資料６－２

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

安全・信頼性検討作業班報告

～「ネットワークのIP化に対応した安全・信頼性対策（案）」～

IP ネットワーク設備委員会　安全・信頼性検討作業班報告

目次

Ⅰ　審議事項

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（以下「委員会」という。）では、平成 17 年 11 月より、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 10 月 31 日諮問）について審議を行ってきた。本報告は、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、情報通信ネットワークの安全性・信頼性向上に関する事項の検討結果についてまとめたものである。

Ⅱ　委員会及び作業班の構成

委員会の構成は、別表 1 のとおりである。

審議の促進を図るため、委員会の下に、安全・信頼性検討作業班を設置して検討を行った。安全・信頼性検討作業班の構成は、別表 2 のとおりである。

Ⅲ　審議経過

安全・信頼性検討作業班の設置以降、これまで、委員会 3 回及び作業班 8 回の会合を開催して審議を行い、ネットワークの安全性・信頼性向上に関する事項を報告書として取りまとめた。

⑴　委員会での検討

①　第 3 回委員会（平成 18 年 8 月 29 日）

災害や、通信機器の故障等による通信障害（以下「事故」という。）に対する審議の促進を図るため安全･信頼性対策を専門的に検討する安全・信頼性検討作業班の設置を決定した。

また、技術検討作業班における検討状況について報告を受け、IP ネットワーク設備の技術的課題に関する検討の方向性について審議を行った。

②　第 4 回委員会（平成 18 年 12 月 4 日）

安全･信頼性検討作業班における検討状況について報告を受け、ネットワークの安全･信頼性を確保するための検討課題について審議を行った。

また、技術検討作業班におけるこれまでの審議を取りまとめた報告を受け、技術的条件案について審議を行った。

③ 第 5 回委員会（平成 19 年 1 月 10 日）

安全・信頼性検討作業班における検討状況について報告を受け、ネットワークの安全・信頼性対策の検討の方向性について審議を行った。

また、技術検討作業班の報告に関する意見募集の結果を踏まえ、委員会報告及び一部答申（案）を取りまとめた。

(2) 安全・信頼性検討作業班での検討

① 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。

② 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。

③ 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。

④ 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。

⑤ 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等、検討の方向性について審議を行った。

⑥ 第 6 回安全・信頼性検討作業班（平成 19 年 3 月 1 日）

検討課題に対する具体的な取組みについて審議を行った。

⑦ 第 7 回安全・信頼性検討作業班（平成 19 年 3 月 29 日）

作業班報告書の骨子（案）について審議を行った。

⑧ 第 8 回安全・信頼性検討作業班（平成 19 年 4 月 10 日）
作業班報告（案）ついて審議を行った。

（参考）

0AB～J 番号を使用する IP 電話の基本的事項について、委員会に別途設置している技術検討作業班において検討を行っているところである。

技術検討作業班での検討は、以下のとおりである。

① 第 1 回技術検討作業班（平成 17 年 11 月 29 日）
技術検討作業班の運営方針、審議方針やネットワークの IP 化に関する動向と課題について審議を行った。

② 第 2 回技術検討作業班（平成 17 年 12 月 21 日）
ネットワークに求められる要求条件の整理及び技術基準における課題と論点について審議を行った。また、技術的条件の審議において次世代 IP ネットワーク推進フォーラムと連携していくこととした。

③ 第 3 回技術検討作業班（平成 18 年 1 月 17 日）
次世代 IP ネットワークに求められる要求条件について審議を行った。

④ 第 4 回技術検討作業班（平成 18 年 2 月 16 日）
IP ネットワーク設備の技術的条件について、検討項目を抽出するための審議を行った。

⑤ 第 5 回技術検討作業班（平成 18 年 3 月 29 日）
IP ネットワーク設備の技術的条件について、検討項目を抽出するための審議を行った。

⑥ 第 6 回技術検討作業班（平成 18 年 6 月 27 日）
IP ネットワーク設備の技術的条件に関する検討項目の方向性について審議を行った。

⑦ 第 7 回技術検討作業班（平成 18 年 9 月 21 日）
IP ネットワーク設備の技術的条件に関する検討の方向性について審議を行った。

⑧ 第 8 回技術検討作業班（平成 18 年 10 月 31 日）

IP ネットワーク設備の技術的条件に関する作業班報告骨子（案）について審議を行った。

⑨ 第 9 回技術検討作業班（平成 18 年 11 月 21 日）

技術検討作業班報告（案）について審議を行った。

⑩ 第 10 回技術検討作業班（平成 19 年 4 月 2 日）

これまでの審議経緯とともに、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以外の主な課題と論点について審議を行った。

Ⅳ　審議結果

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」のうち、ネットワークの安全性・信頼性向上に関する事項について、別紙のとおり作業班としての報告を取りまとめた。

別表 1

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　構成員

（敬称略　五十音順）

	氏　名	所　属
主　　査	後藤（ごとう）　滋樹（しげき）	早稲田大学　理工学部　教授
主査代理	相田（あいだ）　　仁（ひとし）	東京大学大学院　新領域創成科学研究科　教授
	相澤（あいざわ）　彰子（あきこ）	国立情報学研究所　教授
	池田（いけだ）　　茂（しげる）　(～H18.10)	情報通信ネットワーク産業協会　専務理事
	五十川（いそかわ）　洋一（よういち）	日本電気（株）　執行役員 ブロードバンドネットワーク事業本部長
	稲田（いなだ）　修一（しゅういち）　(H18.9～)	（独）情報通信研究機構　理事
	歌野（うたの）　孝法（たかのり）	（株）エヌ・ティ・ティ・ドコモ　取締役 常務執行役員　研究開発本部長
	江﨑（えさき）　　浩（ひろし）	東京大学大学院　情報理工学系研究科　教授
	大塚（おおつか）　隆史（たかし）　(～H18.9)	（社）日本 CATV 技術協会　常任副理事長
	沖中（おきなか）　秀夫（ひでお）	ＫＤＤＩ（株）　執行役員　技術渉外室長
	加藤（かとう）　　徹（とおる）	（株）ジュピターテレコム　取締役　商品戦略統轄部長
	河内（かわうち）　正孝（まさたか）　(～H18.9)	（独）情報通信研究機構　理事
	窪田（くぼた）　美男（よしお）	（独）国民生活センター　情報分析部システム管理室　室長
	小林（こばやし）　昌宏（まさひろ）　(～H18.1)	（株）パワードコム　常務執行役員 マーケティング・商品統括本部長
	志岐（しき）　紀夫（のりお）	（社）テレコムサービス協会　常任理事　ＶｏＩＰ推進協議会会長
	杉本（すぎもと）　晴重（はるしげ）	沖電気工業（株）　常務取締役　ＣＴＯ
	資宗（すけむね）　克行（よしゆき）　(H18.10～)	情報通信ネットワーク産業協会　専務理事
	竹村（たけむら）　哲夫（てつお）	（株）日立製作所　情報通信グループ　グループ長付
	津田（つだ）　俊隆（としたか）　(H18.8～)	富士通研究所（株）　常務取締役
	土森（つちもり）　紀之（のりゆき）	（株）ケイ・オプティコム　常務取締役
	所（ところ）　眞理雄（まりお）	ソニー（株）　特別理事
	中村（なかむら）　　隆（たかし）　(～H18.8)	富士通（株）　経営執行役
	橋本（はしもと）　　信（しん）	日本電信電話（株）　常務取締役 第二部門長
	平井（ひらい）　正孝（まさたか）	（財）電気通信端末機器審査協会　専務理事
	藤咲（ふじさく）　友宏（ともひろ）　(H18.9～)	（社）日本 CATV 技術協会　常任副理事長
	堀崎（ほりさき）　修宏（のぶひろ）	（社）情報通信技術委員会　専務理事
	水谷（みずたに）　幹男（みきお）	パナソニック　コミュニケーションズ（株）　副社長ＣＴＯ

	三膳　孝通（みよし　たかみち）	（株）インターネットイニシアティブ　取締役　戦略企画部　部長
	山崎　吉一（やまさき　よしかず）	ソフトバンクモバイル（株）　モバイルネットワーク本部 業務執行役員　コアネットワーク設計部長
	大和　敏彦（やまと　としひこ）	シスコシステムズ（株）　執行役員　ＣＴＯ アライアンス･アンド･テクノロジー担当
	弓削　哲也（ゆげ　てつや）	ソフトバンクテレコム（株）　専務執行役　ＣＴＯ　研究所長 兼　接続本部長
	渡辺　武経（わたなべ　たけつね）	（社）日本インターネットプロバイダー協会　会長

別表 2

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　安全・信頼性検討作業班　構成員

（敬称略　五十音順）

	氏　名	所　属
主　任	相田（あいだ）　仁（ひとし）	東京大学大学院　新領域創成科学研究科　教授
	井手（いで）　正広（まさひろ）	（株）ケイ・オプティコム　通信サービス技術本部 技術運営グループ　運営チーム　チームマネージャー
	稲田（いなた）　晃典（あきのり）(H18.10～)	（株）ＮＴＴドコモ　ネットワーク本部 コアネットワーク部 コアネットワーク企画担当部長
	永楽（えいらく）　昌大（まさとも）	ソフトバンクモバイル（株）　業務執行役員　保全運用部長
	榎本（えのもと）　洋一（よういち）	ソフトバンクテレコム（株）　ネットワーク本部 高度ネットワーク部長
	雄川（おがわ）　一彦（かずひこ）	日本電信電話（株）　第二部門次世代ネットワーク推進室 担当部長
	笠井（かさい）　康伸（やすのぶ）	（株）ジュピターテレコム　商品戦略本部長補佐
	北川（きたがわ）　和雄（かずお）	（社）日本ＣＡＴＶ技術協会　規格・標準化委員会　幹事
	倉澤（くらさわ）　聡（さとし）	沖電気工業（株）　ネットワークシステムカンパニー ネットワークシステム本部　サービスプラットフォームＳＥ部長
	久留島（くるしま）　豊（ゆたか）	社団法人　電気通信事業者協会　安全・信頼性協議会　会長
	齋藤（さいとう）　保夫（やすお）	（財）電気通信端末機器審査協会　機器審査部　主幹
	高尾（たかお）　俊明（としあき） (～H18.10)	（株）ＮＴＴドコモ　研究開発本部 研究開発推進部　担当課長
	高村（たかむら）　幸二（こうじ）	（株）日立製作所　品質保証本部 ネットワークソリューション品質保証部　部長
	東方（とうほう）　幸雄（ゆきお）	社団法人　電気通信事業者協会　安全・信頼性協議会
	中西（なかにし）　廉（やすし）	情報通信ネットワーク産業協会　ＮＧＮ－ＩＰ　ＷＧ委員
	萩原（はぎわら）　隆幸（たかゆき）	シスコシステムズ（株）　サービスプロバイダー営業 サービスプロバイダーシステムエンジニアリング本部長
	平原（ひらばる）　正樹（まさき）	独立行政法人　情報通信研究機構 新世代ネットワーク研究センター ネットワークアーキテクチャグループ　グループリーダー
	益田（ますだ）　淳（すなお）	ＫＤＤＩ（株）　運用統轄本部　設備運用本部　運用企画部長
	松本（まつもと）　隆（たかし）	日本電気（株）　キャリアネットワークビジネスユニット 主席技師長

	三膳（みよし）　孝通（たかみち）	（株）インターネットイニシアティブ　取締役　戦略企画長
	茂木（もぎ）　克之（かつゆき）	富士通（株）　ネットワークサービス事業本部 FENICS システム統括部　担当部長
	持麾（もちざい）　裕之（ひろゆき）	（社）テレコムサービス協会　技術・サービス委員会副委員長

別紙

目次

第 1 章　ネットワークの IP 化の現状と動向

我が国では、情報通信分野における急速な技術革新や、競争政策等の推進により、世界最速で、かつ、最も低廉なブロードバンド環境が実現し、インターネット・プロトコル（IP）を利用した IP 電話等の新しい ICT サービスが急速に普及・拡大している。

国内外の主要な電気通信事業者（以下「事業者」という。）においても、従来の従来の電話ネットワークを IP ネットワークに移行する計画を相次いで打ち出しており、また、各国が国際電気通信連合（ITU）等における国際標準化活動に戦略的に取り組むなど、次世代 IP ネットワークの実現に向けた動きが活発化している。

その一方、このようにネットワークの IP 化が進展し、様々な新しい IP 系サービスの利用が拡大する中で、昨今、IP 系サービスにおける通信障害などの事故件数が増加する傾向にある。また、事故の特徴についても、従来の電話ネットワークとは異なってきており、①人為的要因による事故の増加、②ソフト的な不具合に起因する事故の増加、③事故の大規模化と復旧の長時間化といった傾向が顕れてきている。

