次世代ネットワークに関する世界的な動向調査 概要

Researches on Next Generation Network

村主 俊彦 Toshihiko Suguri
NRI セキュアテクノロジーズ 情報セキュリティコンサルティング事業部
（〒100-0005 千代田区丸の内 1-6-5 丸の内北口ビル E-mail: suguri@nri-secure.co.jp）

１．背景

次世代の情報通信ネットワークとして、NGN に注目が集まり、標準化の動きも活発化してきている。NGN は IP をベースとしたネットワークであり、各種マルチメディアサービスの提供、固定通信網と移動通信網を統合したシームレスなサービス(FMC)機能の提供、ネットワークの品質や端末の能力に応じたエンド・ツー・エンドでの QoS 制御機能の実現など、新しい通信サービス基盤として期待されているが、NGN で必要とされるセキュリティ対策に関する研究開発動向や実験プロジェクトの有無に関しては、必ずしも明確ではない。

２．目的

各国における NGN の導入状況、標準化動向について調査し、日本と海外との NGN に対する取り組み方の相違や、NGN の標準化動向、特にセキュリティに関連する標準化の動向を明らかにし、日本の今後の NGN への取り組み方針について考察することを目的とする。

３．NGN の概要

（1）ITU による NGN の定義[1]

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

（2）NGN が提供するサービス

- マルチメディアサービス
- PSTN/ISDN エミュレーションサービス
- PSTN/ISDN シミュレーションサービス
- インターネットアクセス
- その他のサービス
- 公衆インターネットサービス

４．NGN の標準化動向

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、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 [2]として、2 部構成の文書にまとめられている。

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) [3]において議論されることとなった。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。

- 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 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)

[1] http://www.itu.int/ITU-T/ngn/definition.html

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

[3] http://www.itu.int/ITU-T/ngn/index.phtml

５．NGN の主要な構成要素

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、PSTN と同等の機能を実現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)[4]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を行うのが IMS(IP Multimedia Subsystem)であり、そのベースとなるプロトコルが SIP(Session Initiation Protocol)である。

■ IMS の概要

IMS の概要を以下に示す。

- 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
- 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
- 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。
- IETF 標準のプロトコルである SIP、SDP、DIAMETER をベースとしている。
- 課金、請求、セキュリティをサポート
- 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 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にまたがる課金を提供

６．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 では、NGN をストラタムとプレーンによって構成されるとしており、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それぞれ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

７．NGN セキュリティの標準化状況

現在、NGN における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[5]。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。2006 年 7 月に開催されたジュネーブ会合において、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 が提出された。

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[6]。

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。

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。

[4] http://www.ietf.org/rfc/rfc3261.txt?number=3261

[5] www.itu.int/ITU-T/studygroups/com17/tel-security.html

[6] 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)

■ **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[7]。

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

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。

８．ETSI TISPAN による NGN セキュリティ要求条件

NGN リリース 1 に対するセキュリティ要件が ETSI[8]の技術委員会 TISPAN[9]から提案されている。TISPAN が作成したセキュリティ要件に関する文書の概要を以下に示す。

- ETSI TS 187 001 V1.1.1　NGN Security : Requirements

NGN リリース 1 のセキュリティ要件をまとめたもの

- ETSI TS 102 165-1 V4.2.1 Method and proforma for Threat, Risk, Vulnerability Analysis Part 1

セキュリティ上の脅威とリスク分析の詳細を規定

- ETSI TR 187 002 V1.1.1　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』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。

TS 102 165-1 と TR 187 002 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。

- ETSI 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

９．X.805 勧告の概要

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 勧告は、以下の 3 つの課題に対する解決策を見

[7] http://www.itu.int/ITU-T/studygroups/com17/ict/part03.html
[8] http://www.etsi.org/
[9] http://www.etsi.org/tispan/

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 勧告では、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が用いられる。

- セキュリティディメンジョン
  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

- セキュリティレイヤ
  1. インフラストラクチャレイヤ
  2. サービスレイヤ
  3. アプリケーションレイヤ

- セキュリティプレーン
  1. マネジメントプレーン
  2. 制御プレーン
  3. エンドユーザプレーン

X.805 勧告では、X.800 勧告に記載されている以下のセキュリティ脅威を想定している。

- 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

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、これらの脆弱性と脅威に前記の 8 つのディメンジョンにより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。

１０．各国の標準作成組織と標準化への取り組み

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

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

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 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[10]。

１１．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

（1）日本

日本では、2001 年に策定された e-Japan 戦略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、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ている。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[11]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)

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[12]。

- 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

総務省の研究会『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』[13]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

[10] http://portal.etsi.org/docbox/TISPAN/Open/NGN_Published/
[11] http://www.johotsusintokei.soumu.go.jp/field/tsuushin01.html
[12] 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
[13] http://www.soumu.go.jp/s-news/2004/040608_2.html

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

（2）EU

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[14]。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

（3）イギリス

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。

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、企業向けの FMC サービスが開始されている。

今後の計画として、2010 年に次世代ブロードバンドサービスを 2,000 万人以上に利用可能とし、2011 年に 21CN への移行を完了するとしている。

（3）フランス

2004 年に発表されたブロードバンド戦略 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
- 2007 年にブロードバンドの人口カバー率を 95%
- 2010 年に産業地域における光ファイバの普及率を 90%

