地域 WiMAX
共通ネットワーク･ガイドライン

第 1.1 版

2010 年 1 月

地域 WiMAX 推進協議会

技術部会　コアネットワーク検討分科会

目次

【改版の履歴】

バージョン番号	改版年月日	備　　考
第 1.0 版	2009 年 7 月 29 日	オリジナル
第 1.1 版	2010 年 1 月 29 日	• 文書名称の変更“ローミングの在り方に関する要件書⇒共通ネットワーク･ガイドライン” • 現状の地域WiMAX事業者の状態を示すSTEP1/2の表記を STAGE 0 に変更。および該当する詳細説明の削除 • STEP3/4 の表記を STAGE1/2 に変更 • その他、上記の変更に関連する箇所の加筆･修正

１．目的と範囲

1.1　目的

『地域 WIMAX 推進協議会』は、地域におけるデジタル・ディバイドの解消、地域の公共サービスの向上等、地域の公共の福祉の増進に資する地域 WiMAX の普及促進を図るとともに技術的諸課題について検討を行い、地域 WiMAX の健全な発展を推進するために、設立された。

本文書『地域 WiMAX 共通ネットワークガイドライン』は、地域 WIMAX 推進協議会 コアネットワーク分科会において、地域 WiMAX 事業者による市販端末（リテール端末）の利用、および地域 WiMAX 間あるいは地域 WiMAX と全国 WiMAX 間でのローミングの提供をひとつの地域 WIMAX 発展へのマイルストーンと捉え、これを地域 WiMAX 事業者が実現するために必要な仕様要件を明らかにすることを目的に作成された物である。

仕様要件を明確にすることにより、地域 WIMAX の構成要件、インタフェース条件を WiMAX フォーラム標準に統一し、地域 WiMAX 間あるいは、地域 WiMAX と全国 WiMAX 間でのローミングが可能になる。

さらに、端末開発も統一的に行うことができるため、多くの端末メーカ・ベンダが地域 WiMAX にも対応したリテール端末での地域 WiMAX 利用も期待できる。

換言すれば本文書は、地域 WiMAX 事業者が解決すべき技術的課題を明らかにし、WiMAX の特徴である総合互換性を確保するための要求条件を記載している。各地域 WiMAX 事業者は、本要件を満たすことによって、地域 WiMAX 全体の利便性が向上し、発展させることができる。

1.2　範囲

本文書の範囲は、自前での地域 WiMAX システムの導入時、地域 WiMAX 事業者同士のローミング時に、必要な要件を記載している。

1.3　参考文献

我が国においては、直交周波数分割多元接続方式広帯域移動無線アクセスシステムの無線局の無線設備の技術的条件は、無線設備規則第 49 条の 28 に基づき、総務省告示第六百五十一号第一項によらなければならない。社団法人電波産業会（ARIB）では、これによって課せられる当該無線設備への要求条件を ARIB 標準「OFDMA Broadband Mobile Wireless Access System (WiMAX™ applied in Japan) ARIB STD-T94 Version 1.4」で標準化している。本標準は、また、上記直交周波数分割多元接続方式広帯域移動無線アクセスシステム（以後、モバイル WiMAX システム）の無線通信についても標準化している。本標準は、我が国においてモバイル WiMAX 設備を使う場合、上記無線設備規則による。また、上記モバイル WiMAX システムは、WiMAX Forum®が仕様化した WiMAX™ mobile System Profile 及び WiMAX End-to-End Network Systems Architecture に従わなければならない。

本要件書が随所で参考とした WiMAX End-to-End Network Systems Architecture は ARIB STD-T94 Version 1.4 第 1 分冊及び第 2 分冊に付属している。

ARIB STD-T94 Version 1.4 第 1 分冊
WiMAX End-to-End Network Systems Architecture
WiMAX Forum® Network Architecture Release 1.0 Version 4
(Stage 2: Architecture Tenets, Reference Model and Reference Points)
WM フォーラムネットワークアーキテクチャ(ステージ 2: 構成基本要件、参照モデル、参照点)
文献 1．[Stg2-1]
STD-T94 Attachment 4-3
http://www.arib.or.jp/english/html/overview/doc/1-STD-T94v1_4-1p2.pdf
[Part 1]
http://www.wimaxforum.org/sites/wimaxforum.org/files/WMF-T32-002-R010v04_Network-Stage2-Part1_2.pdf

- Section 1 - Document Scope
  ドキュメントの範囲
- Section 3 - References used in the document
  このドキュメントで用いられる参考文献
- Section 4 - Tenets for WiMAX Network System Architecture
  WiMAX ネットワークシステムの構成基本要件

・Section 5 - Identifiers: List of identifiers used in a WiMAX network
識別子: WiMAX ネットワークで用いられる識別子リスト
・Section 6 - Network Reference Model, a logical representation of the network architecture.
ネットワーク参照モデル、ネットワーク構成の論理的表記

文献２. [Stg2-2]
STD-T94 Attachment 4-4
http://www.arib.or.jp/english/html/overview/doc/1-STD-T94v1_4-1p2.pdf
[Part 2]
http://www.wimaxforum.org/sites/wimaxforum.org/files/WMF-T32-003-R010v04_Network-Stage2-Part2.pdf
・Section 7 - Functional Design and Decomposition
機能設計とその要素分解
・Section 8 - ASN Profile Introduction
ASN プロファイル紹介

文献３. [Stg2-3]
STD-T94 Attachment 4-5
http://www.arib.or.jp/english/html/overview/doc/1-STD-T94v1_4-1p2.pdf
[Part 3]
http://www.wimaxforum.org/sites/wimaxforum.org/files/WMF-T32-004-R010v04_Network-Stage2-Part3.pdf
Informative Annexes for Stage 2
ステージ２についての有益な情報の付録
・Annex A: WiMAX Reference Architecture Deployment Scenarios
WiMAX 参照構成展開シナリオ
・Annex B: MS Movement with FA change, no PC change
MS の FA 変更あり、呼出しコントローラ不変の移動
・Annex C: ASN-GW Selection Protocol
ASN-GW 選択プロトコル
・Annex D: ‘RRM’: Spare Capacity Report per QoS Profiles
無線リソース管理: QoS プロファイルごとの残余キャパシティ報告
・Annex E: Ethernet Operational Behavior
イーサネット運転についての動作
・Annex F: TECHNICAL ANNEX: SUPPORT OF REAL TIME SERVICES
技術情報付録: リアルタイムサービスのサポート

文献４．[Stg3]
ARIB STD-T94 Version 1.4 第２分冊　Attachment 4-9
http://www.arib.or.jp/english/html/overview/doc/1-STD-T94v1_4-2p2.pdf
WiMAX Forum® Network Architecture Release 1.0 Version 4
(Stage 3: Detailed Protocols and Procedures)
WM フォーラムネットワークアーキテクチャ(ステージ 3: プロトコルと手順の詳細)
http://www.wimaxforum.org/sites/wimaxforum.org/files/WMF-T33-001-R010v04_Network-Stage3-Base.pdf
文献５．[PKIOverview]
WiMAX Public Key Infrastructure (PKI) Users Overview
WiMAX 公開鍵基盤利用者向け概要
http://www.wimaxforum.org/sites/wimaxforum.org/files/documentation/2009/wimax_pki_users_overview_may27.pdf
文献６．[DevCert]
WiMAX Forum X.509 Device Certificate Profile Approved Specification Version 1.0.1
WiMAX フォーラム X.509 デバイス証明書プロファイル承認済み仕様
http://www.wimaxforum.org/sites/wimaxforum.org/files/documentation/2009/wimax_forum_x509_device_certificate_profile.pdf
文献７．[ServCert]
WiMAX Forum X.509 Server Certificate Profile Approved Specification Version 1.0.2
WiMAX フォーラム X.509 サーバ証明書プロファイル承認済み仕様
http://www.wimaxforum.org/sites/wimaxforum.org/files/documentation/2009/wimax_forum_x509_server_certificate_profile.pdf
文献８．[EAP-TTLS]
IETF draft-pppext-eap-ttls-05
EAP Tunneled TLS Authentication Protocol (EAP-TTLS)
拡張可能認証プロトコル-トンネル型トランスポートレイヤセキュリティ認証プロトコル
http://tools.ietf.org/html/draft-ietf-pppext-eap-ttls-05

文献９．[MIP]
RFC3344　IP Mobility Support for IPv4
　　IPv4 に対する IP 移動性サポート
　　http://www.ietf.org/rfc/rfc3344.txt
文献１０．[RevTunnel]
RFC3024　Reverse Tunneling for Mobile IP, revised
　　モバイル IP に対する逆方向トンネリング、改訂版
　　http://www.ietf.org/rfc/rfc3024.txt
文献１１．コアネットワーク検討分科会　勉強会（H.21.2.27）　資料 2「WiMAX 事業者のローミング」

2．用語と定義

用　　語	定　　義
ローミング	Roaming
ハンドオーバ	Hand-over あるいは Hand-off
NSP	Network Service Provider、ネットワーク･サービス･プロバイダ
H-NSP	Home NSP、ホーム･ネットワーク･サービス･プロバイダ
V-NSP	Visited NSP、訪問先ネットワーク･サービス･プロバイダ
NAP	Network Access Provider、ネットワーク･アクセス･プロバイダ
H-NAP	Home-NAP、ホーム･ネットワーク･アクセス･プロバイダ
V-NAP	Visited-NAP、訪問先ネットワーク･アクセス･プロバイダ
クリアリング･ハウス	Clearing House
ローミング交換	Roaming Exchange
ローミングイン	Roaming in
ローミングアウト	Roaming out
MS	Mobile Station、WiMAX 端末（移動端末）
BS	Base Station、WiMAX 基地局
ASN	Access Service Network、アクセスサービスネットワーク
CSN	Connectivity Service Network、コネクティビティサービスネットワーク
ASN-GW	Access Service Network Gateway、アクセス･サービス･ネットワーク･ゲートウェイ
HA	Home Agent、ホーム･エージェント
PF	Policy Function、ポリシー･ファンクション
MIP	Mobile IP、モバイル IP
PMIPv4	Proxy Mobile IPv4
CMIPv4	Client (Based) Mobile IPv4
Simple IPv4	シンプル IP
NAP ID	Network Access Provider ID あるいは Operator ID
NSP ID	Network Service Provider ID あるいは Operator ID
BS ID	Base Station ID
Controled Device	コントロール端末（ユーザ ID とパスワードを書込済みの端末）
Retail Device	リテール端末（市販端末）

３．地域 WiMAX システムの基本要件

本章では地域系 WiMAX 事業者が同システムを運用する際に必要な基本要件を記す。しかし、十分要件ではないので、実際の運用場面で遭遇する問題を解決するには WiMAX Forum ネットワークアーキテクチャ[Stg2][Stg3]などを参照する必要がある。

当該の基本要件とは次のような事項である。

◇ 端末はどのように網にアクセスし、インターネットへの接続に至るのか。
◇ そのような網にはどのような機能が必要なのか。
◇ 正しい加入者を識別する認証の仕組みはどのように実現されているのか。
◇ これらの結果として、ローミングはどのように実現されるのか。

3.1 WiMAX ネットワークの基本構成

3.1.1 ネットワーク参照モデル(NRM)とは

参考: [Stg2-1]6.1 Overview

NRM はネットワークアーキテクチャ(構造)をロジカルに表現したものである。NRM は機能主体(エンティティ)とそれら機能主体間で相互接続が行われる参照点を示すものである。機能主体とは MS、ASN、CSN であって、NRM を構成する。

上記機能主体は単一の物理機能主体で実現しても、複数の物理的機能主体に分散させてもかまわない。

ASN 内に定義される機能をどのように物理装置へグルーピングするか、または分散させるかによって、ASN の 3 つの相互接続プロファイル―プロファイル A、B、C が定義されている。

NRM の意図はひとつの機能主体について複数の実装方法を許し、かつ様々な実装方法の機能主体間で相互接続を達成することにある。
相互接続は、エンドエンドにわたるシステム全体の機能（例えばセキュリティ管理や移動管理）を実現しようとする各機能主体間での通信プロトコルとデータプレイン処理に基づいて行われる。よって、参照点の両側の機能主体は制御プレインとベアラプレインの終端点が集まったものと言える。

上述の構成上の約束があれば、相互接続性は参照点を通過する外部に現れたプロトコル

のみに基づいて検証することができる。相互接続性の検証は、ネットワーク全体にわたってサポートされる使用シナリオに基づくエンドエンドの機能や能力によって違ってくる。

WiMAX Forum ネットワークアーキテクチャ仕様書はサポートされる機能・能力について、参照点上でのプロトコルの標準用法を仕様化している。もしひとつの実装がある機能をサポートしていると主張し、参照点を有しているならば、当該実装は本仕様書に従ったものでなければならない。下の 図 3.1_1 ネットワーク参照モデル(NRM) に NRM を図示する。

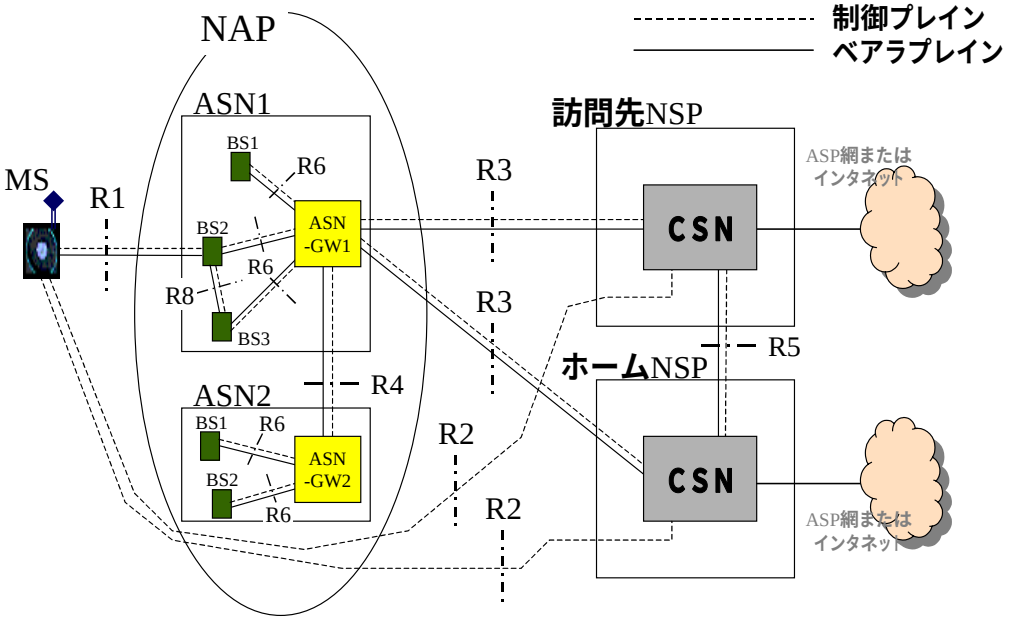


図 3.1_1 ネットワーク参照モデル(NRM)

(参考: [Stg2-1] Fig6-1)

3.1.2 参照点

参考: [Stg2-1]6.2 Reference Points

1） 参照点 R1

MS-BS 間のエアインタフェイス(PHY、MAC)の参照点である。本インタフェイスは IEEE802.16e-2005、802.16-2004 および IEEE802.16g に従う。

2） 参照点 R2

MS-CSN 間のロジカルなインタフェイスの参照点である。CSN は AAA 機能やその他ネットワーク要素機能(DHCP 機能など)をつかさどる。AAA インタフェイスは認証やサービスの承認、課金、IP ホストコンフィグ管理をサポートする。

3） 参照点 R3

ASN-CSN 間の制御プレインとベアラプレインの参照点である。制御プレインのプロトコル

は AAA、ポリシ実行、移動管理機能をサポートする。ベアラプレインはユーザデータを転送するためのベアラプレイン方式（例えばトンネリング）をサポートする。

４） 参照点 R4

２つの ASN 間のインタフェイスの参照点である。ASNs 間や ASN-GWs 間で MS が移動するとき、その移動管理を取り仕切る ASN 上の各種機能に発着する制御とベアラプレインのプロトコルから成る。

５） 参照点 R5

２つの NSP、すなわち H-NSP と V-NSP 間の制御とベアラプレインのプロトコルから成る。両 NSP がローミング合意に至った場合に用いられるトラディショナルローミングアーキテクチャである。

６） 参照点 R6

BS―ASN-GW 間の制御およびベアラプレインのプロトコルの参照点である。

3.1.3 ASN の参照モデル

参考: [Stg2-2]8. ASN Profile Introduction

WiMAX Forum では 3 つの異なる ASN プロファイルを定めたが、このうちのひとつ、プロファイル A は次バージョン Rel1.5 から除かれる。

各プロファイルは ASN を構成する機能を BS と、対応する ASN-GW に配置する。これによって参照点を通過するプロトコルとメッセジが規定される。また、ASN 機能を運用する事業者をネットワークアクセス事業者(NAP)と呼ぶ。

１）プロファイル B

ASN-GW-BS 間の外部にオープンな参照点 R6 を規定しない。このため ASN 内での相互接続性については記述されない。しかし、R3、R4 参照点を介して、他のどのようなプロファイルの ASN とも接続できる。また、R4 参照点を介してひとつの ASN から他の ASN へのハンドオーバが可能である。本プロファイルでは ASN を構成する各機能が単一の物理筐体内に実装される場合、異なる物理筐体内に実装される場合とがある。

２）プロファイル C

ASN 機能主体の参照点 R3、R4 の他に、ASN-GW-BS 間の参照点 R6 が外部にオープンになっている。

下の 図 3.1_2 ASN 参照モデル プロファイル C にプロフィアル C による ASN 参照モデルを示す。

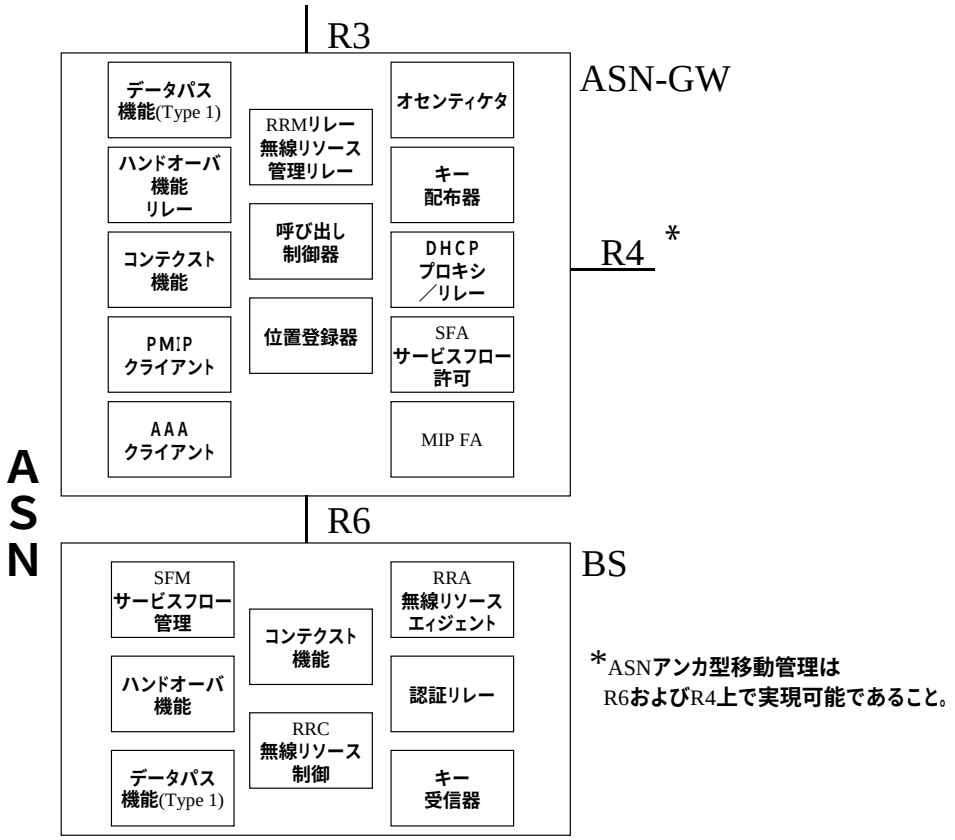


図 3.1_2 ASN 参照モデル プロファイル C

(参考: [Stg2-2] Fig8-3)

3.1.4 CSN の参照モデル

CSN 機能主体の内部の参照点は WiMAX Forum 仕様の対象外である([Stg2-1]6.6 CSN Reference Model)。

CSN はインタネットへの接続サービスを提供するネットワークサービス事業者(NSP)の IP コア部とも呼ばれ、当該サービスのための主要機能の総体である。CSN はこれらの主要機能―AAA(認証、オーサラゼイション、課金)、IP アドレス割付、モバイル IP 用 HA、その他各種アプリケーション機能―を提供し、制御する。IMS(IP Multimedia Subsystem)機能もここに置かれ、他メディア網との相互接続仕様が整えられている。下の 図 3.1_3 CSN 参照モデル一例 に CSN の参照モデルの例を掲げる。

