスが異なると違う通信とみなされる

移動透過性に係る研究は将来のIPv6普及を見越して、IPv6に関するものがほとんど(国内、国外とも)

## Mobile IP (RFC2002)

MN; Mobile Node  
CN; Corresponding Node  
HA; Home Agent



第三の装置の助けを借りて移動透過性を実現  
CNが一般サーバであることを想定した技術

### 課題

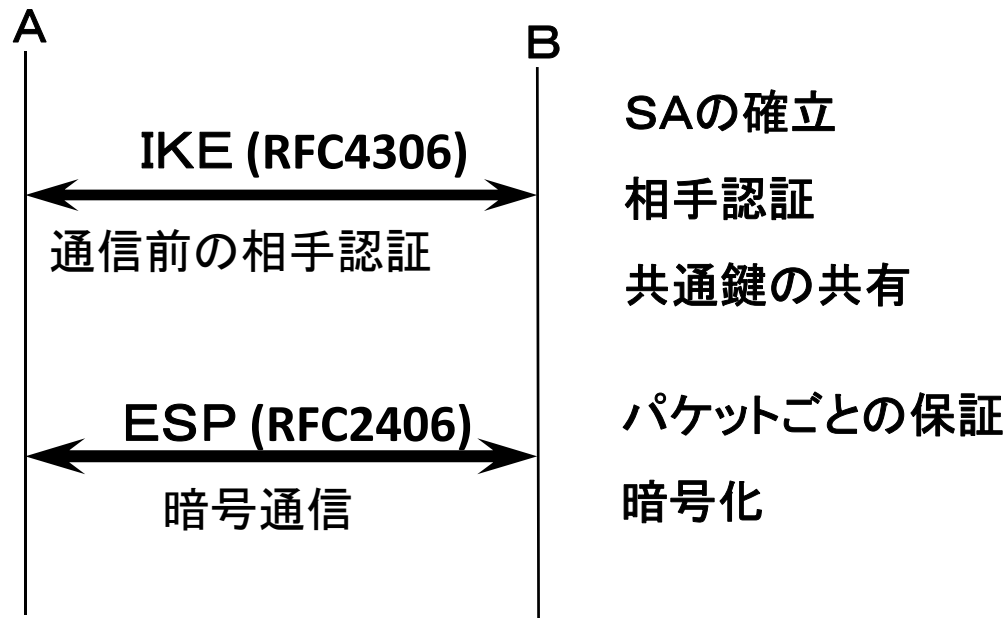
- ・不自然な経路→不正パケットとして廃棄される可能性
- ・CNが動く場合は別のHAが必要

# IPv4の課題3: エンドエンドの認証と暗号化

セキュリティ確保のための管理負荷が大きい

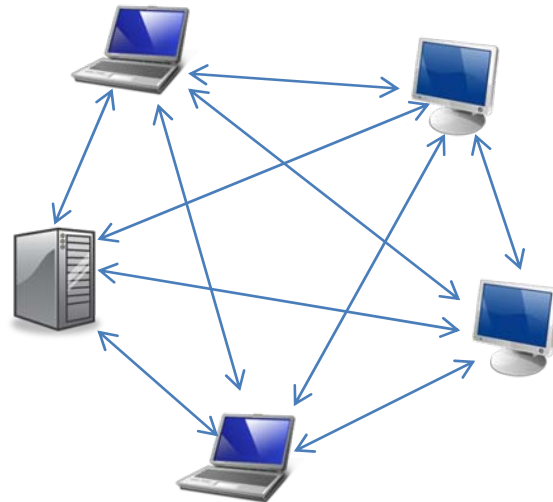
NATを跨る確実なエンドエンドセキュリティ技術がない

(IPsecはNATの存在を考慮していなかった)



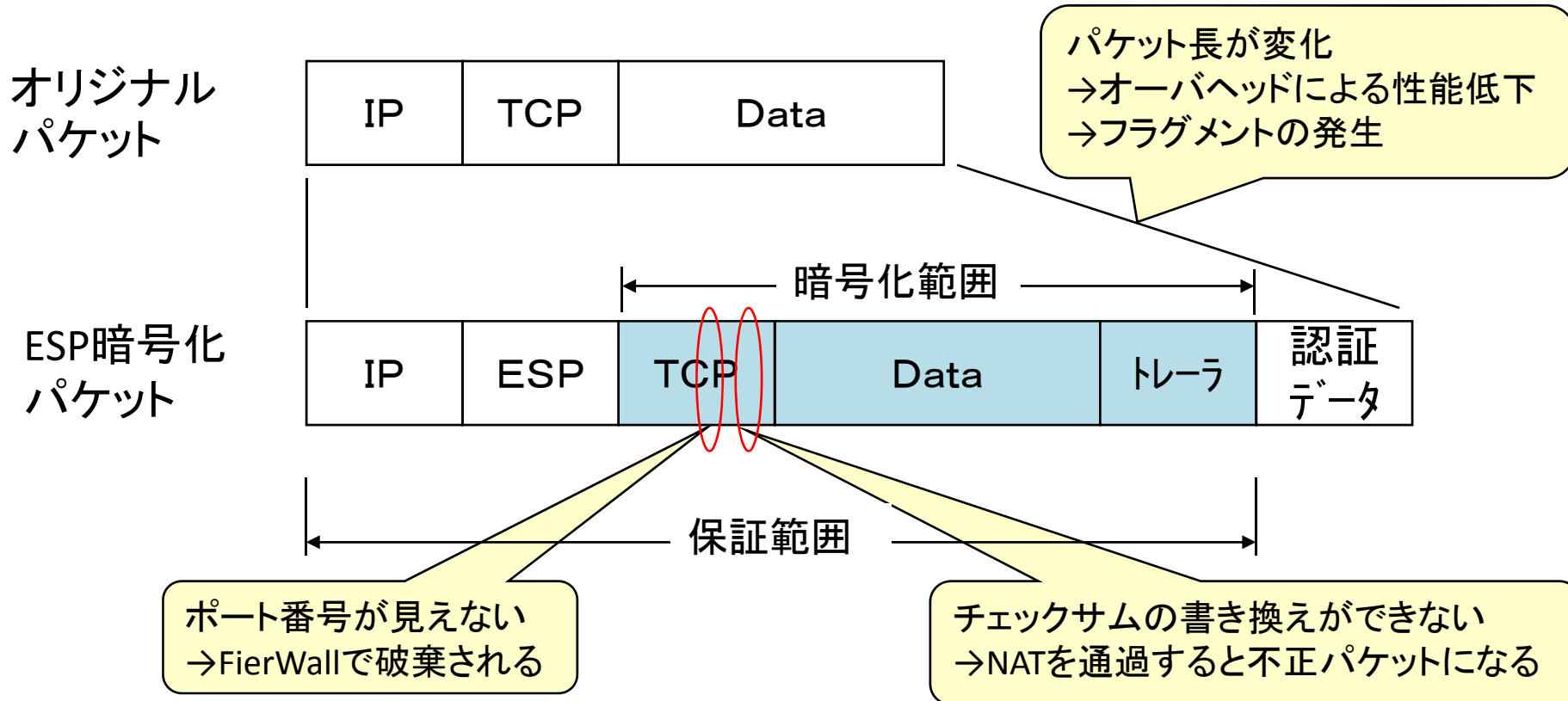
IKE (RFC4306)は通信ペアごとに定義する必要がある  
通信グループメンバの数が増えると管理負荷が膨大になる  
汎用性を重視しているため、もともと設定項目が多い  
端末が移動した場合は再定義が必要となる

### IKEによる通信グループの定義



# ESP(RFC2406)ではNATを跨る暗号化通信が困難

NATでアドレス変換されると、不正パケットと判断される



NATを跨る暗号化のための方法: UDPトンネル(RFC3948)  
IP/UDPヘッダは保証範囲外となる

## ベースとなる技術の紹介

NAT越え、移動透過性、セキュリティを同時に満たすネットワークをFPN (Flexible Private Network) と呼ぶ

FPNを実現するアーキテクチャをGSCIP (Grouping for Secure Communication for IP; ジースキップ) と呼ぶ

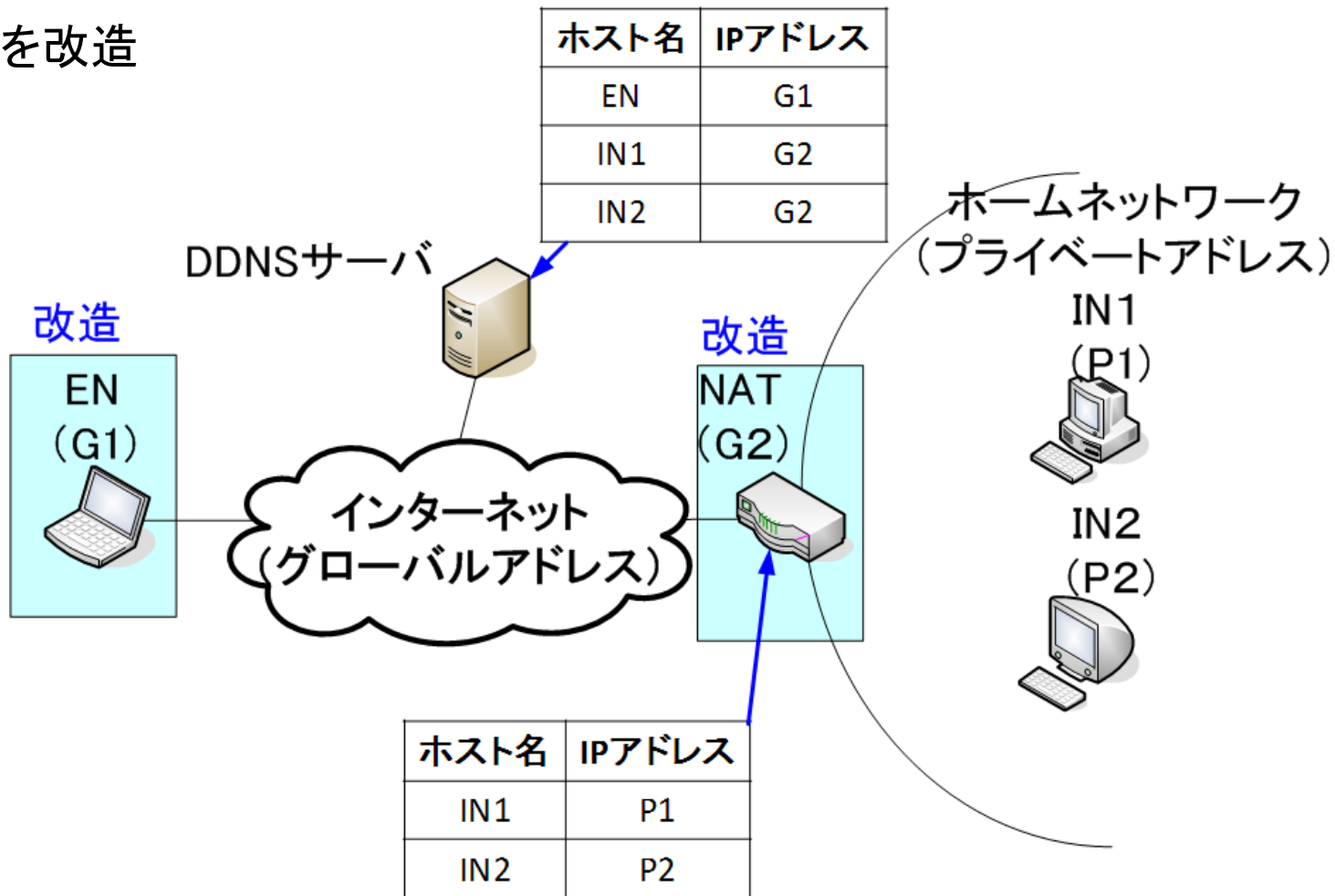
### GSCIPを構成する主要プロトコル

プロトコル名	機能	キーとなる技術
NAT-f	NAT越え	仮想アドレス IP層でのアドレス変換
Mobile PPC	移動透過性	IP層でのアドレス変換
DPRP	グループ認証	アドレスに依存しないグルーピング
PCCOM	暗号化通信	独自のチェックサム演算

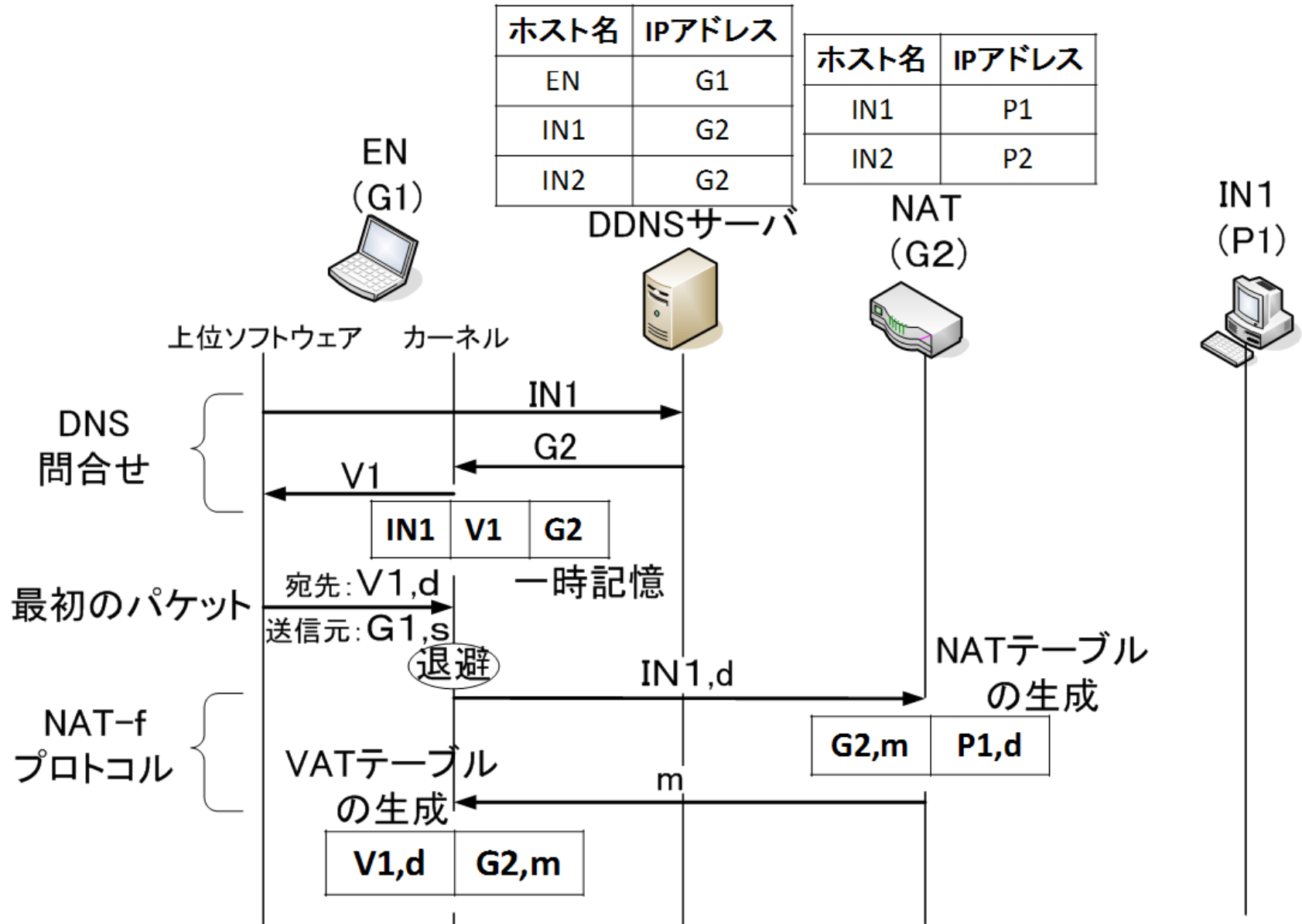
# NAT越えを実現するNAT-f (NAT-free protocol)

