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
2010,9,3

名城大学
渡邊

研究背景

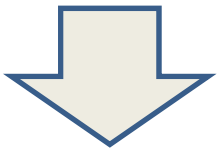
モバイル通信の発展が予想される
IPv4には、様々な通信の制約がある
- NAT越え問題
- 移動透過性
- エンドエンドのセキュリティ

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

・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）
　－IPv4で蓄積したノーハウがある
　－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

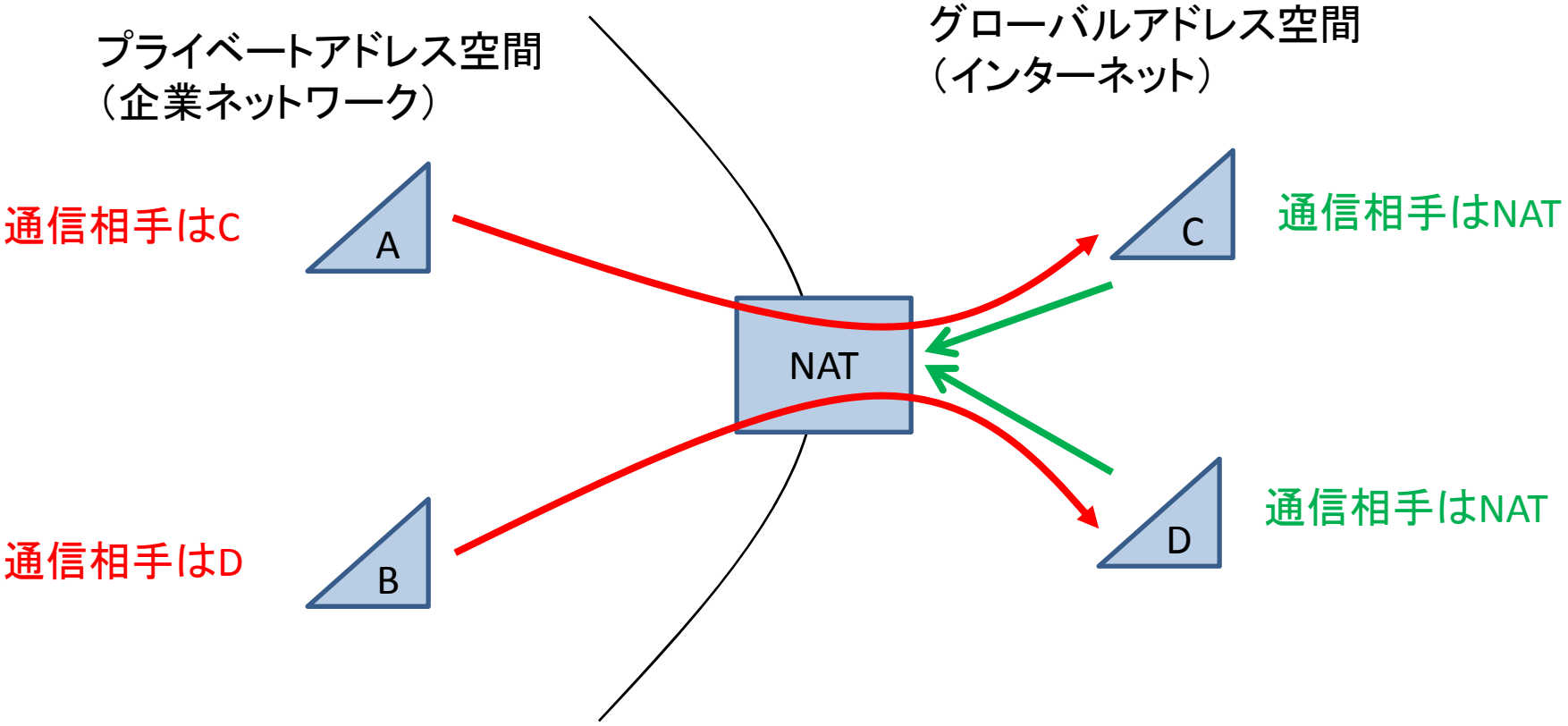
IPv4における通信の制約を除去する
　NAT越え問題の解決
　通信中の自由な移動
そのうえで、エンドエンドのセキュリティを確保する

条件：

・現状のネットワーク環境を変えない（エンドエンドだけで対応）
・スケーラビリティがある
・一般端末の混在が可能（上位互換性）
・IPv6との共存に向けた発展性がある
・性能が劣化しない

IPv4の最大の課題：NAT越え問題

インターネット側（NATの外側）からの通信開始ができない



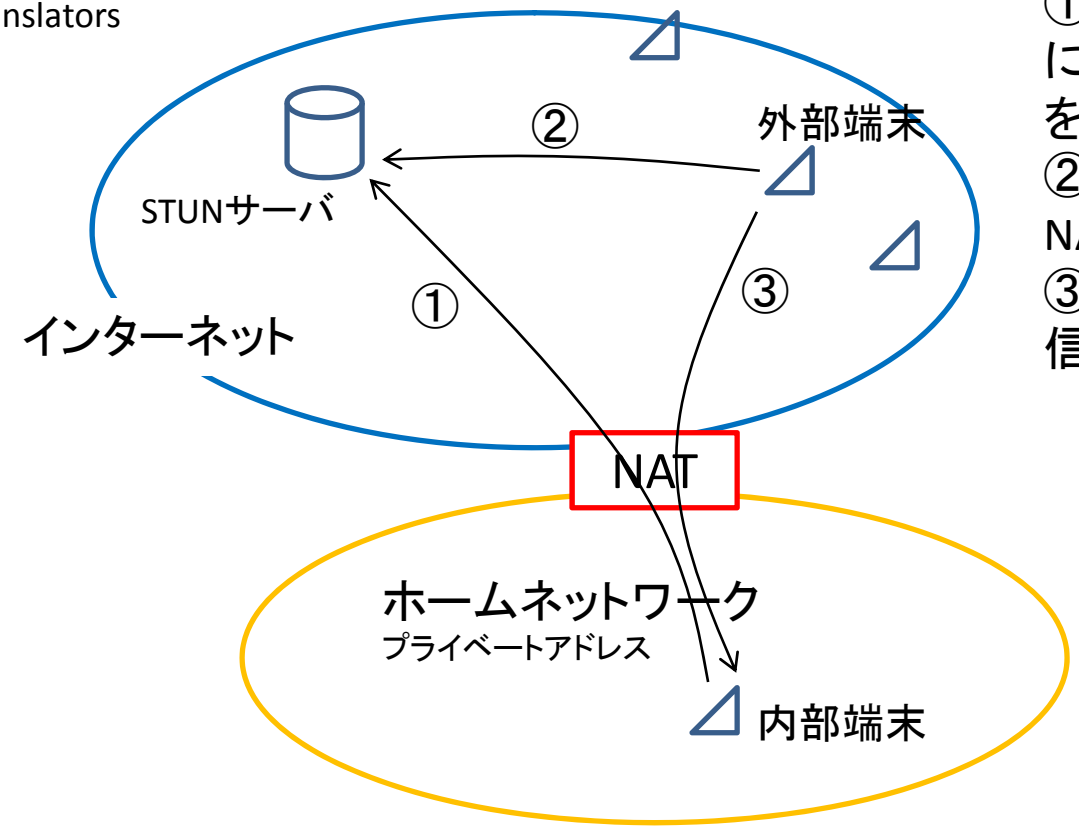
NAT; Network Address Translation

NAT越え技術の例とその課題

既存技術

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）
・端末の移動は全く考慮していない

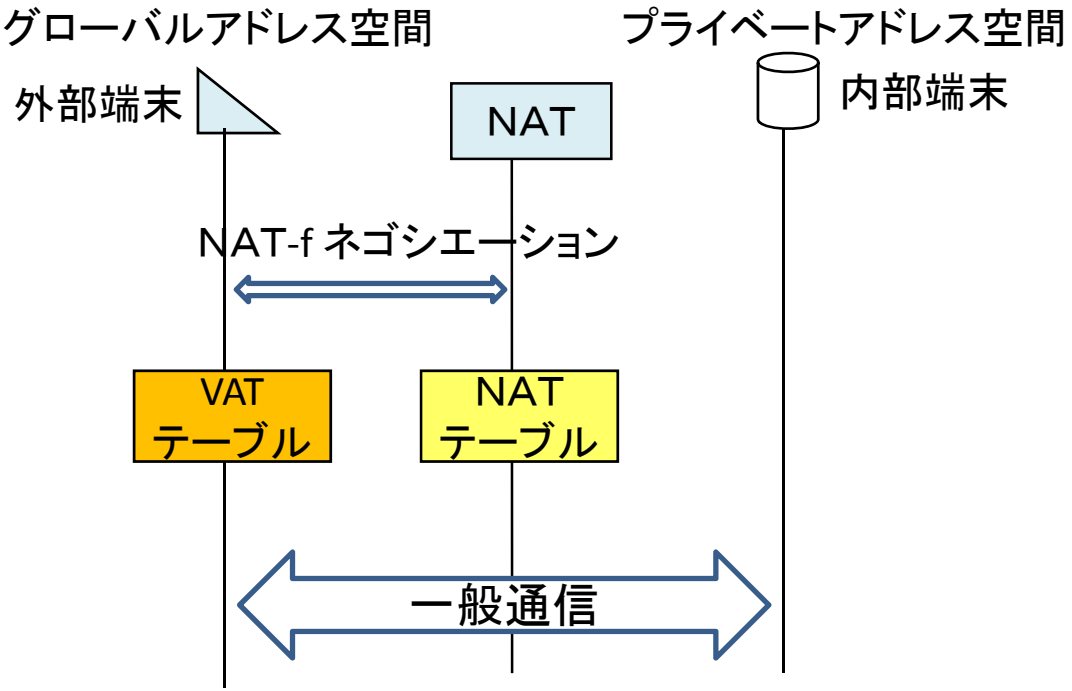
提案済み技術

NAT-f (NAT-free Protocol)

NATと、外部端末（GA）のカーネルを改造することによりNAT越え問題を解決(*)

・通信開始時に、NATと外部端末がNATテーブルの情報を交換する（NAT-fネゴシエーション）。

・NATテーブルの内容に合わせて、外部端末のカーネル内でパケットのアドレス/ポート番号を変換する。



VAT; Virtual Address Translation table

開発済み、または開発中のNAT越え技術

①NAT-f (NAT-free protocol)

NATと外部端末のカーネルを改造
通信に先立ちNATと外部端末がネゴシエーションを行いNATテーブルを強制的に生成

[1]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.
[2]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.

