資料 7-2

ネットワークの IP 化に対応した
安全・信頼性対策（案）

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報告案

IP ネットワーク設備委員会報告 案

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 4 回及び作業班 8 回の会合を開催して審議を行い、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、情報通信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 17 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、情報通信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。

④ 第 6 回委員会（平成 19 年 4 月 17 日）

安全・信頼性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、委員会報告（案）について審議を行った。

また、技術検討作業班の審議経過報告を行った。

(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）
情報通信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、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について、別紙のとおり委員会としての報告（案）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　事業開発統轄部長
	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　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　理事　情報・通信グループ ネットワーク事業統括
	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）　コーポレート・エグゼクティブ　SVP
	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

	みずたに　みきお 水谷　幹男	パナソニック　コミュニケーションズ（株）　副社長ＣＴＯ
	みよし　たかみち 三膳　孝通	（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
	やまさき　よしかず 山崎　吉一	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
	やまと　としひこ 大和　敏彦	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
	ゆげ　てつや 弓削　哲也	ソフトバンクテレコム（株）　専務取締役　ＣＴＯ　研究所長 兼　渉外部担当
	わたなべ　たけつね 渡辺　武経	（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）　インターネット・データ事業本部長
	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。

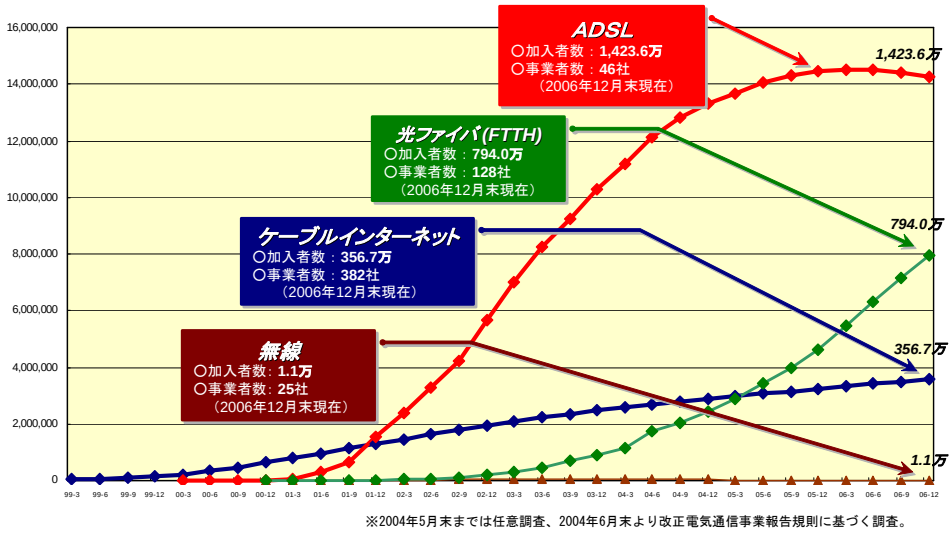


図 1-1　ブロードバンドサービスの加入者

(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。

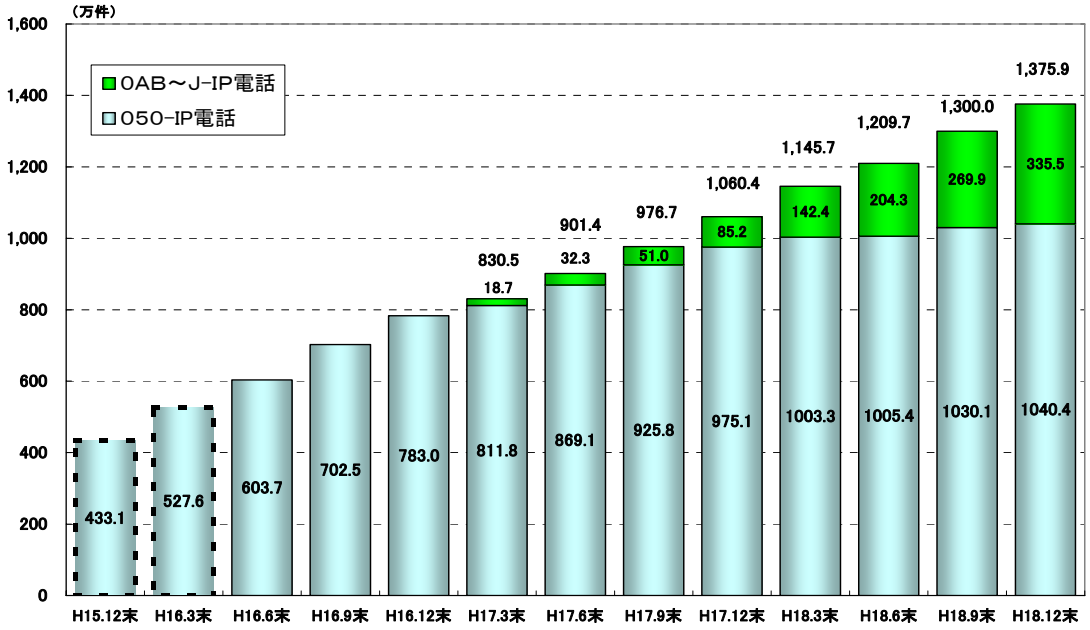


図 1-2　IP 電話の利用数の推移

(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。

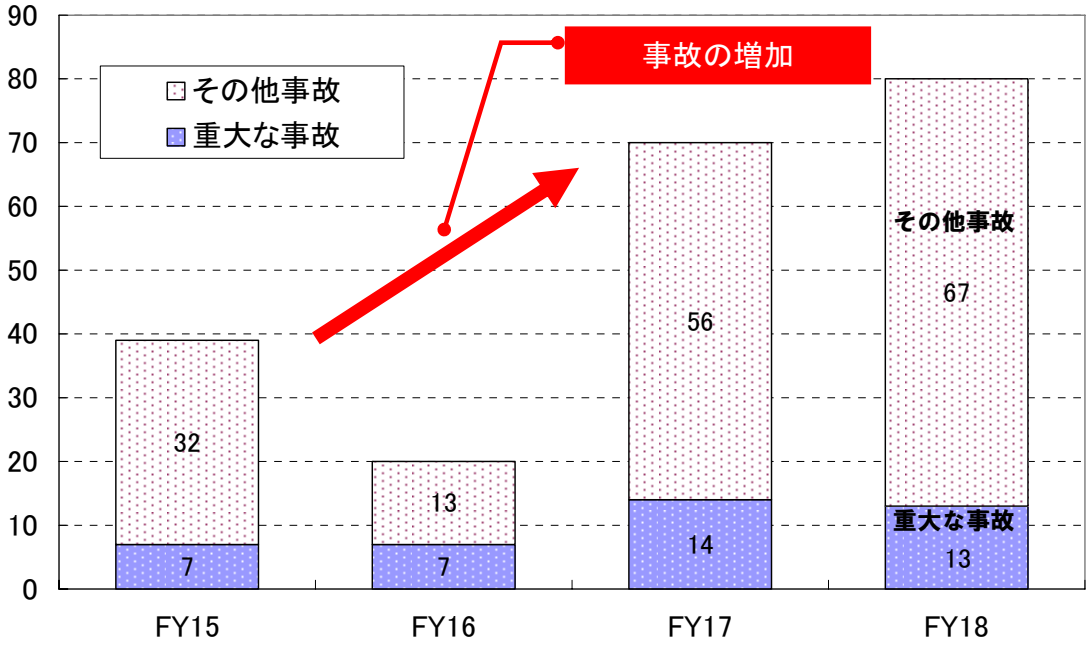


図 1-3　事故等の発生件数推移

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。

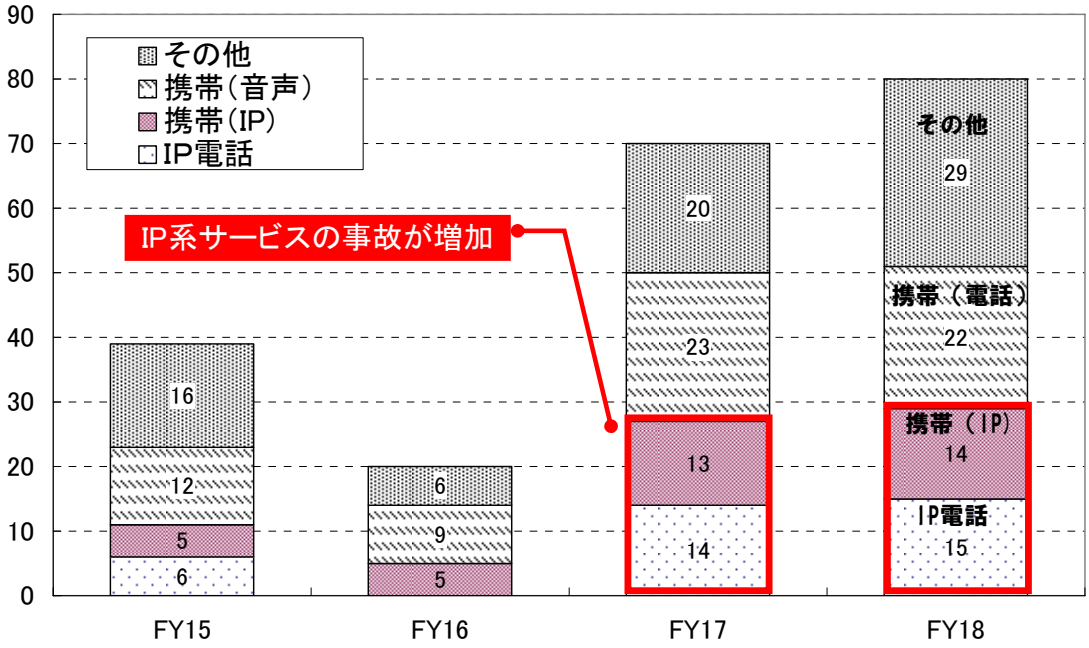


図 1-4　サービス別の事故等の発生件数推移

(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大規模な事故発生状況（平成 18 年～）

発生時期	影響数	影響地域	サービス種別
19 年 5 月	239 万	東日本エリア （東京 23 区, 神奈川, 千葉, 埼玉を除く）	ネット接続、IP 電話
4 月	412 万	全国	携帯 IP 接続
2 月	25 万	関東地方	携帯 IP 接続
18 年 11 月	200 万	全国	携帯 IP 接続
10 月	83 万	西日本エリア	IP 電話
9 月	86 万	東日本エリア	IP 電話
9 月	36 万	東海地方	携帯等メール
8 月	82 万	西日本エリア	IP 電話
8 月	93 万	東日本エリア	IP 電話
7 月	193 万	全国	メール

6 月	29 万	近畿地方	携帯等メール
5 月	23 万	近畿地方	IP 電話
4 月	10 万	中国、四国地方	IP 電話
3 月	39 万	西日本エリア	IP 電話
3 月	230 万	全国	携帯等メール
3 月	390 万	東京都	携帯等メール
2 月	148 万	全国	メール
2 月	246 万	全国	携帯等メール
2 月	180 万	全国	携帯等メール

表 1-2　IP 系サービスにおける復旧までに
長時間を要した事故発生状況（平成 17 年度～）

発生時期	影響時間	サービス種別
19 年 5 月	6 時間 51 分	ネット接続、IP 電話
18 年 10 月	40 時間 30 分	IP 電話
9 月	30 時間 44 分	IP 電話
5 月	5 時間 31 分	IP 電話
4 月	4 時間 4 分	IP 電話
3 月	11 時間 20 分	IP 電話
2 月	79 時間 32 分	メール
17 年 12 月	5 時間 41 分	携帯 IP 接続
12 月	7 時間 31 分	IP 電話
12 月	7 時間 33 分	IP 電話
7 月	10 時間 10 分	メール

※　複数日にわたって断続的に発生した事故については、合計時間を記載

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、平成 18 年度は 16 件（平成 16 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 18 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 28 件となっており、ソフト的な不具合等に起因する事故も多い。

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。

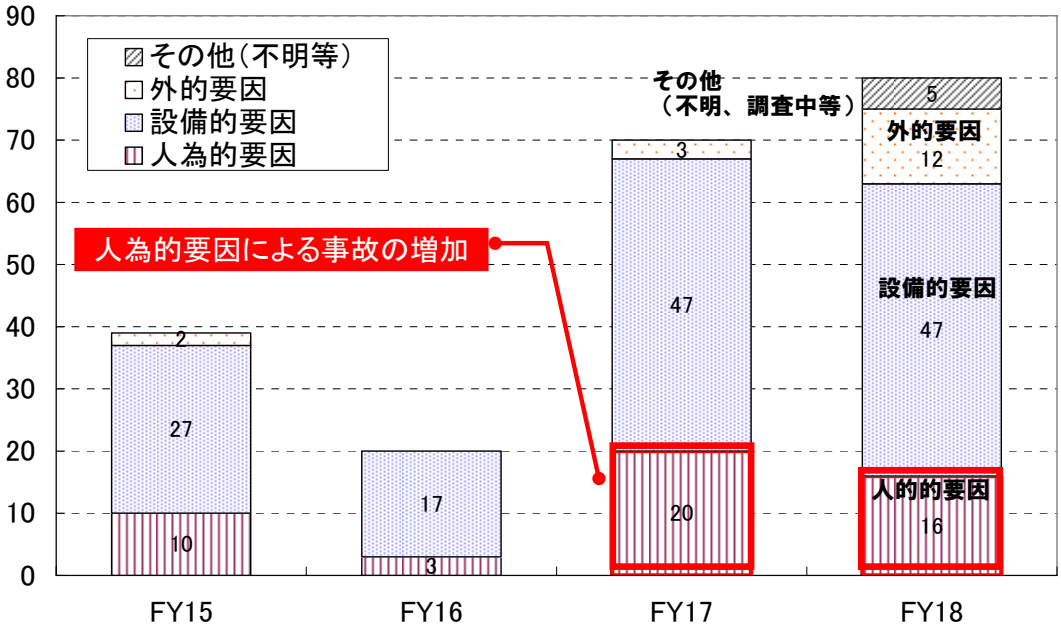


図 1-5　発生要因別事故等発生件数推移

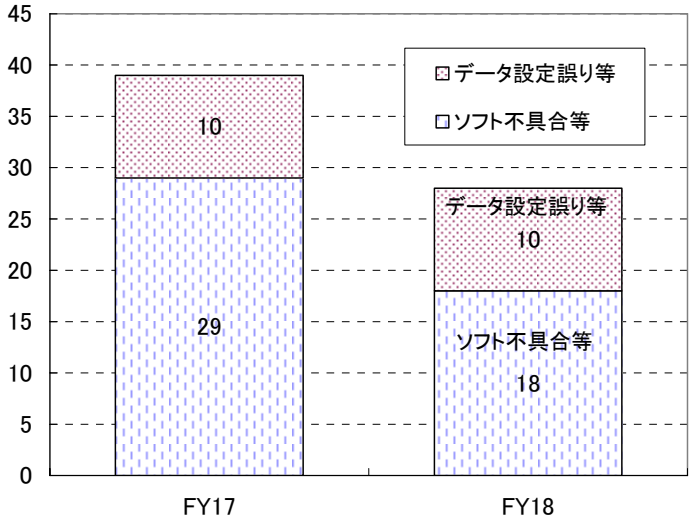


図 1-6　ソフト的な不具合等に起因する事故発生状況

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

(4) 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、情報通信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、現行の情報通信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、情報通信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、情報通信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、情報通信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。