これらの状況を踏まえ、当審議会では、ネットワークの IP 化に対応した安全・信頼性の確保のための対策について審議を進めてきたものである。

1.1　IP ネットワークを巡る現状とその動向

(1)　ブロードバンドサービスの普及状況

我が国では、情報通信分野における急速な技術革新や、競争政策等の推進により、図 1-1 にあるようにブロードバンド環境が急速に普及・進展している。

特に、昨今では、これまで我が国のブロードバンド化を牽引してきた DSL やケーブルインターネットといった比較的廉価なサービスにかわり、高速な光ファイバサービス（FTTH）の加入者が加速度的に増加しており、今後も、我が国のブロードバンド環境は一層の高度化が進展していくものと見込まれている。

また、これに伴い、このような高度なネットワーク環境を利用した新しい IP 系サービスが急速に普及・拡大している。

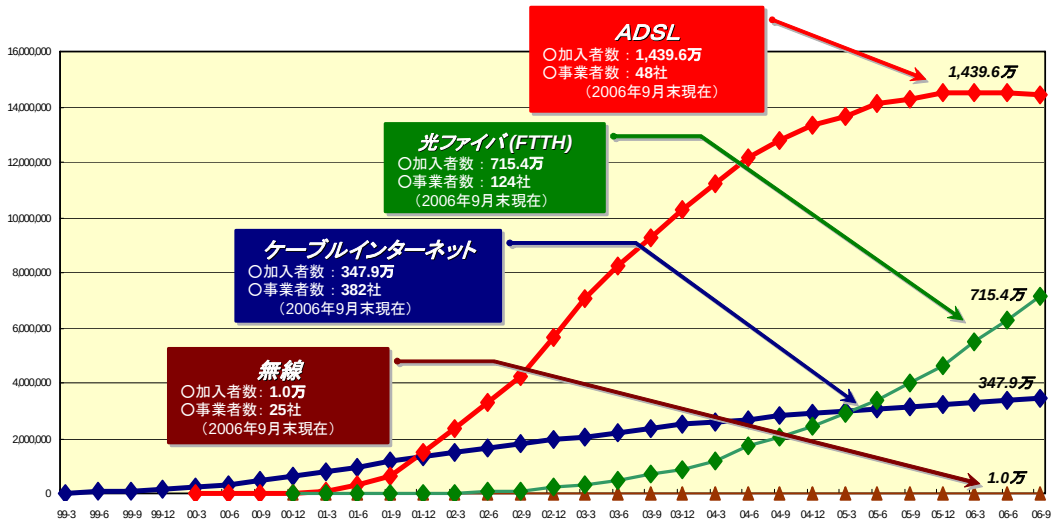


図 1-1　ブロードバンドサービスの加入者

(2)　IP 電話サービスの現状と動向

ブロードバンドサービスの進展とあいまって、我が国においては、他国に先駆けて IP 電話サービスの本格的な普及が始まっており、図 1-2 に示すとおり、平成 18 年 12 月末現在で利用者数が 1,375 万を超えている状況にある。

なお、我が国においては、IP 電話サービスに用いられる電気通信番号は、以下の 2 種類が存在する。

ア　0AB～J 番号

技術基準や緊急通報（110 番、119 番等）などについて、アナログ電話と同等の要件を満たす IP 電話サービスに指定されるもの

イ　050-CDEF-GHJK 番号（以下「050 番号」という。）

電話として利用できる最低限の品質を有し、地理的識別性を有しない（ロケーションフリーで利用可能である）IP 電話サービスに指定されるもの

このうち 050 番号については、利用番号数が平成 18 年 12 月末現在で 1,040 万に達しているものの、ここ 1 年程度はほぼ横ばいとなっている。

一方、従来の固定電話と同じ電話番号体系である 0AB～J 番号を使用する IP 電話については、利用番号数は平成 18 年 12 月末現在で 335 万に達しており、現在、急速に普及・拡大しているところである。

今後とも、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 電話は急速に普及・拡大していくものと予想される。

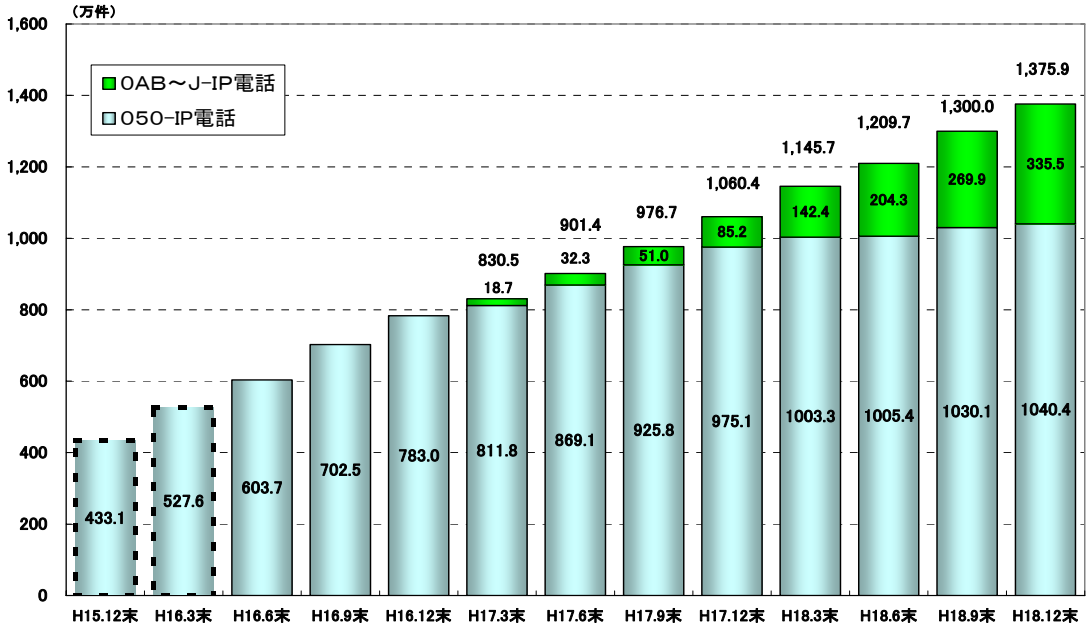


図 1-2　IP 電話の利用数の推移

(3)　ネットワークのＩＰ化の動向

本章の冒頭で述べたように、IP 系サービスの急速な普及と合わせて、国内の主要な事業者が、従来の電話ネットワークを IP ネットワークに移行する計画を相次いで公表している。

日本電信電話（株）においては、2004 年 11 月に公表した中期経営戦略の中で、端末機器からネットワークまで一貫して IP 化したネットワークとして次世代 IP ネットワークを構築し、2010 年には 3,000 万（全契約者約 6,000 万）の利用者が次世代ネットワークにシフトすることとしている。また、次世代 IP ネットワークの本格導入に先立ち、2006 年 12 月より、技術確認等のためのフィールドトライアルを実施しており、その中でアプリケーション／端末におけるインタフェースや他網との相互接続条件等を提示しているところである。

KDDI（株）においては、2003 年 10 月に、FTTH により、映像、高速インターネット、高品質な IP 電話のトリプルプレイサービスを開始し、2004 年 9 月に固定電話網 IP 化計画を発表している。2005 年 2 月には、加入者電話回線（メタル回線）を IP ネットワークに直接接続し、2007

年度末までには IP によるソフトスイッチへの置換を完了させることとしている。

ソフトバンクテレコム（株）においては、2000 年に IP-VPN と VoIP サービスの複合サービスを開始し、2005 年に FTTH による映像、高速インターネット、高品質な IP 電話のトリプルプレイサービスを開始している。また、既存の固定電話の IP 化への置換えについても推進している。

1.2 安全・信頼性の確保に関する新たな課題

(1) 情報通信ネットワークの安全・信頼性確保に関する主な取組み

ICT サービスは国民生活や社会・経済活動を支える社会インフラとして、どのようなときにも安定的に利用できることが必要である。

このため、電気通信事業法においては、電気通信役務の円滑な提供の確保が法の目的に掲げられ、事業者に対するネットワーク設備の技術基準適合維持義務と、それを担保するための措置として管理規程の届出義務や電気通信主任技術者の選任義務が規定されているところである。

また、ネットワーク設備を持たない事業者も含めて、サービスの安定的な提供を確保するためのガイドラインとして、情報通信ネットワークの安全・信頼性基準が定められている。

さらに、政府全体としても情報セキュリティの確保のための取組みを推進しているところである。

平成 17 年 12 月には、情報セキュリティ政策会議（議長：内閣官房長官）において「重要インフラの情報セキュリティ対策に係る行動計画」が決定され、その中で

- 電気や水道等の重要インフラにおいて発生する ICT 障害が国民生活・社会経済活動に重大な影響を及ぼさないよう対策を講じる必要があるとして、「重要インフラにおける情報セキュリティ確保に係る『安全基準等』の策定」
- ICT 障害の未然防止、発生時の被害拡大防止・迅速な復旧及び再発防止を目的として、「重要インフラ毎の情報共有・分析機能（CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response）の整備」

等の計画が明確化されたところである。

このような中、平成 18 年 4 月に、事業者の情報セキュリティ対策を促進するとともに、事業者間の連携体制を強化することを目的として、

「電気通信分野における情報セキュリティ対策協議会」が設立され、同年 9 月には、同協議会が上記の行動計画を受けた「電気通信分野における情報セキュリティ確保に係る安全基準（第 1 版）」を策定したところである。また、電気通信分野の CEPTOAR（以下「T-CEPTOAR」という。）についても、同協議会で具体化に向けて検討が進められ、平成 19 年 3 月に整備されたところである。

(2) ICT サービスの事故の発生状況

従来の電話ネットワークから IP ネットワークへとネットワーク構造が変化する中で、事故の発生状況にも変化が見られるようになってきている。

実際に、事業者が電気通信サービスを停止した事故等の発生件数は、図 1-3 に示すとおり全般的に増加傾向にある。

なお、図中の「重大な事故」とは、電気通信事業法第 28 条に基づき総務大臣に報告された事故のことであり、「その他事故」とは、事業者が自主的に総務省に報告した事故を指す。

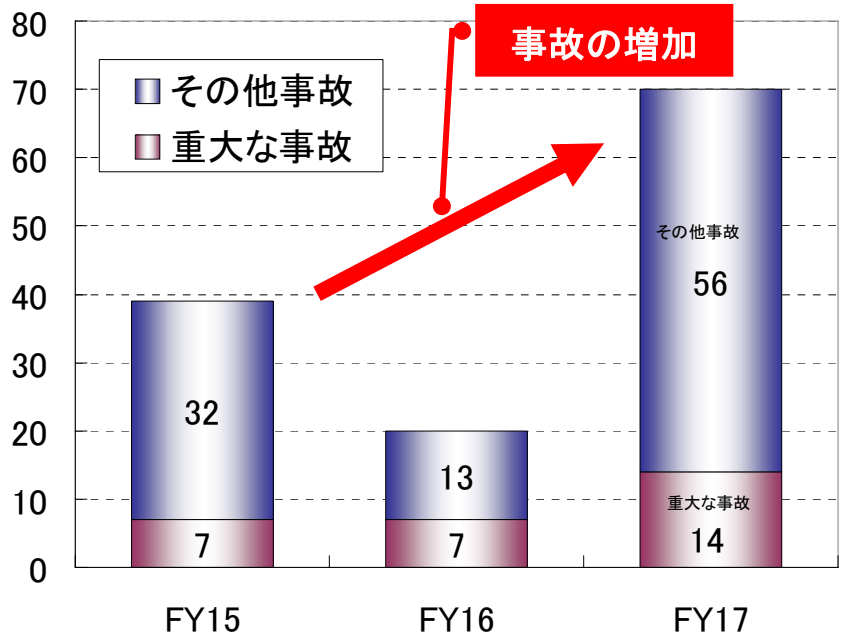


図 1-3　事故等の発生件数推移

また、事故等の発生件数をサービス別に分析すると図 1-4 のとおりとなる。IP 電話をはじめ様々な IP 系サービスが急速に普及すると同時に、IP 系サービスの事故が増加する傾向にある。

