資料９－４

電気通信事故検証会議
（構造問題関係）
の検討事項等について

令和５年１月
事務局

１．通信事故の背景にある構造的な問題※について

※　業界共通的な組織・態勢面等の問題

【参考】 ヒアリング事項①

１．保守運用理念・基本方針

- ✓ 通信障害の防止に関して、御社の保守運用に関する理念・基本方針をご説明願います。簡潔なもので構いません。（その際、重大な事故に対する考え方等がございましたら併せてご説願いします。）

２．安全対策に関するガバナンス

- ✓ 管理規程には各事業者の安全対策の方針・体制・方法が規定されていますが、当該管理規程の遵守・実施状況等について、社内又は社外で定期的な監視・監査を実施しているかについてご説明願います。
- ✓ 併せて、内部又は外部監査（もしくは両方）の実施頻度、実施主体、監査項目、監査結果の活用方法等についてご説明願います。
- ✓ 管理規程の公表の可否についてもご説明願います。

３．新規設備に関するリスクの洗い出し体制・方法

- ✓ 新機器の商用稼働までにおけるプロセスにおいて、設備仕様、動作検証時等含め、リスクの洗い出しをどのように行い、設備の機能に反映させているか、代表的な設備について、障害パターン等のリスク評価項目、評価数、評価内容等を例示して、ご説明願います。
- ✓ これらについて、故障時の影響が大きい重要設備と位置付けているものとそれ以外のものでどのような違いがあるかもご説明願います。

４．商用稼働済設備の保守・管理態勢

- ✓ 商用稼働済設備に関して、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ご説明願います。
- ✓ リスク評価の一環として、ソフトウェアバグの精査方法・体制等についてもご説明願います。
- ✓ 併せて、想定外の事態が発生した場合、速やかに正常動作への復帰を可能とするための方法を、BCP（事業継続計画)等にどの程度定めているかご説明願います。

【参考】 ヒアリング事項②

５．平時からの事故対応に係る教育・訓練・人材育成

✓ ヒューマンエラーを防ぐための取組をご説明願います。

✓ 併せて、訓練の種類（メンテナンス訓練、社内関連部署間の連携訓練、新規サービス導入時の訓練、復旧措置における訓練、全社一斉訓練等）、実施頻度（●回/年）、対象者、（可能な範囲で）訓練実施者数（●人/年）、保守運用人員における年間訓練実施者の割合等をご説明願います。

６．その他の障害対応について

（１）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

✓ 設備等が完全に故障するのではなく、一部故障となり、想定した機能を十分発揮できないが、予備系に切り替わるほど故障しなかった場合、（潜在的リスクの洗い出しや影響評価は、どの程度、どのように実施しているか等のリスク評価の実施状況とリスク評価の実施状況と）速やかに正常動作への復帰を可能とするため実施している内容（復旧措置に加え当該措置を確実に実施するための取組含む）をご説明願います。

（２）複数の機能・システムの連携不全等による障害対応

✓ 故障が他の設備の故障に波及する等により、複数の機能とシステムの連携が不全となる場合、（潜在的リスクの洗い出しや影響評価は、どの程度、どのように実施しているか等のリスク評価の実施状況と）速やかに正常動作への復帰を可能とするため実施している内容（当該措置を確実に実施するための取組含む）をご説明願います。

（３）著しい高負荷時の挙動検証

✓ 著しい高負荷時に想定していた機能を発揮せずに大規模な障害が発生する場合がありますが、特に障害時の影響が大きい設備に関して、挙動の検証に関して、どの程度高負荷時を想定して検証しているかご説明願います。（PCRF等の加入者データベース、その他の代表的なコア設備で例示下さい。）

通信の信頼性確保に関するガバナンス・モニタリング

- ✓ 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**のではないか。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がほとんど存在しない**のではないか。
- ✓ 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**ではないか。

✓ 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について説明願います

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

設備に関するリスクの洗い出し体制・方法

- ✓ 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**ではないか。
- ✓ 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**のではないか。

✓ 設備仕様、動作検証時等含め、リスクの洗い出しをどのように行い、設備の機能に反映させているか。

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

商用稼働済設備の定期的な点検

✓ 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**のではないか。他方、現在、そうした対策を求める制度は特段ない。