この図には AAA 機能が自 NSP 内の HA ばかりではなく、外部の HA の制御も行っている様子を示した。

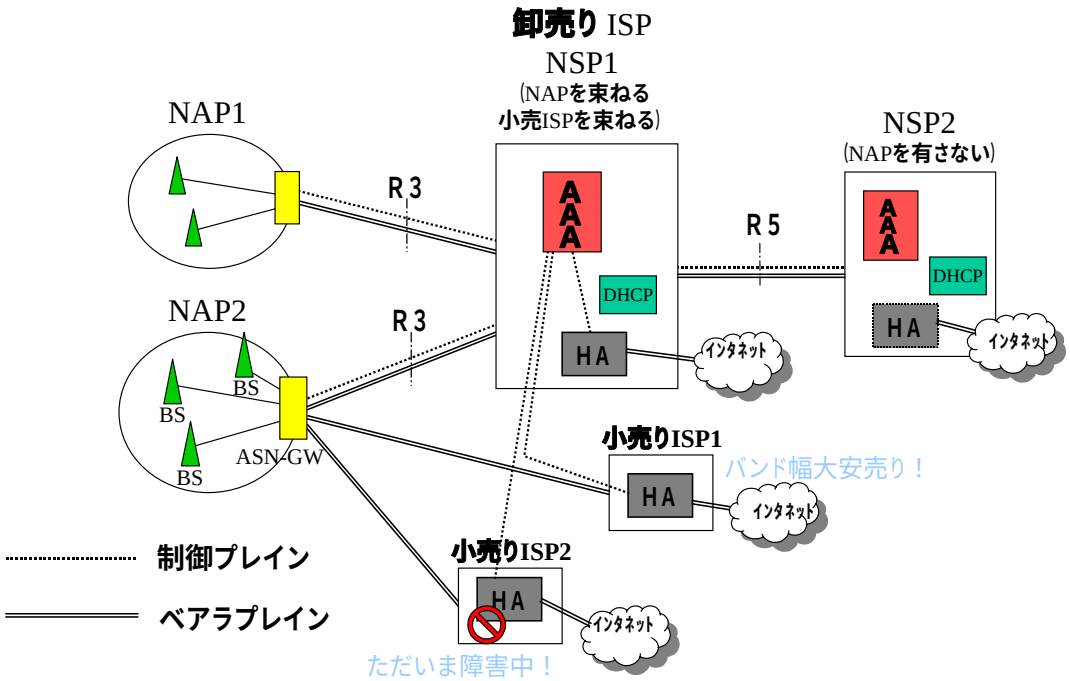


図 3.1_3 CSN 参照モデル一例

3.1.5 NAP+NSP および NAP シェアリング

NAP と NSP には、それぞれ当該事業者を区別するための識別子が割り当てられる。この識別子は端末がアクセスすべき ASN および CSN を複数の ASNs、CSNs の中から識別するために使用される。これらの識別子は異なる NAP がそれぞれのエリアをオーバラップし、あるいは隣接している状況下で自網を識別する場合や、ホーム NSP とローミング契約のある訪問先 NSP を識別する場合を考慮して、ユニークに割り当てられていなければならない。

これらの識別子(NAP-ID,NSP-ID)は Operator ID とも呼ばれ、それらの割当ては IEEE Registration Authority(RAC)により受けなければならない（[Stg2-2]7.1.4.1 WiMAX NAP Discovery、7.1.4.2 NSP Access Discovery 第 1 パラグラフ)。Operator ID については、コアネットワーク検討分科会　勉強会(H21.2.27)資料 2「WiMAX 事業者のローミング」【付録 1】BSID と NAP ID、NSP ID に詳述されているので参照されたい。

一方、単一の事業者が単一の ASN および単一の CSN のみを運用している場合、その構成は NAP+NSP と表記されることが多い。NAP+NSP 構成の場合には、以下の図 3.1_4 NAP+NSP 構成 に示すように NAP-ID と NSP-ID は同一の値を使用してもよいとされている。

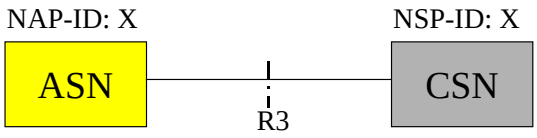


図 3.1_4 NAP+NSP 構成

(参考: [Stg2-3] FigA-5)

さらに、単一の ASN が複数の NSPs に接続を提供する運用を NAP シェアリングという。複数の NSPs が複数の MVNOs に対応すると考えられる。各 MVNO が同一の無線インフラ(ASN)を共用して、独自のインタネット接続サービスを提供する。この場合には、各 NSP を識別するため NSP-IDs は異なっていなければならない。図 3.1_5 NAP シェアリング に一つの NAP が 2 つの NSPs と接続している様子を示す。

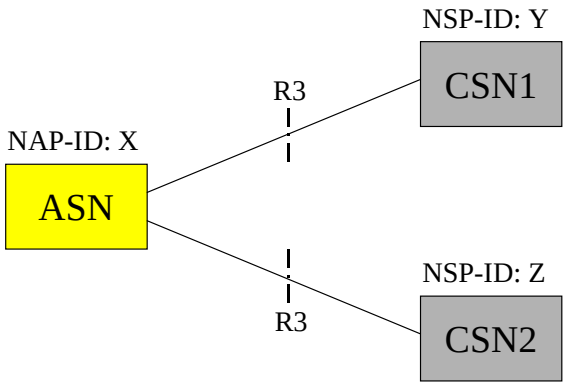


図 3.1_5 NAP シェアリング

(参考: [Stg2-3] FigA-6)

3.1.6 ローミングアーキテクチャ

参考: [Stg2-3]A. WiMAX Reference Architecture Deployment Scenarios

ローミングとは、ホーム NSP に加入契約をしているユーザの端末が、このユーザと直接かつ事前の契約を有していない訪問先 NAP あるいは訪問先 NSP を介してインタネット接続を行うことをいう。

ローミングが成立するための主要な要件は、R2 コネクションを端末―ホーム NSP 間に設定し、ホーム AAA がユーザ認証や鍵配布などセッションの確立、維持のための制御を可能ならしめることである。

この要件を満足する接続構成には、ホーム事業者(ホーム NSP)がローミングパートナ事業

者と R3 または R5 参照点でインタフェイスする 2 つの接続構成モデルがある。

1) R3 および R5 参照点を経由するトラディショナルローミングモデル
端末からホーム AAA に至る R2 コネクションを、訪問先 NAP-(R3)-訪問先 NSP-(R5)-ホーム NSP(ホーム AAA)とする構成をトラディショナル（またはレガシ）ローミングモデルということがある。Wi-Fi Alliance のリコメンデイション、Wireless ISP Roaming(WISPr)は、上記のトラディショナルローミングモデルである。
2) R3 参照点のみを経由する NAP シェアリングモデル
1)のように R2 コネクションがローミングパートナ事業者の NSP(訪問先 NSP)を経由することなく、訪問先 NAP-(R3)-ホーム NSP(ホーム AAA)とする構成を NAP シェアリングモデルという。パートナ事業者とローミング契約が結ばれれば、ホーム NSP はパートナ事業者の NAP(訪問先 NAP)と R3 参照点で接続する。訪問先 NAP が訪問先 NSP およびホーム NSP と共有されるため、NAP シェアリングモデルと呼ばれる。

1)、2)どちらのモデルにおいても、端末に発着するインタネットトラフィック(ベアラトラフィック)は、訪問先 NSP を経由しても、ホーム NSP を経由してもかまわない。これはローミングパートナ事業者との契約によって決められる。
ローミングが成立する場合、加入契約者、NAP、NSP との間には契約関係が必要である。これらの契約関係を下の 図 3.1_6 ローミング成立のための契約関係 に示す。

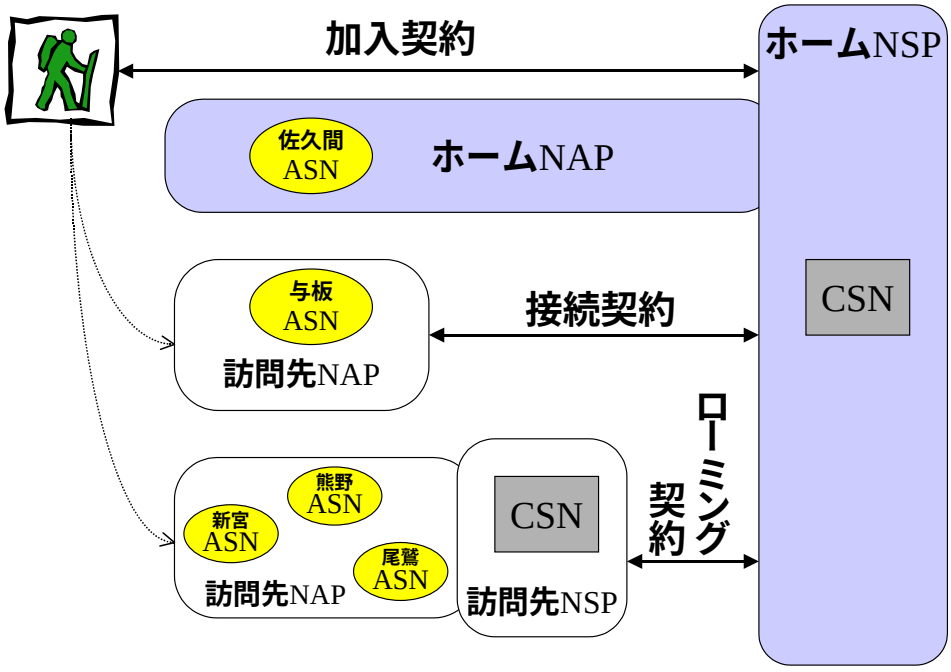


図 3.1_6 ローミング成立のための契約関係
(参考: [Stg2-3] FigA-1)

トラディショナルローミングモデルおよび NAP シェアリングモデルとが組み合わされた ASN と CSN の接続構成の一例を下の 図 3.1_7 ローミング接続構成の一例 に図示する。

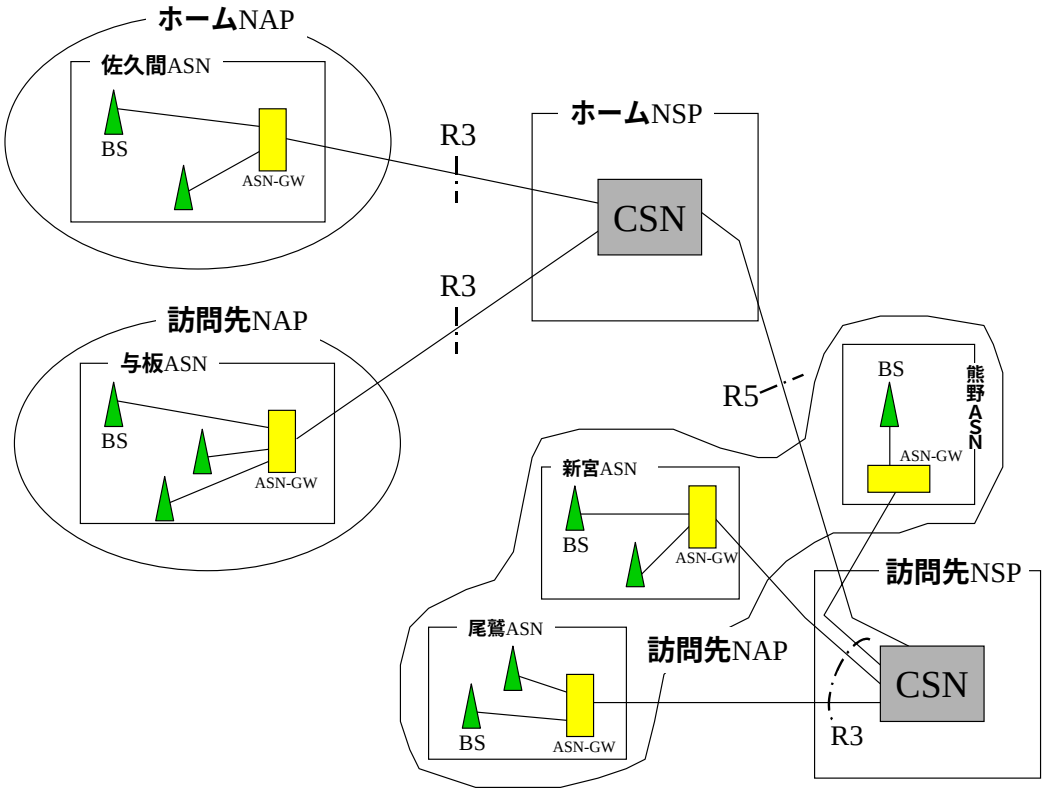


図 3.1_7 ローミング接続構成の一例

3.2 端末の網アクセスーネットワークエントリ

ネットワークエントリ手順は、端末の初期レンジングから始まる。引き続いて、端末と BS は、通信基礎能力の交渉、PKMv2 を使用した認証、PKMv2 を使用した TEK(トラフィック暗号化キー)の確立、ネットワークへの登録、およびその他 IP アドレスの配布、取得などを行う。しかし、端末は BS へレンジングを開始する前に、まず、その電源が投入され、BS の電波を受信し、自分が初期レンジングを開始してよい状況下にあるかどうか判断することが必要である。

3.2.1 端末の電源が投入されると――ND&S

参考: [Stg3]4.1.1 General、[Stg2-2]7.1.4 NAP,NSP Discovery and Selection

端末は、その電源が投入されると、ネットワーク検出と選択(NW Discovery and Selection ND&S)を開始する。ND&S は次の４つの手順に大別される。

a) NAP 検出
b) NSP 検出
c) NSP の列挙と選択
d) 選択した NSP に基づく ASN への接続

端末はこれらの手順を行うに当たって、まず、BS の電波の受信を試みる。しかし、どの帯域を、どのような順番でスキャンしてダウンリンクサブフレームを見つけるのか。ダウンリンクサブフレームを発見したが、これを発信する BS は自分がアクセスを許可された NAP の NAP-ID を報知しているのか。許可されていない NAP-ID を検出したが、もしや自分は訪問先のネットワークにローミング中ではないのか。そうであるなら、その許可されていない NAP が接続している NSP はホーム NSP とローミング契約があるのか。帯域スキャンの結果、複数の利用可能な NAP-ID を検出した場合に備えて、あるいは、複数の利用可能な NSP-ID を検出した場合に備えて、アクセスを開始する NAP-ID、NSP-ID の優先度をきめておかなければならない。

3.2.1.1 端末のコンフィグ情報

ND&S を進行させるため、端末には、判断基準をプロビジョニングしておくことができる。これらの判断基準のため、OMA DM MOs(Open Mobile Alliance Device Management Management Objects)と呼ばれるデータ属性が定義されている。この判断基準に相当する端末のコンフィグ情報とは次のものを設定すべきである([Stg3]4.1.3 Configuration Information)。

① CAPL(Contractual Agreement Preference List 契約合意済み優先リスト)

CAPL は、ホーム NSP と直接関係（接続）を有す NAPs のリストである。本リストは、ホーム NSP が一つ以上の NAP によって到達が可能である場合に、NW エントリを開始する１つの NAP を決定するのに用いる。

CAPL は、NAP-ID が記載され、各 NAP についての優先順位を付けることができる。また、CAPL は NAP 選択ポリシを付けることができる。NAP 選択ポリシとは次のものである。

厳格ポリシ： 端末は、ホーム NSP に対して CAPL 中に存在しない NAPs によって接続してはならない。

一部緩和ポリシ： 端末は、CAPL 中に存在しない NAP を選択することができるが、その前に CAPL に存在する NAPs を選択することを試みること。

完全緩和ポリシ： 端末はどの NAP を使用してホーム NSP へ接続してよい。CAPL 中の NAPs のうち優先順位を付されていないものは、CAPL 中に存在しない NAPs と同一の優先順位である。

② RAPL(Roaming Agreement Preference List; ローミング合意済み優先リスト)

RAPL はホーム NSP と直接関係(接続)を有する訪問先 NSPs のリストである。本リストは、ホーム NSP に対して直接接続を有する NAPs が利用可能でないとき、すなわちローミング中であるとき、最高優先順位を持つ 1 個の NSP を決定するのに用いられる。

RAPL は VNSP-ID が記載され、各 VNSP についての優先順位を付けることができる。また、RAPL も CAPL 同様、VNSP 選択ポリシを付けることができる。

③ NAP/NSP マッピングリスト

NAP/NSP マッピングリストは、NAP 毎のサポート中 NSPs およびこれらに対応するバーバス NSP 名前 s を示す。

④ NSP チェンジカウント

NSP チェンジカウントは、一つの NAP に対するサポート中 NSPs またはこれらに対応するバーバス NSP 名前 s のリストに変更があったかどうかを示す。

⑤ NSP レルム

24 ビットの NSP-IDs と当該 NSPs に対応するレルムのマッピング表である。

⑥ チャネルプラン

チャネルプランは複数のチャネル（エントリ s）から成る。1 つのチャネル(エントリ)ごとに、物理情報であるスキャンすべき中央周波数 s、その範囲、バンド幅、FFT サイズ、プリアンブル、複信モードが記載され、さらに CAPL 中の NAP との紐付けをする ID が含まれる。

チャネルプラン情報を端末に供給する主要な意味は ND&S をスピードアップすることにある。チャネルプランは CAPL にリストされる複数のまたは全ての NAPs の物理情報をカバーすることができる。さらに、チャネルプランは CAPL にリストされない NAPs の物理情報をカバーしてもよい。

チャネルプランには、端末がサポートしなければならないルートチャネルプランとオプ

ションである NAP ベースチャネルプランがある。

ルートチャネルプランは全てのチャネルプランエントリ s を含んでいる。全てのチャネルプランは優先順に並べる必要があり、この優先順位を付けて並べられた全チャネルエントリをルートチャネルプランという。

端末は、ルートチャネルプランに基づく NAPs の探索を全チャネルについて尽くした後に、CAPL の指定に基づいて、見出した NAPs の内から最高順位の NAP を選択することが許される。端末は、当該端末がサポートするバンド s の範囲内で、CAPL によるルールに適合する NAPs が見出せない場合に限って RAPL(すなわちローミングするため)を参照するべきである。

NAP ベースチャネルプランとは、特定の NAP を見出し、選択するために、関連するチャネルプランエントリに基づいて、当該チャネルを調べる手順である。ルートチャネルプランが全チャネルをスキャンし、全ての NAPs を見出した後、１つの NAP を選択するのとは異なり、NAP ベースチャネルプランに従いチャネルをスキャンする場合には、優先順位の高い NAP を見出したら、そこで NAP の探索を打ち切ることができる。

⑦　セキュリティパラメタ

セキュリティパラメタは、認証するために一つの NSP がユーザをユニークに識別する ID としてのクレデンシャルなどがある。

⑧　NW 展開モード

各 NAP の NW 展開モード。すなわち、NAP+NSP モード、あるいは NAP シェアリングモード。

3.2.1.2 CAPL と RAPL の関係

3.2.1.1 節①CAPL および②RAPL について、下の図 3.2_1 CAPL と RAPL の関係に図示する。

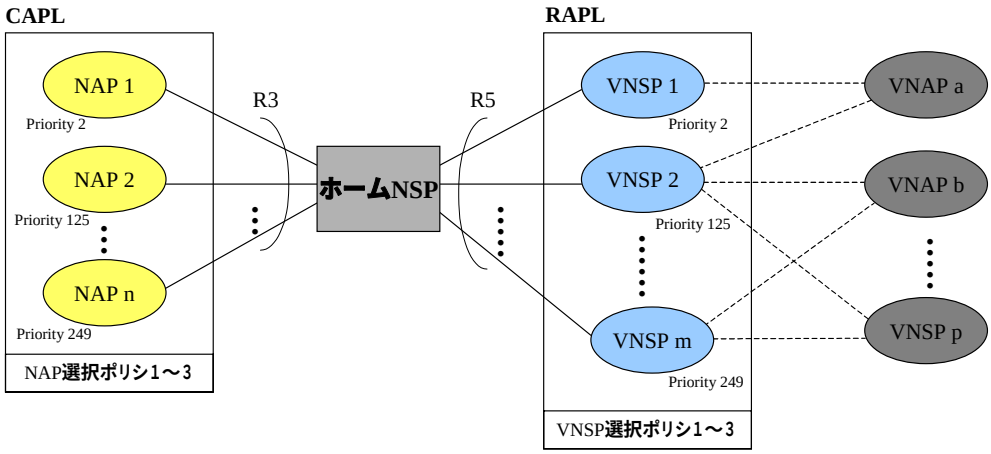


図 3.2_1 CAPL と RAPL の関係

3.2.1.3 チャネルプランの例示

チャネルプランの一例を挙げ、ルートチャネルプラン、NAP ベースチャネルプランがどのように行われるかを説明する。

図 3.2_2 H-NSP を中心とした直接接続の関係と各サービスエリアの例 には、ホーム NSP 直接接続の合意契約を持つ NAP や訪問先 NSP を示し、NSP 配下の各 NAP が運用するサービスエリアを想定した。サービスエリア A、B、D では中心周波数が全て r1 であるチャネルが使用されている。サービスエリア C では中心周波数が u1、u2 である 2 つのチャネルが使用されているとした。

