NTMobileにおけるトンネル終端装置の提案

田中　慶吾 †*，鈴木　秀和 †，内藤　克浩 ‡，　渡邊　晃 † († 名城大学，　‡ 愛知工業大学)

Proposal for Tunnel Terminator in NTMobile

Keigo Tanaka†, Hidekazu Suzuki†, Katsuhiro Naito‡, Akira Watanabe† (†Meijo University, ‡Aichi Institute of Technology)

1　はじめに

インターネットが普及し社会のインフラとなっている．しかし, インターネット上には悪意を持つユーザがおり安全に利用するためにエンドツーエンド通信における安全性が重要である．これを実現するため, ユーザ間の認証と暗号化により, ユーザを完全に囲い込むことができると有用である (これを密閉型ネットワークと呼ぶ). NTMobile(Network Traversal with Mobility)[1] は密閉型ネットワークを実現できる技術の 1 つである．しかし, 完全に密閉されたネットワークは安全性は高いがインターネット上の一般サーバなどとの通信が一切できない. そこで, NTMobile のトンネル通信を終端するトンネル終端装置を経由して一般ネットワークとの通信を可能とする方法を提案する．

2　密閉型ネットワークと NTMobile

インターネットは誰でも利用できるためセキュリティ対策を行わないと危険である．そこで安全が保証されたネットワークの構築が必要である. NTMobile は通信相手の設置場所にかかわらず必ず通信経路を確立することができ, エンドツーエンドのセキュリティを保証する技術である. エンドノードのアプリケーションは NTMobile で割りあてられた仮想 IP アドレスを用いて通信を行う．すべての通信パケットは実アドレスでカプセル化されトンネル通信が行われる．DC(Direction Coodinator) はインターネット上に設置される装置で, 仮想 IP アドレスの配布と経路指示を行いエンドツーエンドの通信を実現する．さらに DC にてエンドノードのグルーピングを定義することにより, 同一グループの NTM ノードだけが相互に通信を行える．これにより密閉型ネットワークが実現できる. しかし, 密閉型ネットワークは安全であるがインターネット上のサーバなどとの通信が全くできないという課題がある．

3　提案方式

NTMobile の密閉型ネットワークにおいてトンネル通信を終端し, 一般装置との通信を可能とするトンネル終端装置 TT(Tunnel Terminator) を提案する．TT は密閉型ネットワークと一般装置との通信を中継する装置で, アプリケーションレベルでセキュリティの責任を持つ必要がある．TT が NTMobile の通信を終端し, DNS 名前解決, 仮想アドレスと実アドレスのアドレス変換を行うことによって NTM ノードと一般端末との通信を可能とする. Fig. 1 に TT を利用した NTMobile のシーケンスを示す. TT は NTM ノードの機能を拡張した装置である．Fig. 1

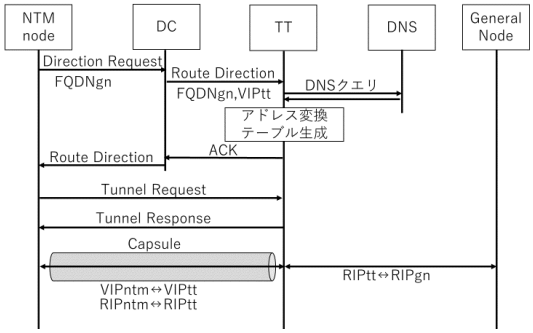


Fig. 1　TT を利用した NTMobile のシーケンス図

においてアドレス変換テーブルは TT を利用するために拡張された情報である．Fig. 1 は簡単のため NAT の存在を省略している．GeneralNode とはグローバル空間にある一般装置 (以下 GN とする) である．NTM ノードは GN と通信したい場合, DC に通信したい相手である GN の FQDN(FQDNgn) を送信して経路指示を仰ぐ．DC は TT へ経路指示とともに FQDNgn の送通知と仮想 IP アドレス (VIPtt) の割り当てを行う．一般の NTM ノードの仮想 IP アドレス (VIPntm) は立ち上げ時に決まるが, VIPtt はこの時配布される点が異なる．これにより複数の NTM ノードが一台の TT を共有することができる．TT が DNS による名前解決を行い, VIPntm と GN の実 IP アドレス (RIPgn) の変換テーブルを生成する．このテーブルは TT から複数の GN をアクセス可能とするために利用し, 複数の GN がある場合の識別は TT が生成するポート番号によって行う．DC が構築した経路で NTM ノードと TT は NTMobile によるトンネル通信を行う．TT は NTM ノードと TT 間の仮想アドレス通信を TT と GN 間の実アドレス通信に変換する．このことによって GN からみた通信相手は TT となる．TT がアプリケーションレベルのセキュリティを保証することにより密閉型ネットワークを保つことができる．

4　まとめ

密閉型ネットワークにおいて一般通信を可能にするトンネル終端装置 TT(Tunnel Terminator) を提案した．

文　献

[1] 鈴木秀和, 他：NTMobile における通信接続性の確率手法と実装, 情報処理学会論文誌 Vol.54, No.1, pp.367–379, 2013.

NTMobileにおけるトンネル終端装置の提案

田中慶吾†,鈴木秀和†,内藤克浩‡,渡邊晃†
†名城大学 理工学部
‡愛知工業大学 情報科学部

Watanabe Lab.

