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)

Proposal of Authentication Mechanisms in Mobile PPC

Masaki Sejimo, Motoki Takeuchi, Akira Watanabe (Meijo University)

１．はじめに

インターネットでは，ノードが移動するとIPアドレスが変化し，通信が切断されてしまうという問題がある．そこで，ノードの移動による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．

移動透過プロトコルとして Mobile IP(1)が提案されているが，HA(Home Agent)のような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くなっている．我々は，位置管理エージェントを不要とし，常時P2P通信をおこなうためのプロトコルである Mobile PPC(2)の研究を行っている．しかし，従来の Mobile PPC には移動ノード(MN)が移動した際に通信相手ノード(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 PPC とその課題

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することで，ノード移動透過性を実現する．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 MN の識別子としてノードの IP アドレスを知ることができる．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 (BU) を用いて通知する．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，以後の通信では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．

しかし，現状の Mobile PPC では，BU の際に不正なノードによる通信の乗っ取りの懸念がある．このセキュリティの観点から BU における MN の認証が必須である．Mobile PPC は Flexible Private Network (FPN) (3)という閉じた環境を前提としていたため BU における認証は不要だった．従って Mobile PPC は FPN 以外の環境では使用できず汎用性に欠けていた．

３．Mobile PPC における認証方式の提案

本研究では Mobile PPC における認証機構として，Diffie-Hellman 鍵交換(4)を利用した認証方式を提案する．

認証方式の流れを図 1 に示す．通信開始時において，Diffie-Hellman 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，秘密鍵を共有する．MN が移動し，IP アドレスが変化したときは，BU に共有秘密鍵で作成した証明書(MAC)を付加して送信する．CN は通信開始時に共有した秘密鍵を用いて MAC の検査を行い MN の認証を行う．これにより CN は移動通知処理前後の MN が同一の端末であることを確認することができる．

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．

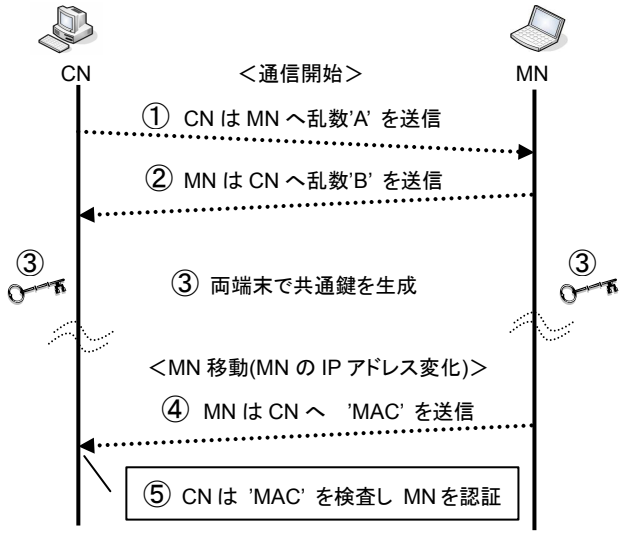


図 1. Diffie Hellman 交換を利用した認証方式

４．むすび

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

文　献

(1) C. E. Perkins,"IP Mobility Support," RFC 2002,Octorber 1996

(2) 竹内元規， 渡邊晃，" 移動体通信におけるコネクションを維持した通信方式の研究"， 情報処理学会第 66 回全国大会 講演論文集 3-463，March 2004.

(3) 鈴木秀和, 渡邊晃, "GSCIP を構成する DPRP の仕組みの検討", 情報処理学会第 66 回全国大会 講演論文集 3-479, March 2004.

(4) W.Diffie, M.E. Hellman "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol. IT-22, No.6 November 1976