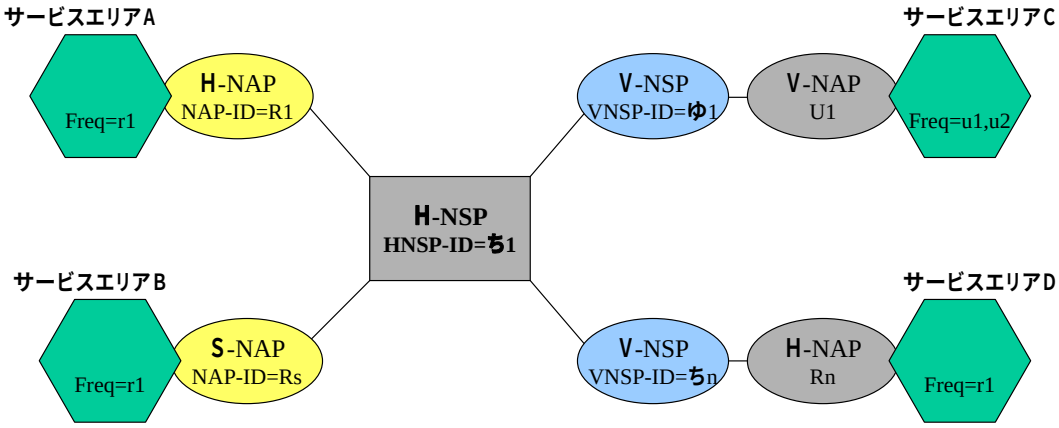


図 3.2_2 H-NSP を中心とした直接接続の関係と各サービスエリアの例

1） ルートチャネルプランの使用例

ルートチャネルプランを使用した端末コンフィグ情報の例を、図 3.2_3 端末コンフィグ―ルートチャネルプラン に示す。

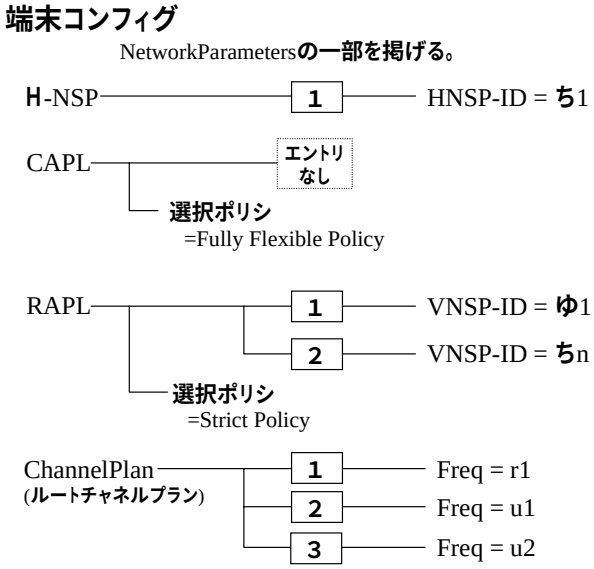


図 3.2_3 端末コンフィグ―ルートチャネルプラン

ルートチャネルプランでは ChannelPlan の各エントリは、優先順に並べられている。このため、BS の電波の受信は、エントリ順位の順番に行われる。CAPL については、選択ポリシは Fully Flexible Policy(完全緩和ポリシ)であって、直接接続 NAPs についてのエントリはない。すなわち、ルートチャネルプランに従って、電波をスキャンして、報知中の NSP-ID(VNSP-ID といってもよい)＝ち 1(HNSP-ID)ならば、その NAP を選択して、NW エントリを開始してもよい。もし、全チャネルのスキャンを終了したが、ち 1(HNSP-ID)を報知する NAP を検出できない場合には、RAPL のチェックに移る。すなわち、端末はローミングしていることを認識する。RAPL は、ここでは厳格ポリシが設定されているので、RAPL にリストされている VNSP-ID＝ゆ 1、ち n を報知している NAP エリア内でのみ NW エントリを開始できる。

-サービスエリア A の端末のふるまい

本エリアは H-NAP(NAP-ID＝R1)のエリアであり、周波数 r1 のスキャンをすることにより、NAP-ID＝R1、HNSP-ID＝ち 1 が検出される。その後、その他の周波数 u1、u2 のスキャンを実施するが、当該電波は受信されず、スキャンは終了する。このため、NAP-ID＝R1 が NW エントリの対象として選択される。

-サービスエリア B の端末のふるまい

本エリアでの端末のふるまいはサービスエリア A と同様である。たんに、検出された NAP が H-NSP を共有している S-NAP であることである。NAP-ID＝Rs が NW エントリの対象として選択される。

-サービスエリア C の端末のふるまい

本エリアでは、周波数 r1 のスキャンによってはどの NAP も検出されない。優先順位２、３番目の周波数 u1、u2 をスキャンすると VNAP-ID＝U1 が検出される。この V-NAP の報知情報からは VNSP-ID＝ち 1＝HNSP-ID は見出せない。よって、端末は RAPL を参照する。すると、V-NAP の報知情報、VNSP-ID＝ゆ 1 と同一値がリストされている。これによって、端末は自分がローミング契約のあるサービスエリア C にローミング中であることを知り、当該サービスエリアを運用している V-NAP(VNAP-ID＝U1)に NW エントリを開始する。

-サービスエリア D の端末のふるまい

本エリアでは、端末は、ルートチャネルプランに従って全ての周波数をスキャンし終えると、VNAP-ID＝Rn のみを検出する。しかし、この V-NAP は HNSP-ID＝ち 1 を報知していない。このため、端末は RAPL を参照し、その中の VNSP-ID＝ち n が報知情報中の VNSP-ID と一致していることを知る。よってローミングが許可されているので、端末は VNAP-ID＝Rn を有する V-NAP に NW エントリを開始する。

２） NAP ベースチャネルプランの使用例

NAP ベースチャネルプランを使用した端末コンフィグ情報の例を、図 3.2_4 端末コンフィグ―NAP ベースチャネルプラン に示す。

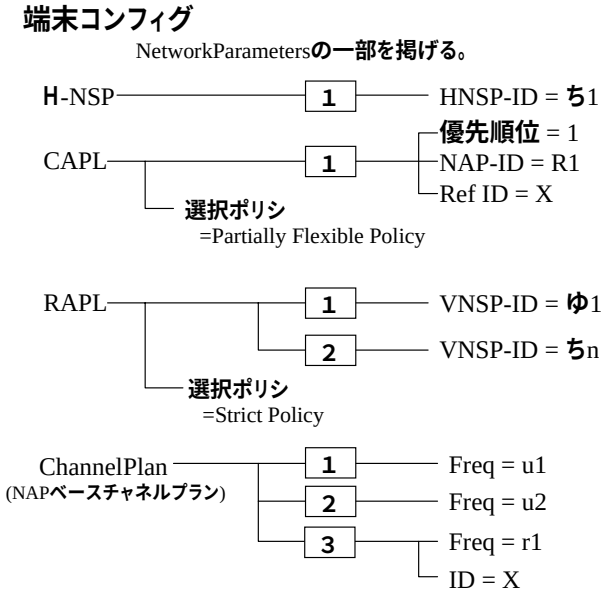


図 3.2_4 端末コンフィグ―NAP ベースチャネルプラン

NAP ベースチャネルプランでも ChannelPlan の各エントリは、ルートチャネルプランのとおり優先順に並べられている。しかし、優先的に検出したい NAP について、CAPL 内の当該

エントリに RefID が設定されており、この参照値と同一の ID を有す ChannelPlan のエントリに従って、指定された周波数をスキャンする。ここでは、H-NAP(NAP-ID＝R1)に RefID＝X が設定され、この参照値 X によって紐付けられる周波数 r1 が最初にスキャンされる。NAP-ID＝R1 が見つかると、この NAP-ID は優先順位＝1 であるため、もはやその他の NAP の検出は行うことがないため、本 NAP(NAP-ID＝R1)への NW エントリを開始する。もし、NAP-ID＝R1 が見出せない場合は、CAPL の選択ポリシが、ここでは、Partially Flexible Policy(一部緩和ポリシ)に設定されているため、HNSP-ID＝ち 1 を報知する NAP を次優先順位の NAP とする検出を行う。以後の NAP 検出および V-NSP の検出はルートチャネルプランの場合と同様に行われる。

-サービスエリア A の端末のふるまい

端末は、NAP ベースチャネルプランに従って、HNAP-ID＝R1 を検出しようとする。本エリアは H-NAP(NAP-ID＝R1)のエリアであり、周波数 r1 のスキャンをすることにより、NAP-ID＝R1、HNSP-ID＝ち 1 が直ちに検出される。その後、その他の周波数 u1、u2 のスキャンを実施せずに、スキャンは終了して、NAP-ID＝R1 が NW エントリの対象として選択される。

-サービスエリア B の端末のふるまい

本エリアでの端末のふるまいはサービスエリア A と同様であるため、端末は NAP-ID＝R1 を検出しようとする。しかし、これが検出できず、SNAP-ID＝Rs を検出する。この S-NAP は H-NSP を共有しているため、HNSP-ID＝ち 1 を報知している。端末は、CAPL の選択ポリシが一部緩和ポリシなので、この S-NAP を NW エントリの候補として列挙する。さらに、端末はルートチャネルプランに基づいて ChannelPlan の残りのエントリによって指示される周波数をスキャンする。しかし、なんら電波が検出されないため、先ほど列挙した SNAP-ID＝Rs が NW エントリの対象として選択される。

-サービスエリア C の端末のふるまい

本エリアでも、端末は NAP ベースチャネルプランに従って、HNAP-ID＝R1 を検出しようとする。周波数 r1 のスキャンによってはどの NAP も検出されないことを知った後、ルートチャネルプランに従って周波数 u1、u2 をスキャンする。以下、VNAP-ID＝U1 を検出してから、RAPL を参照し、NW エントリを開始する手順は、１）の場合と同様である。

-サービスエリア D の端末のふるまい

本エリアでも、サービスエリア C 同様、端末は、NAP ベースチャネルプランに指定される HNAP-ID＝R1 を検出することができず、ルートチャネルプランに従って残りの周波数をスキャンし終えると、VNAP-ID＝Rn のみを検出する。しかし、この V-NAP は HNSP-ID＝ち 1 を報知していない。その後、端末は RAPL を参照し、ローミングが許可されているかを判断し、

V-NAP に NW エントリを開始する手順は１）と同様である。

なお、１）ルートチャネルプラン、２）NAP ベースチャネルプランにおいても、端末のコンフィグ情報をどのように解釈し、ND&S 手順を進めてゆくかは、実装依存の部分が大きいことが想定される。しかし、そうであっても、NW エントリは、R1 参照点を通過するプロトコルが網―端末間で標準に従っていれば、ND&S 手順がどのような動きをするものであれ、完了できる。

さらに、上記で紹介したチャネルプランは、端末が最初に、一つのサービスエリアに入ったときに、あるいは、別のサービスエリアから移動して当該サービスエリアに入ったときに実行されるものであって、場合によってはネットワークエントリの完了までに相当の時間を要す場合も考えられる。しかし、一度でもそのサービスエリアでのネットワークエントリが成功すると、端末はこの成功体験のコンフィグを記憶し、次回からは本コンフィグ情報に基づいてネットワークエントリを試みることが推奨されている。その結果、ネットワークエントリ時間は短縮される。

3.2.2 初期レンジング

初期レンジングでは、一つの BS 配下にある複数の端末がこれにアクセスしようとしている場合、BS はそれらの端末に競合を許し、アップリンク内の初期レンジング用共通スロットを使用させ、接続要求を送信するチャンスを与える。初期レンジングが完了すると、ネットワークにアクセスしようとする端末は適切なパラメタ(同期タイミングオフセット、周波数偏差、送信電力レベル)を得て、BS と通信することが可能となる。

① 端末はダウンリンクサブフレーム上のフレーム開始プリアンブルを受信し、同期タイミングを見つけ、周波数偏差を修正する。少なくとも一つの DL-MAP(ダウンリンクマップ)メッセジを受信・識別したとき、端末は MAC 層の同期がとれたという。次いで、UCD(アップリンクチャネル識別子)メッセジ読み取って、アップリンクチャネルの内容を知る。

② 次いで、端末は UL-MAP(アップリンクマップ)メッセジを読み、初期レンジング用のメッセジを送出することのできるアップリンクに割り当てられた競合スロットの期間（位置）を知る。また、DCD(ダウンリンクチャネル識別子)メッセジから BS の現送信出力と最大受信電力を知り、これと自身で測定した BS の受信信号電力値とを用いて、最大の送信電力レベルを決める。

③ 端末は､当該期間内に初期レンジング用にランダムに選択した CDMA コードを送信する。BS は、たとい、複数の端末が同一の競合スロットの期間に CDMA コードを送信しても、それらのコードの直交性によって、複数の端末からのレンジング要求を識別することができる。BS はその後、RNG-RSP(レンジング応答)メッセジによってタイミングや周波数、送信電力の修正値を連絡し、引き続いて UL-MAP メッセジによって、端末が RNG-REQ(レンジング要求)メッセジを送出するためのバンド幅の割当てを行う。

③　BS は上記の割り当てられたバンドで RNG-REQ メッセージを受信すると、RNG-RSP メッセージを返す。本応答メッセージには当該端末の MAC アドレス、端末に新たに割り付けられるベーシックおよびプライマリ CIDｓを含んでいる。
⑤　BS が④RNG-RSP メッセジで「成功」を返せば、初期レンジングは終了し、端末は割り付けられたベーシック CID に対応するバンド位置で、次節に記す SBC-REQ メッセジを送信することができる。他方、BS が「継続」を返すと、端末はタイミングや周波数、送信電力を変更して、割り付けられた本ベーシック CID に対応するバンド位置で RNG-REQ メッセジを送信し、初期レンジングをやり直す。

3.2.3 通信基礎能力の交渉

ここでは、端末が BS に対してサポートしている通信能力に関するパラメタを呈示して提案する。これに対して、BS が受け入れ可能なパラメタを返答する。
①　端末は SBC-REQ(端末基礎能力要求)メッセジに端末基礎能力を示すパラメタを付加して送出する。主なパラメタを次に示す。
-　物理層パラメタ　各変調方式に対応した最大送信出力。この SBC-REQ メッセジを運ぶ送信バーストの現送信出力。動作可能復調機能（64QAM、CTC(ｺﾝﾎﾞﾘｭｰｼｮﾅﾙﾀｰﾎﾞｺｰﾄﾞ)、BTC(ﾌﾞﾛｯｸﾀｰﾎﾞｺｰﾃﾞｨﾝｸﾞ)、STC(ｽﾍﾟｰｽﾀｲﾑｺｰﾄﾞ)、AAS(適応ｱﾝﾃﾅｼｽﾃﾑ)）。動作可能変調機能（64QAM、CTC、BTC、サブチャネライゼイション）。FFT サイズ。サブキャリア順序交換機能。MIMO 機能パラメタ。AAS 機能パラメタ。セキュリティ機能パラメタ。パワー制御機能パラメタ。省電力機能パラメタ。ハンドオーバ機能パラメタ。
②　BS は SBC-RES(端末基礎能力応答)メッセジに、端末が提案した端末基礎能力を示すパラメタのうちから同意できるパラメタを記入して送出する。
交渉が必須であるセキュリティパラメタは、PKM バージョン、PKMv2 セキュリティ能力、およびオーサラゼイションポリシ(デバイス認証をサポートするかどうか、およびその要求条件)である（[Stg2-2]7.3.8.1 PKMv2 Procedure During Initial Network Entry(1) b)）。

3.2.4 認証とトラフィック暗号鍵（TEKs）の確立

通信基礎能力の交渉が成功裏に終わると、BS は ASN-GW に存するオセンティケタに無線リンクの確立を伝える。すると、BS は、オセンティケタから指示を受け、PKMv2-RES メッセジに EAP-REQ/Id パラメタを載せて、端末に対して EAP による認証を要求することで、EAP 手順を開始する（[Stg2-2]7.3.8.1 PKMv2 Procedure During Initial Network Entry (1) 最終パラグラフ）。本手順は、端末とホーム AAA 間で EAP 方式による認証が実施され、その結果が出力され、BS が端末に PKMv2-RES（EAP-Success パラメタ）メッセジを返すと終了する。
その後、TEK を生成・所有するため、まず、端末と BS が同一の有効な AK(認証キー)を所有

していること（SA が確立していること）を三段握手によって確認する。次に、端末は BS に対して、上り下り方向それぞれの SA について、二つの TEKs を生成して送付するよう要求する。

以上のように、端末のオーサラゼイションとは、BS が端末との SA を承認し、以後送受信されるデータの暗号用の TEKs を配布することである。

3.2.5 端末のネットワークへの登録

端末は REG-REQ(登録要求)メッセジを BS へ送出する。BS は REG-RES(登録応答)メッセジを返す。この会話の中で、端末は使用する IP バージョンや自動再送要求(ARQ)、MAC 誤り訂正の使用可否を申告すると共に、BS からセカンダリ管理コネクション用の CID を割り当てられる。IP 接続はこのセカンダリ管理コネクション上に開通することとなる。

さて、ここまでに登場した MAC 管理メッセジ達は、RNG-xxx、SBC-xxx、PKMv2-xxx、REG-xxx であった。これらの MAC 管理メッセジにはコネクションタイプが決められており、始めの二つのコネクションタイプはベーシック、残りの二つはプライマリ管理に分類されている。MAC 管理メッセジは、例えば「RNG-xxx」に相当する管理メッセジタイプ(1 バイト)とその内容である各種パラメタで構成される。コネクションタイプ「ベーシック」は、短ディレイが要求される MAC 管理メッセジに、「プライマリ管理」は少し長めのディレイが許容できる MAC 管理メッセジに割り当てられている。また、コネクションタイプにしたがって割り当てられる CID(コネクション識別子)の数値の範囲が決まっており、この CID 値は BS の CS(コンバージェンスサブレイヤ)が割り付ける。例えば、初期レンジング用 RNG-xxx MAC 管理メッセジでは必ず 0x0000 を使用する。

一方、本節冒頭に、IP 接続はこのセカンダリ管理コネクション上に開通すると述べた。端末のネットワークへの登録では、セカンダリ管理コネクション用 CID を BS が割り当てる。これは MAC 管理メッセジタイプを有しておらず、正確には MAC 管理メッセジではない。セカンダリ管理とユーザデータについては同種の CID 値の範囲から割り当てられる。

セカンダリ管理コネクションは、ディレイを許容することができる標準プロトコルベースのメッセジを転送するのに使用される。例えば、ネットワークへの登録終了以降に開始される DHCP、TFTP、SNMP などがある。すなわち、セカンダリ管理コネクションは IP データグラムを運んでいる。

このように、セカンダリ管理コネクションが割り当てられた端末はネットワークへの登録済みであり、管理配下の端末という。

管理配下の端末は直ちに割り当てられセカンダリ管理コネクション上に IP セッションを開始できるわけではない。どのようなセッションの品質を当該コネクション上で提供するのかというサービスフローを決定し、この識別情報(SFID)を当該セカンダリ管理コネクシ

ョンに結びつける手順が実行される。これについては [Stg2-2]7.2.1.3 Dynamic IP Configuration Setup for Fixed and Nomadic Access Scenarios 2) を参照されたい。サービスフローは QoS に関連する重要なトピックであるが、紙面の都合上、ここでは割愛する。

ここでセカンダリ管理コネクションにかかわるもう一つの留意点を述べる。
ベーシックおよびプライマリ管理コネクションを使用する MAC 管理メッセジは、レンジング、登録、その他の MAC 管理運用を円滑に処理するために暗号化されておらず、平文で送信される。(ただし、これらのうちいくつかの MAC 管理メッセジは、鍵付きメッセジ認証コード(HMAC、CMAC)を伴って完全性、真正性が確保される。) しかし、セカンダリ管理およびユーザデータの各情報が格納されるペイロードは、これらの CID に紐づいた SA に含まれる TEK によって暗号化される。このペイロードの前に付加した MAC ヘッダ(6 バイト)と、後ろに付加した CRC(誤りチェック　4 バイト)を合わせて、MAC PDU(ﾒﾃﾞｨｱｱｸｾｽｺﾝﾄﾛｰﾙﾚｲﾔﾌﾟﾛﾄｺﾙﾃﾞｰﾀﾕﾆｯﾄ)という。暗号化されているか、されていないかは、MAC ヘッダ内の EC(暗号化制御)ビットを見ることで識別できる。

3.2.6 IP アドレスの配布、取得

端末は DHCP-Discover メッセジを BS に送出する。このメッセジはホーム NSP または訪問先 NSP に存する DHCP サーバへ転送される。DHCP サーバは、DHCP-Offer メッセジに PoA(ポイントオブアタッチメント)用のグローバル IP アドレスを付して端末に返送する。次いで、端末はこの IP アドレスを HA(ホームエイジェント)に登録するために、BS に対して DHCP-Request メッセジを発する。ASN が PMIP(プロキシモバイル IP 管理)を提供していれば、PMIP クライアントは DHCP リレーから DHCP-Request を受けると、HA に対して PoA および CoA(ケアオブアドレス　当該端末をその配下に置く FA(フォーリンエイジェント)の IP アドレス)のペアを登録する。これにより、FA-HA 間のデータ転送用の MIP トンネルが設定される。登録が完了すると、DHCP リレーは PMIP クライアントから受け取った登録の結果を付して、DHCP-Request を DHCP サーバに中継する。端末は BS から DHCP-Ack を受け取る。本節の手順は、[Stg2-2]7.2.1.3 Dynamic IP Configuration Setup for Fixed and Nomadic Access Scenario、および[Stg2-2]7.8.1.8.3 Proxy-MIP Connection Setup Phase に詳しいので、参照されたい。

また、端末の移動管理の手法について 3.4 節で再び取り上げ、どのようにグローバルなインタネットからローミングが許可された端末にパケットが送り届けられるのかを説明する。