研究背景

- インターネット
  - 社会のインフラ
  - 安全なネットワークを構築する必要

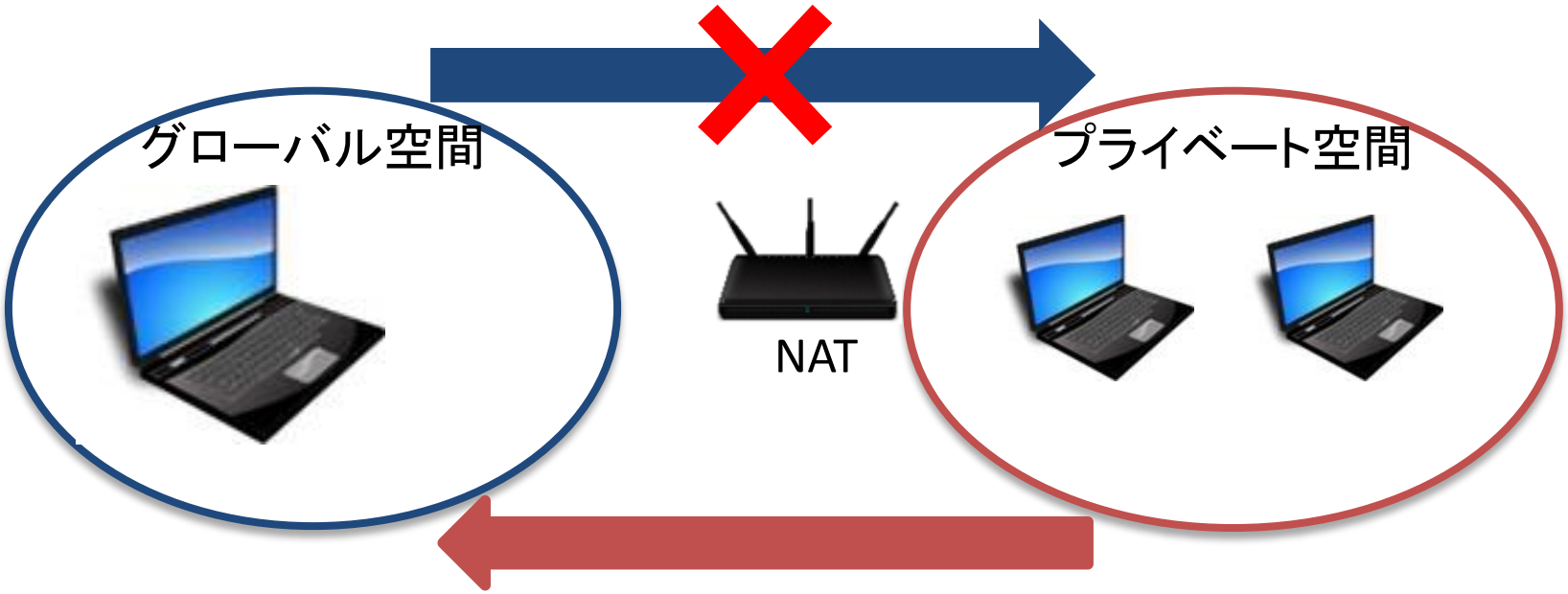
  - 課題
    ① IPv4グローバルアドレス枯渇問題
    ② NAT越え問題
    ③ 移動透過性が必要

アドレス枯渇問題

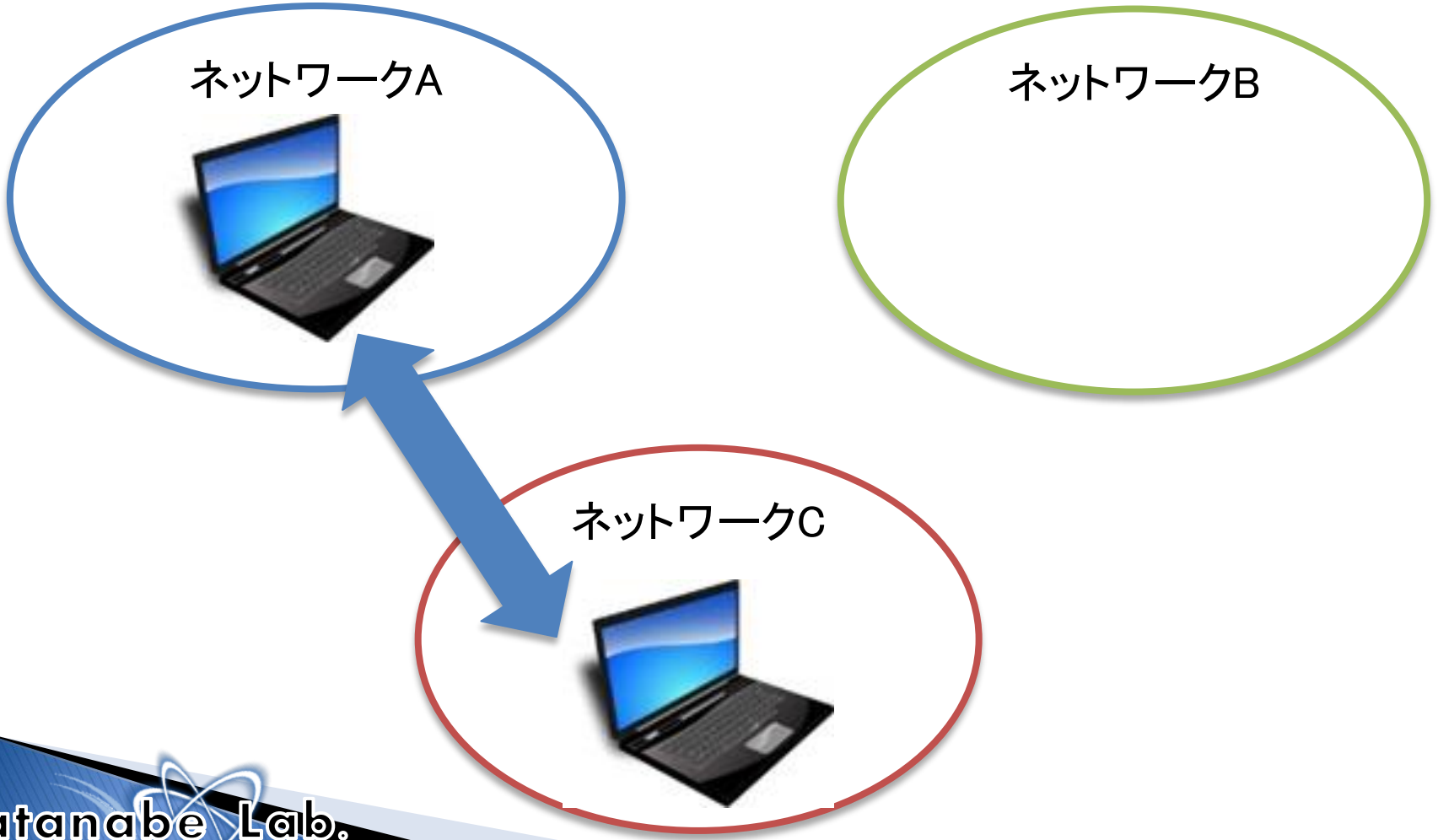
- IPv4グローバルアドレスの数が不足している
  - 解決策
    - NATを利用し，複数のプライベートIPアドレスを1つのグローバルアドレスIPアドレスに変換
      →NAT越え問題
    - IPv6アドレスの導入
      →IPv4との互換性がない