Mobile PPCにおける認証方式の提案

Proposal of Authentication Mechanisms in Mobile PPC

名城大学理工学部

瀬下 正樹　竹内 元規　渡邊 晃

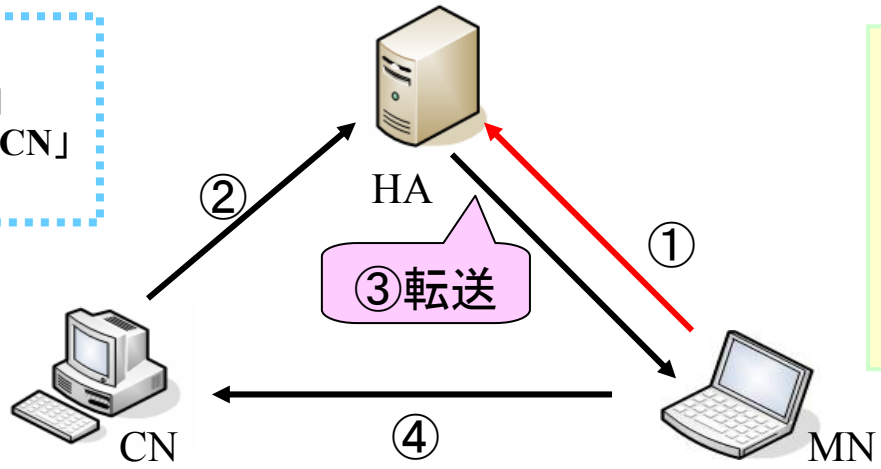
研究背景

- 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
- 目的
  - 移動中にIPアドレスが変化しても通信を継続する

既存技術：Mobile IPとその課題

- HA(Home Agent)と呼ぶプロキシサーバを用いる

本発表では
移動ノードを「MN」
通信相手ノードを「CN」
と呼ぶ



動作順序
①移動ノード(MN)は現在のIPアドレスをHAに登録
②通信相手ノード(CN)はMNへのパケットをHAへ送る
③HAはパケットをMNに転送
④MNからCNはHAを利用せず通信

⇒MN宛てのパケットをすべてHAが代理受信することで解決

- Mobile IPの課題
  - 特別なプロキシサーバ，HA(Home Agent)　が必要
    ⇒導入するための敷居が高い
  - パケットがHAを経由⇒通信経路が冗長

  } 大きな課題

  - HAとMNの間でパケットがトンネリング=>パケット長の増加
  - MNからCNへパケットを送信するとき送信元がHAのアドレスになる
    ⇒ルータに破棄される可能性がある

Mobile PPCについて
（MOBILE Peer to Peer Communication）

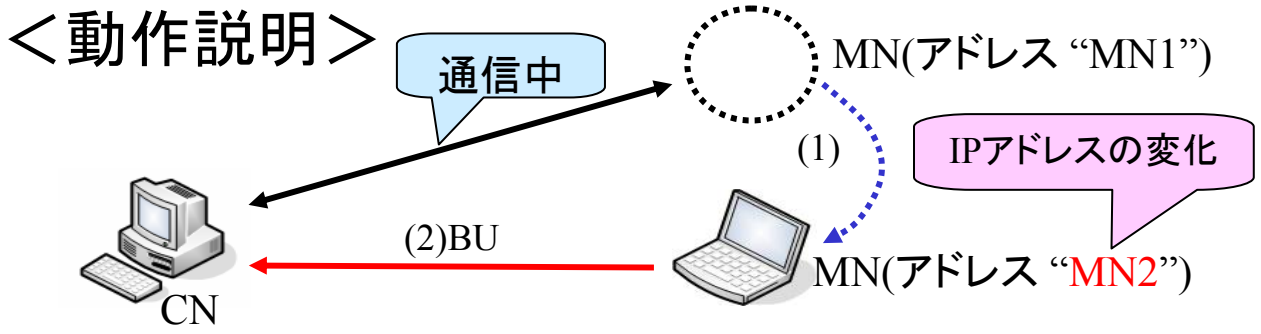
✧ プロキシサーバ(HA)を用いないエンドツーエンドによる手法

＜動作概要＞

- 端末間で移動前後の通信の対応関係を示すテーブルを保持
- 継続させたい通信はBU(Binding UPDATE)で移動通知
  ⇒テーブルを更新
- 移動後のMNとの通信はテーブルに従って，IP層でアドレスの書き換え処理

