参考　３－１

電気通信事故検証会議

電気通信事故に係る
構造的な問題の検証に関する報告書

令和　５　年　３　月

電気通信事故検証会議

目次

１．検討の背景 2

２．通信事故の背景にある構造的な問題について 4
2.1　通信の信頼性確保に関するガバナンス・モニタリング 4
2.2　設備に関するリスクの洗い出し体制・方法 5
2.3　予備系設備への切替え不能 6
2.4　著しい高負荷時の挙動検証 7
2.5　商用稼働済設備の定期的な点検 7
2.6　平時からの事故対応に係る教育・訓練・人材育成 8
2.7　ヒューマンエラー防止策 9
2.8　利用者への周知広報・透明性確保 10
2.9　通信事故の背景にある構造的な問題の整理 11

３．構造的な問題を踏まえた対策について 14
3.1　ガバナンスの強化 14
3.2　外部モニタリング 17
3.3　リスク管理 22
3.4　予備系設備への切替え不能時の対処 23
3.5　著しい高負荷時の動作検証 25
3.6　データ蓄積型設備への定期監視 26
3.7　訓練 26
3.8　ヒューマンエラー防止対策 28
3.9　利用者への周知広報 29
3.10　構造的な問題を踏まえた対策の整理 30

４．今後の対応及び検討課題 32

はじめに

電気通信サービスは、人と人とのコミュニケーションや自由な情報発信の実現に加え、物流や自動車、行政、金融など多岐にわたる分野に利用されるなど、国民生活や社会経済活動に欠かせない基盤として重要性が増している。

この電気通信サービスにおいて、近年、電気通信事業者による通信事故の発生が増加している。個々の通信事故については、これまで事案ごとに個別に検証を行い、影響が大きな事案については個別の検証報告書を作成して公表を行ってきた。他方、こうした通信事故が多発する背景には、リスク評価やリスク項目の洗い出しの不足、ヒューマンエラー防止や訓練面での課題、保守運用態勢に対するガバナンスの不足等、共通する課題も多いと考えられる。

緊急通報に関する事故は国民の生命や安全にも大きな影響を及ぼす問題であり、また、デジタル化が進展した現代社会において、携帯電話やインターネット等の通信インフラが利用できない等の通信事故は、国民生活や社会経済活動にも多大な影響が及ぶ重要な問題である。こうした事情を踏まえると、通信事故の背景にある構造的な問題の検証、また当該問題を踏まえた対策について検討していくことが急務と考えられる。

このため、令和４年 12 月より、電気通信事故検証会議において、通信事故の背景にある電気通信事業者に共通する構造的問題とその対応策について検討を行うこととした。

本報告書は、電気通信事故検証会議（令和４年度第６回、第７回、第９回～第12 回）において、検討を行った結果を取りまとめたものである。

なお、本電気通信事故検証会議は、開催要綱[1]にも記載のとおり、「①重大な事故に係る報告の分析・検証、②四半期ごとに報告を要する事故に係る報告の分析・検証等を行うことにより、電気通信事故の発生に係る各段階で必要な措置が適切に確保される環境を整備し、電気通信事故の防止を図ること」を目的とするものであり、本報告書は、当該目的に基づき、検討を行ったものである。

---

[1] 「電気通信事故検証会議」開催要綱
(https://www.soumu.go.jp/main_content/000852282.pdf)

1. 検討の背景

電気通信サービスは、人と人とのコミュニケーションや自由な情報発信の実現に加え、物流や自動車、行政、金融など多岐にわたる分野に利用されるなど、国民生活や社会経済活動に欠かせない基盤として重要性が増している。

この電気通信サービスにおいて、図表 1−1 のとおり、近年、電気通信事業者による通信事故の発生が増加している。個々の通信事故については、これまで事案ごとに個別に検証を行い、必要に応じて、個別の検証報告書を作成して公表を行ってきたが、こうした通信事故が多発する背景には、リスク評価やリスク項目の洗い出しの不足、ヒューマンエラー防止や訓練面での課題、保守運用態勢に対するガバナンスの不足等、共通する課題も多いと考えられる。

発生日時 （継続時間）	通信 事業者	影響サービス	影響範囲 （地域、利用者数）	発生原因
7月2日(土) (61時間25分)	KDDI	音声通話、SMS※、 ホーム電話、 データ通信	全国 音声通話：約2,278万人 データ通信：765万人以上 【重大事故に該当】	**人為的ミス**
8月25日(木) (5時間47分)	NTT 西日本	インターネット サービス (フレッツ光)	西日本エリア 最大211万回線(品質低下) サービス停止は最大1時間50分 【重大事故に該当】	**設備故障**
9月4日(日) (2時間6分)	楽天 モバイル	音声通話、 データ通信	全国エリア 最大130万回線 【重大事故に該当】	**設備故障**
12月17日(土) (4時間54分)	NTT ドコモ	データ通信	西日本エリアの一部 データ通信：約242万人 【重大事故に該当】	**設備故障**
12月20日(火) (2時間2分)	NTT ドコモ	データ通信	西日本エリアの一部 データ通信：約70万人 【重大事故に該当】	**人為的ミス**

図表 1-1　最近（令和４年度）の主な重大な事故

なお、通信事故等の非常時においても、携帯電話利用者が臨時的に他の事業者のネットワークを利用する「事業者間ローミング」等により、継続的に通信サービスを利用できる環境を整備するため、令和４年９月に「非常時における事業者間ローミング等に関する検討会」が創設され、同年 12 月、一般の通話やデータ通信、緊急通報機関からの呼び返しが可能なフルローミング方式による事業者間ローミングをできる限り早期に導入すること等を基本方針として位置づけた「非常時における事業者間ローミング等に関する検討会 第１次報告書」が取りまとめられた[2]。

[2] 「非常時における事業者間ローミング等に関する検討会 第１次報告書 ～事業者間ローミングの導入に向けた基本的な方向性～」参照
https://www.soumu.go.jp/main_content/000852443.pdf

他方、「事業者間ローミング」等により通信事故の全てが解決されるものではなく[3]、各電気通信事業者自身により、通信サービスの確実かつ安定的な提供を確保することは、極めて重要であると考えられる。

このため、令和４年 12 月より、電気通信事故検証会議において、通信事故の背景にある電気通信事業者に共通する構造的問題とその対応策について検討を行うこととした[4]。

[3] コアネットワークの利用者認証・位置登録データベースに障害が発生した場合、フルローミング方式によるローミングは実施困難となる。このため、「非常時における事業者間ローミング等に関する検討会 第１次報告書」において、コアネットワークに障害が発生し、利用者認証及び緊急通報機関からの呼び返しができない場合の「緊急通報の発信のみ」を可能とするローミング方式の導入について、「今後の検討課題」とされており、現在、継続的な検討がなされている。

[4] 本電気通信事故検証会議は、開催要綱にも記載のとおり、「①重大な事故に係る報告の分析・検証、②四半期ごとに報告を要する事故に係る報告の分析・検証等を行うことにより、電気通信事故の発生に係る各段階で必要な措置が適切に確保される環境を整備し、電気通信事故の防止を図ること」を目的とするものである。本会議では、これまで、電気通信事故の大規模化・長時間化やその内容・原因等の多様化・複雑化を踏まえ、電気通信事故の報告について、外部の専門的知見を活用しつつ検証を行う観点から、原則、非公開により開催してきた。今回、個別の事案に留まらない、事業者横断的な検証を、原則、公開により開催したが、事業者の事故報告等を有識者により分析・評価し、総務省の政策立案へ反映を行うことは、当該目的等を逸脱するものではなく、本会議の目的や位置づけが変わるものではない。

2. 通信事故の背景にある構造的な問題について

電気通信事故検証会議では、今回、主要な電気通信事業者[5]を対象に、電気通信サービスの信頼性の確保に関する対策の状況等についてヒアリングを行った。

当該ヒアリング結果を踏まえ、通信事故の背景にある構造的な問題として、①通信の信頼性確保に関するガバナンス・モニタリング、②設備に関するリスクの洗い出し体制・方法、③予備系設備への切替え不能、④著しい高負荷時の挙動検証、⑤商用稼働済設備の定期的な点検、⑥平時からの事故対応に係る教育・訓練・人材育成、⑦ヒューマンエラー防止策、⑧利用者への周知広報・透明性確保、について検討を行った[6]。

2.1 通信の信頼性確保に関するガバナンス・モニタリング

管理規程[7]の遵守・実施状況等に関する内部監査及び外部監査の定期的な監査・点検について、ヒアリングを実施したところ、各事業者の状況は以下の図表 2-1 のとおりであった。

✓ 管理規程の遵守・実施状況に関する内部及び外部の監査や点検の実施状況	
A社	✓ 管理規程の遵守については、社内の各種会議にて確認しております。また、社外監査については実施しておりません。 ✓ 内部での確認は、施策承認、工事計画策定のタイミングで当該工事実施責任者により各部門の責任者を会議に招集し、工事実施手順、工事期間、工事体制等を確認しており内容に不備やリスクがある場合は是正の上進めることとしております。
B社	✓ 当該管理規程の遵守について、社内で会議体を設け、各部門の責任者が確認しております。また、外部監査については実施しておりません。 ✓ 内部での確認は、施策承認、工事実行計画策定のタイミングで当該工事実行責任者により各部門の責任者を会議に招集し、工事実施手順、工事期間、工事体制等を確認しております。内容に不備等があれば各部門責任者の最終合意が完了するまで審議を継続して実施しております。
C社	✓ 社内において通信障害を全社的なリスクとして定め、内部監査組織にて社内体制・技術的機能の具備、機器ベンダーや事業者との連携、利用者への周知等に**関する監査を年2回実施し、社内統制を図ってます。** ✓ 外部監査については定期的には実施おりませんが、大規模なNW切替工事実施の際、必要に応じて受検しています。 NWや工事の専門性を有する外部組織を監査主体とし、工事に関する体制や作業手順書のチェックを実施いただき、作業の安全性向上を図っています。
D社	✓ 管理規程の遵守状況を確認するため、事業用電気通信設備管理規程に則り、同規程管理部門から設備の工事設計・維持・運用部門へ、それぞれの**業務が管理規程に沿って行われているか（遵守性の点検）の監査を毎年1回実施しています。** ✓ 外部監査：今般の重大事故の対策を含め、第三者機関（コンサルティング会社）による外部監査を現在実施しております。
E社	✓ ISOの認定に基づいて内部、および外部監査をおこなっています。 頻度：外部1回/年、**内部：2回/年**
F社	✓ 当社の内部統制に加えて、「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（安全・信頼性協議会）」に基づき、それぞれの対策の実施状況を定期的に点検し、必要に応じて対策の改善（内規の見直し等を含む）を実施しています ✓ 内部監査には、社長直轄組織として内部監査部があり、年間計画などに基づき各種の内部監査を実施しています。通信確保に関する事項も含まれ、「財務報告に関わる内部統制の評価及び監査に関する実施基準」に基づく内部統制監査に加えて、事業継続計画などのテーマを設定した監査なども実施しています ✓ 更に、ISO/IEC27001への準拠性、諸法令に基づく内部監査なども実施しています

図表 2-1 内部及び外部の監査・点検に関する各社の状況

[5] 東日本電信電話株式会社、西日本電信電話株式会社、株式会社 NTT ドコモ、KDDI 株式会社、ソフトバンク株式会社、楽天モバイル株式会社の 6 社を対象に実施した。

[6] 構造的な問題は存在しないとする一部事業者もあり、事業者による認識の違いも見られた。

[7] 電気通信事業法（昭和五十九年法律第八十六号）第 44 条において、（電気通信回線設備を設置等する）電気通信事業者は、事業法電気通信設備の管理の方針、体制、方法を定めた管理規程を定め、電気通信事業の開始前に、総務大臣に届け出なければならないとされている。

これを踏まえ、事故が多発する背景として、内部監査については概ね実施されているものの、ヒューマンエラー、リスク評価不足やリスク項目の洗い出し不足、復旧措置実施の場合の想定復旧時間の甘さ等も含め、通信の信頼性を確保するためのガバナンスが十分でないところもあると考えられる。また、外部監査等、通信の信頼性を確保するための外部モニタリングに関しては、定期的に実施されている例は多くない点にも、課題が見られる。

