

画像情報特論 (11)

- その他の話題 (2)

- モビリティ
- セキュリティ

- 授業のまとめ

2004.07.09

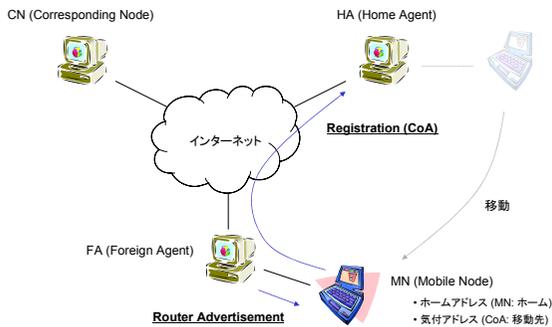
情報ネットワーク専攻 甲藤二郎
E-Mail: katto@waseda.jp

モビリティ

- L3モビリティ: Mobile IP
- L7モビリティ: SIP Mobility

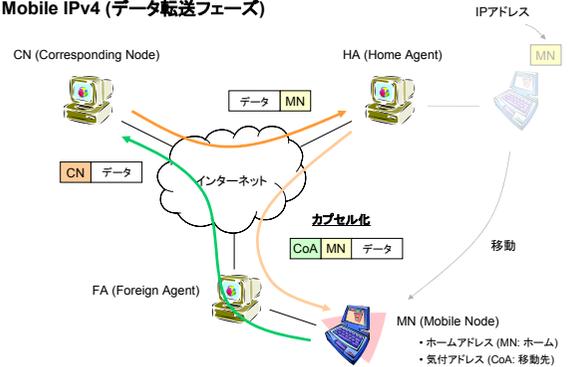
Mobile IP (1)

• Mobile IPv4 (制御フェーズ)



Mobile IP (2)

• Mobile IPv4 (データ転送フェーズ)



Mobile IP (3)

• Mobile IPv4 (定義と手順)

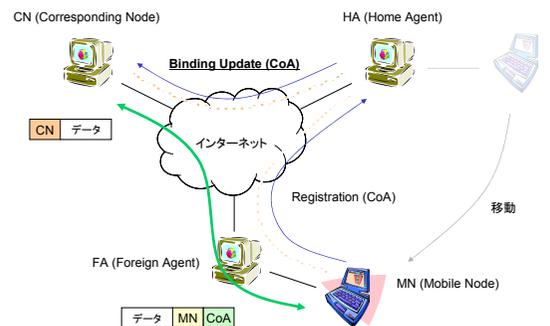
- 定義:
- MN (Mobile Node): 移動端末
 - CoA (Care of Address): 気付アドレス (共存気付と外部気付)
 - HA (Home Agent): 移動元エージェント
 - FA (Foreign Agent): 移動先エージェント
 - CN (Corresponding Node): 通信相手

共存気付アドレスの場合:

- MN が FA から CoA をもらう (**Discovery**: Advertisement, DHCP 等)。
- MN が HA に CoA を登録する (**Registration**)。
- CN からのパケットを HA が MN にカプセル化転送する (**Delivery**)。
- MN は、受信パケットのカプセル化をほどきデータを受信。
- MN は、送信元アドレスは MN のまま、CN に対してパケットを送信。

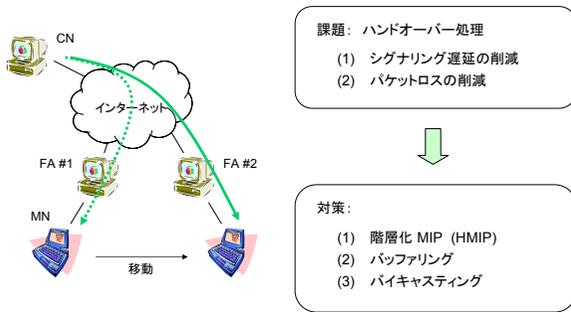
Mobile IP (4)

• Route Optimization (三角経路の回避オプション)



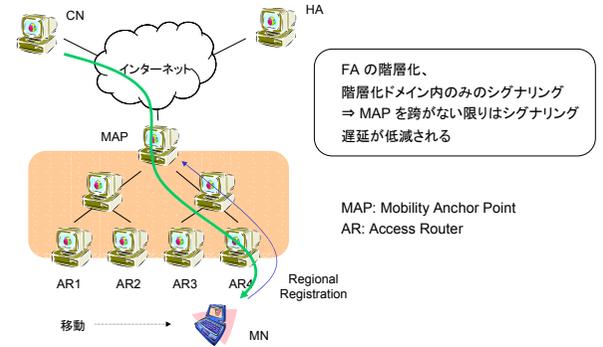
Mobile IP (5)

