本資料について

本資料は下記文献を基にして作成されたものです．文書の内容の正確さは保証できないため，正確な知識を求める方は原文を参照してください．

著者：F.Adrangi，H.Levkowetz

文献名：Mobile IPv4 Traversal of VPN Gateways

種類：Internet Draft

発表日：February 14,2004

Mobile IPv4 のVPNアクセスで発生する問題についての提案

渡邊研究室　　瀬下　正樹

発表内容

1. Introduction
2. **基礎技術の説明**
   - 2.1. IPsec
   - 2.2. Mobile IPv4
3. **具体的な**Mobile IP **と**VPN**の配置**

1. Introduction

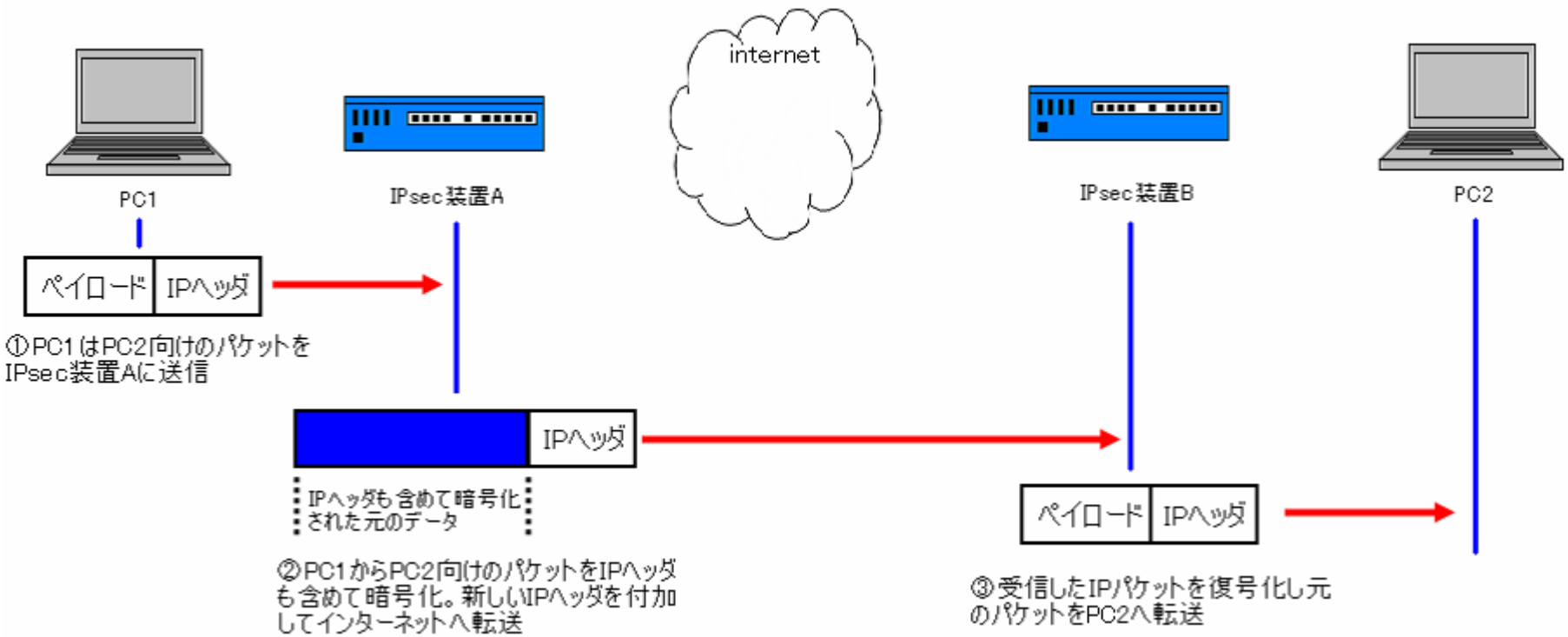
- **現在、**Mobile IP **を利用することで移動ノードが接続中の通信を維持したまま移動することが可能**
- **しかし、**Mobile IP**の**VPN**へのアクセスには多くの問題が存在**
- **この発表は、これらの問題について説明する**

2. 基礎技術の説明
2.1. IPsec 説明

- IPsec とはIPパケットを安全に運ぶための技術
- VPNはIPsecを利用し構築

2.1. IPsec 説明 (続き)
IPsec-ESP トンネルモード

- **場面設定**：PC1からPC2へパケットを送信

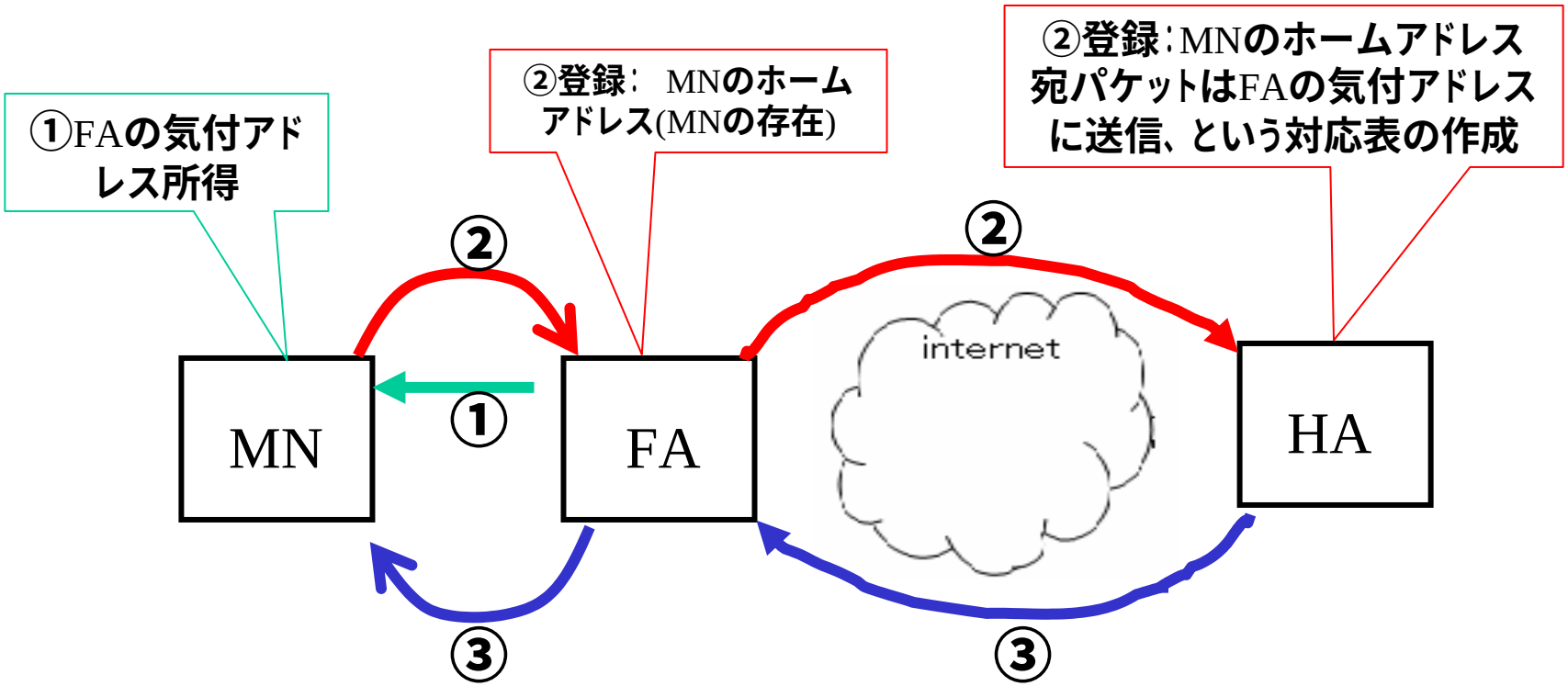


2.2. Mobile IP 説明

- インターネットでノード移動性を実現する技術
- ノードが移動しIPアドレスが変化しても接続中の通信を維持することが可能
- FA(Foreign Agent)を使用する、しないによって二つのmodeが存在
  - FAを利用：non co-located mode
  - FAを利用しない:co-located mode

