Mobile IP概要

東芝 研究開発センター
通信プラットホームラボラトリー
井上 淳

inoue@isl.rdc.toshiba.co.jp

Agenda

- Mobile IPの概要
  - IETF Mobile IP WG
  - Mobile IP protocol specification(RFC2002～2004)
  - Other topics
- Mobile IP の今後の方向性（普及に向けて）
  - **次世代移動通信に向けた拡張**(AAA/DIAMETER)
  - **プロトコルの拡張例**
- Mobile IP の実装・製品、関連情報
  - **東芝の取り組み**（NCG, **東芝版**Mobile Node）
  - **接続試験と実装一覧**
  - **参考文献**

Mobile IPとは？

- IETF Mobile IP WGで議論、規定されている Internet上で、ホスト移動性(mobility)を透過的にサポートするプロトコル
  (→See http://www.ietf.org/html.charters/mobileip-charter.html)
- サブネット間のroamingをサポート
  - **移動しても同一のネットワーク識別子（IPアドレス～ホームアドレス）を使用できる**
  - **移動してもセッションを保持して通信を継続できる**（Mobility, NOT Nomadicity）
- その他、認証、経路制御、セキュリティ、管理など様々なトピックを扱っている

Mobile IP関連RFC

- IP in IP Tunneling (RFC1853)
- IP Mobility Support (RFC2002)
- IP Encapsulation within IP (RFC2003)
- Minimal Encapsulation within IP (RFC2004)
- Applicability Statement for IP Mobility Support(RFC2005)
- The Definitions of Managed Objects for IP Mobility Support using SMIv2 (RFC2006)
- Mobile IPv4 configuration option for PPP IPCP(RFC2290)
- Reverse Tunneling for Mobile IP (RFC 2344)
- Sun's SKIP Firewall Traversal for Mobile IP (RFC 2356)

Mobile IP関連Draft(99年10月現在)

- **Route Optimization in Mobile IP**
- **Mobility Support in IPv6**
- **Mobile IP Regionalized Tunnel Management**
- **Mobile IP Challenge/Response Extensions**
- **Mobile IP Network Access Identifier Extension**
- **Requirements on Mobile IP from a Cellular Perspective**
- **IP micro-mobility support using HAWAII**
- **Paging support for IP mobility using HAWAII**
- **Mobile IP Vendor/Organization-Specific Extensions**
- **IP Mobility Support for IPv4, revised**
- **Mobile IP Authentication, Authorization, and Accounting Requirements**

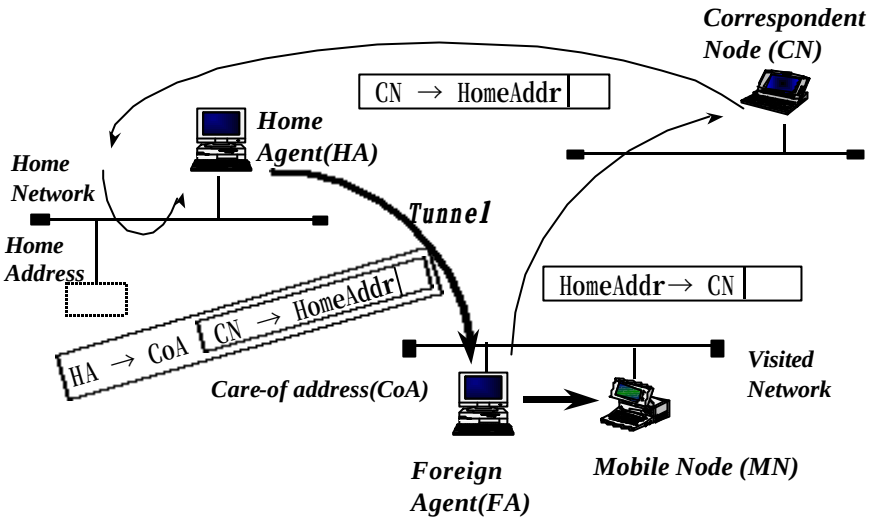
（その他もろもろ）

- **DIAMETER Mobile IP Extension**

Mobile IPドキュメントをどう読むか？

- RFC2002, 2003, (2004)は（一応）必須
  - RFC2005は相互接続の基準、RFC2006はMIB拡張のみ
- ドラフトは息の長いものは要フォロー
  - 現在は、Mobile IPv6, DIAMETER関連
  - あとは各人の興味に従って読めば良い
  - 但し1回の発表で消えるもの、標準化に遠い単なる研究発表もあるので、要チェック
  - 最近はv4プロトコルは適用事例ばっかり
  - 関連WG:IPNG,IPSEC,PPPEXT,SVRLOC,AAAあたり？
- 後はML(mobile-ip@standards.nortelnetworks.com)に参加する

