プライベートアドレス空間とグローバルアドレス空間を跨る移動透過性の実現

榎本 万人　鈴木 秀和　坂本 順一　渡邊 晃

名城大学大学院理工学研究科

Realization of Mobile Communications over a Private Address Area and a Global Address Area.

Kazuto Enomoto　Hidekazu Suzuki　Junichi Sakamoto　Akira Watanabe

Graduated School of Information and Science, Meijo University

1　はじめに

通信端末の小型化や無線ネットワーク環境の普及により，いつでもどこでも通信が可能なユビキタスネットワーク環境が構築されつつある．このような環境では，ネットワークに接続した状態で，通信に影響を与えず自由に移動できることが求められる．しかし，通信端末が通信中に別のネットワークへ移動し，IP アドレスが変化すると，それまでの通信が継続できない．これは，通信端末のトランスポート層では IP アドレス，ポート番号などのコネクション識別子が異なる通信は別の通信と見なされてしまうためである．これまで，移動により IP アドレスが変化しても，それまでの通信を継続できる移動透過性の研究は盛んに行われている [1].

この移動透過性を実現するための技術には Mobile IP [2] や LIN6（Location Independent Networking for IP ｖ６） [3] などがある．しかし，Mobile IP では Home Agent，LIN6 では Mapping Agent と呼ばれる特殊なネットワーク機器が必要となるため，導入するための敷居が高いという課題がある．そこで，我々は特殊な装置を必要とせず，エンド端末だけで移動透過性を実現する Mobile PPC（Mobile Peer to Peer Communication） [4] の研究を行っている．Mobile PPC は通信端末が別のネットワークへ移動し，新たな IP アドレスを取得した場合，その後，送受信する通信パケットに対し，IP 層でアドレス変換処理を行う．これによりエンド端末の上位ソフトウェアから IP アドレスの変化を隠蔽することができる．

IPv4 通信環境ではプライベートアドレス（以後 PA) 空間とグローバルアドレス (以後 GA）空間が存在する．ユビキタスネットワークでは，このようなアドレス空間の違いを意識することなく，通信中に通信端末が自由に移動できることが望ましい．しかし，これまでの移動透過性技術は同一アドレス空間内での移動にしか適用できず，GA 空間と PA 空間といった異なるアドレス空間を対象とした移動透過性についての検討はなされていない．

本稿では Mobile PPC をベースに，異なるアドレス空間を跨る移動通信を実現するための手法を検討した．このようなケースでは，通信経路上にアドレス変換装置 NAT（Network Address Translator) が存在する．Mobile PPC では NAT の存在により通信パケットへのアドレス変換処理がネットワーク構造に対して正しく行われず，通信の継続が出来ない．そこで，通信端末が移動したとき，移動後の NAT の存在有無を確認する．通信経路上に NAT が存在する場合，通信端末は移動後の自身のアドレスと NAT のグローバルアドレスを通信相手に知らせるよう Mobile PPC の機能を拡張する．通信相手はこの情報を参照して，NAT が介在する通信に対応したアドレス変換を行うことで異なるアドレス空間を対象とする移動透過性を実現できる．

2　Mobile PPC

Mobile PPC は第３の特殊な装置を必要とすることなく，エンド端末だけで移動透過性を実現することが出来るプロトコルである．

通信開始時において通信相手の IP アドレスを知ることを「初期 IP アドレスの解決」と呼ぶ．Mobile PPC では初期 IP アドレスの解決にすでに実用的に用いられているダイナミック DNS (DDNS) [5] を利用する．

一方，通信中において，移動端末の移動後の IP アドレスを知ることを「継続 IP アドレスの解決」と呼ぶ．継続 IP アドレスの解決は，Mobile PPC の機能により移動前と移動後の情報を移動した端末から相手に通知することにより実現する．そして，移動前後の情報をもとに通信パケットに対してアドレス変換を行うことで通信の継続を可能にする．

以下に Mobile PPC の機能を詳しく説明する．Mobile PPC を実装する端末では，移動により変化した移動後のコネクション識別子と移動前のコネクション識別子の対応関係を示すテーブル「Connectin ID Table（以後 CIT)」を保持する．コネクション識別子とは通信を行っている両エンド端末の IP アドレスとポート番号の組，プロトコル番号の５つの情報である．パケット送受信の際，CIT の対応関係に従って，IP 層にて通信パケットのアドレス変換を行う．この動作により，上位ソフトウェアに対してアドレスの変化を隠蔽し，通信を継続することが出来る．移動端末が移動し，新たな IP アドレスを取得すると，IP アドレスの変化に対応して CIT レコードの書き換えを行う．

図 1 に Mobile PPC による移動情報の通知方法を示す．同じ場所に位置する通信端末を CN（Correspondent Node），移動する端末を MN（Mobile Node）と呼ぶ．CN，MN は Mobile

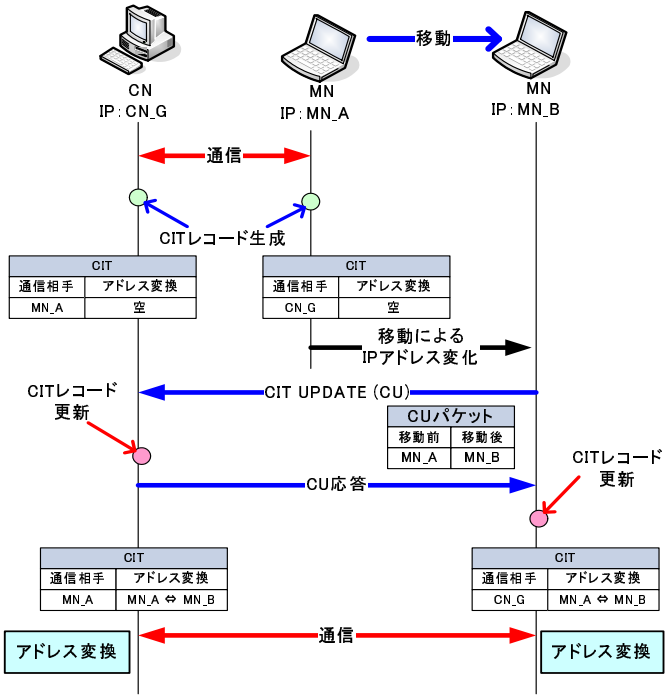


図 1: Mobile PPC による移動情報の通知方法

PPC を実装している．両者の間で通信が開始されると，最初に送受信される通信パケットの情報をもとに CIT レコードが両端末で生成される．この時点での CIT レコードのアドレス変換に利用する情報は空であり，パケットのアドレス変換は行われない．その後，MN が別のネットワークへ移動して IP アドレスが変化すると，その直後に MN から CN に対して移動前と移動後のコネクション識別子を格納したパケットを送信する．このパケットを「CIT UPDATE（以後 CU)」と呼ぶ．CU を受信した CN は，CU 内に格納されている MN の移動前のコネクション識別子に一致する CIT レコードを検索する．そして，一致するレコードに対して，CU に格納されている MN の移動後のコネクション識別子をアドレス変換に利用する情報として書き込む．CN で CIT レコードの更新が完了すると，CN は MN へ CU 応答を返し，それを受信した MN は CN と同様に自身の CIT を更新する．その後の通信では送受信パケットに対して CIT に従った IP アドレスやポート番号のアドレス変換を IP 層で行う．

3　異なるアドレス空間を跨る移動通信

PA 空間と GA 空間を跨る移動には大きく分けて次の A〜D の 4 パターンがある．(A) CN が GA 空間に属し，MN が PA 空間から GA 空間へ移動する．(B) CN が GA 空間に属し，MN が GA 空間から PA 空間へ移動する．(C) CN が PA 空間に属し，MN が PA 空間から GA 空間へ移動する．(D) CN が PA 空間に属し，MN が GA 空間から PA 空間へ移動する．

本稿では，移動パターン A と B について移動透過性を実現する方法を述べる．図 2 に NAT を介した通信例を示す．相手端末 CN は GA 空間に，移動端末 MN は PA 空間に属しているものとする．異なるアドレス空間での通信では，両者の間に NAT の機能を持った装置が必ず存在する．この装置を NAT BOX と

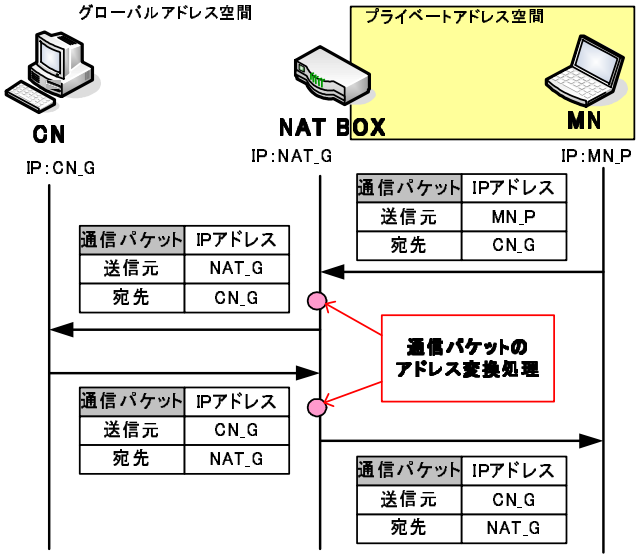


図 2: NAT を介した通信例

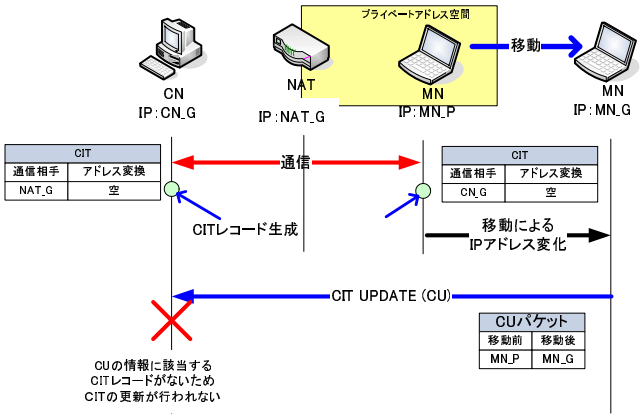


図 3: 移動通信の限界（PA 空間→ GA 空間)