さらに、各事業者において通信サービスの確実かつ安定的な提供を確保するための設備管理の方針・体制・方法を「管理規程」に規定しており、対策の遵守性を点検している事業者も一部いるが、遵守性等の点検のみならず、通信の信頼性を確保するために、現行の保守運用態勢（ヒト, モノ, カネ, 組織等）が十分か等、自ら定期的に点検をしていく取組も必要と考えられる。

2.2 設備に関するリスクの洗い出し体制・方法

設備仕様、動作検証時等含め、リスクの洗い出しの実施状況ついて、各事業者の状況は以下の図表 2-2 のとおりであった。

✓ 設備仕様、動作検証時等含め、リスクの洗い出しの実施状況ついて	
A社	✓ 新機器導入時には要求仕様を提示し、適合する製品における正常動作、高負荷状態等異常状態での動作等を確認しています。過去の故障や他社の事例等に基づきリスクの洗い出しを行い、想定される異常パターン（回線故障、PKG 故障、IF 故障等）について検証を装置単体検証および検証用ネットワークでの動作検証を実施し、リスク低減に努めています。なお、リスク評価項目等については新機器・システム全体の構成や機能により異なるため一概に定められた値は ありません が、代表的なコア装置（保守・監視機能を含む）においては数百項目の検証を行い、リスク評価を実施しています。 ✓ 故障時の影響が大きい設備は冗長構成を取る等により即時サービス影響が出ない構成と しています 。それ以外の設備を含めて監視対象設備に対しては遠隔措置に加え即時現地修理対応を実施することとしており、大きな違いは ありません。
B社	✓ 新機器調達時には装置にかかわる仕様を提示し、メーカーが実装するため、高負荷状態等異常状態下の動作や諸元等を、その中で規定しております。 ✓ 過去の故障や他社の事例等に基づきリスクの洗い出しを行い、想定される異常パターン（回線故障、構成品故障等）について検証を装置単体検証および結合検証を実施し、リスクを排除するよう努めております。 ✓ 装置単体の検証や、他システム・装置との結合検証等を行う際に、回線故障、構成品故障等を想定した項目について検証を実施しております。 ✓ なお、リスク評価数については新機器・システム全体の構成や機能により異なるため一概に定められた値はございませんが、代表的なコア装置（保守・監視機能を含む）においては数百項目の検証を行い、リスク評価を実施しております。
C社	✓ リスクの洗い出しは、自社で発生した通信障害のみならず他社事例やグローバル製品情報に基づき都度実施しております。洗い出したリスクに基づき、新機器の商用稼働までの各工程において、利用する文書やチェック観点を見直すPDCAサイクルを随時行っており、導入設備の品質向上に努めています。 ✓ リスク評価項目としては、試験工程では機能要件非機能要件を網羅的に確認するだけでなく、様々な観点でシステム全体の安定動作を確認しています。 ✓ 評価内容については、開発手法やソフトウェア製造有無等により異なりますが、例えばソフトウェア製造有の場合は、バグ密度バグ曲線等による定量的評価に加え、発生したバグの内容や発生状況を踏まえた定性的評価を開発工程毎に実施しており、後工程へのバグ流出や見落としを排除するよう努めています。 ✓ 新機器の商用稼働にあたっては、小規模エリア等の商用環境でのフィールドテストを行い、本格商用展開事前の最終正常性確認を行います。
D社	✓ システム導入・作業ガイドラインに規定されている「障害パターン分類表」に従い、開発プロセスにて想定される障害パターンと冗長機能の動作を洗い出します。その後の検証プロセスにて仕様書に沿って作成した機能試験とは別に、障害パターン分類表に従った障害試験にてシステム評価を行います。 ✓ 評価は「片系障害、両系障害、輻輳、電源障害等」の観点にてシステム毎に詳細検討が必要なため、項目や数はそれぞれ異なります。
E社	✓ 【検証フェーズ】 設備仕様の詳細把握を行い、以下の方針で検証することによりリスクの低減と、洗い出しを実施しています。 ・3GPP等の標準に準拠していること　・ベンダーの組み合わせを意識した仕様調整　・異常を検知する仕組みの確認　・各種法令に準拠していること 実際の検証項目数としては機器×組み合わせ×インタフェース数により増減しますが、数百項目～数千項目になります。 ✓ 【商用適用フェーズ】 商用に適用する際には、最小規模のトラフィックを対象に一定の期間適用し、正常性を十分確認したうえで、段階的にトラフィックを拡大していくことで、リスクの極小化に努めています。
F社	✓ コア装置（EPC/IMS）レベルは、状況に応じて切り離し手順を準備し、各々の影響について検証環境にて確認しています ✓ ネットワークの設計においては検証運用技術部門等の関係部門が連携して潜在的リスクの洗い出しや影響評価を実施しています ✓ 例示として、当社での冗長化の検討の手法として、1.アーキテクチャデザイン：構成、切替シナリオの検討、2.TestCase：切替シナリオが動くかを検証、 3.Bugreport：既知バグの影響を考慮し検証、の三段階の検討・検証を実施しています。また、その後の運用の中で生じた問題・懸念について、上記の検討・検証に実施することによって、潜在的リスクの洗い出しや影響評価を実施しています

図表 2-2 リスクの洗い出し等に関する各社の状況

リスクの洗い出しについては、事故の未然防止等の観点から極めて重要であり、概ね各社実施されているが、網羅的なリスクの洗い出しには限界があり、洗い出しができるのは既知のリスクに限られ、未知リスクの洗い出しは困難である等の課題があると考えられる。

一方で、（現在、リスク認識について事業者間で連携する取組はなされていないが、）各社でリスクの既知性には違いがあり、ある社の未知のリスクが他社では既知のリスクとして対応済みの場合もあり得ると考えられ、未知のリスクに対する制度的対応についても検討が必要と考えられる。

2.3 予備系設備への切替え不能

通常、電気通信回線設備を設置する事業者においては、現用系と予備系の設備による冗長構成が取られており、ある設備が故障しても予備系の設備へ切り替わり、サービスの継続を可能とする取組がなされているが、半故障[8]等により予備系設備に切り替わらない場合の対応について、各事業者の状況は以下の図表 2-3 のとおりであった。

✓ 半故障等により冗長設備への切替え不能時における対応について	
A社	✓ 冗長構成としている装置は自動切換えに加え手動による遠隔措置により予備系でのサービス継続を 行うことを主たる対応としています。正常に切り替わらない等の場合は現地修理派遣 等も含めた措置にて 速やかなサービス復旧を 行うこととしています。半故障等の一部 の障害に対し全体の系を切り替える（現状サービス影響のない回線も影響が出る状況）に対しては課題もあり、昨今の障害を踏まえて必要な措置等を整理して いく所存です。
B社	✓ 正常系、準正常系だけでなく、異常系についても検証を行うことにより潜在的リスクの洗い出しを実施し、復旧に関する措置手順や正常性確認方法を保守運用マニュアルとして制定しております。 ✓ ただし、異常系について、すべてのパターンを洗い出し、検証を実施することは困難なため、自社・他社の故障事例から復旧手順を策定する等、常にブラッシュアップを図っております。
C社	✓ 開発工程で考慮すべきリスクの洗い出しについては、自社で発生した通信障害のみならず他社事例やグローバル製品情報に基づき、都度実施しております。また実施内容は、現存のシステムおよび開発中のシステムに対し、リスク影響を考慮し必要に応じて機能改修等を行っています。また、ヒアリング項目5で述べたとおり、設計・試験・構築・運用を通じて、文書・チェック観点の見直しを行うなどのPDCAサイクルも回しており、更なる品質向上に努めています。 ✓ 半故障等によりアラームを検知できない場合、各装置のCPU・メモリ使用率、トラヒックの流れ等を解析しつつ、被疑箇所を絞り込み、特定する。被疑箇所特定後は緊急措置マニュアルに従い対処する。 ✓ 速やかに正常動作への復帰を可能とするために、ヒアリング項目No.9にも定める緊急措置マニュアルに基づく対応を実施し、それでも復旧しない場合は手動による再起動、または、予備系への切り替えを実施するワークアラウンドを準備しています。
D社	✓ 一部故障により予備系に切り替わらない事象についても、システム導入時にガイドラインに基づき「冗長機能が動作しない障害パターン」として洗い出しを行い、対応手順を準備しています。洗い出し粒度についてシステムや実装機能によりバラつきがあるため、事故発生時にはその内容を横展開するなど、障害事例集やノウハウの共有により補完しています。 ✓ また、障害発生時に自動で予備系に切り替わらない場合を想定し、手動切替手順の準備や、対向設備から当該装置への通信を別ルートへ迂回させる手順を準備すると共に、速やかな復旧に備え、監視部門でも実施できるツール化や訓練を含めて運用引継ぎを行うようにルール化しています。
E社	✓ 各設備は常時、アラームの監視に加え、各システムのパフォーマンス等異常ログの有無やトラフィックトレンドの監視を実施しており、異常が認められた場合には、監視員による手動での冗長設備への切替を実施します。
F社	✓ 運用設備における作業に関しては、必ず当社試験環境で事前検証を行った後に実行するプロセスとしています ✓ 承認済のHLDおよび製品リリース情報を元に、機器ベンダーおよび当社技術・検証・運用の三部門が合同で作業手順書および新旧設備の仕様差分も考慮した検証項目を準備し、検証部門において事前検証を実施しています

図表 2-3 予備系設備への切替え不能時の対応に関する各社の状況

半故障等による予備系設備への切替え不能が原因で事故が発生することが非

[8] ここでは、「現用系の設備が正常に動作しているとシステム上では認識されているが、実際には電気通信サービスが継続できていない状態」をいう。

常に多い現状がある。各社で一定の取組はなされているが、切替え不能時の対応手順等は決めていても、当該対応を実施した場合の影響評価や訓練まで実施できていない者もいる。また、事故の長時間化の背景には、対応手順等を実施した場合の想定復旧時間の甘さ等もあると考えられる。

2.4 著しい高負荷時の挙動検証

コアネットワーク等の設備に対する、著しい高負荷時の挙動検証について、各事業者の状況は以下の図表 2-4 のとおりであった。

✓ 著しい高負荷時の挙動検証について	
A社	✓ 固定電話と IP ネットワークにて異なります。 ✓ 電話 ：企画型輻輳（特定番号への通話集中）の場合、当該番号への発信規制等により重要通信を確保するとともにネットワーク全体の機能維持 を 行います 。 ✓ IP ：特定ユーザによるトラフィック増等は監視で 対処します。セッション数 はトレンド等を見ながら設備増強等を 実施します。
B社	✓ 特にコア網等重要な装置については、過負荷試験や切替の繰り返し実施、長期安定試験等により潜在的リスクの洗い出しを実施し、復旧に関する措置手順や正常性確認方法を保守運用マニュアルとして制定しております。
C社	✓ システムに諸元を大きく超えるトラヒックが流入することで高負荷状態となることを想定し、諸元値の数倍の負荷または対向装置から流入される可能性のある最大トラヒック量以上の負荷をかけて検証しております。 ✓ なお弊社システムでは、高負荷に陥らぬよう、例えば端末がランダムに位置情報登録を行うことで位置登録信号を分散・平準化する機能を加入者DBに実装したり、加入者DB（PCRF）へのアクセス集中時に対向装置へ送出信号を減らす指示を行い輻輳を緩和する機能を実装するなどに取り組んでおります。
D社	✓ 各設備は過負荷に対する保護機能を有しており、負荷試験においては保護機能が動作する負荷を印加し、その挙動や設備の運用状態を評価しています。
E社	✓ 設備導入時及びソフト更新時において、装置の性能上限やネットワーク保護機能に関する技術情報をベンダーより入手し、検証環境において負荷試験装置を用いた性能試験や各種負荷制御機能の動作検証を実施しています。
F社	✓ 過負荷に対してトラフィック制御機能を具備する装置に関しては、相応の負荷を試験環境でシミュレータにより付加し制御動作を確認しています ✓ それ以外の装置は設計容量内のトラフィックを付加し、安定稼働する事の確認を行っています

図表 2-4 著しい高負荷時の挙動検証に関する各社の状況

各社一定程度は過負荷試験などを実施しているものの、著しい高負荷時の挙動検証の不足により事故が大規模化及び長時間化した事例がある。また、著しい高負荷時の挙動検証について、現行制度では義務化されていない点にも、課題があると考えられる。