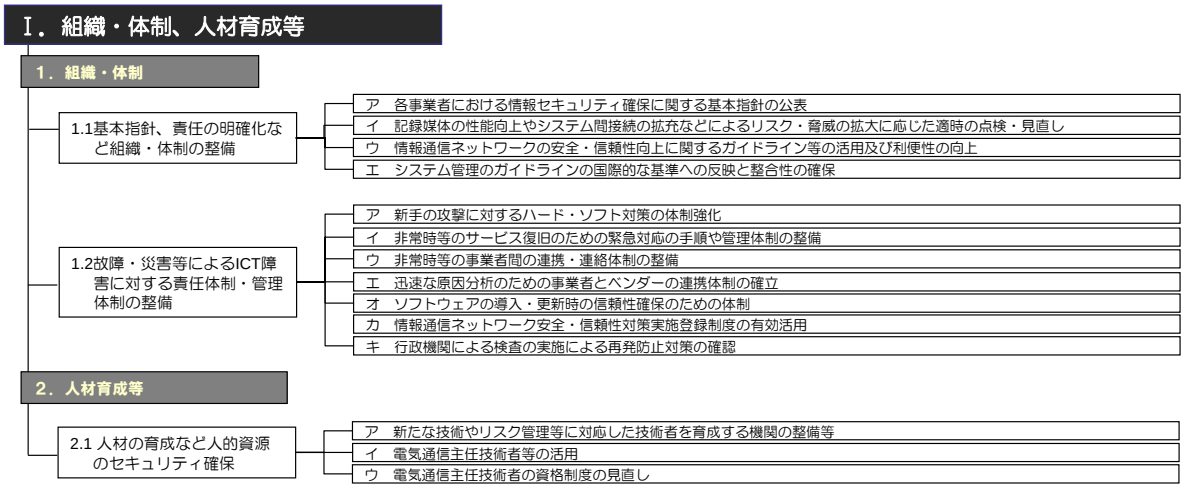
具体的には、情報通信ネットワークの「設備面」、「運用・管理面」、それを実現する「体制面」を３本柱として、

① 新しいネットワーク技術に対応した社内体制や業界内の連携体制の在り方と、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早急な復旧を実現するネットワークの運用・管理
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。

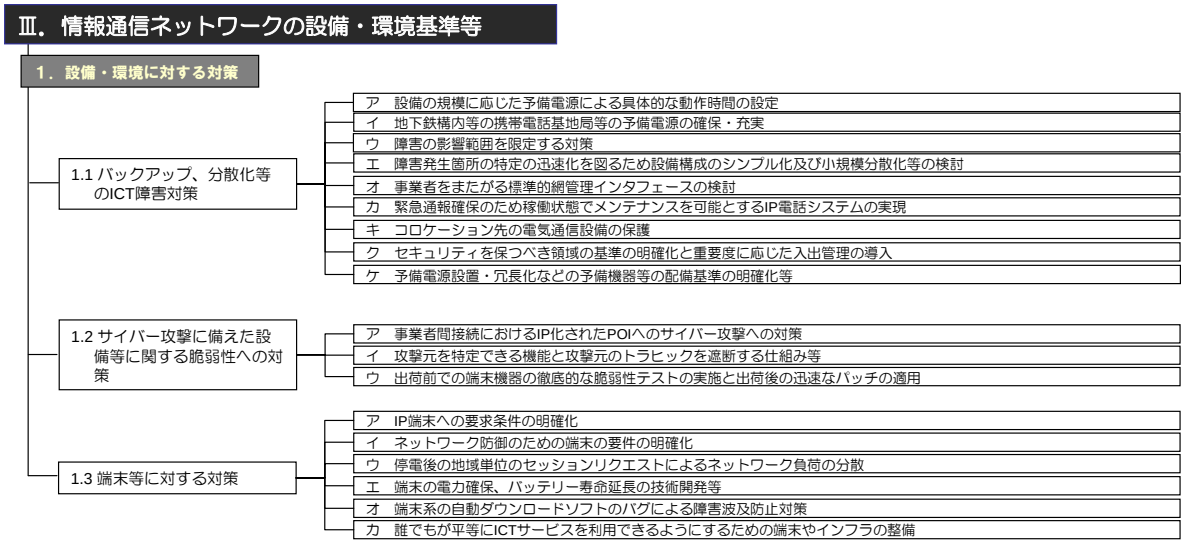


2.3　情報通信ネットワーク管理に関する対策

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　情報通信ネットワークの設備・環境基準等に関する対策

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対策

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　情報通信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) 情報通信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情報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を共通化する検討が必要である。

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。事業者が効率的に情報通信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情報通信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、資格試験の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対策

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、必要に応じて適切に見直すことが必要である。

事業者ごとに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（Mean Time Between Failure 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、情報通信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、ベンダーが情報通信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

情報通信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、セキュリティの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。

事業者内のシステム監視は各事業者により実施するものであるが、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　災害時における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を行うことが必要である。（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、今後さらに必要となる対策や改善措置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故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、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することが必要である。

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状況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。

具体的な手法については､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の者による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対策

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ことが適当である。

(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・運用する者以外の者が、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情報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図る必要がある。

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・故障率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安全・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

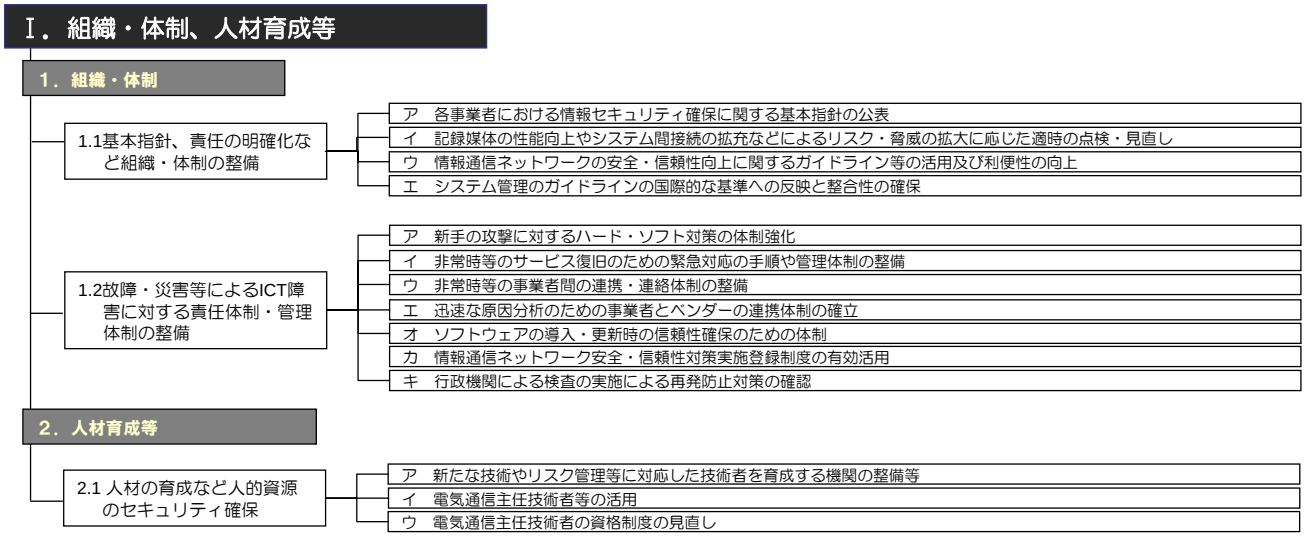
定期的に Web 上の特定アドレスにアクセスし、自動でバージョン情報を取得し差分を取得するソフトが実装されている端末製品、もしくはウィルス対策ソフトに代表されるように自動バージョンアップが標準的な機能である製品ソフトウェアそのものについては、バージョン不具合が生じた場合における波及が大きいことが懸念されていることを踏まえ、端末系の自動でダウンロードされたソフトのバグによる障害波及防止の有効な対応策について事業者、端末ベンダー等で検討しガイドラインを作成することが必要である。

参考資料

目次

参考資料１

個別課題ごとの検討結果


Ⅰ．組織・体制、人材育成等
１．組織・体制
1.1基本指針、責任の明確化など組織・体制の整備
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　情報通信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
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
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
２．人材育成等
2.1 人材の育成など人的資源のセキュリティ確保
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


Ⅱ．情報通信ネットワーク管理
1．設計・設備能力管理
1.1 ネットワークシステムの容量の適切な計画・設計
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
1.2 開発及びサポートプロセスにおける管理
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
2．保全・運用管理
2.1 故障検知・解析
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
2.2 ネットワークふくそう対策
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　災害時における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
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
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
2.4 重要通信の確保
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
3．情報セキュリティ管理
3.1 社内の重要情報の管理
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
3.2 サイバー攻撃に備えた管理体制
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
3.3 情報漏えい防止対策
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
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
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

Ⅲ．情報通信ネットワークの設備・環境基準等

1．設備・環境に対する対策

- 1.1 バックアップ、分散化等のICT障害対策
  - 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
- 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
  - 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
- 1.3 端末等に対する対策
  - 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

分　類	第３章　組織・体制・人材に関する対策 └3.1 組織・体制に関する検討 └3.1.1 基本指針、責任の明確化など組織・体制の整備

ア　各電気通信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

【現状】

情報セキュリティに関する自社の事例、および他社の事例を踏まえ、再発防止や内部統制、企業の社会的責任といった観点から、事業者が主体的に情報セキュリティ確保のための体制、方針の整備を行うとともに、責任体制を明確化したうえで、体制・管理の概要を適宜公表している場合もある。一方、具体的な各種情報の取扱い基準、手段及び実際の運営管理方法の一部の情報については、セキュリティ上の観点から非公開とすべき事項を含んでいるためユーザーへの公表を限定せざるを得ない面がある。

セキュリティ管理を徹底するために ISMS など外部認証を取得し、その旨の公表を行っている事業者もある。

【当面の改善策】

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。

【将来に向けて改善すべき事項】

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。

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

【現状】

情報セキュリティを取り巻く環境は、日進月歩で変化しており、特に記録媒体の性能向上やシステム間接続の拡充・拡大などに伴い、セキュリティに対するリスク・脅威は拡大している。これらの状況に対応するために、事業者は ISMS 認証を取得するなど情報セキュリティやリスク管理体制を構築し、定期的な点検・改善活動を実施している。

【当面の改善策】

情報セキュリティを取り巻く環境は、日進月歩で変化しており、各事業者は策定したセキュリティの基本方針に基づき PDCA(Plan-Do-Check-Action)のサイクルを用いて継続的な改善・フィードバックを行うことが必要である。

特に記録媒体の性能向上やシステム間接続の拡充・拡大などに伴い、セキュリティに対するリスク・脅威は拡大しており、セキュリティルームの設置、入退室管理システムなど物理的対策のほか、アクセスや情報利用に関する制御・記録機能の強化、外部委託や人材派遣の管理など総合的な対策を継続していくことが必要である。

なお、これらの実施の適切性を担保するために、ISMS 認証、ISO27000 等の外部認証の活用も有効である。

【将来に向けて改善すべき事項】

外部監査によるチェック機能（日本版 SOX 法※、ISMS など）に対する要求条件の変化や通信・情報ネットワーク管理・技術の進歩を反映し、追加・検討すべき事項の有無について定期的に検証を行うことが必要である。

※日本版 SOX 法：米国のサーベンス・オクスリー法（SOX 法）に倣って整備された法規制であり、企業に対して会計の不正を防止するために監査や内部統制を強化するように求めている。

ウ　情報通信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

【現状】

事業者は、法令に定められた技術基準や法令に準じて国が定める推奨基準（国のガイドライン）に加え、業界団体等が定める業界横断的な業界標準（業界のガイドライン）や事業者自らが定める内規等を目的に応じて整備し、これらを遵守している。こうした取り組みは電気通信サービスのレベルをより向上させるために必要である。

しかしながら、現状において情報セキュリティに関する政府・その他のガイドラインが複数存在するため、「どのような状況でどのガイドラインを参照すべきか」の判断が難しいという問題も指摘されている。

また、既存のガイドラインは方針と基準について概念レベルの記載となっており、記載内容に関する具体的な基準、適用方法、参考値などの情報が求められている。

＜参考＞

電気通信事業に関係するガイドライン

- 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）
- 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）（電気通信分野における情報セキュリティ対策協議会　平成 18 年 9 月 29 日）
- 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対策協議会　平成 18 年 6 月 29 日）

【当面の改善策】

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。

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

【現状】

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。

【当面の改善策】

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。

分　類	第３章　組織・体制・人材に関する対策 └3.1 組織・体制に関する検討 └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

ア　新手の攻撃に対するハード・ソフト対策の体制強化

【現状】

サイバー攻撃はソフトウェア等の脆弱性をついて行われるため、開発段階で脆弱性を極力なくすことが必要である。

しかしながら、運用開始後新たな脆弱性が発見されることも少なくはなく、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。

【当面の改善策】

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。

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

【現状】

サービス品質、設備管理の一環として他事業者との連絡体制を含め事業者が主体的にマニュアルの整備、更新を行っているが、その規定範囲や内容は事業者毎に異なっている。

しかしながら、ネットワークの IP 化の進展に伴い、これまでの事故・障害対応の見直しの必要性が高まっているほか、新型インフルエンザなど新たな脅威に対する対応の必要性が指摘されている。

【当面の改善策】

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情報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。

ウ　非常時等の事業者間の連携・連絡体制の整備

【現状】

各事業者は災害時に備え、独自にバックアップルートの整備や設備の分散配置などを行っている。また、各事業者間および事業者と各ベンダー間は緊急保守、故障対応などのため、それぞれ連絡体制を整備している。災害時を想定したバックアップ計画や具体的な復旧体制については、各事業者が提供するネットワークや設備の構成が異なり、また、予備設備の確保には設備投資を伴うことから、緊急的な光ファイバー伝送路の相互融通など一部のケースを除き、各事業者がそれぞれの責任範囲で非常時等の復旧体制を整備している。