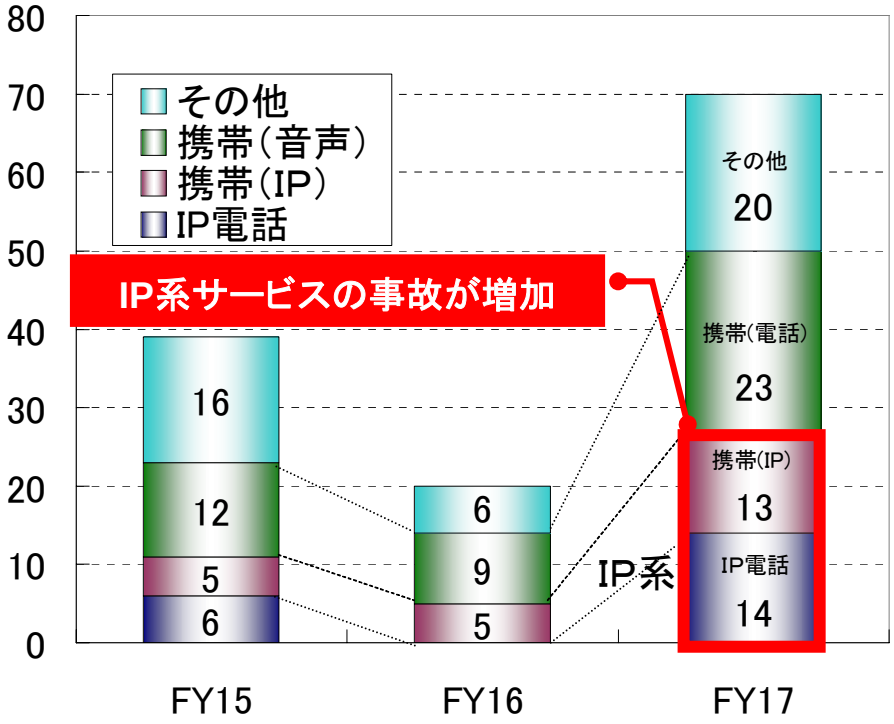


図 1-4　サービス別の事故等の発生件数推移

(3)　事故の発生規模と時間

上述したように IP 系サービスの事故が増加する傾向にあるが、その内容にも変化が見られる。

具体的には、従来の固定電話のサービスと比較すると、一回の事故で影響を受ける利用者の数が増加しているほか、復旧までにかかる時間が長時間化する傾向にある。（表 1-1、表 1-2 参照）

表 1-1　IP 系サービスにおける事故の規模（平成 17、18 年度）

影響を受けた利用者数	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	携帯等メール	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
29 万	近畿地方	携帯等メール	その他（1 時間 57 分）

22 万	近畿地方	IP 電話	その他（3 時間 1 分）
10 万	中国、四国、 九州地方	IP 電話	重大な事故
39 万	西日本エリア	IP 電話	重大な事故
230 万	全国	携帯等メール	その他（1 時間 58 分)
390 万	関東地方（東京都）	携帯等メール	その他（54 分間)
148 万	全国	メール	重大な事故
246 万	全国	携帯等メール	その他（遅延）
180 万	全国	携帯等メール	その他（遅延）
34 万	関西地方	携帯等メール	その他（遅延）
1,950 万	全国	携帯等 IP 接続	重大な事故
15 万	近畿地方	IP 電話	重大な事故
10 万	九州地方	IP 電話	重大な事故
951 万	北海道、東北、 関東、東海地方	携帯等 IP 接続	重大な事故
57 万	全国	メール	重大な事故
50 万	全国	携帯等 IP 接続	その他 （サービス品質低下）
100 万	全国	携帯等 IP 接続	重大な事故

表 1-2　IP 系サービスにおける復旧時のトラブル（平成 17、18 年度）

サービス種別	発生状況	影響時間
IP 電話	障害復旧の際、中継サーバへのアクセスが集中し回復までに時間を要した。	4 時間 04 分
メール	障害時に滞留した外部からのメールによりふくそう状態となり回復までに時間を要した。	79 時間 32 分
携帯 IP 接続	外部サーバの不具合により、DNS サーバへのバースト的なクエリが発生し、回復に時間を要した。	5 時間 41 分
IP 電話	障害により認証サーバの再立ち上げを行ったところ、認証サーバが過負荷となり回復に時間を要した。	7 時間 31 分
IP 電話	装置故障による復旧の際、認証サーバへのアクセスが集中し回復までに時間を要した。	7 時間 33 分
メール	障害時に滞留した外部からのメールによりふくそう状態となり回復までに時間を要した。	10 時間 10 分

(4)　事故の発生要因

(3)で述べたような変化が生じている大きな原因としては、IP 電話等のネットワークでは、1 台のサーバに多くのトラヒックが集中する傾向があることや、ふくそうの波及を防止するノウハウの蓄積が十分でないこと、さらに、ソフトウェアのバグが原因でその特定に時間を要することや、復旧作業中のミス等があげられる。

これらの中には、新しい技術である IP ネットワークへの移行の過渡期であるが故の事故であるケースが多く含まれている。

図 1-5 に発生要因別に実際の事故件数をまとめた。人為的要因による事故が平成 17 年度は 20 件（前年度 3 件）発生しており、件数、割合とも増加している。また、平成 17 年度の事故の発生要因は、図 1-6 に示すとおり、ソフトウェアの不具合やデータ設定ミス等に起因する事故が全体の半数以上の 39 件となっており、ソフト的な不具合等に起因する事故が多い。

さらに、表 1-3 に示すとおり、データ設定ミスに起因する事故のように、作業手順の策定や、作業時に確認を十分行うことで事故の発生を防止可能であったと推定される人為的なミスによる事故も発生している。

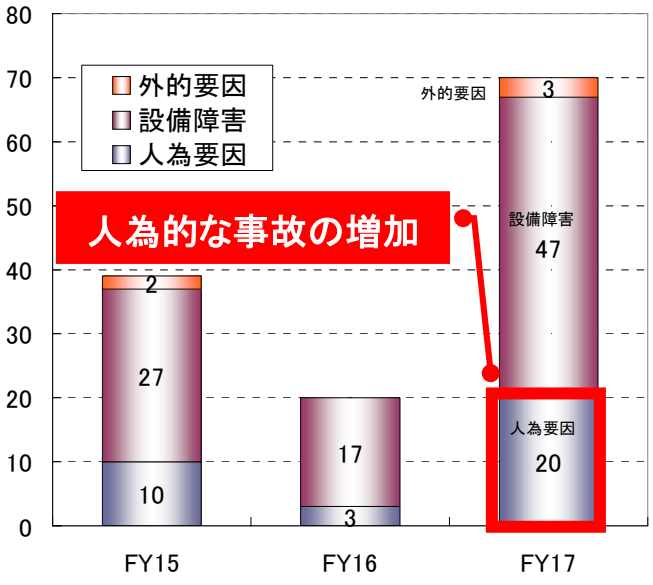


図 1-5　発生要因別事故等発生件数推移

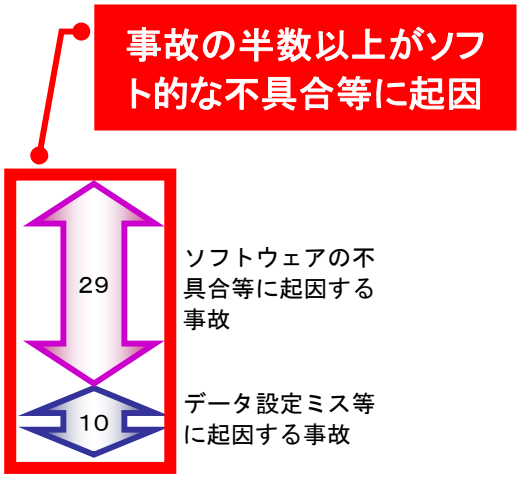


図 1-6　ソフト的な不具合等に起因する事故発生状況

表 1-3　人為的なミスによる事故発生状況（平成 17、18 年度）

サービス種別	発生状況	事故種別
携帯電話	交換機の設定変更ミスにより、特定事業者あての通話が利用できない状態になった。	重大な事故
空港 MCA	工事中に誤ってブレーカーを断とし、システム全断となった。	その他
専用線	他事業者光端子盤を誤って撤去し、光ファイバ 12 回線が約 5 時間にわたって不通となった。	その他
IP 電話	機器変更工事中の設定ミスにより IP 電話 2,500 回線が利用できない状況となった。	その他
携帯電話	基地局データ更新ミスにより携帯電話から緊急通報が一部地域で使えない状況となった。	その他
IP 電話 (0AB-J)	呼制御装置のデータ入力ミスにより、緊急通報が一部地域で使えない状況となった。	その他
IP 電話、ADSL	通信機器の設定ミスにより全国 3.2 万のユーザーが通話困難となった。	その他
携帯電話	基地局データ入力ミスにより携帯電話が一部地域で使えない状況となった。	その他
携帯電話	基地局データ入力ミスにより緊急通報が一部地域で使えない状況となった。	その他
ADSL 他	工事中の光ケーブルの誤切断により ADSL サービス等約 1.6 万回線が不通となった。	その他
IP 電話 (0AB-J)	緊急通報機関と未接続のままサービスを開始した。	その他

(5)　新たな課題の解決に向けて

これまで述べてきたように、現在、国内外の情報通信ネットワークの構造が、通信品質保証型の「従来の電話ネットワーク」から、ベストエフォート型のインターネットの技術をベースとした「IP ネットワーク」へと移行しつつある。

その結果、新しい IP 系サービスが次々と導入され利用者の選択肢が広がる一方で、これらのサービスにおける情報セキュリティやサービス品質の確保、さらには技術者の不足など、ネットワークの安全・信頼性の面で新しい課題が発生しつつある。

情報通信ネットワークが、社会インフラとしての機能を維持し、利用者の利益を損なうことのないよう、今まさにこれらの課題解決が急がれている状況にある。

第２章　安全・信頼性の確保のための重点対策

2.1　概要

第１章で述べてきたように、ネットワークの IP 化が進展する中、新しい ICT サービスが国民生活に急速に浸透しつつあり、社会経済活動を様々な形で支えている状況となっている。

その一方で、IP 電話やメールなどの IP 系サービスにおいては、サービス停止等の事故・障害が増加、長時間化する傾向にあり、また、人為的ミスやソフトウェアの不具合が原因となるなど、その内容や原因にも変化が見られる。

また、パソコンの普及やインターネットの利用の増加に伴い、固定電話の時代にはなかったサイバー攻撃に対する情報セキュリティの確保の問題も新しい社会的課題となっている。

このような状況の中で、利用者が安心して社会インフラである電気通信サービスを利用できるようにするためには、従来の固定電話のノウハウを活かしつつ、新しいネットワークに適切に対応した運用・管理を行うことが必要となっている。

このため、当審議会においては、ネットワークの技術革新に対応するため、現行のネットワークの安全・信頼性確保の対策について、改めて総合的に点検し、必要な見直しを行うこととしたものである。

電気通信事業法においては、ネットワークの安全・信頼性を確保するため、電気通信回線設備を設置する事業者に対して技術基準適合維持義務を規定し、ネットワーク設備の冗長化や局舎等建築物の安全確保、通信品質の確保等、設備面の技術基準を定めているところである。

また、同法では、これを担保するための措置として、ネットワークの管理面において、電気通信主任技術者の選任義務や管理規程の届出義務を課している。

このほかにも、総務大臣の告示において、全ての事業者を対象としたガイドラインとして、ネットワークの安全・信頼性基準が定められており、設備面、管理面を含めて各事業者が取り組むべき具体的な対策が定められているところである。

さらに、業界団体や各事業者の独自の検討により、安全・信頼性を確保するための対策が検討されている。

当審議会の検討においては、これまでの安全・信頼性対策が適切に実行されているにも関わらず、新しいサービスにおいて事故等が増加傾向にあることを踏まえ、まずは、最近の技術動向や事故等の分析を行い、設備面や運用・

管理面の安全・信頼性対策を一層充実させるとともに、組織・体制や人材育成といった、これまで事業者が独自に取り組んできた部分も含めて総合的に点検を行うことにより、必要な対策について議論を進めてきた。

