Mobile PPC における認証方式の提案

瀬下　正樹†　竹内　元規‡　渡邊　晃†
名城大学理工学部†　名城大学大学院理工学研究科‡

１．はじめに

ノートパソコンや PDA(Personal Digital Assistant)などのモバイル端末の普及と，無線ネットワーク環境の広がりにより，端末が自由に移動しながらインターネットに接続するという利用形態が増えつつある．そのような状況下では，端末が移動しても通信を継続することが要求されるが，移動に伴い IP アドレスが変化するため，この要求を満たすことが難しい．そこで，端末の移動による IP アドレスの変化を隠蔽し，通信を継続できるようにする移動透過性の研究が行われている．

移動透過性保証プロトコルとして Mobile IP[1]が提案されているが，ホームエージェント(以下 HA)と呼ぶ特別な位置管理エージェントを用意する必要があり，導入するための敷居が高い．我々は，特別な位置管理エージェントを不要とし，常時 P2P 通信をおこなうことができる Mobile PPC[2]の研究を行っている．しかし，これまでの Mobile PPC には移動ノード(以下 MN)が移動した際に通信相手ノード(以下 CN)との間で成りすましを防止するための認証機構が定義されていなかった．そこで，本研究では Mobile PPC における認証方式についての提案を行う．

２．Mobile IP

Mobile IP においては，MN はノード固有の IP アドレスであるホームアドレスと移動先で割り当てられる気付けアドレスの二つの IP アドレスを持つ．MN は気付けアドレスが変わると HA へホームアドレスと気付けアドレスの対応関係を登録する．登録の際には，セキュリティの観点から HA は MN を認証する必要があるが，HA と MN の間に事前に共有鍵を保持させておき，この共有鍵を使った認証を行う．

Mobile IP によるデータ通信を図 1 に示す．CN は MN へパケットを送信する場合は，宛先を MN のホームアドレスとして送信する（①）．ホームアドレス宛のパケットは HA が受信する（②）．HA は MN から常に最新の気付けアドレスの通知を受けているため，ホームアドレス宛のパケットの宛先を知ることが可能となる（③）．この際，HA は MN にパケットが CN から送信されているように見せかけるためにトンネリング処理を行う（④）．MN から CN へのパケットは送信元をホームアドレスとして CN に直接送信する（⑤）．しかし，送信元アドレスとして使われるホームアドレスがインターネット内での位置を正しく表していないため，途中のルータで不正パケットと見なされ破棄されてしまう可能性があり，このような場合は HA を経由するトンネリング処理を行う必要がある．

Mobile IP の問題点は，HA という特殊な装置が必要であり導入するための敷居が高いということと, HA を経由した冗長な通信経路になることが挙げられる．また HA は複数設置することができないため, HA による一点障害の危険がある．

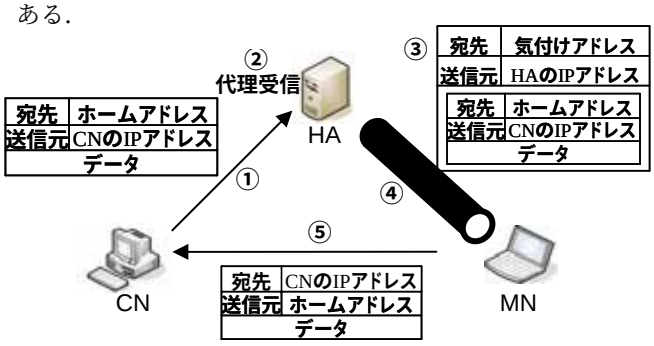


図１．Mobile IP の通信

なお Mobile IPv6[3] では通信経路の冗長を解決するために CN と MN が直接通信する経路最適化機能が追加された．経路最適化機能は CN にもホームアドレスと気付けアドレスの対応関係を保持させ，IP 層において対応表と拡張ヘッダを利用したアドレス変換を行うことによって移動性を可能にしている．しかし，通信初期の数パケットや登録の際の認証において HA を使用するため， HA による一点障害の問題は解決されていない．また，拡張ヘッダの追加によりヘッダオーバヘッドが発生する．

３．Mobile PPC とその課題

３．１　Mobile PPC の概要

Mobile PPC では，通信開始時において相手の IP アドレスを知る方法(初期 IP アドレスの解決)と通信中に IP アドレスが変化しても通信を継続できる方法(継続 IP アドレスの解決)を異なるアプローチによって解決しており，後者が Mobile PPC 特有の機能である．初期 IP アドレスの解決には，ホスト名と IP アドレスの関係を動的に管理する Dynamic DNS(DDNS)を利用する．これにより，ホスト名を識別子として通信開始時における端末の IP アドレスを知ることが可能となる．一方，継続 IP アドレスの解決には，IP アドレスが変化した直後に MN から CN に対して，移動後の IP アドレスと継続させる通信の識別情報を Binding UPDATE(以下 BU)により通知する．BU により，エンド端末間では新旧 IP アドレスの対応関係を示すテーブルが作成され，以後の通

“Proposal of Authentication Mechanisms in Mobile PPC”
†Masaki Sejimo & Akira Watanabe
Faculty of Science and Technology，Meijo University
‡Motoki Takeuchi
Graduate School of Science and Technology，Meijo University

信では図 2 のようにパケット送受信時に IP 層でこのテーブルを参照してアドレス変換を行う．これにより，TCP/IP プロトコルスイートを含む上位ソフトウェアに対し IP アドレスの変化を隠蔽し，通信を継続させることができる．Mobile PPC では拡張ヘッダや HA を使用しないため，ヘッダオーバヘッドや HA を経由することによる通信経路の冗長および一点障害などの問題がない．また IPv4 と IPv6 のどちらにも実装可能である．

