INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2005 情財第 1068 号

次世代ネットワークに関する
世界的な動向調査報告書

2007 年 4 月

独立行政法人 情報処理推進機構

目次

Ⅰ章　次世代ネットワークの概要と標準化動向及び各国における取り組み状況

1. 次世代ネットワークの概要

1.1 次世代ネットワークの定義について

次世代ネットワークには、以下の二つの解釈がある。
1）現在のインターネットが進化し、機能や通信速度が向上したネットワーク。従来と同様にベストエフォート型のサービスであり、誰でも接続できる。
2）通信事業者が構築する IP ベースのネットワークで、音声や動画の統合されたサービスを提供する。インターネットとは異なり、通信品質やセキュリティが確保されている。

2)の意味での次世代ネットワークは、通信に関する標準化を行う国際機関である ITU(International Telecommunication Union）が提唱した通信ネットワークであり、一般的には NGN(Next Genereation Metwork)と呼ばれている。ITU において、NGN のアーキテクチャや通信プロトコルなどに関する標準化が行われている。

本報告書では、次世代ネットワークを 2）の意味におけるネットワークとして扱うこととし、1）の進化したインターネットの意味では用いない。以降では、次世代ネットワークを NGN と記す。

ITU による NGN の定義 [1]を以下に記載する。

『テレコミュニケーションサービスを提供する機能を有するパケットベースのネットワークで、下記の特徴を有するネットワーク』

- QoS の確保が可能な、複数のブロードバンドトランスポート技術の利用
- サービスに関連する機能がトランスポート技術に依存しない
- ネットワークとサービスプロバイダ及び選択したサービスへの自由なアクセス
- 汎用的なモビリティをサポートし、一貫性のあるユビキタスなサービスを提供する

1.2　NGN が提供するサービス

交換機をベースとした公衆交換電話網(PSTN：Public Switched Telephone Network)において提供されてきた電話(音声通話)サービスは、IP ベースの NGN への移行に伴い、各種データ通信サービスの中の一サービスとして提供されることになる。以下に、NGN が提供するサービスを記す[2]。

- マルチメディアサービス

  - 従来の公衆交換電話網(PSTN)及びモバイルネットワークと接続可能な音声通話サービス
  - Point to Point のインタラクティブマルチメディアサービス
  - インスタントメッセージング/ショートメッセージ/マルチメディアメッセージ等のメッセージングサービス
  - コンテンツ配信サービス
  - ブロードキャスト／マルチキャストサービス
  - ロケーションベースサービス

[1] http://www.itu.int/ITU-T/ngn/definition.html
[2] ITU-T NGN FG Proceedings Part II NGN リリース 1 Scope P118-122

- PSTN/ISDN エミュレーションサービス

  - 従来の電話機を使用して通話が出来るようにするために、IP インフラストラクチャとの整合をとることによって、PSTN/ISDN(Integrated Sevices Digital Network)の機能とインタフェースを提供するサービス。

- PSTN/ISDN シミュレーションサービス

  - IP 電話機やアダプタを介して接続された従来の電話機からの PSTN/ISDN の利用をサポートするためのサービス。IMS(IP Multimedia Subsystem)コンポーネントの機能を使用して、IP インタフェース及びインフラストラクチャにセッション制御を適用することにより実現する。

- インターネットアクセス

  - NGN コアネットワークを介したインターネットアクセスをサポート

- その他のサービス

  - VPN サービス、ファイル転送、オンラインアプリケーション、センサーネットワーク、住宅機器等のリモート制御、OTN(Over the Network)デバイス管理

- 公衆インターネットサービス

  - 合法的盗聴、緊急通信、身障者への対応、ネットワーク／サービスプロバイダーの選択、消費者保護、プライバシーの保護、悪意ある通信のトレースなど(これらのサービスの実装は、本文書のスコープ外である。)

2. NGN の標準化動向

現在の公衆交換電話網(PSTN)では、国際電話や海外へのファクシミリの送信といった、国をまたがる通信ができるのは当然であるが、それを実現するためには、公衆交換電話網の通信プロトコルやインタフェースがグローバルに統一(標準化)されていなければならない。電話やファクシミリのような通信網に関する標準化を行ってきた機関が、国際電気通信連合(International Telecommunication Union：ITU) [3]であり、ITU において公衆交換電話網の標準化が行われた結果、国際電話や海外とのデータのやりとりができるようになったのである。

現在は、インターネットを利用して世界中の誰とでも電子メールのやりとりができたり、世界中のウェブサイトにアクセスしたりすることができるが、これは、インターネットが、IP(Internet Protocol) というグローバルに共通の通信プロトコルをベースに構築されているからである。

公衆交換電話網がベースとしている電子交換機ではなく、ルータやスイッチといった IP ベースの汎用通信機器によって運用される NGN においてもグローバルな通信の確保は必須であり、それに向けた標準化が ITU において行われている。

以下では、ITU における NGN の標準化の概要と NGN のアーキテクチャを紹介する。

[3] ITU の概要については、http://www.ituaj.jp/03_pl/itu/itu_outline.html を参照

2.1 ITU における NGN の標準化

ITU における NGN の標準化は、2003 年に JRG(Joint Rapporteur Group)として開始された。JRG の成果として以下の NGN に関する基本的な勧告が作成された。

- Y.2001: General overview of NGN
- Y.2011: General principles and general reference model for next generation networks

JRG において議論が完結しなかった項目については、2004 年 5 月から 2005 年 11 月までの期間限定で設置された FG-NGN (Focus Group on Next Generation Network)において継続して議論が行われることとなった。

FG-NGN では、サービス要求条件、機能アーキテクチャ、QoS、信号、セキュリティ、ネットワーク移行、次世代パケット網などに関する検討が行われた。その成果が、2005 年 11 月にリリースされた NGN リリース 1 である。NGN リリース 1 は、NGN FG Proceeding[4]として、2 部構成の文書にまとめられている。

2003 年から 2005 年にかけて ITU-T が発行した NGN に関する主な文書や勧告を以下に示す。

■ 2003 年

- Y.2001 勧告 ：General overview of NGN　NGN の概念を定義
- Y.2011 勧告 ：General principles and general reference model for Next Generation Networks
  NGN の参照モデルを定義

■ 2005 年

- NGN リリース 1

FG-NGN によりまとめられた最終的な文書や合意内容の総称であり、NGN のスコープ、要求条件、アーキテクチャ、セキュリティ要求条件、移行シナリオ等に関する文書により構成される。

2.2 FG-NGN の概要

FG-NGN における標準化作業は、以下に示す WG1～WG7 の 7 つのワーキンググループにより行われた。

- WG 1 SR (サービス要件)
- WG 2 FAM (機能アーキテクチャとモビリティ)
- WG 3 QoS (サービス品質)
- WG 4 CSC (制御とシグナリング)
- WG 5 SeC (セキュリティ能力)
- WG 6 Evol (進化)
- WG 7 FPBN (次期パケットベースベアラネットワーク)

FG-NGN において議論された主なトピックを以下に示す。

1. Services requirements and capabilities

[4] http://www.itu.int/ITU-T/ngn/release1.html

2. Functional architecture and mobility
3. Quality of service (QoS)
4. Control aspects (including signalling)
5. Security capability (including authentication)
6. Migration of current networks into NGN (PSTN, ISDN etc.)
7. Future packet based network requirements

NGN リリース 1 の公表をもって、FG-NGN はその役割を終えたが、FG-NGN で積み残しとなった課題については引き続き NGN-GSI(Global Standard Initiative)[5]において議論されることとなった。

2.3 NGN-GSI の概要

NGN-GSI では、SG13：Next Generation Networks がリーディンググループとなって、標準化が進められている。

NGN-GSI におけるスタディグループのうち、主なものを以下に示す[6]。

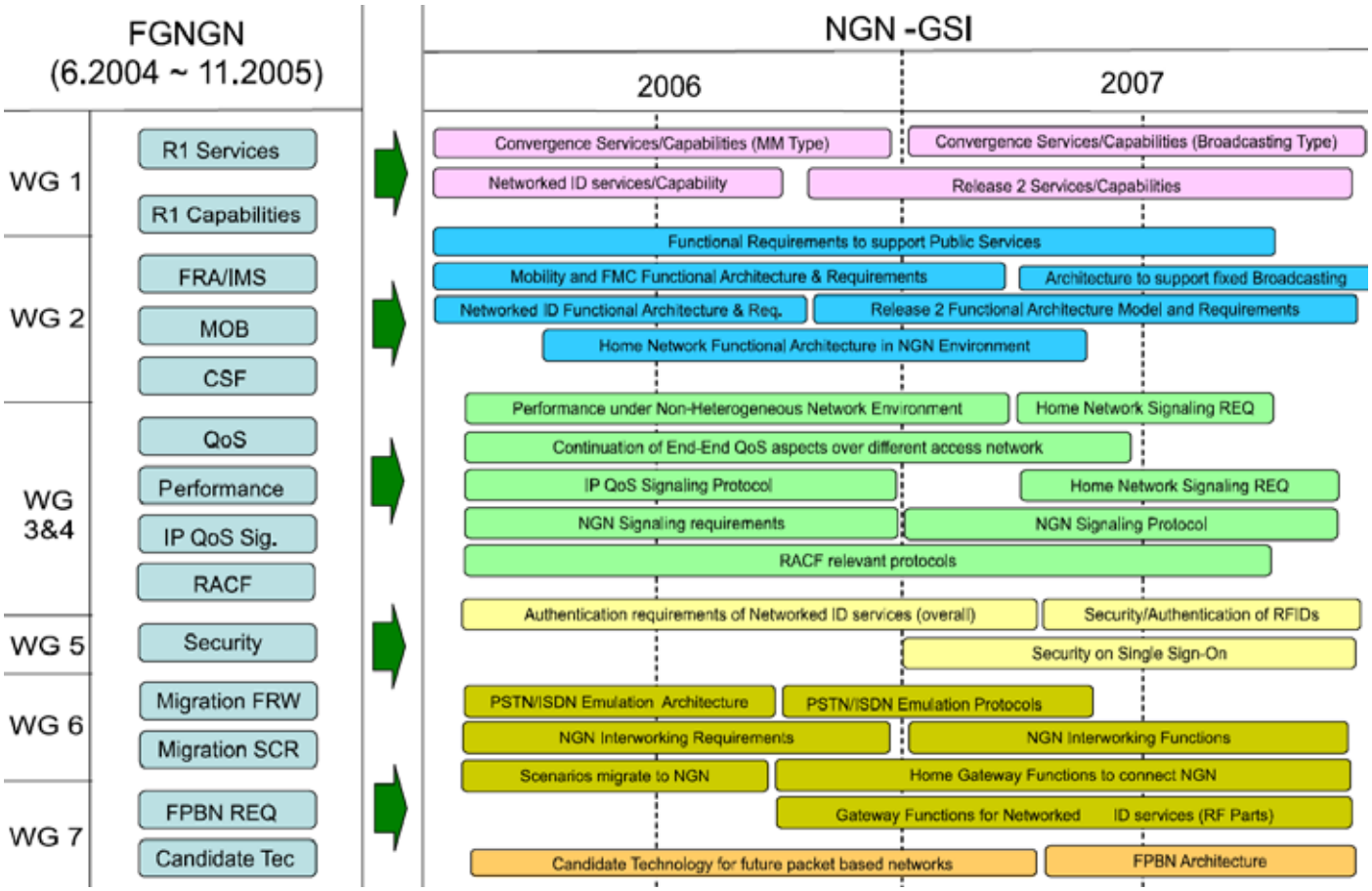
SG 2	numbering, naming and addressing
SG 4	NGN Management
SG 9	cable and television networks etc.
SG 11	Network signaling requirements, control functional architectures and protocols in emerging NGN environments
SG 12	Performance and quality of service
SG13	Next Generation Networks
SG 15	broadband access and transport
SG 16	multimedia terminals and applications
SG 17	NGN Security
SG 19	Fixed and Mobile Convergence (FMC) and Mobility Management

また、NGN-GSI において議論されている項目のうち主なものを以下に示す[7]。

- リリース 2 のサービスと機能
- 機能アーキテクチャと要求条件
- モバイルマネジメントと FMC
- IPv6 の NGN への適用
- End-to-End QoS
- NGN リソース受付制御のあるシグナリング
- 移行と相互動作
- NGN セキュリティ
- ホームネットワーキング(2005 年に JCA-HN(Joint Coordination Activity)が設置された)
- ネットワークの側面から見た身元証明システム(RFID を含む)
- IPTV (2006 年に IPTV-FG(Focus Group)が設置された)

NGN-GSI の 2007 年までのロードマップと FG-NGN との対応を図 1.1 に示す [7]。

[5] http://www.itu.int/ITU-T/ngn/index.phtml
[6] http://www.itu.int/ITU-T/studygroups/index.phtml
[7] ITU-T Next Generation Networks, Nov 2006



(出所 ：ITU-T Next Generation Networks, Nov 2006)

図 1.1　NGN-GSI のロードマップと FG-NGN との対応

2.4　NGN の主要な構成要素 IMS

NGN は、IP をベースとしたネットワークであり、従来の公衆交換電話網と同様の音声通話サービスを提供するためには、IP ベースのセッション制御(電話網における通信路の確立やサービスの制御)やデータの遅延・損失のリアルタイム制御といった機能を有するデータ通信装置が必要となる。

そのような機能を有するデータ通信装置の開発では、携帯電話の方が先行しており、IP ベースでのセッション制御プロトコルとして SIP(Session Initiation Protocol)[8]が、SIP による通信制御を行う装置として IMS (IP Multimedia Subsystem)がそれぞれ開発されていたことから、NGN においても携帯電話網で使用されているこれらのプロトコルや通信装置を固定通信ネットワーク向けに改良して使用することとなった。したがって、NGN において、セッション制御や課金、QoS といった機能を提供するのが IMS であり、そのベースとなるプロトコルが SIP ということになる。

なお、SIP は IETF(Internet Engineering Task Force)[9]において標準化が行われたプロトコルであり、IMS の仕様作成と標準化は、第 3 世代携帯電話に関する標準化をとりまとめている 3GPP(3rd Generation Partnership Project)[10]により行われた。ITU-T では、3GPP の Release7 の IMS 仕様を参照している。

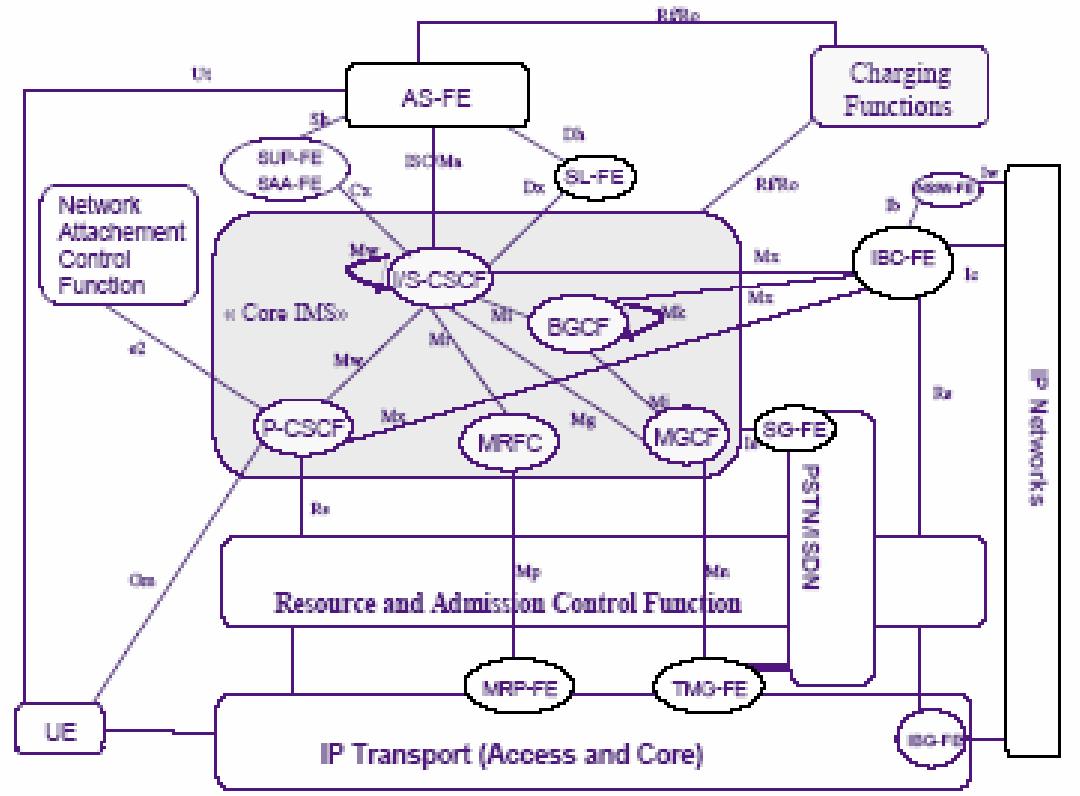
[8] http://www.ietf.org/rfc/rfc3261.txt?number=3261
[9] http://www.ietf.org/
[10] http://www.3gpp.org/

2.4.1　IMS の概要

IMS は、事業者が提供する SIP ベースのサービスへのアクセスをサポートするコアネットワーク機能要素の集合である。IMS の概要は以下のようになる[11]。

- 通信相手の認証、通信相手の発見、番号の翻訳、端末が有する能力のネゴシエーション、セッション(通信)の確立と終了などを行う。
- 課金、請求、セキュリティをサポート
- アプリケーションサーバに対する課金、セキュリティのインタフェースを提供
- トランスポートレイヤとのインタフェースをサポートし、QoS 機能やサービスレイヤ／セッションレイヤ／トランスポートレイヤ間の課金の整合を確保

IMS のアーキテクチャを図 1.2 に示す[11]。



(出所 ：TTC シンポジウム資料 NGN リリース 1 アーキテクチャと今後の展望)

■ IMS の主な構成要素の凡例

UE : User Equipment　ユーザ機器

HSS : Home Subscriber Server　ホームサーバ ： ユーザ情報を一元管理

P-CSCF : Proxy Call Session Control Function　ユーザが最初に接続する SIP サーバ

S-CSCF : Serving Call Session Control Function　ユーザが契約している ISP の SIP サーバ

AS : Application Server　アプリケーションサーバ

PSTN : Public Switched Telephone Network　電話網

PCF : Policy Control Function ポリシー制御機能

MGW : Media Gateway　メディアゲートウエイ

MGCF : Media Gateway Control Function　メディアゲートウエイ制御機能

MRFC : Media Resource Function Controler メディアリソース機能制御装置

[11] TTC シンポジウム資料 NGN リリース 1 アーキテクチャと今後の展望（2006 年 10 月）

図 1.2　IMS のアーキテクチャ

2.5　NGN のアーキテクチャ

NGN のアーキテクチャは Y.2011 勧告によって規定されている。NGN の特徴の一つは、サービスの制御とデータ伝送を分離している点にある。Y.2011 勧告では、NGN をストラタムとプレーンによって構成されるネットワークであるとしており、ストラタム及びプレーンそれぞれの観点から NGN を構成するエレメントを定義している。

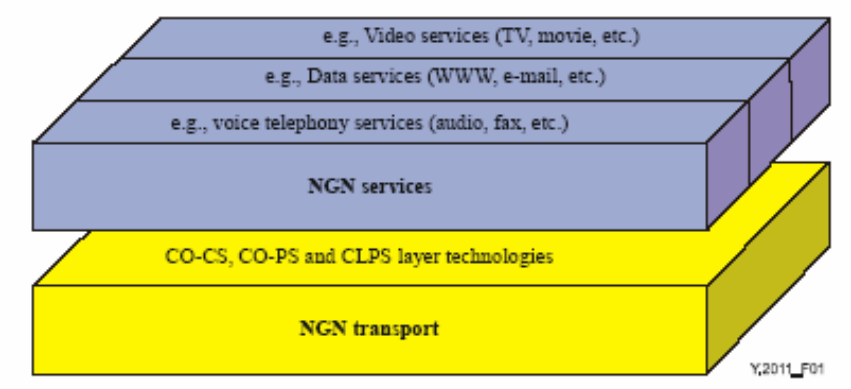
■　ストラタム
　データの伝送やリソース管理といった特定の機能を提供するパーツ

■　プレーン
　ストラタム内のデータの転送に使用される機能あるいは、ストラタム内のエンティティの制御や管理のために使用される機能

つまり NGN は、サービス制御を行うサービスストラタムと、データ伝送を司るトランスポートストラタムの各ストラタムにより構成され、サービスストラタムとトランスポートストラタムはそれぞれ、データプレーン、コントロールプレーン、マネジメントプレーンによって構成されるということになる。
サービスストラタムは、ユーザサービスに必要なデータの伝送を行うユーザ機能と、サービスリソース及びネットワークサービスの制御・管理機能を提供する。
トランスポートストラタムは、データ伝送機能と、データ伝送に必要なリソースの制御・管理機能を提供する。トランスポートストラタムは、データ伝送の主体であるユーザとサービスプラットフォームに対して、以下の機能を提供する。

- ユーザ同士の接続
- ユーザとサービスプラットフォームの接続
- サービスプラットフォーム同士の接続

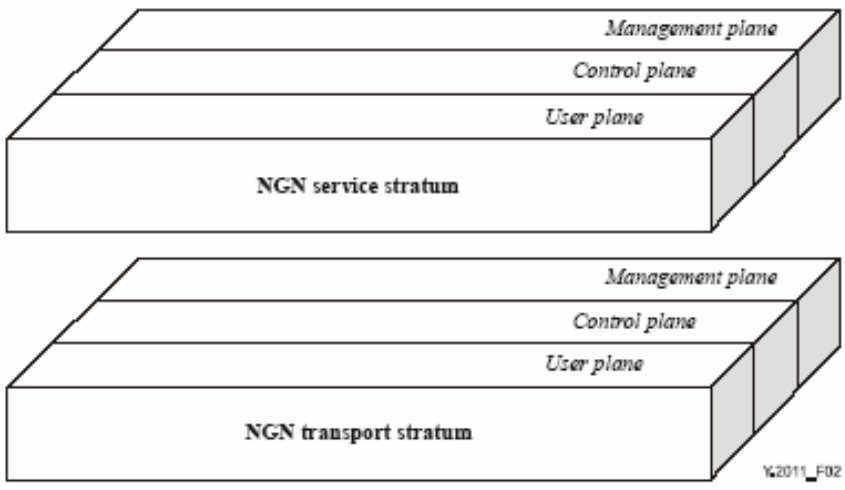
ストラタムとプレーンの二つの観点による NGN のアーキテクチャを図 1.3 に示す[12]。



サービスストラタムとトランスポートストラタム

(出所 ITU-T Y.2011)

[12] ITU-T Y.2011

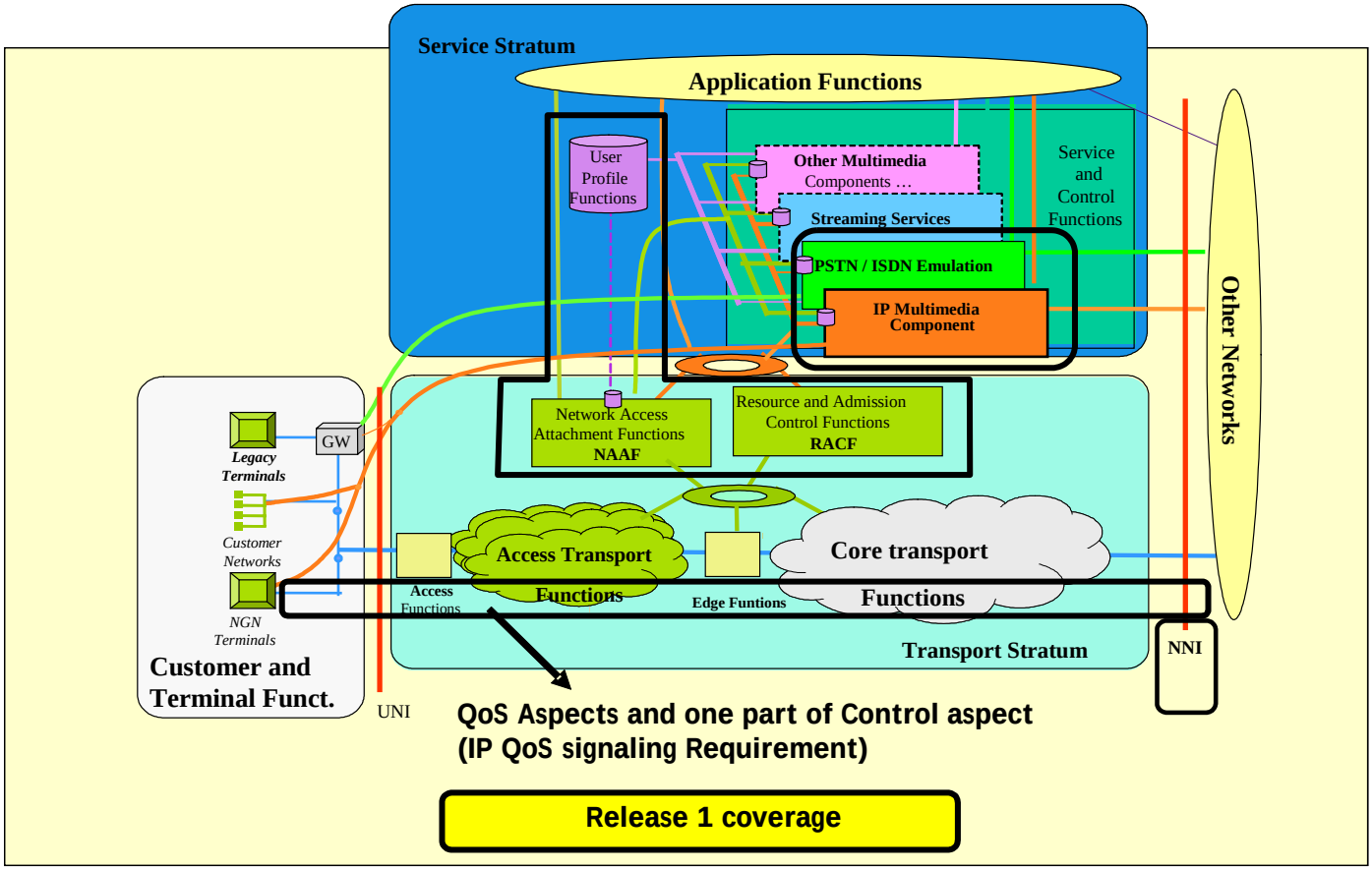


サービスストラタム／トランスポートストラタムと各プレーンの関係

（出所 ITU-T Y.2011）

図 1.3　ストラタムとプレーンの二つの観点による NGN のアーキテクチャ

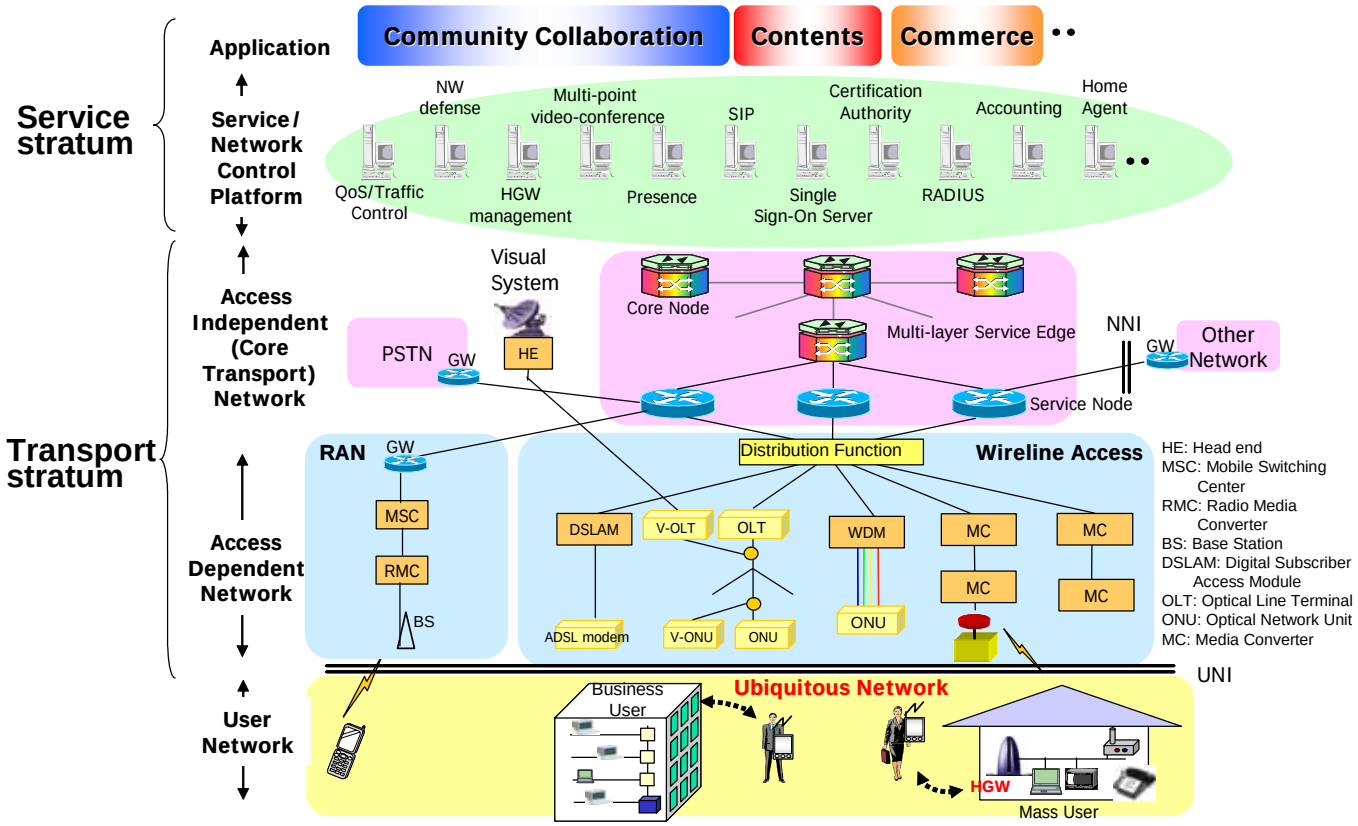
サービスストラタム及びトランスポートストラタムと、NGN の各機能要素との対応を図 1.4 に示す [7]。図中の黒い線で囲まれた部分が NGN リリース 1 がカバーする範囲である。



（出所 ：ITU-T Next Generation Networks, Nov 2006）

図 1.4　サービスストラタム及びトランスポートストラタムと NGN の各機能要素との対応

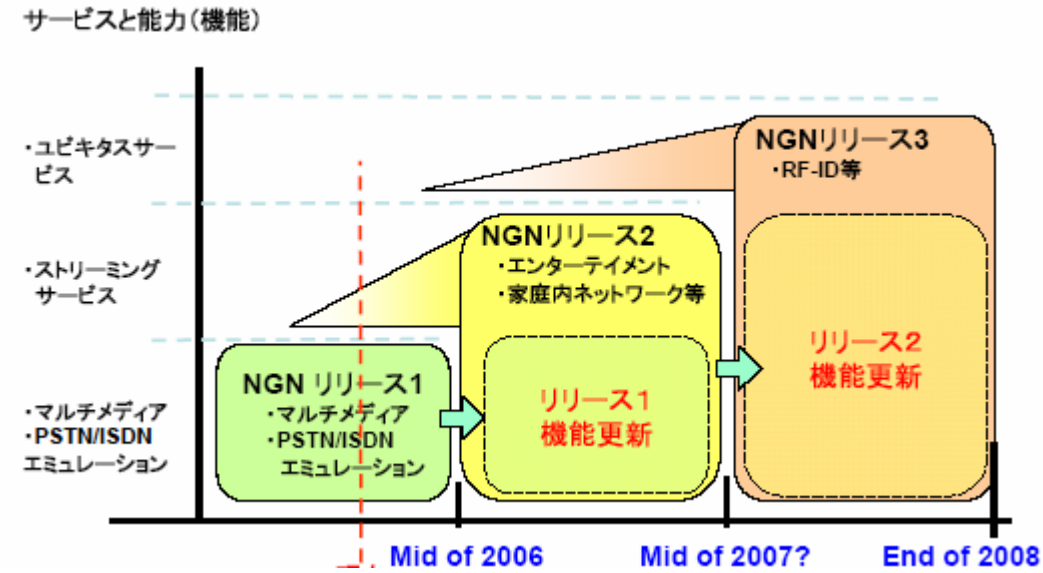
各ストラタムと対応するネットワークエレメントのイメージを図 1.5 に示す [7]。