発生規模・時間帯にもよるが、広域災害時などにおいては複数の事業者が同時に影響を受けることから、全体のネットワーク資源の不足、故障を復旧する施工要員やネットワーク運用要員が絶対的に不足することが想定される。

【当面の改善策】

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を共通化する検討が必要である。

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。

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

【現状】

一般に事業者とベンダーの連携については保守契約等により定め、データ取得手順、切り分け手順については事業者が定めている。多くの場合、事業者において 1 次保守（監視、故障装置切り分け、サービス回復作業）を行い、ベンダーが 2 次保守（切り分け支援、故障に対する代替品提供）及び故障原因の解析を行なう契約となっている。

障害発生時、1 次保守者は原因解析作業よりもサービス回復を優先するため、ベンダーが故障原因の解析に必要なログが充分に取得できない場合がある。また、ベンダーで故障原因を解析するにあたり事業者から提供される情報が限定的であることや、事業者の設備の使い方や設計ポリシーを入手しないと故障原因を解析できないにもかかわらず、その種の情報提供が事業者からされないこともある。

さらに汎用サーバや汎用ソフトウェアで通信設備を構成する形態が増えているため、解析ルートが複数ベンダーを経由するなど体制が複雑化する傾向もある。また、保守契約内容によって対応レベルが低い場合は、調査することが不可能な場合もある。

故障の原因が設備であるか特定できない現象や、端末の設定環境が影響するようなケースでは責任範囲、改善の主体があいまいになりがちである。

【当面の改善策】

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を検討する必要がある。

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。

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。

【将来に向けて改善すべき事項】

障害発生時に障害情報を自動的に残す機能を具備することの検討が必要である。

オ　ソフトウェア導入・更新時の信頼性確保のための体制

【現状】

ソフトウェアパッチ、セキュリティパッチの適用等のソフトウェアの導入や更新は、事業者が必要に応じベンダー等と保守契約等を締結し、ベンダー又はシステム技術者が事前に運用者に通知の上、検証設備で確認した後に実運用中の設備に適用するのが一般的手順である。通常、これらの検証は、多くの場合、事業者が自らの検証機器によりベンダーから提示された検証内容・手順に拠って実施しており、事業者独自に細部の受入条件を規定している事例は少ない。

特にマルチベンダー環境においては各事業者が導入する設備や、その保守形態は多様化しており、ソフトウェア導入や更新時の信頼性確保体制については、個々の事業者が運用基準として基本的な方針のみを内規的に定めている。

【当面の改善策】
　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。

【将来に向けて改善すべき事項】
　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。

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

【現状】
　総務省は、情報通信ネットワークのうち社会的に重要なもの又はそれに準ずるものを対象とし、その安全・信頼性対策の指標を定めることにより、安全・信頼性対策の普及を促進し、情報通信ネットワークの健全な発展に寄与することを目的として、「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）」を制定し、また、この基準のうち一定の対策が実施されている情報通信ネットワークを登録する制度として「情報通信ネットワーク安全・信頼性対策実施登録規程（昭和 62 年郵政省告示第 74 号）を制定している。

【当面の改善策】
　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。事業者が効率的に情報通信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 項で言及してい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。

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

【現状】
　電気通信事業法第 166 条において「総務大臣は、この法律の施行に必要な限度において、事業者等に対し、その事業に関し報告をさせ、又はその職員に、事業者の営業所、事務所その他の事業所に立ち入り、電気通信設備、帳簿、書類その他の物件を検査させることができる。」としている。

【当面の改善策】
　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。

分　類	第３章　組織・体制・人材に関する対策 └3.2 人材育成等に関する検討 　└3.2.1 人材の育成など人的資源のセキュリティ確保

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

【現状】
　ネットワークの IP 化、情報セキュリティに対する脅威の高まりを受け、各事業者においては情報セキュリティを確保するための運用方策を講じている。しかし、一般的に、セキュリティ技術者の育成には時間を要すること等から、外部の専門機関を併用するなどの対策がとられている。
　情報セキュリティに関する技術や管理手法は十分確立されていないため、産学官それぞれの領域において専門家の育成、より強固な管理体制・制度の構築への取り組みが必要と考えられる。しかしながら、専門家を育成する機関の体系的整備など国レベルの人材育成策は十分とはいえない。

現在、業界団体が認定している資格としては、ネットワーク情報セキュリティマネージャー資格がある。これは、情報通信ネットワークの安全性・信頼性を確保するための専門家を育成することを目的として業界団体と総務省が協力して設立したネットワーク情報セキュリティマネージャー（NISM）推進協議会が認定するセキュリティ育成プログラムであり、情報セキュリティ技術と情報セキュリティ管理について基礎から専門レベルまでをカバーしており、レベルに応じて以下の資格を設定している。

① ネットワークセキュリティ基礎資格
② ネットワークセキュリティ実践資格
③ サーバセキュリティ実践資格
④ セキュリティ監視実践資格
⑤ セキュリティポリシー実践資格
⑥ セキュリティ監査実践資格

この資格制度は、平成 13 年より開始され、平成 19 年 3 月末現在の資格取得者数は、2,677 人となっている。

【当面の改善策】

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。

【将来に向けて改善すべき事項】

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。

イ　電気通信主任技術者等の活用

【現状】

電気通信主任技術者の選任に関する課題としては、例えば、現在、管理規程における電気通信主任技術者の監督範囲や業務が、主に対象の事業場設備としており、網全体やサービス全体の品質や信頼性確保といった観点での監督・指導に関与していないケースが多いと考えられる。

さらに、電気通信主任技術者は、事業場毎に選任することが原則であるが、無人局や顧客宅内に設置される設備も多いため、拠点からの駆けつけ時間や、設置される設備内容を踏まえ各事業者が選任・届出している。しかしながら、当該事業場の組織上の運営管理者が電気通信主任技術者として選任されているケースや、ネットワークの工事・保守運用業務に直接的に関与しない部門から選任されるケースもあり、日常的な監督や事故発生時対策、総務省への報告やユーザーへの通知、重大事故やヒューマンエラーの再発防止策など日常の設備管理に電気通信主任技術者が必ずしも関与しているとは言えない状況にある。

これらは、電気通信主任技術者の選任義務を定めている法令において、その具体的な選任基準、要件が十分に明確になっていないことにも起因している。

【当面の改善策】

電気通信主任技術者は、引き続き相互接続の拡大や情報通信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

ウ　電気通信主任技術者の資格制度の見直し

【現状】

ネットワークの IP 化の進展により実際のネットワーク運営において、既存の伝送交換、線路といった技術に加え IP 技術の重要性が増している。特にネットワークのセキュリティ管理等のスキルが必要とさ

れており、すでに電気通信主任技術者の伝送交換分野の試験項目にセキュリティに関する項目も設定されている。

一方、電気通信主任技術者については、安全・信頼性確保のためにこれまで以上に重要な役割を担うべきとの意見もあり、その資格制度の見直しも視野に入れる必要が出てきている。

電気通信主任技術者資格者証には、

① 法第 41 条第 1 項及び第 2 項の電気通信事業の用に供する伝送交換設備並びにこれらに付属する設備の工事、維持及び運用を行う「伝送交換主任技術者資格者証」

② 法第 41 条第 1 項及び第 2 項の電気通信事業の用に供する線路設備並びにこれらに付属する設備の工事、維持及び運用を行う「線路主任技術者資格者証」

がある。

試験科目については、平成 13 年 7 月に情報セキュリティに関する項目を追加し、ハッカーやコンピュータウィルス対策等に関する専門的知識の要求に対応するための改正が行われている。

【当面の改善策】

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、資格試験の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」の視点での制度強化、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。

【将来に向けて改善すべき事項】

必要に応じて、伝送交換、線路といった現行の区分を見直し、情報セキュリティや IP ネットワーク管理などを中心とした新たな資格制度について検討することが必要である。

分　類	第４章　情報通信ネットワーク管理に関する対策 └4.1 設計・設備能力管理に関する検討 └4.1.1 ネットワークシステムの容量の適切な計画・設計

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

【現状】

ネットワークの IP 化にともない、重要なネットワーク設備が従来の交換機からルータやサーバ等へとシフトしてきている。

これらの設備等の選定は、電気通信事業者がそれぞれ需要予測を行い、ネットワークの構成や規模を決定し、構築、運用しており、ネットワークの品質基準も各社が独自に設定しているところである。事業者及び機器ベンダーは、これらの点について他社との差別化を図ることにより、より魅力的なサービスを提供すべく競争している。

具体的な手法に関しては、各事業者が個々に安全・信頼性に係る内規や指標を策定し、評価等を行っており、競争戦略上これらを公開することは難しく、使用設備の選定やネットワークの設計等に関して統一的な基準や、定期点検等の共通的な運用方法などは決められていない。

【当面の改善策】

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、必要に応じて適切に見直すことが必要である。

事業者ごとに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（Mean Time Between Failure 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。

【将来に向けて改善すべき事項】

設備やネットワークの許容限界の設計方法等の研究開発について検討が必要である。

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

【現状】

通信量が装置（交換機等）の処理能力を超えると、他の装置へも連鎖的に影響を及ぼし、ネットワークの機能を広範囲に麻痺させるおそれがある。事業者は、こうした事態を未然に防ぐため、トラヒック量の把握や需要を予測したうえで、設備の増強を計画・実施している。

しかしながら、IP 電話の急速な普及などにより、予想を超える通信量の発生による能力超過や、装置が当初想定していた能力を発揮できないことによる能力超過等により、通信サービスが広範囲かつ長時間にわたり停止・機能低下する事例が発生している。

近年、IP 電話が急速に普及して、社会インフラとしての重要性も高まりつつある中、これらの課題に対する対策が急務となっている。

【当面の改善策】

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。

【将来に向けて改善すべき事項】

障害拡大防止や、障害の極小化対策において共通に適用できる具体的事項のガイドライン化について検討が必要である。

ネットワークに障害が発生した場合においても重要通信が確保できるよう、事業者を跨って迂回措置を講ずる等、事業者間で連携が可能となるような仕組みについて検討が必要である。

10 年後のトラヒック予測等について、有識者、事業者、ベンダーで検討し、将来ネットワークに必要な設備や機能の開発を各ベンダーが推進していく必要がある。また、ベンダーでの開発が推進されるように、支援体制について検討していく必要がある。

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

【現状】

HATS 推進会議（高度通信システム相互接続推進会議）が昭和 63 年に設立され、ネットワークに接続する高度な通信機器やシステムの相互接続性を確保するための相互接続試験を実施している。

IP 網における相互接続性については、従来の音声網の相互接続にならい、関連する事業者間で接続試験の項目、事前試験手順などを協議して実施しており、試験の中には一定の準正常、異常処理のチェックも含まれている。しかしながら、想定外のふくそうや異常時を想定した事前試験については、商用時と全く同じ条件、環境を再現することは困難であるため、その精度には限界がある。また、近年のワイヤレス高速モバイルアクセス網等では、適応変調・MIMO（Multiple Input Multiple Output：限られた無線周波数帯域で大容量伝送を実現する無線技術）などの高度な技術が利用されるため、機器間の相互接続性は一段と条件が厳しくなり、理論的な通信速度を達成できないなどの状態が起こり得る。このような場合に NAP（ネットワークアクセスプロバイダ）が、IP 網への入り口となる無線基地局との間で問題を全て切り分け、個別に検証し・障害情報を管理するのは困難である。また、高速ネットワーク利用を目的とした電波利用ではセル間干渉や他の無線業務からの混信により、キャリア毎の WAN、小規模 LAN に比べて異常事象の把握が難しいため事前の試験確認にも限界が生じている。

IP 網は比較的安価にネットワークを構成することができるため、従来に比べ新規参入が容易であるため競争も激しく、各事業者は、新サービスを早く市場にリリースし優位性を保つ必要に迫られている。また、IP 網の装置は従来の装置と比較すると、製品サイクルが短く接続性試験の頻度が従来ネットワークの構成装置に比べ増大する傾向にあるが、各事業者が採用する通信方式や設備に独自性があり、また、マルチベンダーにおける検証環境の構築・準備はコスト面を含めて大きな負担になるため、実運用と同等のアプリケーションを含む相互接続性を事前に検証する共通的な仕組みを事業者間で共有することは難しい課題となっている。

【当面の改善策】

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。

【将来に向けて改善すべき事項】

相互接続性の検証に関しては、事業者とベンダー等が共同で装置間の相互接続検証を行うための実験環境の構築と運営・管理体制を検討することが必要である。

その検証をもとに、事業者間での技術事項、保守運用確認書、重大故障時の対応手順を具体化するとともに、事業者間標準の網管理インタフェースの定義とシステム化による試験時間の短縮、相互接続検証試験の自動化の研究・開発を行うことが必要である。

総務省や公的機関は、第三者により通信速度・品質などについて客観的に評価・管理する仕組みを検討することが必要である。また、ベンダーや事業者などの協力を得た上で、技術基準適合証明などとは別に、相互接続性や通信品質を確保するため、無線ネットワーク機器や端末の接続試験環境を整備するとともにその運用母体について検討することが必要である。

公的研究機関においては、実運用上の予期しない事態に備え、電波の基礎的な性質に立ち戻って現象を分析し対応可能な研究体制を維持・構築していくことが求められる。

エ　サーバ等機器の事前機能確認の充実

【現状】

各事業者が個々にサーバ等設備の事前機能の確認を行っている。競争戦略上これらを公開することは難しく、サーバ等使用する設備や構成も異なっている。危険抑止ために必要な実装機能等の明文化や、事業者間、ベンダーでの共有化は行われていない。

【当面の改善策】

サーバ等機器の事前機能確認は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。

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

【現状】

各事業者の使用設備やネットワーク構成は異なっており、障害を未然に防ぐ対策については各社のノウハウとなっている部分である。しかし、IP 電話をはじめとする IP 系サービスについては、複雑なシステム構成や多様化された技術要素等により、原因特定や対処に時間を要しているケースが増えている。

【当面の改善策】

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、情報通信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、ベンダーが情報通信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。

カ　産学官連携による事前検証体制の構築

【現状】

通信トラヒックの定期的観測・分析の仕組みや運用手順、閾値の設定・管理、設備増強の考え方等は、各事業者で規定し運用している。

しかしながら、昨今、ネットワークの IP 化に伴い、通信プロトコルの階層化や特性により、制御フレーム送受信の増大、障害時の再送の増大など、想定していないことが原因でふくそうが発生するといった事態が発生している。例えば、先般の IP 電話の大規模な障害では、故障への 1 次対処の後に周辺サーバに負荷がかかるなど、従来の経験では予想できないネットワークの挙動が発生し、その結果、障害が拡大し復旧までに長時間を要している。