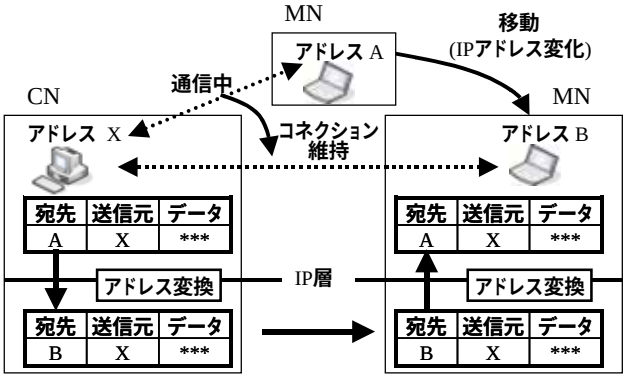


図 2. アドレス変換の例

3.2 Mobile PPC の課題

現状の Mobile PPC は FPN (Flexible Private Network) [4]という閉じた環境を前提に検討されているため FPN 以外の環境では移動時の成りすましに対する認証機能がなく汎用性に欠けている．FPN 以外の環境で使用する場合，セキュリティの観点から BU パケットの確実な認証が必要である．

端末間で認証を行う方法として，共有鍵暗号を利用した認証と公開鍵暗号を利用した認証がある．前者は認証したい相手端末と共有鍵，後者は認証したい相手端末の公開鍵，を事前に設定しておく必要があるが，Mobile PPC では CN と通信する MN は任意であるため事前に鍵を設定しておくことは難しい．なお，公開鍵暗号を利用した認証は，PKI を利用することで，事前に鍵を設定しておかなくても認証したい相手端末の公開鍵を安全に取得することができるが，現在の PKI が未整備である状況を考慮すると現実的でない．このため，Mobile PPC における端末間の認証では，CN と MN の間で認証に使用する鍵をどのようにして安全に交換するかが解決すべき課題となる．

Mobile IPv6 で導入されている Return Routability では HA と MN の静的な関係を利用した鍵交換経路の工夫により CN と MN 間で安全に共有鍵を生成することができるが，HA のような特別な位置管理サーバを使用しない Mobile PPC においては Return Routability の適用は難しい．

4．Mobile PPC における認証方式の提案

本研究では BU における MN を認証するための機構として，Diffie-Hellman 鍵交換[5]を利用した認証方式を提案する．Diffie-Hellman 鍵交換とは，両端末間において，離散対数問題を利用したアルゴリズムにしたがって生成した乱数を交換することにより，その乱数を盗聴されたとしても盗聴者には知ることのできない共有鍵を生成する鍵交換方式である．本提案方式では Diffie-Hellman 鍵交換を通信に先立って実行しておくことにより MN と CN に共有鍵を保持させておき，移動時にこの共有鍵を用いて BU パケットの認証を行う．

認証方式の流れを図 3 に示す．通信に先立って，Diffie-Hellman 鍵交換のアルゴリズムによって生成した乱数を両端末間で交換し（①，②），共有鍵を生成する（③）．その後，通常の IP 通信が行われる．MN が移動し，IP アドレスが変化したときは，BU に共有鍵で作成した認証データ(MAC)を付加して送信する（④）．BU を受信した CN は共有鍵を用いて MAC の検査を行い BU の認証を行う（⑤）．これにより CN は MN が移動前後で，同一の端末であることを認証することができる．乱数の交換および BU の通知は IP 層で実現し，上位のソフトウェアには影響を与えない．

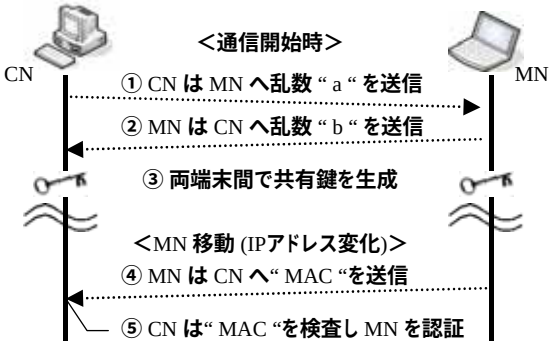


図 3. Diffie-Hellman 鍵交換を利用した認証方式

5．評価

本提案方式を Mobile PPC へ実装することにより BU における通信の成りすましを防止することが可能となる．本提案方式は特別なサーバを必要とせずエンド端末間のみで実現可能であるということと，IP 層ですべての処理を行うため上位のソフトウェアに影響を与えないという利点がある．

6．むすび

Mobile PPC における認証方式の提案を行った．今後は提案方式の実装と有効性の確認を行う．

謝辞

本研究は栢森財団の助成を受けて実施したものである．

参考文献

[1] C. E. Perkins.”IP Mobility Support for IPv4,” Aug.2002.RFC 3344.
[2] 竹内元規，渡邊晃，“ モバイル端末の移動透過性を実現する Mobile PPC の提案，” 情報処理学会研究報告，2004-MBL-30, pp.17-24, Sep. 2004.
[3] D.Johnson, C. Perkins, J. Arkko, “Mobility Support in IPv6,” June 2004.RFC3775.
[4] 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 の仕組み, ”情報処理学会研究報告，Vol.2004, No.75, 2004-CSEC-26, PP259-266, July.2004.
[5] W.Diffie, M.E. Hellman “New Directions in Cryptography,” IEEE Transactions on Information Theory, Vol. IT-22, No.6 Nov.1976.

