

# Mobile PPC における認証方式の提案

01j060 瀬下 正樹  
渡邊研究室

## 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盛んに行われている。我々は、移動透過性の一方式として、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[1]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 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により移動透過性を保証する。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 は BU の際に通信を乗っ取られる危険があり、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という課題があった。

## 3. Mobile PPC における認証方式の提案

本研究では MN を認証するための機構として、Diffie-Hellman 鍵交換[2]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 1 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。

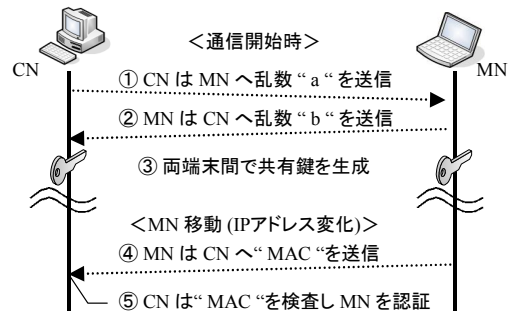


図 1. Diffie-Hellman 鍵交換を利用した認証方式

## 4. 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。本提案方式は特殊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。

## 5. 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。

## 参考文献

- [1] 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.
- [2] 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*

---

*渡邊研究室  
01J060 瀬下 正樹*

---

# 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

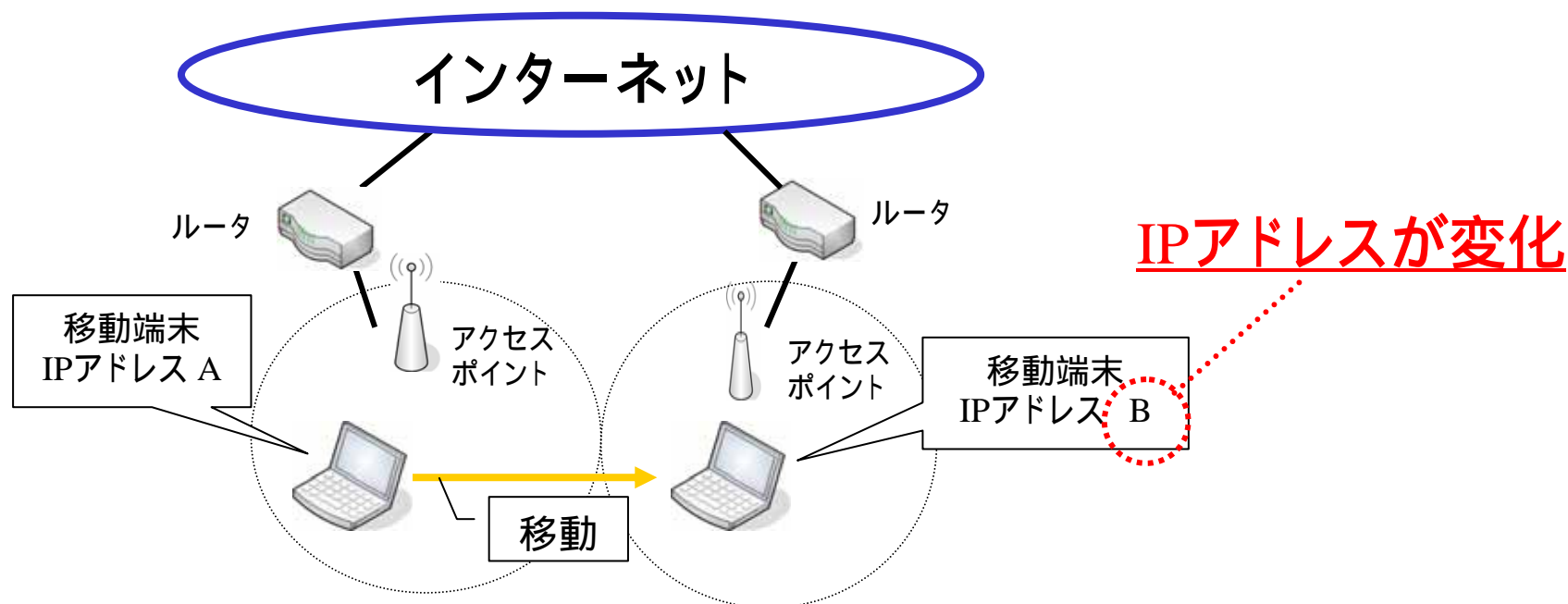
## ■ 目的

- 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