②NTSS (NAT Traversal Support System)

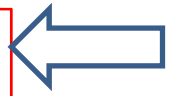
DNSサーバとNATを改造。エンド端末は変更なし
通信に先立ち、DNSサーバとNATがネゴシエーションを行いNATテーブルを強制的に生成

[3]宮崎 悠，鈴木 秀和，渡邊 晃，「端末の改造が不要なNAT越え通信システム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.

③NTMobile (NAT Traversal with Mobile)

エンド端末のカーネルを改造（NATは改造しない）
通信に先立ちエンド端末と指示サーバが連携してNATテーブルを生成

開発中



今回の開発

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

移動透過性技術とは：

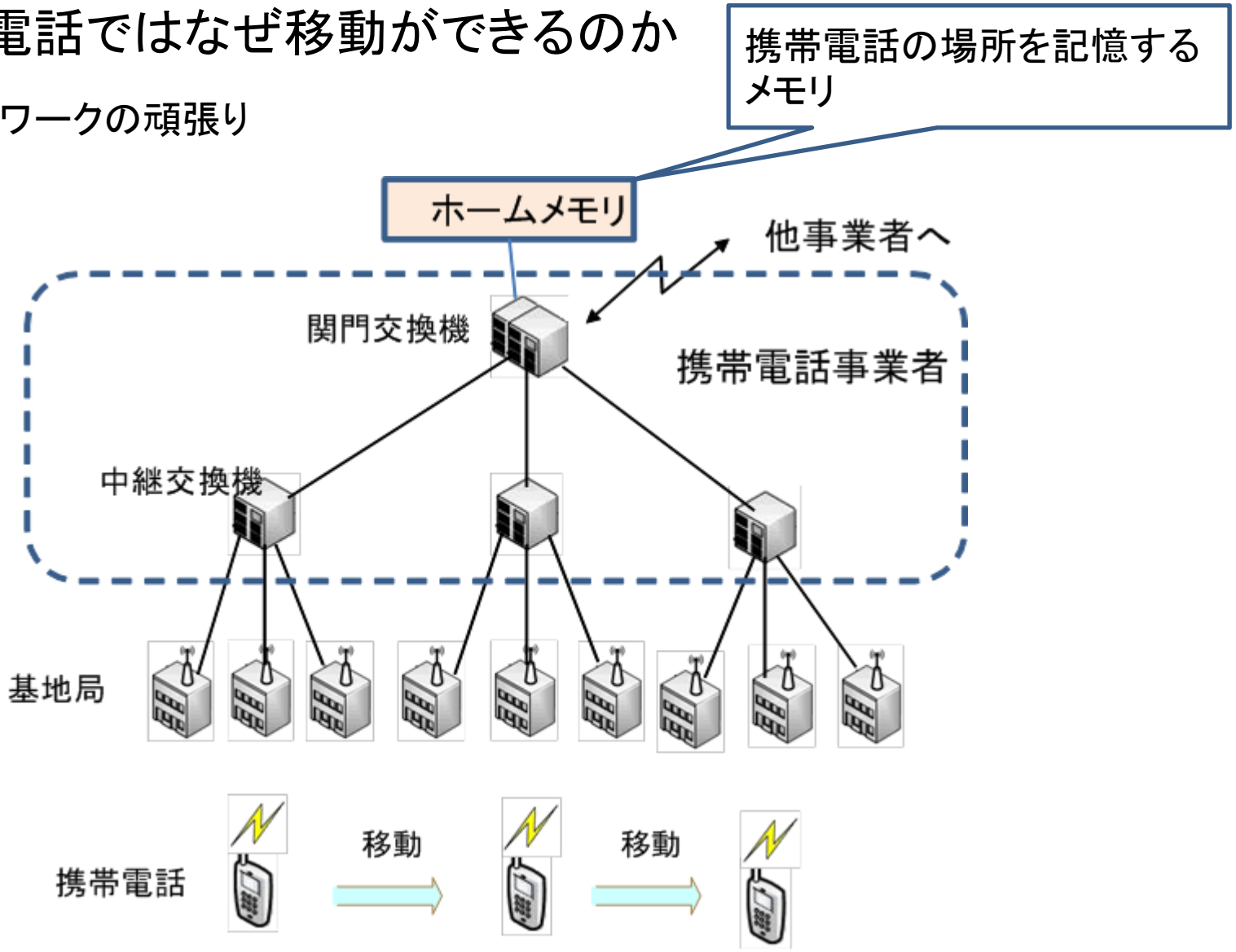
通信中にIPアドレスが変わっても通信の継続を可能とする技術

・パケットを正しくルーティングできる

・上位ソフトウエアはIPアドレスの変化に気付かない

携帯電話ではなぜ移動ができるのか

ネットワークの頑張り

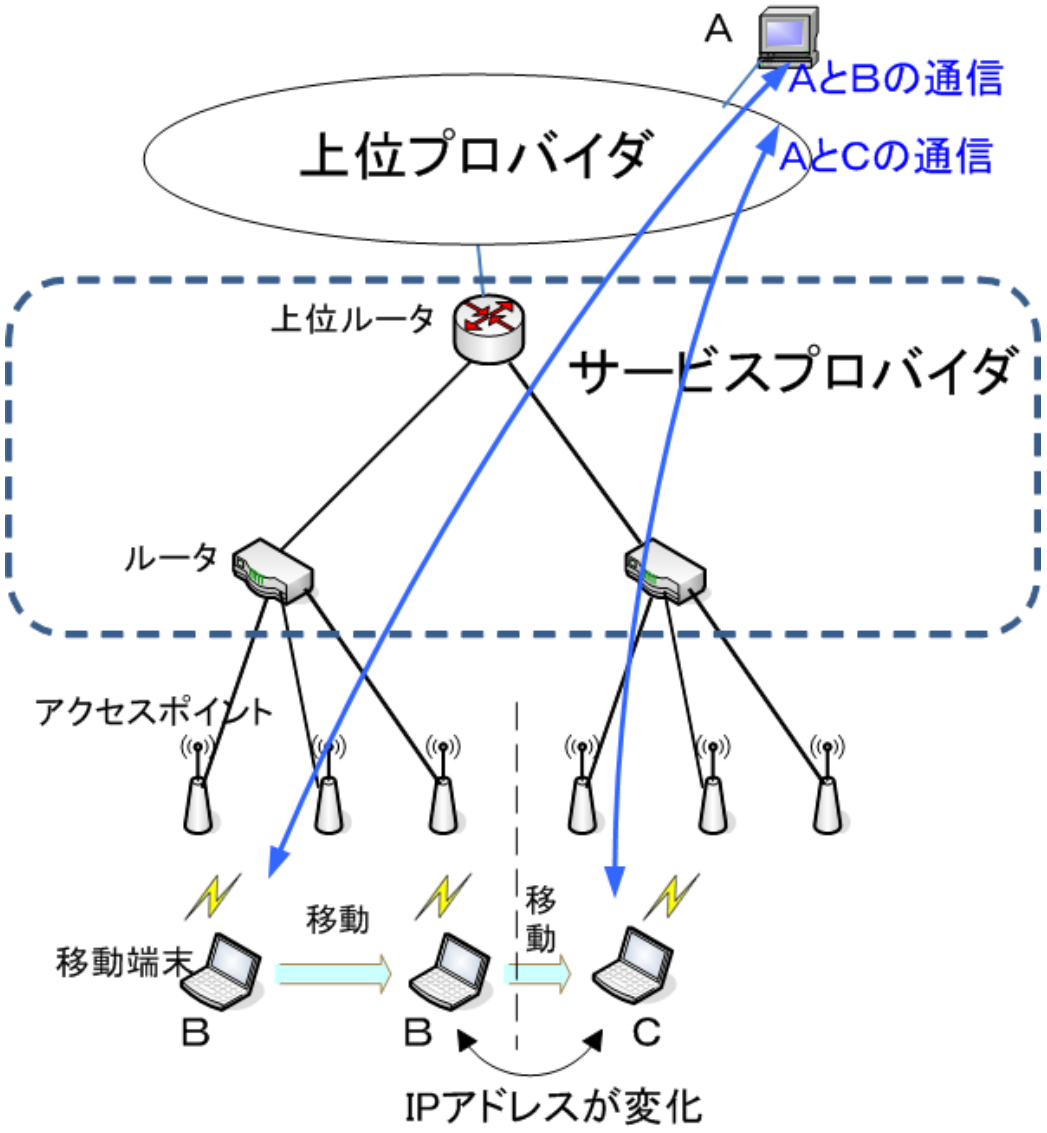


電話番号は変わらない

電話番号とIPアドレスをマッピングすることにより、IPアドレスを変化させないまま場所を移動できる

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

↓

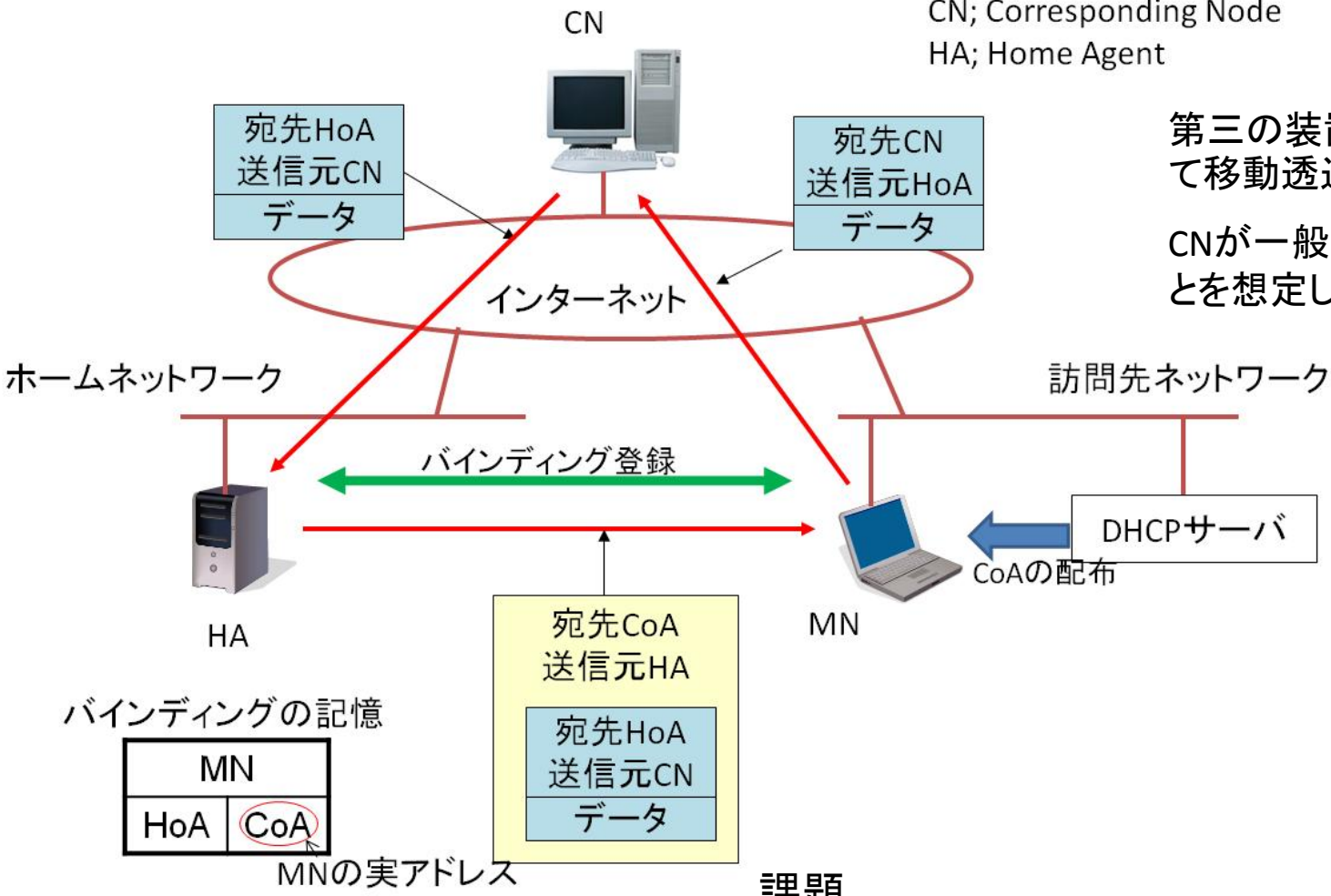
アドレスが異なると違う通信とみなされる

既存技術の例とその課題

既存技術

Mobile IP

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

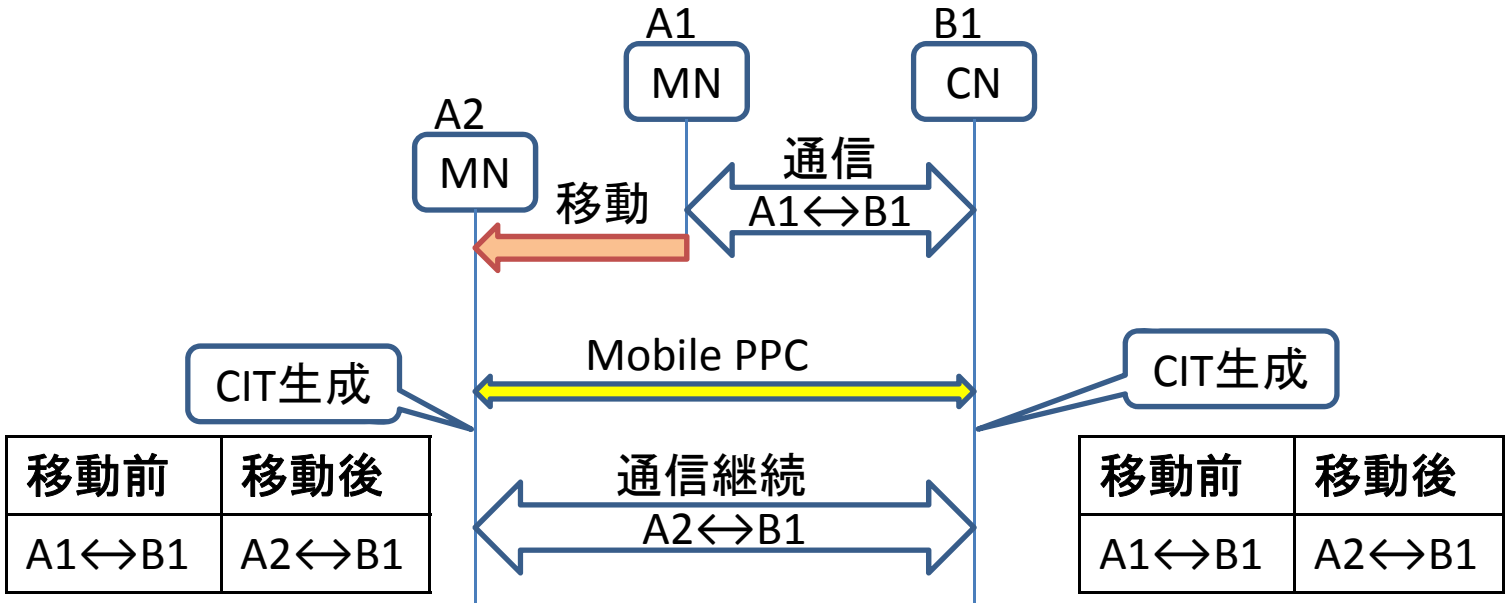
CNが一般サーバであることを想定した技術

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

MobilePPC (Mobile Peer to Peer Communication)

提案済み技術

エンド端末間で直接アドレスの変化情報を交換
IP層内に共通のアドレス変換テーブル（CIT）を生成し、IPパケットのアドレス変換を行う
　上位アプリケーションはA1↔B1の通信と認識
　ネットワーク上はA2↔B1の通信



移動前	移動後
A1↔B1	A2↔B1

移動前	移動後
A1↔B1	A2↔B1

・HAが不要
・高スループット
・不正パケットの心配なし

CIT (Connection ID Table)；IP層におけるアドレス変換テーブル

開発済みまたは開発中の移動透過性技術

①Mobile PPC (Mobile Peer to Peer Communication)

エンド端末のカーネルを改造
移動時にエンドノードが情報交換し、IP層にアドレス変換テーブルを生成

[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]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
[3]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.

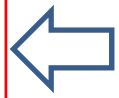
②ロスレスハンドオーバ

移動端末のカーネルを改造
通信インタフェースを2枚搭載し、ロスレスのハンドオーバを実現

[4]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の提案」，情報処理学会論文誌，Vol.50，No.1，pp.133-143，Jan.2009.

③NTMobile (NAT Traversal with Mobile)

