本資料について

本資料は下記の文献をもとに作成されました。
文章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。

文献：ワイヤレス・ユビキタス
　　－高速無線LAN / UWB / 3.5G携帯電話－
　　第8章 「8.1　モバイルIP」
著者：石山 政浩　　監修：阪田 史郎
発行所：株式会社 秀和システム
発行日：2004年8月3日

ワイヤレス・ユビキタス
― モバイルIP ―

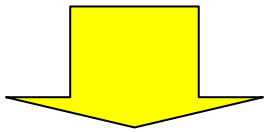
石川政浩 阪田史郎

名城大学理工学部 渡邊研究室

榎本 万人

はじめに

- インターネットは社会的な基盤として認知され、多様な場面で利用される。
- ノードの小型軽量化、無線技術の発達により、ノードは移動しながらでもインターネットへの接続が可能。



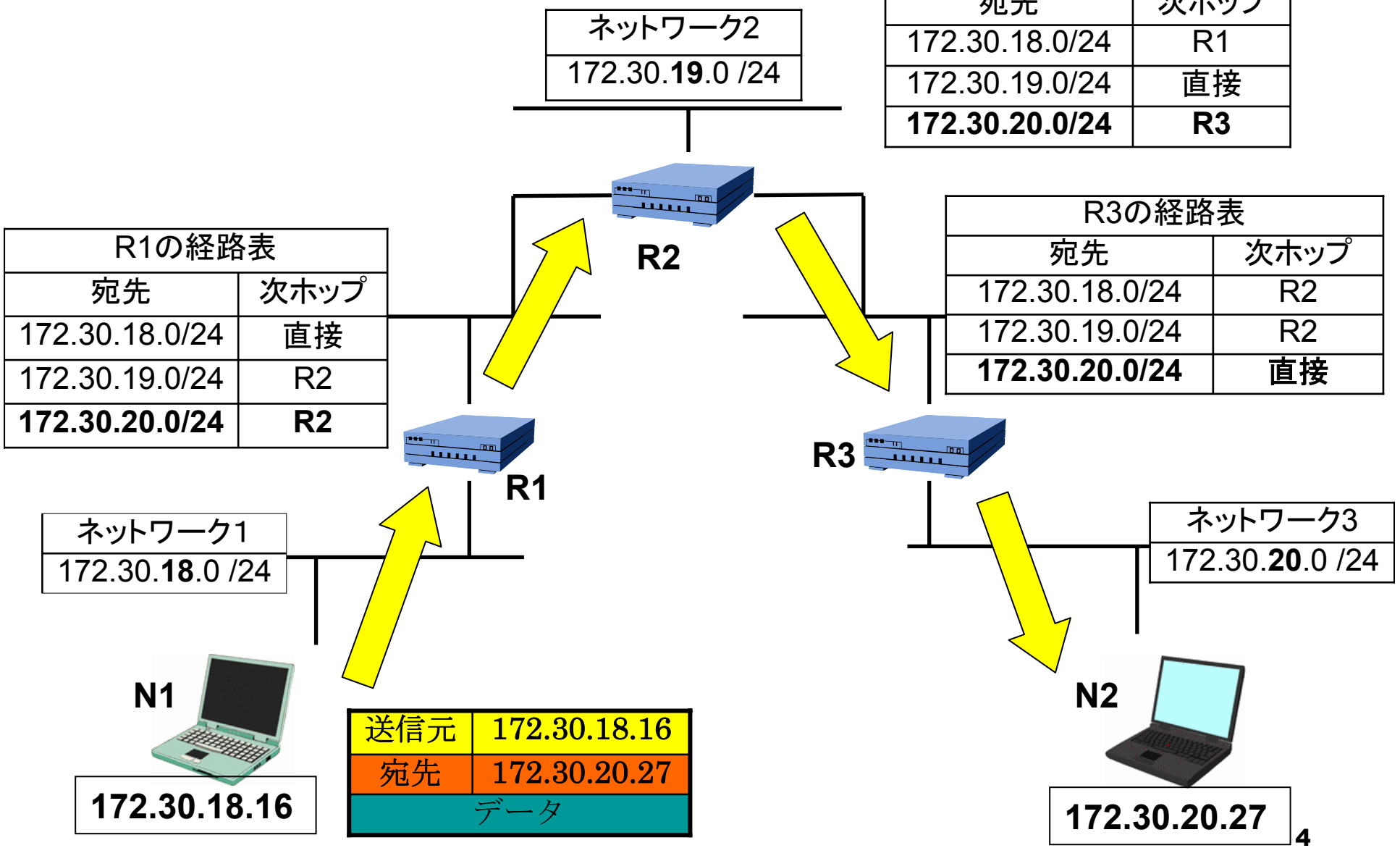
現在のインターネット・プロトコル(IP)では、ノードの移動に問題がある。

ノードの移動に伴う問題

R2の経路表	
宛先	次ホップ
172.30.18.0/24	R1
172.30.19.0/24	直接
172.30.20.0/24	**R3**

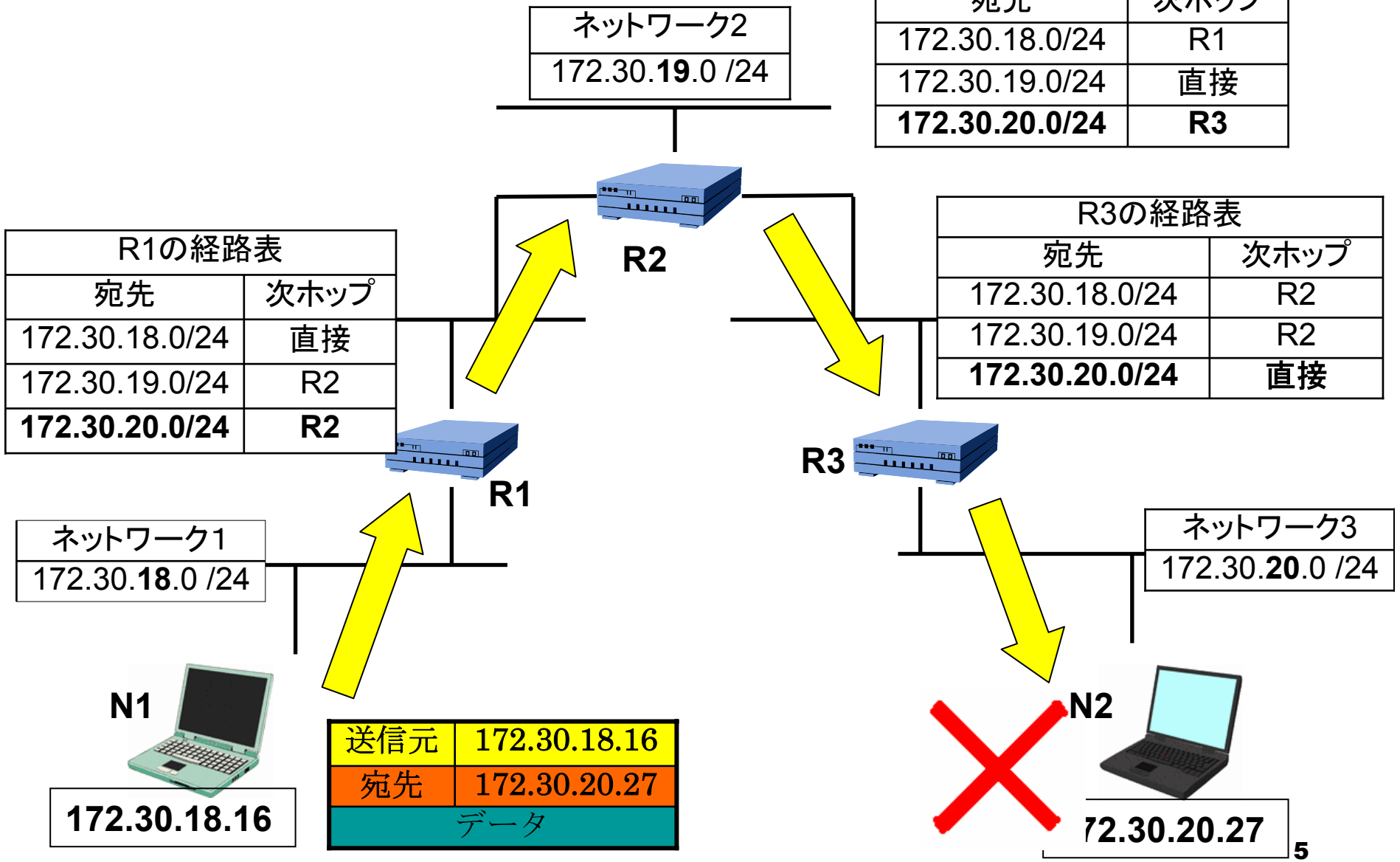
R1の経路表	
宛先	次ホップ
172.30.18.0/24	直接
172.30.19.0/24	R2
172.30.20.0/24	**R2**