呼ぶ．NAT BOX が介在する環境では，GA 空間側から通信を開始することが出来ない．そのため，ここでは通信の開始は PA 空間側の MN から行うものとする．

最初の通信パケットが NAT BOX を通過する際，パケットの送信元は MN のプライベートアドレス MN_P から NAT BOX のグローバルアドレス NAT_G へと変換され，CN へ送信される．同時に NAT BOX には MN_P と NAT_G を対応付ける NAT テーブルが生成される．CN から MN への返信パケットは，宛先を NAT BOX 宛の NAT_G として送信される．このパケットが NAT BOX へ到達すると，先ほど生成した NAT テーブルに従い宛先 NAT_G が MN_P へと変換され，MN へ届けられる．このように，GA 空間側の CN は通信相手が NAT BOX であるように見える．そのため，CN は通信相手を NAT BOX として CIT レコードを生成する．このような状況で，図 3 のように MN が PA 空間から GA 空間へ移動した場合を考える．MN から通知される CU には MN の移動前情報 MN_P と移動後情報 MN_G の情報が格納されている．しかし，現状の CIT 更新処理では，CU の移動前情報 MN_P に一致する CN の CIT レコードが存在しないため，アドレスの変化に対応した CIT の更新が行うことが出来ない．

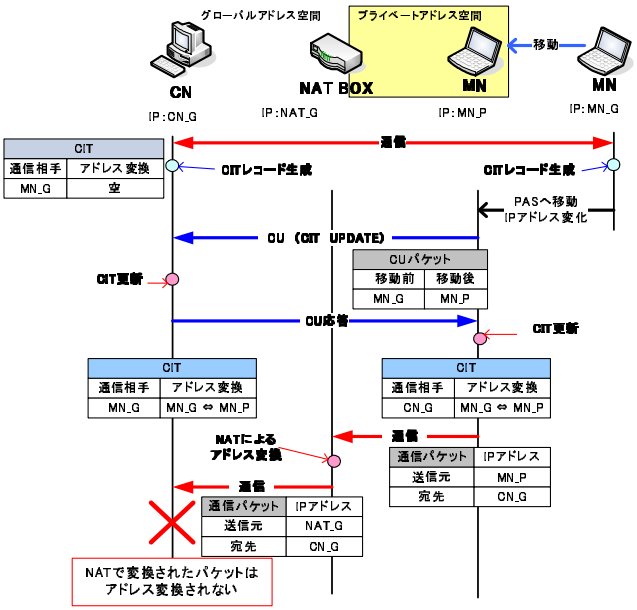


図 4: 移動通信の限界（GA 空間→ PA 空間）

次に，MN が GA 空間で通信を行い，通信中に PA 空間へ移動した場合の様子を図 4 に示す．移動前は GA 空間同士の通信であり，CN と MN の間に NAT BOX は存在しない．CN は通信相手を MN_G として CIT レコードを生成する．MN が GA 空間から PA 空間へ移動し，IP アドレスが変化すると，移動前情報 MN_G と移動後情報 MN_P を格納した CU を CN へ通知する．CN では，CU の移動前情報 MN_G に一致する CIT レコードが存在するため，移動後情報 MN_P をアドレス変換に利用するよう CIT レコードが更新される．しかし，このままでは移動後の NAT が介在するネットワーク構成に対して整合性がとれない．たとえば，移動後に MN から CN へパケットを送信すると，パケットの送信元アドレス MN_P は NAT で NAT_G へ変換され，CN へ到達する．CN では送信元アドレス NAT_G に該当する CIT レコードが存在しないため，パケットに対しアドレス変換が実行されない．従って，移動後はそれまでの通信が継続できない．

4 Mobile PPC の拡張

異なるアドレス空間での移動通信において，Mobile PPC で移動透過性を実現するには CN と MN の通信経路上に NAT BOX が存在するとき，CN は MN のプライベートアドレスと NAT のグローバルアドレスを取得する必要がある．アドレスを取得する方法には拡張 DPRP（Dynamic Process Resolution Protoco）を利用する．DPRP とはシステム構成の変化を動的に管理するプロトコルであり，別途研究が行われている [6] [7]. 拡張 DPRP は通信に先立ち CN と MN の間で実行され，通信経路上での NAT の有無を判別することが可能となる．NAT が存在するとき，MN のプライベートアドレスと NAT のグローバルアドレスを DPRP の制御パケットに格納し，CN へ送信する．

また，CU も拡張する．移動後に MN から CU を送信する際，拡張 DPRP と同様に通信経路上に NAT BOX が存在するかどうかの確認を行う．NAT BOX が存在するとき，CU は NAT

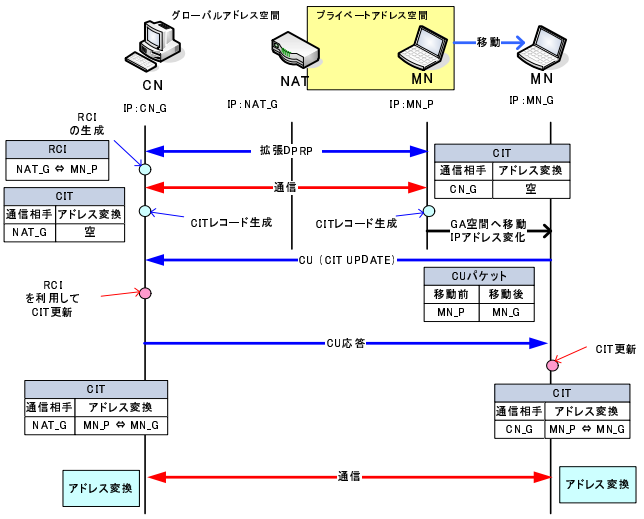


図 5: 移動パターン A への対策（PA 空間→ GA 空間）

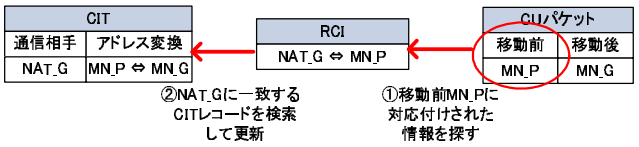


図 6: RCI の参照（PA 空間→ GA 空間）

を通過する際に NAT のグローバルアドレスを取得して CN へ到達する．CU には MN の移動後のプライベートアドレスも格納されているため，CN は MN のプライベートアドレスと NAT のグローバルアドレスを CU から獲得できる．

拡張 DPRP あるいは CU の通知が NAT BOX を介在して実行されたとき，CN は獲得した NAT のグローバルアドレスと MN のプライベートアドレスを相互に対応付けたテーブルを生成し，保持する．このテーブルを「Related Correspondence Information（以後 RCI)」と呼ぶ．そして，端末の移動により自身の CIT 更新を行う際，生成した RCI を参照して，NAT が介在するネットワーク構造に対し整合性が取れるよう CIT の更新を行う．

4.1 移動パターン A への対策

移動パターン A への対策を図 5 に示す．通信に先立ち，拡張 DPRP が端末間で実行される．NAT BOX が介在しているため，拡張 DPRP により CN は NAT のグローバルアドレス NAT_G と MN のプライベートアドレス MN_P を獲得する．そして，CN は NAT_G と MN_P を対応付けた RCI を生成し，保持する．

MN が通信中に GA 空間へ移動すると，MN は従来と同様に，アドレスが変化した直後に CU を通知する．これを受信した CN は CIT 更新の際，RCI を参照する．図 6 に RCI を参照した CIT 更新方法を示す．通知された CU の移動前情報 MN_P に対応付けられた NAT BOX のアドレス NAT_G を RCI から検索する．次に NAT_G を用いて，CIT レコードの検索を行う．CN の CIT レコードには NAT_G に一致する情報があるため,CU の移動後情報 MN_G をアドレス変換に利用する CIT 更新処理を