エンド端末のカーネルを改造
移動時にエンド端末と指示サーバが連携してIP層のアドレス変換テーブルを更新
開発中



今回の開発

IPv4の課題3：エンドエンドのセキュリティ

セキュリティ確保のための管理負荷が大きい

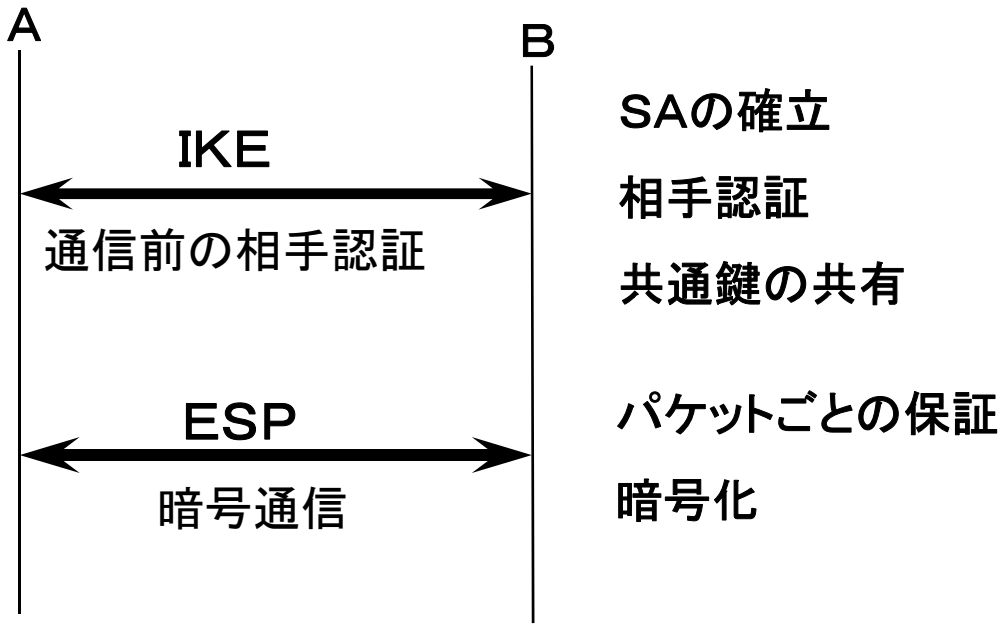
NATを跨る確実なエンドエンドセキュリティ対策が存在しない

セキュリティ対策の例

- 暗号技術による相手認証と暗号通信　←ここに着目
- ウィルス対策
- ファイアウォール

暗号技術の代表IPsec

既存技術



IKE; Internet Key Exchange

ESP; Encryption Security Payload

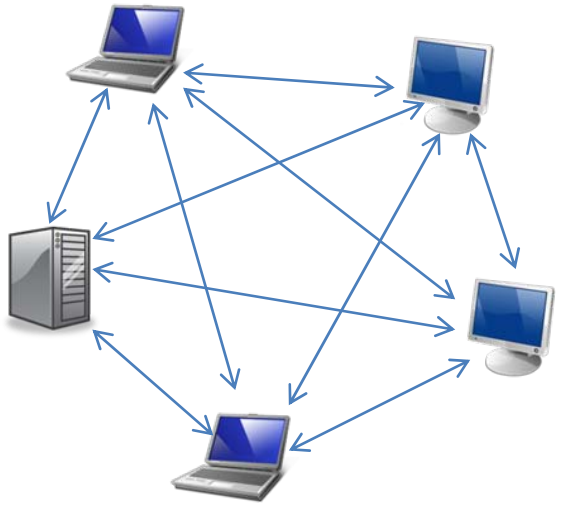
SA; Security Association

（通信モード、暗号化アルゴリズム、暗号鍵、シーケンス番号初期値の組合せ）

既存技術

IKE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

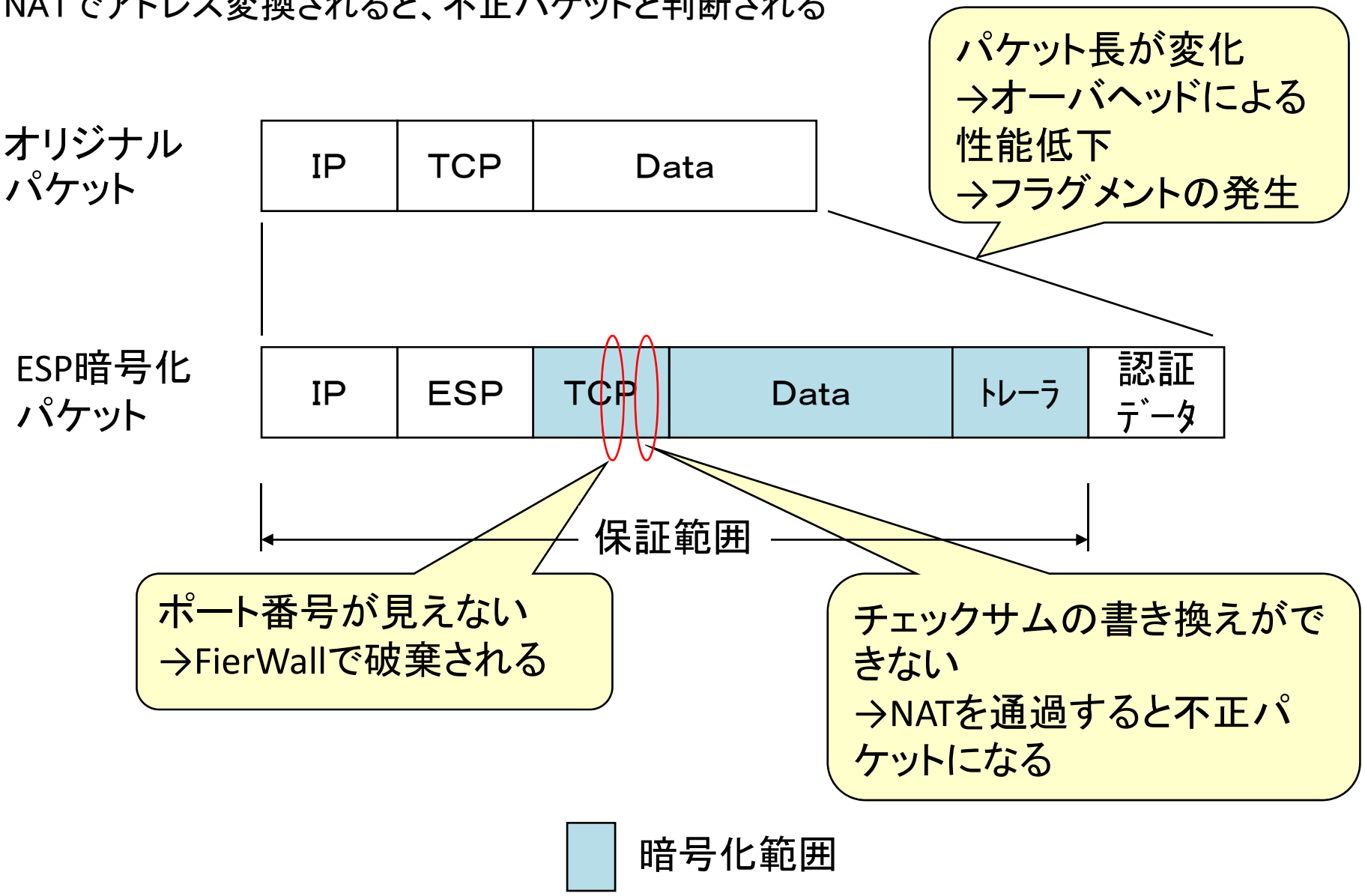
IKEによる通信グループの定義



ESPではNATを跨る暗号化通信ができない

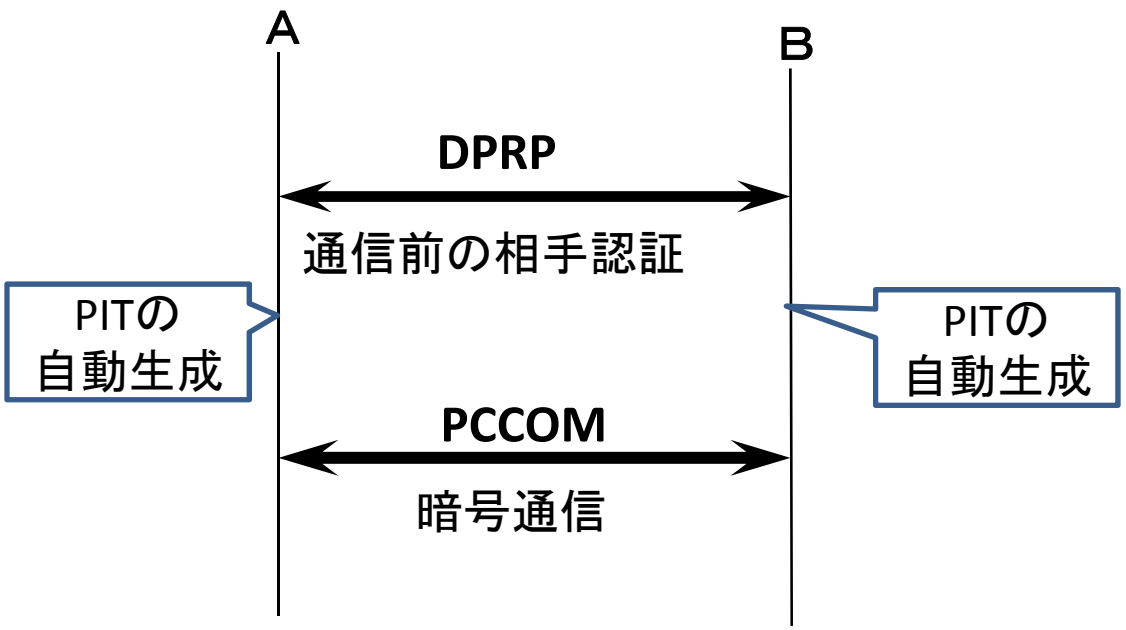
既存技術

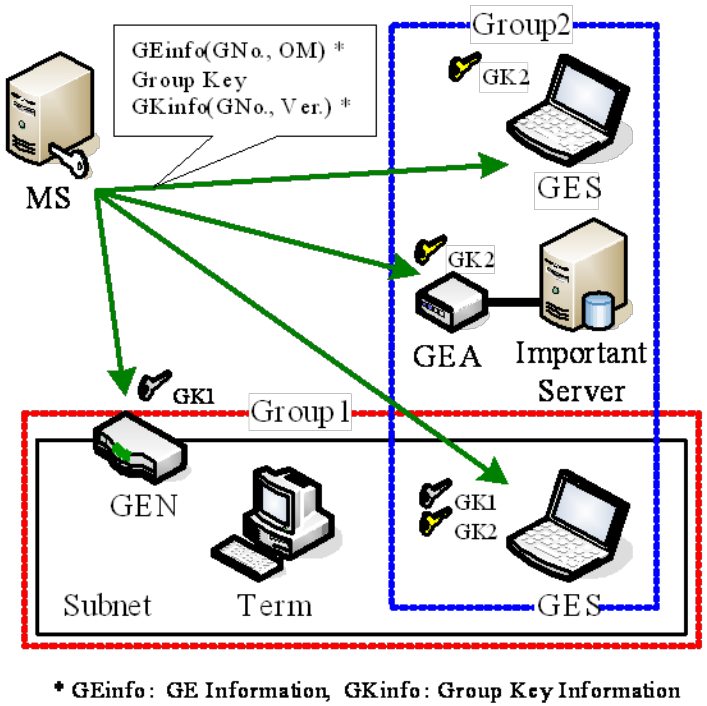
NATでアドレス変換されると、不正パケットと判断される



DPRPとPCCOM

提案済み技術





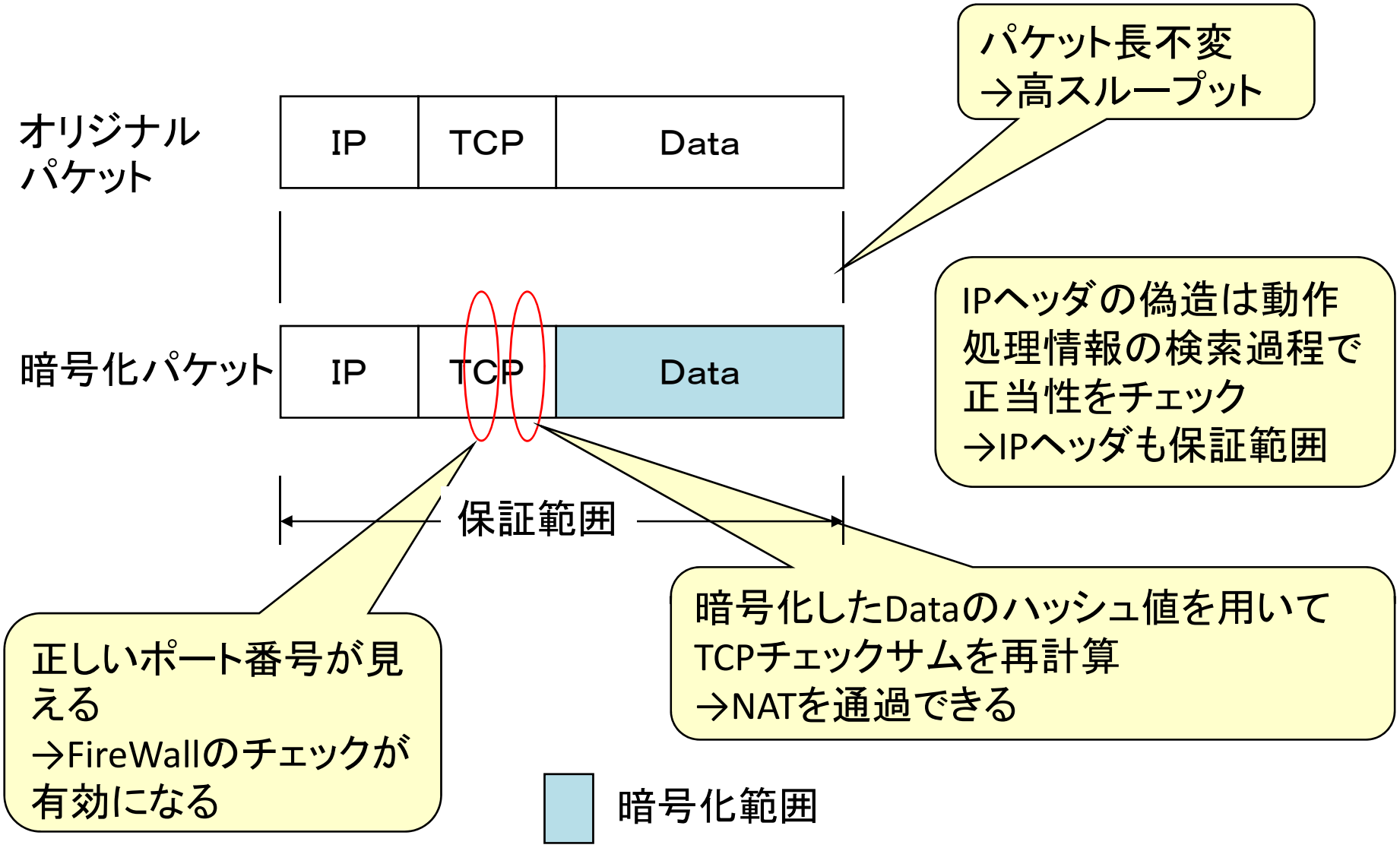
DPRP (Dynamic Process Resolution Protocol):
通信グループと暗号鍵を1対1に対応付けることにより、設定項目を現象
システム構成を学習することにより管理負荷を大幅に削減（PITの自動生成）

PIT (process Information Table): 動作処理情報（暗号化、廃棄、透過中継など）

PCCOM（Practical Cipher COMmunication Protocol）

提案済み技術

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



開発済みまたは開発中のセキュリティ技術

①PCCOM (Practical Cipher COMmunication)

エンド端末のカーネルを改造
暗号化範囲をTCP/UDPヘッダ以降とし、独自のTCP/UDPチェックサムを生成することによりNATを跨る暗号化通信を実現

[1]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.