Mobile IPプロトコルの概観



Mobile IPプロトコルの概観

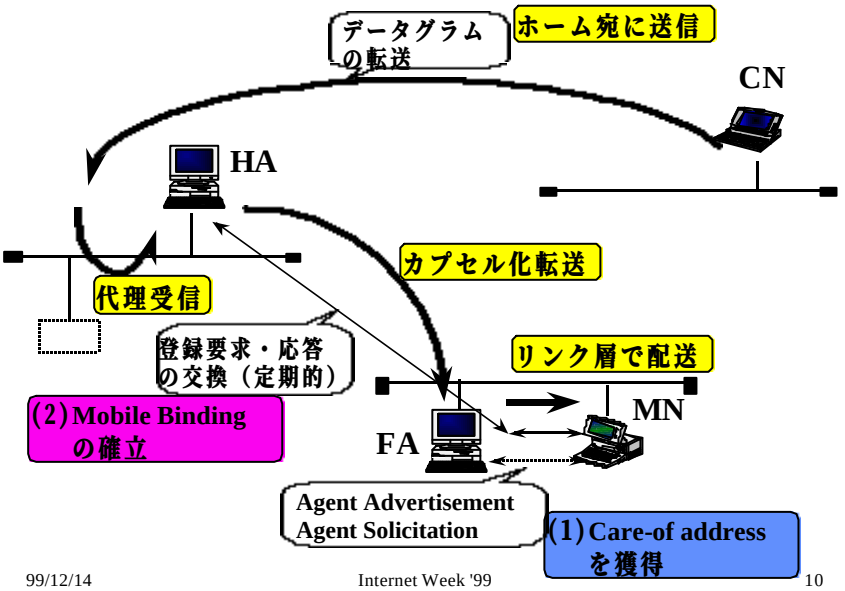
- 構成要素
  - **MN(Mobile Node)とCN(Correspondent Node)が通信する**
  - **HA(Home Agent)：MNのホームネットにあって、現在位置を管理し、データを配送するルータ**
  - **FA(Foreign Agent)：MNの訪問先にあって、MNに現在位置を通知し、MN宛データを仲介するルータ**
- 移動サポートの方法
  - **MNが移動してもNetwork ID(Home address)は不変（常に同一アドレスでアクセス）**
  - **MNは移動すると、現在地を示すCare-of addressと関連づけられる**
  - **HA,FAがCare-of addressの登録、Home address宛データのMNへのカプセル化転送を行う**

2つの動作モード(FAの有無)

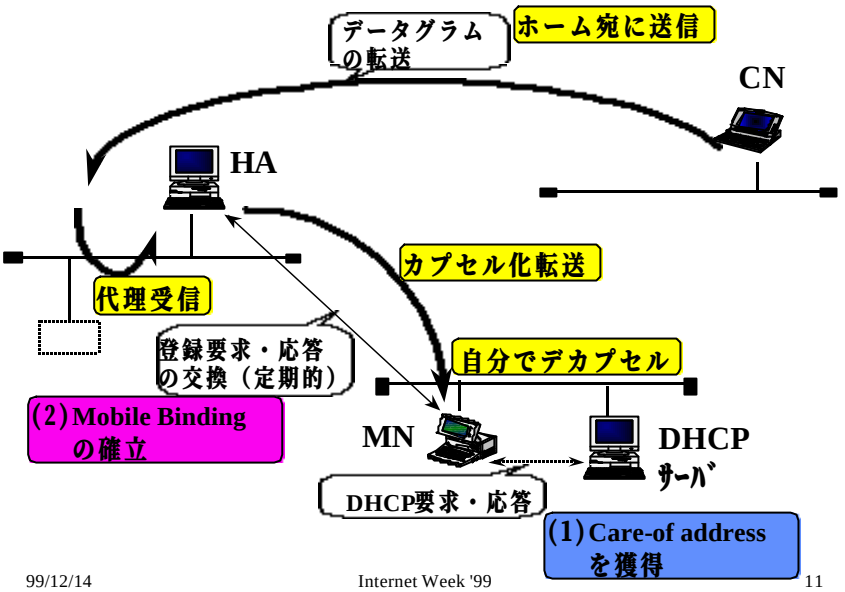
◆FAモード
- 訪問ネットにForeign Agentが存在する
- Care-of AddressはFAのIPアドレス(MN用にアドレスを割り当てる必要がない)
- FAが、HA発のデータをデカプセルし、リンク層アドレスでMNに配送する。

◆Co-located Care-of Addressモード
- 訪問ネットにForeign Agentが存在せずMNがFAを兼ねる
- MNの現在位置検出がad hocな方法になってしまう
- Care-of AddressはMN自身がDHCPなどで獲得する
- 移動先の制約はないが、訪問するMN毎に１つアドレスを浪費する

