資料４－５

モバイルセキュリティの動向と課題

2008年 1月31日（木）

KDDI株式会社

本日は、通信事業者の観点から、モバイル系を中心に、通信事業環境の現況と、今後の端末やネットワークの進化、それらに伴うセキュリティ上の課題についてお話し致します。

1．モバイルとブロードバンドの融合の流れ

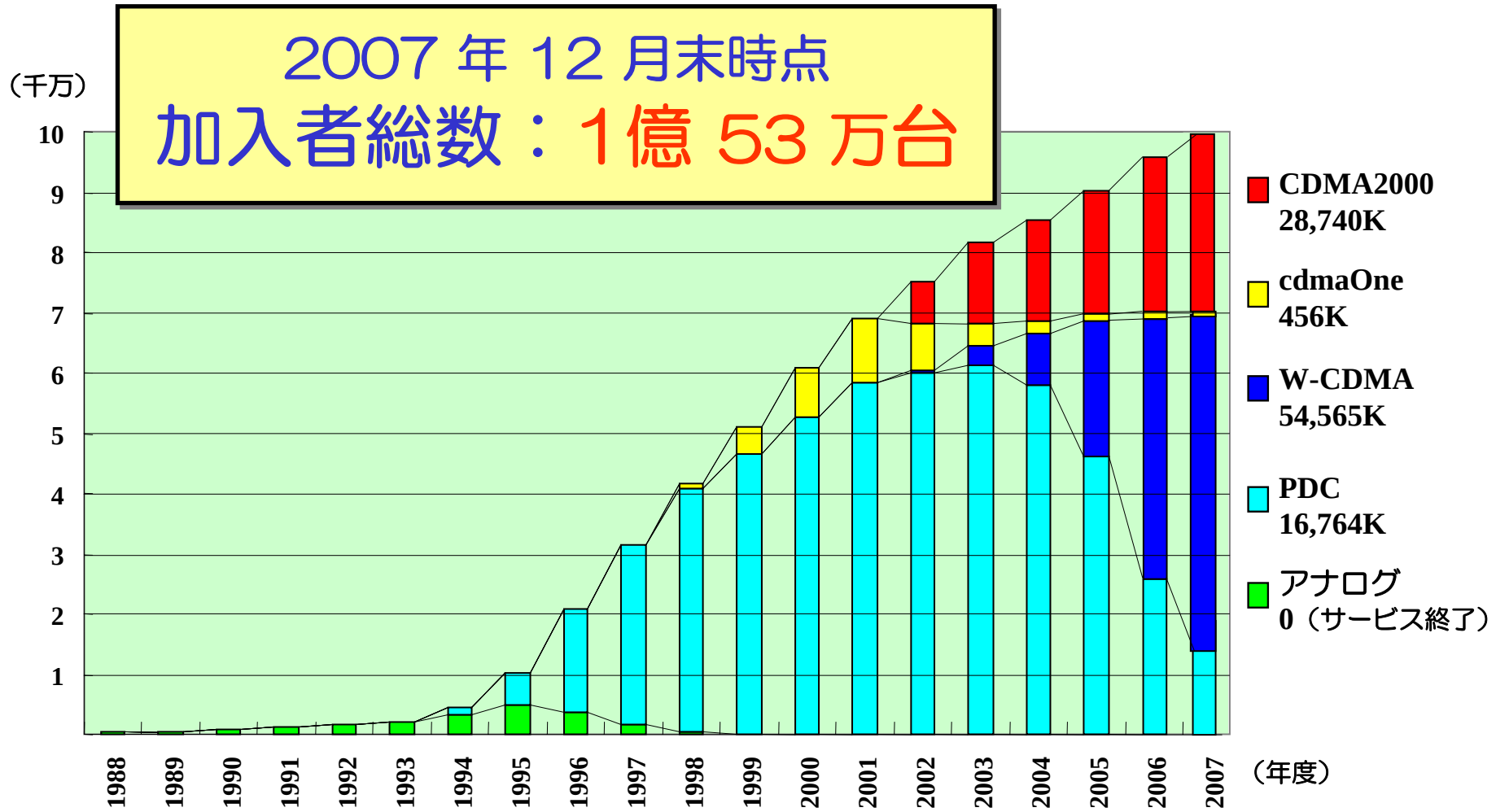
2．拡張・連携を模索するモバイルIT環境

3．モバイルネットワークの現状と課題

4．将来のモバイルIT環境にむけての課題と対策

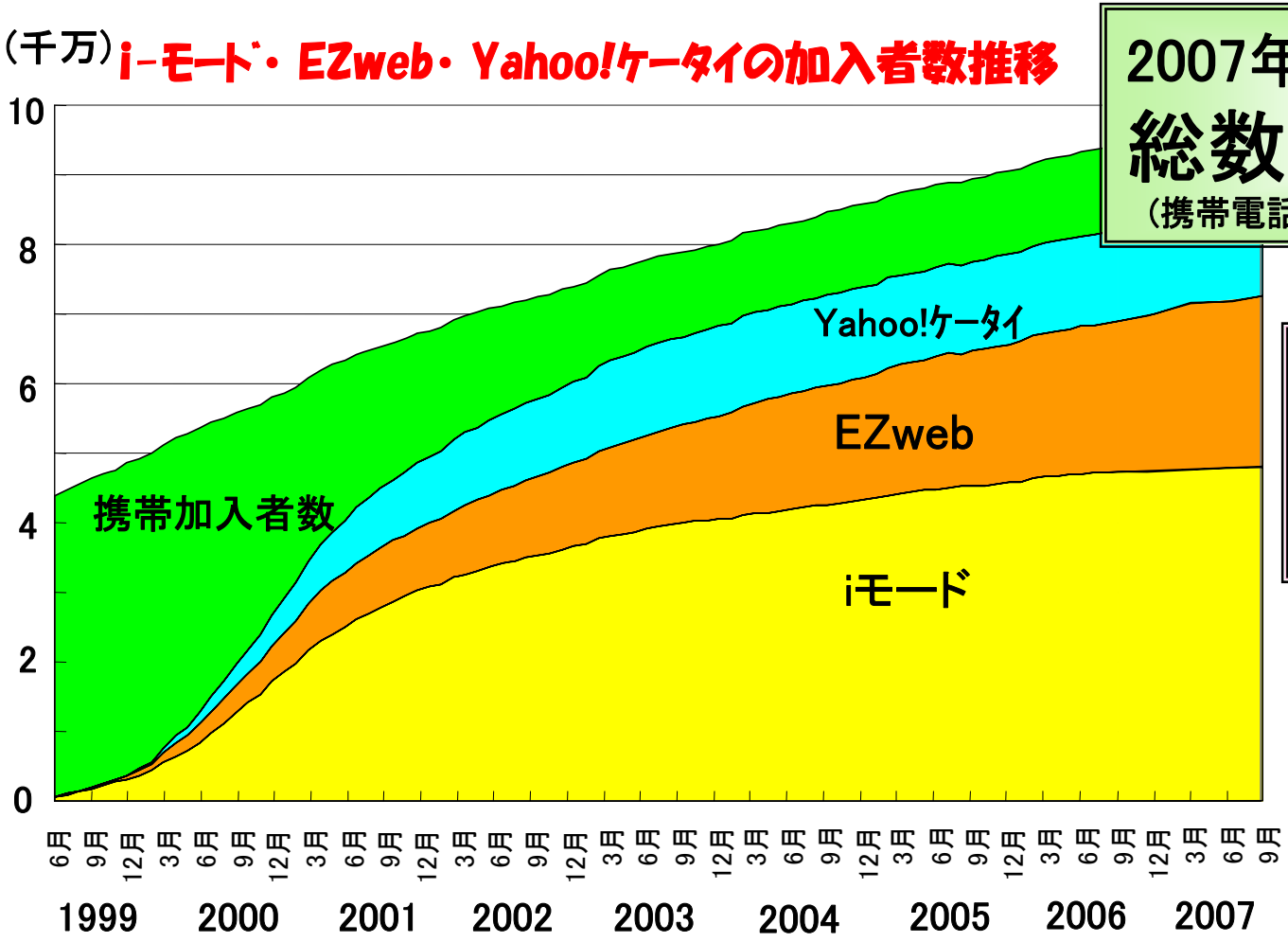