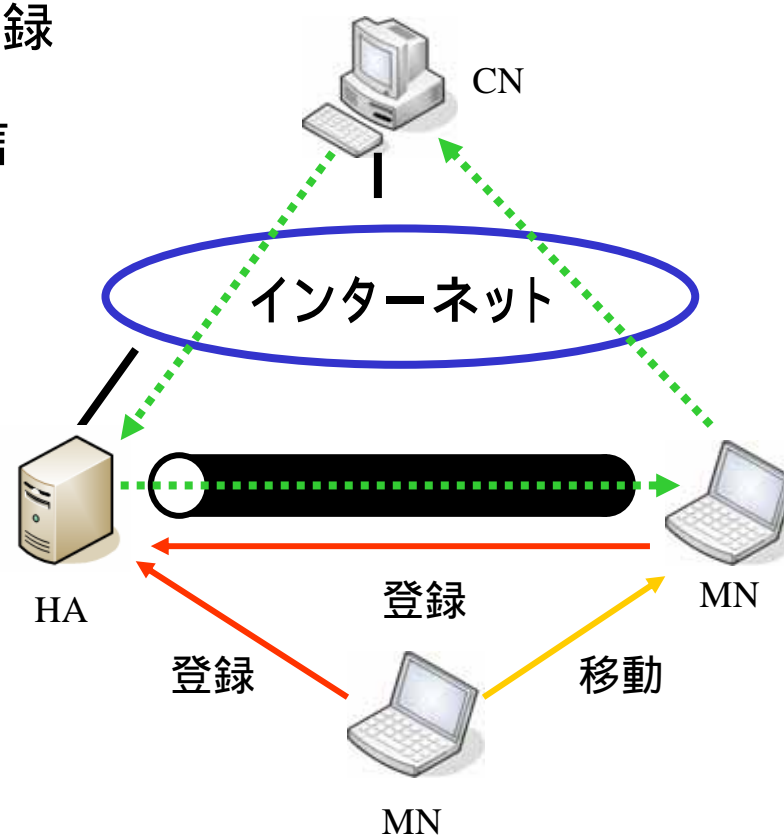
- IPv4においてノード移動透過性を実現する技術

### 「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 packets 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

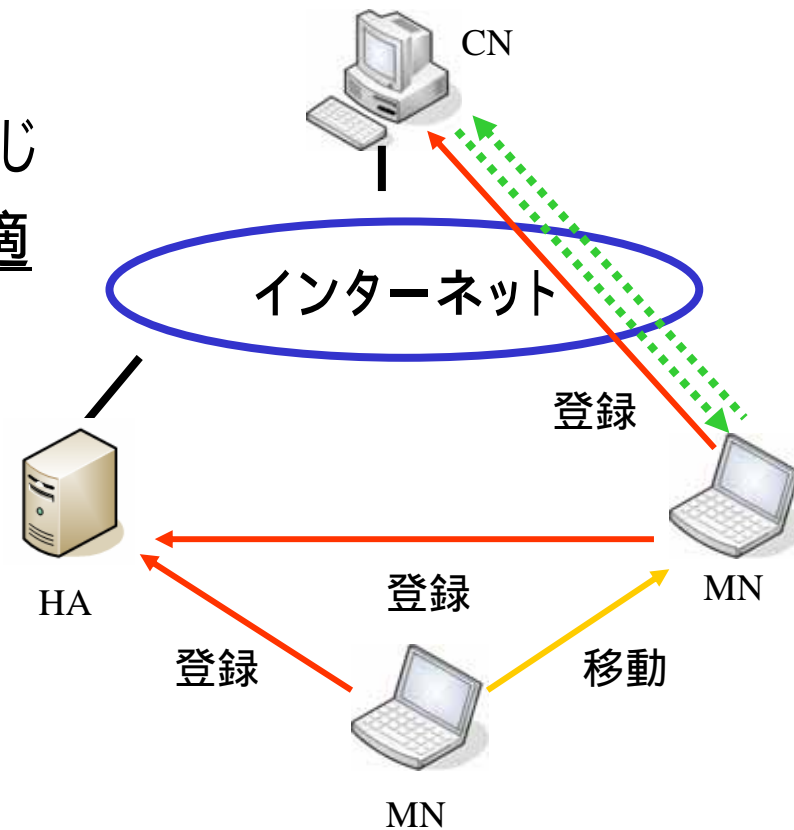
## ■ Mobile IPv6

- 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

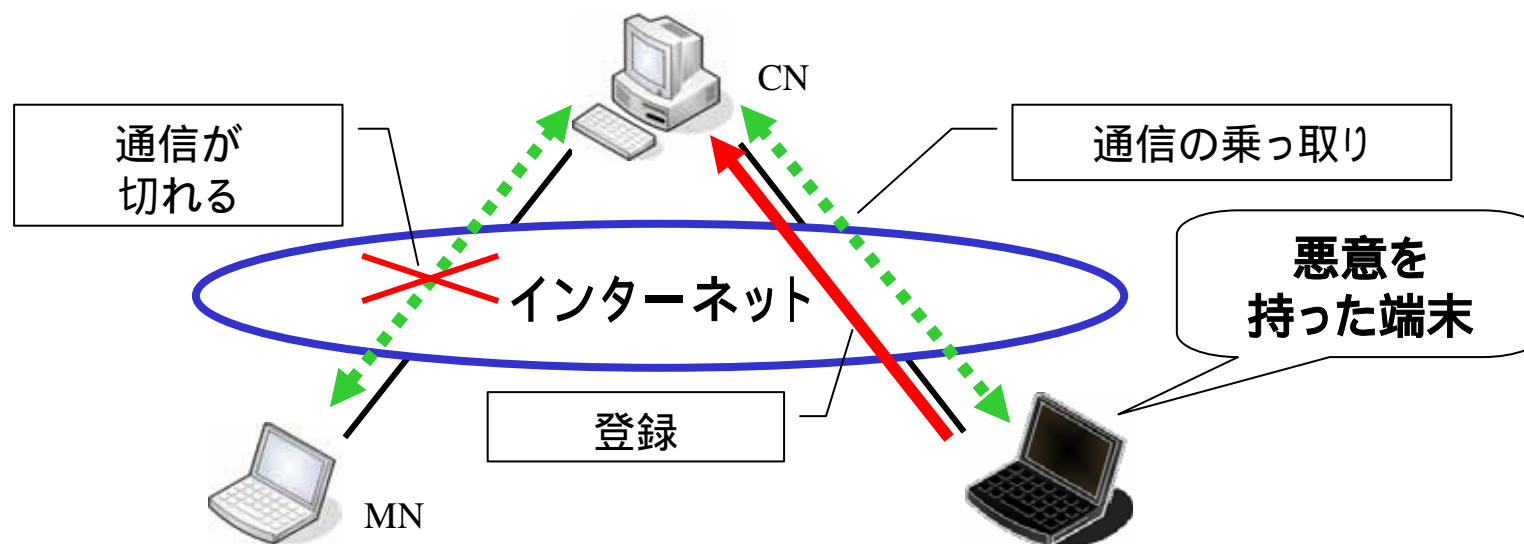
## ■ CNとMNが直接通信する経路最適化機能が新たに追加

- 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

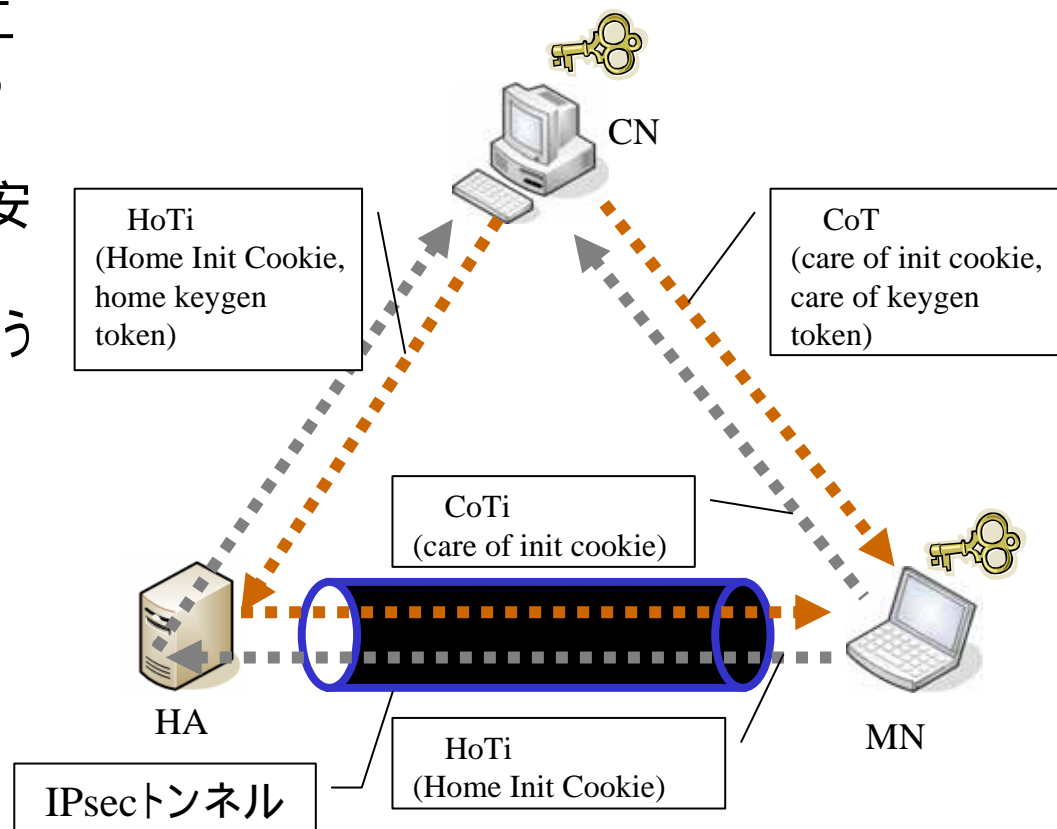
# Mobile IPv6における認証機構

## ■ 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( から )
- 共有鍵(パスワード)を安全に生成( )
- 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