具体的には、ネットワークの「設備面」、「運用・管理面」、それを実現する「体制面」を３本柱として、

① 新しいネットワーク技術に対応した社内体制の在り方とその実現のために必要な人材を確保するための方策

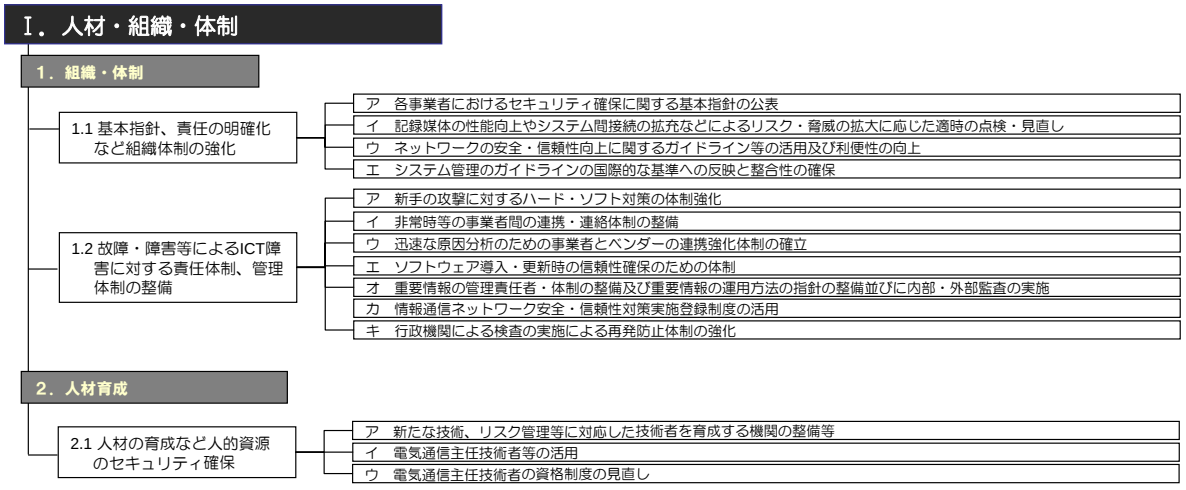
② 故障や障害を未然に防ぐとともに、実際に起きてしまったときには早急な復旧を実現するネットワークの運用・管理や、新しい技術に対応するための業界内の連携体制

③ ネットワーク機器の高度化・複雑化の進展やサイバー攻撃等の新たな脅威に対応するためのネットワークや端末等に求められる条件

等について、以下のとおり、特に重点的に取り組むべき課題について総合的に検討を行ったものである。

2.2 組織・体制、人材育成等に関する対策

事業者の社内体制のほか、事業者間や事業者とベンダー間など業界内の連携体制の整備など組織・体制に関する課題、新しい技術に対応した人材の育成や電気通信主任技術者の選任義務や資格制度の在り方など人材育成等に関する課題について検討を行った。

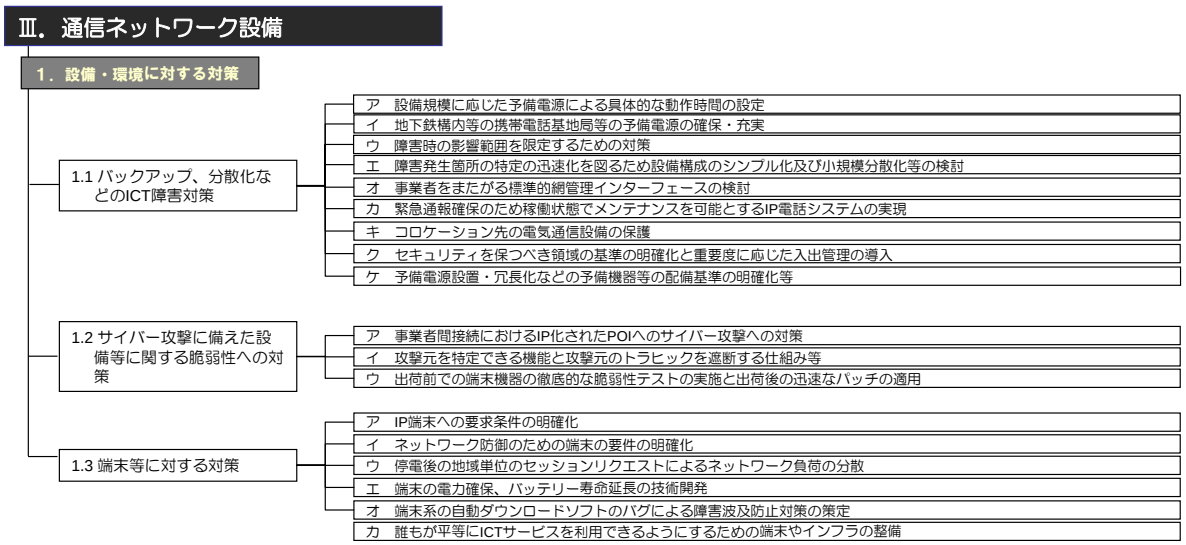


2.3　ネットワーク設備の運用・管理面に関する対策

ネットワーク設備の運用・管理面については、設備の運用前のシステム設計やシステム開発・工事に関する課題、故障対策やふくそう対策、緊急時の対応など設備の保全・運用管理に関する課題、サイバー攻撃や情報漏えいなどに対する情報セキュリティ管理に関する課題について検討を行った。

2.4　ネットワーク設備に関する対策

ネットワークのIP化に対応した電気通信設備の技術的条件について検討を行っている当審議会の IP ネットワーク設備委員会技術検討作業班の検討状況を踏まえ、設備の冗長化や予備電源の高度化等の対策や研究開発など安全・信頼性確保のために取り組むべき課題について検討を行った。



第３章　組織・体制、人材育成等に関する事項

3.1　組織・体制に関する検討

本項では、組織・体制に関する事項として、基本指針、責任の明確化など組織・体制の整備、故障・災害等による ICT 障害や情報漏えいに対する責任体制・管理体制の整備及び災害や障害対応訓練・演習の実施等について検討を行った。

3.1.1　基本指針、責任の明確化など組織・体制の整備

セキュリティ確保に関する基本指針、責任の明確化など組織・体制の整備に関して、以下の項目の対策が必要である。

ア　各事業者における情報セキュリティ確保に関する基本指針の公表
イ　記録媒体の性能向上やシステム間接続の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
ウ　ネットワークの安全・信頼性向上に関するガイドライン等の活用及び利便性の向上
エ　システム管理のガイドラインの国際的な基準への反映と整合性の確保

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主な対策は以下のとおりである。

(1) 各事業者における情報セキュリティ確保に関する基本指針の公表

近年、電気通信事業においてもコンピュータウィルス等や記録媒体の持ち出しによる情報流出などが絶えない状況にあり、これらが社会的な関心事項となっていることを踏まえ、各事業者はセキュリティ確保の基本指針や体制、その実施状況などをホームページや配布物などを通じて公表に努めることが適当である。

また、将来に向けて事業者共通の情報セキュリティ確保に関する基本指針の在り方、情報の取扱いルール及びそれらの公表について検討が必要である。

(2) ネットワークの安全・信頼性向上に関するガイドライン等の活用及び利便性の向上

国や業界団体等で定めているガイドラインの活用について周知徹底を図るとともに、技術革新やサービスの多様化、国際標準化の動向を考慮したガイドラインの作成、更新、複数ガイドラインの整理・統合などを検討する場を設ける必要がある。その中で「情報通信ネットワーク安全・信頼性基準（告示）」や「電気通信事業者における情報セキュリティ関連の安全基準やガイドライン」等複数存在しているガイドラインの改版・整理統合等の検討が必要である。

また、各事業者が、経験・蓄積している事故事例の特徴、再発防止策や電気通信サービスの提供者としての役割等に関して意見交換を行うとともに、事例検討等を通じて事業者間で用語の定義、障害検知の基準、発生時の連絡体制等の検討を深め、継続的にガイドラインの充実を図ることが必要である。

(3) システム管理のガイドラインの国際的な基準への反映と整合性の確保

ISO（国際標準化機構）等により、システム管理のガイドラインや技術基準が作成され、我が国では、これらの国際標準化動向を参照しながら情報セキュリティ関連の安全基準やガイドラインを作成している。

今後も国際標準化動向に合わせて、電気通信事業における情報セキュリティ関連の安全基準やガイドラインを適切に改版していくことが必要である。

また、日本から国際標準化活動に積極的に参加し、日本の技術を国際標準に反映するように取り組むことが必要である。

さらに、ネットワークを通じて必要なアプリケーションの機能を提供するサービスなど、ネットワークの高度化や技術革新により生まれる新しい電気通信サービスに関する情報セキュリティ対策等について、ネットワーク環境や市場、国際動向等の変化に応じて、随時対応することが必要である。

3.1.2　故障・災害等による ICT 障害に対する責任体制・管理体制の整備

故障・災害等による ICT 障害に対する責任体制・管理体制の整備に関して、以下の項目の対策が必要である。

ア　新手の攻撃に対するハード・ソフト対策の体制強化
イ　非常時等のサービス復旧のための緊急対応の手順や管理体制の整備

ウ　非常時等の事業者間の連携・連絡体制の整備
エ　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
オ　ソフトウェアの導入・更新時の信頼性確保のための体制
カ　情報通信ネットワーク安全・信頼性対策実施登録制度の有効活用
キ　行政機関による検査の実施による再発防止対策の確認

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主な対策は以下のとおりである。

(1) 新手の攻撃に対するハード・ソフト対策の体制強化

ネットワークシステムの脆弱性についての情報は機器の保守契約等を通してベンダーから事業者に提供されており、事業者が自社のネットワーク構成を踏まえリスク評価を行い、リスクに応じた対応をとっている。依然として、ネットワークシステムの脆弱性が発見されることが多い現状を踏まえ、それに対処できるように内部統制や社内ルールを随時見直し、新手の攻撃に対しても迅速にハード・ソフト両面で対処できる体制を確立・強化することが必要である。

しかしながら、事業者毎にネットワークの運用体制は異なっているため、具体的な体制を一律に規定することは難しい。そのため各事業者において自らの設備にふさわしい社内体制を構築することが適当である。

(2) 非常時等のサービス復旧のための緊急対応の手順や管理体制の整備

ネットワークの IP 化の進展に対応するため、ノウハウの蓄積が十分でないことを踏まえ、各事業者は、障害の対応マニュアルの整備や、災害時、重大故障時のサービス復旧のための緊急対応の手順や管理体制の整備を行うことが必要である。

具体的な対策などは各事業者が主体的に実施すべき事項であるが、故障対策、冗長設計のポリシーや基準など、通信事業者間・ベンダー間などで共通的に策定可能なものについて検討を行うことが必要である。

また、相互接続している事業者間の連携、緊急通報や重要通信の確保、故障状況の広報などの在り方については、事業者間で共通に運用可能なマニュアルの策定について検討を行うことが必要である。

さらに、新型インフルエンザなどの脅威による非常事態が発生した場合においても、国民の安全確保や社会経済活動の維持のために電気通信ネットワークが確実に機能する体制が必要である。このため、法令で非

常事態が発生した場合の対応等を定めた管理規程の整備等が事業者に義務付けられており、これを受け、非常時等に迅速かつ的確に対応するための危機管理マニュアル等を定める等の対応を図っているところである。しかしながら、これらの脅威は、従来想定していた状況を超える状況も想定されることから、各事業者においては、想定する脅威を随時再点検し、対策や体制の一層の充実を図ることが適当である。

(3) 非常時等の事業者間の連携・連絡体制の整備

事業者間の連携促進のための情報交換連携の仕組み（事象のレベル分け、レベルに応じた情報連携の整理）が必要である。連携にあたっては、相互接続を意識して、事業者とベンダーでの連携を図る際にやり取りされる情報のフォーマットの共通化の検討が必要である。

障害が発生した場合においては、まず各事業者が自らサービスの早期復旧に取り組むことが必要であり、そのための予備設備の設置・手配は各事業者が主体的に実施すべき事項である。一方、緊急通信や重要通信確保のためのネットワーク資源の確保及びその運用・管理などについては共通化の検討が必要であり、信頼度・設計基準の統一、故障時の相互バックアップの可否などについての共同研究を行うことが適当である。

ICT 障害に限らず、社会的に影響の大きいイベント、災害時を考慮した関係事業者間、ベンダー、施工業者、行政機関などの連絡体制の一元管理、疎通状況の共有・公開など、障害の影響拡大防止、早期復旧を目的とした事業者間協力のレベルや範囲の取り決めなどを行っておくことが適当である。

なお、災害発生初期における電気通信設備の復旧にあたり必要となる、道路状況など重要インフラ各分野を越えた情報交換については、CEPTOAR-Council の場での検討を見守ることが適当である。

(4) 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

設備の運用等においてベンダーへの依存度が高くなっていることを踏まえ、故障時の迅速な原因分析のため事業者とベンダーの連携体制を確立することが必要であり、各事業者において次のような項目について検討が必要である。

- ベンダーの原因分析体制や処理時間の実態を書面などで定期的に確認することなどをベンダーとの保守契約などに盛り込む。
- ベンダーに解析を依頼する場合には、解析に必要な十分な情報を提供する。