1．モバイルとブロードバンドの融合の流れ

日本における携帯電話市場の成長



（出展）電気通信事業者協会（TCA）
各年度3月末時点のデータ

日本のインターネット対応携帯電話端末数の推移



2007年12月末

総数: 8,728万加入

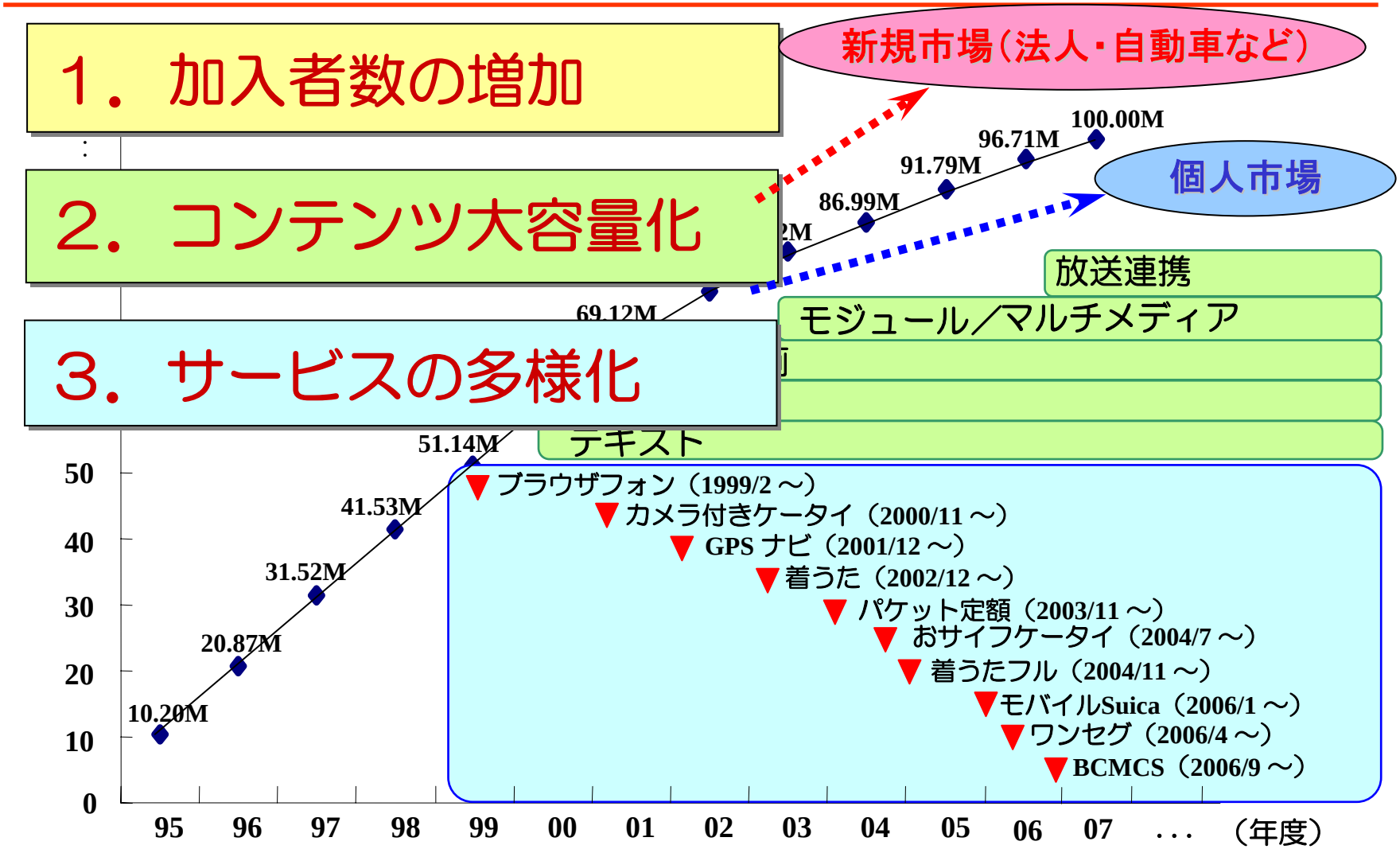
（携帯電話加入者総数 ： 10,053万加入）

〈内訳〉

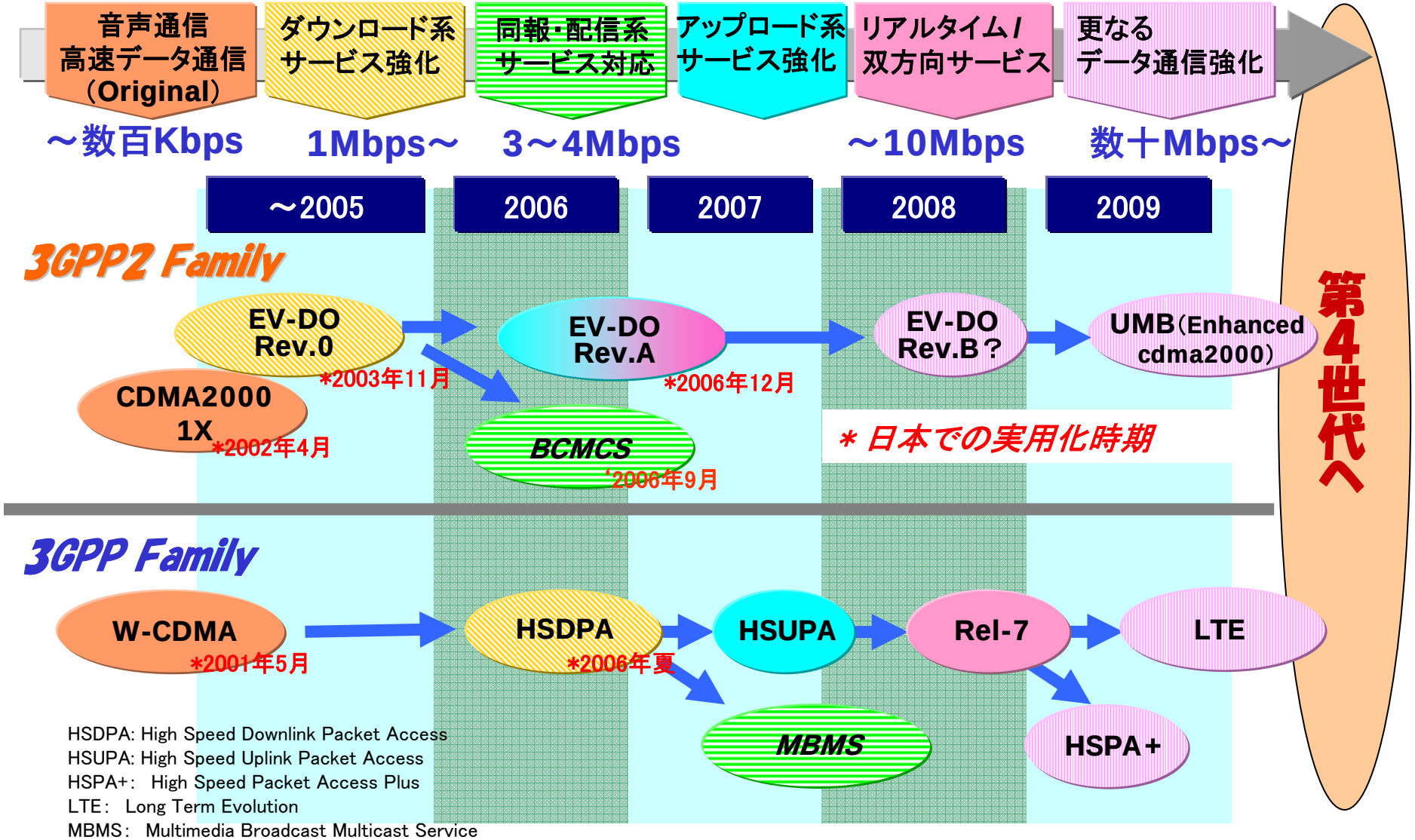
i モード	: 4,783万加入
EZweb	: 2,489万加入
Yahoo!ケータイ	: 1,456万加入