2.2. Mobile IP:FAを利用した登録

登録:HA(Home Agent)にMN(mobile node = 移動端末)の気付アドレスを登録すること



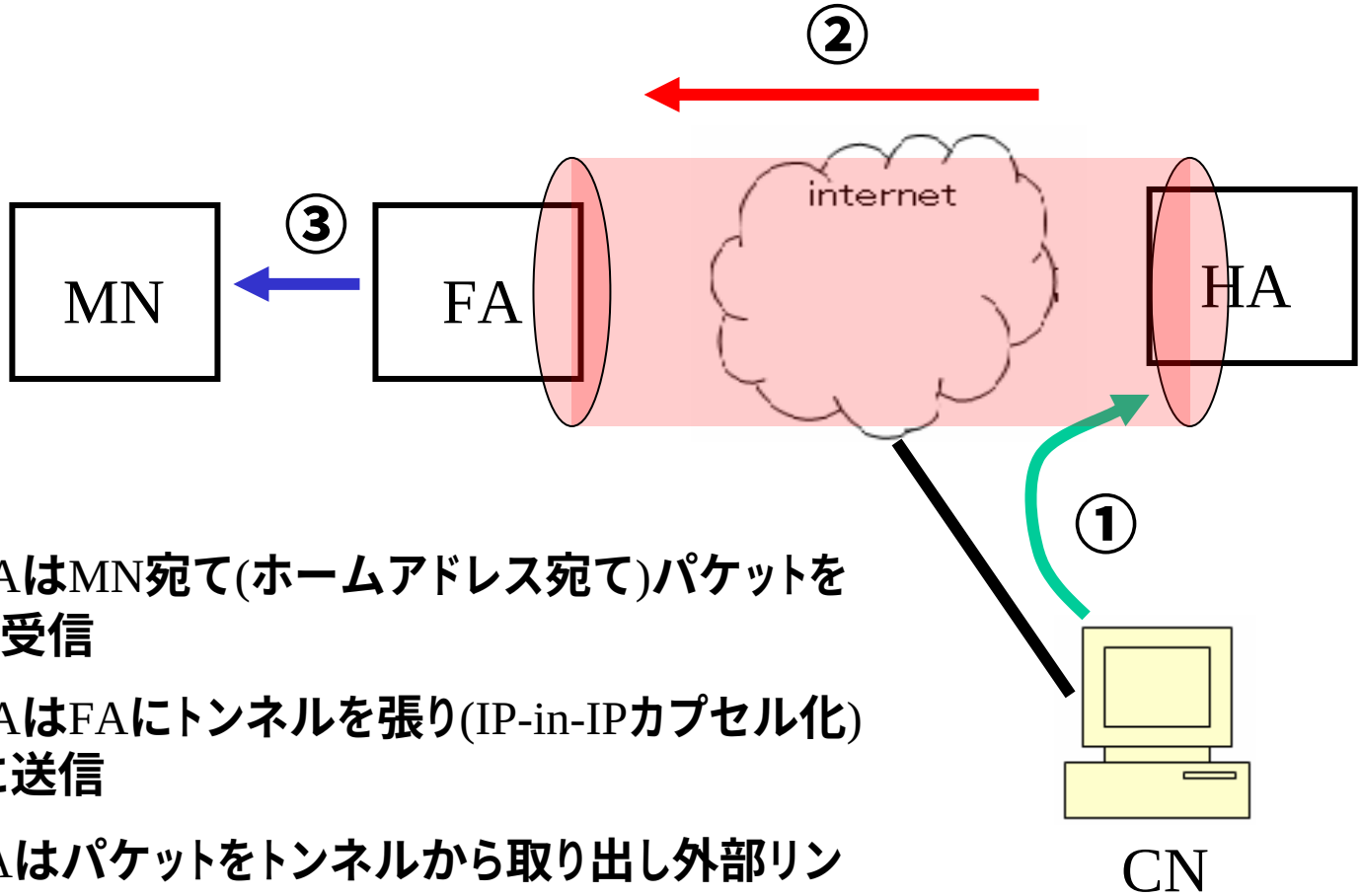
ホームアドレス：移動ノード(MN)に永続的に割り当てられたIPアドレス

①MNはFA広告によりFAの気付アドレスを所得

②登録要求：FAにMNのホームアドレスを登録。その後FAを経由してHAにFAの気付アドレスを登録

③登録応答:HAはMNへ登録を完了したことを知らせる

2.2. Mobile IP:FAを利用したパケット送信



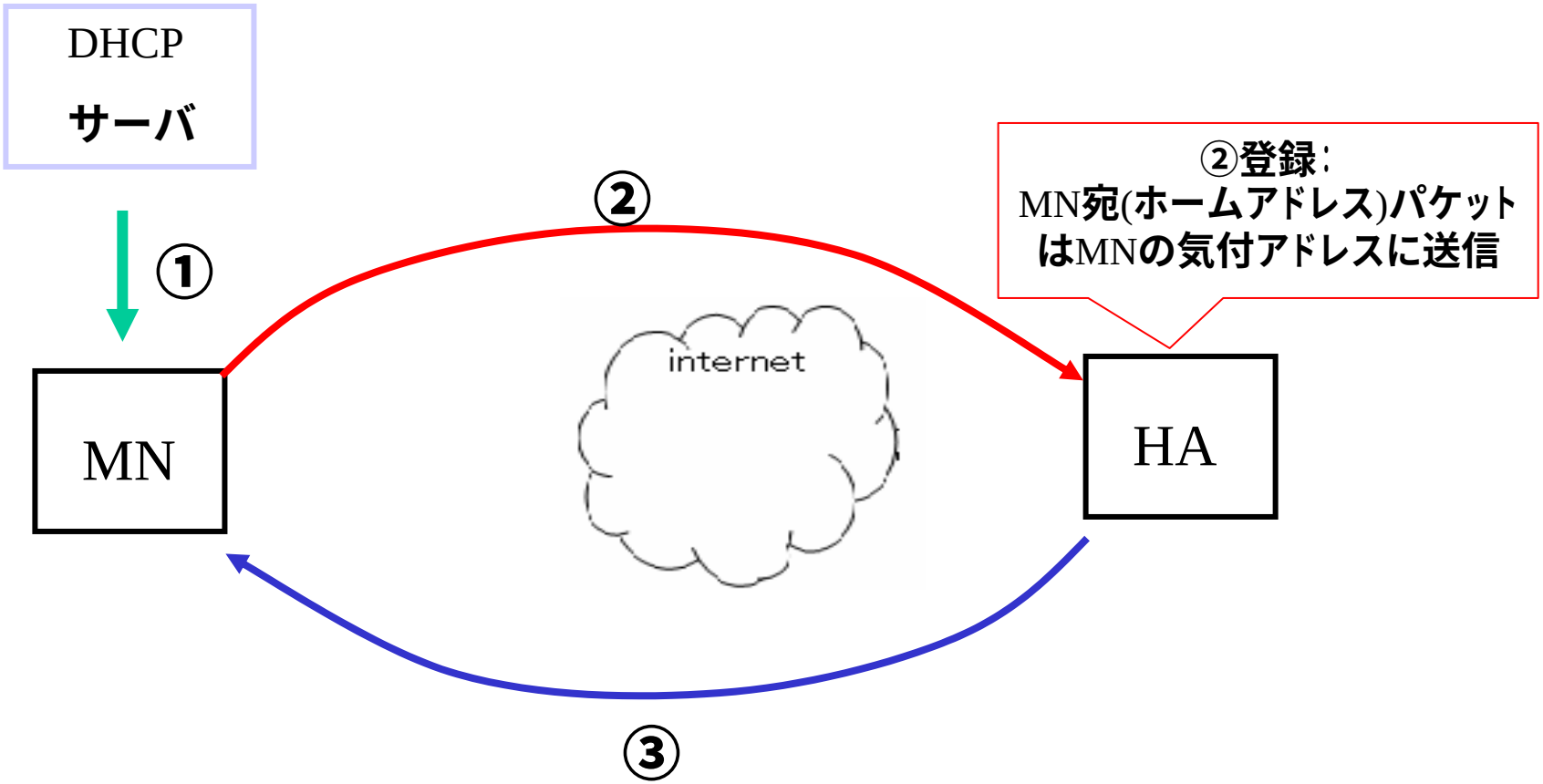
①HAはMN宛て(ホームアドレス宛て)パケットを代理受信

②HAはFAにトンネルを張り(IP-in-IPカプセル化)FAに送信

③FAはパケットをトンネルから取り出し外部リンク上の移動ノードへ配送

※MNからHAへのパケット送信の説明は省略

2.2. Mobile IP:FAを利用しない登録

