資料3

情報通信審議会
IPネットワーク設備委員会の
検討状況について

平成19年3月20日
総務省

情報通信審議会IPネットワーク設備委員会について

背　景

○技術革新やブロードバンド化の進展に伴い、IP系サービスの急速な伸長
○電気通信事業者の通信インフラのIP化に向けた方針の明示
○諸外国においてもIP化の動きが活発化

◆ 固定電話網のIP化への移行に向けた動きが活発化
◆ ２０１０年頃までに次世代IPネットワークが本格的に稼働

早期に、「次世代ネットワーク」の実現に向けた環境整備を進めていくことが重要。
2007年までを目途に技術面の制度の整備。

情報通信審議会に「ネットワークのIP化に対応した電気通信設備に係る技術的条件」について諮問（平成17年10月）

○ ネットワークのIP化に対応した技術基準の見直し
○ 事故・障害が多発しているIP系サービスの安全・信頼性確保対策の策定

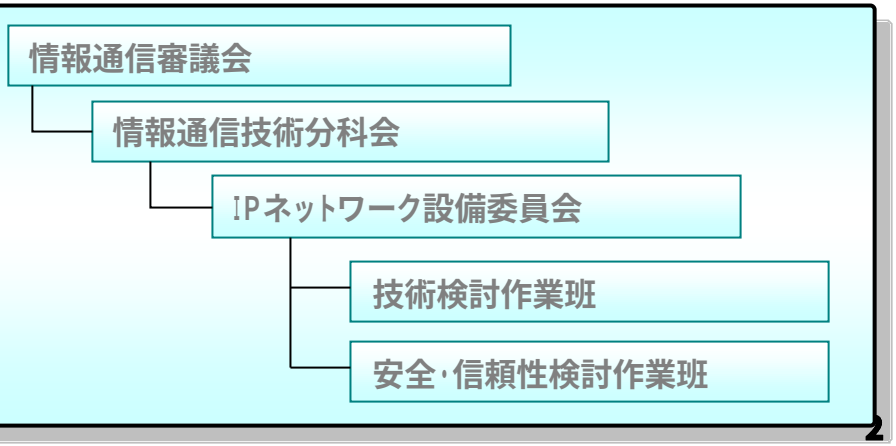
検　討

◆ 深く浸透しているアナログ固定電話の代替として、0AB～J番号※を使用するIP電話に関する技術的条件を検討。

※ 固定電話で使用される番号（「03-」、「045-」等）

⇒ １月２４日一部答申

◆ ネットワークの安全性・信頼性対策



情報通信審議会IPネットワーク設備委員会での審議状況

1．ネットワークのIP化の進展に対応した技術基準の見直しに向けた検討（技術検討作業班）

（1）0AB～J番号を使用するIP電話の基本的事項に関する技術的条件

国民生活に深く浸透している固定電話の代替として、０ＡＢ～Ｊ番号を使用するIP電話について先行して検討を実施。

→ 既存の固定電話と同等のサービス・機能を実現するため、品質規定、重要通信の確保、輻輳対策等の基本的事項に関する技術的条件を本年1月に一部答申。

（2）その他のIP系サービス

同様の視点で、高機能音声サービス、コンテンツ配信サービス、固定・移動シームレスサービス、端末・網等に関して、継続して審議。

2．安全・信頼性確保対策の検討（安全・信頼性検討作業班）

IP系サービスの急速な普及等に伴い、事故・障害が増加・長時間化する傾向。

→ ネットワークの安全・信頼性対策として、事故報告制度、電気通信主任技術者制度、安全・信頼性に係る技術的条件等について、本年4月目途に作業班報告とりまとめ予定。

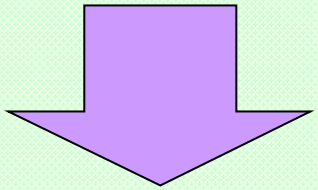
１．　ネットワークのIP化の進展に対応した技術基準の見直しに向けた検討

（技術検討作業班の検討）

審議経過

平成17年10月31日諮問
情報通信審議会諮問第2020号
「ネットワークのIP化に対応した電気通信設備に係る技術的条件」

平成17年11月～平成19年1月
IPネットワーク設備委員会において検討（第1回～第5回委員会）



ネットワークのIP化に対応するために必要な検討課題のうち、
「0AB～J番号を使用するIP電話の基本的事項に関する技術的条件」を検討

※IPネットワーク設備委員会に技術検討作業班を設置して検討を行った。
技術検討作業班においては、次世代IPネットワーク推進フォーラムと連携して検討を進めた。

（参考）
IP系サービスの災害・事故への対策については、委員会に別途設置している安全・信頼性検討作業班において、ネットワークの管理・運用面も含めて総合的な検討を行っているところ。4月目途に作業班報告とりまとめ予定。

審議の背景

○技術革新やブロードバンド化の進展に伴い、IP系サービスの急速な普及・拡大　(例：IP電話サービス、法人向けIPサービス（IP-VPN等）)
○これに呼応し、電気通信事業者も通信インフラのIP化に向けた方針を明示
○諸外国においてもIP化の動きが活発化　(例：英国BTの電話網のIP化計画の発表、NGN標準化の議論)　(次頁参照)

国内外で固定電話網のIP化への移行に向けた動きが活発化

ネットワークのIP化に向けた課題

○IPネットワークへの移行後も現行のサービス・機能をどこまで確保するべきか。
○サービスの品質はどうあるべきか。

品質・機能の確保に関する課題

○IPネットワークへの移行は従来のネットワーク構造を根本から変えるものであり、また、基本的にオープンな構成を基盤としている点を踏まえると、ネットワークの安全性・信頼性をいかに確保するのか。

安全性・信頼性の確保に関する課題

○IPネットワークへの移行は従来のネットワーク構造を根本から変えるものであることを踏まえると、エンド・トゥ・エンドでの相互接続性・運用性をいかに確保するべきか。

相互接続性・運用性の確保に関する課題

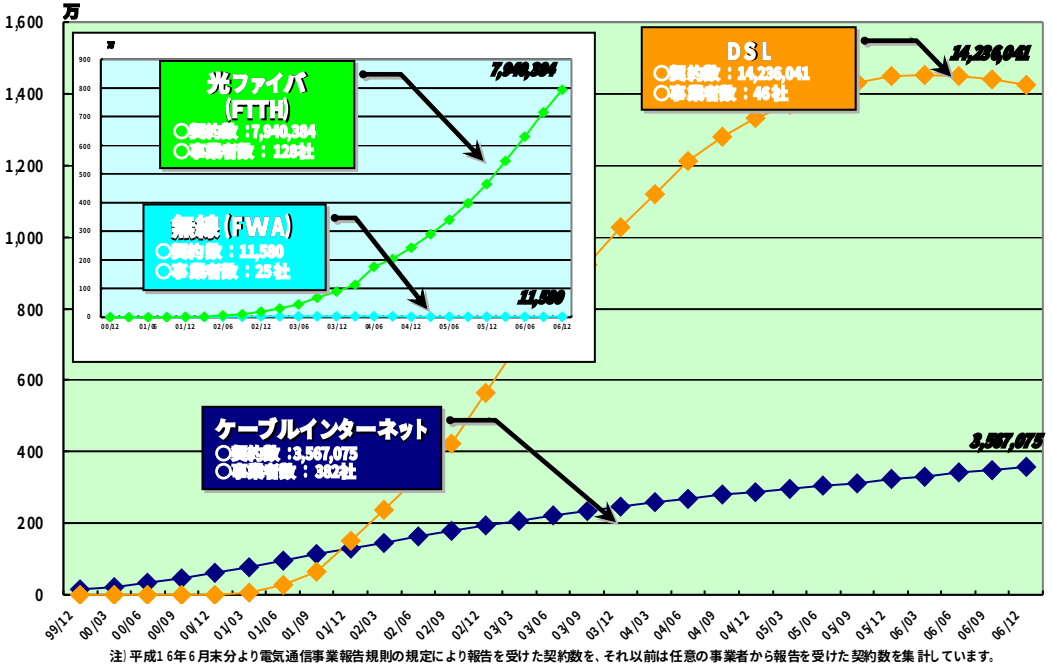
○次世代IPインフラ研究会 第三次報告書～電話網からIP網への円滑な移行を目指して～（平成17年8月）の提言