(出所 ：ITU-T Next Generation Networks, Nov 2006)

図 1.5　各ストラタムと対応するネットワークエレメントのイメージ

今後の NGN のリリーススケジュールの概要を図 1.6 に示す[13]。



(出所： 次世代 IP ネットワーク推進フォーラム 『我が国における NGN 標準化の重要性』)

図 1.6　今後の NGN のリリーススケジュールの概要

[13] 次世代 IP ネットワーク推進フォーラム 研究開発・標準化部会チュートリアル資料 『我が国における NGN 標準化の重要性』 http://ngnforum.nict.go.jp/

NGN リリース 1 の策定において中心的な役割を演じたヨーロッパの標準作成組織 ETSI(European Telecommunications Standards Institute)[14] の技術委員会である TISPAN(Telecommunications and Internet converged Services and Protocols for Advanced Networking)[15] の 2007 年 1 月 24 日時点のワークプラン[16]によれば、TISPAN における NGN セキュリティリリース 2 の検討は、2007 年 5 月にかけて作業が行われる予定となっている。

2.6 NGN セキュリティの標準化状況

2.6.1 NGN リリース 1 のセキュリティ要件

2005 年に作成された NGN リリース 1 におけるセキュリティ要件を以下にまとめる[17]。

■ 一般的なセキュリティ要件は、X.805 勧告のコンセプトに基づいている。

■ トランスポートストラタムに対するセキュリティ要件

- NGN 顧客ネットワークドメイン
- 顧客ネットワークと IP コネクティビティアクセスネットワーク(IP-CAN)とのインタフェース
- コアネットワーク機能
- NGN 顧客ネットワーク相互のインタフェース

■ サービスストラタムに対するセキュリティ要件

- IMS コアネットワークセキュリティアーキテクチャ
- IMS セキュリティアーキテクチャインタフェース要件
- トランスポートドメインと NGN コアネットワークとのインタフェース
- アプリケーションとコアネットワークとのインタフェース
- アプリケーションドメインセキュリティ
- NGN 顧客ネットワークとアプリケーションとのインタフェース
- VoIP セキュリティ要件
- 緊急通信サービス及び災害救助に対するセキュリティ要件
- オープンサービスプラットフォーム及び付加価値サービスプロバイダのセキュリティ

2.6.2 ITU における NGN セキュリティの標準化状況

現在、ITU における NGN セキュリティの標準化は、SG17 を Lead Study Group として進められている[18]。 また、SG13 において、NGN セキュリティフレームワークの検討が行われている。NGN のセキュリティ要件に関する検討は一般的に、NGN のアーキテクチャやプロトコル、機能といった、NGN のベースとなる部分の仕様が固まった後に議論されるため、これらの検討状況に比べると遅れていたが、2006 年 7 月に開催されたジュネーブ会合[19]において、NGN リリース 1 のセキュリティ要件に関する勧告案 Y.2701 (Y.NGN-Security)：Security Requirements for NGN Release 1 が提出され、現在承認プロセスにあることから、今後、NGN のセキュリティに関する検討が加速することが予測される。

---

[14] http://www.etsi.org/
[15] http://www.etsi.org/tispan/
[16] http://portal.etsi.org/docbox/TISPAN/Open/Information/TISPAN_WorkPlan/
[17] NGN FG Proceedings Part I　P75-76
[18] www.itu.int/ITU-T/studygroups/com17/tel-security.html
[19] http://www.itu.int/events/eventdetails.asp?lang=en&eventid=7643

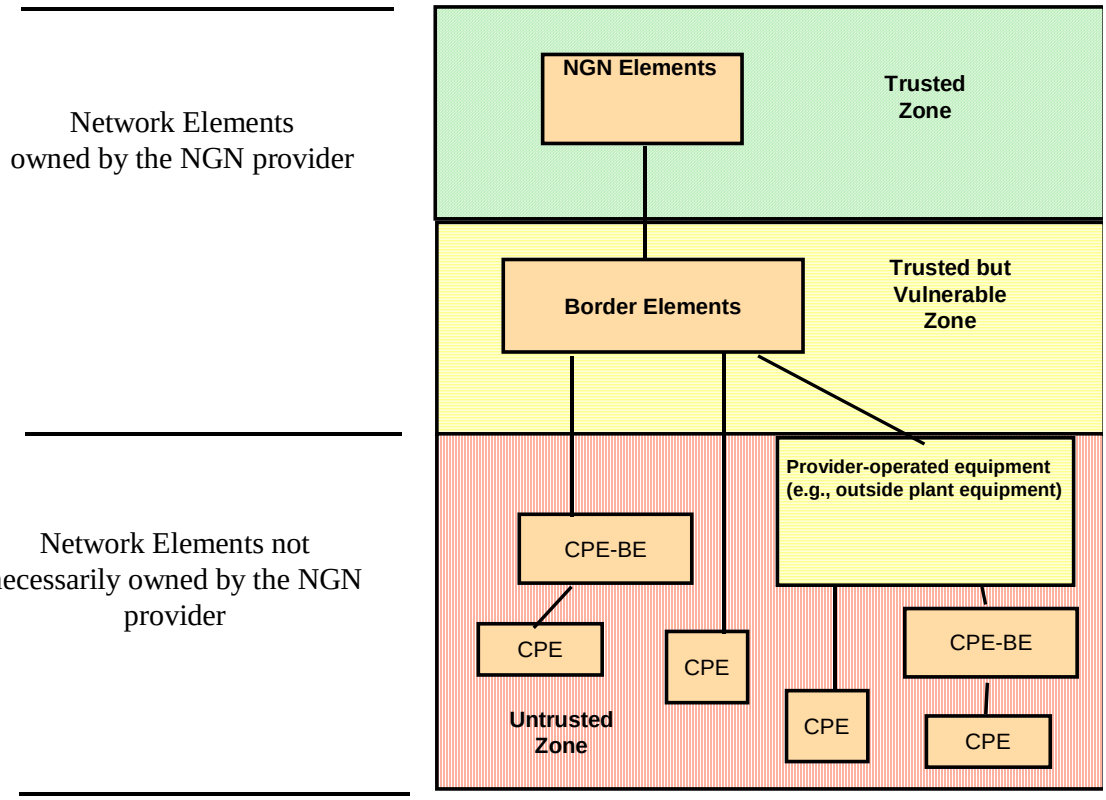
Y.2701 は、ネットワークの資産、サービス、エンドユーザの通信や情報を保護するために、ネットワークが提供するセキュリティについての要求条件を規定したもので、主な内容は以下のようになっている [11]。

① End-to-End のセキュリティはスコープ外。
② X.805 をベースに NGN におけるセキュリティ上の脅威を分析。
③ セキュリティトラストモデルを規定。
NGN プロバイダが所有している機器であるか、物理的に自分の管理下にあるかといった基準により、個々の機器が属するゾーンを以下の 3 つに分類し、ゾーン毎にセキュリティ要求条件を規定。

- trusted zone：信頼できるゾーン
- untrusted zone：信頼できないゾーン
- trusted but vulnerable zone：信頼できるが脆弱性があるゾーン

④ セキュリティの目標を、共通の目標および X.805 勧告が定める 8 個のセキュリティ分野：アクセス制御、認証、否認不可、データ秘匿性、通信セキュリティ、データ完全性、可用性、プライバシーについて規定。
⑤ セキュリティの要求条件を、共通条件とトラストゾーンごとに必要な条件とに分けて規定。
⑥ Appendix として ETS (緊急通信)を国際間接続する時の要求条件を規定。

図 1.7 に、Y.2701 に規定されているセキュリティトラストモデルを示す [11]。



(出所：TTC シンポジウム資料 NGN リリース 1 アーキテクチャと今後の展望)

凡例　CPE：Customer Premise Equipment：ユーザ側の機器
CPE-BE：CPE Border Element

図 1.7　Y.2701 に規定されているセキュリティトラストモデル

ゾーンについての基本的な考え方は、NGN 事業者が保有する機器には信頼できる NGN 機器と、信頼できるが脆弱性がある境界機器があり、NGN 事業者が保有していない機器(ユーザ機器など)は信頼できないということになる。

2.6.4 ITU-T が策定した NGN セキュリティ関連の勧告及び今後勧告化予定の項目

ITU-T がこれまでに策定した NGN セキュリティ関連の勧告と今後勧告化が予定されている項目を以下に示す。

1. 策定済みの勧告

- セキュリティアーキテクチャ
  - X.800：Security Architecture for Open Systems　オープンシステムのセキュリティアーキテクチャ
- 通信のセキュリティ
  - X.805：Security architecture for systems providing end-to-end communications
    end-to-end 通信システムのセキュリティアーキテクチャ
  - X.1051：Information security management system Requirements for telecommunications
    通信事業者における情報セキュリティマネジメントシステム（ISMS-T）
  - X.1081：A framework for specification of security and safety aspects of telebiometrics
  - X.1121：Framework of security technologies for mobile end-to-end communications
  - X.1122：Guideline for implementing secure mobile systems based on PKI
- セキュリティプロトコル
  - X.273：Network layer security protocol
  - X.274：Transport layer security protocol
- セキュリティ技術
  - X.841：Security information objects for access control
  - X.842：Guidelines for the use and management of trusted third party services
  - X.843：Specification of TTP services to support the application of digital
- ディレクトリサービスと認証
  - X.509：Public-key and attribute certificate frameworks　公開鍵証明書フレームワーク

2. 今後勧告化が予定されている項目

ITU において現在勧告化に向けて作業が進められている NGN セキュリティ関連の主な標準には、以下がある[20]。

- X.805+　　Division of the security features between the network and the users

[20] http://www.itu.int/ITU-T/studygroups/com17/ict/part03.html

• X.805nsa	Network security certification based on ITU-T Recommendation X.805
• X.ngn-akm	Authentication and key management framework for NGN
• X.1051 (Revised)	Information security management guidelines for telecommunications based on ISO/IEC 17799
• X.1051 (2004) Amd.1	Information security management system for telecommunications (ISMS-T), enhancements
• X.imm	Incident management methodology
• X.ism-1	Code of practice for information security management
• X.ism-2	ISMS requirements specification
• X.rmg	Risk management guidelines in use of X.1051
• X.rmm	Risk management methodology
• X.sim	Security incident management guidelines for telecommunications
• X.homesec-1	Framework for security technologies for home network
• X.sap-2	Secure communication using TTP service
• X.websec-1	Security Assertion Markup Language (SAML)[21]

X.805 勧告をベースとしたネットワークとユーザとのセキュリティ機能分担(X.805+)やネットワークセキュリティ認証(X.805nsa)、認証と鍵管理(X.ngn-akm)、通信事業者向けセキュリティマネジメントガイドライン ISMS-T(X.1051 (2004) Amd.1)、インシデントマネジメント(X.imm, X.sim)、リスクマネジメント(X.rmg, X.rmm)、ホームネットワークのセキュリティ(X.homesec-1, 2, 3)、TTP(Trusted Third Party)を利用したセキュア通信 (X.sap-2)、SAML (X.websec-1)などの標準化が検討されていることがわかる。

2.7 ETSI TISPAN による NGN セキュリティ要求条件

本節では、ETSI TISPAN が作成した NGN におけるセキュリティに関する文書の概要を紹介する。ETSI TISPAN は、NGN のセキュリティに関する以下の文書を作成している。

- ETSI TS 187 001 V1.1.1 NGN Security：Requirements
- ETSI TR 187 002 V1.1.1 NGN Security：Threat and Risk Analysis
- ETSI TS 187 003 V1.1.1 NGN Security：Security Architecture
- ETSI TS 102 165-1 V4.2.1 Method and proforma for Threat, Risk, Vulnerability Analysis Part 1

2.7.1 TS 187 001 V1.1.1 NGN Security：Requirements

本文書は、NGN リリース 1 のセキュリティ要件をまとめたものであり、以下のセキュリティ要件を規定している。

- セキュリティポリシー
- 認証、認可、アクセス制御
- アイデンティティ、セキュア登録
- 通信とデータのセキュリティ
- プライバシー
- 鍵管理
- セキュアマネジメント

[21] ID やパスワードなどの認証情報を安全に交換するための XML 仕様。標準化団体 OASIS が策定。
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

- NAT／ファイアウォールの相互動作
- 否認防止
- 可用性と DoS 攻撃からの保護
- 信頼性
- 保証
- セキュリティメカニズムの強度

また、リリース 1 セキュリティ要件と、NASS(Network Access SubSystem： 登録や認証などのアクセス制御を行う)、RACS(Resource Admission Control Subsystem： リソース制御や優先度付けなどの転送制御を行う)、IMS、PES(PSTN/ISDN Emulation Subsystem)、AS(Application Server)などの NGN の構成要素との対応についても記述している。

2.7.2 TS 187 003 V1.1.1 NGN Security：Security Architecture

本文書は、NGNリリース1のセキュリティアーキテクチャを規定したもので、TS 187 001 V1.1.1 NGN Security：Requirements に規定されているセキュリティ要件を満たすとともに、NGNの機能アーキテクチャと各サブシステムを保護するためのセキュリティアーキテクチャについても言及している。

この文書の規定は、ITU-T Recommendation I.130『Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN』の要求条件に従ったものである。

NGN リリース 1 のセキュリティアーキテクチャは、以下のパーツにより構成される。

- NGN セキュリティドメイン
- セキュリティサービス：認証、認可、ポリシー執行、鍵管理、機密性、完全性
- セキュリティプロトコル：以下のプロトコルに関するものを含む
  - IMS アクセスセキュリティ
  - SIP HTTP ダイジェスト
  - XCAP
- アプリケーションごとの鍵管理
- セキュリティゲートウエイ機能
- レガシー端末のセキュアアクセスのための IMS Residential Gateway
- NGN セキュリティメカニズム
  - 明示的な回線認証に基づく NASS 認証
  - 物理的な回線認証に基づく NASS 認証
  - NASS-IMS バンドル認証
- NGN サブシステムのセキュリティ対策

2.7.3 NGN におけるセキュリティ上の脅威及びリスクの分析

ETSI TISPAN は、NGN におけるセキュリティ上の脅威及びリスクの分析に関する文書として、以下の文書を作成している。

- ETSI TS 102 165-1 V4.2.1 Methods and protocols Part 1

Method and proforma for Threat, Risk, Vulnerability Analysis

Threat Vulnerability and Risk Analysis(TVRA)の詳細な方法を規定。

- ETSI TR 187 002 TISPAN NGN Security：Threat and Risk Analysis

  NGN リリース 1 の二つのシナリオである、PSTN/ISDN エミュレーション(PES)と NASS-IMS における認証を対象として行ったリスク分析の結果が記載されている。

これらの文書におけるリスク分析は、攻撃による影響(impact)にフォーカスしたものとなっており、攻撃に対する耐性にフォーカスしたセキュリティ要件であるISO15408を補完するものという位置づけである。リスク分析において想定する脆弱性は、ISO/IEC 13335『Information technology - Security techniques - Guidelines for the management of IT security』の定義に基づいたものとなっており、Threatsによって悪用されるWeaknessの組み合わせによりモデル化されている。

ETSI TS 102 165-1 におけるリスク分析は、以下のステップにより行われる。

1) Identification of the objectives resulting in a high level statement of the security aims and issues to be resolved.
   高度なセキュリティが求められると判断された対象と解決すべき課題の明確化

2) Identification of the requirements, derived from the objectives from step 1.
   ステップ 1 の目的から導かれる要件の明確化

3) Inventory of the assets.
   資産のインベントリ

4) Identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result.
   システムの脆弱性、脆弱性を悪用する脅威、発生して欲しくないインシデントの明確化と分類

5) Quantifying the occurrence likelihood and impact of the threats.
   発生確率と脅威がもたらすインパクトの定量化

6) Establishment of the risks.
   リスクの確立

7) Identification of countermeasures framework (architecture).
   対策フレームワーク(アーキテクチャ)の明確化

ステップ 5 におけるインパクトの定量化は、ETSI ETR 332『Security Techniques Advisory Group (STAG); Security requirements capture』と ISO/IEC 15408『Information technology - Security techniques - Evaluation criteria for IT security』に基づいている。

さらに、リスク分析に関して以下のような記載がされている。

- リスク分析の結果必要であると判断された対策を実施することによりシステムに資産が追加された場合に、追加された資産に関する新たな脆弱性が生成されることがある。したがって、リスク分析と対策の実施を繰り返し行うことにより、全てのリスクが許容可能なレベルにまで削減されるべきである

- 攻撃の可能性が変化した場合に再度分析を行うようにすることにより、新しい攻撃に関する知識が入手できた時にシステムのリスクの再評価が実施できる。

- 分析を規則的に行うために、システムの構成要素、脅威、脅威の要因、weakness、脆弱性をデータベースに記録するためする事を推奨する。

リスク分析は、Time、Expertise(攻撃に必要な技能)、Knowledge(知識)、Opportunity(機会)、Equipment(機器) の 5 つの観点から行われる。

表 1.1 に ETSI TS 102 165-1 におけるリスク分析の評価基準を、表 1.2 に ETSI TS 102 165-1 におけるリスク分析の結果と脆弱性レベルとの対応をそれぞれ示す。

表 1.1　ETSI TS 102 165-1 におけるリスク分析の評価基準

Factor	Range	Value
Time (1 point per week)	≤1 day	0
	≤ 1 week	1
	≤ 1 month	4
	≤ 3 months	13
	≤ 6 months	26
	> 6 months	See note 1
Expertise	Layman	0
	Proficient	2
	Expert	5
Knowledge	Public	0
	Restricted	1
	Sensitive	4
	Critical	10
Opportunity	Unnecessary / unlimited access	0
	Easy	1
	Moderate	4
	Difficult	12
	None	See note 2
Equipment	Standard	0
	Specialized	3
	Bespoke	7
NOTE 1: Attack potential is beyond high. NOTE 2: Attack path is not exploitable.		

(出所 ：ETSI TS 102 165-1)

表 1.2　ETSI TS 102 165-1 におけるリスク分析の結果と脆弱性レベルとの対応

Range of values	Resistant to attacker with attack potential of:
0 to 2	No rating
3 to 6	Basic
7 to 14	Moderate
15 to 26	High
> 26	Beyond high

(出所 ：ETSI TS 102 165-1)

表 1.3 に ETSI TS 102 165-1 における脆弱性レベルと攻撃が発生する可能性との対応を示す。

表 1.3　ETSI TS 102 165-1 における脆弱性レベルと攻撃が発生する可能性との対応

Vulnerability rating	Likelihood
Beyond high	Unlikely
High	
Moderate	Possible
Basic	Likely
No rating	
NOTE: Motivation is not considered explicitly in the vulnerability rating.	

(出所：ETSI TS 102 165-1)

ETSI TR 187 002 TISPAN NGN Security：Threat and Risk Analysis では、『PSTN/ISDN エミュレーション』と『NASS-IMS における認証』を対象としたリスク分析を実施している。

リスク分析結果の例を表 1.4 に示す。これは、PES のユーザ側のインタフェースにおいて情報が傍受されるリスクの分析結果を示したもので、技能の熟練度合いや評価対象に関する知識が入手可能かどうか、攻撃を実行するのが容易かどうかといった観点から攻撃の実現性を評価したものとなっている。

表 1.4　PES のユーザ側のインタフェースに関するリスク分析結果の例

Factor	Assigned weighting	Value
Elapsed time (1 point per week)	<= 1 week	1
Expertise	Proficient	2
Knowledge of TOE	Public	0
Access to mount attack	Moderate	4
Equipment	Standard	0
Total	Moderate - possible	7

(出所：ETSI TR 187 002)

2.8　X.805 勧告の概要

本節では、NGN リリース 1 のセキュリティ要件のベースとなっている X.805 勧告：End-to-End 通信システムのセキュリティアーキテクチャ(Security architecture for systems providing end-to-end communications)の概要を述べる。

2.8.1　X.805 勧告の目的と解決しようとする課題

X.805 勧告は、End-to-End 通信のセキュリティを確保するために必要となるセキュリティ関連のアーキテクチャ要素を定義し、End-to-End 通信のセキュリティを確保するためのより詳細な勧告を作成する際の基礎として活用されることを目的とする。

2.8.2　X.805 勧告が解決しようとする 3 つの主な課題

X.805 勧告は、以下の 3 つの課題に対する解決策を見つけるための考え方を提供する。

- どのような脅威に対して、どのような保護策が必要か
- 保護が必要なネットワーク機器と設備のタイプは何か
- 保護が必要なネットワーク活動のタイプは何か

X.805 勧告は、標準的な課題解決を行うために、セキュリティディメンジョン、セキュリティレイヤ、セキュリティプレーンという概念を用いる。

2.8.3 セキュリティディメンジョン

ネットワークセキュリティの特定の側面に対処するためのセキュリティ対策であり、以下の 8 の対策を規定している。

1. アクセス制御
2. 認証
3. 否認防止
4. データの機密性確保
5. 通信のセキュリティ
6. データの完全性
7. 可用性
8. プライバシー

2.8.4 セキュリティレイヤ

ネットワーク機器及びネットワーク設備の階層を意味する。X.805 勧告では、以下の 3 つの階層を定義している。

- **インフラストラクチャセキュリティレイヤ**

セキュリティディメンジョンによって保護されたネットワーク伝送設備と個々のネットワーク機器。ルータ、スイッチ、サーバといった、ネットワーク、サービス、アプリケーションの基本的な構成要素を表している。

- **サービスセキュリティレイヤ**

サービスプロバイダが顧客に提供するサービスのセキュリティ。サービスは、基本的な伝送サービスから、付加価値サービスまで多岐に渡る。サービスプロバイダと顧客の双方を保護するために使用される。

- **アプリケーションセキュリティレイヤ**

サービスプロバイダの顧客がアクセスするネットワークベースアプリケーションのセキュリティ
ウェブ、電子メール、電子商取引、CRM アプリケーションなど。

2.8.5 セキュリティプレーン

セキュリティディメンジョンによって保護されるネットワーク活動を意味する。X.805 勧告では、以下の 3 つのプレーン[22]を定義している。

- **マネジメントセキュリティプレーン**

[22] X.805 勧告での「プレーン」は、「**2.5　NGN のアーキテクチャ**」で触れた Y.2011 勧告での「プレーン」とは、直接的な対応関係は無いが、類似の概念である。

ネットワークエレメント、伝送設備、バックオフィスシステム、データセンタの運用、管理、メンテナンス、供給に関する機能の保護を行う。

- **制御セキュリティプレーン**

ネットワーク経由での情報、サービス、アプリケーションの効率的な配信を実現するための活動の保護伝送機器間での制御情報の保護などが該当する。
制御情報は、IP ネットワークでは帯域内、PSTN(公衆交換電話網)では帯域外で伝送される。

- **エンドユーザセキュリティプレーン**

サービスプロバイダのネットワークへのアクセスや利用に関わるセキュリティ。

2.8.6 セキュリティ脅威

X.805 勧告では、オープンシステムのセキュリティアーキテクチャを規定した X.800 勧告に記載されている以下のセキュリティ脅威が想定されている。

- 破壊：可用性に対する攻撃。情報やネットワーク資源の破壊等
- 毀損：完全性に対する攻撃。データの改ざん等
- 削除：可用性に対する攻撃。情報の窃盗や削除等
- 漏えい：機密性に対する攻撃。不正アクセス等
- 中断：可用性に対する攻撃。ネットワーク障害等

セキュリティ脅威とセキュリティディメンジョンとの関係を表 1.5 に示す。Y と記された欄は、該当するセキュリティ脅威に対する有効なセキュリティ対策であることを示している。

表 1.5　セキュリティ脅威とセキュリティディメンジョンとの関係

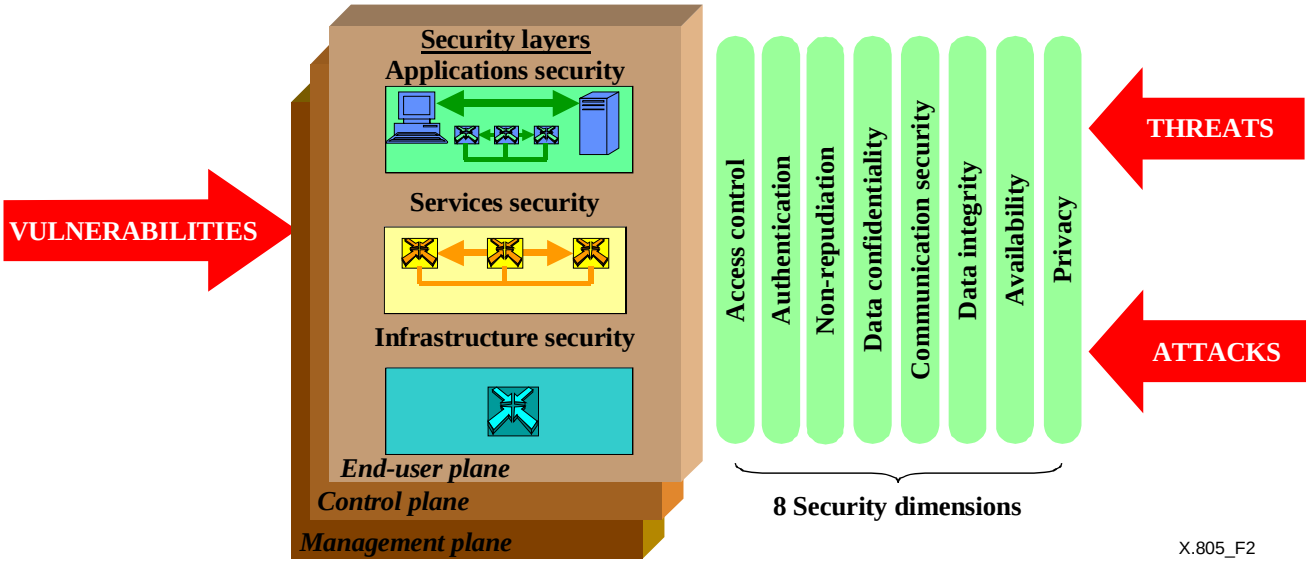
Security dimension	Security threat				
	Destruction of information or other resources	Corruption or modification of information	Theft, removal or loss of information and other resources	Disclosure of information	Interruption of services
Access control	Y	Y	Y	Y	
Authentication			Y	Y	
Non-repudiation	Y	Y	Y	Y	Y
Data confidentiality			Y	Y	
Communication security			Y	Y	
Data integrity	Y	Y			
Availability	Y				Y
Privacy				Y	

(出所：X.805 勧告 Data Neteorks and Open System Communications Security)

セキュリティディメンジョン、セキュリティレイヤ、セキュリティプレーンと、脆弱性、脅威、攻撃との関係を図 1.8 に示す。

X.805 勧告においては、セキュリティを扱う際に、3 つのセキュリティレイヤと 3 つのセキュリティプレーンの組み合わせをベースとしたアプローチがとられる。

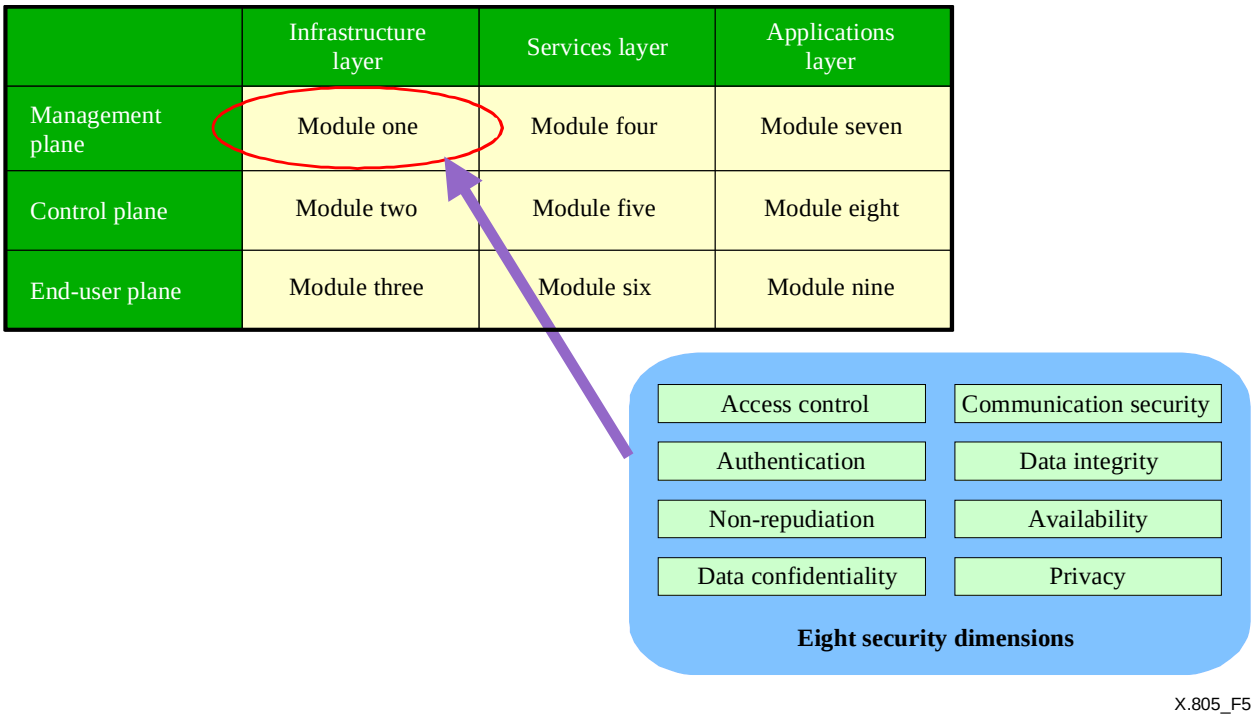
つまり、この組み合わせによって生成されるマトリックスの 9 個の要素それぞれに固有の脆弱性と脅威があり(図 1.8 の右側の矢印)、前記の 8 つのディメンジョンにより、これらの脆弱性と脅威に対処するというのが、X.805 勧告におけるセキュリティの基本的な考え方である。



(出所：X.805 勧告 Data Neteorks and Open System Communications Security)

図 1.8　セキュリティディメンジョン、セキュリティレイヤ、セキュリティプレーンと
脆弱性(Vulnerabilities)、脅威(Threats)、攻撃(Attacks)との関係

セキュリティレイヤとセキュリティプレーンとの組み合わせにより生成されるマトリックスと、マトリックスの各要素(モジュールと呼んでいる)に適用されるセキュリティディメンジョンとの関係を図 1.9 に示す。これは、モジュール 1～9 のそれぞれに存在する固有の脆弱性や脅威(図には明示されていない)に、8 つのセキュリティディメンジョンによって対処することを示した図である。



(出所： X.805 勧告 Data Neteorks and Open System Communications Security)

図 1.9　セキュリティレイヤ／セキュリティプレーンとセキュリティディメンジョンとの関係

2.9　NGN の標準化に関わる組織

2.9.1　ITU における標準化のプロセスの概要

ITU における標準化のプロセスの概略は、以下のようになっている。

1. 各国の国内の標準作成組織(Standards Development Organizations：SDO)における寄書の作成
2. ITU 会合における寄書の提出とその内容に関する議論
3. 寄書に対するコメントを反映したドラフトの作成
4. ドラフトの承認投票(郵便投票または電子投票)