NAT越え問題

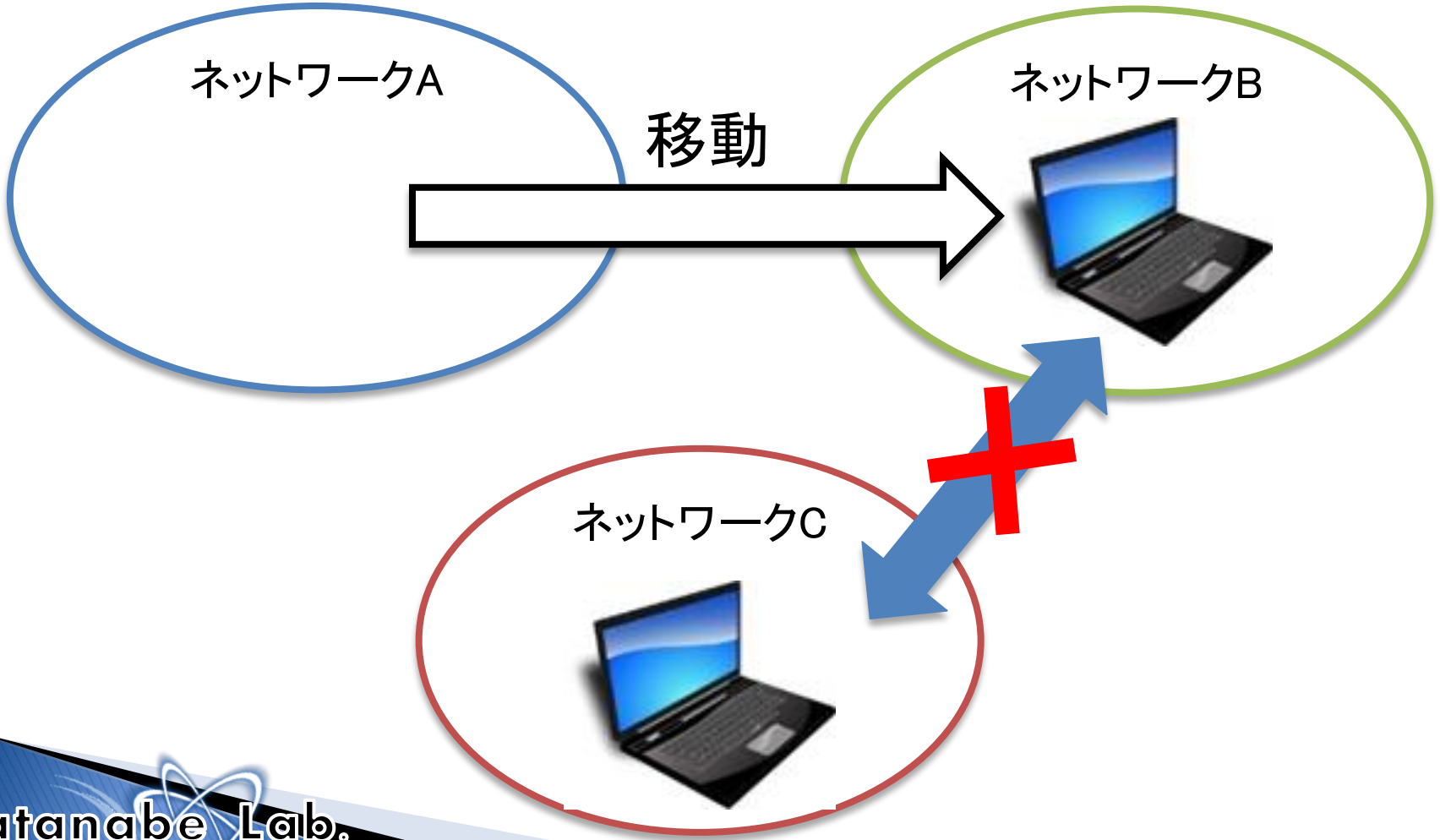
- グローバル空間からプライベート空間への通信を開始できない



移動透過性



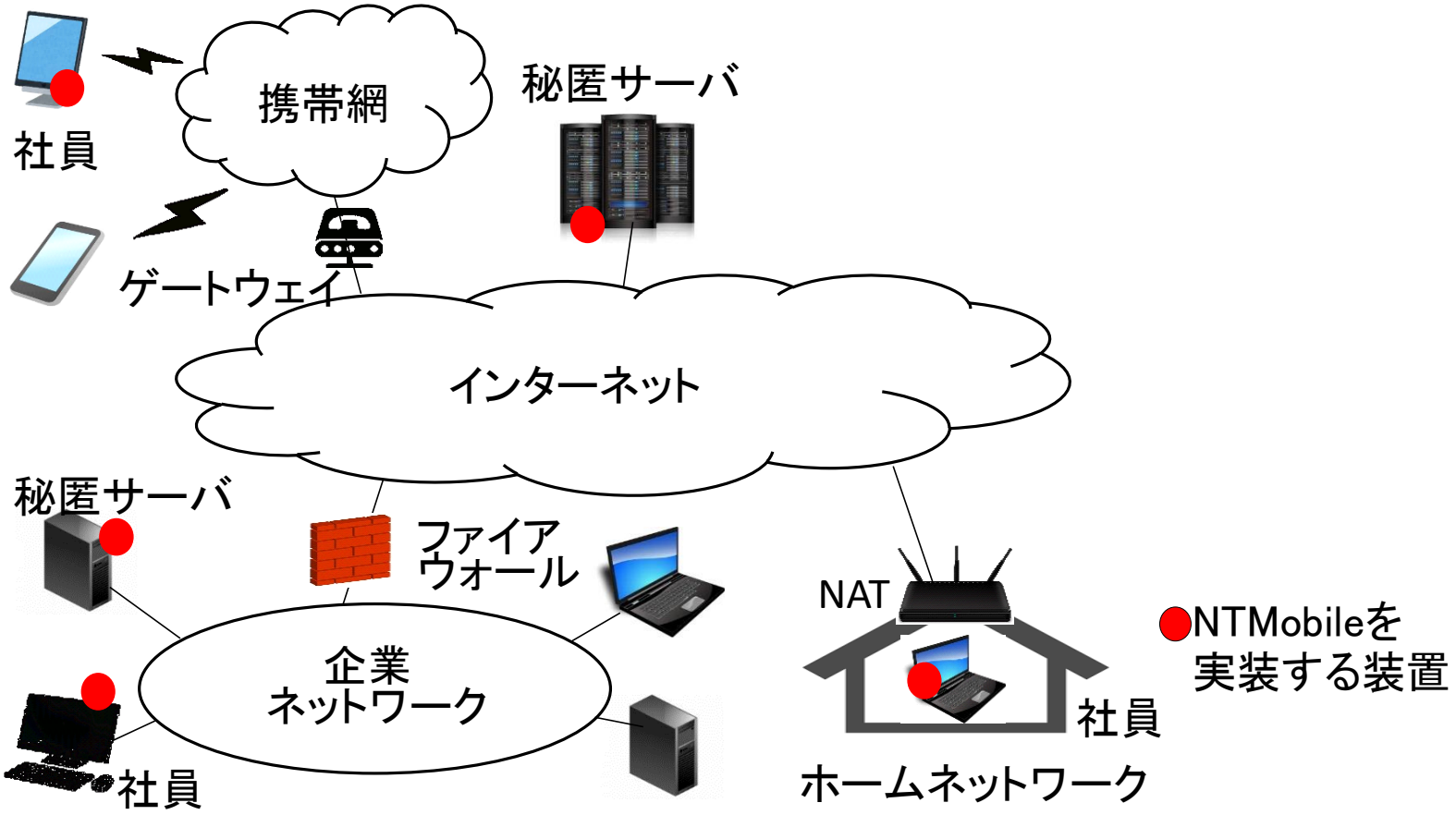