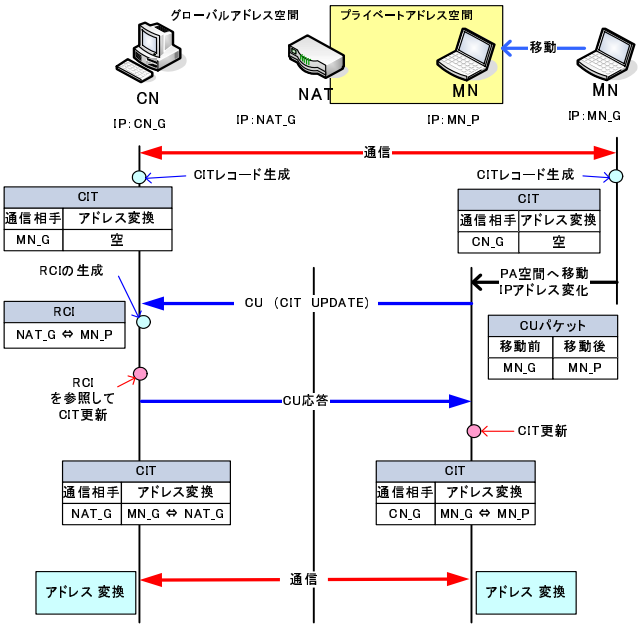


図 7: 移動パターン B への対策（GA 空間→ PA 空間)

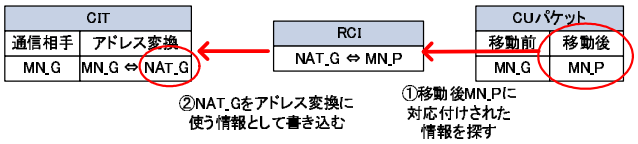


図 8: RCI の参照（GA 空間→ PA 空間）

実行することが出来る．

4.2 移動パターン B への対策

MN が GA 空間で通信中に PA 空間へ移動する場合の例を図 7 に示す．はじめに MN は GA 空間に属している．CN との通信開始時に DPRP が行われるが，MN と CN との間に NAT が介在していないため，CN は RCI を生成しない．その後，通常の通信により CN は MN を通信相手として CIT レコードを生成する．次に MN は NAT BOX 配下の PA 空間へ移動すると，MN から CN へ CU を通知する．CN と MN の間に NAT BOX が存在しているため，CU が NAT を通過する際，NAT のグローバルアドレス NAT_G を取得して CN へ届けられる．従って，CN は MN のプライベートアドレス MN_P と NAT のグローバルアドレス NAT_G を CU から知ることが出来る．CU が NAT BOX を介して CN へ通知されたとき，移動パターン A と同様に，CN は NAT_G と MN_P を対応付けた RCI を生成し，保持する．その直後，RCI を参照し CIT 更新を行う．

図 8 に RCI を参照した CIT 更新の方法を示す．更新する CIT レコードの検索は CU の移動前情報 MN_G で行う．CIT レコードの更新を行う際，CU の移動後情報 MN_P に対応付けられた NAT のグローバルアドレス NAT_G を RCI から検索する．そして，NAT_G をアドレス変換に利用する情報として CIT レコードに書き込む．以上のような処理を行うことで，以後の通信では整合性のとれたアドレス変換を行うことができ，移動透過性を実現できる．

4.3 その他の移動パターンへの対策

移動パターン C と D では，CN が NAT 配下の PA 空間に属するため，MN から通信を開始することが出来ない．CN から通信を開始したとしても，MN が CN とは異なる PA 空間に属していると NAT を越えた通信は出来ない．この問題を解決するために，我々は NAT- f（NAT-free Protocol）[8] と呼ぶ技術の開発を別途行っている．NAT-f は GA 空間と PA 空間のそれぞれに属する端末間の通信において，GA 空間側からの通信開始を可能とする技術である．移動パターン C，D では NAT-f の技術を利用し，Mobile PPC をさらに拡張することによって移動透過性を実現する．

5 むすび

Mobile PPC の機能を拡張し，PA 空間と GA 空間を跨る移動透過性を実現するための検討を行った．従来の Mobile PPC では，NAT が介在する異なるアドレス空間での通信において，整合性の取れたアドレス変換処理が実行されず，通信が継続できない．移動端末が通信開始時に NAT 配下の PA 空間に属しているときには拡張 DPRP を利用し，通信中に PA 空間へ移動したときには CU を利用することで通信相手は移動端末のプライベートアドレスと移動端末のグローバルアドレスを知る．そして，通信相手はこれらの情報を対応付けたテーブルを生成し，CIT 更新の際に，このテーブルを参照して整合性の取れるよう CIT を更新することで問題を解決している．

今後は今回未検討である移動パターンについて検討を行っていく．また，提案方式の実装と，その有効性の確認を行う．

参考文献

[1] 寺岡文男,“ インターネットにおけるノード移動透過性プロトコル, ”電子情報通信学会論文誌, Vol.J87-D-I, No.3,pp.308-328, March.2004.

[2] C. E. Perkins, “ IP Mobility Support for IPv4, ” RFC 3344, Aug. 2002.

[3] M. Kunishi, M. Ishiyama, K. Uehara, H. Esaki, and F.Teraoka, “ LIN6: A new approach to mobility support in IPv6 ”, Third International Symposium on Wireless Personal Multimedia Communications, pp.1079-1084, Nov. 2000.

[4] 竹内元規, 鈴木秀和, 渡邊晃：モバイル端末の移動透過性を実現する Mobile PPC の実装, 情報技報, 2005-DPS-122, pp.351-356 (2005)

[5] Vixie（Ed.）, P., Thomson, S., Rekhter, Y. and J. Bound, : ”Dynamic Updates in the Domain Name System ”, RFC2136, April 1997

[6] 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 ”, 研究報告「コンピュータセキュリティ」No.2005-CSEC-028 , March 2005

[7] 後藤裕司, 鈴木秀和, 渡邊晃：グローバルアドレスとプライベートアドレス空間を跨る DPRP の検討, 情報処理学会第 68 回全国大会 講演論文集, March 2006

[8] 加藤尚樹, 柳沢信成, 鈴木秀和, 渡邊晃, ”アドレス空間の違いを意識しない通信方式 NATF の提案と実装”, 情報技報, 2005-DPS-122, pp.351-356 (2005)

プライベートアドレス空間とグローバルアドレス空間を跨る移動通信の実現

名城大学大学院理工学研究科
榎本 万人　鈴木 秀和　坂本 順一　渡邊 晃

研究背景[1]