（出展）;
電気通信事業者協会

モバイル通信市場のマクロトレンド

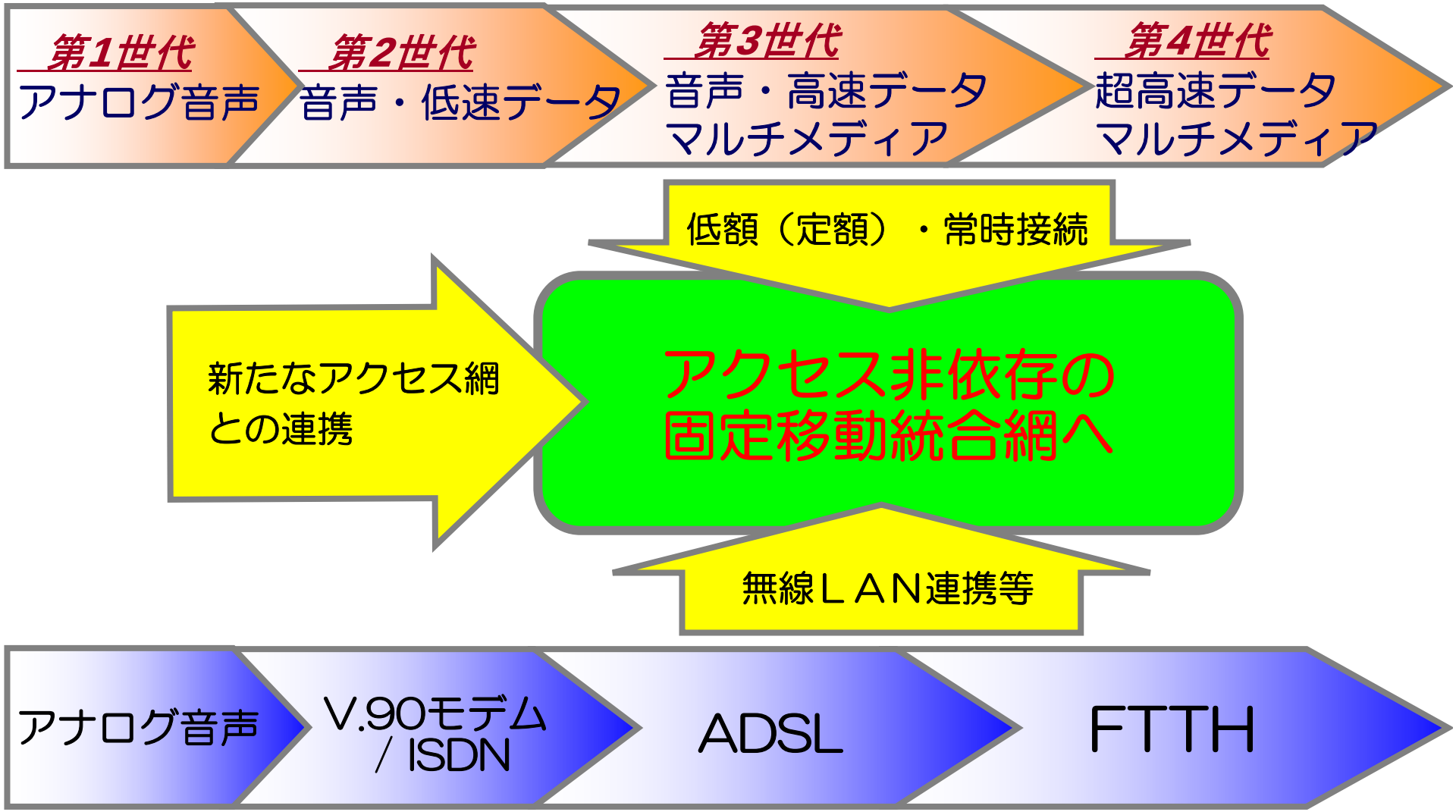


3Gシステムの進化



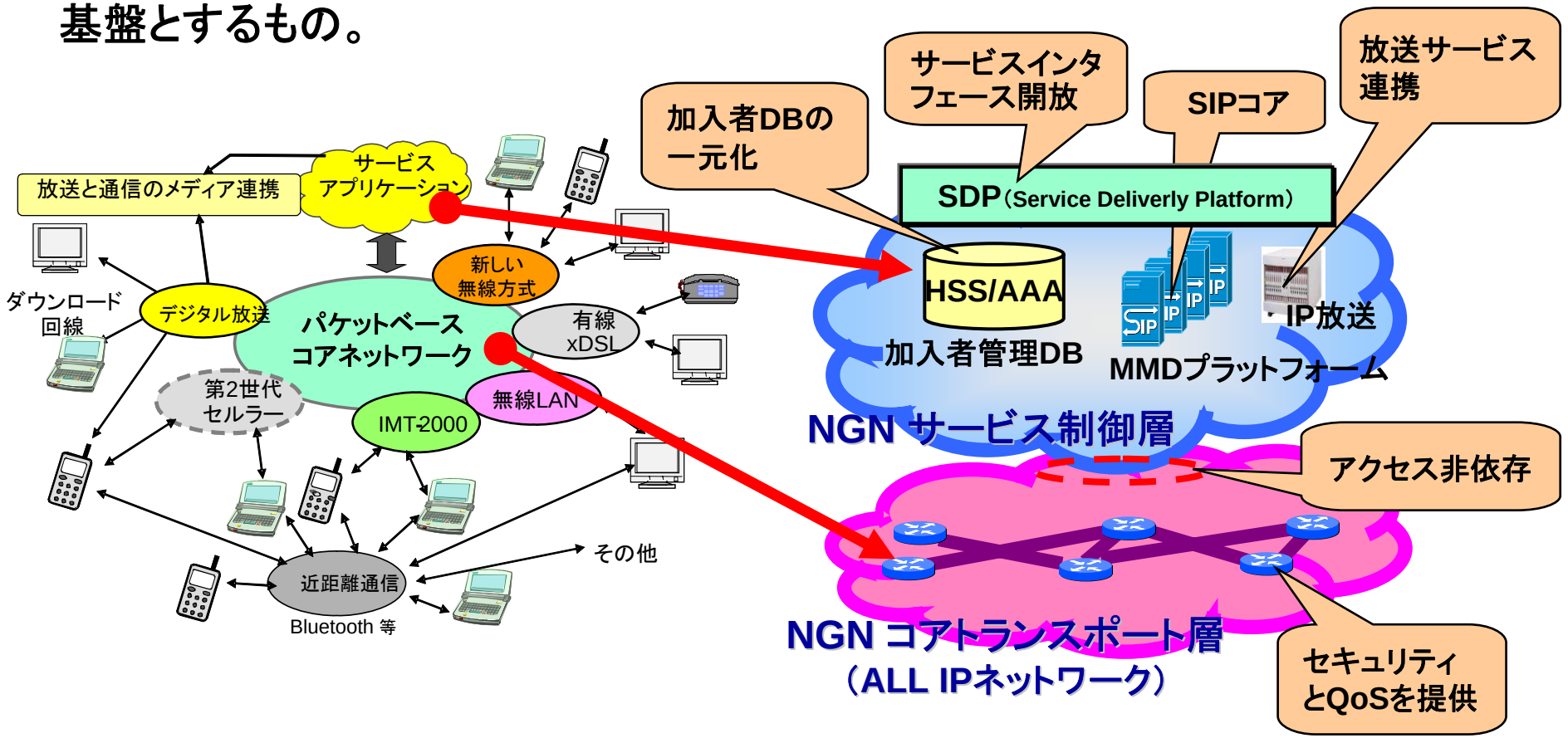
HSDPA: High Speed Downlink Packet Access
HSUPA: High Speed Uplink Packet Access
HSPA+: High Speed Packet Access Plus
LTE: Long Term Evolution
MBMS: Multimedia Broadcast Multicast Service

モバイルとブロードバンドの融合への流れ



KDDIのウルトラ3G構想

「ウルトラ3G構想」とは、移動体コア（MMD）をベースに、多様なアクセス網との相互連携が可能な、KDDIの NGNを構築し、FMC（FMBC）サービスの提供基盤とするもの。