FAモードの動作



Co-located Care-of addressモードの動作



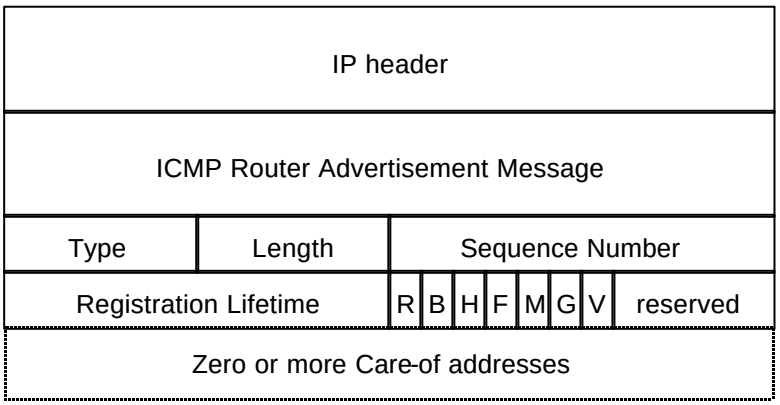
RFC2002の構成

1. Introduction
2. Agent Discovery →MNの現在位置の検出
   - **2.1. Agent Advertisement , 2.2. Agent Solicitation**
3. Registration →MNの現在位置の安全な登録
   - **3.1. Registration Overview ,3.2. Authentication, 3.3. Registration Request,**
   - **3.4. Registration Reply, 3.5. Registration Extensions**
4. Routing Considerations →MNへのデータ転送
   - **4.1. Encapsulation Types , 4.2. Unicast Datagram Routing,**
   - **4.3. Broadcast Datagrams , 4.4. Multicast Datagram Routing,**
   - **4.5. Mobile Routers, 4.6. ARP, Proxy ARP, and Gratuitous ARP**
5. Security Considerations
6. Acknowledgments

Agent Advertisement/Solicitation

- FAモードで、訪問先でのCare-of addressを獲得
- MNがホームにいるか、移動中かを判定
  - →**一定時間**Agent Advertisement**を聞いて、受信できなければ**Solicitation**で問い合わせ**
- Agent Advertisement →ICMP router advertisementの拡張
- Agent Solicitation→ICMP router solicitationと同じ(TTL=1)

Agent Advertisementのパケット形式



R:Registration Required B:Busy
H:Home Agent F:Foreign Agent
M:Minimal Encapsulation G:GRE Encapsulation
V:Van Jacobson header compression

Mobile IPの登録 (Registration)

Request packet

IP header	UDP header	Registration request	Mobile-Home Auth. Ext.	Mobile-Foreign Auth. Ext.

MN→FA→HAに送信

Reply packet

IP header	UDP header	Registration reply	Mobile-Home Auth. Ext.	Mobile-Foreign Auth. Ext.

HA→FA→MNに返信

Authentication Extention

Type	Length	SPI
		Authenticator

Registrationのパケット形式

Type	Flags	Lifetime
Home Address		
Home Agent		
Care-of Address		
Identification		
Extensions		

<登録要求>

Type	Code	Lifetime
Home Address		
Home Agent		
Care-of Address		
Identification		
Extensions		

<登録応答>

Code:
0,1=OK
64～88=NG(FA)
128～=NG(HA)

[Flags]

S	B	D	M	G	C	rsv

S:Simultaneous Binding
B:Broadcast Datagrams
D:Decapsulation by Mobile Node
M:Minimal Encapsulation
G:GRE Encapsulation
V:V.Jacobson Header Compression

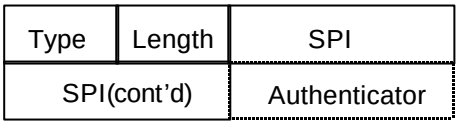
RegistrationのExtension

◆MD5でホストを認証する

–**Mobile-Home Authentication Extension (必須)**

– **Mobile-Foreign Authentication Extension**

– **Foreign-Home Authentication Extension**



Type:32(Mobile-Home)
33(Mobile-Foreign)
34(Foreign-Home)

– **最近、この他のextension(NAI, challenge-response)も提案されている**

Proxy ARP, Gratuitous ARP

◆Home Agentの代理受信機構を制御

◆Proxy ARP

– **あるノードが他のノードの代理でARP応答すること**

– **MN留守中にHAが代理でパケットを受信するために使う**

◆Gratuitous ARP

– **あるノードが、他のノード群の特定のARPキャッシュエントリをクリアするよう要求**

– **MNがホームを離れた場合、HAが発行**

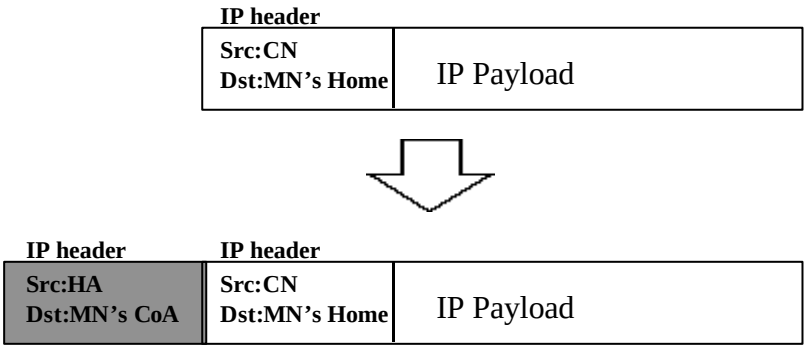
– **MNがホームに戻った場合、MNが発行**

（詳細はRFC2002 section4.6）

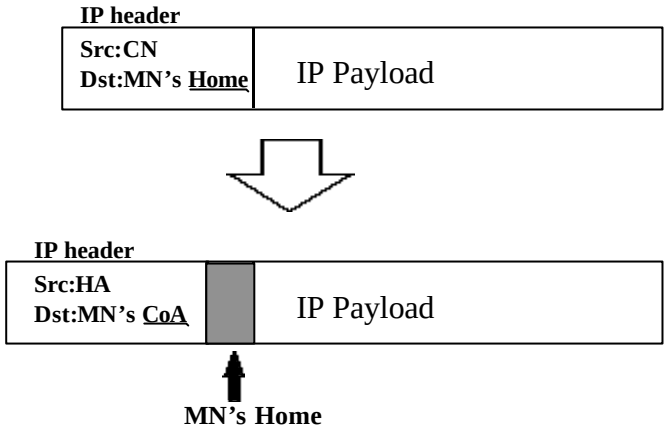
DatagramのMN宛転送

- ◆HAはカプセル化を行ってCare-of addr宛に転送
- ◆カプセル化方式
  - – IP-in-IP (RFC2003)
  - – Minimal Encapsulation (RFC2004)
  - – GRE Encapsulation (RFC1701)
- ◆FAモードでは、FAがカプセル化を解き、ホームアドレス宛パケットをリンク層でMNに転送
- ◆Co-located CoAでは、MN自身がカプセル化を解き、ホームアドレス宛パケットを抽出