○「2010年には世界最先端のICT国家として先導する」との目標を踏まえ、早期に、次世代IPネットワークの実現に向けた環境整備を進めていくことが重要。
⇨2007年までを目途に技術面の制度の整備

ネットワークを巡る現状と動向（1／2）

ブロードバンドサービス加入者数の推移

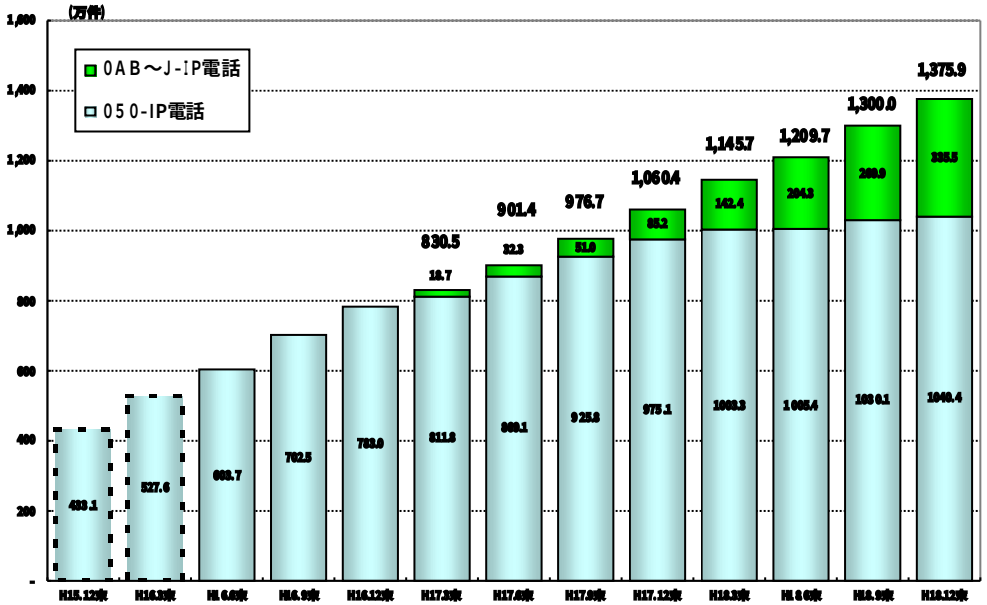
○ ブロードバンド環境が近年急速に普及・進展



注）平成16年6月末分より電気通信事業報告規則の規定により報告を受けた契約数を、それ以前は任意の事業者から報告を受けた契約数を集計しています。

IP電話の利用数の推移

○ IP電話サービスの利用数が急速に増加。
今後、FTTH等のIP系高速アクセスサービスの普及等に伴って、0AB～J番号を使用するIP電話も急速に普及していくものと予想される。



ネットワークを巡る現状と動向（2／2）

国内外の電気通信事業者のIP化へ向けた取組

○　我が国では、ＮＴＴ、ＫＤＤＩ、ソフトバンクテレコムをはじめとする電気通信事業者が、ネットワークのＩＰ化に向けた取り組みを開始。

○　諸外国においても、例えば英国のＢＴ（ブリティッシュ･テレコム）が固定電話網のＩＰ化計画を発表した他、米国、ドイツ、韓国等においても、電気通信事業者のＩＰ化、ブロードバンド化に向けた計画を作成。

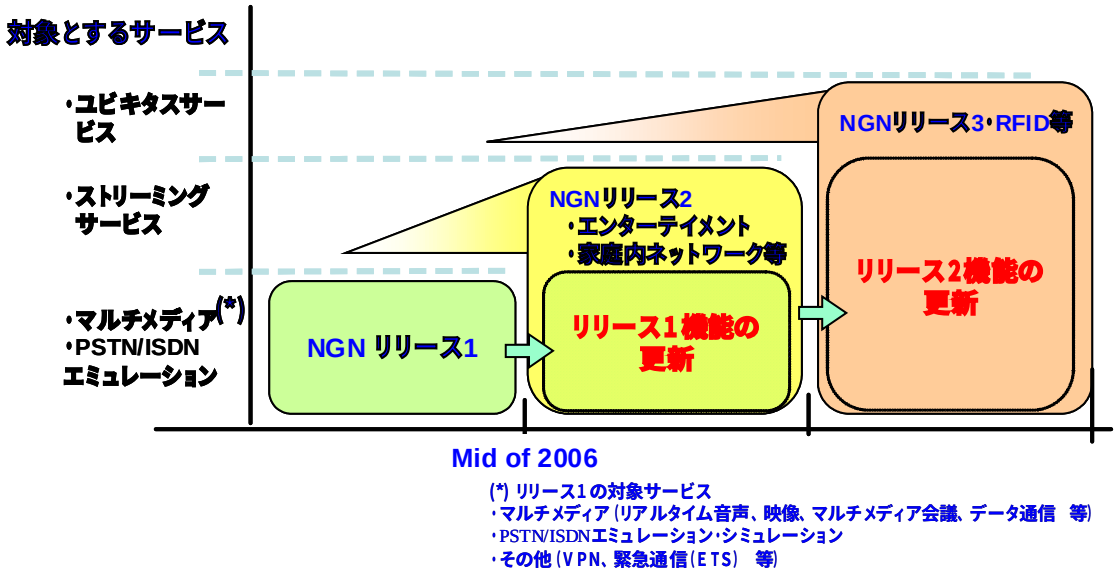
次世代IPネットワークの国際標準化の取組

○　ITU、ETSI等においては、NGN (Next Generation Network)として次世代IPネットワークの標準化活動が活発化。

○　NGNの国際標準化は、ＩＴＵ－Ｔの新会期（2005-2008）の最も重要な課題。

○　ITU-Tにおいては、2006年７月にNGNのスコープ、要求条件等を中心とするNGNリリース１の基本的勧告案が確定。今後は具体的なプロトコルを定める関連技術勧告を2007年９月までに完成予定。

