

モバイルネットワークを活用した モノのネットワーク

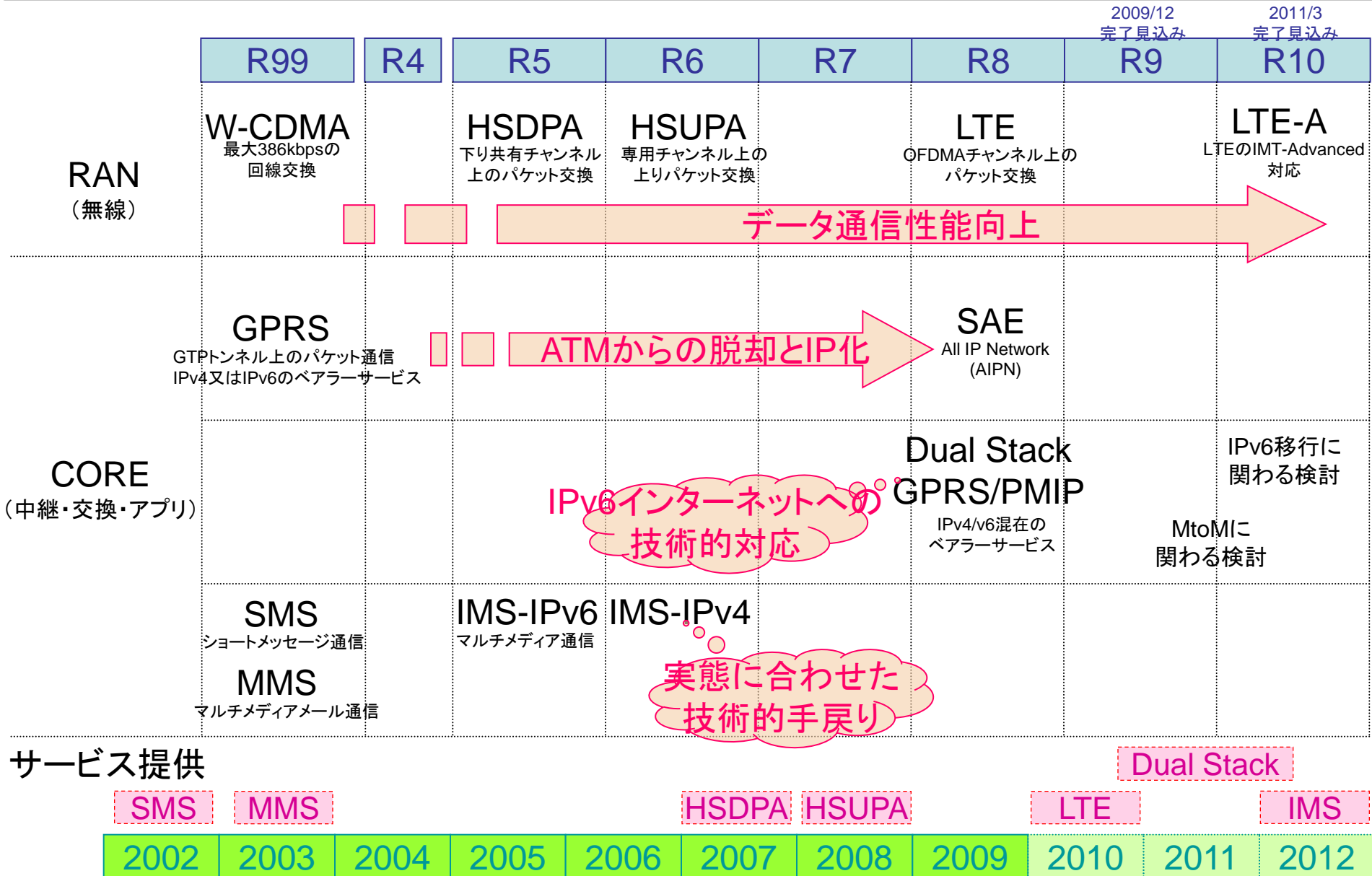
2009年10月14日

イー・モバイル株式会社

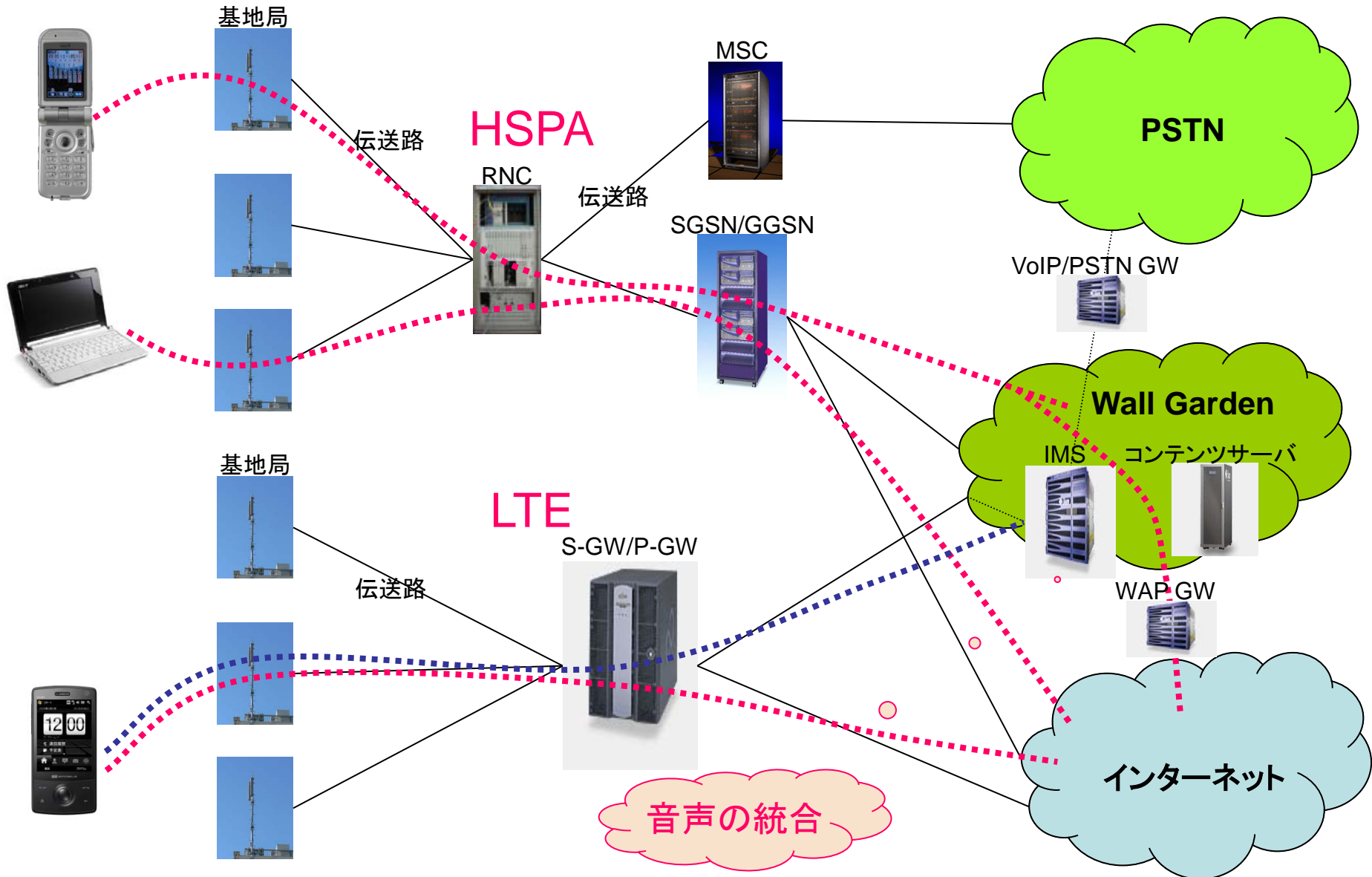
専務執行役員 小畑 至弘

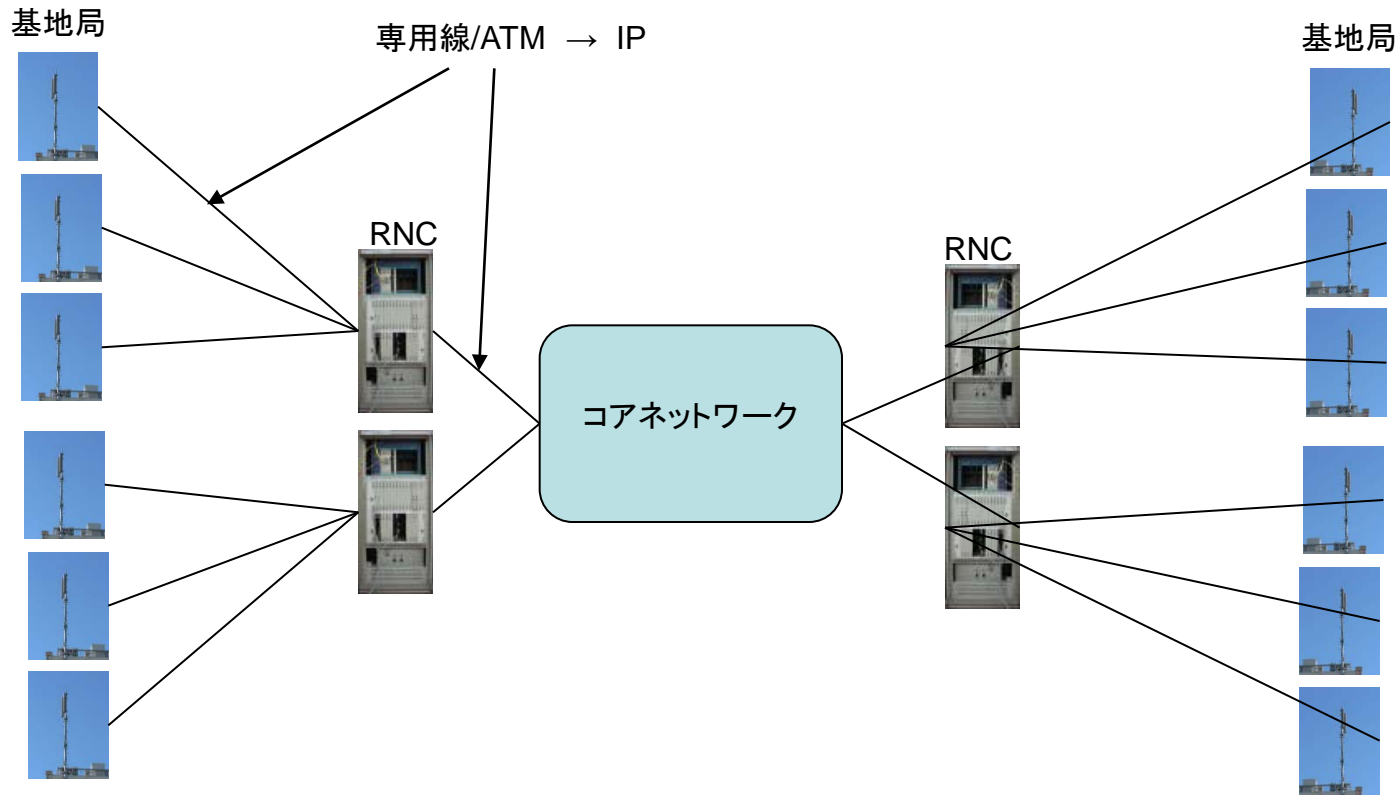