2.5 商用稼働済設備の定期的な点検

商用稼働済設備の定期的な点検・検査、設備メンテナンス等の頻度、実施方法等について、各事業者の状況は以下の図表 2-5 のとおりであった。

✓ 商用稼働済設備の定期的な点検・検査、設備メンテナンス等の頻度、実施方法等について	
A社	✓ 各装置 の CPU 使用率、メモリ使用率、トラヒック、収容回線数等の設備使用率についてリアルタイムに把握。取得したデータを定期的に分析し、設備増設計画や異常検知に 活用しています。24 時間 365 日監視体制を維持して おり、監視 の中 でメジャー 警報であれば即時対応（ベンダー解析、遠隔措置、現地手配等）を行うとともに、マイナー警報についても情報把握は行い措置要否を 検討 しています 。 ✓ ソフトウェアバグ等が想定される、仕様として定めた動作と異なる場合はベンダーでの確認を 依頼しています。 ✓ 他社を含めて過去発生した故障についても類似故障の再発防止、通信サービスの早期復旧に向けて手順を整理するとともに、監視部門へ展開 しています。一定 規模以上に影響すると思われる想定外の故障が発生した場合には、復旧統制チームと情報統制チームに分けて対応 します 。 ・復旧 統制チームには社内装置主管部門やベンダーとの連携態勢を構築し対応 。 ・情報 統制チームは影響規模、社会影響、公表等について 対応。
B社	✓ ルータ・伝送装置やサーバ等装置類の CPU 使用率、メモリ使用率、トラヒック、収容ユーザ数等設備使用率について常時取得。取得したデータを定期的に分析し、設備増設計画や異常検知に活用。なお、常時監視の中で、 CPU 使用率やトラヒックで異常があった場合は、即座に解析し、対応。 ✓ ソフトウェアバグについては、ベンダーからの情報提供および自社で故障等が発生した際にはベンダーに確認しバグによるものか解析依頼を実施しております。 ✓ アップデートに際しては、机上検討確認に加えて、検証環境でデグレードしていないか、他の不具合が顕在化しないか等、確認を実施し、適用を判断しております。アップデート時にも、トライアルで一部設備に適用し、問題があれば切り戻す等でリスクの排除に努めております。 ✓ マイナーなバグ含めてサービス（主信号）への影響、保守への影響の分析を行い、社内関係部で優先度含めて実施判断を行います。 ✓ 既知の故障については、自社以外で発生したしたものについても復旧手順を整理するとともに、オペレータへの展開を実施しております。手順を定めていない想定外の故障が発生した場合には、社内の開発部門や NOC 内の技術支援担当から有スキル者を集めるとともに、メーカー等との連携体制を構築し、対応を行います。
C社	✓ 原則24H365D保守・監視を行う体制となっており、障害の状況によってはベンダーを含めた技術支援体制を整備、それ以外の設備は適切なSLAを定め保守体制を構築しています。人員体制は次頁参照（NOC要員：383人、保守要員：2,481人、無線従事者：8,551人、電気通信主任技術者：29人） ✓ コアネットワーク系一部装置では、日々定期で装置の正常性を確認するためのシナリオコマンドを自動で投入し、結果を出力を実行し、その結果を確認しています。 ※異常が確認されれば、詳細解析を行い、状況に応じた措置を実施
D社	✓ 商用稼働済み設備については、正常動作を常時監視しており異常検知時は速やかに復旧措置を実施し必要に応じて保守保全（機器の交換等）を行っております。
E社	✓ 定期的に点検・検査を実施しており、必要に応じて予備系への切替等の措置を実施しています。
F社	✓ 当社で、ベンダーに協力を求めつつ、事前に点検・検査対象項目と異常値などを定めて監視し、その結果に基づく必要な管理作業を実施する方法でメンテナンスを行っています ✓ 具体的には、アラームを監視する事項、アラーム化されていない計数を確認する事項、目視でログを点検する事項などがあります。また頻度は、例えば、１日に3回点検している項目を週次や月次ではその推移で点検するなど、項目ごとに必要な間隔や方法を定めて確認しています

図表 2-5 商用稼働済設備の定期点検に関する各社の状況

定期点検については、特にログファイル等、徐々にデータを蓄積して、最終的には領域を圧迫しうるファイルについて、定期点検が不足している事業者もいる。他方、現在、そうした対策を求める制度は、電気通信事業法等において特段存在しない点にも、課題があると考えられる。

2.6 平時からの事故対応に係る教育・訓練・人材育成

平時からの教育・訓練について、各事業者の状況は以下の図表 2-6 のとおりであった。

✓ 訓練の種類、実施頻度（●回/年）、対象者等について	
A社	✓ ネットワーク運営の機能毎に必要な訓練を 実施しています。保守監視部門においては日々実施する危険予知訓練を始め、週ごと、月ごと、四半期ごとに、復旧措置に加えて情報 連携も 含めて訓練企画しています。全社横断的な訓練は対応 要員等の入れ替わりが多い時期等に年 1 回実施。情報 統制チームに対するブラインドかつシナリオレスでの訓練を 2 回 月程度の頻度で実施中 。各部署毎に業務所掌内での習熟訓練を実施中。
B社	✓ 以下の演習、研修を実施しております。 ・復旧措置演習 ：年間 4 回で全 NOC 配置者対象 ・技術向上研修 ：年間 5 6 回で毎年 NOC 配置者の 一部対象 ✓ 上記の NOC を対象とした演習・研修に加え、年 1 回程度社外組織との連携やお客様への周知、幹部エスカレも含めた全社演習も実施しております。
C社	✓ NW関連部においては、サービス基盤障害訓練、及びNW設備全体の連携訓練を定期的に実施しています。また、広報対応などを含む全社訓練はマニュアル更新時の読み合わせを通した模擬訓練を不定期に実施しています。 ✓ 定期的な研修以外にも新装置導入（基地局設備等）の際に、核要員育成を目的とした導入研修を適宜開催しています。 ✓ OJTに関しては、新規着任者等に各組織にて適宜実施しています。
D社	✓ 訓練については以下の5パターンを行っております。 (1)社間部門間連携訓練　(2)新規設備新サービス運用開始前訓練　(3)一時間未満復旧訓練 (4)実際の障害を題材とした訓練　(5)経営層を含めた復旧体制の構築および周知広報の訓練 ✓ 訓練対象者の範囲は、(1)～(4)の訓練は監視者および保守運用者、(5)の訓練は技術・広報・営業・CSの各部門および経営層となります。
E社	✓ 事故を想定した以下の訓練を、部門間連携訓練も含め年間100回程度実施しています。訓練には事故発生時に対応すべき部門（事故対策統制、監視、情報発信対応、保全対応）が参加して実施しています。 ・初動体制構築訓練 ・設備の復旧対応訓練 ・周知広報の対応訓練
F社	✓ 次のような教育・訓練を実施しています ・年数回の全社訓練（主に社内連絡と顧客周知などを確認　・コアネットワーク重要設備の冗長切り替え訓練　・ネットワーク輻輳対応訓練等の訓練 日常業務の中に含んで実施している場合、例えば作業手順書の定期的な読み合わせなどもあり頻度の記載は難しいものの、新しい仕組みの導入当初は頻度を増やすなど、習熟度や訓練種類に応じた対応としています。また、訓練の対象者について、訓練種類や、訓練目的に応じた参加を設定し、実施しています。なお、上記のような様々な訓練等の教育機会を設けているため、人数等を明確に記載することは難しい状況です ✓ 仮想化環境においても、実施すべき訓練には違いはありませんが、検証施設において、電源断を想定した訓練なども実施しています

図表 2-6 訓練に関する各社の状況

訓練について、各社で一定の取組はなされているものの、事故の長時間化や周知広報の遅れの背景には、訓練面での課題も少なからずあると考えられ、定期的な訓練は不可欠と考えられる。なお、現行制度では、具体的な訓練は義務化されていない点にも、課題があると考えられる。

2.7 **ヒューマンエラー防止策**

ヒューマンエラーを防止するための対策について、各事業者の状況は以下の図表 2-7 のとおりであった。

✓ ヒューマンエラーを防ぐための取組について	
A社	✓ 作業手順の定型化、ツール化によるエラー 回避、複 数人による チェック、サービス 影響の大きい設備に対する作業時の体制 構築等を取り組んでいます。なおツールについてはベンダの協力も頂きシナリオ から Config 作成する等して 運用中です。
B社	✓ 如何なる作業についても、検証機器等を使い、手順書を作成するとともに、注意点を記載したチェックシートを作成します。 ✓ さらに、作業時には、複数の作業者による、2Way 確認を実施しながら手順書、チェックシートに従い、作業を実施します。 ✓ また、ヒューマンエラーの極小化のために可能な限りツール等による自動化を推進しております。 ✓ トラブル発生時は事象・原因・再発防止策を明確にし、関連組織で評価・共有を速やかに実施することとしています。
C社	✓ 作業手順書を都度準備し、手順に従った作業を行っています。また、作業にあたっては、複数人での作業・ツールの導入などを行うことでヒューマンエラーを防止するよう努めています ✓ ヒヤリハット事例の共有・スキルアップ勉強会などを行い意識醸成・人材育成強化も図っています。
D社	✓ ヒューマンエラー防止を推進する会議体にて、ヒューマンエラーの事例共有・対策の水平展開を行うと共に、各作業実施部門では、安全作業を行う上で注意すべき事項を纏めた「作業の心得」を随時確認し安全意識の向上に努めています。また、作業を実施する前には、危険予知ミーティングを行い、周知展開されたエラーと同様のミスを起こさないように注意喚起をしています。
E社	✓ 人為的なミスを含む過去発生した問題事象の発生原因・実施した対策について、トレースおよび定期的（月次）に社内関連部門へ水平展開して風化を防止する活動を行っています。
F社	✓ 作業手順書は、その作成段階で各作業単位での変更内容を当社技術部門が精査し、事前検証を行う事としています ✓ 作業手順書による設定変更作業手順の妥当性および効果の評価は自社の責任範囲であり、当社試験環境において、変更時の影響を受ける箇所を含め、当社が提供するサービス全般の事前・事後検証を実施しています ✓ 検証済み手順書を用いて当社技術部門員が実行する体制をとり、未検証作業手順書による運用設備作業は禁止しています ✓ なお、ヒューマンエラー防止のため、ネットワーク作業に当たっては、 １設備設計部門 ２セキュリティ部門 ３設備運用部門 ４作業統括部門 の４段階承認加えて運用部門責任者も承認します ※作業手順書は作業承認システムからダウンロードしており、正しい手順では手順書の取り違えることは起こりません

図表 2-7 ヒューマンエラー防止策に関する各社の状況

ヒューマンエラーの防止策については、各社でも一定の取組はなされているが、ヒューマンエラーが原因で重大な事故に至るケースも少なくない現状がある。また、電気通信事業法等の現行制度では、ヒューマンエラーの防止策が義務化されていない点にも、課題があると考えられる。

2.8 利用者への周知広報・透明性確保

昨年夏以降、大規模な通信事故が発生しているが、これら事案における利用者への周知広報の状況は、以下の図表 2-8 のとおりであった。

発生日時 （継続時間）	通信 事業者	影響サービス	影響範囲 （地域、利用者数）	発生原因	発生から利用者への 初報時間
7月2日(土) （61時間25分）	KDDI	音声通話、SMS、 ホーム電話、 データ通信	全国 音声通話：約2,278万人 データ通信：765万人以上 【重大事故に該当】	人為的ミス	1時間41分 緊急通報機関へ連絡**なし**
8月24日(水) （45分間）	KDDI	音声通話、SMS、ホーム 電話、 データ通信	東日本エリア 最大8.3万人	設備故障	1時間17分 緊急通報機関へ連絡**あり**
8月25日(木) （5時間47分）	NTT 西日本	インターネットサービス （フレッツ光）	西日本エリア 最大２１１万回線(品質低下) サービス停止は最大1時間50分 【重大事故に該当】	設備故障	2時間53分
9月4日(日) （2時間28分）	楽天 モバイル	音声通話、 データ通信	全国エリア 最大１３０万回線 【重大事故に該当】	設備異常	1時間05分 緊急通報機関へ連絡**なし**
9月4日（日） （37分間）	ソフト バンク	音声通話、 データ通信	中国・四国・九州地方 ４Ｇ回線：最大約105万回線 ５Ｇ回線：最大約730回線	人為的ミス	2時間03分 緊急通報機関へ連絡**あり**
12月17日（土） （4時間54分）	NTTドコモ	データ通信	最大約242万人 【重大事故に該当】	設備異常	1時間22分
12月20日（火） （2時間02分）	NTTドコモ	データ通信	最大約69万人 【重大事故に該当】	人為的ミス	58分