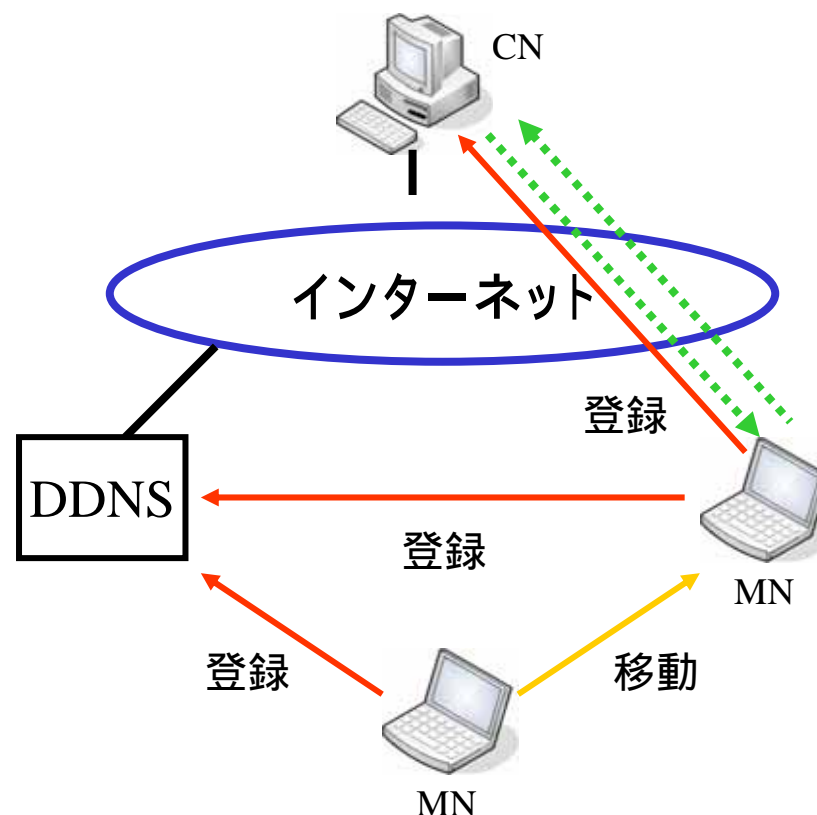
# Mobile PPC (Mobile Peer to Peer Communication)

## ■ 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」

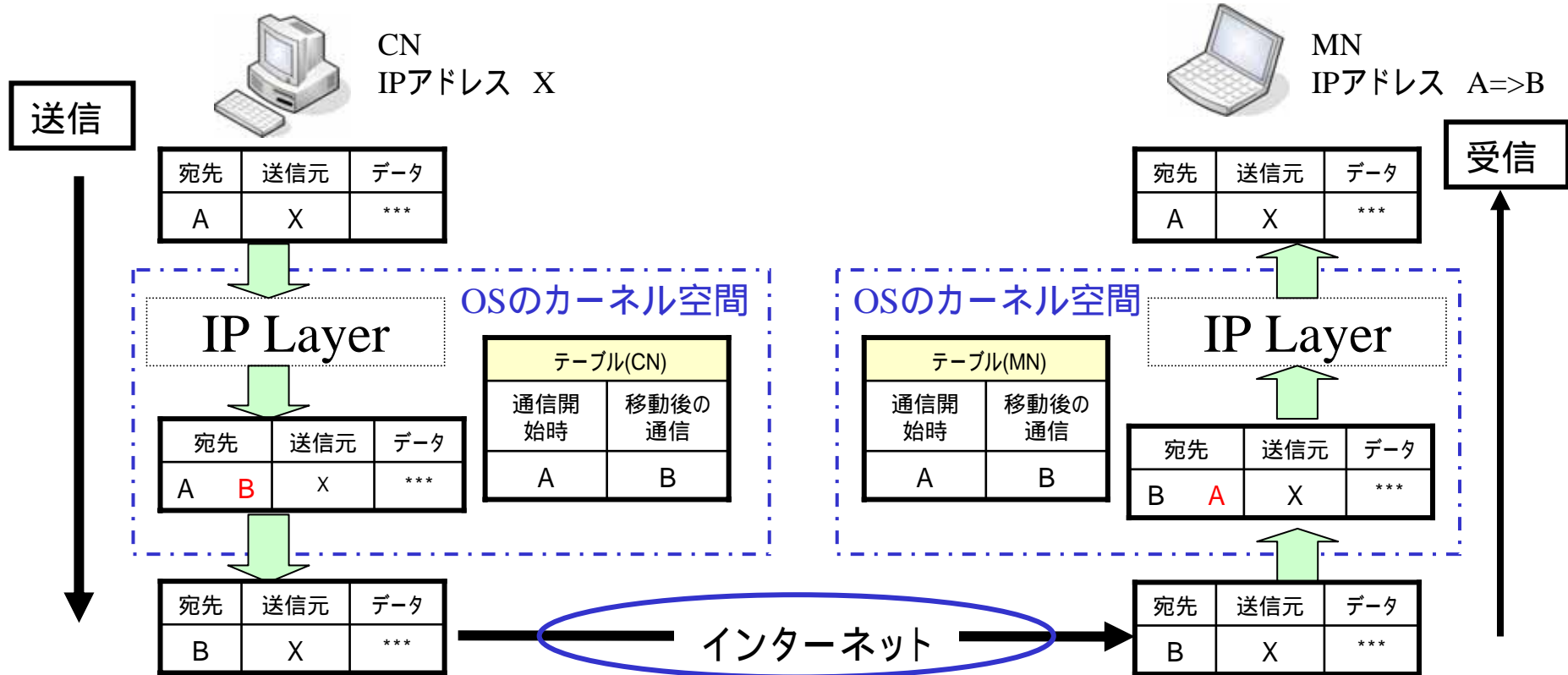
- 初期IPアドレスの解決にはDDNS (Dynamic DNS)を使う
    - ホスト名とIPアドレスを動的に管理
      - DDNSはDNSの延長
- ホスト名を識別子としてMNへ通信を開始
- 通信中のIPアドレスの変更はエンドエンドで通知する
    - 移動前後の対応関係を示すテーブルを生成
    - IP層でアドレス変換を行うことにより上位層にIPアドレスの変化を隠蔽