■ ユビキタスネットワーク環境

- モバイル端末や無線環境の普及
- プライベート空間とグローバル空間が存在

  ⇒ 異なるアドレス空間において通信中に自由に移動できることが望ましい

- 既存の移動透過性技術
  - 移動範囲が同一アドレス空間内に限定
  - 異なるアドレス空間を跨る移動通信は対象外

⇒ NATの存在が通信の継続を阻害する

Mobile PPCによる
異なるアドレス空間を対象とした移動透過性を検討

Mobile PPCの概要

Mobile PPC（Mobile Peer to Peer Communication）

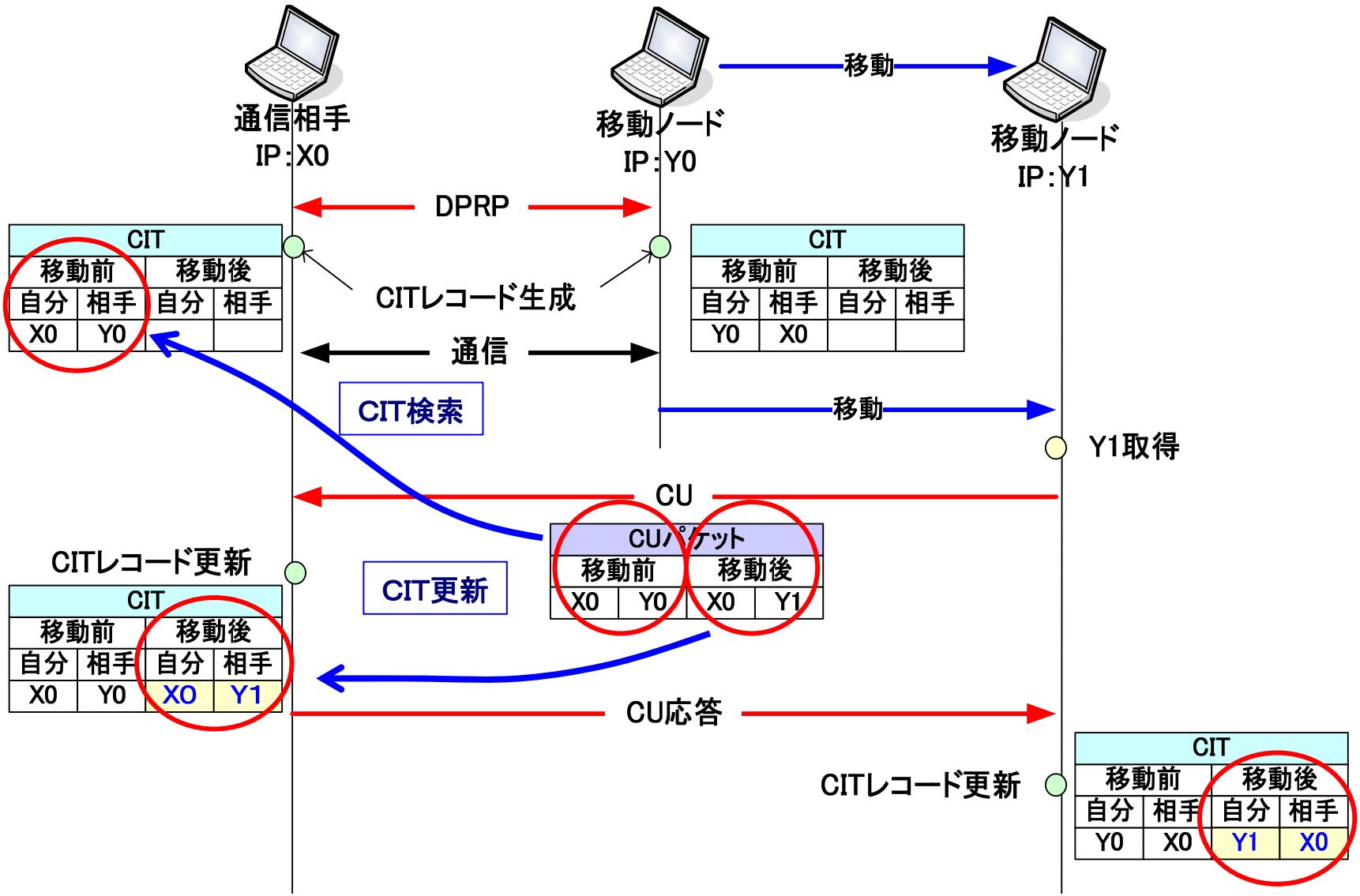
特殊な装置を必要としない
P2P方式で移動透過性を実現

- Mobile PPCの機能をIP層に追加
- 通信端末はCIT（Connection ID Table）を保持

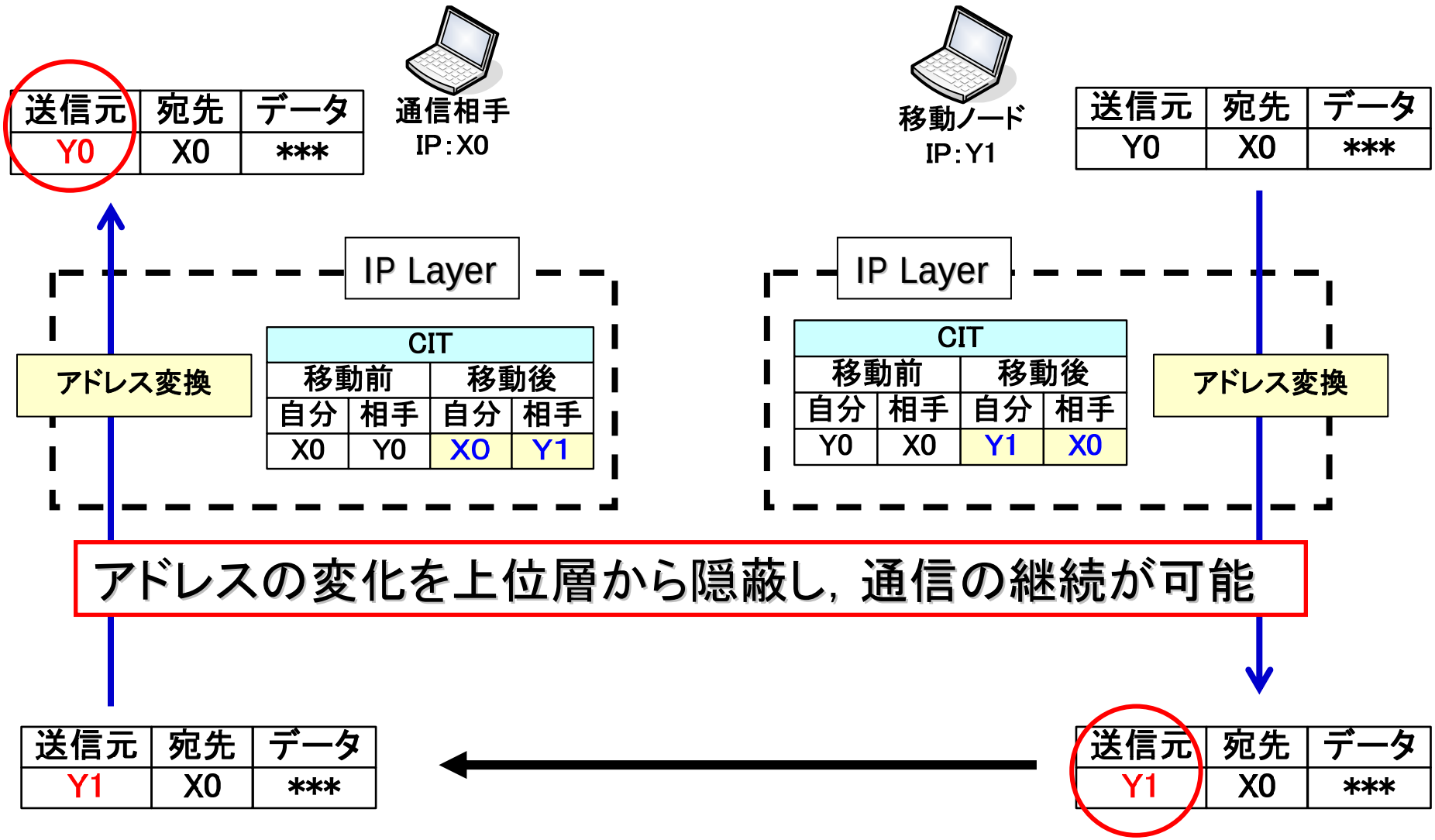
CIT：　移動前後の通信情報（IPアドレス）
の対応関係を示すテーブル

- IPアドレス変化 ⇒ CU（CIT UPDATE）により移動情報を通知
- CUを受信するとCITの情報を更新
- パケットに対し，エンド端末でCITに基づいたアドレス変換を行う

Mobile PPCによる通信[1]



Mobile PPCによる通信[2]