また、今後は新しく導入されるサービスの障害について考慮することが必要であり、従来の経験が活かせないケースが増加していくことが考えられる。

IP ネットワークが社会インフラとなってその重要性が増し、サービスの高度化・多様化が進むにつれ、こうした問題を解決するために、IP ネットワークの挙動についての研究開発に産学官連携して取り組む必要性が高まっている。

【当面の改善策】

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。

【将来に向けて改善すべき事項】

- 階層間の送達確認の低減、再送の抑止など制御フレームトラヒック抑止等の通信プロトコルをベンダー主導で開発していくことが必要である。
- 運用技術の研究開発連携は事業に近いため、共通テストベッド等を事業者、ベンダーなどが利用しやすい共同研究契約スキームを検討することが必要である。
- 単独でも大規模試験が可能な実ネットワークに近いテスト環境の構築を検討する。また事業者のトラヒックパターンを共同研究目的に開示する方法の検討も必要である。
- 電気通信設備自身が自己診断や隣接ネットワークの監視を行い、異常検知時に障害情報を自動通報すること等によりサービスを停止させないデペンダブルなネットワーク技術の研究開発等に取り組むことが必要である。

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

【現状】

ネットワークの IP 化により、システムのオープン化とインタフェースの標準化を背景に、複数ベンダーからのシステムの調達やアウトソーシングが急速に進展した。一方、ベンダーから調達等した設備

の回路構成やソフト内部構成はノウハウにかかわる部分であること等から事業者に対して情報は開示されていない状況である。その結果、障害が発生した場合、最終的な回復や原因究明はベンダーに依存せざるを得ないものとなっている。
　通常、これらの設備に必要な要件定義や接続構成等のシステム設計は各事業者が行っており、設備や構成は事業者毎に異なるため、検査・品質測定手法の共通化等はされていない。
　また、事業者が実施できる検査や品質測定には限界があり、例えば、過負荷試験などで十分でない場合がある。

【当面の改善策】
　情報通信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。

【将来に向けて改善すべき事項】
　システムの一層の安全・信頼性を向上させるために、高度な機能の実装、検査、評価手法について研究開発が必要である。

ク　ソフトウェア選択基準の明確化

【現状】
　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っている現在、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も高まっている。
　業界における「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）」において、ソフトウェアの管理についての記載がある。各事業者は各社のソフトウェア選択基準に則り、自主的に導入をしている。

【当面の改善策】
　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。

【将来に向けて改善すべき事項】
　技術の進歩が激しく、将来的には利用者が守るべき事項とともに、事業者が持つべきセキュリティ機能のひとつとして共通項目をガイドライン化することを検討する必要がある。

分　類	第４章　情報通信ネットワーク管理に関する対策 └4.1 設計・設備能力管理に関する検討 　└4.1.2 開発及びサポートプロセスにおける管理

ア　保守点検の手順書の作成

【現状】
　事業者はベンダーから提示される装置の保守マニュアル等を活用しつつ、自らのネットワーク全体の保守に必要なドキュメントを自ら作成し、運用している。ドキュメントには保守点検項目や、保守手順や運用方法を盛り込んでいる。
　こうしたドキュメントは定期的に見直し、最新化する必要がある。

【当面の改善策】
　各事業者はサーバなどネットワーク機器の保守点検項目、保守手順、運用方法をドキュメント化し、ネットワーク構成の変更、ソフトウェアのバージョンアップ、パッチ適用による変更を迅速に織り込める維持管理を徹底する必要がある。
　同様に装置の管理方法（設置、移動、処分等）も各事業者においてドキュメント化し、規定の遵守を徹底する必要がある。

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

【現状】

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、運用開始後に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。

【当面の改善策】

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。

ウ　セキュリティチェックのための体制

【現状】

セキュリティ確保は業界全体の課題と認識されており、事業者、ベンダー共に ISMS 等のセキュリティの確保、認証取得に取り組んでいる。

【当面の改善策】

各事業者は、セキュリティチェックができる体制を構築するとともに、セキュリティ意識を高めることが必要である。具体的な手法については、各事業者がそれぞれに対応する対策を講じることが適当である。

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

【現状】

現状ではセキュリティの脅威に対し、利用者の注意による防止策が依然として最も効果的な対策となっており、「させない」防止策については効果的な方策が少ない状況である。

セキュリティの脅威に対し、事業者間で事象を共用することはしていない。

また、維持・保守などサポート運用プロセスや開発プロセスでの情報漏えいなどの対策も充分とれていない場合がある。

【当面の改善策】

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、セキュリティの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。

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

【現状】

電気通信事業者は、工事の際の安全性の確保について十分配慮を行っているが、通信インフラが生活に欠かせない要素になっている現状を踏まえると、一層の安全性確保のための対策が求められている。

【当面の改善策】

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。

【将来に向けて改善すべき事項】

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。

カ　安全かつ容易な設備増強、拡張性確保手法の確立

【現状】

各事業者が構成の異なる IP ネットワークを構築・運用している。

中長期的トラヒック対策として、設備設計に反映する基礎データ収集のためにトラヒック量収集機能と設備設計機能を連携させるシステムの統合化が行われているが、機能が複雑になっている。

また､ネットワークの IP 化等に伴う新たなサービスに対する需要に対応できないなど設備増強の判断ミスによる事故が発生している。さらに、設備増強のための工事において作業ミスが減らない状況がある。その上、個々の通信設備へのトラフィック集中度が高くなっているため、工事ミスなど判断・手順を誤った場合のサービス提供への影響が拡大する傾向にある。

【当面の改善策】

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。

【将来に向けて改善すべき事項】

メンテナンス時においても、無中断でサービスを提供することについてガイドラインを策定することが適当である。

分　類	第４章　情報通信ネットワーク管理に関する対策 └4.2 保全・運用管理に関する検討 └4.2.1 故障検知・解析

ア　運用監視体制の充実

【現状】

電気通信回線設備を設置する事業者は電気通信事業法で定められた技術基準にしたがい、故障を速やかに検知することが義務づけられており、速やかに検知・回復処置が行えるよう 24 時間 365 日の運用体制を実施している。ただし、運用監視の対象範囲は付帯系装置を含めると事業者判断となっているため、対応にばらつきがある。

【当面の改善策】

事業者ごとに使用している製品やネットワークの構成が異なるため、共通的なガイドラインを作成することは難しいが、迅速な障害対応等を行うために各事業者がサービス特性や重要性などを考慮して運用監視体制の改善に取り組んでいくことが必要である。

イ　相互接続時のネットワーク管理体制の強化等

【現状】

情報通信ネットワーク安全・信頼性基準において、情報通信ネットワークの動作状況の監視、保守及び制御等について規定されており、各事業者は、法令や安全・信頼性基準等を踏まえて、自らが運用するネットワークの監視を実施している。

事業者内のシステムの統合監視や障害の切り分け機能の具備についての要求条件は、各事業者の運用ポリシーや運用規模に委ねられること、また、対象となる通信設備の仕様や管理要求も異なることから、事業者横断的に実装可能な共通要件の策定、維持管理は困難である。このため、事業者間や事業者と顧客との間の監視情報、制御方法、相互に確認すべきセキュリティ確保を含むシステム間接続用インタフェース（情報定義、プロトコルなど）の標準化を検討することが有効と思われる。(ITU-T　電気通信網管理（TMN）勧告シリーズ参照)

現行のネットワークにおいてはそれぞれの事業者が、システムの運用監視をしており、障害の切り分けについても、各事業者が技術・ノウハウを保有蓄積し、こうした運用の良否が、他社との差別化のひとつとなっている。

さらに、物理的な制約から同一拠点内で複数の部門が設備の監視・管理を行い、装置ごとに運用ノウハウも異なるため運用部門が分散するケースもある。その結果、複数の監視システムを複数の監視体制で運用したり、業務規模によりネットワーク毎に別組織で運用したりするなど、全体を統合した運用体制を整備するのが難しい状況にある。

【当面の改善策】

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。
　事業者内のシステム監視は各事業者により実施するものであるが、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。

【将来に向けて改善すべき事項】
　事業者間の情報交換を効率化するための仕組み（例：共通インタフェースの仕様化など）の検討が必要である。
　サービス単位・装置単位の監視を実施するとともに、ユーザー単位での監視をすることにより、ユーザー～サービス提供者の間の一貫した運用監視が可能になる。よって、ユーザーを一元的に監視するシステム、及び監視体制の両方を具備していく必要があり、この手法について研究・開発することが必要である。
　また、ベンダーは、障害発生時に保管した検出手順・復旧手順について、事業者から供給を受け、故障切り分け機能向上（自動化等）を研究・開発することが必要である。

ウ　問題発生時に検知、通報する機能や体制の確立

【現状】
　問題発生時の検知・通報は、事業用電気通信設備規則に「故障検出」としてその故障を直ちに検出し保守者に通知する事が定められている。各事業者は当該規則を遵守するべく対策を行っているところである。
　スパム等の攻撃の検知は、トラヒック流量等の定期的な統計情報を、ネットワーク運用者が一括してチェックすることにより検知している。また、このようなネットワーク運用者が検出した検知情報に関しては、人手を介して関係部署に通報されている。

【当面の改善策】
　問題発生時に確実に検知、通報する機能や体制を構築していくことが必要である。
　なお、具体的な運用については、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て運用を行っていくことが適当である。

【将来に向けて改善すべき事項】
　ネットワークの IP 化の進展に伴い、ネットワークへの攻撃パターンも複雑化し検出が困難になる事態が予測される。このような場合でも攻撃を受けにくく、攻撃の検出・回避が可能なネットワーク構成・機能について、研究開発を行う必要がある。
　スパム等の攻撃への対策は、ネットワークのノード間で相互に収集した統計情報等を交換しあい、その情報に基づいて各ノードが自律的にスパムであるかを判断し、遮断する手法の研究開発が必要である。そのためには、各ノードでの検出、遮断の情報を一括して管理し、それによる影響度合いを判断して関係部署に通知するシステムの実現が必要である。

エ　IP ネットワークの早期異常検知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

【現状】
　各事業者が異なるネットワークを構成しており、設備監視技術等はノウハウの部分となっている。このため、現状では、これらのノウハウの事業者間共有、意見交換及び共同研究などは行われていない。

【当面の改善策】
　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。

【将来に向けて改善すべき事項】
　早期異常検知や予備系への切替、エンドツーエンドのスループット低下、レスポンス遅延、劣化など

通信異常の把握等の研究開発が必要である。

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

【現状】

情報通信ネットワーク安全・信頼性基準において、保守・運用作業の手順について規定されており、事業者は、法令や安全・信頼性基準等を踏まえて、保守・運用作業の手順化を実施している。現在の故障箇所特定のためのデータ取得手順、切り分け手順は、使用している機器ごとに異なっている。

故障箇所特定のためのデータ取得手順については、大規模ネットワークにおいては運用システム毎に異なっており、サーバでは、ベンダー独自のシステムログを取得し障害箇所の特定を行っているケースが多い。また、定期的にヘルスチェックを行い、運用されているサーバの潜在的な故障の有無を自動的にチェックしたり、電気通信設備に対する工事等のイベント前に保守者がヘルスチェックを行なったりするなど、運用中以外にも故障を検出する場合がある。

故障箇所の切り分け手順については、事業者内のシステムの統合監視や切り分け機能の具備についての要求条件が、各事業者の運用ポリシーや運用規模により異なるため、通常は各ベンダー及び事業者毎に策定されている。

このように、対象となる通信設備の仕様や管理要求も異なることから、相互に確認すべきセキュリティ要件やシステム間の標準インタフェースを検討することが有効と考えられる。

【当面の改善策】

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

【将来に向けて改善すべき事項】

故障原因の特定に対しては装置単体での解析には限界があり、複数ベンダー内のデータを迅速確実に収集する手順の共通化が重要になる。また、収集後のデータは過去の事例に対応づけてデータを分析し、再発防止手順を導き、その手順を事業者の運用手順に反映させることが必要であるため、自動化などによるアプローチを研究開発することが必要である。

また、事業者間等の情報交換の効率化を促進するための仕組み（例：共通インタフェースの仕様化など）が必要である。

カ　故障箇所の特定及び故障原因の特定の迅速化対策

【現状】

IP ネットワークとサービスを構築する設備の多くは、導入の効率性から汎用製品（サーバー、基本ソフト・ミドルウェアなど）を利用したシステム開発が主流となっている。

これらのシステム内にも故障を検知・特定する仕組みがあるが、想定外のトラヒックによる処理遅延、ソフトウェアバグなどによるサービス品質の劣化を検知する機能や、故障原因を迅速に切り分け・特定する機能が十分とはいえない。そのためこれらのシステムとは別に、外部にトラヒックやリソースの状態を監視する個別システムを追加設置して、異常の監視や故障箇所の切り分けを行っているケースが多い。

また、汎用製品の組み合わせで通信システムを構築するため、一旦、複雑な故障が発生すると解析ルートが複数ベンダーを経由するなど、故障処理・改善体制が複雑化する傾向にあり、さらに装置毎にメンテナンス方法が異なるなど故障箇所の特定や原因解析に時間を要することが多い。これに加え、ベンダー間の相互接続性は向上してきているが、サービスの拡大によりネットワーク構成も複雑化しており、メンテナンス性は低下する方向にある。

さらに、事業者においては 1 次保守（監視、故障装置切り分け、サービス回復作業）を行い、ベンダーが二次保守（切り分け支援、故障に対する代替品提供）および故障原因の解析を行なう形態が多いが、故障発生時、1 次保守者はサービス回復を優先するため、その後の故障解析に必要なログを充分に取得できない場合もある。また、事業者からベンダーへ提供される情報が限定的であり、事業者の使い方や

事業者の設計ポリシーが理解できないと的確な分析が出来ないケースもある。
故障特定に関しては特定のスペシャリストへの依存度も高く技術者の確保・育成も課題となっている。

【当面の改善策】
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

【将来に向けて改善すべき事項】
保守者がログ等取得しなくても機器が自律的に原因究明できる機能を具備することについて研究開発していくことが必要である。

キ　原因の究明を迅速に行うための分析技術の研究開発

【現状】
原因究明に必要なログ収集はログ収集サーバを設置するなどして、事業者が個々に対応している。また、事業者のログ収集対応や原因の究明方法については、事業者とベンダーの保守契約内容によるものであり、事業者間等で共通化や共同研究されているものはない。
現在、IP ネットワークに関連する事故では、原因を究明するのに必要なログが取得できない、又は直ぐに把握できないために、復旧に長時間要することが度々起こっている。

【当面の改善策】
事業者が使用している製品やシステム構成が異なるので共通的な仕組みの研究開発は難しいが、事業者が原因究明を確実に行うためのベンダーとの最低限必要な保守運用形態、共有化できる必要事項について検討することが必要である。