⇒通信を切断することなくコネクション維持

＜動作説明＞



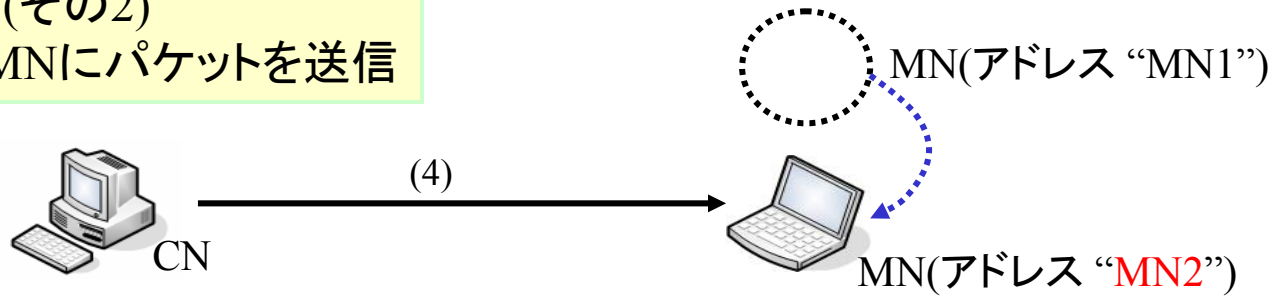
テーブル(CN)	
通信開始時	移動後の通信
MN1	MN2

(3)テーブルの更新

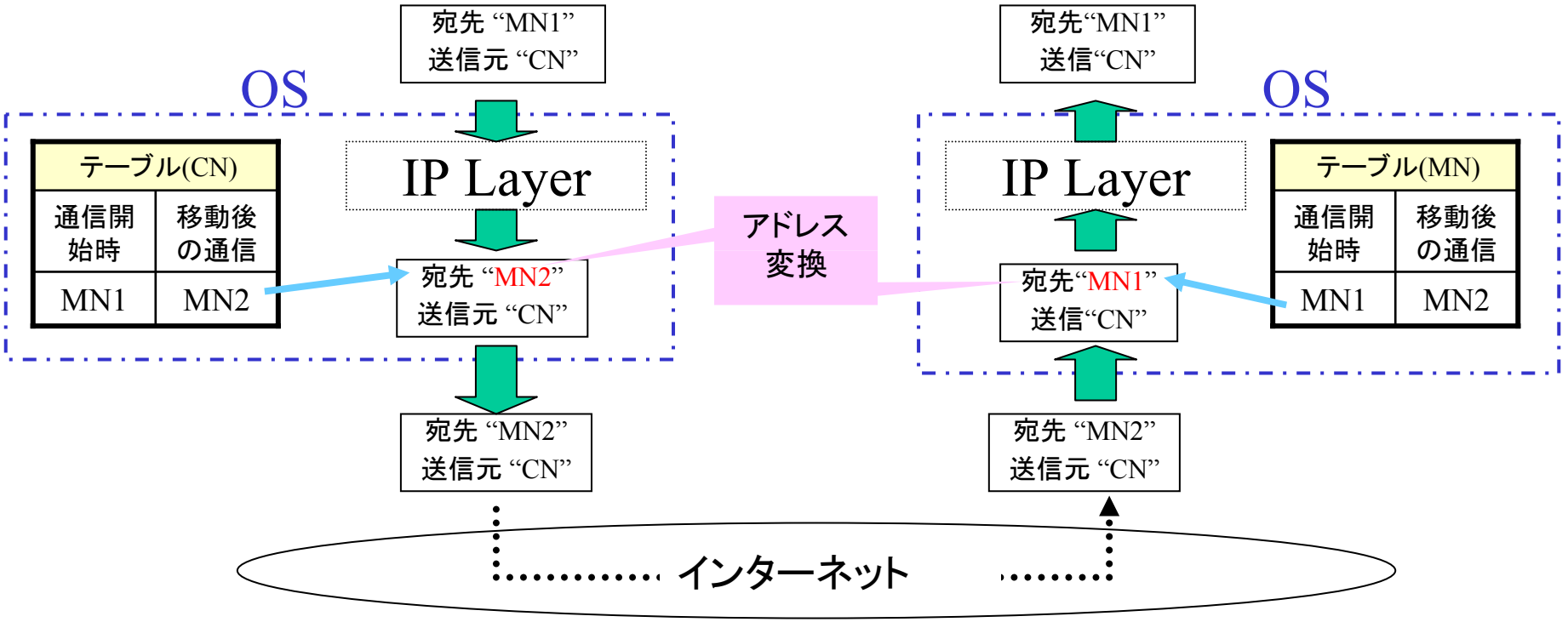
テーブル(MN)	
通信開始時	移動後の通信
MN1	MN2

Mobile PPCの動作順序
(1)通信中に移動ノードが移動しIPアドレスが変化
(2)MNはアドレスが変化した直後にCNへBU(アドレス更新要請)を送信
(3)BU後，BUを元に両端末でテーブルを更新

Mobile PPCの動作順序(その2)
(4)テーブルを使い，MNにパケットを送信



• アドレス変換処理の詳細



•IPアドレスの変化を上位層に隠蔽⇒コネクション維持

認証方式の提案

- Mobile PPCにおける課題
  - 移動時の認証機能
    - 移動時，通信の乗っ取りの懸念
- 認証機構として，Diffie-Hellman鍵交換を利用した認証方式を提案
  - Diffie Hellman鍵交換
    - ある乱数を交換するだけで安全に鍵交換を行う鍵交換方式