ITUにおけるＮＧＮ標準化のステップ



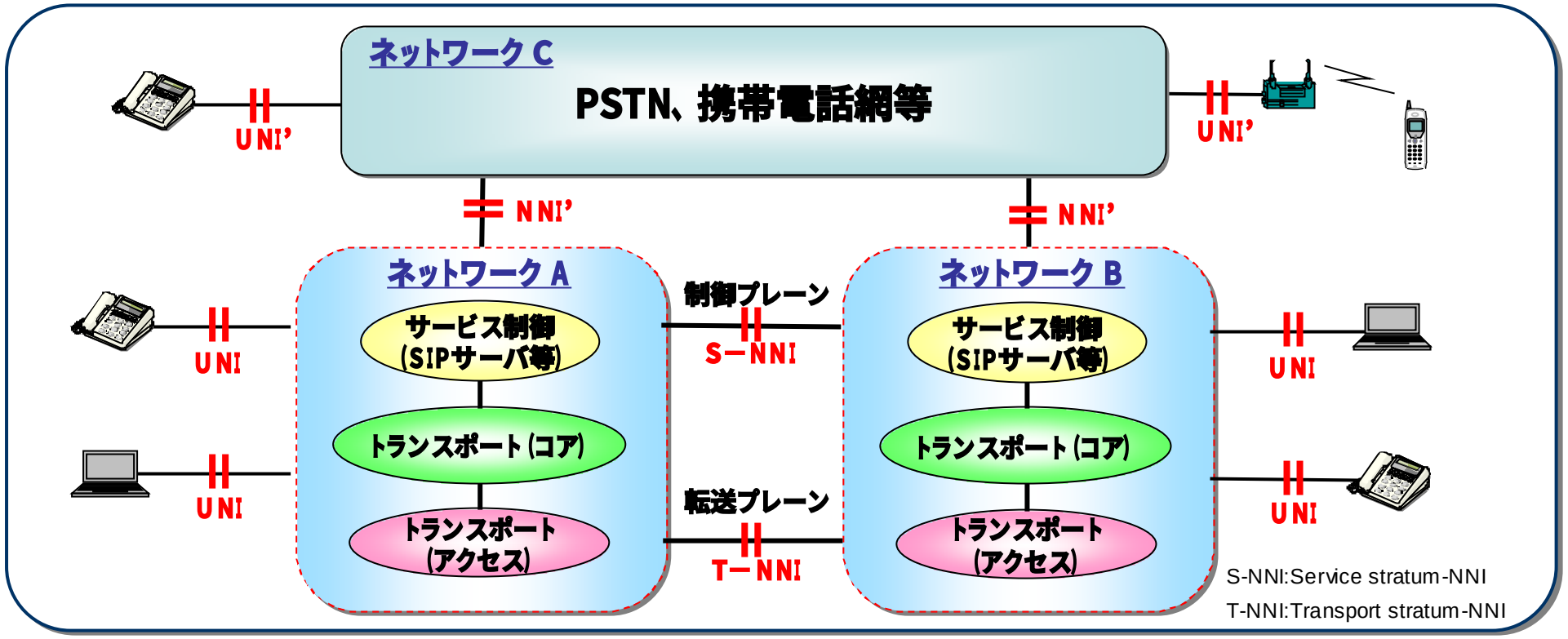
(*) リリース1の対象サービス
・マルチメディア（リアルタイム音声、映像、マルチメディア会議、データ通信　等）
・PSTN/ISDNエミュレーション・シミュレーション
・その他（VPN、緊急通信（ETS）　等）

検討の対象範囲

電話サービスが、
◆国民生活の最も基本的なコミュニケーション手段として大きな役割を担っていること
◆双方向･リアルタイム性の極めて高いサービスの実現が要求されることを踏まえ、まずは

現行のアナログ電話相当として位置付けられる0AB～J番号を使用するIP電話の基本的事項に関して検討

◆検討にあたっては、2010年頃までに次世代IPネットワークが本格的に稼働し、
現行のアナログ電話が0AB～J番号を使用するIP電話に移行していくことを想定し
現在発生している問題への対処、将来的に発生することが予想される問題への対処を認識して検討。
◆検討を効果的に進めるため、以下の共通モデル（ネットワーク間接続パターン）をベースとして検討。



個別課題の検討の方向性

「ネットワークのIP化に対応した電気通信設備に係る技術的条件」のうち「0AB～J番号を使用するIP電話の基本的事項に関する技術的条件」について

【品質・機能の確保】

○ 現行の電話のサービス・機能の維持

○ 安定的サービス提供の確保

【安全性・信頼性の確保】

○ オープンなIPネットワークにおける安全・信頼性の確保

【相互接続性・運用性の確保】

○ 複数のIPネットワークを介したEnd to Endでの相互接続性・運用性の確保

○ IPネットワークが相互接続されることへの対応
（End to Endの品質基準において個々のIPネットワークごとに満たすべき基準）

○ 通信ライフラインとして不可欠な機能
（重要通信の確保、緊急通報の実現等）

○ その他安定的なサービス提供に必要な機能
（端末に具備される無効呼抑止機能、保守機能、ふくそう回避機能等）

○ オープン化に伴うセキュリティ脅威の増大に対するサービス・機能の安全性の確保に必要な対策
（異常ふくそう対策、不正アクセス対策、発信者番号偽装対策、通信の秘密の保持等）

○ IP化による信頼性低下要因への対策等
（故障対策、端末に具備される自動再発信回数制限、ソフトウェア更新機能等）

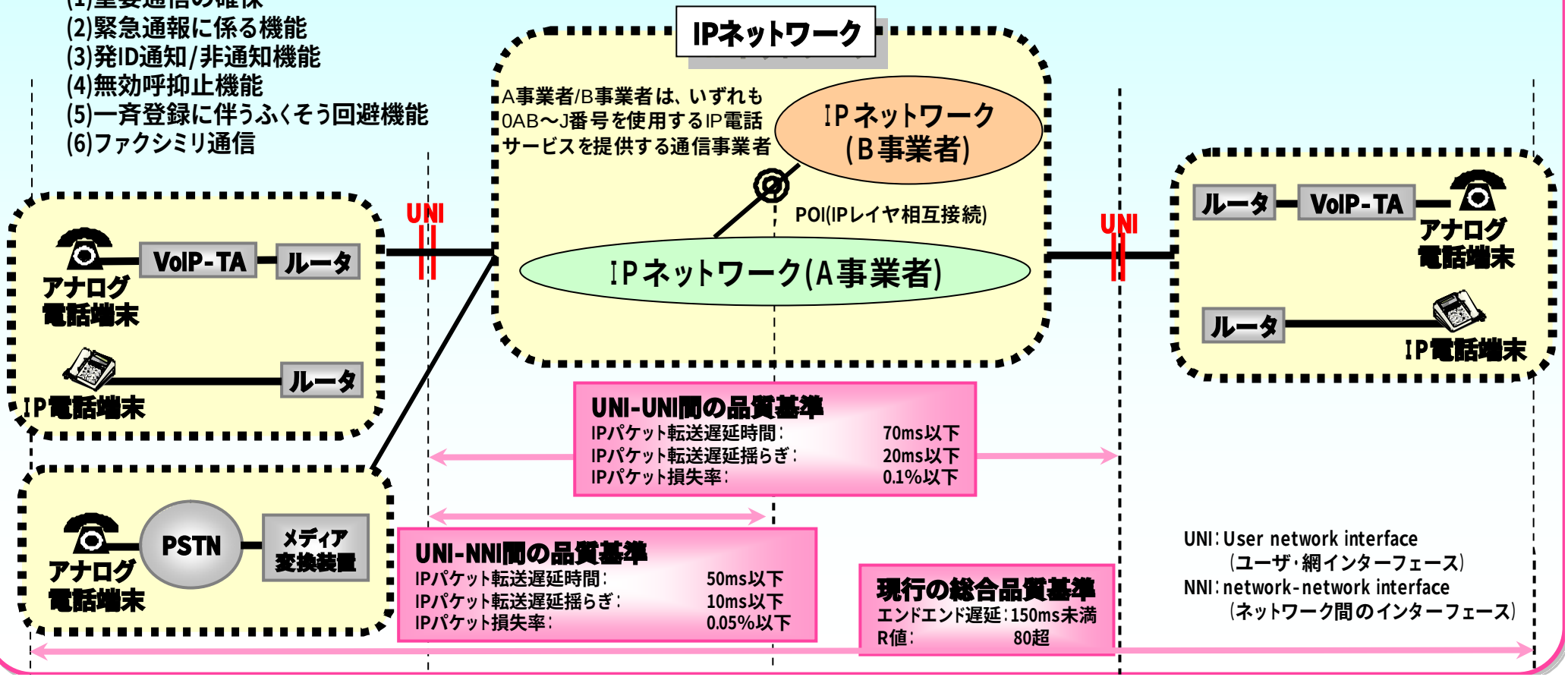
○ IPネットワーク間、IPネットワーク・PSTN間の相互接続性の確保に必要な事項
（呼制御プロトコル、インターフェース規定、符号化方式、優先取扱い等）