Mobile PPCにおける認証方式の提案

名城大学　理工学部
瀬下正樹　竹内元規　渡邊晃

研究背景

- 研究背景
  - モバイル端末の普及
  - 無線ネットワーク環境の普及

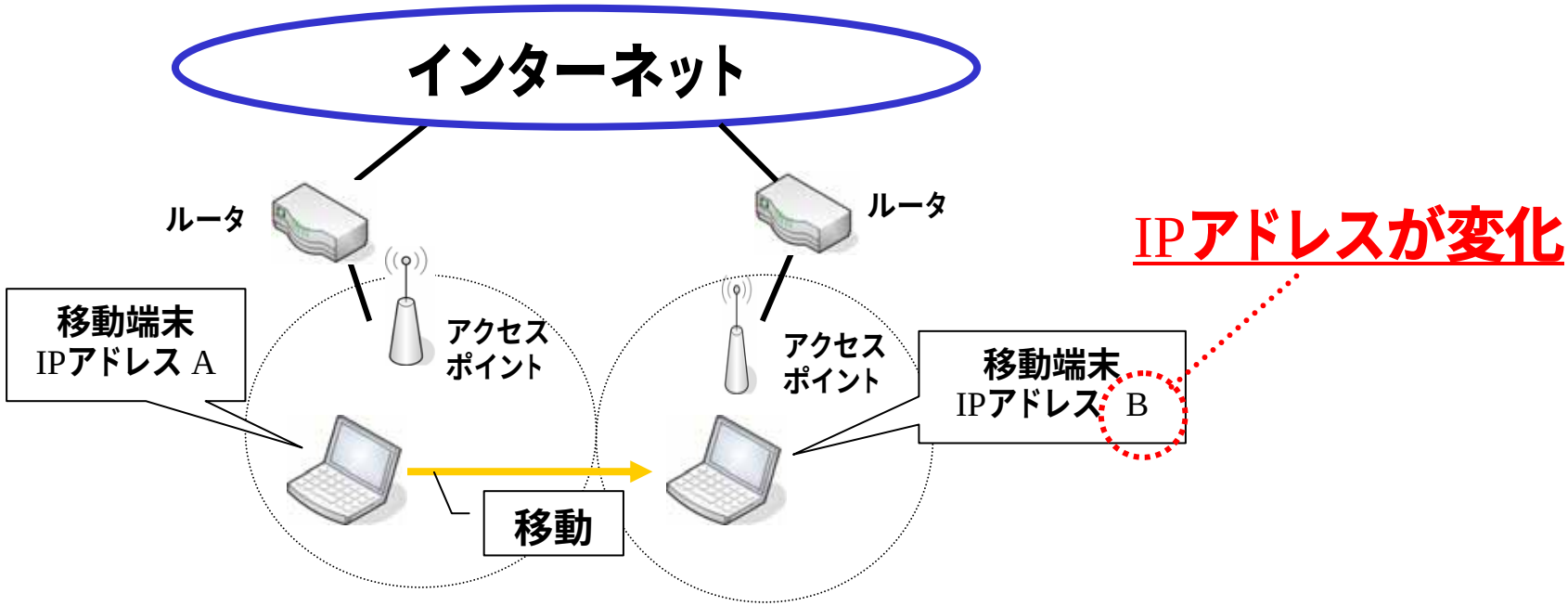
  ⇒端末が自由に移動しながらネットワークに接続するというニーズが増加
- 目的
  - 移動中にIPアドレスが変化しても通信を継続する

⇒ノード移動透過性の実現

移動すると通信が継続できない理由

- インターネットにおける通信(IP層より上位層)
  - IPアドレスとポート番号によって識別.

- **インターネットでは**
  - **端末が通信中に移動すると**



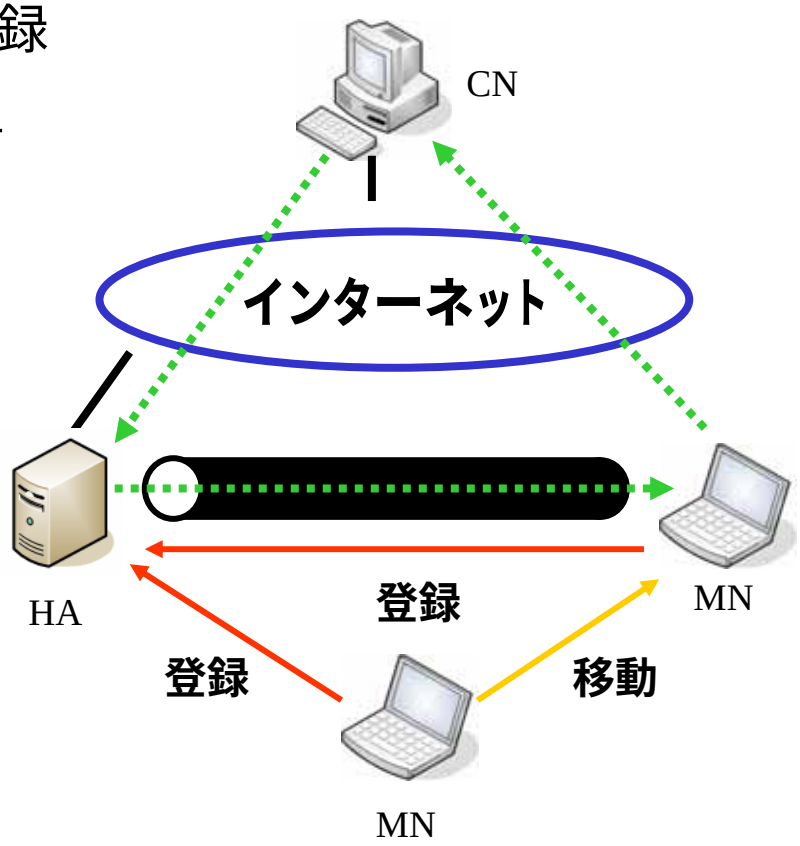
⇒別の通信とみなされ通信が切れる

既存技術　Mobile IP

- Mobile IPv4
  - IPv4においてノード移動透過性を実現する技術

「Mobile IPv4の動作概要」

- 移動ノード（以下 MN）は現在のアドレスをHA (Home Agent)へ登録
- 通信相手ノード（以下　CN）からMN宛のパケットはHAが代理受信
  - HAはパケットをMNへ転送
- MNからCNへの通信は直接行う