ITU における勧告の策定プロセスを図 1.10 に示す[23]。図中の WTSA は World Telecommunication Standardization Assembly：世界電気通信標準化総会と呼ばれる電気通信標準化部門(ITU-T)における標準化活動の方向性を決める会議であり、4 年に 1 度開催される。前回(2004 年)の会議 WTSA-04 では、次世代ネットワーク(NGN)の標準化を、研究会期(2005～2008 年)の最重要課題として本格的に推進することが決定され、以下の項目について合意がなされた[24]。

1. NGN の標準化を取り扱う新たな研究委員会(SG:Study Group)の設置(NGN−SG(SG13))

2. NGN の標準化は、通信方式の標準化を行う SG11 や移動網の標準化を行う SG19 等の ITU-T の多くの SG が総合的に取り組むことが必要であるため、NGN−SG は ITU-T 全体の NGN の標準化活動の総合調整と標準化のスケジュール管理を実施

3. このような体制強化により NGN の標準化に関する産業界のニーズに迅速かつ効果的に対応、2 年後に更なる体制の見直し

[23] ITU-T Guide for Beginners
[24] http://www.soumu.go.jp/s-news/2004/041015_4.html

(出所　ITU-T Guide for Beginners)

図 1.10　ITU における勧告の策定プロセス

2.9.2　各国の標準作成組織と標準化への取り組み

2004 年 6 月にイギリスの BT が「21 世紀ネットワーク(21st Century Network(21CN))計画」を発表したのを初めとして、各国の通信事業者が NGN への移行を表明しており、通信事業者や通信機器ベンダを中心として、NGN に関する標準化活動が活発化している。

ITU における NGN の標準化に積極的に関与している SDO のうち、主なものを以下に挙げる。

- ヨーロッパ：ETSI(European Telecommunications Standards Institute) [14]
- 米国：ATIS (Alliance for Telecommunications Industry Solutions) [25]
  CableLabs(Cable Television Laboratories, Inc.) [26]
- 日本：TTC (The Telecommunication Technology Committee) 情報通信技術委員会 [27]
  ARIB(Association of Radio Industries and Businesses) 電波産業会 [28]
- 韓国：TTA (Telecommunications Technology Association) 情報通信技術協会 [29]
- 中国：CCSA (China Communication Standards Association) 中国通信標準化協会 [30]

特に、ヨーロッパの ETSI は、ITU に積極的に寄書の提出を行っており、NGN リリース 1 は、ETSI の技術委員会 TISPAN[15] の提案内容がかなり反映されたものとなっている。TISPAN が発行した NGN 関連の仕様は多数あり、そのリストが一覧としてまとめられている[31]。

ヨーロッパが NGN の標準化に積極的である理由の一つに、ヨーロッパ各国の通信事業者が、3GPP に

[25] http://www.atis.org/
[26] http://www.cablelabs.com/
[27] http://www.ttc.or.jp/
[28] http://www.arib.or.jp/
[29] http://www.tta.or.kr/English/new/main/index.htm
[30] http://www.ccsa.org.cn/english/
[31] http://portal.etsi.org/docbox/TISPAN/Open/NGN_Published/

おいて第 3 世代携帯電話の標準化を推進してきたという背景や、固定ネットワークとモバイルネットワークの両方を持つ通信事業者が多く、固定通信とモバイル通信を融合したサービスを提供することによるメリットが大きいなどといった要因がある。

米国はインターネット発祥の地であることや、競争原理によって優れた技術や方式が選別されるという考え方が強いことから、ETSI と比較すると、NGN の標準化への取り組みは進んでいない。そのような状況の中、IPTV やトリプルプレイに対するニーズが高いことが NGN への移行を促す要因となっており、通信事業者の業界団体である ATIS は、IPTV の標準化に積極的に取り組むとともに、以下の NGN 関連の文書を発行している。

- ATIS Next Generation Network (NGN) Framework Part I: NGN Definitions, Requirements, and Architecture
- ATIS Next Generation Network (NGN) Framework Part II: NGN Roadmap 2005
- ATIS Next Generation Network (NGN) Framework, Part III：Standards Gap Analysis

また、米国では電話会社を出自とする通信事業者とケーブルテレビ事業者との競合が激しく、ケーブルテレビの回線を利用したインターネットアクセスが ADSL に匹敵するほどの数を占めている。そのような競争環境の中で、ケーブルテレビ事業者は、モバイルネットワーク、固定網、ケーブルネットワークの相互接続を実現するための手段として IMS を使用することを決定している[32]。そのためケーブルテレビ事業者は、IMS の標準化を重要課題と捉えており、ケーブルテレビ事業者により構成される非営利の研究開発コンソーシアムである CableLabs から 3GPP に代表者を派遣したり、IMS の仕様に対する変更リクエストを提出するなど、IMS の標準化に積極的に関わっている。また、ケーブルネットワークにおける IP 通信に関する技術仕様 PacketCable の一つである PacketCable 2.0 Security Technical Report[33]において、ケーブルネットワークにおける IP 通信のセキュリティや、PacketCable と IMS との関係、PacketCable のセキュリティ上の脅威について言及している。

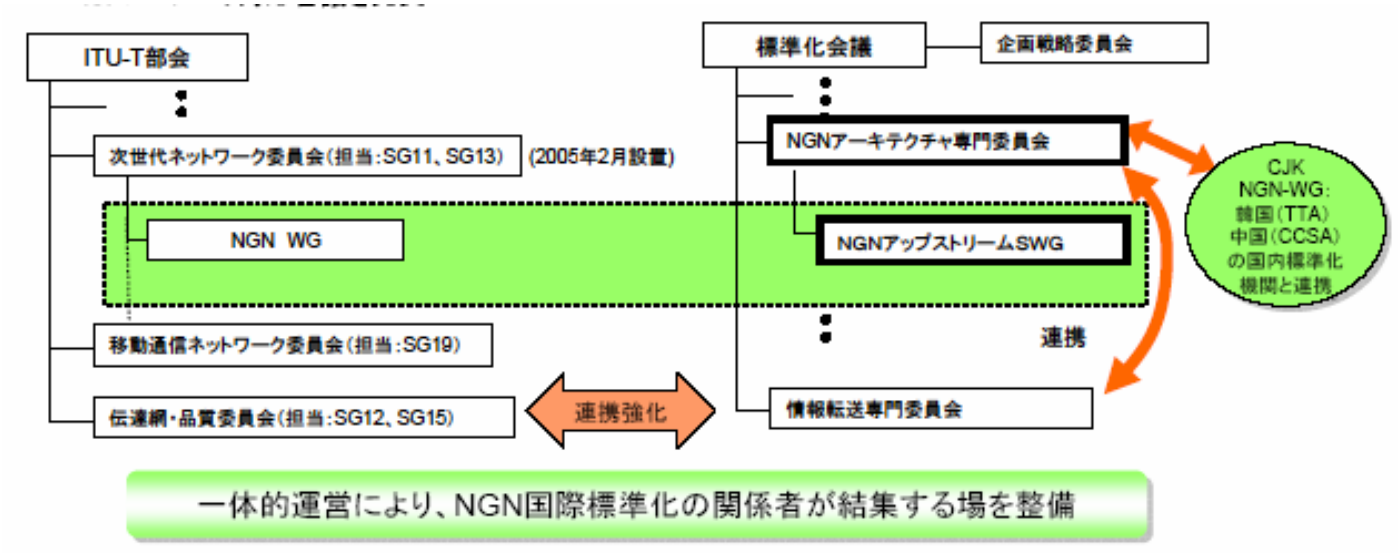
日本は、いくつかの SG においてリーダーシップを取るなど標準化におけるプレゼンスを高めつつあるが、単独での活動では ETSI に対抗することが難しいことから、韓国、中国との連携を強化し、アジア地域全体としての標準化への取り組みの強化が行われている [34]。

具体的な活動としては、WTSA-04 会合において、NGN 関連 SG(SG11, SG13, SG15, SG16, SG19)の議長、副議長ポストを確保するとともに、国内における体制整備の一環として、知的財産推進計画 2005 において、国際標準化に関する以下の決定がなされている。

- 研究開発プロジェクトにおける知財戦略、標準化戦略の一体的推進
- 官民による戦略的な国際標準化活動の強化
- 民間の標準化活動の促進

日本における NGN の標準化に関する国内体制の強化の概要を図 1.11 に示す[35]。

[32] CableLabs の 3GPP メンバへのインタビューより
[33] http://www.packetcable.com/downloads/specs/PKT-TR-SEC-V02-061013.pdf
[34] http://www.ttc.or.jp/j/link/cjk/index.html
[35] 総務省 次世代ネットワーク(NGN)標準化への取組み（2005 年 11 月）



(出所 ： 総務省 次世代ネットワーク(NGN)標準化への取組み (2005 年 11 月))

図 1.11　日本における NGN の標準化に関する国内体制の強化

■ 標準化機関／標準作成組織における連携

NGN の標準化においては、必要に応じて、各国の標準作成組織と IETF や 3GPP、3GPP2[36]との連携が行われている。

また、ITU が 3GPP 及び 3GPP2 とのリエゾンを設立し、NGN 標準に両組織のアウトプットを取り込むという取り組みも行われている。3GPP と ETSI TISPAN とは、NGN に関して非常に密接に作業を行っており、今後の検討の結果次第では、NGN リリース 3 の内容に大きな影響を与えるという見方をしている関係者もいる。

[36] http://www.3gpp2.org/

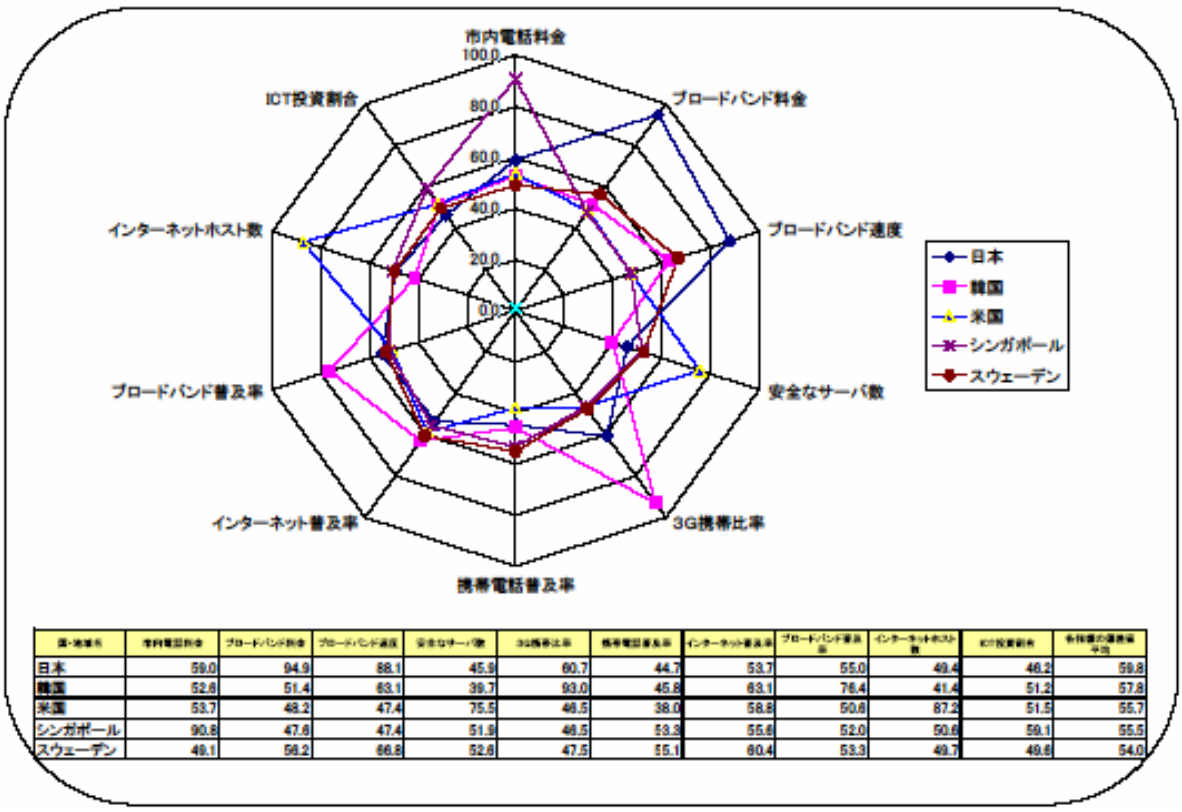
3. 日本及び各国における次世代ネットワークへの取り組み状況

3.1 日本の状況

日本では、2001 年に策定された e-Japan 戦略 [37]によってブロードバンド化に向けた取り組みが開始されるとともに、総務省によって通信事業者が保有する回線を解放する政策が取られたことから、ADSL によるブロードバンド化が急速に進展し、ブロードバンド回線の普及率と速度の両面において世界の中でも先進的なブロードバンドインフラ保有国となった。その後、ADSL の普及は一段落し、現在は NTT が光ファイバによるブロードバンド化を強力に推進しており、2010 年には 3,000 万回線の光ファイバ加入が実現するとみられている。2006 年 9 月末時点における日本のブロードバンドアクセス回線に関する統計値[38]を以下に示す。(カッコ内は 2006 年 6 月末時点の数値)

- インターネット接続契約総数　30,243,341　(31,441,108)
- FTTH　7,154,550　(6,305,597)
- DSL　14,396,034　(14,490,994)
- ケーブルテレビ　3,479,605　(3,409,789)
- FWA　10,954　(10,632)
- 公衆無線 LAN　5,704,018　(5,502,488)
- 携帯電話・PHS 端末　84,058,645　(82,911,225)

2006 年 6 月末時点の数値と比較すると、FTTH、ケーブルテレビ、公衆無線 LAN、携帯電話・PHS 端末が増加しているのに対し、DSL は減少している。後述するヨーロッパや米国と比べて、FTTH 加入者数が非常に多いのが特徴であり、また、図 1.11 に示すようにブロードバンド回線の使用料は、欧米及びアジアの ICT 先進国の中で最も安価である[39]。



日本	59.0	94.9	88.1	45.9	60.7	44.7	53.7	55.0	49.4	46.2	59.8
韓国	52.6	51.4	63.1	39.7	93.0	45.8	63.1	76.4	41.4	51.2	57.8
米国	53.7	48.2	47.4	75.5	46.5	38.0	58.8	50.6	87.2	51.5	55.7
シンガポール	90.8	47.6	47.4	51.9	46.5	53.3	55.6	52.0	50.6	59.1	55.5
スウェーデン	49.1	56.2	66.8	52.8	47.5	55.1	60.4	53.3	49.7	49.8	54.0

図 1.11　欧米及びアジアの ICT 先進国のブロードバンド関連指標の比較 (総務省資料 [39] より引用)

[37] http://www.kantei.go.jp/jp/it/network/dai1/1siryou05_2.html
[38] http://www.johotsusintokei.soumu.go.jp/field/tsuushin01.html
[39] 総務省 日本の ICT インフラに関する国際比較評価レポート http://www.soumu.go.jp/s-news/2005/050510_2.html

日本におけるこれまでの主な IT 関連政策(ブロードバンドインフラの推進策を含む)を以下に示す[40]。

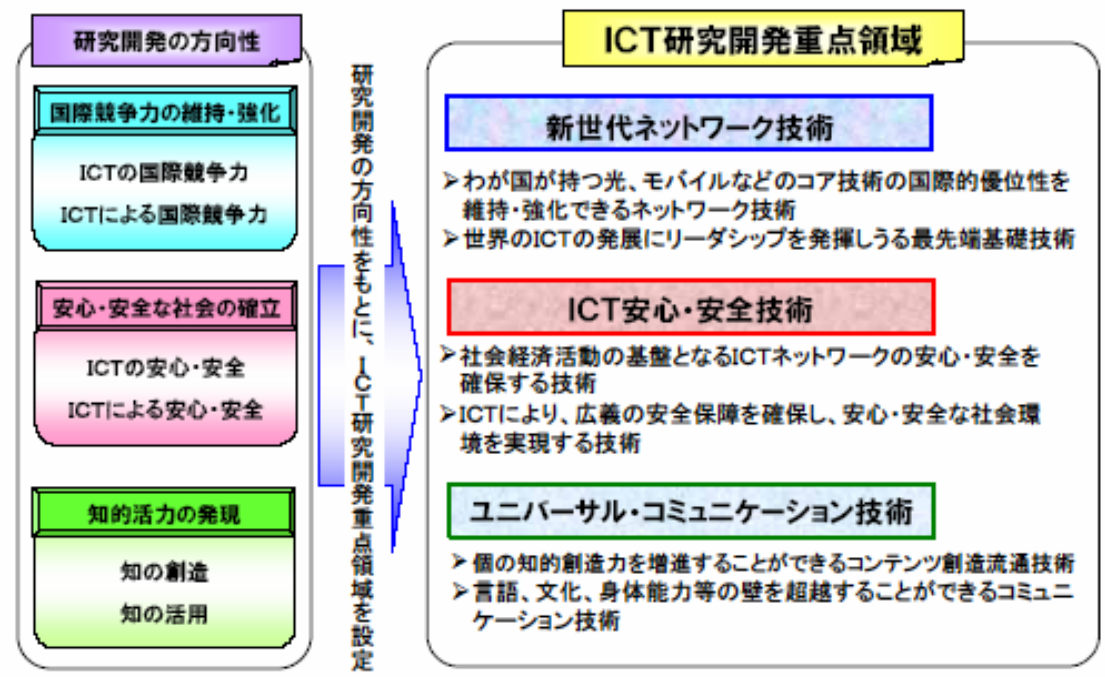
- 2001 年 1 月に高度情報通信ネットワーク社会推進戦略本部(IT 戦略本部)を設置し、「我が国が 5 年以内に世界最先端の IT 国家になること」を目指した「e-Japan 戦略」を策定
- 2002 年 e-Japan 重点計画-2002
- 2003 年 e-Japan 戦略 II
- 2004 年 e-Japan 戦略 II 加速化パッケージ
- 2005 年 IT 政策パッケージ
- 2006 年 IT 新改革戦略

また、総務省が 2004 年に u-Japan[41]政策を策定し、有線・無線を意識することなく扱うことができるシームレスなユビキタスネットワーク環境の整備へ向けた取り組みが開始された。

さらに、総務省の平成１８年度重点施策[42] (平成 17 年 8 月 30 日)において、u-Japan 政策の一部として、世界を先導する ICT 研究開発の推進が掲げられ、以下に示す戦略を柱とする「UNS[43]戦略プログラム」に基づき、重点領域における研究開発を強力に推進するとしている。

- ユニバーサルコミュニケーション(Universal Communications)技術戦略
- 新世代ネットワーク(New Generation Networks)技術戦略
- ICT 安心・安全(Security and Safety)技術戦略

図 1.12 に UNS 戦略プログラムにおける ICT 研究開発の重点領域を説明した図を示す[44]。



(出所 ： 情報通信分野推進戦略プロジェクトチーム第 1 回会合資料
第 3 期分野別推進戦略(情報通信)について ～ユビキタスネット社会に向けた研究開発～)

図 1.12　UNS 戦略プログラムにおける ICT 研究開発の重点領域

[40] IT 関連の各種計画については、http://www.kantei.go.jp/jp/singi/it2/index.html 参照
[41] http://www.soumu.go.jp/menu_02/ict/u-japan/index2.html
[42] http://www.soumu.go.jp/s-news/2005/050830_2.html
[43] Ubiquitous Network Society
[44] 情報通信分野推進戦略プロジェクトチーム第 1 回会合資料 第 3 期分野別推進戦略(情報通信)について ～ユビキタスネット社会に向けた研究開発～

また、上記の 3 つの戦略に基づいて、以下の研究開発プロジェクトを設置するとしている。

1. 新世代ネットワークアーキテクチャ
2. ユビキタスモビリティ
3. 新 ICT パラダイム創出
4. ユビキタスプラットフォーム
5. セキュアネットワーク
6. センシング・ユビキタス時空基盤
7. ユビキタス&ユニバーサルタウン
8. 高度コンテンツ創造流通
9. スーパーコミュニケーション
10. 超臨場感コミュニケーション

同プログラムでは NGN についても言及しており、『欧米に加え、中国、韓国等も権益確保に必死。我が国も、光通信技術、GMPLS 技術等を武器に、国際競争を先導することが必要。』であるとし、NGN におけるグローバル競争においてリードするために、特に光通信分野における技術面での優位性の確保が必須であるとの認識を示している。

前記の平成１８年度重点施策では、次世代 IP ネットワーク(NGN)の基盤技術の研究開発、標準化及び相互接続の推進や、研究成果の国際標準化の推進、研究開発に携わる人材育成など、研究開発を強力に推進するための体制・環境の整備についても言及している。

また、総務省は、次世代ネットワークに関連した各種の研究会／委員会を開催しており、主なものに、『次世代 IP インフラ研究会』[45]、『情報通信審議会 情報通信技術分科会 IP ネットワーク設備委員会』[46]、『全国均衡のあるブロードバンド基盤の整備に関する研究会』[47]、『IP 化時代の通信端末に関する研究会』[48]、『次世代ブロードバンド技術の利用環境整備に関する研究会』[49]がある。

『全国均衡のあるブロードバンド基盤の整備に関する研究会』がまとめた『次世代ブロードバンド構想 2010』では、2010 年までのブロードバンドインフラ整備目標として以下が掲げられている。

- 100%の国民が高速又は超高速のブロードバンドを利用できる環境の整備
  - 2008 年までにブロードバンド・ゼロ市町村を解消
  - 2010 年までにブロードバンド・ゼロ地域を解消
- 次世代双方向ブロードバンド(上り 30Mbps 級以上)を 90%以上の世帯で利用可能とする

この目標をブロードバンドを利用可能な世帯カバー率で表すと、高速ブロードバンドについては 100%、超高速ブロードバンドについては 90%ということになる。また、回線種別ごとの普及世帯数で表すと、ブロードバンド全体で 3,500 万～3,700 万世帯、光ファイバ：1,200 万～1,500 万世帯、ADSL：1,500 万～1,700 万世帯、ケーブルインターネット：450～480 万世帯が、2010 年までの目標ということになる。

このように日本では、多種多様な ICT／ブロードバンド関連の施策が明確な目標の基に実施されている点が特徴であり、このことが、ブロードバンドインフラの整備において質量両面での大きな進展が実現した理由であると考えられる。

[45] http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/jise_ip
[46] http://www.soumu.go.jp/joho_tsusin/policyreports/joho_tsusin/ipnet/ipnet.html
[47] http://www.soumu.go.jp/s-news/2004/040608_2.html
[48] http://www.soumu.go.jp/s-news/2006/061201_6.html
[49] http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/bbseibi/index.html

3.2 EU の状況

ヨーロッパ全域に関するブロードバンド化に向けた取り組みとしては、2005 年 6 月に EU が採択した「i2010：欧州の情報社会 2010」がある[50]。i2010 は、デジタルコンバージェンスが、EU 単一市場の強化に向けた主要な牽引役となると見ており、以下の 3 つの項目が目標として掲げている。

1. 手頃で安全なブロードバンド通信、豊かで多様なコンテンツとデジタルサービスを提供する単一欧州情報空間の実現
2. ICT 分野における研究と技術革新の強化
3. 高品質の公共サービスを提供し、生活の質を向上させる包括的情報社会の実現

i2010 において NGN という言葉が明示的に使われているわけではないが、NGN に関連するものとしてモバイルテレビに関する標準化と相互接続性に関する取り組みの推進を挙げている。

情報通信分野における研究開発の面では、EU 全体における研究開発プログラム FP(Framework Programme)の最新版である FP7[51]において、ICT 関連の研究開発に 90 億ユーロ(約 1 兆 4,000 億円)が、2007 年から 2013 年にかけて投じられる予定となっている[52]。

FP 委員会によって作成された、FP7 における ICT 分野の研究開発テーマの詳細が記載された文書『ICT - INFORMATION AND COMMUNICATION TECHNOLOGIES Work Programme 2007-08』[53]には、次世代インターネットやネットワークセキュリティ、ユビキタス／モバイル通信に関する研究開発テーマが挙げられており、これらのなかには、NGN への応用が可能な技術もあるものと考えられる。

以降において、イギリス、フランス、ドイツの各国における次世代ネットワーク(ブロードバンドネットワーク)への取り組みについて述べる。

3.3 イギリスの状況

イギリスでは 2001 年に「UK Online：the broadband future」が公表され、2005 年までに G7 諸国の中で最も競争的でかつブロードバンドが広範に普及した市場とするという目標が設定された。

また、2004 年 9 月にブレア首相が「2008 年までに希望する全ての家庭にブロードバンド・サービスを提供する」と表明したり、2005 年 3 月に、ICT とブロードバンド化によってデジタル・ディバイドの解消に取り組むこととした「Connecting the UK：the Digital Strategy」を策定するなど、ヨーロッパ諸国の中では比較的ブロードバンド化に力を入れている様子がうかがえる[54]。

通信事業者の中では、BT が電話網の完全 IP 化を表明するとともに、ブロードバンド化に注力している。BT が構築する次世代ネットワークは 21CN と呼ばれ、これまでに以下のような NGN を利用したサービスが提供されている[55]。

- 21C Global venture (Dec, 2006)

  BT における 21CN の開発により得られた経験を他の国の通信事業者が NGN を構築するのを支援するコンサルティングサービス 21C Global venture を発表。イギリス国内における通信網の構築だけでなく、それによって得られた技術的なノウハウを活用し、NGN の設計、構築、引渡しまでのコンサルティングサービスを提供する。最初の顧客は、トルコの通信事業者 Turk Telecom である。

[50] http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm
[51] http://cordis.europa.eu/fp7/ict/
[52] ICT in FP7 At A Glance (mid November, 2006)
[53] ftp://ftp.cordis.lu/pub/fp7/ict/docs/ict-wp-2007-08_en.pdf
[54] 総務省 2006 年度通信白書及び次世代ブロードバンド構想 2010 (http://www.soumu.go.jp/s-news/2005/050715_8.html)
[55] http://www.btplc.com/21CN/WhatisBTsaying/Keymilestones/Keymilestones.htm

- IPTV サービス BT Vision の提供開始（Dec, 2006）

- 21CN を利用した最初の通話が提供される。（Nov, 2006）

- 企業向けの FMC サービスを開始（Sep, 2006）

また、今後の計画としては、以下のようなマイルストーンが設定されている [56]。

- 2007 年

  - 国内のブロードバンドサービスの半数が、21CN により提供される。

- 2008 年

  - イギリス国内全域において、21CN への移行が開始される。
  - PSTN の 15%以上が、21CN に移行。

- 2009 年

  - 次世代ブロードバンドサービスが、1600 万人以上に利用可能になる。
  - ブロードバンドネットワークの 65%、PSTN の 50%が、21CN に移行

- 2010 年

  - 次世代ブロードバンドサービスが、2,000 万人以上に利用可能になる。
  - 21CN に移行がかなりの程度まで進展する。

- 2011 年

  - 21CN への移行完了。

BT の 21CN への移行計画の 2011 年までのマイルストーン[57]を図 1.13 に、2006 年から 2008 年にかけての移行計画の詳細[58]を図 1.14 に、BT の次世代ネットワーク 21CN のアーキテクチャ[59] を図 1.15 にそれぞれ示す。

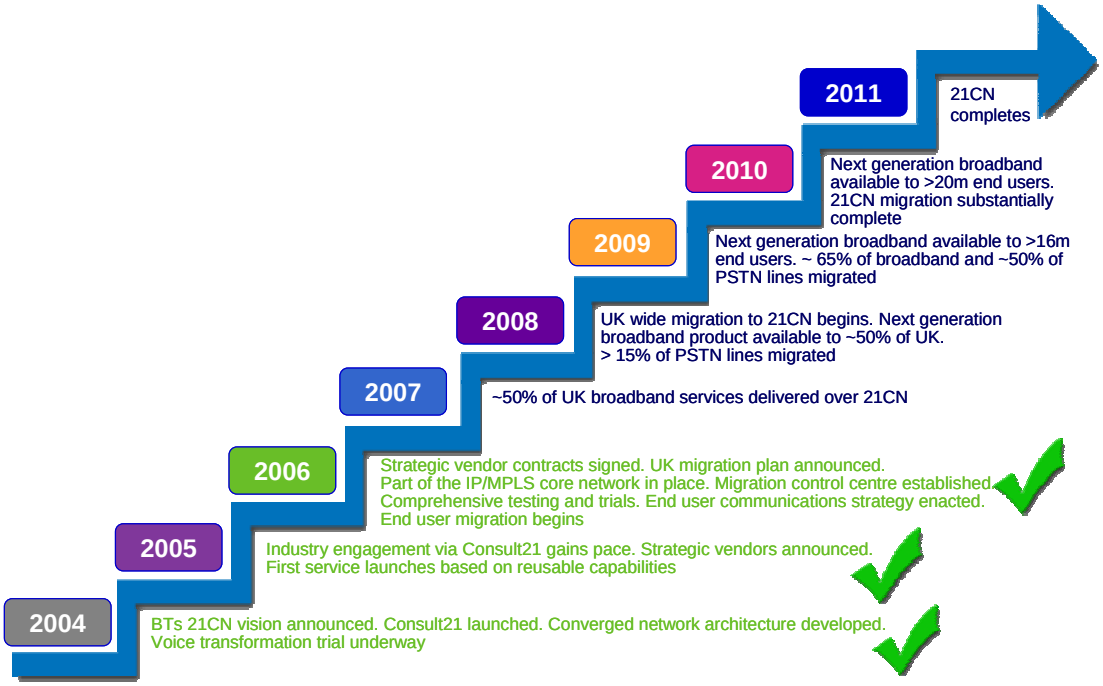
光ファイバの導入に関しては、2006 年 12 月に開催された DigiWorld 2006 [60]において BT Wholesale 部門 CEO の Paul Reynolds が以下のように述べている [61]。

- 2007 年に従来の ADSL の改良版であり、最大速度 24Mbps の ADSL2+ の提供を開始する予定
- 光ファイバについては、まだニーズがないと考えているが、LLU 事業者はメタル回線の代わりに FTTH を使用することも出来る

これらの発言から、現時点でイギリスにおけるブロードバンド回線の主役は ADSL であり、光ファイバに対するニーズはまだ少ないということが推測できる。

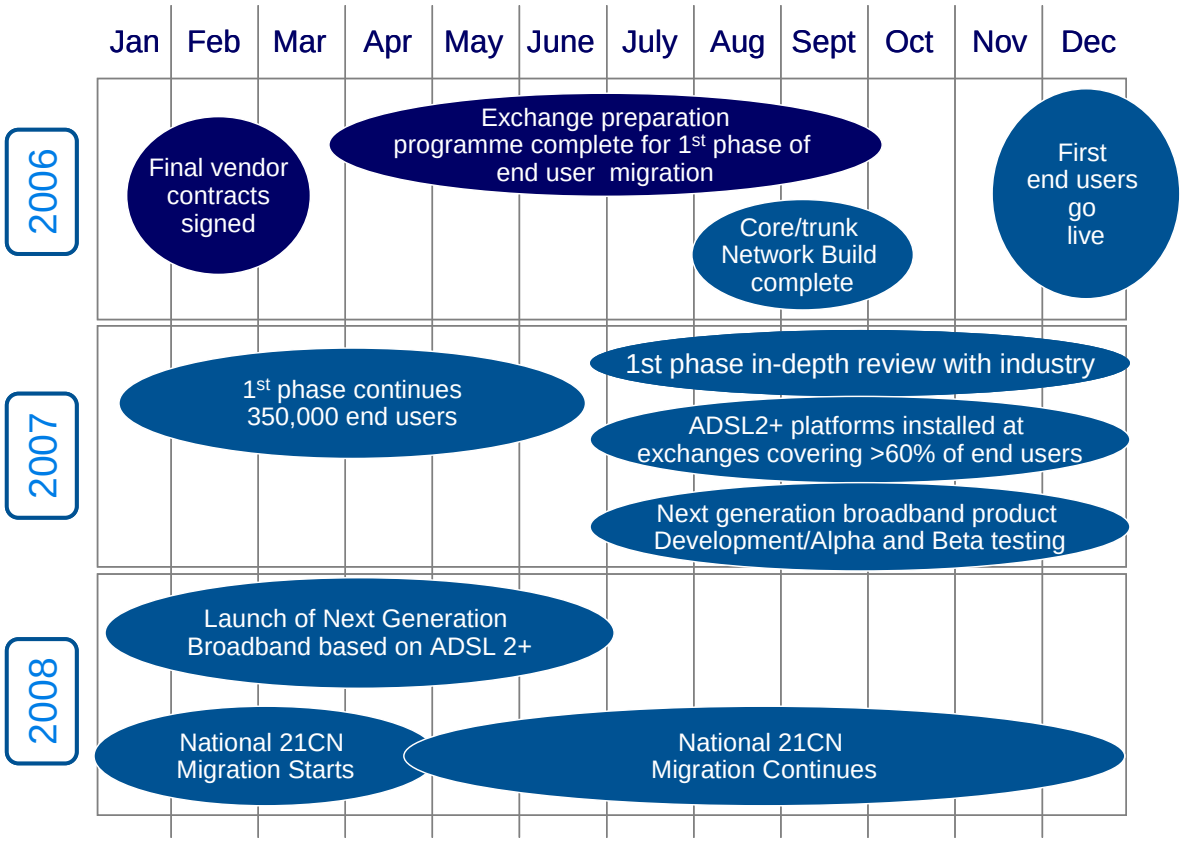
---

[56] http://www.btplc.com/21CN/Theroadto21CN/Keymilestones/Keymilestones.htm
[57] BT's 21st Century Network
[58] BT's 21CN Programme
[59] “IMS based NGN Architecture and its application”, ITU-T Workshop NGN and its Transport Networks, Kobe, 20-21 April 2006
[60] http://www.digiworldsummit.com/pages/?all=accueil&idl=22
[61] http://www.itpro.co.uk/internet/news/98234/%20bt-rules-out-deployment-of-fibretothehome.html