3.2.7 ネットワークエントリのまとめ

これまで概説したネットワークエントリの手順について、次の 図 3.2_5 ネットワークエントリ手順 にまとめるので参考にされたい。

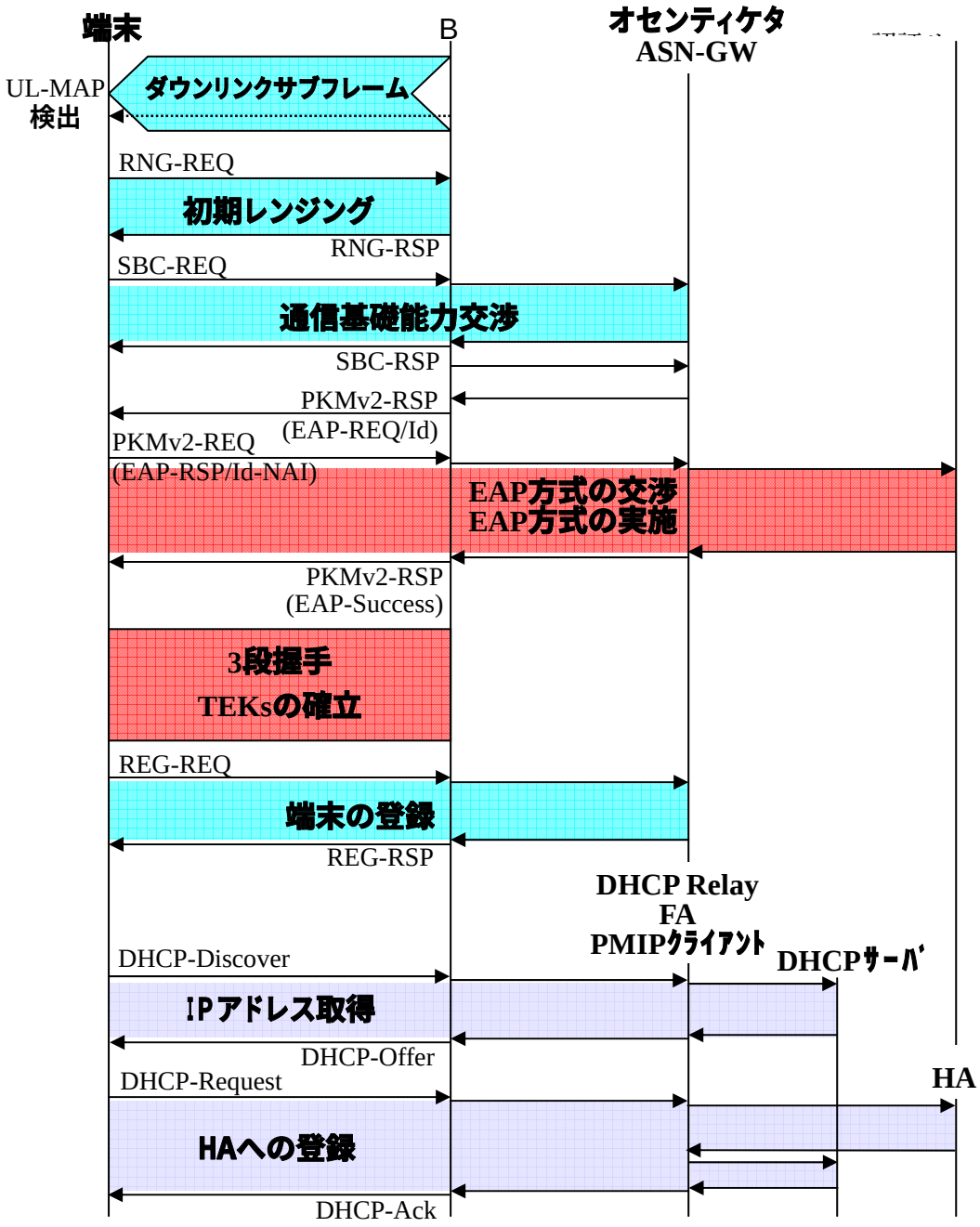


図 3.2_5 ネットワークエントリ手順

(参考: [Stg2-2] Fig7-26、[Stg3] Fig4-41)

3.3 EAP 方式――EAP-TTLS

参考: [EAP-TTLS]EAP Tunneled TLS Authentication Protocol (EAP-TTLS)

EAP-TTLS(Extensible Authentication Protocol-Tunneled Transport Layer Security)は認証をするための一つの方法、または方式である。ここでは EAP Method を EAP 方式と訳す。EAP-TTLS では、まずユーザは、今アクセスしようとしているネットワークが、自分が加入契約を結んでいる事業者に相違ないかどうかをチェックする。これは IEEE802.16e の PKMv2(プライバシキー管理 v2)としての特徴である。すなわち、IEEE802.16d ではネットワークが端末をチェックするのみであったが、モバイル WM では相互認証ができるようになった。ただし、ユーザに対して、端末のユーザインタフェイスがどのように認証結果表示をするかは、実装による。端末は相手事業者が信用できないときのみ、警告を出すようになっているかも知れない。

このユ-ザによるネットワークのチェックが成功裏に終了すると、ネットワークは端末の実在と真正性をチェックする。すなわち、当該端末に割り当てられた MAC アドレスが誤りなく端末ベンダによって書き込まれ、当該 MAC アドレスを付与された端末が今まさにネットワークにアクセスしようとして存在することである。これをデバイス認証と言う。デバイス認証は、端末側は要求されれば応じなければならないが、ネットワークがこれを行うかはオプションになっている。

以上の仕組みはセキュアなブラウザで一般的になっている https と同様の公開鍵基盤により実現される。前者の認証では、ユーザがこれから自分自身のデータを送信する宛先にあるサーバのサーバ証明書が使われる。後者の認証では、ネットワークは端末に格納されているデバイス証明書を要求する。これらの電子証明書は X.509 フォーマットによることとされ、WiMAX Forum が運用するルート認証局の下位認証局が発行することとなっている。以上の二つの認証手順は EAP-TLS でも同様に行われる。

EAP-TTLS では、さらに、NW がユーザ認証を行う。既に、ユーザは認証サーバの正当性チェックを終了した。実は、このとき認証サーバとユーザの端末との間に、https でよく知られた暗号トンネルが張られている。この暗号トンネルを介すことによって、ユーザは認証サーバとの間で、事業者(ネットワーク)と事前に共有・設定した秘密、すなわち ID/PW などを外部に盗み見られることなく、取り交わすことができる。

ユーザ認証においても、デバイス認証と同様、ユーザの実在と真正性を証明するために電子証明書を用いることが可能であるが、プリシェアドキー（事前にユーザと NW が他人に知られないように合意し、ユーザと NW が共有する ID/PW のこと。）を用いることが一般的であろう。[Stg3]4.4.1.2.3 EAP-TTLS によれば、NW、端末とも MSCHAPv2(RFC2759)の利用は必須ではないが、サポートすることが必須とされている。

ここで注意しなければならないのは、この暗号トンネルは EAP-TTLS が認証手順を終了すると解除されることである。このため、その後の無線区間に流すデータの秘匿のための暗号

用鍵やモバイル IP のセッションのセキュリティアソシエイション(SA)を確保するための鍵が生成され、認証サーバ(AAA)から所定の機能主体に配送される。(この鍵の配送はセキュアに行う必要がある。)
EAP-TTLS の産物は、正当な加入契約者であることが確認(Authentication)された後に生成される鍵 s である。これらの鍵 s を用いて、端末や NW の所要の機能主体が IP セッションを行うことを許可(Authorization)される。

3.3.1 概要

WiMAX Forum ネットワークアーキテクチャ節では、ユーザ認証を行うためには、端末、ホーム NSP ともに EAP-TTLS または EAP-AKA をサポートすることとしている([Stg3]4.4.1.2 EAP Method)。さらに、ユーザ認証に加えて、公開鍵証明書によるデバイス認証の両者を 1 回の EAP 手順内で行うデュアル認証を実施するためには、EAP-TTLS が適当であるとしている([Stg2-2]7.3.7.2.3 Executing User and Device Authentication 第 2 パラグラフ、[Stg3]4.4.1.4.1.1.2 Authenticating Subscriber and Device Credentials 第 1 パラグラフ)。

EAP-TTLS を使用する場合には、TTLS version0(IETF draft-pppext-eap-ttls-05)をサポートしなければならない。また、トンネルされる内 EAP は MSCHAPv2 を使用し、加入者クレデンシャルは ID およびパスワードを用いることとなっている([Stg3]4.4.1.2.3 EAP-TTLS 第 1 パラグラフ)。

ここでは EAP-TTLS の概要の紹介として、上記 IETF 文書「1 章 はじめに」を記載する。

拡張可能な認証プロトコル(EAP)によって、サーバは(端末や PC 内に存する)クライアントをこれらの両者が合意した認証プロトコルに基づいて認証することができる。認証プロトコルを IANA に登録すれば、EAP はその認証プロトコルを追加して使用できるようになる。

トランスポートレイヤセキュリティ(TLS)は、サーバによるクライアント認証またはクライアントおよびサーバがお互いを認証しあう相互認証を提供する。加えてサーバとクライアント間で安全な暗号化材料セットの交渉と鍵交換も提供する。TLS は EAP-TLS 内で使用する認証プロトコルとして定義されている。

広く普及している認証プロトコルは、パスワードベースのプロトコルである。これらのクレデンシャルを格納した大型のデータベースは RADIUS や Diameter、その他 AAA サーバによってアクセスされる。これらのプロトコルは非 EAP プロトコルとして、PAP、CHAP、MS-CHAP、MS-CHAPv2 があり、EAP プロトコルとして MD5 Challenge がある。

EAP-TTLS は EAP-TLS を拡張した EAP プロトコルである。EAP-TLS では TLS 握手(サーバとクライアントが公開鍵基盤に沿った手順によって信号を交換し、通信相手の真正性を確認する手順)がクライアントとサーバを相互に認証するのに用いられる。EAP-TTLS は TLS 握手によって確立した安全な接続を使用して、認証ネゴシエイション(EAP-TLS)をさらに拡張して、クライアント―サーバ間で情報を交換する。EAP-TTLS では TLS 握手は相互方向で行うことができる。または、片方向であってもよい。その場合にはサーバのみがクライアントに対して認証される。サーバは、その握手で作られた安全な接続を介して、RADIUS のような広く用いられている認証インフラを用いてクライアントを認証することができる。クライアント認証は、EAP そのものであってもよいし、PAP、CHAP、MS-CHAP、MS-CHAPv2 など、他の認証プロトコルであってもよい。

このような方法によって、EAP-TTLS では既存の認証データベースについて、レガシなパスワードベースの認証プロトコルが利用可能となっている。他方、これらのレガシプロトコルを立ち聞きや中間人等のセキュリティ攻撃から、防御もしている。

EAP-TTLS ではクライアントとサーバの両者は、クライアント―アクセスポイント(ASN-GW 内のオセンティケタ)間のデータ伝送用の接続に用いられるキー材料を作成する。キー材料は TLS 握手にもとづき、クライアント―サーバ間で非明示的に作成される。

EAP-TTLS では、クライアントとサーバは TLS 内で暗号化された属性値ペア(AVP)を用いて通信する。この一般性は認証とキー交換の他にも、AAA インフラと互換性が保たれているならば、EAP ネゴシエイションに任意の機能の追加を可能としている。

3.3.2 デバイス認証とユーザ認証

これら両認証共に、ネットワークが、そのネットワークに接続を要求しているユーザおよび／または端末が正当なもの、サービスを受けうる権利者であって、成り済まされていないかをチェックする。この認証結果に附随して、ネットワークはその後、様々な処理をすることができる。

デバイス認証結果：デバイス証明書は、WiMAX Forum の認定検査に合格した端末のみについて発行される。また当該証明書には MAC アドレス、モデル名、および製造者名が記載されている。だから、MAC アドレス、モデル名を判定することによって、当該アクセス中端末は技適を満足していない端末である、未だ取扱っていないリテール端末である、高利得アンテナ付き端末である、盗品の届けが出ている端末である等、端末の実在が確認されたからと言って、認証結果を失敗とすることもできる。

ユーザ認証結果：ユーザが保有する ID/PW とユーザ認証サーバに格納されているプリシェアドキー（ID/PW）との一致が確認されるとユーザ本人が特定される。しかし、本人を特定する加入者アカウントがあっても、その中にはサービスを制限する様々な属性が書き込まれているので、必ずしも有効なアカウントとは限らない。すなわち、認証結果を失敗とすることもできる。例えば、それら属性として、利用料金滞納（与信情報)、ブラックリストユーザ、このアカウントの有効期間、その他この事業者のユーザ管理条件などがある。また、利用サービス、サービス品質、ローミング契約の有無、課金方法など事業者が提供するサービスを制御するための属性もある。さらに、端末の属性を加入者アカウントに格納し、加入者と端末を紐付けることもできる。デバイス認証によって得た端末情報から、ひとりのユーザが複数の端末を同時に利用するシナリオも可能であるし、複数の端末のうち一台のみにセッションを制限することもできよう。

3.3.3 NAI

初期ネットワークエントリの段階にある端末は、未だ IP アドレスの割当てを受けておらず、インタネットに接続されている状態ではない。この場合、端末のホーム AAA 認証サーバを目指して EAP パケットが網内を走行する（ルーティング）ためには、EAP パケット(EAP-Response/Identity メッセジ)に NAI(Network Access Identifier)と呼ばれる識別子を書き込む。これを網内のオセンティケタ（ASN-GW に置かれる機能。NAS(Network Access Server)とも呼ばれる。）が読み取り、ホーム AAA へ向かうルートに送出する。

[Stg2-1]4.1.2 List of Identifiers によれば、NAI は次のように定義されている。
NAI はホーム事業者が WM 加入者に割り当てる。NAI は AAA 目的のための主要な ID として働く。WiMAX ネットワークでは RFC4282(The Network Access Identifier)に定義される NAI を使用する。本 RFC はローミングの際に必要な装飾 NAI を許容する。

NAI は次の形で用いる。

username@FQDN

ここで、FQDN(Fully Qualified Domain Name　完全修飾ドメイン名)は NAI のレルム部とも呼ばれる。RFC4282 4 章 IANA Considerations によれば、事業者は FQDN を IANA に登録し、ユニークな FQDN の使用権を占有しておくことがローミング管理上重要であると記載されている。
username は当該 FQDN が示すレルム内で、ユーザをユニークに決定する名前である。

EAP-TTLS では端末は NAI を指定するチャンスが 2 回ある。本 EAP 方式でどのように NAI が使用されているのか、[Stg3]4.4.1.2 Network Access Identifier および同 4.4.1.2.1 Outer-Identity を参照し、説明する。

最初に NAI が指定されるのは、端末が EAP-Request/Identity メッセジに応答し、EAP-Response/Identity メッセジに書き込まれる場合である。この NAI を outer-identity といい、ここでは外 EAPid と呼ぶこととする。また、3.3.1 節で述べたように、サーバ認証が行われた後に端末と EAP-TTLS サーバ間には暗号トンネルが形成されるが、この暗号トンネル内で EAP-Response/TTLS メッセジに書き込まれる NAI を inner-identity という。ここでは内 EAPid と呼ぶこととする。

外 EAPid のレルムはホーム AAA、すなわち TTLS サーバの宛先を示す。目的はサーバ認証である。TTLS サーバがサーバ認証を実施するためには、ユーザネイム部を必要としない。この時点で暗号トンネルは未だ形成されていないため、外 EAPid は平文のまま送信される。このため、ユーザネイムの露出を嫌い、これを擬似 ID に置き換えて送信することとなっており、この擬似 ID は端末が生成しなければならない。網側は当該擬似 ID を保存し、この擬似 ID を含む外 EAPid をその後開通するセッションを特定するのに用いる([Stg2-2]7.3.7.2.1 NAI(Network Access Identifier)第 4 パラグラフ、[Stg3]4.4.1.3.1 Outer-Identity Username:)。

一方、内 EAPid は暗号化されるから、ユーザネイム部には真の ID を設定することができる。そのため、例えば、真のユーザ ID や MAC アドレスなどを設定してよい。すなわち、内 EAPid はログイン ID のように働く。

以上のようなことから、外 EAPid はオセンティケタがそのレルム部を判断して TTLS サーバにルーティングし、内 EAPid は TTLS サーバがそのレルム部を判断してユーザネイム部を識別する、例えば MSCHAPv2 サーバ等にルーティングする。この様子を 図 3.3_1 EAP-TTLS 外 EAP 内 EAP に示す。ここで特筆すべきは、内 EAPid は必ずしもホーム AAA のドメインを宛先に含んでいなくてもかまわないことである。すなわち、事業者は、端末の種類やユーザの特定のカテゴリによって、それらを事業者の指定する認証サーバに導き、そこで最も都合のよい管理を行うことができる。

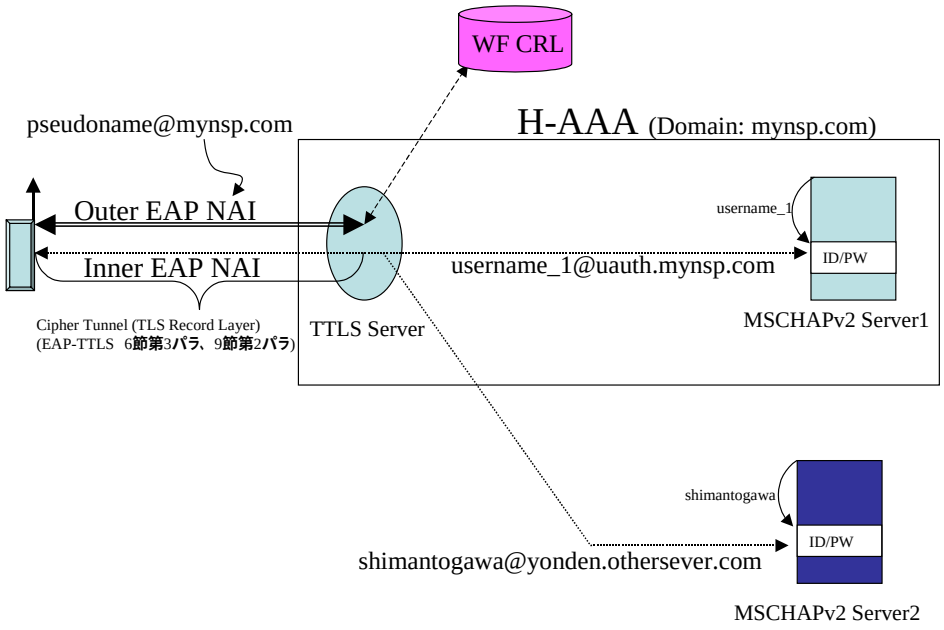


図 3.3_1 EAP-TTLS 外 EAP 内 EAP

端末が V-NSP にローミングしたときには、端末は外 EAPid をルーティングレルム部を付加し構成する必要がある。ルーティングレルム部はホームドメインを示し、ユーザネイムの左に「！」によって区切られて挿入される。NAI のレルム部には V-NSP のドメインが記入される。こうすることによって、外 EAPid は V-AAA サーバによって判断され、EAP-Response/Identity メッセジは V-AAA によって H-AAA に向かって送出される。下の 図 3.3_2 ローミングでの EAP-TTLS にローミング時の外 EAPid を示す。

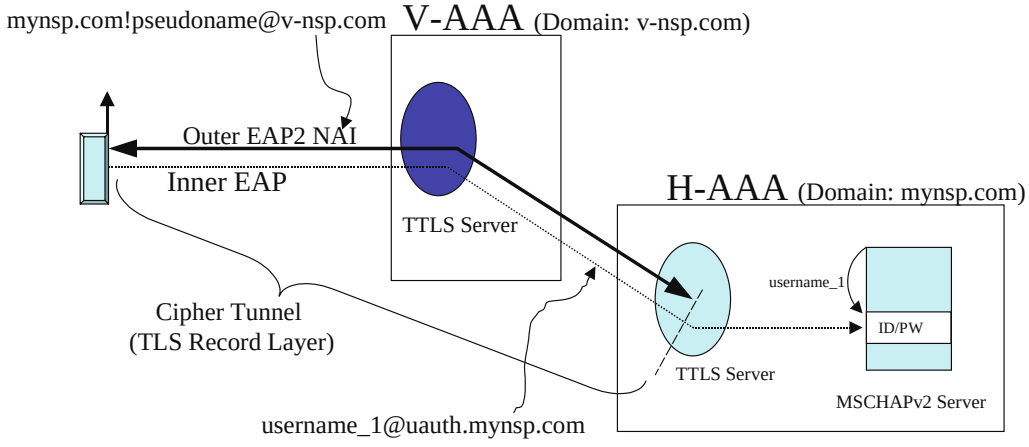


図 3.3_2 ローミングでの EAP-TTLS

3.3.4 電子証明書――サーバ証明書とデバイス証明書

WiMAX ではサーバ認証およびデバイス認証は公開鍵基盤(Public Key Infrastructure, PKI)を使用して行われる。このために WMF がオーソライズしたサーバルート認証局(Server Root CA(Certification Authority))およびデバイスルート認証局(Device Root CA)をトップの認証局とし、下位認証局を配下に置く２階層または３階層のハイアラキが採用されている。最下位のサーバ CA が AAA サーバに設定するサーバ鍵ペア（私有鍵と公開鍵）およびサーバ証明書を生成・発行する。同様に最下位のデバイス CA が端末に設定するデバイス鍵ペアおよびデバイス証明書を生成・発行する。

これらの電子証明書とその失効リスト(CRL)のフォーマットは、ITU-T が X.509 によって定めている。WiMAX フォーラムも本フォーマットを使用することとしており、公開鍵証明書(電子証明書)のことを X.509 証明書と表記することがある([PKIOverview]1.2 X.509 Certificates)。

2009 年 7 月現在、WiMAX フォーラムの証明書関連ホーム頁（http://www.wimaxforum.org/resources/pki）には、AAA サーバ向けのルート CA と端末向けのルート CA が利用可能であることが明記されており、あわせて 4 つのサーバルート CA 証明書と３つのデバイスルート CA 証明書も開示されている。この公に開示されている公開鍵の値と自身(AAA サーバまたは端末)が信用する証明書チェインのトップであるルート CA の証明書に書き込まれている公開鍵の値との一致を確認することによって、ルート CA 証明書の真正性を確かめることができる。

証明書チェインとは自分自身のサーバまたはデバイス証明書から、その上位認証局をたどり、自分自身が信用するルート CA 証明書にまで連なる公開鍵証明書に記載された証明書発行者と証明書所有者のリンクである。AAA サーバにはサーバ証明書チェインが、端末にはデバイス証明書チェインが格納され、端末がサーバ認証を行う際に、または AAA サーバがデバイス認証を行う際に、相手方に向かって送出される。