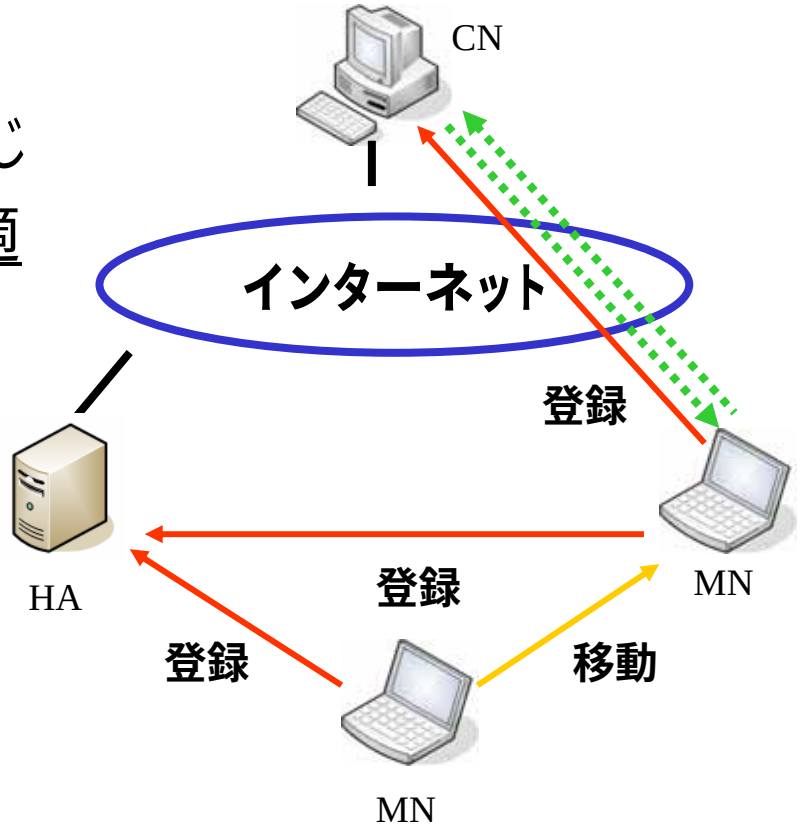


- Mobile IPv4の課題
  - 通信経路が三角経路となる
  - HAとMN間はトンネル転送となる
  - 特殊な装置(HA)が必要となる

Mobile IPv6

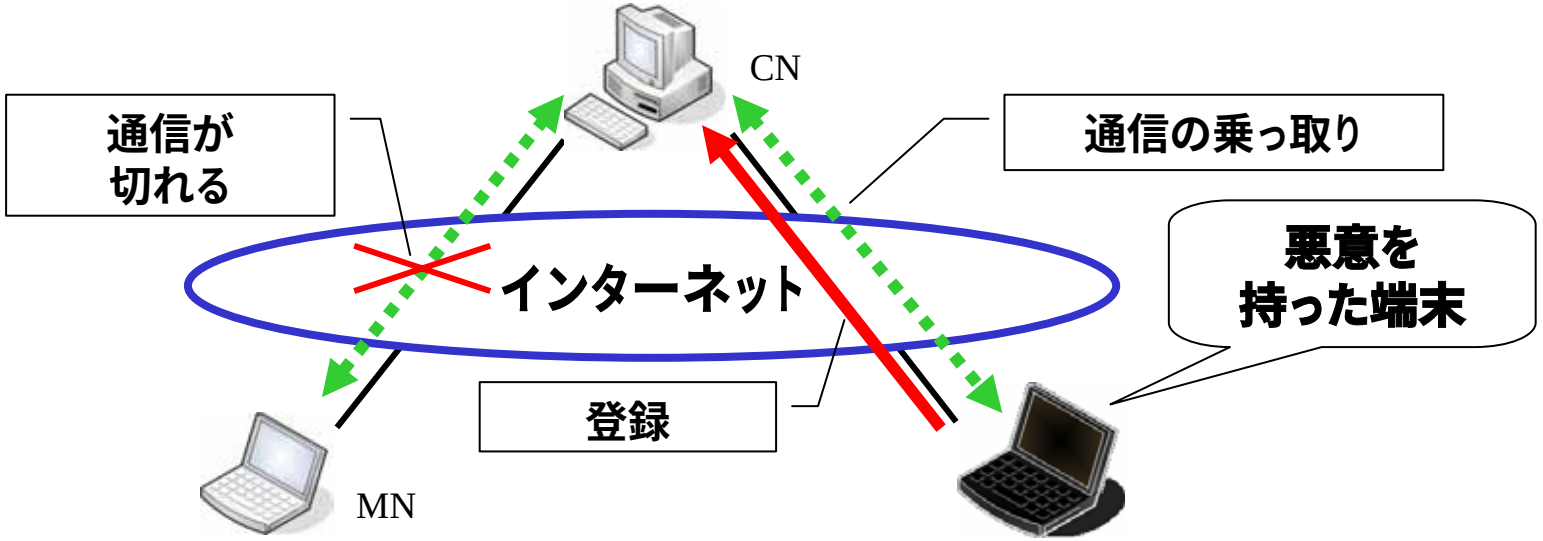
- Mobile IPv6
  - IPv6においてノード移動透過性を実現する技術

- 基本的な動作はMobile IPv4と同じ
- CNとMNが直接通信する経路最適化機能が新たに追加
  - CNに対してもアドレス登録
  - IP層で拡張ヘッダを利用したアドレス変換



経路最適化の課題

- MNとCNが通信中
  - 悪意を持った端末がアドレス登録



⇒通信の乗っ取りが起こる

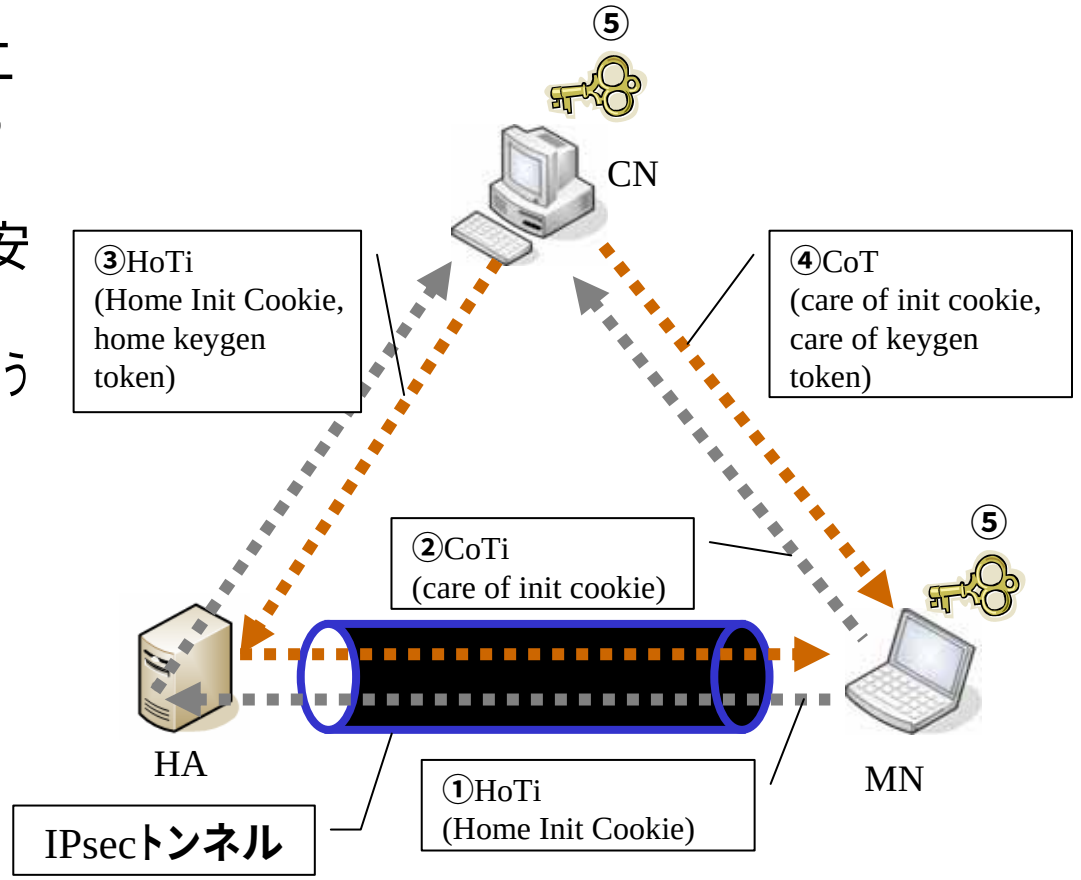
- CNにアクセスしてくるMNは不特定多数
  - 事前に認証に必要なMNの鍵を持つことは難しい
  - PKI の利用は現在の普及状況では現実的でない