品質・機能の確保に関する検討

○ IPネットワークが相互接続されるネットワーク形態等に対応するためにそれぞれのネットワークが満たすべき品質基準
○ 通信ライフラインとして不可欠な機能、基本サービスの安定的な提供に必要な機能
について、主に以下の項目を検討。

【品質の確保に関する検討】
(1)ネットワーク品質
(2)ネットワークと端末との遠隔切り分け機能
及び総合品質測定機能

【機能の確保に関する検討】
(1)重要通信の確保
(2)緊急通報に係る機能
(3)発ID通知/非通知機能
(4)無効呼抑止機能
(5)一斉登録に伴うふくそう回避機能
(6)ファクシミリ通信



安全性･信頼性の確保に関する検討

○ オープン化に伴うセキュリティ脅威の増大に対するサービス･機能の安全性の確保に必要な対策等
○ IP化による信頼性低下要因への対策等
の基本的事項について設備面を中心として、主に以下の項目を検討。

※なお、IP系サービスの事故･障害への対策については、別途設置している安全･信頼性検討作業班において、ネットワークの管理･運用面も含めて総合的に検討しているところ。

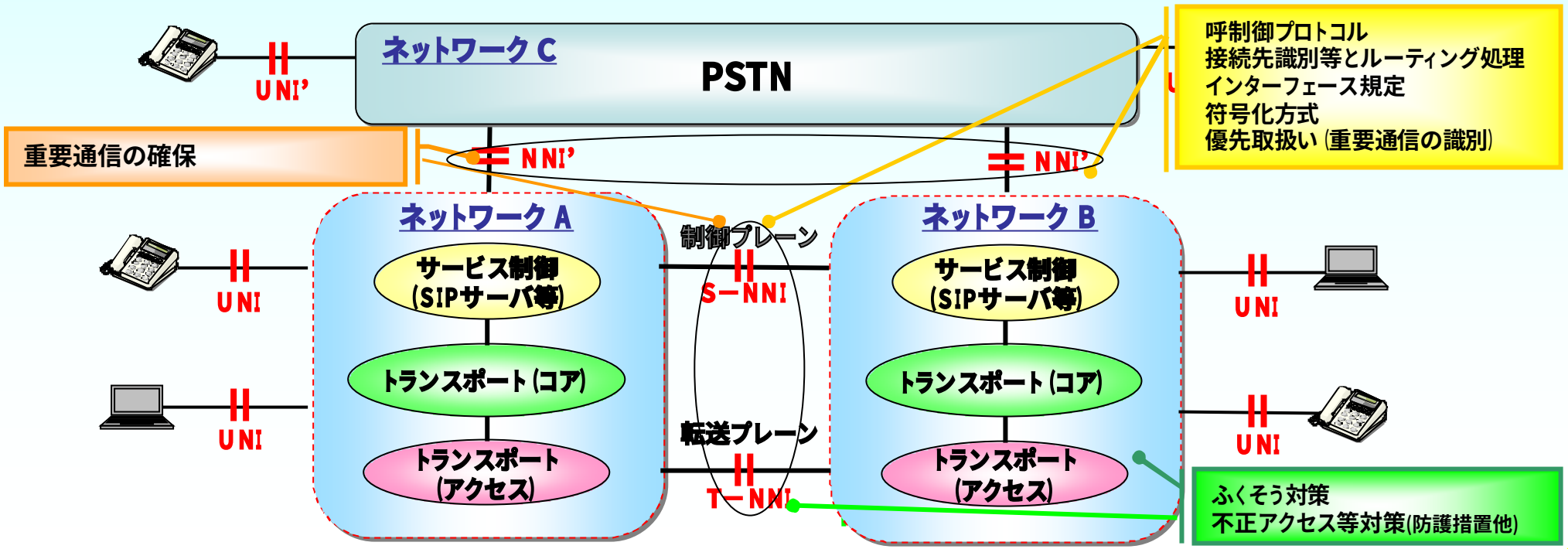
【安全性の確保に関する検討】
(1)重要通信を優先的に取り扱うためのルール等
(2)異常ふくそうからのネットワークの保護
(3)不正アクセス等対策
(4)発信者番号偽装対策
(5)個人情報の保護
(6)通信の秘密の保持

【信頼性の確保に関する検討】
(1)障害箇所の特定
(2)設備の損壊･故障及び通信路の途絶対策
(3)端末における自動再発信回数制限
(4)端末のソフトウェア/ファームウェア更新機能

相互接続性･運用性の確保に関する検討

○ 相互接続性の確保の観点から、品質･機能、安全性･信頼性の確保に関する事項
○ IPネットワーク間、IPネットワーク･PSTN間の相互接続性の確保に必要な事項
について、主に以下の項目を検討。

(1)ネットワーク品質
(2)重要通信の確保
(3)不正アクセス等対策
(4)呼制御プロトコル
(5)番号に基づく接続先識別/接続出方路の判定とルーチング処理
(6)Uプレーンインタフェースにおける低位レイヤからIPレイヤまでの各階層のインタフェース規定
(7)Uプレーンインタフェースにおける符号化方式
(8)試験呼の識別表示
(9)オプションサービスに関する規定
(10)IPネットワーク相互間の優先取扱い



今後の検討課題等（1／2）

【0AB～J番号を使用するIP電話の基本的事項以外のIP電話に関する課題】

主な検討課題として以下のものが挙げられる。

(1) 050番号を使用するIP電話に関して、電話サービスに最低限必要とされる品質レベル等

(2) IP電話において広帯域音声符号化方式を利用してより高い品質を実現できるサービスに関して、その品質レベルの考え方や、ネットワーク端末間のインタフェース条件等

(3) 動画を付加したテレビ電話等、IP電話に様々なアプリケーションが付加されていくことが想定されるが、そうした付加的なアプリケーションの品質確保等の考え方や、ネットワーク端末間のインタフェース条件等