【将来に向けて改善すべき事項】
ログ取得を行わなくても、原因究明が行える機能や自動的にログをとる技術について研究開発していくことが必要である。

分　類	第４章　情報通信ネットワーク管理に関する対策 └4.2 保全・運用管理に関する検討 └4.2.2 ネットワークふくそう対策

ア　ふくそう監視手法や事業者間連携

【現状】
IP ネットワークにおいて大規模なふくそうが発生し、長時間にわたりサービスに影響がでる事例が発生している。サービス復旧に長時間を要するのは、対応ノウハウが十分蓄積されていないことや、対応手段が確立されていないことがひとつの要因として考えられる。

【当面の改善策】
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。

イ　ふくそう時のユーザー間の公平性の確保

【現状】

現状の IP ネットワークサービスは、ほとんどがベストエフォート型のサービスである。ベストエフォート型サービスでは、ごく一部の高トラヒックユーザーがネットワークの使用帯域のほとんどを占めるという報告もあり、費用負担の観点から不公平感は高い。

【当面の改善策】

ベストエフォート型のサービスの不公平感の解消や、ふくそう時のユーザー間の公平性を確保することが必要である。

そのために、ユーザーがトラヒックの種類等によって使い分けられる帯域保証型サービスの実現について検討を行うことが必要である。

さらにベストエフォート型サービスを利用しているユーザー間で公平になるようにするためには、例えばネットワーク内を流れるトラヒックを観測し、特定ユーザーのトラヒックがネットワーク帯域を圧迫するような事態に対しては、そのユーザーのトラヒックを制限するといったことが必要となる。実施する場合には、事業者は事前にユーザーにその旨周知徹底を図り、手続きを明確化しておくことが必要である。

【将来に向けて改善すべき事項】

ネットワークに流入するトラヒックの制御、特にベストエフォート型サービスのトラヒックを動的に制御する手法について検討が必要である。

ウ　企画型ふくそうを防止するための情報収集の仕組み

【現状】

事業用電気通信設備規則において異常ふくそう対策として交換設備にふくそうの検出とふくそうを解消するための機能の具備が定められており、企画型ふくそうについても当該規則を遵守するべく事業者が自助努力により対策を進めている。例えば、企業に対して企画型ふくそうのおそれのあるイベントを実施する際には、事前の情報提供を依頼している。

しかしながら、トラヒックの集中によるネットワークへの影響が十分理解されていないこともあり、情報の確実な入手にまでは至っていない。

【当面の改善策】

各事業者が個々のユーザー対応によって情報収集に努める必要がある。

しかし、トラヒックの集中によるネットワークへの影響について一部の企業が、予告無くマスコミを通して受付電話番号を案内し企画型ふくそうを招くような事態を完全に防ぐことは困難である。そのため企画型ふくそうの兆候を迅速に把握し、ふくそう制御が行える仕組み・体制を各事業者が整備することが必要である。

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

【現状】

災害の発生や障害を発端とした異常動作等による通信量の増加が交換機の処理能力を超えると、当該交換機だけでなく、対向している周辺の交換機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、法令において「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、かつ、通信の集中を規制する機能を有するものでなければならない」ことを定めている。事業者は法令に基づき、交換機への接続を制限する機能を設け、トラヒックを常時監視し、基準を超えた場合には警報を出して保守者に通報するとともに、交換機において各種の接続制限を行うことによりトラヒックを適正化する対策を講じている。

しかしながら、近年発生している IP ネットワークサービスの事故では、従来のネットワークで行われてきた手法によるトラヒック制御が十分機能せず、ふくそうが長期化するケースがあり、ふくそう対策の高度化が求められている。

また、おめでとうコール疎通対策や地震災害時の経験に基づき、事業者内および事業者間での連絡・情報交換、利用上の制限、顧客案内などが行われている。

【当面の改善策】
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。

【将来に向けて改善すべき事項】
ふくそうの自動早期検知・予測システムの開発、ネットワーク間設備に対する自動制御やふくそう監視（しきい値設定、予兆観測)による予兆検知時の対応手順、ふくそう発生時の対応手順、ふくそう予測の精度を高めるシミュレーション技術等の研究開発に取り組み、高度なふくそう対処手法を研究開発することが必要である。

オ　ノードが具備すべきふくそう対策

【現状】
IP 化に伴い、1 つのノードで大規模トラヒックを扱う傾向にあり、信頼性の確保が課題となっている。

【当面の改善策】
1 つのノードに障害が発生した場合に極めて広範囲に影響が及ぶことになるため、その集約度に応じたノードのふくそう対策の検討が必要である。現状では、事業者がそれぞれベンダーやネットワーク構成の異なる IP ネットワークを構築・運用していることを踏まえ、大規模トラヒックを扱うノードに具備すべきふくそう対策の検討が必要である。

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

【現状】
異常ふくそうに対しては、事業用電気通信設備規則に「異常ふくそう対策」として、交換設備に対してふくそうの検出とふくそうを規制するための機能の具備が義務づけられており、各事業者は当該規則を遵守するべく対策を行っている。

【当面の改善策】
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を行うことが必要である。(関連項目：5.1.3)

【将来に向けて改善すべき事項】
0AB～J 番号を使用する IP 電話以外の ICT サービスについて、ふくそう対策に関する技術的条件の検討が必要である。
また、今後の技術開発の進展を見て、ふくそう対策について各事業者共通のガイドラインを必要に応じて作成していくことが必要である。

キ　ふくそう発生のユーザー端末への自動通知

【現状】
ネットワーク側でサービスを実現している従来の固定電話と異なり、IP 系サービスはネットワーク側

と端末側の双方で機能を分担し、連携しながらサービスが提供されるようになる。こうした機能分担や連携は、サービスの実現のみならずネットワークの安全・信頼性の確保においても同様である。例えば、発信制限、障害の切り分け、一斉登録防止等の機能を端末側で実現することなどが検討されている。

【当面の改善策】

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。

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

【現状】

災害用伝言ダイヤル等は、災害時等にふくそうが発生し通信規制が行われた場合にも規制の影響を受けることなく安否確認が行えるシステムである。このシステムの利用により、結果として安否確認やお見舞い電話の件数を減少させることができるため、ふくそう軽減策として非常に有効である。

「平成 17 年度電気通信サービスモニターに対する第 1 回アンケート調査」の結果においても、大規模災害発生時における家族や知人との安否確認等の連絡に有効な通信手段については、回答者の約 6 割が災害用伝言ダイヤル（音声によるメッセージ）を有効な通信手段と認識されている。その他にも、携帯電話又は PHS が 50.1%、携帯電話からのメールが 46.7%%、固定電話（自宅、会社等）が 45.2%%となっており、災害用伝言板（携帯電話からのテキストメッセージ）は 33.6%、公衆電話は 32.5%との選択率となっている。

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。

【当面の改善策】

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。

ケ　災害時における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

【現状】

災害時のお見舞いコールの大量発生など、ユーザーの振る舞いに起因し突発的に増大するトラヒックによるふくそうに即時対応するため、事業者がそれぞれネットワーク内のトラヒック監視・制御手段を用意し、体制を構築している。

また、停電復旧時や地震の揺れによる受話器の一斉脱落、水害時の電話線の短絡などによって一斉に呼が発生するなど、ユーザーの振る舞い以外にも通信設備への負荷が突発する事象があり得る。従来の固定電話設備では、これまでの経験に基づき対策が施されている。

さらに、IP 電話端末に特有な事象として、停電復旧時一斉にサーバアクセス（REGISTER 登録等）が発生し、通信設備に負荷が集中する事例もあった。

【当面の改善策】

災害時における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について、アナログ電話での経験を参考にしつつ、IP 電話等においても検証を行うことが必要である。

【将来に向けて改善すべき事項】

技術検討作業班での IP 電話の一斉発呼、一斉登録防止機能についての検討結果を踏まえて、各事業者がそれぞれ自らのネットワークにふさわしい具体的実現手法を検討することが必要である。

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

【現状】

ネットワークの IP 化により一つの故障がネットワークの広範囲に影響を与える傾向がある。そのため、ネットワークの安全・信頼性を確保するためには、レガシーネットワークと比べて冗長度の高い構成を検討する必要がある。

【当面の改善策】

各事業者が自らのネットワークにふさわしい安全･信頼性対策を講じる必要がある。そのためにも様々な研究開発状況を把握し、新しい技術を適時取り入れることが必要である。

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

【現状】

問題発生箇所の検知・通報については、現在、事業用電気通信設備規則に「故障検出」としてその故障を直ちに検出し保守者に通知することが規定されている。また、異常ふくそうに対しても、事業用電気通信設備規則に「異常ふくそう対策」として交換設備はふくそうの検出とふくそうを解消するための機能を具備し、相互接続した他の事業者へ影響を及ぼさないようにすることが規定されており、各事業者はこの内容を遵守し必要な対策を行っている。

ふくそうの種類には、サービスを提供するサーバのふくそう、パケットを流通させているネットワークのふくそう、と大きくわけて 2 つがあり、それぞれのふくそう対策をさらに強化する必要がある。

サーバのふくそう対策が困難になっている原因としては、サーバのふくそうが途中のネットワーク機器（ルータ等）のトラヒック制御に反映されないこと、端末のふくそう対策が十分でないこと等が考えられる。

ネットワークのふくそう対策が十分でない原因としては、詳細なトラヒックの監視ができていないこと等が考えられる。各ノード（ルータ、スイッチ等）を流れるトラヒック量の総量のみを監視しているケースが多く、この手法ではネットワークのふくそうが発生する可能性が高いと推測される箇所を特定することができる程度である。

通信トラヒックの定期的観測・分析の仕組みや運用手順、閾値の設定・管理、設備増強の考え方は各事業者が規定し、運用している。また、イベントや災害などに起因する突発的なトラヒックによるふくそうへ即応するための監視・制御の手段および体制は事業者毎に策定し、実施している。

しかしながら、IP ネットワークでは映像配信などによるトラヒック増に加え、通信プロトコルの階層化や通信プロトコルの特性より送受信される制御信号が多く、障害時には制御信号の再送により通信量が増大し思わぬところでふくそうが発生するなどの事態を招いている。また一度ふくそうが発生すると沈静化までに長時間要するのが現状である。

今後 IP 化されたネットワークを相互接続するにあたって、運用品質のばらつきを防止し IP ネットワーク全体の運用品質を維持・向上させることが必要である。

【当面の改善策】

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。

【将来に向けて改善すべき事項】

障害の中でふくそうは理論的にも困難な問題で研究開発が特に必要な領域である。

サーバのふくそう対策については、ルータをサービスアウェアにしサーバのふくそう状態をネットワーク層のふくそう回避機構へと伝えるクロスレイヤ制御等の研究開発が考えられる。また技術検討作業班で検討された端末での無効呼抑止機能、一斉登録に伴うふくそう回避機能、自動発信回数の制限などの具体的実装について検討が必要である。

ネットワークのふくそうについては、各リンクの帯域使用量を管理し、帯域に空きがある場合に一時的に帯域を割り当てるアドミッションコントロール等ネットワークに流入するトラヒックのコントロール方法について検討することが必要である。またトランスポート層やアプリケーション層のレベルでトラヒックを分散できる L4 スイッチ、L7 スイッチ、フロールータ等を活用したふくそう対策についても研究開発が必要である。

さらに IP 化されたネットワークを相互接続するにあたっては、技術検討作業班での検討を踏まえ、事

業者間の運用品質のばらつきをどのように克服するかについて検討が必要となる。
また、階層毎の送達確認や再送による制御信号の増大を防ぐ通信プロトコルの検討および開発が今後必要である。

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

【現状】

検証試験等に用いる集中呼パターン情報は、各事業者における過去の障害事例や想定で検討され、また各通信設備のベンダー側でも独自のトラヒックパターン及び試験機器により実施している。しかしながら、通信設備やトラヒックプロファイルを商用と同じ環境で事前試験することは困難なことから、障害時の集中呼パターンや連携する現用システムを含めた組合せ試験を全て実施するには限界がある。

また、設備のマルチベンダー化、トラヒックの変動要素が大きいこと、提供サービスの複雑化、時間的制約があること等から、必ずしも十分な試験が出来ず、故障やふくそうの再発防止に有効に機能しないケースがある。

【当面の改善策】

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

【将来に向けて改善すべき事項】

新たなサービスについてパターン試験方式の開発や集中呼のパターン情報を蓄積・解析することによる再現方法の開発、検証試験の為のネットワークモデルと試験項目の開発など事業者接続によるテストベッドによる共同実験などの可能性について検討が必要である。

分　類	第４章　情報通信ネットワーク管理に関する対策 └4.2 保全・運用管理に関する検討 └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

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

【現状】

電気通信事業は、社会経済活動に必要なサービスを提供する公共性の高い事業であり、継続的・安定的なサービス提供が求められる。このため、大規模で長時間のサービス停止等が発生した場合、事業者は、電気通信事業法第 28 条に基づき、その状況を国に報告する義務を負っている。報告の対象となる重大な事故の基準は、電気通信事業法施行規則第 58 条で規定されており、それ以外は各事業者の判断により自主的に報告、及び対外告知を実施している。

各事業者とも電気通信事業法に対応するため重大事故対策・報告体制を整備しており、報告する事故の基準についても、総務省と事業者の間で適時確認が行われている。

一方、ICT サービスの多様化や国民生活への浸透に伴い、故障やサービスの遅延などの情報をより迅速、よりきめ細かく報告・公開することについて利用者のニーズが高まっている。

しかしながら、IP 系ネットワークでは、基準の時間には満たないものの、従来想定していた規模をはるかに上回る規模の事故の発生や、「電話がつながりにくい」「メール等の遅延」などサービスの停止に至らないものの社会的影響が大きい事故が発生するケースが増加しているが、これらは現行の基準では報告義務の対象にはならない等、重大な事故の報告基準が必ずしも現状の ICT サービスに適応していない場合がある。

【当面の改善策】

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、

①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、今後さらに必要となる対策や改善措置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。

②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もと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。

【将来に向けて改善すべき事項】

情報の自動配信、広報周知の迅速化、情報検索などのシステムの検討が必要である。

イ　多様なメディアによる障害内容の利用者への提供

【現状】

各事業者ともサービスの停止など重大事故発生時はお客様に対する情報提供に努めており、災害時などでは随時マスコミを通じての周知も行われている。

現状では、障害内容や復旧状況の情報通知手段としてはホームページへの掲載が主流である。事業者によっては、企業ユーザーへ能動的に故障を通知するサービスや、希望するユーザーに対して、障害情報をメールやファクシミリで配信するサービスを開始しているが、これらの情報伝達に関して共通のルール・基準は設けられていない。