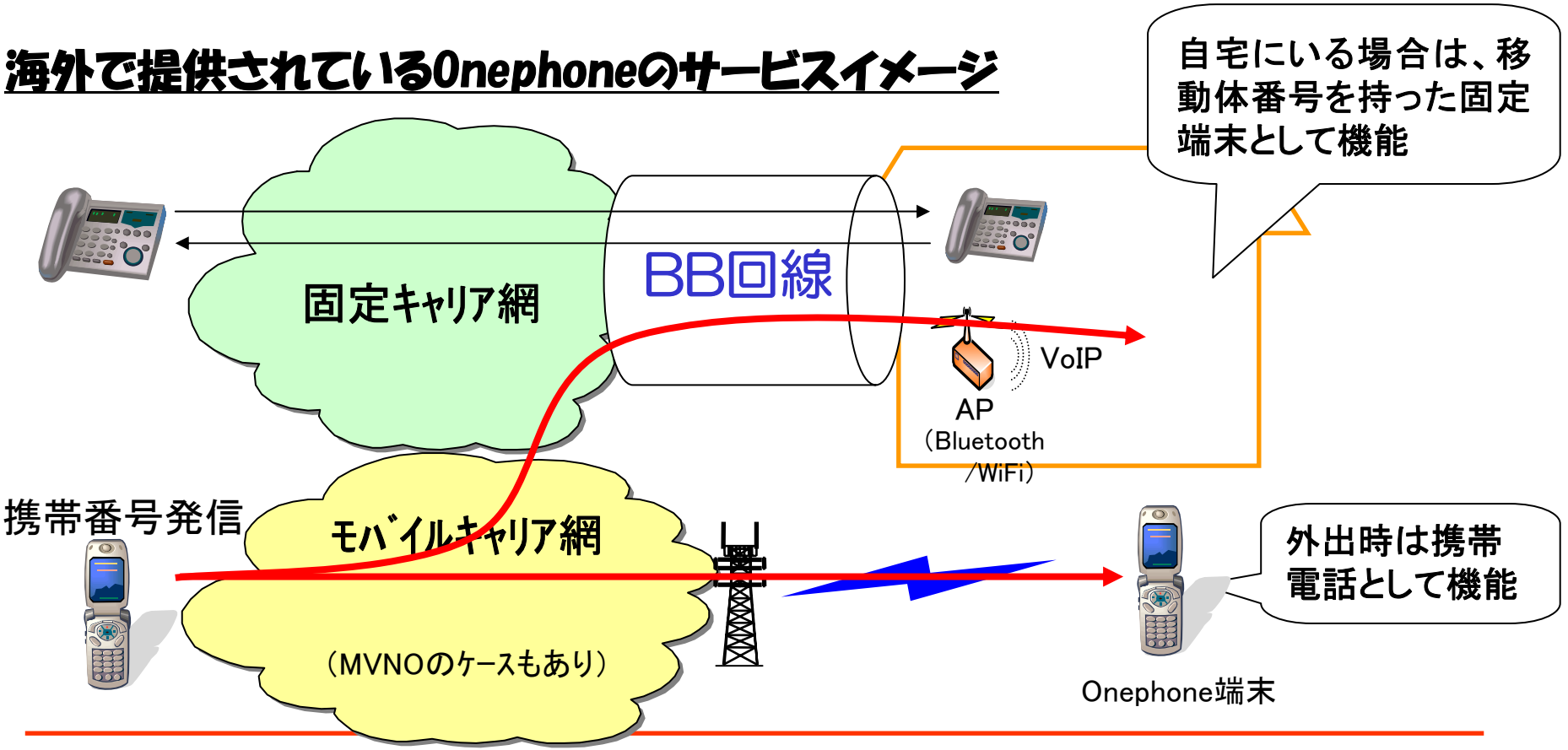


MMD：Multimedia Domain
NGN： Next Generation Network

FMCサービス例：Onephone

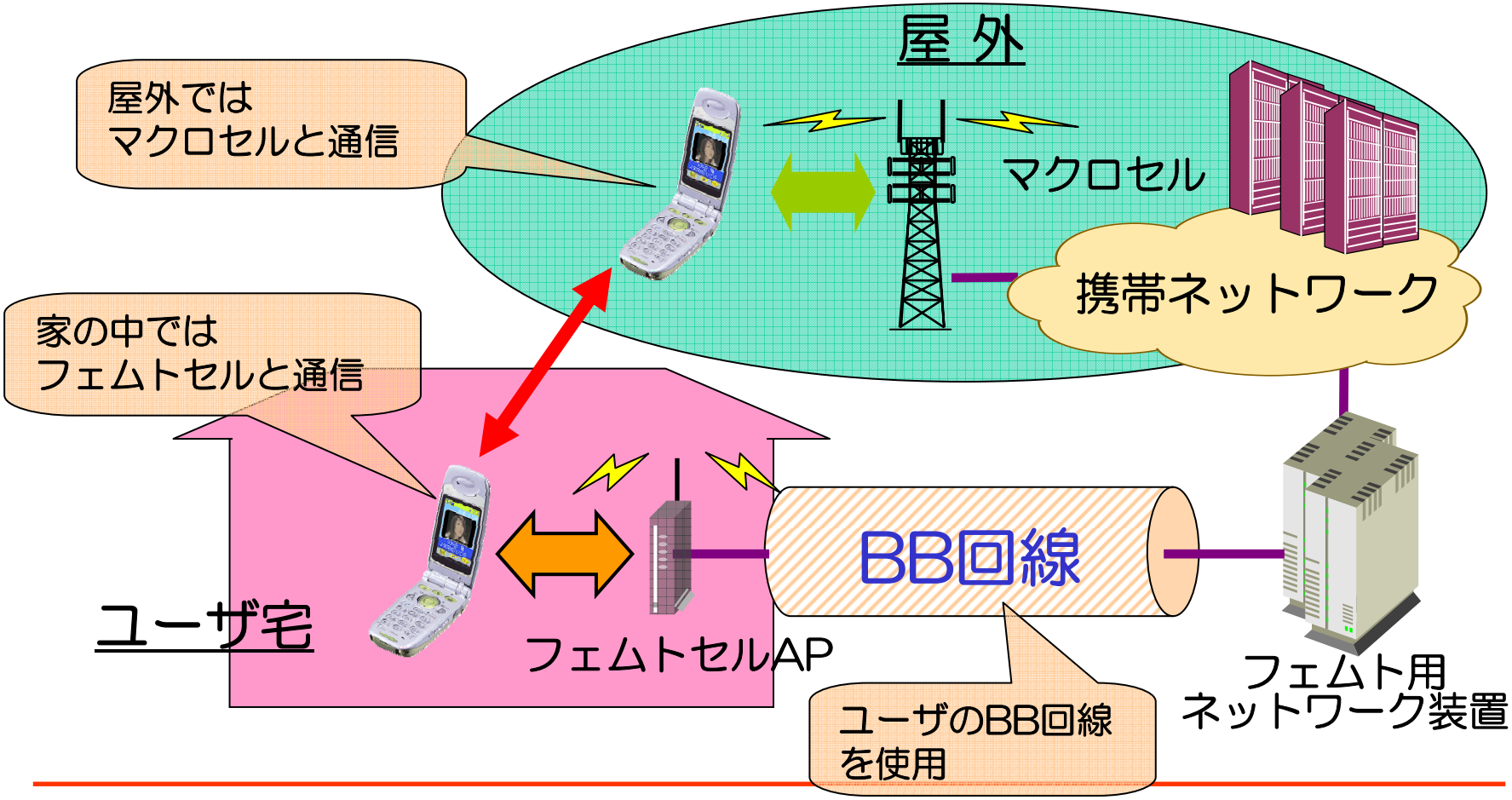
Onephoneは、FMC型サービスとして、今後期待されるものの一つ。国内ではまだ普及に至っていないが、英国や韓国などFMC先進国とされる国々では、既に多くのキャリアがOnephone型サービスを提供している。

海外で提供されているOnephoneのサービスイメージ



FMCサービス例：フェムトセル

フェムトセルも、固定網と移動体網を組み合わせたサービスとして、今後展開が予想されるFMCサービスの一つと位置づけられる。



2．拡張・連携を模索するモバイルIT環境

ケータイを使った個人認証の活用例

- 携帯電話に格納されたUIMに個人情報を記録
- 携帯環境のPKIを活用

携帯を使ったセキュアな個人認証が可能に。

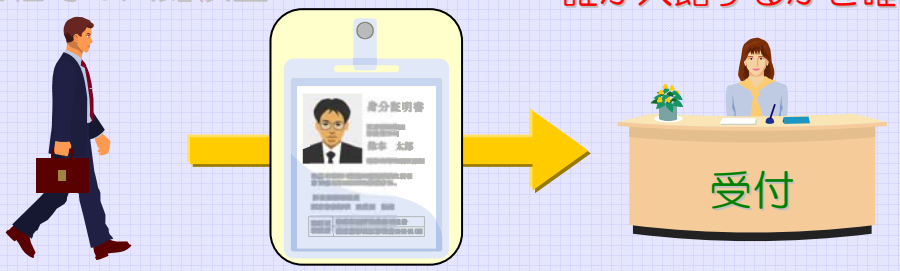
- 運転免許証
- レンタル会員証
- 社員証・学生証
- 診察券
- 旅行クーポン券