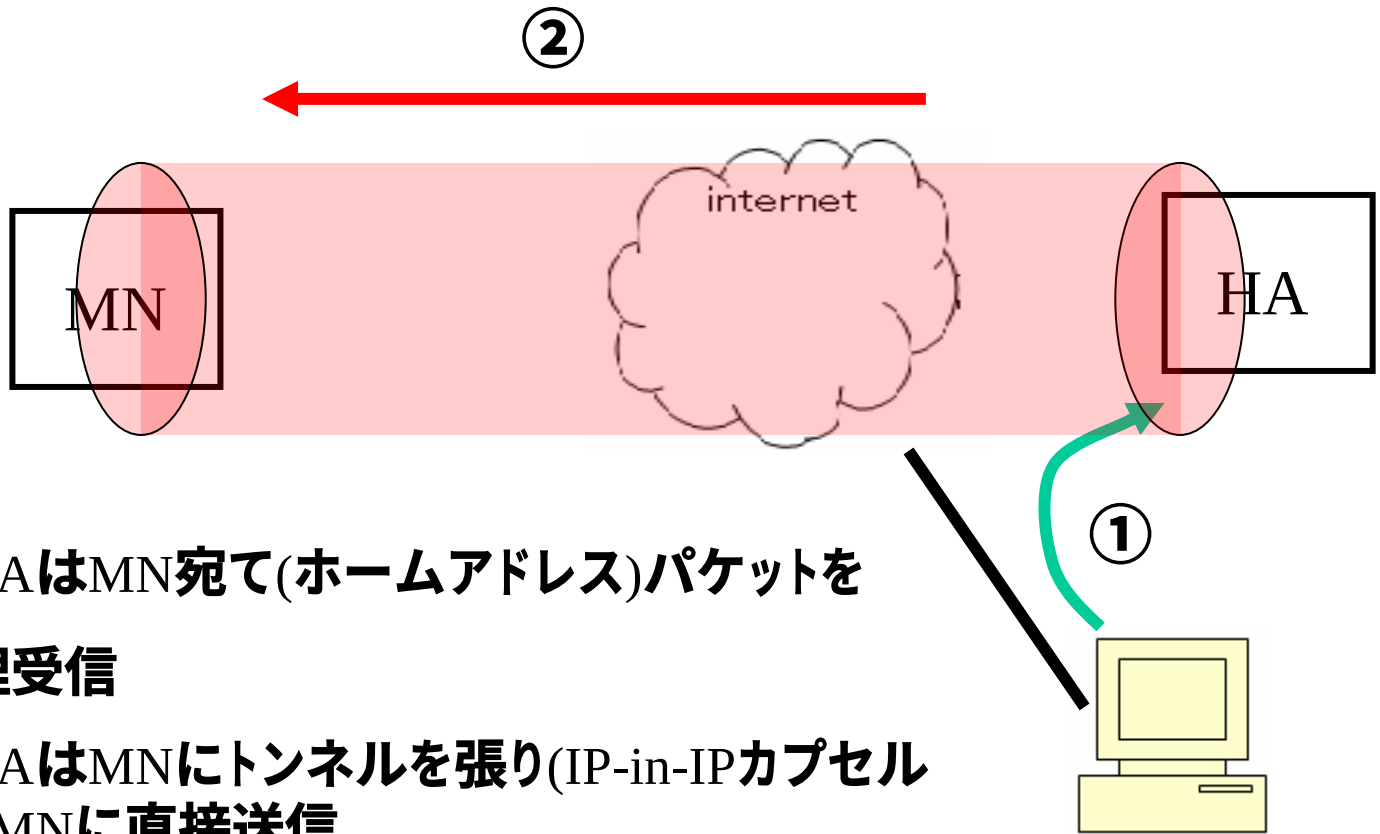


①MNはDHCPなどから気付アドレスを所得

②登録要求：MNの気付アドレスをHAに登録

③登録応答：HAはMNへ登録を完了したことを知らせる

2.2. Mobile IP:FAを利用しないパケット送信



①HAはMN宛て(ホームアドレス)パケットを代理受信

②HAはMNにトンネルを張り(IP-in-IPカプセル化) MNに直接送信

※MNからHAへのパケット送信の説明は省略

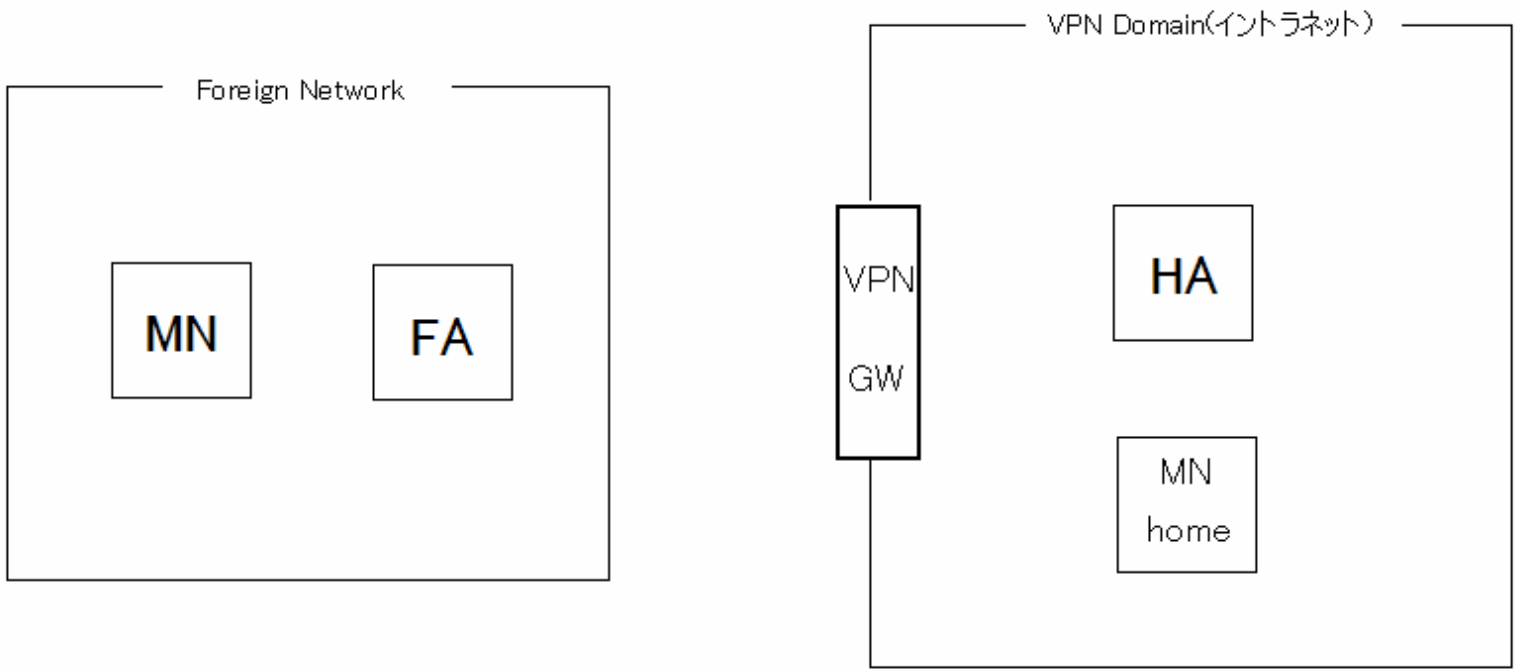
3. Mobile IP とVPNの配置シナリオ

- MIP(Mobile IP)とVPNのための実用的な配置シナリオの例を挙げる
- 場面設定：MNとMN homeの通信

補足説明

- シナリオではVPNドメイン(イントラネット)の内側では暗号化を実施しない
- MNはIPsec装置の機能を持っている
- MNからMN home宛のパケット送信は特に問題が発生しないので省略してある