故障発生時の周知については、現在、次のような課題が認識されている。

・メールシステムの遅延・故障時は、事業者のホームページでの情報提供の他は、広く周知する手段は限られており、コールセンターや営業所などへの問合せ・苦情となって連絡され、その都度、説明・対応しているケースが多い。また、同時に多数のサービスに影響がある場合には、利用者・関係者に的確なルートでタイムリーに必要十分な情報が提供できない場合がある。

・障害時は、IP 網に限らず故障やふくそうの発生箇所により無音のまま接続できないケースや、エラー、トーキー接続が適切に行えない場合も発生する。また、障害によっては、話中音が流れるケースがあるなど、利用者が障害発生に気づかない場合や、端末側かネットワーク側かの区別が簡単には判別できないことから、これらがふくそうに拍車をかける要因ともなっている。

・利用者はホームページに障害情報が掲載されていることを認識していない、または認識するのが遅れるため、掲載された障害情報をタイムリーに得られない場合がある。

なお、情報通信審議会（IP ネットワーク設備委員会技術検討作業班）では、0AB～J 番号を使用する IP 電話端末については、発信時にネットワークがふくそうしている旨のエラーレスポンス等の通知を受けた場合は、再呼を抑止するために利用者に対し、その旨を何らかの方法で通知する機能を有することが必要であり、端末への実装に関する標準化を図るなどしながら、普及促進を図ることが必要であることが答申されている。

【当面の改善策】

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。

【将来に向けて改善すべき事項】
業界団体等において、事故・障害情報等の情報伝達手段や内容に関するガイドラインの作成と周知が必要である。
災害時なども考慮した重大故障の発生状況など、事業者共同のホームページ運営、放送等のマスコミ利用、広告塔などの設置や交通機関情報での定時周知等が必要である。また、障害情報について集中的に提供する方法と周知手段の検討が必要である。
事業者とベンダーが連携して、技術検討作業班での検討を踏まえ、利用者の端末に事業者の設備にて障害が発生していることを表示する機能の開発、具備を推進する必要がある。

ウ　他社ユーザーへの障害情報等の提供

【現状】
各事業者がお客様対応の窓口を設定するとともに障害内容、復旧状況等について、報道発表、事業者のホームページ掲載等により情報提供しており、他事業者のユーザーは必要な場合には、事業者のホームページ、報道等により情報を入手している。各事業者判断にて実施しているホームページでの告知は、自ユーザーだけでなく他ユーザーも閲覧可能であり、必要により相互接続事業者間での情報提供方法（内容、通知方法等）を取り決めて実施している。
一方、複数の事業者にまたがる場合の情報連絡等について想定されるケースを明確化していく必要がある。情報セキュリティに関連する共有の仕組みである T-CEPTOAR の活用も含め、今後どのような場で情報共有すべきかを検討していくことが必要である。

【当面の改善策】
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。

【将来に向けて改善すべき事項】
電気通信事業者協会（TCA）、総務省など共同運営による事業者情報、サービスの停止情報等の能動的かつタイムリーな公開方法の検討を行うことが必要である。

エ　利用者等への対外的な公表基準の策定

【現状】
電気通信サービスへの影響がある事故発生時等には、事業者はそれぞれ基準を定めて、必要と判断するものについては、ホームページや報道機関への発表を行う等の手段により、利用者への告知を実施している。これらの実施は各社の判断に委ねられており、実施の判断、実施までの（目標）時間、内容、方法、障害回復後の掲載期間等についての業界統一的な基準はない。
また、正確性を求めるあまり情報の提供が遅くなる事例がある一方、情報提供を急ぐために提供される内容が詳しくないといった指摘もされている。また、障害の状況説明がユーザーにとって適切でない事例もある。
現在、総務省では、重大な事故の発生状況に関する個別の情報は公表していないが、これらの重大な事故の発生状況については、情報の公開を望む声も出されている。

【当面の改善策】
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。

分　類	第４章　情報通信ネットワーク管理に関する対策 └4.2 保全・運用管理に関する検討 └4.2.4 重要通信の確保

ア　ネットワークの IP 化に対応した重要通信の確保

【現状】
電気通信事業法第 8 条において、「天災、事変その他の非常事態が発生し、又は発生するおそれがある

ときは、災害の予防若しくは救援、交通、通信若しくは電力の供給の確保又は秩序の維持のために必要な事項を内容とする通信を優先的に取り扱わなければならない。」と定めている。その際に重要通信を優先的に取り扱った結果、他の通信を取り扱えなくなる事態を想定し、「必要があるときは、総務省令（電気通信事業法施行規則第 56 条）で定める基準に従い、電気通信業務の一部を停止することができる。」としており、告示において具体的な機関名を定めている。

昨今、社会情勢の変化等により、告示に規定されている重要通信の対象機関以外の機関から、通信の優先的取り扱いに対する要望が複数あがっている。最近では、平成 17 年 7 月 23 日に発生した千葉北西部地震において、多数のエレベータが停止したが、復旧の際に、エレベータ保守会社の本部とエレベータ保守要員の間で携帯電話による連絡がとれず、結果として、現場に向わせる指示に支障を及ぼし、復旧に手間取るなどの問題が顕在化した。その後、首都直下型地震等の災害に備えるため、これらのエレベータ保守会社や、災害時に警察からの指示により車両の撤去作業を行う団体、災害時にライフラインを確保する電力設備保守会社等から新たに災害時優先電話の指定についての要望があがっている。さらに、携帯電話の普及により、消防、救急等の緊急機関の人命救助の場面等において携帯電話の利用が増加し、災害時において、より多数の電話が災害時優先電話として扱えるよう要望があがっている。

一方、重要通信の取り扱いの具体的手法やその運用基準については、各事業者にゆだねられており、システム方式や設備容量等を考慮して独自に運用している。

なお、政府の方針としても「セキュアジャパン 2006（情報セキュリティ政策会議決定）」で 2008 年までにネットワークの IP 化に対応した重要通信運用技術を確立することとしている。

【当面の改善策】

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。

【将来に向けて改善すべき事項】

今後、電話以外の多様な ICT サービスの実現が想定され、重要通信に関する社会的コンセンサスを踏まえた上で、こうした多様な通信手段を、災害時や緊急時に利用できる可能性の検討が必要である。

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

【現状】

広域分散受理等の対策はすでに一部の事業者で導入されているところであるが、大規模な災害発生時には現在のシステムで設備容量の不足が懸念されているところである。

IP 化されたネットワークでは、アナログ電話のようにネットワーク側が機能を持つだけでなく、ネットワークと緊急通報受理機関側の双方で機能を分担し、連携しながらサービスの提供が行われると考えられる。

【当面の改善策】

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。

ウ　誰もが容易に緊急通報できる手段の確保

【現状】

各緊急通報受理機関で検討が行われており、一部では緊急通報としてではなく一般の通信としてメールによる通報を実施している機関もある。

また、携帯電話や IP 電話について、平成 19 年 4 月 1 日からは音声通話に併せて緯度経度等の位置情報を通知する緊急通報の位置情報通知の制度が施行されている。

【当面の改善策】

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。

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

【現状】

110 番通報などを行った際は、発信者の住所等から最寄りの緊急通報受理機関に接続される。各事業者は、この機能を実現するために、電話の設置場所住所（基地局設置場所住所）と最寄りの緊急通報受理機関との関係をしめすデータベースを構築している。当該データベースは、行政区域の変更、緊急通報受理機関の管轄変更、基地局の追加、利用者の追加などの際に変更、追加が必要となる。

一方、近年これらのデータベースの入力誤り等により、110 番通報ができないといった事例が毎年数例報告されている。

緊急通報は、安心・安全な生活を実現するために重要であり、これらのトラブルを根絶することが重要な課題となっている。

【当面の改善策】

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。

【将来に向けて改善すべき事項】

位置情報（住所や緯経度）と緊急機関を選択することで適切な緊急通報受理機関を選択できる共通のシステム構築の可能性もあることから、将来の通信システムの検討の際に導入の可能性を検討することが適当である。

分　類	第４章情報通信ネットワーク管理に関する対策 └4.3 情報セキュリティ管理 　└4.3.1 社内の重要情報の管理

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

【現状】

電気通信事業者はサービス提供を行う上で、加入者情報、システム情報等様々な情報を取り扱っている。これらの情報の取扱いについては、電気通信事業法等の法令や「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）」で加入者情報やネットワークシステム情報等の管理の基本的事項や管理基準が策定されている。特に、個人情報の取扱いについては、「電気通信事業における個人情報保護に関するガイドライン（平成 16 年 8 月 31 日総務省告示第 695 号）」において基本的事項が定められている。

電気通信事業者は、これらの法令やガイドライン等に沿って、加入者情報等の重要情報の管理方法を内規等で具体的に定めることにより情報の管理を行っている。

しかしながら、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る。また、流出する情報についても個人情報に加え、電気通信システムのセキュリティに係る情報等も見受けられる。

【当面の改善策】

加入者情報やネットワークシステムの情報等について、情報の重要性を分類し、それぞれ管理基準を適切に設定することは、セキュリティを確保しつつ経済性を確保するために必要である。特に最近の情報流出が後をたたない状況を踏まえ、加入者情報、システム情報等の情報の分類を行い、さらに、これらの分類が適切であることの確認を行うとともに必要な場合は随時見直すことが必要である。

その具体的な手法については、電気通信事業者の業務様態がそれぞれ異なることから、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。

イ　情報の管理に関する内部統制ルールの整備

【現状】

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。

電気通信事業者は情報漏えい等の発生を防止するため、情報の管理レベル、取扱規程、管理責任者の設定や情報に応じた利用者アクセスの管理などを内規等で定めることにより情報管理を行っている。ま

た､これらの内規の作成にあたっては､｢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(電気通信分野における情報セキュリティ協議会　平成 18 年 9 月 29 日策定)｣等各種ガイドラインを参考にしている。

しかしながら、電気通信事業に係る情報の流出等は後をたたない状況である。また、流出する情報についても個人情報に加え、電気通信システムのセキュリティに係る情報等も見受けられる。

【当面の改善策】

取扱規程及び管理責任者を適切に設定する等、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。

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

【現状】

近年の急速なブロードバンド化や電子商取引等の ICT サービスの浸透に伴い、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、国民生活・社会経済活動の基盤となる情報システムの障害、大量の個人情報の漏えい等が社会問題化しており、情報セキュリティ問題への取組みを抜本的に強化することが求められている。

このような中、情報通信基盤やそこを流通する情報をサイバー攻撃等から保護するための強固なガード手法について、産学官で積極的に研究開発が行われている。

利用者のアクセス管理に関するガイドラインには、ISO27000 をベースにしている「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)」がある。

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は、各事業者が付加価値サービスと位置づけて、セキュリティ対策を実施している。

【当面の改善策】

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、電気通信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。

【将来に向けて改善すべき事項】

電気通信事業者設備への利用者のアクセス管理方法は、技術革新に対応して常に高度化を図り、同時に上記ガイドラインを適宜改版していくことが必要である。

エ　アクセスログの取得、適切な保管

【現状】

電気通信事業者は、課金のために必要となるアクセスログを保持している。また、事業者は「電気通信事業における個人情報保護に関するガイドライン(平成 16 年 8 月 31 日総務省告示第 695 号)」に従い、当該情報を適切に保管することが求められている。

現在サイバー犯罪条約に対応するための刑事訴訟法の改正が議論されており、制度化された場合は、ログ保管への具体的対応について各事業者が検討することが必要になる。

しかし、一部のインターネット接続サービス（L3）とアクセス回線サービス（L2）事業者のように、

異なる事業者によってサービスが提供される場合、両事業者間の接続点においてそれが突合できるものでなければ実質的に物理的な回線の特定をすることができない。しかしながら、現在一部のL2事業者においては、ログの保存や物理回線とISPの認証パケットの関連付けを行なっておらず、ISPの持つIPアドレス情報から実際の利用者回線の特定を技術上の問題から行なうことが出来ない。

【当面の改善策】

電気通信事業者は法律等に則り、アクセスログの取得、適切な保管を行うことが必要であり、各事業者（アクセス回線提供事業者も含む）がそれぞれ保管すべきアクセスログを明確にして、ルール(内容、保管期間等)を作成することが適当である。また、必要に応じて事業者間でアクセスログの取得や管理方法について意見交換し、それを踏まえながら各事業者で対応することが適当である。

【将来に向けて改善すべき事項】

各電気通信事業者共通のルールを策定する目的は、主に相互参照にあると考えられるが、これは、個人情報保護法並びに電気通信事業における個人情報保護に関するガイドラインに直接的に関係する事項であり、その取り扱いには十分な注意を要すると考えられる。本項目については、十分に方向性が明確になっていないこと、また、IPネットワークに特化した問題ではないことから、適切な議論の場を設定し、共通的なルールを設定することの必要性から議論することが適当である。

分　類	第４章情報通信ネットワーク管理 └4.3 情報セキュリティ管理 └4.3.2. サイバー攻撃に備えた管理体制

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

【現状】

警察庁によると不正アクセス禁止法違反による検挙及び相談受理件数は、急激に増加してきている。

事業者団体において、他の利用者に悪影響等を与えているユーザーに対する契約の破棄に関するガイドラインが示されている（例：(社)テレコムサービス協会の「インターネット接続サービス契約約款モデル条項」）。

また、(社)電気通信事業者協会、(社)テレコムサービス協会、(社)日本インターネットプロバイダー協会、(社)日本ケーブルテレビ連盟が発行する「インターネット上の違法な情報への対応に関するガイドライン」では、他の利用者への悪影響の具体的な事例を示している。

契約約款によっては、他の利用者に悪影響を与えている事が明白な場合(例えば、ISPの契約において、他の利用者に著しい悪影響を与えており、警告に対してもそれを受け入れない場合など)に契約を解除できるという条項がある。具体的な運用は、他の利用者への悪影響の定義が必ずしも一意的に決まっていないため、各電気通信事業者に委ねられている。

ユーザー網や相互接続網からの不正アクセスへの対策に関しては、事業用電気通信設備規則に「事業用電気通信回線設備の防護措置」「異常ふくそう対策」が規定されている。

本来は、不正アクセスへの対策としては、不正アクセスの発生元となっている利用者等からの通信を緊急遮断することが有効であるが、現状ではその基準が明確になっていない状況である。同様に、電気通信契約の強制破棄に関するガイドライン等も明確になっていない状況である。

【当面の改善策】

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。

【将来に向けて改善すべき事項】

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。

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

【現状】

現状はスパムメールなど発信元での規制ではなく、その受信を検知してフィルタリングするなど受動的な対応となっており、その間、相当のリソースが占用されるため情報通信ネットワークの効率を低下させている。早期検知のためのツール、規制手段も改善されてきているが、新たな脅威の発生により後追いの状況となっている。１社のみでは解決が難しい問題も多いことから、これらネットワークに重大な影響を及ぼすサイバー攻撃を想定した事業者間の連絡について総合演習などを通じて共通課題の整理に着手している。