✓ 商用稼働済設備に関して、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ご説明願います。

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

ヒューマンエラー防止策

- ✓ 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。**

✓ ヒューマンエラーを防ぐための取組をご説明願います。

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

平時からの事故対応に係る教育・訓練・人材育成

- ✓ 訓練についても、各社で一定の取組はなされている。他方、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。**
- ✓ 他方、**現行制度では、具体的な訓練は義務化されていない。**

✓ 併せて、訓練の種類、実施頻度（●回/年）、対象者、（可能な範囲で）訓練実施者数（●人/年）、保守運用人員における年間訓練実施者の割合等をご説明願います。

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

その他の障害対応（冗長設備への切替え不能）について

- ✓ **半故障等による冗長設備への切替え不能が原因で事故が発生することが非常に多い。**
- ✓ 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、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のではないか。

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

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

その他の障害対応（著しい高負荷時の挙動検証）について

- ✓ **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。**
- ✓ 他方、**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。**

著しい高負荷時の挙動検証	
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

利用者への周知広報・透明性確保について

- ✓ 最近、大規模な通信障害が連続して発生しているが、通信障害発生時において、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**のではないか。
- ✓ なお、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。

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

通信事故の背景にある構造的な問題

✓ 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のではないか。

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に機能していないのではないか

✓ 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等、委託先を含む**保守運用態勢に対するガバナンスの不足があるのではないか。** **【論点①】**

✓ **第三者による監査・モニタリングの不足があるのではないか。** **【論点②】**

2. 個別の論点として以下の課題がみられるのではないか。

① 設備におけるリスクの洗い出しが不十分 **【論点③】**

② 冗長が機能しない半故障時の対処が不十分 **【論点④】**

③ 著しい高負荷時の動作検証が不十分 **【論点⑤】**

④ データ蓄積型の設備への定期監視が不十分 **【論点⑥】**

⑤ 訓練が不十分（メンテナンス訓練等） **【論点⑦】**

⑥ ヒューマンエラーの防止策が不十分 **【論点⑧】**

⑦ 利用者への周知広報・透明性確保が不十分 **【論点⑨】**

⇒ **上記課題を踏まえた対策として、現行制度の見直しも含め、これら論点について、検討していくことが必要ではないか。**

（参考）電気通信事業法における設備規律について

電気通信事業者

（2022年11月30日現在）

登録 332者	届出 23,557者	
回線設置等 約450者	有料かつ大規模 回線非設置 4者	回線非設置 約2.3万者

設備基準

技術基準

●電気通信事業者の事業用電気通信設備の技術基準

予備機器、停電対策、耐震対策、防護措置、通話品質等を規定。

【法第41条・第42条等、事業用電気通信設備規則(省令)】

●利用者の端末設備等の接続の技術基準

安全性、電気的条件、責任の分界、セキュリティ対策等を規定。登録認定機関等が技術基準 適合認定等を実施。登録修理業者は修理された端末機器の技術基準適合性を確保義務。

【法第52条・第86条等、端末設備等規則(省令)、技術基準適合認定等に関する規則(省令)】

運用基準

管理規程

●事業用電気通信設備の管理に係る事業者毎の特性に応じた自主基準

設備管理の方針、法令遵守、責任者等の職務、組織内外の連携、設備の設計・維持・運用、情報セキュリティ対策、ソフトウェアの信頼性確保、ふくそう対策、利用者への情報提供等を定める義務。

【法第44条等、電気通信事業法施行規則(省令)】

監督責任

電気通信設備統括管理者

●経営レベルの事業用電気通信設備の統括管理

電気通信事業者が経営陣で実務経験のある者から選任、事故防止対策に主体的に関与。

【法第44条の3等、電気通信事業法施行規則(省令)】

電気通信主任技術者

●事業用電気通信設備の工事・維持・運用を監督

電気通信事業者が資格者を選任して事業用電気通信設備を監督。電気通信主任技術者に登録講習機関による講習を受けさせる義務。

【法第45条等、電気通信主任技術者規則(省令)】

工事担任者

●端末設備等の接続の工事を実施等

資格者が利用者の端末設備等の接続の工事を実施・実地監督。

【法第71条・第74条等、工事担任者規則(省令)】

なし
（自主的な取組のみ）

報告義務

事故報告

●通信の秘密の漏えい又は一定の基準を超える規模の電気通信事故が発生した場合に報告

【法第28条、電気通信事業用施行規則(省令)、電気通信事業報告規則(省令)】

（参考）電気通信事業法施行規則（管理規程）について

第二十九条　法第四十四条第二項の総務省令で定める管理規程の内容は、次のとおりとする。

一　電気通信役務の確実かつ安定的な提供を確保するための事業用電気通信設備の管理の**方針**に関する事項
　イ　組織の全体的かつ部門横断的な事業用電気通信設備の管理の方針に関すること。
　ロ　関係法令、管理規程その他の規定の遵守に関すること。
　ハ　通信需要、相互接続等を考慮した事業用電気通信設備の管理の方針に関すること。
　ニ　災害を考慮した事業用電気通信設備の管理の方針に関すること。
　ホ　情報セキュリティの確保のための方針に関すること。