UIM（User Identity Module）
：携帯電話会社が発行する契約者情報を記録したICカード

本人認証（存在認証）

出社時の入館検査

誰が入館するかを確認



太郎さん

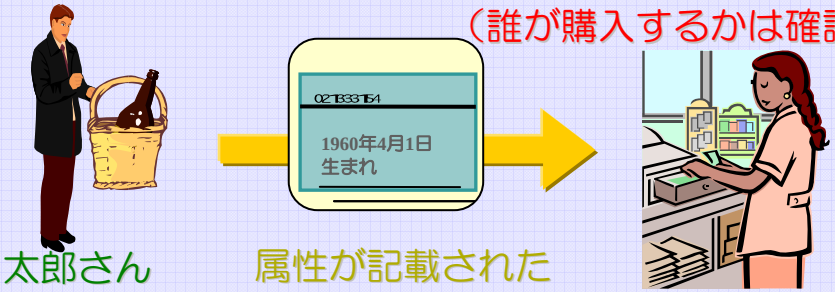
本人性が記載された証明書を提示

入館チェック

属性認証（資格認証）

酒屋でお酒を購入

20歳以上であることを確認
（誰が購入するかは確認不要）

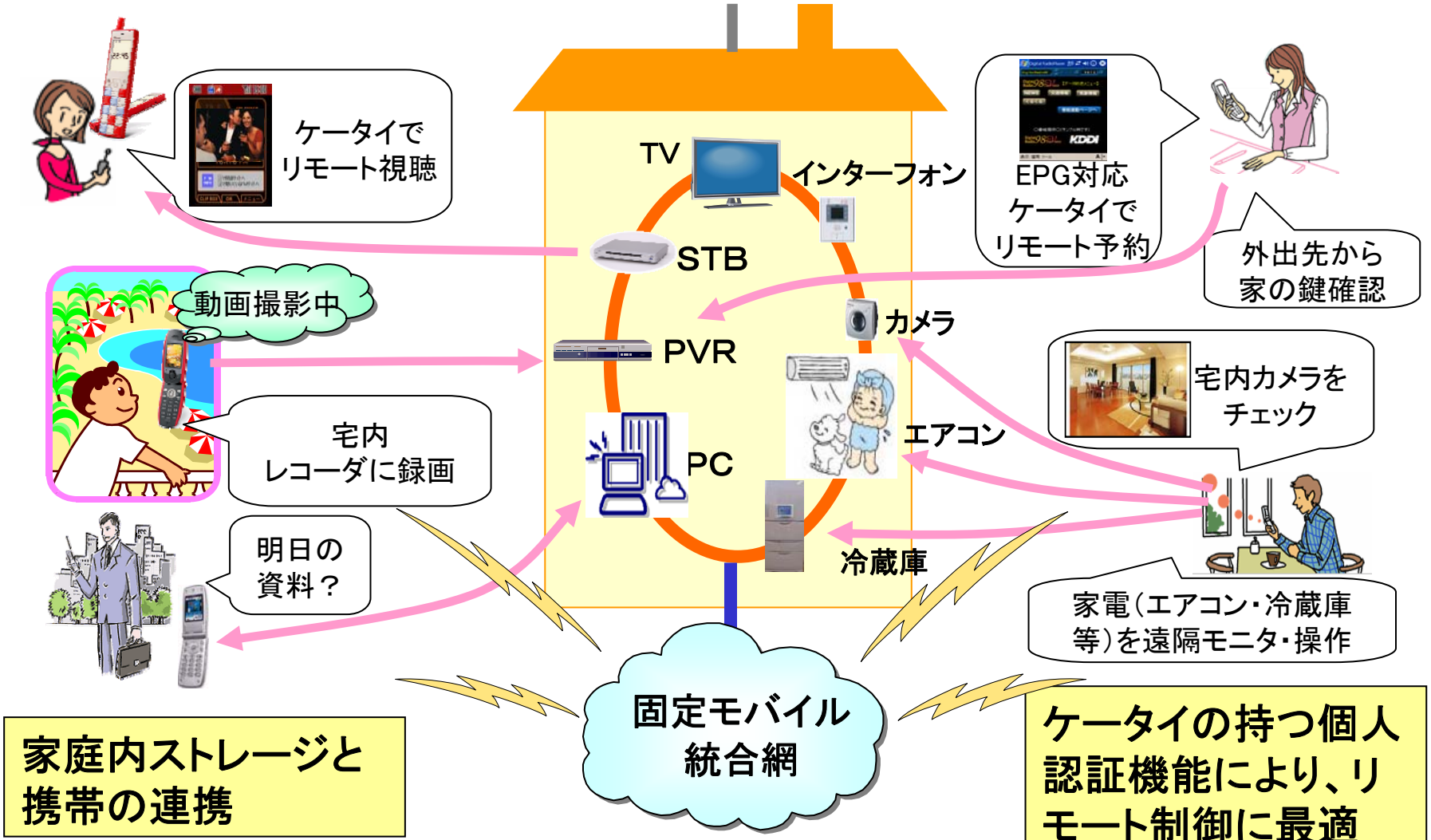


太郎さん
（1960年4月1日生）

属性が記載された証明書を提示

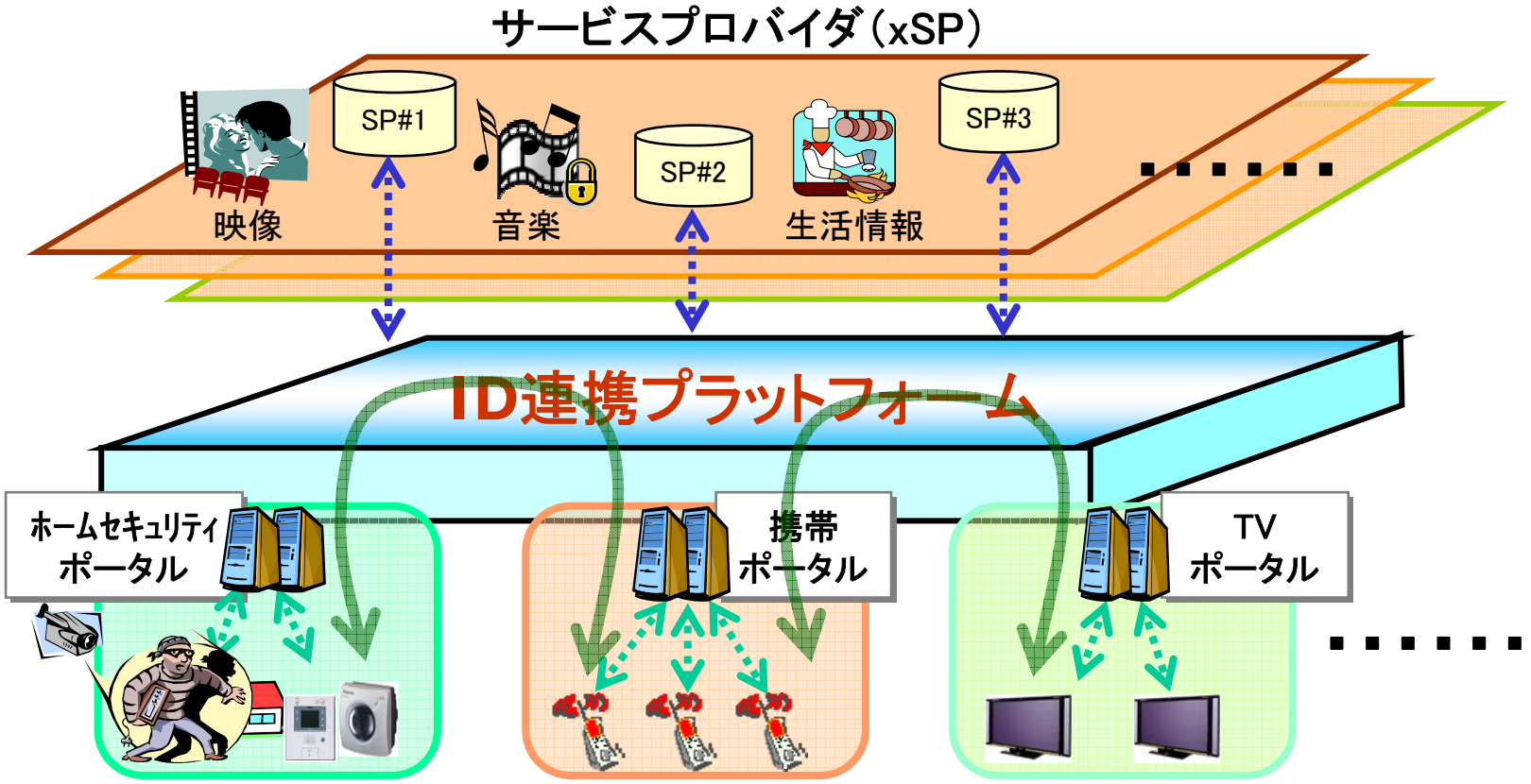
酒屋店員

ストレージ連携とケータイ個人認証



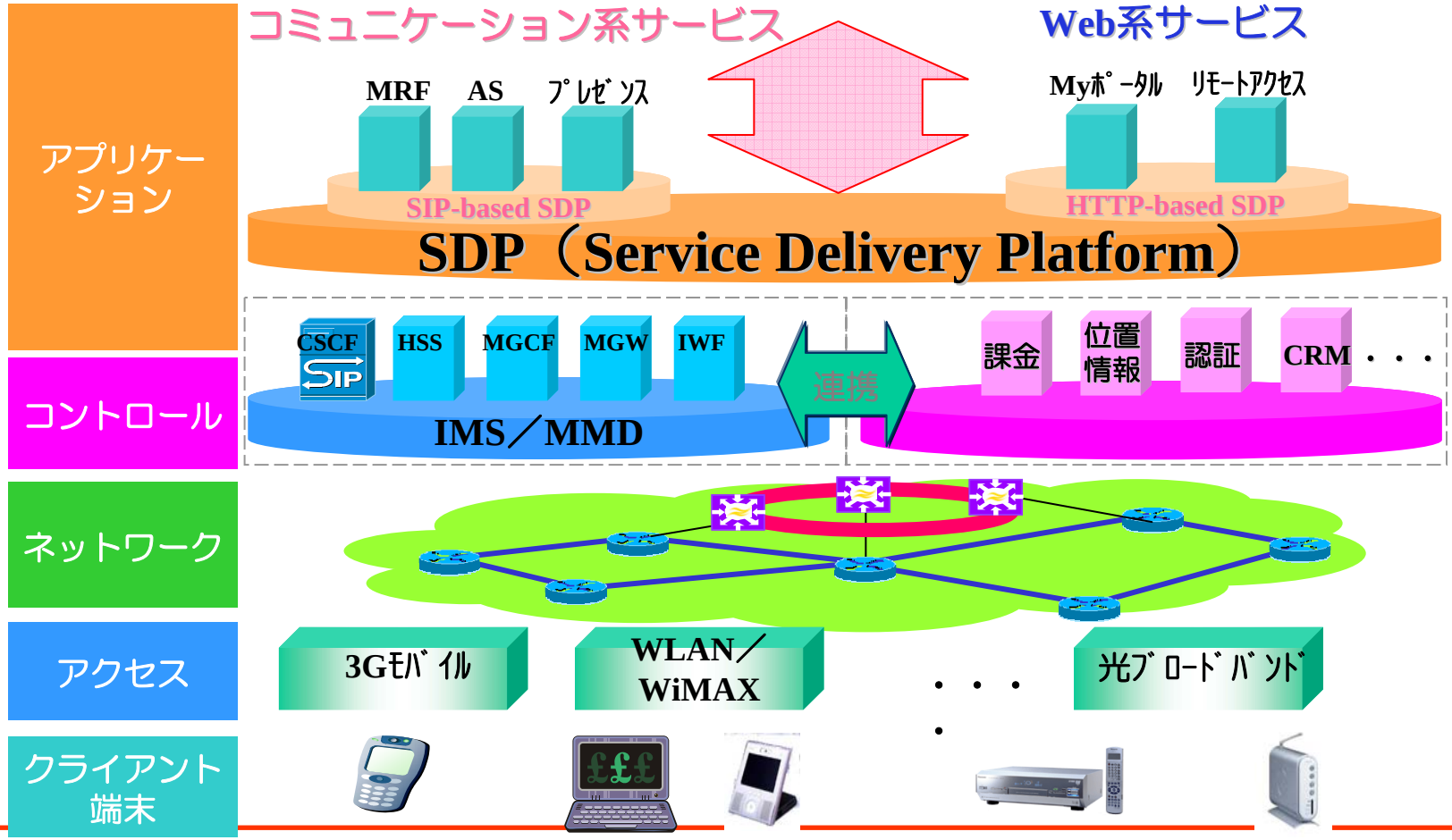
ID連携（ポータル連携）の概念

事業ドメインをまたがる端末間の安全なアクセス制御、コンテンツ連携、課金連携などの実現が期待される。



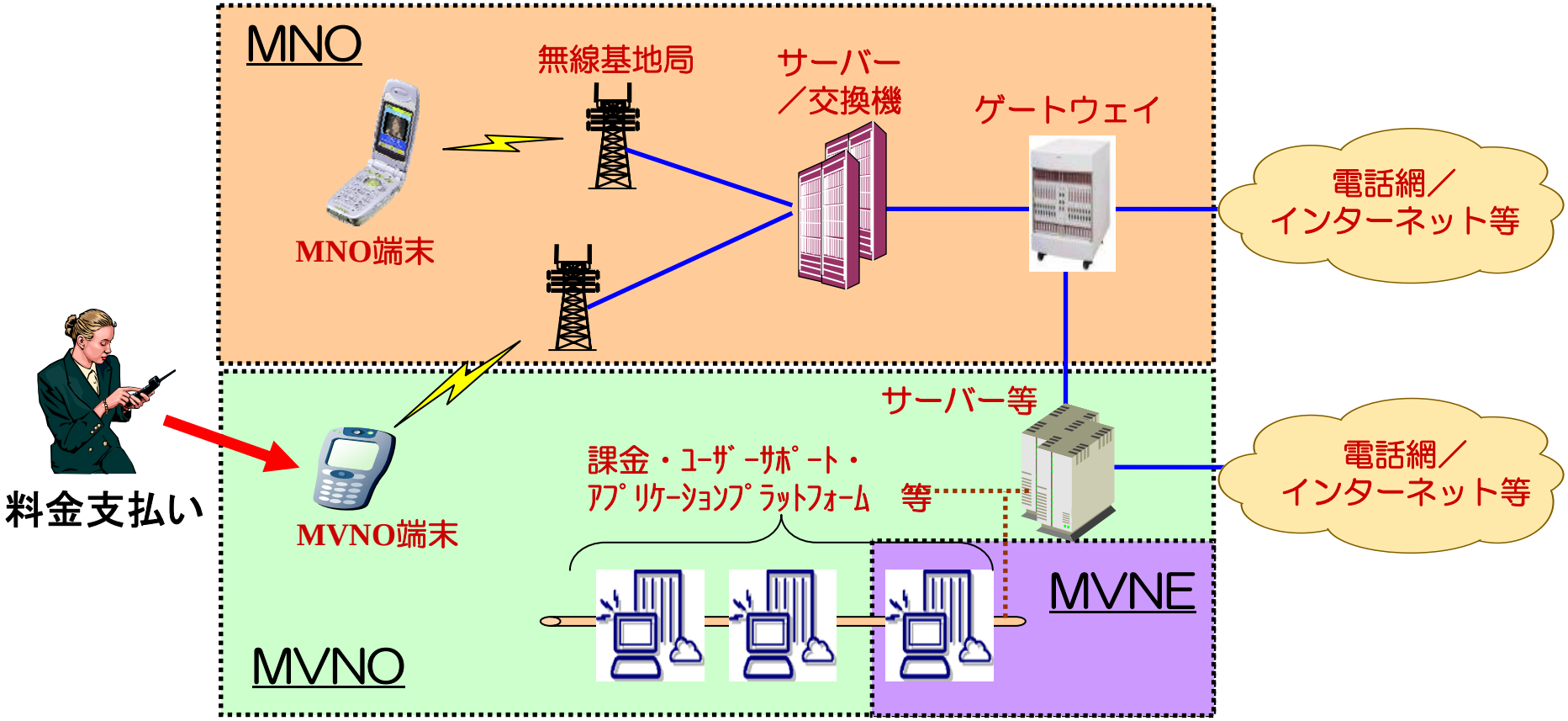
サービス提供プラットフォーム（SDP）

SDPによる網機能のオープンな利用環境が整えば、キャリア以外のプレイヤーによる新規サービス、新規ビジネスモデル提供の可能性が広がる。



MNOとMVNOの連携

MVNO（MVNE）の登場により、モバイル通信サービスの提供形態は複雑・多様化する。