⇒ **新たな認証機構が必要**

Mobile IPv6における認証機構

- Return Routability
  - 1.HAとMNの信頼関係を利用
  - 2.共有鍵（パスワード）を二つに分け，異なる経路から配送（①から④）
  - ⇒共有鍵（パスワード）を安全に生成（⑤）
  - 3.共有鍵を用いた認証行う
- 問題点
  - CN近傍において共有鍵の盗聴が可能
  - 登録の直前に実行

  ⇒それ以前の通信における乗っ取りは防げない



Mobile IPv6の課題

- Mobile IPv6の課題
  - 拡張ヘッダを使う
  - 通信初期の数パケットや認証に特殊な装置(HA)が必要

独自技術

Mobile PPC (Mobile Peer to Peer Communication)

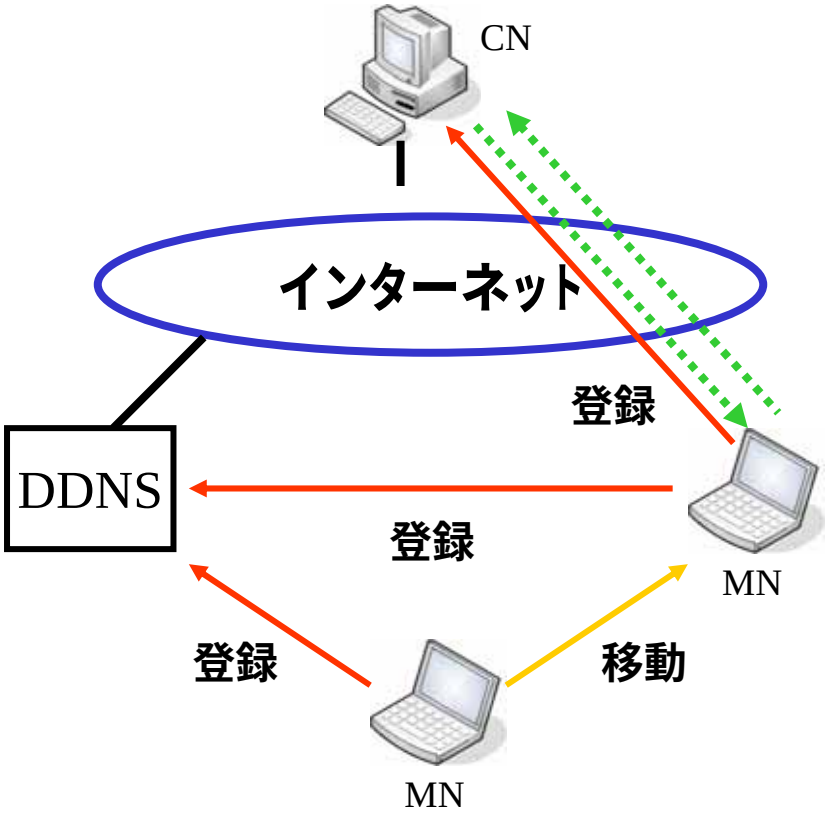
- Mobile PPC
  - エンドエンドでノード移動透過性を実現

「Mobile PPCの仕組み」

- 初期IPアドレスの解決にはDDNS (Dynamic DNS)を使う