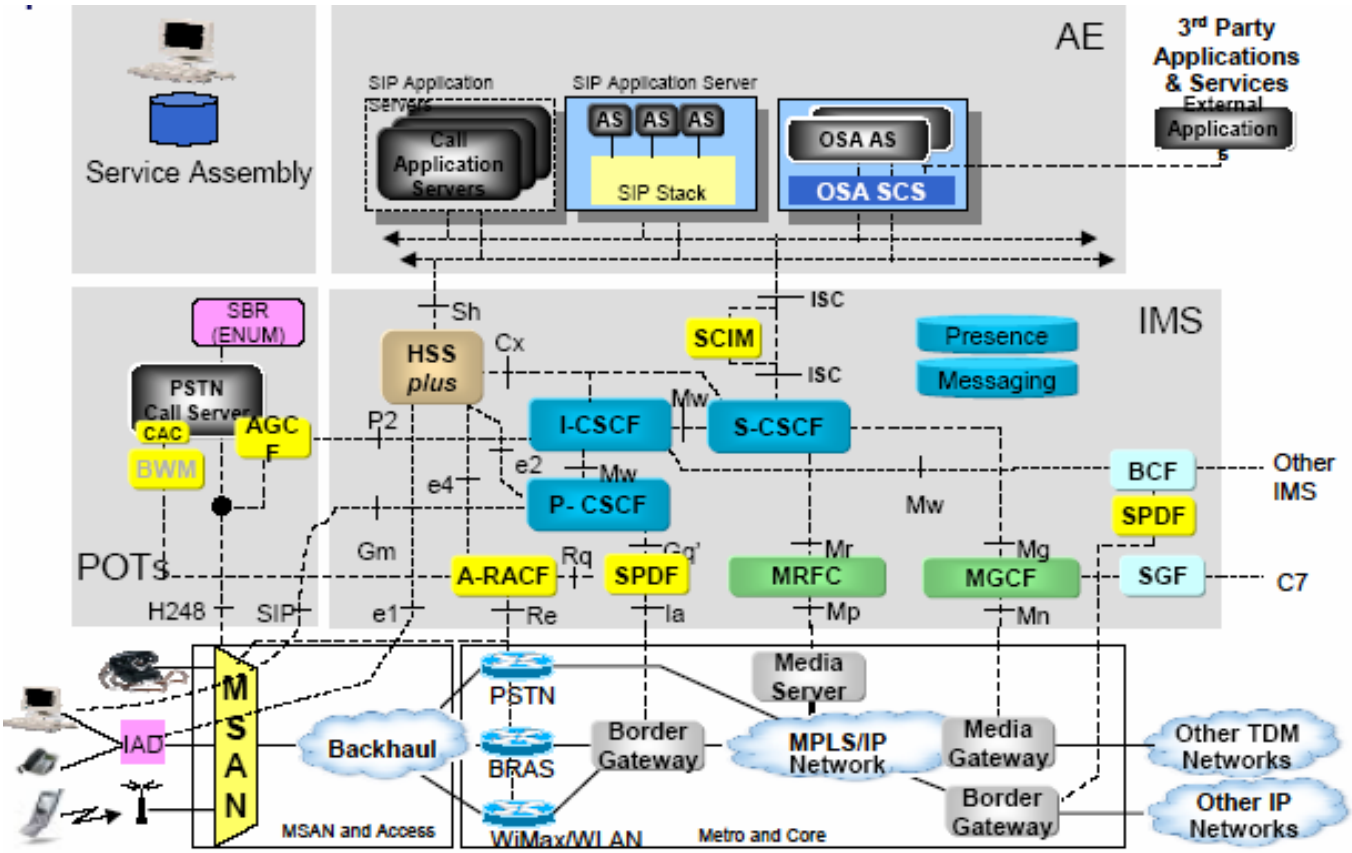
(出所：BT's 21st Century Network)

図 1.13　21CN への移行計画の 2011 年までのマイルストーン



(出所：BT's 21CN Programme)

図 1.14　BT の 21CN への移行計画のうち、2006 年から 2008 年にかけての詳細



(出所：IMS based NGN Architecture and its application)

図 1.15　BT の次世代ネットワーク 21CN のアーキテクチャ

3.4 フランスの状況

3.4.1 ブロードバンドインフラの整備／普及状況

2004 年に発表されたブロードバンド戦略[62]において、以下の目標が掲げられた。

- 2007 年までにブロードバンド接続加入者数を 1,000 万とする
- 2007 年にブロードバンドの人口カバー率を 95%とする
- 2010 年に産業地域における光ファイバの普及率を 90%とする

また、通信事業者の FT(France Telecom) が、2005 年末までに県人口の少なくとも 95%をカバーするという業務協定を全県と締結している[63]。

電子通信に関する規制機関 ARCEP(Autoritè de Règulation des Communications Electroniques et des Postes) [64]がまとめたブロードバンドに関する統計『High-speed Internet Observatory 3rd Quarter 2006』によれば、2006 年 11 月末の時点におけるブロードバンド接続加入者数は 1,180 万であり、そのうちの 1,110 万が ADSL、ケーブルが 65 万、光ファイバは WLL(Wireless Local Loop：無線接続回線)と合わせて 7,000 に留まる。

同レポートに記載されている、フランスにおけるブロードバンド接続加入者数の 2001 年からの推移を図 1.16 に示す。

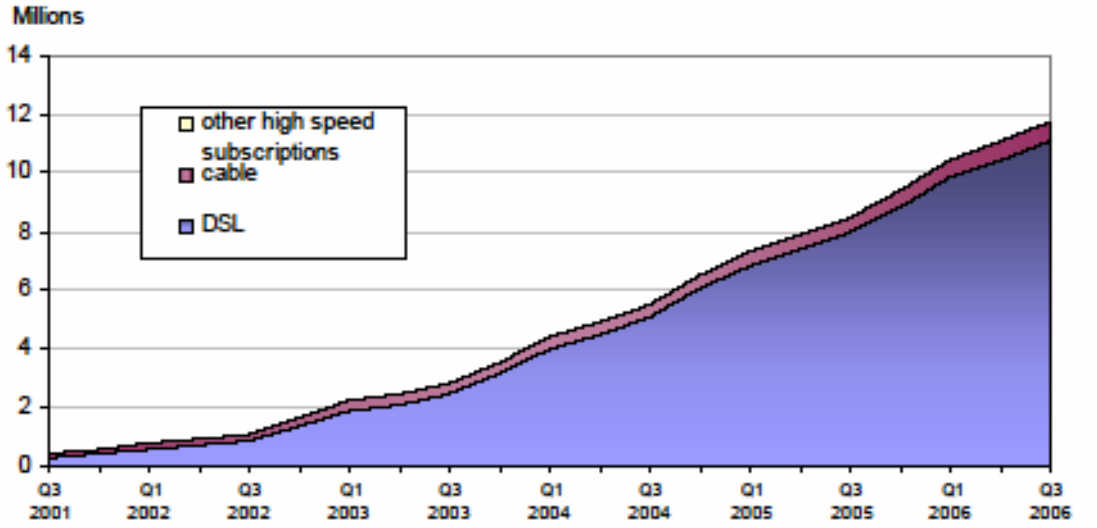


図 1.16　フランスにおけるブロードバンド接続加入者数の 2001 年からの推移

フランスにおけるブロードバンドアクセス回線の主役もイギリスと同様 ADSL であり、光ファイバの普及はまだこれからという状況である。

フランス国内におけるブロードバンドサービス事業者の最大手はフランステレコムであり、ADSL によるブロードバンドインターネット接続加入者数は約 550 万で、国内シェア約 50%を占めている [65]。

フランステレコムは、2006 年 5 月に、インターネット接続、デジタル TV、モバイル通信の各サービスのブランドを Orange に統一し[66]、一般家庭からのアクセス用に Livebox と呼ばれるホームゲートウエイ(無線モデム)を導入した。Livebox は、2006 年 9 月時点で約 290 万台が貸し出されている。

---

[62] http://www.internet.gouv.fr/informations/information/plan_reso2007/
[63] 総務省 次世代ブロードバンド構想 2010　http://www.soumu.go.jp/s-news/2005/050715_8.html
[64] http://www.arcep.fr/index.php?id=1&L=1
[65] http://www.francetelecom.com/en/group/organisation/key_figures/Q3_06_home/
[66] http://francetelecom.com/en/financials/journalists/press_releases/CP_old/cp060531.html

Orange が提供する FMC サービスは Unik と呼ばれ、2006 年 9 月にサービスが開始された。Unik は、自宅では WiFi で Livebox に接続して ADSL 回線で通話し、自宅以外では、通常の携帯電話網を使って通話するというものである。

また、8Mbps のインターネットサービス、デジタル TV、一定の通話時間まで通話料無料の音声通話サービスのパッケージである Orange Optimales を提供している。

ビジネス向けのインターネットアクセスサービスとしては、2006 年 6 月に、PC、PDA、スマートフォンから、3G、EDGE(Enhanced Data rates for GSM Evolution)、WiFi、ADSL、GPRS (General Packet Radio Service)、PSTN のいずれのネットワークにもアクセスできる Business Everywhere の提供を開始している [67]。Business Everywhere は、フランス国内の他にポーランド、ベルギー、スペイン、スロバキア、スイス、ルーマニア、イギリスにおいても提供されている。

フランステレコムによるブロードバンドへの取り組みとしては、2007 年 3 月に、パリとその周辺において、最大 100Mbps でのインターネットアクセス、インターネットによる HDTV 放送、PC によるテレビ受信、定額通話料金サービスが開始される予定である。さらにこのサービスは、2007 年 7 月には、リヨン、マルセイユ、ツールーズなど 12 の都市において提供される予定となっている[68]。

光ファイバの導入については 2006 年の第 1 フェイズにおける試験的な導入に続いて、2007 年には FTTH 導入の第 2 フェイズが開始される計画となっている。

2006 年の光ファイバの試験導入の成果として、以下が挙げられている。

- 100,000km の光ファイバ敷設
- 11,500 世帯(接続可能な世帯の 5%に相当)への接続が可能

光ファイバによるブロードバンド接続に関する今後のマイルストーンとして、以下が示されている。

- 2008 年末には、人口 100 万人あたり 150,000～200,000 のユーザが接続できるようにする。
- 2 年間の総投資額は、2 億 7,000 万ユーロ(約 420 億円)。

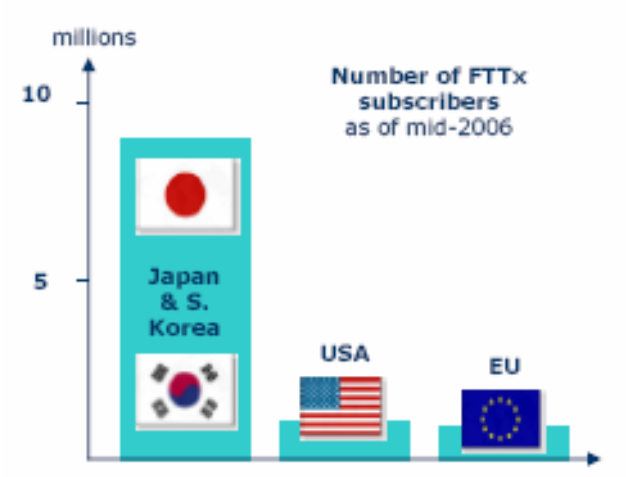
ADSL の次の段階である、光ファイバを利用したブロードバンド接続に対するフランステレコムの見解は、『大規模マーケット向けの超高速ブロードバンドを開発するためには、機器メーカ、運用者、サービスプロバイダが超高速ブロードバンドにある程度対応していなければならないが、それには少なくとも 2 年を要すると考えられる。』というものであり、光ファイバの本格的な導入は、2009 年以降になるとしている [68]。

ARCEP が 2006 年 11 月に発行したレポート『Very high-speed Points of reference and outlook』では、光ファイバの普及が進まない最も大きな要因として敷設コストを挙げており、ビルディングへの光ファイバの敷設にはコストの観点から GPON が利用されているが、1 回線の敷設に 2,000 ユーロが必要であるという試算がされている。

また、同レポートでは、pay-TV 普及の最も大きな driving force である TV over DSL の契約者数が 150 万に近づいていることから、光ファイバベースの超高速ブロードバンドに対する潜在的な需要は大きく、光ファイバによって、高精細番組、複数チャネルの同時配信、VoD の瞬時のダウンロードといった新たなサービスを展開する道が開けるとしている。

さらに、上記レポートでは、ヨーロッパにおけるブロードバンドインフラの構築が、日本や韓国、米国に比べて遅れていることに対する危機感が、各国の FTTH 加入者数のデータに基づいて示されている。図 1.17 に、同レポートに示されている地域別の FTTH 加入者数の比較グラフを示す。

[67] http://www.francetelecom.com/en/financials/journalists/backgrounders/att00038884/BEW_FactsFigures_2006_August_06.pdf
[68] http://www.francetelecom.com/en/financials/journalists/press_releases/CP_old/cp061215-ftth.html



（出所：ARCEP　Very high-speed Points of reference and outlook）

図 1.17　ARCEP のレポートに示されている FTTH 加入者数の地域別の比較

3.4.2　NGN 関連の研究開発動向

フランステレコムにおけるセキュリティ関連の研究開発には、暗号及び暗号アルゴリズム、安全性評価：安全性の技術監査、リスク分析、製品のテスト／評価、IDS／ファイアウォール等の選択／導入支援といった項目が挙げられている[69]。

情報通信分野における研究開発の面では、フランステレコムが、前述した EU の研究開発プログラム FP7 の一つ前のタームのプログラム FP6 において実施された、eMobility[70]、ePerSpace[71]、SPICE[72]などの研究開発に参加している[73]。これらの研究開発プロジェクトは、EU 内の他の企業や大学と協力して実施されたものである。例えば、SPICE には、Telecom Italia、Telefonica、Telenor、Alcatel、Ericsson、Nokia、Siemens などの企業が参加している。
以下で、eMobility、ePerSpace、SPICE の概要について述べる。

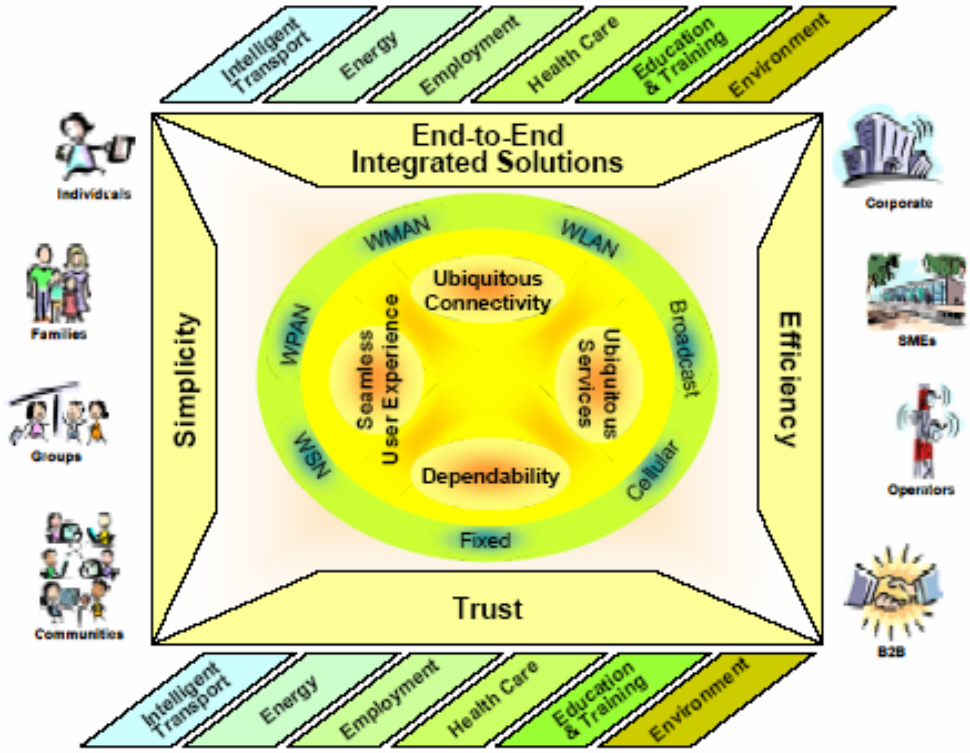
- eMobility

将来の多様なサービスとネットワークにより構成されるシステムにおける、ネットワークと端末の間での、より一般的なモビリティとサービスの継続性の確保を目的としている。
『いつでもどこでも』という従来のパラダイムから、『適切なコンテンツとコンテキストによって、安全かつ信頼できる方法で任意の端末から任意のネットワークに』という新しいパラダイムへの転換を促進する。
eMobility に関する研究領域として、以下が挙げられている。

- シームレスなユーザエクスペリエンス
- セキュリティと信頼性
- ユビキタスサービス
- ユビキタスコネクティビティ
- 新しい柔軟なビジネスモデル

[69] http://www.francetelecom.com/en/group/rd/offer/expertises/Domaines_New/CS/indexCS.html
[70] http://www.emobility.eu.org/
[71] http://www.ist-eperspace.org/default.htm
[72] http://www.ist-spice.org/
[73] France Telecom Research & Development DDM September 2006

図 1.18 に eMobility のイメージを示す[74]。



(出所：eMobility Mobile and Wireless Communications Technology Platform Staying ahead! Strategic Research Agenda Ver5)

図 1.18　eMobility のイメージ

- ePerSpace

家庭におけるパーソナル化されたサービスのマネジメントを目的とし、テレビ、セットトップボックス、コンピュータ、家電等あらゆる機器がブロードバンドネットワークに接続されるようになった場合のサービスや機器のコントロール／マネジメントの確保が課題として挙げられている。

研究開発の成果は、ETSI の NGN@home や HGI(Home Gateway Initiative)における標準化への貢献という形でアウトプットとなった。

図 1.19 に、ePerSpace のインフラストラクチャイメージを示す[75]。

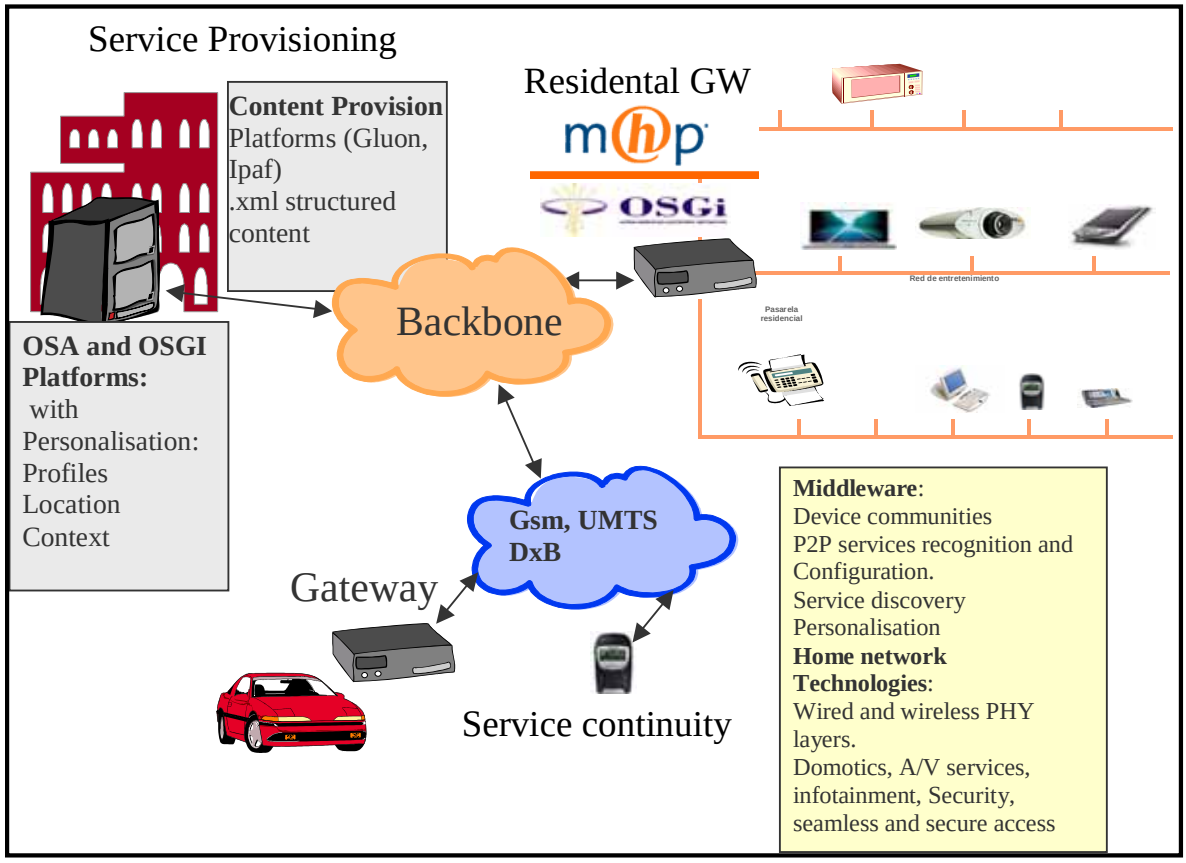
- SPICE(Service Platform for Innovative Communication Environment)

インテリジェントかつパーソナルなモバイル通信サービス、コンテンツサービス、情報サービスの迅速な創出・実装のためのオーバーレイアーキテクチャ・フレームワークに関する研究であり、以下を実現することを目的とする。

- 開発期間、コスト、リスクの削減しながら、革新的なサービスの創出と実装を簡易かつ単純に行うための手法
- プラットフォーム、ネットワーク、端末の種別によらずにサービスを提供するための、統合されたシームレスな方法
- パーソナル化及びカスタマイズによって、サービスや端末の簡易な利用を実現するための、信頼できるオープンなプラットフォーム

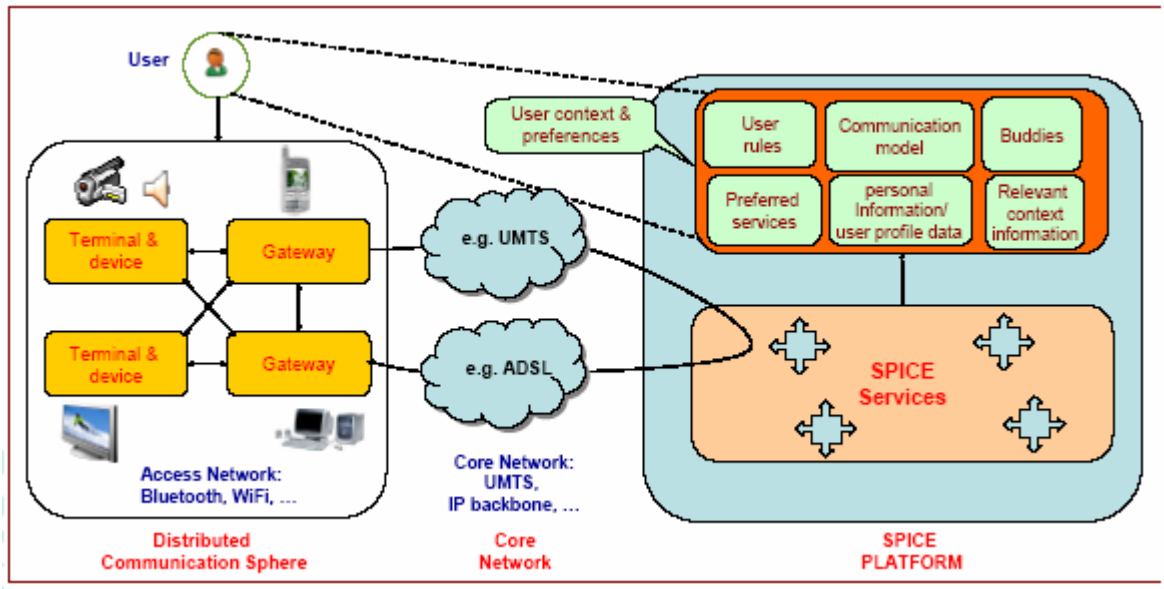
[74] eMobility Mobile and Wireless Communications Technology Platform Staying ahead! Strategic Research Agenda Ver5, August 2006
[75] ePerSpace Concertation meeting (11/03/2004)

図 1.20 に、ネットワークにおける SPICE の位置づけ[76]を示す。



(出所：ePerSpace Concertation meeting)

図 1.19　ePerSpace のインフラストラクチャイメージ



(出所：Service Platform issues in WWI : Introduction to the SPICE project)

図 1.20　ネットワークにおける SPICE の位置づけ

[76] Service Platform issues in WWI : Introduction to the SPICE project, February 3rd, 2006

3.5 ドイツの状況

ドイツにおけるブロードバンド政策としては、2003 年に発表された「Information Society Germany 2006」[77]があり、2005 年までにインターネットを人口の 75%まで普及させると同時にブロードバンドをインターネット接続の主要方式とするという目標が掲げられている。

通信事業者の動向としては、2005 年にドイツテレコムは、2012 年を目標として加入電話網を IP 化することを表明している**エラー! ブックマークが定義されていません。**。

次世代ネットワーク関連のサービスとしては、ドイツテレコムが 2006 年 8 月に、固定網でも携帯網でも使用できる端末として T-One を導入している[78]。T-One には、2 つのバージョンがあり、GSM とインターネットを利用した VoIP (WiFi 経由)が使えるものと、GSM と通常の固定網が使えるものとが用意されている。

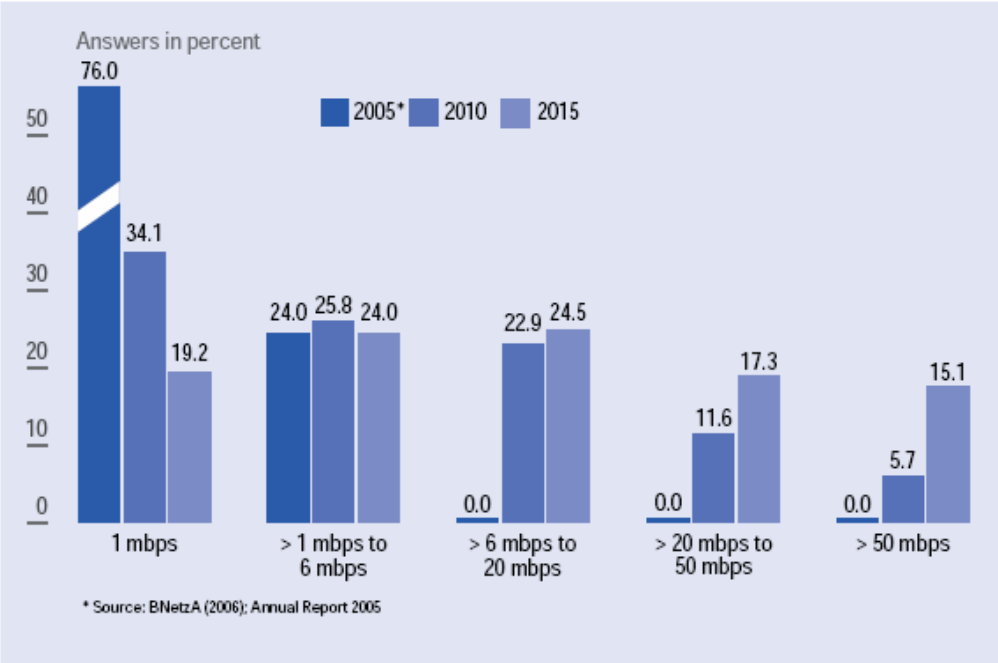
また、ドイツテレコムの発表 Customer benefits and confidence[79]によれば、2006 年 11 月時点のブロードバンド接続数は 700 万であり、2015 年には 2,700 万(70%の世帯)に達する見込みであるという。また、そのうちの 1/4 は、VDSL ベースとなっている。

ドイツにおけるブロードバンドネットワークの展望に関しては、2006 年に発行されたレポート『Deutschland Online 4 Report 2006』[80]に以下の記述がある。

- トリプルプレイは、VDSL ベースのブロードバンドアクセスにより実現される。
- デジタルビデオレコーダ付きのテレビセットトップボックスが、家庭におけるデジタルコンテンツメディアセンタになると予測される。
- インターネット TV ユーザは、2015 年に 700 万以上になると見込まれる。

以下では、同レポートから、ブロードバンドネットワークに関する動向に関する記述をピックアップして紹介する。

図 1.21 に回線速度別にみたブロードバンドユーザの推移の予測を示す。



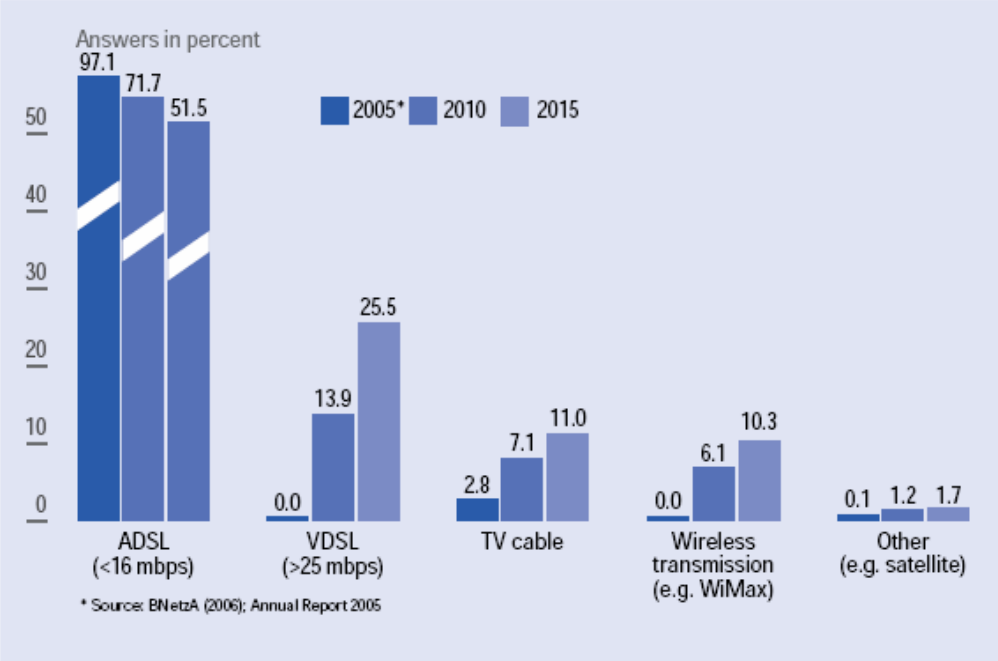
(出所：Deutschland Online 4 Report 2006)