図表 2-8 最近（令和４年度）の通信事故における利用者への周知広報の状況

これらを踏まえると、通信事故発生時において、利用者への初報に多くの時間を要するもの、必ずしも利用者が必要とする情報の発信ができていないもの、利用者に大きな混乱を生じさせる表現で情報発信を行ったもの、緊急通報に影響があるにも関わらず緊急通報受理機関への連絡がなされないもの等、電気通信事業者による周知広報の在り方や透明性の確保についても課題が見られる。

これを踏まえ、昨年 10 月から「電気通信事故検証会議　周知広報・連絡体制 WG」が開催され、本年１月 27 日（金）に報告書が取りまとめられた。また、本取りまとめを踏まえ、総務省において、本年３月に「電気通信サービスにおける障害発生時の周知・広報に関するガイドライン」の策定が行われた。電気通信事業者においては、こうした取組も踏まえて、利用者への適切な周知広報を行っていくことが必要であると考えられる。

2.9 通信事故の背景にある構造的な問題の整理

以上を踏まえると、電気通信分野において、以下のように、ガバナンス、リスク管理、利用者周知などの組織・態勢面での共通的課題（構造的問題）があると考えられる。

① 通信の信頼性を確保するための保守運用態勢に対するガバナンス及びモニタリングが十分でない

✓ ヒューマンエラー、リスク評価の不足、想定復旧時間の甘さ等も含め、委託先を含む保守運用態勢に対するガバナンスの不足　【論点①】

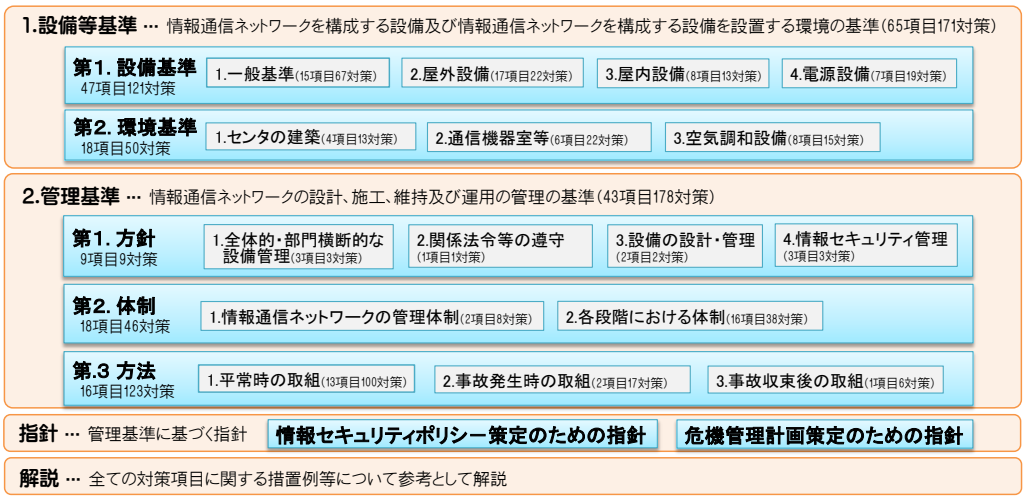
✓ 第三者による監査・モニタリングの不足 【論点②】

② また、個別の論点として以下の課題が見られる
✓ 設備におけるリスクの洗い出しが不十分 【論点③】
✓ 冗長が機能しない半故障時の対処が不十分 【論点④】
✓ 著しい高負荷時の動作検証が不十分 【論点⑤】
✓ データ蓄積型の設備への定期監視が不十分 【論点⑥】
✓ 訓練が不十分（メンテナンス訓練等） 【論点⑦】
✓ ヒューマンエラーの防止策が不十分 【論点⑧】
✓ 利用者への周知広報・透明性確保が不十分 【論点⑨】

上記論点について、現行制度の見直しも含め、検討していくことが必要である。

図表 2-9 電気通信事業法における設備規律について

- 情報通信ネットワーク全体から見た対策項目につき網羅的に整理・検討を行い、**ハードウェア及びソフトウェアに備えるべき機能やシステムの維持・運用等**を総合的に取り入れた安全・信頼性に関する**推奨基準（ガイドライン）**として策定。
- **技術基準等の対象となるネットワーク**（回線設置事業者、ユニバーサルサービス提供事業者、有料で利用者100万以上のサービス提供する回線非設置事業者のもの）に加え、**自営情報通信ネットワーク**や**ユーザネットワーク**も対象。
- 全国5Gの特定基地局の開設指針等において、サプライチェーンリスクを考慮した機器調達（基地局、ネットワーク設備）を申請者に促すため、**認定の条件として、本基準に留意**することを規定。



図表 2-10 情報通信ネットワーク安全・信頼性基準

3. 構造的な問題を踏まえた対策について

電気通信事業者による大規模な通信事故が連続して発生する中、利用者の利益を保護していくためには、前述のとおり、電気通信分野において、ガバナンス、リスク管理、利用者周知等の共通的課題を踏まえた対策について検討することが急務である。

このため、前項「2.9　通信事故の背景にある構造的な問題の整理」で記載した、①ガバナンスの強化、②外部モニタリング、③リスク管理、④予備系設備への切替え不能時の対処、⑤著しい高負荷時の動作検証、⑥データ蓄積型設備への定期監視、⑦訓練、⑧ヒューマンエラー防止対策、⑨利用者への周知広報、の９つの論点について検討を行った。

3.1 ガバナンスの強化

（１）課題・論点

昨年の夏以降、大規模な通信事故が多発しているが、こうした事故が多発する背景として、ヒューマンエラー、設備の諸元の確認不足、ソフトウェア情報の見落とし等も含め、電気通信事業者自身によるガバナンスが十分でない危惧があり、ガバナンス強化について検討が必要である。

（２）検討

国民生活や経済活動の基盤となるインフラであり、機能の停止や低下により大きな混乱を招くと見込まれる、通信、金融、航空、鉄道、電気、ガス、水道等のいわゆる重要インフラにおいては、安全管理対策等について自主的な点検を義務付けているものが多い。具体的には、電気分野では、定期安全管理検査が義務付けられている[9]。ガス分野でも定期自主検査等が義務付けられている[10]。銀行分

---

[9] 昭和 39 年に制定された電気事業法の電気保安規制については、国による直接的な検査が実施されていたが、電気事故の増加や時代の変化に伴い、安全実態の向上等を踏まえ、平成 11 年に国による直接検査を原則廃止し、自主検査化および自主検査の品質を国等が審査するための法改正が行われた。

（参照）今後の電気保安のあり方について，経済産業省 電力安全課，平成 27 年 3 月 20 日
https://www.meti.go.jp/shingikai/sankoshin/hoan_shohi/denryoku_anzen/pdf/009_02_00.pdf

[10] 平成 11 年のガス事業法改正に伴い、これまでの国による定期検査が廃止され、ガス事業者による定期自主検査が行われることとなり、公共の安全を確保することを目的として、ガス事業者が、当該ガス事業の用に供するガス工作物を経済産業省令で定める技術上の基準に適合するように維持することが義務付けられている。

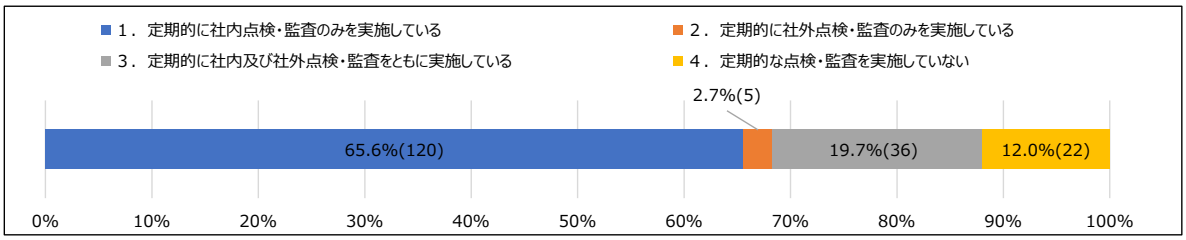
（参照）ガス工作物定期自主検査要領，経済産業省 商務流通保安グループ，平成 29 年 4 月
https://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/citygas/hourei/teikijis

野でも、年度ごとに業務の状況等を記載した業務報告書の作成及び提出義務がある。他方、通信分野においては、現在、定期的に自主点検を求める制度が存在しない。

分野	主な自主点検に係る制度の内容
電気	・特定電気工作物を設置する者が定期安全管理検査を自主的に実施。
ガス	・ガス製造事業者等が定期自主検査を自主的に実施。
金融（銀行）	・銀行は、事業年度ごとに中間業務報告書及び業務報告書を作成し、内閣総理大臣に提出する義務がある。
運輸（鉄道・航空運送事業）	・国土交通大臣が、毎年度輸送の安全に関わる情報を公表。 ・事業者が、毎事業年度安全報告書を公表。
水道	・水道事業者が水質検査を定期的（おおむね一箇月に一回以上等）に実施。

図表 3-1 他分野における自主点検に係る制度の概要

また、今回、総務省において、電気通信回線設備を設置する事業者等を対象にしたアンケート調査[11]（以下「電気通信事業者アンケート調査」という。）を実施した。当該調査結果によると、管理規程の遵守・実施状況について「定期的に社内点検・監査のみを実施」が 65.6%、「定期的に社内及び社外点検・監査をともに実施」が約 19.7%であり、約 85%は定期的な内部点検・監査を実施している。



図表 3-2 管理規程の定期的な点検・監査等実施状況

さらに、仮想化技術等の進展によって、モバイル網のコアネットワークのよう

yukensayouryou.pdf

[11] 調査期間：令和４年１２月２２日～令和５年１月１２日（※〆切後に受領した回答も含む）
調査対象者：回線設置事業者（４５２者）及び国民生活に重要な役割を果たすサービス（有料かつ大規模なサービス）を提供する回線非設置事業者（４者）
回答数：１８７者
調査形式：選択回答形式によるアンケート
調査実施者：総務省 総合通信基盤局 電気通信事業部 安全・信頼性対策室

な電気通信回線設備の伝送交換の制御に係るコア機能を自ら管理せず、外部から当該コア機能の提供を受けて、電気通信サービスの提供を行うことが技術的に可能となっており、諸外国では5Gのコアネットワークの機能の一部をクラウド化・アウトソース化している事例も出てきている[12]。このような場合であっても、外部から提供を受けた当該コア機能に関しても電気通信サービスの確実かつ安定的な提供のために不可欠なものとなることから、適切にガバナンスを強化していく取組が重要である。

（３）対応の方向性

電気通信事業者の一層のガバナンス強化を図るため、情報通信ネットワーク安全信頼性基準（以下「安信基準」という。）や、事業者自らが管理の方針・体制・方法を定めた管理規程に関して、

① 設備の保守運用をする外部の委託先事業者等を含め、同規程の遵守状況等（安信基準の参照状況や論点③で記載の想定復旧時間等、復旧手順の実施によるサービスの影響評価の実施状況含む）、

②当該遵守状況等（影響評価等含む）を踏まえ、現行の管理規程の見直しは不要か、現行のヒト、モノ、カネ、組織等の態勢が十分か

等について、経営層により、費用と効果のバランス等も総合的に考慮の上で、事業者自身で毎年点検を行うことを求めることが必要である[13]。当該点検結果を踏まえ、事業者自身で、信頼性の高い電気通信サービスの提供と、デジタル社会の形成等を牽引するイノベーションの促進等も考慮しつつ、Plan（計画）、Do（実行）、Check（評価）、Action（改善）のPDCAサイクルを回していくことが適当である[14]。

さらに、次項「3.2　外部モニタリング」に記載のとおり、事業者自身の自主性を尊重しつつ、事業者によるガバナンスの取組を補完するため、当該事業者自身による点検結果に対する外部からのモニタリングも必要と考えられる。

---

[12] 米国の通信事業者であるAT&Tが仮想化したコアネットワークの機能をMicrosoftのクラウド上に移管する旨が発表されている。
（参考）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 第二次報告（令和５年２月）