(4) 端末設備の技術基準に関して、新たな機能の具体的な技術方式の実現における、試験方法等の具現化

(5) その他に留意すべき課題として、社会的動向や必要性を見ながら検討を要する課題として以下のものが挙げられる。

① 発信者番号より発信者の位置を特定する逆探知
② 端末への迷惑行為に対して端末に特定の通信を拒否する機能を搭載する等の対策
③ 端末のバッテリー搭載等停電対策の考え方
④ 重要通信以外の一般的な音声通信について、他の音声以外の通信に対して優先的に取扱う等の在り方
⑤ 広域災害に対して、「災害基本法」、「大規模地震対策特別措置法」、「武力攻撃事態における国民の保護のための措置に関する法律」等の関連法令をもとに、防災計画や緊急時の連絡体制等の備えが図られているが、これら連絡手段の統一的な方法

今後の検討課題等（2／2）

【新たなサービス等に関する課題】

主な検討課題として以下のものが挙げられる。

(1) コンテンツ配信サービスのネットワークモデルの具現化とともに、品質条件等の品質・機能の確保、ふくそう対応等の安全性・信頼性の確保、相互接続・運用性の確保の在り方等

(2) 迷惑メールの今後の進化やIPネットワークの発展性を考慮し、ネットワークとメール配送機能の連携による迷惑メールの抑止手段の可能性等

(3) 固定・移動シームレスサービスについて、アクセス手段の変化を考慮した最適な通信品質の確保の在り方等

(4) 新たな重要通信、緊急通報の確保方法として、IPネットワークにおける電話以外の多様な通信サービスに関して、災害時や緊急時における重要通信・緊急通報としての利用の新たな可能性

(5) ホームネットワーク等の端末側に多様なサービス・機能を有する端末網が発展することが想定されるが、こうした端末網の品質の基準の考え方や、ネットワークから端末までの相互接続性の確保、ネットワークと端末の機能分担・連携の在り方等

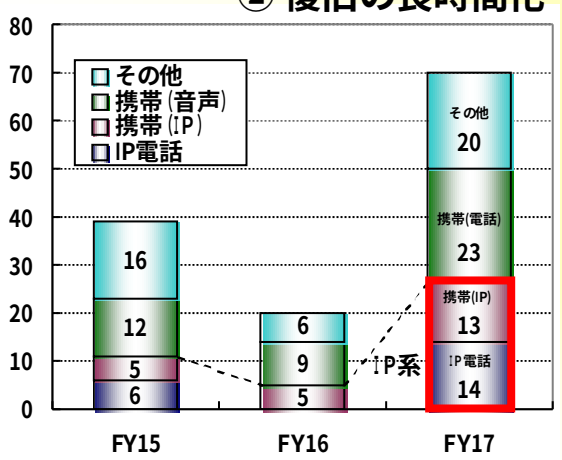
2．安全･信頼性確保対策の検討

(安全･信頼性検討作業班の検討)

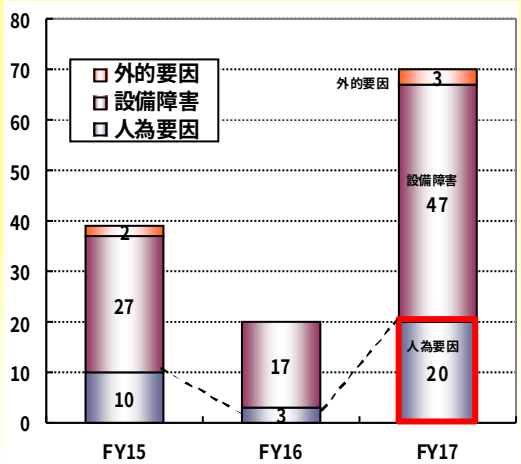
安全・信頼性確保対策の検討

背景

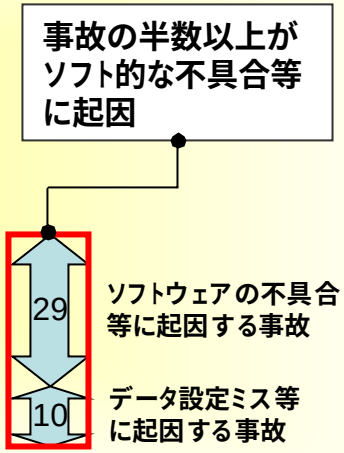
- ◇ IPネットワークへと情報通信インフラの移行が進展、IP系サービスにおける事故の増加
- ◇ 人為的要因による事故が増加
- ◇ 事故の半数以上がソフト的な不具合等に起因
- ◇ IP系サービスにおける事故の傾向
  - ① 事故の広域化・大規模化
  - ② 復旧の長時間化



サービス別事故発生件数の推移



要因別事故発生件数の推移



ソフト的な不具合等に起因する事故の発生状況

IP系サービスの事故増加への対応策が必要

安全・信頼性検討作業班を設置
(H18.9.22第1回会合)

IT戦略本部　重点計画2006

2009年度初めまでに、重要インフラにおけるIT障害の発生を限りなくゼロにする

主な検討課題

- ○ 障害発生時の対応、監視体制、予防対策などの検討
- ○ 電気通信主任技術者などによる管理体制の在り方の検討
- ○ 関連する技術基準などの検討

検討結果を技術基準等の制度へ反映

事故の発生状況

◆IP系サービスにおいて、
事故が大規模化・広域化する傾向にある。

IP系サービスにおける大規模な事故の発生状況（平成17、18年度の一部）

影響エリアの拡大（交換局→地方）
影響者数の増加（数万→10万超）

影響数	影響地域	サービス種別	事故種別
86万	東日本エリア	IP電話	その他（12時間27分）
86万	東日本エリア	IP電話	その他（10時間58分）
36万	東海地方	携帯メール	重大な事故
82万	西日本エリア	IP電話	その他（2時間15分）
93万	東日本エリア	IP電話	その他（2時間15分）
250万	全国	メール	重大な事故
230万	全国	携帯メール	その他（1時間58分）
390万	関東地方（東京都）	携帯メール	その他（54分間）
148万	全国	メール	重大な事故
246万	全国	携帯メール	その他（遅延）
180万	全国	PHSメール	その他（遅延）
1，950万	全国	携帯IP接続	重大な事故
951万	北海道、東北、関東、東海地方	携帯IP接続	重大な事故
57万	全国	メール	重大な事故
50万	全国	PHS-IP接続	その他（サービス品質低下）
100万	全国	携帯IP接続	重大な事故

安全・信頼性検討作業班での検討経過

◆ これまでに5回の会合を開催

○ 第1回安全・信頼性検討作業班（平成18年 9月22日）

安全・信頼性検討作業班の運営方針、審議方針について審議を行い、情報通信ネットワークの災害・事故の状況及び安全・信頼性対策の現状を把握した。

○ 第2回安全・信頼性検討作業班（平成18年10月25日）

情報通信ネットワークにおける安全・信頼性対策の現状の詳細について構成員から報告を受け、意見交換を行った。

○ 第3回安全・信頼性検討作業班（平成18年11月 1日）

情報通信ネットワークにおける安全・信頼性対策の現状の詳細について構成員から報告を受けたほか、検討課題の抽出を目的とするアンケートの実施について審議を行った。

○ 第4回安全・信頼性検討作業班（平成18年11月27日）

アンケート結果をもとに、情報通信ネットワークにおける安全・信頼性向上のために　　必要な検討課題について審議を行った。

○ 第5回安全・信頼性検討作業班（平成19年1月10日）

検討課題について重点的に議論すべき事項の検討の方向性について審議を行った。

安全・信頼性検討作業班での検討内容(1/2)