✧離散対数問題を利用

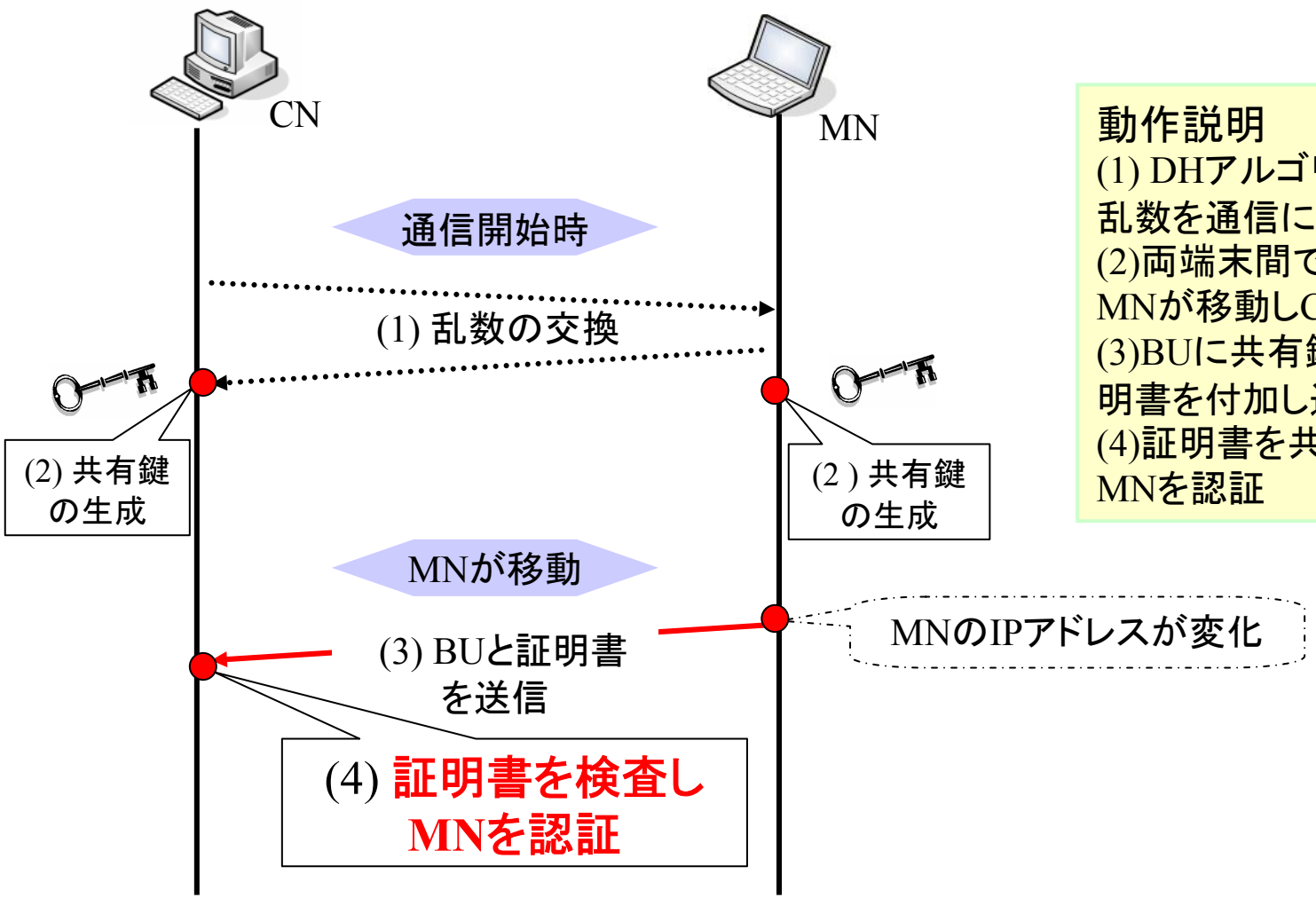
＜動作概要＞

- 通信に先立ち
  - Diffie-Hellman鍵交換⇒共通鍵を共有
- BU時に共通鍵を使って認証

IP層で処理

提案する認証方式のシーケンス

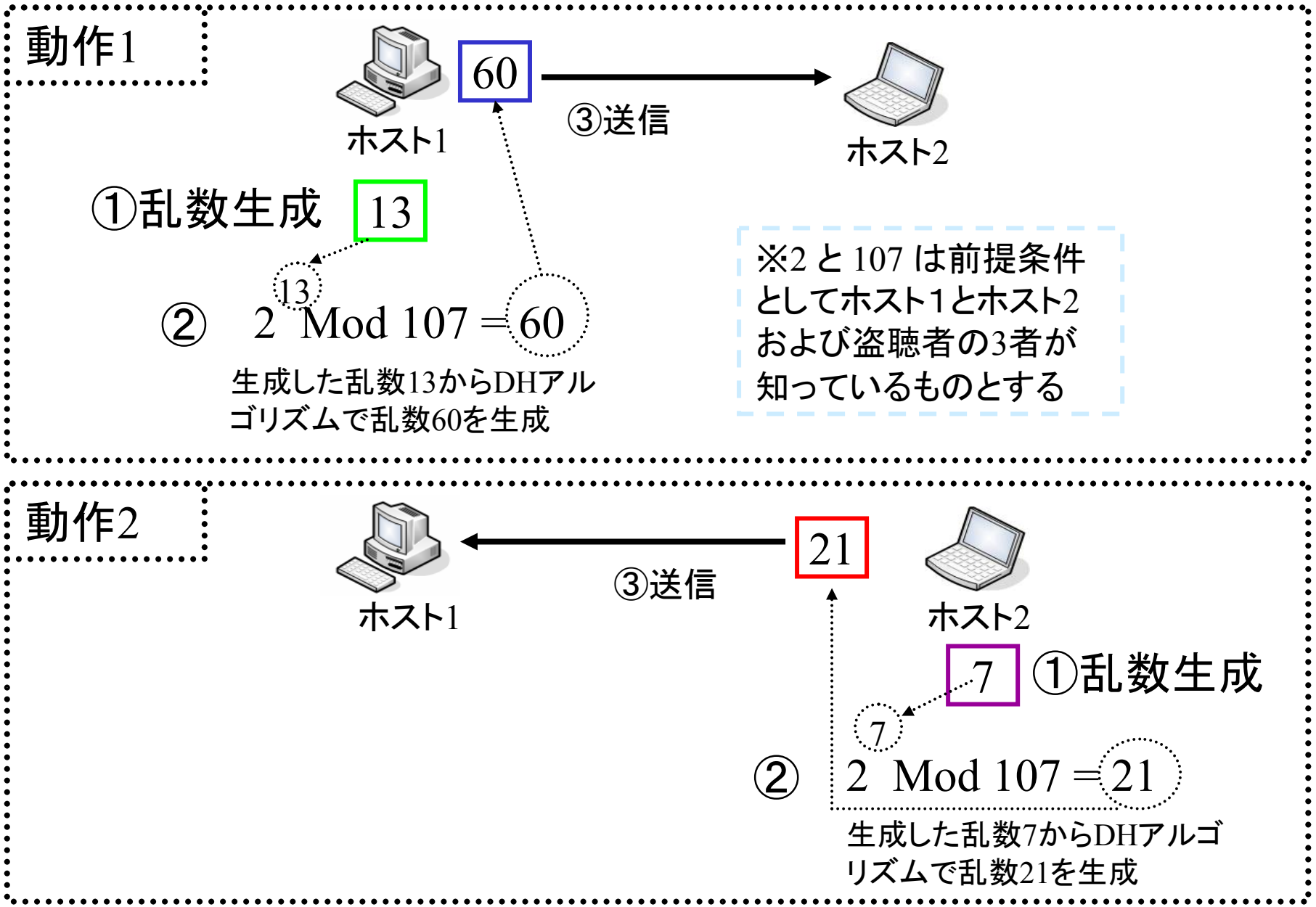
- 認証方式のシーケンス



動作説明
(1) DHアルゴリズムで生成し乱数を通信に先立ち交換
(2)両端末間で共有鍵を生成
MNが移動しCNへ移動通知
(3)BUに共有鍵で生成した証明書を付加し送信
(4)証明書を共有鍵で検査しMNを認証

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

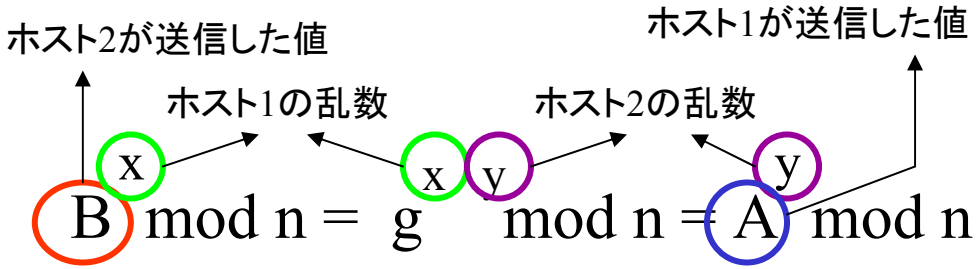
ホスト1

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



※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

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

⇒この式から x , y を求めることは事実上不可能