  - ホスト名とIPアドレスを動的に管理
    - DDNSはDNSの延長

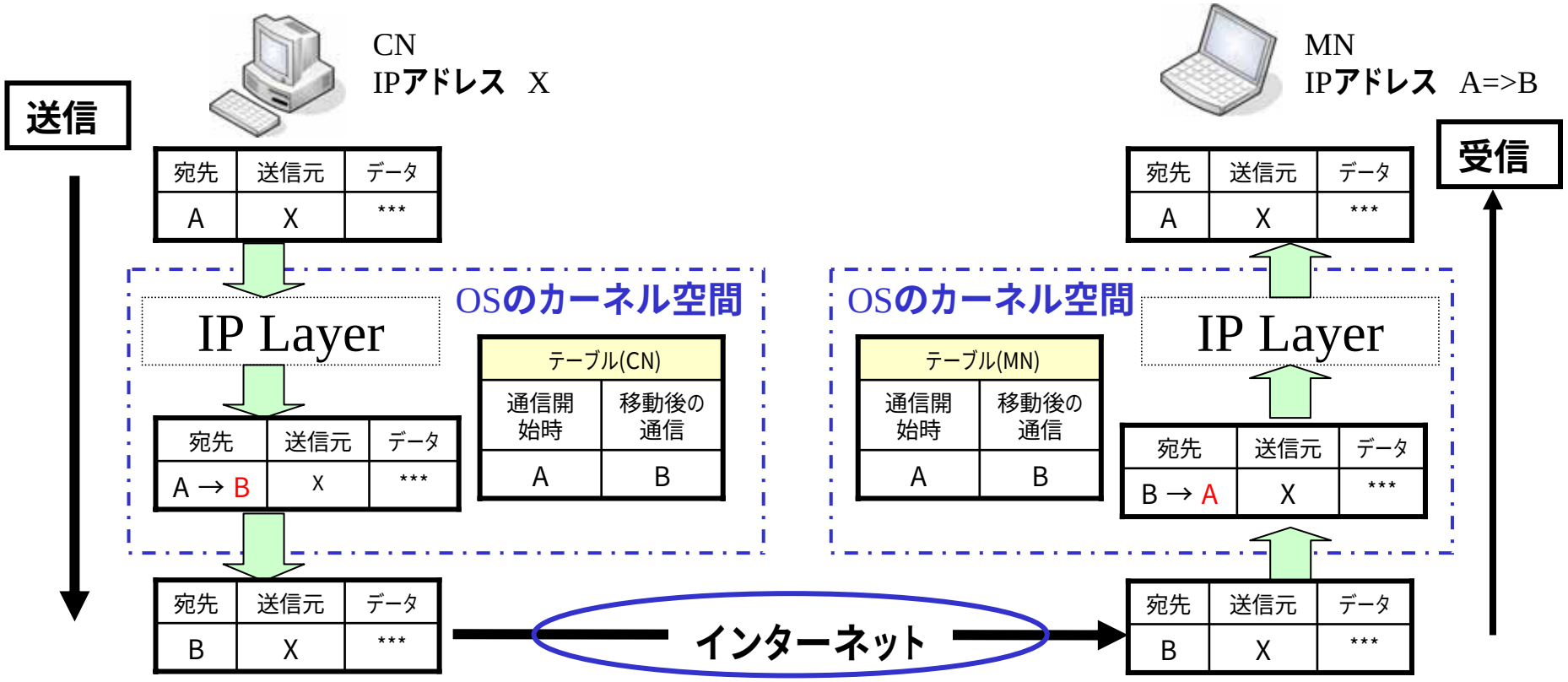
⇒ホスト名を識別子としてMNへ通信を開始

- 通信中のIPアドレスの変更はエンドエンドで通知する
  - 移動前後の対応関係を示すテーブルを生成
  - IP層でアドレス変換を行うことにより上位層にIPアドレスの変化を隠蔽



～アドレス変換の詳細～

＜場面設定＞
通信中，CNがMNからアドレス登録(AからBに変更) を受け取り，テーブルを更新後，
CNからMNへパケットを送信



•IPアドレスの変化を上位層に隠蔽
⇒コネクション維持

Mobile PPCの課題

- アドレス登録の際の認証機構がない
  - もしも悪意を持った端末が
    - MNに成りすましてアドレス登録を行う

⇒通信の乗っ取りが起こる

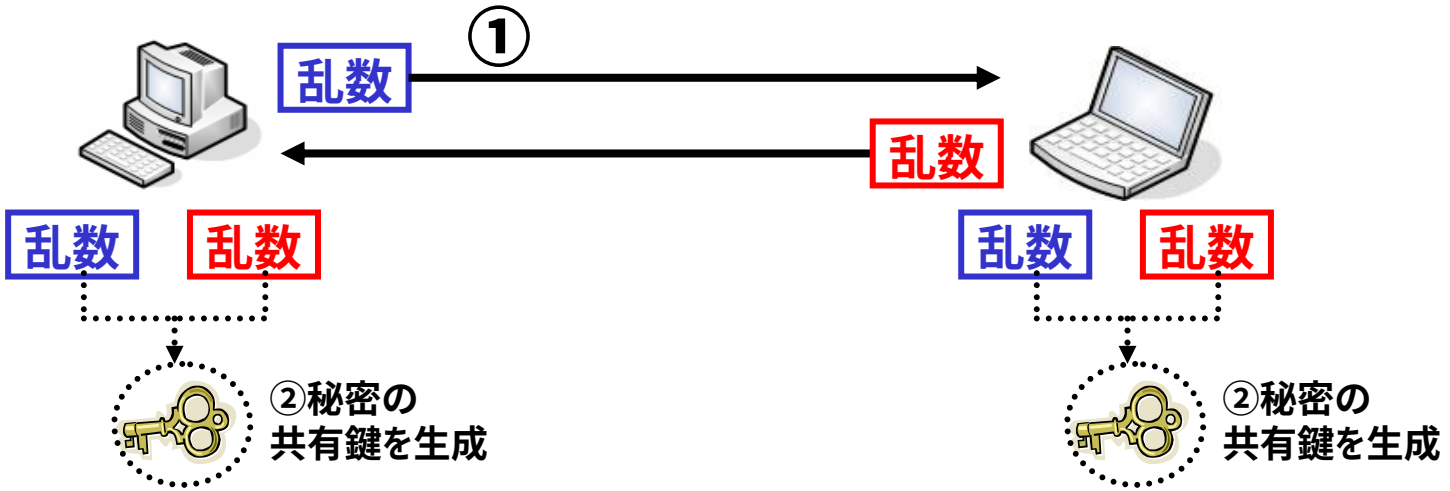
- Mobile IPv6で導入されているReturn Routability
  - HAのような特殊な装置を利用した認証