サーバ認証を行う端末は AAA サーバから受信したサーバ証明書チェインが信用できるものであるか、各公開鍵証明書の有効性を調べ、そのチェインのトップにあるサーバルート証明書が、端末が予め自身が信用するルート CA の公開鍵証明書として格納しておいたサーバルート証明書と一致するかどうかを確認する。同様に、デバイス認証を行う AAA サーバもデバイス証明書チェインの有効性と予め自身が格納しておいたデバイスルート証明書と端末から受信したデバイスルート証明書の一致を確認する。

[PKIOverview]2.1 The Certificates to be Provisioned in SSs and Servers 第 4 パラグラフ には次のように記載されている。
将来、サーバルート証明書は、この証明書の性質から、そのリスト追加(新たなサーバルート認証局が増設されること)はありそうにない。デバイスルート証明書は、そのリストが増えるかもしれない。それに伴って AAA サーバはそれら証明書が入手可能になったならば、プロビする必要がある。

下の 図 3.3_3 AAA サーバと端末にプロビされた各種公開鍵証明書 に証明書チェインとルート証明書が格納された端末と AAA サーバを模式的に示す。

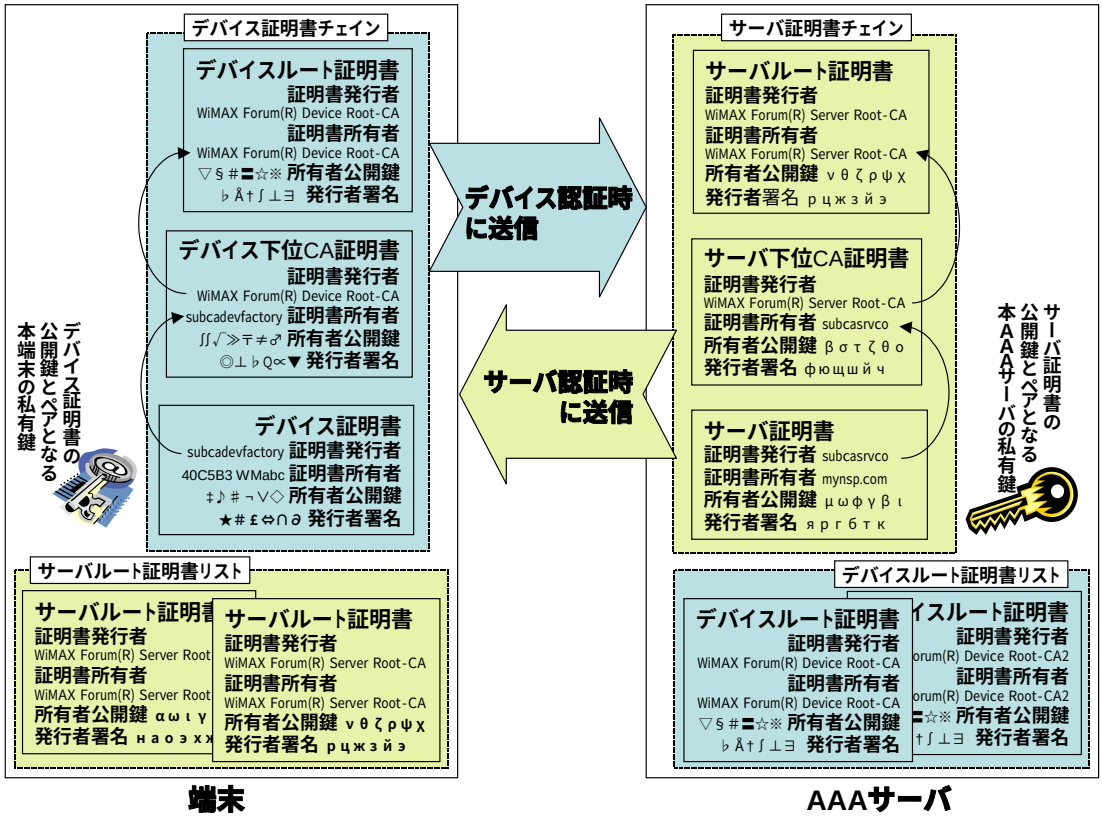


図 3.3_3　AAA サーバと端末にプロビされた各種公開鍵証明書

(参考: [PKIOverview] Fig3)

3.3.5 公開鍵証明書(電子証明書)に記載される特徴的な事項

公開鍵証明書に記載された事項は、その全ての記載事項について、その上位認証局が電子署名を施している。すなわち、当該上位認証局がその記載事項の真正性(内容の正しさと改ざんされていないこと)を保証している。公開鍵証明書を受信したエンティティは、そこに付されている電子書名をその上位認証局の公開鍵（当該上位認証局の公開鍵証明書内に記載されている）で正しく解読することができれば、その記載事項を信用することができる。公開鍵証明書に記載される主な記載事項を次の 表 3.3_1 公開鍵証明書の主な記載事項に紹介する。

表 3.3_1 公開鍵証明書の主な記載事項

(参考: [DevCert]Table5-5、[ServCert]Table5)

公開鍵証明書に共通する記載事項	
項目	意味
issuer 証明書発行者	その証明書を発行した認証局の名前
subject 証明書所有者	その証明書が発行され、対になる私有鍵を所有している端末または AAA サーバの名前
validity 証明書有効期限	有効期間が開始日付と終了日付で記載される。
SubjectPublicKeyInfo 公開鍵	RSA 公開鍵 1024 ビットまたは 2048 ビット長
SignatureValue 電子署名値	上位認証局によるこの公開鍵証明書への電子署名
サーバ証明書に特徴的な事項	
subject 証明書所有者の構成細目	
サービスプロバイダのドメインネイム	CommonName CN に設定される。この値はサービスプロバイダのレルムを含んでいなければならない。また、AAA サーバは端末から受信した NAI 内のドメインネイムとレルムとの一致をチェックする。
サービスプロバイダの名前	OrganizationName に設定される。この値は読解可能な名前であること。
NSP ID	OrganizationName に設定される。この値はサービスプロバイダの NSP ID であること。
デバイス証明書に特徴的な事項	
subject 証明書所有者の必須構成細目	
MAC アドレスおよびモデル名	CommonName CN に設定される。はじめの 12 バイトが ASCii による MAC アドレスであり、１つのスペースを置いて WiMAX Modem Model のモデル名が記載される。
製造者名	OrganizationName に設定される。値は WiMAX Modem Model の製造者名である。

3.3.6 WiMAX Forum から電子証明書の入手

サーバ証明書およびデバイス証明書を入手する方法が、[PKIOverview]3 Obtaining Certificates 以下に記載されている。これによると認証局は要求者に対して PGP を使用したセキュアメイルによって、そのメイルと添付した証明書ファイルおよび私有鍵ファイル

を暗号化し送信することとなっている。

PGP を使用するためには、要求者はまず、WiMAX Forum のウェッブサイトにアクセスして、オーサライズドユーザとしての登録をしなければならない。要求者は WiMAX Forum のメンバ会社の従業員でなければならない。次に PGP を使用する際には、要求者が認証局に届け出る PGP 公開鍵には認証局に予め登録されているオーサライズドユーザネイムと同一名が設定されていなければならない。

3.4 MIP と Simple IP

インタネットでは、端末は IP アドレスを割り当てられる。IP アドレスはこの端末が接続しているレイヤ 2 リンクを示すネットワークアドレス部と本リンク中で端末自身を示すホストアドレス部から成る。そして、端末はこのリンクに必ず接続しているものとして、グローバルインタネットから、ネットワークアドレスめがけて、IP パケットがやってくる。しかし、モバイル WiMAX 端末は、通信中にレイヤ 2 リンクに相当する BS 間をハンドオーバするので、ネットワークアドレスが通信中にも変化することとなる。こうなると、グローバルインタネットの向こうにいる相手端末は、この変化に追従して WiMAX 端末のいるネットワークアドレスを変更しないと IP セッションを維持できない。しかし、このような仕組みは実現されていない。このため、WiMAX 端末がレイヤ 2 リンクを変更しても、グローバルインタネットには、CSN と ASN が共同してあたかもネットワークアドレスの変化がなかったかのように見せかける仕組みを MIP（モバイル IP）という。一部の移動性はあきらめて、ASN 内のみでの端末のハンドオーバを行うようにした仕組みを SimpleIP という。

3.4.1 グローバルインタネットから端末へのルーティング

本節ではグローバルインタネットから、ある BS の配下にいる端末（MS）に IP パケットがどのように配送（ルーティング）されるのか、その仕組みを記述する。すなわち、MS の移動管理については触れずに、IP パケットのルーティングを与る各種データプレインがどのように接続されているのかを明きらかにする。

図 3.4_1 IP パケットの配送 に IP パケットの MS までの配送にかかわる HA(Home Agent)、FA(Foreign Agent)、BS を示し、各エンティティが当該パケットをどのようにルーティングしているかを示す。

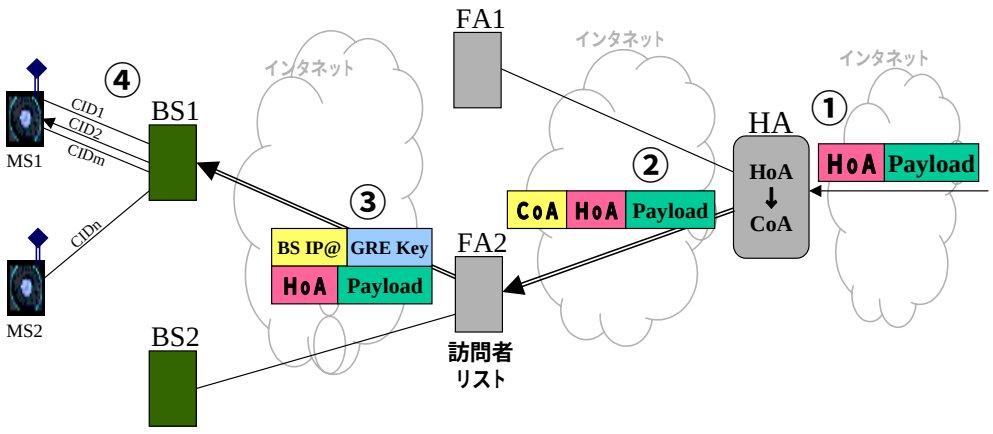


図 3.4_1 IP パケットの配送

(参考: [Stg2-2] Fig7-92)

① IP ヘッダの宛先 IP アドレスには HA 管理下のネットワークアドレスを含む HoA(MS Home Address)(PoA(Point of Attachment)とも呼ばれる。)が記述されているので、HA は、このパケットを受信する。
② HA は HoA と CoA(Care of Address　FA の IP アドレス)の対応テーブル（訪問者リスト）を参照して、このパケットを転送する先の FA を決定する。さらに、この CoA を宛先 IP アドレスとして、先に受信した IP パケットをカプセル化して、IP-in-IP トンネルで当該 FA に向かって送出する。
③ カプセル化パケットを受信した FA（ASN-GW に存する。）は、カプセルを外し、HoA を取り出す。HoA と MS ID(MS の MAC アドレス)の対応テーブルを参照し、このパケットが向かうべき MS を決定する。次いで、ASN-GW に存在する Data Path Fn（データパスファクション　R6、R4 を互るデータプレインを設定する）は、MS ID に対応した Data Path があるかどうか調べる。もし、対応する Data Path が存在すれば、この Data Path を構成する属性から GRE(Generic Routing Encapsulation)カプセル化するために必要な属性値を取り出す。GRE とは IP-in-IP トンネルの一方式である。必要な属性値とは、GRE トンネルの宛先 IP アドレス（MS を接続中のサーブ中 BS となる。)、MS あるいはこのパケットが搬送される無線区間の CID と紐付ける GRE Key(Data Path ID とも呼ばれる。)である。後者のように、CID との紐付けを要求され、サービスフローを区別する（すなわちダウンリンクコネクションの QoS を識別する）必要がある場合には、Data Path にはパケットクラス分け規則が設定されている。この場合には、Data Path Fn はオリジナルのパケットヘッダの内容を見て、このパケットを当該クラス分け規則に従って分類し GRE Key を決定する。
④ GRE カプセルを受信した BS の Data Path Fn は、その GRE Key を見て、直ちにパケットを送出すべき MS とパケットを搬送する CID を決定する。

3.4.2 Data Path Fn(データパスファンクション)

本節では上記 3.4.1 節③のデータプレインを設定するための ASN 内の MS の移動管理について触れる。

Data Path Fn とは、R4 参照点、または R6 参照点をはさみ、2 つの ASN-GW 間または ASN-GW と BS 間にトラフィックを転送するためのデータプレインを設定する。言い換えると IP パケットを転送する GRE トンネル(RFC1701 Generic Routing Encasuplation)を設定する。
ASN-GW に存する Data Path Fn はアンカ Data Path Fn と言い、MS が BS1 から BS2 へハンドオーバするとき、それぞれの BS へ接続する Data Path のアンカ点(ASN-GW 側に固定された終端点)となる。アンカ Data Path Fn は受信したパケットを BS に存するサーブ中 Data Path Fn に転送する([Stg2-2]7.7.2.2.2 Data Path Function ・Anchor DP Function)。
ASN-GW の Data Path Fn では BS に向かう Data Path を自ら設定することはできず、これを設定するための GRE Key 等を BS の Data Path Fn から予め受け取っておかなければならな

い（[Stg2-2]7.11.10.1 IP-in-IP Tunnel Protocol GRE 第 1 パラグラフ)。この手順が[Stg2-2]7.7.4.2.2 Path-Reg-Req、7.7.4.2.6 Path-Reg-Rsp、7.7.4.2.10 Path-Reg-Ack に定められている。
BS の Data Path Fn が送出する Path-Reg-Req には、主として次の情報要素が設定されている([Stg2-2]7.7.4.2.1 Information Elements conveyed with Data Path Primitives)。

-MS ID→MS の MAC アドレス
-Tunnel Endpoint→この Data Path(GRE トンネル)の宛先 IP アドレス
もし、本情報要素が設定されていないときは、Path-Reg-Req を送信した発信元 IP アドレスとする([Stg3]5.3.2.194 Tunnel Endpoint Description)。すなわち BS の IP アドレスになる。
-Data Path Info→
　＊Data Path Type→GRE
　＊Data Path ID→GRE Key
　＊Packet Classification Rule(パケットクラス分け規則)([Stg3]5.3.2.114　Packet Classification Rule/Media Flow Description(one or more))→
　　》クラス分け規則優先度
　　　》DSCP(Differentiated Services Code Point　QoS 制御のための優先度)範囲
　　》発信元 IP アドレス
　　》宛先 IP アドレス
　　》プロトコル
　　》プロトコル発信元ポート範囲
　　》プロトコル宛先ポート範囲

　パケットクラス分け規則とは、BS の Data Path Fn が CID 毎に QoS を区別したデータプレインを設定することを要求する場合に設定される。すなわち SF ID 毎にパケットクラス分け規則が BS から ASN-GW の Data Path Fn に通知される。ASN-GW の Data Path Fn はこれを参照し、これから BS へ送出する IP パケットの属性値があてはまるパケットクラス分け規則を有する GRE Key を使用して GRE トンネルを設定する([Stg2-2]7.7.2.2.2.2 Type-1 Bearer Operation、[Stg2-2]7.7.4.2.1 Information Elements conveyed with Data Path Primitives Data Path Info. List of Classifiers)。
なお、ASN-GW の Data Path Fn は、HoA と MS ID の対応テーブルから MS ID を知ることができる。このテーブルは HoA と CoA のペアを HA へ登録する MIP 登録回答を FA が受信したとき、FA で作成された訪問者リストである（[MIP]3.7.1 Configuration and Registration Tables、3.7.3.2 Forwarding Replies to the Mobile Node)。

3.4.3 FA を取り替える移動管理―MIP

参考: [MIP]RFC3344 IP Mobility Support for IPv4

本節では上記 3.4.1 節②に記述した HoA と CoA の対応テーブルがどのように作成されるのか説明し、R3 参照点を亙るデータプレインを設定するための MS の移動管理(MIP)を概説する。これによって MS、HA、FA がホームネットワーク上にいない MS に向かって IP パケットをルーティングするためにどのような動作を行うのかが分かる。

MS 内の MIP クライアントまたは ASN 内にあって MS の代理をする PMIP クライアントは、その HA へ MS のホームアドレス(HoA)と現在の位置を示す CoA を FA を介して登録する。登録によって HA は、MS の HoA を、ホーム NW ではない立ち寄り先のネットワーク（例えばローミング先のネットワークなど）を配下に有する FA のアドレス(CoA　HA から張られるトンネルの終端アドレスであって、気付けアドレスとも言う場合がある。)と一定期間（寿命)、紐付ける。これをモビリティバインディングと言う。

また FA は、MS ID、HoA、HA アドレスなどの項目を記載した前述した訪問者リストを管理する。

なお、WiMAX ネットワークアーキテクチャでは、CMIPv4 での co-located CoA(MIP クライアントが自ら取得した外部ネットワークに所属するアドレスのこと。この場合は FA が不要になる。)はサポートしないこととなっている（[Stg2-2]7.8.1.9 Client MIP R3 Mobility Management 最後のパラグラフ)。

3.4.3.1 CMIP と PMIP

CMIP(Client Mobile IP)および PMIP(Proxy Mobile IP)の両クライアントは、MIP Registration Request（登録要求）メッセジを FA 経由で HA に送信し、モビリティバインディングを要求し、その結果、HA から MIP Registration Reply（登録回答）メッセジを受信する。

モビリティバインディングのきっかけは次の三つである（[Stg2-2]7.8.1.5 CSN Anchored Mobility Management triggers)。

-MS が新たな FA 配下の新 BS にハンドオーバした。

-MS がアイドルモードに入った ASN と異なる ASN 内で起き上がった。

-MS のハンドオーバの動きと連動せずに、ASN がリソース最適化のため、R3 終端点をサーブ中 FA から新 FA に移動した。

CMIP は MS 内にあって、自ら、FA が広告する MIP Agent Advertisement（エージェント広告）メッセジから CoA を取り出し、これを MIP 登録要求メッセジに含め HA に送出する。このとき、HoA に相当する IP アドレスは未取得なので、HA から割当ててもらうことを依頼するため、自 MS を示す NAI 拡張部と HoA=0.0.0.0 と設定したホームアドレスフィールドを含める（[Stg3]4.8.3.1.3 HA Requirements 第３パラグラフ)。CMIP のモビリティバインディング

の機能構成を、図 3.4_2 CMIP 機能構成 に示す。

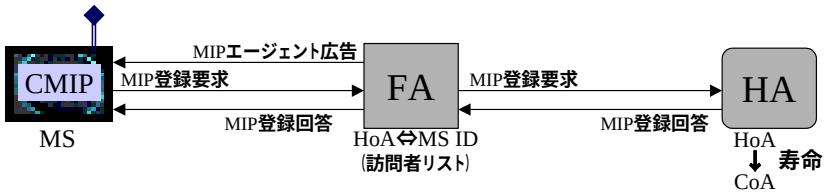


図 3.4_2 CMIP 機能構成

(参考: [Stg2-2] Fig7-102)

PMIP クライアントとは ASN-GW 内にあって、MS に代わって HoA として登録される IP アドレスを取得し、その後、CoA を含めて MIP 登録要求メッセジを HA へ送出する。PMIP クライアントは、MS についての情報を DHCP リレー機能が紐付け用のキーとして通知する MS の擬似 NAI を使用して、同じ ASN に同居するオセンティケタから得ることができる([Stg3]4.8.2.1.3 PMIP Client Requirements 第 1～4 パラグラフ)。MS 自身は IP アドレスの配布を受けるための DHCP 手順を実施するのみで足り、モビリティバインディングは実施しない。PMIP のモビリティバインディングの機能構成を、図 3.4_3 PMIP 機能構成 に示す。

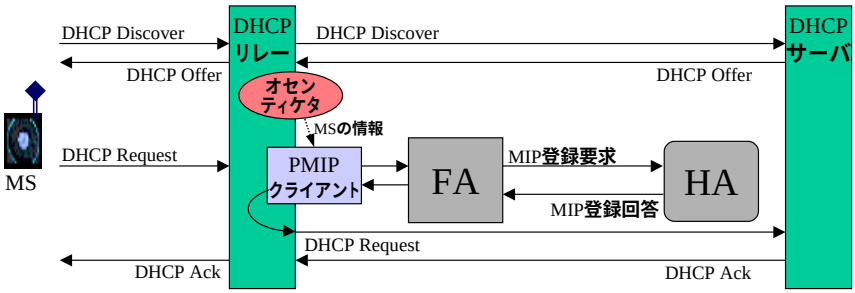


図 3.4_3 PMIP 機能構成

(参考: [Stg2-2] Fig7-94)

CMIP、PMIP とも、網側のサポートは必須である ([Stg2-2]7.8.1.2 Functional Requirements 第 9 の・)。また、本仕様では、同一端末で PMIP4 および CMIP4 を同時に使用することはサポートされない([Stg3]4.8.1 Introduction 最後のパラグラフ)。

3.4.3.2 リバーストンネリング

参考: [RevTunnel]Reverse Tunneling for Mobile IP, revised

ここまで MIP 手順による HA→FA 下り方向のトンネルの設定について解説した。

上り方向 FA→HA の逆方向トンネルについても、WiMAX ネットワークアーキテクチャでは必須の要件となっている([Stg2-2]7.8.1.2 Functional Requirements 第 3 の・)。
これは、次のセキュリティ要件に対応するためである。
一般にルータはセキュリティ上の問題（例えば、成りすまし攻撃）を回避するため、パケットを転送する際に、その宛先 IP アドレスだけを参照するのではなく、送信元 IP アドレスと宛先 IP アドレスとがトポロジ的に正当かどうかを判断している。すなわち、MS が、自身に与えられた HoA を送信元 IP アドレスとして、IP パケットを ASN からインタネット網へ送出しても、これを受信したルータが当該パケットの到着したルートとの関係において転送を許可しないかもしれない。
リバーストンネリングを用いれば、HA→FA 下り方向トンネルを通過するパケットのように、上り方向についても FA→HA 逆方向トンネルを通過させ、トポロジ的に正しい IP パケットとすることができる。