◆4つの柱、3つの重点項目ごとに、安全・信頼性を確保するための検討課題、　検討の方向性、具体的に取り組むべき事項を議論

- 4つの柱
  - 組織・体制の整備及び資源の確保
    - セキュリティに関わる人材育成や役割の設定等、組織・体制等の項目を明確化。
  - 取扱い情報の管理の明確化
    - 重要度に応じた適切な措置をするために、取り扱う情報に対して、種類や責任等を明確化。
  - 情報通信ネットワーク管理要件の明確化
    - 障害や情報の重要度に応じた、満たすべき情報通信ネットワーク管理要件の明確化。
  - 情報通信ネットワークについての対策
    - 情報通信ネットワーク管理要件に対応した対策項目を、装置やシステムごとに明確化。
- 3つの重点項目
  - IT障害の観点から見た事業継続性確保のための対策
  - 情報漏えい防止のための対策
  - 外部委託における情報セキュリティ確保のための対策

安全・信頼性検討作業班の検討課題（1／2）

４つの柱　基本的に取り組むべき事項

柱１．組織・体制の整備及び資源の確保

セキュリティに関わる人材育成や役割の設定等、組織・体制等の項目を明確化。

- 基本指針、責任の明確化など組織体制の整備
- 人の育成、罰則など人的資源のセキュリティ確保
- サイバー攻撃に対する責任体制・管理体制の整備
- ネットワーク輻輳に対する責任体制・管理体制の整備
- 故障・災害等ＩＴ障害に対する責任体制・管理体制の整備
- 重要情報漏えいに対する責任体制・管理体制の整備

柱２．取扱い情報の管理の明確化

重要度に応じた適切な措置をするために、取り扱う情報に対して、種類や責任等を明確化。

- 情報システム、取扱情報に対する責任と情報の分類
- サイバー攻撃に備えたサーバ等に格納された情報管理
- 重要情報の格付け、取扱いルールなど重要情報管理

柱３．情報通信ネットワーク管理要件の明確化

障害や情報の重要度に応じた、満たすべき情報通信ネットワーク管理要件の明確化。

- 情報通信ネットワークのセキュリティ管理
- 利用者アクセスの管理
- ネットワークアクセス制御
- サイバー攻撃対策
- ネットワーク輻輳対策
- 重要通信の確保
- 重要情報漏えい対策

柱４．情報通信ネットワークについての対策

情報通信ネットワーク管理要件に対応した対策項目を、装置やシステムごとに明確化。

- セキュリティを保つべき領域での物理的管理
- 自社の管理外の場所に設置する設備管理
- 需要予測に基づく、システムの容量の適切な計画・設計
- 開発及びサポートプロセスにおける管理
- 故障検出、動作ログ取得などによる監視
- サイバー攻撃に備えた設備等に関する脆弱性への対策
- 通信トラヒック量の観測などネットワーク輻輳対策
- バックアップ、分散化など故障・災害等ＩＴ障害対策

安全・信頼性検討作業班の検討課題（2／2）

３つの重点項目

特に重点的に取り組みが求められている項目

重点１．ＩＴ障害の観点から見た事業継続性確保のための対策

- 事業継続管理における情報セキュリティの側面
- 情報等の管理・障害検知・切り分け
- 緊急時の情報連絡（迅速な連絡・対応体制）
- ＩＴ障害対応の訓練・演習の計画・実施
- サイバー攻撃対策
- ネットワーク輻輳対策（迅速な連絡・対応体制）
- 故障・災害等ＩＴ障害対策（迅速な連絡・対応体制）
- 重要情報漏えい対策

重点２．情報漏えい防止のための対策

- 媒体の取扱い
- 情報の交換
- 重要情報漏えい対策

重点３．外部委託における情報セキュリティ確保のための対策

- 秘密保持
- 外部組織
- 第三者が提供するサービスの管理
- 重要情報漏えい対策

検討の方向性（1／ 9）

柱１．組織・体制の整備及び資源の確保

（セキュリティに関わる人材育成や役割の設定等、組織・体制等の項目を明確化。）

◎：重点的に検討すべき事項

（１）基本指針、責任の明確化など組織体制の整備

1 ◎各事業者によるセキュリティ確保の体制など会社の基本指針の公表

2 ◎情報セキュリティ管理専任組織の設置などによる責任の明確化と、外部監査の活用による実施確認

◎記録媒体の性能向上やシステム間接続拡充などによるリスク・脅威の拡大に応じた適時の点検見直し（PDCA）

3 ◎信頼性向上に関するガイドライン等の利便性の向上

4 ・システム管理のガイドラインの国際的な基準との整合性の確保

（２）人の育成、罰則など人的資源のセキュリティ確保

1 ◎新たな技術やリスク管理等の対応を含めた技術者を育成する機関の整備など人材育成の強化

2 （主任技術者等の制度の見直し）

◎IP化の進展に合わせた、電気通信主任技術者資格区分、試験内容、及び制度の見直し（主任技術者等技術者の具体的活用方策）

◎IP化に対応した資格認定者の普及と認定資格者の現場での配備、活用

◎事故対策や、内部監査・報告などの面での電気通信主任技術者の活用

3 ◎サイバー攻撃に対処できる人材の確保・育成

◎ネットワーク、サーバ機器などを保守運用する技術者の育成や体制の整備

◎重要情報漏えい防止のための教育

（３）サイバー攻撃に対する責任体制・管理体制の整備

1 ◎セキュリティ情報管理レベルの規定、及び攻撃者への対処

2 ◎サイバー攻撃に備えた監視項目の明確化、監視体制の整備、ソフトウェアパッチなど運用方法の確立

（５）故障・災害等ＩＴ障害に対する責任体制・管理体制の整備

1 ◎IP化に対応した障害時のマニュアルの整備・見直し

2 ◎故障時のサービス回復のための緊急対応の手順や管理体制の整備、及び設備増強など長期的な視点での対策

◎IT障害事象の種別と対応メニュー、エスカレーション及び対応指示ルールの策定、及び事業者とベンダーが連携して検証できる体制

3 ◎ふくそうや障害の影響拡大防止、早期復旧のため、事業者間の連絡体制や設備を融通できる体制整備並びに広域災害対応を考慮した事業者間およびベンダー連携体制の確立

4 ◎サイバー攻撃、事故情報、ふくそう情報等を関係者から広く収集して対策を立案、情報公開する体制の整備

（６）重要情報漏えいに対する責任体制・管理体制の整備

1 ◎重要情報の管理責任者・体制の整備、及び重要情報の運用方法の指針の整備。また、内部・外部監査による実施

検討の方向性（2／ 9）

柱２．取扱い情報の管理の明確化

重要度に応じた適切な措置をするために、　　取り扱う情報に対して、種類や責任等を明確化。

- （1）情報システム、取扱情報に対する責任と情報の分類
  - 1 ◎情報の管理レベル、取扱規定、管理責任者の設定など内部統制ルールの整備・適宜見直し
    ◎保守マニュアルなど紙、保管、参照権限、廃棄手段の明確化と情報に応じた利用者アクセスの管理など管理基準の策定
  - 2 ・ネットワーク内の装置類やサービスの属性に応じた情報の分類
- （2）サイバー攻撃に備えたサーバ等に格納された情報管理
  - 1 ◎情報の暗号化、パスワードや有効期限の設定などのアクセス権制御対策など、情報の秘密を確保する対策・手順の明確化