（参考）総務省 MVNOガイドライン

3．モバイルネットワークの現状と課題

社会インフラとしてのケータイに求められる条件

ケータイは既に社会インフラの一要素。
あらゆるインフラとの親和性（接続性）から、将来コア的存在に。

信頼性

- サービス継続性の確保
- ネットワーク稼動率の確保（故障等からの早期復旧）
- 重要通信の確保
- 大規模災害の影響範囲極小化

広義に捉えれば、これらは全てセキュリティ面の課題

安全性

- 個人情報等の機密性確保、外部漏洩回避
- 内外からの違法な攻撃に対するセキュリティ確保

公共性

- 迷惑メール撃退、有害サイトアクセス規制等の社会的責任
- 緊急通信位置情報付加、災害伝言板等の公共性高いサービスの提供

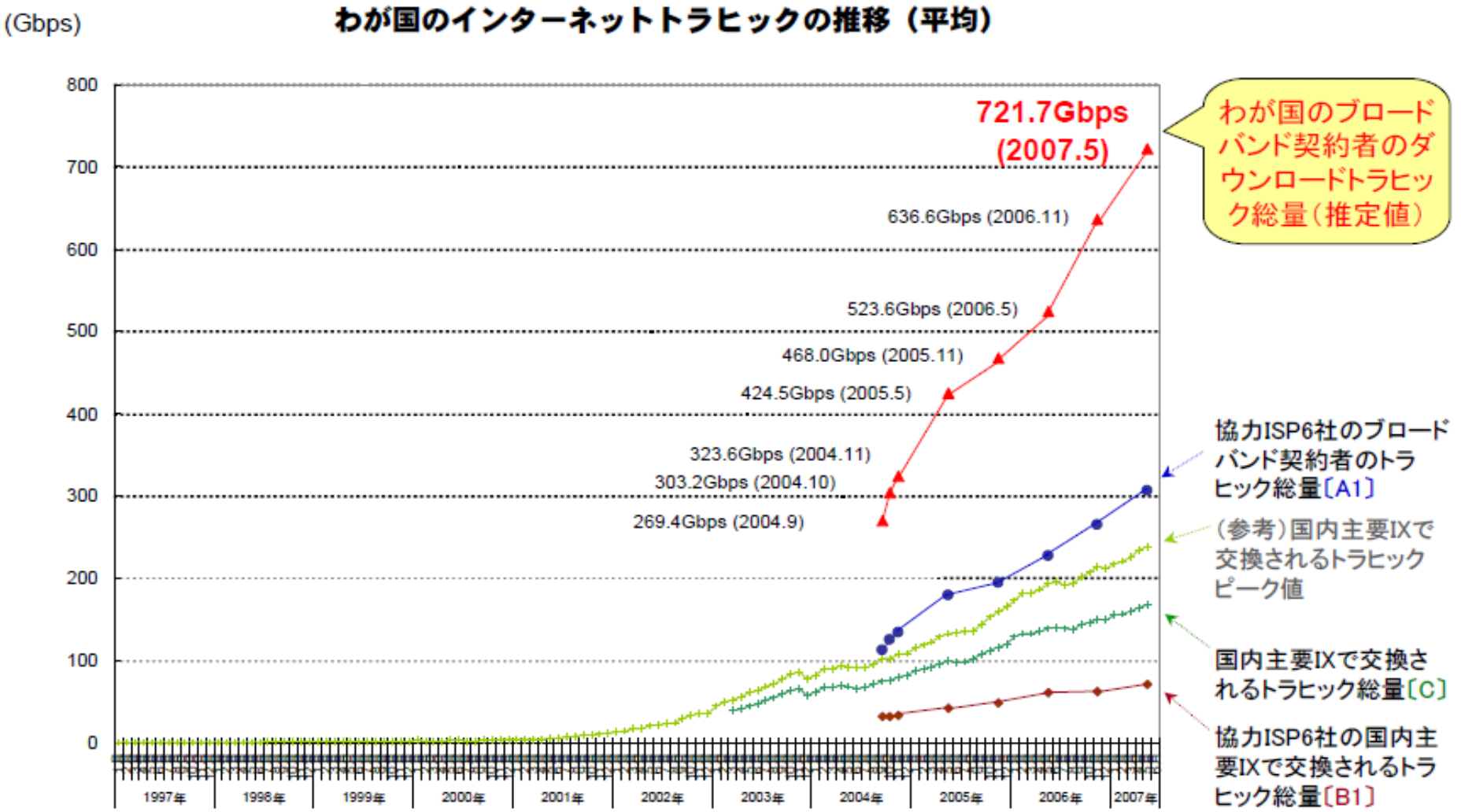
ケータイ利用者への様々な攻撃

携帯利用者の多くは、様々な脅威に曝されていることを知らない。

現状の対策例

盗聴	通信内容の暗号化
迷惑メール・ワンギリ	メールフィルタ等の防御機能 サービス機能の制限
有害サイト	URLフィルタサービスの提供 年齢認証によるwebアクセス制限
ウイルス、DoS攻撃	IDS設置、Fire Wall強化 端末へのウイルススキャン導入
なりすまし	PKI、バイオメトリクス認証
盗難・紛失	移動機遠隔ロックや遠隔データ消去 活性化デバイス（SPCなど）