移動透過性



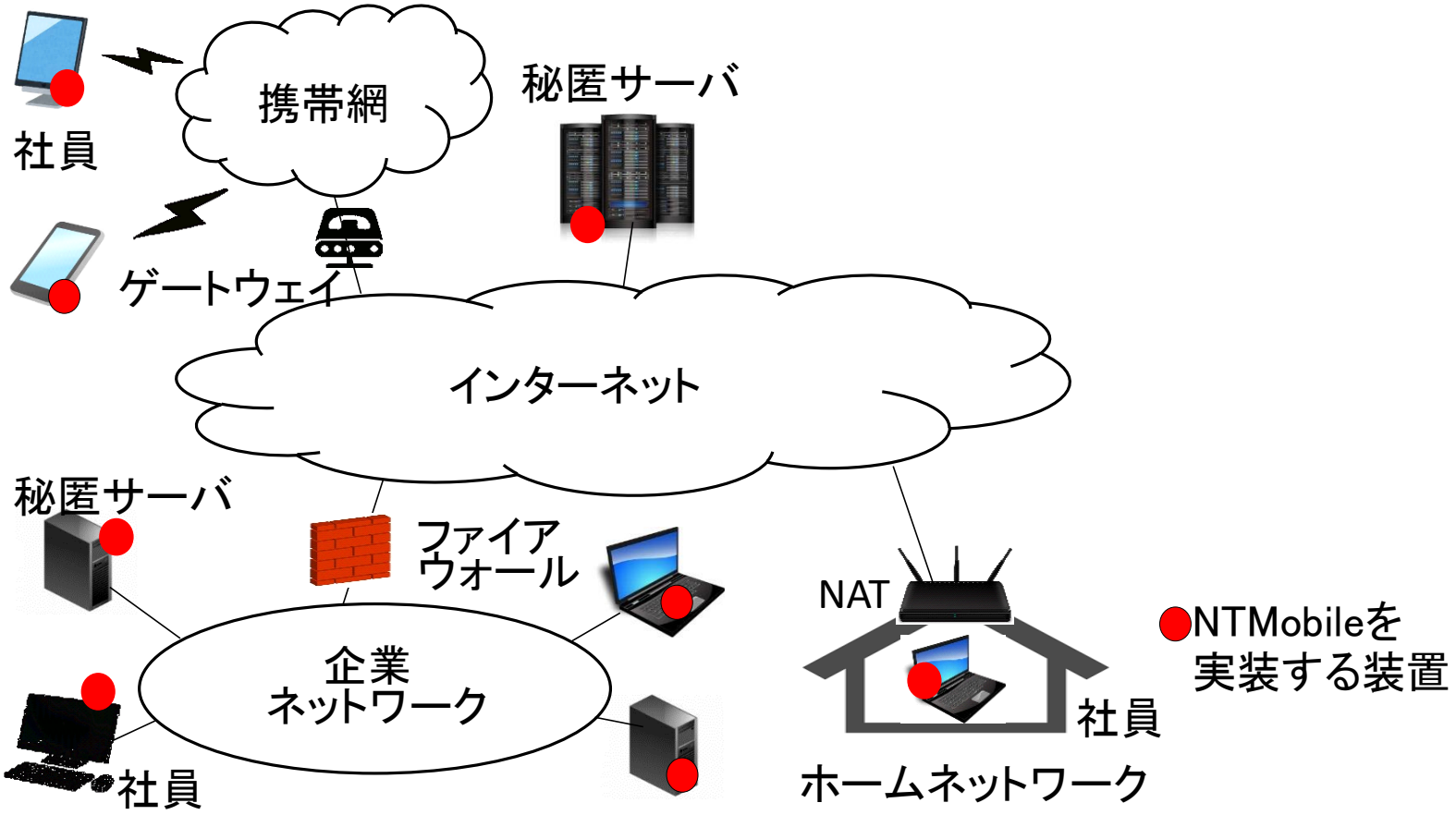
NTMobile (Network Traversal with Mobility)