検討の方向性（3／ 9）

柱３．情報通信ネットワーク管理要件の明確化

障害や情報の重要度に応じた、満たすべき情報通信ネットワーク管理要件の明確化。

- （１）情報通信ネットワークのセキュリティ管理
  - １・ソフトウェア選択基準の明確化
  - ２◎アクセス集中時のブロック、負荷分散機構等ネットワークのＩＰ化への対応
  - ３◎問題発生時に検知、通報させる機能や体制の確立
  - ４・他の利用者へ悪影響等を与えているユーザーに対する契約の破棄の明確化
- （２）利用者アクセスの管理
  - １◎パスワード設定ルールや利用者認証方式等、利用者のアクセス管理の確実化
  - ２・アクセスログの取得、適切な保管
  - ３・ブラックリスト等の事業者間共通管理レベルの明確化
- （３）ネットワークアクセス制御
  - １・証明書発行、管理、有効期限の設定など強固な認証サーバの導入
  - ２◎ネットワーク防御のための端末の要件の明確化
  - ３・事業者間相互接続における不正アクセスの流入・流出の対策
- （４）サイバー攻撃対策
  - １◎攻撃元を特定できるネットワーク・端末の機能の検討、及び攻撃元のトラヒックを遮断する仕組み
    ◎発信元を偽装することを防ぐ機能の実現
- （５）ネットワーク輻輳対策
  - １◎ふくそうの検出、ふくそうレベルに応じた規制、事業者間の切離しに関する機能の実現
  - ２◎ふくそう検知後の規制実施方法などのノウハウの蓄積
  - ３◎画像コンテンツなど高トラヒックの規制・遮断
    ◎著作権のあるコンテンツに関する利用方法のガイドライン、著作権の侵害があるトラヒックの規制
- （６）重要通信の確保
  - １◎重要通信の対象機関の適正化、及び重要通信の取扱いの明確化
  - ２・汎用機器で構成されるIPネットワーク上で重要通信を確保するため、各階梯・機器に具備すべき最低限の機能について検討、関係者間での認識の共通化
  - ３・大規模災害発生時の緊急通報の設備容量不足への対応
  - ４◎ふくそう/規制時のIP電話の緊急通報等の確実な確保
  - ５・誰もが容易に緊急通報できる手段の確保
- （７）重要情報漏えい対策
  - １◎ファイル交換ソフトなどによる情報漏えい対策
  - ２・接続ネットワークに応じた適切な端末管理

検討の方向性（4／ 9）

柱４．情報通信ネットワークについての対策

情報通信ネットワーク管理要件に対応した対策項目を、装置やシステムごとに明確化。

（1）セキュリティを保つべき領域での物理的管理	1 ・セキュリティを保つべき領域の基準の明確化 ・重要度に応じた入出管理の導入
（3）需要予測に基づく、システムの容量の適切な計画・設計	1 ◎ルータ等設備に対する最低限の品質基準の策定
	2 ◎将来の利用動向に対応できる設備計画の策定など障害の拡大防止、極小化対策に関する設計指針等の対策の策定
	3 ・ベンダーによりブラックボックス化されたシステムを用いる場合における、事業者が行う検査手法、品質評価手法の確立
	4 ◎網の信頼性基準・指標の策定、実網の定期点検等の運用方法の策定
	6 ・サーバ等機器の事前機能確認の充実
	7 ◎ネットワークの重要障害を検証するための設備、手段、条件、シミュレーション方式、結果の報告ルールなどの策定と標準化
（4）開発及びサポートプロセスにおける管理	1 ・通信設備のソフトウェアのパッチ、セキュリティパッチの適用に関する運用方法の確立
	2 ・端末系の自動ダウンロードソフトのバグによる障害波及防止対策の策定
	3 ◎実ネットワークに近いテスト環境の整備、ネットワーク実運用時の挙動の事前検証
	4 ・なりすまし、改ざん、不正アクセス、盗聴、情報漏えい、フィッシングなど脅威の明確化、及び脅威に対するシステムファイルの保護手段などの対策
	5 ・セキュリティチェックのためのチェック体制
（5）故障検出、動作ログ取得などによる監視	1 ◎IP化に対応するためのネットワークの早期異常検知と機能等の設備監視技術と装置の予備系への自律切替などの研究開発
	2 ・故障原因解析における事業者とベンダーの連携
	3 ・原因の究明を迅速に行うための分析技術の研究開発
	4 ・運用監視体制の充実
（6）サイバー攻撃に備えた設備等に関する脆弱性への対策	1 ◎エンドユーザーの機器(例えば、ブロードバンドルータ)がサイバー攻撃の踏み台にされ、事業者のサーバ等の電気通信設備を攻撃するリスクを軽減するための、機器ベンダーによる出荷品質検査の推奨
	2 ・事業者間接続におけるIP化されたPOIへのサイバー攻撃への対策
	3 ◎内部統制、社内ルールの適時見直し、新手の攻撃に対するハード／ソフト対策の体制強化

検討の方向性（5／ 9）

柱４．情報通信ネットワークについての対策

情報通信ネットワーク管理要件に対応した対策項目を、装置やシステムごとに明確化。

（７）通信トラヒック量の観測などネットワーク輻輳対策

1 ◎トラヒックの監視、ボトルネックの把握、閾値の管理、ネットワークのリソース管理に加えて、通信トラヒック量以外の観測項目の検討や、観測・分析結果の全事業者間の共有