- 間欠的に故障が発生する場合においても、故障が固定化、拡大化する前にベンダーと適切な対策を立てる。
- ベンダーとの共同訓練を実施する。

(5) ソフトウェアの導入・更新時の信頼性確保のための体制

ネットワークシステムの中でソフトウェアの重要性が増大しており、信頼性の高いソフトウェアの採用やソフトウェア更新時の信頼性を確保することが必要である。

ソフトウェア導入・更新時のセキュリティ確保については、OS、ミドルウェアベンダーとベンダー間、ベンダーと事業者間で連携して対策を実施し、現状を整理しながら、両者間で情報共有・改善していくことが適当である。

その際、事業者毎にネットワーク設備や構成、提供しているサービスが異なることを踏まえ、各事業者において自らの設備にふさわしい対策を講じることが適当である。

将来、汎用ソフトウェアの運用やセキュリティパッチの適用等に関する基本事項等について、既知の障害発生リスクを回避するために事業者間で共通的な基準を検討することが必要である。

(6) 情報通信ネットワーク安全・信頼性対策実施登録制度の有効活用

情報通信ネットワークの安全・信頼性対策の指標として、「情報通信ネットワーク安全・信頼性基準（昭和 62 年郵政省告示第 73 号）」が規定されており、この基準に沿って対策を行っている事業者について登録制度が設けられているところである。事業者が効率的にネットワークの安全・信頼性を向上させることができるよう、3.2.1 項で後述する電気通信主任技術者の配置要件の明確化の検討と併せて、本制度の一層の有効活用を図ることが必要である。

(7) 行政機関による検査の実施による再発防止対策の確認

繰り返し事故を発生させている事業者については、電気通信設備上の問題に加え、設備の管理上の問題が内在していることが考えられる。このため、利用者保護の観点から検査の実施基準を明確にした上で監督官庁などによる検査を適切に実施することにより、再発防止策等の適切性を確認することが必要である。

3.2　人材育成等に関する検討

本項では、近年の事故発生要因として人為的なミスが原因で発生した事故が増加していることを踏まえ、人材に関する事項として、人材の育成など人的資源のセキュリティ確保について検討を行った。

3.2.1　人材の育成など人的資源のセキュリティ確保

人材の育成など人的資源の確保策に関して、以下の項目の対策が必要である。

ア　新たな技術やリスク管理等に対応した技術者を育成する機関の整備等
イ　電気通信主任技術者等の活用
ウ　電気通信主任技術者の資格制度の見直し

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主な対策は以下のとおりである。

(1) 新たな技術やリスク管理等に対応した技術者を育成する機関の整備等

事業者に必要十分な情報セキュリティ管理体制、運用ルールに関する共通認識の醸成を行い、情報セキュリティの専門家の育成、技術の進歩に合わせた人材開発方法を検討することが必要である。

その際には、安全・信頼性の確保のために必要な技術者の配置像を俯瞰した上で、各種制度の活用も含めた検討が必要である。

さらに将来に向けて、業界団体による研修コースの開発や大学における情報セキュリティや情報リスク管理を扱うカリキュラムの強化等、訓練機関の整備に取り組むことについて検討することが必要である。

(2) 電気通信主任技術者等の活用

電気通信主任技術者は、引き続き相互接続の拡大やネットワークの安全・信頼性確保のため監督機能を果たすことが必要である。その際、電気通信主任技術者の業務範囲等が必ずしも明確になっていないことから、国は、電気通信主任技術者の配置要件をガイドライン化することが必要である。

具体的には、電気通信主任技術者に、一定の監督責任を果たす権限を持たせるなど、その位置付けについて検討することが必要である。同様

に、総務大臣に対して「重大な事故」の報告をする際に、電気通信主任技術者に何らかの報告の責任を持たせること等が必要である。

なお、通信局舎・電力・空調等のインフラ技術領域も電気通信サービスを安定的に提供するためには、電気通信主任技術者の下に適切な管理が行われることが必要であり、引き続き各事業者における電気通信主任技術者の選任、監督範囲の検討に際しては、これらの技術要素も考慮することが必要である。

(3) 電気通信主任技術者の資格制度の見直し

電気通信主任技術者の試験科目等について、ネットワークの IP 化に対応して、資格試験科目の見直し及び資格の種類の見直しについて検討が必要である。

このほか、近年、通信機器のメンテナンスの施工中の事故が発生しており、工事中の事故の事前防止及び事故発生時の迅速な復旧の観点から、電気通信主任技術者の「工事計画、工程管理、品質管理、安全管理」の視点での制度化、人材育成に取り組むことが必要である。

また、ネットワーク情報セキュリティマネージャー資格（NISM）のカリキュラムの適切性を確認し、電気通信主任技術者資格を補完する資格としての積極的な活用についても検討が必要である。

第４章　情報通信ネットワーク管理に関する事項

4.1　設計・設備能力管理に関する検討

本項では、設計・設備能力管理に関する事項として、システムの容量の適切な計画・設計及び開発及びサポートプロセスにおける管理について検討を行った。

4.1.1　ネットワークシステムの容量の適切な計画・設計

事業者がネットワークの IP 化を進める場合には、ネットワークシステムの容量を適切に計画・設計するため、以下の項目の対策が必要である。

ア　ルータ等の重要な設備の安全・信頼性基準・指標及び定期点検等の実施方法の策定と適切な見直し
イ　将来の利用動向に対応できる設備計画の策定及び障害の極小化対策等に関する設計指針等の策定
ウ　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
エ　サーバ等機器の事前機能確認の充実
オ　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などの策定と標準化
カ　産学官連携による事前検証体制の構築
キ　ベンダーから提供されるシステムについての事業者における検査手法、品質評価手法の確立
ク　ソフトウェア選択基準の明確化

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主な対策は以下のとおりである。

(1) ルータ等の重要な設備の安全・信頼性基準・指標及び定期点検等の実施方法の策定と適切な見直し

ルータ等の重要な設備の安全・信頼性基準・指標及び定期点検等の実施方法を策定するとともに適切に見直すことが必要である。

事業者において異なるベンダー設備を利用し、サービス競争をしているため、取り組みとしては難しいところがあるが、ルータ等設備における MTBF（平均故障間隔）算出の考え方、障害への対応事例、ソフトウェアのバージョンアップ方法や障害影響範囲の拡大防止対策などにつ

いて、事業者間で意見交換していくことが適当である。

(2) 将来の利用動向に対応できる設備計画の策定及び障害の極小化対策等に関する設計指針等の策定

装置の処理能力を適切に把握するとともに通信需要を適切に予測し、将来の設備増強計画に反映していくことが必要である。また、事故や障害が増加している状況を踏まえ、導入前の装置等の処理能力の確認方法、将来の需要予測に基づく適切な設備増強計画、障害の拡大防止・極小化対策等をネットワークの設計指針に反映していくことが必要である。

その手法については、各事業者が使用している設備、ネットワーク構成等が異なることを踏まえ、各事業者において自らの設備にふさわしい対策を講じることが適当である。

(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

IP 接続における相互接続のルールについても既存の電話交換網レベルのように相互接続に関する技術的条件を明確化し、その技術条件に準拠していればどの通信事業者のネットワークとも接続性が確保できるようにルール化を図ることが適当である。

ベンダーが開発した機器やシステムの接続性を検証できる環境・設備を第三者機関等に整備すること、事業者が機器を採用する場合に第三者機関等で接続性の検証を事前実施していることを条件とすること等の検討が必要である。

(4) サーバ等機器の事前機能確認の充実

サーバ等機器の事前機能確認を十分に実施することが必要である。

事業者毎に使用している機器は異なるが、サービスの安定的な提供のために、事前に確認することが必要な最低限の事項について事業者、ベンダーなど関係者でガイドライン化することについて検討が必要である。

(5) 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などの策定と標準化

システムの複雑化により復旧時間が長時間化したケース等については、ネットワークの安全・信頼性向上や利用者利益保護を目的として、事業者、ベンダー間で情報共有する仕組みを整理し、共通的なシミュレ

ーション方式の可能性について検討するなど、各事業者、ベンダーがネットワークの安全・信頼性の向上に向けて取り組むことが適当である。

(6) 産学官連携による事前検証体制の構築

共通の障害事例の機器故障パターン、トラヒックパターンの蓄積、サービス種別ごとのトラヒック特性とサーバ動作を考慮したシミュレータなど、IP 機器対象の共通的な評価手法や共通テストベッドの開発が必要である。

これにより、サービス種別ごとのトラヒック特性とサーバ動作を考慮したシミュレーションの実現、ネットワーク実運用時の挙動の事前検証ができる体制を産学官連携のもとで整備していくことが適当である。

(7) ベンダーから提供されるシステムについての事業者における検査手法、品質評価手法の確立

ネットワークの安全・信頼性の確保のために、必要最低限行うべき共通的な検査・品質測定手法の確立について事業者及びベンダーが連携して検討することが必要である。

(8) ソフトウェア選択基準の明確化

ハードウェアの汎用化に伴い、各種ネットワーク機能をソフトウェアで実現する比重が高まり、ソフトウェア不具合に起因するネットワーク障害対策の重要性が高まっている。サービス品質は、利用者の事業者選択基準のひとつであり、詳細な基準を共通的に決めることは難しいが、最低限必要なソフトウェア選択基準についてガイドライン化していくことが適当である。

4.1.2 開発及びサポートプロセスにおける管理

開発及びサポートプロセスにおける管理に関して、以下の項目の対策が必要である。

ア　保守点検の手順書の作成
イ　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
ウ　セキュリティチェックのための体制
エ　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

オ　工事実施者とネットワーク運用者による工事実施体制の確認や工事手順の策定 カ　安全かつ容易な設備増強、拡張性確保手法の確立

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主な対策は以下のとおりである。

(1) 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

ソフトウェアの脆弱性は開発段階で極力なくすことが必要であるが、運用開始後新たな脆弱性が発見されることも少なくなく、そのような場合は迅速なパッチ適用等によりいち早く脆弱性を取り除くことが必要である。

このような、開発段階で見過ごされた脆弱性を発見するために定期的にソフトウェアを点検し、リスク分析を行うことが必要である。

なお、具体的な点検周期や手法はソフトウェアの重要性や影響を考慮し、各事業者が検討し、ふさわしい対策を講じることが適当である。

(2) 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

なりすまし、改ざん、不正アクセス、盗聴、情報漏えい、フィッシングなどセキュリティに関する脅威を明確化し、セキュリティ脅威に対する情報を事業者間で情報共有していくとともに、これらを活かしたシステムファイル保護手段の導入の取組みについて各事業者で対応していくことが適当である。

(3) 工事実施者とネットワーク運用者による工事実施体制の確認や工事手順の策定

工事を実施する際に工事の実施手順や体制について、工事実施者とネットワーク運用者間での情報共有は広く行われているが、工事中の事故による影響の拡大の状況を踏まえ、工事ミスが発生した場合のリカバリー手法の確認を工事前に実施することが必要である。

また、将来に向けて、工事の安全性を一層高める対策として、工事手順について工事業者から意見を募り、安全性の観点から製品に反映すべき事項、工事計画に反映すべき事項等をまとめたガイドラインを作成することや、遵守状況のチェック体制を確立することが適当である。

(4) 安全かつ容易な設備増強、拡張性確保手段の確立

各事業者が安全かつ容易に設備増強を実施できる手順書を作成することが必要である。また、作業の自動化及び作業確認の強化を実施することにより人為的要因によるサービス中断を回避するとともに、工事ミス時のリカバリー手順を確立することが適当である。

将来的には、通信サービスの無中断機能提供のガイドラインを策定することが適当である。

4.2 保全・運用・管理に関する検討

本項では、保全・運用・管理に関する事項として、故障検知、ネットワークふくそう対策解析、緊急時の情報連絡（迅速な連絡・対応・報告体制）連携及び重要通信の確保等について検討を行った。

4.2.1 故障検知、解析

故障が発生した場合に迅速な対応を図りサービスへの影響を最小限にするとともに、原因を解析し再発防止策に活かすために、故障の検知や解析に関して、以下の項目の対策が必要である。

ア　運用監視体制の充実
イ　相互接続時のネットワーク管理体制の強化等
ウ　問題発生時に検知、通報させる機能や体制の確立
エ　IP 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予備系装置への自律切替などの研究開発
オ　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
カ　故障箇所の特定及び故障原因の特定の迅速化対策
キ　原因の究明を迅速に行うための分析技術の研究開発