R3の経路表	
宛先	次ホップ
172.30.18.0/24	R2
172.30.19.0/24	R2
172.30.20.0/24	**直接**



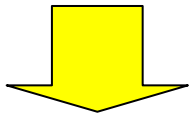
ノードの移動に伴う問題

R2の経路表	
宛先	次ホップ
172.30.18.0/24	R1
172.30.19.0/24	直接
172.30.20.0/24	**R3**



ノードの移動に伴う問題

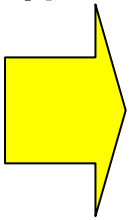
ノードが別のサブネットへ移動する



移動ノードはパケットを受信することが出来ない

パケットを受信するには

- 接続したサブネットに適したIPアドレスへ変更
- 確立していた通信を全て廃棄
- アドレス変更の情報を通信相手N1との間で交換



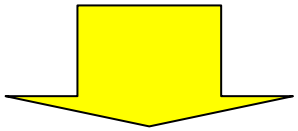
アプリケーションの複雑化

通信の遅延の発生

モバイル IP

問題解決のため、モバイルIPが考案。

- ノードが移動した場合、同じIPアドレスを使用可能にし、通信を維持する。
- 水平ハンドオーバだけでなく垂直ハンドオーバも実現可能。

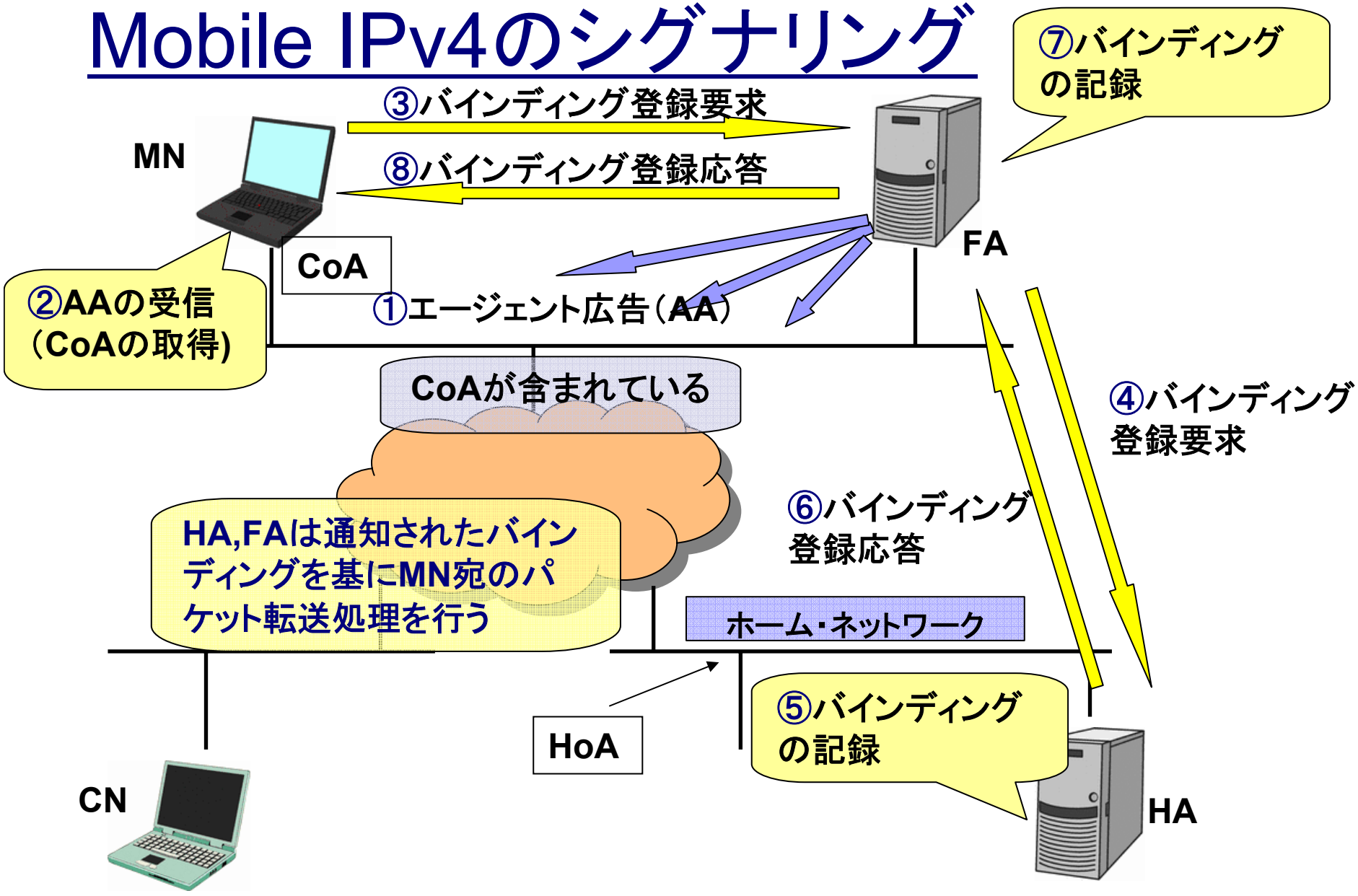


モバイル・コンピューティングの多様化を支援する基盤技術になることが期待される。

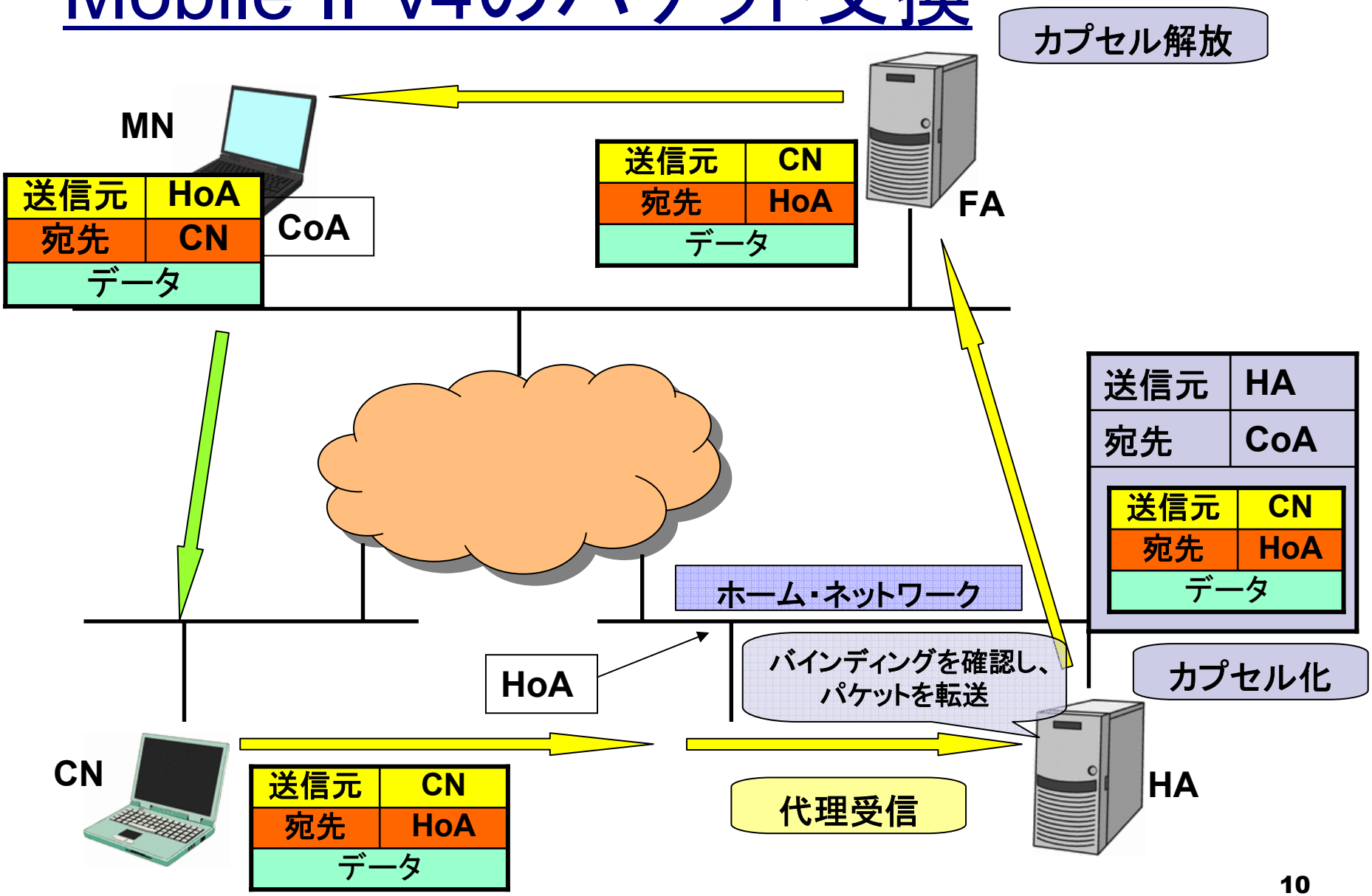
モバイルIPの用語

用語	略語	機能
ホーム・アドレス	HoA	移動ノードが使い続けるアドレス
気付アドレス	CoA	移動ノードが訪問したサブネットで使用するアドレス
バインディング	ー	HoAとCoAの組およびそれらに付随する情報。
ホーム・エージェント	HA	ホーム・ネットワークにいる転送エージェント
訪問先エージェント	FA	MNの訪問先のネットワークにいるエージェント