IP-in-IPカプセル化 (RFC2003)



Minimal Encapsulation (RFC2004)



Other MobileIP topics

- 経路が冗長である
  - **経路最適化**
  - End-to-End**完結型**Mobility support（**後述**）
- セキュリティの課題
  - MN**発パケットのソースアドレス問題**（address spoofing**と思われちゃう問題**）
  - **ファイアウォール透過モデル**
- Mobile IPv6

経路最適化(Route Optimization)

- Binding Cache
  - MNの現在のCare-of Addressをキャッシュする
  - FA,HAだけでなく、CNにも持たせる
- MNが移動したらBinding UpdateパケットをUDPで送信

  MN→CN、新FA→旧FA

  HA→CN（CNからの要求に応じて）
- 既存のCNへのインパクトが問題
- V6ではデフォルトでrouting optionにより最適化されるので、これに期待する？

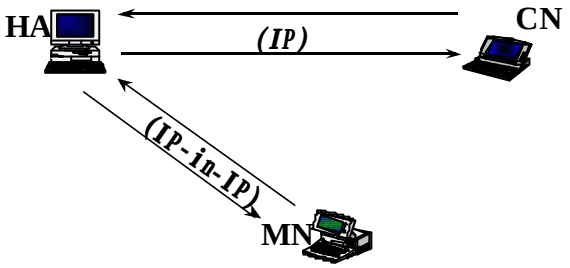
Mobile IPにおけるセキュリティの課題

- ソースアドレス偽造のパケットフィルタ対応
  - MN発パケットが組織外から来ると、内部アドレスを騙って侵入するものと同様に見える

  →パケットフィルタで通過を禁止される
- IPレベルのセキュリティ(IPSEC)との協調
  - ノード間のセキュリティアソシエーション(SA)
  - 認証ヘッダ(AH)、暗号化ペイロード(ESP)
- ファイアウォール透過の問題
  - 訪問先～外(インターネット)
  - インターネット～組織内

Reverse Tunneling

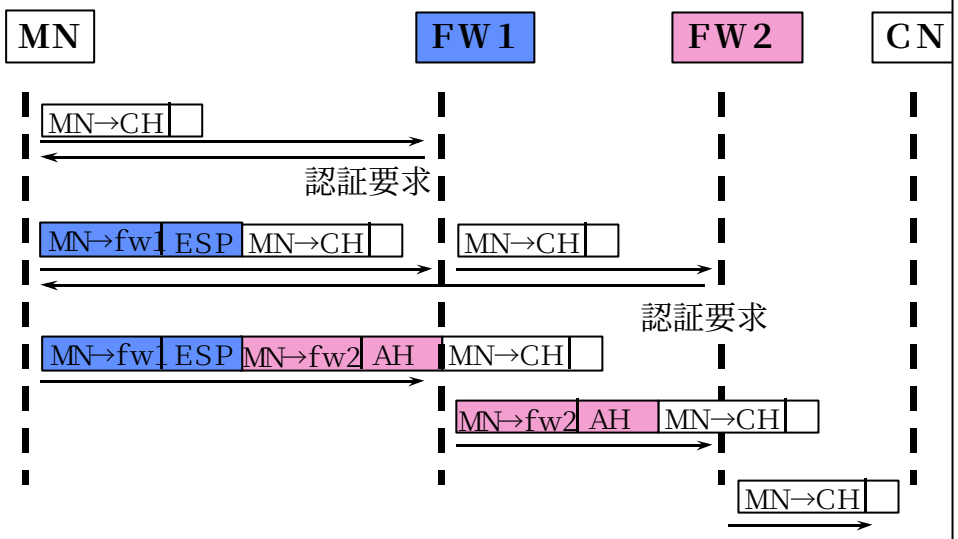
- ソースアドレス偽造のフィルタ対応
  - MN発パケットをtunnelingでHA経由でCNに転送
  - MN発パケットの外側ソースはCare-of Address(トポロジー的に正しい位置）になる
  - 但し、経路がさらに冗長になってしまう



IPSECとの協調

- RFC2356:Sun’s SKIP firewall traversal for Mobile IP
  - IPSECで認証を行ってファイアウォール透過を行うモデル
  - 外向き内向き双方を規定、多重ファイアウォールも想定
- 東芝のISS’97論文（井上、石山、福本、津田）
  - End-to-End SAで内容保証
  - Link-by-link SAで透過の認証
  - IPSECヘッダ多重化のオーバーヘッドを削減