モバイルブロードバンドの技術動向

3GPPにおけるIP通信の標準化

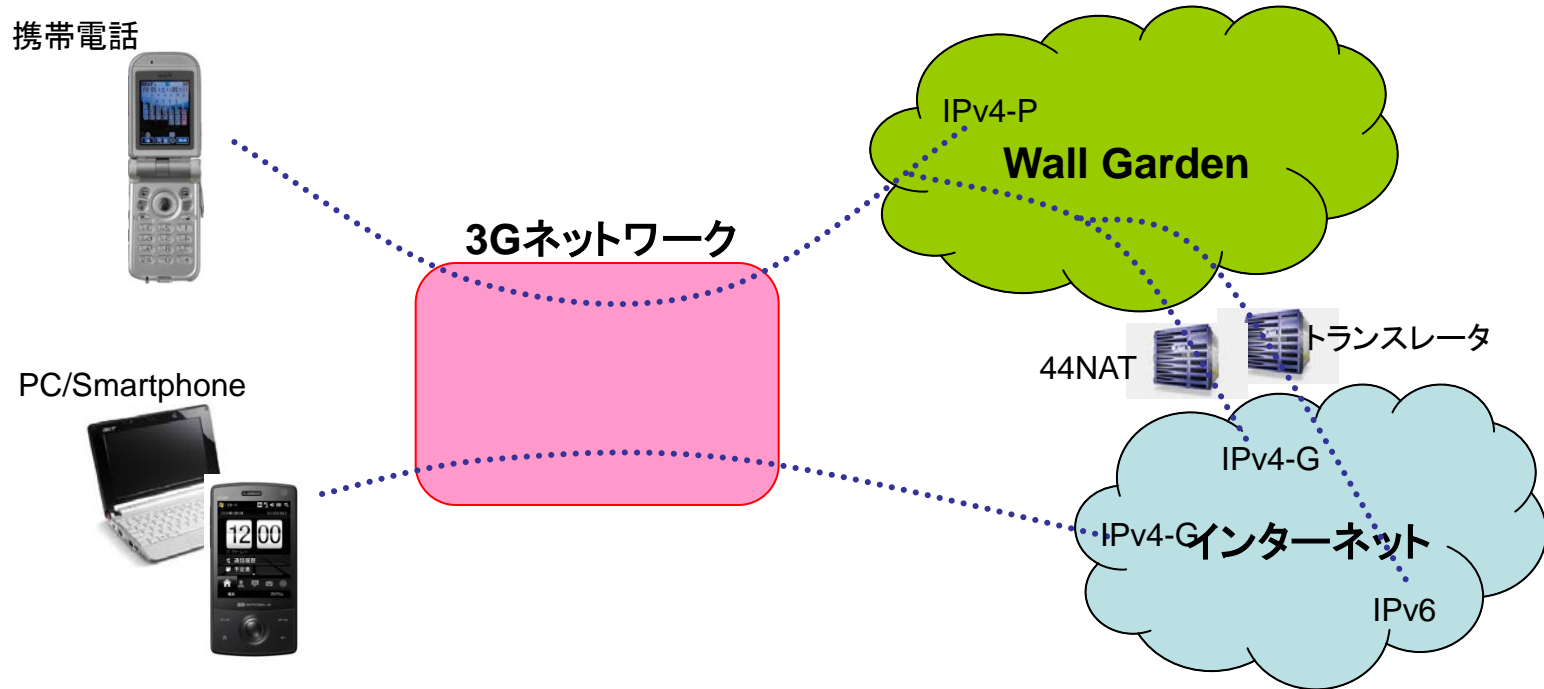


3GネットワークのアーキテクチャとIP通信



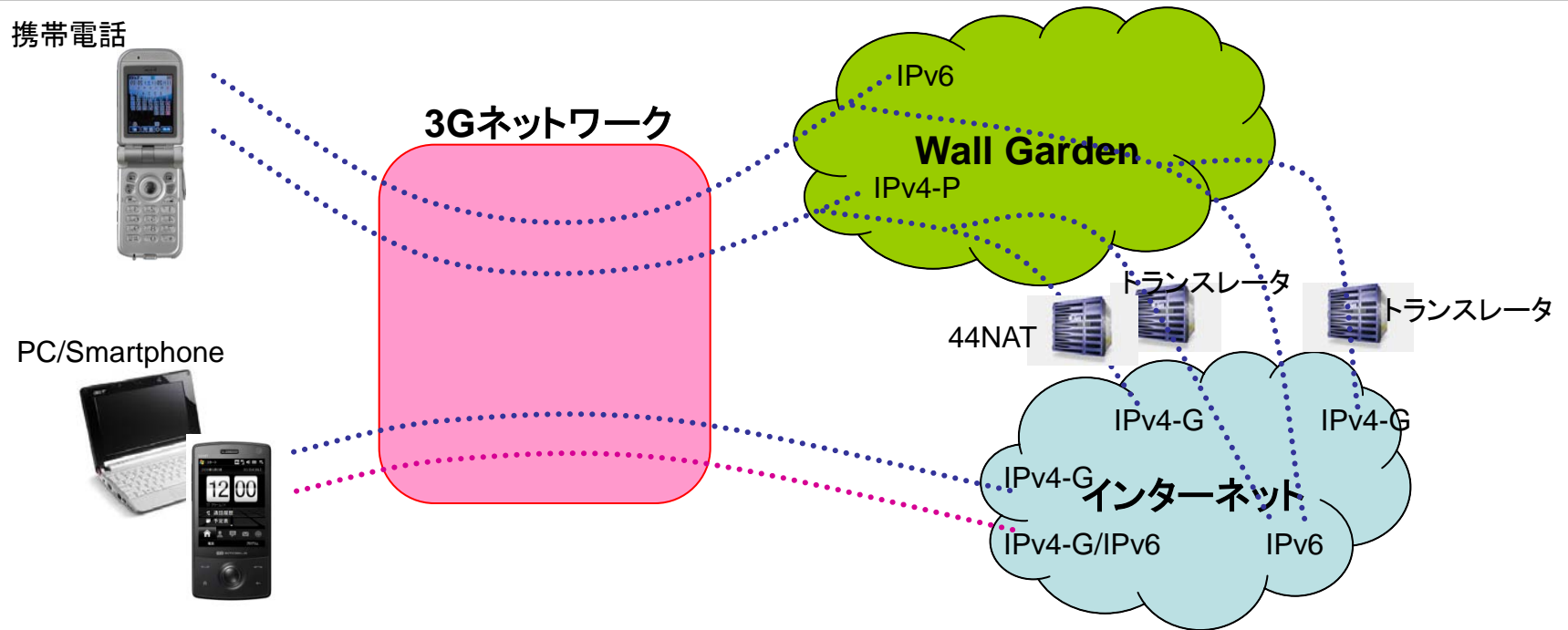


- トラフィックの増大と共に専用線(一般的にT1/E1ベース)やATM(STM-1)からイーサネット専用線へ移行しつつある:IPトランスポート
- IPトランスポートには通常プライベートアドレスが付与され、インターネットとは分離した閉じたネットワークを構成している
- IPトランスポートの回線数は基地局数と同等であるために、番号空間の逼迫が起こる可能性は少なく、**IPv6への移行を特に必要としない**