Mobile IPv4のシグナリング



Mobile IPv4のパケット交換

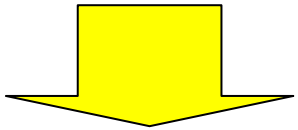


Mobile IPv4が抱える問題

送信元アドレス詐称攻撃と誤認される可能性がある。

送信元アドレス詐称攻撃

悪意をもつユーザが逆探査を逃れるために攻撃パケットの送信元を偽って送信する攻撃



対策として、イングレス・フィルタリングが推奨

Mobile IPv4が抱える問題

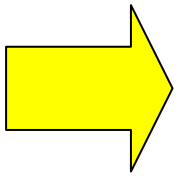
イングレス・フィルタリング

ルータがパケットをフォワードする際

- 送信元アドレスを確認
- ネットワークの構造に対して、送信元アドレスが正しくない場合、パケットを破棄

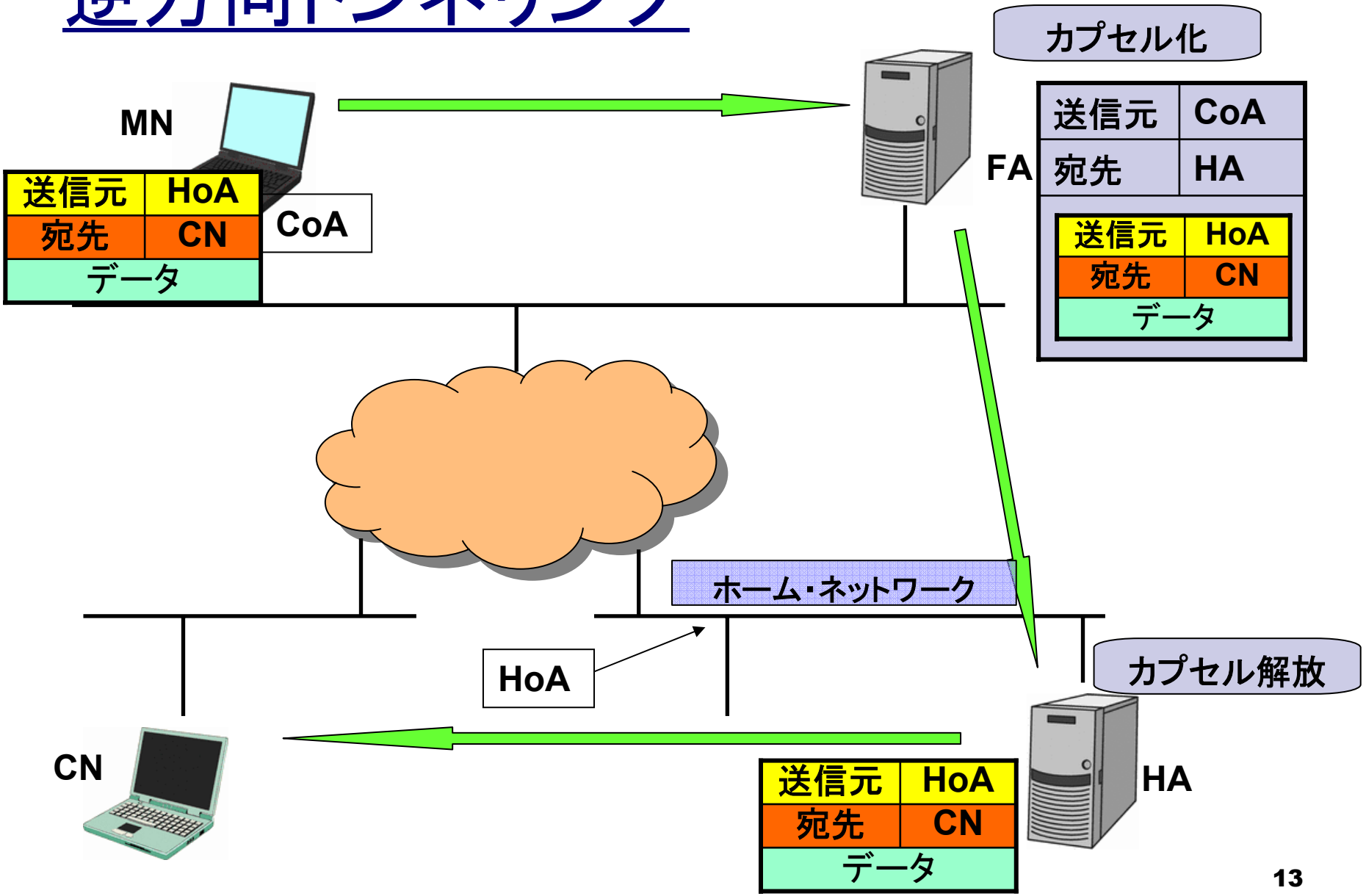
自組織内からの攻撃を出さない

MNからのパケットの送信元は「HoA」
ネットワーク・トポロジー的に正しくない



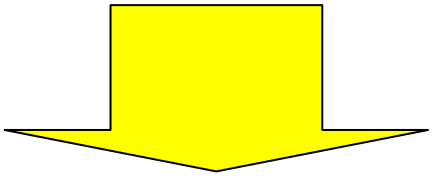
モバイルIPのパケットはイングレス・フィルタリングを通過できない