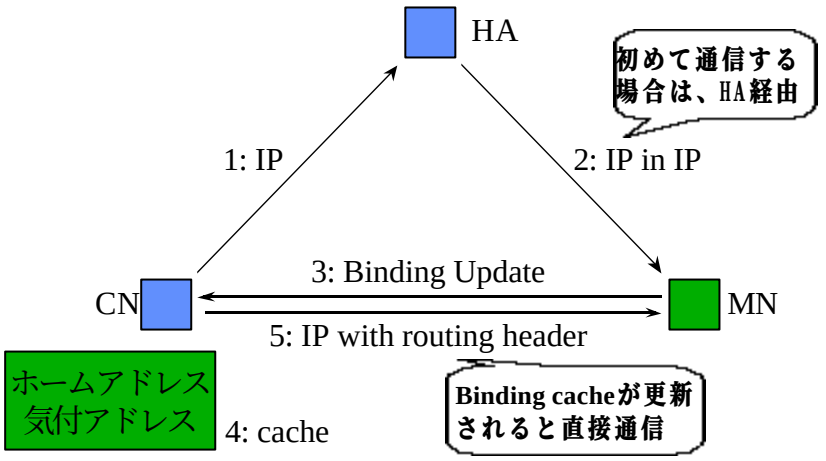
IPSECによるファイアウォール透過



Mobile IPv6

- FAなし（Co-located CoAのみ）
  - Care-of Addressはstateful/statelessアドレス自動構成で獲得
- IPv6 Destination Optionを使用
  - Care-of Addressへの転送(Routing headerを使用）
  - Binding Updateを行う（経路最適化がデフォルト）
- その他の拡張
  - anycastを使ったDynamic Home Agent Discovery
- なかなか、Last call, RFC化に至らない
  - 実装が少ない (KAMEなどの普及に期待）
  - 他のWG(IPNG, IPSEC)との連絡不徹底

Mobile IPv6の通信経路



最近の話題

◆IMT-2000、セルラ適用を狙った提案
- •Cellular IP (コロンビア大)
- •IMT-2000 requirement（エリクソン）

◆AAA(Authentication Authorization and Accounting)　サーバとの連携
- •認証に関するスケール性を改善
- •課金の枠組を導入し、ISPにとっての魅力を高める
- •AAA-WG, 3GPP2などでも議論中（Draft: cdma2000 Wireless Data Requirement for AAA)

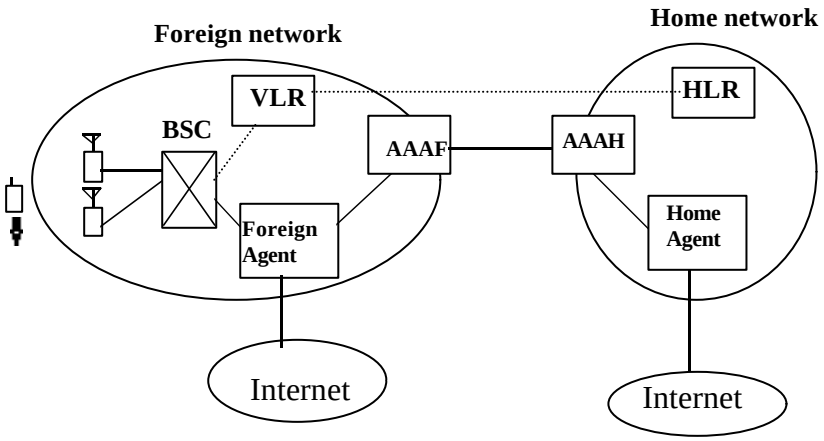
AAAって何？

- Authentication/Authorization/Accountingの略
  - 結構、盛況なIETFのWGだが……
  - ５つのsub-WGから成る

  (1) Authentication, (2) Authorization,

  (3) Accounting, (4) Mobile IP, (5) E-commerce
- なぜMobile IP？
  - 米国版IMT2000 by ANSI(TIA:Telecommunication Industry Association aka 3GPP2)で、これを用いた認証、課金を検討しているから
  - RADIUSまたはDIAMETER(後述)を使うことを検討中