提案済み技術

## 外部ノードとNATを改造

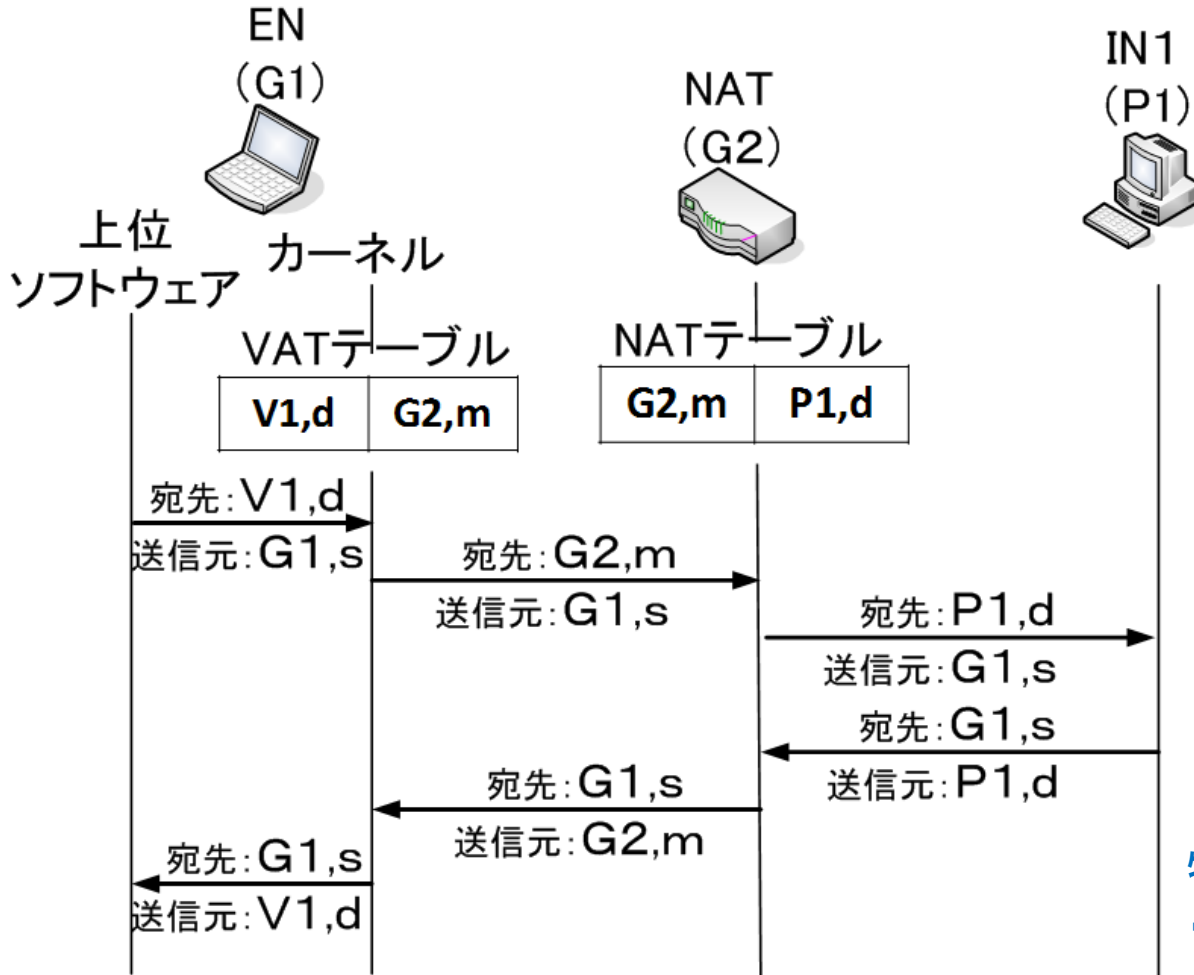


# 通信前のネゴシエーション





# 通信時のアドレス変換の様子



NATテーブルに合わせてアドレス/ポート変換を行う

## 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

## 課題

- ・NATの改造が必要

## ポイント:

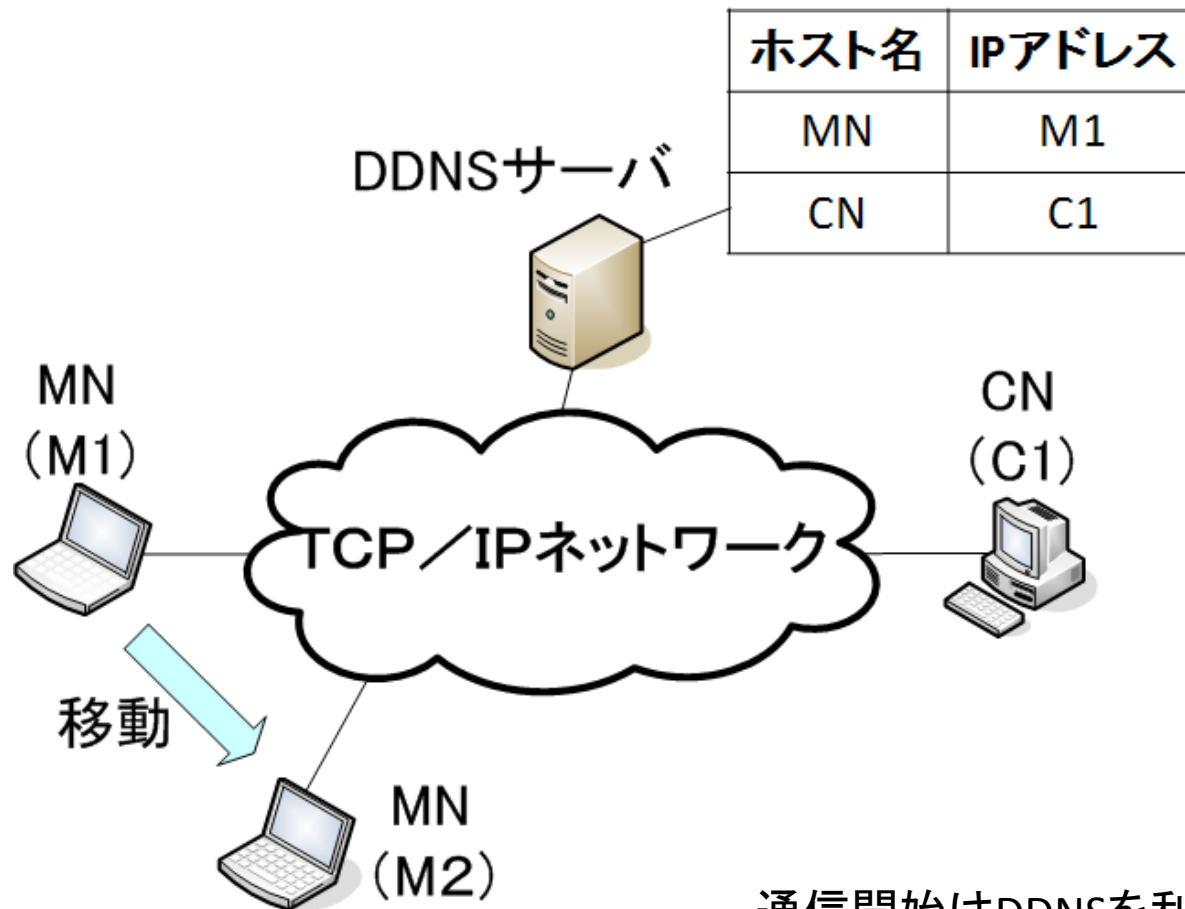
仮想アドレスの技術

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

提案済み技術

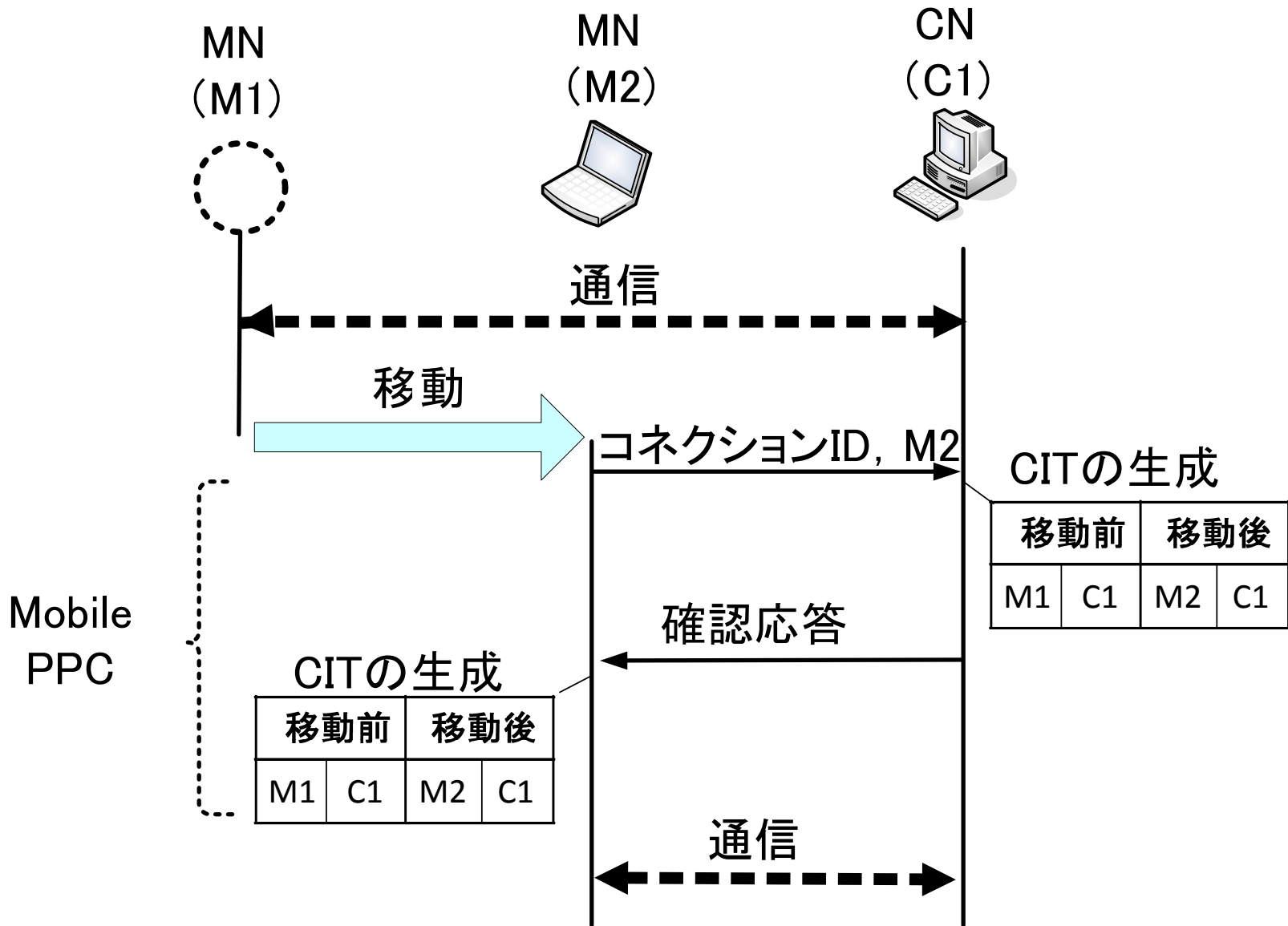


エンドノードを改造

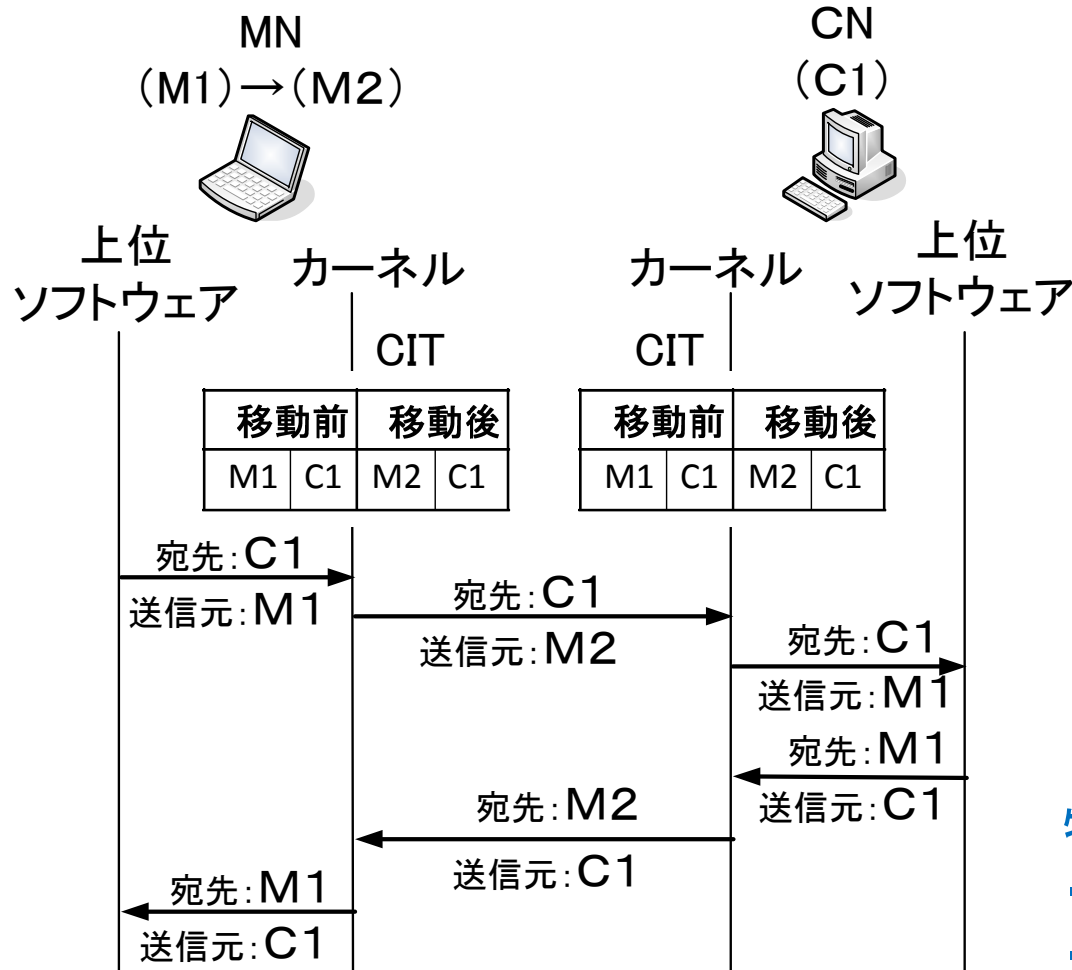


通信開始はDDNSを利用  
移動時にMobile PPCを実行

# 移動時のネゴシエーション



# 通信時のアドレス変換の様子



パケットは正しくルーティングされる  
上位ソフトウェアはアドレスの変化に気付かない

ポイント:  
IP層でのアドレス変換

## 特長

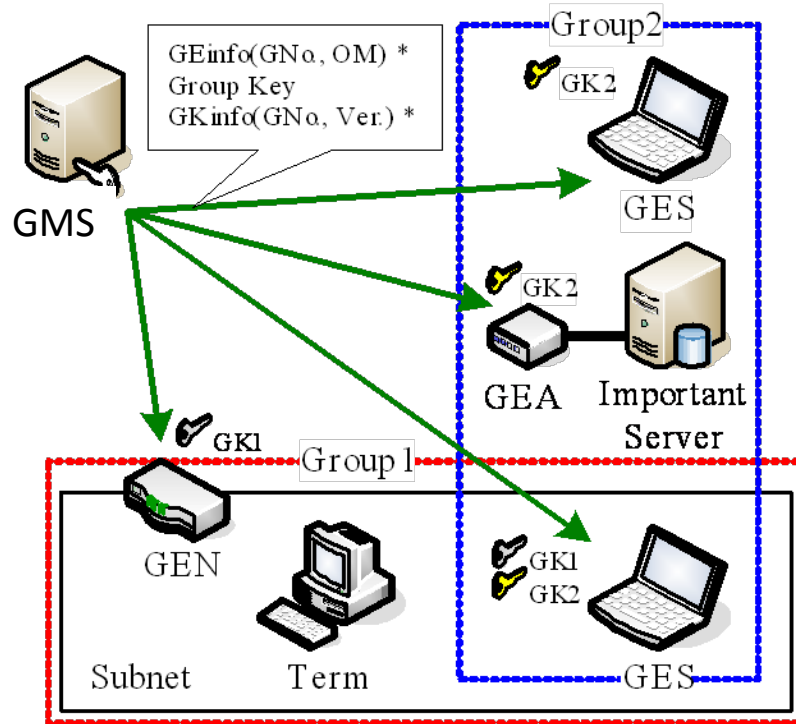
- ・余分な装置がない
- ・アプリケーションに影響がない
- ・高スループット
- ・既存端末と上位互換