[13] 具体的には、電気通信事業法施行規則（昭和六十年郵政省令第二十五号）において、事業者が定める管理規程に、経営層による管理規程の遵守状況等の点検についての記載を求めることが考えられる。

[14] PDCAサイクルを補強するものとして、『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　第五次報告』においては、特に想定外や変化がある短期的環境に適用される理論として、未然に防ぎきることは不可能である状況等不測の事態においては、Observe（内外環境の観察）、Orient（方向付け・情勢判断）、Decide（方針・意思決定）、Act（行動）の「OODAループ」的な対応も重要とされている。

3.2 外部モニタリング

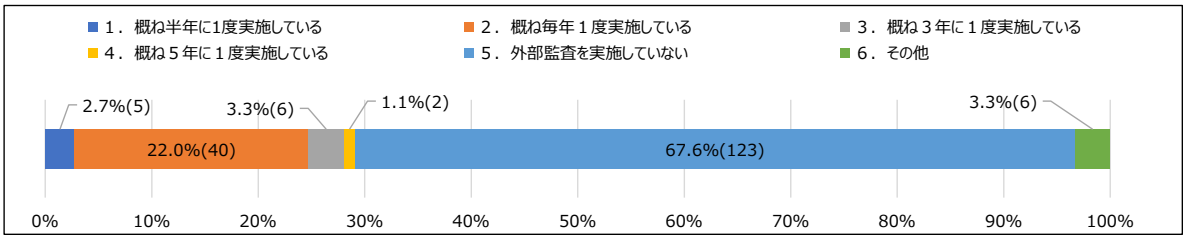
（１）課題・論点

事業者自身のガバナンスを補完する上で、外部からのモニタリングについても検討が必要である。

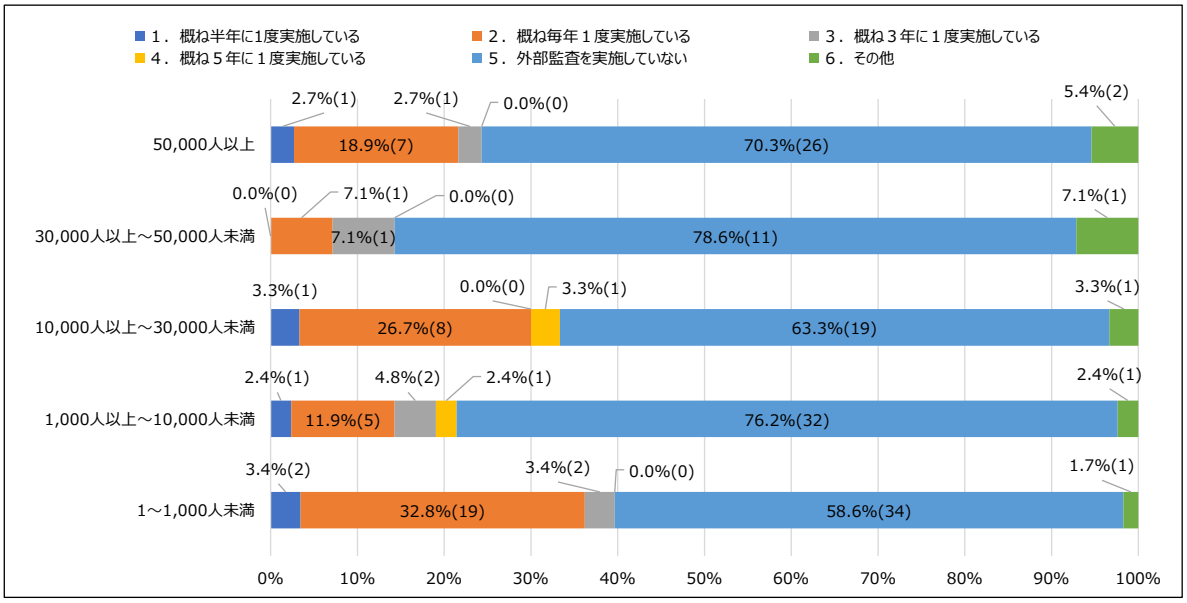
（２）検討

電気通信事業者アンケート調査によると、図表 3-3 のとおり、安全管理に対する外部監査の実施状況について、半年に１度実施と毎年１度実施を合わせ約 25%は毎年少なくとも 1 度は外部監査を実施しているものの、そもそも外部監査を「実施していない」が 67.6%存在する。

図表 3-4 は、契約者の規模別の外部監査の実施状況を示したものであるが、契約者数が 5 万人以上を有する事業者においても「外部監査を実施していない」が 70.3%存在しており、利用者に与える影響力が大きな事業者であっても、外部監査を実施していない事業者が多い。



図表 3-3 安全管理に関する外部監査の実施状況



図表 3-4 契約者の規模別の外部監査の実施状況

また、国民生活や経済活動の基盤となるインフラであり、機能の停止や低下により大きな混乱を招くと見込まれる、通信、金融、航空、鉄道、電気、ガス、水道等のいわゆる重要インフラにおいては、図表 3-5 のとおり、分野によって細部の違いはあるものの、多くの分野において平時モニタリングが導入されている。

具体的には、電気分野では、重要な設備は政府が設備ベースの定期検査を実施するとともに、事業者に自主的な安全管理の検査を義務付け、当該検査の実施体制について政府が審査を行う制度となっている。また、政府が定期的に業務及び経理の監査を行う制度がある。

ガス分野も、自主的な検査等を義務付けるとともに、政府が定期的に事業の監査を行う制度がある。

銀行分野では、サイバーセキュリティやシステム等の対策を含め幅広い事項について、実態把握や対話を通じ、政府が検査・監督を行う制度がある。

運輸分野では、鉄道、航空、自動車、海運等含め、「運輸安全マネジメント評価[15]」として、安全重点施策等、政府が広範囲に評価を行う制度があるとともに、定期的に監査計画に基づき政府が監査を実施している。

一方、通信分野においては、そうした平時から定期的に政府による監査・点検等を行う制度は現在存在しない。

分野	主なモニタリング制度の内容
電気	・経済産業大臣が特定重要電気工作物を設置する者に対して、定期検査を原則年に一回実施。 ・**特定電気工作物を設置する者が定期**安全管理**検査を自主的に実施**。 ・当該定期安全管理**検査の実施に係る体制について**、**経済産業大臣又は登録安全管理審査機関が**原則**年に一回審査**を実施。 ・**経済産業大臣**（又は電力・ガス取引監視等委員会）**が業務及び経理の監査を、年に一回実施**。
ガス	・ガス小売事業者等がガス成分の検査を毎週一回実施。 ・ガス製造事業者等が熱量等の測定を毎日実施。 ・ガス製造**事業者**等**が定期自主検査を自主的に実施**。 ・**経済産業大臣**（又は電力・ガス取引監視等委員会）**が事業の監査を、年に一回実施**。
金融 （銀行）	・**金融庁が検査監督基本方針に基づき**、社外取締役、監査役、経営トップ、顧客等、金融機関内外の様々なレベルの者との幅広い対話等の**金融モニタリングを実施**。
運輸 （鉄道）	・**国土交通省が鉄道事業者に対して、運輸安全マネジメント評価を実施**。 ・鉄道分野、航空分野、自動車分野（貸切バス事業者を除く）及び海運分野の合計で、年間９０から１１０事業者程度を目安として、計画的かつ効率的に実施。 ・**国土交通省が監査計画に基づいて保安監査（立入検査）を実施**。令和３年度実績として、32事業者に実施。
運輸 （航空運送事業）	・**国土交通省が本邦航空運送事業者に対して、運輸安全マネジメント評価を実施**。 ・鉄道分野、航空分野、自動車分野（貸切バス事業者を除く）及び海運分野の合計で、年間９０から１１０事業者程度を目安として、計画的かつ効率的に実施。 ・**国土交通省が「航空運送事業等の安全監査に関する基本方針」に基づいて保安監査（立入検査）を実施**。 （本社4回／年、主基地2 回／年、地方基地1回／4年、訓練所1回／2年 等）
水道	・水道事業者が水質検査を定期的（月に一回以上等）に実施。

図表 3-5 他分野のモニタリング制度の概要

---

[15] 平成 17 年 4 月に発生した JR 西日本の福知山線における脱線事故等、運輸に係る事業においてヒューマンエラーが原因とみられる事故等が多発したことがきっかけで、安全管理体制を国が監視する仕組み（安全マネジメント評価）を導入することが提言され、翌年 10 月から運輸マネジメント制度が開始された。
（参考）運輸安全一括法に規定する安全管理規定に係るガイドラインの手引、平成 19 年 12 月、国土交通省大臣官房 運輸安全管理官室
https://www.mlit.go.jp/unyuanzen/pdf/tebiki_guideline.pdf

諸外国においても、図表 3-6 のとおり、対象に違いはあるものの、通信分野で平時モニタリングが導入されている国・地域がある。具体的には、米国では、緊急通報サービスに関して、ネットワーク監視の集約点等における監査の実施について、政府によるモニタリングの制度がある。EU では、ポリシーの監視とログの取得、緊急対応計画の実行等について、政府による平時モニタリングの制度が欧州電子通信コードで言及されている。英国でも、2021 年に改正された通信法規則で、モニタリングの制度が存在する。

国／地域	主なモニタリング制度の内容	備考
米国	・**連邦規則**「CFR Title 47 Part 9 Section 19（Reliability of covered 911 service providers）」**において、緊急通報サービス（911）に関するネットワークモニタリングについての規則が盛り込まれている**。 ・対象となる911サービスのプロバイダは、**毎年、**それぞれの**911サービスエリアにおいて**、ネットワーク監視データを収集するために使用する**集約点における物理的冗長性の監査**を実施すること等**が義務付けられている**。 ・**規則の対象事業者は、緊急通報サービス（911）を提供する全ての事業者**等。	2012年に発生したデレチョ（嵐/竜巻）において、バックアップ電源等の設備に不足があったことに起因して、6州の911サービスが中断されたことに伴い制定。
ＥＵ	・**EUが定めた電気通信に関する制度「EECC（欧州電子通信コード）」において**、事業者がネットワーク・サービスに対するセキュリティ対策が適切に遂行されていることを保証する、第40条「Security of networks and services」に、**政府からのモニタリングに際して、最低限具備しておくべき要件**（ポリシーの監視とログの取得、緊急対応計画の実行等）**が定められている**。	各国の既存の法令・ガイドラインや、政府の方針によって、個別の国ごとにどのような実装をしているかは異なっている。
英国	・**2021年に改正された通信法**の規則「Section 105Z11」**に「モニタリング」に関する記載が存在**。 ・Ofcom（通信当局）は国務長官の指令によって通信サービス事業者をモニタリング。	対象事業者・頻度に関する特段の定めはない。

図表 3-6 海外の通信分野のモニタリング制度の概要

なお、図表 3-7 のとおり、設備ごとに障害パターンの洗い出しを行い、サービス影響や復旧対処等を分析している事業者も存在する。「2.2　設備に関するリスクの洗い出し体制・方法」で前述のとおり、各事業者において網羅的なリスクの洗い出しには限界があり、洗い出しができるのは原則として既知のリスクに限られ、未知リスクの洗い出しは困難である。一方で、各社でリスクの既知性には違いがあり、ある社の未知のリスクが他社では既知のリスクとして対応済みの場合もあることから、こうした設備ごとに洗い出されたリスクについて、設備ごとに共通の視点で第三者が点検を行い、同意の得られる範囲で、不足するリスク認識について事業者に指摘を行うことは、事業者のリスク認識を広げ、事故の未然防止につながる効果が一定程度期待できると考えられる。

障害パターンごとの評価例
・障害パターンに当てはめ、事前に動作想定を検討、検知手法やサービス影響を確認
・それぞれのパターンで復旧対処を検討・検証し運用スキームに追加

装置構成（例）
・２台の冗長構成
（両方ともACT）

障害パターン	片系障害	両系障害	輻輳	電源障害
事象状況	設備 設備	設備 設備	設備 設備	設備 設備
想定動作	①設備から応答がある ②設備から応答無し	①設備から応答がある ②設備から応答無し	①両設備が均等に輻輳 ②輻輳程度に差分あり	①片系のみ電源障害 ②両系とも電源障害
検知	①設備からのアラーム ②対向装置/死活監視	①アラーム/サービス監視 ②死活監視/サービス監視	①②アラーム/リソース監視/トラヒック監視	①②アラーム/死活監視等
サービス影響	①影響無し ②影響あり(1/2で失敗)	①②影響あり	①②影響無し(一時的輻輳で影響あるケース有り)	①影響無し ②影響あり
復旧対処*	①故障設備を切り離し ②回線閉塞/装置リセット	①②設備リセット/他拠点の設備群へ迂回	①規制/増設 ②負荷分散設備の確認	①故障設備を切り離し ②他拠点の設備群へ迂回