②DPRP (Dynamic Process Resolution Protocol)

エンド端末のカーネルを改造
通信に先立ち、相手端末を認証するとともに、通信に必要となる動作処理情報を自動生成

[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]後藤裕司，鈴木秀和，渡邊晃，「NATを跨るセキュア通信グループの構築」，情報処理学会論文誌，条件付採録

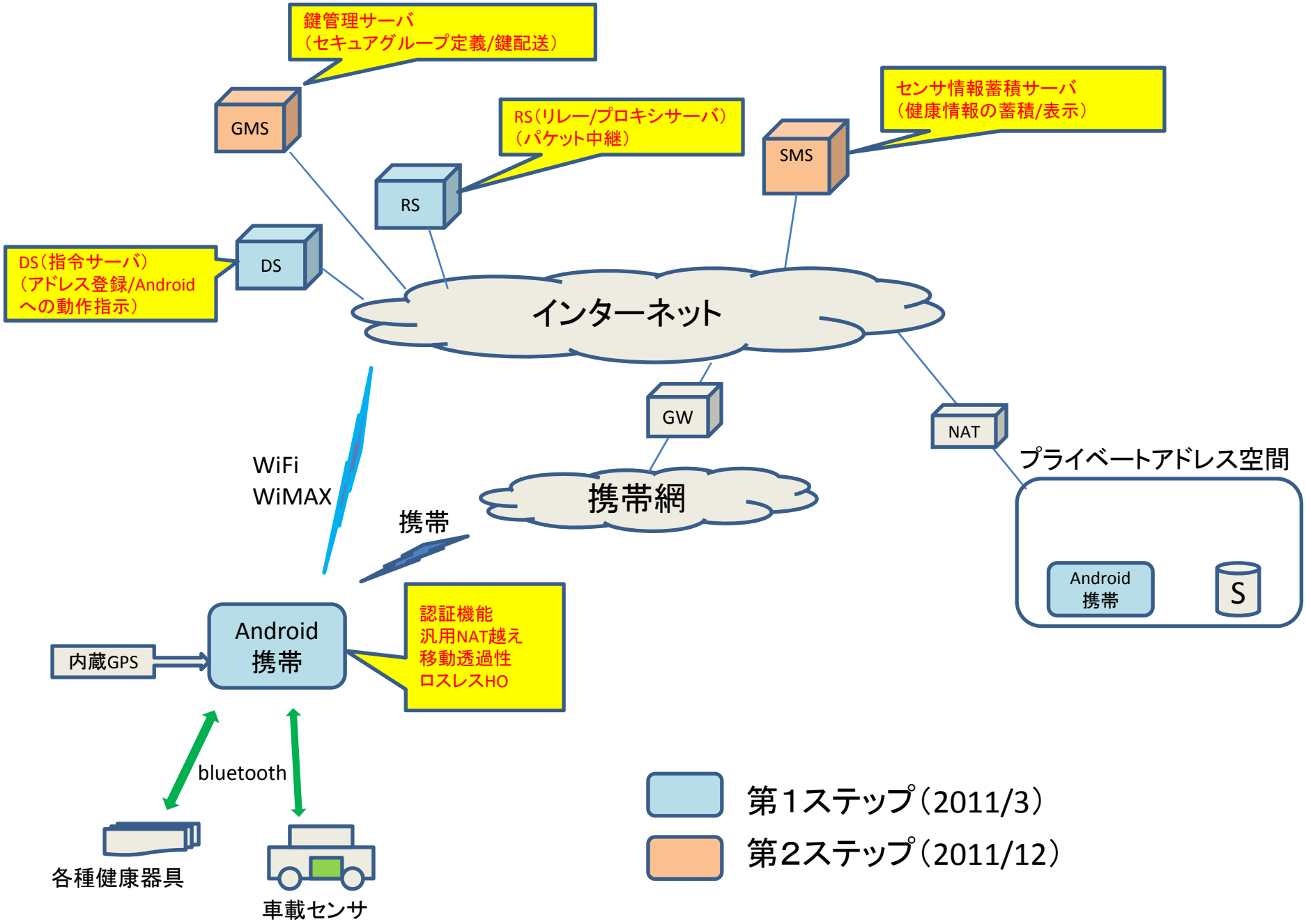
NTMobileでは、DPRPとPCCOMをそのまま適用する

NTMobileの概要

特長:
・NATがあっても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
・移動時にパケットロスが発生しない
・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
・既存ノードとの上位互換性
・IPv4/IPv6混在ネットワークへの拡張が可能

システム構成:
・DS (Direction Server)
　エンドノードのホスト名と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
　DNSサーバを改造したもの
・RS (Relay Server)
　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

NTMobileの概念図



キーとなる技術

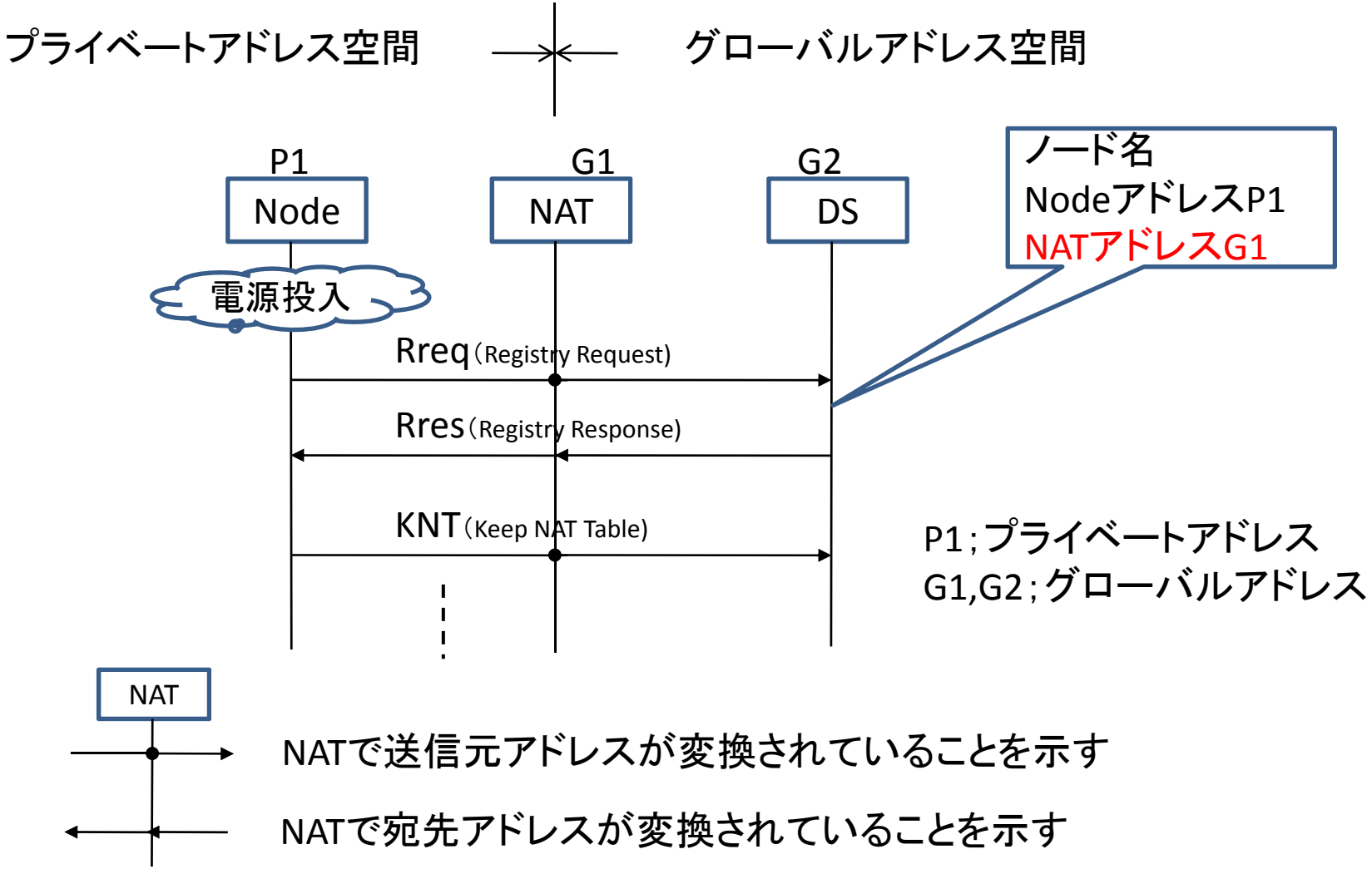
・IP層でのアドレス変換　　⇒Mobile PPCの技術を流用
　移動時に上位層に対してアドレスの変化を隠蔽する
　カーネルの改造
・グループ認証　　⇒DPRPを適用
　通信開始時に相手を認証する
　カーネルの改造
・暗号化技術　　⇒PCCOMを適用
　NATを通過できる暗号化通信
　カーネルの改造
・トンネル転送
　NATのSPIを回避するため、NAT通過時はトンネル転送とする
　カーネルの改造
・DNSサーバ
　名前解決の部分にオプションデータを追加。各ノードに対して動作の処理を指示
　DNSサーバの改造。アプリケーションの新規開発