## ～ 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, テーブルを生成後, 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

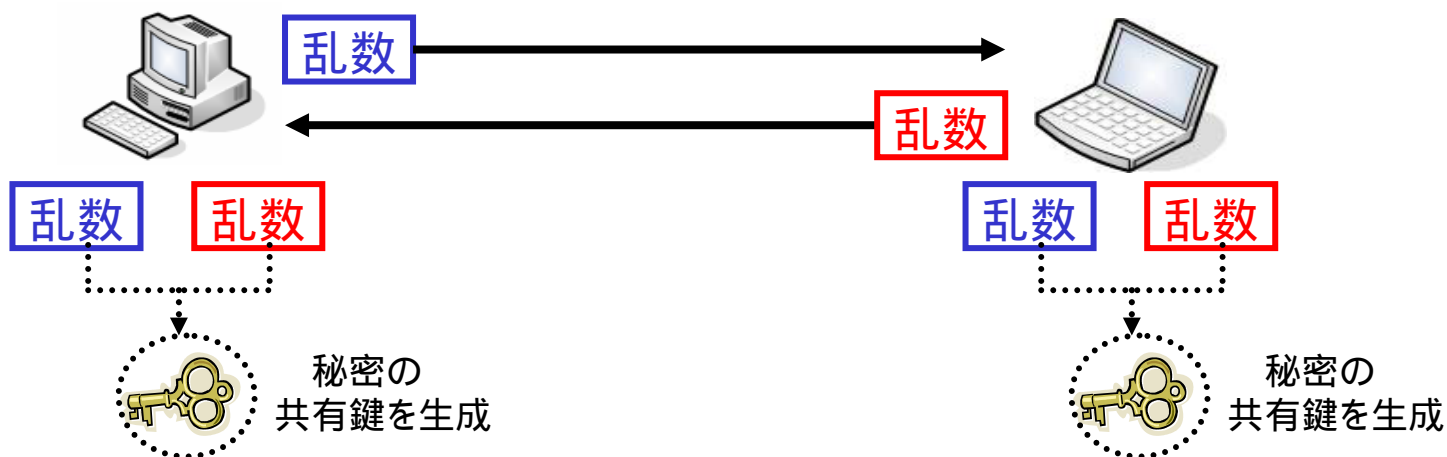
### Mobile PPCへの適用は難しい

■ 認証機構として, Diffie-Hellman鍵交換を利用

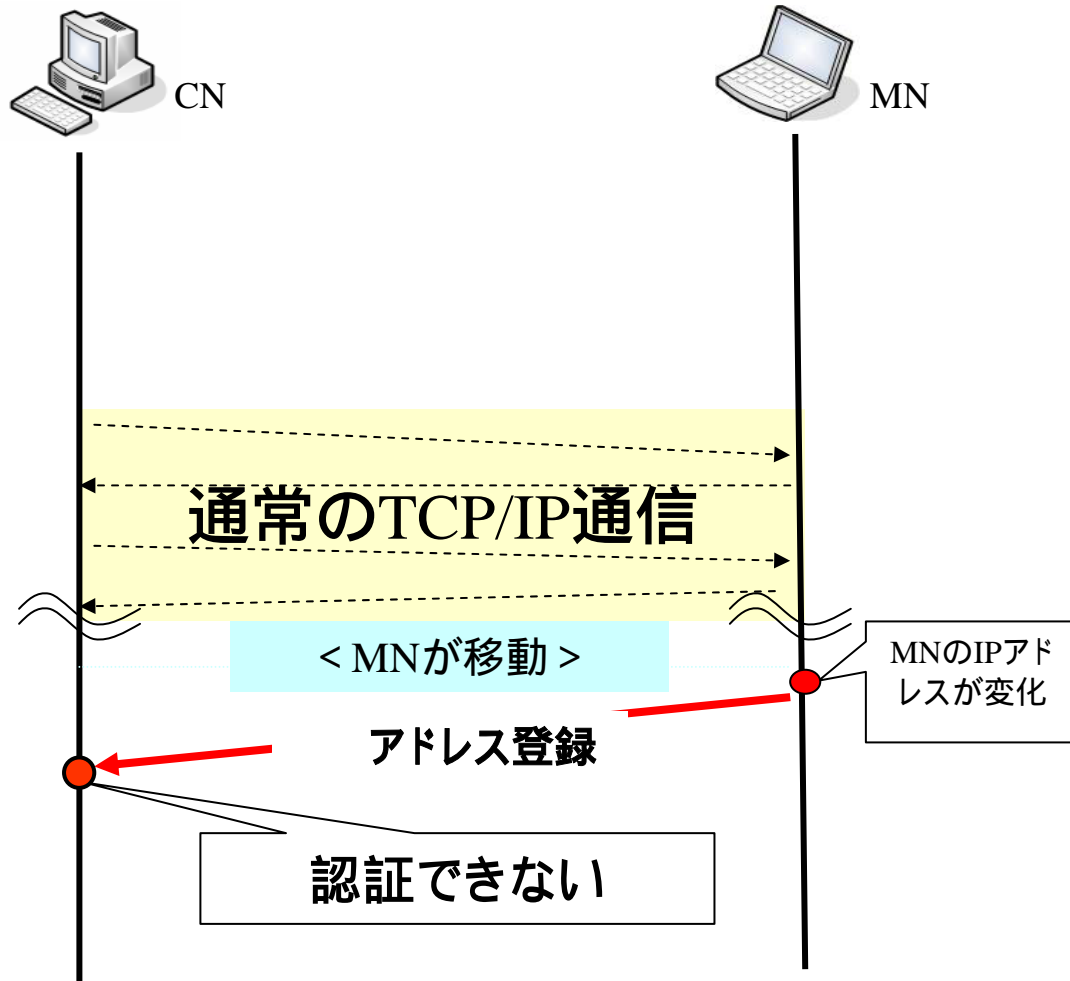