また、インターネット利用においては、匿名による誹謗中傷・風評・反社会的メールおよび掲示板書込みが増加しており、社会的な影響も無視できない状況となっている。また、サイバー攻撃を助長する技術的情報を掲載したり、サイバー攻撃ツールを有料販売している Web サイトがあるなど、情報通信ネットワークの使われ方や内容に対して、国や電気通信事業者がどのような運用、規制を行うべきか、どのような責任を持つのかといった課題がある。

【当面の改善策】

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。

【将来に向けて改善すべき事項】

CEPTOAR との関係を含めた事業者間での連携方法について検討が必要である。

ウ　サイバー攻撃発生時の迅速な情報共有方法の確立

【現状】

電気通信事業法において、重大な事故については総務大臣への報告が義務づけられているが、サイバー攻撃発生時については明確な取り決めがない。

さらに、代表的なサイバー攻撃事例を共有するなど電気通信事業者間の更なる協調が必要となっている。

【当面の改善策】

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。

分　類	第４章情報通信ネットワーク管理 └4.3 情報セキュリティ管理 　└4.3.3.情報漏えい防止対策

ア　媒体の種類に応じた廃棄処分方法の明確化

【現状】

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。

電気通信事業者は情報漏えい等の発生を防止するため、媒体を処分する際の手順などを内規等で定めることにより情報管理を行っている。これらの内規の作成にあたっては、「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（電気通信分野における情報セキュリティ協議会　平成 18 年 9 月 29 日策定）」等各種ガイドラインを参考として作成している。

しかしながら、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る。

【当面の改善策】

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、電気通信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。

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

【現状】

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。

電気通信事業者は情報漏えい等の発生を防止するため、メール等を利用した情報交換を行う場合の情報の暗号化、パスワード設定などの手順などを内規等で定めることにより情報管理を行っている。これらの内規の作成にあたっては、「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（電気通信分野における情報セキュリティ協議会　平成 18 年 9 月 29 日策定）」等各種ガイドラインを参考として作成している。

しかしながら、メールの暗号化を怠ったためウィルスに感染したメール受信者の PC から情報が漏えいした事案も報告される等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る。

【当面の改善策】

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。

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

【現状】

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必要性が認識されるようになっている。

【当面の改善策】

事業者は、情報漏えい防止のための監査チェック項目を策定し、内部及び外部監査を実施することにより、情報漏えいの防止を着実に履行できるようにすることが必要である。

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

【現状】

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、国民生活・社会経済活動の基盤となる情報システムの障害、大量の個人情報の漏えい等が社会問題化し、情報セキュリティ問題への取組みを抜本的に強化することが求められている。しかしながら、事業者間で、情報漏えいに対する技術的・人的な対策方法や考え方について、情報・意見交換することが十分に行われていない。

【当面の改善策】

急速に拡大する ICT の利活用に対応し、次々と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、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、すべての電気通信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。

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

【現状】

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る。これらの情報流出では、個人情報に加え、電気通信システムのセキュリティに係る情報の流出も見受けられる。

漏えいしたシステム情報には、その機能を停止・低下させ社会機能に影響を及ぼすおそれのある情報

が含まれている場合がある。また、自社のセキュリティに関わる情報のみならず、他社のシステムセキュリティに関わる情報が含まれている情報の漏えいも発生している。
　電気通信事業法では、電気通信業務に関し通信の秘密の漏えいが生じたときは、その旨をその理由又は原因とともに総務大臣に報告しなければならないと定めている。(電気通信事業法第 28 条)
　しかしながら、システムに係る情報漏えいの事案については、報告を求める規定がないため監督官庁への報告義務は発生しない。

【当面の改善策】
　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することが必要である。

カ　コンピューターウィルス等による情報漏えい対策

【現状】
　Winny などのファイル交換ソフトに起因する、自衛隊、警察、地方公共団体、原子力発電所などの機密情報の漏えい、病院・企業がもつ顧客の個人情報の漏えいが起こり、社会問題となっている。
　事業者のネットワーク設備は、「事業用電気通信設備規則」第 6 条により、端末設備又は自営電気通信設備から受信したプログラムによって、当該事業用電気通信設備が電気通信事業者の意図に反する動作を行うこと、その他の事由により電気通信役務の提供に重大な支障を及ぼすことがないよう、当該プログラムの機能の制限その他の必要な防護措置が講じられているようにすることが定められている。
　また、電気通信事業法第 4 条にて「秘密の保護」、第 6 条にて「利用の公平」の観点から遮断することは適当でないが、事業者において一部のユーザーが回線の全帯域を占有することが無い様に帯域を制限する措置が取られている場合もある。
　利用者においてもリスクを理解した上でそれぞれ対処することが求められている。
　また、本項目については「ネットワークの中立性に関する懇談会」等で議論をされているところである。

【当面の改善策】
　ファイル交換ソフトなどがコンピュータウィルスの感染により情報漏えいを招かないような対策や、ユーザー認証、アクセス管理等、データアクセスに関わるログ取得・保管、データ不正アクセスの検知、ネットワーク上での不正行為の検知など情報の重要度レベルに応じて、各電気通信事業者で対応基準／手順／方式を明確にし、運用していくことが適当である。この際、外部への PC やメディアに持ち出した情報についても考慮することが必要である。

【将来に向けて改善すべき事項】
　ユーザーの通信を遮断することについては、議論を継続することが必要である。また、情報漏えい対策についての技術開発を継続的に実施し、ネットワーク利用者があまねく利用できる技術の提供を検討することが必要である。

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

【現状】
　事業者は、不正利用・不正アクセスから、電気通信回線設備や利用者の各種情報を保護するため、自らのネットワークに最適な認証機能を設定している。

【当面の改善策】
　不正利用・不正アクセスから、電気通信回線設備や正規利用者の各種情報を保護するため、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を行っていく必要がある。具体的な手法については、各事業者が各々のサービスに適した形で、整備していくことが適当である。

分　類	第４章情報通信ネットワーク管理 └4.3 情報セキュリティ管理 　└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

ア　業務委託先の選別の評価要件の設定

【現状】

昨今、電気通信事業に係る個人情報や重要なシステム情報の漏えいが発生している。これらの情報漏えいの流出経路として事業者から直接流出する他に、業務委託先から情報が流出する場合がある。

電気通信サービスが多様化するとともにシステムが高度化・複雑化し、業務の外部委託の活用が経常化しているため、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など外部委託先と連携した情報セキュリティ対策が重要となっている。

事業者は外部委託先での情報セキュリティ対策が十分であることを確認するために、セキュリティに関わる認証を取得していること等を委託先の基準として内規等で定めることにより、セキュリティが確保されていることの確認を行っている。その際「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（電気通信分野における情報セキュリティ協議会　平成 18 年 9 月 29 日策定）」等の各種ガイドラインが活用されている。

【当面の改善策】

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状況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。

イ　守秘義務契約、誓約書、情報管理規定の保持

【現状】

昨今、電気通信事業に係る個人情報や重要なシステム情報の漏えいが発生している。これらの情報漏えいの流出経路として事業者から直接流出したものの他、業務委託先からのものが含まれている場合がある。

電気通信サービスが多様化するとともにシステムが高度化・複雑化し、業務の外部委託や派遣職員など外部リソースの活用が経常化する運用状況の中、委託先等の外部機関等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等外部委託先と連携した情報セキュリティ対策が重要となっている。

電気通信事業者は外部委託先での情報セキュリティ対策が十分であることを確認するため、セキュリティに関わる認証を取得していること等を委託先の基準として内規等で定めることにより、セキュリティが確保されていることの確認を行っている。その際「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（電気通信分野における情報セキュリティ協議会　平成 18 年 9 月 29 日策定）」等の各種ガイドラインが活用されている。

【当面の改善策】

業務の外部委託や派遣職員の活用など外部の活用が経常化する運用状況の中、電気通信事業者が自らの情報セキュリティレベルの向上を図ることはもとより、外部委託先の情報セキュリティレベルの向上を図ることが必要である。

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。

具体的な手法については、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。

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

【現状】

電気通信設備の故障が発生した際に、電気通信事業者で十分な原因究明ができない場合には、ログ等の記録媒体をベンダー等に提供したうえで原因を究明している。この際にベンダーのセキュリティレベルが十分確保されていない場合には、情報漏えいの危険性が内在することとなる。

近年発生している情報漏えい事案についても、電気通信事業者から業務を請け負った事業者からのも

のが報告されている。
　このような危険性を回避するために、電気通信事業者は内規等に保守契約の際の情報の取扱いを定めることや、必要により認証の取得等を基準に定めることによりセキュリティを確保していることを確認している。

【当面の改善策】
　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、電気通信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の者による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。

分　類	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対策 └5.1 設備・環境に対する対策に関する検討 └5.1.1 バックアップ、分散化などの ICT 障害対策

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

【現状】

事業用電気通信回線設備は、事業用電気通信設備規則第 11 条（停電対策）において、『自家用発電機又は蓄電池その他これに準ずる措置が講じられなければならない』と法令で予備電源の設置が義務付けられている。しかしながら、具体的な予備電源の種別や動作時間は規定されておらず、事業者は設備の重要度に応じて必要とする予備電源の動作時間を設定している。

通常、電気通信設備は主に局舎やハウジングスペースに設置されており、予備電源は主に局舎やハウジングスペースが用意しているものを利用している。事業者がハウジングスペースなどに自ら無停電電源装置を設置するケースもあるが、電源停止時の装置保護を目的とする場合が多い。

予備電源の動作時間は局舎やハウジングスペースのバッテリー容量およびエンジンが設置されている場合は蓄積されている燃料等に依存する。(場所によっては移動電源車の手配や燃料補給等によって長時間運用できるような対策も考えられている。)

しかしながら、設備によって重要度が異なり、重要度に応じて必要とする予備電源の動作時間は異なる。

【当面の改善策】

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。

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

【現状】

事業用電気通信設備規則第 16 条第 2 項では、利用者の建物又はこれに類するところに設置する事業用電気通信回線設備において適用除外になる規定（耐震対策、停電対策等）が定められている。

しかしながら、昨今、地下街や駅構内等の比較的規模の大きい施設では、基地局の機能停止による影響が無視できない状況になっている。この状況を鑑み、電気通信事業者は、公共性の高い場所や規模の大きい施設に対しては、予備電源の設置等、適切な停電対策等を実施している。

一方、地下街や駅などの設備が設置される施設側からは、電気通信事業者が個別に設置を依頼し、個別に設備を置くことに対して、改善要望が挙がっている。

【当面の改善策】

停電対策については、非常時等に、ネットワークを長時間運用できるよう各事業者が総合的に取り組んでいるところである。IP ネットワーク設備においても、設備の重要度に応じて必要な予備電源が確保できるよう、各事業者は対策を実施する必要がある。

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ことが適当である。

ウ　障害の影響範囲を限定する対策

【現状】

電話交換機と同様に、SIP サーバの障害時の影響範囲は、そのサーバに収容されているユーザーに限定されることになる。通常、事業者は、IP 電話サービスのユーザー数がまだ少ない時点では少数の SIP サーバに全国のユーザーを収容し、効率的にネットワークを構成しているため、1 台の SIP サーバの障害の影響が全国のユーザーにおよぶこともある。

しかし、事業者によっては、ユーザー数の増大にあわせて SIP サーバを増設しており、その結果、1 台の SIP サーバの障害による影響がその地域に限定されるようになりつつある。

【当面の改善策】

各事業者は、アナログ電話並に、障害発生時に影響範囲を限定的にする対策を進める必要がある。その手法としてSIPサーバの影響範囲を限定することは有効な手法であるが、手法については、事業者が自らのネットワークの構成や運用実態を踏まえ判断することが適当である。

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

【現状】

サービスの安全・信頼性を高める方法としては大きく分けて、システムを大規模化し集中的に信頼性向上策を講じる方法と、システムを分散化し障害発生時の影響を限定的にする方法が考えられるが、それぞれ利点と欠点がある。

【当面の改善策】

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をする必要はあるが、具体的なネットワーク構成については、事業者が自らのネットワークの構成や運用実態を踏まえ判断することが適当である。

オ　事業者をまたがる標準的な網管理インタフェースの検討

【現状】

固定電話網では事業者間の網管理機能がプロトコルとして標準化されており、国内・国外のキャリア間で運用されている。

今後は、ネットワークのIP化にあわせ事業者間接続におけるPOIのIP化が進むと予想されるため、IP化されたPOIを介したキャリア間の網管理機能の検討が必要である。

【当面の改善策】

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。

【将来に向けて改善すべき事項】

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。

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

【現状】

IP電話は、従来のアナログ電話と比較してメンテナンスに伴うサービス停止の頻度が多い傾向がある。

【当面の改善策】

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に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。

キ　コロケーション先の電気通信設備の保護

【現状】

法令では、事業用電気通信設備が収容される通信機器室等に火災報知器の設置等の防火対策を適切に施すことが定められている。これは、通信機器室において火災が発生した場合は、電気通信回線設備自体にも甚大な被害が及ぶおそれがあるため、そのような事態を防ぐことを趣旨として設けられた規定である。

また、電気通信回線設備を設置する事業者の電気通信設備については、事業用電気通信設備規則において、事業用電気通信設備を収容、又は設置する通信機器室の防火対策が規定されているところである。

電気通信回線設備は一般に弱電流の電子機器から構成されており、通常の状態では自ら発火する可能性は低いが、近年サーバが高密度化され、消費電力が大きくなる傾向にあり、電源設備が発火・発煙する事例が発生している。しかしながら、現在、電源設備をはじめ事業用電気通信設備に対して発火・発

煙等の防止に関する基準は設けられていない。
　また、電気通信回線設備を設置していない事業者についても、他の事業者のビルにコロケーションしている設備が故障した場合には、同一ビルに収容されている全ての事業者のユーザーの通信に影響を与えるおそれがあり、社会的影響が大きい。しかしながら、現在、電気通信事業法上の技術基準適合維持義務は電気通信回線設備を設置していない事業者には適用されない。

【当面の改善策】
　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。

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

【現状】
　法令では、事業用電気通信回線設備を設置する建築物等について、電気通信設備を工事・維持・運用する者以外の者が、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必要な措置をとることが定められている。
　しかしながら、セキュリティを保つべき領域の具体的な基準は定められておらず、各電気通信事業者が、事業者個別の状況を踏まえセキュリティを保つべき領域について検討、決定した上で、該当する領域での入出管理等を実施している。また、入出管理システムについても具体的な基準は定められておらず、各事業者が事業用電気通信設備規則等にのっとり、様々な入出管理システムにより対応している。実際の入退出管理システムは、施錠式、カード式が多いが、データセンタ事業者等では同業他社との差別化を図るため、生体認証システム等の高度なシステムの導入も進んでいる。
　また、事業者の中には、ISMS 等の認証取得を行い、入出等システムの審査を受けているものもある。