⇒Mobile PPC**への適用は難しい**

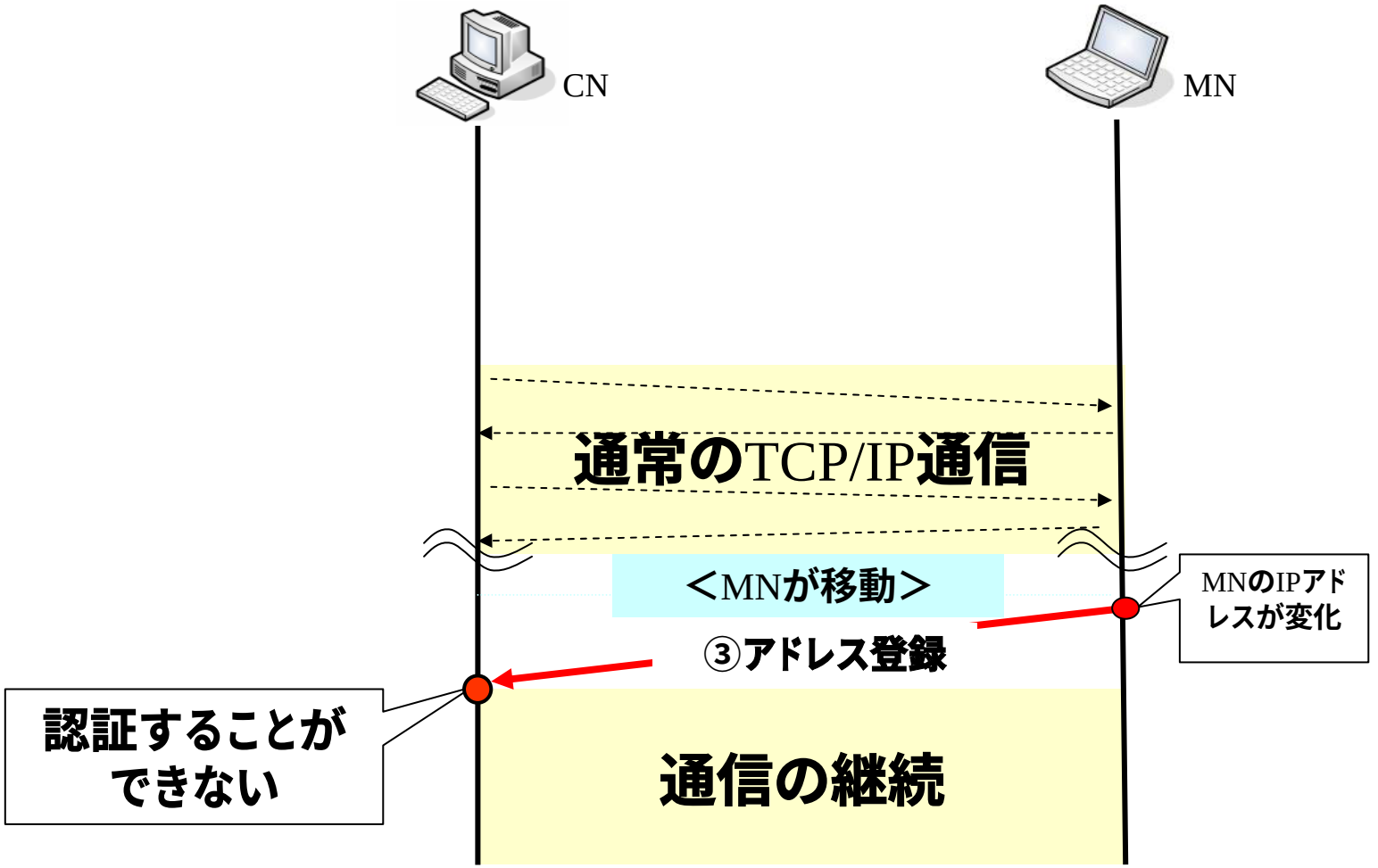
エンドエンドで実現可能なMobile PPCにおける認証方式

- 認証機構として，Diffie-Hellman鍵交換を利用
  - Diffie Hellman鍵交換
    - ある乱数を交換することによって（①）
    - 盗聴者がいても安全に端末間で共有鍵(パスワード)の生成をする技術（②）

✧離散対数問題を利用



現状のMobile PPCのシーケンス



提案方式を追加したMobile PPCのシーケンス

動作概要

＜通信に先立ち＞

①Diffie-Hellman鍵交換

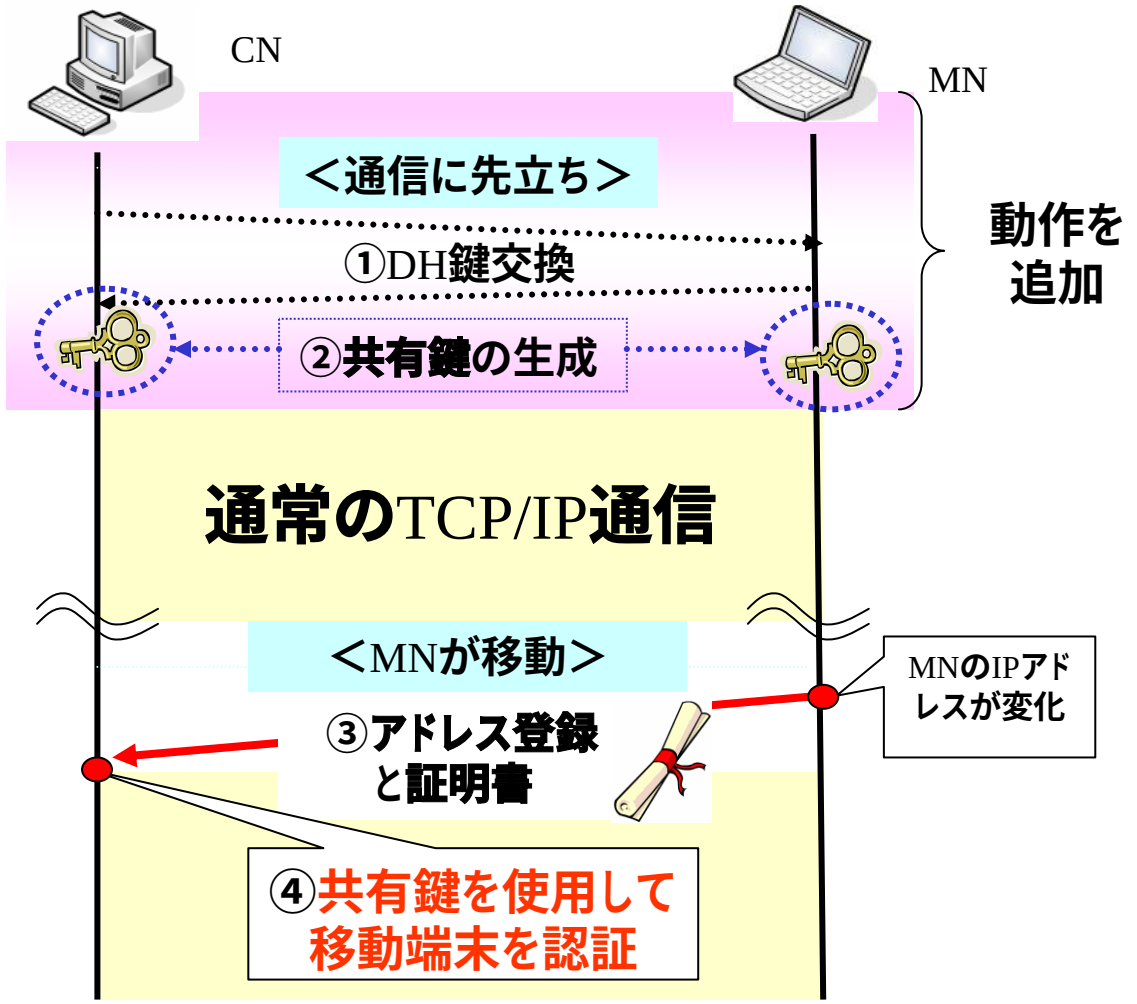
②共有鍵を共有
(パスワードの合意)