## 課題

- ・CN側にも改造が必要

# グループ認証を実現するDPRP (Dynamic Process Resolution Protocol)

提案済み技術



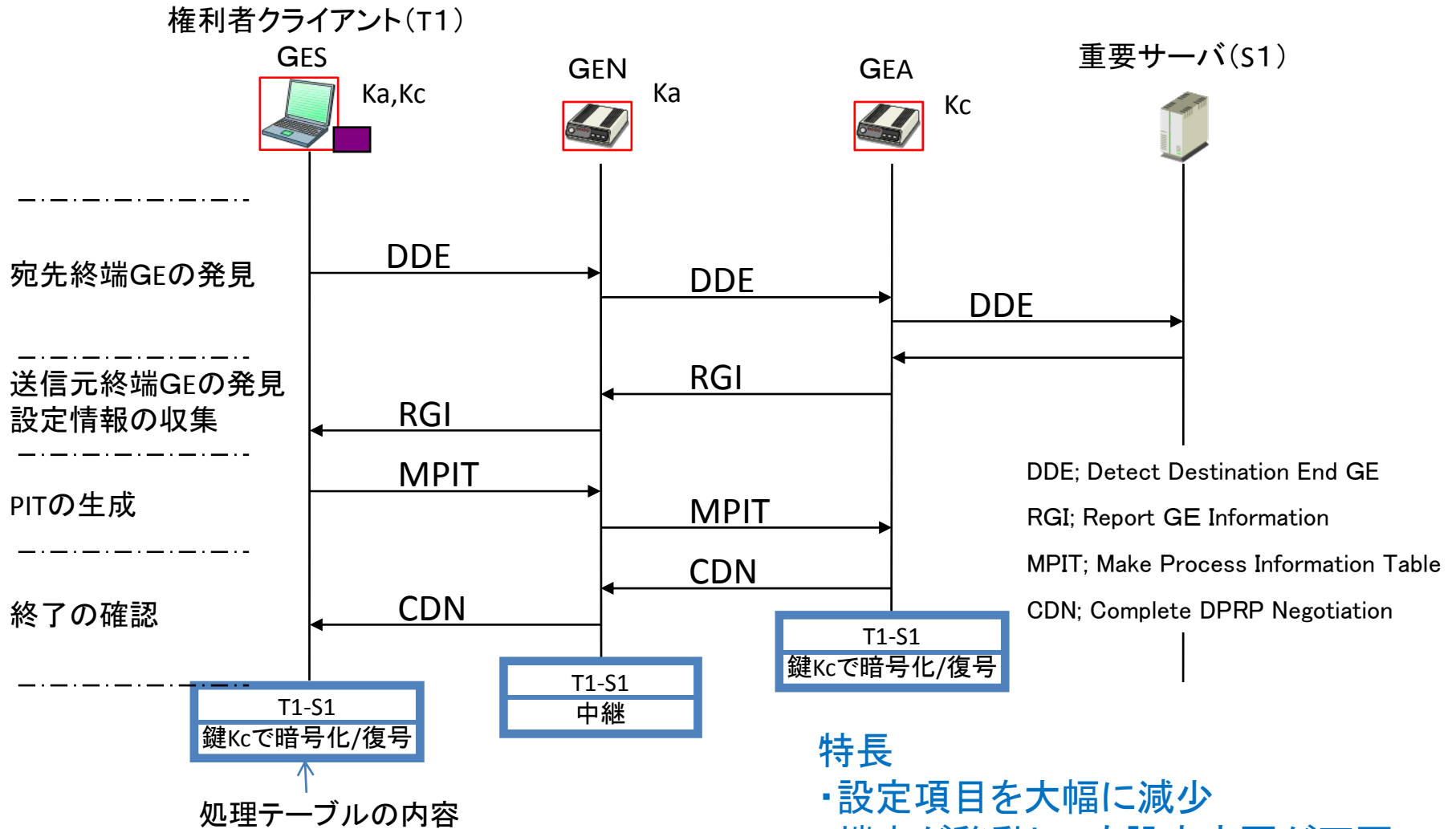
通信グループと暗号鍵を1対1  
に対応付ける

システム構成を学習する

グループ鍵はGMSからオフライ  
ンで配送

GMSとGE間はPKIなど既存の認  
証のしくみを利用

# DPRPのシーケンス



ポイント:  
グループ認証

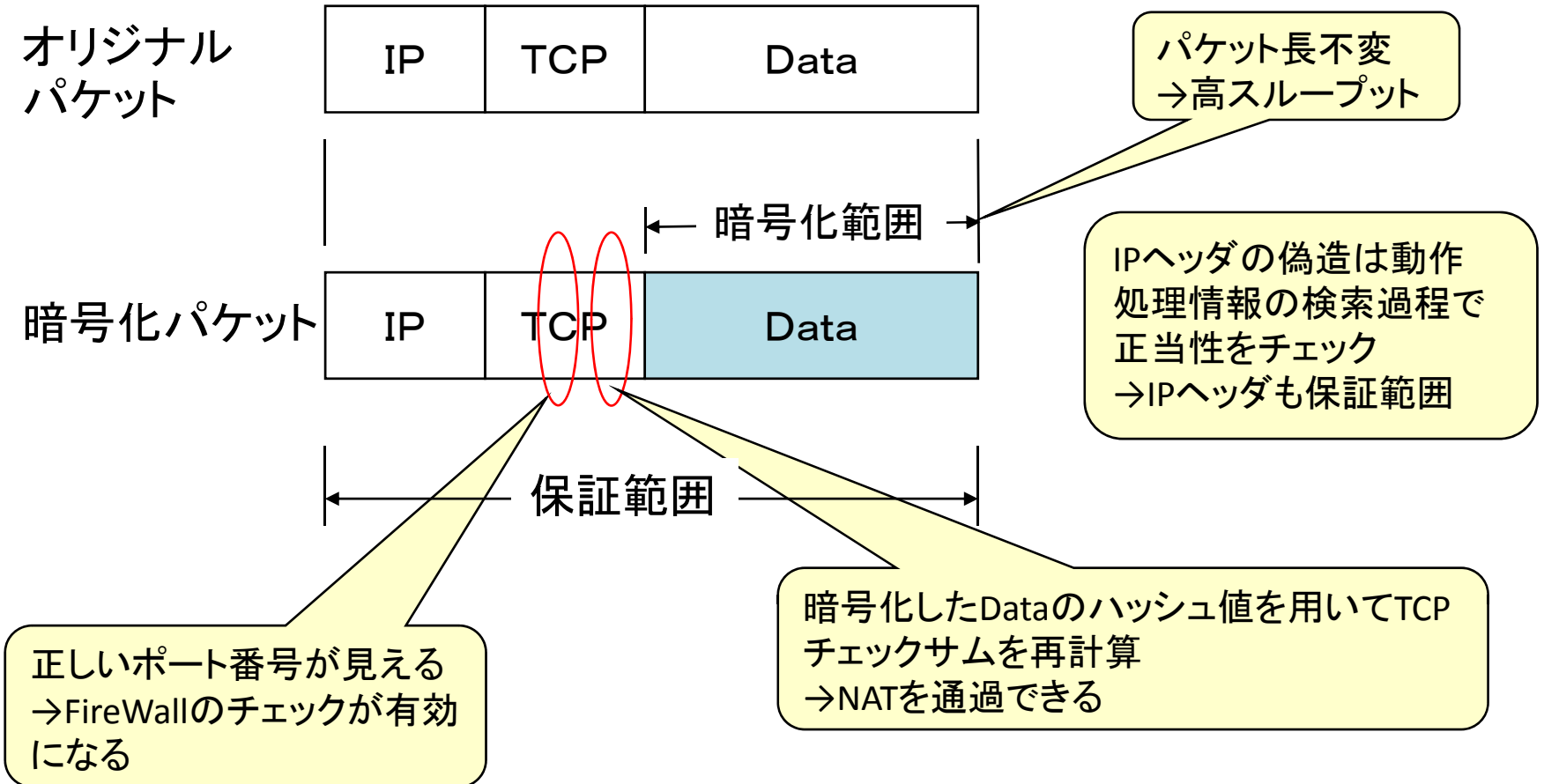
## 特長

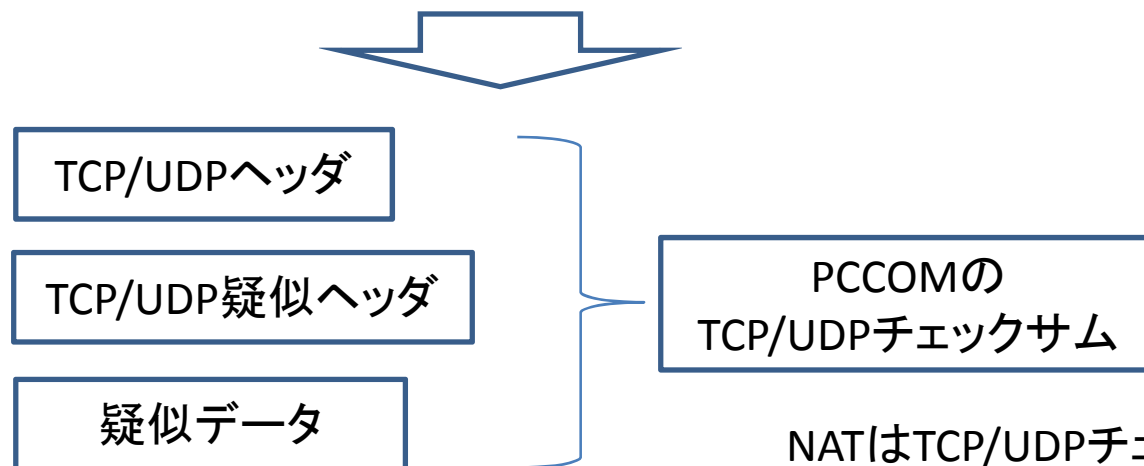
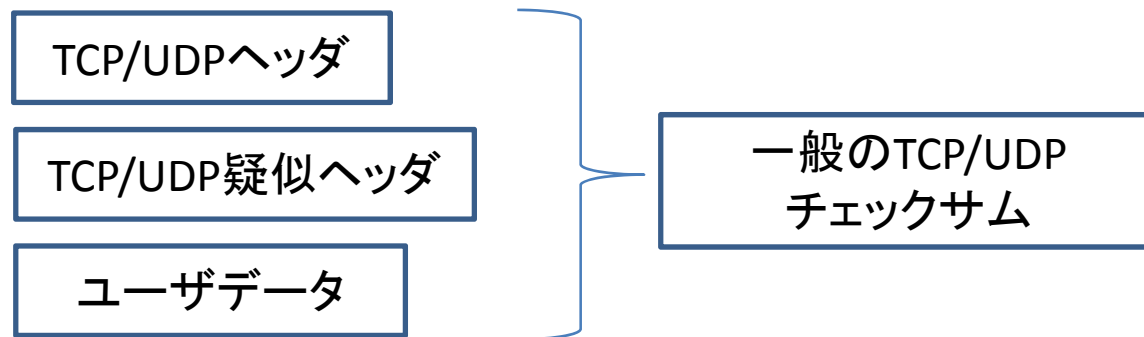
- ・設定項目を大幅に減少
  - ・端末が移動しても設定変更が不要
  - ・個人単位とドメイン単位の混在が可能
- 課題
- ・プロトコルが複雑

# NATを跨る暗号化通信PCCOM

(Practical Cipher COMMunication Protocol)

TCPチェックサムを独自の内容に置き換えることによりNATを跨った暗号通信を実現





↑  
暗号化データと暗号鍵  
のハッシュ値

NATはTCP/UDPチェックサムをIPアド  
レス変化の差分で再計算する  
(RFC1631)

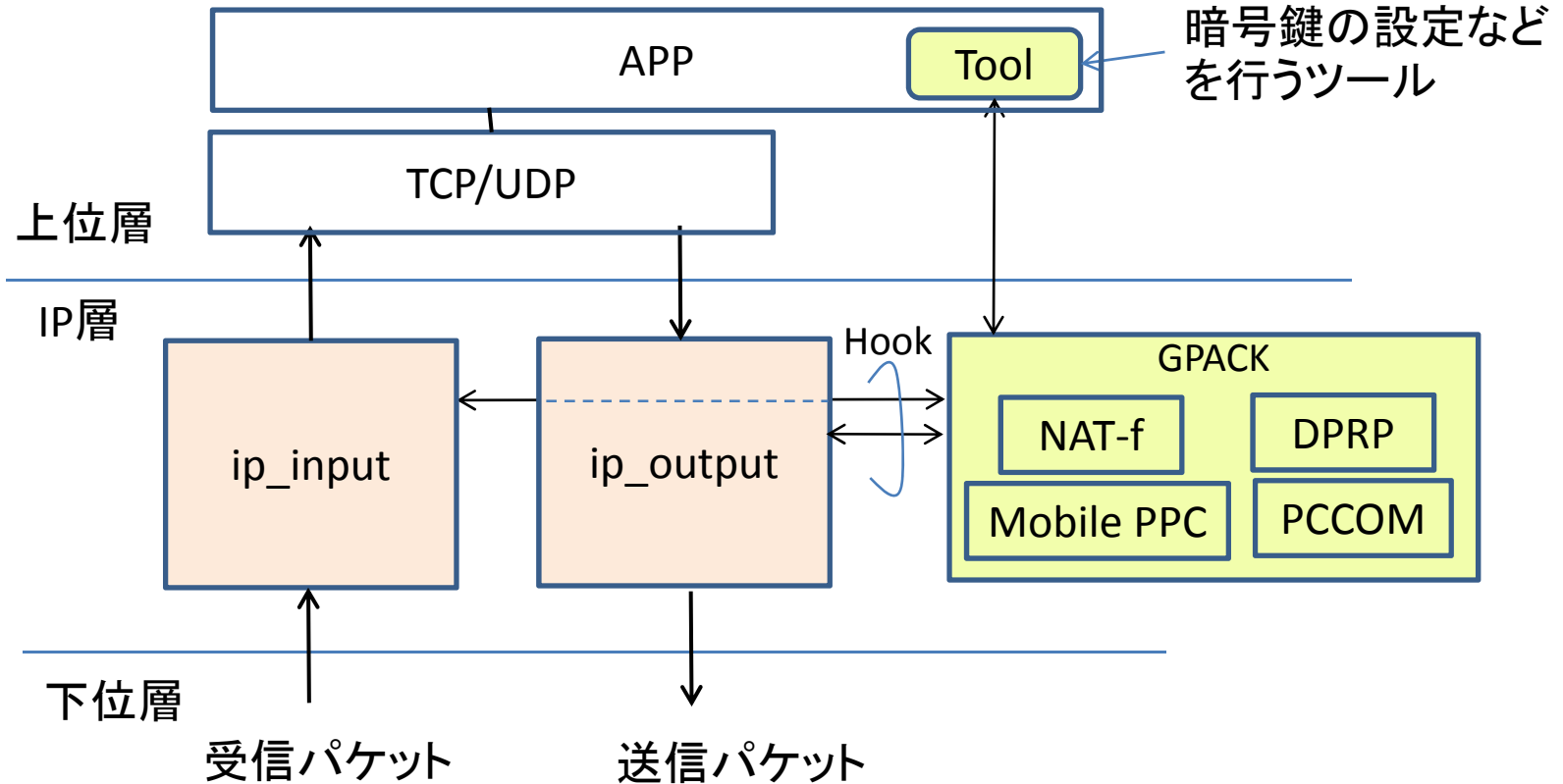
特長:

- ・NATを跨る暗号化
- ・高スループット

ポイント:  
独自のTCPチェックサム演算



# GPACKの実装 (Free BSD)



GPACK; GSCIP Package

IP層のip\_input, ip\_outputよりGPACKを呼び出し  
LINUXへ移植中

**カーネルのバージョンアップに伴う変更が頻発**

# NTMobileの概要

## 特長:

- ・NATの有無にかかわらず自由に通信を開始できる(NAT越え問題の解決)
- ・NATを跨る移動透過性を実現できる
- ・エンドエンドのセキュリティを確保できる
- ・NATを改造しなくてよい
- ・プライベートアドレスが重複していてもよい
- ・既存ノードとの互換性がある
- ・IPv4/IPv6混在ネットワークへの拡張が可能
- ・移動時にパケットロスが発生しない