【当面の改善策】
　電気通信事業者は、電気通信設備を工事・維持・運用する者以外の者が、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、各電気通信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。

【将来に向けて改善すべき事項】
　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。

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

【現状】
　法令では、アナログ電話用設備の交換設備相互間を接続する伝送路設備は、なるべく複数の経路により設置されなければならないと定められるとともに、「情報通信ネットワーク安全・信頼性基準」において、異経路伝送路設備の設置、電気通信回線の分散収容について規定されており、電気通信事業者は、これらを踏まえてネットワークの構築を行っている。なお、安全・信頼性向上に資する一部の設備につ

いては、電気通信システム信頼性向上促進税制により固定資産税が軽減されている。
　サービス提供の継続性確保のための通信路・システムの冗長構成やバックアップシステムの構築は、基本的には各事業者が、経営方針に基づきそれぞれの利用者への影響等を考慮したうえで、事業内容に応じた条件や手段により主体的に実施しており、その実施内容や信頼度や提供条件は、利用者が電気通信事業者を選択する際の一要素となっている。
　しかしながら、IP ネットワークサービスにおいては、広域かつ大規模で、復旧までに長時間を要する故障が発生しており、利用者利益の保護の視点から安全・信頼性対策の強化が必要となっている。

【当面の改善策】
　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図る必要がある。

【将来に向けて改善すべき事項】
　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・故障率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安全・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。

分　類	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対策 └5.1 設備・環境に対する対策に関する検討 　└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

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

【現状】
　事業者はそれぞれ自社ネットワークの網構成に応じたセキュリティ対策基準を設け対策をすでに講じている。(例えばインターネットに接続している網と接続していない網とではリスクが異なるため、対策が異なっている。)
　しかしながら、今後はネットワークの IP 化にあわせ事業者間接続における POI（Point Of Interface 電気通信事業者同士が相互に通信網を接続する際の接続点）の IP 化が進むと予想されるため、IP 化された POI を介した不正アクセス等についての対策検討が必要であり、技術検討作業班で検討が行われている。

【将来に向けて改善すべき事項】
　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。

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

【現状】

発信元を偽装する不正アクセスには、「メール発信元の偽装」「ボット(不特定多数の端末を踏み台にしての攻撃)」「フィッシング(発信元偽装メールなどからの不正ホームページへの誘導)」など、様々な手口が次々と発生してきている。それに対して、本人認証の手段として、「ID/パスワードによる認証(定期的にパスワード変更を推奨)」「発信者番号チェック(ダイヤルアップ)」「ワンタイムパスワード(接続時毎にパスワードを取得)」等の方法で対応しているが、利用者の不注意などもあり不正アクセスによる被害は絶えない。

発信者番号偽装表示の問題については、(社) 電気通信事業者協会 (TCA) にて対策が検討され、電気通信事業者がとるべき対策として「発信者番号偽装表示対策ガイドライン」が取りまとめられており、各事業者は、この内容を遵守し必要な対策をとっているところである。一方で、ネットワークの IP 化に伴い、オープンな技術・ネットワークを利用することで、通信経路の特定を困難にすることで発信元も特定しにくくする等、不正利用の方法についても複雑化している。

利用者に対する啓発活動については、e ネットキャラバン、ボット対策プロジェクト(Cyber Clean Center)等、官民あげて実施しているところである。しかし、悪意を持った攻撃者は新たな脅威を次々と生み出し、端末を踏み台にして攻撃をしかけてきており、サイバー攻撃に対する防御等に関する技術開発はいたちごっこの状態になっている。

また、不正アクセスを防止するために、関係省庁、事業者団体等が合同の会合を開催しており、例えば、フィッシング対策では、電気通信業界団体、インターネット関連企業、内閣府、警察庁、経済産業省、総務省等が参画した「フィッシング対策推進連絡会」を開催して、① 送信者認証技術の導入・促進 (迷惑メール対策とも連携)、 ② フィッシングサイトへの対応 (サイトの削除等)、 ③ ISP 間の情報共有、ユーザーへの周知啓発などについて検討をして、平成 17 年 8 月 10 日に「フィッシングの現状及び ISP によるフィッシング対策の方向性」を公表し、対策を進めている。

送信元アドレスの偽装の防止策として各種方法(イングレスフィルタによる方法(RFC2827)やルータの経路表を用いる方法(RFC3704)) が推奨されている。しかしながら、これらはネットワーク全体が導入してこそ効果が高まる方法であり、ネットワーク全体での導入が容易ではないため送信元アドレスの偽装が起き、追跡技術が必要となっている。

そのため、サイバー攻撃や分散型サービス拒否攻撃 (DDoS) の根本的対策は攻撃元の特定でありその問題を解決する研究開発が重要である。

なお、電気通信事業者によっては送信元アドレスが偽装されたパケットを自ネットワークの外部に流出させない仕組みを導入している。

【当面の改善策】

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、発信元を偽装すること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。

【将来に向けて改善すべき事項】

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。

例えば、端末認証を強化する手法には、一般の利用者端末とサービス提供者の間においては、ネットワークに接続する時点で、予め登録済の IP アドレスを確認し、同時に個人認証及びアクセス認可を行い、登録されていないものをすべて排除することが検討されており、既に実験も行なわれている。また、キャリアと ISP の間においては、ゲートウェイでの不正トラヒックの検出メカニズムの確立、端末認証の強化による偽装端末の排除、端末状態のリモート管理／運用等が可能となるような端末とネットワークとが連携したシステム全体の Plug and Work (デバイスをネットワークに接続しただけで利用できる技術) の確立が必要とる。

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。

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

【現状】

端末機器のソフトウェアは開発段階で機器ベンダーが脆弱性をチェックしている。

しかしながら、市販された後にソフトウェアの脆弱性が発見され、脆弱性に関する情報が流通し、脆弱性をついた攻撃が行われる事例が増加している。攻撃の具体例としては、他ユーザーへの不正アクセスの踏み台として使用される場合や、端末機器に保管されている個人情報等が盗み取られ暴露される場合などがあり、社会問題となっている。

【当面の改善策】

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。

【将来に向けて改善すべき事項】

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。

分　類	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対策 └5.1 設備・環境に対する対策に関する検討 └5.1.3 端末等に対する対策

ア　IP 端末への要求条件の明確化

【現状】

ネットワークの IP 化の進展に対応するためには、今後の適合性認証制度は、端末機器接続の技術基準の設定と技術基準適合性の認証を行うという現行の枠組みを踏襲し、①端末とネットワークの接続性／運用性の確保、②利便性向上の確保、③安全・信頼性の確保といった要素を考慮し、実施されることが必要であると考えられる。

【当面の改善策】

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。

イ　ネットワーク防御のための端末の要件の明確化

【現状】

今後の IP 化されたネットワークでは、アナログ電話のようにネットワーク側だけが機能を持つのではなく、ネットワークと端末の双方で機能を分担し、連携しながらサービスの提供が行われると考えられる。

機能分担や連携については、自動発信制限のみならず、障害の切り分けや特定、一斉登録防止、端末ソフトウェア/ファームウェア更新等のネットワーク保全に関わる各種事項も対象になると考えられる。

【当面の改善策】

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。

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

【現状】

一般に IP 電話端末は電源投入後の初期化処理において機器固有のタイミングでサーバへのアクセス（REGISTER 登録等）が発生する。停電からの回復時は該当エリア内の IP 電話端末が一斉に電源投入された状態となり、同種の IP 電話端末から同じタイミングで一斉にサーバアクセスが発生し、通信設備へ負荷が集中する可能性がある。

IP 電話端末に限らず、電源投入後一定時間を経てサーバにアクセスする端末では同様の問題が発生する可能性がある。

【将来に向けて改善すべき事項】

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。

エ　端末の電力確保、バッテリー寿命延長の技術開発等

【現状】

従来のアナログ固定電話と異なり IP 電話をはじめとする IP 系サービスの端末は停電時には利用できない。特に 0AB～J 番号を使用する IP 電話は、緊急通報受理機関への接続が義務付けられており、いざという時にも利用できることが望ましい。

しかしながら、昨年の東京大停電の際に、IP 電話が利用できないといった事例も報告される等、従来のアナログ電話とは異なり停電時にも利用を可能とするためには、利用者側で電源を確保することが必要な状況である。また、利用者は停電時に IP 電話が利用できないといったことに関して認識が十分ではない状況である。

【当面の改善策】

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】

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。

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

【現状】

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。その波及抑止に向けた対応は事業者共通なものはなく、各事業者にて対応している。

【当面の改善策】

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。

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

【現状】

情報化社会の進展に伴い、電気通信は国民一人一人の日常生活において必要不可欠な手段となっている。このような状況の中で障害者・高齢者を含む全ての人々にとって電気通信設備及びサービスが円滑かつ容易に障壁なく利用できるようにするといったアクセシビリティを確保することが重要である。

これらの取組みについては、「障害者等電気通信設備アクセシビリティガイドライン」（電気通信アクセス協議会　平成 13 年 5 月 8 日）が作成されている。また、JIS X8341 においても情報アクセシビリティ向上のための規格が策定されている。

また、高齢者が容易に情報活用できるためのヒューマンインタフェースの開発については、産学官で様々な取組がされているところである。

【当面の改善策】

障害者・高齢者を含む全ての人々にとって電気通信設備及びサービスが円滑かつ容易に障壁なく利用できるようにする必要があり、既にガイドライン等をもとに電気通信事業者で対応しているところである。しかしながら、サービスの変化・技術動向・社会状況の変化により、求められる基準も変化に迅速に対応していくことが必要であり、電気通信事業者は、アクセシビリティ対応項目を適宜見直し、具体化しドキュメント等に定め、取組みを明確にしていくことが必要である。

その手法については、サービスの形態があることを踏まえ、各事業者において自らのサービスにふさわしい対策を講じることが適当である。

参考資料２　用語解説

- 空港 MCA（MCA：Multi-Channel Access）
  　大規模な空港で地上業務用として複数のチャネルを共用して使用する陸上移動通信システムのこと。
- ADSL（Asymmetric Digital Subscriber Line：非対称デジタル加入者線）
  　DSL（Digital Subscriber Line：デジタル加入者線。電話用のメタリックケーブルにモデム等を設置することにより、高速のデジタルデータ伝送を可能とする方式）のうち、加入者から電話局へ送るデータの通信速度と電話局から加入者へ送るデータの通信速度が非対称となるもの。
- CEPTOAR（Capability　for Engineering of Protection, Technical Operation, Analysis and Response：情報共有・分析機能）
  　「情報セキュリティ政策会議」（議長：内閣官房長官）により示されたものであり、IT 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のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係重要インフラ事業者等間で共有すること。
  　なお、重要インフラとは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるインフラのこと。
- CEPTOAR-Council（重要インフラ連絡協議会）
  　重要インフラ事業者等において、分野横断的な情報共有の推進を図り、多様な知見をサービスの維持・復旧に活かしていくため、各 CEPTOAR 間での横断的な情報共有の場のこと。
- DDoS 攻撃（Distributed Denial of Service）
  　DoS 攻撃（メールやファイル、あるいは不正なパケットを大量に送りつけることで、システムのサービスを停止させたり、サーバなどをダウンさせたりする攻撃の総称）の手法の一つであり、複数のサーバを踏み台にして一斉に攻撃を仕掛けるもの。
- FTTH（Fiber To The Home）
  　電気通信事業者から各加入者宅まで光ファイバ・ケーブルで接続し、家庭でも超高速データ等の高速広帯域情報を送受できるようにするもの。
- ICT（Information and Communication Technology：情報通信技術）
  　情報通信技術を表す総称。
- ISMS（Information Security Management System：情報セキュリティマネジメントシステム）

企業などの組織が情報を適切に管理し、機密を守るための包括的な枠組みのこと。

- ISO/IEC17799

  人や組織の運用面に関する情報セキュリティの標準ガイドラインであり、ISMS の基盤となるもの。英国規格である「BS7799(British standard 7799」を基に、ISO 標準として承認・出版された。

- IP（Internet Protocol: インターネットプロトコル）

  インターネットによるデータ通信を行うために必要な通信規約。

- IP-VPN（IP-Virtual Private Network：IP の仮想プライベートネットワーク）

  電気通信事業者の保有する広域 IP 通信網を経由して構築される仮想私設通信網のこと。

- IP 電話（IP Phone）

  通信ネットワークの一部又は全部において IP 技術を利用して提供する音声電話サービス。

- IP ネットワーク（IP Network）

  インターネットプロトコルにより通信を行う通信網。

- ITU（International Telecommunication Union: 国際電気通信連合）

  電気通信に関する国連の専門機関であり、多国間の円滑な通信を行うため、世界各国が独自の通信方式を採用することによる弊害の除去や、有限な資源である電波の混信の防止、電気通信の整備が不十分な国に対する技術援助等を目的としている。

- MAC アドレス（Media Access Control address）

  各 Ethernet カードに固有の ID 番号。全世界の Ethernet カードには 1 枚 1 枚固有の番号が割り当てられており、これを元にカード間のデータの送受信が行われる。

- MTBF（Mean Time Between Failure：平均故障間隔）

  システムや装置に故障が発生する確率（「稼動時間／故障回数」で求められる）であり、信頼性を表す 1 つの指標である。

- NGN（Next Generation Network）

  IP ネットワークをベースとした次世代のネットワーク

- NISM（ネットワーク情報セキュリティマネージャー）

  ハッカーやサイバーテロの脅威に対処し、情報通信ネットワークの安全性・信頼性を確保するために、情報通信サービスを提供する事業者に配置する専門家を育成することを目的として創設され、資格認定のための講習(認定講習)を受講し、一定のレベルに達すると、有資格者として認定される資格のこと。

- POI（Point Of Interface：相互接続点）
  各電気通信事業者が所有する回線の相互接続点のこと。
- SIP（Session Initiation Protocol）
  IP ネットワーク上で、電話の呼び出し等を実現するためのプロトコル。
- T-CEPTOAR（電気通信分野における情報セキュリティ関連情報の「情報共有・分析機能」）
  電気通信分野の CEPTOAR であり、2007 年 4 月より運用を開始している。
- VoIP（Voice Over Internet Protocol）
  IP ネットワーク上における音声データを送受信する技術。IP 電話やインターネット電話と呼ばれるサービスはこの技術を用いたもの。