その後，通常のTCP/IP通信

＜MNが移動時＞

③アドレス登録
(共有鍵で作成した認証データを含む)

④共有鍵を使用して認証



アドレス登録時における
通信の乗っ取りを防止することが可能

評価　Return Routabilityとの比較

	Return Routability	提案方式
通信開始時における乗っ取り	×	×
移動時における乗っ取り	△	○

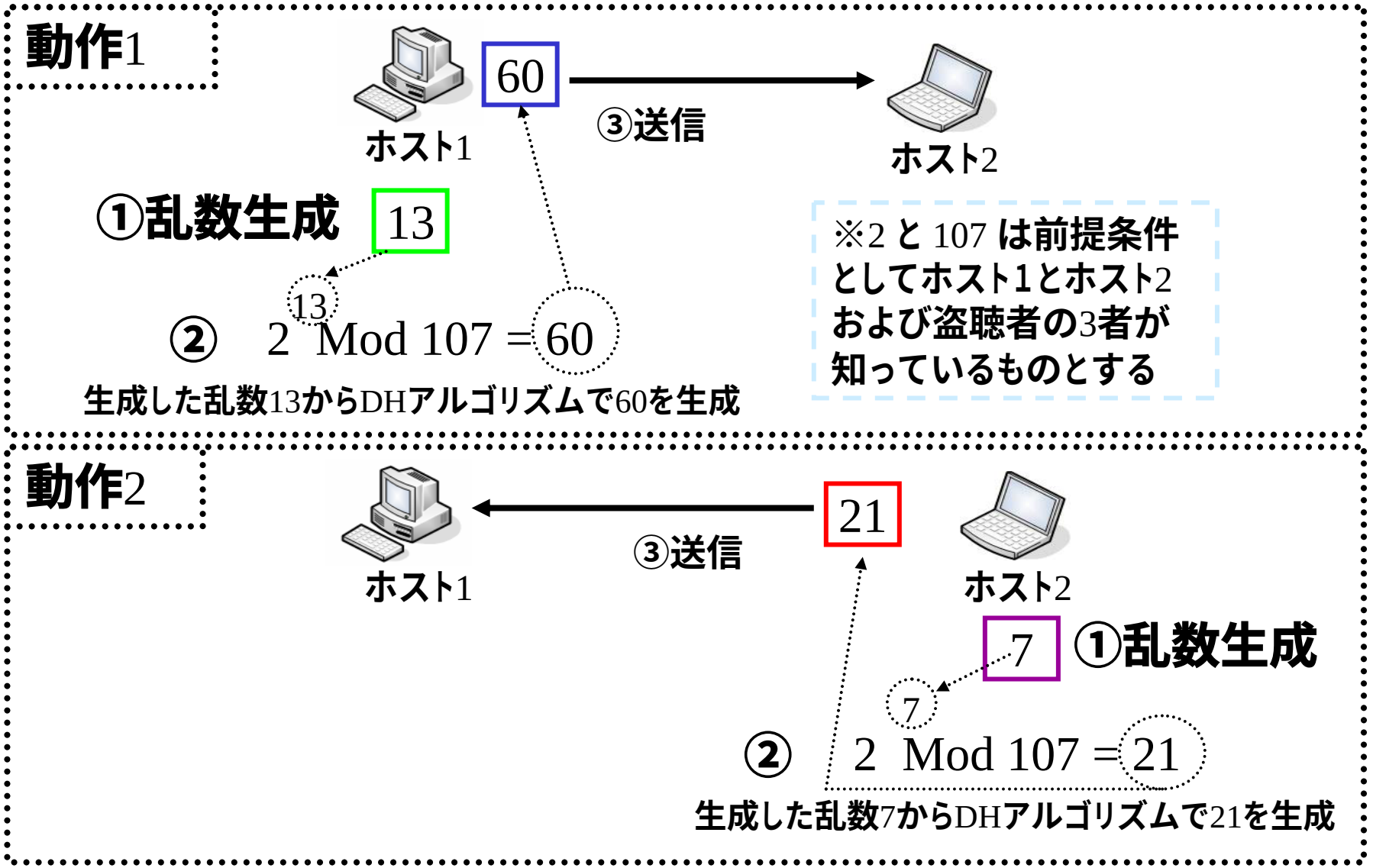
•通信開始時における乗っ取りは両方式とも危険あり
⇒しかし，Mobile IPv6**や**Mobile PPC**を導入する以前から，**TCP/IP**通信に存在する問題**
•移動時における乗っ取り
　　—Return Routability**は脆弱性のある鍵交換が移動時に実行**
　　—提案方式は通信に先立って共有した共有鍵を使用して認証を行う

むすび

- Mobile PPCにおける認証方式を提案
- 今後は提案方式をMobile PPCへ実装し，有効性の確認を行う

おわり

付録. Diffie Hellman鍵交換の詳細例（その1）



付録. Diffie Hellman鍵交換の詳細例（その2）

動作3

ホスト1

ホスト2

$21^{13} \text{ Mod } 107 = 70$　　$60^{7} \text{ Mod } 107 = 70$

計算結果が一致

- **上記したDiffie Hellman 交換は以下の式が成り立つことを利用**

ホスト2が送信した値　ホスト1が送信した値

ホスト1の乱数　ホスト2の乱数

$B \bmod n = g^{x} \bmod n = A^{y} \bmod n$

※g=2 と n=107 は前提条件としてホスト1とホスト2および盗聴者の3者が知っているものとする

- **盗聴者が流れた乱数を盗聴したとして，共通鍵「70」を知るには以下の計算が必要**

$$21^{x} \text{ Mod } 107 = 2^{x\,y} \bmod 107 = 60^{y} \bmod 107$$

⇒**この式から x , y を導き出すことは事実上不可能**