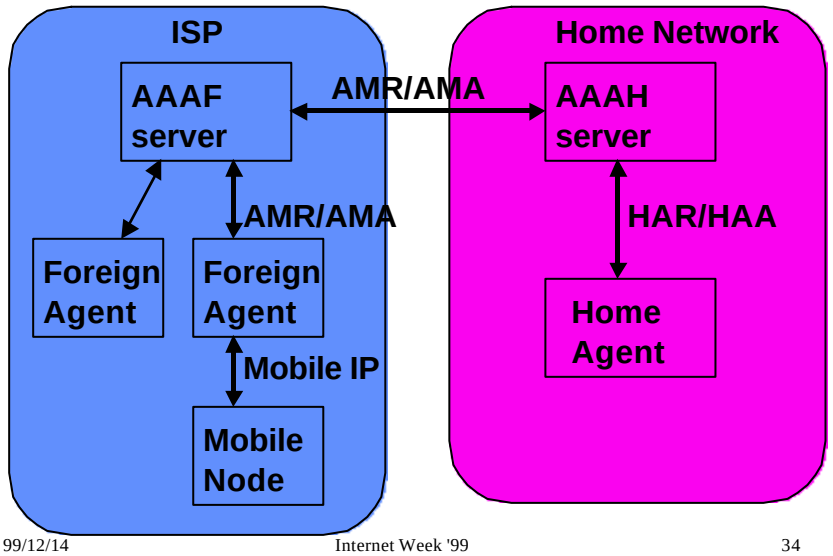
ANSI Mobile IP model for IMT2000



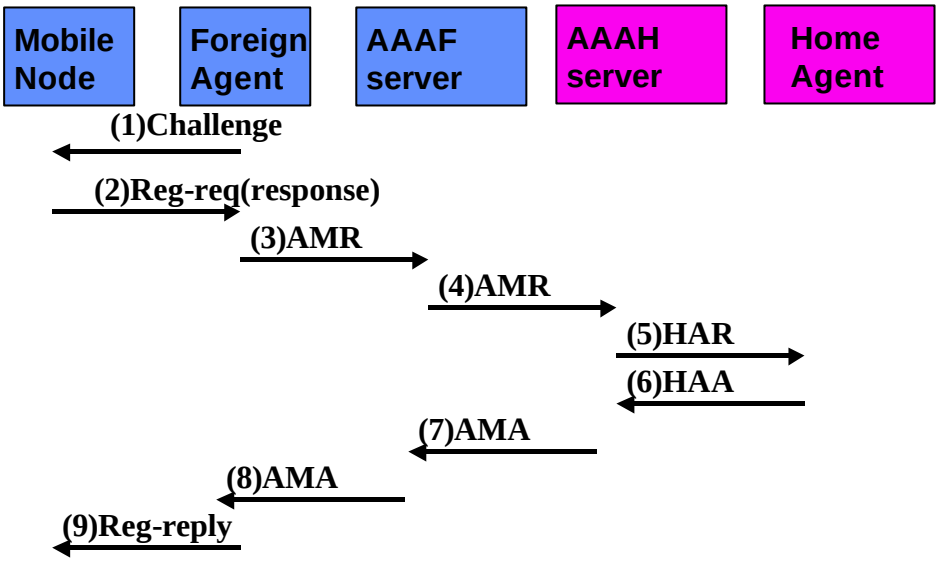
DIAMETER Mobile IP extension

- 既存のMobile IPの問題
  - エージェント間で個別に認証extentionのSAを保持するのでスケール性に問題
  - 課金が欠けているのでISPにとって魅力が薄い
- 本extensionで何ができるか・嬉しいか？
  - cross-domain authenticationとauthorization
  - 大規模ISPでもスケールするSAの鍵配布機構
  - 移動ノードへのホームアドレス動的割り当て
  - ホームエージェントの動的割り当て
  - 課金情報はAccounting Extensionで既定
  - 移動ノードをIPアドレスだけでなく、NAI(Network Access Identifier)で識別できるようになる

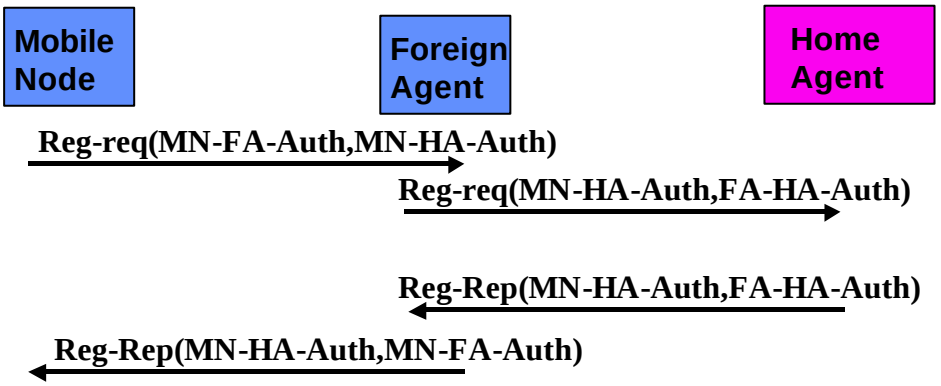
Inter-domain Mobile IP network



AAAメッセージの流れ



SA確立後のMIP登録



Mobile IPの効用とは？

◆可搬性(Nomadicity)だけでない、移動透過性(Mobility)をサポート
- •移動によるセッション喪失の回避
- •IPアドレスがノード識別子として利用可能

◆しかし、課題も多い
- •三角経路のための耐障害性の低下
- •ホームエージェントの設置が面倒
- •ファイアウォールモデルとの不適合

◆でも事業者は結構暖かい目で見ている。なぜ？
- •米国、欧州：無線事業者のサービス範囲が狭く、お互いがローミングする環境では旨味がある、日本は？

Mobile IPアーキテクチャの問題点

◆全てはHAを介した三角経路に起因する

が、HAはMobile IPの根幹であり、解決は困難

◆移動透過性を提供する新規プロトコルが必要

「End-to-Endで完結したIP層による移動透過性保証の一方式」（石山他、IPSJ DiCoMo研究会'99)