図 1.21　ドイツにおける回線速度でみたブロードバンドユーザの推移の予測

[77] http://www.bmbf.de/pub/aktionsprogramm_2006_gb.pdf
[78] http://www.telekom.de/dtag/cms/content/dt/en/9250
[79] http://www.deutschetelekom.com/dtag/cms/content/dt/en/7532
[80] http://www.studie-deutschland-online.de/do4en/0000.html

2015 年になっても、50Mbps 以上の回線を使用するユーザは 15.1% までしか増加しないと予測されている。

次に回線種別でみたブロードバンドユーザの推移の予測を図 1.22 に示す。



(出所：Deutschland Online 4 Report 2006)

図 1.22　ドイツにおける回線種別でみたブロードバンドユーザの推移の予測

2015 年時点でも、一般的な 16Mbps 以下の ADSL が半数以上を占めている一方、25Mbps 以上の VDSL が 25.5%まで増加すると予測している。

サービスの面ではトリプルプレイがブロードバンドインターネットの普及に欠かせないサービスとして認識されており、2015 年にはユーザ数が 750 万人に到達すると予測している。

また、トリプルプレイにより提供されるサービスとして、インターネット電話が必須であり、その他に VOD、HDTV、インターネット TV に対するニーズが高い事を指摘している。

VDSL 回線を使用してトリプルプレイを提供するためのデバイスとして、テレビ、ビデオ、DVD プレイヤー、ステレオシステム、PC が一体化されたメディアセンターが、標準的な装置となるだろうという指摘もされている。

同レポートにおいても、前記フランスの ARCEP が発行したレポート『Very high-speed Points of reference and outlook』と同様に、ヨーロッパにおける通信インフラの構築が、アジアや米国に比べて遅れていることに対する危機感を表明しており、ヨーロッパの中では比較的ブロードバンド環境が整備されていると思われる両国が同じ見解を示している。

■　ヨーロッパ各国の状況のまとめ

ヨーロッパにおけるブロードバンドの状況をまとめると、以下のようになる。

- 電話網の IP 化とブロードバンドインフラの構築は、イギリスが進んでいる。
- ブロードバンドアクセス回線は DSL が中心で、光ファイバ回線の普及は遅れている。
- その理由は、ニーズがない、敷設コストが高いといったものである。
- 次世代サービスの主役は、FMC と デジタル TV である。
- 米国や日本、韓国と比較してインフラ整備が遅れていることに危機感を持っている。

3.6 米国の状況

FCC(連邦通信委員会)[81]等が個別に政策目標を出しているが、日本の e-Japan 戦略のような規制政策以外の戦略も含めた包括的でかつ具体的なブロードバンド政策・計画はない。そのため、「国家的なブロードバンド政策を構築すべき」との意見を述べる電気通信関係者が多い[82]。

FCC は 2001 年 10 月に、ブロードバンド化推進に向けて以下の四つの原則と政策目標を掲げ[83]、全ての国民へのブロードバンド・サービスの普及促進と、ブロードバンドに対する投資を促進するため、必要最小限の規制のみを課すことを示した [82]。

① ブロードバンド・サービスに関わるユニバーサルな利用可能性を促進
② 多様なプラットフォーム(DSL、ケーブルモデム、衛星等)間の競争を促進
③ ブロードバンドの規制を必要最小限とし、投資と技術革新を促進
④ 多様なプラットフォームに対する整合的な分析枠組みを開発

また、2004 年 3 月 26 日にブッシュ大統領が、「2007 年までにブロードバンドテクノロジーへのアクセスを米国のどこからでも安く行えるようにするべきである。」という考えを表明している。

3.6.1 米国におけるブロードバンドの状況

米国におけるブロードバンドネットワークの状況について、FCC が 2006 年 4 月に発行したレポート『High-Speed Services for Internet Access：Status as of June 30, 2005』をベースにまとめる。

米国では、高速アクセス回線の定義が以下のようになっており、高速回線あるいは高度回線という言葉により想起される回線速度に関して、日本との差異が大きい。

■ 米国における高速アクセス回線の定義

- 高速アクセス回線 ： 上りまたは下りのいずれかが 200 kbps 以上
- 高度アクセス回線 ： 上りと下りの両方が 200 kbps 以上

表 1.6 に、上記 FCC のレポートに記載されている米国におけるブロードバンド回線の加入者数を示す。表 1.6 から、以下のことがわかる。

- 200 kbps 以上 2.5 Mbps 以下の回線種別では ADSL が最も多い。
- 2.5 Mbps 以上 10 Mbps 以下の回線種別ではケーブルモデムが最も多い。
- 回線種別、回線速度を総合して最も加入者数が多いのは、2.5 Mbps 以上 10 Mbps 以下のケーブルモデムである。
- 光ファイバ回線においても、100 Mbps 以上の回線は少なく、ほとんどが 10 Mbps 以下である。

また、回線速度別の加入者数の割合は以下のようになっている。

- 200 kbps 以上 2.5 Mbps 以下　　38.2%
- 2 Mbps 以上 10 Mbps 以下　　61.2%
- 10 Mbps 以上　　0.6%

---

[81] http://www.fcc.gov/
[82] 総務省 次世代ブロードバンド構想 2010　http://www.soumu.go.jp/s-news/2005/050715_8.html
報告書 諸外国におけるブロードバンド・サービスの提供と政策動向 http://www.soumu.go.jp/s-news/2005/pdf/050715_8_04_05.pdf
[83] http://www.fcc.gov/Speeches/Powell/2001/spmkp109.html

米国においても現時点でブロードバンド回線の主役は ADSL であり、回線速度も 10 Mbps 以下のものが最も多いことがわかる。

表 1.6　米国におけるブロードバンド回線の加入者数

Technology [2]	Exceeding 200 kbps in only one direction	Exceeding 200 kbps in both directions, and:				
		Greater than 200 kbps and less than 2.5 mbps in the faster direction	Greater than or equal to 2.5 mbps and less than 10 mbps in the faster direction	Greater than or equal to 10 mbps and less than 25 mbps in the faster direction	Greater than or equal to 25 mbps and less than 100 mbps in the faster direction	Greater than or equal to 100 mbps in the faster direction
ADSL	3,143,036	10,844,762	2,189,061	5,178	*	*
SDSL	24,280	393,970	5,214	*	*	0
Traditional Wireline	10,949	453,905	4,379	286	9,501	2,913
Cable Modem	1,273,196	2,297,006	20,222,612	144,218	*	*
Fiber	1,396	185,369	623,788	31,943	12,581	9,754
Satellite	366,010	11,281	0	0	0	0
Fixed Wireless	18,604	172,306	19,314	2,695	*	*
Mobile Wireless	358,457	21,078	*	0	0	0
Power Line and Other	698	3,576	*	*	*	*
Total Lines	5,196,625	14,383,254	23,064,948	184,572	23,627	13,442

(出所：FCC　High-Speed Services for Internet Access：Status as of June 30 2005)

3.6.2　米国の通信事業者の動向

米国における通信事業者によるブロードバンドインフラ整備に関する主な動向を以下にまとめる[84]。

- Verizon は、2004 年から光ファイバ投資を本格化させている。FTTP(Fiber To The Premises)の提供可能世帯数を 2005 年中に 300 万世帯とする計画を発表している。また、ケーブルテレビ事業者との競合が激しいことから、FTTH を積極的に推進し、2008 年までに加入数の 60%をカバーすることを目標としている。

- SBC(AT&T との統合により現在は AT&T)は、2004 年 11 月に Project Lightspeed[85]を発表し、20～25Mbps のブロードバンドサービスを 2007 年までに約 1,800 万世帯に提供するとしている。ネットワーク構成は、加入者回線の幹線部分に光ファイバを用いている(Fiber To The Node：FTTN)が、利用者宅への引き込みは既存の電話線又は同軸ケーブルを利用している。
  2006 年 5 月には、衛星通信、固定無線アクセス、WiMAX などの革新技術によるブロードバンド提供の拡大と Project Lightspeed の低所得世帯層への提供を発表した[86]。
  発表の具体的な内容を以下にまとめる。

  - 現在通信回線によるブロードバンド・サービスが提供されていない一般家庭向けサービス対象地域のうちの一部の地方向けに、衛星通信を利用したブロードバンド・サービスを提供。

[84] 総務省 次世代 IP インフラ研究会 第三次報告書
[85] http://www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=21458
[86] http://www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=22272

- 3 年以内に 550 万以上の低所得世帯層に IP 対応ビデオ・サービス Project Lightspeed を提供。

- 約 46 億ドルを Project Lightspeed に投資し、初期展開の一環として 2008 年末までに約 1,900 万世帯へのサービス提供を実現する予定。

- WiMAX および他の固定無線アクセス・テクノロジーに関連した市場活動範囲を拡大。

3.6.3 米国における NGN 関連の研究開発の状況

ある米国の大手通信機器ベンダは、IMS 製品を 3～4 年前から開発しており、主要な IMS 構成要素をカバーする完全な製品ラインを持っている。また、複数のキャリアが既にこれらの IMS 製品を使用したサービスのトライアルを開始している。これは、実際に顧客に対して VoIP と IPTV を試験的に利用させるフィールドトライアルである。

この企業では、NGN に関する標準化活動への取り組みを通じて標準に関する情報をいち早く入手することにより、ITU で批准された完全な NGN アーキテクチャに基づいた迅速な製品開発を行っている[87]。

米国における政府による ICT 全般に関する研究開発は、National Science and Technology Council (NSTC)[88]が策定する NITRD(Networking and Information Technology Research and Development)[89]計画に基づいて行われている。NGN のセキュリティに関する研究開発については、NSTC 傘下の組織である Cyber Security and Information Assurance (CSIA)Interagency Working Group (IWG)により作成されたレポート『Federal Plan for Cyber Security and Information Assurance Research and Development』[90](2006 年 4 月)に以下の記述がある。

NGN においても最低限、PSTN と同等のセキュリティが必要である。NGN サービスには、各種のネットワーク、アクセス技術、サービスプロバイダネットワークに一貫してセキュリティ対策を適用するためのセキュリティポリシーが必要である。

NGN セキュリティに関して、以下に示す技術の研究開発を実施する必要がある。

- 大規模アイデンティティマネジメント技術
- 拡張性の高い認証アーキテクチャ及び複数の認証ファクタ(ID、パスワード、SIM カードなど)を活用する技術
- 否認防止技術：ネットワークにフォーカスした機能としてではなく、ユーザレベルでの技術。
- コントロールプレーン及びメディアプレーンにまたがって、また、全てのセキュリティレイヤにまたがって、データの完全性、記述性、可用性を確保する技術
- ある程度のプライバシー保護を確保しながら、上記のセキュリティ要件を実現する技術

さらに、President's National Security Telecommunications Advisory Committee (NSTAC)[91]が、国家セキュリティの観点から NGN のセキュリティに関する提言をまとめた報告書『Next Generation Task Force Report』(2006 年 3 月)[92]は、国家セキュリティ通信に NGN を採用することを大統領に提言している。同報告書は、NGN への移行によって、国家セキュリティと緊急時への準備(national security and emergency preparedness (NS/EP)に関わる通信を取り巻くリスクシナリオも根本的に変化するという認識の基に、NGN におけるセキュリティ上の課題を解決する必要があるとしている。

---

87 海外通信機器ベンダへのインタビュー調査(V 章)より
88 http://www.ostp.gov/nstc/
89 http://www.nitrd.gov/
90 http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf
91 http://www.ncs.gov/nstac/nstac.html
92 http://www.ncs.gov/nstac/reports/2006/NSTAC%20Next%20Generation%20Networks%20Task%20Force%20Report.pdf

NS/EP 通信のセキュリティを確保する上では、特にアイデンティティマネジメントが重要であり、ユーザ、デバイス、プロセス、通信のそれぞれについての強力な認証が前提となるとし、研究開発を行うべき領域として、NGN のコントロールプレーンを保護し、コントロールプレーンの機能に対する不正アクセス防止に関する方法を挙げている。

3.7 韓国の状況

韓国における次世代ネットワークは、BcN(Broadband convergence Network)と呼ばれている。現時点での主なアクセス手段は、DSL とケーブルインターネットである。

ブロードバンドインフラ整備に関する政策としては、2004 年に「u-Korea 推進戦略(IT839 戦略)」を公表し、通信・放送・インターネットの間でシームレスなインフラとして広帯域統合網 BcN を構築し、2010 年までに 2,000 万人の加入者に対して 50～100Mbps での BcN への接続を可能にするという目標を掲げた[84]。

2006 年 3 月には、世界最高水準のユビキタス社会の実現を目指した「u-KOREA 基本計画」を策定。また、2004 年に策定された IT839 戦略の見直しが、u-KOREA 戦略と歩調を合わせて実施され、2006 年 2 月に「u-IT839 戦略」として発表された[93]。

通信事業者の KT は、「FTTH 推進戦略」を策定し、2004 年 10 月の光州地域の 100 加入者に対するモデルサービスを経て、2009 年までに 100Mbps 級の速度の光ケーブル 174 万 9000 回線を普及させる計画を発表している [84]。

また、u-Korea 推進戦略(IT839 戦略)に従って、2010 年までにネットワークのオール IP 化を計画しており、2006～2007 年に市外網を IP 化し、2008～2010 年ですべての電話交換機を IP ベースのデータ転送装置に交換することを計画している [84] **エラー! ブックマークが定義されていません。**。

2005 年末時点での韓国のインターネット利用者数は 3,301 万人(人口比で約 70%)であり、ブロードバンドサービスの加入者は 1,219 万人となっている[94]。

3.7.1 BcN の構築計画

BcN は、以下の 3 つのフェイズに分けて構築される計画となっている。

■ Phase 1 (2004 - 2007) PSTN からの移行

- PSTN の移行 ： 韓国でも電話交換機の老朽化への対処が、NGN へ移行する動機となっている。
- toll switch のクラス 4 ソフトスイッチへの交換
- local switch のクラス 5 ソフトスイッチへの交換

■ Phase II (2006 - 2008) 通信の統合

- IP ネットワークと PSTN の BcN への統合
- 音声／データの統合 ： マルチメディア通信ビジネス
- 有線／無線の統合 ：FMC ビジネス
- 統合通信ブロードキャストビジネス

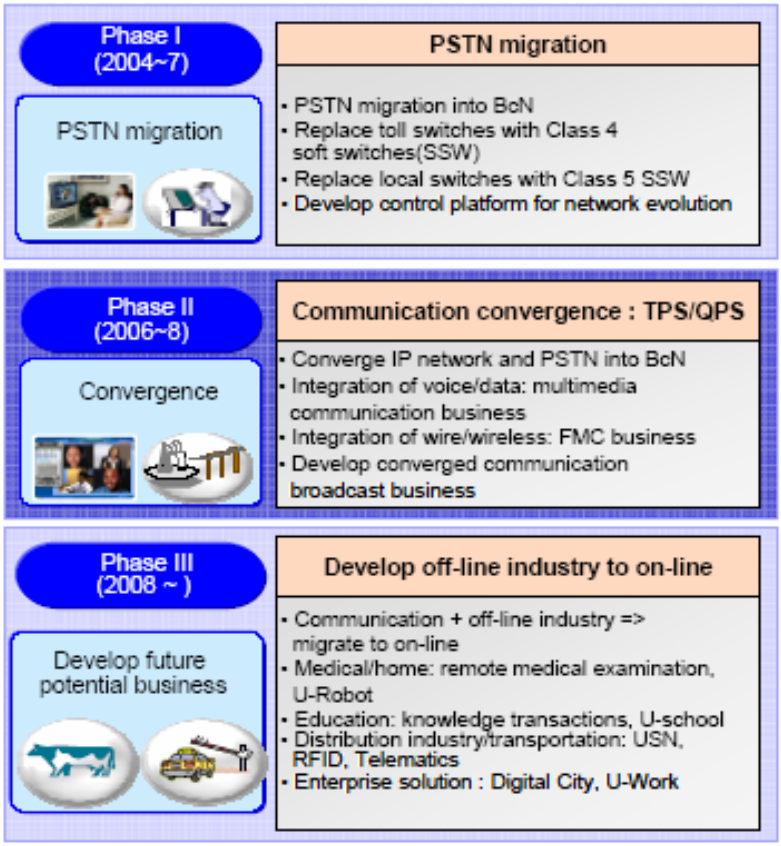
■ Phase III (2008 -) オフライン産業のオンライン化

- 遠隔医療の試験、U-ロボット
- 教育 ： 知識処理、U-School
- センサネットワーク、RFID、テレマティークス
- 企業ソリューション ： デジタルシティ、U-Work

BcN 構築計画の概要を図 1.23 に示す[95]。

---

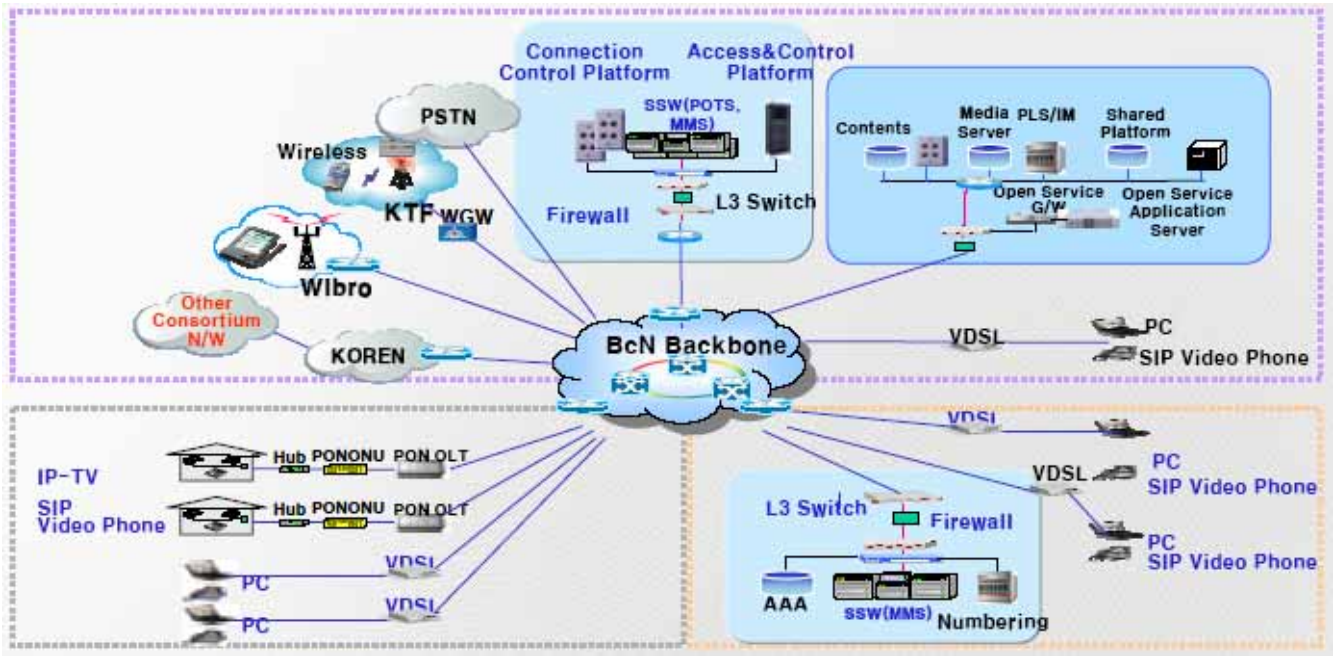
[93] http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h18/html/i2625000.html
[94] 総務省 2006 年度通信白書
[95] KT BcN service strategy



(出所 ：KT BcN service strategy)

図 1.23　BcN 構築計画の概要

BcN のインフラストラクチャ構成を図 1.24 に示す[96]。

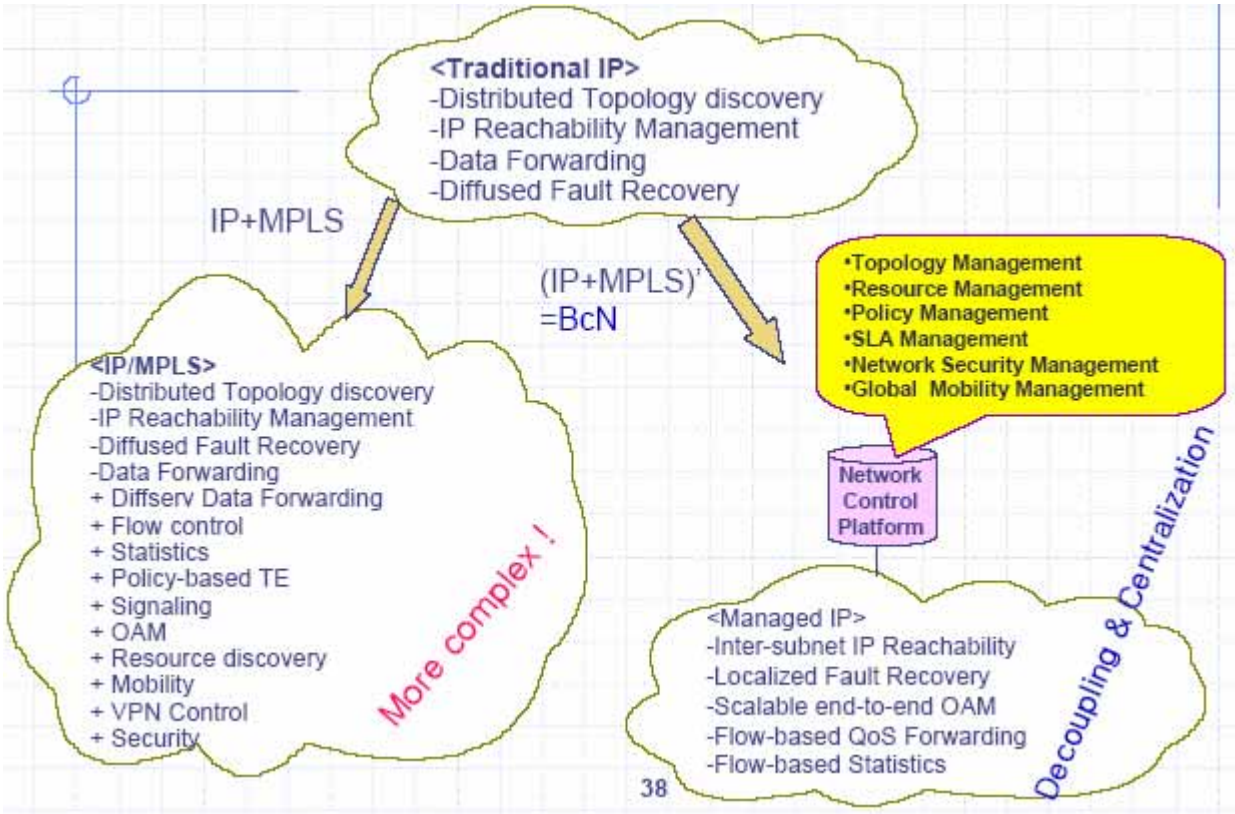


(出所 ：KT's FTTH Service Scenario)

図 1.24　BcN のインフラストラクチャ構成

[96] KT's FTTH Service Scenario (2006 年 9 月)

BcN のコンセプトを図 1.25 に示す[97]。



(出所 ：BcN Control and Management (ETRI BcN Research Division))

図 1.25　BcN のコンセプト

3.7.2　BcN のセキュリティ対策

BcN のセキュリティに関しては、MIC(情報通信省)がセキュリティ対策を推進しており、現在、以下の政策／技術開発が実施されている。

- 異常トラフィックを感知・遮断・対応する高性能ネットワーク統合セキュリティシステムの開発
- RFID やセンサーネットワーク環境に適合した超軽量暗号モジュール及びセキュアセンサーノードの開発
- 安全な情報通信環境のための法制度施行
- フォレンジックス関連技術の開発
- トラフィック監視システムの構築
- セキュリティテストベッドの構築

また、以下のセキュリティに関する項目の必要性が認識されており、今後の取り組みが予定されている。

- 統合セキュリティインシデント管理体系の構築
- インシデントの波及範囲の拡大(インターネット、放送網、電話網)への対処
- 高性能 QoS-Aware ネットワークセキュリティ技術の開発
- 新規サービスと多様な複合ターミナルに対するセキュリティ技術の開発

[97] BcN Control and Management (ETRI BcN Research Division)

Ⅱ章　次世代ネットワークに関するセキュリティ技術の動向

1. 次世代ネットワークに求められるセキュリティ機能及びそれを実現するための技術とその標準化動向、実験プロジェクトの動向

次世代ネットワークに求められるセキュリティについては、I 章で述べたように、以下のセキュリティ機能が求められている。

■　トランスポートストラタムに対するセキュリティ要件

- NGN 顧客ネットワークドメイン
- 顧客ネットワークと IP コネクティビティアクセスネットワーク(IP-CAN)とのインタフェース
- コアネットワーク機能
- NGN 顧客ネットワーク相互のインタフェース

■　サービスストラタムに対するセキュリティ要件

- IMS コアネットワークセキュリティアーキテクチャ
- IMS セキュリティアーキテクチャインタフェース要件
- トランスポートドメインと NGN コアネットワークとのインタフェース
- アプリケーションとコアネットワークとのインタフェース
- アプリケーションドメインセキュリティ
- NGN 顧客ネットワークとアプリケーションとのインタフェース
- VoIP セキュリティ要件
- 緊急通信サービス及び災害救助に対するセキュリティ要件
- オープンサービスプラットフォーム及び付加価値サービスプロバイダのセキュリティ

また、NGN におけるセッション制御に IMS を使用することが決まっていることから、IMS 自体のセキュリティ確保が課題である。

日本における NGN の実験プロジェクトとしては、セキュリティに特化したものではないが、NTT による NGN のフィールドトライアル[98]が実施されており、通信機器ベンダや ISP、エレクトロニクスメーカなどが参加している[99]。また、NGN のフィールドトライアルショールーム NGN Open Trial Exhibition(NOTE)[100]において、以下に示すサービスのデモンストレーションが実施されている。

■　ビジネス向けサービス
- ハイビジョン映像コミュニケーション
- 高品質 IP 電話会議装置
- 企業向けネットワークサービス
  - 広帯域で高品質なＱｏＳを実現したＮＧＮ広域イーサ
  - 暗号化通信などを組み合わせたセキュアなセンタエンド型ＶＰＮ
- 遠隔病理診断支援システム
- PTMN：Push to Talk with Multimedia over NGN
  音声のみではなく、動画、静止画などの様々なメディアを共有しながら、複数の人々が同時にコミュニケーションできるシステム

[98] http://www.ntt.co.jp/trial/
[99] CISCO 社の TelePresence (http://www.cisco.com/japanese/warp/public/3/jp/solution/uc/telepresence/index.shtml) など
[100] http://www.ngn-note.jp/top.html

■ コンシューマ向けサービス
- ハイビジョン IP テレビ電話
- 高品位フレッツフォン
- 高品質 IP 電話機
- ワンフォン
- 地上デジタル放送 IP 再送信
- ハイビジョン映像配信サービス

■ 福祉／災害対応サービス
- ホームセキュリティ・コントロール
- 災害時の安心サービス
- 介護ヘルスケア
- 多目的 AV 家電連携端末
- ユビキタス見守り
- ロボットによる優しい見守り

NGN におけるセキュリティについては、総務省の次世代 IP ネットワーク推進フォーラム [13] 及び情報通信審議会 情報通信技術分科会 IP ネットワーク設備委員会[101]において検討が行われている。

ここでは、次世代 IP ネットワーク推進フォーラムの技術基準検討 WG(第 1 回)／各 SWG(第 1 回)合同会合(平成 18 年 1 月 27 日)における資料『技術基準における課題と検討の方向性』と、情報通信審議会 情報通信技術分科会 IP ネットワーク設備委員会における資料『IP 化に対応した電気通信設備のための技術的条件における課題と検討の方向性』を基に、NGN におけるセキュリティ上の課題をまとめる。
表 2.1 及び表 2.2 に、それぞれの資料に記載されているセキュリティ上の課題と検討の方向・内容を示す。

表 2.1 次世代 IP ネットワーク推進フォーラムにおいて挙げられた NGN におけるセキュリティ上の検討項目

検討項目	論点	検討の方向性
• セキュリティガイドラインの公開範囲と方法	• セキュリティのガイドラインは、どこまでをどのように公開し、クローズにすべき内容をどこでどのように規定すべきかの考え方を整合すべきではないか。 • セキュリティ保護上の公開条件について、海外の状況も踏まえて、議論すべきではないか。	
• 個人認証・個人情報 IP 網における IP アドレスや位置情報などの個人情報を保護する手段の検討	• 個人認証、個人情報保護は事業者のサービス上の観点、個人情報保護法の観点からあるべき姿。 • IP アドレスから利用者が特定でき、また、在圏する網(位置情報)も容易に分かることから、これらのような個人情報の保護についても整理すべきではないか。	• 技術基準として設ける必要はないのでは。
• 障害対策	• サイバーテロ、コンピュータウィルスなどの新たな脅威への対応 • 技術検証を含めた整理 • ネットワークを論理的に複数のセキュリティゾーンに離し、各レベルに応じた対策	• IP 網共通のセキュリティ対策は議論すべき。 • サービスに依存するセキュリティ対策は議論対象外とすべき。
• 利用者端末のセキュリティ対策対処機能	• セキュリティ対策として端末のファームウェアのアップデートを利用者任せにするのではな	• 信頼性の観点から議論は必要。 • 端末の機能の観点から議論すべき。

[101] http://www.soumu.go.jp/joho_tsusin/policyreports/joho_tsusin/ipnet/ipnet.html

	く、ネットワーク側からの指示でできるような機能を予め備える必要があるのではないか。	
• アプリケーションのセキュリティを確保するためのネットワークでの対策	• 今後起き得る変化に対応するために、安全性・信頼性の基準を柔軟に考えられる形にしておく必要があるのではないか。	• アプリケーションの拡張の可能性も重要だが、電話のようにライフラインとして規格を規定すべき。 • ネットワークが、サービスを意識してセキュリティや信頼性を確保する観点からは、いくつかのセキュリティレベルを規定しておくことも良いのでは。
• モデリング	• 著作権保護の見地から DRM システムの構築が必須となる一方で、ユーザーの利便性も考慮すべきではないか。	• 検討のベースとなるモデルを策定 • 多様なビジネス形態、プレイヤーを許容できるネットワークモデルをベースとして議論すべき。 • 検討範囲は NGN トランスポートストラタムとサービスストラタム(含む API)とすべき。

(「次世代 IP ネットワーク推進フォーラム」技術基準検討 WG(第 1 回)／各 SWG(第 1 回)合同会合(平成 18 年 1 月 27 日)
配布資料　技術基準における課題と検討の方向性より作成)