Fast Handover (1) 概要



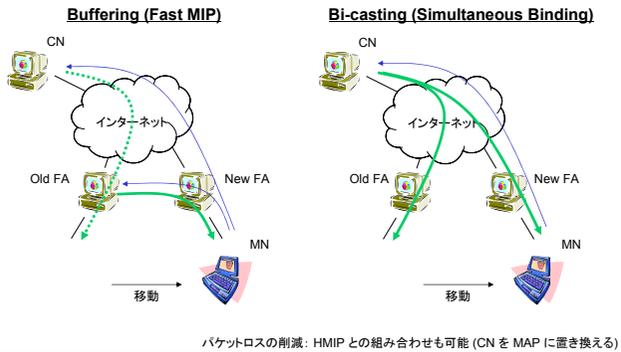
Mobile IP (6)

Fast Handover (2) 階層化 MIP



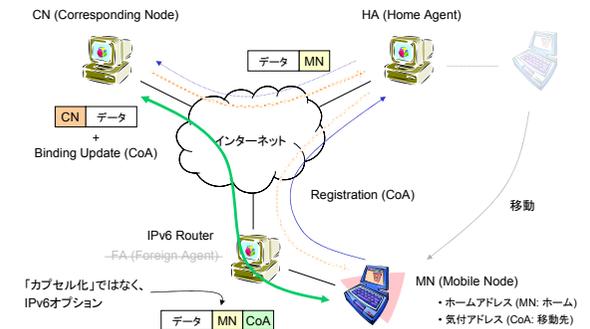
Mobile IP (7)

Fast Handover (3) バッファリングとバイキャストイング



Mobile IP (8)

Mobile IPv6 (データ&制御)



Mobile IP (9)

Mobile IPv6 (定義と手順)

IPv4 との違い:

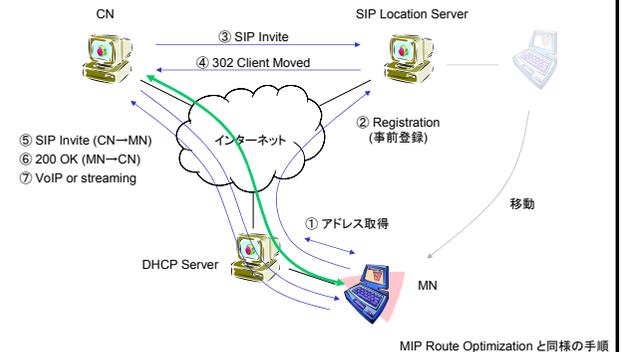
- FA の廃止: IPv6 Stateless Address Autoconfiguration
- Home Address Option: MN は発信元アドレスを CoA として送信
- Destination Option: Binding Update をデータパケットに乗せられる
- => Route Optimization を (MIP 拡張ではなく) IPv6 としてサポート

MIPv6 の手順:

- MN が CoA を取得する (Stateless Address Autoconfiguration)。
- MN が HA に CoA を登録する (MIP Registration)。
- CN からのパケットが、HA からカプセル化されて MN に転送。
- MN は、Binding Update を乗せて、CN にパケットを送信。
- 以降、MN と CN は、HA を介さずにパケットを送受信。

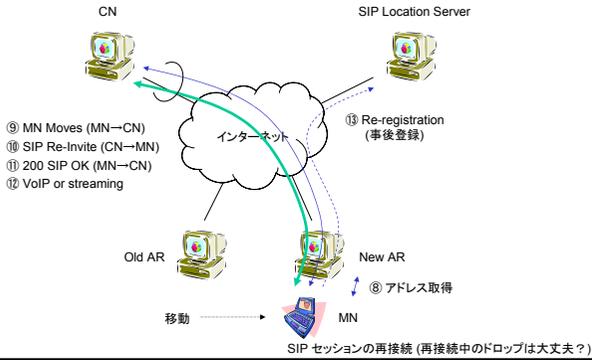
SIPモビリティ (1)

プレコール・モビリティ: セッション前



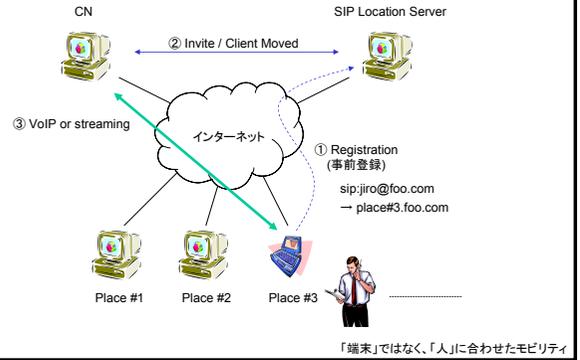
SIPモビリティ (2)

・ミッドコール・モビリティ: セッション中



SIPモビリティ (3)

・パーソナルモビリティ



MIP Mobility vs. SIP Mobility

| | Mobile IP | SIP Mobility |
|---------|--|---|
| 移動の単位 | 端末 (IP アドレス) | ユーザ (SIP URL) |
| レイヤ | L3 | L7 |
| 三角経路問題 | あり (MIPv4) 【対策】 (1) Route Optimization (MIPv4) (2) MIPv6 | なし |
| ハンドオフ対策 | HA への再登録 遅延要因: アドレス取得遅延+HA までのラウンドトリップ遅延 【対策】 (1) Hierarchical MIP (localization) (2) バッファリング (loss reduction) (3) バイキャストリング (loss reduction) | Location Server への再登録 遅延要因: アドレス取得遅延+Location Server までのラウンドトリップ遅延 |