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主な対策は以下のとおりである。

(1) 相互接続時のネットワーク管理体制の強化等

各事業者が導入する監視・制御システムの要求条件、体制構築については、各事業者が主体的に実施するものであるが、相互接続の際に事業者間では網運用・管理情報の交換に関する機密情報の管理や連絡体制な

どを確認するとともに、適切なオペレーションの実現に向けた事業者間のやり取りに必要な情報の抽出について検討が必要である。

事業者内の監視は各事業者により運用するものであるが、相互接続箇所における監視、切り分け手段についてメール、VoIP などのサービス別に協議し、障害発生時の復旧手順を事業者間で共有した上で、障害の切り分け機能の向上につながる項目の具体的な検討が必要である。

(2) IP 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予備系装置への自律切替などの研究開発

IP 化に対応するためのネットワークの早期異常検知技術及び設備監視技術、装置の予備系への自律切替技術などの研究開発を行うことが必要である。特にエンドツーエンドの通信異常（障害、品質劣化等）に関する研究開発が求められている。

早期異常検知や予備系への切替、エンドツーエンドの通信異常の把握に関する基盤的な技術については産学官で連携して研究開発等を行うことが必要である。また、設備への実装技術については、各事業者が異なるベンダー製品を利用していることを踏まえ、事業者毎に検討を行うことが適当である。

(3) 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

故障の迅速な復旧や二次障害等を防止するために、故障箇所を特定するためのデータの取得手順や切り分け手順等を整備しておくことが必要である。

各事業者のシステム構成が異なるため、共通的な手順書の作成による運用は難しい。このため、監視・制御システムの要求条件・体制構築については、各事業者が主体的に実施することが適当であるが、次のような項目については共同で検討が必要である。

- 事業者間の網運用・管理情報交換に関する方針、情報項目
- 故障特定方法に関して共通化できる項目の抽出
- ベンダーによるネットワーク切り分け手順作成や実技講習の積極的な開催

(4) 故障箇所の特定及び故障原因の特定の迅速化対策

故障が発生した際に故障箇所や原因の特定を迅速化し、サービスへの影響をできる限り少なくするための対策を講じることが必要である。

各事業者が採用するネットワーク技術、設備が異なること、また、ベ

ンダー同士が競争していることからも共通の故障対応方針、仕組みを構築することは難しいが、具備すべき故障検知機能、冗長機能などネットワーク管理技術や機器への要求条件として国際・国内標準化機関、関連コンソーシアムなどを中心に、主に次のような項目について研究等を促進することが適当である。

- 障害発生時の故障処理体制、サービスの早期回復手段の準備、事業者がベンダーに解析依頼をする場合の情報提供要件、方法
- 故障発生時の初動解析を効果的に実行するため故障時のデータや故障発生前の重要箇所のデータを積極的に蓄積する仕組み
- 故障解析のために事業者とベンダーが連携すべき項目や考え方

4.2.2　ネットワークふくそう対策

災害、社会的な事件、電話リクエスト等による通信量の増加が交換機等のネットワークシステムの処理能力を超えると、対向している周辺のネットワークシステムにまで連鎖的に影響を及ぼし、ネットワーク全体の機能を麻痺させるおそれがある。こうした状況を未然に防止するため、以下の項目の対策が必要である。

ア	ふくそう監視手法や事業者間連携
イ	ふくそう時のユーザー間の公平性の確保
ウ	企画型ふくそうを防止するための情報収集の仕組み
エ	ふくそうの波及防止手順の整備及び長期的視点の対策
オ	ノードが具備すべきふくそう対策
カ	アクセス集中時のブロック、負荷分散機構等の機能の実現
キ	ふくそう発生のユーザー端末への自動通知
ク	災害用伝言ダイヤル等の利用促進によるふくそう軽減
ケ	災害時にユーザーの振る舞いや端末の挙動がネットワークに与える影響の事前検証
コ	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
サ	ふくそうの予測・回避技術、問題箇所を迅速に把握する機能の研究開発
シ	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

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主な対策は以下のとおり

である。

(1) ふくそう監視手法や事業者間連携

ネットワークの IP 化が進展する中、その安全・信頼性を確保することは利用者利益の保護の観点から重要である。このため、より具体的なふくそうの検出手法やふくそう制御手法を検討し、各事業者に共通的な事項については制度化やガイドライン化の検討が必要である。

また、トラヒックの増加に対応した設備設計手法については、各事業者が自らのネットワーク構成等を踏まえて検討することが必要である。

なお、この検証に必要な設備への支援措置についても検討することが望ましい。

(2) ふくそうの波及防止手順の整備及び長期的視点の対策

ふくそう対策については、法令に基づき事業者において基本的な対策を講じているが、IP 系サービスでふくそう制御が十分できなかった事例が発生したことを踏まえ、更なる対策の強化が必要である。

対策の具体的内容については、事業者がそれぞれ異なる設備構成でネットワークを構築・運用していることを踏まえ、各事業者において、ふくそうの波及防止について一層のノウハウの蓄積を図ると共に、ふくそう時における通信規制など緊急対応の実施手順や管理体制の整備、さらにふくそうを事前に防止するための設備増強等の長期的視点での対策に取り組むことが適当である。

また、IP 系サービスの信頼回復に業界として取り組むことが重要であることから、重大なネットワークふくそうにより他事業者にも影響を及ぼす場合を想定した事業者間連携、そのための事業者間での共通用語の定義、連絡基準・連絡体制、さらにユーザー（消費者）への周知の基準・内容について業界団体でガイドライン化の検討が必要である。

(3) アクセス集中時のブロック、負荷分散機構等の機能の実現

アクセス集中時のブロック、負荷分散機構等の機能については、技術検討作業班において、0AB～J 番号を使用する IP 電話について、「現行のアナログ電話用設備等と同様に、交換設備は、異常ふくそうが発生した場合に、これを検出し、通信の集中を規制する機能又はこれと同等の機能を有することが適当である。また、相互接続した他事業者に対して重大な支障を及ぼすことがないように、相互接続されている交換設備は直ちに異常ふくそうの発生を検出し、通信の集中を規制する機能を有す

ることが適当である」とされているところである。アクセス集中時のブロック、負荷分散機構など異常ふくそう対策は、技術検討作業班での検討結果を踏まえて技術基準を策定することが必要である。

なお、具体的な手法については、各事業者の設備状況が異なることを踏まえ、各事業者がそれぞれの状況に応じた検討が必要である。（関連項目：5.1.3）

(4) ふくそう発生のユーザー端末への自動通知

ふくそう発生をユーザーに通知することは、それによって再呼が防止できるため、ふくそうの長期化を抑制する上で必要である。ふくそうの発生をユーザーに通知するための具体的手法（ネットワーク側と端末側双方への機能の実装）については、技術検討作業班の検討結果を踏まえ、各事業者がそれぞれ取り組んでいくことが適当である。

ただし、こうした機能の端末への実装によって端末の自由度をいたずらに制限する事にならないように注意することや、標準化の動向と整合を図ることも重要である。

また、ユーザーに対して、ふくそうが通知された場合はむやみに再呼を繰り返さないよう周知徹底を図ることが適当である。

(5) 災害用伝言ダイヤル等の利用促進によるふくそう軽減

事業者は災害時の安否情報の伝達手段として災害用伝言ダイヤル等の利用について周知徹底をはかり、災害時のふくそう軽減に努めている。

しかしながら、調査結果では、災害用伝言ダイヤルの利用状況については、利用したことがある（体験利用を含む）が 3.9%、利用したことはないが、使い方は知っているが 24.6%との結果となり、そういうサービスがあることは知っているが、使い方は知らないが 63.7%と多数を占める結果が出ている。このように十分認知されているとは言えないことから、引き続き各事業者等が周知徹底に努めることが必要である。

(6) ふくそうの予測・回避技術、問題箇所を迅速に把握する機能の研究開発

ネットワークの IP 化に対応したふくそうの予測・回避技術、サーバの自律監視が機能しない場合（サーバのサイレント障害）の問題箇所特定技術、IPsec 等で暗号化されているパケットのトラヒックの観測から状況を予測する技術等の研究開発を行うことが必要である。

(7) 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

各事業者のネットワーク運用・管理体制の強化を図るため、各事業者やベンダーにおいては、次のような取り組みを行なうことが適当である。

- イベントなどトラヒック急増時のふくそう対策などの措置手順、連絡体制の整備
- 各事業者における開発・試験環境の充実、具体的障害事例を用いた、分析と改善策の情報交換・検討
- トラヒック生成装置（集中呼）を用いた評価試験の実施

4.2.3　緊急時の情報連絡（迅速な連絡・対応・報告体制）及び連携

緊急時に事業者内、事業者間、ベンダー、利用者、国等関係者間で適切な対処を行うため、迅速な連絡・対応・報告及び連携について、以下の項目の対策が必要である。

ア　社会的影響の変化に伴う事故報告基準の見直し及び明確化
イ　多様なメディアによる障害内容の利用者への提供
ウ　他社ユーザーへの障害情報等の提供
エ　利用者等への対外的な公表基準の策定

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主な対策は以下のとおりである。

(1) 社会的影響の変化に伴う事故報告基準の見直し及び明確化

電気通信サービスの安全・信頼性対策として、事業者に対して事故の報告を求め、統計分析を行うことは、

- ユーザー保護の観点から、電気通信サービスが安定的に提供されているかどうかをマクロ的に把握し、国民生活や社会経済活動に影響を与える事故・障害等について、必要な対策、改善等の提言及び再発防止のための検討を行うことができる。
- 報告された重大な事故について統計分析した結果を公表することにより、利用者は自らが利用しているネットワークの品質を客観的に把握することができる。

等の点で重要である。

そのためには、今日のネットワークの IP 化に対応して、事故の規模、時間及び事象が、社会的影響度を適切に反映した事故報告基準の下で収

集されることが必要である。

具体的には、現状では、IP 系サービスに多く見られる「つながりにくい」といったサービスレベルの著しい低下は報告対象となっていないが、ICT サービスの安全・信頼性を確保し、利用者利益を確保する上では、このような事故のうち影響の大きいものについては、報告対象となるよう報告基準を見直すことが必要である。

また、使用する用語や事象の説明を事業者、総務省、マスコミ、消費者などが共通して理解しやすい内容とするための配慮が必要であり、そのうえで報告基準の適用（報告の要否）について具体的な例示等を総務省ホームページに掲載するなどにより運用の統一を図ることが必要である。

また、小規模・短時間の事故の中にも、将来の大規模・長時間な事故へ発展する要因を含む事故が内在することが考えられることから、事業者は、これらの情報を国や業界内で共有し事故の状況を把握したうえで、国の政策等に的確に反映することが必要である。

さらに、利用者の登録業務など直接通信サービスに影響を及ぼしていないものの、利用者に大きな影響を及ぼすシステムについては、MNP（携帯電話番号ポータビリティ）の開始に伴い事故が発生したこと等を踏まえ、報告対象とすることが必要である。

(2) 多様なメディアによる障害内容の利用者への提供

事業者は、サービスの停止等のトラブルが発生した場合に障害内容や復旧状況を利用者や関係者に適切に提供することが必要である。また、情報の提供にあたっては、現在、主に用いられているホームページの掲載のみならず、多様な情報提供媒体を通して、利用者に通知することが必要である。

具体的な手段等については、サービスの種類や利用形態等を考慮して事業者が適切な手段を選択することが適当である。

さらに、複数事業者が同一の要因で ICT 障害を発生させている場合等には、T-CEPTOAR 等を活用して障害内容を利用者へ情報提供するための具体的な手法等を検討することが必要である。

(3) 他社ユーザーへの障害情報等の提供

障害発生により、他社ユーザーにも影響を与えている場合は、他社ユーザーに対しても、自社ユーザーと同等レベルの情報提供ができる仕組みを T-CEPTOAR 等の場を利用して構築していくことが適当である。

(4) 利用者等への対外的な公表基準の策定

利用者に対して事故の発生状況を統一的な基準で公表し、サービス利用のための判断情報を適切に提供するために、業界で統一的基準を設定する、又は制度として公表することが必要である。

4.2.4 重要通信の確保

社会状況の変化やネットワークの技術革新に適切に対応して重要通信を確保するためには、以下の項目の対策が必要である。

ア　ネットワークの IP 化に対応した重要通信の確保
イ　大規模災害発生時の緊急通報の設備容量不足への対応
ウ　誰もが容易に緊急通報できる手段の確保
エ　警察、消防等への緊急通報接続システムのデータ共有化