- NAT越え問題, IPv4とIPv6の非互換性, 移動透過性を解決し
  安全な通信をすることができる技術
  - 通信相手の設置場所に関わらず通信経路を確立
  - 装置は割り当てられた仮想IPアドレスを用いて通信
  - 通信パケットは実アドレスでカプセル化されトンネル通信を行う

開放型ネットワーク


携帯網
秘匿サーバ
社員
ゲートウェイ
インターネット
秘匿サーバ
ファイア
ウォール
NAT
NTMobileを
実装する装置
企業
ネットワーク
社員
社員
ホームネットワーク

密閉型ネットワーク


携帯網
秘匿サーバ
社員
ゲートウェイ
インターネット
秘匿サーバ
ファイア
ウォール
NAT
NTMobileを
実装する装置
企業
ネットワーク
社員
社員
ホームネットワーク

密閉型ネットワーク

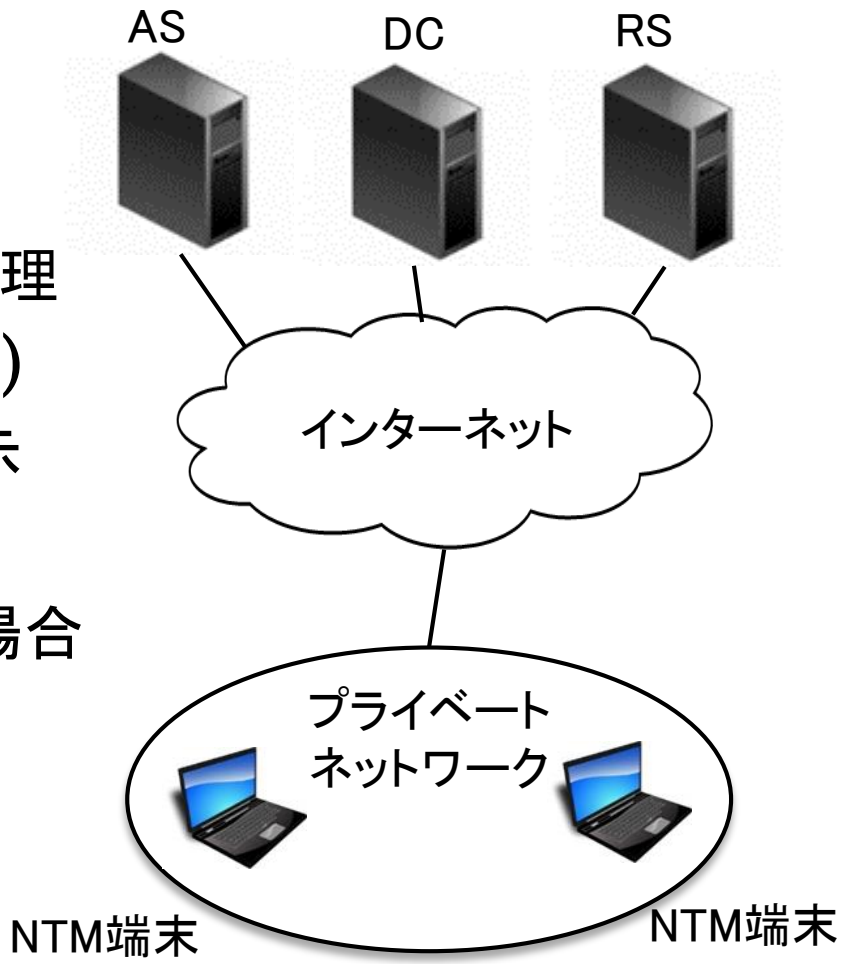
- すべてNTMobileの通信を行う
- セキュリティが高い
  - 外部と通信しないため侵入経路がない