二　電気通信役務の確実かつ安定的な提供を確保するための事業用電気通信設備の管理の**体制**に関する事項
　イ　経営の責任者の職務に関すること。
　ロ　電気通信設備統括管理者の職務に関すること。
　ハ　電気通信主任技術者の職務及び代行に関すること。
　ニ　各部門の責任者の職務に関すること。
　ホ　各従事者の職務に関すること。
　ヘ　組織内の連携体制の確保に関すること。
　ト　組織外の関係者との連携及び責任分担に関すること。

三　電気通信役務の確実かつ安定的な提供を確保するための事業用電気通信設備の管理の**方法**に関する事項
　イ　基本的な取組に関すること。
　ロ　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。
　ハ　事業用電気通信設備の設計、工事、維持及び運用に関すること。
　ニ　通信量の変動を踏まえた適切な設備容量の確保に関すること。
　ホ　情報セキュリティ対策に関すること。
　ヘ　ソフトウェアの信頼性の確保に関すること。
　ト　重要通信の確保及びふくそう対策に関すること。
　チ　緊急通報の確保に関すること。
　リ　防犯対策に関すること。
　ヌ　イからリまでに掲げる事項に関する取組の実施状況等現状の調査、分析及び改善に関すること。
　ル　ふくそう、事故、災害その他非常の場合の報告、記録、措置及び周知に関すること。
　ヲ　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。
　ワ　事故の再発防止のための対策に関すること。

四　**電気通信設備統括管理者の選任及び解任**に関する事項
五　当該**管理規程の見直し**に関すること。
六　その他事業用電気通信設備の設計、工事、維持及び運用に関し、電気通信役務の確実かつ安定的な提供の確保のために必要な事項

情報通信ネットワーク安全・信頼性基準（昭和62年2月14日郵政省告示第73号）

- 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。

1.設備等基準 … 情報通信ネットワークを構成する設備及び情報通信ネットワークを構成する設備を設置する環境の基準（65項目171対策）

第1. 設備基準 47項目121対策	1.一般基準（15項目67対策）	2.屋外設備（17項目22対策）	3.屋内設備（8項目13対策）	4.電源設備（7項目19対策）
第2. 環境基準 18項目50対策	1.センタの建築（4項目13対策）	2.通信機器室等（6項目22対策）	3.空気調和設備（8項目15対策）	

2.管理基準 … 情報通信ネットワークの設計、施工、維持及び運用の管理の基準（43項目178対策）

第1. 方針 9項目9対策	1.全体的・部門横断的な設備管理（3項目3対策）	2.関係法令等の遵守（1項目1対策）	3.設備の設計・管理（2項目2対策）	4.情報セキュリティ管理（3項目3対策）
第2. 体制 18項目46対策	1.情報通信ネットワークの管理体制（2項目8対策）	2.各段階における体制（16項目38対策）		
第.3 方法 16項目123対策	1.平常時の取組（13項目100対策）	2.事故発生時の取組（2項目17対策）	3.事故収束後の取組（1項目6対策）	

指針 … 管理基準に基づく指針　**情報セキュリティポリシー策定のための指針**　**危機管理計画策定のための指針**

解説 … 全ての対策項目に関する措置例等について参考として解説

２．構造的な問題を踏まえた対策について

論点①　ガバナンスの強化

検討事項①

- 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、**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はないか。**

検討の視点

- 他分野では、**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。ガス分野でも定期自主検査等が義務付けられている。**銀行分野でも、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。
- 今回、電気通信回線設備を設置する事業者等を対象にアンケート調査を実施した。当該調査によると、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**外**点検・監査のみを実施」が2.7%、「定期的に社内及び社外点検・監査をともに実施」が約19.7%、「定期的な点検・監査を実施していない」が12%であり、**約85%は定期的な内部点検・監査を実施**している。