ただし、共存は可能

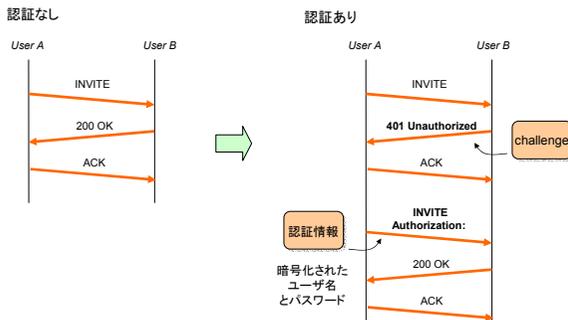
セキュリティ

- ・SIP Security (シグナリングレベル)
- ・Secure RTP (セッションレベル)
- ・NAT/ファイアウォール対策

調査中...

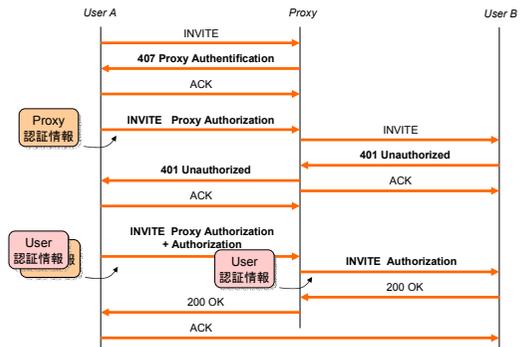
SIP Security (1)

・HTTP認証 (Digest認証): ユーザ認証



SIP Security (2)

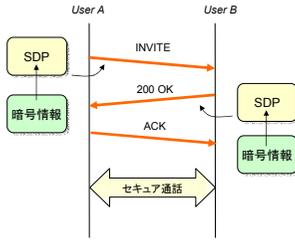
・プロキシ経由: ユーザ認証



Secure RTP

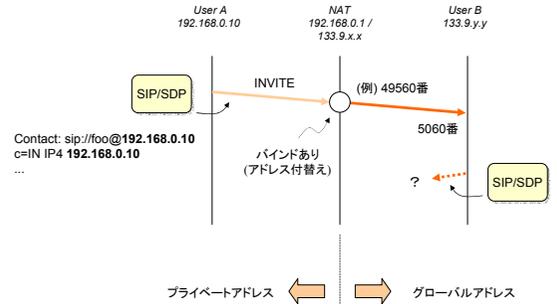
• RTP/RTCPパケットの暗号化

SDPIに暗号化情報を含める



NAT/ファイアウォールの問題

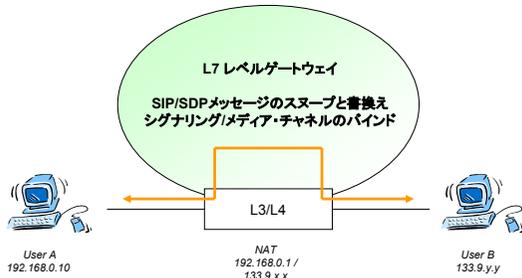
• SIP の場合



プライベートアドレスにリプライを返せない

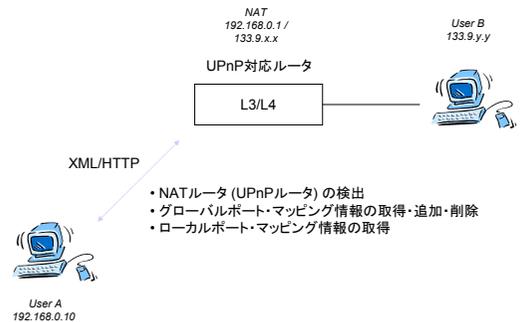
NAT/ファイアウォール対策 (1)

• アプリケーションレベル・ゲートウェイ



NAT/ファイアウォール対策 (2)

• UPnP (ユニバーサル・プラグアンドプレイ) と NAT Traversal



例: Microsoft SSDP / Windows XP

Security のまとめ

ダイジェスト認証: ユーザ認証

S/MIME: ユーザ認証、メッセージの完全性・機密性の保証

Secure RTP: RTP/RTCP パケットの暗号化

(NAT/Firewall)

ALG: アプリケーション (L7) レベル・ゲートウェイ

UPnP: ポート・マッピングの設定・追加・削除

(その他)

TLS: Layer 4 の暗号化

IPsec: Layer 3 の暗号化

ストリーミングソフトウェア について

Word 文書参照

まとめ

まとめ

【電話網】

キャリア企業による網管理とサービス提供



サービス、アプリケーションを使う
アプリケーションの構造を検討する

【インターネット】

一般ユーザへのプロトコルスタックの開放



サービス、アプリケーションを使う
アプリケーションの構造を検討する

作れ、と言われたら自分で作る (作ることができる)

電話、放送



インターネット電話、インターネット放送