電子通信に関する規制機関 ARCEP(Autoritè de Règulation des Communications Electroniques et des Postes)[15]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。

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。

光ファイバによるブロードバンド接続計画として、2008 年末には、人口 100 万人あたり 150,000～200,000 のユーザが利用可能とすることとされている。

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いう見解が出されている。

（4）ドイツ

2003 年に発表された「Information Society Germany 2006」[16]があり、2005 年までにインターネットを人口の 75%まで普及させるという目標が掲げられた。また、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。

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。

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、『Deutschland Online 4 Report 2006』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。
- 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でり、2015 年にはユーザ数が 750 万人に到達する。
- 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。

（5）米国

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・目標を策定した[17]。

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

---

[14] http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm

[15] http://www.arcep.fr/index.php?id=1&L=1

[16] http://www.bmbf.de/pub/aktionsprogramm_2006_gb.pdf

[17] 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

米国の信事業者の動向のうち主なものを以下に示す。

- SBC(現 AT&T) : 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。

- Verizon : 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。

ベンダの NGN への取り組みについては、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。

NGN のセキュリティに関する研究開発については、政府主導による下記の報告書に基づいた計画がある。

- NSTC[18] :『Federal Plan for Cyber Security and Information Assurance Research and Development』[19]

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り、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という認識の基に、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としている。

- 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

- NSTAC[20] :『Next Generation Task Force Report』[21]

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。

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。

[18] http://www.ostp.gov/nstc/
[19] http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf
[20] http://www.ncs.gov/nstac/nstac.html
[21] http://www.ncs.gov/nstac/reports/2006/NSTAC%20Next%20Generation%20Networks%20Task%20Force%20Report.pdf

（6）韓国

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。

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。

2006 年 3 月に「u-KOREA 基本計画」を策定されたのに伴い IT839 戦略の見直しが実施され、2006 年 2 月に「u-IT839 戦略」として発表された。

通信事業者 KT の「FTTH 推進戦略」では、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となっている。

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
- Phase II (2006 - 2008) 通信の統合
- Phase III (2008 -) オフライン産業のオンライン化

次世代ネットワークのセキュリティに関しては、MIC(情報通信省)が推進してしており、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

１２．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

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が実施されている。

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において検討が行われている。後者において課題項目として挙げられているものを以下に示す。

- なりすまし／発 ID 偽装対策
- 個人情報保護
- 逆探知
- 端末からの脅威(SPIT、ワン切)への対策
- INVITE 呼集中防止対策
- ネットワークからの脅威(DDoS、スパム、不正アク

セス)
- 通信の盗聴等
- SIP と連動しない音声通信流通の制限
- 端末機能の安全性確保
- 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、他網からの流入防止の双方対策
- 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

NGN のセキュリティ関連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)において、以下の技術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

（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

海外の通信事業者及び通信機器ベンダへのインタビュー調査の結果によれば、NGN におけるセキュリティ上の重要な課題として、アイデンティティ管理、ユーザ認証、SIP／IMS 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。

IMS のセキュリティについては、3GPP において検討が進められているが、通信事業者、通信機器ベンダともにセキュリティ機能を積極的に有効にしようとしない傾向があるという問題点が指摘されている。

IMS 以外のセキュリティ上の課題として通信事業者が挙げたものには、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がある。

いずれの課題についても取り組みは開始されたばかりという状況ではないかと思われる。

１３．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

日本における光ファイバベースの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。ヨーロッパにおいては、2010 年ごろまでは ADSL によるブロードバンドが主流であると予測される。

通信事業者のネットワークの NGN への移行については、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。

NGN リリース 1 のセキュリティ要件が勧告化に向けて作業中であることや、IMS のセキュリティが検討中であることから、十分にセキュリティが確保された NGN の実現はもう少し先になると思われる。

（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、高度なブロードバンドインフラが整備された。NGN はセキュリティ機能を提供するが、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、ユーザが自ら責任を持たなければならない。

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が必要となる。

海外に対する支援の点では、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。

産業育成の点では、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の検討が必要である。具体的には、以下の利点を活かす施策の検討が必要である。

- 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

施策例としては、各国のマーケットのニーズにあわせた製品やサービスの投入、日本の R&D の先進性を活かした高機能・高性能なサービスのショーケースの構築と海外への販売、NGN セキュリティ適合性評価制度の運営、高いセキュリティが確保されたネットワークを利用して提供する高付加価値サービスといったものが考えられる。

１４．今後の検討課題とまとめ

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は重要な検討課題である。

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。

以下に、技術以外の観点からの検討が必要な課題の例を示す。

（1） 標準化の専門家の育成

近年の日本の標準化への取り組みは、非常に積極的なものとなっているが、ヨーロッパ諸国の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、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、企業において標準化に対する貢献を成果として認めるための体制を整備するといったことも必要になる。

（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 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。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(情報セキュリティ機能)が必要になる。

情報セキュリティ機能は、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。

遠隔医療は一例に過ぎないが、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。

１５．参加企業

NRI セキュアテクノロジーズ株式会社