ご議論頂きたい事項

- **電気通信事業者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はないか。**
- また、次項論点②のとおり、**当該結果に対する外部点検も必要**ではないか。

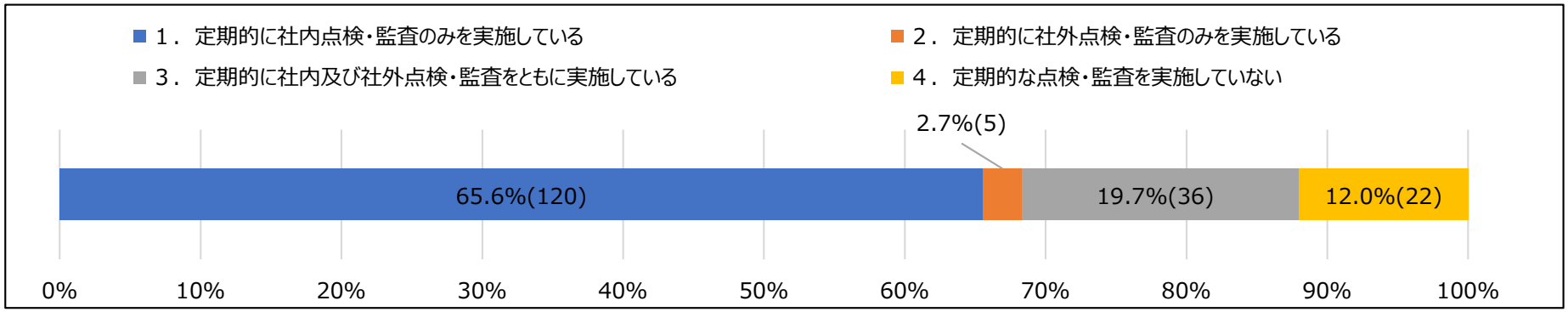
（参考）他分野における自主点検に係る制度の概要

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（月に一回以上等）に実施。

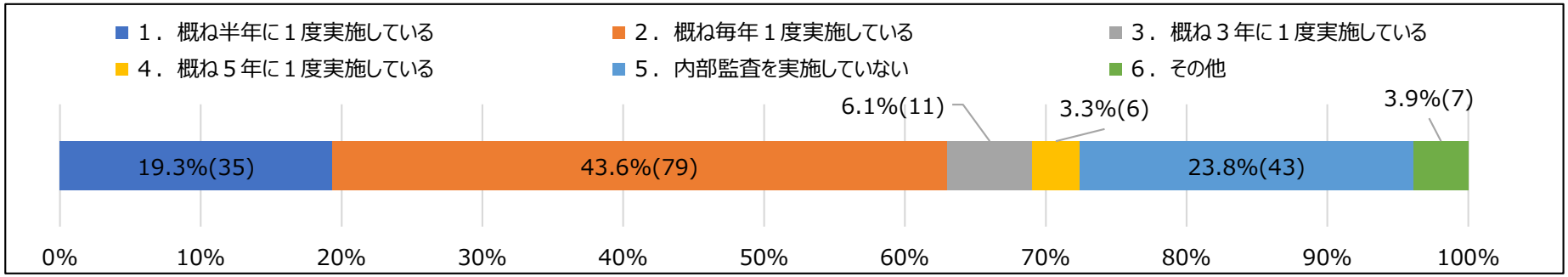
※EYストラテジー・アンド・コンサルティング株式会社提出資料（令和５年１月１３日・電気通信事故検証会議）を基に作成。

（参考）ガバナンスの取組状況に関する事業者調査の結果

■ 管理規程の定期的な点検・監査等実施状況（単一選択式、回答事業者数183、無回答4）



■ 安全管理に対する内部監査の実施状況（単一選択式、回答事業者数181、無回答6）



【（参考）事業者調査の概要】

- ✓ 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 電気通信技術システム課 安全・信頼性対策室

論点②　外部モニタリング

検討事項②

- 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はないか。

検討の視点

- 電気通信回線設備を設置する事業者等に対するアンケート調査によると、安全管理に対する**外部監査の実施状況について、「実施していない」が約68%**である。
- 他分野では、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。
  - 電力分野では、**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。
  - 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」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。
- 海外でも、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。
  - 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。
- なお、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。