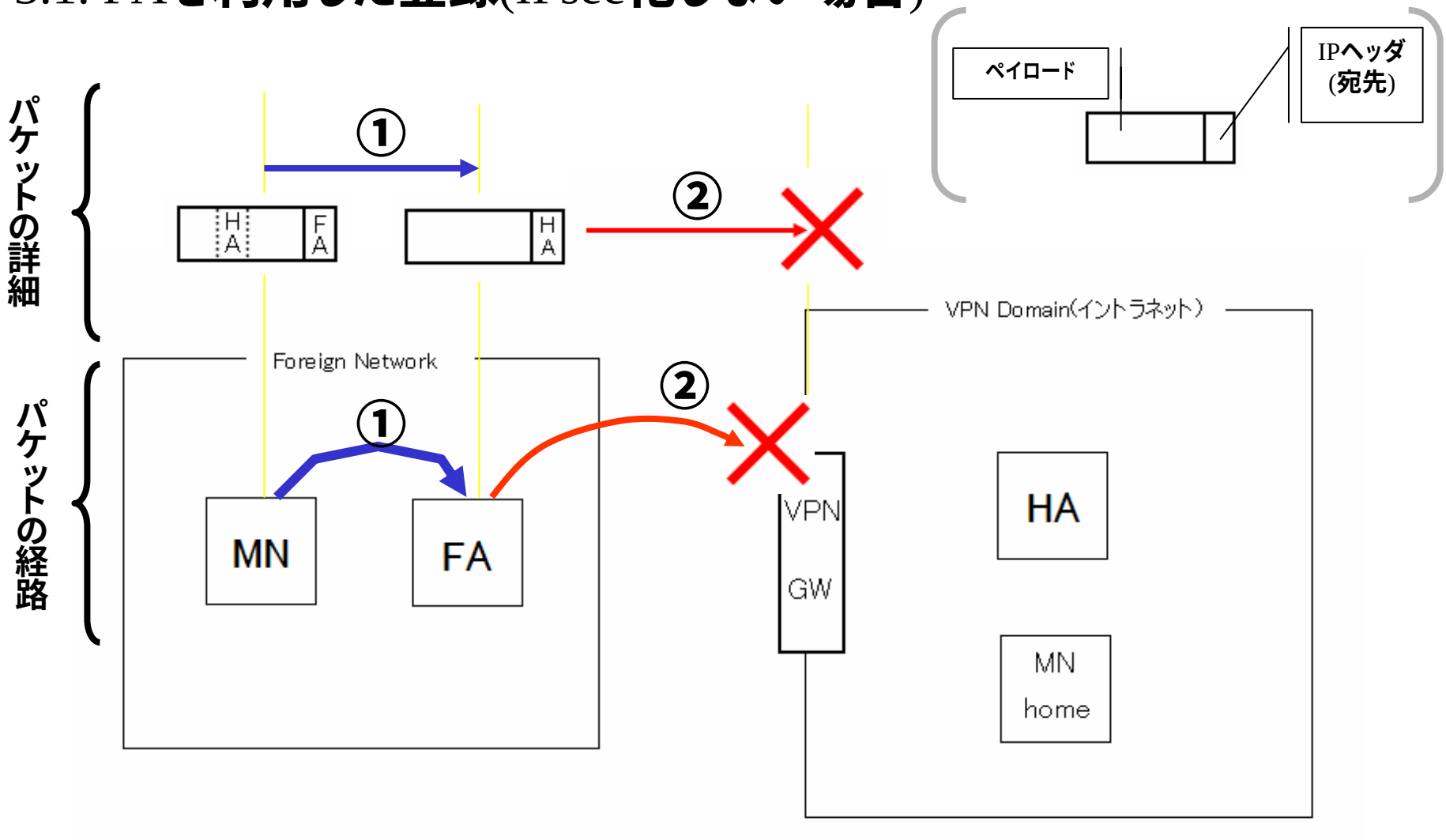
3.シナリオ1：VPNゲートウェイの後ろにあるイントラネットの内側のHA



配置説明

- MIP HAがVPNゲートウェイによって守られたイントラネットの内側に配置
- MNはイントラネットの外部から、直接HAにアクセスすることができない

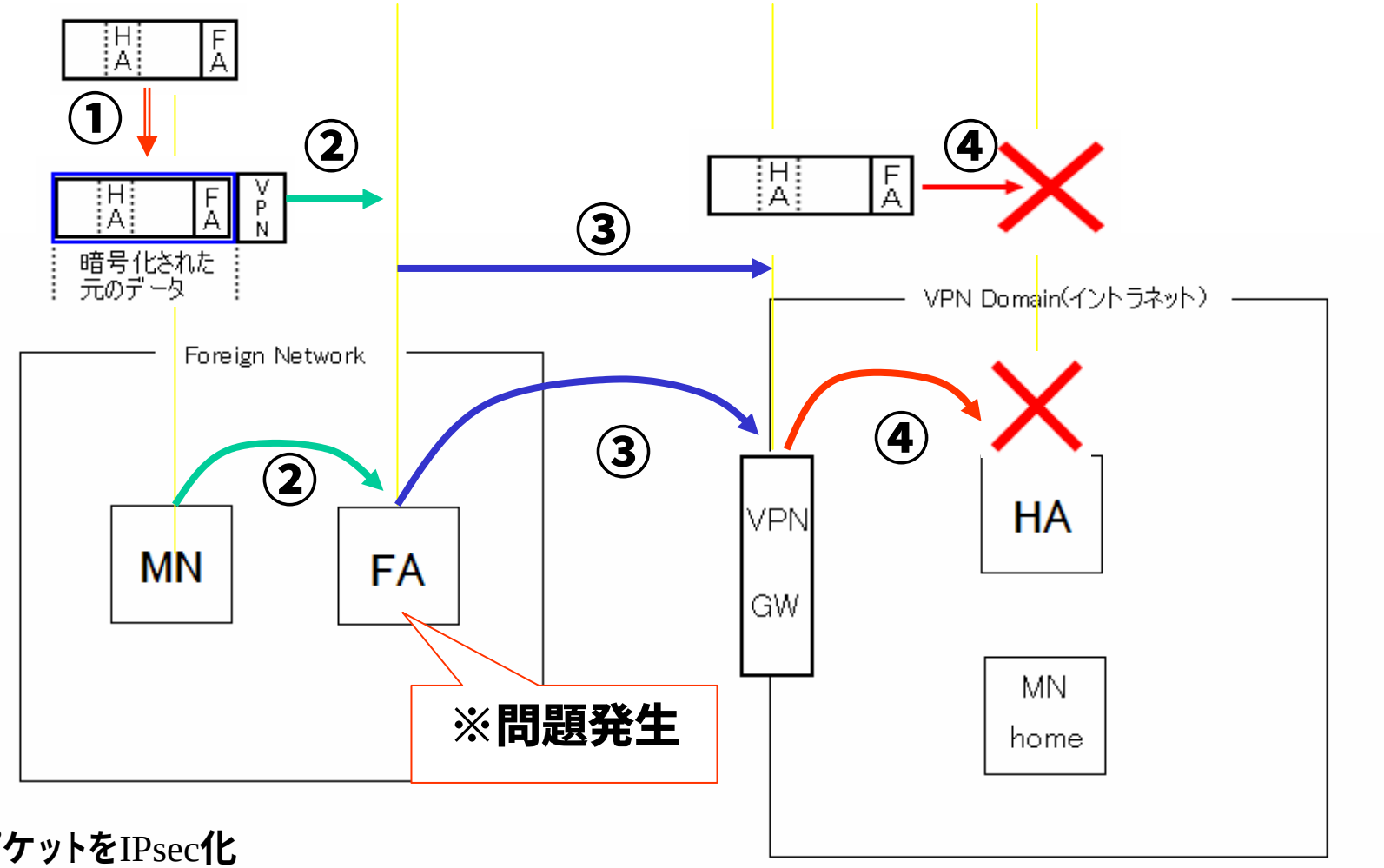
3.1. FAを利用した登録(IPsec化しない場合)