3.4.4 Simple IP

Simple IP によって IP アドレスを配布するネットワークは、MIP 手順を実施するためのネットワーク構成要素(FA、HA)を有していない。このため、CSN を固定し、R3 参照点を通過するベアラプレインを変更する、すなわち FA を取り替える管理機能(MIP)はない。
Simple IP では、網と端末は単に DHCP 手順を実施し、IP アドレス配布・取得が行われる。HCSN または VCSN には DHCP サーバが置かれる。DHCP サーバから端末が取得する IP アドレスは CSN に存するコアルータ(CR)配下の PoA になる。
Simple IP の機能構成を、図 3.4_4 Simple IP 機能構成 に示す。

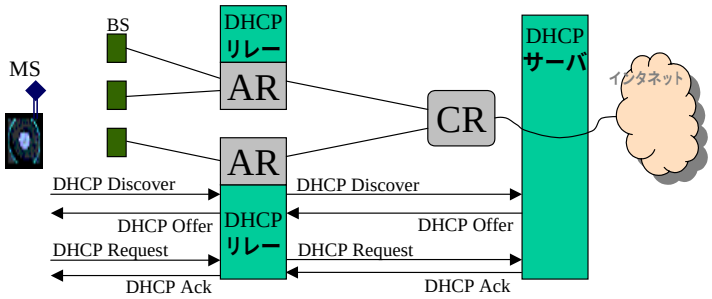


図 3.4_4 Simple IP 機能構成

この PoA は、FA の変更に応じて CoA とバインディングが行われるものではなく、コアルータ(CR)と ASN-GW 内の アクセスルータ(AR)間に、予め設けられているベアラプレイン配下の固定的な IP アドレスを示す。このため、MS は ASN-GW 内 AR を変更する移動ができない。言い換えると、Simple IP サービスではアンカ Data Path Fn は動かすことができない。アンカ Data Path Fn は MS のネットワークとの IP セッションの期間の間ずっと、MS が最初に

接続した AR 内に留まる。
それにもかかわらず MS が ASN を取り替える移動をした場合には、MS は NW 再エントリを実行する。このとき網は MS に IP アドレスを再取得するよう要求する。その IP アドレスは以前の IP アドレスとは異なる。その結果、IP セッションの継続性はなくなる。しかし、セッションの継続性を確保するため、ASN 間で R4 参照点で渡りを付けるハンドオーバをすることができる。このため、ASN はアンカ ASN と目的 ASN(新しいサーブ中 ASN)間に R4 Data Path を設定する。MS は移動性が Simple IP によってサポートされているのか、PMIP でサポートされているのか、意識する必要はない。
このような Simple IP の特徴は、収容される ASN-GW が異なる BS 間のハンドオーバトラフィックが比較的少ないと考えられる環境では、MIP による移動管理と遜色ない。WiMAX ネットワークシステムアーキテクチャ Rel 1.5 では、ネットワークは Simple IP をサポートしなければならないこととなっている。

3.4.5 MIP 登録メッセージの認証

参考: [Stg2-2]7.8.1.14 R3 Mobility Session Authentication and Authorization

モビリティバインディングを実施する MIP 管理機能にとって、MIP 登録メッセージが改ざんされていないこと、およびそのメッセジの発信元を確認することはきわめて重要である。これは第三者が成りすまして、偽の CoA をバインディングしてしまうと、その MS に係る下り方向のトラフィックが第三者の指定した不正な FA(偽 CoA)に転送されてしまうからである([MIP]5.2 Areas of Security Concern in this Protocol)。
このため MIP 登録メッセジを、AAA とオセンティケタがアクセス認証完了時に予め共有していた PMIP キーを使って認証を行う。本キーによる鍵付ハッシュ関数(HMAC Hash-based Message Authentication Code)の結果を MHAE(モバイルノードホームエージェント認証拡張)情報要素に設定し、MIP 登録メッセジに含めて送信することで、受信側は、当該メッセジ内容が改ざんされていないこと、および発信元が正当な PMIP クライアントであることをチェックすることができる。
MIP 登録メッセジの認証が行われる様子を図 3.4_5 MIP 登録メッセジの認証 に示す。

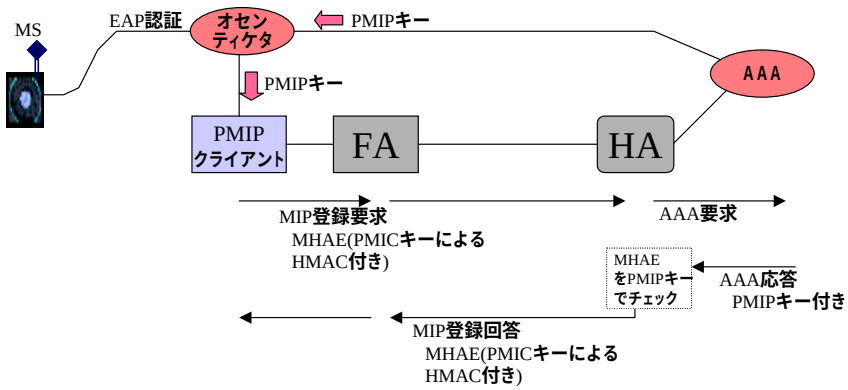


図 3.4_5 MIP 登録メッセジの認証

(参考: [Stg2-2] Fig7-110)

この図では HA が始めて登録要求メッセジを受信し、当該メッセジ NAI 拡張情報要素に記載される擬似 NAI と PMIP キーに対応した SPI(Security Parameter Index)値を AAA に呈示し、認証を受けている様子が示してある。AAA が擬似 NAI と SPI の対応を正当と判断すると、その結果、HA に対して PMIP(MN-HA)キーが返される。これを使用して登録要求メッセジの MHAE の HMAC ハッシュ値を確認することで、登録要求メッセジの認証をすることができる([Stg3]4.8.2.1.5 HA Requirements)。

以後 PMIP キーの寿命中に行われる FA の取替えでは、HA はこのキーを保存しているので、AAA の認証を行うことなく登録要求メッセジを認証する。

４．地域 WiMAX のロードマップ案（検討前）

4.1 ビジョン

地域事業者が実施する地域 WiMAX サービスは、その免許方針（審査基準）にも示されているように、

・ 地域の公共サービスの向上
・ デジタルディバイドの解消

など、地域の公共の福祉の増進に寄与することを目的に実施することとされている。

こうした地域社会の全ての住民の利便性を向上させ、目的を達成していくことは、当然、事業としての安定性や継続性も求められる。

すなわち、事業の継続した成長を図るための地域 WiMAX の「ビジョン」あるいは「ロードマップ」を持つことが重要であり、当初から目指すべき方向の議論がなされてきた。

地域 WiMAX の特徴は、地域個別のサービスでありながら、その技術標準や端末の普及予測から、将来、地域に限らないサービスに拡大すると予想されている。

したがって、ロードマップの“コンセプト”を以下のように捉えている。

（1）目指すもの

- 個々の地域事業者の成長
  - ➢ 各々の地域での成功
- 地域連携の実現
  - ➢ WiMAX 産業・市場の成功

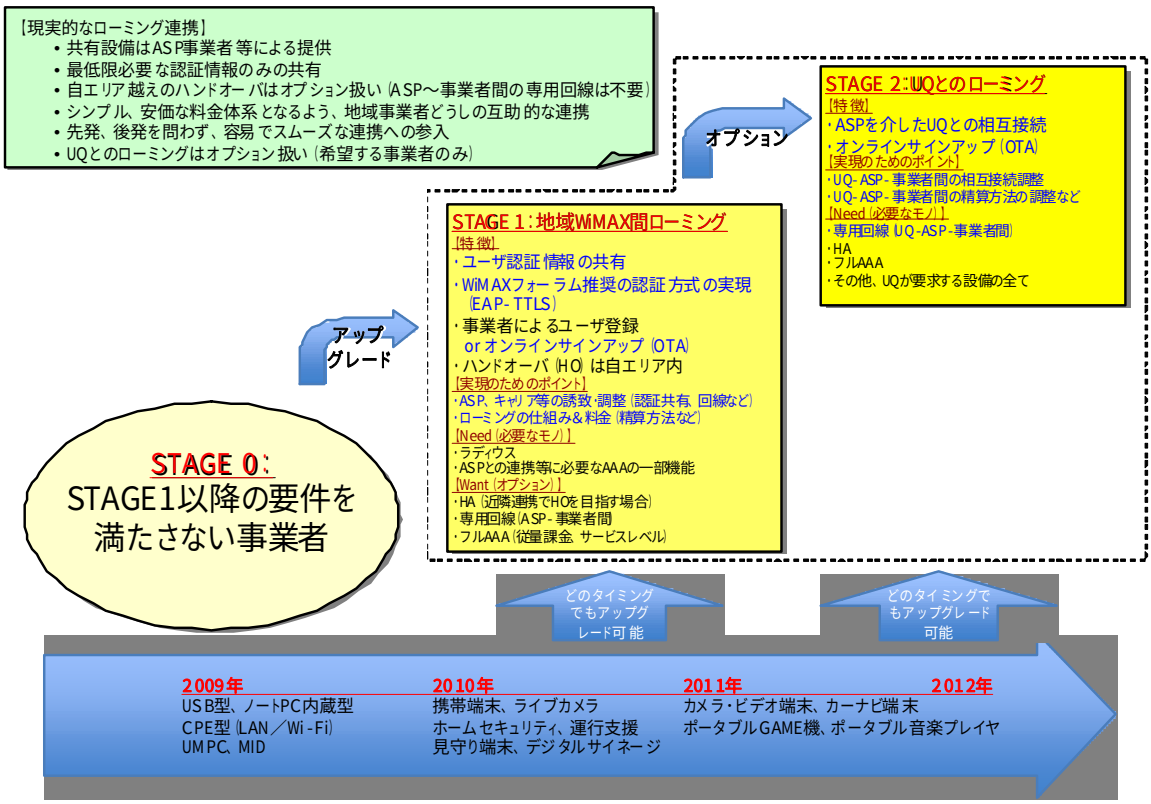
（2）実現のキー・ファクター

1st　：リテール端末のサポート
2nd　：地域連携の方法と仕組み

4.2 地域 WiMAX のロードマップ案（検討前）

前項の“コンセプト”を踏まえ、技術的な詳細検討に入る前に整理された、地域 WiMAX の「ロードマップ（ビジョン）」を図 4.2_1 に示す。

全ての地域 WiMAX 事業者が、どの STAGE からでも連携サービスに参加できることを目指した発展型ロードマップである。



※）点線内は、本ガイドラインの対象範囲

図 4.2_1 地域 WiMAX のロードマップ案

５．地域 WiMAX の共通ネットワーク･システム構成検討

5.1 はじめに

本章では、4 章で示された『地域 WiMAX のロードマップ案（将来ビジョン)』の実現を具体的に推進するために、条件・必要事項・構成・現実的可能性等について調査検討し、方向性を絞り込める材料（仕組みの共通化）を準備する。

5.2 前提条件

5.2.1 制約条件

制約条件を以下の通りとする。

- ロードマップ案で示している「リテール端末の利用」および「地域連携に向けた STAGE1/2」は、早期に立案されたものであり、十分な検討はなされていないものの、直面する問題とその解決要望がこめられている。従って、ロードマップ案の内容は最も優先順位が高いものと解釈する。
- 本検討では CSN を中心に展開するものとし、ASN 内部については検討対象外とする。既に複数ベンダの ASN システムが存在するが、ASN は１つの機能ブロックと捉え、特に ASN 内外の IOT 問題には触れないこととする。
- WiMAX によるサービス提供や運用は、WiMAX フォーラムによる推奨方式が存在するので、特に相互運用性やローミングサービスを視野に、地域連携の実現時(STAGE1 以降)では、標準方式を採用するものとする。
- 小規模の地域 WiMAX 事業者の参入障壁とならないよう、個別投資のバランスを考慮した STAGE 内容とする。
- STAGE1 へのマイグレーションを前提とした場合、STAGE0 からの移行作業（ASN パラメータ、ユーザ情報など）が現実的となるよう配慮する。

5.2.2 前提条件

前提条件を以下の通りとする。

(1) STAGE1 以降の要件を満たさないシステム（構成）【STAGE 0】

単独で ASN-CSN を構築する事業者や、既に地域事業者連携を視野に独自のネットワーク構成を構築する事業者もあるが、それらのいずれの方式についても本ガイドラインでは言及しない。

ただし、STAGE1 以降では、WiMAX フォーラムが推奨する標準ネットワークで構築されるため、現状の地域事業者は、STAGE1 への移行に支障のないような配慮が望ましい。

(2) 連携構成（ローミング実現）【STAGE 1】

実装ネットワーク	：Simple IP ネットワークを標準とし、事業者間 Hand-over はサポートしない（HA による Mobile IP 実装はオプション扱い） 事業者間の専用線接続は避ける
オンラインサインアップ	:“契約は窓口扱い”を基本としたいが、“リテール端末のサポート”を実現するため、システムとしての OTA 導入を前向きに検討する
リテール端末	：サポートする
認証方式	：EAP-TTLS をサポート、またデバイス認証も考慮する
ローミング料金精算	：H 事業者が V 事業者に支払う形態のみ想定。定額制、従量制の両方サポートを想定する
UQ との接続	：直接的な検討の対象外とするが、将来起こりうる STEP として配慮する

5.3 単独事業者構成の整理

前述のとおり、既存の地域事業者が構築しているネットワーク構成については本ガイドラインで言及しないが、“共通ネットワーク”を検討する上で、単独事業者としての一般的なネットワーク構成を理解することは重要である。

したがって本項では、WiMAX 標準とされる CSN 構成を概観し、地域事業者として想定される CSN システムの推奨機能について確認する。

(1) CSN の提供機能

WiMAX フォーラムでは、標準的な CSN として次の機能を想定している。

- MS が IP 通信の為に必要なセッションを確立するための IP アドレスと各種パラメータの割り当て
- インターネット接続
- AAA プロキシーサーバまたは AAA サーバ
- 加入者の特性（プロファイル）に準じたアクセス制御
- ASN-GW との連携（トンネリング）
- 加入者への課金や事業者間の請求処理
- ローミングの為の事業者（CSN）間の連携（トンネリング）
- ASN 間の移動管理（モビリティ）
- その他付随サービス
  - P2P、IP マルチメディア通信（VoIP)、プロビジョニング、履歴・・・

（2） CSN 提供機能とハードウェアの関係

CSN の基本機能と、それらを構成する各ハードウェアの関係を分かりやすくするために、以下のように整理した。

[DHCP]

IP アドレス払い出し

実機イメージ：DHCP サーバ

[AAA]

利用者や端末、サービスの認証・管理

実機イメージ：RADIUS サーバ

なお以後、特に指示のない限り、AAA＝RADIUS サーバとして扱う

[PF]（ポリシー･ファンクション）

利用者プロファイルに基づいた管理

QOS 等を意識したサービス

実機イメージ：RADIUS サーバ

==========

[(HA)] ※）5.2.2 項前提条件から、オプション扱いとする

モビリティ管理とローミング

実機イメージ：IP ルータ

[(Billing)] ※）各社各様、定額制/従量制の選択にもよる

利用者の課金と決済

既存の課金の仕組みと連携

実機イメージ：サーバ

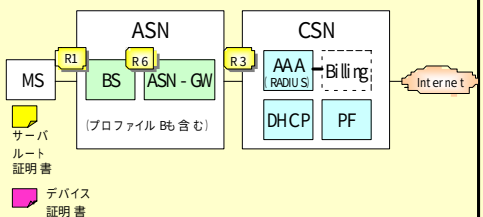
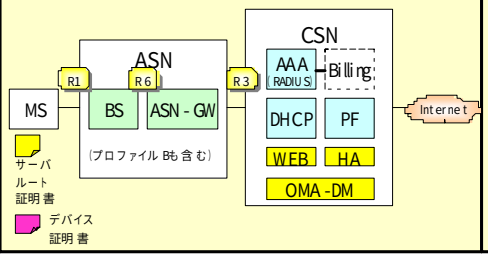
（3）地域向け CSN システムの推奨機能

5.2.2 項『前提条件』も含め、地域事業者が AAA サーバ等を設置して運用する一般的な CSN システムの推奨機能をまとめた。表 5.3_1 に示す。

『Home Agent』、『OMA-DM（OTA によるオンライン・サインアップ等を提供するシステム）』を組み合わせた WiMAX フォーラム標準システムについても参考として示した。

ただし、リテール端末を本格的に採用する場合、現状では CSN に『OMA-DM システム』が必要となる。

表 5.3_1 地域向け CSN システムの推奨機能

方　式	構　成	CSNの主要機能	ユーザ操作
AAA with EAP-TTLS認証 ※）デバイス認証を含む		• EAP-TTLS認証＋X.509サーバ証明＋X.509デバイス証明 • IPアドレスの割り当て • ユーザ毎のサービスレベル - up/downlink flow単位 • 課金情報(ASN-GWから収集) - Mobile IP、DHCP、ICMPなど管理パケットのカウント - Acct-In/output ～大容量のパケットカウントを扱える	•ユーザID/パスワードの手入力が必要な場合と不要な場合がある
【参考】 AAA with EAP-TTLS認証 ＋ Home Agent ＋ OMA-DM		• 上記の機能プラス・・・ • ASN間の移動管理 • Mobile IP関連の情報管理 - Home Agent AddressのFAへの通知 - Mobile IP関連の暗号鍵の生成や転送 • オンライン・サインアップ	•ユーザID/パスワードの入力不要 •Webポータルによるオンライン・サインアップ

5.4　リテール端末の検討

地域事業者が目指す地域 WiMAX サービスのビジョンとして、市場に出回る WiMAX 端末を利用者が安価に入手でき、事業者はその利用者に対して容易に確実にサービスを提供できるオープンな環境が望まれている。

リテール端末（市販端末）のサポートは、こうした環境の提供には不可欠となるが、前述のとおり、それを実現する仕組みとして CSN に『OMA-DM システム』が必要である。

ここでは、日本国内で事実上のリテール端末をサービスに取り扱う UQ コミュニケーションズ株式会社（UQ）が採用する端末ベンダ･メーカ数社へのヒアリング結果を示すと共に、そこから見えてくる地域向けリテール端末の未来像について整理する。

なおリテール端末とは、正しくは“特定の事業者情報等を書き込んでおらず、どの事業者とも契約･接続の可能な端末、いわゆる『白ロム端末』”を指すものであり、特定の事業者に紐付けされたり、あるいは利用者情報が書き込まれたコントロール端末、いわゆる『黒ロム端末』とは区別されるものである。しかしながら実際には、その中間的な（曖昧な）半リテール端末、半コントロール端末が存在する。そのため本項では、それらの端末も含め、広く“リテール端末”として扱うこととする。

5.4.1 端末の実態把握

（1） 状態と動作

リテール端末を製造するベンダ数社に、現状の作り込み（仕様、構成、制限など）についてヒアリングを実施した。その結果を表 5.4_1 に示す。

以下、ポイントを箇条書きに示す。

- このうち 1 社については、2009 年 3 月時点で既に市場に投入されており、UQ の提供する『UQ WiMAX』サービスで利用されている。
- いずれも端末ハードウェア（H/W）と接続ユーティリティ･ソフトウェア（S/W）の組合せで動作する。
- いずれも OMA-DM をサポートする EAP-TTLS 認証＋デバイス認証であり、S/W 上で『ユーザ認証情報』等を入力する仕組みはない。
- 2009 年 6 月末までの『UQ WiMAX（お試し期間)』サービスでは、リテール端末はコントロール端末化されて利用されている。つまり、ユーザ認証情報まで H/W に書き込まれている。
- 周波数スキャンについては、必ずしも地域バンドをスキャンさせない仕様とはなっていない。

（2） 動作要件

現在のリテール端末の仕様では、WiMAX システムで扱うために以下に示す条件を満たす必要がある。

- オンラインでプロビジョニングを実現する OMA-DM システムの設置。ただし、ユーザ情報を書込み済みで出荷される場合は、OMA-DM システムは必須とならない。
- EAP-TTLS 認証＋デバイス認証を組み合わせた、UQ と同等のネットワーク・エントリ手順を実現する仕組み。

表 5.4_1 WiMAX リテール端末メーカ・ベンダへのヒアリング結果

各社方式 / 比較項目	A社 製品化：今後予定	B社 製品化：済み（提供中）	C社 製品化：今後予定
端末のタイプ	USBドングル型	USBドングル型	ノートPC内蔵型
準拠	IEEE802.16e-2005 Wave2	IEEE802.16e-2005 Wave2	IEEE802.16e-2005 Wave2
認証方式	EAP-TTLS＋デバイス認証	EAP-TTLS＋デバイス認証	EAP-TTLS＋デバイス認証
使用周波数帯	2.49GHz～2.69GHz （2587/2600/2610/2620）	2.49GHz～2.69GHz （2600/2610/2620）	2.49GHz～2.69GHz （2587/2600/2610/2620）
対応OS	Win XP/Vista	Win XP/Vista	Win XP/Vista
システム構成	端末H/W コネクションマネージャS/W	端末H/W コネクションユーティリティS/W	内蔵チップセットH/W コンフィグレーションユーティリティS/W
S/Wの操作	ユーザで可能（接続/切断）	ユーザで可能（接続/切断）	ユーザで可能（接続/切断）
S/Wへの情報入力	不可（ユーザID/PWDなど）	不可（ユーザID/PWDなど）	不可（ユーザID/PWDなど）
H/WとS/Wの関係（役割分担）	H/Wは最小構成 S/W側で差異を吸収	H/Wは最小構成 S/W側で差異を吸収	H/Wは最小構成 S/W側で差異を吸収
S/Wの修正の容易さ	比較的容易	比較的容易	比較的容易
周波数スキャン・ロック	なし（地域バンドで利用可）	あり（地域バンドで利用不可）	なし（地域バンドで利用可）
その他	－	・現状のUQ WiMAXサービス（お試し期間中）では、コントロール端末として提供（ユーザ認証情報を書込み済）	・17社との提携（報道発表済み） ・当面はコネクションユーティリティが改変なく使われる見込み