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
　→移動透過性の実現を困難にしている一つの原因

通信前の準備

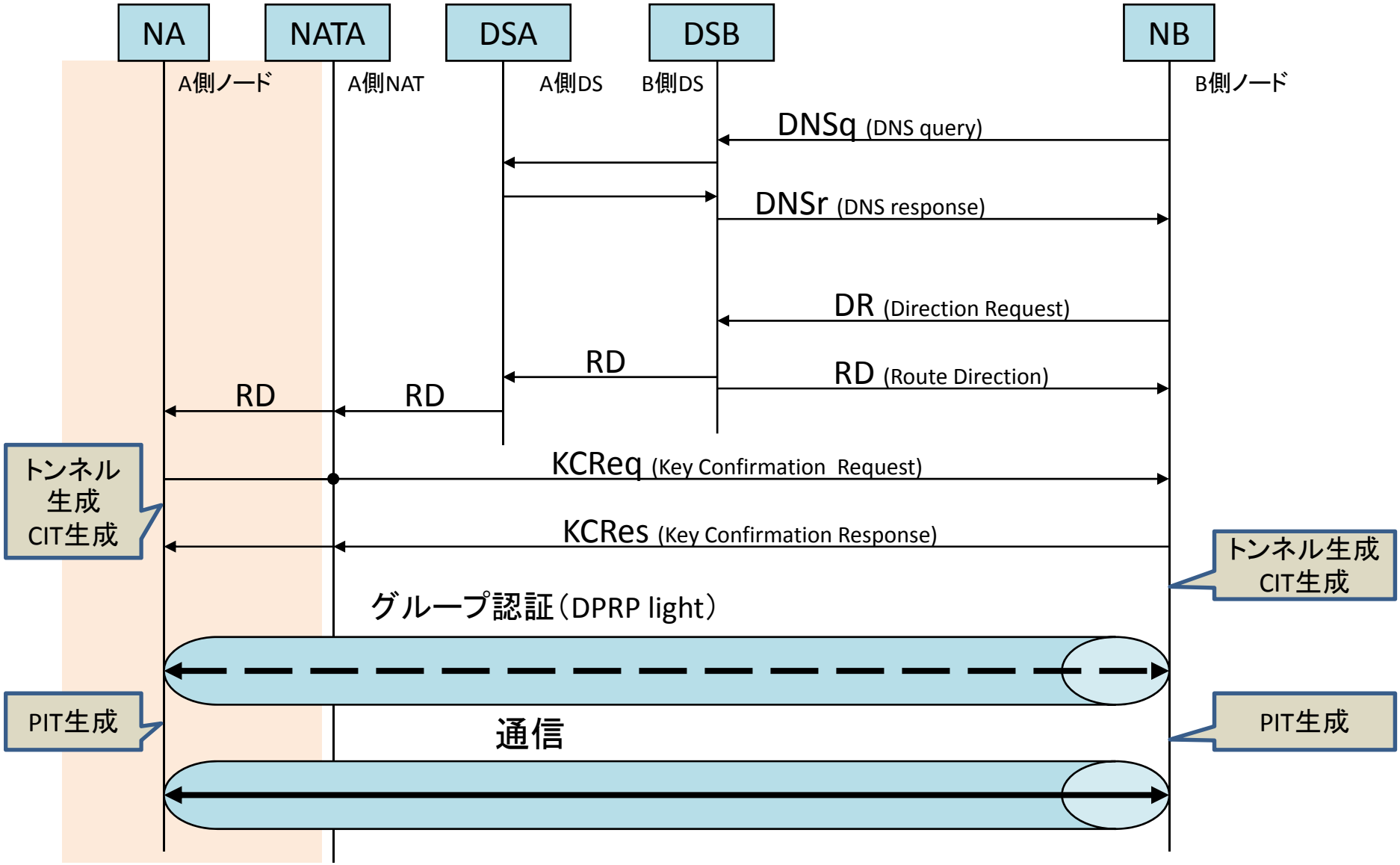
電源立ち上げ時に、ホスト名とアドレスをDSに登録（Dynamic DNSと同じ考え）