①MNはFAへパケットを送信

②FAはパケットのデータを参照し、HA宛のIPヘッダを付加し送信。しかしIPsec化されていないのでイントラネット内に入ることができない=>登録失敗

3.1. FAを利用した登録(IPsec化した場合)



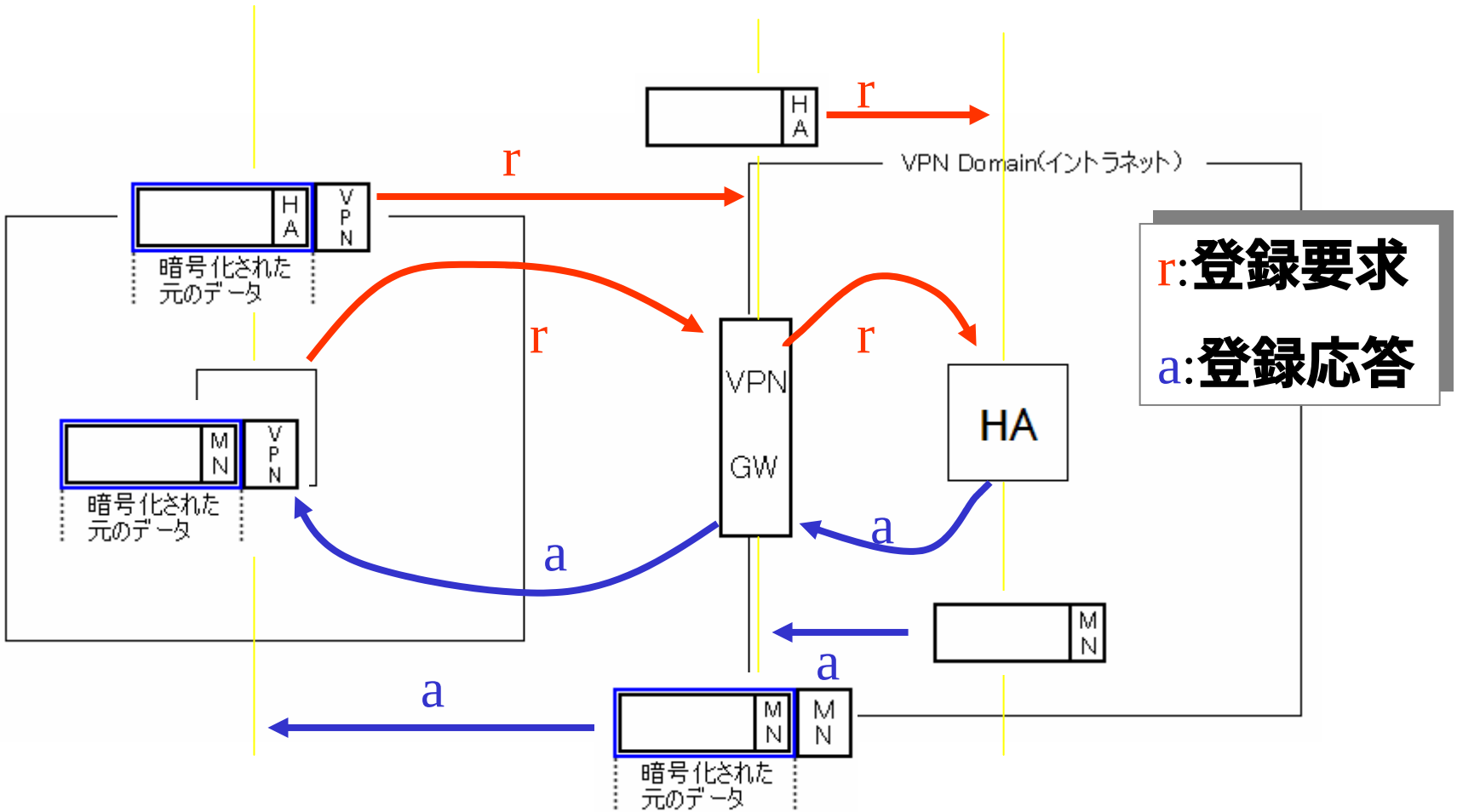
①パケットをIPsec化

②MNからFAへパケットを送信。しかしパケットが暗号化されているためFAはデータを見ることができない。

③IPヘッダを変更せず、VPN-GWに送信

④IPヘッダの宛先がFAになっているので、HAには送信できない=>登録失敗

3.1. FAを利用しない登録

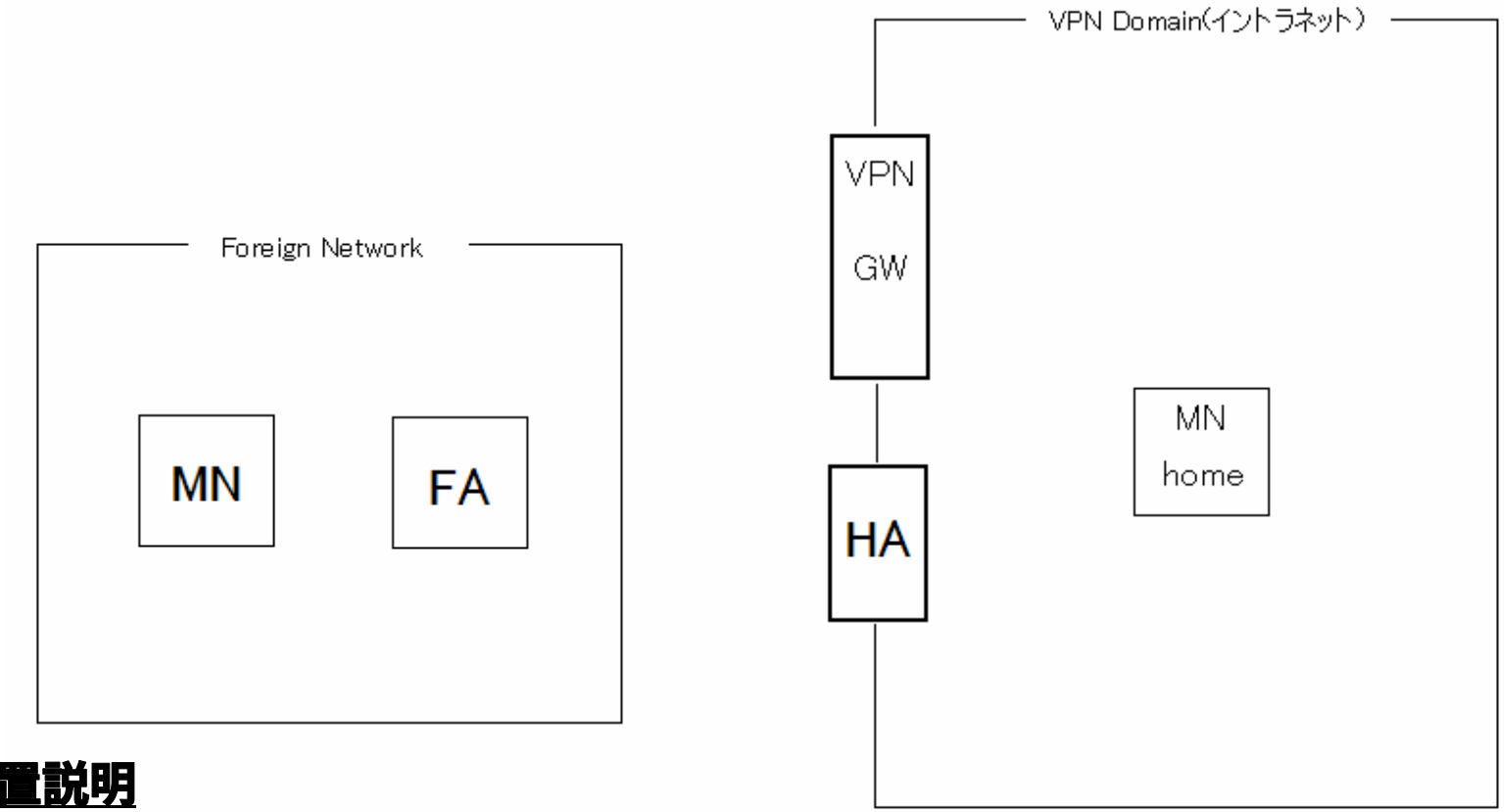


FAを利用しなければ**登録することが可能**

※しかしMNの所属ネットウォークが変わるたびにVPNトンネルをリ･ネゴシエートする必要がある

メモ：パケットの送信は問題がないので省略

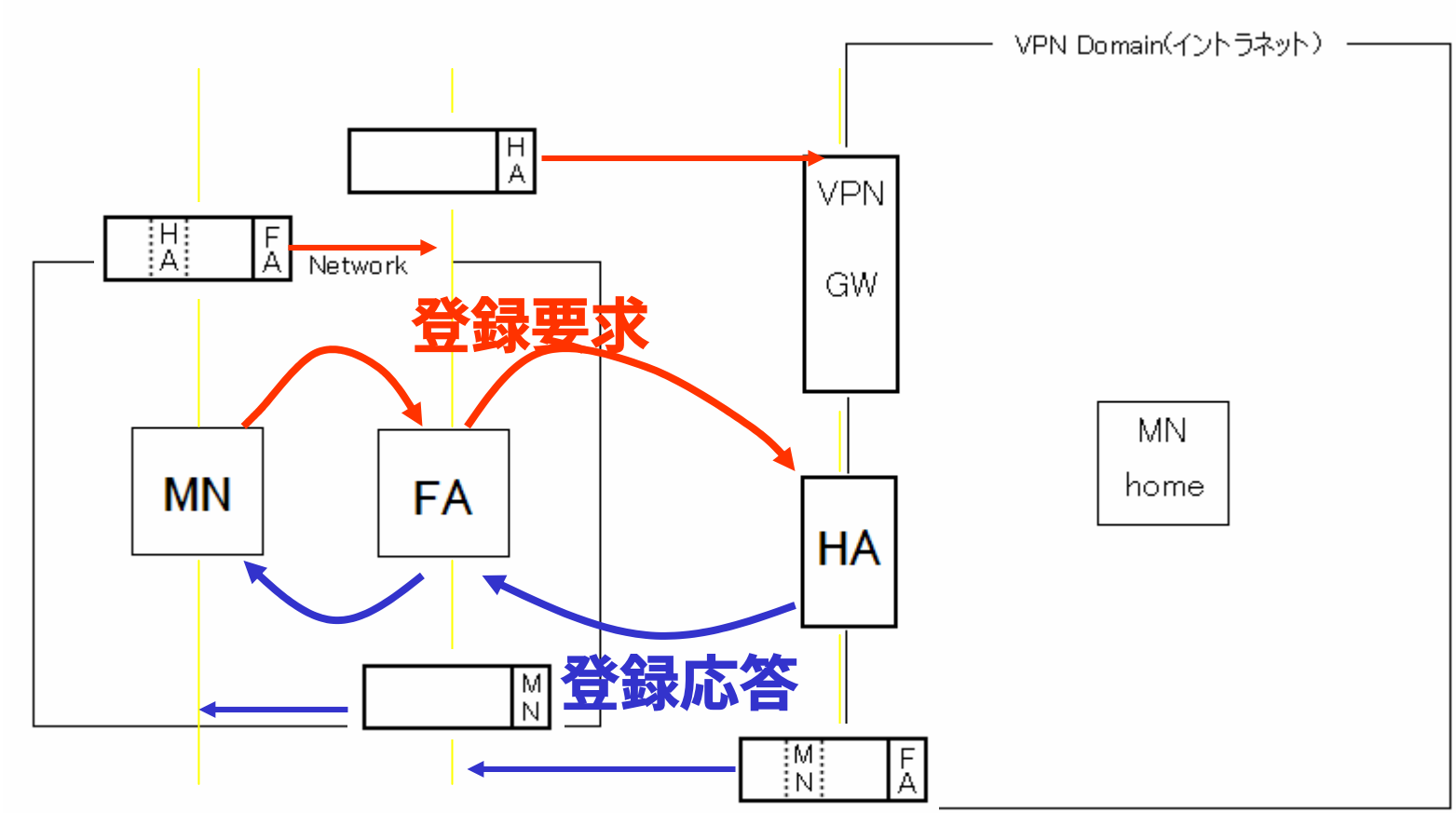
3.シナリオ2：VPNドメイン境界上のVPNゲートウェイとMIPv4 HA(s)



配置説明

- HAがVPN-GWと共に、VPNドメイン境界上に配置
- MNからHAへはイントラネットの内、外からでも直接アクセス可能
- 「IPsecトンネル内部のMIP」と「MIPトンネル内部のIPsec」の二つの展開が存在