論点②　外部モニタリング

ご議論頂きたい事項

- **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、論点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を行うような取組（ガバナンスのモニタリング）が必要**ではないか。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のではないか。
- **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有意義ではないか。**
- 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、(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があることも踏まえ、)**リスクの洗い出し項目についても行政等がモニタリング（設備ベースのモニタリング)を行い、不足するリスク認識についてフィードバックを行う取組も有意義ではないか。**
- 当該**２つのモニタリング（ガバナンスのモニタリング、設備ベースのモニタリング）は**、対象を限定し、例えば、**当面は、指定公共機関**（電気通信分野では、NTT持株、NTT東西、NTTドコモ、NTTコミュニケーションズ、KDDI、ソフトバンク、楽天モバイルの８者）**に対象を限定**することが考えられるか。ただし、**対象となる者については、事業者による事故の状況や電気通信事業を取り巻く環境の変化等も踏まえ、不断の見直しが必要**ではないか。
- また、電気通信分野は非常に変化が激しい分野であることに鑑み、環境の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のように、**政府が点検を行う基本方針等を策定し実施していくことが考えられるのではないか。**

（参考）他分野のモニタリング制度の概要

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。

※EYストラテジー・アンド・コンサルティング株式会社提出資料（令和５年１月１３日・電気通信事故検証会議）を基に作成。

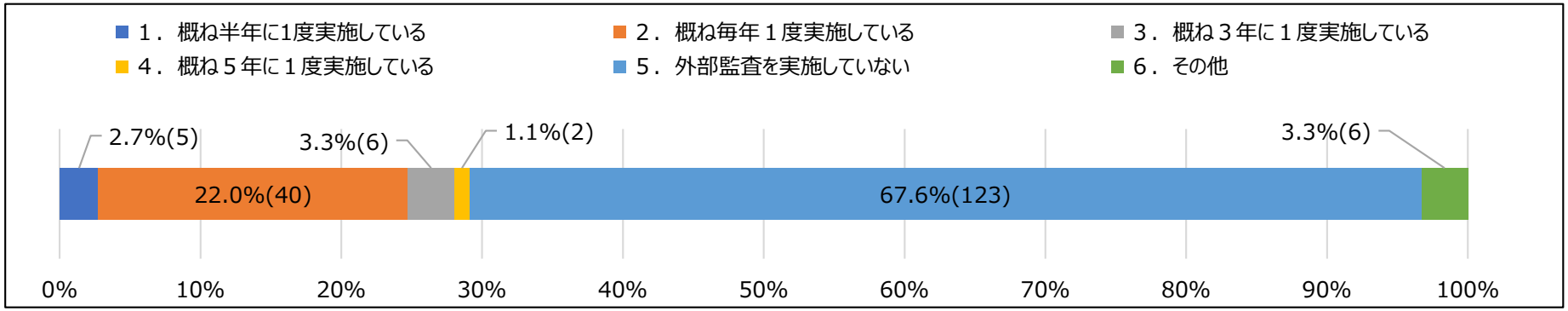
（参考）海外の通信分野のモニタリング制度の概要

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。

※株式会社野村総合研究所提出資料（令和５年１月１３日・電気通信事故検証会議）を基に作成。

（参考）外部モニタリングに係る事業者調査の結果等

■ 安全管理に関する外部監査の実施状況（単一選択式、回答事業者数182、無回答5）



（参考）設備ベースのリスクの洗い出しの事例

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）

設備
設備

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）

論点③　リスク管理

検討事項③

- 設備に対するリスク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のではないか。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はないか。

検討の視点

- 電気通信回線設備を設置する事業者等に対するアンケート調査によると、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**、(全て実施を合わせて)**約85%がリスクの洗い出しを実施**しているが、未実施の事業者も約15%存在。
- また、洗い出された全てのリスクについて、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。**他方、リスクの洗い出しをしても対応措置が定まっていなければ事故の未然防止につながらないのではないか**。また影響評価の実施も推奨が必要ではないか。