逆方向トンネリング


カプセル化
MN
送信元
HoA
宛先
CN
データ
CoA
FA
送信元
CoA
宛先
HA
送信元
HoA
宛先
CN
データ
ホーム・ネットワーク
HoA
カプセル解放
CN
HA
送信元
HoA
宛先
CN
データ

逆方向トンネリング

- カプセル化を行い、FAからHAへ向かうパケットの送信元アドレスは「CoA」
- カプセル解放を行い、HAからCN宛パケットの送信元アドレスは「HoA」



ネットワーク・トポロジー的に正しいパケット

イングレス・フィルタリングと共存可能

Mobile IPv4の特徴

- 利点
  - 既存のIPv4ネットワークへ影響を与えないように設計されている。
  - Mobile IPv4プロトコルを理解しないノードも、Mobile IPv4の移動ノードと通信可能。

- 不利な点
  - HAを経由するため、経路の冗長、通信の遅延。

Mobile IPv6

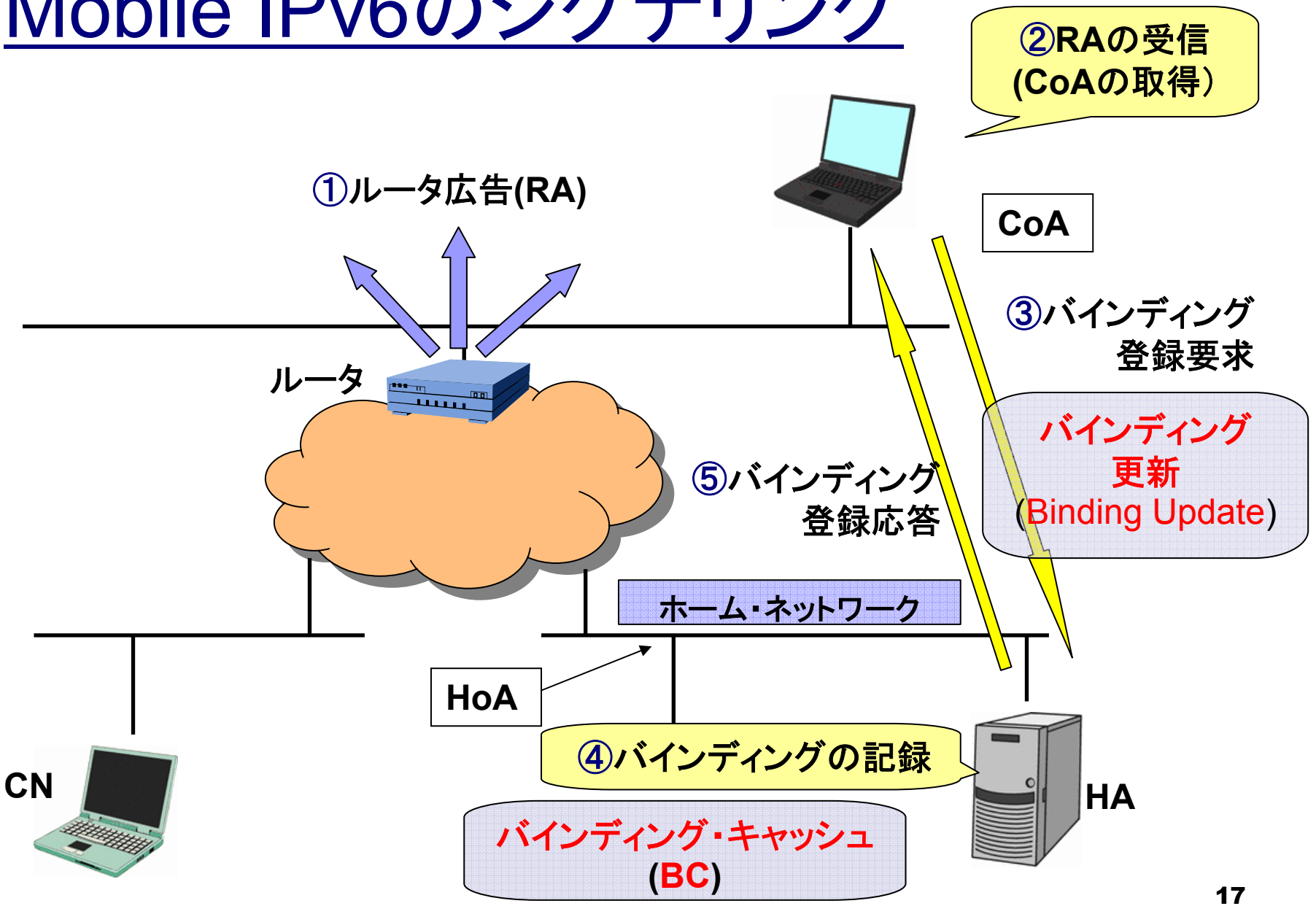
- Mobile IPv4からの変更点
  - FA（訪問先エージェント）の廃止