## システム構成:

- ・DS (Direction Server)
  - DDNS (Dynamic DNS)サーバを改造
  - エンドノードのホスト名とホスト・IPアドレス、NAT・IPアドレスの関係を登録
  - エンドノードに対する動作指示
- ・RS (Relay Server)
  - DSの一部機能を分離
  - 特定のケースにおいてデータを中継
  - 相手端末が一般端末の場合のプロキシサーバ
- ・移動端末としてはスマートフォンを想定

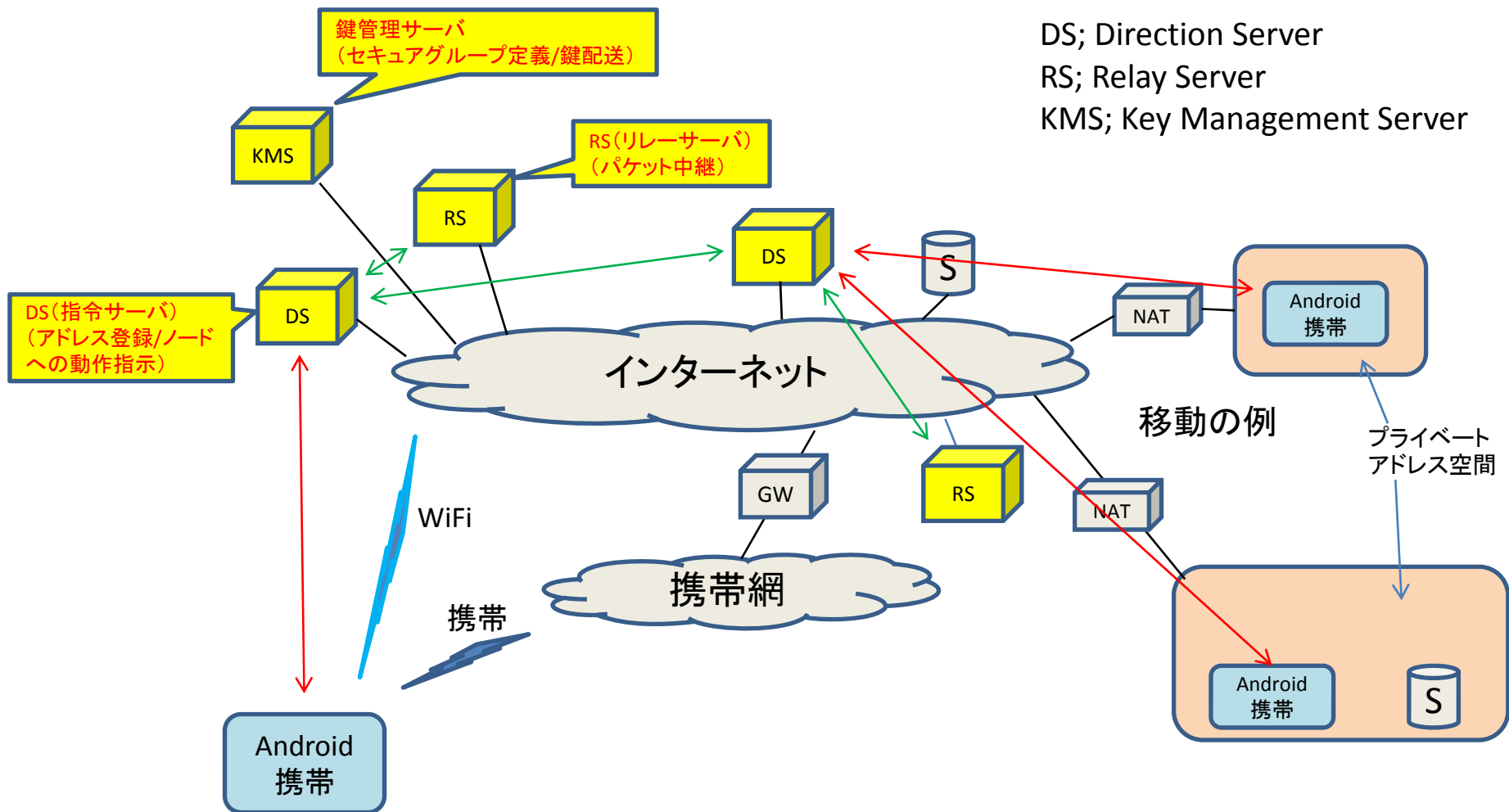
# キーとなる技術

- ・IP層でのアドレス変換  
移動時に上位層に対してアドレスの変化を隠蔽する⇒Mobile PPCの技術を流用  
上位層ではアドレスを仮想アドレスで認識する ⇒NAT-fの技術を流用
- ・グループ認証 ⇒DPRPを適用  
通信開始時に相手を認証する
- ・暗号化技術 ⇒PCCOMを適用  
高速暗号化通信
- ・トンネル転送  
NATのSPIフィルタの回避、およびNATを跨る移動を実現するため、NAT通過時は原則としてUDPトンネル転送
- ・DS (Direction Server)  
NATアドレスをDNSリソースレコードとして追加
- ・KMS (Key Management Server)  
暗号鍵の管理

SPI (Stateful Packet Inspection):

TCPにおける不正なシーケンスのパケットを破棄する機能

→移動透過性の実現を困難にしている一つの要因



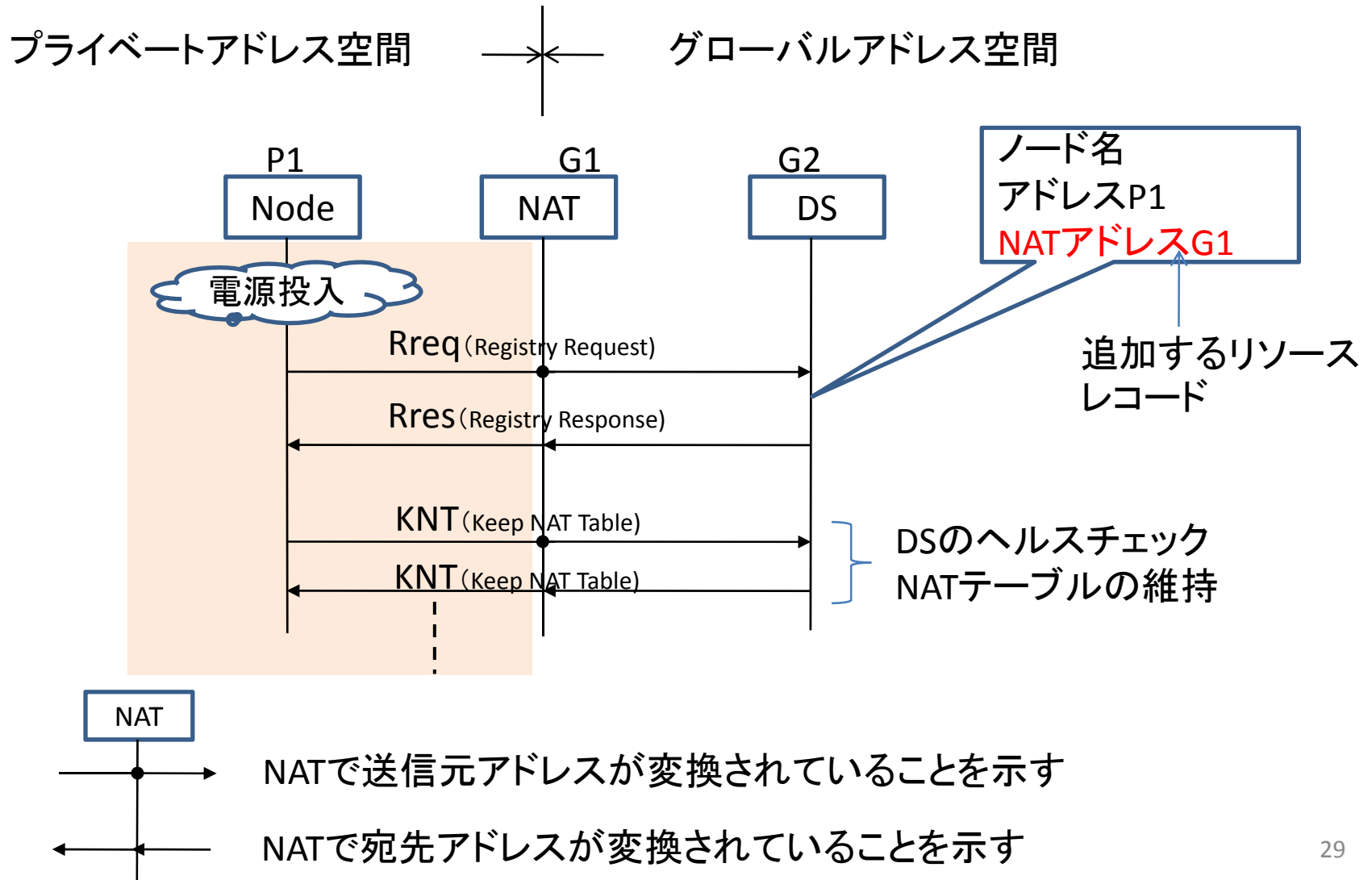
DS; Direction Server  
RS; Relay Server  
KMS; Key Management Server

## 前提

- ↔ エンドノードとDS間には信頼関係がある
- ↔ DSどうし、DSとRS間には信頼関係がある

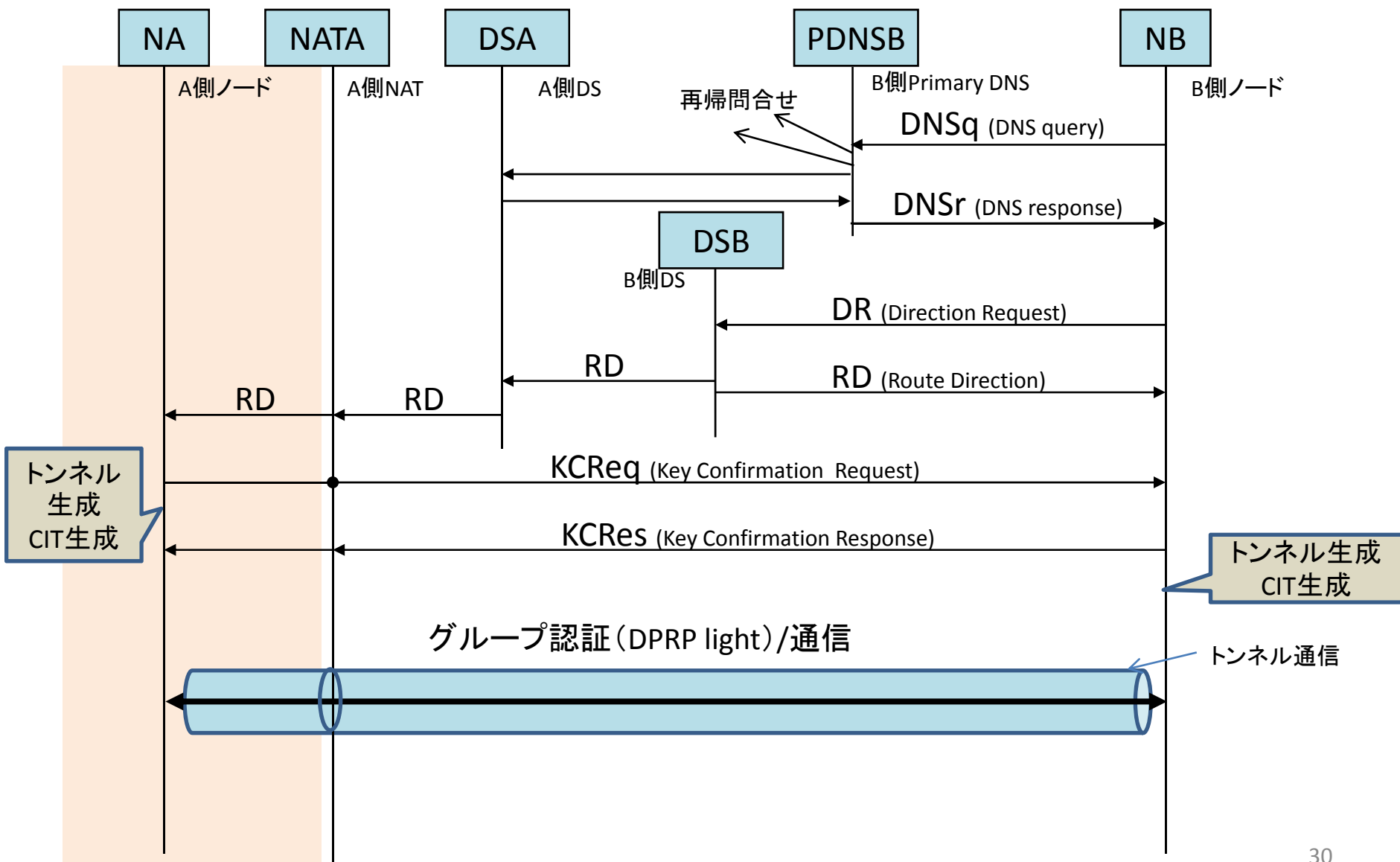
# 通信前の準備

電源立ち上げ時に、ホスト名とアドレスをDSに登録(Dynamic DNSと同じ)