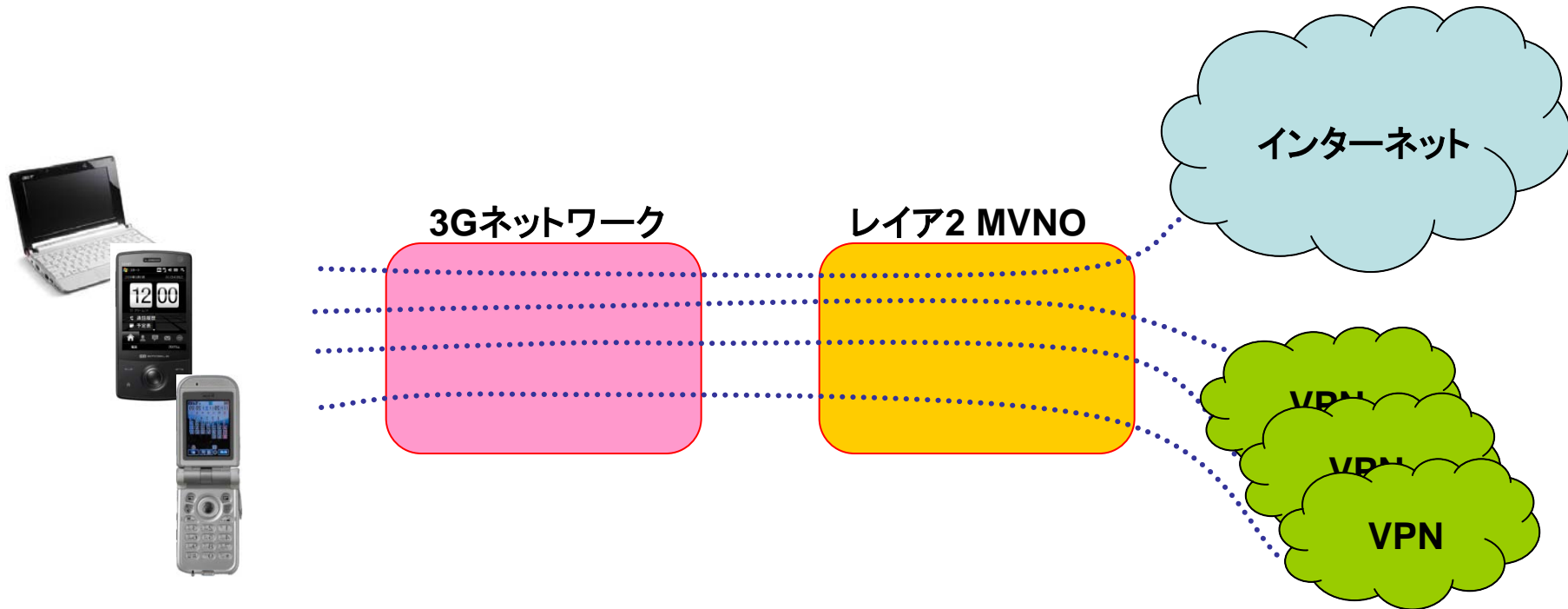


- 携帯電話によるMMS等のメール、携帯コンテンツのための通信は一般的にプライベートアドレス空間内で行われるが、インターネットへの接続もこの空間を経由して行われる。インターネットへの接続の際にはゲートウェイ(44NAT)にてIPアドレス等を変換して行われる。
- 通常は携帯電話によるIP通信は通信時間が短く、IPアドレスが随時割当されるために**アドレス使用率は非常に小さい**。よって、本アドレスを**IPv6に移行するニーズは小さい**。また、インターネット上のIPv6ホストへの接続のニーズが生じた際には、ゲートウェイにおけるIPv4/IPv6トランスレータによる対応が望ましいと思われる。但し、IPv6-IPSEC等のセキュリティ対応のためには、ゲートウェイにおけるアプリケーションレベル変換が必要となるかもしれない。
- USBドングル等を利用したネットブックやスマートフォンによる通信は一般的に**グローバルIPv4アドレス**が用いられる。しかしながら、W-CDMA/HSPAにおいては、通信後にタイマーや端末アプリケーションによる強制切断が行われるために固定ブロードバンド回線ほどは**IPアドレス使用率が高くない**。インターネット上のIPv6ホストへの接続のニーズが生じた際には、コアネットワークを**Dual Stack化**するのが望ましいと思われる。しかしながら、W-CDMA CoreにおいてAll IP化を採用しDual Stack(Release8)が実装されるかどうかは将来に亘っても不明である。

3GネットワークのIP化とIPv6の導入- AIPN



- All IP Networkにおいては、IPv4、IPv6、IPv4/IPv6の3種類のIPベアラーを設定可能である。よって、用途によって、端末毎に、あるいはアプリケーション毎にこれらのベアラーを使い分けることとなると思われる。IPv4のベアラーでは基本的にIPアドレスは随時割当であり、タイマー等により使用後にアドレスが解放される。これに反して、IPv6のベアラーではアイドル時も基本的にはIPアドレスは解放しないことを前提に設計されている。また、IPv4/IPv6Dual Stackのベアラーでは、IPv6は常時割当、IPv4は随時割当が前提となっている。
- IMSは基本的にIPアドレスにより発着信するために、IPv6を利用する方がアプリケーションへの親和性が高い。しかしながら、既存インフラの実装状況を考慮して、IPv4によるIMSも標準化がされており、その実装も進んでいる。巨大な電話番号空間を持った事業者が空間を統一してIPv6によるIMSを提供するか、空間を分割してIPv4によるIMSを提供するかは今後AIPNが採用されていくに従って事業者毎に判断される。但し、W-CDMA/HSPAを最初からAIPNで構成する事業者はまだ現れていない。よって、大多数の事業者はAIPNを導入するのはLTEを導入する時期に合わせるものと思われる。
- 3Gネットワークにおいては、アプリケーション毎にベアラーを選定することが出来るので、基本的にはNTT-NGNIにおけるようなマルチプレフィックス問題は生じないものと思われる。しかしながら、モバイル端末がルータとして動作するようなケースでは、その配下にある端末がどのようにしてベアラーを選定するかについては実装上の課題が生じてくるとと思われる。



- レイヤ2 MVNOは基本的に3Gネットワーク上で自由にIPアドレスを付与し、複数のIPネットワークを運用することが出来る。
- IPベアラーサービスの種別も自由に選択できるため、IPv4、IPv6、Dual Stackの選択もMVNO側で自由に行い、更に複数のネットワークに分けて運用し、それぞれの用途に応じた顧客に提供すれば良いと思われる。IPv6を使用するメリットは、複数ネットワークに分割して運用した時にアドレスの重複が起きないことである。また、IPv6マルチプレフィックス問題については、端末の実装(アプリケーション毎のベアラー選択)次第で解決可能である。