[方針]
- **ノード間通信はEnd-to-Endで完結**
- **セキュリティ保証**
- **既存ノードとの通信が可能**

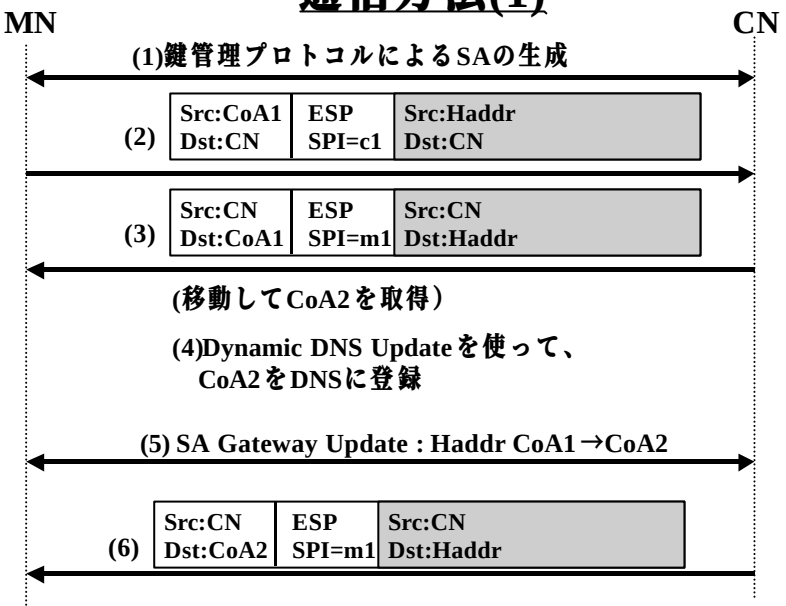
新規Mobility protocol

- ◆IPsec Tunnel Modeを使用
  - – ノード間はEnd-to-End通信
  - – デフォルトでセキュリティをサポート
- ◆不変のアドレス(Haddr)と移動先アドレス(CoA)
- ◆ Tunnel Endpointを動的に変更するプロトコル
  - – SA Gateway Update/ SA Local Update
  - – 移動によるセッション喪失を回避
- ◆DNSにHaddrを示すResource Recordを新規定義
  - – HAAAA/HA
  - – 移動ノード宛発呼をサポート
  - – 既存ノード通信との互換性

通信方法(1)

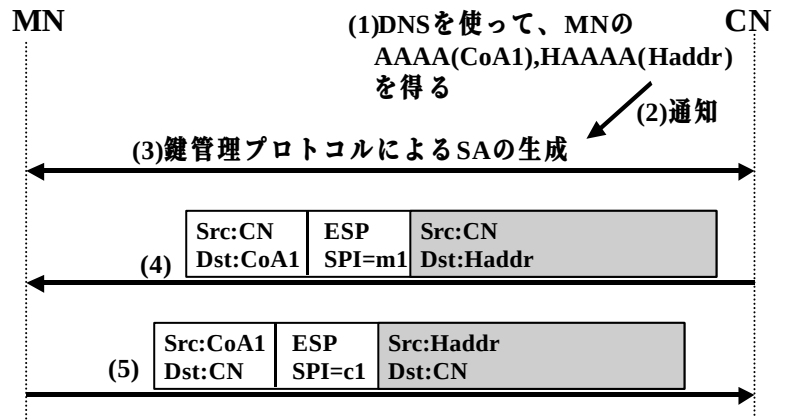
- ◆MNとの通信はIPsec Tunnel Modeを使用
  - – ApplicationはHaddr、IPsec EndpointはCoAを使う
- ◆MNが移動すると、
  - – Dynamic DNS updateで、自分のアドレスレコードをCoAに変更
  - – SA Local updateで自分のSAを変更（destフィールドが以前のCoAのものを現在のCoAに）
  - – SA Gateway updateで、通信相手のSA変更を要求（dest フィールドが自分でない通信相手に対し、以前のCoAを新規CoAに変更する旨、発行）

通信方法(1)



通信方法(2):MNへの発呼

- DNSを使ってAAAA/HAAAAを取得
- AAAAを使ってSAを生成するよう鍵管理プロトコルに通知
- アプリケーションにはHAAAAを通知



従来ノードとの通信

- IPsecが利用できない
  - CoAを使って通信する
- SA Gateway Updateが利用できない
  - IPsec Tunnelで通信が行われる
- HAAAAを利用できない
  - 移動ノードにはCoAが宛先になってパケットが届く

移動透過性は保証されないが、通信は可能

Mobile IPの接続試験

- 過去３回(95年11月、97年4月、99年7月）開催
  - 接続マトリクスを作成
  - 匿名で直後のIETFで報告
- 1, 2回はBase protocol(v4,v6)の確認
  - 参加者はソフトベンダ、大学が中心
  - UNIXベースのスタック実装中心
- 3回はBase protocol + DIAMETER･AAAの確認
  - 参加者はキャリア、機器ベンダが中心
  - 製品レベルの実装

実装例:URL(1)

- **Stanford (Linux):**
  http://mosquitonet/stanford.edu/software/mip.html
- **CMU (FreeBSD):**
  http://monarch.cs.cmu.edu/software.html
- **National Univ. of Singapore (Linux, Windows?):**
  http://mip.ee.nus.edu.sg
- **Portland State univ. (FreeBSD):**
  http://www.cs.pdx.edu/research/SMN/index.html
- **Politehnica univ. of Bucharest (Windows NT):**
  http://mip-nt.aii.pub.ro/
- **Lancaster univ (Linux):**
  http://www.cs-ipv6.lancs.ac.uk/MobileIP
- **IKV++ GmbH (Windows NT):**
  http://www.ikv.de/products/roamin
- **Sun (Solaris, Linux):**
  http://playground.sun.com/pub/mobile-ip