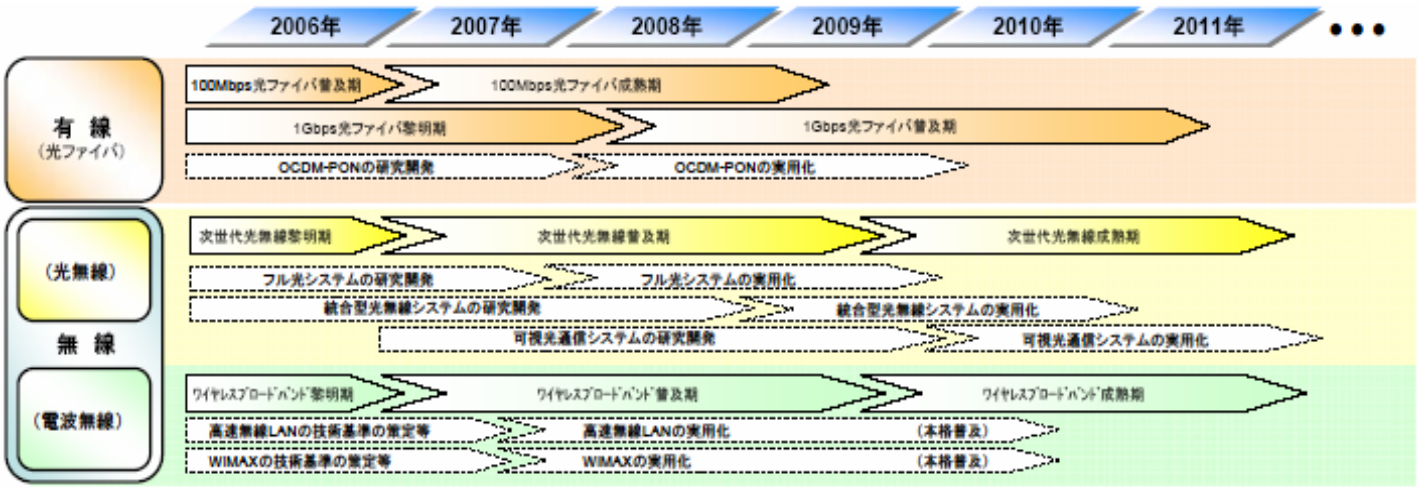
表 2.2　IP ネットワーク設備委員会において挙げられた NGN におけるセキュリティ上の課題

大項目	中項目	課題項目	検討内容
安全性	個人認証／個人情報	• なりすまし／発 ID 偽装対策	重要通信の妨害や各種のセキュリティ攻撃につながる発 ID／IP アドレス／ユーザ等のなりすましへの対策
		• 個人情報保護	発 ID や回線情報等のユーザ情報などの個人情報の保護対策
		• 逆探知	発信者の回線情報／エリアを特定するために必要なネットワーク設備及び端末の要件
	サイバー攻撃対策	• 端末からの脅威(SPIT、ワン切)への対策 • INVITE 呼集中防止対策	• SPIT やワン切などの電話を使った攻撃を防止するためのネットワーク設備／端末の機能要件 • INVITE 呼集中による機能停止等を防止するためのネットワーク設備／端末の機能要件
		• ネットワークからの脅威(DDoS、スパム、不正アクセス)	• ネットワーク境界(UNI,NNI)でのフィルタリング等のあり方 • ユーザネットワークや相互接続網からのウィルス伝染や、異常トラフィックが流入した際の緊急遮断ルール
		• 通信の盗聴等	通信の秘密を確保する対策(暗号化等)
		• SIP と連動しない音声通信流通の制限	P2P 等を利用した攻撃目的での電話端末への直接通信を防止するための対策
	端末機器	• 端末機能の安全性確保	端末のセキュリティ関連機能の改ざん防止対策
サービス制御機能	セキュリティ確保	• 不正利用、不正アクセス(なりすまし)／SIP 脆弱性攻撃防止 • 自網からの流出防止と、他網の流入防止の双方対策	本検討課題においては C プレーンに係わるセキュリティ確保について検討する。 • 不正利用、不正アクセス(なりすまし)、SIP 脆弱性攻撃防止について － 不正利用、不正アクセス(なりすまし)を防止するため、自ユーザを認証する。 － 電気通信事業者協会(TCA)策定の発信者番号偽装対策ガイドラインに従う。

			― DoS 攻撃対策を実施する。 • 自網からの流出防止と他網からの流入防止の双方の対策について ― SIP 信号疎通の制限を実施する。
トランスポート(IP ネットワーク)機能	セキュリティ確保	• ウィルス／ワーム等の流入／流出の防止 • 盗聴／RTP 偽装の防止等	• ウィルス／ワーム等の流入/流出の防止 ―事業者網内の装置が原因で、ウィルス／ワーム等が他網へ波及することがないよう処置をとる。 ―C プレーンと連携した U プレーンのみの疎通とする。 • 盗聴／RTP 偽装の防止 ―通信の秘密を守る処置をとる。 ―事業者網内トポロジーの隠蔽をするための仕組みを導入。 ―DoS 攻撃対策をとる。

(総務省 情報通信審議会 情報通信技術分科会 IP ネットワーク設備委員会作業班 検討状況報告 ～ IP 化に対応した電気通信設備のための技術的条件における課題と検討の方向性 ～ (平成 18 年 4 月 17 日)より作成)

NGN の基盤となる次世代ブロードバンド技術の研究開発については、総務省資料『ブロードバンドの全国整備に向けた取組』[102]に、2011 年までのマイルストーンが示されている(図 2.1)。



(出所 ： 総務省資料『ブロードバンドの全国整備に向けた取組』)

図 2.1　総務省が提示する次世代ブロードバンド技術の研究開発計画

NGN のセキュリティ技術の研究開発については、総務省傘下の情報通信研究機構(National Institute of Information and Communications Technology：NICT [103])が委託研究の計画書[104]を公開しており、以下のセキュリティ関連技術の開発が計画されている。

- セキュリティや QoS などのサービス機能を提供するサーバの連携技術
- IPSec／IKE に関する相互接続のための検証技術の研究開発
- 端末からのシグナリングを契機として、必要な QoS やセキュリティを自動的に設定する機能の実現
- 認証サーバ連携によるセキュリティ高度化技術
- サービスのセキュリティ属性に応じた接続制御を行う技術

[102] www.soumu.go.jp/joho_tsusin/policyreports/ chousa/bbseibi/pdf/061127_2_si4.pdf
[103] http://www.nict.go.jp/index-J.html
[104] 平成 18 年度 新規委託研究「次世代ネットワーク(NGN)基盤技術の研究開発」研究計画書 www2.nict.go.jp/q/q265/s802/ info/20061130koubo/theme_b001_koubo.pdf

2. 通信事業者や通信機器ベンダにおける次世代ネットワークに関するセキュリティ技術への取り組み動向

以下では、次世代ネットワークに関するセキュリティ技術への取り組みについて、海外の通信事業者や通信機器ベンダを対象として実施したインタビュー調査の結果をまとめる。インタビュー調査の詳細な結果については、V 章に記載する。

2.1 NGN のセキュリティにおける重要な課題

- 携帯電話がインターネットに接続される際のセキュリティ
- ルーティングインフラストラクチャのセキュリティ
- SIP のセキュリティが課題である。SIP は、シグナリングを行う権利をエンドユーザに渡しており、これが脆弱性につながる。
- Identity 管理
- サービス契約者(ユーザ)の認証及び認可
- アクセスセキュリティ、デバイスセキュリティ、アプリケーションセキュリティ、シングルサインオン
- ITU X.805 セキュリティモデルで言及されている脅威への対応
- IPTV のセキュリティ

2.2 NGN において早期に解決すべきセキュリティ上の課題

- 通信事業者、機器ベンダともにセキュリティへのフォーカスが欠落していること
  具体的には、多くの製造業者(manufacturers)が既にあるセキュリティ対策の全てを実装しているわけではないことと、キャリアが既に機能として存在するセキュリティ対策を有効にしていないこと。
- プラットフォームセキュリティ(特に携帯電話)
- ソフトウェアのアップグレードの自動化
- 認証、認可、Identity 管理
- SPIT と SPAM
- NGN がクローズドなネットワークであるべきか、オープンなネットワークであるべきかに関する問題

2.3. NGN が広く利用されるようになった時に解決される、あるいは解決すべきセキュリティ上の課題

- DoS 攻撃
- ウイルスやスパム
- レガシー端末の移行に関する課題（移行が完了した後には、信頼性を確立するために SIM カードのような、なんらかの物理的なデバイスを端末に組み込む必要がある。）

2.4 暗号の危殆化への対応

- ITU としてのアルゴリズムは開発しないが、NGN においていずれの暗号が最もよく動作するかを提示する。
- ETSI において暗号に取り組んでいるグループは、暗号の危殆化を問題として認識している。
- IMS には、アルゴリズムが危殆化した場合に、代替アルゴリズムに置き換える機能がある。

- より脆弱性の低い鍵付きハッシュ関数(Keyed hash function)を使っている。

2.5 NGN に接続する端末に関する規制について

- NGN が独立したネットワークであれば､接続ルールを規定することができる｡そうでなければ、そのようなルールを作ることはできない。
- ネットワークに接続する全てのデバイスの特定と認証を強く推し進めようという動きが見られる。
- ソフトウェアについては特定の規制は必要ではない。
- ETSI は、NGN において USB 版の SIM を使う事を決定した。これによって、NGN への接続を可能にするデバイスとして、USB SIM が採用される可能性が大きく増加するだろう。

2.6 モバイル IP について

- ITU は、3GPP2 におけるモバイル IP に関する作業の結果を取り込む。
- 3GPP は、LTE(Long Term Evolution)イニシアティブの一部として、モバイル IP を利用することを考えている。

2.7 DRM について

- ITU は DRM の仕様を策定していないが、トリプルプレイと深い関連がある IPTV に関する標準が策定されることによって、結果的に DRM に関する標準を策定しなければならなくなるだろう。
- ケーブルテレビ業界も DRM に関する独自のアプリケーション仕様を作成する予定である。

2.8 UDP トラフィックの増加が引き起こすと予想される問題について

- UDP トラフィックを絞ることがトラフィック増加への唯一の対処方法である。
- いかなるデータストリームについても、適格であり、かつ認証され、認可されたものであることを確実なものとする。
- DoS 攻撃を防止するために、スプーフィングは許可されず、トラフィック制限を超過したデバイスはネットワークから切り離されるだろう。
- ETSI TISPAN WG7 では、DoS 攻撃に対する保護策についての議論は開始されていない。
- IMS には DoS 攻撃に対するソリューションがあるので、ケーブルネットワーク事業者はそれに従う。

2.9 IMS のセキュリティについて今後必要となる、あるいは、開発予定の機能

- ITU における我々のゴールは、セキュリティが、"ベアラ通信路" にも適用されるようにする(データの中身のセキュリティも確保する)ことである。
- ファイアウオールの導入が IMS に必要なセキュリティ強化策である。
- モバイルネットワークにおける認証のためのスマートカード(SIM カード)の使用に関する課題
- ブロードバンドネットワークにおけるセキュリティの確保が必要
- IPTV のセキュリティ要件への対応が必要
- IMS を固定ネットワークに適用できるようにするためのセキュリティ要件の追加が必要

- ケーブルネットワークの要件に合うように IMS の仕様を改訂する必要がある

2.10 3GPP 及び 3GPP2 において標準化をリードしている組織

- 3GPP2 では Lucent, Qualcomm, Sprint, Cisco が最も active である。
- ETSI TISPAN WG7 は、3GPP のセキュリティグループと非常にうまく協力している。
- IMS に関して本当にアクティブなのは､新しいネットワークアーキテクチャの展開によって多くを得る製造業者(manufacturers)である。

2.11 3GPP 及び 3GPP2 で議論されているセキュリティ上の課題

- Network Firewall Configuration and Control(NFCC)
- 認証が、固定、ワイヤレス、ケーブルといった様々なタイプのネットワークにおいて動作することを保証すること
- 3G ネットワークにおけるレガシー(2G)端末の扱い
- 携帯電話におけるインターネットベースの認証
- モバイル環境に対応した認証

2.12 NGN の開発プログラム、NGN ベースのサービスのロードマップについて

- いくつかのキャリアが既に開発した IMS 製品の IPTV と VoIP への適用トライアルを開始している。
- 既に提供している NGN サービスをグローバルに展開する予定である。
- ユーザが自ら放送サービスを提供できるようにする
- 携帯電話から家庭のテレビへ、あるいはその逆へと、シームレスにコンテンツの視聴を可能とする
- 全ての通信事業者(モバイル通信事業者、固定通信事業者、ケーブル通信事業者)が IMS ベースのアーキテクチャを採用した時の相互運用性確保

2.13 FMC について

- MD5 により生成された HTTP ダイジェストを使用するレガシー端末の問題を解決する必要がある
- モバイル端末が WiFi のような他のデータアクセスメカニズムを持っている場合のセキュリティの確保
- 呼がモバイルネットワークと固定ネットワークのどちらのネットワークを起点にしたものか、あるいは、契約者がモバイル事業者と固定事業者のどちらに属するのかという問題

2.14 NGN に必要な技術の獲得方法

- ヨーロッパでは伝統的に、キャリアが必要とするものをベンダに伝え、ベンダがそれを実現する製品を開発している｡その際の一般的な手法は､通信事業者とベンダとでコンソーシアムを立ち上げ、共同でソリューションを開発するというものである。

2.15 ネットワークの中立性について

- ネットワークへのオープンかつ平等なアクセスという点では賛成するが、規制については懐疑的。
- 料金を支払った人に対して、あるいは、緊急事態が発生した場合に優先してサービスを提供する技術を持っている。

2.16 通信事業者に適用される法律や規制への対応について

- 全ての通信記録を保存する機能を持っており、令状(warrant)が出された場合に使用される。
- 要件は国によって大きく異なるのではないか。
- NGN であれ PSTN であれ、サービスが同じである以上、同一の規制が適用される。

2.17 PSTN と NGN との通信ログの保存に関する違いについて

- 両者で大きな違いがあるのは、放送サービスとマルチキャストサービスの場合である。ユーザが、複数の人と通信を行う場合には、セッションの記録やログの作成は、より難しいものとなる。

2.18 日米欧における携帯アプリケーションの嗜好の相違

- 日本では、携帯電話を使ってインターネットを閲覧する際に、PC と同様の高度な機能を使うが、ヨーロッパではより限定された機能しか使わない。

2.19 標準化への取り組みに力を入れている国、ヨーロッパと米国の取り組み方の相違

- IPTV 以外の分野では、ATIS は ETSI よりもアクティブではない。
- 通信事業者に関する標準は米国においては通常はオプションであるのに対し、ヨーロッパにおいては義務であることを認識する必要がある。
- ヨーロッパでは多くのキャリアが依然として、固定通信とモバイル通信とを一つの企業の中に有していることが、NGN 推進のインセンティブとなっている。
- 米国では、トリプルプレイがキャリアの NGN への移行のインセンティブとなっているようである。
- ヨーロッパは、政府によってネットワークのアップグレードが義務付けられているが、米国では PSTN の補完というアプローチのようである。
- 米国では、プロプライエタリなソリューションが開発されると、競争優位を確保するために、できるだけ早期に市場に投入しなければならない。
- ヨーロッパでは、キャリアとベンダが ETSI に深く関わっており、ETSI の標準によく従っている。
- ヨーロッパが標準の策定に重点的に取り組んでいる理由は、これまでに 3G に取り組んできたことにある。
- ヨーロッパの GSM モバイル事業者が 3GPP を創設したことから、現在でも彼らがリードしている。

2.20 標準化に取り組む目的について

- 中国の場合、国内に創業間もない企業が多数あり、それらは非常に速い成長を望んでいる。そのような企業は、標準に寄与することによって NGN に向けた開発競争でリードできると考えているの

ではないか。
- 製品と NGN のフレームワークとの間に、ギャップが存在しない事を確実なものとしたいと考えている。
- ベンダは、NGN 用の機器を売ることが出来るので、IMS と NGN を推進している。
- キャリアにとってもコスト削減など、all IP ネットワークに移行する大きな動機がある。
- NGN 標準に準拠した製品の方が独自仕様の製品よりも経済性が高い
- 他の通信手段(ワイヤレス、固定)とのコンバージェンスによる利益

2.21 海外インタビュー調査のまとめ

NGN におけるセキュリティ上の課題としては、アイデンティティ管理、ユーザ認証、SIP のセキュリティ、プラットフォームセキュリティといった項目が挙げられている。アイデンティティ管理とユーザ認証は、後述する米国政府による NGN への取り組みにおいても言及されている課題であり、重要度が高いといえる。

NGN への取り組みの面で米国と欧州とで異なるのは、通信事業者を取り巻く環境である。ヨーロッパの通信事業者が NGN を推進する理由には、以下のようなものがある。

- 固定ネットワークとモバイルネットワークの両方を持つ通信事業者が多い。このような通信事業者には、固定通信とモバイル通信を融合したサービスを提供することにより、大きなメリットがもたらされる。
- 政府による通信設備更改の義務付け。

一方、米国においては、固定ネットワークとモバイルネットワークのいずれかを持つ通信事業者が多いため、ヨーロッパの通信事業者ほどには NGN から受ける恩恵は多くない。また、通信設備更改が義務付けられているわけでもないため、NGN への移行を積極的に推進する状況ではない。しかし、電話会社を母体とする通信事業者とケーブルテレビ事業者との競争が激化していることから、IPTV やトリプルプレイ(インターネット接続、電話、テレビ番組の配信)の提供による新たな収益源の確保が、電話系通信事業者の NGN への移行を推進する動機づけとなっているようである。

通信機器ベンダが標準化を推進する理由としては、自社が保有する技術を標準に反映することにより競争の優位性を確保することができる、標準に関する情報をいち早く入手することにより、タイムリーな技術開発／製品開発が可能になる、標準から外れた仕様・規格の製品を設計・製造しなくて済むため、効率的かつ迅速な製品開発が行えるというものがある。しかし、最も大きな理由は、通信事業者の NGN への移行は、時期的な相違はあるにしても最終的には実施されるものであることから、通信機器ベンダは確実に NGN 向けの製品を売ることが出来ることである。

標準化のメリットとしては、効率的な製品開発により、開発コストが削減され、通信事業者の設備投資に必要なコストの削減につながり、最終的にはエンドユーザの利用料金が安くなるというものもある。

標準化された製品によって構築される NGN において、通信事業者が競争力を持つためには、いかにして、ユーザのニーズに合ったサービスを安全・安心に利用できる環境を整備するかという点にかかっている。NGN ではネットワークのセキュリティは確保されていることから、アイデンティティ管理とユーザ認証、アクセス制御が、競争力の確保においても重要となる。

Ⅲ章　次世代ネットワークの実現時期に関する考察及び次世代ネットワークに対する日本の取り組みに関する考察・提言

1. 次世代ネットワークの実現時期に関する考察

次世代ネットワークが実現したといえるためには、誰でも利用できるブロードバンドインフラが整備されることと、通信事業者のネットワークの PSTN から NGN への移行が完了することが前提となる。前者については、国の政策または通信事業者の計画から、後者については、通信事業者の計画から、それぞれ読み取ることができる。

ブロードバンドインフラの整備については、総務省の計画[63]から、日本におけるブロードバンドインフラの整備は 2010 年までにほぼ完了すると考えられる。

通信事業者のネットワークの移行に関しては、移行計画を明らかにしている NTT と BT については、計画通りに進めば、それぞれ 2010 年と 2011 年にネットワークの IP 化が完了すると考えられる。

日本においては、ADSL による高速ブロードバンド及び光ファイバよる超高速ブロードバンドインフラの整備が進展していること、NTT による NGN のフィールドトライアルが開始されていることから、NTT の中期経営戦略にうたわれているように、2007 年度下期からエッジノード及びサービス制御機能の導入が開始された後、漸次、次世代ネットワークをベースとしたサービスの提供が開始され、2010 年には 3,.000 万ユーザが光アクセスと次世代ネットワークサービスを利用できるようになるであろう。

ただし、現在勧告化に向けて作業が行われている NGN リリース 1 のセキュリティ要件(Y.2701)の他に、2.6.4 で挙げた現在検討が進められている NGN セキュリティに関する様々な勧告が今後リリースされる見込みであること、さらに、IMS のセキュリティ確保[105]が今後の課題として残されていることから、セキュリティが確保された NGN の実現にはもうしばらく時間がかかると思われる。

それまでの間は、ネットワークも端末もセキュリティに関する勧告がリリースされるたびに要求条件に適合するようバージョンアップをすることになるであろう。その意味では、次世代ネットワークは進化し続けるネットワークであり、NGN の実現時期は、必要十分なセキュリティが確保され、真に安全・安心な NGN が実現した時点ということになるのかもしれない。その時期を現時点で予測することは難しい。

NGN の採算という観点で考えると、NGN が提供する高度なサービスを利用するユーザの数がどの程度になるかが重要である。NGN のインフラが整備されたとしても、提供されるサービスが魅力的なものでなければ、従来の PSTN と同様に音声通話の利用者が大部分ということになりかねない。例えば、ヨーロッパにおける NGN を利用したサービスの中でニーズが高いのが、固定電話サービスと携帯電話サービスをシームレスに提供する FMC と、ブロードバンドによるテレビ番組の視聴(IPTV)である。BT の見解にもあるように、通信事業者は当面は ADSL によるブロードバンド回線で FMC と IPTV を提供し、より帯域幅の広い回線が必要となるサービスに対するユーザのニーズが高まった時点で、光ファイバインフラの構築に踏み切るものと思われる。BT によれば、その時期は 2009 年以降ということになる。日本が 2010 年のブロードバンドインフラ整備目標の達成までに 6～7 年かかることを考えると、ヨーロッパにおいて NGN が実現するのは、2015 年以降ということになるのかもしれない。

日本においては、NGN のフィールドトライアルの一環として、地上デジタル放送の IP 再送信が開始された[106]ことから、ヨーロッパに先駆けて光ファイバによる IPTV が実現することになる。ヨーロッパのブロードバンドユーザが日本の IPTV を見て、ADSL による配信との画質や音質の違いを実感した結果、ヨーロッパの通信事業者による光ファイバの敷設が早まるということも考えられる。

---

[105] 3GPP2 から IMS Security Framework という文書がリリースされている

[106] http://www.ntt.co.jp/news/news07/0701/070126a.html

2. 次世代ネットワークに対する日本の取り組みに関する考察・提言

日本では、総務省と通信事業者の先見性のある取り組みによって、非常に高度なブロードバンドインフラが整備されたといえる。日本におけるブロードバンド環境の特徴は、高度なインフラに加えて、一般家庭に、ホームネットワークやデジタル家電、多機能な端末といった、高度な通信設備・機器が普及している点である。しかし、NGN へのアクセスポイントから先の部分におけるセキュリティは、通信事業者の責任分界点の外であり、ユーザ機器に対するセキュリティ対策は、ユーザ自身がケアしなければならない。

また、NGN が提供する主な機能は、セキュリティと QoS であるが、End to End でそれらを保証するためには、ネットワークとエンドユーザが使用する機器との間での役割分担が必要である。

端末やデバイスのセキュリティに関しては、これまでに CC(Common Criteria)や、TCG といった取り組みがなされてきており、これらの成果を活かしながら NGN における端末やデバイスのセキュリティについての検討を行う必要がある。

ユーザ機器に対するセキュリティの確保に加えて、NGN を利用して提供されるサービスを安全・安心なものとするために、ユーザ機器とネットワークとを統合された一つのシステムとして考えた場合のセキュリティの確保に向けた取り組みも必要となるだろう。

海外に対する支援という面では、現在、総務省の主導によるアジアブロードバンド計画を初めとして、次世代のネットワークインフラ整備に向けた海外支援策が推進されている。アジアブロードバンド計画では、以下の目標が掲げられている [94]。

① すべての人々がブロードバンドへアクセス
② アジア・北米・欧州間の情報流通量を均衡化
③ IPv6 への移行、ICT でアジアが世界をリード
④ 人々が安心して情報通信技術を利用できる環境の整備
⑤ 文化的財産等のデジタル・アーカイブ化
⑥ 主要言語間の機械翻訳技術の開発・実用化
⑦ 情報通信分野の技術者・研究者を大幅に増加

また、アジアブロードバンド計画のこれまでの取り組みの例として、『アジアブロードバンドプラットフォームの構築：光ファイバ等によるテストベッドを活用したアプリケーションの開発・実証等』が挙げられている。

欧米における NGN に関する動向の項で述べたように、BT が次世代ネットワーク 21CN の構築を通じて得たノウハウを活かした NGN 構築支援コンサルティングサービス 21C Global Venture を提供している。日本は、光ファイバインフラの構築において最先端にあることから、その技術的なノウハウを活かして、これから光ファイバインフラを整備する国を対象に技術支援を行うことが、国際貢献の点からも重要である。

また、欧米における NGN インフラの構築状況からもわかるように、欧米では日本で構築が進んでいる超高速なブロードバンドインフラや、それによって提供される高品質かつ高機能なサービスが実現するのはもう少し先のことになると思われる。

さらに、日本のマーケットは、R&D レベルの高性能かつ高機能な製品がユーザに受け入れられる特殊なマーケットであるが、そのようなハイスペックな製品を海外で販売しても日本ほどには受け入れられない可能性が高い。その典型的な例が携帯電話であり、海外では機能的にシンプルな端末の方が人気が高い。

従って、海外のマーケットにおいて製品を販売するためには、国内のマーケットと海外のマーケットの違いを正しく認識し、海外に対しては国内とは異なる戦略で臨む必要がある。例えば、海外に対しては、個々の国のユーザニーズに合ったスペックの製品やシステムを用意するなどといった対策が必要となる。

このような事を考慮した上で、日本の先進的な部分や技術的に強い領域をどのように産業育成に活かすか、特に、海外マーケットにおいて受け入れられるためにはどうすればよいかを検討する必要がある。

日本が強い領域、先進的である領域を以下に示す。

- 100Mbps でのアクセスが可能な光ファイバインフラの普及が進んでいる
- ホームネットワークの普及とホームネットワークに接続される端末の多様化、高機能化、高性能化
- 高機能な携帯端末と多様なモバイルサービスが普及している

これらの利点を活かす具体的な方策としては以下が考えられる。

- 国内と海外のマーケットの特性の違いを考慮し、グローバルマーケット向けのカスタマイズされたスペックの製品・サービスと国内向けのスペックの製品・サービスの両方を用意し、マーケットに合わせて投入する。例えば、全体のアーキテクチャを構築しておいて、国内向けにはフルスペックの製品、海外向けには個々にカスタマイズされたスペックの製品という使い分けができるようにしておく。
  セキュリティスペックの観点では、各国の法律や規制、ユーザニーズなどに合わせたセキュリティポリシーを用意しておいて、それぞれの国の事情に合わせて製品やサービスにポリシーを適用する、あるいは、各国のマーケットに合わせたセキュリティ機能を実装した製品を製造するということが考えられる。

- 製品の場合、スペックごとの製造ラインの振り分けを考える必要がある。例えば、セキュリティ機能のブロックごとにパーツ化し、パーツの付加・削除によって、容易に様々なセキュリティスペックを持った製品が製造できるようにしておくことなどが考えられる。

- R&D の先進性を活かしたサービスのデモンストレーション用のショーケースを作って一般公開し、同様のサービスに対するニーズがある国に対して、システムの構築を支援することが考えられる。
  その際にコアとなる技術は開示せずに、構築に必要な技術だけを教えることにより、ノウハウを盗まれないようにするといった配慮も必要である。

- NGN 向けセキュリティ認証基準の策定や、それをベースにした認定ビジネスが考えられる。例えば、ISMS 適合性評価制度と同様のスキームによる NGN セキュリティ適合性評価制度といったものである。NGN に接続する端末のセキュリティ要件や、NGN が提供する機能と端末の機能とのインタフェースを定義し、それを基に NGN に接続する端末のセキュリティ認証・認定を行う。

- 携帯電話の場合は、インターネットとは異なり、閉じたネットワークとすることによってセキュリティが確保されている。オンラインで決済ができるのも現状では携帯電話だけである。NGN においても携帯電話と同等のセキュリティが確保されれば、固定網を融合したシームレスな決済システムの構築が可能になる。ISMS 認証取得数が世界一であることなど、セキュリティレベルの高さをセールスポイントにして、世界中の決済業務を一括して日本で請け負い、国際決済センタとなるといったことも考えられる。

- 製品・サービス以外では、システム構築などに関するトレーニングの実施をビジネス化することが考えられる。

Ⅳ章 今後の検討課題とまとめ

総務省の競争政策と通信事業者によるブロードバンドインフラ整備によって、日本は世界でもトップクラスのブロードバンドインフラを保有する国となった。今後、NTT による光ファイバの敷設が進み、2010 年に 3,000 万加入という目標が達成されたとして、そのハイスペックなインフラをどう活用するかが検討すべき課題の一つである。その点における政府の役割として考えられるのは、少子高齢化社会の安全・安心の確保や、地球温暖化防止に向けた対策など、国家として取り組むべき課題の解決に向けて NGN をどのように活用するかを検討することであろう。

また、NGN はセキュリティが確保されたネットワークであるが、NGN に接続する端末については、ユーザが自らセキュリティを確保する必要があることから、NGN に接続する端末のセキュリティが検討すべき課題である。日本において先行して導入が進んでいる IPv6 や、ハードウェアのセキュリティ評価スキーム Common Criteria、ハードウェアベースのセキュアなコンピューティング仕様を策定している TCG などとの整合をとりながら、NGN が備えているセキュリティ機能との相乗効果が発揮できるようなセキュリティ基準やセキュリティ評価手法を策定することも重要な課題である。

NGN を活用した産業の育成や国際競争力の向上という観点では、光ファイバによる高速アクセス回線やホームネットワーク、高性能・高機能な端末といった日本の先進的な分野・技術をいかにして産業育成や国際競争力の向上につなげるかが検討課題となる。先に述べたように、NGN では、NGN が提供する各種機能と端末の機能との役割分担が必要となることから、NGN において提供される具体的なサービスをイメージし、サービス提供においてネットワークと端末が相互に連携すること想定して、端末に必要なセキュリティ技術の開発を行うことが求められる。

情報セキュリティにおいては、既にある製品やソフトウェアに対して、あとからセキュリティ対策を施すよりも、設計段階からセキュリティを組み込む方が、トータルでのセキュリティ対策コストは少なくてすむというのが一般的な考え方である。

これは、ネットワークがインターネットであろうと NGN であろうと同じであり、NGN 向けの製品やサービスについても設計段階からセキュリティが組み込まれるようにするための設計ガイドラインを作成するとともに、作成したセキュリティガイドラインを普及させることが必要であろう。

以上、技術的な観点から NGN 今後の検討課題について考察したが、技術以外の観点からの検討が必要な課題もある。それらの課題のうち主なものを以下にまとめる。

1. 標準化の専門家の育成

日本における標準化への取り組みは、基本的に通信事業者や通信機器ベンダから ITU などの標準化機関に代表者を派遣することにより行われている。これまで、日本の提案や要求を多数の国際標準に反映させることに成功してきたという点で、非常に大きな貢献をしてきたことは確かであるが、ヨーロッパの国際標準に対する取り組みと比較すると、まだ及ばない点がある。

標準化において日本のプレゼンスを高めるためには、標準化会合という高度かつ多様な能力が求められる場において、欧米の代表と互角に渡り合える人材を育成する必要がある。また、欧米の代表者が長期に渡って標準化に携わるのに対し、日本では数年で任期を満了して新しい人が引き継ぐことが多いため、標準化会合において顔が利くという状態にまではなかなかならないようである。長期的なスパンで標準化に取り組むことができるようにするためには、標準化に人を派遣する企業において、標準化に対する貢献を成果として認める体制を整備するなどの施策が必要である。欧米の企業における標準化に関わる人材の育成や企業における評価の仕方の事例などをベースに、日本企業の取り組みを推進するための施策を検討することが必要ではないだろうか。

2. NGN を利用した多様なビジネスの創造を促進するための規制緩和への取り組み

NGN を利用したビジネスでは、様々な業種の企業が連携することが想定されるため、特定の業種における規制が適用された結果、ビジネス全体の立ち上げに影響を与えることが考えられる。

NGN では、従来のインターネットではエンドユーザが責任を持たなければならなかった認証や情報の機密性保護といった情報セキュリティ機能と、伝送データの品質を保証する QoS の機能がネットワークレベルで提供される。

このような NGN の各種機能を活用することにより、法律や医療といった、これまで公的な認可を受けたあるいは公的な資格を保有する主体のみがサービスを提供することができた分野や、様々な規制があるために新規参入が容易ではなかった分野において、多様なサービスを提供することが可能になると予想される。

NGN を活用した新たなサービスとして期待されているものの一つに遠隔医療がある。ネットワークを介して患者の診察を行うためには、プライバシー保護などのセキュリティ機能と、高精細な画像データを欠落なく伝送する QoS 機能が必須であるが、NGN ではこれらの機能が標準で提供されるため、遠隔医療は、NGN を利用して提供するのに適したアプリケーションであるといえる。