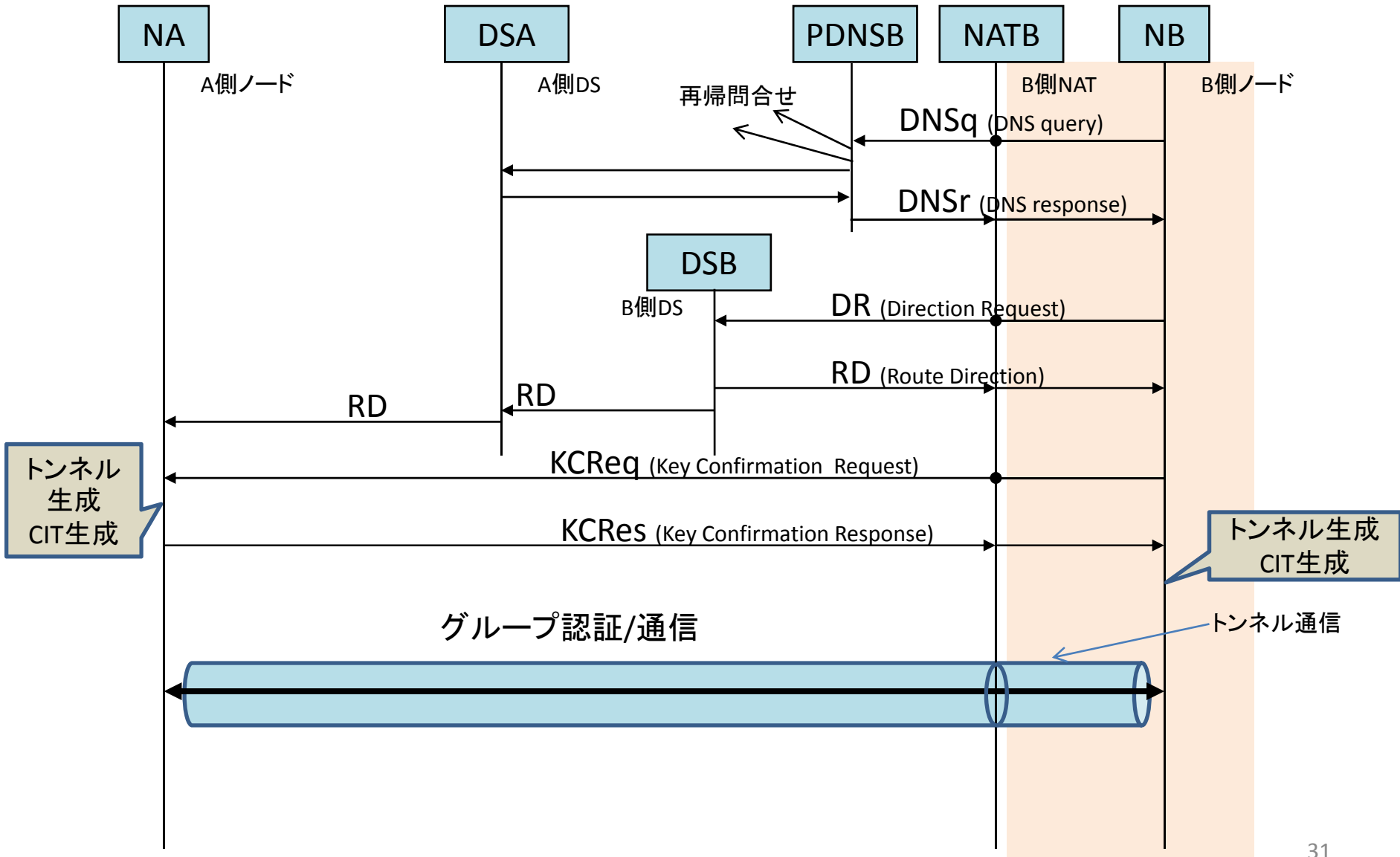


# NBから通信を開始する場合

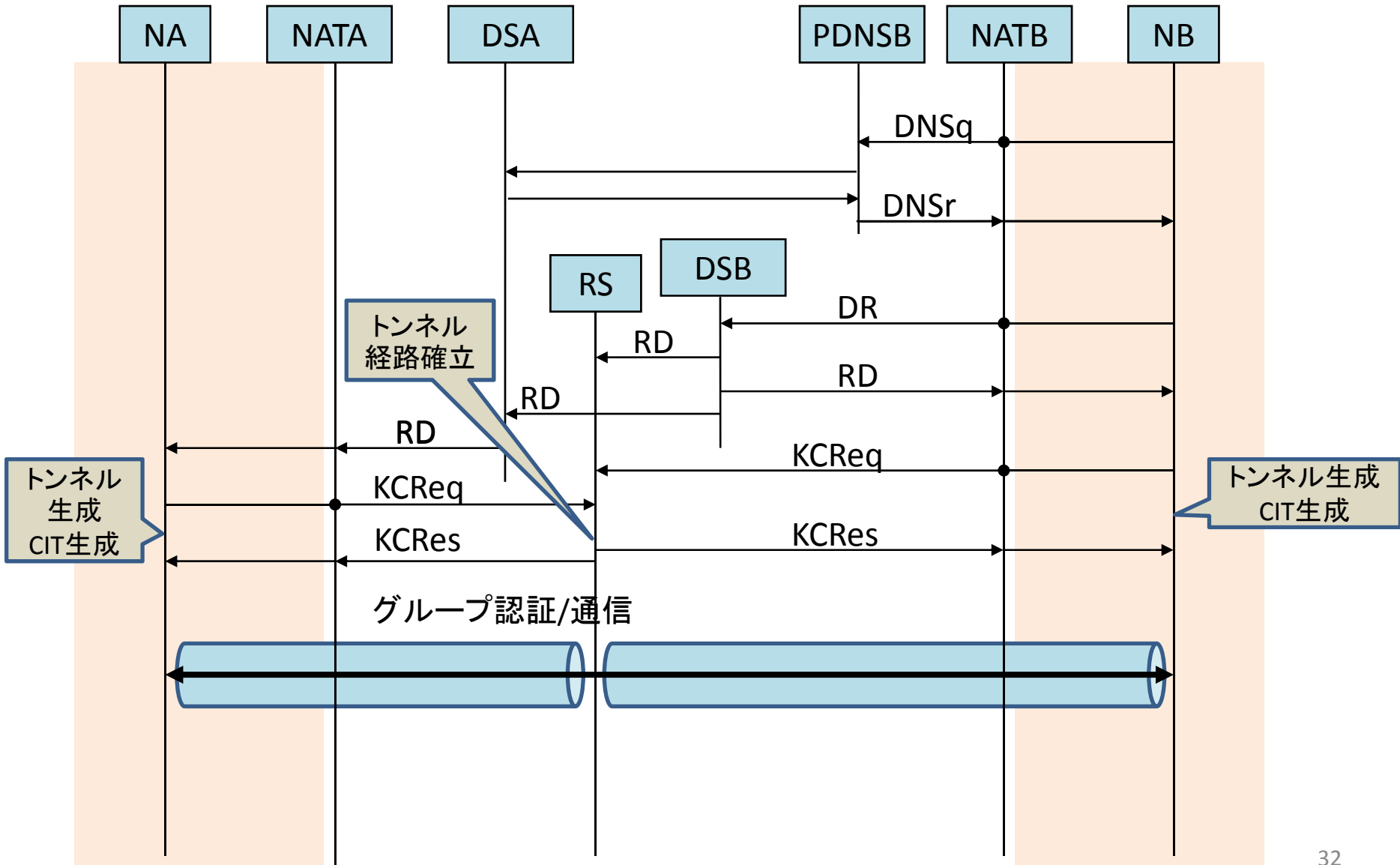
相手ノードNAがNAT配下



# NBがNAT配下

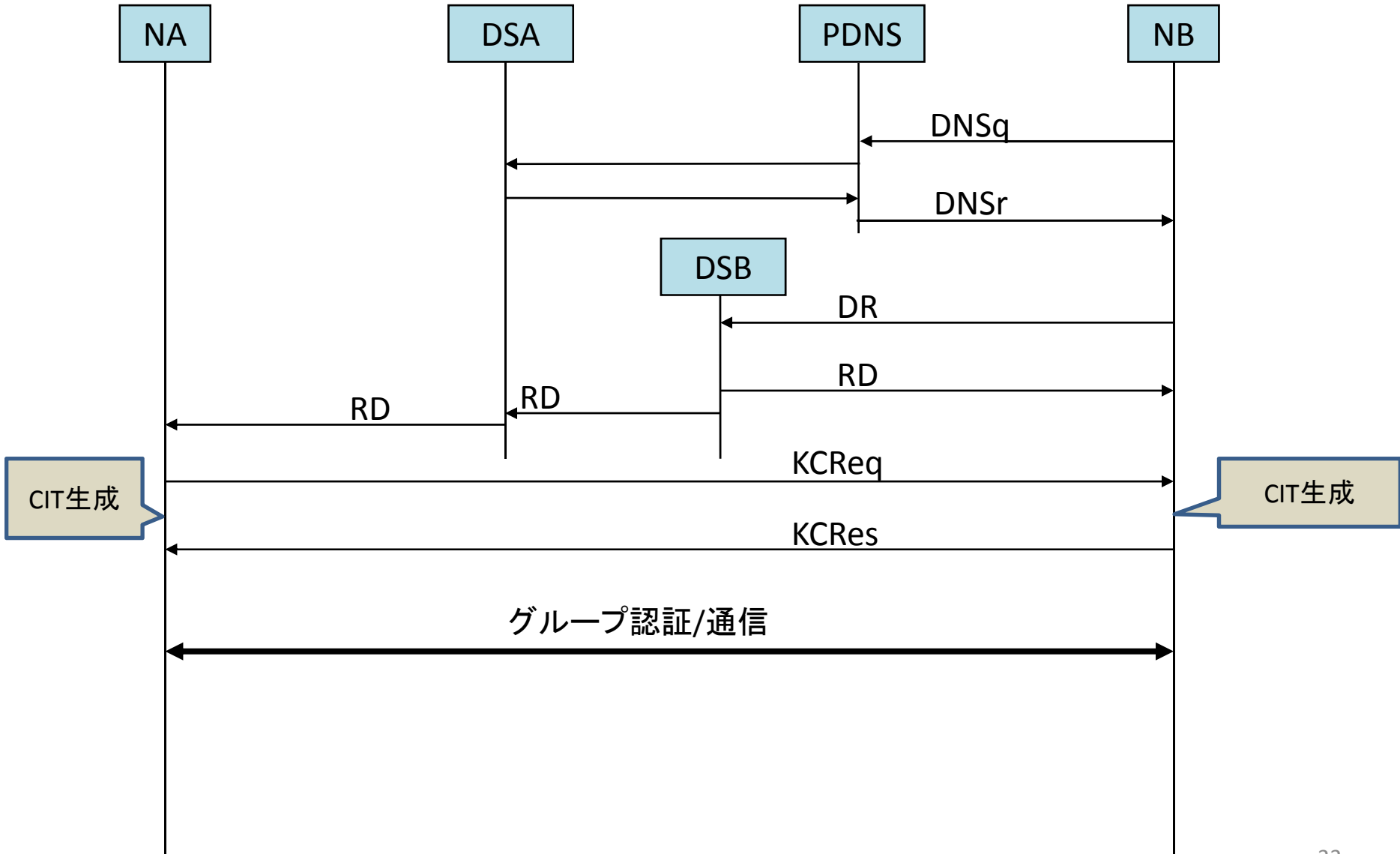


# 両エンドノードがNAT配下

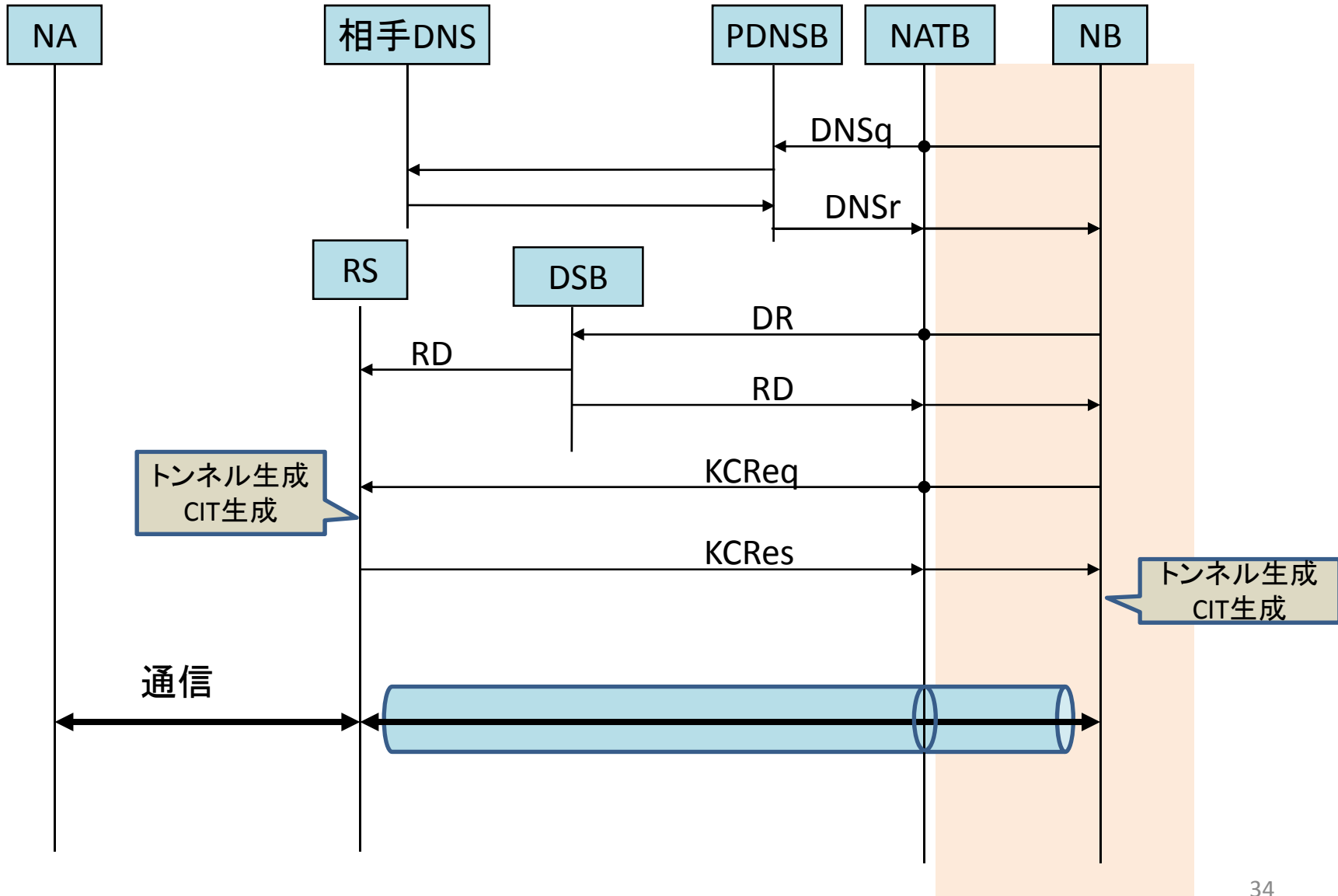




# 両ノード間にNATがない



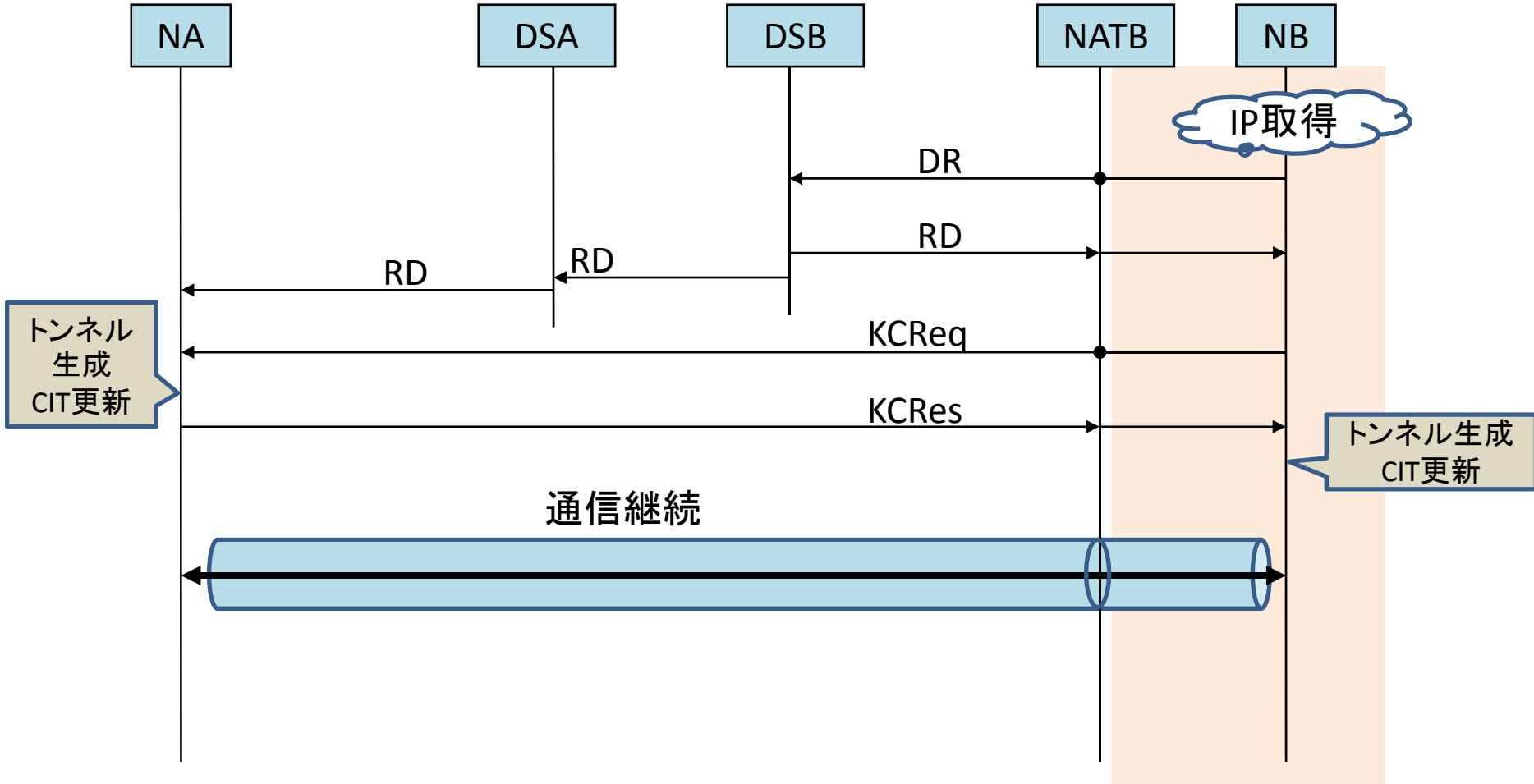
# 相手ノードNAが一般サーバ(グローバルアドレス)