DS; Direction Server



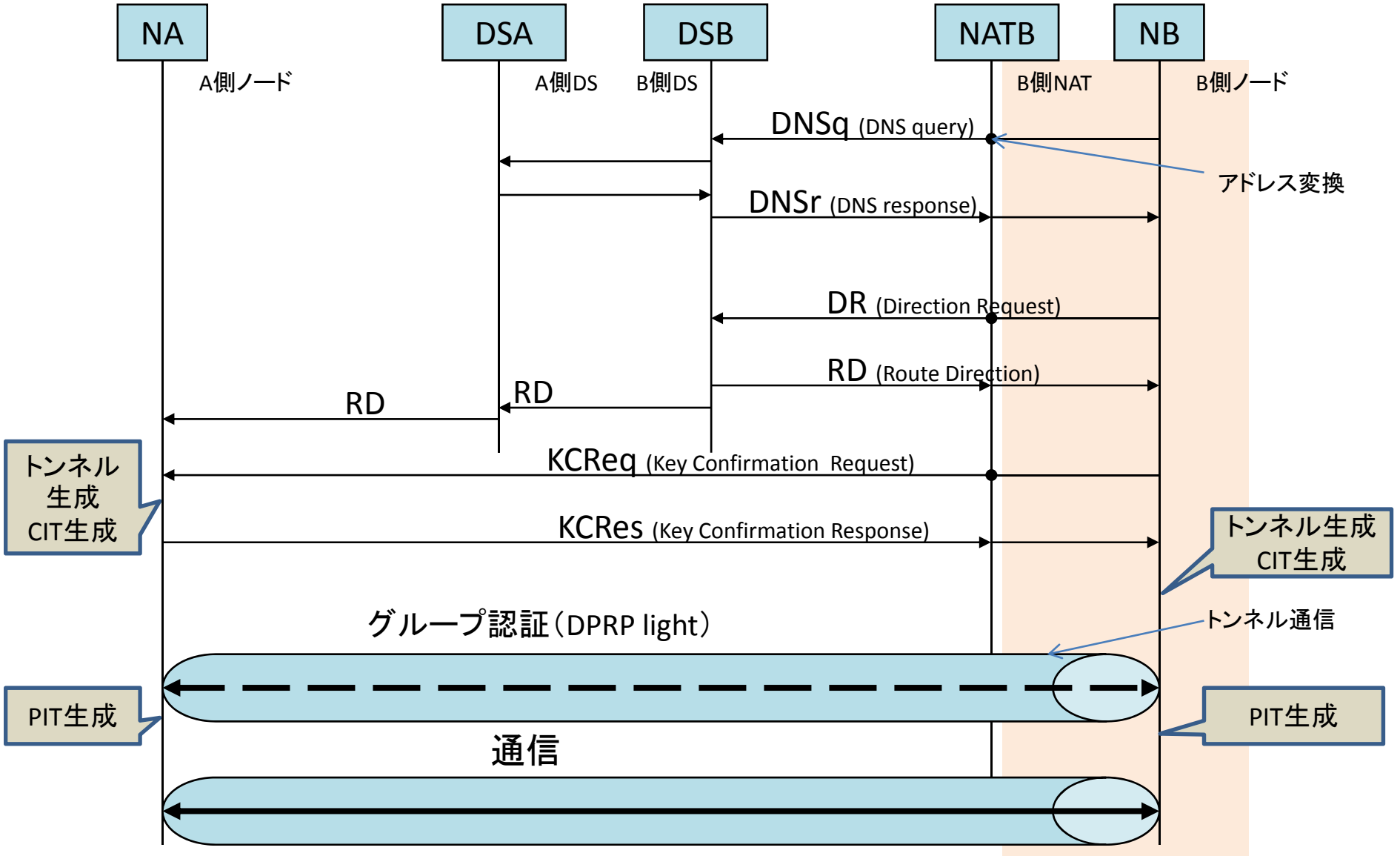
NBから通信開始

相手ノードNAがNAT配下の場合



NBから通信開始

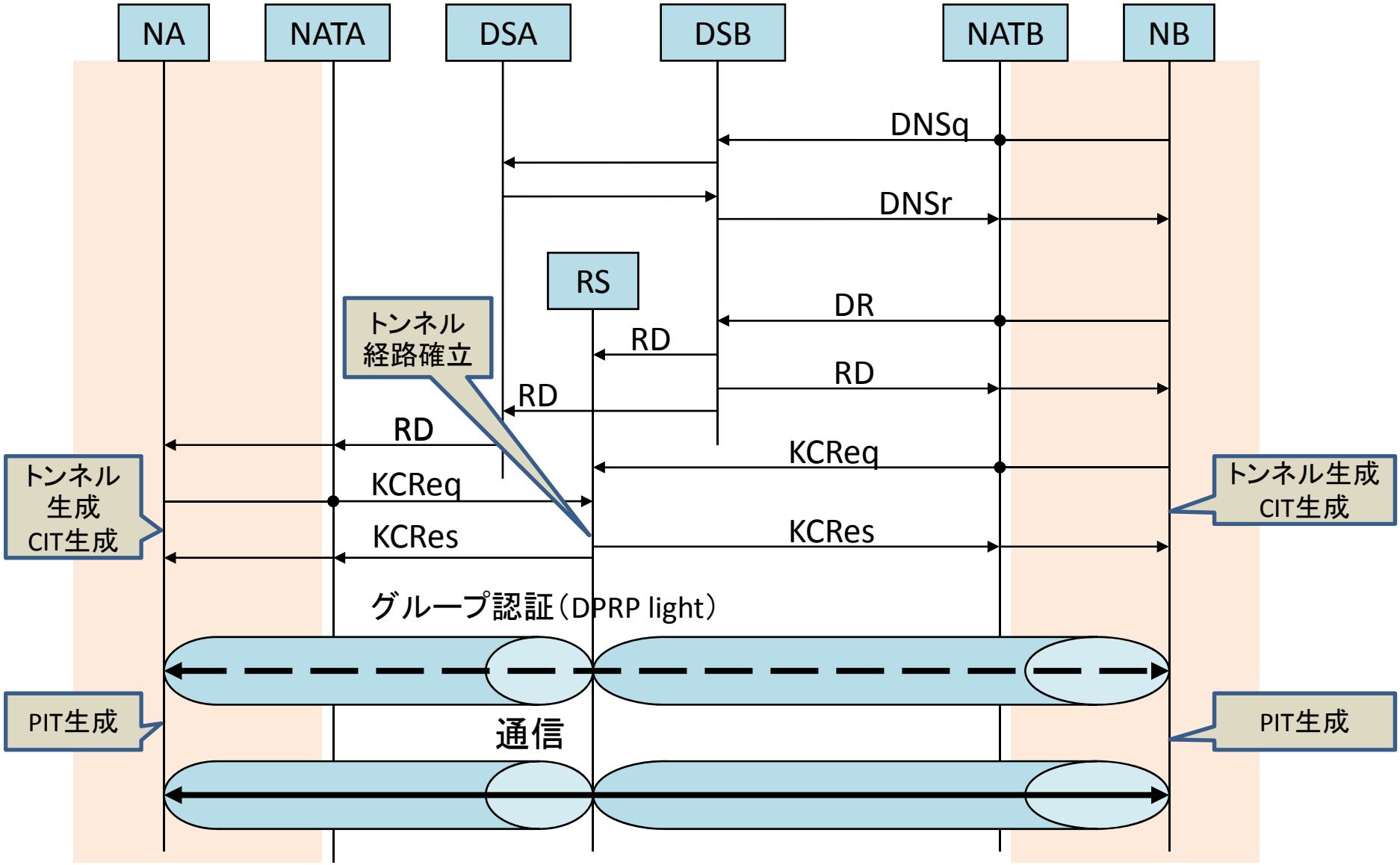
NBがNAT配下の場合



NBから通信開始

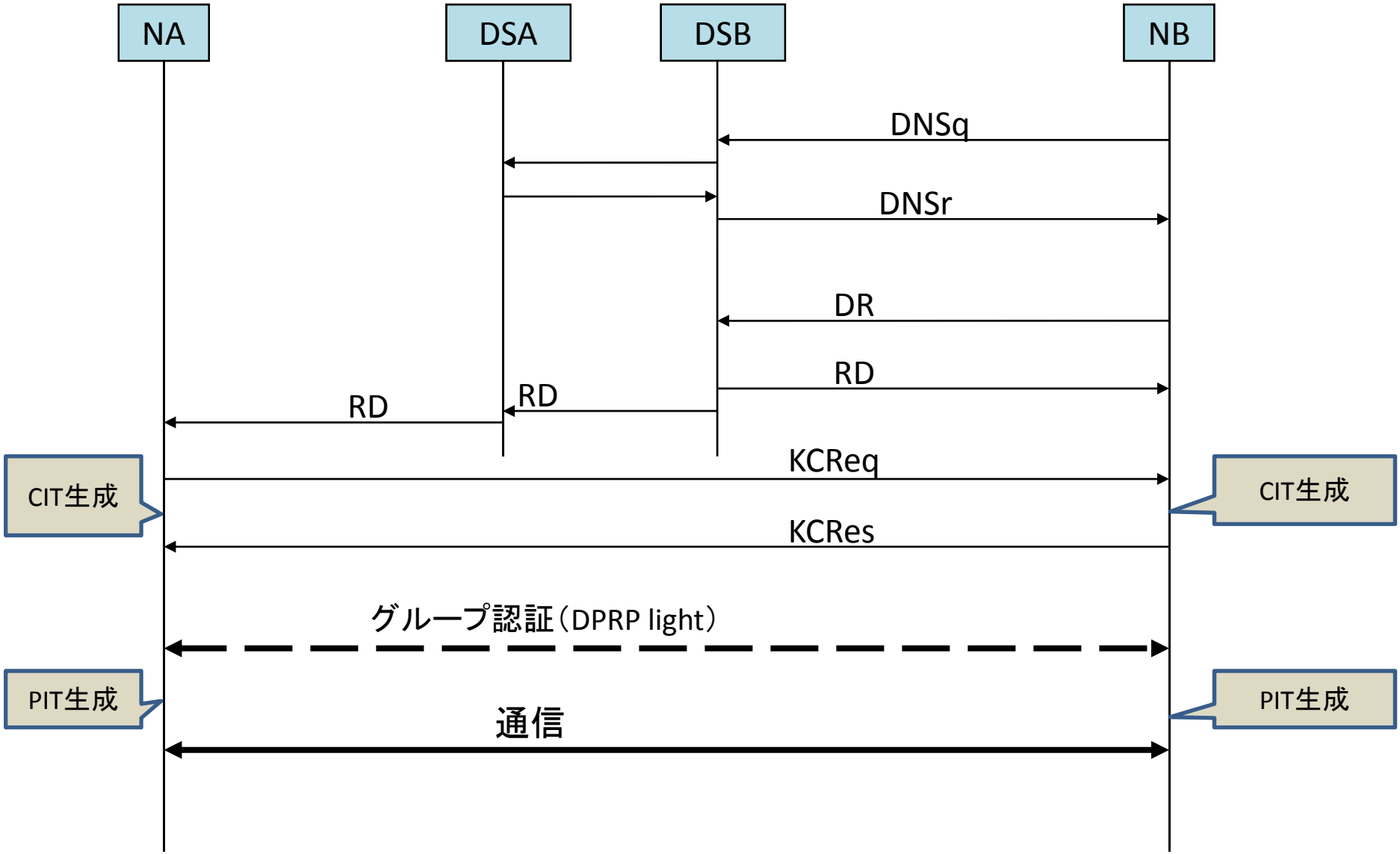
両ノードがNAT配下の場合

RS; Relay Server