これまでは、制度や仕組みの不備により発生しうる間違いや不正な意図を持った人間による悪用といった問題は、法律や規制によって回避されてきたが、通信ネットワークを利用した遠隔医療を実現するためには、不正や悪用を防止するための技術的な仕組み(情報セキュリティ技術)が必要になる。

遠隔医療に必要となるセキュリティは、NGN あるいは NGN に接続する端末の機能により提供することが可能であり、そのようなセキュリティが確保されている場合には、法律や規制の適用から除外するといった運用が必要になる。

遠隔医療は一例であるが、NGN を利用したサービスの創造を促進するためには、法律や規制によって新しいサービスの創出が妨げられることがないように、臨機応変に規制緩和を行うことが重要であり、規制緩和を迅速に行うための省庁間の連携強化などについての検討を始めておくことが必要なのではないだろうか。

V 章　海外通信事業者・通信機器ベンダに対するインタビュー調査の詳細内容

本章では、米国及び欧州の通信事業者や通信機器ベンダにおいて NGN の標準化に関わっている方を対象として実施したインタビュー調査のまとめを記す。

インタビューに応じていただいた方によって専門としている領域が異なるため、回答者によって回答していただいた質問は異なる。参考として、回答していただいた方の所属企業の業種と現在参加しているまたは過去に参加していた標準作成組織とを記す。

1. 携帯電話事業者（ Former Vice Chair of 3GPP2 TSG-S Working Group 4 (Security))

1.1. NGN のセキュリティにおける重要な課題

現行の携帯電話と次世代の携帯電話とを比較すると、現行の携帯電話は常時ネットワークに接続しているという違いがある。接続先がキャリアの POP に限定されている限り問題はないが、既にインターネットに接続されるようになってきていることから、セキュリティレベルをインターネットにおける脅威に見合ったものとしなければならない。

1.2. 早期に解決すべきセキュリティ上の課題

特に 3GPP2 ネットワークにおいて重要な課題として、多くの製造業者(manufacturers)が既にあるセキュリティ対策を全て実装しているわけではないことと、キャリアが既に機能として存在するセキュリティ対策を有効にしていないことがある。(2G、3G においても全てのセキュリティ機能が実装されているわけではないようである。)しかし、これは鶏と卵の問題である。製造業者にとっては、キャリアがセキュリティ機能を有効にするまでは、セキュリティ機能を追加するインセンティブがない。

対照的に 3GPP は、セキュリティ機能を最初から実装することを義務付けている。つまり、セキュリティが適切に機能するだけでなく、通信事業者がセキュリティ機能を有効化しなければならない。
(しかし、実際には、3GPP のセキュリティ仕様のほとんどが無視されている。)

このように、セキュリティへのフォーカスが欠落していることが、NGN においても未だに大きな問題となっている。この領域は、セキュリティの実装を命令するなど、政府による貢献が可能な領域である。

1.3.　NGN によって解決されるセキュリティ上の課題

プラットフォームセキュリティが重要である。NGN はプラットフォーム自体をセキュアなものにしようとしている。インターネットでは、Windows を絶え間なくアップデートしなければならないが、プラットフォーム自体がセキュアであれば、理論的にはファイアウオールもアンチウイルスソフトウェアも必要ない。携帯電話には、そのような(プラットフォーム自体の)セキュリティが必要であり、セキュリティ機能を常に有効にしている必要がある。

また、ソフトウェアのアップグレードを自動化する必要があるが、携帯電話については、配送上の困難が伴うことから、現状では有効な方法がない。

1.4.　FMC のマイルストーン

NGN では、サービスを利用するに際して固定電話を使っているか携帯電話を使っているかによる相違はなくなるが、いくつかの問題がある。例えば、固定電話では帯域幅が問題となることはないが、携帯電話においては問題となる。

1.5. IMS が持つべきセキュリティ機能

3GPP2 においては、MMD が IMS に相当する。両者は基本的には、マルチメディア通信のための機能を提供する。

MMD は、IMS の特定のバージョンを取り込んでいる。IMS は、トラフィック制御セキュリティ、シグナリングセキュリティ、各種データストリーム(音声、ビデオ、文字)セキュリティといった、複数のセキュリティプロトコルを取り込んでいる。

1.6. 3GPP 及び 3GPP2 における標準化をリードしている組織

3GPP2 では Lucent, Qualcomm, Sprint, Cisco が最も active である。

1.7. 3GPP 及び 3GPP2 において議論されているセキュリティ上の課題

3GPP2 のセキュリティワークグループは、セキュリティ標準の実装に関して、多くの活動をしている。3GPP2 のセキュリティワークグループは常に、暗号や他のセキュリティ標準の実装が義務化されるであろうという仮定の元に活動を行っているが、他のワークグループはセキュリティガイドラインの実装をオプション扱いとしている。

そのため、多くのワークは、セキュリティガイドラインのうち、どれについて実装を義務化するかを明確化することに費やされている。

さらに、新しい仕様が作成された時に、セキュリティ WG は、セキュリティ要件／メカニズムの設定に関わるようにしている。つまり、セキュリティ WG は、他の WG が仕様を作成する際に、その仕様がセキュリティを考慮したものとなるように支援している。

セキュリティ WG は、TLS にも注意を向けているが、TLS のセキュリティプロファイルの作成には時間がかかるだろう。

最後に、Network Firewall Configuration and Control(NFCC)という試みがある。プラットフォームがセキュアであればファイアウオールは不要であるが、無線区間を経由した攻撃により端末(handset)が攻撃された場合には、そのような攻撃から端末を護るための手段が必要となる。

1.8 NGN の開発プログラム、NGN ベースのサービスのロードマップについて

NGN に向けた開発を強力に推進しているが、標準に準拠した開発を行っているのか、開発中のものが標準となるように活動しているのかについてはわからない。(過去には、両方の形態で行っている。)

1.9. ネットワークの中立性について

ネットワークへのオープンかつ平等なアクセスという点では、ネットワークの中立性には大いに賛成である。しかし、規制がかけられることについては、懐疑的である。なぜなら、規制は、インターネットを部分的に制限することによって、全てのユーザを平等にするようにみえるからである。

1.10. 携帯電話のアプリケーションの国による相違

オーストラリアにおける傾向はヨーロッパに似ている。米国では、ユーザもキャリアも携帯電話の一般的なアプリケーションに関心があるのに対し、オーストラリアでは携帯電話へのビデオ配信に対する関心が強い。

日本については、携帯電話及び携帯電話を使ってできることという点においては、その文化を受容する傾向が極度に高まるように見える。

2. セキュリティコンサルタント（IETF におけるセキュリティ分野のダイレクタ）

2.1. NGN のセキュリティにおける重要な課題は何か

ルーティングインフラストラクチャのセキュリティはトッププライオリティである。
もう一つは、SIP のセキュリティである。Early Media との接続がなされるまでは、SIP はセキュアであると考えられていた。Early Media は、SIP における呼が確立する前に、2 つの SIP エージェントが通信する機能である。Early Media のサポートは、PSTN との相互運用性を確保する上で重要であるが、多くの SIP デバイスにおいて、Early Media のセキュリティが確保されていない。

2.2. NGN において早期に解決すべきセキュリティ上の課題は何か

1 で述べた課題は早期に解決されなければならない。解決されなくともシステムは動作するが、悪用可能なセキュリティ上の欠点が残るだろう。
Skype についても同様のセキュリティ上の問題がある。

2.3. NGN が広く利用されるようになった時に解決されるセキュリティ上の課題は？

ITU に NGN とはどのようなネットワークであるかという質問したところ、全ての ITU 関係者が、新しいネットワークとインターネットを改良したものの両方であると回答した。
私は、NGN の要求条件によって、複数のある程度の大きさの新しい IP ベースネットワークがインストールされることになると信じている。
しかし、それが可能ではない場所(開発途上国など)においては、IP パケットをハンドルするためのあらゆる手段(音声トラフィックを優先するための QoS 制御など)が講じられるだろう
日本は資本が潤沢なので、インターネットとは別の NGN をインストールする可能性が高い。音声トラフィックのみが独立した IP ネットワークを流れる場合、現在 PSTN で行われている制御と同様の制御を行うことが可能である。
NGN によって生じる課題は、コストであると考えている。資本支出が必要なことから、理論的に NGN における接続にはより多くのコストが必要である。誰がそのコストを支払うのか？消費者か？キャリアか？政府か？何らかの財源が必要である。電話会社が一つしかない国では、費用を負担するのは消費者だろう。なぜならそれしか選択肢がないからである。

2.4 NGN セキュリティのロードマップは？

IETF は、NGN セキュリティのロードマップを持っていない。また、NGN に関する議論を行っていない。しかし、NGN は IP ベースのネットワークであるから、従来のインターネットを利用するにしろ、新しいネットワークを構築するにしろ、IETF がインターネットのために行ったことを NGN に適用することは可能である。

2.5. 暗号の危殆化はどのように扱われるのか

IETF はこの問題に対して強力に取り組んでいる。IETF のプロトコルはどれも、アルゴリズムの変化に対応することができる。
これまでにいくつかの課題があったが、ゴールは任意の暗号アルゴリズムが使用できるようにすることである。(相互運用性を推進するために、プラグアンドプレイで使用できるようにする。)

2.6. NGN に接続する端末に関する規制について

NGN が独立したネットワークであれば、接続ルールを規定することができる。そうでなければ、そのような規制を作ることはできない。

前にも述べたように、キャリアが NGN とは何であるか、NGN がどのように動作し、どのような事ができるのかを明確化するまでは、新しい IP ネットワークに投資することができない全ての国において、NGN を使った通信ができるようにするために、NGN と PSTN とをつなぐ大きなゲートウエイが必要である。これは、Skype から PSTN に接続するための方法と同様である。

どのような場合にも国は、全員が同じ方向を向いている(NGN に向かっている)ということを知るまでは、規制をつくることはできない。

2.8. DRM について

IETF は DRM に関する問題を扱っていない。

2.9. UDP トラフィックの増加が引き起こすと予想される問題について

DoS 攻撃は、主にルータにおいて発生する。通常の呼設定が行われるネットワークにおいては、単にビジーシグナルを発生させることで対応する。しかし、UDP では呼の設定は行わないので、UDP トラフィックを絞ることがトラフィック増加への唯一の対処方法である。

3. 通信機器ベンダ（ITU-T SG 13 Rapporteur for Security）

3.1. NGN のセキュリティにおける重要な課題

Identity 管理が最も重要である。

3.2. NGN において早期に解決すべきセキュリティ上の課題

認証、認可、Identity 管理 - これら全ての課題が並行して解決されるだろう。しかし、Identity 管理の問題が早期に解決されれば、他の二つの課題の解決に役立つだろう。

3.3. NGN が広く利用されるようになった時に解決されるセキュリティ上の課題

NGN は管理されたネットワークであるため、本質的に DoS 攻撃が発生してはならない。プライバシーは、解決されるであろうもう一つの課題である。問題は、今日のインターネットにおける脅威の多くが広く理解されていない点にある。人々は、インターネットを容易に過信しており、インターネットがどれほど安全でないかということを理解していない。例えば、ウイルスは相対的には大きな問題ではないが、添付ファイルを何も知らずにクリックする人によって、より大きな被害をもたらすようになる。

ウェブサイトスプーフィングは、人々に損害をもたらすもう一つの脅威である。これは、人々がクレデンシャルを信頼しすぎていることが理由である。

NGN は、インターネットと共存する、管理されたネットワークという形態をとり、インターネットは、ユーザがアクセス可能な管理されていないサービスを提供することになるだろう。

3.4 NGN セキュリティのロードマップ

ITU は、国連の機関であり、その目的の点で、産業界ではなく政府が役割を担う唯一の国際的な標準機関である。ISO も同様の組織であるが、通信の標準は扱っていない。

通信ネットワークにおけるセキュリティというトピックは、ITU において長期に渡って扱われてきたものであり、ISO との協力の基で証明書管理のような多くの標準が策定されてきた。

NGN に取り組んでいる組織が 3 つある。ATIS は北米の通信事業者を、ETSI は EU を代表しているのに対して、ITU は全ての通信事業者と各国の政府を代表している。

ETSI と ATIS は、物事が批准される ITU という場に対して貢献している。しかし、私の意見では、ETSI の方がよりアクティブに貢献している。IPTV 以外の分野では、ATIS は ETSI よりもアクティブではない。

3 年前に ITU が NGN フォーカスグループをスタートした時、セキュリティと QoS が NGN のキーコンポーネントであることが明確化された。特に NGN は、プライバシーを保護する一方で、自身に対する攻撃を回避する能力がなければならないことが明確化された。これは、3G パートナーシップがかつて行ったこととは異なっていた。

ITU によって採用された IMS は、"ベアラ通信路"における QoS とセキュリティを扱う事を突然やめてしまった。

IMS は、いくつかのシグナリングプロトコルと、呼の設定に必要な情報(電話番号や認可に関する情報)に関するセキュリティを扱っていたが、トラフィックフローの内側については何も行っていない。つまり、IMS は、セキュアなコネクションの確立は行うが、通信の内容に対するセキュリティはケアしない。

これは、ITU のセキュリティワーキンググループが NGN のセキュリティをどのように見るようになったかを決める大きな核となった。具体的には、IMS から引き継いだセキュリティホールを埋めること、つまり、IMS を固定ネットワークに適用する際に、不足しているセキュリティプロトコルを追加することである。

ITU は、シグナリングとベアラ通信路の分野だけでなく、identity 管理の分野において多くの課題を明確化した。identity management は現在、非常に大きな問題となっている。

ITU は、NGN セキュリティを検討していた間に多くの技術レポートを提供してきた。

今年の 1 月から検討を行っていたものであるが、NGN ワーキンググループの SG13 が、セキュリティ仕様に関する指示書をまとめた。当初は 5 人だったメンバが 30 人まで増加し、日本からの参加者も多い。

NGN セキュリティ仕様 Release 1 は、現在承認のプロセスにある。次期バージョンでは、認証に関する項目がより詳細に規定されることになるだろう。さらに、identity 管理がより詳細に検討され、その仕様が ITU の他の SG 及び ISO と協力して策定されることになるだろう。

3.5 暗号の危殆化はどのように扱われるのか

ITU は、暗号に対する取り組みを行っていない。NIST のような組織と ISO が国際的な取り組みを行っている。しかし、我々はそれらの組織によって提供される結果と協力するだろう。したがって、ITU としてのアルゴリズムは開発しないが、NGN においていずれの暗号が最もよく動作するかを提示する。

ハッシュ関数についても同様のプロセスが実施される。

3.6 NGN に接続する端末に関する規制について

規制に関する問題は、我々の SG における技術的な議論としては扱っていない。ITU の他の SG が規制に関する問題を扱っている。しかし、ネットワークに接続する全てのデバイスの特定と認証を強く推し進めようという動きが見られる。

規制当局は、しばしば我々に、NGN において彼らが望むこととそうでないことを伝えてくる。

3.7 モバイル IP への対応

NGN は、統合された IP ネットワークであり、無線機器に対しても有線機器に対しても同じであるべきということを意味する。

しかし、モバイル機器を扱う方法は数多くある。 3GPP は、モバイル IP を取り上げなかったが、3GPP2 は、モバイル IP に対してよりアクティブであるように見える(3GPP2 は IETF と共同で作業を行っている)。

究極的には、我々は、3GPP2 における作業の結果を取り込むことになるので、その意味では、我々はモバイル IP を取り込むということになる。

3.8 DRM について

DRM は ITU において言及されているが、仕様は策定されていない。しかし、IPTV に関する標準が策定されることによって、我々が DRM に関する標準を策定しなければならなくなるだろうと考えている。

トリプルプレイは NGN の使用における大きなテーマであり、それによって IPTV が NGN に組み込まれることになり、結果的に必要なセキュリティも取り込まれることになるだろう。

これら全ては互いに関連しながら進められる。DoS 攻撃は、コンテンツ配信キューに影響を与えることが予想されることから、結果的に IPTV と音声サービスにも影響を与えることになるだろう。

3.9 UDP トラフィックの増加が引き起こすと予想される問題について

我々はこの問題を検討しているが、まだ公開したものは何もない。この領域における我々の提案は、ネットワークに入ってくるいかなるデータストリームについても、適格であり、かつ認証され、認可されたものであることを確実なものとすることである。そのような前提の基で、ネットワークのデータストリームが予め決められた上限を超えないようにすることは、QoS の仕事ということになる。

DoS 攻撃を防止するために、スプーフィングは許可されず、トラフィック制限を超過したデバイスはネットワークから切り離されるだろう。

現在の PSTN でも、トラフィックが超過した場合には、電話をかけようとしてもビジートーンがかえってくるだけであり、これと同様のことが NGN でも起きる。つまり、トラフィックが超過した場合には、ユーザは、ビジートーンに相当する信号を受信することになる。

3.10 FMC について

ITU は FMC の検討を行っているが、現段階で公表された仕様はない。しかし、無線デバイスと有線デバイスの両方に対応する IMS を利用することにより、NGN アーキテクチャは当初から FMC に対応できるように設計されている(真に統合されたネットワークである)。

3.11 IMS のセキュリティについて

IMS は、セキュアに呼を確立することができる(シグナリングについてのみ)という意味で、よく定義されたセキュリティを有している。しかし、通信路上の音声やコンテンツに対して何かをするわけではない。

ITU における我々のゴールは、このギャップを埋めることである。つまり、セキュリティが、"ベアラ通信路" にも適用されるようにする(データの中身のセキュリティも確保する)ことである。

3.12 3GPP 及び 3GPP2 において議論されているセキュリティ上の課題

ITU は、3GPP 及び 3GPP2 と共同で作業を行っており、両方の組織とのリエゾンを設立している。ITU の NGN は、両方の組織からのアウトプットを取り込むよう試みる予定である。

3.13 NGN の標準策定に最も関わっている国

難しい質問だが、全ての国が関わっている。しかし、中国は NGN の会合に現時点で他のどの国よりも多くの人間を送り込んでいるように見える。

前にも述べたように、一般にヨーロッパ諸国は ETSI を通じて米国(ATIS を通じて)よりも NGN に対してアクティブに取り組んでいる。

しかし、通信事業者に関する標準は米国においては通常はオプションであるのに対し、ヨーロッパにおいては義務であることを認識しなければならない。

これによって、EU には、NGN を推進する上でのより大きなインセンティブが与えられることになる。

3.14 標準化に取り組む目的

中国の場合、国内に創業間もない企業が多数あり、それらは非常に速い成長を望んでいる。それらの企業は、標準に寄与することによって既に彼らが行っている仕事において一歩先んじることが出来、NGN に向けた開発競争のスタートにおいて、先頭に立つことができると考えているのではないかとみている。

彼らは NGN に対して非常に積極的であり、多くの若い才能ある人材が携わっている。

4. 通信機器事業者（Chairman of the 3GPP Workgroup for Security, 3GPP TSG SA WG3）

4.1 NGN のセキュリティにおける重要な課題

契約者(ユーザ)の認証が最も重要だろう。

4.2 NGN において早期に解決すべきセキュリティ上の課題

認証の問題が最初に解決されるべき問題である。

4.3 NGN が広く利用されるようになった時に解決される、あるいは解決すべきセキュリティ上の課題

セキュアなプラットフォームという NGN の本質的な設計に鑑みると、ユーザの観点からすれば、ウイルスやスパムといった問題はあってはならない。

4.4 暗号の危殆化への対応

IMS には、アルゴリズムが危殆化した場合に、代替アルゴリズムに置き換える機能がある。

4.5 NGN に接続する端末に関する規制について

NGN クライアントがソフトウェアベースである場合、携帯電話の場合のように全てのデバイスが SIM カードをもっていなければならないといった問題は生じない。したがって、ソフトウェアについては特定の規制は必要ではない。

注意すべき分野は、ほとんどの国が持っている、盗聴や監視といった機能である。3GPP は、最初からこれを考慮しているが、それぞれの国において、NGN を扱うためにこれらの機能を変更する必要があるかもしれない。

4.6 モバイル IP について

ローミングの手段としてモバイル IP の研究は行っているが、IMS には採用されていない。

4.7 DRM について

3GPP は、DRM は OMA において扱うべき領域であるという決定をした。IMS が DRM を扱うこともできたが、IMS はプラットフォーム以外の何者でもないことから、コンテンツを扱う必要はないという結論に達した。

4.8 FMC について

FMC に対する 3GPP の回答が IMS である。IMS は、当初から融合されたネットワークを想定して設計されており、有線ネットワークと無線ネットワークのハンドオフを扱う機能がある。

4.9 モバイルアプリケーションの固定網への適用について

固定網へ適用できるのは、ロケーションベースのサービスではないか。

4.10 IMS のセキュリティについて

IMS は、一つの重要な領域においてセキュリティが欠落している。ファイアウオールをどう扱うかである。広帯域ネットワークにはファイアウオールがあるが、モバイルネットワークにはファイアウオールがない。

したがって、ファイアウオールの導入が IMS に必要なセキュリティ強化策である。もう一つのセキュリティ問題は、モバイルネットワークにおける認証のためのスマートカード(SIM カード)の使用である。

IMS の中で、認証にスマートカードを使用することとアクセスとは独立しているが、NGN ではネットワーク内部において追加的な認証機能が必要になる。

いくつかの問題があることから、スマートカードは NGN の端末では使用されないであろう。しかし、ユーザのホームゲートウエイでは使用される可能性がある。

例えば、ユーザに対して、他の回線から IMS へアクセスすることを許可するためには、認証のためのもう一つのレイヤが必要になるだろう。

暗号も重要である。

モバイル環境では、暗号化に必要なオーバヘッドが無線区間の帯域を制限する可能性があることから、暗号の使用は限定される。したがって、IMS による暗号化も制限される。

しかし、広帯域区間ではこれらの制限がないため、より適切な暗号化が使用される。従って NGN は、IMS に対してより適切な暗号化機能を付加することになる。

IMS には、メッセージ保護のために暗号化以外の手段がある。それは、要約すれば、認証コードの形態をとる "鍵" システムである。

4.11 3GPP 及び 3GPP2 において議論されているセキュリティ上の課題

3GPP のセキュリティ WG は、3GPP のミニチュア版である。ほとんどのモバイルキャリア、ネットワーク／端末ベンダからの代表者により構成される 45 人のメンバ(WG としては平均的な人数)がいる。

他の WG との相違点は、スマートカードベンダからの参加者がいることである。彼らはスマートカードのセキュリティについて心配している。

セキュリティ WG は、IMS を含む 3GPP 由来の全ての新しいサービスについて、セキュリティの観点からの取り組みを行っている。

これは、セキュリティグループが必要に応じて相談を受けるという他の標準策定組織における取り組み方と大きく異なる点である。

しかし、いくつかの単体のセキュリティプロジェクトにも取り組んでおり、それらのプロジェクトから仕様の公開も行っている。例えば、現在、3G に続く次世代無線通信におけるセキュリティ連係についての検討を行っている。

3GPP の NGN に対するパースペクティブは、"ATIS と ETSI TISPAN が ITU とともに行っている何か"というものである。従って、我々は特に NGN に対して取り組んでいるというわけではない。しかし、それらの組織との情報交換は行っている。

3GPP の NGN に対する大きな貢献は、IMS である。IMS がアクセスに依存しないという理由により、ETSI が、NGN において IMS を使用する事を決定した。

IMS は GPRS(General Packet Radio Service) のトップでうまく動作しているが、セキュリティの観点から見ると、ブロードバンド環境においてはそうでもない。このような領域において、NGN のセキュリティに関する多くの活動、つまり、IMS のセキュリティギャップを埋めるための活動が行われている。

ETSI が IMS に対して行ったことが、異なるバージョンの IMS を生み出すことを心配する人もいることから、我々は、改変の結果が、単一のユニバーサルな IMS の策定という結果につながるよう多大な努力をしている。

4.12　NGN の開発プログラム、NGN ベースのサービスのロードマップについて

様々な標準策定組織に参加することによって、NGN に貢献している。当社の NGN に対するコミットメントのうちで最も具体的なものは、現在研究所においてテストが行われている IMS 製品の試行版を開発したことである。

4.13　標準化におけるヨーロッパの強み及び標準策定に関わる理由について

多くのキャリアが依然として、固定通信とモバイル通信とを一つの企業の中に有しており、独占的な地位にあるという点において、ヨーロッパはやや有利である。これによって、キャリアには、NGN に向かって進むというさらなるインセンティブが与えられた。なぜなら、キャリアは、NGN がもたらす融合によって真に利益を得ることができるからである。

NGN を使うことにより、ヨーロッパの PTT は、顧客に対して、より少ないコストで、より多くのサービスを提供することができるようになるだろう。

米国では、トリプルプレイが、キャリアを NGN へと向かわせる主な動機付けになっているように見える。

5. 通信機器事業者

5.1 NGN のセキュリティにおける重要な課題

NGN が扱う必要があるセキュリティ上の課題には、主にサービスレイヤに関わる IMS に関するセキュリティの課題以外に、アクセスセキュリティ、デバイスセキュリティ、アプリケーションセキュリティ、シングルサインオン、アイデンティティ管理といった、他のレイヤの課題がある。

ITU が言及する脅威への対処も必要である。ITU X.805 セキュリティモデルは、これら全てを扱っており、サブシステムである IMS には見られないガイダンスを提供している。

5.2 IMS が持つべきセキュリティ機能

サブシステムとしての IMS は非常に拡張性が高いが、全ての問題を解決するわけではない。3GPP はそのことを理解しており、それが IMS の継続的な進化の理由となっている。

しかし、IMS を使いたいと考えている non-3GPP グループも、IMS と彼らが必要とするものとのギャップを埋めることにより、IMS を完成させようとしている。

これには、既に IMS が有しているセキュリティも含まれるが、特に、独自の要求条件がある IPTV を提供したいと考えている有線キャリアの要件を満たすには十分ではない。

IMS 標準に取り組んでいる組織が多く存在するが、それぞれの組織が、一貫した標準にしようという努力をしている。

5.3 NGN の開発プログラム、NGN ベースのサービスのロードマップについて

10 人に NGN の定義を質問すれば、10 通りの回答が返ってくるという点で、NGN はいくらか流動的なコンセプトである。

多くの人は、あと 5 年間は NGN に取り組み続けるだろうと言うであろうし、それは恐らく正しい。ITU の NGN への取り組みは、フレームワーク以上のものである。

ITU の NGN が決定したことがそのまま実装されることはないだろう。むしろ、既にキャリアが構築したものが ITU の NGN に対応付けられる可能性が高い。

ITU が伝統的に標準の牽引役ではなかった事に注意が必要である。従って、ITU のアウトプットとして目にするものは、その性質上、完全に新しい標準というよりは、仕様をまとめたものである。

キャリアによる将来の NGN の実装は、ITU NGN フレームワークによってガイドされるが、それは正確な表現ではないだろう。

ITU NGN フレームワークに価値がないと言っているのではなく、ITU NGN フレームワークは、いかにして全ての部品をつなぎ合わせるかを示すものであり、ITU はセキュリティとリソース／受付制御の分野において、いくらか重要な仕事をしたということである。

NGN に関して、当社にとって重要な事は、NGN のうちのセッションベースのサービスが IMS によってドライブされるようになることである。

当社は、IMS 製品を過去 3～4 年にわたって開発しており、全ての主要な IMS 構成要素をカバーする完全な製品ラインを持っている。ほとんどの場合において、これらの製品は、特に IMS 用に開発されたものである。

いくつかのキャリアが既にこれらの IMS 製品のトライアルを開始していることから、我々の方針は正しいと考えている。(24 のトライアルが進行中である。)これらのトライアルのうちのいくつかは、実際に顧客が利用しているフィールドトライアルである。これらのトライアルに最も共通することは、IPTV と VoIP の両方を展開していることである。

IMS を見る際のもう一つの視点は、次世代のソフトスイッチという視点である。IMS は、ソフトスイッチの全ての機能を分解した後に標準化した結果できたものである。

従って、キャリアが次世代インフラストラクチャを構築するために何を購入すべきかを探す際には、NGN の次世代のセッション制御システムとして IMS が指定されていることから、IMS を採用したいと考えることが自然であろう。

5.4 標準化に取り組む理由

当社の観点では、ITU の NGN は、あらゆる点において、我々が既に行っていることと整合している。従って、我々は、ITU で批准された完全な NGN アーキテクチャに基づいて我々が行っていることについて重大な変更があるとは全く考えていない。

これが、我々が標準の策定活動 - ITU, ETSI, ATIS に関わる理由の一つである。

我々は、我々の製品と NGN のフレームワークとの間に、ギャップが存在しない事を確実なものとしたいと考えている。従って、重大な製品の変更はなく、正常な製品開発を継続するだけである。

5.5 標準化におけるヨーロッパの強みについて

ベンダの観点から言うと、IMS と NGN に対する関心という点において、ヨーロッパと米国は同じレベルにある。

しかし、出発点は異なっているようにみえる。ヨーロッパは、政府によるネットワークのアップグレード義務付けという理由から、PSTN の代替により大きくフォーカスしているのに対し、米国は、光ファイバによるオーバーレイネットワークが、PSTN を補完するというアプローチが主流のように見える。

一方、ヨーロッパのキャリアにみられるように、有線ネットワークと無線ネットワークの両方を保有するキャリアは、デュアルモードサービスに対する関心が非常に高い。

6. 通信事業者（Chair person of ETSI TISPAN WG7 (Security)）

6.1 NGN のセキュリティにおける重要な課題

認証と認可が重要である。なぜなら、任意のネットワークを経由して IMS サービスを利用する際に、これらが必要になるからである。認証については、あらゆるネットワークにおいて首尾一貫していることをユーザは望むだろう。

長期的には、IMS セキュリティ機能を 3GPP から利用したいと考えている。

しかし、短期的には我々は他のソリューションを模索している。それらのうちのいくつかは、危なっかしい(shaky)ものであった。

これが、我々の全ての新しい標準に対して脅威分析を行う理由である。脅威分析によって、我々が、セキュアでないものを標準化しているのではないことを確認する。

間もなく登場する IPTV についても脅威分析を行う予定である。IPTV には多くの異なるセキュリティ上の課題がある。

6.2 NGN において早期に解決すべきセキュリティ上の課題

SPIT と SPAM は憂慮すべき二つの脅威である。我々は、これらの問題を TISPAN において検討している。

モバイル端末を使用するときは常に、ウイルスなどの外部からやってくる脅威に注意する必要がある。モバイル端末の OS やソフトウェアには、ウイルスに対する脆弱性がある。

6.2 NGN セキュリティのロードマップ

現在、NGN リリース 2.0 に取り組んでいる。これは、3GPP の IMS リリース 7 と同期したものになっている。

NGN リリース 1 には、セキュリティ要件のセット、セキュリティアーキテクチャ、脅威分析が含まれていた。

リリース 2.0 は、それを拡張したものであり、メディアセキュリティ(現在 IPTV に取り組んでいる)や意図しない通信といった新しい領域についても考慮したものとなる予定である。

3GPP においていくつかの問題は解決されたが、3GPP には固定ネットワークに対する視点が欠けているため、我々のゴールは、固定ネットワークの問題を解決することである。

我々の WG は、EU の代わりに、NGN のスコープ外のセキュリティ上の課題にも取り組んでいる。さらに、ベンダが新しい製品に適用するための共通の標準を持つことが出来るように、製品に対する基準も作成している。

NGN リリース 3 については、まだ検討していない。その主な理由は、ETSI TISPAN と 3GPP の融合に関して、議論があることにある。議論の結果如何では、NGN の将来図が劇的に変わることになるため、これ以上先を見通すことには意味がない。

6.4 暗号の危殆化対策

暗号の標準は、ETSI の他のグループが扱っている。3GPP においてもいくつかの暗号に関する作業が行われた。従って、新しいアルゴリズムが必要な時は、他のグループに問い合わせる。

暗号が破られるのはほとんどの場合、鍵長が十分ではないことに起因するのではないかと考えている。暗号に取り組んでいるグループは、暗号の危殆化を問題として認識している。