- W-CDMAばかりでなくLTEにおいても技術的には、①携帯電話端末の利用、②閉域網における音声を含むコンテンツ通信、③端末による複数サービス・ネットワークの使い分け、が基本的な前提条件となっている
- モバイルネットワークにおけるIPv6のニーズは、IMS(電話を含む)による閉域網端末数の増大に起因した運用上の課題への解決策、多数のVPNを並行運用するにあたってのIPアドレス重複の回避とインターネットにおけるIPv6の普及等が考えられる
- 基地局投資がコアネットワーク投資と比較して圧倒的に大きいこととAll IP NetworkとLTEの検討が同期していることを考慮するとコアネットワークへ大きなインパクトがあるIPv6導入が容易なのはLTEの導入と同期させた場合である
- IPv6に対する具体的なニーズが明確にならなかったためにIMSにおいてIPv4の使用も考慮せざるを得なくなったという経緯を考慮すると、LTE導入に合わせて世界的に**IPv6に対する具体的なニーズの明確化が必要**である
 - 標準化と実装の実態を考慮すると、ニーズが固まってから(Study Itemの完了)商用化まで最短で2.5~3年程度(例:IPv6移行の要求条件が2010年末に固まったとして、商用レベルの製品化がされるのは2013年頃)
- **モノのインターネットに関わる検討は着手**(2009年に合意)したところであり、これまでの標準化にあたって行われたシミュレーションの前提条件の見直し、実装上のリソース(メモリー、キュー、プロトコル遅延等)制限の確認、SIMカード利用の前提、端末呼び出しメカニズム、低コスト端末のセキュリティ確保、常時接続のためのセキュリティ確保、ネットワーク性能等が検討されると思われる

モノのインターネットのビジネスモデル

通信キャリアから見たモノのインターネット

エンドユーザのニーズにマッチしたサービスの提供

- 家庭毎に複数端末、エンドユーザ毎に複数端末
- ユーザビリティ、セキュリティの自己責任・自己管理は困難
- 支出の増分は最低限(通信費から削るか、家電等の購入費用から削るか)

既存のブロードバンドサービスの大幅な見直しが必要

- インターネットの基本原則(オープン性、ドメイン名によるアドレスの視覚化、ネットワークの相互接続性)
- 通信事業、製造業のビジネスモデル
- セキュリティの確保の観点

見直しの観点

- スケール
 - 接続する端末の数
 - 人と人、人とサーバ→モノとモノ、モノとサーバ
 - 通信量のダイナミックレンジ
 - ごく少量通信(例:センサー)~超大容量通信(例:ピアトゥピアファイル転送)
- ビジネスモデル
 - 単純な垂直統合モデル、水平分業モデルからの脱皮
- 提供責任
 - 製造物責任と契約約款に基づく責任及び責任分解点の見直し
 - エンドユーザサポート

制限事項

- 金融システム上の制限
 - リスクマネーの規模の限界を考慮すべき
- 財務的制限
 - 現実的な設備投資、収支バランスの維持、極度なカニバリゼーションの排除
- 運用上の制限
 - モノのインターネットが既存ネットワークの運用に大きな影響を与えてはいけない
- 既存インフラの制限
 - 既に広範囲に実装されている技術の早急な入れ替えは現実的ではない