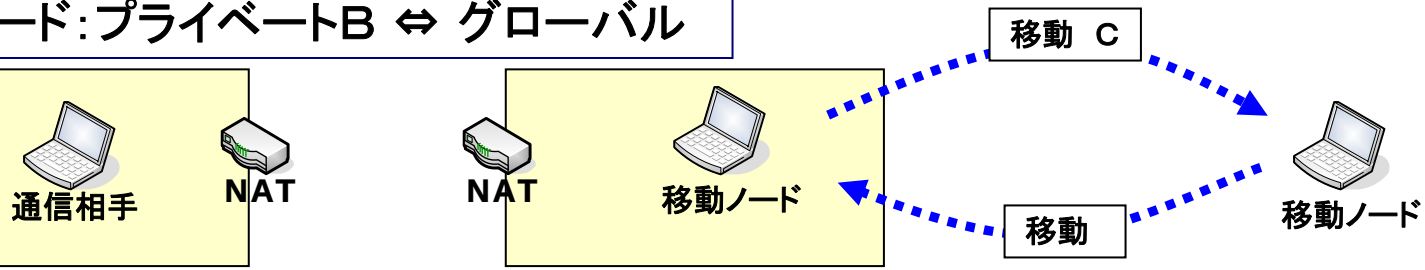


異なるアドレス空間の移動パターン

今回の検討対象

通信相手：グローバル
移動ノード：プライベート ⇔ グローバル

通信相手：プライベートA
移動ノード：プライベートB ⇔ グローバル

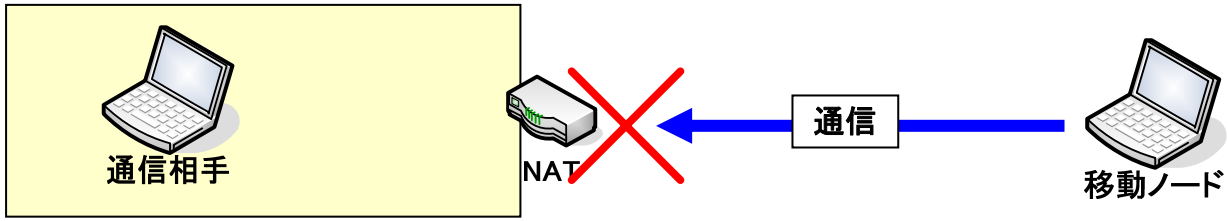


通信相手：プライベートA
移動ノード：プライベートA ⇔ グローバル

グローバル側からの通信開始の場合

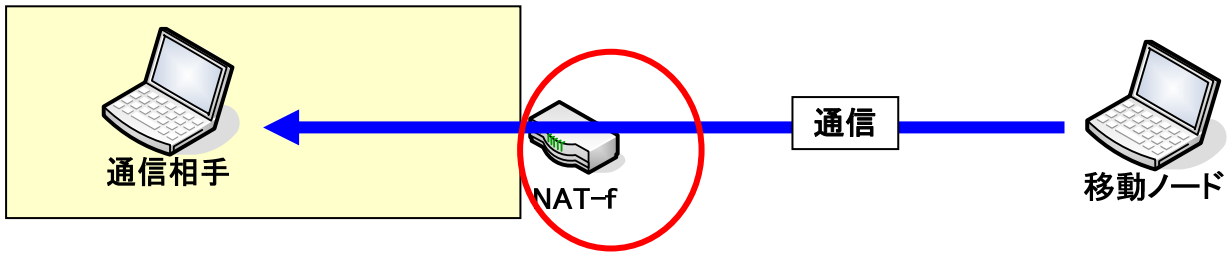
NAT越え問題

グローバル空間側から通信を開始することが出来ない



NAT-f を適用

グローバル空間側から通信開始を可能にする

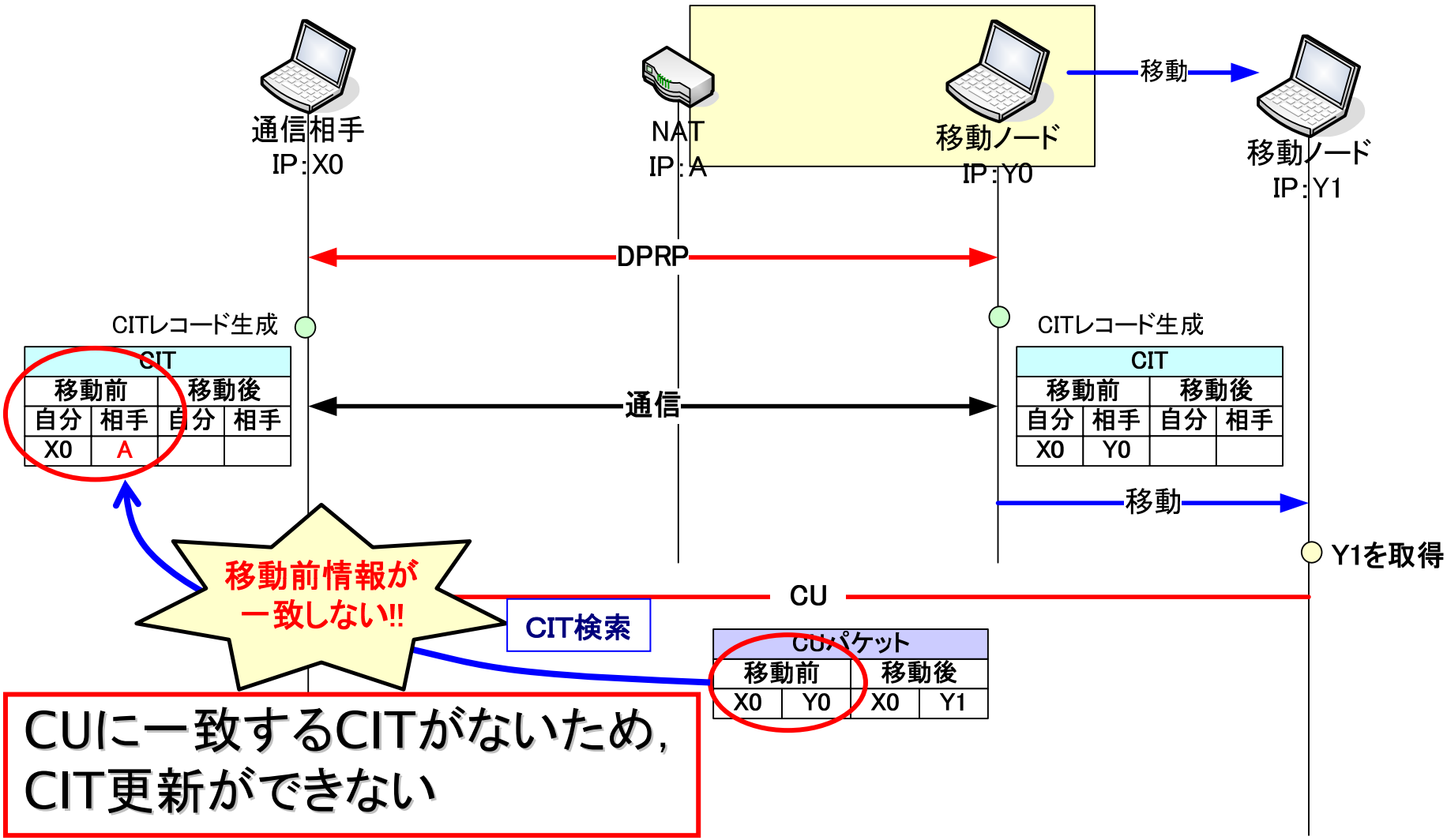


［4D1］アドレス空間透過性を実現するNAT-fの実装と評価　鈴木秀和　渡邊晃

以後の説明ではNAT越え問題は解決されているものとする

アドレス空間を跨る通信[1]