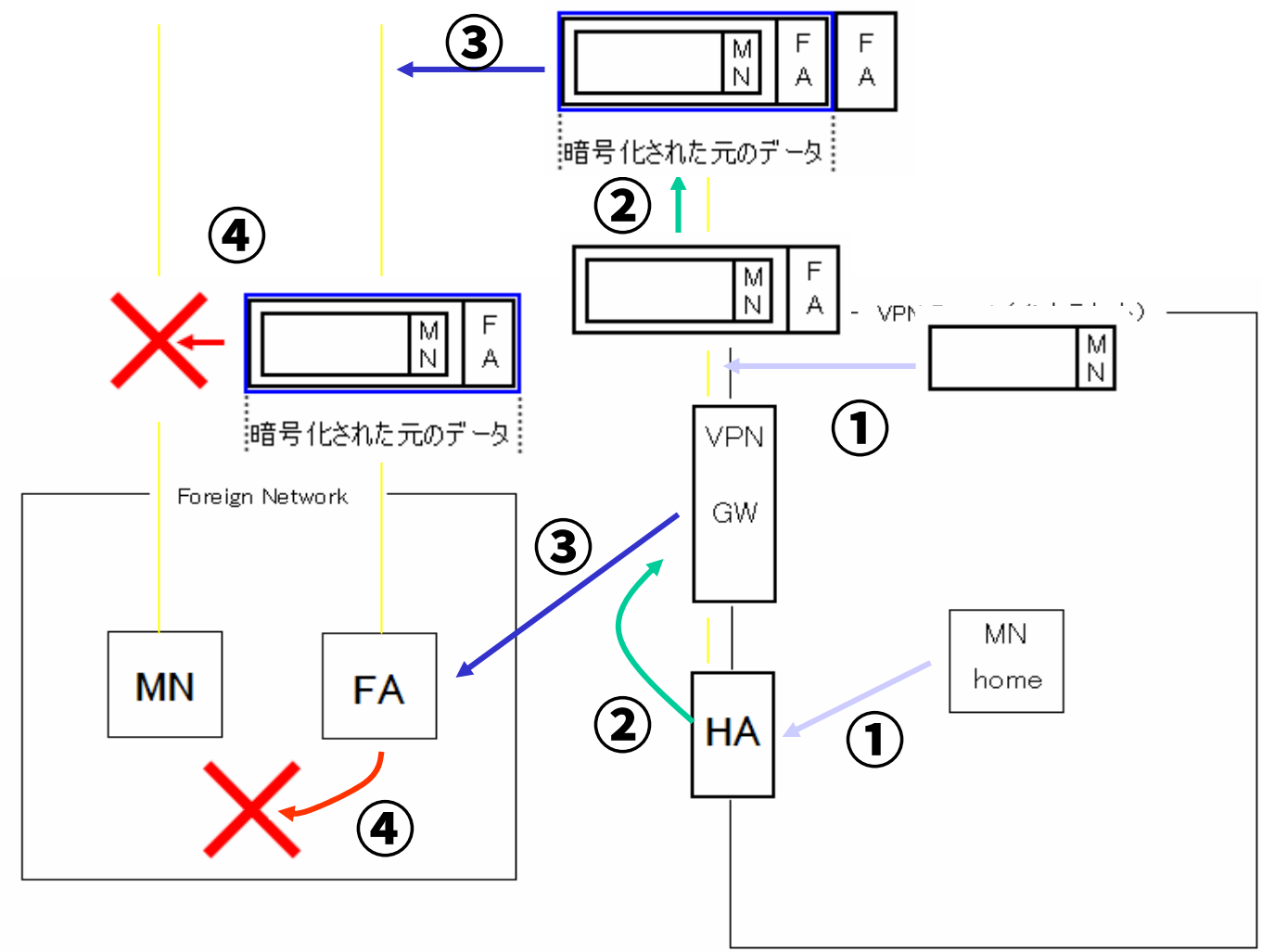
3.2. FAを利用した登録



FAを利用し**登録することが可能**

メモ：説明は省略するがFAを利用しなくても登録可能

3.2. MN HomeからMNへのパケット送信（IPsecトンネル内部のMIP）

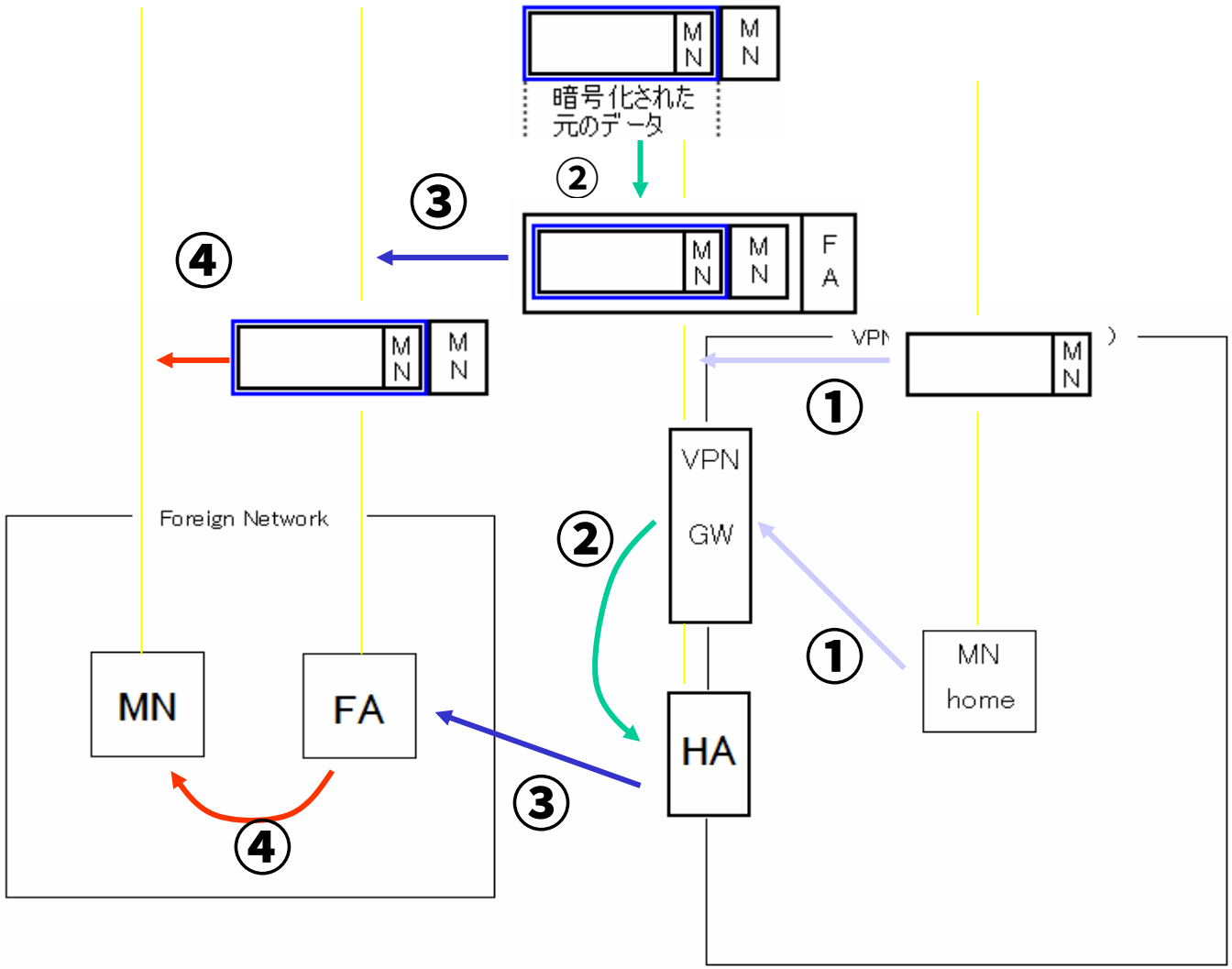


①MN homeからHAに送信　②IP-in-IPカプセル化しVPN-GWへ送信　③IPsec化しFAに送信

④データが暗号化されておりFAはMNへ送信できない =>パケット送信失敗

※FAを利用しないco-located modeならば送信可能。しかし2.1. と同じ問題（リ・ネゴシエーション）が発生。

3.2. MN HomeからMNへのパケット送信 (MIPトンネル内部のIPsec)

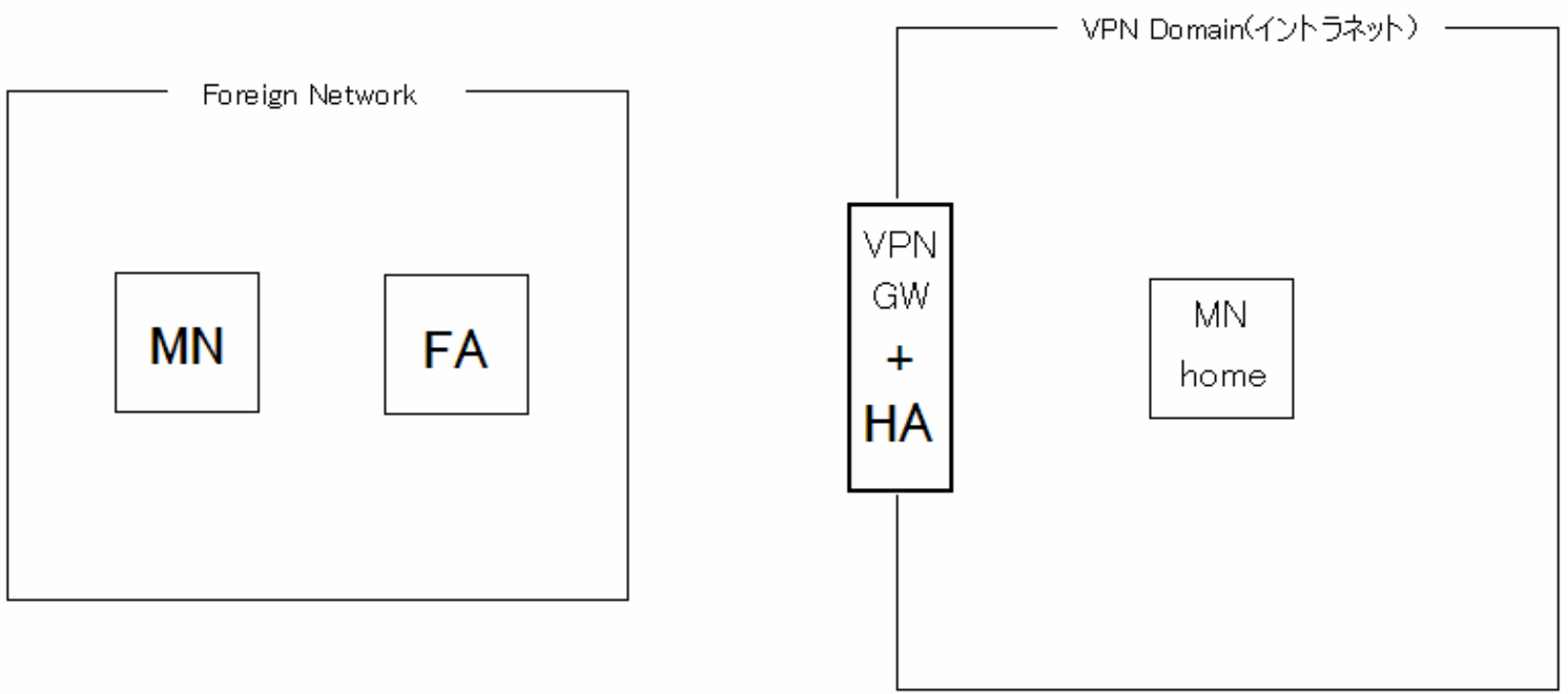


①MN homeからVPN-GWへ送信　②IPsec化しHAへ送信

③IP-in-IPカプセル化しFAへ送信　④FAからMNへ送信 =>パケット送信成功