- インターネット上のサーバーなどと一般通信が全くできない

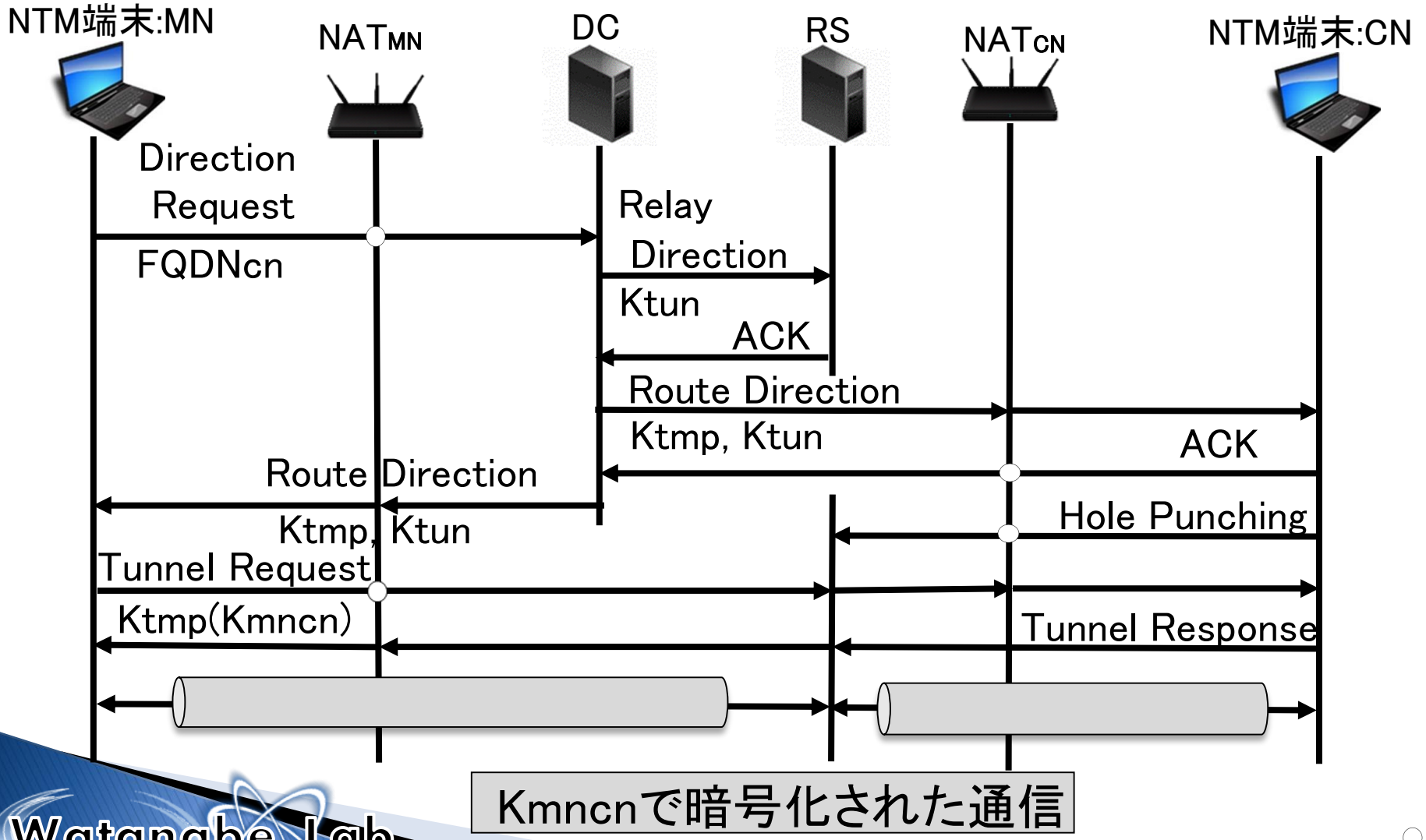
  →通常業務が制限される

NTMobileの概要

- NTM端末
  - NTMobileを実装した端末
- AS(Account Server)
  - NTM端末のアカウント情報の管理
- DC (Direction Coodinator)
  - 仮想IPアドレスの配布, 経路指示
- RS (Relay Server)
  - NTM端末が直接通信できない場合中継する