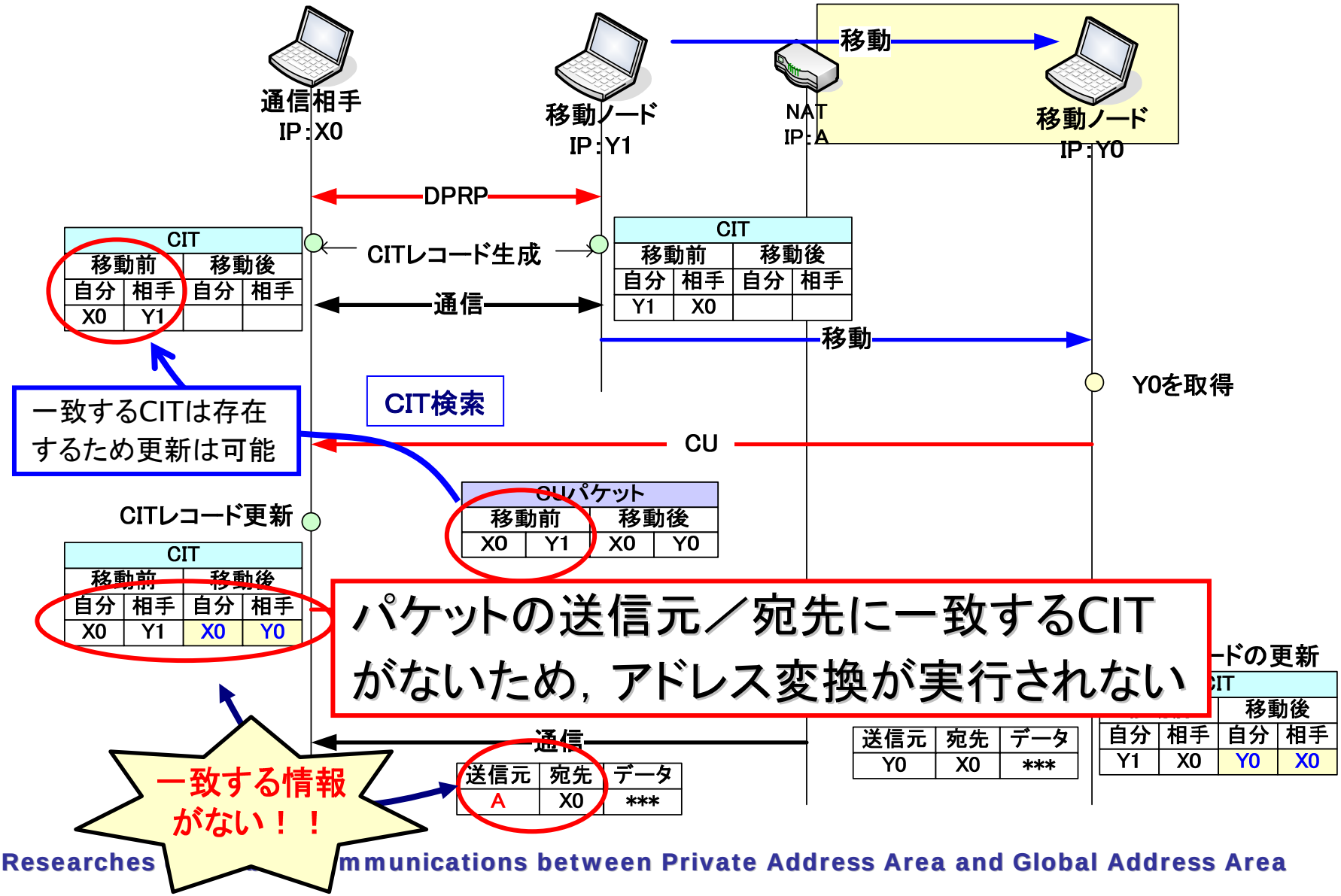
移動パターンA
通信相手:グローバル
移動ノード:プライベート ⇒ グローバル



CUに一致するCITがないため，
CIT更新ができない

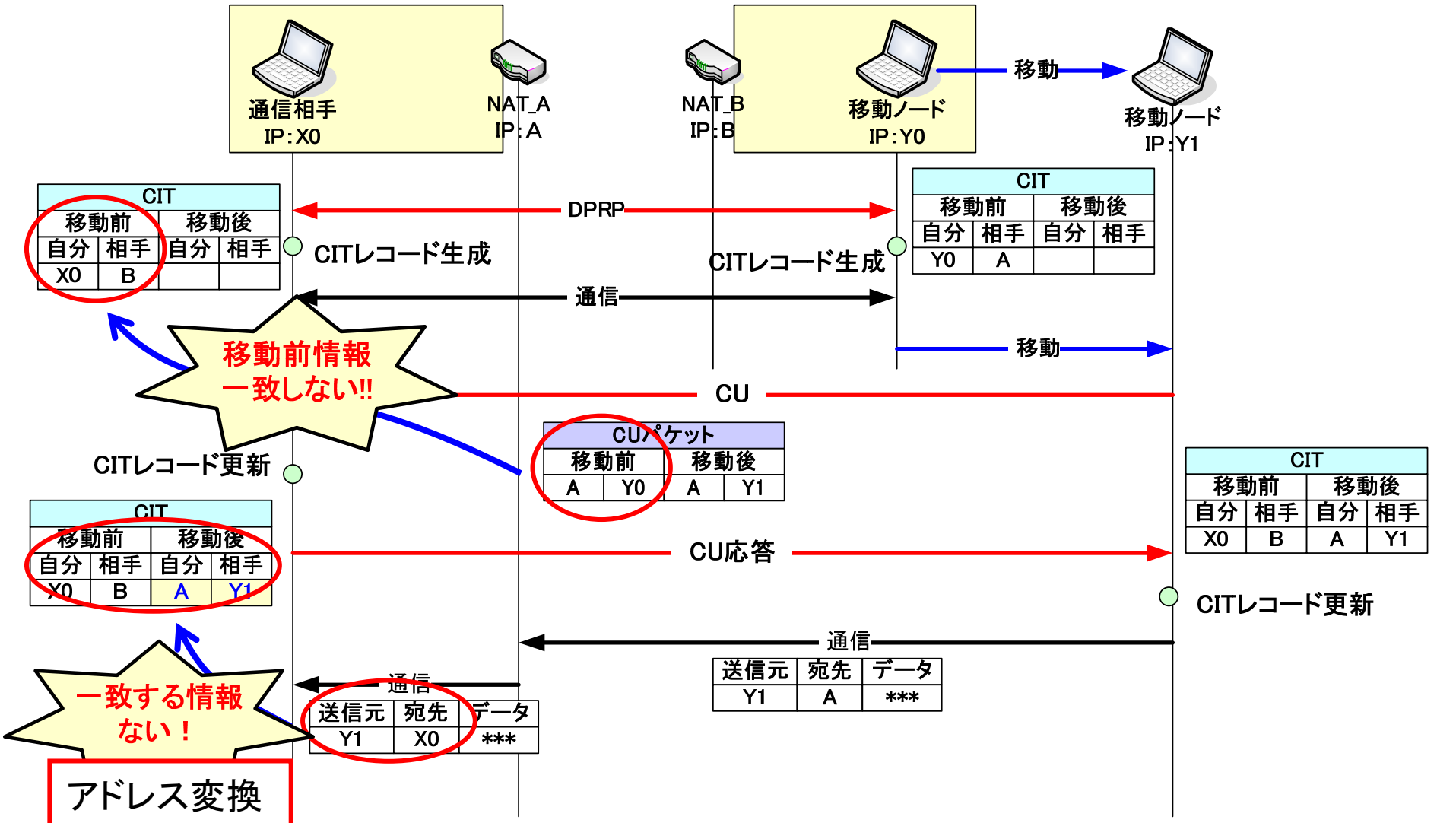
アドレス空間を跨る通信[2]

移動パターンB
通信相手：グローバル
移動ノード：グローバル ⇒ プライベート



アドレス空間を跨る通信[3]

移動パターンC
通信相手：プライベートA
移動ノード：プライベートB ⇒ グローバル



NATによる移動透過性の阻害

移動透過性技術は

- 同一アドレス空間内の移動
  ⇒通信継続は可能

- グローバル空間とプライベート空間を跨いだ移動通信
  ⇒ NATが介在するため，通信継続が出来ない

Mobile PPCの場合，CITが正しく更新できない

NATが介在するネットワーク構成に対し
整合性の取れたCITの更新を行う手法を提案

提案手法の概要[1]

通信相手は以下の情報を知る必要がある

- 移動ノードがプライベート空間に属する
  ⇒ 移動ノードのプライベートアドレス
- 自分がプライベート空間に属する
  ⇒ 自分が属するNATのグローバルアドレス

これらのアドレスを知る方法として
DPRP（Dynamic Process Resolution Protocol）を利用

- 通信に先立ち制御パケットの交換を行う
- 通信経路上に存在する装置が情報を交換
- CU通知・応答の際にも装置間で情報交換

提案手法の概要[2]

- 通信に先立ち　DPRP
- 通信中の移動より　CU

整合性のとれたCIT更新に必要な情報を付加できるようにする

通信端末がプライベート空間に属する場合

⇒ NATのグローバルアドレスと端末のプライベートアドレス

を獲得できる

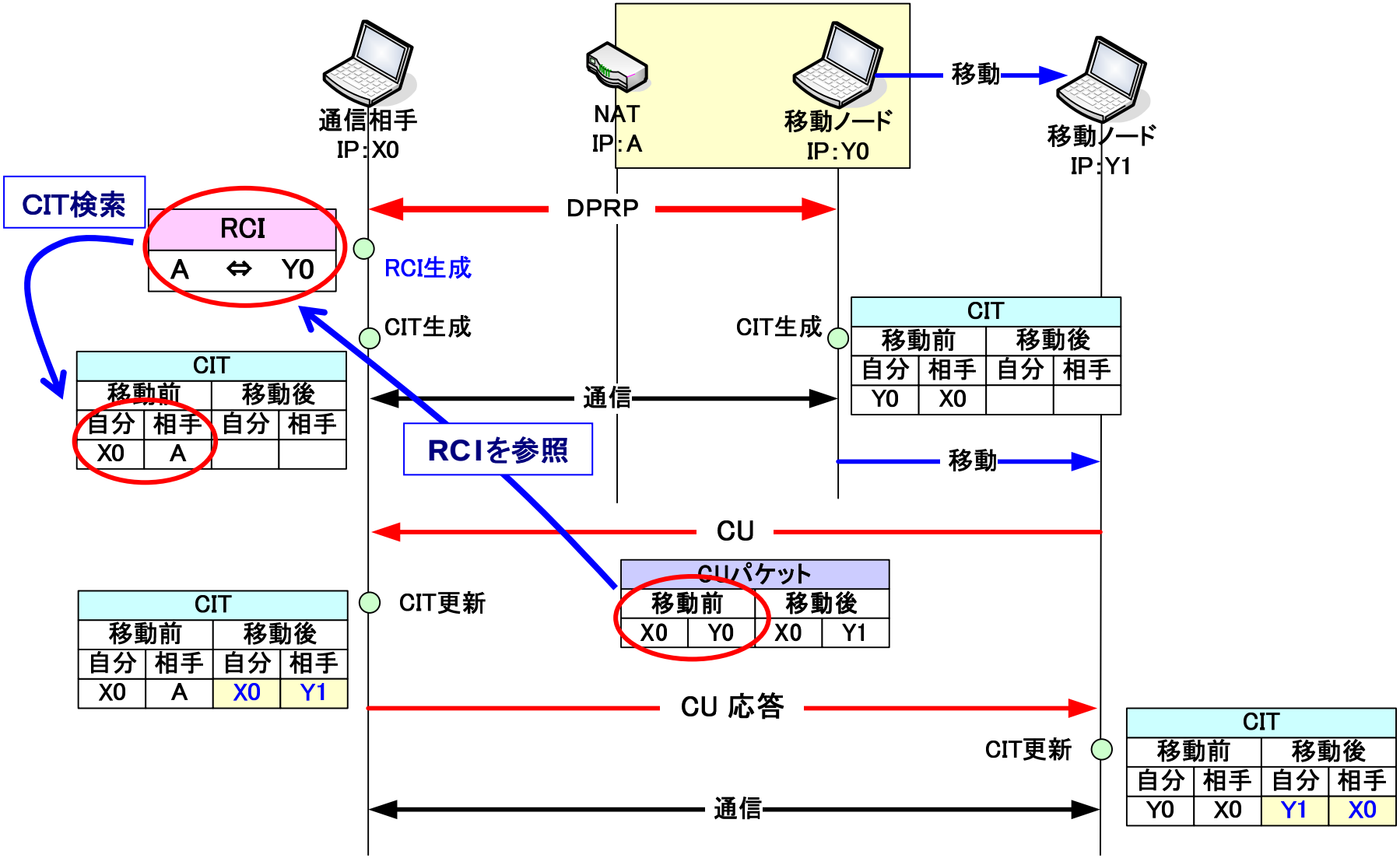
これらのアドレスを対応付けたテーブル
RCI(Related Correspondence Information)を生成する