– Diffie Hellman鍵交換

- ある乱数を交換することによって( )
- 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( )

◇ 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 >

Diffie-Hellman鍵交換

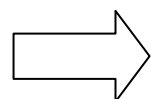
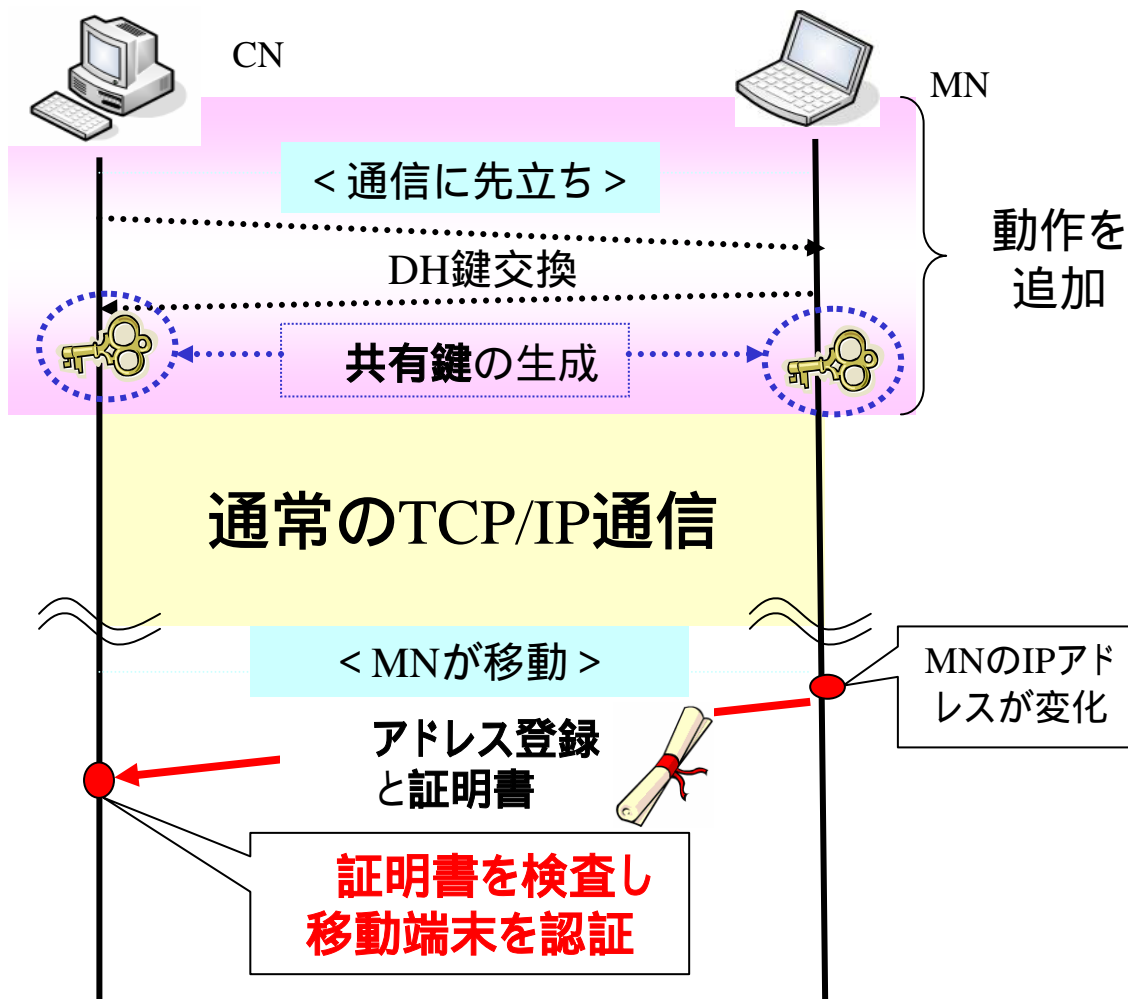
共有鍵を共有  
(パスワードの合意)