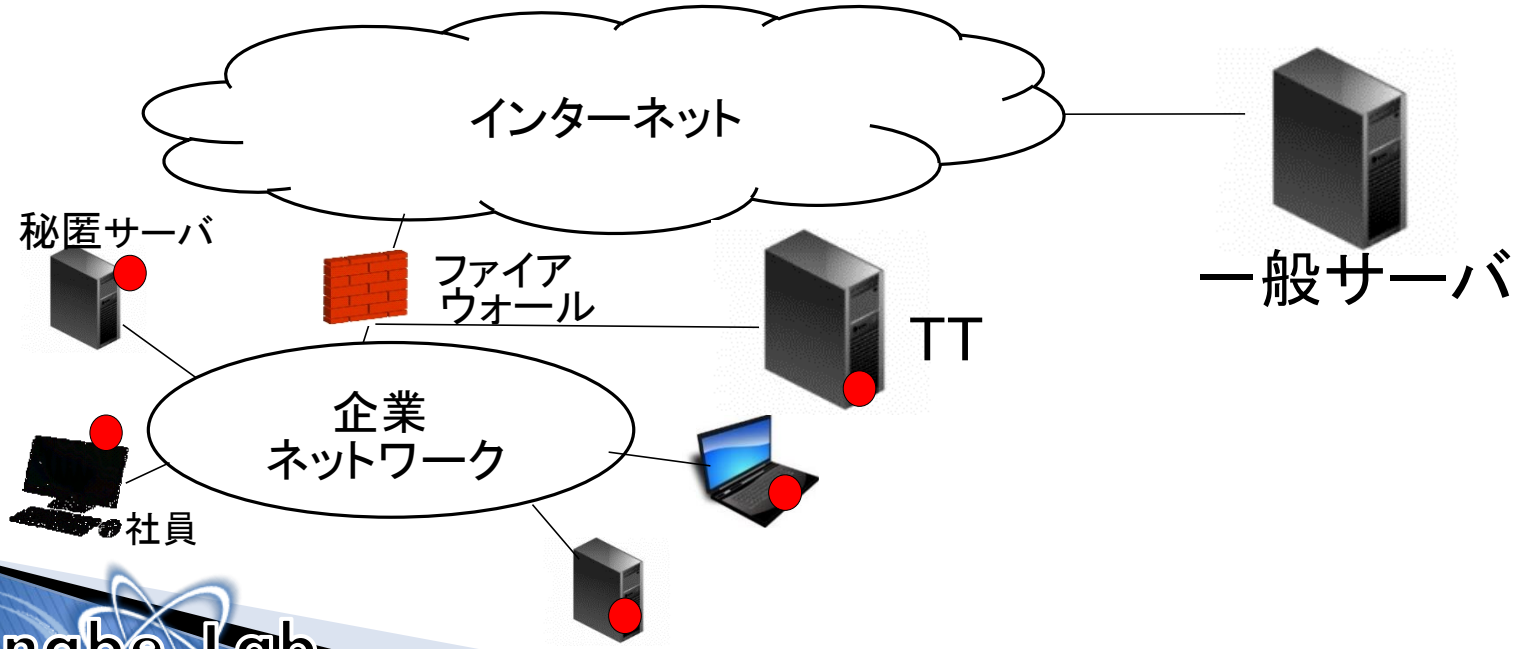
NTMobileのシーケンス



Kmncnで暗号化された通信

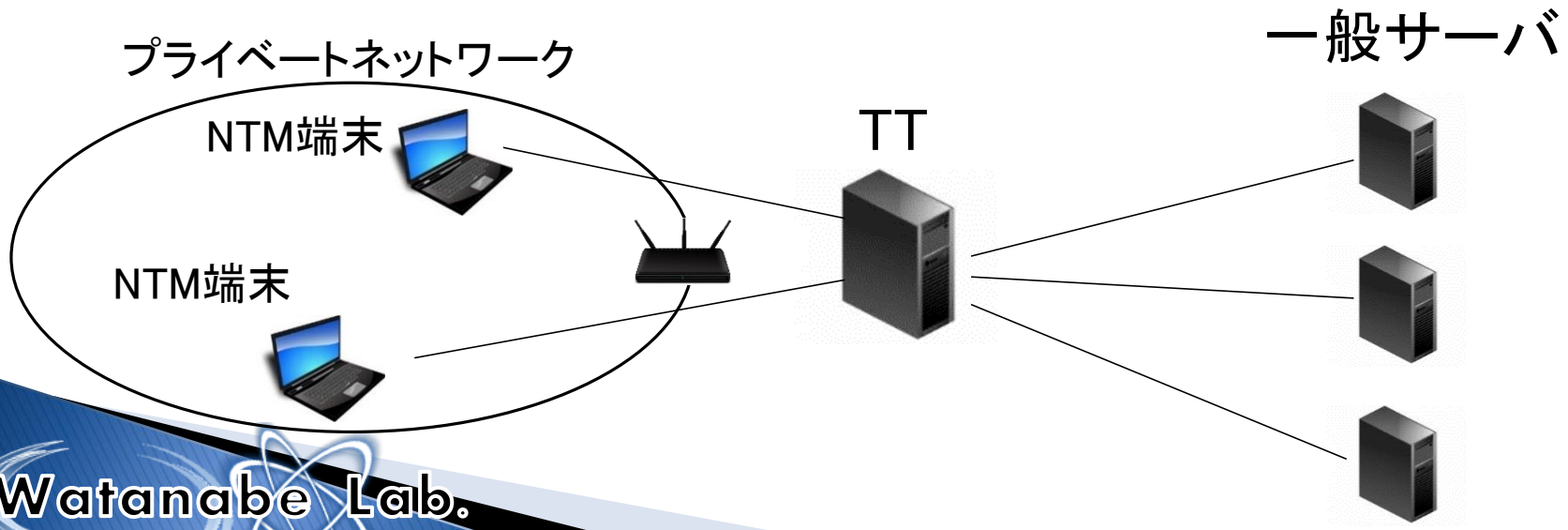
提案方式

- 密閉型ネットワークのセキュリティを保ちつつ一般通信を可能にするトンネル終端装置
  - TT(Tunnel Terminator)
- NTMobile端末と一般サーバの通信を中継