持続可能な事業モデルの創造

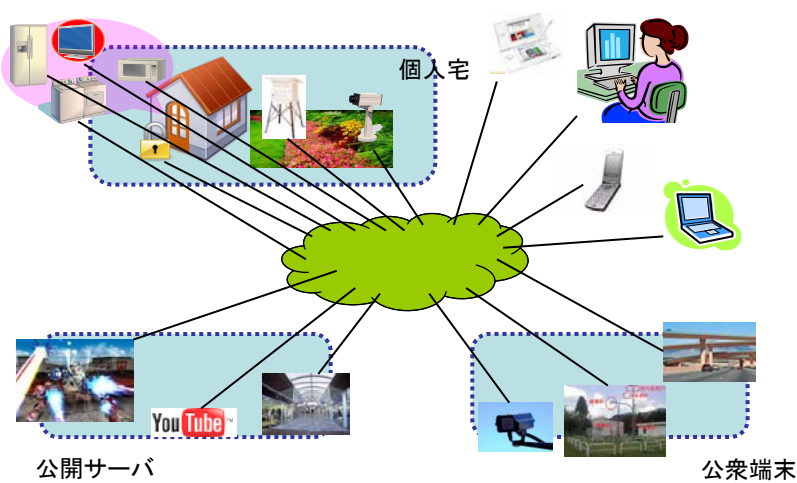
- ネットワーク
- アプリケーション(サービス)
- 事業体と事業範囲

-受益者による分類: 公衆利用と個人利用

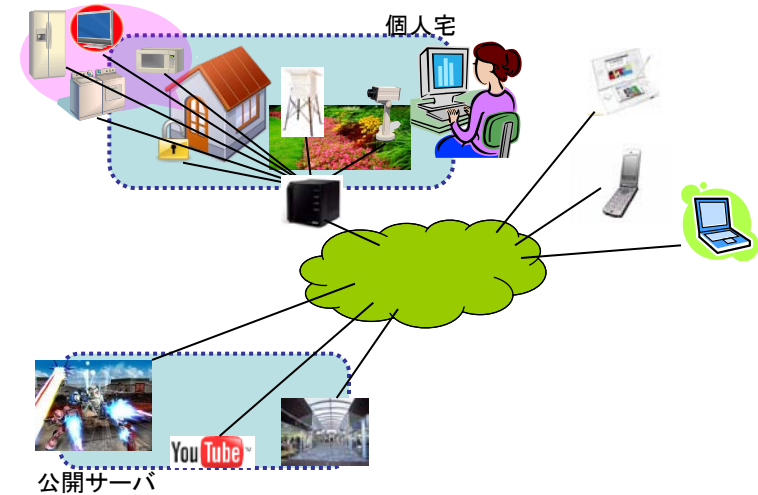
-アクセスインフラによる分類: 固定系と無線系

モノのインターネットの提供モデル

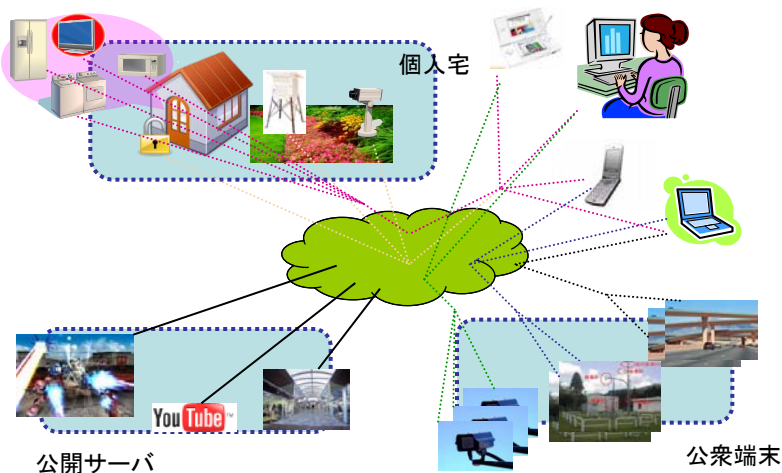
1. フラットネットワークモデル



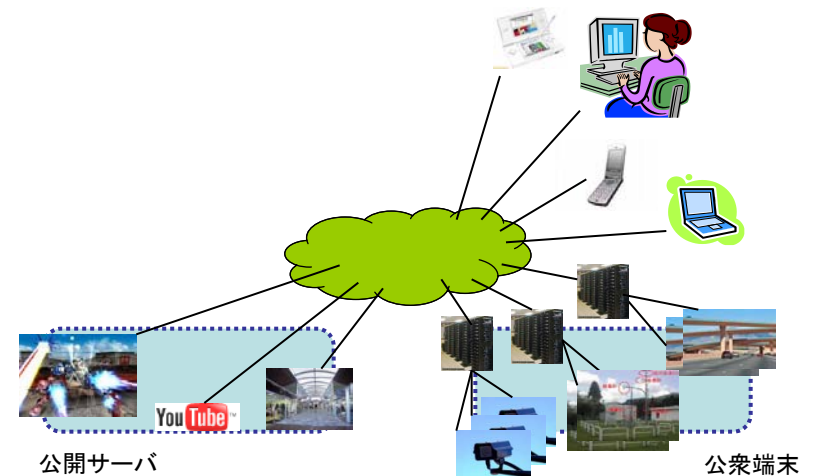
2. ホームサーバモデル



3. VPNモデル



4. 公衆サーバモデル



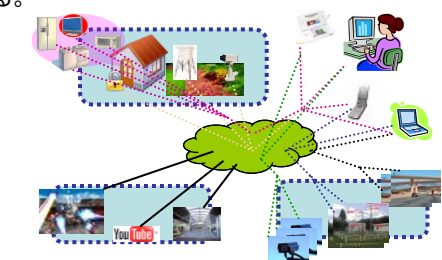
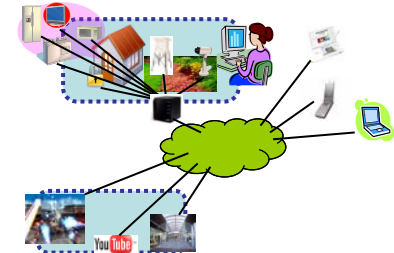
それぞれのモデルの特徴

- フラットネットワークモデル
 - 全ての端末がIPアドレスを持ち、インターネットに直接接続される
 - 端末間の通信は端末の種類に関わらず、全て通信事業者が提供する
 - セキュリティの確保はDoSアタック対応も含めて端末にて行う
- ホームサーバモデル
 - 家庭やオフィス内の端末はLANに接続され、LAN内のサーバを通してインターネットに間接的に接続される
 - サーバとの通信は通信事業者が提供するが、LAN内端末との通信は家庭やオフィスが自己責任で行う
 - セキュリティの確保は、DoSアタックについてはサーバやアクセス回線終端装置で確保し、ウィルス等のユーザ通信やアプリケーションに起因するセキュリティ脅威は端末やホームサーバで対応する
- VPNモデル
 - 端末がサービス、事業や通信されるコンテンツ等毎に別々のVPNに接続される
 - VPNは場合によってはLAN内まで浸透する
 - VPNの提供方法としては、通信事業者が提供するネットワークレイアに重畳する場合(例:IPoverIPやL2TP)とネットワークレイアを分割して利用する場合(例:MVNO)がある
 - 端末との通信は、通信事業者とVPN提供事業者が協調して提供する
 - セキュリティの確保は、VPN毎に端末認証による不正端末排除とフィルター等による不正利用排除により行う
- 公衆サーバモデル
 - 端末はプライベートなネットワーク(VPNを含む)を通して公衆ネットワーク上のサーバに接続される
 - サーバとの通信は通信事業者が提供するが、端末との直接通信は行われない
 - セキュリティの確保はDoSアタック対応も含めて公衆サーバにて行う

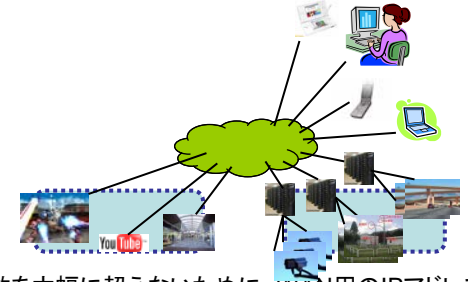
各モデルの比較

	私 的	公 的	端末IPアドレス数	公衆回線総コスト	端末検索の容易性	端末毎の管理	セキュリティ
フラットネットワークモデル	○	○	人口の数倍:IPv6が必須	携帯電話の数倍	既存技術では困難	全てのアプリケーションをカバーする標準化が必要	各端末にてセキュリティ確保が必要なために端末コストが増大
ホームサーバモデル	○		世帯数程度	固定ブロードバンド程度	容易	家庭用端末管理のためのデファクトスタンダードが必要	ホームサーバにてセキュリティ確保するためにコストが限定的
VPNモデル	○	○	事業数の数倍~人口の数倍:IPv6の利用かVPN毎にプライベートアドレスを利用して繰り返す	固定ブロードバンド程度	容易	家庭用端末管理のためのデファクトスタンダードが必要 非家庭用端末は事業毎に独自アプリケーションにて管理	VPNへの参加によりセキュリティ確保するために端末への影響が小さい
公衆サーバモデル		○	事業数の数倍	固定ブロードバンドの数分の一	容易	非家庭用端末は事業毎に独自アプリケーションにて管理	サーバにてセキュリティ確保