RCI
NATのグローバルアドレス　⇔　端末のプライベートアドレス

RCIテーブルを利用し，整合性の取れたCIT更新を行う

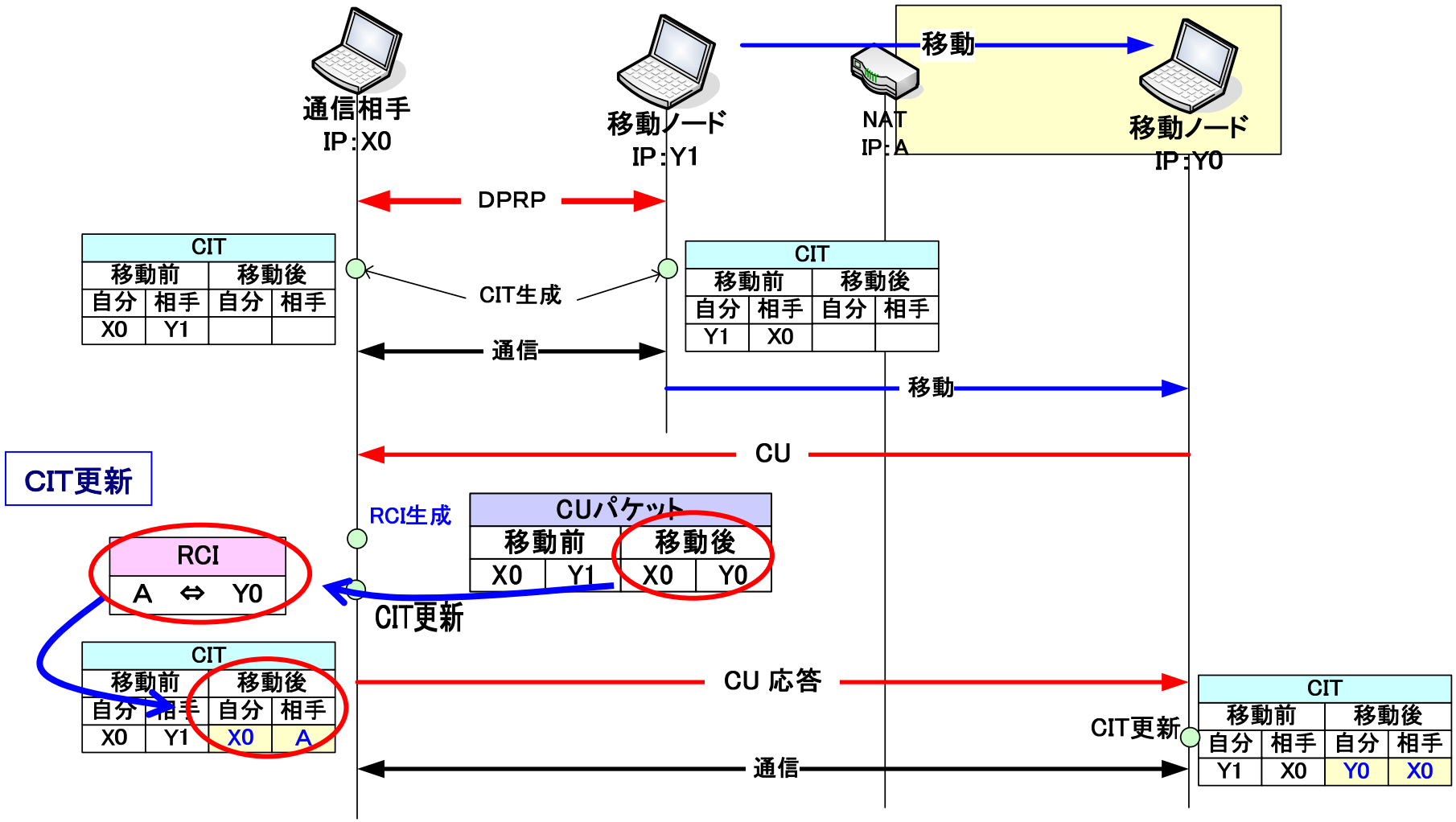
提案方式の通信[1]

移動パターンA
通信相手:グローバル
移動ノード:プライベート ⇒ グローバル



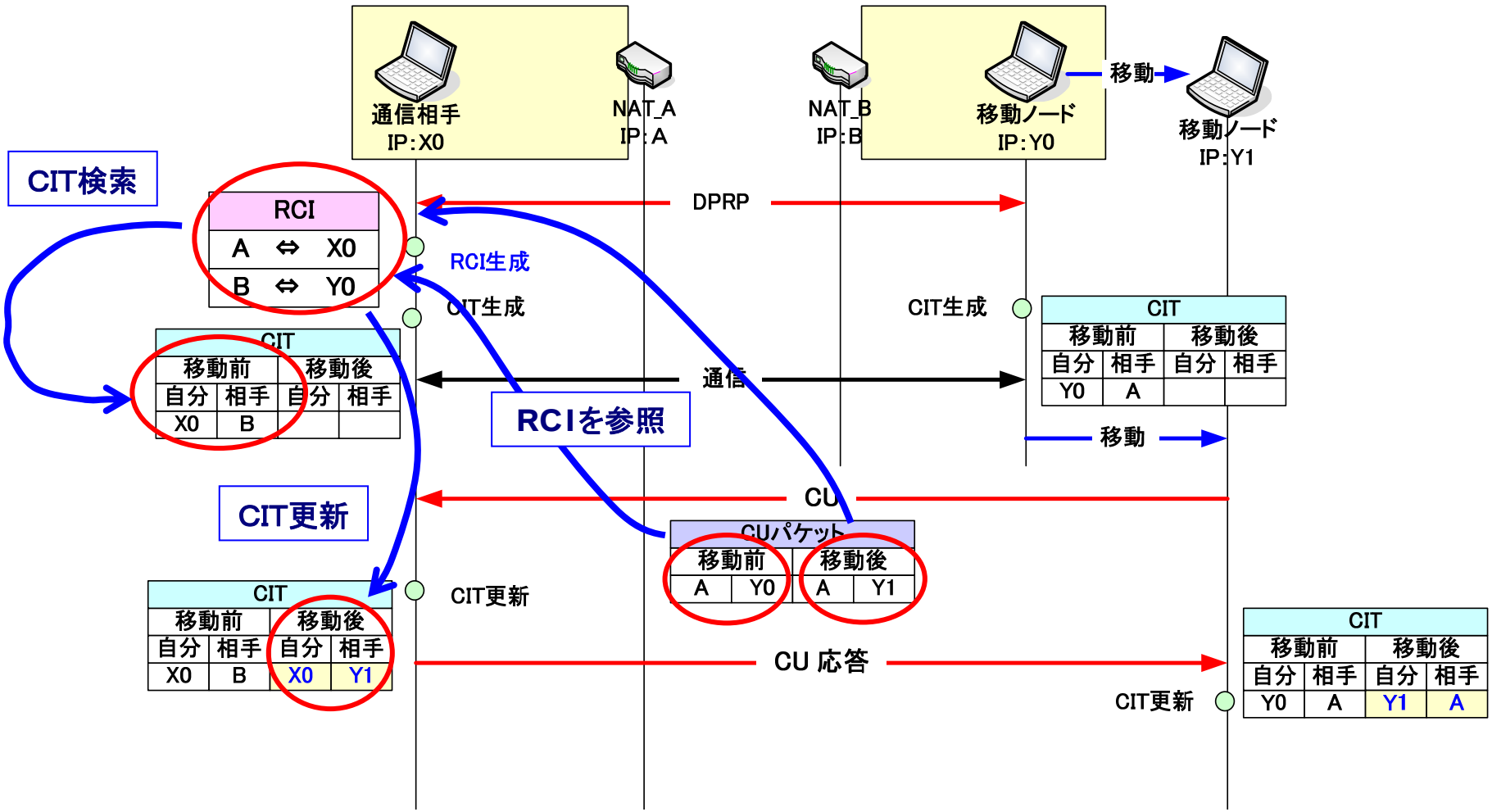
提案方式の通信[2]

移動パターンB
通信相手:グローバル
移動ノード:グローバル ⇒ プライベート



提案方式の通信[3]