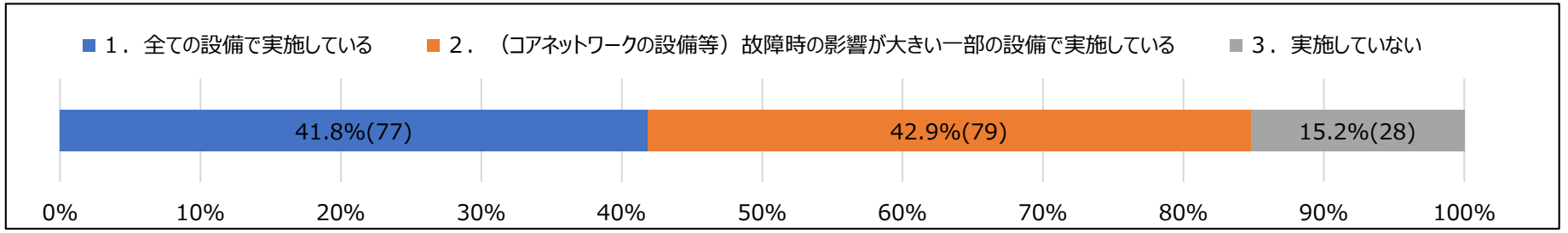
ご議論頂きたい事項

※事業者が想定可能なリスクが対象、想定できないリスクは除く

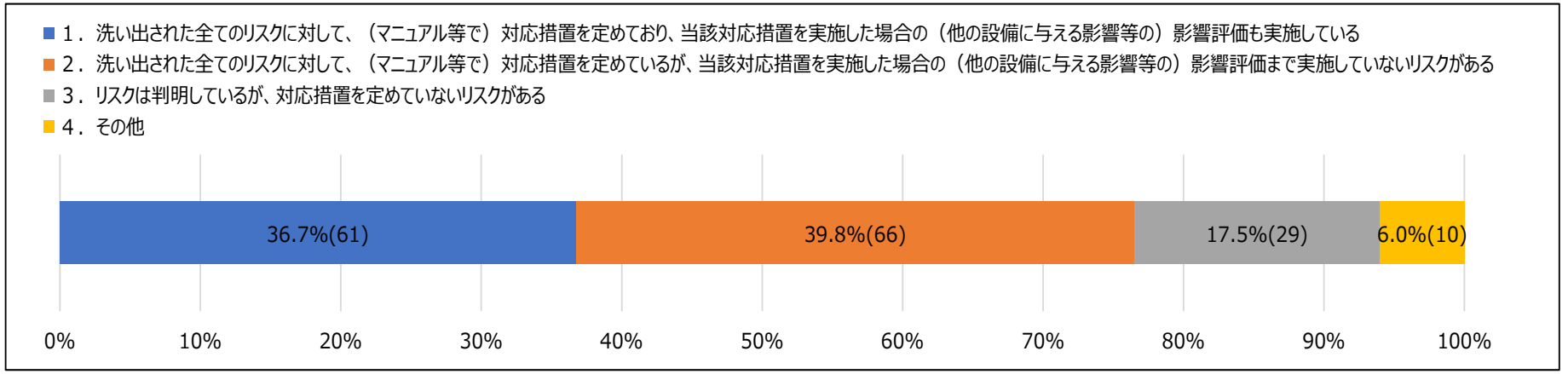
- 電気通信回線設備を設置する事業者等に対して、少なくとも利用者に与える影響が大きい**コアネットワークの設備については、①リスク項目の洗い出し、②洗い出された各リスクに対する対応措置・復旧手順の整備、③当該手順実施時のサービスへの影響評価（想定復旧時間含む）を義務化する**※ことが適当ではないか。またこれを踏まえた**事業継続計画（BCP）についても策定を義務化する**べきではないか。
- 併せて、「安信基準」で、①**コアネットワーク以外の設備に対するリスク項目の洗い出し等**、②洗い出された**リスク項目に対する復旧手順の訓練について**(利用者への影響が出ない範囲で)**推奨することが適当か。**
- また前述のとおり、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の第三者が設備ベースでモニタリングを行い、不足するリスク認識についてフィードバックをしていく取組も有意義**ではないか。

（参考）リスクの精査・洗い出しに関する事業者調査の結果

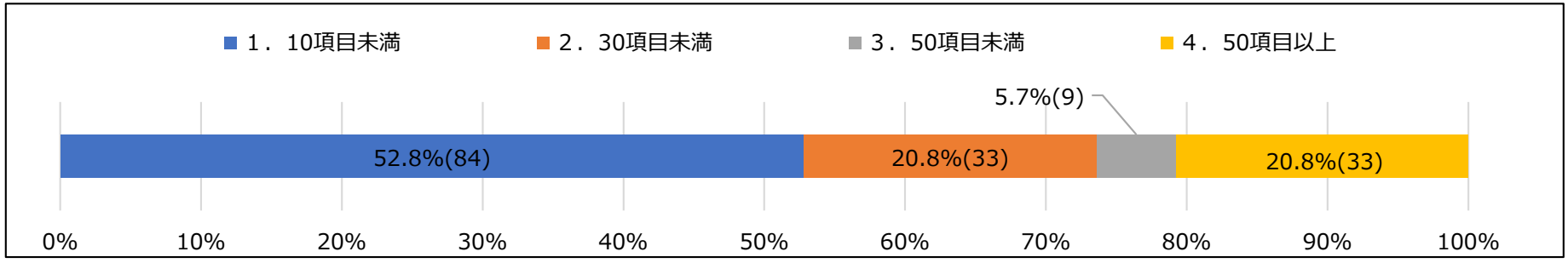
■ 商用稼働までの設備ごとのリスク洗い出し実施状況（単一選択式、回答事業者数184、無回答3）