- 個人利用とは、モノのインターネットの各端末を特定の個人・法人が利用するケース
- ホームサーバモデル
 - 概要
 - 各家庭やオフィスにホームサーバを設置し、家庭やオフィス内の情報家電等はホームサーバを経由して情報の蓄積や端末の制御を行う。また、外部端末から家庭・オフィス内の端末へのアクセスも、ホームサーバが外部端末を認証した上でホームサーバ経由で行う。端末のセキュリティはアプリケーションレイヤについてはホームサーバにて確保し、ネットワークレイヤについてはホームサーバと宅内のファイアーウォールの協調動作にて確保する。
 - サービス提供主体
 - ホームサーバ提供事業者ないしはメーカー
 - 実例
 - ホームセキュリティ用のサーバやDLNA等を利用して相互に接続されたAV家電
 - 普及への課題
 - 端末とサーバのインターフェースの標準化によりメーカーを跨った利用を可能とすること
 - アラーム機能の充実による災害防止
 - 単純な電源のオンオフ、AV家電の制御やホームセキュリティ等を越えたニーズへの対応
 - IPv6の利用
 - WAN回線数が家庭やオフィスの総数を大幅に超えないために、WAN用のIPアドレスはそれほど必要としない
 - LAN内のネットワークの自動構築のためにIPv6の諸機能の活用は有効だが、ホームサーバでWANとLANを中継しているためにWAN側は特にIPv6にする必要が無い
- VPNモデル
 - 概要
 - 各家庭やオフィスを跨り、サービス毎にVPNを構築する。家庭やオフィス内の情報家電等は各サービスを管理するVPN内の公衆サーバを経由して情報の蓄積や端末の制御を行う。また、外部端末から家庭内の端末へのアクセスも、本サーバが外部端末を認証した上で本サーバ経由で行う。端末のセキュリティはアプリケーションレイヤについてはサーバにて確保し、ネットワークレイヤについてはVPNにて確保する。
 - サービス提供主体
 - サーバ・VPN提供事業者
 - 実例
 - 不明
 - 普及への課題
 - サービス毎にVPNを構築するためのVNO/MVNOモデルの普及
 - VPN毎コストの低廉化
 - 端末のネット関連機能の充実
 - IPv6の利用
 - 固定回線上のVPNの場合にはWAN回線数が家庭やオフィスの総数を大幅に超えないために、WAN用のIPアドレスはそれほど必要としないが、無線回線上のVPNの場合には端末数だけ無線回線数が必要のためにIPv4空間の利用ではVPN毎にプライベートアドレスを重畳使用する必要がある。
 - IPアドレスの重畳使用を回避するためにIPv6の利用は非常に有効

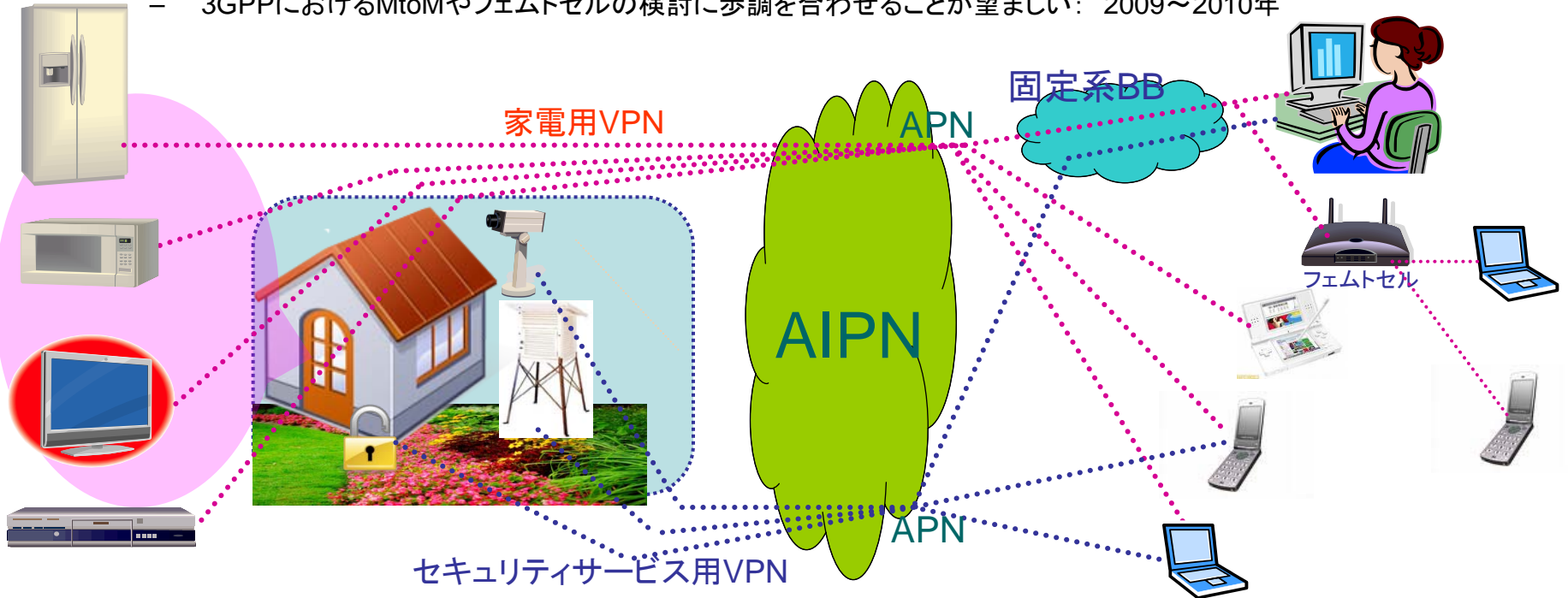


- 公衆利用とは、モノのインターネットの各端末を不特定の個人・法人が利用するケース
- 公衆サーバモデル
 - 概要
 - インターネット上にサーバを設置し、各端末はインターネット、VPNや専用線を通して本サーバに接続する。各端末の制御や情報のやり取りは本サーバを通して不特定のインターネットユーザが行う。端末のセキュリティはアプリケーションレイヤについてはサーバにて確保し、ネットワークレイヤについては宅内のファイアウォールVPNや専用線にて確保する。
 - サービス提供主体
 - サーバ提供事業者
 - 実例
 - 気象情報サービス(Weatherunderground社等)、オンラインゲーム
 - 普及への課題
 - 不特定アクセスが可能な端末の普及
 - 公衆端末から利益を上げるためのビジネスモデル
 - IPv6の利用
 - 公衆回線を利用して端末が接続される場合に、固定回線の場合にはWAN回線数が家庭やオフィスの総数を大幅に超えないために、WAN用のIPアドレスはそれほど必要としないが、無線回線の場合には端末数だけ無線回線数が必要なためにIPv4空間では足りず、IPv6の利用が必須である。