2 ◎安全かつ容易な設備増強、拡張性確保の設計指針の策定

3 ◎IPネットワークのふくそうが起きる前の予測・回避技術の研究開発、ふくそう発生時に問題箇所を迅速に把握する機能の研究開発

4 ・ふくそう時のユーザー間の公平性の確保

5 ◎企画型ふくそうを防止するための、企画の情報収集の仕組み

（８）バックアップ、分散化など故障・災害等ＩＴ障害対策

1 ◎予備電源の設置について、設備規模に応じた具体的な動作時間の設定

2 ◎分散化、予備機配備、冗長化、迂回経路設定など具備すべき基準の策定

3 ・地下鉄構内等公共施設に設置されている携帯電話基地局等の予備電源の確保

4 ◎IP端末（特に電話端末）の給電対策

5 ◎停電後、復電時に生じる地域単位のセッションリクエストによるネットワークへの過負荷を分散させる仕組み

6 ・クラスタを使用したサーバの冗長系について、冗長系自動切替え機能の強化やリモート対応で電源OFFする仕組み

7 ・定期的なソフトウェアのリスク分析とバージョンアップの計画

8 ・機器単体保守契約からシステム的保守契約への移行

9 ◎固定電話網相当のふくそう、故障通知機能の検討や、共通線信号方式の網管理機能を参考にした、キャリアにまたがる網管理機能の実装

10 ◎SIPサーバについて、地域ごとに設置されている交換機と同等レベルで、障害時の影響範囲を限定する手法

11 ◎広域災害時の被災範囲などの情報連携や事業者間の相互補完の仕組み

12 ◎災害時におけるユーザーの振る舞い、端末の挙動がネットワークに与える影響の事前検証

13 ◎コロケーション先の電気通信設備の保護

14 ・工事の際、工事実施者とネットワークの運用者による、工事実施体制の確認や工事手順の策定

15 ・保守点検の手順書の作成、定期的な見直し

検討の方向性（6／ 9）

重点１．ＩＴ障害の観点から見た事業継続性確保のための対策

（1）事業継続管理における情報セキュリティの側面	1 ◎事業継続リスクアセスメントのためのチェック項目、評価基準の策定や監査の仕組み
（2）情報等の管理・障害検知・切り分け	1 ◎故障箇所の特定及び故障原因の特定の迅速化対策
	2 ◎検証試験等に活用するためのデータとして、障害時の集中呼のパターンを再現できる試験方法の確立
	3 ◎IP網における相互接続性を十分に確保するための試験・検証
	4 ◎障害事例、故障検知等のノウハウの蓄積及び事業者間の情報共有の仕組みづくり
	5 ・再発防止の観点から事業者とベンダー間の情報共有体制の確立、行政機関による検査の実施
	6 ◎ソフトウエアのパッチ、セキュリティパッチの適用に関する運用方法の確立、ベンダーとの保守契約に基づく体制の確立
	7 ◎ネットワークの統合的な監視システム・体制の構築
	8 ◎故障箇所特定のためのデータ取得手順、切り分け手順等の整備
	9 ◎迅速な原因分析のための事業者とベンダーの連携体制の確立
（3）緊急時の情報連絡（迅速な連絡・対応体制）	1 ◎社会的影響の変化にともなう事故報告基準の見直し及び明確化
	2 ◎障害状況等の多様なメディアによる利用者への提供
	3 ◎サービス階層をまたがるユーザーへの障害情報等の提供
	4 ◎利用者等への対外的な告知基準の策定
	5 ◎円滑な災害対応等を行うための事業者間の連携体制
	6 ◎単独の事業者で対応不可能なサイバー攻撃に対する対応
	7 ◎故障原因の探求に関して事業者、ベンダー間の連携強化
（5）サイバー攻撃対策	1・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の策定
	2・サイバー攻撃発生時の国レベルでの迅速な情報共有方法（国への報告ルール）やサイバー攻撃に備えた監視項目の明確化、監視体制の整備、ソフトウェアパッチなど運用方法の確立
	3・攻撃利用回線を特定するための通信内容の確認について根拠となる法令の整備及び攻撃元事業者への攻撃停止措置の要請、攻撃元事業者での措置の実施ルールの策定
	4 ◎IPネットワークで送信元アドレスを容易に偽装されることを防ぐ対策、及び偽装されても送信元を特定できる機構（攻撃元特定のための手段、収集情報、蓄積）の導入
	5 ・定期的な専門機関による脆弱性診断と対策の検討

検討の方向性（7／ 9）

重点１．ＩＴ障害の観点から見た事業継続性確保のための対策

（６）ネットワーク輻輳対策（迅速な連絡・対応体制）

1 ◎ふくそうの波及防止を考慮した対応手順の整備（波及：ネットワーク内への波及、他アプリケーションへの波及など）及びふくそうを事前に防止するための設備増強など長期的視点の対策の実施

2 ・旧来のネットワークシステムで用いられた現用・予備によるバックアップ体制にとらわれない対応策の検討

3 ◎ふくそう発生時にユーザー端末等にシステム的に通知し、ふくそう拡大を防止する技術の開発や検討（発信規制や再送制御防止など、IP電話であればサーバ負荷にならない手法など)並びにこれらの規格化

4 ◎災害用伝言ダイヤル等の利用によるふくそう軽減策

5 ・ふくそう監視手法や事業者間連携情報項目の明確化

6 ・１つのノードにおけるトラヒック集約度合い等を考慮した、当該ノードが具備すべき輻輳対策（個別ノードが具備すべき機能、事業者が整備すべき対策手順）の検討

（７）故障・災害等ＩＴ障害対策（迅速な連絡・対応体制）

1 ◎システムの冗長化やセンタ分散化等の障害対策に関わる設備投資に対する税制優遇等の支援措置並びに通信経路等のシステムの冗長確保及びノード毎に具備するべき機能や配備するべき冗長構成の検討

2 ・電話、インターネット等のサービス毎のネットワーク分離又は帯域分離

3 ・障害発生箇所の特定の迅速化を図るため設備構成のシンプル化及び小規模分散化等の検討

4 ・端末の電力確保、バッテリ寿命延長の技術開発

5 ・稼働状態でメンテナンスを可能とするシステムの実現（IP電話）

6 ◎IP伝送設備の機能集約の簡便性やオープン性を考慮した、故障・災害時の加入者保護並びに他事業者設備への影響を最低限に抑えるための対応・復旧手順を明確化

7 ・大規模災害に備えた復旧ケーブルの確保等、資材備蓄等の支援

（８）重要情報漏えい対策

1 ・情報漏洩後の二次被害を最小化するため、情報を取得したことが明らかなユーザへの対応(削除依頼等)について事業者で共通・統一的の見解をまとめることの検討

検討の方向性（8／9）

重点２．情報漏えい防止のための対策

- （１）媒体の取扱い
  - １ ◎ベンダーに送付する故障物品内に格納された情報の漏えいを防止する観点での対策手順の明確化
    ◎事業者からベンダーに送付されたサーバの障害ログ媒体の扱いの取り決め防止する観点での対策手順の明確化
  - ２・媒体の種類に応じた廃棄処分方法の明確化
- （２）情報の交換
  - １・保守、他作業用端末(PC)などの使用基準、セキュリティ対策基準、情報コピーの制限など管理基準の策定、監査機能の設置
- （３）重要情報漏えい対策
  - １・情報漏洩に対する技術的・人的な対策方法や考え方について事業者間の情報・意見交換の場の設定
  - ２・個人情報以外の重要な設備情報（特に他社のセキュリティ情報等）の漏えいについての報告

重点３．外部委託における情報セキュリティ確保のための対策

- （１）秘密保持
  - １・外部委託先の会社の情報セキュリティレベルを客観的に知ることのできる情報セキュリティマネジメントシステム（ＩＳＭＳ）の認証制度の普及、および委託業務のセキュリティ要求度の高いものは、ＩＳＭＳの認証取得企業であることを条件とするなどの委託会社の選別
  - ２・守秘義務契約、誓約書、情報管理規定の保持
  - ３・定期内部及び外部監査の実施、及び監査チェック項目と是正処置のための指針の策定
- （２）外部組織
  - １・守秘義務事項、対象の洗い出し
    ・情報漏えい防止のための外注業者、派遣者への教育強化、誓約書提出及び誓約内容の見直し
- （４）重要情報漏えい対策
  - １・セキュリティルームの整備、不正コピー、持ち出しの監視ツールの導入等の整備
    ・PCの内部からの完全削除のルールなど委託終了時のルールについて明確化

検討の方向性（9／9）

その他

（1）障害者、高齢者、子供が安全に使える仕組みや技術の開発	1 ◎誰でもが平等に情報が共有できるようなインフラ整備についての検討 ◎IP電話端末等のアクセシビリティに関するガイド整備
（3）IPネットワークにつながる端末要件の明確化/法規制化	1 ◎IPネットワークにおいては、ネットワーク側のみ対処しても完全ではなく、端末を含めて考える必要があることを考慮した、IP網に接続される端末への要求条件の明確化
（4）公共施設設備での安全確保	1 ◎運用支援システムへの設備投資支援
	2 ・データ設定ミス等をなくすための警察、消防等への緊急通報接続システムのデータ共有化
（5）国際標準動向を意識した施策の制定、および、国際標準化での日本発の活動の活性化	1 ・情報フィルタリングの条件の基準化 ・携帯電話事業者とインターネットにおけるメール接続基準作成の検討