※）2009年3月末時点でのヒアリング結果に基づく

表 5.4_2 リテール端末を地域 WiMAX で扱うための対策案

対策案 / 項　目	① S/Wの修正 （H/Wはオリジナルのまま）	② 認証情報を工場出荷前に書込み （コントロール端末化）	③ オリジナルのまま （NSP IDのみ追加）
内　容	・ユーザ認証（EAP-TTLS）で、ユーザID/PWD等の手入力ができるようにする ・地域バンドの周波数を優先スキャンするようにする	・あらかじめユーザ認証情報を端末に書き込んでもらう（コントロール端末化） ・地域バンドの周波数を優先スキャンするようにする	・地域事業者のNSP IDのみS/W側に書き込んでもらう ・地域バンドの周波数を優先スキャンするようにする
有効な接続・認証方式	STAGE 0 から	STAGE 0 から	STAGE 1 以降：地域連携システム
NAP ID	・全ての地域事業者のNAP IDを端末側で保持する必要あり ・ローミング時も同様に必要	・全ての地域事業者のNAP IDを端末側で保持する必要あり ・ローミング時も同様に必要	・全ての地域事業者のNAP IDを端末側で保持する必要あり ・ローミング時も同様に必要
実現性	△ 難しい？ （S/Wの変更対応について端末ベンダとの調整が必要）	○ 可能性あり （複数事業者の情報を事前登録する必要がある）	○近い将来 （地域連携時の共通CSNで実現）

5.4.2 地域向けリテール端末の方向性

（1） リテール端末化

完全なリテール端末を扱うことは“フル CSN”を持つことと等価であり、個別の地域事業者にとって現実的ではない。

一方で、端末ベンダへのヒアリング結果から、工場出荷前の端末へのユーザ情報の書き込み（コントロール端末化）や S/W の軽微な変更については、「比較的容易」あるいは「H/W の変更よりは対応しやすい」といった可能性が見えている。

ここでは、そうした可能性を考慮して、個別の地域事業者の WiMAX システムでリテール端末を扱えるようにするための、具体的な対策案を整理した。その結果を表 5.4_2 に示す。

①の方法は、地域事業者にとって自由度の高い方式ではあるが、UQ 向けに最適化された仕様と作り込みのため、ユーザ認証のインタフェース変更等で端末ベンダの了解が得られるのか課題が残る。

②の方法は、地域事業者にとって選択の自由度は狭まるものの、元々の端末仕様にほとんど手を加えることなく、地域 WiMAX でも扱える可能性がある。ただし、事前に決めるべきことが多く、端末ベンダとの調整が必要である。

③の方式は、リテール端末にほとんど手を加えない方法であり、地域連携が実現する STAGE 1 以降を想定している。この方式③が地域 WiMAX でのリテール端末を示すものとなるが、完全なリテール端末の扱いを目指すには、まだ解決すべき課題も多い。

以上のことから、地域事業者のリテール端末への取り組みは、現状の UQ 向け端末を事実上のリテール端末と捉えれば、先ずは“コントロール端末”でスタートし、将来的に“リテール端末化”を果たしていくステップが現実解であるとみる。

（2） オペレータ ID の扱い

オペレータ ID（NAP ID）は、基本的に各々の地域事業者ごとに取得する必要がある。一方で、“事業者フリーのリテール端末”としてローミングサービスを受ける場合には、端末がローミング先の全ての地域事業者の NAP ID をあらかじめ保持すべきケースがある。（地域連携の構成にもよるが、それは後述する）

従って、NAP ID を地域事業者個別に取得するか？あるいは地域 WiMAX 用の共通 NAP ID として 1 個を取得し、それを使いまわすか？について方針を決めるべき、との意見が出ている。

これについて、複数のリテール端末メーカ・ベンダへ問合せた結果、「どちらでも対応可能。運用する地域事業者がルールを決めるのが望ましい」との意見であった。

NAP ID 取得の方針については 6 章で詳しく述べる。

5.5 連携構成検討（共用 CSN）

本項では、前項までに整理された地域事業者による単独の CSN 構成も参考に、地域事業者が発展的に地域事業者間のサービス連携を図るための『共用 CSN システム』のあり方について検討する。

ポイントは、地域事業者にとって参加しやすい仕組み、価値、コスト、サービス提供等のメリットが得られることである。

5.5.1 共用方式の条件整理

（1） 連携による地域事業者のメリット

地域事業者が、お互いに連携を図ることのメリットは何か？いま一度、明確にすることで、地域連携方式のモデル化を試みる。代表的なものを以下に示す。

- ◎リテール端末の本格的な利用が可能になる（Key Factor①）
  - 普及が見込まれるリテール端末を扱うための OMA-DM システム等の共同利用
- ◎地域事業者のサービスエリアを越えたエリアでの接続サービスの実現（Key Factor②）
  - モバイル利用者へのローミングサービス（隣町、隣県、国内、海外）
- 地域事業者単独では提供が難しいサービスの実現
  - 例） 広域・共通のコンテンツサービス、モバイル TV、IP 電話・・・
- 共同プロモーションの実現
  - 共同広告・ブランド・ロゴなどの活動が、連携サービスと密接に連動
- これまでの地域固有サービスのプレゼンスが高められる
- UQ コミュニケーションズや海外事業者とのローミングの実現
  - 集約したシステムを介しての団体交渉が有効

（2） 検討方式のモデル化

連携のメリットから導かれる“設備の共用や集約”は、まさしく『CSN の共用化』を意味する。

CSN が共通化されれば、広域で共通サービスを展開する場合にも、具体的な投入場所（=共用 CSN）が定まることとなり好都合である。

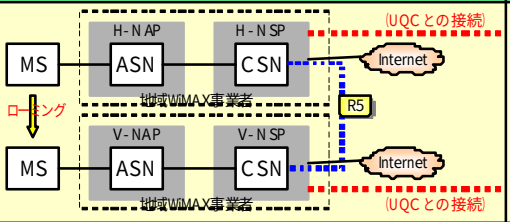
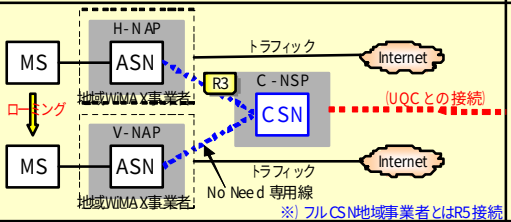
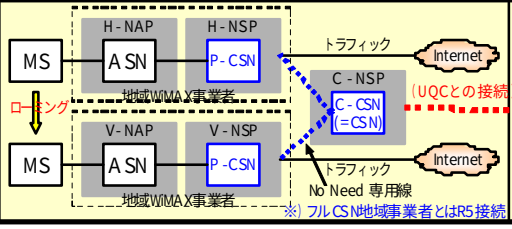
モデル化をするにあたり、フル設備を持つ WiMAX 事業者同士がローミング契約をするケースも含め、3 つの方式を取り上げることとした。

- R5 接続（参考として）
- NSP シェアリング（NAP シェアリングの変則形）
- 分散 CSN

それぞれの特徴などを表 5.5_1 に示す。

「NSP シェアリング」および「分散 CSN」の両方式とも、実現できるネットワークやサービスの姿に大差ないと考えるが、トータルコスト、運用性、移行性、実現性、参入しやすさ等、比較検討することが必要である。

表 5.5_1 共用 CSN 方式の検討

共用方式	構 成	特 徴	留意点
【参考】 R5接続		・WiMAX 事業者の標準的なローミング方式 ・全てローミング事業者同士の個別契約	・各々の事業者でフル設備が要求される（実際は、お互いのローミング合意や契約による）
NSPシェアリング （NAPシェアリングの変則形）		・地域事業者がCSNを共用する方式（共用CSN） - ユーザ認証/サービスレベル - Simple IPネットワーク ・地域事業者はASNのみの設備投資（=NAP） ・ベアラトラフィックは共用CSNを経由しない	・ユーザ情報がC-NSPで物理的に一元管理される（運用上のユーザ登録は各々で可能） ・地域連携の参加時に、自前のCSN設備は不要となる
分散CSN （P-CSN / C-CSN）		・地域事業者がCSN（C-CSN）を共用する方式（共用CSN） - Simple IPネットワーク ・ユーザ情報/サービスレベル等の個別情報を、各々のP-CSNで直接管理できる ・ベアラトラフィックは共用CSNを経由しない	・C-CSNはユーザ情報を持たず、必要の都度P-CSNに問合せる連携 ・C-CSNと連携可能なP-CSNの構築が必要 ・C-CSNとP-CSN（事業者分）全体の導入コスト・運用コストの把握

※） P-CSN：Partial-CSN, C-CSN：Common-CSN

（3） もう１つの共用モデル「ASN-GW（CSN）共用型」について

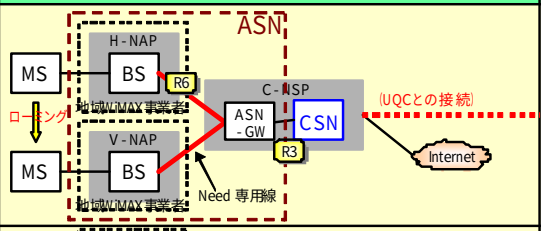
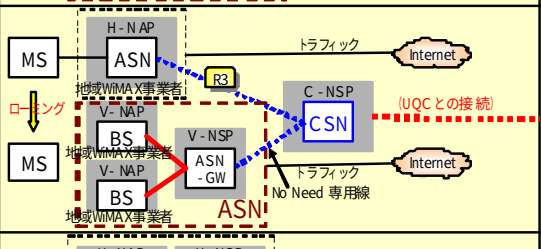
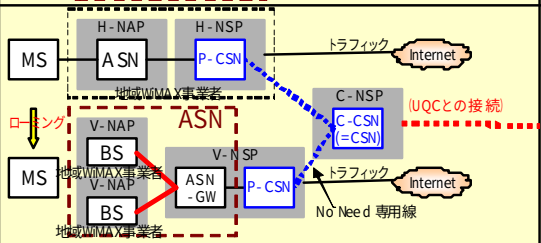
共用 CSN のモデル化においては、5.2 項『前提条件』で示している“ ASN の透過性 ”や“ 地域事業者-共用 CSN 間の専用線は不要 ”といった内容からは外れるものの、ASN-GW を複数事業者で共用するモデルも考えられる。

この『ASN-GW（CSN）共用型』方式は、各地域事業者が ASN のうち“ BS のみ ”に投資を抑えられるメリットがあり、地域単位での広域連携利用などが想定される。

反面、前述した“ ASN の透過性 ”や、今後想定される共用 CSN 事業者（C-NSP）の誘致活動における条件の明確化（ASN と CSN の水平分離）が難しくなる側面を考慮し、個別のモデル化はせず“ NSP シェアリング ”や“ 分散 CSN ”方式に包含して考えることとする。（表 5.5_2）

ただし将来、C-NSP が『“ ASN-GW（CSN）共用型 ”をサービス品目に加える」と独自判断する場合には、十分に許容されるものである。

表 5.5_2 「ASN-GW（CSN）共用型」の共用 CSN 方式における取り扱い

共用方式	構 成	共用CSNの考え方
ASN-GW（CSN）共用型		・ASNは複数メーカ・ベンダの存在を許容（多くの事業者が個別にASNを所有 することを想定） ・ASN内の「R6」におけるIOTは本 検討の対象外 ・STEP3でCSNの共用化を図る際、NSP（=CSN）側はNAP（=ASN）に対してニュートラルな 位置付け ・NSPの主な役目は、全てのNAP（=ASN）に対する共通のCSNサービス提供 ・したがって、ASN-GW（CSN）共用型は、
NSPシェアリング		1つのASNと考え NSPシェアリングに包含される ものとする
分散CSN（P-CSN / C-CSN）		1つのASNと考え 分散CSNに包含される ものとする

※） P-CSN:Partial-CSN, C-CSN:Common-CSN

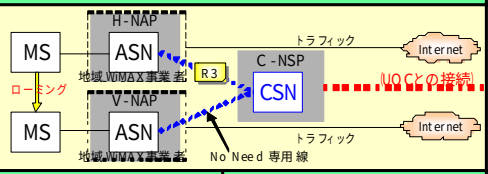
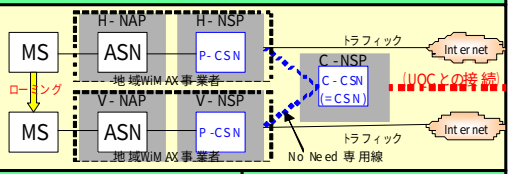
5.5.2 共用方式の比較評価

2 つの CSN 共用方式「NSP シェアリング」および「分散 CSN」について比較評価を行なった。その結果を表 5.5_3 に示す。

なお、評価における重み付けとして、地域事業者の立場に立った 4 章『ロードマップ』の方針に合わせ、次の項目を最優先事項として捉えることとしている。

- 参入のしやすさ（料金体系、運用性、回線）
- シンプルな構成（設備、料金体系など）

表 5.5_3 共用方式の比較結果

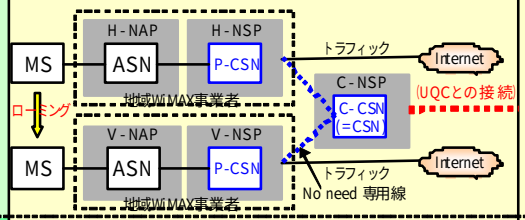
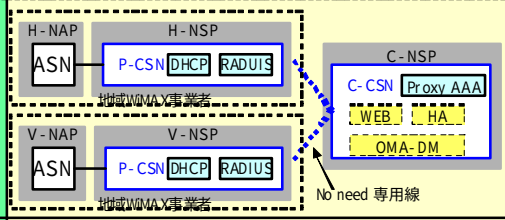
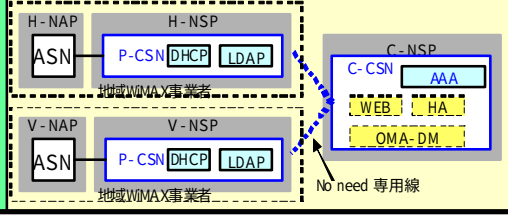
比較項目	NSPシェアリング		分散CSN	
共用方式				
	ポジティブ（＋）	ネガティブ（－）	ポジティブ（＋）	ネガティブ（－）
運用性	・分界点が明確化しやすい ・ASNのみのシンプルな運用・保守 ・ユーザ管理は、自社の顧客管理システム上で実現（その裏側で共通CSNと連携）	・ユーザ情報を直接持たず、共用CSN側に預けることとなる ・自社の顧客管理システムとのI/F調整が複雑になりやすい ・共用CSNの障害＝即サービス停止になる	・ユーザ情報を直接的に管理できる（見た目には、自社の顧客管理システム上での管理） ・顧客管理システムとのI/F調整が自社内でしやすい ・共用CSNの障害＝即サービス停止とはなりにくい	・P-CSNの扱い（どちらの所有物？）にもよるが、分界点が不明確になりやすい ・P-CSNの保守について十分な調整が必要
経済性	・CSN関連は、設備投資、運用・保守費を別途考慮する必要がない	・CSNに関連する費用は全てASPサービスとして受ける必要がある ・ASN～CSN間のトラフィックが頻繁に生じる	・P-CSN設備が地域事業者所有であれば、ASP利用料の削減が見込める ・P-CSNの機能実装によってはASN-CSN間のトラフィックを抑えられる（例えばユーザ認証はP-CSN）	・P-CSN設備投資＆運用保守費＋ASP利用料で、結果的にコスト高になる可能性もある
移行性 （STAGE 0 ⇒STAGE 1）	・共用CSNの異メーカASNへの対応状況にもよるが、移行は比較的容易（ASNのみのシンプルな管理）	・既存のCSN設備は不要となる ・端末MAC情報、ユーザ認証情報、サービスレベル情報のデータ移行が生じる	・P-CSNを共用CSNと同様にRADIUSで構築する場合、STAGE 0で既存CSN設備を流用できる可能性がある	・P-CSNが共用CSN事業者からの提供の場合、既存のCSN設備は不要となり、ユーザ認証情報等のデータ移行が生じる
実現性	・例えばASNとAAAサーバの接続の場合、広くIOTが進んでおり、多くのASNと接続可能なAAAサーバが出てきている。	・共用CSNが、異メーカのASN設備を束ねる場合、各ASNの差異を吸収する負荷が高くなる、という意見がある（共用CSN事業者の判断か？）	・異メーカのASNを共用CSNで束ねる場合、各ASNの差異をP-CSNで調整することが可能、という意見がある（共用CSN事業者の判断か？）	・P-CSNの作り込みによってはC-CSNと変わらない設備規模となる可能性もあり、若干不透明である。

※） P-CSN：Partial-CSN、C-CSN：Common-CSN

また併せて、「分散 CSN」における P-CSN の実現方法についても 2 つの方式（RADIUS、LDAP）で比較評価した結果を表 5.5_4 に示す。

共用 CSN の AAA サーバは、現状では RADIUS サーバを想定しているので、P-CSN の構築も RADIUS ベースで進めるのが適当と考える（AAA サーバについては、将来的には Diameter への移行が推奨されているが、RADIUS の是非を問うことは現時点では難しい）

表 5.5_4 分散 CSN 方式における P-CSN の検討

共用方式		構　成	機　能	メリット	デメリット	その他
分散CSN			C-CSNのAAAサーバは、RADIUSサーバを想定	–	–	–
P-CSNの方式	RADIUSサーバ		• P-CSNでのユーザデータ管理 • P-CSNでのサービスレベル管理	• RADIUS同士の通信 • 課金情報も個別に-P-CSNで収集できる • P-CSNのRADIUS冗長が容易	• ややコスト高？ • オンラインサインアップの場合は、ユーザデータの転送が発生する（初回のみ）	• 認証の判断は、P-CSNのRADIUS
	LDAPサーバ		• P-CSNでのユーザデータ管理 • P-CSNでのサービスレベル管理	• 比較的低コスト • LDAP内でユーザ情報の拡張が容易。 • WiMAXでの事例あり	• オンラインサインアップの場合は、ユーザデータの転送が発生する（初回のみ） • 課金情報をどこで管理するか？ • LDAPの冗長はやや面倒	• 認証の判断はC-CSNのAAA

※）P-CSN:Partial-CSN、C-CSN:Common-CSN

5.5.3 共用方式の方向性

今回のような比較評価で共用 CSN 方式をどちらの方式に絞り込むかは難しく、共用 CSN 設備の実装構成や他設備（ASN、顧客管理システム等）とのインタフェースの作り込み等によって大きく変わる可能性がある。例えば、AAA サーバのメーカ選定によっても、IOT 実績等で条件が変わりえる。

したがって、結論的なまとめ方をすれば、以下のようになる。

- 「共用 CSN」構成の基本的な考え方としては、「NSP シェアリング」方式とするのが、ASN（=NAP）と CSN（=NSP）の役割分担の明確化、という点においても理解しやすい。
- 一方で、共用 CSN 設備は、共用 CSN 事業者がどこまで作り込むか、つまりサービス枠をどこまで広げるかによって地域事業者への提供範囲が変わってくる。例えば、共用 CSN 事業者が「P-CSN」を提供するかどうかも、サービスの１つであると見ることができる。
- よって「分散 CSN」方式は、共用 CSN 事業者との協議、あるいは判断によって選択されるものとし、現時点での結論づけは避けたい。6 章であらためて述べることとする。

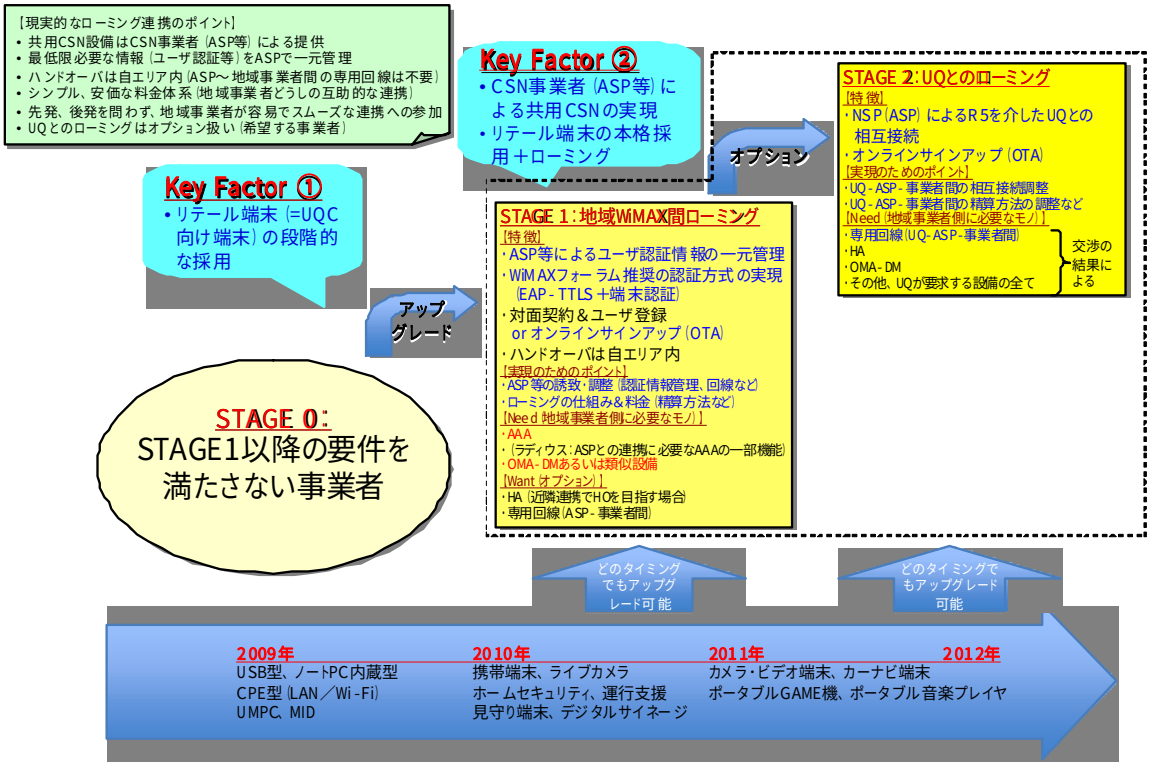
6．まとめ

6.1 ロードマップ（完成版）

5 章「システム構成検討」での検討結果をふまえ、現状のロードマップを次のとおりの内容で確定させる。

ロードマップ上に示す STAGE1/2 については、WiMAX フォーラムが推奨する標準ネットワークに準拠したシステムで構築されることを前提とする。このため STAGE 0 についても、支障のないスムーズな移行ができるシステム構築および端末利用がされていることを指針とする。