わが国のインターネットトラヒックの推移



「出典：総務省総合通信基盤局 調査」

(*)1日の平均トラヒックの月平均

携帯ユーザーの利用形態の変化

コンテンツビジネスはダウンロード型から個人参加型へ

・ユーザが*自ら情報発信*

・個人コンテンツがサービス創造に寄与

サービス例

- wikipedia
- YouTube
- ブログ
- SNS
- EZ GREE

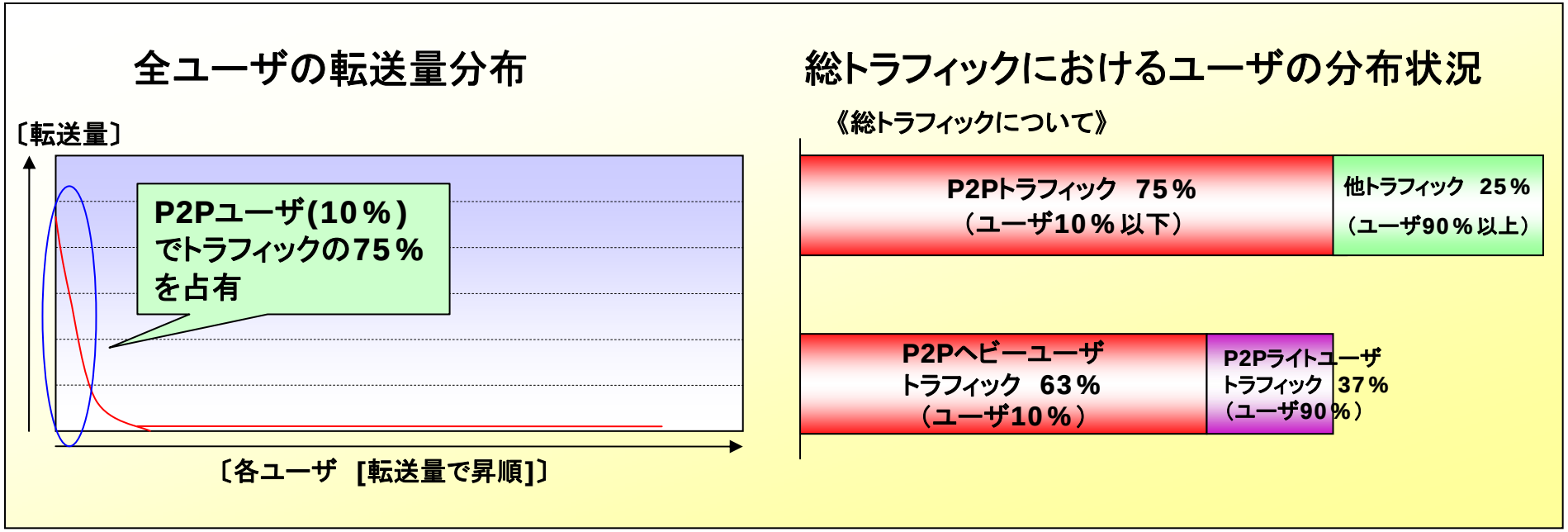
支える技術

ユーザのネット接触機会の拡大	ネットワークのアップロード対応	大容量ストレージの普及
・放送連携、FMBC (IP over デジタル放送)	・FTTH ・ケータイの上り帯域拡大 (EVDO-Rev.A) (HSUPA)	・ネットワークストレージ ・宅内ストレージ HDDレコーダー1TByte

ヘビーユーザーの寡占状況

昨年の「ネットワーク中立性懇談会」にて一部のヘビーユーザーがインターネットトラヒックの多くの割合を占めている状況が報告されているが、携帯利用環境においても同様の傾向がみられるようになっている。

「ネットワーク中立性に関する懇談会　報告書」の記述より抜粋



携帯Eメールの状況

海外からのe-mailの増加

・世界各国から届く（発信国は常に変化・増加）
・英文が多いが、和文記述のものも散見
・送信間隔は一定周期
・個々のIPアドレスから数通ずつ送信
・宛先不明が多く、一般のメール疎通に影響

詐称したメールの増加

・KDDIやauなどのキャリア、またはmixi等を詐称
・ドメインは“@au.jp”,”@ezweb.co.jp”等 架空
・現状は、一見して詐称とわかるレベル
・送信元、urlリンク先サーバは海外

「適正」なのか「迷惑」なのか、送り方だけでなく
本文でも判別が難しいメールが増加

さらに、、、

地域密着型メルマガ利用の拡大

・多くは防災、防犯系のメール
・メール配信に、リアルタイム性が求められる

メルマガ新規参入も拡大

・アドレス帳管理状態の悪い配信業者も
・宛先不明メールが多い送信元を規制

スマートフォンの拡大

スマートフォンでは、オープンなプラットフォームが採用されているため、キャリア以外のプレイヤーがアプリケーションを開発・提供することが可能。新たなビジネスモデルの創成が期待されている。

- 大容量ストレージ
- アプリ追加が簡便・汎用アプリも利用可能
- 多種多様なインターネット接続I/F
- webブラウザもフル機能で搭載

インターネット環境で培われてきた技術の多くがスマートフォンに適用されており、今後、事業者ブランドの携帯電話とは異なる発展形を見せる可能性も。

スマートフォン拡大による脅威

- **汎用プラットフォームの採用、インタフェースオープン化による脅威の増大**
  - 米国で発売されたA社のスマートフォンは、発売後1ヶ月で脆弱性が発見され、攻撃コードも公開された。有力プレイヤーによるスマートフォン提供はハッカー・クラッカーの興味の的。 G社のオープンPFは？
  - オープン化によりアプリ開発の自由度があがるとともに、ハッキング・クラッキングツール類も拡充。
  - 通信ネイティブアプリがオープンPF上に実装されることで、ネットワークへの攻撃手法も多様化。
- **インターネットアプリの移植、開発の自由度向上に伴う潜在的な脆弱性**
  - PC系アプリ（オープンソース）の移植増加により、PC系のウイルスがスマートフォンをも攻撃。
  - PC並みの本格的なウイルス駆除機能がスマートフォンには必要になるかもしれないが、ハードウェア・スペックはPC並みにあらず、限界も。
- **携帯電話の特性も併せもつことで、総合的な脅威は携帯電話やPCよりも大きい**
  - 端末内に、アドレス帳などの個人情報や業務メールなどの機密情報が多く格納される。
  - 利用者はみな常時持ち歩く。ウイルス感染機会はPCとは比較にならない。紛失・盗難の危険性は携帯電話並みに大きい。
  - スマートフォンに搭載されるwebサーバー機能のセキュリティホールを攻撃されると、端末に格納されている個人情報や重要情報が不正に搾取される恐れ。

PC環境のセキュリティ対策と携帯電話のセキュリティ対策の双方をうまく組み合わせた、総合的な対策強化が必要。

４．将来のモバイルIT環境にむけての課題と対策

課題と対策①

海外BOT端末からのスパム攻撃・迷惑メールへの対応

- 設備保護を目的とした受信フィルタだけでは、正当な送信元からのメールが巻き添えになるといった課題もあり、対策として不十分。
- 特定ユーザーを対象としたスピア型攻撃が拡大すると、設備保護対応の名目が成り立たず、ユーザー申告頼みとなる恐れもある。
- 受信側対策だけでは限界、送信元をおさえていく対策も必要か？

ソーシャルエンジニアリングを駆使した犯罪行為への対処

- “なりすまし”させないための技術的対策や法制度整備は次世代環境においても必要。“匿名性を認めても良い範囲”があれば、考慮すべきだが。
- 巧妙化する犯罪手口に迅速に対策するためには、攻撃元の動向や具体的な攻撃手法などについて、関係間で逐次情報共有することも大事。
- ウイルスやマルウエアが関与するケースも想定、ネットワークへの流入状況をリアルタイムモニタすることも有効な手段。通信の秘密遵守との関係は要整理。

課題と対策②

NGN化進展、IPリーチャブルな端末の拡大等による新たな脅威

- 音声サービスのVoIP化が進展。SIPベースの相互接続の時代を見据えると、事業者間で協調した対策検討も必要。
- IPv4→IPv6への移行、IPv6アドレス割り当て端末の普及等でどのような脅威が起こりうるのか？
- オープンな仕様、汎用的な技術が多く採用されることから、事前の対策だけでは考慮漏れの恐れ、対症療法的なメカニズムの確立も重要。

MVNOやスマートフォン、FMCサービス等の登場で、新たなビジネスモデルが伸張

- オープン化の潮流においては、各ステークホルダーが協調してセキュリティ対策に取り組める体制づくりも必要。
- FMCサービスにおいては、どのような脅威が想定されるのか、具体的な分析掘り下げを行うことも有効。

IPv6プロトコル仕様上の課題

既に多くの報告にもあるとおり、以下のようなプロトコル上の課題への対処は、次世代のIPv6環境において必須。

①ステートレス自動設定に関する問題

ネットワーク上に故意に別アドレスを報知する機器やルータが設置されると、IPv6 ネットワークが動作不全に追い込まれたり、他ノードの通信傍受が可能となる恐れがある。

②マルチキャストの悪用

マルチキャスト・アドレスとして「すべてのルーター宛て」や「すべての DHCP サーバー宛て」にパケットを送信すると、サイト中の当該ノードから返答を得られ、全サービス・ノードの IPv6 アドレスが入手される恐れ。

③ICMPv6 のエラー返答の悪用

エラーを引き起こすようなパケットをマルチキャストアドレス宛てに送信すると、大量の ICMPv6 トラフィックが発生。このような不正パケットの始点アドレスが詐称されると、特定のホストに対するDoS 攻撃につながる。

④経路制御ヘッダ利用によるアクセス・フィルタの回避

経路制御ヘッダに関しては、終点アドレスが順次書き換えられるため、経路制御ヘッダを利用することによって終点アドレスによるアクセス・フィルタが回避されてしまう可能性。