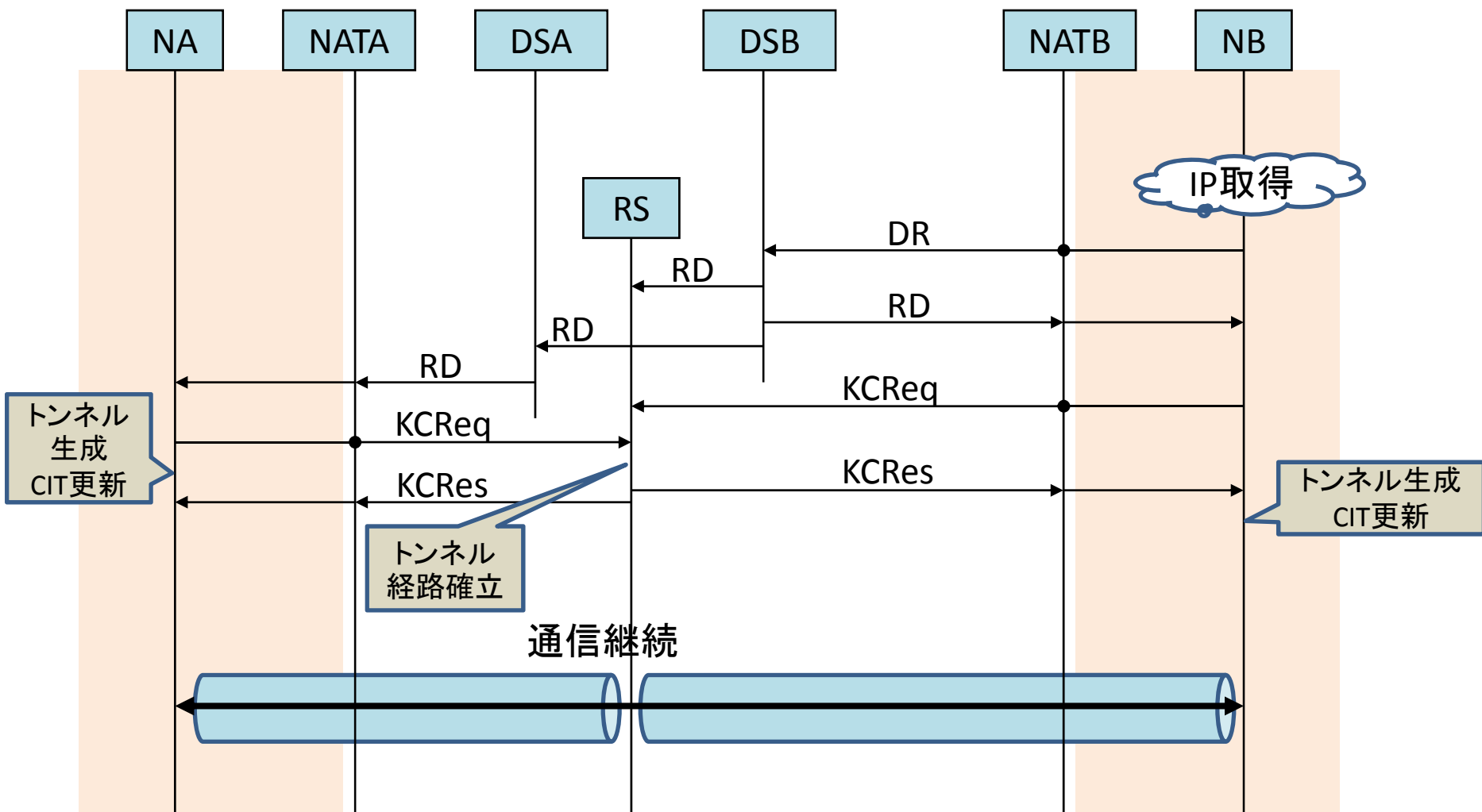
# NBが通信中に移動した場合

(DR以降のシーケンスは通信開始と全く同じ)

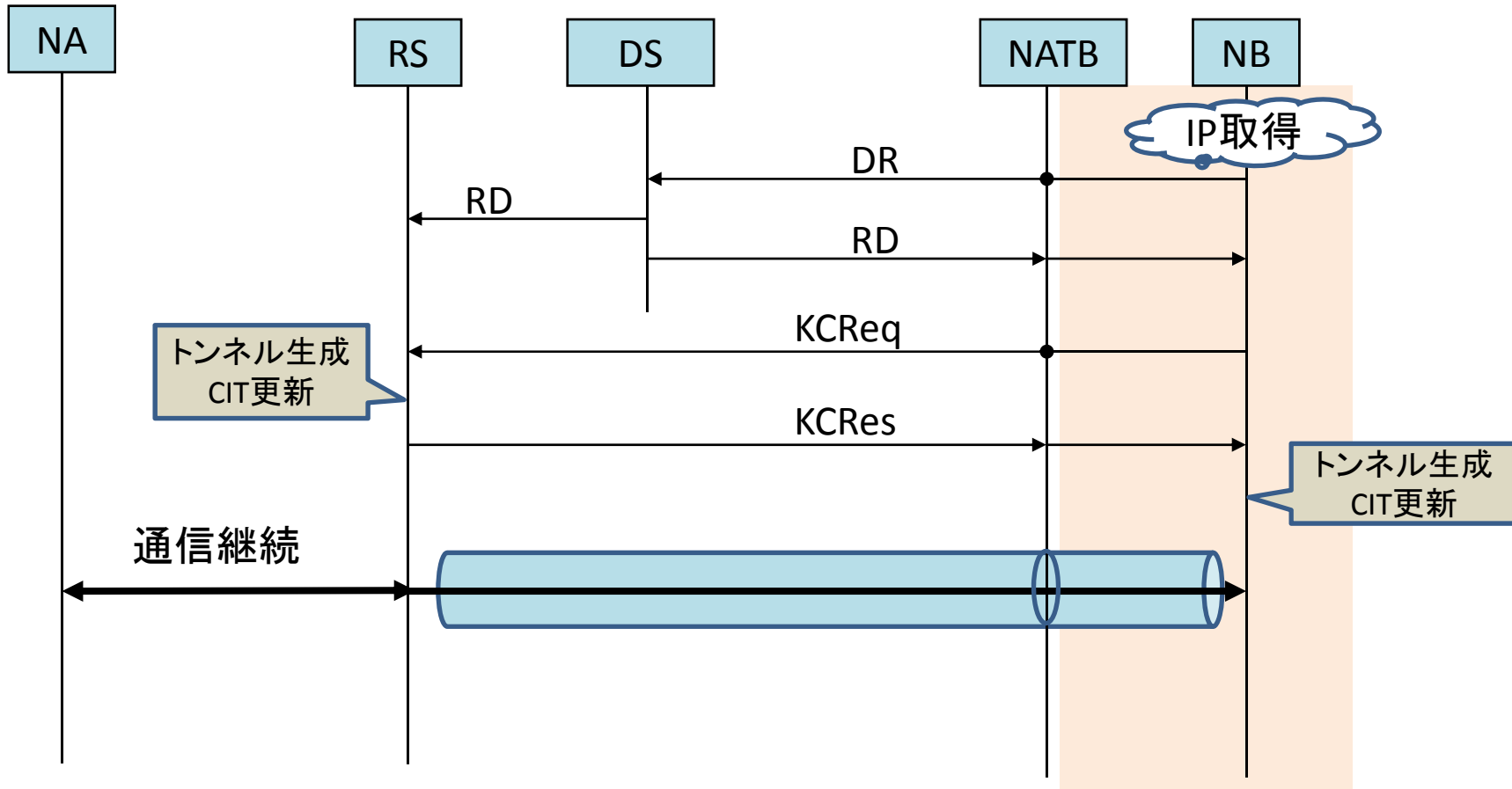
## NBがNAT配下に移動



# 両ノードがNAT配下に移動



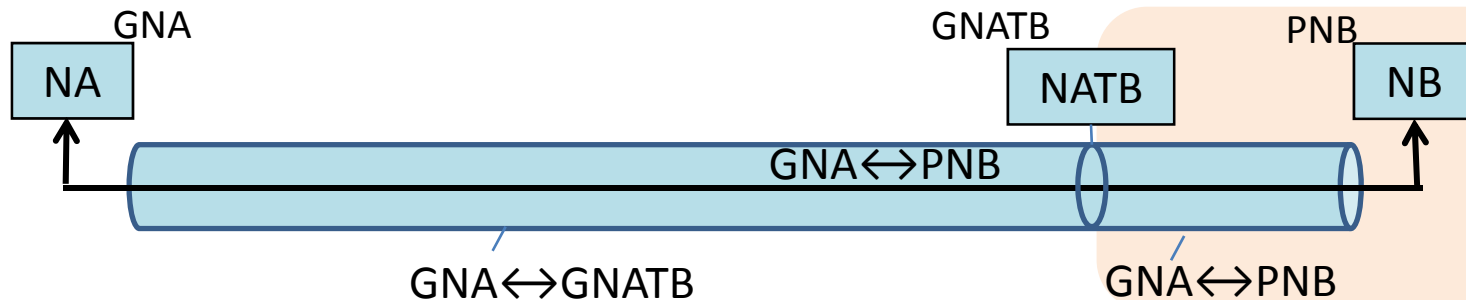
# 相手ノードNAが一般サーバで、NBがNAT配下に移動



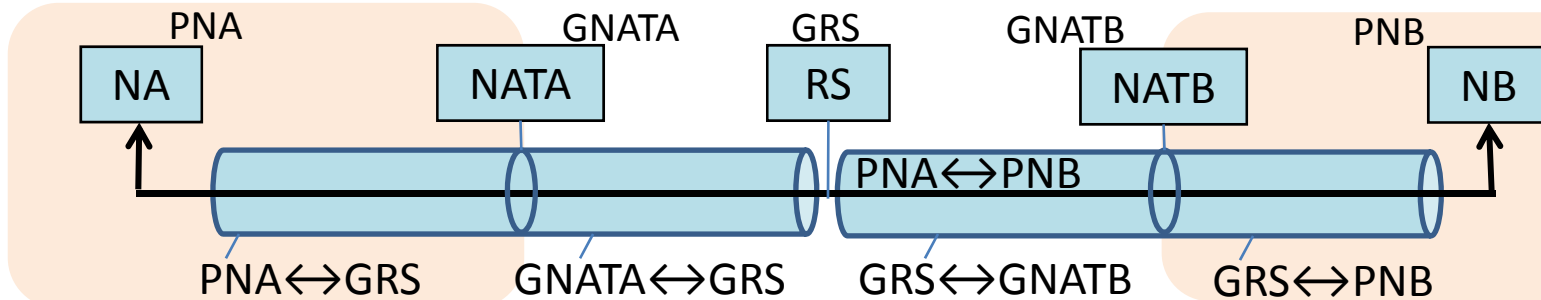
# アドレスが変化する様子



NBがNAT配下に移動



NAがNAT配下に移動



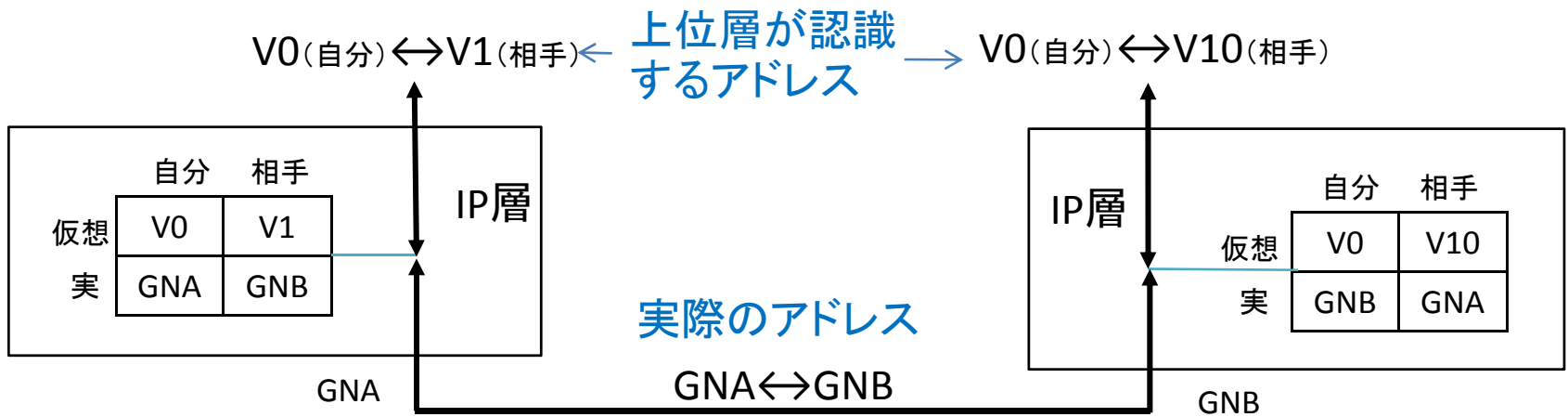
# 仮想アドレスの導入

上位層: 仮想アドレス(通信識別子とみなす)  
 下位層: 実アドレス(位置識別子とみなす) IP層でアドレス変換

## 仮想アドレスの例

自分のアドレスはV0 (固定値でよい)  
 相手のアドレスはV1, V2, ...

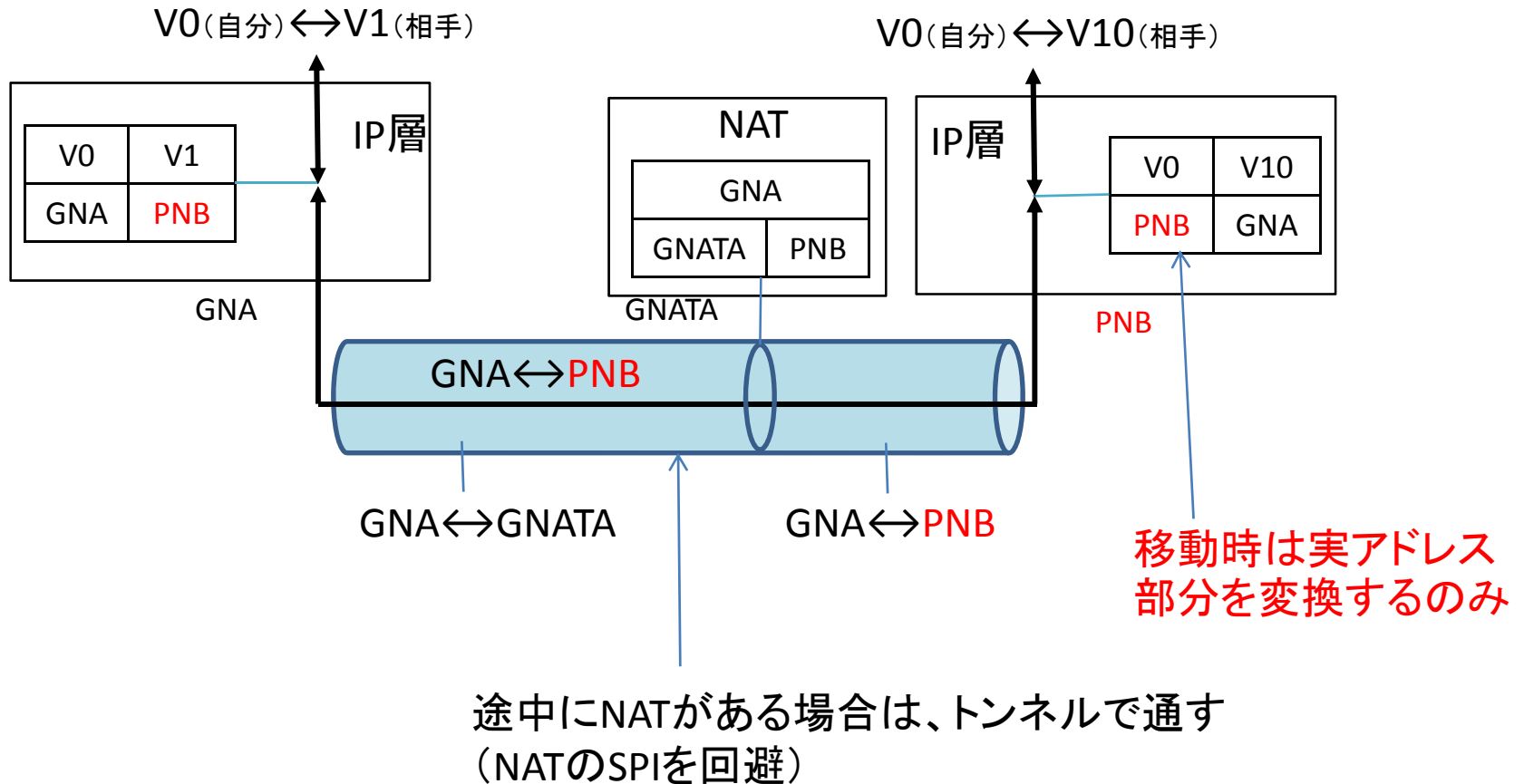
アドレス変換の表現方法  
 $\{V0 \leftrightarrow V1\} \Leftrightarrow \{GNA \leftrightarrow GNB\}$