■ リスクへの対応状況（単一選択式、回答事業者数166、無回答21）



■ 故障時の影響が大きい代表的な設備に係る障害パターン等のリスク評価項目数
（単一選択式、回答事業者数159、無回答28）



論点④　冗長設備への切替え不能時の対処

検討事項④

- 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、**冗長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はないか。

検討の視点

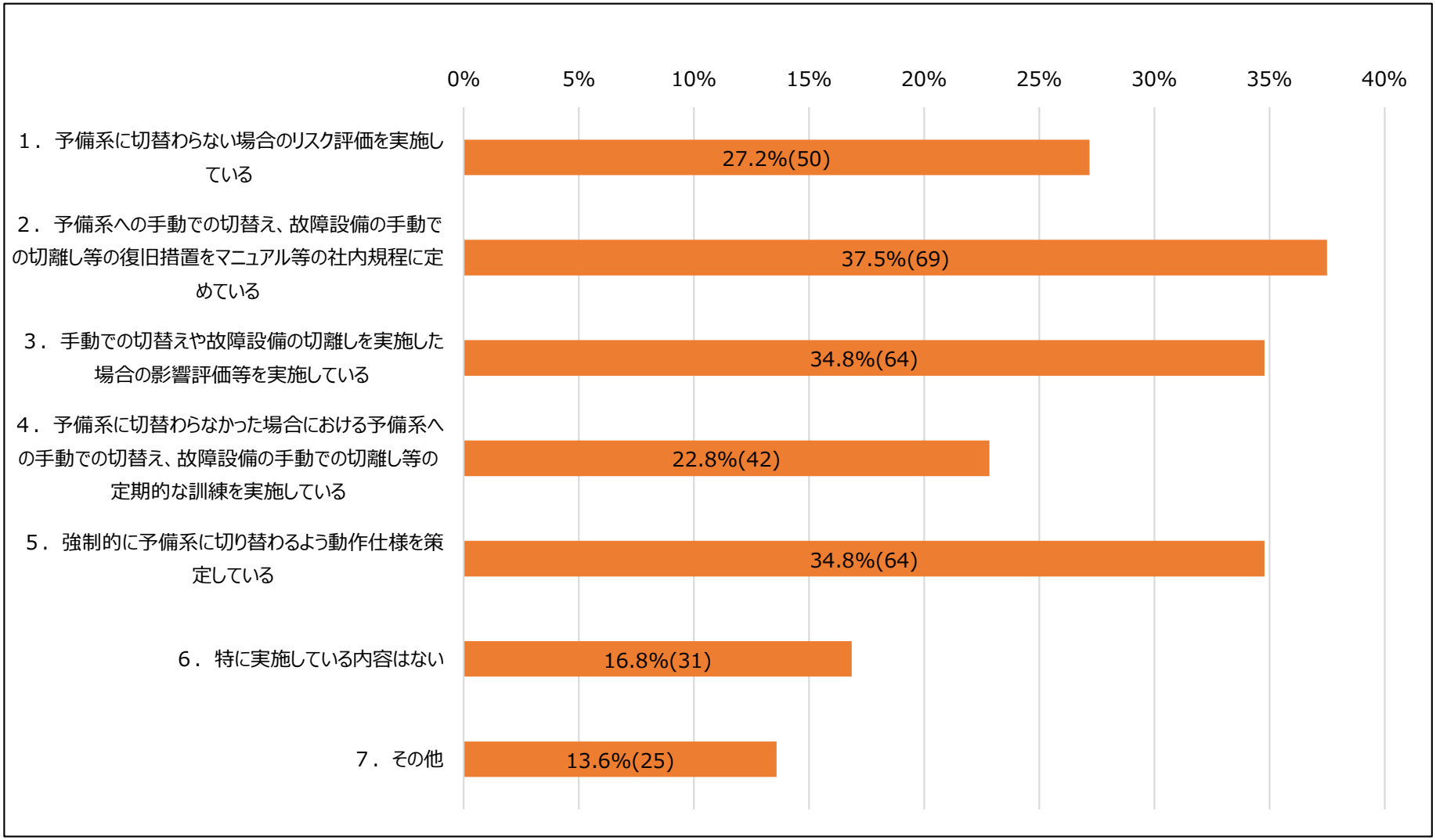
- 電気通信回線設備を設置する事業者等に対するアンケート調査によると、「予備系に切替わらない場合のリスク評価を実施している」が27.2%、「復旧措置をマニュアル等の社内規定に定めている」が37.5%、「手動での切替えや故障設備の切離しを実施した場合の影響評価等を実施している」が34.8%、「定期的な訓練を実施」が22.8%、「強制的に予備系に切り替わるよう動作仕様を策定」が34.8%、**「特に実施している内容はない」が16.8%**である。
- 冗長設備への切替え不能を原因として重大な事故に至るケースが非常に多いことに鑑みると、少なくともコアネットワークの設備に関しては、十分な対策が必要ではないか。
- 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**ではないか。