※パケット送信可能だが、HAやVPN-GWのルーティングロジックの修正、変更が必要

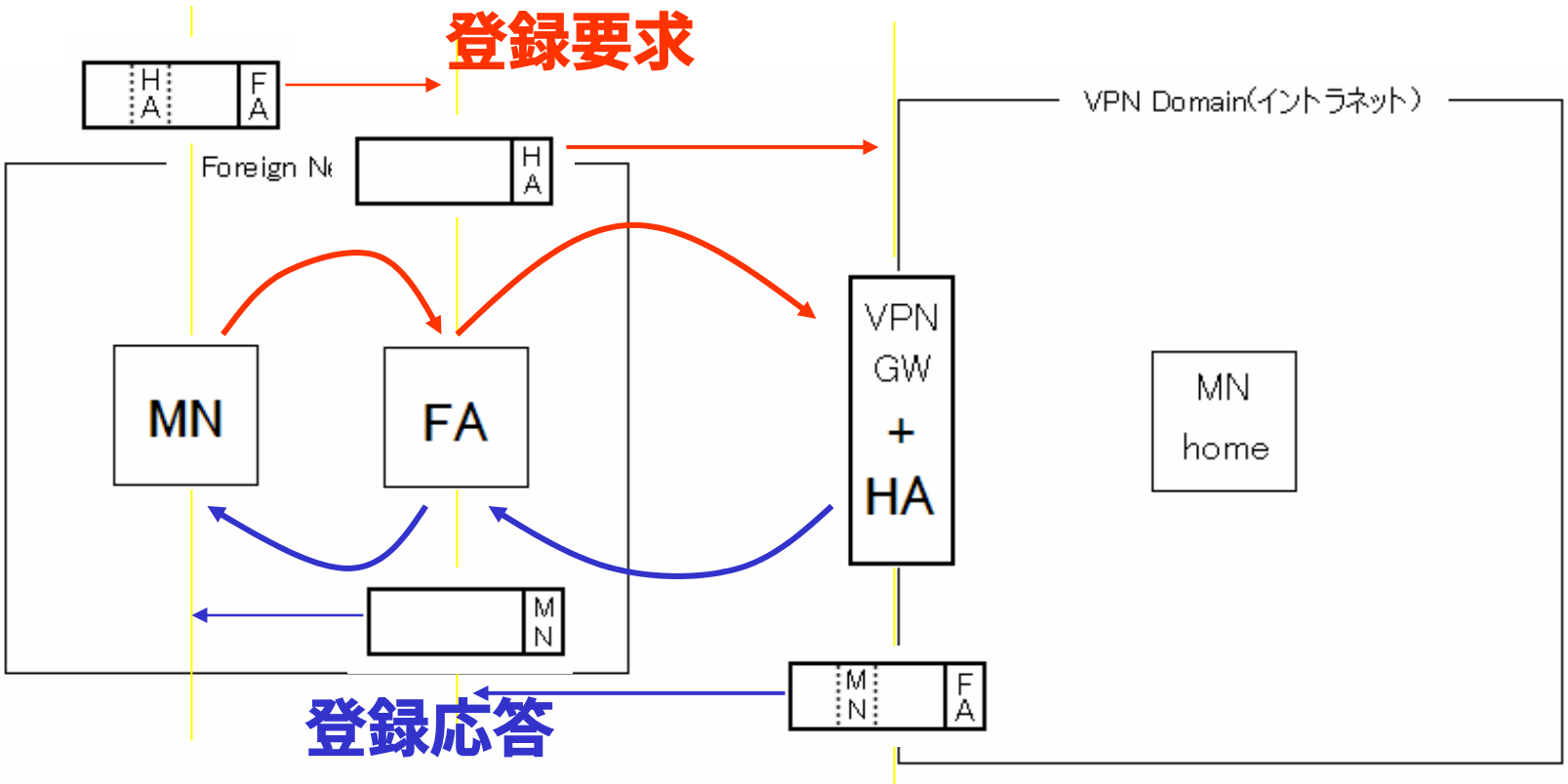
3.シナリオ3：VPN GW + HA



配置説明

- 2.2と類似した配置シナリオ
- 異なる点：VPN-GWとHAが同じ機器上で動作
- 2.2で存在するルーティングの問題を解決できる

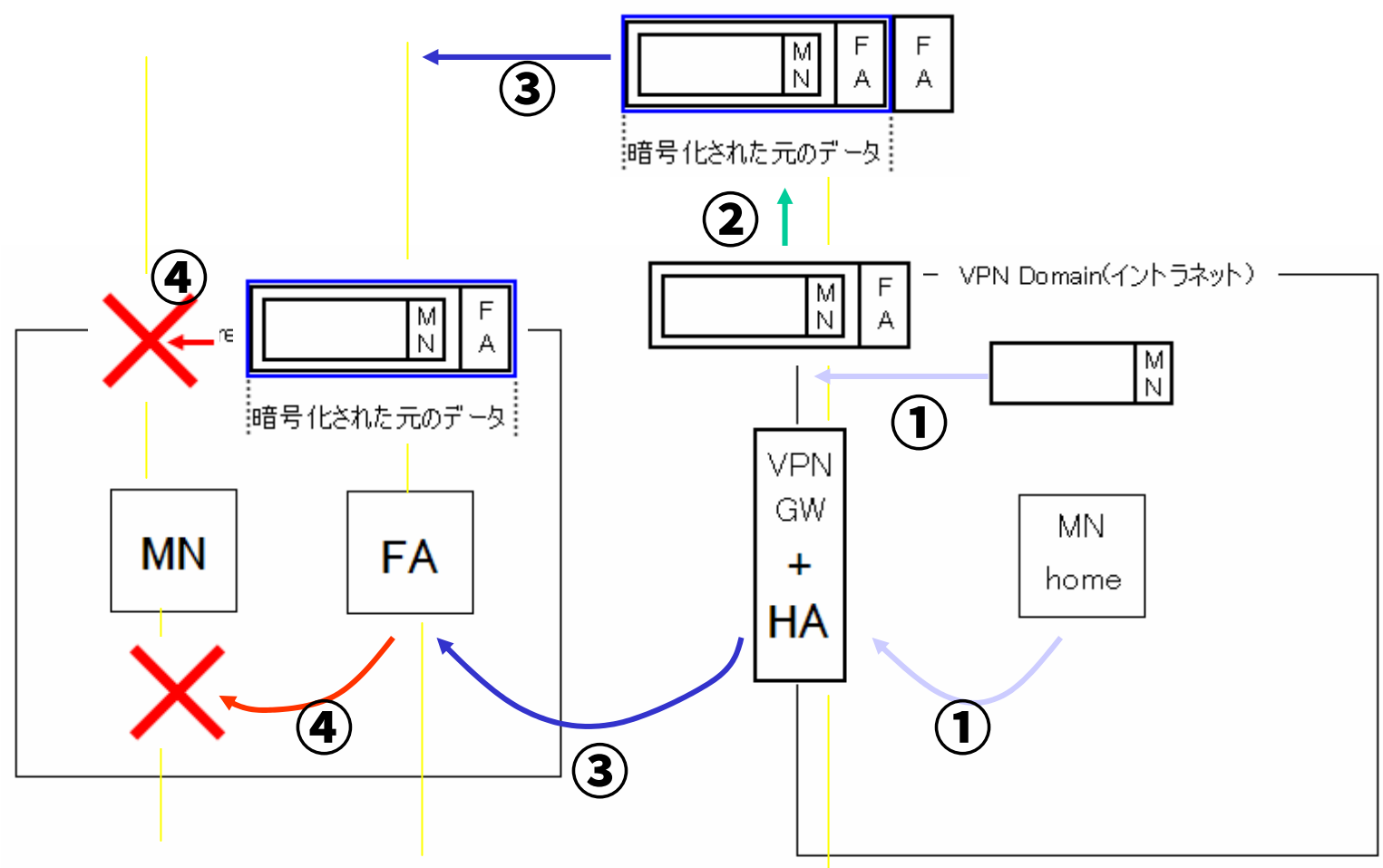
3.3. FAを利用した登録



FAを利用し登録することが可能

メモ：FAを利用しなくても登録可能

3.3. MN HomeからMNへのパケット送信 (IPsecトンネル内部のMIP)

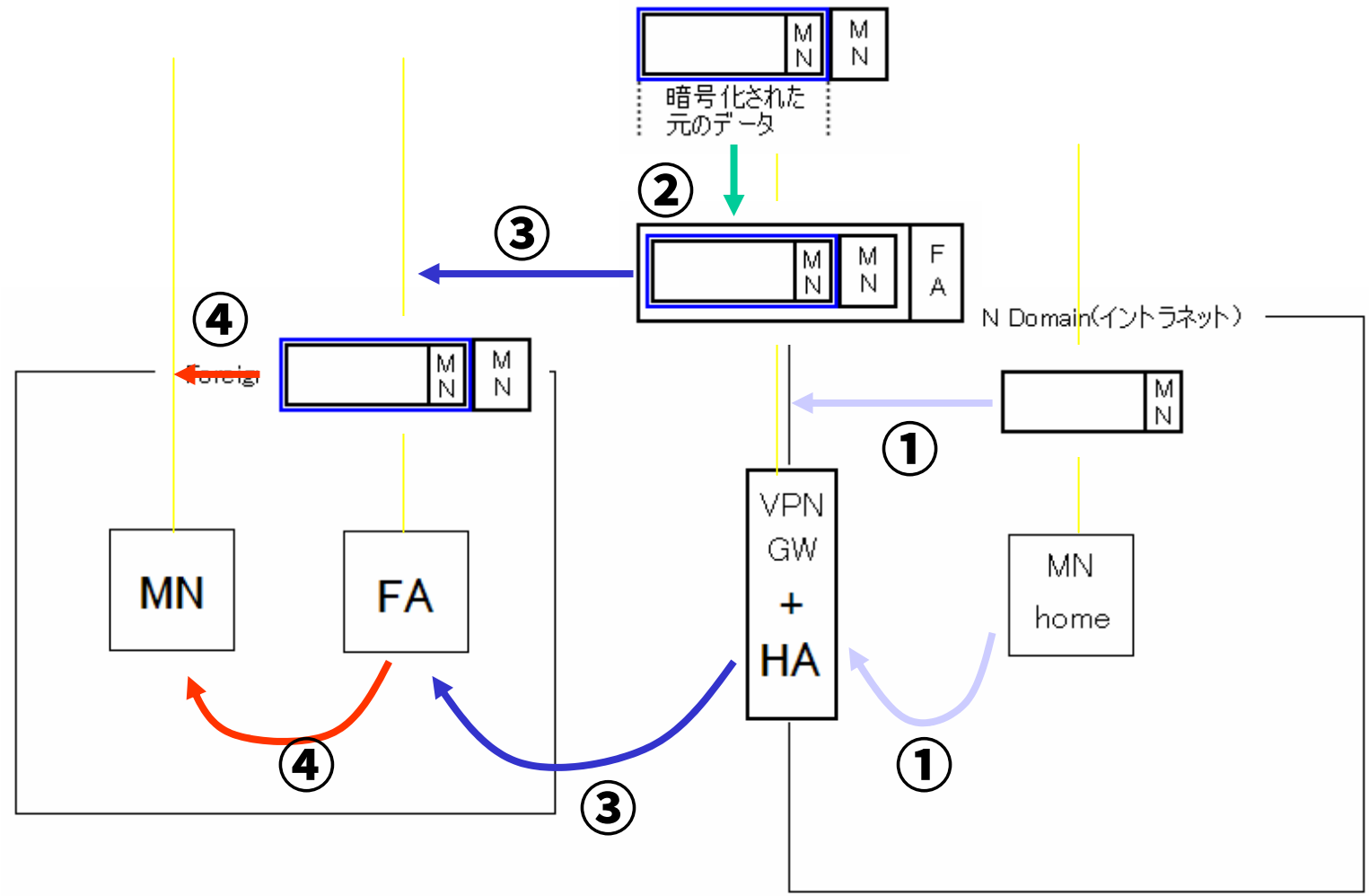


①MN home から　VPN-GW+HAへ送信　② VPN-GW+HA上でIP-in-IPカプセル化③ VPN-GW+HA上でIPsec化しFAへ送信 ④FAは受信したパケットが解析できないためMNへ送信できない