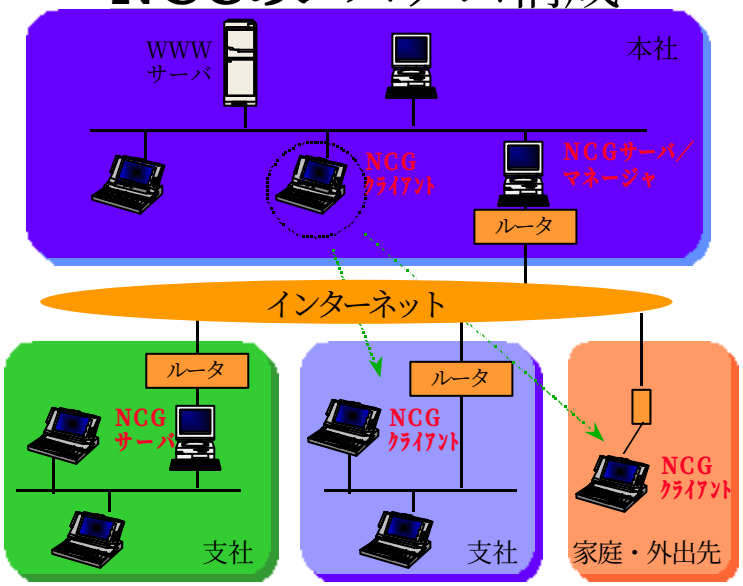
実装例:URL(2)

- **Cisco (IOS):**
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/mobileip.htm
- **Ecutel (Windows):**
  http://www.ecutel.com/viatores.html
- **Telxon (embeded):**
  http://www.telxon.com
- **Toshiba (Solaris, Windows):**
  http://www.toshiba.co.jp/product/nc/ncg
- **Helsinki univ. (Linux):**
  http://www.cs.hut.fi/Research/Dynamics
- **Microsoft (Windows):**
  http://www.research.microsoft.com/msripv6
- **Charles Perkins:**
  http://computer.org/internet/v2n1/perkins.htm
  http://www.svrloc.org/~charliep

東芝の実装

- Network CryptoGate (NCG)
  - **Mobile IPとIPSECを統合した製品**
  - **http://www.toshiba.co.jp/product/nc/ncg**
  - **ソフトウェア・プロダクト・オブ・ザ・イヤー'99受賞**
- Mobile Nodeソフトウェア
  - **Windows 95/98上のMNソフトウェア**
  - **HA/FAは、Ciscoルータ(IOS 12.0T以上)を想定**
  - **サポートプロトコルはMobile IP(MN), DHCP, PPP**
  - **近日発売予定**

NCGのシステム構成



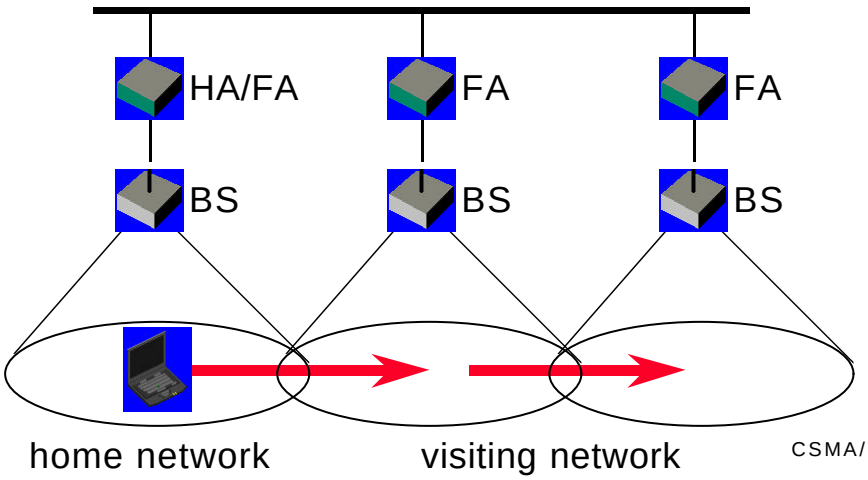
NCGの製品構成

◆NCG Server
- – Solaris workstation/WindowsNT server上で動作
- – 暗号化機能／Mobile-IPホームエジェント機能

◆NCG Client
- – Windows NT/95 PC上で動作
- –暗号化機能／Mobile-IP移動ノード機能
- –ＬＡＮ接続／ダイアルアップ接続サポート

◆NCG Manager
- –NCGのVPN状態、移動状態、鍵情報を管理
- –GUIサポート　（HP OpenView(ｵﾌﾟｼｮﾝ)を使用）

MobileNode適用事例：キャンパス・ネットワーク



参考文献、学会など

- Jim Solomon:Mobile IP -- The Internet Unplugged
  （詳説Mobile IP 寺岡文男、井上淳監訳）
  Prentice Hall社
  MOBILEIP WGの元Chairが動向をまとめたもの。
  よくまとまっている。
- Charles E.Perkins: Mobile IP -- Design Principles and Practices, Addsison Wesley
  RFC2002の編者による。Advanced topicsなども広くカバー
- **情報処理学会：ﾓﾊﾞｲﾙｺﾝﾋﾟｭｰﾃｨﾝｸﾞ研究会**
- **ACM: MobiCom(MC2R)**