    IPアドレス数を節約する必要がない。
    IPv6ルータのもつ機能で代用可能。
  - 送信元アドレスがHoAではなくCoAへ変更

    イングレス・フィルタリングの重要性が高まり、
    送信元アドレス詐称攻撃と誤認されないため。
  - 経路最適化の基本仕様への導入

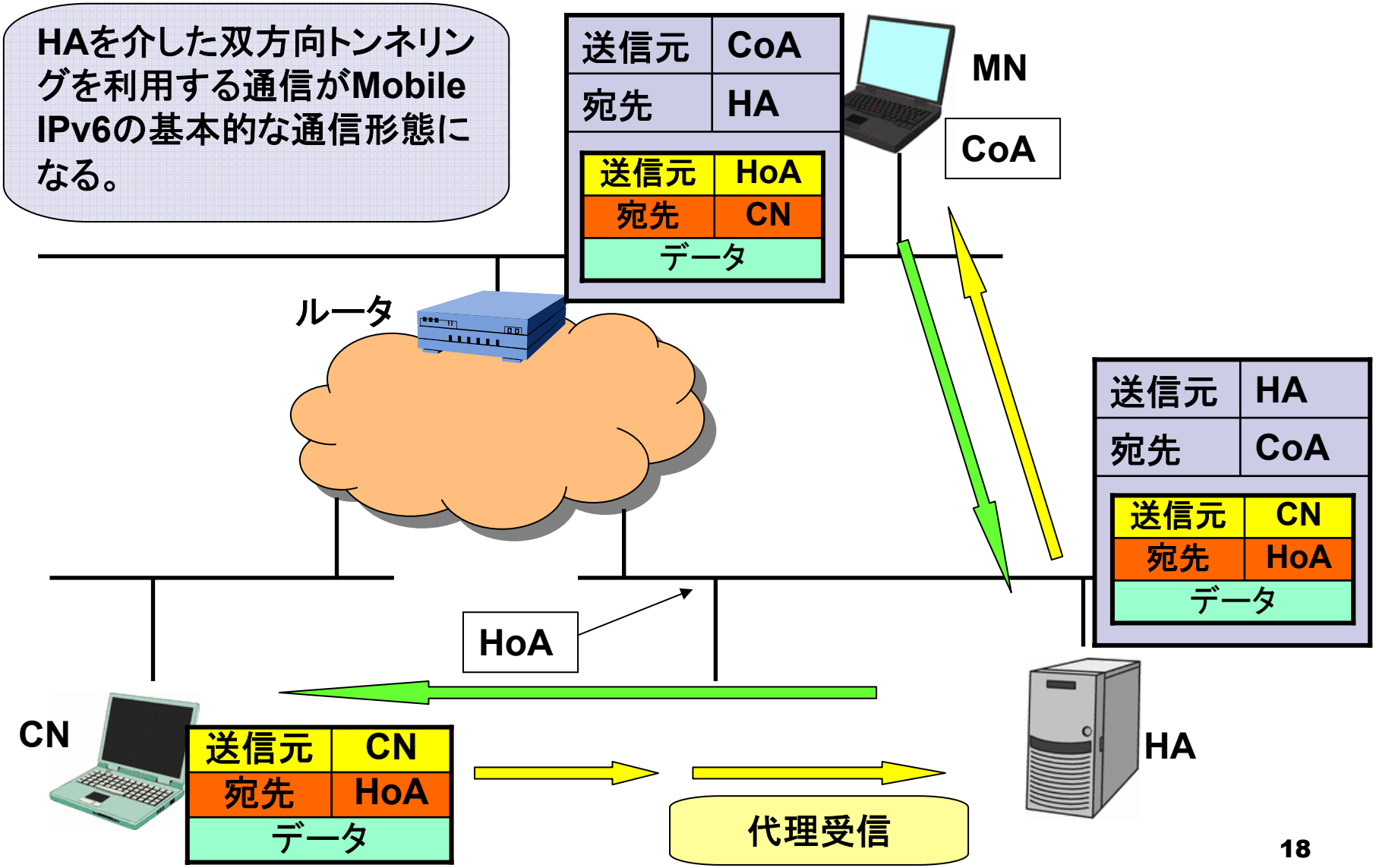
    遅延増大の問題等を避けるため。

Mobile IPv6のシグナリング



Mobile IPv6のパケット交換

HAを介した双方向トンネリングを利用する通信がMobile IPv6の基本的な通信形態になる。



HAを介さない通信

- バインディング・キャッシュ（BC）はCNが持っても良い。
- MNは、CNに対してバインディング更新を送信することが出来る。

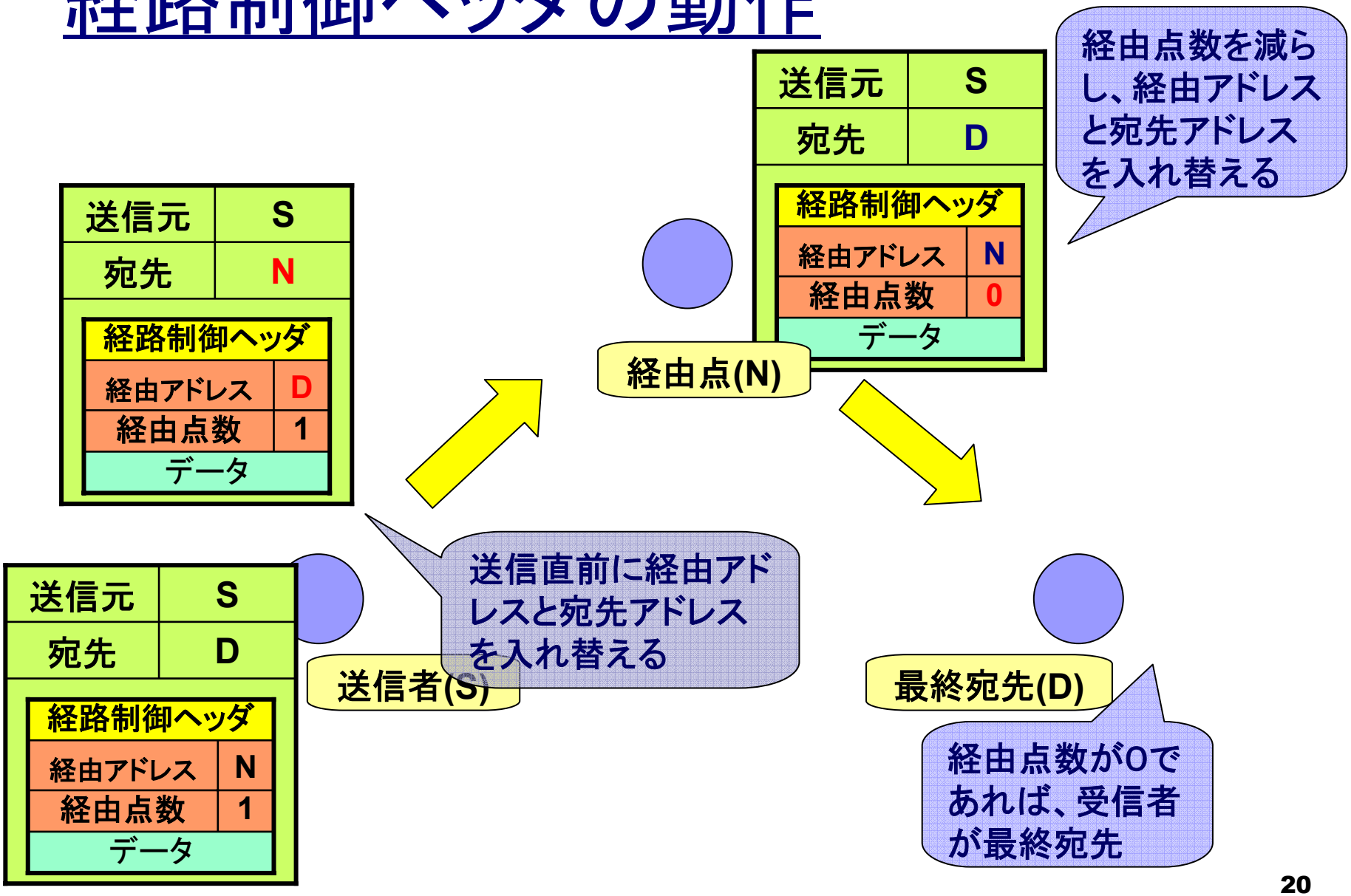
CNがBCを持っている場合

経路制御ヘッダ(Routing Header)を利用することで、HAを介さない通信が可能。

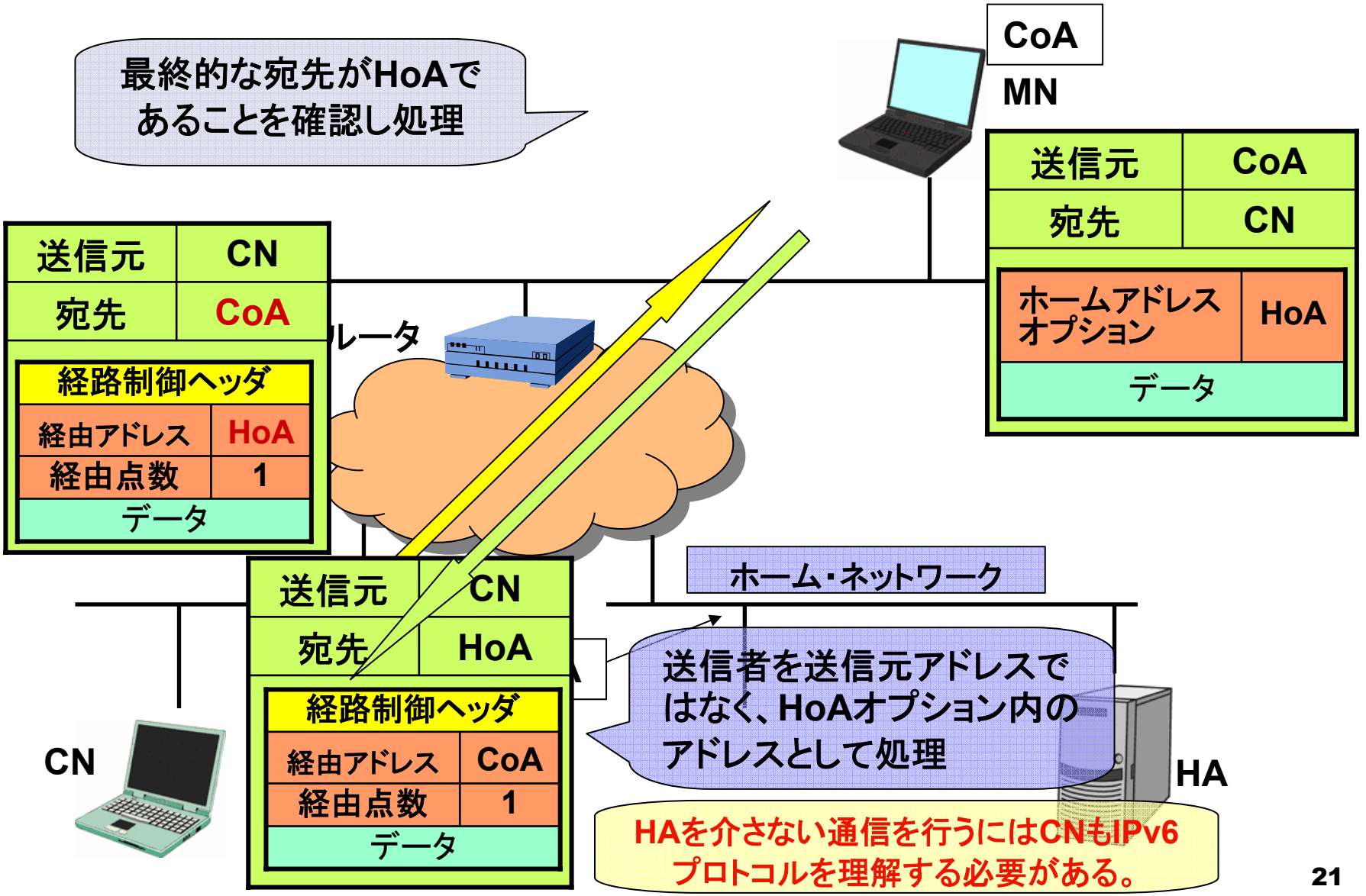
経路制御ヘッダ

途中で経由するノードを指定するIPv6の拡張ヘッダ。

経路制御ヘッダの動作

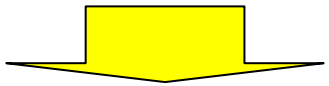

送信元 S
宛先 N
経路制御ヘッダ
経由アドレス D
経由点数 1
データ
送信元 S
宛先 D
経路制御ヘッダ
経由アドレス N
経由点数 0
データ
経由点数を減らし、経由アドレスと宛先アドレスを入れ替える
経由点(N)
送信元 S
宛先 D
経路制御ヘッダ
経由アドレス N
経由点数 1
データ
送信直前に経由アドレスと宛先アドレスを入れ替える
送信者(S)
最終宛先(D)
経由点数が0であれば、受信者が最終宛先

経路制御ヘッダを用いる通信



バインディング認証の問題点

送信されたバインディングを基に送信、転送を行う。



バインディングが正しい送信元からのものか、認証が必要。

- HAにバインディングを登録する場合
  秘密鍵を共有し、IPSecを利用する。
    モバイルIPv4では、HAとMNは秘密鍵を事前に共有しておくことを前提としている。