なお、STAGE1 およびそれ以降の具体的な開始時期（目標）については、今後のマスター・スケジュール調整により明確化される。



※）点線内は、本ガイドラインの対象範囲

図 6.1_1 地域 WiMAX のロードマップ

6.2 共通ネットワーク･システムの必要条件（ガイドライン）

5 章までの検討結果から、地域事業者が“共用 CSN による地域連携”サービスを実現するために必要とされる、共通ネットワーク構成のガイドラインを示す。

なお、端末 IOT の問題については、このガイドラインに沿って、今後、具体的な作業が進められる。

6.2.1 「NSP シェアリング」と「分散 CSN」

地域 WiMAX サービスを開始した地域事業者が（STAGE 0)、

- リテール端末のサポート
- 他エリアの地域事業者との接続（＝地域間ローミング）

の 2 大テーマを実現するためのステージが、ロードマップの“STAGE 1”に該当する『地域連携構成』である。

5 章での検討の結果、基本となる共用方式は、表 6.2_1 に示す『NSP シェアリング』とする。また表 6.2_2 にその詳細を示す。

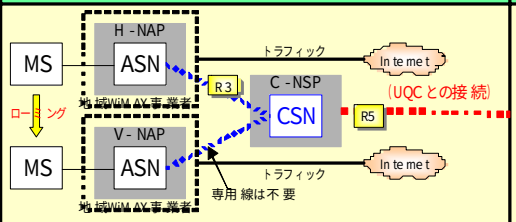
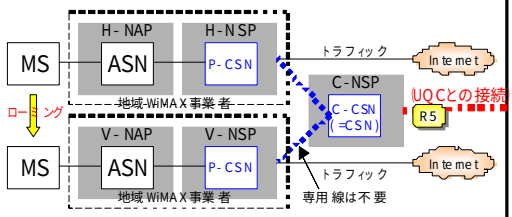
そのポイントは、以下のとおりである。

- CSN を共用設備とし（共用 CSN)、地域事業者とは別の事業者が共用 CSN を運用するモデルである。また ASN のみを運用する地域事業者に対して、ASP として CSN 機能を提供する。
- 共用 CSN 事業者には、ASP、ISP、キャリア等が想定される。
- 共用 CSN は、複数メーカ・ベンダが存在する ASN に対してニュートラルに接続し､全ての地域事業者に共通の CSN サービスを提供できることを目指す。

ただし、検討時にも触れたとおり、『分散 CSN』方式については、“R3 インタフェース”における異種メーカ･ベンダ問題の差異を吸収しやすい、という見解も示されているので、以下のように結論付けたい。

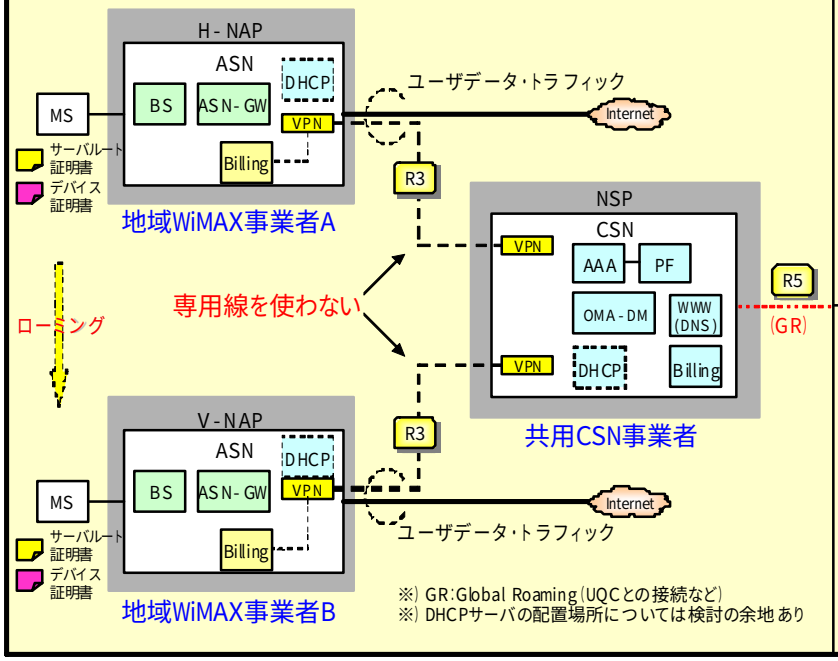
- 各々の地域事業者が P-CSN を持つ必要があるかどうかは、今後決められる予定の共用 CSN 事業者（C-NSP）の判断とする。つまり見通しとしては、ASN メーカ・ベンダによって、P-CSN が必要なケースや不要なケース、あるいは地域事業者が要・不要を決めるケースが考えられる。
- また P-CSN については、共用 CSN の AAA サーバと同様に、現状では「RADIUS」を使うのが適当と考えられるが、上記の理由により、最終的には共用 CSN 事業者の判断とする。

表 6.2_1 共用 CSN による地域連携構成時のシステム条件（STAGE 1）

共用方式	構　成	特　徴
NSPシェアリング		• 地域事業者がCSNを共用する方式（共用CSN） - ユーザ認証/サービスレベル - Simple IPネットワーク • 地域事業者はASNのみの設備投資（=NAP） • 共用CSNは、ASP、ISP、キャリア等による独立運用 • ベアラトラフィックは共用CSNを経由しない
分散CSN （P-CSN / C-CSN） 【この方式は、共用CSN事業者との調整事項とする】		• 地域事業者がCSN（C-CSN）を共用する方式（共用CSN） - Simple IPネットワーク • 「NSPシェアリング方式」の共用CSNと実質的な差はない • 地域事業者はASNに加え、P-CSNの設備投資 • ユーザ情報/サービスレベルは、各々のP-CSNで独立管理 - ユーザ認証/サービスレベル制御はP-CSN （共用CSNに対する、異種メーカ・ベンダASNの差異を吸収する目的としてP-CSNが使われる可能性もある） • 共用CSNは、ASP、ISP、キャリア等による独立運用 • ベアラトラフィックは共用CSNを経由しない

※） P-CSN：Partial-CSN、C-CSN：Common-CSN。共用CSNのAAAは、RADIUSベースを想定

表 6.2_2 NSP シェアリングの詳細（STAGE 1）

設備構成（機器配置）	詳　細
	地域WiMAX事業者 • BS • ASN-GW • （DHCPサーバ） 各々の地域事業者がベアラ・トラフィックを分担するので、DHCPの管理が想定されている • Billingサーバ（事業者の既存設備） 各地域事業者の顧客管理＆課金システムと、AAAサーバとの連携 共用CSN事業者 • AAAサーバ（　RADIUSサーバ） ユーザ認証/サービス許可/課金管理 PFを含む • OMA-DMサーバ（あるいは類似設備） リテール端末の扱うためのOTA実現 • WWWサーバ ユーザへの契約＆サービス提供 地域事業者へのBilling向け情報提供 • （DHCPサーバ） 共通CSN事業者からのIP払出しも可能

6.2.2 STAGE 0 からの移行

地域事業者が、共用 CSN 事業者の CSN サービスを受ける場合、基本的には ASN のみを所有・運用すればよいので、地域事業者が既に運用中の CSN 設備は運用を終了することとなる。

また、ユーザに紐付けられた運用中の情報（MAC アドレス情報、ユーザ認証情報、QoS サービス情報等）は、共用 CSN 側への移行を行ないたいもの、不要となるもの、既運用中の情報をそのまま地域事業者側で使用できるもの等がある。

ただし、現状の地域事業者の WiMAX 設備には複数のシステム構成が存在すると想定されるため、各々の固有な状態には触れず、共通的に関連する以下の項目について留意点を示す。

（1） ユーザ認証情報の移行

EAP-TTLSの内EAPidとして用いられるユーザ認証情報(ユーザＩD/パスワード)は、当該情報を格納するサーバとともにそのまま使用できる可能性がある。このとき、移行に伴ってサーバのドメインを変更しなければならない場合には、端末に設定する内 EAPid のドメイン名を変更する必要がある。

（2） サービスレベル（QoS）の移行

サービスレベル（QoS）については、“ベストエフォート”以外の設定は、サービス品目への積極的な利用を避けることとしたい。(推奨)

（3） EAP-TTLS に関わる「X.509 証明書」の扱い

EAP-TTLS による認証の際に使われる X.509 サーバ証明書は、WiMAX フォーラムが推奨する標準システムに準拠し、『WiMAX フォーラム サーバ CA 署名済みの証明書』へ一本化することとしたい。これは、サービスに利用する端末の標準化とも関連する。

（4） オペレータ ID の取得

オペレータ ID（NAP ID）については、各地域事業者毎に IEEE より取得することを条件としたい。これについては、詳細を後述する。

6.3 リテール端末メーカ・ベンダとの調整･交渉

6.3.1 地域 WiMAX 向け対応と運用

5.4 項でも触れたとおり、将来的なリテール端末の本格採用を目指して端末ベンダ･メーカと段階的に協力していくことは必要な作業であり、特に今後は地域事業者が扱う WiMAX 端末の標準化を整備することが重要となる。

この標準化とは、新たな端末仕様を策定することではなく、現存する WiMAX 端末の地域向け対応を運用のルール化と軽微な（追加･変更）作業で実現することである。

具体的には、5.4.2 項でも示したとおり、以下の方向性が想定される。

コントロール端末（STAGE 0 から ） ⇒ リテール端末の本格採用（STAGE 1 以降）

以下に、端末ベンダとの調整項目や地域事業者側で整備が必要な運用面でのキーポイントを示すが、詳細は今後あらためて議論されるものとする。

地域 WiMAX 向け対応

- 現 地域事業者で利用可能な、リテール端末のコントロール端末化（STAGE 0）
  - NAP-ID、NSP-ID、地域周波数スキャン、ユーザ情報、レルム･･･など
- 将来のリテール端末の本格採用（STAGE 1 以降）
  - NAP-ID、NSP-ID、地域周波数スキャン･･･など

UQ＆地域の両対応

- 地域 WiMAX 専用品ではなく、1 つの端末で UQ・地域 WiMAX のどちらにも対応可能とするための対応策
- 複数契約情報の書込み対応
  - UQ･地域 WiMAX の両契約情報を順不同で設定できるようにするための対応策

運用　その他

- 契約時の操作、登録
  - 契約時に端末を利用可能とするための操作、登録など
  - リテール端末を扱う際の初期 Web ポータル（事業者振り分け用）
- ユーザサポート
  - クレームや質問等の問合せ 1 次窓口、2 次窓口、故障対応等のフローなど
- ローミングサービス
  - 契約時の操作など（STAGE 1 以降）

6.3.2 IOT における方針と実施

リテール端末メーカ･ベンダ向けの交渉は、前項までの地域 WiMAX 側のシステム標準化、およびそれに基づく交渉の枠組みを決めることである程度進められるが、具体的な対応においては、リテール端末の IOT 問題を物理的に解決していかなければならない。

その活動は、『IOT 推進分科会』での取り組みによるところが大きく、今後は、以下の項目を踏まえて、IOT 推進分科会を支援していくことになる。

- 本ガイドライン（STAGE1/2）に沿った『地域 WiMAX 端末ガイドライン』の準備
- IOT 設備の構築
  - 地域 WiMAX 事業者で既に採用されている複数メーカ･ベンダの ASN 設備を扱える IOT テストベッドを用意し、リテール端末メーカ・ベンダの参入を促進する

6.4 オプション機能の整理

ここでは、ロードマップ上の STAGE 1 でオプション扱いとなっている以下の機能・設備について、整理する。

6.4.1 Home Agent（HA）

端末の移動管理（移動端末への IP アドレス割付）については、ロードマップ上の方針とおり、各地域事業者のエリアを単位基本としている。つまり、ASN を主体とした移動管理をサポートする Simple IP の実装を標準方式としている。

一方で、隣接する地域など複数の地域事業者エリア間でハンドオーバを実現するには、Mobile IP を実装する必要があり、CSN に HA を持つこととなる。

STEP3（共用 CSN）での Mobile IP ネットワークの提供は、以下の方針で提供されることとなる。

- 共用 CSN は、Mobile IP 環境をオプションサービスとして提供するために HA を実装
- 地域事業者は、本サービスを利用することにより、同様にオプションサービスを受ける地域事業者との間でハンドオーバを実現
- HA の導入・運用コスト負担については、オプションサービスを受けない地域事業者には発生しない

6.4.2 オンラインサインアップ

オンラインサインアップとは、OMA-DM システムによる OTA（On The Air）での契約行為を指す。

地域 WiMAX では現状、地域密着のキーファクタでもある“対面契約”を基本としているが、今後リテール端末をサポートしていくと、契約者との対面契約は非効率との見方もある。それは、リテール端末は OTA によるオンラインサインアップを基本とし、契約情報（ユーザ認証情報等）は OTA で端末に書き込まれるようになり、必ずしも対面契約の必要がなくなるからである。

このため、対面契約を維持するとしても、STAGE 1 でリテール端末を扱うためには、端末に契約情報等を別の方式（例えば、ROM ライターのような専用装置）で書き込めない限り、OMA-DM システムが必要となる。

現状 OMA-DM は高額なシステムであるため、1 地域事業者が所有するには非効率なシステムであるが、STAGE 1 における“共用 CSN システム”としての導入であれば、スケールメリットが活かした投資対効果が期待できる。ただし、その導入時期については共用 CSN システムを運用する事業者の判断によるところもある。

したがって、“オンラインサインアップ　OMA-DM（あるいは類似）システムの導入”については、リテール端末採用の実現を果たしていく中で、その実現時期の判断を、今後に選定される『共用 CSN 事業者』との協議により進めることとする。

6.4.3 課金・精算

STAGE 1 では、共用 CSN 設備を介して、リテール端末が問題なく扱えるようになり、また地域事業者間のローミングも実現される。単純な想像の範囲でも、以下のようなサービスが考えられる。

- 基本サービス:リテール端末のプロビジョニングを含む、ユーザ契約情報の管理と端末接続の提供
- ローミングサービス：地域事業者間のローミング
- Mobile IP サービス：HA を利用するオプションサービス
- UQ とのローミング：オプションサービス（6.5 項で説明）

これに加えて、STAGE 1 の要点に“ASN～共用 CSN 間を専用線接続しない”があり、これは各事業者が各々持つ上位回線を訪問者（端末）に提供する“互助的連携”がベースにある。

課金・精算の問題は、“定額制 or 従量制”も含め、仕組みの問題ではなく、取決めの問題であるため、ここでは言及せず、今後に選定される『共用 CSN 事業者』との協議により決めていくこととする。

6.5 全国 WiMAX 事業者との接続検討に向けた整理

STAGE 1による「地域連携」の実現は、

- リテール端末の正式サポート
- 地域事業者間のローミング

を同時に実現するものであり、STAGE 1の到達は地域事業者にとって必要なマイルストーンであるといえる。

一方で、全国 WiMAX 事業者とのローミングは、STAGE 1の「共用 CSN 設備」を介して実現される STAGE 2 に該当するもので、オプションサービスとしている。

これは、必ずしも全ての地域事業者が、全国 WiMAX 事業者とのローミングを希望しているわけではないこともあり、実際には希望する事業者のみに提供される、以下のようなサービスが想定される。

- 共用 CSN は、全国 WiMAX 事業者とのローミングをオプションサービスとして提供するための設備を実装。
- 地域事業者は、本サービスを利用することにより、全国 WiMAX 事業者のエリアではローミングサービスを受けることができる。
- 全国 WiMAX 事業者とのローミングに必要な導入･運用コスト負担については、オプションサービスを受けない地域事業者には発生しない。

ただし、全国 WiMAX 事業者とのローミングに必要な設備や運用ルールは現状未確定であり、これらは今後のローミング交渉によって明確化していくこととなる。

なお全国 WiMAX 事業者との交渉においては、少なくとも以下の設備について調整が必要と考えられる。

- HA：Mobile IP の実装が必要な場合
- 専用回線：“全国 WiMAX 事業者～共用 CSN ”間、および“共用 CSN～地域事業者 ”間
- OMA-DM システム：ローミングサービスにおいては基本的には不要と思われるが、運用上の必要性について要確認

また、以下のような場合の端末動作についても、事前の調整と把握が必要である。

- 全国 WiMAX 事業者エリアと地域事業者エリアが重なっているときのローミン

グ動作

- 全国 WiMAX 事業者エリアと地域事業者間ローミングエリアが重なっているときのローミング動作

6.6 オペレータ ID（NAP ID）取得のお願い

オペレータ ID（NAP ID）は、全ての地域事業者（NAP）が、各々所有の WiMAX 基地局をグローバルユニークに識別するために必要な情報（ID）であり、地域事業者毎に取得すべきものである。（なお、NAP と NSP が同一の場合はオペレータ ID に NSP ID も含まれることとなるが、ここでは NAP ID のみを対象とする）

“地域連携”の推進は、

- リテール端末の正式サポート
- 地域事業者間のローミング

の 2 つの実現を含んでいることは既に述べたが、NAP ID はこの“地域連携”にも深く関連する。つまり、

- WiMAX 端末は、端末自身が保持する NAP ID 情報に合致した基地局（BS）のみと接続できる。
- 地域事業者間のローミングでは、WiMAX 端末に全ての地域事業者の NAP ID 情報を持たせなければならない。

したがって、WiMAX 端末（リテール端末も含む）には、NAP ID 情報を更新（追加・削除）できるインタフェースが必要である。

一方で、NAP ID を全ての地域事業者で統一する『共通 NAP ID』案も考えられた。地域事業者同士は、その免許制度と物理的な制約から、サービスエリアが重ならないので、NAP ID を一本化することで利便性が向上するというものであった。しかしながら、以下の理由により採用を見送ることとした。

- リテール端末メーカ・ベンダへのヒアリングで「運用する地域事業者側のルールの問題」と特段の要望がなかったこと
- 隣接する地域事業者エリアの境界で、NAP ID が共通の場合、優先順位がつけられないため、端末が両事業者の基地局への接続・切断を頻繁に繰り返す可能性がある。（NAP ID が異なる場合は、端末が持つ NAP ID リストで優先順位を設けることができる）
- 隣接する地域事業者エリア間でハンドオーバ（Mobile IP オプションサービス）

を実現させたい場合、両事業者の NAP ID が同一だと、両事業者の WiMAX 基地局 ID（BS ID）が重ならないように、お互いに事前調整を図らなければならない。（BS ID は 48 ビットで構成されるが、その前半の 24 ビットが NAP ID となっている）

- NAP ID を使用する機能や処理が将来出てくる可能性を想定し、個別の標準化は避ける

オペレータ IP（NAP ID）は、IEEE 登録局に各地域事業者ごとに申請して取得することができる。なお申請手数料は、US$1,200 である。

【コアネットワーク検討分科会構成員】

事業者名	氏　名
株式会社テクノロジーネットワークス	湯浅 賢一
伊藤忠テクノソリューションズ株式会社	高橋　智彦
伊藤忠テクノソリューションズ株式会社	長谷川　真一
株式会社ＮＴＴＰＣコミュニケーションズ	倉持　祐一
株式会社キャッチネットワーク	林　佳紀
ＫＤＤＩ株式会社	鬼頭 達男
ケーブルテレビ無線利活用促進協議会	林　英雄
株式会社コミュニティネットワークセンター	日比野　敦
株式会社シー・ティー・ワイ	渡辺　貞和
玉島テレビ放送株式会社	金辺　重彦
徳島中央テレビ株式会社	石田　賢司
日本電気株式会社	八木　学
日本無線株式会社	小林　保
ひまわりネットワーク株式会社	大澤　博実　（分科会長）
中村　光則（株式会社フジクラ、WiMAX フォーラム日本オフィス　マーケティングワーキンググループ地域 WiMAX 担当タスクグループリーダー）	中村　光則
富士通株式会社	小野　光洋
富士通ネットワークソリューションズ株式会社	友松 聖詞
株式会社ブロードネットマックス	伴　泰次
株式会社ブロードバンド地上波デジタル総合研究所	中司　公彦
モトローラ株式会社	山崎　潤
三菱電機株式会社	杉山　直行
ＵＱコミュニケーションズ株式会社	小池　竜太
株式会社嶺南ケーブルネットワーク	西野幸二
株式会社ネイルコム	兼久　信次郎
高島　洋輔	高島　洋輔
ワイヤレス・オープン・プラットフォーム株式会社	宮町　秀恒
株式会社ベイ・コミュニケーションズ	岩崎　也寸史
レノボ・ジャパン株式会社	堀越　秀人