移動パターンC
通信相手：プライベートA
移動ノード：プライベートB ⇒ グローバル



むすび

- まとめ

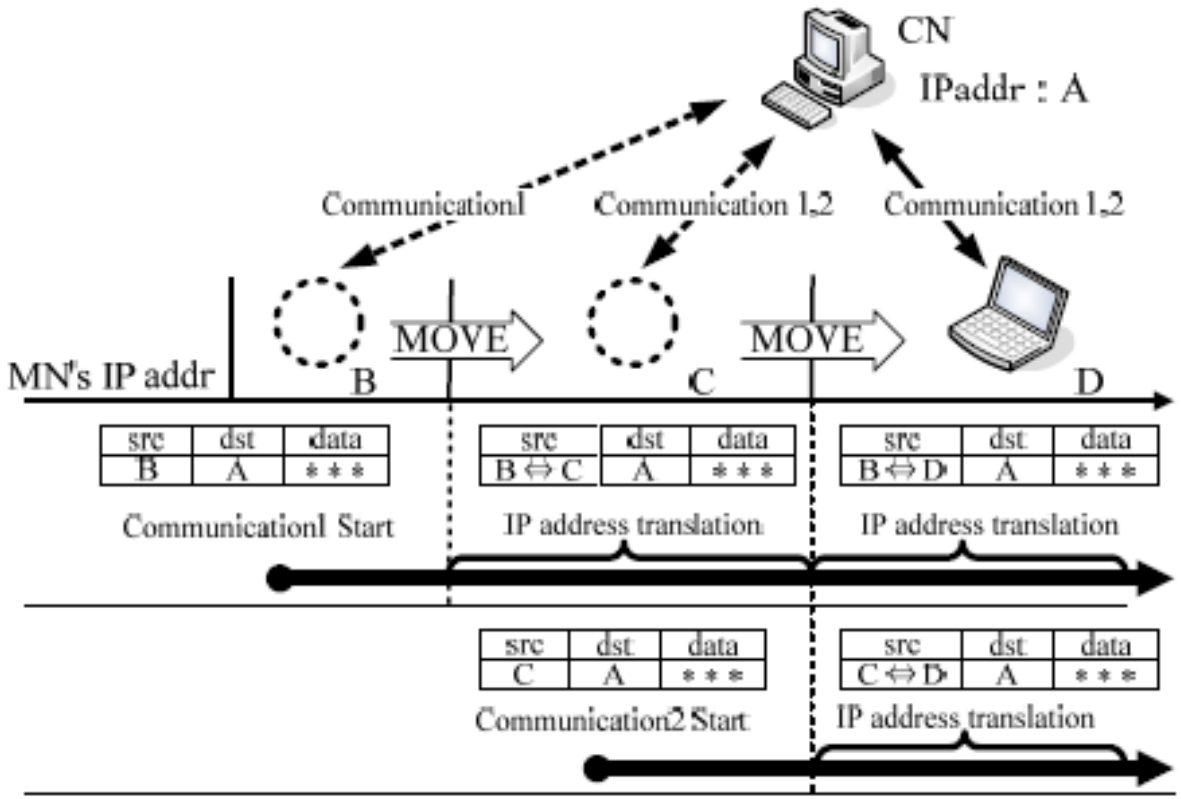
  Mobile PPCによる異なるアドレス空間を対象とした移動透過性を検討

  - NATと通信端末の対応関係を示すRCIを生成し、それを利用してCITを更新

- 今後

  - 通信相手と移動ノードが同一プライベート空間にいる場合の移動パターンを検討
  - 提案手法の実装，評価

連続移動への対応



- CITの移動前情報は常に通信開始時の情報
- 通信開始時 「B」
- 移動1 「C」に変化

  B ⇔ C
- 移動2 「D」に変化

  B ⇔ D

旧IPアドレスが再利用された場合

- アドレス変換を適応する通信と，新しく開始する通信の上位層における通信識別子（両端末のIPアドレス，ポート番号，プロトコル番号）が一致する場合

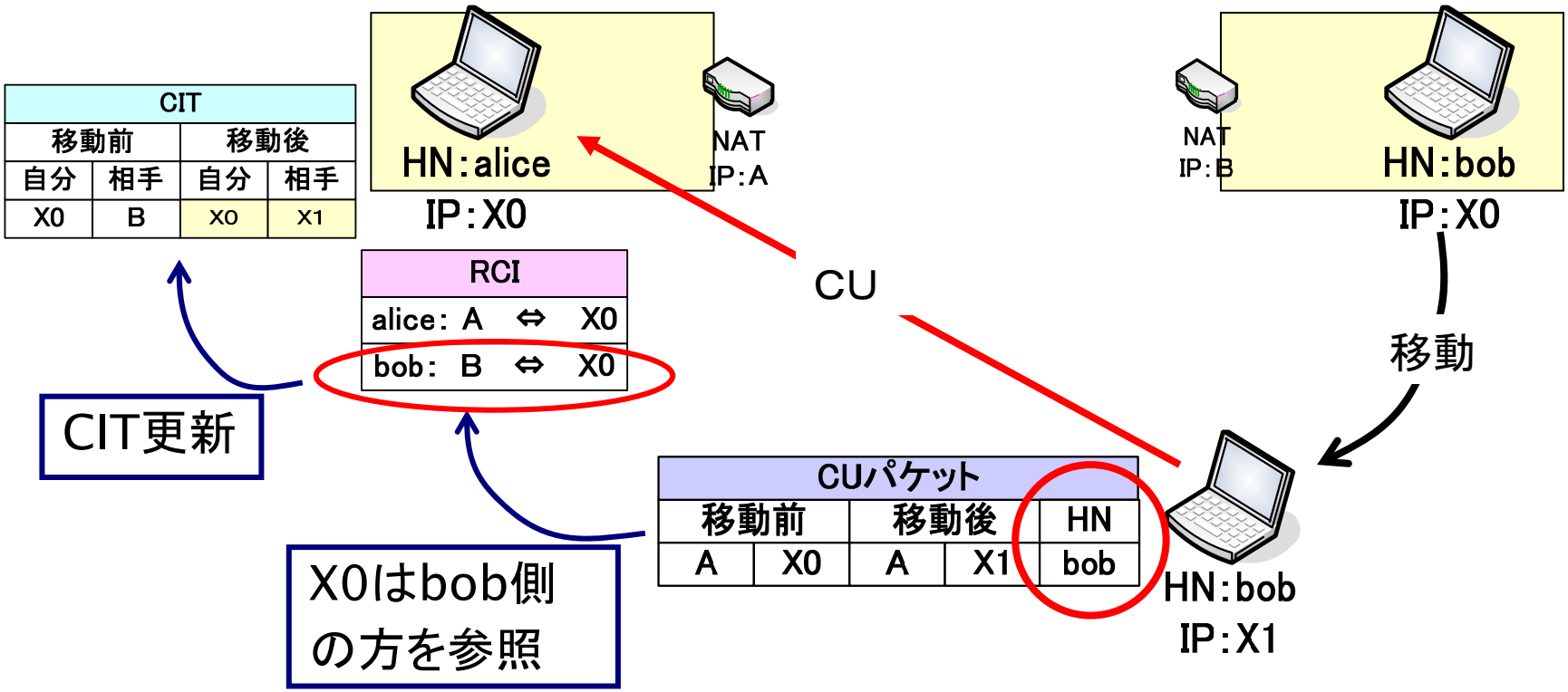
⇒　Mobile PPCでは新たな通信の通信識別子が通信中の通信識別子と一致することを検出.

新たな通信に対してポート変換を適応する.

※CIT内の変換情報にはIPアドレスのほかにポート番号も含まれている.

別プライベート空間で同一IPアドレス利用の場合

- DPRP，CUには通信端末のホスト名も格納される．RCI生成にホスト名も付加．



我々の研究室で目指すもの

セキュア通信アーキテクチャ

柔軟性とセキュリティを兼ね備えたグループ通信

- DPRP　－　グルーピング通信を実現
- Mobile　PPC　－　自由な移動通信を実現
- NAT- f　－　ホームネットワークへのアクセスを実現

DPRPネゴシエーション

- 端末間の認証
- グループ情報，動作モードの交換
- 動作処理情報の決定と通知

⇒

- 相手端末の認証
- 通信の暗号化

Mobile IPv4によるNAT越え移動での通信継続[1]

- 移動端末（MN）が通信中にNAT配下へ移動した場合
  - MNがホームエージェント（HA）へ気付アドレス（CoA）として送信するIPアドレスはHAにとって意味がないもの
  - Mobile IPにおけるカプセル化通信は上位層（トランスポート層）が使用するポート番号などの情報を含まないため，NAT/NAPTはパケットの受け渡し先の端末を判別できなくなる．

⇒ NATにFAの機能が付いていない限り，通信の継続ができない．

Mobile IPv4によるNAT越え移動での通信継続[2]

- NATに対応する場合
  - 規定のトンネリングでは対応できない
  - UDP(ポート434)を利用したトンネリングにより対応できる
  - RFC3519

Mobile PPC実装によるパケット処理時間

表 1　パケット処理時間

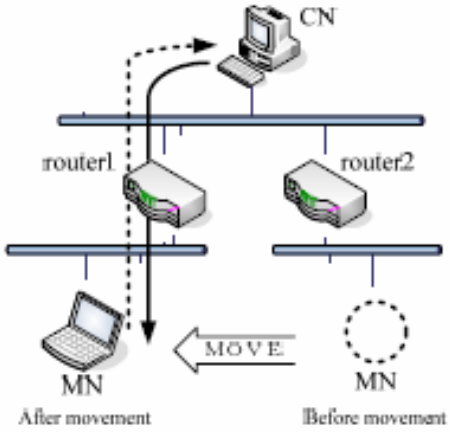
Table 1　Packet processing time.

アドレス変換の有無	変換なし	変換あり
パケット処理時間の平均 [μ秒] (パケット処理時間の占める割合[%])	0.31 (1.47%)	0.54 (2.53%)
パケット中継にかかる処理時間 [μ秒]	21.03	21.26

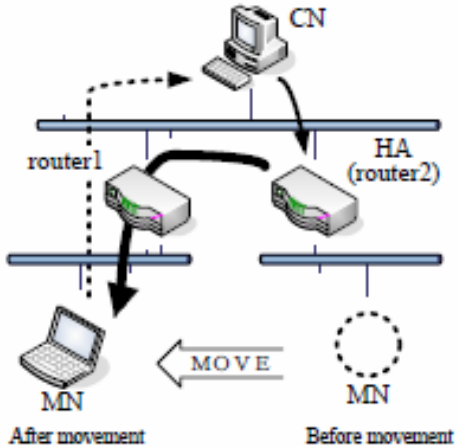
パケット処理時間とは，ip_input/ip_outputからMobile PPCモジュールが呼び出されアドレス変換が行われた後，差し戻すまでの時間．すべてのパケットに対しCIT検索が行われるため，そのオーバヘッドを調査．パケット処理時間の占める割合はアドレス変換を行わない場合1.47%，アドレス変換を行う場合は2.53%

⇒　Mobile PPCをじっそうしたことによるオーバヘッドの増加を小さいといえる

Mobile IPv4とのスループット比較



(a) Mobile PPC の構成



(b) Mobile IP の構成

表5 スループットの比較

Table 5 Comparison of throughput.

状態		スループット	割合
General	case1	93.237 Mbps	100.000
Mobile PPC	case2	93.236 Mbps	99.999
	case3	93.193 Mbps	99.953
Moible IP	case4	93.231 Mbps	99.994
	case5	85.202 Mbps	91.382

Case1：Mobile PPCを実装しない状態

Case2：Mobile PPCで移動前

Case3：Mobile PPCで移動後

ほとんどスループット低下はない

Case4：Mobile IPで移動前

Case5：Mobile IPで移動後

移動後，IPカプセル化と経路冗長により9%のスループット低下