AIPNによるVPNモデルの実現例

- 固定系ネットワークの課題をモバイルネットワークによって克服
 - VNO網の容易な構築
 - エッジからコアネットワークまで分割可能
 - 旧来のFletsモデルと同様
 - 無線であるためにアクセス回線リソースの分割が容易で回線(無線回線)単価を下げやすい:但し、価格のトラヒックセンシティブティが高くなる
 - VNOに分割することによってエンドエンド通信サービスを分散させ、多様化させることが出来る
- 各サービス毎にMVNOを構築し、ベアラサービス(RAN)、IPネットワーク(CORE)をMVNO毎に割り当てる
 - MVNOへの分割をレイア2MVNOが担当し、2階層とすることも可能
 - 家電ネットワークの単位が家電の種類毎、メーカー毎かどうかは市場動向に依存
- LTE/SAEのネットワークリソース利用に大きな影響を与えるため、標準化において十分な検討が必要
 - 通信キャリア、通信機器メーカー、通信端末メーカー以外のメーカーやMVNOからの早急なインプットが必要
 - 3GPPにおけるMtoMやフェムトセルの検討に歩調を合わせることが望ましい: 2009~2010年



ワイアレスブロードバンドネットワークの動向と IPv6導入への課題

- ユビキタス社会に向けて3Gネットワークにおいて様々な課題の解決が進んでいる
 - 端末のプロビジョニング: OTA技術とSIMカードによる端末自動設定
 - 端末の探索: SIMカードとIPアドレス割当の連携
 - 端末コストの低廉化: パテントプール方式を採用したWiMAXとの競争の影響を受けたビジネスモデルや商習慣の変更
 - VPN構築: L2-MVNOサービスによりMVNOが自由にVPNを構築
 - FMC技術: フェムトセルによる固定回線上へのモバイルサービスの展開
- ワイヤレスブロードバンドによるモノのインターネット実現への課題
 - 通信モジュールコスト: 3Gの通信チップ、通信モジュールのコスト構造は携帯電話に最適化されており、人口の数倍に及ぶような数を供給するような事業モデルが確立されていない(WiFiモジュールは1,000円以下だが、3Gは5,000円以上)。
 - SIMカード: SIMカードの利用が3GPP系技術の前提となっているが、SIMカード実装コストや展開コスト及びSIMカードの機能制限によるニーズへの未対応や過剰機能によるコスト高が問題である。
 - 端末の探索: 人口の数倍を超えるとなると電話番号空間では足りないが、それに代わるDNSではスケールしないので、端末探索に関わる新たな技術が必要である。
 - 隠れたスケーラビリティ上の問題: 標準化のためのシミュレーションや機器への実装において、セル内端末数やネットワーク内端末数、端末のトラフィックパターンが既存の携帯電話利用を前提に行われており、スケールが数倍大きくなった時の実装仕様へのインパクトが未検討。
 - 周波数の不足: 音声からデータへ、固定からモバイルへユーザの通信が移行するに伴い、モバイルネットワークの通信量が飛躍的に増大しているが、周波数が他の産業との間で十分に公平に分配されていない。また、事業者間の割当やサービス間の割当も不均衡である。更に、グローバルに広く利用される周波数を決める仕組みがITU-Rのみでは機能しがたくなっており、日本の周波数割当とヨーロッパ、アジア、米国のとが大きくずれる問題が生じている。
- IPv6導入への課題
 - 商用ネットワークにおける利用を目指してIPv6の導入をオープンに進めている事業者は無いため、コアネットワークと端末の間の商用レベルでのIOTはほとんど進んでいない。また、IOT試験に伴って発生する大量の仕様見直しは進んでいない。
 - IPv4及びIPv6のそれぞれを独立に、又はDual Stackにより3Gネットワーク内で提供するための標準化は完了している
 - IPv6はSingle/Dual Stack共にコアネットワークへの実装は進んでいる
 - Dual Stack提供時の実利用面からの課題(品質、スケーラビリティ、性能、インターオペラビリティ等)の検討は十分に進んでいない
 - 3Gネットワークは基本的にトンネルネットワークであるためにVPN構築が容易であり、IPアドレスの繰り返し利用は可能である。また、インターネットへのアクセス時にグローバルIPアドレスを臨時に確保するために、IPアドレスの実使用率は固定ブロードバンドと比較してかなり小さい。更に、現在の3Gサービスでは端末が直結されていてNATが使われていないために、今後ネットワーク側にNATを入れることによるアプリケーションへの影響は小さい(444NAT状態となる可能性が小さい)。特に、音声やミッションクリティカルな通信についてはベアラーを分けることによりNATやマルチプレフィックス問題を避けることが可能である。よって、固定系と比較するとIPv6導入のインセンティブが小さい。

イー・モバイルの取り組み

- イー・モバイルは基本的にオープン
 - 技術的にオープン
 - 汎用技術及び国際標準化された技術のみを使用
 - 特許や個別開発等の技術資産を持たないためあらゆる技術の採用に対してオープン
 - 特定のメーカーと関係を持っていないので、そのメーカーの開発方針に縛られない
 - ビジネスモデル的にオープン
 - 「土管を使う事業」(MVNO等)が「土管」事業との間で公正競争できるモデル
 - 端末・サーバ垂直統合モデルを否定しない、介在しない
 - VoIP、Peer to Peer等の特定のアプリケーションを排除しない
 - 端末に対してオープン
 - ネットワークアクセスにおいて特定の技術的、ビジネス的要件を持たない
 - MVNOに対してオープン
 - レイヤ2 MVNOへの積極的な取り組み
- IPv6等の新技術の採用はインフラの移行にあたってニーズとコストパフォーマンス及びグローバルな動向を見ながら検討している