*復旧対処は自動的に行われるケースもあり(他拠点の設備群へ迂回など)

図表 3-7 設備ベースのリスクの洗い出しの事例

（３）対応の方向性

事業者自身の自主性を尊重しつつ、事業者によるガバナンスの取組を補完するため、「3.1 ガバナンスの強化」で記載の（①管理規程の遵守状況等、②それを踏まえ、管理規程の見直しの要否、現行のヒト，モノ，カネ，組織等の態勢が、費用と効果のバランス等も総合的に考慮の上で十分か等の）経営層による点検結果等を対象として、行政等が毎年モニタリング（以下「ガバナンスのモニタリング」という。）を行うことが適当である。

点検の具体的な内容としては、例えば、①上記点検結果、②内部・外部監査結果のうち通信の信頼性確保に係る対策に関するものが考えられる。

こうしたモニタリングを通じて、他の事業者にも参考となる優良な取組事例等があれば、事業者の競争力の保護とガバナンスの自主性を考慮のもと、事業者の了承を得た上で、安信基準等に反映し、推奨事項としていく取組も適当と考えられる。

また、可能な限りリスクの洗い出しを行うことが、大規模事故の防止につながると考えられることから、各社による設備におけるリスク管理及びリスクの洗い出しの強化のため、ひいては事故の未然防止の一層の強化を図るため、リスクの洗い出し項目及びリスクに対する対応措置についても行政等がモニタリング（以下「設備ベースのモニタリング」という。）を行い、事業者の同意が得られる範囲で、考慮されていないリスク項目等についてフィードバックを行うことが適当である[16]。

[16] 設備ベースのモニタリングについては、毎年、実施計画等において、モニタリングの対象となる設備をいくつか特定し、当該対象設備における①リスクの洗い出し項目及び②各リスクに対する対応措置等について、政府等が共通的な視点で点検を行うことが考えられる。

なお、電気通信事業者のうち、利用者の利益に与える影響が大きい者を対象に、内閣総理大臣は防災行政等において重要な役割を有するものとして「指定公共機関（電気通信分野における、災害対策基本法の指定公共機関をいう[17]。以下同じ。）」を指定している。こうした事業者には、他の電気通信事業者と比較して、電気通信役務の確実かつ安定的な提供が一層期待されていると考えられる。

こうした点や利用者に与える影響の大きさ等を考慮し、当該２つのモニタリング（ガバナンスのモニタリング及び設備ベースのモニタリング）の対象者については、当面は、例えば、電気通信役務を提供する指定公共機関に対象を限定することが考えられる。

また、電気通信分野は非常に技術の進歩や環境の変化が激しい分野であることに鑑み、そうした変化に柔軟に対応できるようにするため、外部モニタリングに際しては、金融庁による金融機関への検査・監督や国土交通省による運輸分野の保安監査では、業法に共通して存在する報告徴求や立入検査等の条文[18]を根拠として、政府が点検を行う基本方針等を策定し実施していることを参考に、基本方針に基づき、毎年、（環境の変化等を踏まえ重視する観点や点検対象となる設備等を記載した）実施計画を策定して、実施していくことが考えられる。

なお、電気通信サービスは非常に変化の激しいサービスであり、通信分野の事故の状況や電気通信事業を取り巻く環境の変化等にも留意しながら、より効果的なモニタリングとなるよう、モニタリングの実施方法等については定期的に見直しを行うとともに、外部モニタリング制度の在り方やモニタリングの対象となる者等を含め、不断の見直しが必要である[19]。

---

[17] 電気通信分野では、日本電信電話株式会社、東日本電信電話株式会社、西日本電信電話株式会社、株式会社 NTT ドコモ、エヌ・ティ・ティ・コミュニケーションズ株式会社、KDDI 株式会社、ソフトバンク株式会社、楽天モバイル株式会社の８者が指定されている。

[18] 電気通信事業法においては、第 166 条が該当する。

[19] 政府等によるモニタリング結果の公表の在り方についても、他分野の状況等を踏まえ、検討していくことが考えられる。なお、「電気通信サービスにおける障害発生時の周知・広報に関するガイドライン案」においては、事故等の通信障害が発生した際には、「障害復旧後も、原因、影響利用者数等の障害の概要を、（ホームページの）分かりやすい場所で少なくとも１年程度は掲載しておく。」とされており、一定程度、利用者に対する透明性を高める取組がなされている。政府等によるモニタリング結果の公表を含め、引き続き、利用者に対する透明性を高める取組について不断の見直しを行うことが適当である。

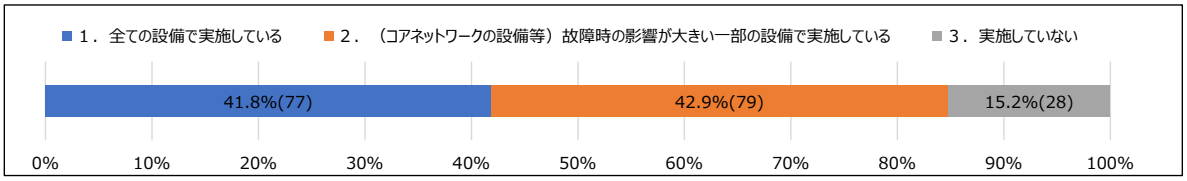
3.3 **リスク管理**

（１）課題・論点

設備に対するリスク項目の洗い出しやリスク評価が適切に実施されるとともに、洗い出されたリスクに対して、対応措置等が事前に検討されていれば、事故の未然防止や大規模化の抑制に寄与すると考えられる。設備におけるリスク管理・リスクの洗い出しに関して、制度的な検討が必要である。

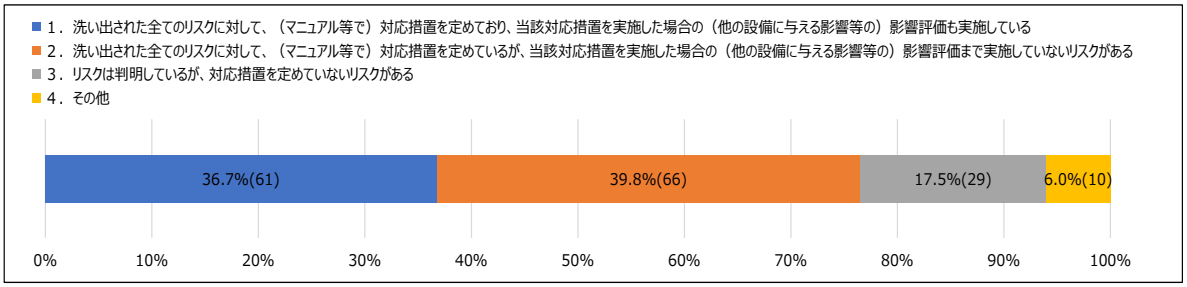
（２）検討

電気通信事業者アンケート調査によると、図表 3-8 のとおり、41.8%が全ての設備でリスクの洗い出しを実施しており、42.9%が少なくとも利用者に与える影響が大きいコアネットワークの設備についてリスクの洗い出しを実施している。このため、合計約 85%が少なくとも利用者に与える影響が大きいコアネットワークの設備についてリスクの洗い出しを実施している。一方、設備におけるリスクの洗い出しを未実施の事業者も 15.2%存在する。



図表 3-8 商用稼働までの設備ごとのリスク洗い出しの実施状況

また、洗い出された全てのリスクについて、図表 3-9 のとおり、マニュアル等で対応措置を定めるとともに影響評価を実施しているのは 36.7%、マニュアル等で対応措置を定めているが影響評価を実施していないのは 39.8%、どちらも実施していないのは 17.5%となっている。しかしながら、リスクの洗い出しを実施しても、当該リスクが発生した時の対応措置が定まっていなければ、確実な事故の未然防止につながらないことに留意が必要である。



図表 3-9 リスクへの対応状況

（３）対応の方向性

電気通信回線設備を設置する事業者等に対して、少なくとも利用者に与える影響が大きいコアネットワークの設備については、

① （各設備において）リスク項目の洗い出し
② 洗い出された各リスクに対する対応措置・復旧手順の整備
③ 当該手順を実施した時のサービスへの影響評価（想定復旧時間含む）
の３つについて、管理規程において実施を義務化することが適当である[20] [21]。

またこれらを踏まえた事業継続計画（BCP）[22]の策定についても、管理規程において義務化することが適当である[23] [24]。

併せて、「安信基準」で、
① コアネットワーク以外の設備に対するリスク項目の洗い出し等、
② 洗い出されたリスク項目に対する復旧手順の訓練
について、(特に訓練については利用者への影響が出ない範囲で)推奨していくことが適当である。

また「3.2　外部モニタリング」で前述のとおり、電気通信役務を提供する指定公共機関を対象に、リスクの洗い出し項目について政府等が設備ベースのモニタリングを行い、事業者に了承が得られた範囲で、他の事業者が不足するリスク認識がある場合には指摘をし、事業者のリスク認識を広げていくことが適当である。

3.4 予備系設備への切替え不能時の対処

（１）課題・論点

設備が十分に機能を発揮できないものの、冗長設備に切替わるほどの故障ではない、いわゆる半故障等、予備系設備への切替え不能を原因として事故に至るケースが非常に多く、制度的な検討が必要である。

（２）検討

---

[20] 具体的には、電気通信事業法施行規則等において、事業者が定める管理規程に、リスクの洗い出し等の実施についての記載を求めることが考えられる。具体的な記載方法については、「管理規程記載マニュアル」において、記載例等を示すことが考えられる。

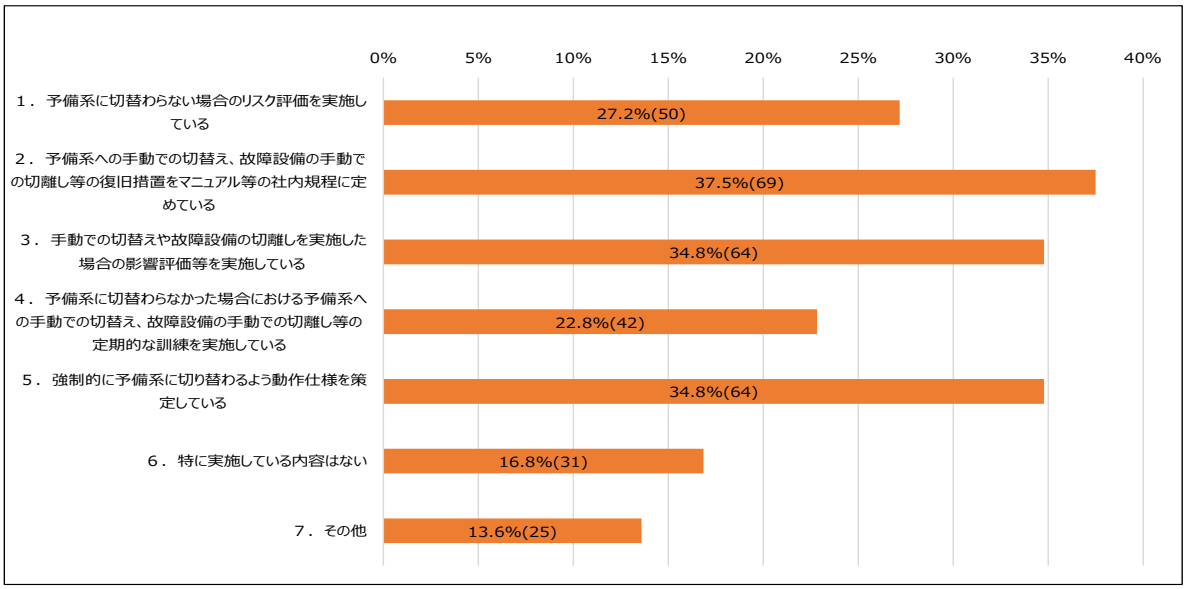
[21] 事業者が想定可能なリスクを対象とするものであり、想定できないリスクは対象とならない。