その後, 通常のTCP/IP通信

#### < MNが移動時 >

アドレス登録  
(共有鍵で作った証明書を  
含む)

共有鍵を使って認証



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登録動作時に実行  
提案方式は登録時において既に共有してある共有鍵を使用して  
認証を行う



# 実装

- オープンソースライブラリ「OpenSSL」を使用
  - Diffie Hellman鍵交換による共有鍵の生成を行う試作プログラムの作成
    - 共有鍵の値が一致することを確認
  - 共有鍵による認証データの作成, および検証を行う試作プログラムの作成
    - 動作を確認

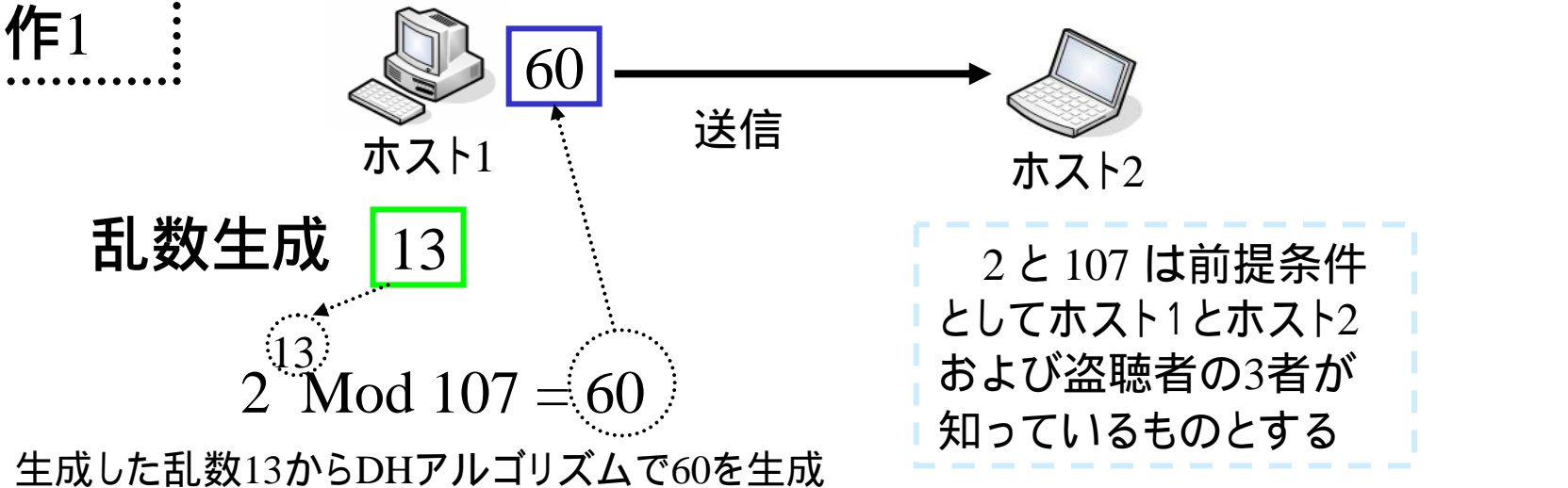
## むすび

- 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