⑤中継点オプションヘッダの悪用

中継点オプション・ヘッダが多数付加されると、パケット転送経路途中のルータすべてに負荷がかかり、必要以上のリソースが占有される恐れ。

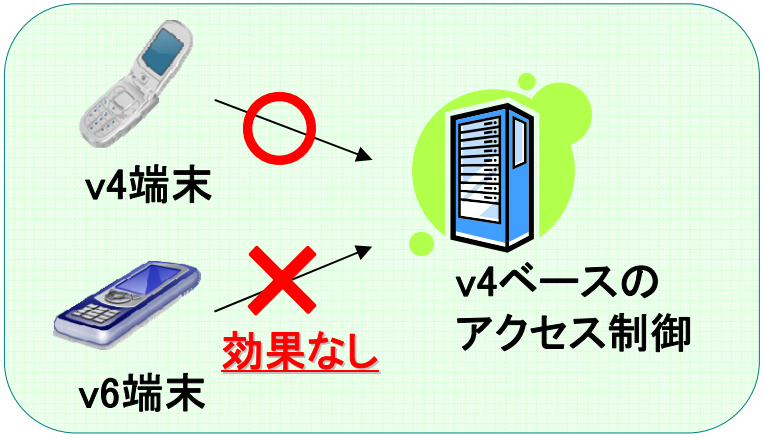
モバイル環境へのIPv6導入課題

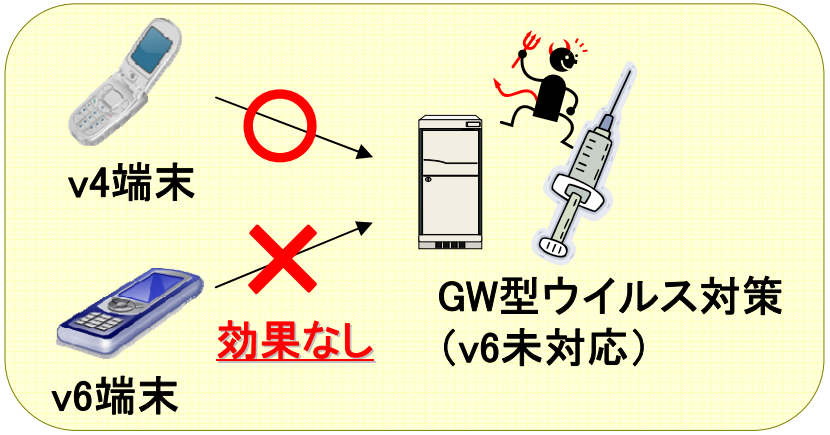
モバイル環境へのIPv6適用が進むことで、インプリ上、運用上のセキュリティ脅威が増大するケースが想定される。

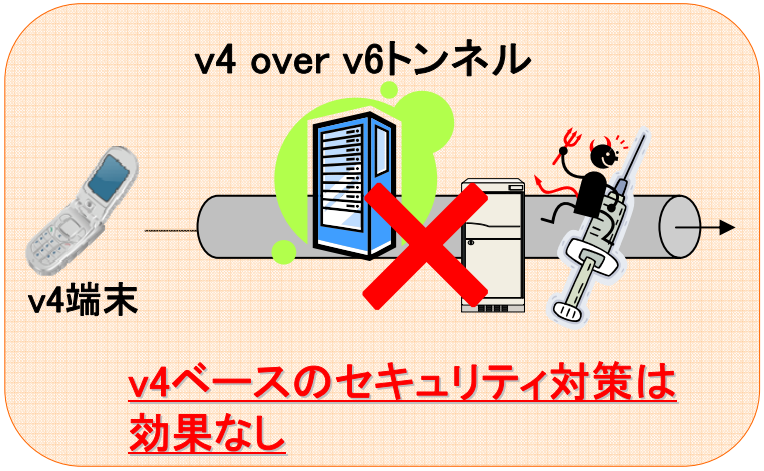
- もともと個人との結びつきが強い携帯電話にIPv6アドレスが割り当てられると、より個人識別性が高まるため、ユーザープライバシーへの配慮は必須。IPv6アドレス自体が電話番号と同じような性格を持つと、電話サービスで起きたことがIPv6環境でも発生する？
- 特定個人を狙った攻撃として、特定IPv6アドレスへの不正パケット送信や、P-Pアプリを悪用した局所的な攻撃なども想定される。
- P-Pアプリの利用が拡大すると、事業者側で不正利用状況が監視できなくなるため、P-Pアプリに特化したセキュリティ対策なるものも要考慮。
- スマートフォンなどの汎用プラットフォーム搭載端末が、IPv6アドレスによりネットへの常時接続を行うようになると、ボット化・ゾンビ化するモバイル端末の数が爆発的に拡大するかも知れない。
- IPv6化は一日にしてならず。IPv4との一時的な並存環境も想定され、運用上の様々な課題・問題が発生する懸念もある。

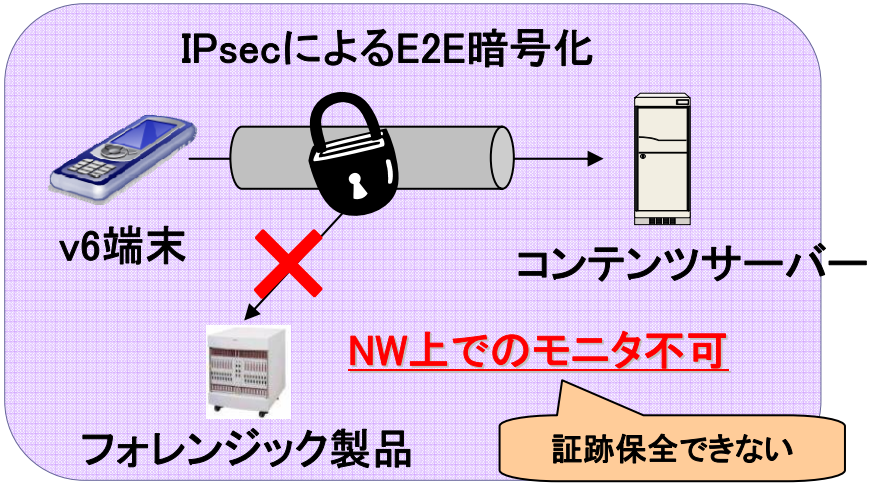
IPv4/IPv6端末並存環境での課題

モバイル環境では、IPv6, v4並存環境が長期化する可能性が高いことから、セキュリティ対策の機能不全が発生しないよう、考慮が必要。









VoIP（SIP）のセキュリティ

- 長いテレコミュニケーションサービスの歴史の中でも、電話サービスは常に可用性と品質（QoS）が厳しく求められてきた。VoIPになっても同じレベルの運用が必要となる。
- 一方で、これまで、様々なセキュリティ上の攻撃を受けてきたIPネットワークが電話サービスのベースとなることから、電話サービスの運用レベルを低下させることがないよう、あらゆる脅威や脆弱性への対処を予め想定し、対策していく必要がある。
- VoIPの脅威や脆弱性を考えるにあたり、
  - VoIP（SIP）プロトコルに対する攻撃
  - VoIPのベースとなるIPネットワークそのものへストレスをかける攻撃手法
  - VoIP運用環境におけるソーシャルエンジニアリングを駆使した犯罪

  に分けて考えてみる。
- さらに、現在のVoIPシステムにおいて、攻撃事例が具体的にどの程度確認されているか、事例検証もよいかもしれない。

VoIP（SIP）の想定攻撃例

VoIP（SIP）プロトコルに対する攻撃

- Fuzzing攻撃：通常とは異なる形式のパケットを送信し、ターゲットとなるSIPサーバー等をクラッシュさせる攻撃。実装段階で生じるセキュリティホールを衝くもの。
- メッセージインジェクション：偽のメッセージをシグナリングチャネルに差し込む攻撃。通話中に突然切れるといったサービス面の影響を引き起こす恐れ。
- 盗聴：IP化により、従来の電話サービスよりも盗聴行為のハードルは低いと想定。シグナリングパケットやRTPパケットの暗号化技術などで対策。

VoIPのベースとなるIPネットワークそのものへストレスをかける攻撃手法

- SIP Flooding：大量のSIPパケット送信によるDoS攻撃。シグナリングパケットやRTPパケットを大量に送りこみ、SIPサーバー等のターゲットを麻痺させる。
- SPIT（SPAM over IP Telephony）：VoIP版スパム。SIPスタックを用いた擬似的な電話発信を大量に行う。電話サービスの安定的運用に対して大きな脅威。
- SIPBOT：BOT化した端末がSPITを繰り返すことにより、影響がさらに拡大。

VoIP運用環境におけるソーシャルエンジニアリングを駆使した犯罪

- ワンギリのような、ナンバースキャニングやSIPスキャニングによる電気通信番号等の不正搾取。

その他（最後に）

- セキュリティ対策の共有、協調により高度な安心・安全環境を構築することは、利用者にとって望ましいこと。ただし、自由な市場競争に任せるべき範囲と、各ステークホルダーが協調して対策を講じるべき範囲を明確にし、分けて議論したい。
- 例えば、
  - 海外BOTなど無差別攻撃については協調して対策。
  - 迷惑メールフィルタのような商品競争色の強い対策は市場競争に任せる？
  - 汎用プラットフォームの脆弱性情報、ソーシャルエンジニアリングによる犯罪行為などは、可能な限り情報共有して対策。

CUSTOMER SATISFACTION.