NAT配下の複数の端末を識別できる  
 上位層では実アドレスの変化を気にしなくてよい  
 自分と相手のアドレスが同じであってもかまわない  
 (異なるプライベートアドレス空間の場合)

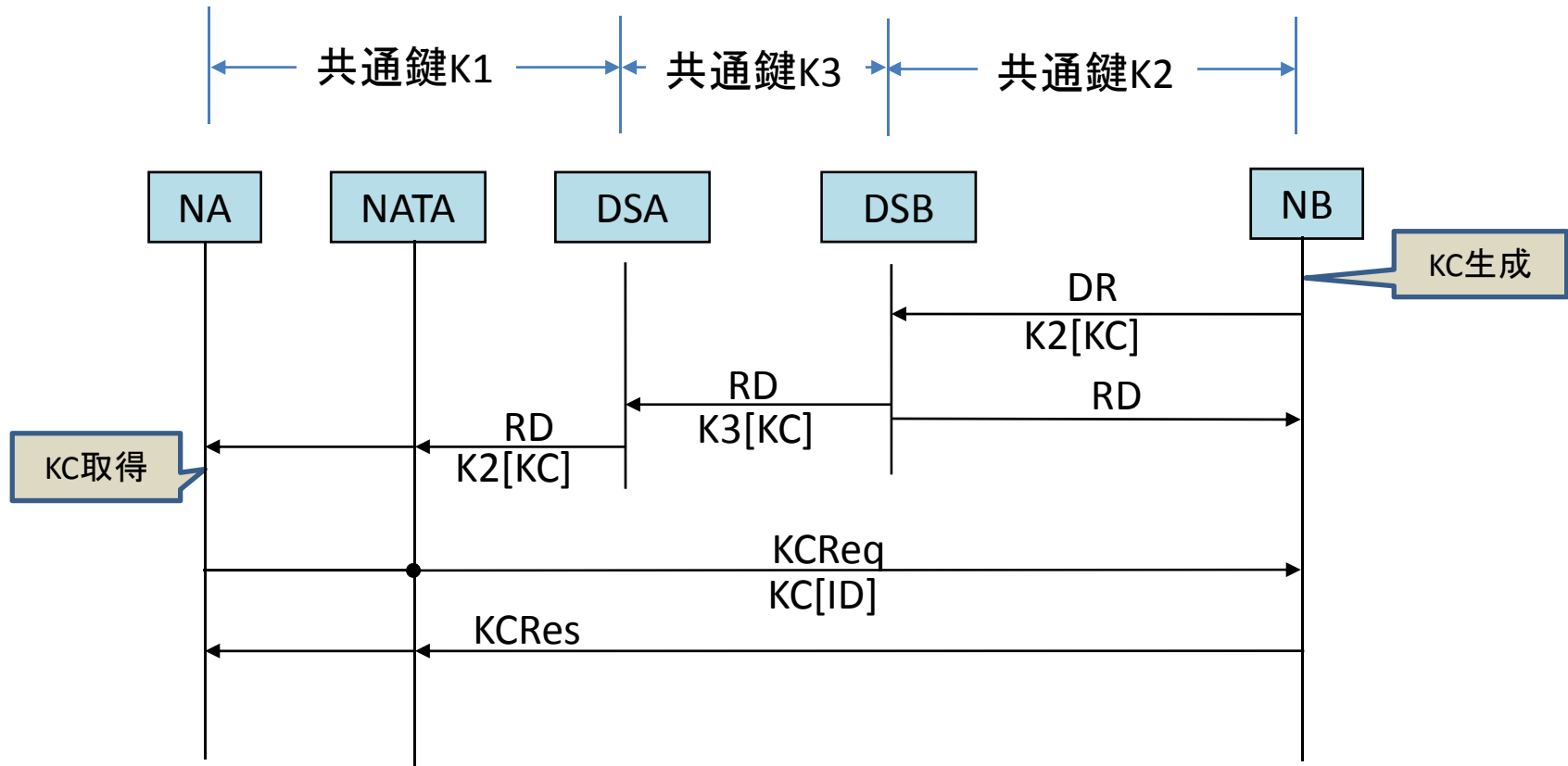
# 移動後のアドレス変換

NBがNAT配下に移動してアドレス変化 (GNB→PNB)