=>パケット送信失敗

※FAを利用しないco-located modeならば送信可能。しかし2.1. と同じ問題 (リネゴシエーション) が発生。

3.3. MN HomeからMNへのパケット送信（MIPトンネル内部のIPsec）



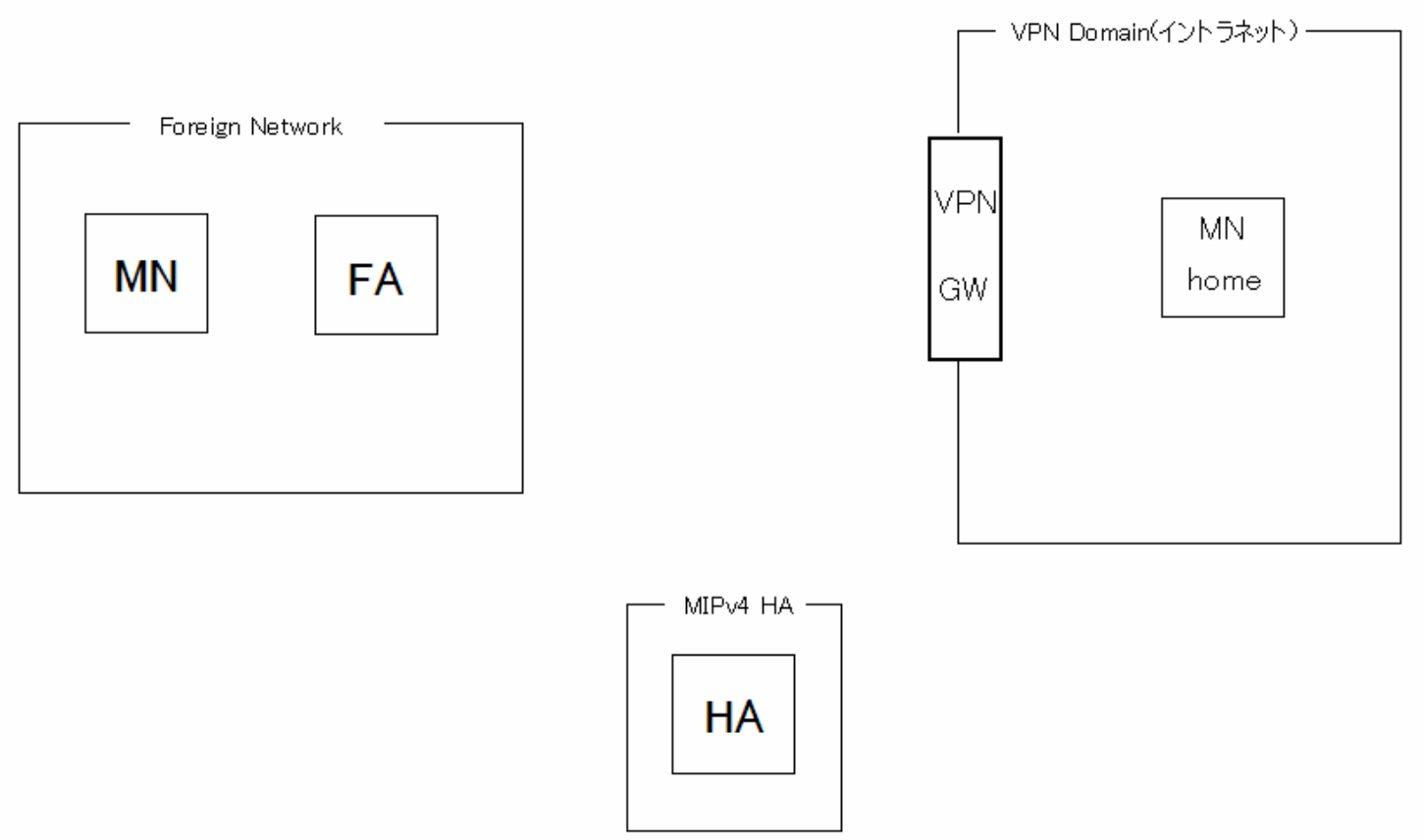
①MN homeからVPN-GW+HAへ送信　②IPsec化　③IP-in-IPカプセル化しFAへ送信

④FAからMNへ送信 =>パケット送信成功

「MIPトンネル内部のIPsec」ならば送信可能

※VPN-GW+HAの相互接続運用性の確認が必要

3.シナリオ4：VPNドメインの外側のMIPv4 HA(s)



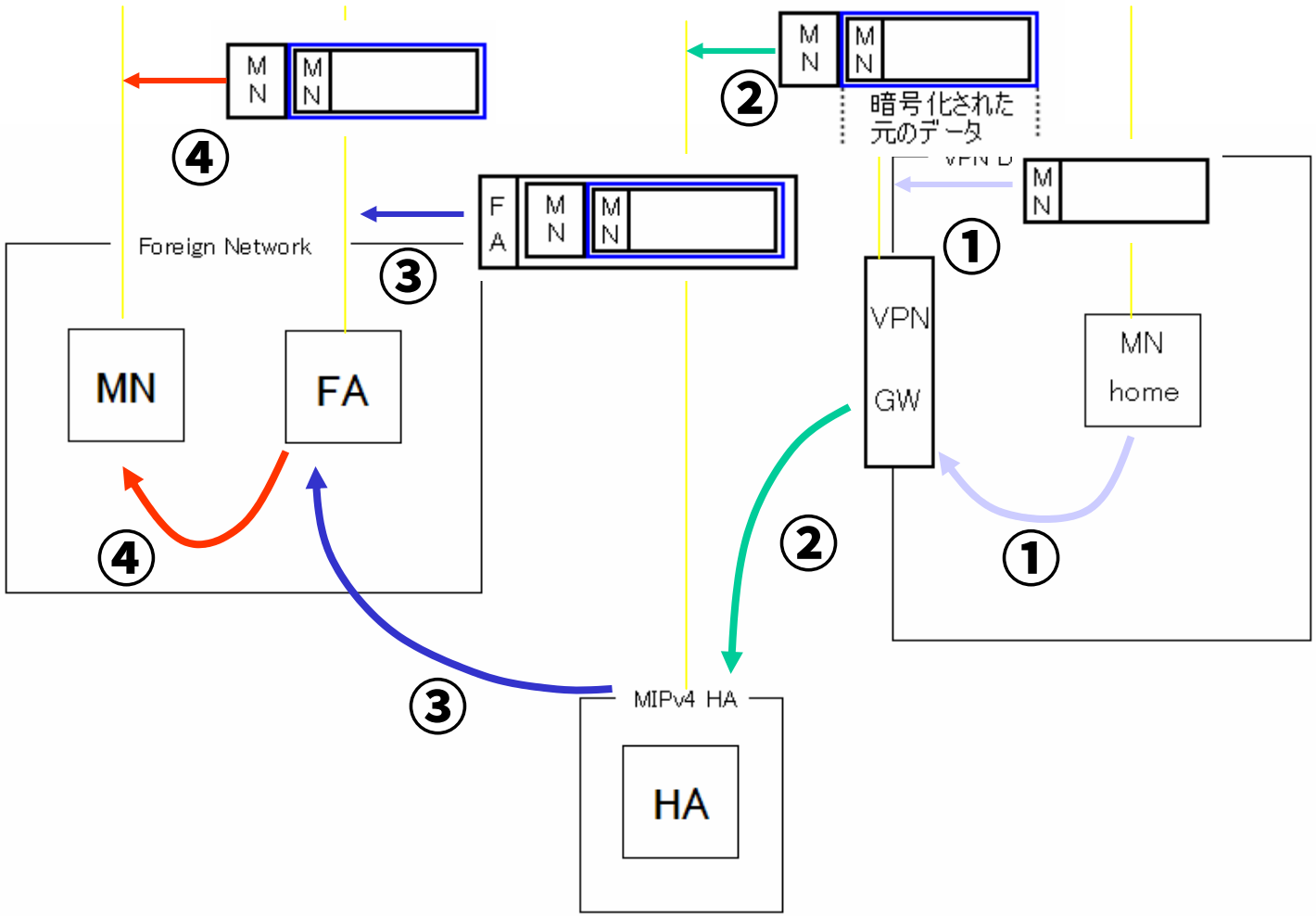
配置説明

- HAがイントラネットの外側に配置

3.4. 登録

- FAを利用する場合、FAを利用しない場合の両方で登録可能(動作図は省略)

3.4. MN home からMNへパケットを転送



①MN home から　VPN-GWへ送信　②IPsec化してHAへ送信　③IP-in-IPカプセル化してFAへ送信　④MNへ送信　=>パケット送信成功

※HAがイントラネットの外側にあるためイントラネットの内側での移動性は提供されない

3章のまとめ

シナリオ1．VPN-GWの後ろにあるイントラネットの内側のHA

- FAを利用しなければ送信可能。しかしモバイル端末の所属ネットワークが変わるたびにリ･ネゴシエーションする必要がある

シナリオ2．VPNドメイン境界上のVPNゲートウェイとMIPv4HA(s)

- 「IPsecトンネル内部のMIPv4」ではFAを利用することができず、シナリオ1と同じ問題が発生
- 「MIPトンネル内部のIPsec」では特に問題はないが、ルーティングロジックの修正、変更が必要

シナリオ3．VPN GW + HA

- シナリオ2のルーティング問題を解決できる

シナリオ4．VPNドメインの外側のMIPv4 HA(s)

- インターネットの内側では移動性が提供されないこと以外は特に問題ない

3章のまとめ（続き）

- シナリオ1,2,3に共通する問題
  - FAを利用しない場合(co-located mode)はモバイル端末の所属ネットワークが変わるたびにVPNトンネルをもう一度ネゴシエートする必要がある

=>MOBIKE workgroup によって解決が可能

3章の感想

- **シナリオ全体での疑問点**
  - MOBIKE**とはどんな技術なのか**
  - 「non co-located mode(FA**利用**)」**と**「co-located mode(FA**利用せず**)**において**MOBIKE**を利用**」**はどちらが優れているのか**
  - **実際どのシナリオが有効なのか**

終わり