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主な対策は以下のとおりである。

(1) ネットワークの IP 化に対応した重要通信の確保

社会構造や社会情勢の変化に伴い、非常時等において重要性の高い通信が変化してきていると考えられる。このため、ネットワークの IP 化といった技術の進展も踏まえ、ネットワークに最低限求められる機能の整理、重要通信の対象機関の見直し、運用ガイドラインの策定について有識者や業界関係者と調整をしつつ検討を行うことが必要である。

(2) 大規模災害発生時の緊急通報の設備容量不足への対応

要求項目を明確にし、事業者と緊急通報受理機関との間で大規模災害発生時の緊急通報の取り扱いについて検討が必要である。

(3) 誰もが容易に緊急通報できる手段の確保

障害者、高齢者、子供など誰もが容易に緊急通報できる手段の確保が必要であり、音声以外での緊急通報などの検討が必要である。

(4) 警察、消防等への緊急通報接続システムのデータ共有化

人為的なデータ設定誤り等により緊急通報が利用できないといった事

故が発生したことを踏まえ、警察、消防等への緊急通報接続システムのデータ共有化等により誤りをなくすことが必要である。

しかしながら、事業者ごとにシステムの構成、データベースの構造、基地局の設置状況が異なるため、すべてを共通のデータベースによって構築することは困難な面があるが、緊急通報受理機関から事業者への管轄情報等の受け渡しの一元化などは、共通のデータベースの保有・活用により可能であることから、導入の可能性の検討が必要である。

4.3 情報セキュリティ管理に関する検討

近年の急速なブロードバンド化や電子商取引の浸透に伴い、世界規模でのコンピュータウィルスの蔓延、サイバー犯罪の増加、データの不適切な管理や不適切なソフトの利用等による個人情報の漏えいや電気通信システムのセキュリティに係る情報等の漏えいが社会問題化している。

本項では、情報セキュリティ管理の対策に関する事項として、社内の重要情報の管理、ネットワークアクセス制御、サイバー攻撃に備えた管理体制、情報漏えい防止の管理体制、外部委託の際の情報セキュリティ対策等について検討を行った。

4.3.1 社内の重要情報の管理

昨今、電気通信事業分野において社内から個人情報など重要情報の漏えい事件が相次いでいるため、社内の重要情報の管理に関して、以下の項目の対策が必要である。

ア　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
イ　情報の管理に関する内部統制ルールの整備
ウ　情報の暗号化、アクセス権制御など情報の秘密を確保する対策・手順の明確化
エ　アクセスログの取得、適切な保管

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主な対策は以下のとおりである。

(1) 情報の管理に関する内部統制ルールの整備

取扱規程及び管理責任者を適切に設定する等により、情報の管理に関する内部統制ルールの整備を行うことは、情報を適切に保護し維持する

ために必要である。特に、最近の重要な情報の流出が後をたたない状況を踏まえ、内部統制ルールに関する事項の整備を行うことが必要である。

内部統制ルールの具体的な内容については、事業者の業務の態様が異なることから、各事業者において情報のレベルに応じた対策を講じることが適当である。なお、これらの実施の適切性を担保するために、ISMS認証等の外部認証の活用も有効である。

(2) 情報の暗号化、アクセス権制御など情報の秘密を確保する対策・手順の明確化

急速に ICT の利活用が拡大する中、次々に発生する新しいセキュリティの脅威に対応するためには、常に最先端の研究開発の成果を取り入れた情報セキュリティ対策を講じることが必要である。このため、新しいセキュリティの脅威に適切に対応するため、産学官連携の下、継続的に研究開発に取り組んでいくことが必要である。

特に大量の個人情報の漏洩等が社会問題化していることを踏まえ、アクセス権限をより確実に制御することにより、セキュリティレベルの一層の向上を図るため、「電気通信事業における情報セキュリティマネジメントガイドライン」、「電気通信分野における情報セキュリティ確保に係る安全基準（第 1 版）」などのガイドラインを参照しながらパスワード設定ルールや利用者認証方式等の利用者のアクセス管理、情報に応じた管理基準を徹底していくことが必要である。

その具体的な手法や基準については、事業者の業務の態様がそれぞれ異なることを踏まえ、事業者毎に最適化して個別に定めることが適当である。なお、これらの確実な実施を確保するために ISMS 認証等の外部認証の活用も有効である。

4.3.2　サイバー攻撃に備えた管理体制

近年、事業者のネットワーク及び端末は、発信元を偽装した大量のメール攻撃、不特定多数の端末を踏み台にしたボット攻撃、発信元偽装メール等からの不正ホームページへ誘導するフィッシングなど攻撃の対象にさらされている。したがって、このようなサイバー攻撃によりサービスが影響を受けることがないように、サイバー攻撃に備えた管理体制として、以下の項目の対策が必要である。

ア　他の利用者へ悪影響等を与えている利用者に対する一時利用停止の明確化 イ　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 ウ　サイバー攻撃発生時の迅速な情報共有方法の確立

上記の項目のうち、法令やガイドライン等の整備が必な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主要な対策は以下のとおりである。

(1) 他の利用者へ悪影響等を与えている利用者に対する一時利用停止の明確化

サイバー攻撃の実態について利用者の認識を高め、攻撃に利用された回線の一時利用停止を約款に盛り込むことについて、利用者のコンセンサスを醸成することが必要である。

また、技術革新や社会の変化に伴い、他の利用者に悪影響を与えている事象も変化していくと考えられるが、そのような事例を洗い出し、当該事象への対応方針を策定し、利用者の合意形成を図ることが適当である。

(2) 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

重大な影響を及ぼすサイバー攻撃や、1 社のみでは解決が難しい攻撃に対しての事業者間の協力体制について検討を行い、情報共有する体制の整備、他社へ協力を依頼するルートの整備、情報共有を行う上での情報管理基準、秘密保持契約等の締結方法等について検討が必要である。

また、攻撃者や違反者に関する情報を共有するシステムの構築（ブラックリストの作成・設定・解除依頼方法の明確化）、規制や接続拒否の実施基準などの諸課題について総合的な検討が必要である。

(3) サイバー攻撃発生時の迅速な情報共有方法の確立

T-CEPTOAR 等において、例えば、サイバー攻撃の危険度の考え方、事業者間での情報共有のあり方について検討する必要がある。

また、サイバー攻撃発生時に、国に提供する情報について検討が必要である。

4.3.3　情報漏えい防止対策

近年の急速なブロードバンド化や電子商取引の浸透に伴い、大量の個人情

報の漏えい等が社会問題化し、情報の管理の取組みを抜本的に強化することが求められている。したがって、情報漏えい防止対策に関して、以下の項目の対策が必要である。

ア　媒体の種類に応じた廃棄処分方法の明確化
イ　メール等を利用した情報交換におけるセキュリティの確保
ウ　外部監査のチェック項目の策定と定期的な内部・外部監査の実施
エ　情報漏えい対策についての事業者間の情報・意見交換の場の設定
オ　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
カ　コンピュータウィルス等による情報漏えい対策
キ　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

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主な対策は以下のとおりである。

(1) 媒体の種類に応じた廃棄処分方法の明確化

媒体を廃棄する際の手順を定める等情報の管理方法を設定することは、情報を適切に保護し維持するために必要である。特に最近、情報流出が後をたたない状況を踏まえ、媒体廃棄の際の手順を具体化して内規等のドキュメントに定めることが適当である。

その手法については、事業者の業務の態様がそれぞれ異なることを踏まえ、各事業者において情報のレベルに応じて適切な対策を講じることが適当である。なお、これらの実施の適切性を担保するために、ISMS認証等の外部認証の活用も有効である。

(2) メール等を利用した情報交換におけるセキュリティの確保

メール等を利用した情報交換を行う際に情報の暗号化、パスワード設定などの手順を定める等情報の管理方法を設定することは、情報を適切に保護し維持するために必要である。特に最近、情報流出が後をたたない状況を踏まえ、メール等を利用した情報交換を行う際の手順を具体化して内規等のドキュメントに定めることが適当である。

その手法については、事業者がそれぞれ異なるメールシステムを利用していることを踏まえ、各事業者においてシステムに応じた対策を講じることが適当である。なお、これらの実施の適切性を担保するために、

ISMS 認証等の外部認証の活用も有効である。

(3) 情報漏えい対策についての事業者間の情報・意見交換の場の設定

電気通信分野における情報セキュリティ対策協議会などの場を活用しながら、技術的・人的な対策等について事業者間の意見交換を行うことにより、すべての事業者がレベルの高い情報セキュリティ対策を講じることが必要である。

(4) 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

電気通信事業に係る情報等の流出は後をたたない状況であり、情報通信システムが社会基盤として位置づけられる中、これらシステムを停止・機能低下させるおそれのある重要なシステム情報の流出については、その事実を的確に把握し対策を徹底することが必要である。

これらの対応のため、重要なシステム情報の流出についても監督官庁へ報告を行うことが必要である。

4.3.4　外部委託における情報セキュリティ確保のための対策

業務の外部委託や派遣職員の活用など外部資源の活用が進む中、電気通信事業に係る個人情報や重要なシステム情報が外部委託先から漏えいするケースが多々発生している。したがって、委託先等の外部機関についても事業者と同様な情報セキュリティ対策を施すことが必要であり、以下の項目の対策が必要である。

ア　業務委託先の選別の評価要件の設定
イ　守秘義務契約、誓約書、情報管理規定の保持
ウ　事業者からベンダーに送付される故障物品内に格納された情報の漏えい防止対策

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主要な対策は以下のとおりである。

(1) 業務委託先の選別の評価要件の設定

第１次情報セキュリティ基本計画（情報セキュリティ政策会議決定 2006.2.2）において「情報システム等の政府調達の競争参加者に対して、

必要に応じて、これらの制度や第三者評価の結果等を活用した情報セキュリティ対策レベルの評価を入札条件等の一つとする。」とされている。これに基づき、政府は、情報システム等の政府調達の競争参加者に対して、必要に応じて、情報通信ネットワーク安全・信頼性対策実施の登録者や情報セキュリティマネージメントシステム(ISMS)等の第三者評価の結果等を活用した情報セキュリティ対策レベルの評価を入札条件等の１つとすることが必要である。

また、事業者は、外部委託先の要件として情報セキュリティに関する外部認証を取得していることを取り入れる等、外部委託先の情報セキュリティを確保していくことが適当である。

(2) 守秘義務契約、誓約書、情報管理規定の保持

自社の社員と守秘義務契約等を結ぶのと同様に、業務を外部委託する場合には、守秘義務・保持契約を義務化するとともに守秘義務・保持契約条項の具体化、秘密保持に係る誓約書の徴収、外部委託先の監査実施、監査時のチェック項目、監査において不具合が発見された際の是正処置依頼・是正処置結果の確認等を定めた情報管理規定の策定等、委託先の取組みを明確化していくことが適当である。

その手法については、様々な業務請負の形態があることを踏まえ、各事業者において状況に応じた対策を講じることが適当である。

(3) 事業者からベンダーに送付される、故障物品内に格納された情報の漏えい防止対策

通信の秘密や個人情報などの漏えいを防止するために必要な対策をとることは、事業者にとって最も重要な事項の１つである。近年のネットワークの IP 化に伴い、ベンダー等事業者以外での保守作業が増加する中、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等、事業者以外の者が取り扱う情報の管理方法を明確にすることが必要である。特に最近の情報流出が後をたたない状況を踏まえ、委託（請負）先での情報管理方法や選定方法を具体化してドキュメントに定め、事業者の管理方法の変更を迅速に織り込んでいくことが適当である。

その手法については、外部事業者の利用が事業者でそれぞれ異なることを踏まえ、各事業者において自らの請負形態に応じた対策を講じることが適当である。

第５章　情報通信ネットワークの設備･環境基準等に関する事項

5.1　設備・環境に対する対策に関する検討

本項では、情報通信ネットワークを構成する設備及び設備を設置する環境の基準に関して、バックアップ、分散化などの ICT 障害対策、サイバー攻撃に備えた設備等に関する脆弱性への対策、端末等における対策について検討を行った。

5.1.1　バックアップ、分散化等の ICT 障害対策

バックアップ、分散化などの ICT 障害対策に関して、以下の項目の対策が必要である。

ア　設備の規模に応じた予備電源による具体的な動作時間の設定
イ　地下鉄構内等の携帯電話基地局等の予備電源の確保・充実
ウ　障害の影響範囲を限定する対策
エ　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
オ　事業者をまたがる標準的網管理インタフェースの検討
カ　緊急通報確保のため稼働状態でメンテナンスを可能とする IP 電話システムの実現
キ　コロケーション先の電気通信設備の保護
ク　セキュリティを保つべき領域の基準の明確化と重要度に応じた入出管理の導入
ケ　予備電源設置・冗長化などの予備機器等の配備基準の明確化等