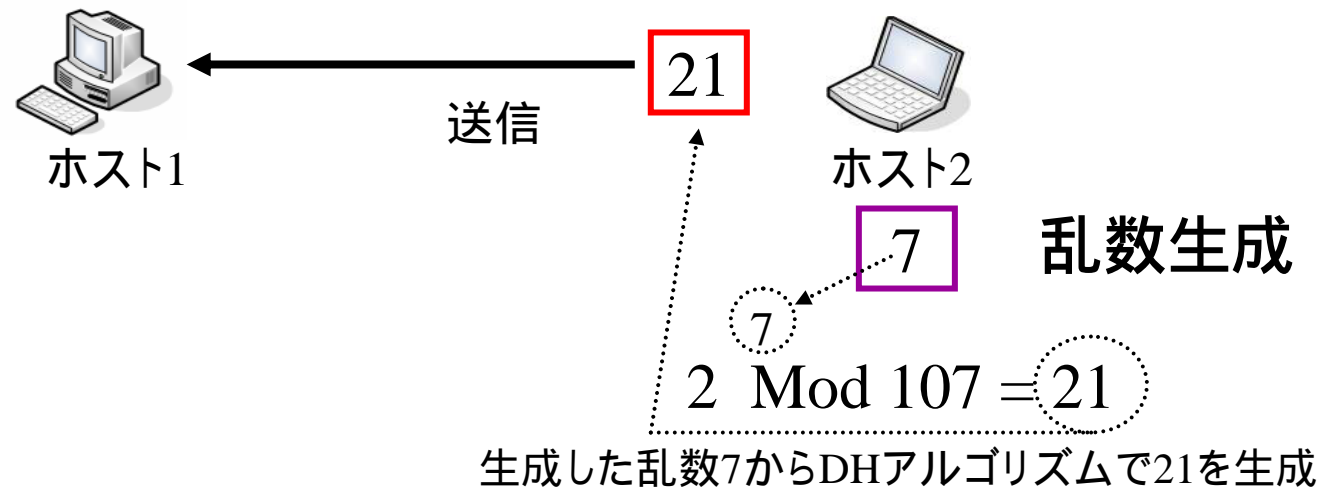
おわり

## 付録. Diffie Hellman鍵交換の詳細例(その1)

### 動作1

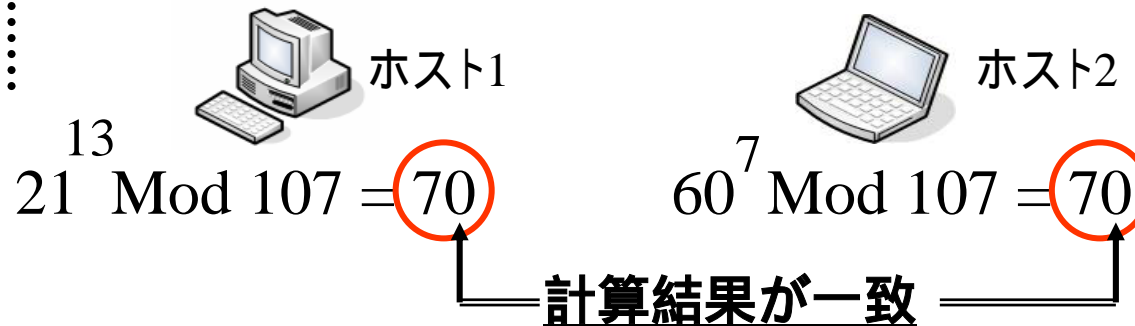


### 動作2

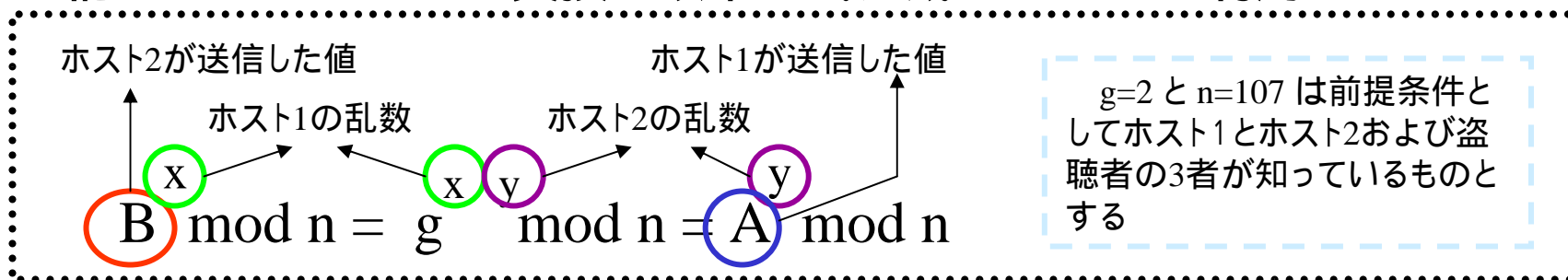


## 付録. Diffie Hellman鍵交換の詳細例(その2)

### 動作3



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



- 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

$$21^x \bmod 107 = 2^{xy} \bmod 107 = 60^y \bmod 107$$

この式から  $x, y$  を導き出すことは事実上不可能