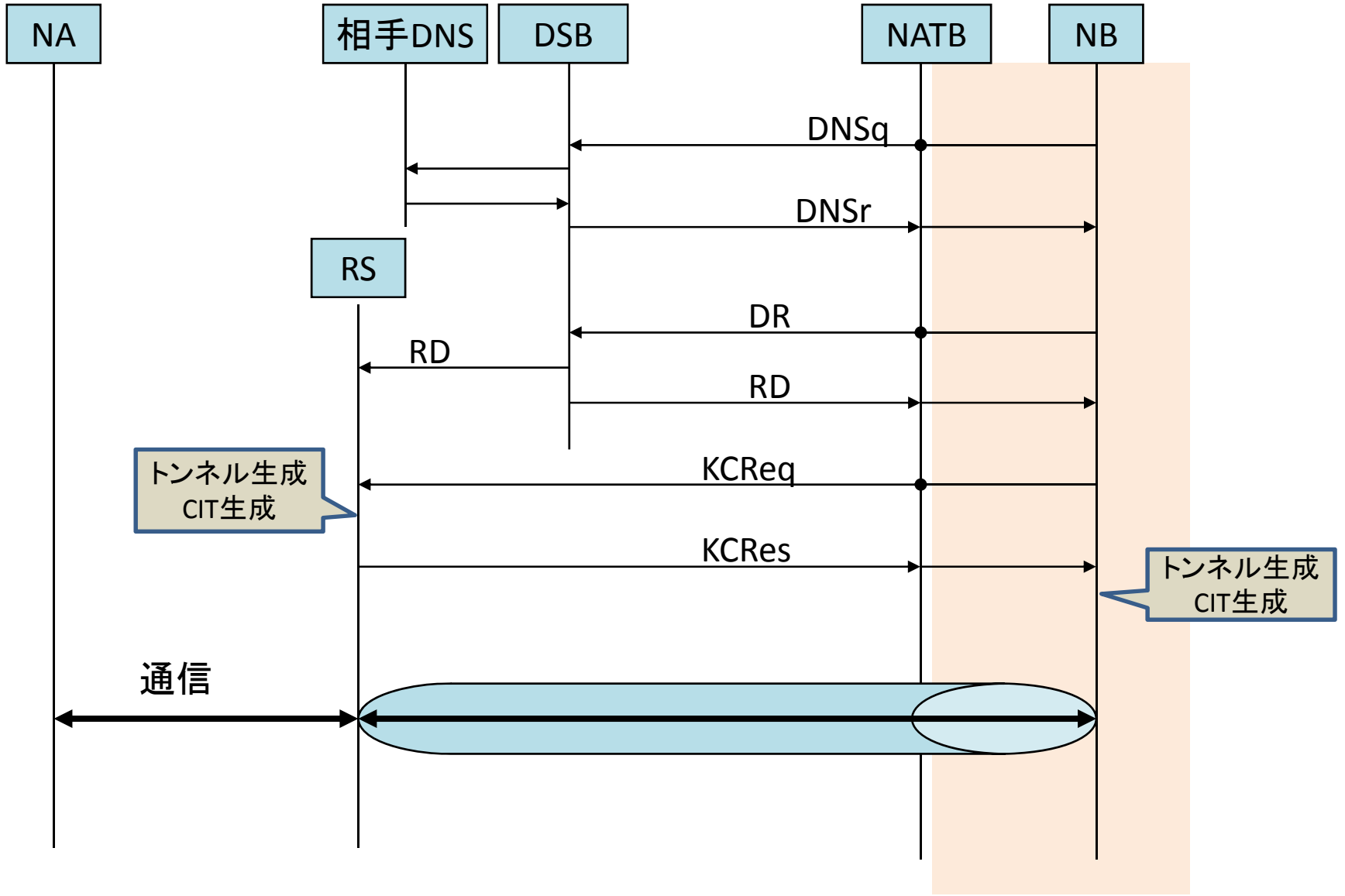
NBから通信開始

両ノード間にNATがない場合



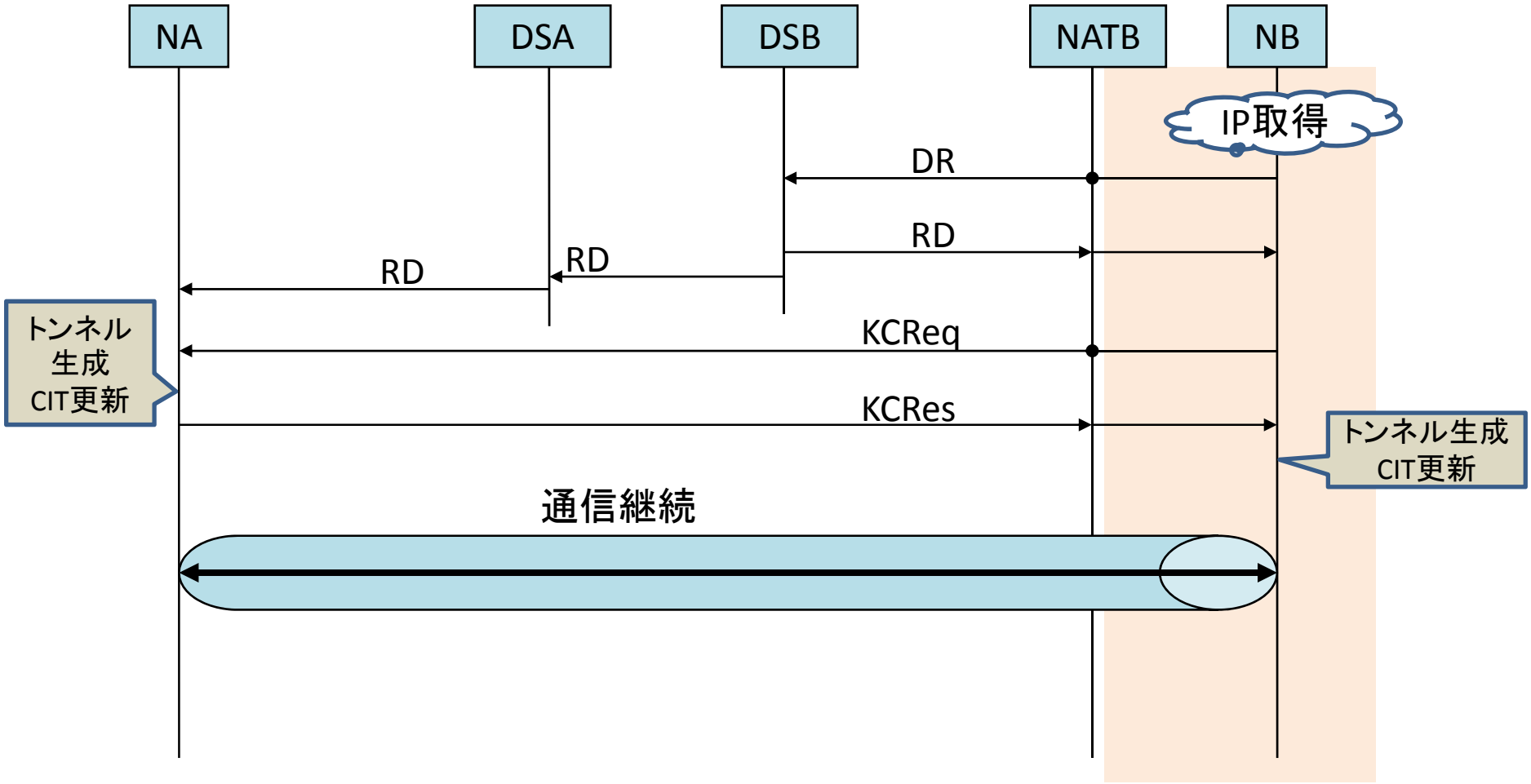
NBから通信開始

相手ノードNAが一般サーバ（グローバルアドレス）の場合



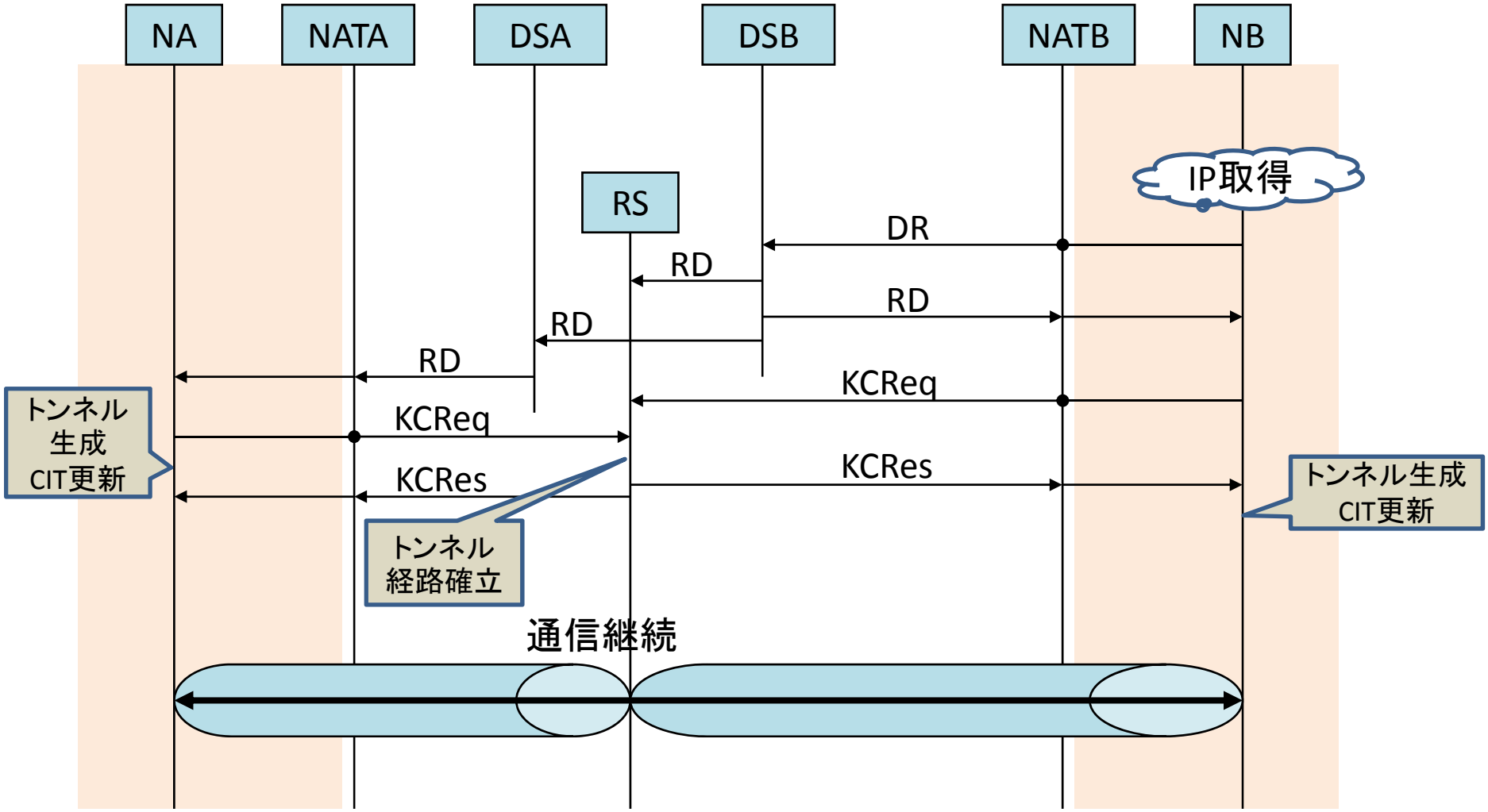
NBが移動

NBがNAT配下の場合



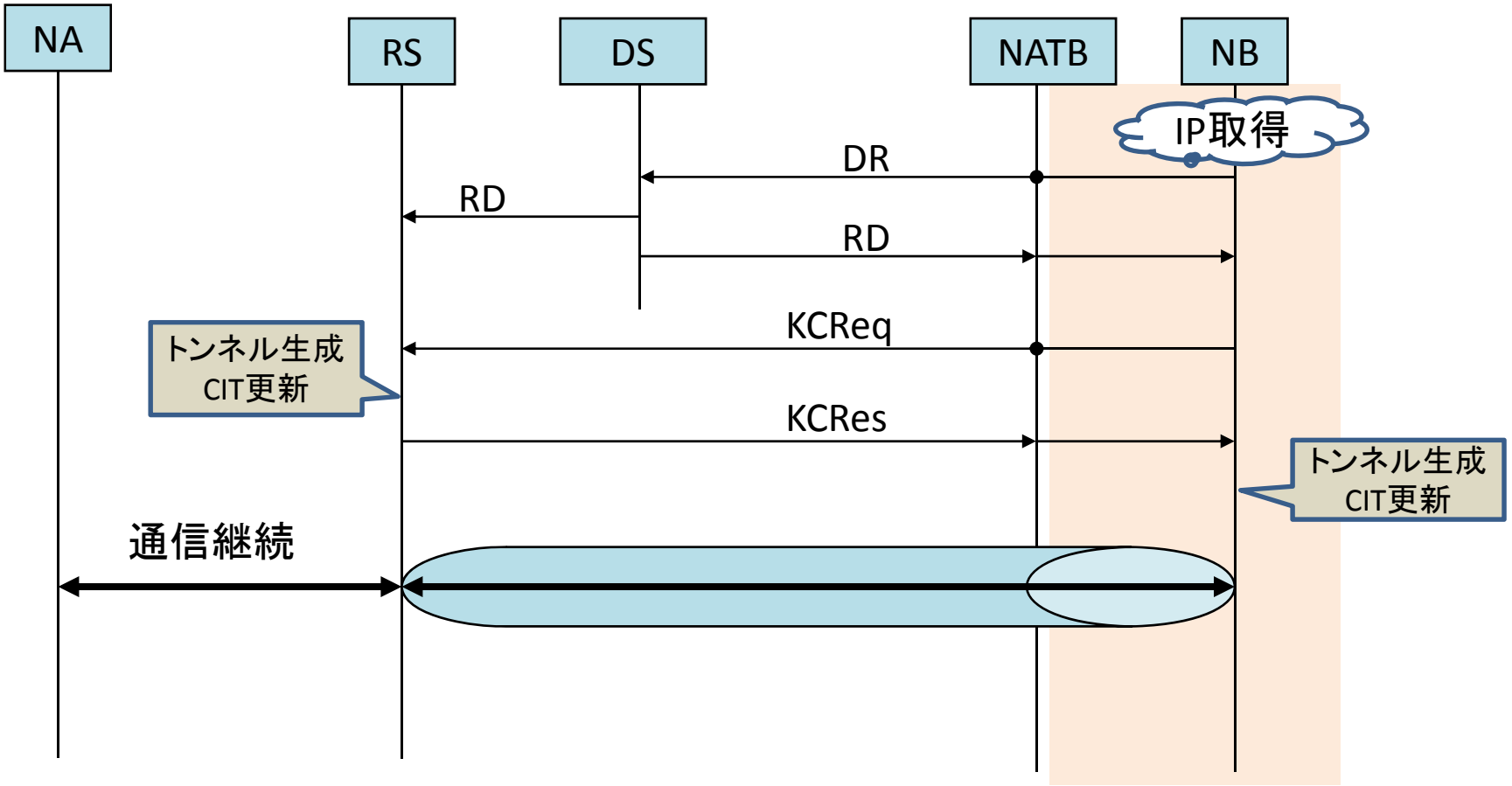
NBが移動

両ノードがNAT配下の場合

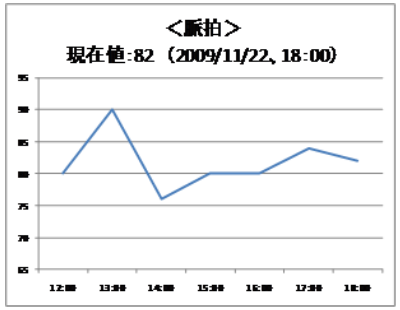


NBが移動

相手ノードNAが一般サーバでNBがNAT配下の場合



応用例:
弱者見守りシステム



管理サーバ

定期的に報告

高齢者

血圧計

歩数計

Bluetooth

スマートフォン

インターネット

ゲートウェイ

ルータ

携帯電話網

基地局

家庭端末

携帯電話

見守る人

2011年3月完成予定