# エンドノード間の鍵共有の方法



# 鍵管理

事前共有鍵の設定、更新の考え方

DS-Node間

DSどうし, DS-RS間

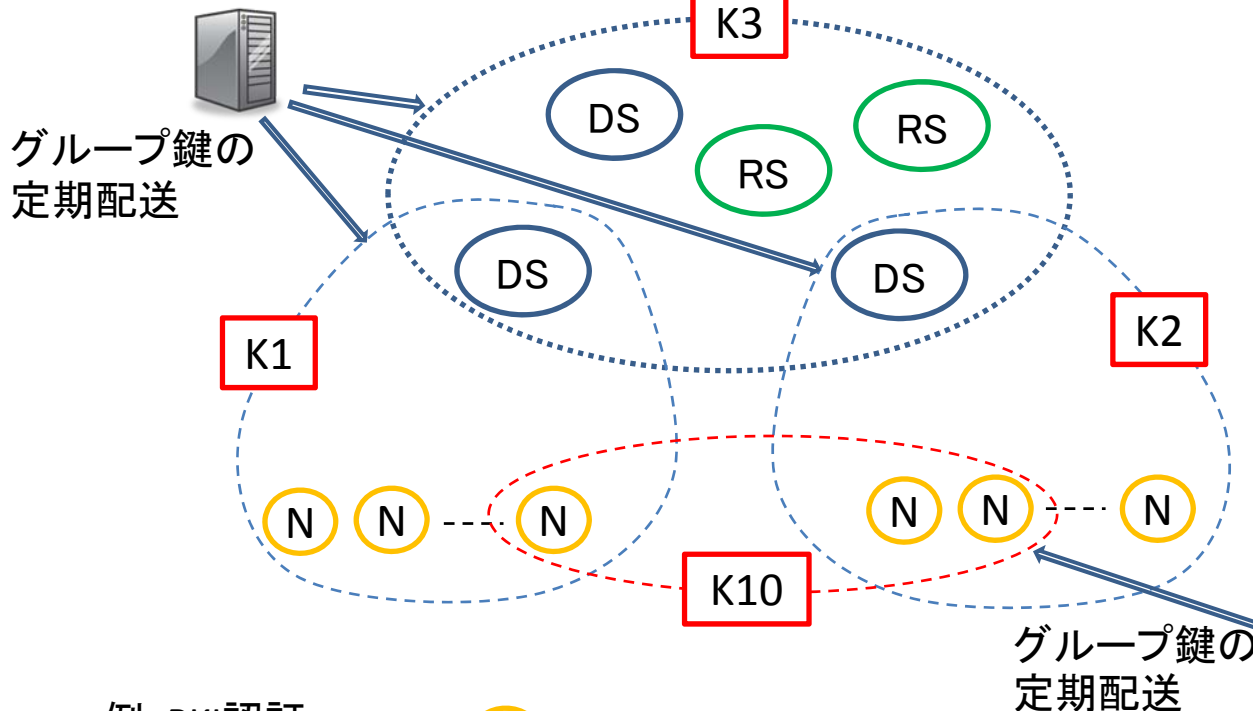
} プロバイダ側の管理

NTMobileシーケンス内で認証

ユーザグループの定義---ユーザ側の管理

DPRPにてグループ認証

プロバイダの鍵管理装置



例: PKI認証



既存の認証のしくみを利用してオフラインで配送

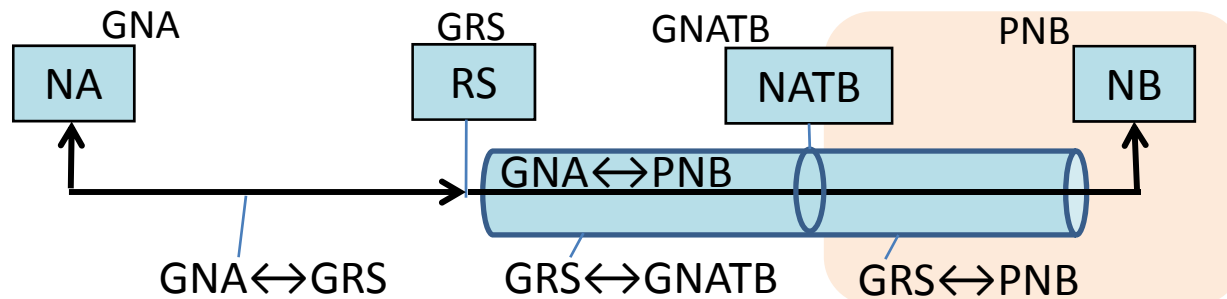
# 一般サーバとの通信方法

相手ノードが一般サーバの場合、RSがNATの役割を果たす

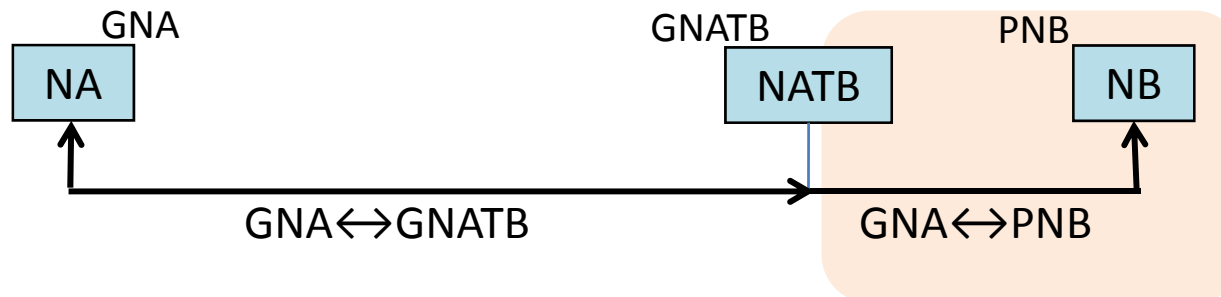
NA(一般サーバ)はRSを通信相手とみなす

NB側から通信を開始し、NBが移動しないことがわかっている場合は直接通信とする

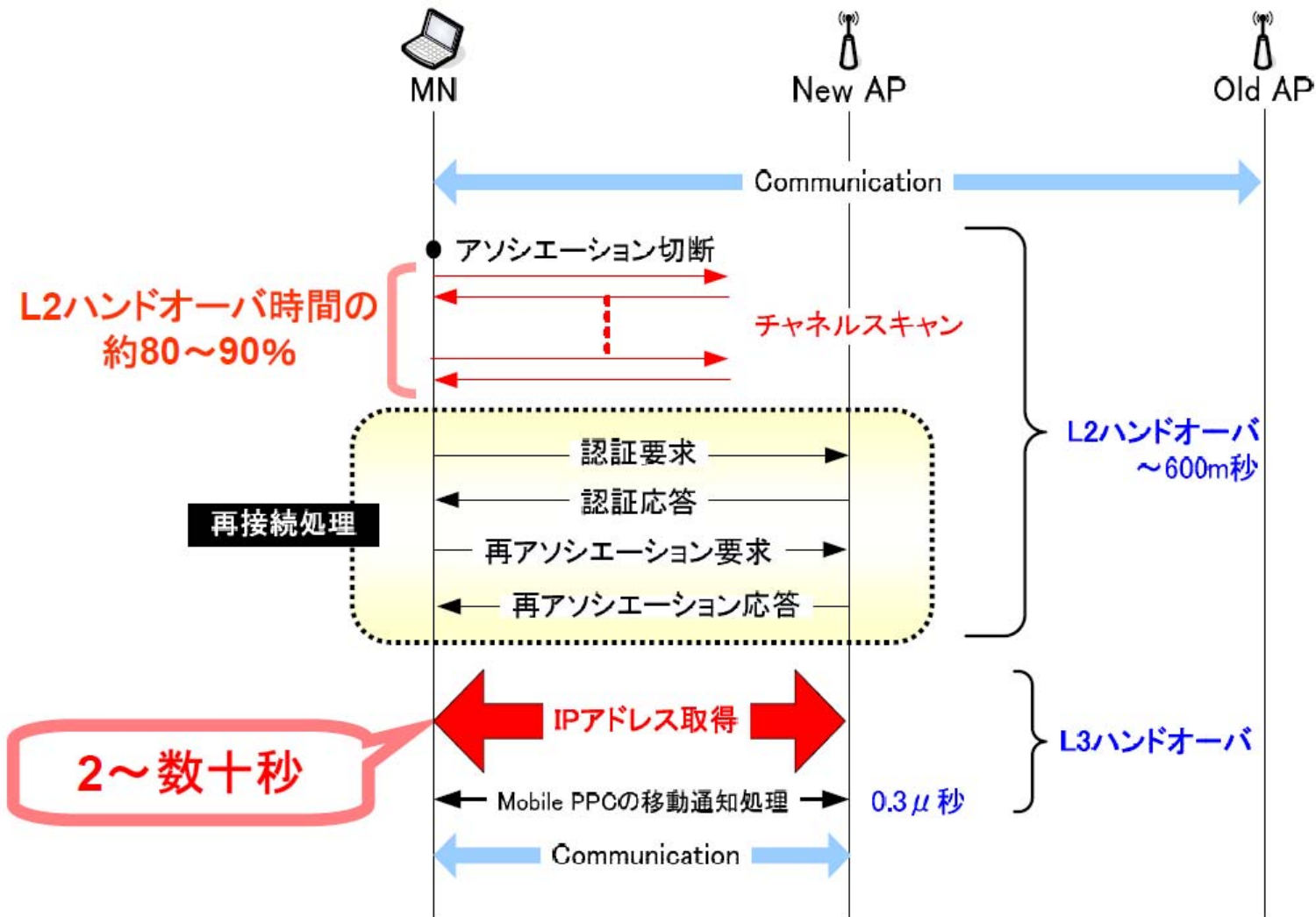
NBが移動する場合



NBが移動しないことがわかっている場合

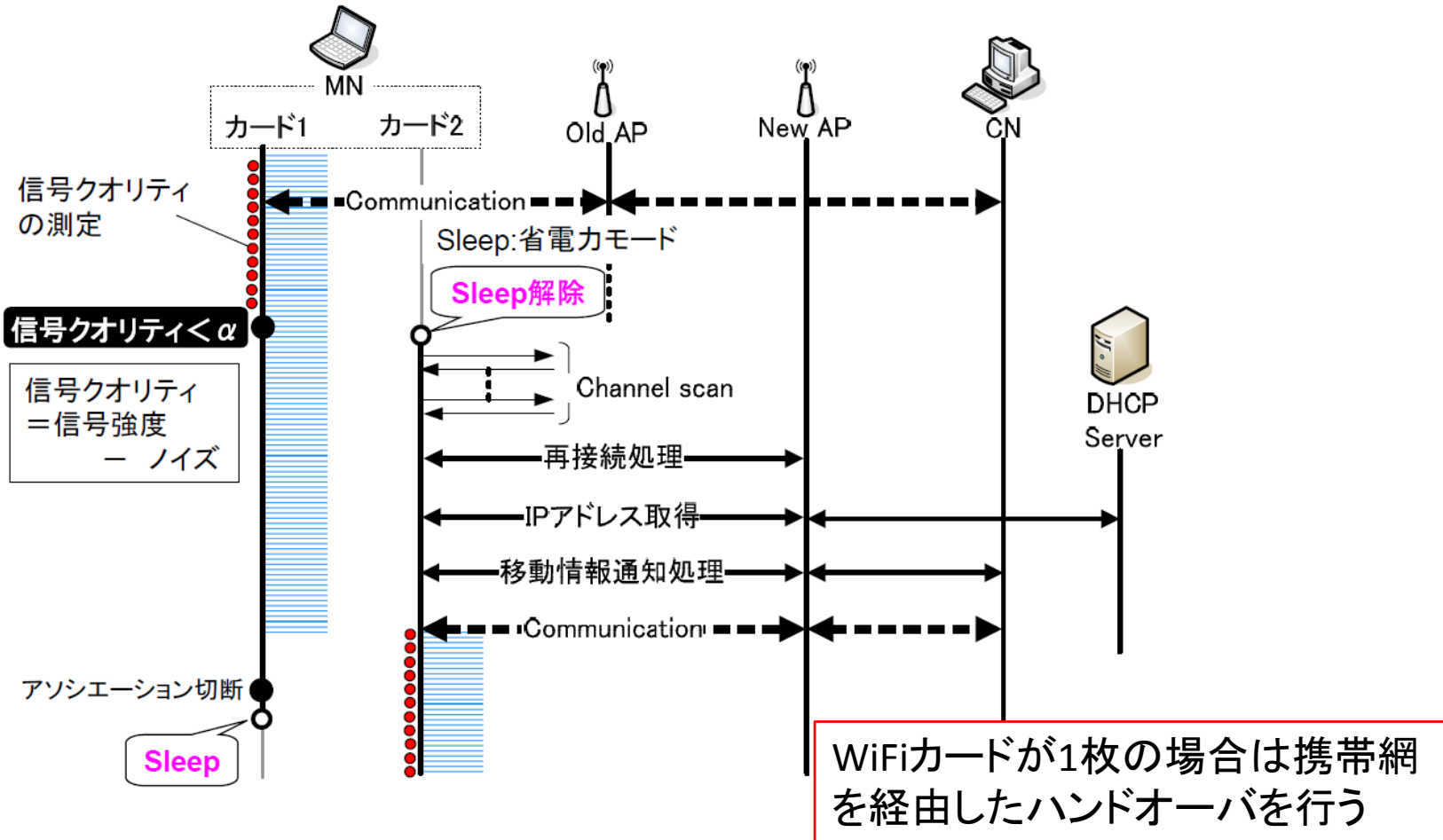


# 移動時の通信断絶について



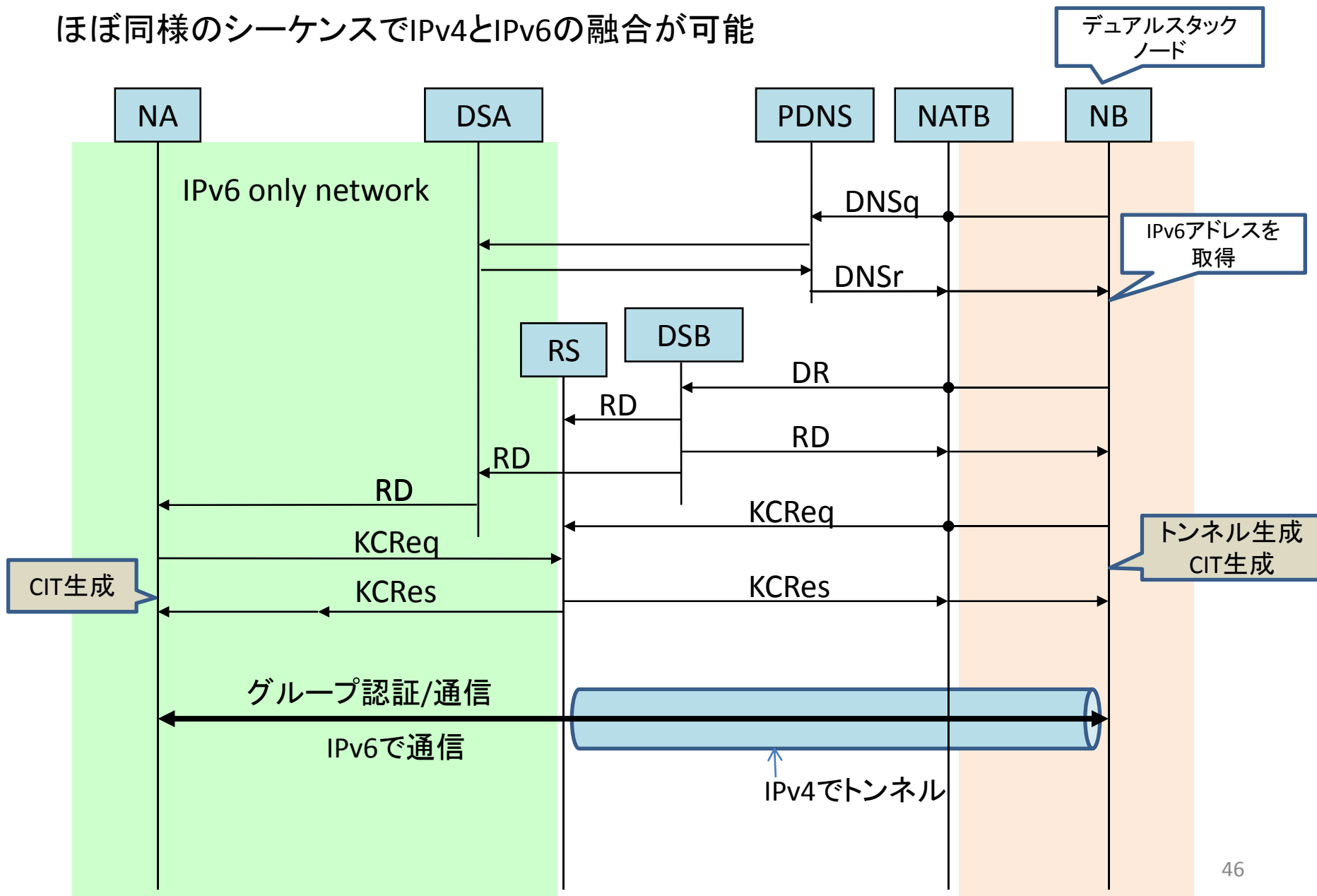
# 解決策：インタフェースカードを2枚使用

- ・カード1で通信開始。カード2はスリープモード
- ・移動時はカード2によりハンドオーバーを実行
- ・移動後はカード2で通信

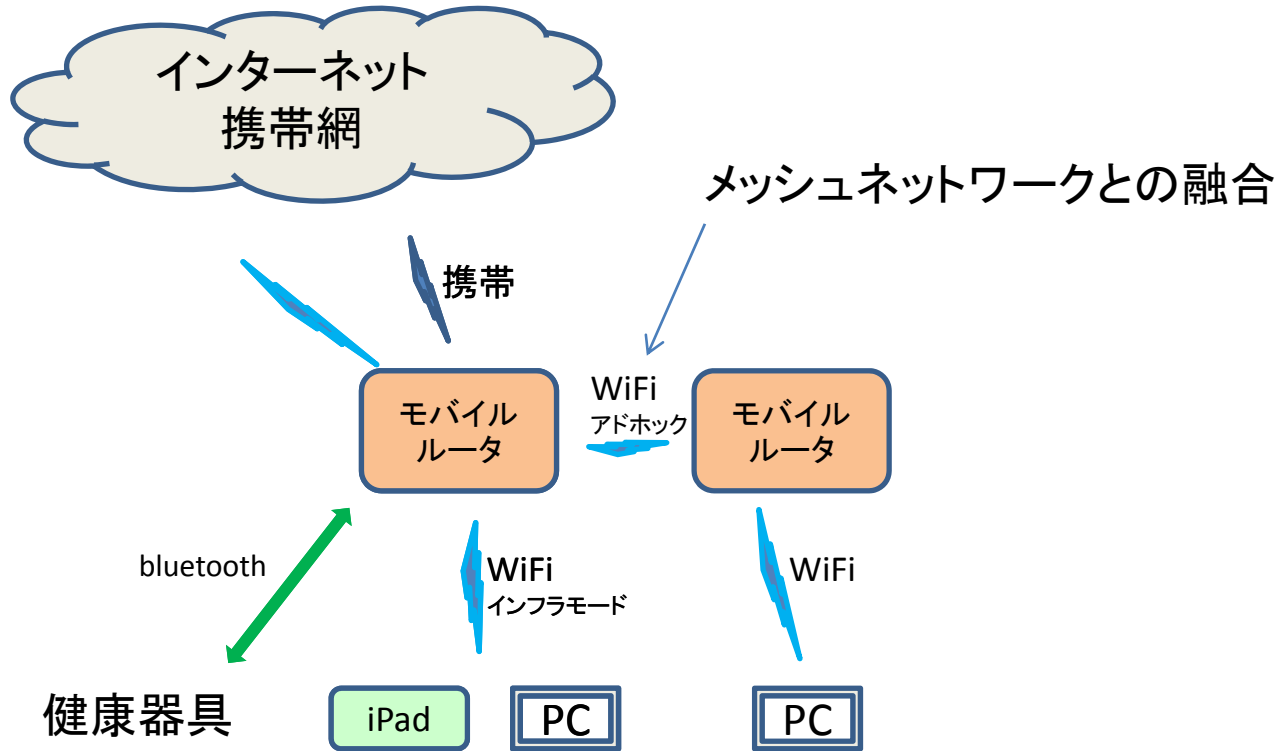


# IPv4/IPv6共存ネットワークへの発展

ほぼ同様のシーケンスでIPv4とIPv6の融合が可能



# モバイルルータへの発展



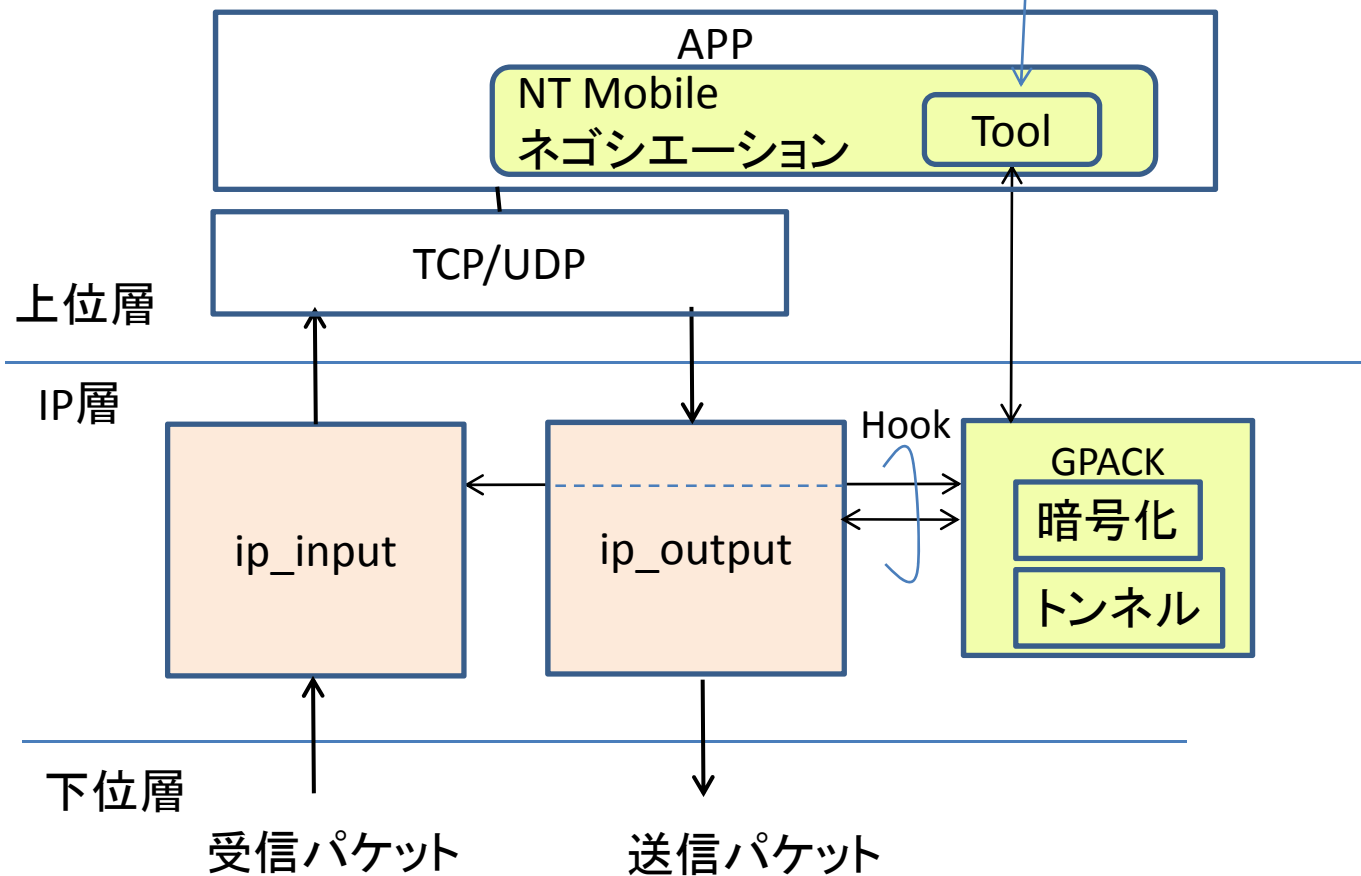
かばんにMRを入れてネットワークを持ち歩く



車に搭載して、車車間通信に利用  
WiFiが届けばメッシュネットワークで直接車車間通信  
届かないときはインターネット/携帯網経由で通信

# 実装

暗号鍵、トンネルヘッダ  
の設定を行うツール



NT Mobileネゴシエーションはアプリケーションで実現  
暗号化とトンネル処理はIP層で実現  
既存カーネルの改造はGPACKの呼出部分のみ



## 関連論文一覧:

- [1] 竹内 元規, 鈴木 秀和, 渡邊 晃, 「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.
- [2] 鈴木 秀和, 渡邊 晃, 「フレキシブルプライベートネットワークにおける動的処理解決プロトコルDPRPの実装と評価」, 情報処理学会論文誌, Vol.47, No.11, pp.2976-2991, Nov.2006.
- [3] 増田 真也, 鈴木 秀和, 岡崎 直宣, 渡邊 晃, 「NATやファイアウォールと共存できる暗号通信方式PCCOMの提案と実装」, 情報処理学会論文誌, Vol.47, No.7, pp.2258-2266, Jul.2006.
- [4] 鈴木 秀和, 宇佐見 庄五, 渡邊 晃, 「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.
- [5] 鈴木 秀和, 渡邊 晃, 「プライベートネットワーク内のノードを通信相手とした移動透過性の実現方式」, 電子情報通信学会論文誌(B), Vol.J92-B, No.1, pp.13, Jan.2009.
- [6] 金本 綾子, 鈴木 秀和, 伊藤 将志, 渡邊 晃, 「IPv4移動体通信システムにおけるパケットロスレスハンドオーバーの提案」, 情報処理学会論文誌, Vol.50, No.1, pp.133-143, Jan.2009.
- [7] 坂本 順一, 鈴木 秀和, 伊藤 将志, 宇佐見 庄五, 渡邊 晃, 「プライベートアドレスによるネットワークモビリティを実現するMobile NPCの提案」, 情報処理学会論文誌, Vol.50, No.10, pp.1-13, Oct.2009.
- [8] 瀬下 正樹, 鈴木 秀和, 伊藤 将志, 渡邊 晃, 「分割Diffie-Hellman鍵交換による移動ノードの鍵共有方式の提案」, 情報処理学会論文誌, Vol.50, No.7, pp.1725-1734, Jul.2009.
- [9] 鈴木秀和, 渡邊晃, 「通信グループに基づくサービスの制御が可能なNAT越えシステムの提案」, 情報処理学会論文誌, Vol.51, No.9, pp.1-11, Sep.2010.
- [10] 宮崎悠, 鈴木秀和, 渡邊晃, 「端末の改造が不要なNAT越え通信NTSSの提案と評価」, 情報処理学会論文誌, Vol.51, No.9, pp.1234-1241, Sep.2010.
- [11] 伊藤 将志, 鹿間 敏弘, 渡邊 晃, 「無線メッシュネットワーク”WAPL ”の提案とシミュレーション評価」, 情報処理学会論文誌, Vol.49, No.6, pp.1859-1871, Jun.2008.