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主要な対策は以下のとおりである。

(1) 設備の規模に応じた予備電源による具体的な動作時間の設定

予備電源による動作時間については、移動電源車の手配や燃料補給等の活用などを含めて総合的に長時間の運用が可能となるように各事業者が取り組んでいるところであり、更に高いレベルの対策を技術基準で

規定することは現実的ではない。しかしながら、停電時の動作確保の重要性を踏まえ、各事業者が設備の重要度に応じて十分な規模の予備電源が確保できるよう、適切な局舎やハウジングスペースの選定、自前の予備電源の設置などの対策を講じることをガイドライン等において明確化する必要がある。

(2) 地下鉄構内等の携帯電話基地局等の予備電源の確保・充実

地下鉄の構内など予備電源設備等のスペースが限られている箇所においては、共同設置など他事業者と積極的に連携をとるのが適当である。

(3) 事業者をまたがる標準的網管理インタフェースの検討

技術検討作業班のこれまでの検討状況を踏まえ、まず各事業者は自らの IP ネットワーク上の交換設備に異常ふくそうを検出する機能や通信の集中を規制する機能の具備を検討することが必要である。

さらに、技術検討作業班の今後の検討状況に合わせて、必要に応じて通信事業者間で障害情報やふくそう情報を伝達できるプロトコルの開発・標準化等を検討することが必要である。

(4) 緊急通報確保のため稼働状態でメンテナンスを可能とする IP 電話システムの実現

IP 電話は、メンテナンスに伴うサービス停止が多い傾向があるが、特に 0AB～J 番号を使用する IP 電話においては、緊急通報が常に利用できるようにするためにも、稼働状態でのメンテナンスを可能とするようシステムの改善を図ること等が必要である。この際、国際標準を十分に踏まえることが必要である。

また、メンテナンス時にサービスを停止する場合は、多様なメディアを通じて、ユーザーに通知できるようにすることが適当である。

(5) コロケーション先の電気通信設備の保護

電源設備について、例えば、異常時電源遮断機能を具備することや、保守点検により正常性を維持すること等、発火・発煙等の防止に関する基準を、電気通信事業法上の技術基準等として設けることが必要である。また、他の事業者のビルにコロケーションしているすべての電気通信設備について、発火・発煙等の防止等の最低限の安全・信頼性が確保されるよう所要の措置を講じることが必要である。

(6) セキュリティを保つべき領域の基準の明確化と重要度に応じた入出管理の導入

事業者は、電気通信設備を工事・維持・運用する者が、みだりに事業用電気通信回線設備を操作して運用を妨げたり通信の秘密を侵したりすることがないようにセキュリティを保つべき領域の具体的な基準を設定することが必要である。具体的な基準の設定については、事業者が種々の領域設定、情報の設定により運用していることを踏まえ、各事業者において適切な基準を設定することが適当である。なお、これらの実施の適切性を担保するために、ISMS 認証取得等の外部認証の活用も有効である。また、次世代 IP ネットワーク等新たなネットワークやサービス形態へ移行していく中で、電気通信事業法等の法令や現行のガイドラインを適宜見直し、それらに基づき、各事業者がそれぞれのサービスに適した形で、取り組んでいくことが適当である。

また、電気通信設備や情報を適切に管理するためには、それらの重要度に応じた適切な入出管理を導入していくことが必要である。近年の情報流出事案の発生等を踏まえ、引き続き法令等に基づく入出管理の徹底を図ることが必要である。入出管理の手法については、各事業者の設備の状況が異なることを踏まえ、各事業者において状況に応じた対策を講じることが適当である。取り組みをより確実なものにするために ISMS 認証等の外部認証の取得も有効である。また、生体認証など新しい認証技術の入出管理システムが開発されていることなどから、技術の進展に沿ってシステムを見直していくことが必要である。

さらに、各事業者の取り組みへの考え方や意識、実施状況に大きな差異がある場合、相互接続等で共有する情報の管理面で問題が生じる恐れがあるため、定期的に取り組み状況等を相互接続している事業者間で情報共有することが必要である。模範的な導入事例等を事業者間で共有するなど、各事業者における入退出管理の高度化の取り組みを促進することが有効である。

(7) 予備電源設置・冗長化などの予備機器等の配備基準の明確化等

阪神・淡路大震災や新潟中越地震などの経験からもわかるように、伝送路の多ルート化は災害や機器の故障等における電気通信ネットワークの安全・信頼性の向上を図る上で、非常に有効である。しかし、すべての伝送路について異経路多ルート化を図るには、莫大な投資と長い整備期間が必要となることから、技術基準においても引き続き努力義務とすることが適当である。しかしながら、義務の対象については、国民生

活への影響等を考慮して適宜見直すことが必要である。

一方、ネットワークのふくそうの事前及び事後の対応策については、有識者を含めて技術的検討を行い、また、予備機器の設置、応急復旧機材の配備、データ等の定常的バックアップ、ネットワーク経路の二重化、オペレーションセンターの分散化、通信経路の迂回措置、ケーブル配線の安全対策、予備電源の設置等、安全･信頼性を確保する観点で対策すべき事項についてガイドラインの充実を行う必要がある。

今後、安全・信頼性向上のための設備投資に対してのさらなる支援制度について検討することが必要である。

また、ネットワーク機器やサーバ等の省電力化、バッテリーの高性能化・経済化、自動迂回時間の短縮化等の開発を産学官が連携して取り組むことが必要である。さらに、サービス稼働率・故障など品質の定義の明確化と一般への公開を行うことが適当である。

なお、予備電源等電気通信サービスの信頼性を向上させるための設備に対しては、取得の際の税制支援が行われているが、より長時間の停電に対応した設備の積極的な導入を各事業者に促すため、引き続き制度を継続することが必要である。インセンティブのより働きにくい地域等での動作時間の長時間化への取り組みに対しては、より手厚く支援する等の検討も必要である。

5.1.2　サイバー攻撃に備えた設備等に関する脆弱性への対策

サイバー攻撃に備えた設備等に関する脆弱性への対策に関して、以下の項目の対策が必要である。

ア　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
イ　攻撃元を特定できる機能と攻撃元のトラヒックを遮断する仕組み等
ウ　出荷前での端末機器の徹底的な脆弱性テストの実施と出荷後の迅速なパッチの適用

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主な対策は以下のとおりである。

(1) 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

相互接続網との間の不正アクセス等の対策について技術検討作業班で検討が行われ、0AB～J 番号を使用する IP 電話では「現行のアナログ電

話用設備等と同様に、事業用電気通信回線設備の防護措置が講じられているとともに、異常ふくそうの発生時には、これを検出し、通信の集中を規制又は同等の機能を有することが適当である」とされ、また「不正アクセス対策としての緊急遮断については、実施の可否も含めて実施に関する基準等（遮断の対象となる攻撃通信の種別・形態、措置の範囲、運用条件他）を明確にすることが望ましい」とされている。今後の緊急遮断についての基準等の検討結果を踏まえ、不正アクセス等への具体的な対策の実施について事業者等において検討が必要である。

(2) 攻撃元を特定できる機能と攻撃元のトラヒックを遮断する仕組み等

攻撃元を特定できるネットワーク・端末の機能及び攻撃元のトラヒックを遮断する仕組み、発信元の偽装を防ぐ機能の研究開発が必要である。ISP では、すでに大量パケットの受信に対する対策を講じたり、危険性があるサイトをアクセス不可にするサービスを提供しているが、今後は、本人認証の手段として、端末認証（MAC アドレス、シリアル番号等）、生体認証（指紋、静脈等)を導入するなど、より高度な認証方式の導入の検討が必要である。

また、利用者への啓発活動として、e-ネットキャラバン、国民のための情報セキュリティサイト等によって、

- 不要な情報サイトにアクセスしないように注意を喚起する。
- 学校・職場などにおいてインターネットの利用方法、危険性を学習させる。

など官民あげての活動を継続していく必要がある。

将来、ネットワークの IP 化の進展と共に、発信元の偽装方法も巧妙化する可能性があることを考慮し、あらかじめ発信元の偽装が困難なネットワーク構成・機能の研究開発を行うことが必要である。

また、高度な端末認証、生体認証などについて、広く普及させていくことにより高度なセキュリティを実現するネットワークを構築することが必要である。

(3) 出荷前での端末機器の徹底的な脆弱性テストの実施と出荷後の迅速なパッチの適用

まず端末機器のソフトウェアに脆弱性が存在しないように開発段階でのチェックを各機器ベンダーで徹底することが必要であり、また機器ベンダーが出荷段階での品質検査を徹底する必要がある。

端末機器が市販された後になって脆弱性が発見された場合は、機器ベ

ンダーが迅速にユーザーにその旨通知し、ソフトウェアパッチの早期適用を徹底することが必要であり、新たに発見される脆弱性への対策としてソフトウェアの更新が必須であることについて、ユーザーの幅広い理解を得るための啓発活動を国、事業者及び関係団体が連携した上で積極的に行うことが必要である。

また、技術検討作業班での検討を踏まえ、脆弱性が発見されたソフトウェアについて早期の更新を確実に実施できる仕組み（例えば自動更新機能）を端末に装備させ、普及促進を図っていくことが必要である。

5.1.3　端末等に対する対策

端末等の対策において、以下の項目の対策が必要である。

ア　IP 端末への要求条件の明確化
イ　ネットワーク防御のための端末の要件の明確化
ウ　停電後の地域単位のセッションリクエストによるネットワーク負荷の分散
エ　端末の電力確保、バッテリー寿命延長の技術開発等
オ　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
カ　誰でもが平等に ICT サービスを利用できるようにするための端末やインフラの整備

上記の項目のうち、法令やガイドライン等の整備が必要な対策、事業者等が連携して取り組む対策及び各事業者が取り組む主な対策は以下のとおりである。

(1) IP 端末への要求条件の明確化

IP 端末等の機能や技術基準等については、総務省で昨年 12 月から開催している「IP 化時代の通信端末に関する研究会」等を参考にしつつ、検討を行うことが適当である。

(2) ネットワーク防御のための端末の要件の明確化

技術検討作業班における検討では、0AB～J 番号を使用する IP 電話端末における機能について、自動再発信機能を備えた端末の自動再発呼回数制限を現行アナログ電話端末と同等とすべきとする技術的条件が提言されており、具体的に IP 電話端末に実装するために必要な標準化作業を継続検討する必要がある。

(3) 停電後の地域単位のセッションリクエストによるネットワーク負荷の分散

IP 電話端末については技術検討作業班で一斉登録に伴うふくそうを回避する機能、端末の無効呼抑止機能、自動発信回数制限などについて検討を実施し、その結果「ネットワークが端末からの登録を受付できない場合に、ネットワークから再登録要求の送信タイミングについて指示があった場合は、端末はその指示に従い送信タイミングを調整し、また、ネットワークから再登録要求の送信タイミングについて指示が無い場合は、端末が送信タイミングを調整し、再登録要求を行う機能を有することが適当」とされている。将来に向けて改善すべき事項として、IP 電話以外の端末についても同様の検討が必要である。

(4) 端末の電力確保、バッテリー寿命延長の技術開発等

様々な電気通信サービスの中から利用者が利点・欠点を正しく理解したうえで目的に適したサービスを選択できるようにすることが重要である。特に、緊急通報に代表されるように、いざというときにしか利用しないような機能については、利用の際に初めてサービスの特質に気づいたのでは手遅れになることが考えられるため、あらかじめ広く利用者に理解してもらう取組みが必要である。

また、近年、バッテリーの発火等の事故が発生していることを踏まえ、安全対策を図ることが必要である。

将来に向けて改善すべき事項としては、端末のバッテリー搭載等停電対策については技術検討作業班の今後の検討課題のひとつに挙げられているため、技術検討作業班での議論を見守ることが必要である。また、バッテリーの長寿命化、高信頼化、経済化等については積極的に研究開発を行うことが必要である。

(5) 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

定期的に Web 上の特定アドレスにアクセスし、自動でバージョン情報を取得し差分を取得するソフトが実装されている端末製品、もしくはウィルス対策ソフトに代表されるように自動バージョンアップが標準的な機能である製品ソフトウェアそのものについては、バージョン不具合が生じた場合における波及が大きいことが懸念されていることを踏まえ、端末系の自動でダウンロードされたソフトのバグによる障害波及防止の有効な対応策について事業者、端末ベンダー等で検討しガイドラインを作成することが必要である。