[22] 事業継続計画（BCP）に相当する各社規程の策定を含む。

[23] 具体的には、電気通信事業法施行規則等において、事業者が定める管理規程に、リスクの洗い出し等を踏まえた事業継続計画（BCP）の策定に係る記載を求めることが考えられる。

[24] 原因不明の故障等による事故も多いことから、原因を問わず、故障等のリスクに対する事業継続計画（BCP）を策定することが適当である。

電気通信事業者アンケート調査によると、図表 3-10 のとおり、「予備系に切替わらない場合のリスク評価を実施している」が 27.2%、「復旧措置をマニュアル等の社内規定に定めている」が 37.5%、「手動での切替えや故障設備の切離しを実施した場合の影響評価等を実施している」が 34.8%、「定期的な訓練を実施」が 22.8%、「強制的に予備系に切り替わるよう動作仕様を策定」が 34.8%、「特に実施している内容はない」が 16.8%である。



図表 3-10 半故障等による予備系設備への切替え不能時の対応状況

予備系設備への切替え不能を原因として重大な事故に至るケースが非常に多いことに鑑みると、少なくともコアネットワークの設備に関しては、十分な対策が必要である。併せて、こうした半故障の場合は、アラートが鳴らないサイレント故障の場合も多く、サイレント故障についても同様に、制度的な対応が必要である。

（３）対応の方向性

特に、半故障等に起因した、①予備系への切替え不能に係るリスク、②アラートが鳴らないサイレント故障のリスク、の２つのリスクについては、これらが原因で大規模な事故に至ることが多い事情を考慮し、コアネットワークの設備に関しては、この２つのリスクについてのリスク評価の実施、対応措置・復旧手順の整備、当該措置実施時のサービスへの影響評価の実施を義務付けることが適当である。

具体的には、管理規程において記載を求める、上記「3.3　リスク管理」のリスク項目の洗い出し等については、これら２つのリスクの洗い出し等を含めることとして、当該管理規程に基づき、コアネットワークの設備におけるこれら２つの

リスクへの対応を求めることが適当である[25]。

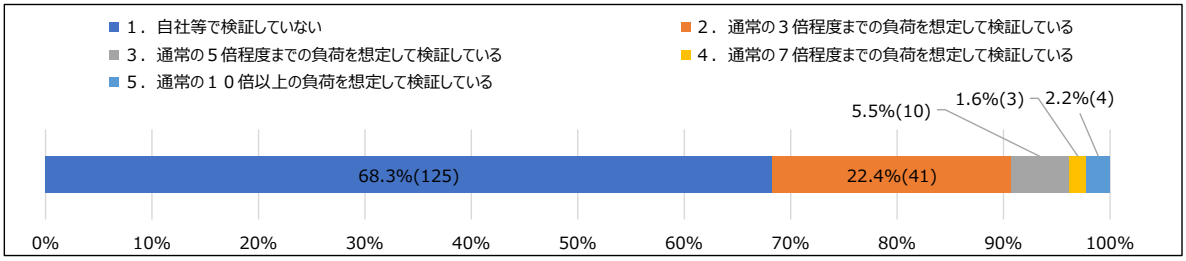
3.5 著しい高負荷時の動作検証

（１）課題・論点

著しい高負荷時の挙動検証の不足により事故が大規模化及び長時間化した事例がある。著しい高負荷時の挙動検証について、現時点では、義務化されておらず各社の対応は様々であるが、事故の未然防止の観点から、制度化に向けた検討が必要である。

（２）検討

電気通信事業者アンケート調査によると、図表 3-11 のとおり、「自社等で検証していない」が 68.3%、「通常の３倍程度までの負荷を想定して検証している」が 22.4%である。



図表 3-11 著しい高負荷時の挙動検証状況

著しい高負荷時の挙動検証の不足により事故が大規模化及び長時間化した事例として、加入者データベース等の設備に高負荷がかかり大規模化した事例が携帯電話事業者においてある。利用者に与える影響が大きな設備については、著しい高負荷時の挙動検証についても実施を求めていくことが必要である。

（３）対応の方向性

著しい高負荷時の挙動検証について、携帯電話用設備における加入者データベース及びコアネットワークの設備については、少なくとも諸元値以上の負荷をかけ、想定した動作を行うか検証を求めることが適当である[26]。

また、当該基準は、設備の基準になることから、技術基準（事業用電気通信設備規則）で実施を求めていくべきと考えられる。

---

[25] 電気通信事業法施行規則等において、事業者が定める管理規程に、上記「3.3　リスク管理」のリスク項目の洗い出し等については、これら２つのリスクの洗い出し等を含める旨の記載を求めることが考えられる。

[26] 具体的には、諸元値を超える負荷が印加された状態（高負荷）のとき、設備を保護する措置(Overload Protection)が動作するか等の挙動検証を求めることが考えられる。

3.6 データ蓄積型設備への定期監視

（１）課題・論点

ログファイル等、徐々にデータを蓄積して、最終的には領域を圧迫するおそれがある設備について、蓄積領域が枯渇等した場合、重大な事故に至る事例もあることから、データ蓄積型設備への定期監視についても制度的な検討が必要である。

（２）検討

通信設備がログデータを蓄積し続けた結果、メモリが枯渇し、自動的に再起動したことが原因で重大な事故に至った事案が過去に発生した。ログデータに限らず、データを蓄積する機能を有する設備については、最終的には領域を圧迫するおそれがあることから、定期的な点検が必要である。

他方、データを蓄積する機能を有する設備には多くの設備が該当し、定期的な点検には相応の人員が必要となることも踏まえ、小規模事業者へも一定の配慮が必要と考えられる。

（３）対応の方向性

電気通信回線設備の設置事業者等を対象として、「安信基準」において、データを蓄積する機能を有する設備に関し、定期な監視・点検を推奨することが適当である。

ただし、一定量まで蓄積された場合は、上書きされるしくみを取り入れているなど、領域が枯渇しないことを確認できた設備[27]については、当該定期的な監視・点検の対象外とすることが考えられる。

3.7 訓練

（１）課題・論点

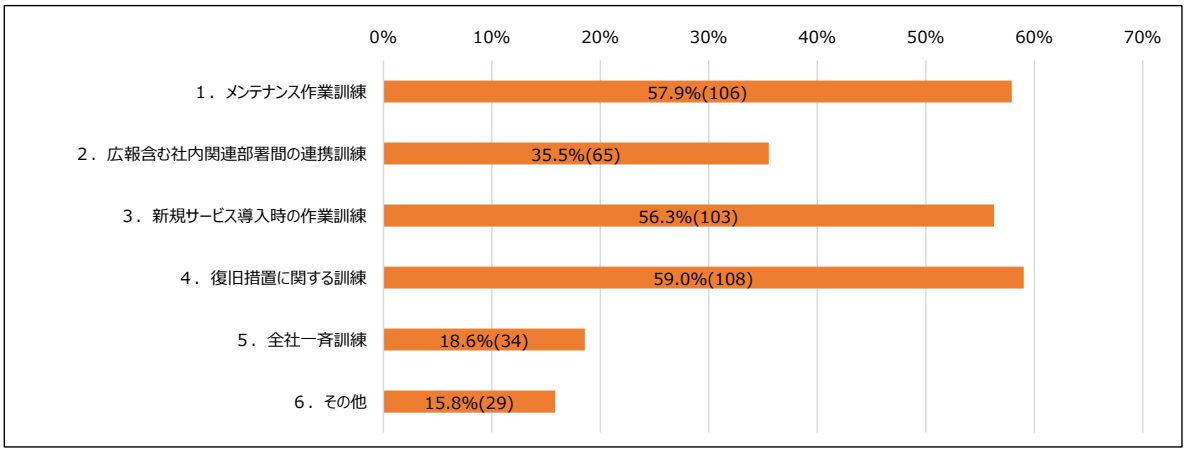
事故の長時間化や周知広報の遅れの背景には、訓練面での課題も少なからずあると考えられ、定期的な訓練は不可欠である。具体的な訓練について、制度化に向けた検討が必要である。

（２）検討

[27] ただし、ソフトウェアによる自動管理によって当該メモリ領域が枯渇しないようにする方法を取る場合には、当該ソフトウェアに潜在するバグによって、当該自動管理が適切に作動しないことがないか、定期的に監視・点検することも重要と考えられる。

現行制度では、電気通信事業法施行規則第 29 条第 1 項第 3 号ロで管理規程への記載を求めている事項として、「事業用電気通信設備の設計、工事、維持及び運用に従事する者に対する教育及び訓練等の実施に関すること。」が規定されており、訓練の実施については義務とされているが、具体的な訓練については求められていない。

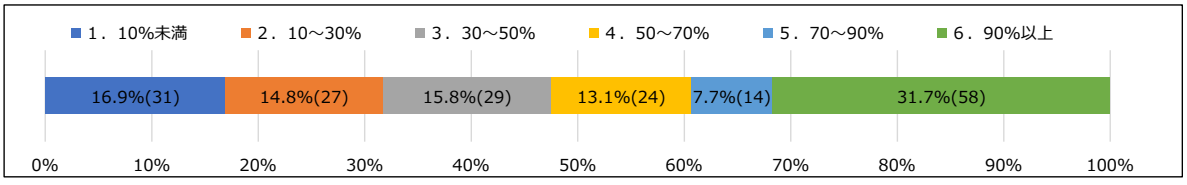
電気通信事業者アンケート調査によると、図表 3-12 のとおり、「メンテナンス作業訓練」が 57.9%、「広報含む社内関連部署間の連携訓練」が 35.5%、「新規サービス導入時の作業訓練」が 56.3%、「復旧措置に関する訓練」が 59.0%、「全社一斉訓練」が 18.6%となっている。



図表 3-12 安全管理関係の実施訓練内容

こうした訓練のうち、少なくとも、事故の発生・長時間化の防止に資する 「メンテナンス作業訓練」、「復旧措置に関する訓練」は実施を求めるべきと考えられる。また、近年、利用者に対する周知広報が遅れる事案が多く発生しており、利用者の利益を保護する観点から、広報部門との連携訓練等についても推奨が必要と考えられる。

さらに、電気通信事業者アンケート調査によると、図表 3-13 のとおり、保守運用人員における年間訓練実施者の割合については、31.7%が９割以上の保守運用人員に対して毎年訓練を実施しているとしている一方、訓練の対象者が１割未満の事業者も 16.9%存在する。出来る限り全ての保守運用員を対象にこうした訓練の実施を推奨していくべきと考えられる。



図表 3-13 保守運用人員における年間訓練実施者の割合

（３）対応の方向性

電気通信回線設備の設置事業者等に対して、事故の発生・長時間化の防止に資する 「メンテナンス作業訓練」、「復旧措置に関する訓練」については、管理規程に記載を求めることで、実施を求めていくことが適当である[28]。

また、「安信基準」により、① 「広報含む社内関連部署間の連携訓練」 、「全社一斉訓練」、シナリオ共有しない訓練等、効果的な訓練についても実施を推奨するとともに、②復旧措置の訓練等も含め、自社及び運営委託会社の「全ての保守運用員」を対象にこうした訓練の実施を推奨していくことが適当である。