バインディング認証の問題点

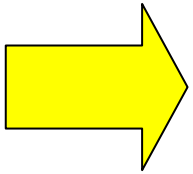
- CNにバインディングを登録する場合

  MNは通信相手(CN)を予測できない

  事前に秘密鍵の共有が不可能

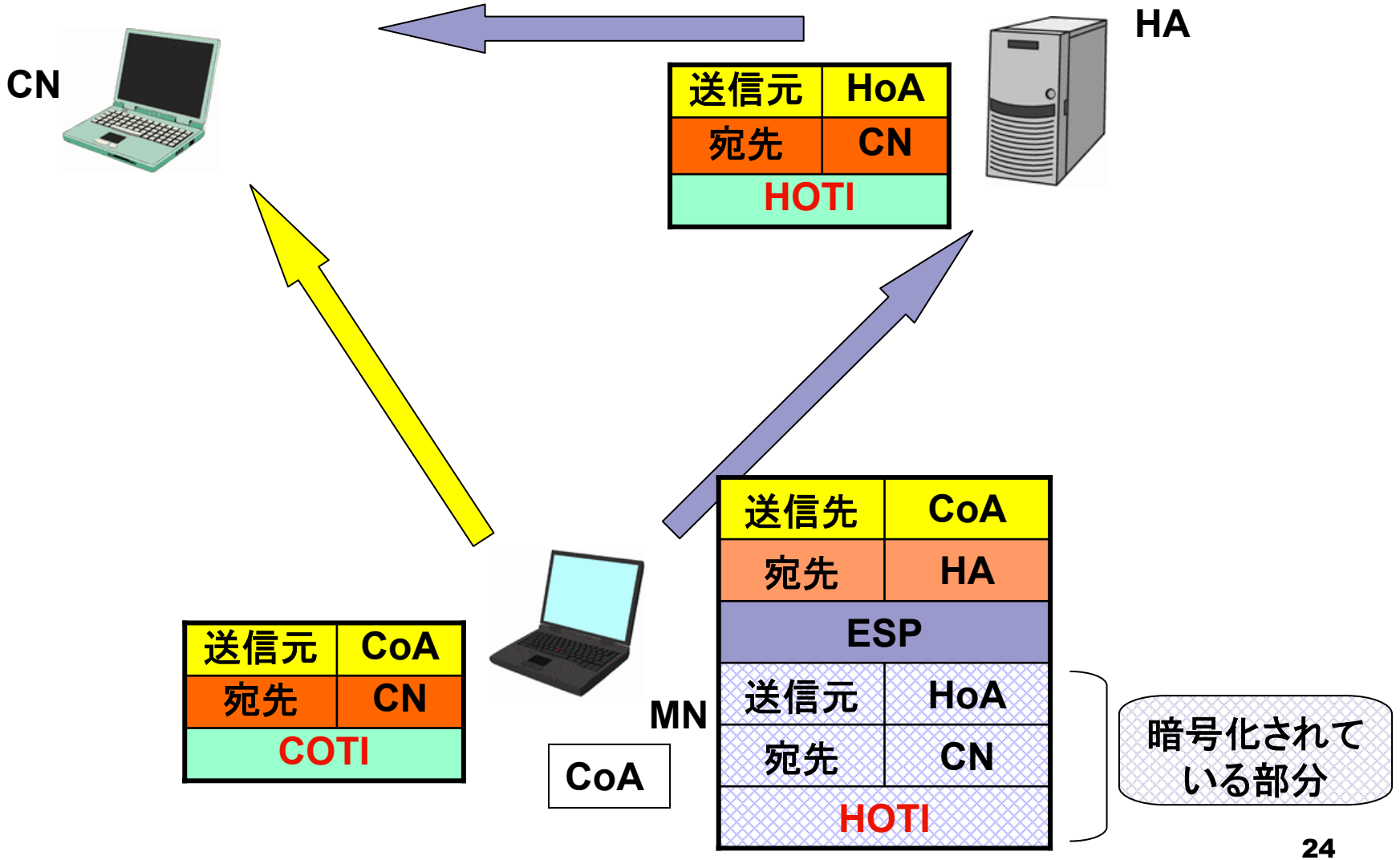
  現在のインターネットには安全に公開鍵を交換する基盤が存在しない

  IKEを利用した鍵交換は期待できない

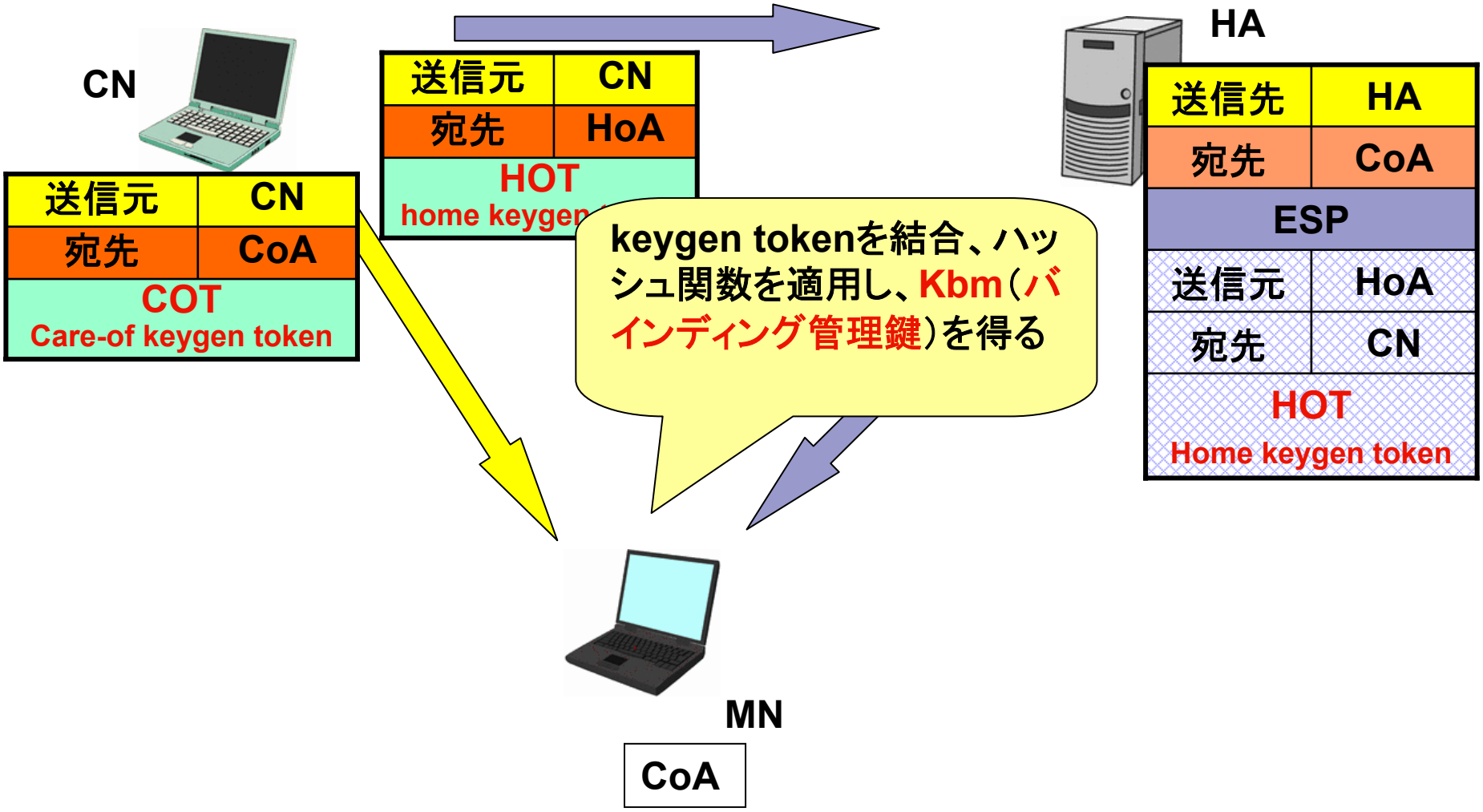


RR(Return Routability)を導入

RR (Return Routability)の動作



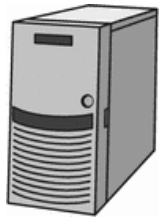
RR (Return Routability)の動作



RR (Return Routability)の動作

CN

HA



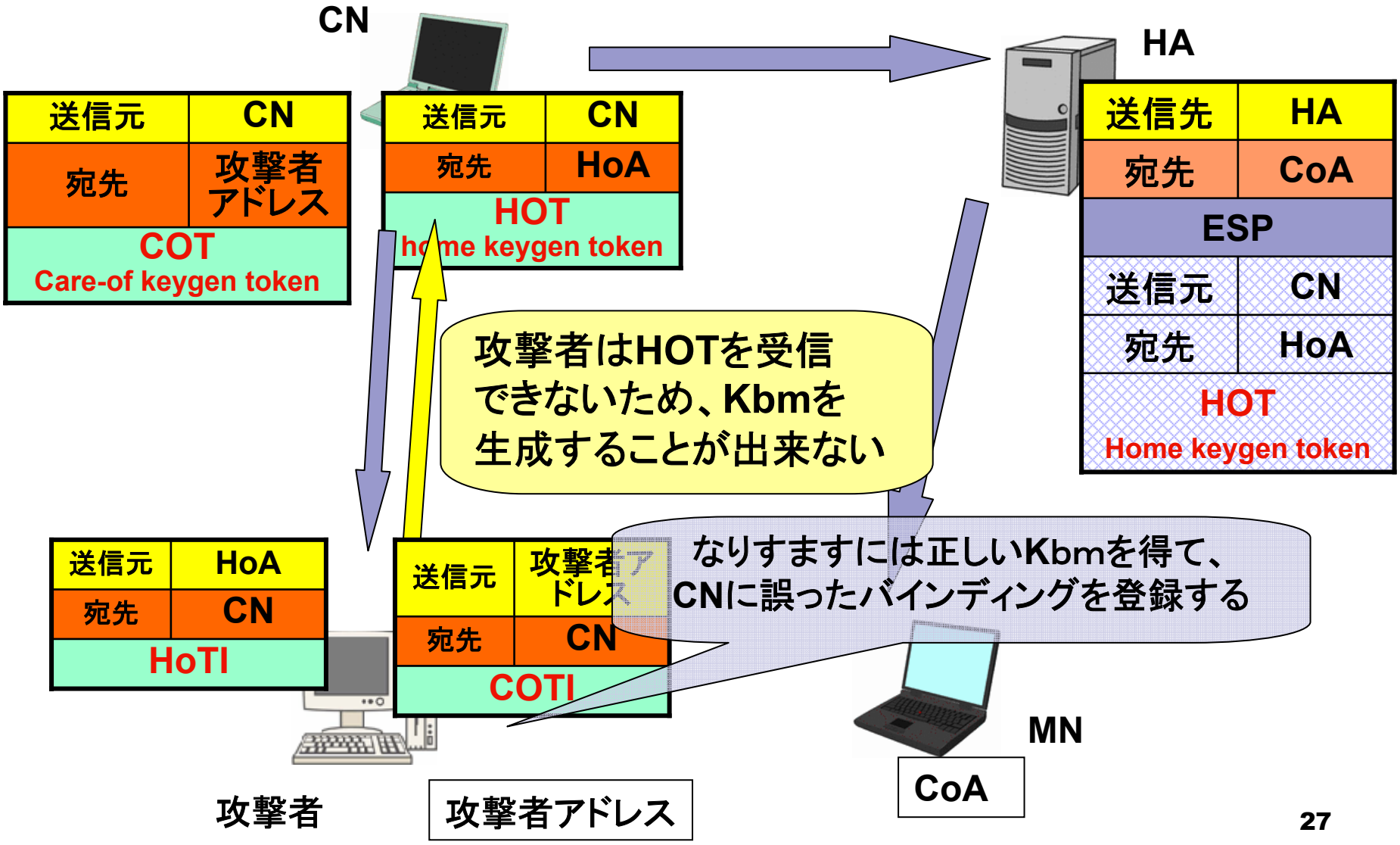
CNが持っている秘密鍵から、このKbmを再計算できるので、CNは正しく署名を検証できる。

MN

CoA

送信元	CoA
宛先	CN
ホームアドレス・オプション HoA	
Kbmを用いた署名を付与したバインディング更新メッセージ	

RR ― 攻撃側の視点 ―


CN
HA
送信元 CN
宛先 攻撃者アドレス
COT
Care-of keygen token
送信元 CN
宛先 HoA
HOT
home keygen token