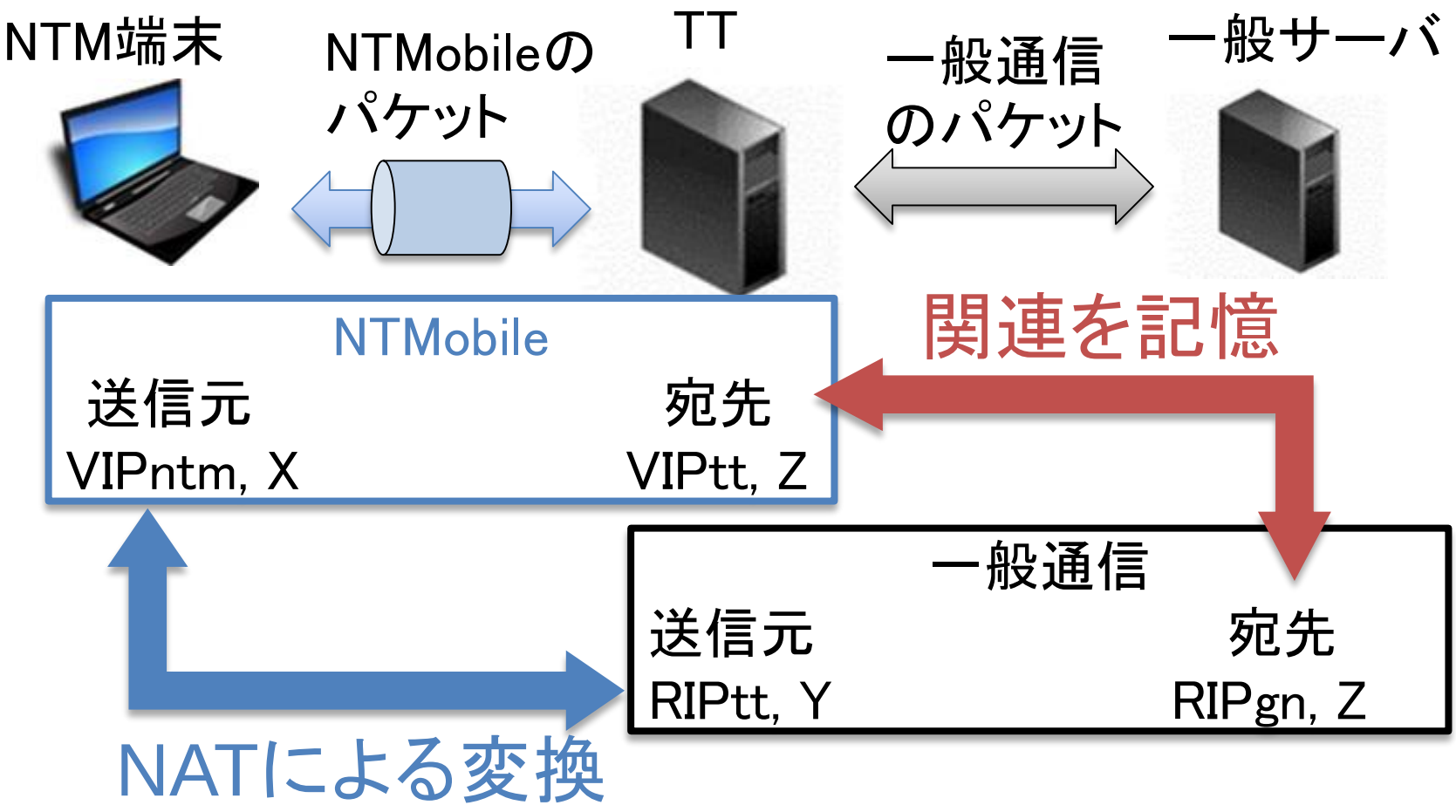


提案方式

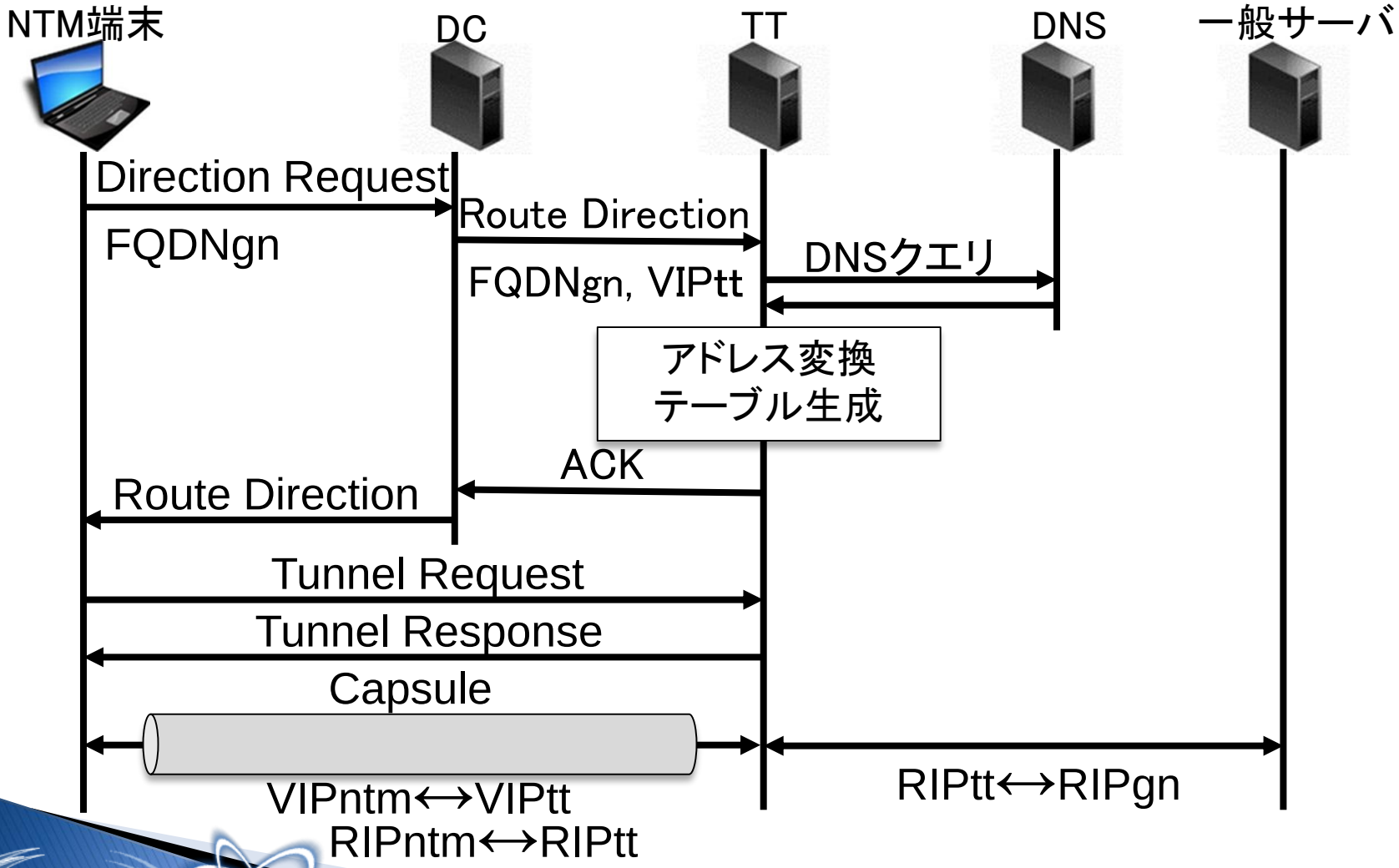
- 一般サーバはNTMobileが導入されていない
  - →仮想アドレスの変換が必要
- NTM端末，一般サーバが複数
  - →装置の識別が必要



アドレス変換


NTM端末
NTMobileの
パケット
TT
一般通信
のパケット
一般サーバ
NTMobile
送信元
VIPntm, X
宛先
VIPtt, Z
関連を記憶
一般通信
送信元
RIPtt, Y
宛先
RIPgn, Z
NATによる変換

シーケンス図


NTM端末
DC
TT
DNS
一般サーバ
Direction Request
FQDNgn
Route Direction
FQDNgn, VIPtt
DNSクエリ
アドレス変換
テーブル生成
ACK
Route Direction
Tunnel Request
Tunnel Response
Capsule
VIPntm↔VIPtt
RIPntm↔RIPtt
RIPtt↔RIPgn

提案方式

- 以上のシーケンスより，密閉型ネットワークにおいて一般通信が可能になる
- 今後は実装に向けて調査を進めていく

まとめ

- 密閉型ネットワークにおいての一般通信を検討
- トンネル終端装置を用いて実現