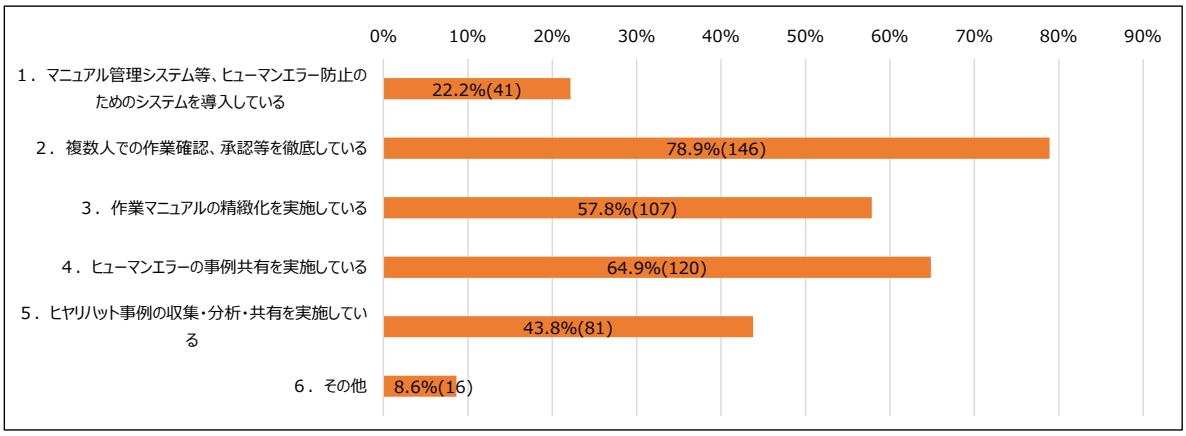
3.8 ヒューマンエラー防止対策

（１）課題・論点

ヒューマンエラーが原因で重大な事故に至るケースも少なくない。現行制度では、ヒューマンエラーの防止策が制度化されていないが、制度化に向けた検討が必要である。

（２）検討

電気通信事業者アンケート調査によると、図表 3-14 のとおり、「ヒューマンエラー防止のためのシステムを導入」が 22.2%、「複数人での作業確認、承認等を徹底」が 78.9%、「作業マニュアルの精緻化を実施」が 57.8%、「ヒューマンエラーの事例共有を実施」が 64.9%、「ヒヤリハット事例の収集・分析・共有を実施」が 43.8%となっている。



図表 3-14 ヒューマンエラーを防ぐための取組内容

ヒューマンエラーが原因で重大な事故に至る事案が少なくないことに鑑みる

[28] 具体的には、電気通信事業法施行規則等において、事業者が定める管理規程に、「メンテナンス作業訓練」、「復旧措置に関する訓練」の実施についての記載を求めることが考えられる。

と、ヒューマンエラーの防止策について、義務として対策を求めていくべきと考えられる。

（３）対応の方向性

電気通信回線設備を設置する事業者等に対して、ヒューマンエラーの防止策について管理規程の記載事項とすることで、対策を義務付けることが適当である[29]。

また、「安信基準」により、「システムの導入・手続きの自動化」、「複数人での作業実施」、「作業の多段階承認」、「ヒューマンエラーの事例共有」、「ヒヤリハット事例の収集・分析・共有」等の効果的な事例について推奨することが適当である。

3.9 利用者への周知広報

（１）課題・論点

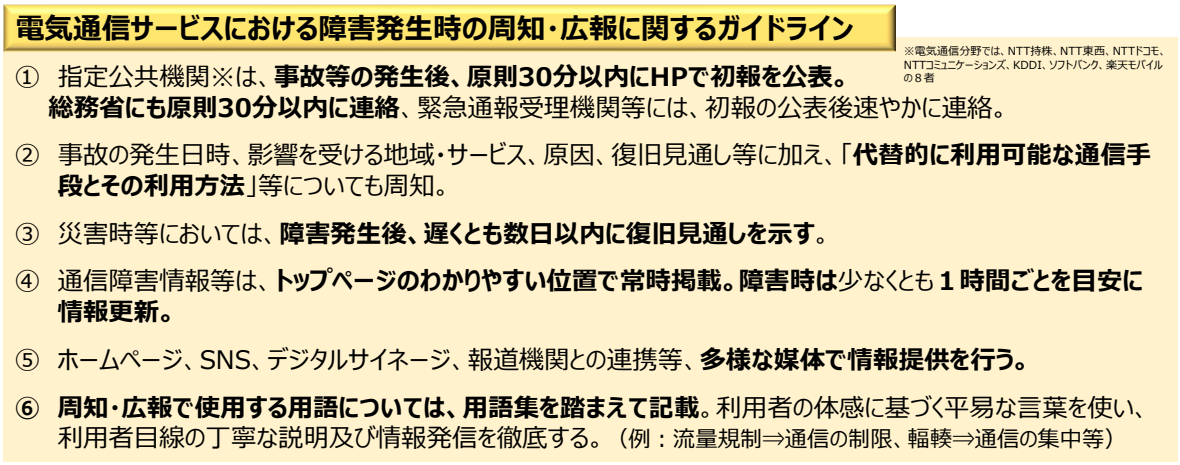
事故等の通信障害が発生した際、利用者への周知広報が迅速になされないものが多く、制度的な見直しが必要である。

（２）検討

電気通信分野における周知広報等の在り方について検討するため、昨年 10 月から「電気通信事故検証会議　周知広報・連絡体制 WG」が開催され、本年１月 27 日（金）に報告書が取りまとめられた。具体的には、指定公共機関は事故等の発生時から原則 30 分以内に初報の公表等が規定されている。

また、本取りまとめを踏まえ、総務省において、図表 3-15 のとおり、本年３月に、「電気通信サービスにおける障害発生時の周知・広報に関するガイドライン」の策定が行われた。

[29] 具体的には、電気通信事業法施行規則等において、事業者が定める管理規程に、ヒューマンエラーの防止策についての記載を求めることが考えられる。



図表 3-15 電気通信サービスの周知・広報に関するガイドライン概要

また、現在、電気通信事業法施行規則第 29 条第 1 項第 3 号ヲにおいて「利用者の利益の保護の観点から行う利用者に対する情報提供に関すること。」を管理規程に記載するよう求めているが、当該取りまとめを踏まえた制度の見直しについても検討が必要である。

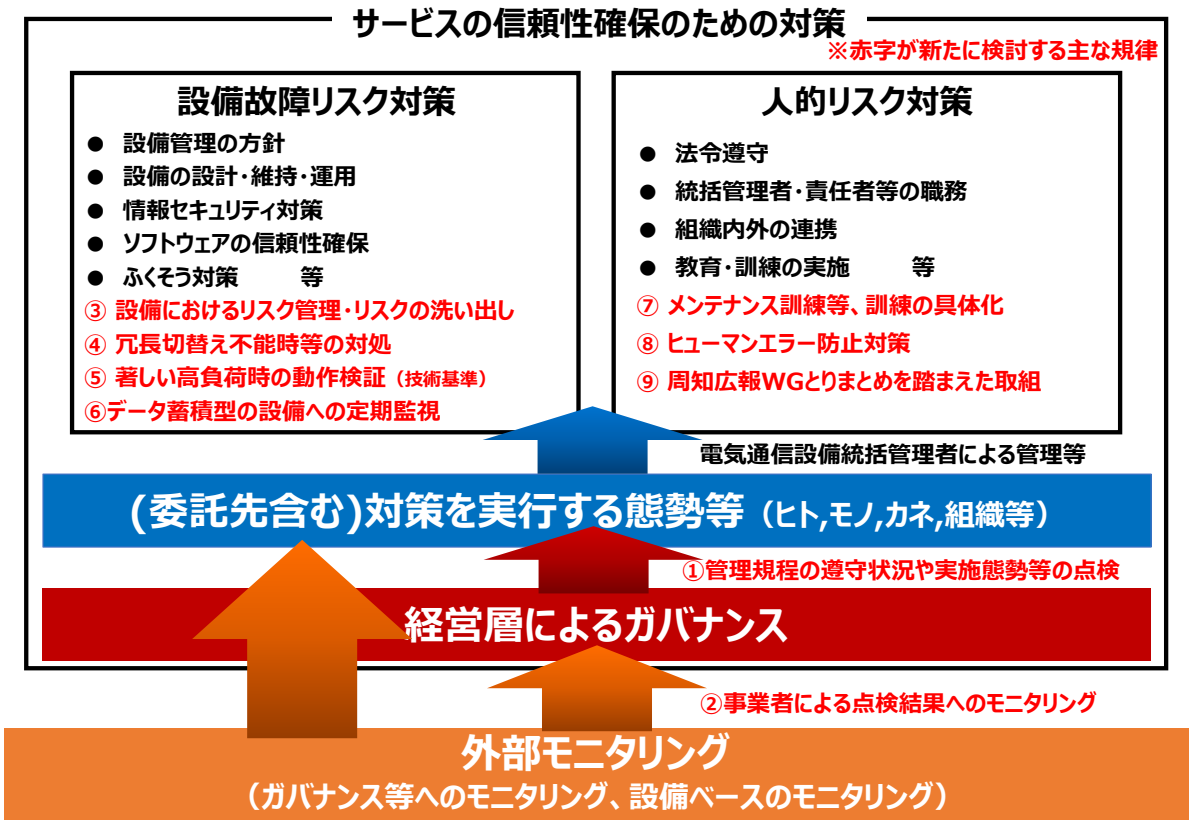
（３）対応の方向性

現在、電気通信事業法施行規則で管理規程への記載を求めている「利用者の利益の保護の観点から行う利用者に対する情報提供に関すること。」の詳細として、「電気通信サービスにおける障害発生時の周知・広報に関するガイドライン案」を踏まえた取組についても言及を求めることが適当である[30]。

3.10 構造的な問題を踏まえた対策の整理

上記「3.1 ガバナンスの強化」から「3.9 利用者への周知広報」で記載したとおり、①ガバナンスの強化、②外部モニタリング、③リスク管理、④予備系設備への切替え不能時の対処、⑤著しい高負荷時の動作検証、⑥データ蓄積型設備への定期監視、⑦訓練、⑧ヒューマンエラー防止対策、⑨利用者への周知広報、の９つの論点については、図表 3-16 のとおり取組を進めることが適当である。

[30] 具体的には、電気通信事業法施行規則等において、事業者が定める管理規程に、電気通信サービスにおける障害発生時の周知・広報に関するガイドライン案を踏まえた取組についての記載を求めることが考えられる。



図表 3-16 構造的な問題への対処のイメージ

４. 今後の対応及び検討課題

近年、社会全体のデジタル化の進展に伴って電気通信サービスは、自由な情報の発信、人と人とのコミュニケーションの手段や自由な情報発信に加え、物流や自動車、行政、金融など多岐にわたる分野を支える社会インフラとして、重要性が急速に増している。

近年、電気通信事業者による大規模な通信事故が連続して発生しているが、通信事故が多発する背景には、リスク評価やリスク項目の洗い出しの不足、ヒューマンエラー防止や訓練面での課題、ガバナンスの不足等、共通する課題も多いと考えられる状況を踏まえると、通信事故の背景にある構造的な問題の検証、また当該問題を踏まえた対策について検討し、利用者の利益の保護及び通信サービスの確実かつ安定的な提供を確保していくことは極めて重要である。

こうした考えに基づき、本報告書では、電気通信分野における通信事故の背景にある電気通信事業者に共通する構造的問題の検証とその対応策について検討を行った。

本報告書が示した方向性について、総務省において、事業者及びそこで働く技術者等の過度な負担にならないことにも配慮しつつ、実効性ある制度とするために、事業者との細部に関する調整を含めて必要な制度改正の検討を進め、利用者の利益の一層の保護や情報通信ネットワークの安全・信頼性の更なる向上に向けた環境を速やかに整備することが重要である。

また、電気通信サービスは非常に変化の激しいサービスであることから、通信分野の事故の状況、電気通信事業における競争環境、情報通信ネットワークの仮想化・クラウド化等を含む技術の進歩等、電気通信事業を取り巻く環境の変化等にも留意しながら、今後も、外部モニタリング制度や制度の対象者等を含め、制度の見直し等を不断に行っていくことが必要である。

（参考）電気通信事故検証会議

構成員一覧

（敬称略、順不同）

＜座長＞

相田　　仁　　東京大学大学院 工学系研究科 教授

＜構成員＞

阿部　俊二　　国立情報学研究所 アーキテクチャ科学研究系 教授

内田　真人　　早稲田大学 理工学術院 教授

加藤　玲子　　独立行政法人国民生活センター 相談情報部相談第２課長

黒坂　達也　　株式会社企 代表取締役

妙中　雄三　　奈良先端科学技術大学院大学 先端科学技術研究科
情報科学領域 准教授

中田　雅行　　EY ストラテジー・アンド・コンサルティング株式会社マネージャー

堀越　功　　株式会社日経ＢＰ 日経クロステック先端技術副編集長

森井　昌克　　神戸大学大学院工学研究科 教授

矢入　郁子　　上智大学 理工学部 情報工学科 准教授

＜オブザーバー＞

東日本電信電話株式会社

西日本電信電話株式会社

株式会社 NTT ドコモ

KDDI 株式会社

ソフトバンク株式会社

楽天モバイル株式会社

一般社団法人 電気通信事業者協会

一般社団法人 テレコムサービス協会

一般社団法人 日本インターネットプロバイダー協会

一般社団法人 日本ケーブルテレビ連盟