6.5 NGN に接続する端末に関する規制について

長期的には、どんなデバイスでも NGN に接続できるようにすることがゴールである。しかし、そのようなゴールに到達するためには、デバイスを接続可能にするためになんらかの SIM カードを使わなければならない。

数週間前に、ETSI は、NGN において USB 版の SIM を使う事を決定した。これによって、NGN への接続を可能にするデバイスとして、USB SIM が採用される可能性が大きく増加するだろう。

6.6 モバイル IP について

これは IETF のスコープなので、変更を依頼する必要がない限り、我々はあまり関与しない。

6.7 DRM について

IPTV における大きな課題の一つであり、リリース 2.0 でも言及している。現時点では、IPTV の要求条件に取り組んでいるところであり、その後に DRM に対する寄書に目を通すことになるだろう。

6.8 UDP トラフィックの増加が引き起こすと予想される問題について

これは大きな問題であり、我々も認識している。SIP を使用する際の本質的な弱点である。しかし、我々の WG では、DoS 攻撃に対する保護についての議論は開始されていない。

6.9 FMC について

FMC に関する標準の作成に関心は持っている。この領域における最も大きな脅威は、MD5 により生成された HTTP ダイジェストを使用するレガシー端末である。この問題は解決しなければならないと考えている。

6.10 IMS のセキュリティ機能

他のレイヤに、必要なセキュリティを追加することにより、IMS を固定ネットワークに適用できるように拡張することに取り組んでいる。

IMS は、モバイルデバイスに焦点をあてて設計されているが、モバイルデバイスのセキュリティは、SIM カードという物理的なデバイスに依存しているため、固定端末よりもセキュリティ的に弱い。

一方、固定ネットワークでは、特に無線 LAN の普及に伴い、より多くのセキュリティ要件が求められる。

しかし、3GPP が、UICC スマートカードによる USIM を使うことは、健全なアプローチである。(例えば、DoS 攻撃を回避することができる。)

SIP が本来的に持っている脆弱性を我々が解決する必要があるということである。

6.11 3GPP 及び 3GPP2 において、標準化をリードしてるのは？

我々は、3GPP のセキュリティグループと非常にうまく協力しており、例えば、認証メカニズムとの共存など、いくつかの検討課題を提案しているところである。メディアセキュリティについても 3GPP と話をする予定である。NAT ファイアウオール越えに対するソリューションが必要な時にも 3GPP と話をした。3GPP は、主にヨーロッパのモバイルキャリアとベンダによってリードされている。

6.12 NGN の開発プログラム、NGN ベースのサービスのロードマップについて

当社の長期戦略についてはわからないが、我々は IMS のテストベッドを持っている。また、当社は、IMS の interworking に関するいくつかのグローバルなイニシアティブに関わっていた。

6.13 NGN に必要な技術の獲得方法

ヨーロッパでは、伝統的にキャリアがベンダに対して大きな影響力を持っている。我々が必要とするものをベンダに伝え、ベンダがそれを実現するものを開発する。しかし、競争が激しくなるにしたがって、そのような状況も変化しつつある。

6.14 ヨーロッパの優位性について

ヨーロッパにおける環境が、一般的により標準ベースのものであるという理由により、ヨーロッパは NGN 標準において強みがある。

米国では、プロプライエタリなソリューションが開発されると、競争優位を確保するために、できるだけ早期に市場に投入される。

ヨーロッパでは、キャリアとベンダが ETSI に深く関わっており、タイミングを気にする必要がないので、ETSI の標準によく従っている。

6.15 標準化に取り組む目的

ベンダは、NGN 用の機器を売ることが出来るので、IMS と NGN を推進している。
キャリアも、コスト削減など、all IP ネットワークに移行する大きな動機がある。

BT と FT は、NGN リリース 1 の標準化を最も強力に推進したキャリアである。

しかし、ベンダの統合(Alcatel と Lucent の統合など)とそれによるキャリアとの力関係の変化により、この状況も変化しつつある。

我々は、ヨーロッパの他のキャリアにおいても同様に、大きな活動を目にしている。

7. 通信事業者（Member 3GPP TSG SA WG3 and TISPAN WG7）

7.1 NGN のセキュリティにおける重要な課題

現在インターネットでは問題となっていないが、IP ベースの NGN では解決することが求められる多くの課題に取り組んできた。合法的な傍受や補完的なサービスがその例である。

7.2 NGN において早期に解決すべきセキュリティ上の課題

恐らく、モバイル通信事業者と固定通信事業者との間で行われている重要な議論は、NGN がクローズドなネットワークであるべきか、オープンなネットワークであるべきかに関するものである。

モバイル通信事業者は、サービスは限定されるが、より強力なセキュリティとコントロールとを提供する"囲われた庭" でサービスを提供することを好む。

固定通信事業者は、一般的に音声、ビデオ、他の特別なサービスについては、サービスと品質の問題が解決可能なことから、モバイル通信事業者と同じ考えを持っているが、強力なセキュリティとコントロールが施されたサービスと同様に、一般的なインターネットアクセスについてもゲートウエイ経由で提供しなければならないことを認識している。その場合、ネットワークの運用者がセキュリティサービス(anti-spam 等)を提供するとしても、リスクはほとんどの場合ユーザ側にある。

クローズドな NGN は､回線交換装置の代わりに強力にコントロールされたルータが使われるという点を除いては、現在の PSTN と同様に運営されるだろう。

この問題を考える際の他の視点としては、モバイル通信事業者がインターネットアクセスを提供する場合がある。モバイル通信事業者は、エンドユーザがインターネットサービスにアクセスする際に、まず GPRS ネットワークに接続するというシナリオを用いる。この場合、GPRS ネットワークからインターネットサービスに接続し、インターネットサービスから GPRS を経由してユーザに戻ってくる。これにより完全にコントロールされた環境が提供される。

7.3 NGN が広く利用されるようになった時に解決される、あるいは解決すべきセキュリティ上の課題

レガシー端末がサポートされなくなるまでには、長い年数がかかるだろう。移行が完了するまでの間、レガシー端末は、変換を行う何らかのゲートウエイによってサポートされる

移行が完了した後には、信頼性を確立するために、SIM カードのような、なんらかの物理的なデバイスを端末に組み込む必要がある。

一般的なコンピュータの場合、プラグによる接続が可能な SIM タイプのチップを USB ポートに接続することになるだろう。(彼らはこれを AKA(Authentication and Key Agreement Protocol) セッションと呼んでいる。)

7.4 モバイル IP への対応について

3GPP は､LTE イニシアティブの一部として､モバイル IP を利用することを考えている。(LTE：Long Term Evolution)

7.5 DRM への対応について

DRM でコンテンツを保護する事はできるが、ネットワークを保護することはできないということを事業者は知っている。DRM には、ハッカーがデータストリームを妨害／改変したり、送信元を偽ったりする事を止める機能はない。また、ユーザのアイデンティティを保護する機能もない。

さらに、クレデンシャルがひとたび破壊されると、コンテンツを復元することが出来ないという問題が

ある。ユーザのハードディスクがクラッシュすれば、コンテンツは失われ、ユーザはコンテンツを再度購入しなければならない。従って、DRM は部分的なソリューションでしかない。

7.6 FMC について

当社は既に、UMA 標準に基づいた FMC サービスを提供している。このサービスは、GSM プロトコルをブロードバンド IP 接続の上でトンネリングさせたものである。

しかし、IMS と SIP を使ってこれを実現するためには、多くの努力が必要であろう。SIP には、ご存知のとおり、大きなセキュリティ上の欠陥がある。SIP は、シグナリングを行う権利をエンドユーザに渡しているが、これが脆弱性につながる。現在の固定ネットワークでは、シグナリングはローカル交換局で行われるので、SIP よりも高いセキュリティが確保されている。

当社の FMC サービスでは、シグナリングは固定ネットワークに残されている一方、ホームアクセスゲートウエイは完全に passive である。

前述のとおり、"囲まれた庭" というアプローチは、ユーザにできることをコントロールするので、インターネットに関わる多くの問題に配慮したものとなっている。これは理論的にはよいが、モバイル端末を完全にコントロールすることは難しい。特に、モバイル端末が WiFi のような他のデータアクセスメカニズムを持っている場合には。

ネットワーク運用者は、セキュリティ上の問題が発生した場合に、ユーザに対するサービスを停止することが出来る一方、ユーザの電話機の他の機能(MP3 やデジタルカメラ)が使えなくならないよう注意しなければならない。

7.7 モバイルアプリケーションの固定網への適用

FMC では理論的には、全てのモバイルネットワークアプリケーションは、固定ネットワークから透過的にアクセス可能である。

例えば SMS(Short Message Service)は、モバイルネットワークから固定ネットワークへ、あるいはその逆の方向へと、境界を超えて提供できなければならない。

しかし、ネットワーク運用者は、store and forward 機能が適切に動作していることを保証する必要がある。さもなければ、ユーザは重複課金されることになる。

7.8 IMS のセキュリティについて

IMS は、多くの仮定の上に構築されている。仮定の一つが、セキュリティは、ネットワークのさらに低いレイヤにおいて扱われるというものである。

我々は、ワイヤレスホットスポットや FMC サービスといった当社が保有している様々なタイプのネットワークにおいて IMS を動作させる自由とともに、独立したアクセスを必要としているので、これについては問題はない。つまり、IMS をアクセスとは独立したものとすることにより、ワイヤレスホットスポットや FMC サービスといった当社が保有している 様々なタイプのネットワークにおいて IMS を動作させることができるようになる。

アクセスの独立性とは、以下をさしている。

1) IMS が使用されているネットワークアクセス技術の種類をケアしない
2) IMS ネットワークが異なる通信事業者にまたがって動作する事が可能
　有線通信事業者が提供するサービスを無線ネットワークへ拡張したり、その逆が行えるようにするため。

2 番目については、信頼メカニズムが実装されていることが必要となる。

7.9　3GPP の標準策定をリードしている組織

3GPP は、1999 年頃にスタートした。当初は、ヨーロッパのモバイル通信事業者だけであったが、その後、北米やアジアの事業者にも門戸を開けた。

しかし、ほとんどの部分で主要な貢献をしているのは、ヨーロッパの事業者である。日本は、三菱電機がいくつかのアルゴリズムで貢献している。

IMS に関して、本当にアクティブなのは、新しいアーキテクチャの展開によって多くを得る製造業者である。

7.10　3GPP におけるセキュリティ上の課題

現在の主要な取り組み課題は認証であり、固定、ワイヤレス、ケーブルといった様々なタイプのネットワークにおいて動作することを保証することである。我々は、TISPAN や他の標準策定組織と完全に合意できるよう努力している。

他に議論されている領域は、3G ネットワークにおける 2G 端末の扱いである。レガシー端末は、セキュリティや新しいサービスを展開する時に考慮が必要となる。例えば、2G の暗号化は 3G に比較して非常に弱い。

■　3GPP のワークプラン

- アクセスセキュリティの強化

これは、我々が取り組んでいる以下の二つの領域をカバーする。

a) デバイスと最初のノード(first node)との間のアクセスセキュリティ
b) IPSec のトンネリングにより全てのネットワークを接続する、コアネットワークセキュリティ
その下のトランスポート層におけるベアラ通信のセキュリティを確保するという問題もある。
例えば、IMS over GPRS はセキュアであるが、IMS over WLAN はセキュアではない。

- Liberty Alliance

ほとんどのデバイスは、HSS(Home subscriber service) のようなプロトコルや、SIM カード、SIM チップあるいは SIM と同等の機能を持つソフトウェアによってセキュリティが確保される。

Liberty Alliance のアイディアの背景にあるのは、電子商取引のために、第 3 者がそれらのクレデンシャルにアクセスできるようにすることである。GAA(generic authentication architecture：GBA としても知られる) は、これを標準 API を用いて達成した。

3GPP は、これらのプロトコルを使って Liberty Alliance との相互運用性を確保するための技術レポートを発行した。

- SS7 TCAP セキュリティゲートウエイ

SS7 は、当初は、メッセージの送信元と種別が正当なものであると考えることができる完全に信頼された環境であった。

しかし、3G の到来と、オープンなメッセージゲートウエイをサービスプロバイダが利用できるようになったことによって、メッセージのオーバーロードに関わる問題が生じていた。

例えば、イギリスにおいて、クリスマスの時期になると、メッセージトラフィックの急激な増加が発生する。

TCAP は、これらのゲートウエイに認証機能を追加し、メッセージゲートウエイへのアクセスを制限するための方法である。
当社はこれを使用するかどうかをまだ決めていないが、モバイルネットワークと固定ネットワークの双方において、莫大な量のテキストメッセージトラフィックが発生していることから、検討は行っている。

■ 携帯電話におけるインターネットベースの認証メカニズムについて：

これを達成するために、Generic Bootstrapping Architecture：GBA をサポートしている。
インターネットにおける認証と携帯電話における認証の最も大きな相違の一つは、インターネットにおける通信は PC をベースに行われるため、セッションに必要になったときに利用できるように PC にクレデンシャルを保存する事が容易なことである。
また、インターネットの場合、接続がブロードバンドであるため、かなり複雑なアルゴリズムを使って認証を行うことが可能である。
一方、携帯電話の場合、PC ほど多くの帯域やストレージがないため、デバイスと接続に責任を持つために、認証は単純なものとならざるを得ない。
また、モバイル端末は移動し続けるものであるから、認証もモバイルに対応したものでなければならない。

7.11 NGN の開発プログラム、NGN ベースのサービスのロードマップについて

当社の NGN に対するビジョンは、完全に TISPAN の標準に従ったものである。完全にネットワークの内側に配置され、外部には接続しない(does not extend out)、emulated PSTN (H.248 が動作している)が付帯する MPLS ベースのコアネットワークを当社は保有している。また、IMS ベースのシステムも保有している。これらの装置を使用して、多くの法人顧客に対して、音声サービスやデータサービスを提供している。ISP にサービスを提供する際にもこれらの装置を使用している。

7.12 NGN を利用して今後提供を予定しているサービス

将来的なゴールは、既に我々が提供しているサービスを、さらに広い範囲で利用できるようにすることである。
例えば、当社の FMC サービスは、イギリス国内のみのサービスであるが、いったん標準が策定されれば、ユーザはグローバルにサービスを利用できるようになる。
もう一つのサービスは、ユーザに放送サービスを提供できるようにするものである。これにより、少数のユーザグループが、IPTV を使って画像メッセージの送受信を行うことが可能になる。
将来に向けてのもう一つのシナリオは、携帯電話から家庭のテレビへ、あるいはその逆へと、シームレスにコンテンツの視聴を可能とするものである。

7.14 NGN の技術開発について

一般的な手法は、当社とベンダとでコンソーシアムを立ち上げ、共同でソリューションを開発するというものである。その際の当社とベンダとの分担割合は、50:50 である。

7.15 ネットワークの中立性について

当社は、料金を支払った人に対して、あるいは、緊急事態が発生した場合に優先してサービスを提供する技術を持っている。しかし、ネットワークの中立性に関する動きはない。

7.16 通信事業者に適用される法律や規制への対応について

全ての通信記録を保存する機能は持っており、令状が出された場合に使用される。一方で、ユーザのアイデンティティを保護する事を義務付けるデータ保護法に従う必要もある。

7.17 PSTN と NGN でのログ保存に関する相違

大きな違いがあるのは、放送サービスとマルチキャストサービスの場合である。ユーザが、複数の人と通信を行う場合には、セッションの記録やログの作成は、より難しいものとなる。
また、令状の対象となる人物が通信を停止した場合には、記録作業は停止しなければならない。

7.18 日米欧における携帯アプリケーションの嗜好の相違

日本は、ヨーロッパよりも前からより限定された WAP を使用した適切なインターネット閲覧方法に関心を持っていたように見える。つまり、日本では、携帯電話を使ってインターネットを閲覧する際に、PC のような高度な機能を使うが、ヨーロッパでは、それに比べてかなり限定された機能しかない WAP ブラウザを使って閲覧するケースが多い。

7.19 ヨーロッパと米国の取り組み方の相違

ヨーロッパが先んじているのは、主に、3GPP TISPAN といった標準策定組織に関わっている人の数が多いことによる。人数が多ければ、より多くの事をより早く行うことができる。

7.20 標準化に取り組む目的

ヨーロッパが標準の策定に重点的に取り組んでいる理由は、これまでにヨーロッパがアメリカよりも非常に長期に渡って 3G ネットワークに取り組んできたことにある。ヨーロッパ各国の 3G ネットワークへの取り組みが NGN に続く道を開いたのである。

7.21 標準化への取り組みに力を入れている国

中国は、固定ネットワークの分野において彼らの作成した標準が許容されるように非常に積極的に活動しているように見える。

8. ケーブルテレビ事業者（Member 3GPP TSG SA WG3）

8.1 暗号の危殆化への対応

3GPP と PacketCable（ケーブルテレビ事業者が設立した非営利の研究開発コンソーシアム。北米のケーブル事業者に対して新しいケーブル通信技術の導入支援を行う)は、これらの問題に対して、より脆弱性の低い鍵付きハッシュ関数(Keyed hash function)を使っている。PacketCable では、AES と 3DES を使用する事を要求している。

8.2 モバイル IP への対応

モバイルについては、現在のところあまり関わっていないが、昨年、Sprint と米国の 3 つの大手ケーブル事業者(Time Warner Cable, Cox Communications and Advance/Newhouse Communications)とが融合された無線アクセスと有線アクセス及びコンテンツを提供するジョイントベンチャーを立ち上げるというアナウンスがあった。

このベンチャーには、Sprint から 1 億ドル、3 つのケーブル事業者から 1 億ドルが拠出される予定であるが、現段階では、漠然としたパートナーシップである。

多くのケーブル事業者が無線通信用の帯域を保有していることはよく知られている。従って、ケーブル業界がモバイルやモバイル IP の分野で何かをしようとしていることは容易に推測できる。

8.3 DRM への対応について

IMS はサービスについては関知しない。従って、メディアセキュリティは他のレイヤに追加されるべきものである。

モバイル業界が OMA (Open Mobile Alliance。我々もウオッチしている)を通じてアプリケーションレイヤに取り組んでいるのと同様にケーブル業界も独自のアプリケーション仕様を作成する予定である。

CableLabs では、OpenCable と呼ばれるグループが、コンテンツ保護と DRM に取り組んでいる。

しかし、メディアセキュリティは難しい領域である。IETF が継続してメディアセキュリティに取り組んでおり、12 か 13 の異なるソリューションがある。

標準が策定されるまでは、メディアセキュリティ技術の開発や導入を推進するかどうかは、ベンダごとに異なるのではないだろうか。

8.4 UDP トラフィックの増加が引き起こすと予想される問題について

DoS 攻撃は、ケーブルネットワークにおいても問題となっている。IMS には、DoS 攻撃に対するソリューションがあり、我々もそれに従う予定である。

しかし、IP データサービスに関するケーブル業界の標準である DOCSIS でも物理層におけるトラフィックと QoS を扱っており、長年にわたりそのようにしてきた。

我々は、PacketCable security architecture の中で、DoS を脅威の一つとしてリストしている。

8.5 FMC について

IMS は、FMC へ至る経路として意図されている。3GPP には実際に、VCC(voice call continuity）と呼ばれる FMC のスタディグループがあり、我々も寄与している。私の理解では、彼らは、解を見出すのに苦労している。問題は、呼がモバイルネットワークと固定ネットワークのどちらのネットワークを基点にしたものかに関するものである。

契約者が、モバイル事業者と固定事業者のどちらに属するのかという問題もある。

8.6 IMS のセキュリティ

IMS は、モバイル環境を想定して設計されているので、我々は、IMS をケーブルネットワークの要件に合うように改訂する作業を行ってきた。例えば、ケーブルモデムとクライアントソフトウェアは、IMS がサポートしない特定のクレデンシャルを扱う必要がある。

一般的には、我々の取り組みは、追加的な認証メカニズムとシグナリング機能の強化にフォーカスしている。しかし、メディアセキュリティのような、我々が要求してきたいくつかの特定のセキュリティ機能もある。TISPAN は、メディアセキュリティに関する作業項目を開始しており、我々はそれをサポートすることを表明している。

CableLabs は、ETSI TISPAN には所属していないが、3GPP のメンバであることから、ミーティングの傍聴者として招待されている。(3GPP と ETSI TISPAN とは非常に密接に作業を行っており、近い将来に一つの組織になるのではないかという噂まである。)

IMS に対する完全なセキュリティ分析はまだ行っていないが、前述したようにセキュリティの観点からの追加要件を提示している。

基本的には、次期バージョンの IMS に我々の提案する機能強化が取り込まれることを望んでおり、それによって将来、"単一の IMS" を得ることができる。

我々は、全ての通信事業者(モバイル、固定、ケーブル)が IMS ベースのアーキテクチャを採用した時に期待される究極の相互運用性を確保することを計画している。

3GPP は、IMS が無線通信だけを目的としたものではないことを十分に理解しているようにみえる。例えば、3GPP は最近、IMS の GPRS 部分を仕様の付録に移動した。

CableLabs は、3GPP、TISPAN と共同で、"他の業界の要求を国際標準に反映するためには"(how to get other industry requirements into international standards)というワークショップを開催した。
そのワークショップには、3GPP2 と WiMax フォーラムからの代表者も参加した。

前述したように、我々は、IMS 文書(delta 仕様として知られている)に対する変更要求を提出することによって 3GPP の IMS セキュリティに対する取り組みに恒常的に貢献している。delta 仕様は、採用されるまではそのままの状態でおかれている。

その作業とは別に、我々は最近、ケーブル業界独自の仕様を公開するとともに、PacketCable security architecture と IMS との相違点を記述した技術レポートを出版した。そのレポートにおいて我々は、多くのセキュリティ上の脅威を概説しているが、それらの脅威の多くは、IMS を使用している他の多くの組織にも関連するものである。

ケーブルテレビ業界は、次世代プラットフォームとして IMS を使う事を決定した。その理由は、通信事業者が NGN のプラットフォームとして選択したのと同様であり、ベンダのスケールによる経済性や、ソリューションの効果といったものである。また、他の通信手段(ワイヤレス、固定)とのコンバージェンスによる利益もある。

CableLabs は、ITU の IPCablecom プロジェクトにも参加している。これは、IP を使用したケーブルテレビネットワーク上でのインタラクティブサービス(主に音声とビデオ)に関する国際標準を作成するプロジェクトである。

しかし NGN に関しては、ITU が他のどの組織よりも影響力のある組織である。

CableLabs は、世界中のあらゆる業界の企業と議論を行い、作業をしてきた。興味深い事に、ITU SG9 の会合で日本の通信事業者と話をしたところ、彼らは、次世代アーキテクチャに非常に興味を示していた。

8.7 3GPP 及び 3GPP2 における標準化をリードしている組織

ヨーロッパの GSM モバイル事業者が 3GPP を創設したことから、IMS の開発を行っている現在でも彼らがリードしているといえる。

8.8 NGN の開発プログラム、NGN ベースのサービスのロードマップについて

IMS ベースではない PacketCable 1.0 は既に公開されており、ケーブル事業者が音声サービスを提供するのに使用されている。

つい最近公開された PacketCable 2.0 は、IMS リリース 6 をベースとしている。

2007 年から 2008 年にかけてケーブル事業者が PacketCable を実装するだろうと予想している。そうなれば、理論的には、ケーブル事業者は、IMS リリース 6 をベースとしたサービスを提供する全ての事業者と調和することになる。

8.9 通信事業者に適用される法律や規制への対応について

PacketCable には、通信記録の保存に関する規定がある。しかし、これに関する要件は国によって大きく異なるというのが私の印象である。

9. 携帯電話事業者（member of ATIS NGN Focus Group）

9.1 NGN のセキュリティにおける重要な課題

NGN における課題は、ほとんどインターネットにおける課題と同じである。まず、ユーザの認証及び認可に関する有効な手段がなければならない。ETSI TISPAN において、これらの問題に関して多くの議論が行われてきたが、私の知るところでは、まだ決議がなされていないと聞いている。

9.2 NGN が広く利用されるようになった時に解決される、あるいは解決すべきセキュリティ上の課題

NGN においても、インターネットにおいて脅威を避けるために使われる技術と同様の技術が使われる。例えば、インターネットにおいて DoS 攻撃を回避するためにトラフィック制御が使われるが、同様の技術が NGN においても使われるだろう。

NGN においてもセキュリティホールの修正が必要である。NGN がオープンになればなるほど、脆弱性は増す。何がオープンになっているのかについて注意しなければならない。

NGN は、多くのレイヤにおいてセキュリティを具備しているが、キャリアによっては、これらのレイヤのセキュリティは他のプロトコルによって既に確保されているかもしれない。

例えば、日本が大きく注力している IPv6 には既に NGN セキュリティをカバーするいくつかのレイヤがある。

9.3 NGN の開発プログラム、NGN ベースのサービスのロードマップについて

当社は、ATIS のメンバであり、実際に寄書を提出している。我々はまだ初期の検討段階にあるので、NGN サービスのロードマップは持っていない。

我々の研究所は、異なるストーリーを持っている。(我々の研究所で開発された技術が、そのまま製品に実装されるわけではない。)研究所は常に新しい実験的な技術を持っており、いくつかの IMS システムの検討が行われている。

9.4 NGN に必要な技術の獲得方法

我々が提供するサービスのうちのいくつかは、内部で開発するが、ほとんどのパートについては、社外の業者を探すことになる。

9.5 NGN における通信事業者の収益源

利益は、NGN を実装することによって提供されるユニークなサービスから生まれる。利益を生み出すためには、拡張性のある新しいサービスを提供することも必要である。よい例は、携帯電話会社である。彼らは、周波数帯域(spectrum)を購入し、その帯域を使ってサービスを提供することにより、利益を生み出している。

9.6 ネットワークの中立性について

ネットワークの中立性が課題であることは誰もが認識しているが、現時点ではいかなる決定もなされていない。

9.7 通信事業者に適用される法律や規制への対応について

他のキャリアと同様に法律に従っている。

9.8 PSTN と NGN でログ保存に違いはあるか

サービス(電話の呼)が同じであるので、両者に違いはない。NGN において異なるサービスを提供した場合、法律に従う必要はないと主張することは可能であるが、サービスが同じである以上、同一の規制が適用される。従って、我々は NGN においても法律に従う。

9.9 標準化への取り組みに力を入れている国、ヨーロッパと米国の取り組み方の相違

一つの国や地域が他の国や地域に比べて、NGN により多くの力を注いでいるとは考えていない。
当社を含め、どの事業者も 3GPP の IMS 標準を使用することに関心を持っている。TISPAN の NGN リリース 1 は、IMS の一つのバージョンをベースにしている。従って、IMS に対する関心は真に国際的なものである。

グローバルに見れば、NGN のアーキテクチャには、細部が異なるバージョンが多く存在することになるだろう。

言い換えれば、全ての国が全ての NGN アーキテクチャを使用するわけではない。(NGN アーキテクチャのうちの必要な部分だけを使用する国もある。)これは、IMS アーキテクチャの単一の実装が存在しないのと同様である。

例えば、日本は、IPv6 に大きく注力しているので、IPv6 が提供する機能については、NGN が提供する機能を実装する必要はない。

NGN のサービスも国によって異なるだろう。

10. 通信事業者研究所(Member ATIS NGN Focus Group)

10.1 NGN のセキュリティにおける重要な課題

インターネットにおける問題の多くは、NGN においても問題となる。これは、通信事業者である我々にとっても重大な関心事である。例えば、IP ベースの通信におけるキーコンポーネントの一つである SIP には、解決すべき多くのセキュリティホールがある。SIP は、これまでセキュリティを念頭において設計されたことはなかったため、後付けでセキュリティを追加しなければならない。SIP には認証メカニズムが組み込まれているが、それでは十分ではない。SIP-S は、SIP セキュリティを解決しようというプロジェクトである。End to end でのシグナリングの暗号化を要求しているが、まだそれを実現するメカニズムはない。

IMS は、通信路をセキュアにするために TLS を使う事を規定しているが、これも十分ではない。エンドユーザは、セッション制御の境界までの間で暗号化のための TLS が設定されたことを確認できるが、暗号化に関しては何の保証もない。つまり、エンドユーザは、その通信の設定に関わる自分の通信事業者を信頼することはできるが、他の通信事業者を信頼することはできない。従って、SIP による通信路設定が行われる場合、電話をかけようとしている相手に本当に電話をかけているということを確認する手段はないということである。

また、何らかの証明書か鍵を使わない限り、通信内容の機密性を保証する手段もない。IETF はこの問題に取り組んでいるが、まだ解決には至っていない。

10.2 NGN が広く利用されるようになった時に解決される、あるいは解決すべきセキュリティ上の課題

IP に関する伝統的な課題は、NGN にもあてはまる。DoS は、最も深刻な問題であるが、ハッカーが攻撃すべき IP アドレスを知っていれば、IMS を容易に機能不全に陥らせることができる。IMS は自身を保護することができないので、ネットワークをそのような攻撃から護るのは、ネットワークプロバイダの責任ということになる。ネットワークプロバイダは、物理層に十分なセキュリティ対策を実施することにより、ネットワークを保護することができる。

10.3 NGN の開発プログラム、NGN ベースのサービスのロードマップについて

ATIS は、主に ITU-T に対してインプットを提出することにより、IMS 標準に対する貢献をしようとしている。

ATIS は、セキュリティに関する独自のフレームワークを開発するとともに、特定の課題に対するより詳細な文書を作成した。しかし、これらは標準とは程遠いものであり、現時点ではさらなる議論が必要な項目である。ATIS においては、PTSC-SAC と PTSC-SEC が、セキュリティに関わる主たるワーキンググループである。これらのグループが作成した文書は、IMS ベースの NGN をサポートすることを目的としており、ATIS では、『進化するネットワーク』と呼ばれている。

SAC と SEC には、3GPP や TISPAN のセキュリティ活動に参加しているメンバもいる。従って、一般的にこれらの ATIS ワーキンググループは、ヨーロッパの標準化組織と協調している。しかし、国際的なレベルでみれば、異なる標準や競合する標準がある場合もある。これらの競合する観点は、ITU において解決されることが定められている。

ATIS と他の標準策定組織との間でより公式なアイディアのやりとりが必要な場合には、公式なリエゾンを設置することができる。例えば、3GPP と ATIS とはしばらくの間リエゾンを設置していた。

10. 4　NGN に接続する端末に関する規制について

端末は SIP を使うことが規定されるため、H.323 端末はサポートされないだろうと考えている。

10.5　NGN の開発プログラム、NGN ベースのサービスのロードマップについて

全員にとっての大きな疑問は、NGN が本当に使われるようになるのかということだ。私は、IMS が徐々に採用されるようになるに従って、NGN も部分的に使われるようになるだろうと考えている。IMS は無線ネットワークにおいて使われるようになってきており、有線ネットワークとのコンバージェンスのためのビークルとして求められている。求められるといったのは、未だにマーケットにおいて、T-Mobile の Hotspot@Home（IMS ベースではない)を除いて統合ソリューションを目にしたことがないからである。IMS が主流となる日が来るであろうが、現時点ではまだやるべきことがある。

10.6　NGN を利用して今後提供を予定しているサービス

研究所において、IMS ベースの製品のトライアルが行われるというアナウンスはあった。当社でも IMS 製品の開発を行っている。

10.7　NGN に必要な技術の獲得方法

我々のネットワークに必要な技術については、ベンダに求めている。ベンダは、NGN と IMS に関しては、よく標準に従っている。ベンダに変更や改良の必要があるかどうかについてたずねることがあるが、答えは決まって標準に準拠しなければならないというものだ。言い換えれば、このアーキテクチャはきわめて標準ベースのものだということだ。しかし、皆が標準に準拠した IMS ベースの NGN を実装しているからといって、ベンダやプロバイダが自分を差異化することができないということではない。IMS のトップに位置するアプリケーションによって差異化することが出来る。IMS はこれらのアプリケーションサーバやアプリケーションゲートウエイを許容するように設定されている。

10.8　標準化への取り組みに力を入れている国、ヨーロッパと米国の取り組み方の相違

中国は、ITU においてアグレッシブであり、ATIS では同意の得られていない標準を推してくる事がある。