送信先 HA
宛先 CoA
ESP
送信元 CN
宛先 HoA
HOT
Home keygen token
攻撃者はHOTを受信できないため、Kbmを生成することが出来ない
なりすますには正しいKbmを得て、CNに誤ったバインディングを登録する
送信元 HoA
宛先 CN
HoTI
送信元 攻撃者アドレス
宛先 CN
COTI
MN
CoA
攻撃者
攻撃者アドレス

RR (Return Routability)の効果

- インターネット上の無制限ななりすましからの防衛は可能
- 安全な公開鍵を交換する基盤であるPKI(公開鍵基盤)などの前提が必要ないので導入が非常に容易

モバイルIPの今後

- セキュリティ問題

  基本プロトコルでは、HAとの秘密鍵を共有することが前提となっているが、よりスケーラブルなセキュリティプロトコルの導入に関して議論が行われている。

- 移動ノードの自動設定

  現在の基本仕様では、様々な情報を設定しておかなければならない。設定や、運用コストを引き上げるため、HAおよびHoAの自動割り当て方式が議論されている。

モバイルIPの今後

- ヘッダの圧縮

  HAとの間のカプセル化処理、経路制御ヘッダやホームアドレス・オプションなど、ヘッダ長の大きい部分がある。効率的なヘッダ圧縮を行うプロトコルが期待される。

- モバイルIPv6の拡張

  基本仕様が決まったばかりであるため、拡張についてはこれから議論されると思われる。モバイルIPv4の議論が応用できる部分も多いため、これらの議論は早く進むと予想される。

おわり