ご議論頂きたい事項

- 論点③のリスクの洗い出し等の義務の中で、**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、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**ことが適当ではないか。
- 具体的には、**管理規程で、論点③のリスク項目の洗い出し等の義務には、これら２つのリスクを含む旨、記載を求める**ことが考えられるのではないか。また、論点①で記載のとおり、当該2つのリスクの影響評価を含む管理規程の遵守状況の点検、それを踏まえて現行のヒト,モノ,カネ,組織等の態勢が十分か等について、費用と効果のバランス等も考慮の上で、事業者自身で毎年点検を行うことが考えられるのではないか。

（参考）冗長設備への切替え不能時対応に関する事業者調査の結果

■ 半故障等による冗長設備への切替え不能時の対応状況（複数選択式、回答事業者数184、無回答3）



論点⑤　著しい高負荷時の動作検証

検討事項⑤

- 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はないか。**

検討の視点

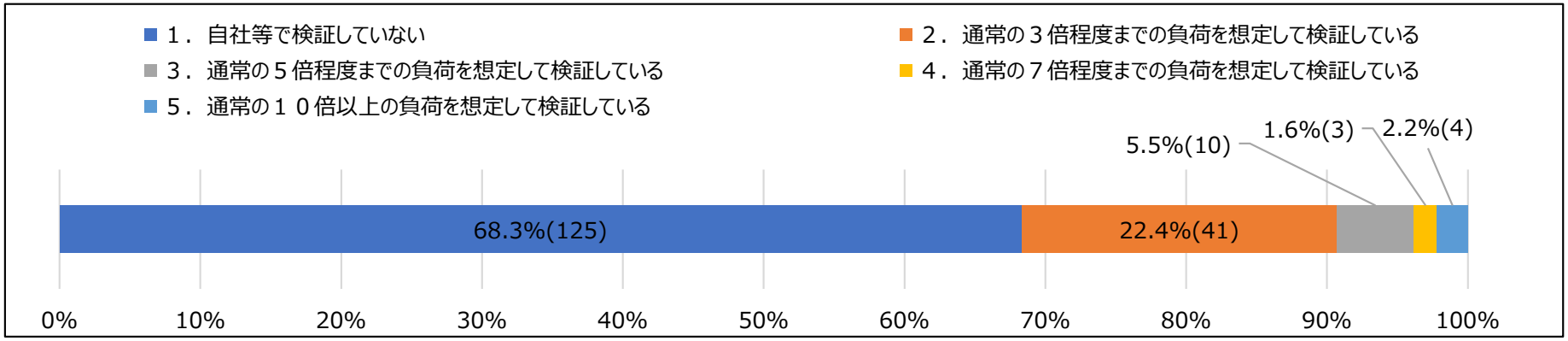
- 電気通信回線設備を設置する事業者等に対するアンケート調査によると、「自社等で検証していない」が68.3%、「通常の３倍程度までの負荷を想定して検証している」が22.4%である。
- 著しい高負荷時の挙動検証の不足により事故が大規模化及び長時間化した事例として、**加入者データベース等の設備に高負荷がかかり大規模化した事例が携帯電話事業者においてある。**利用者に与える影響が大きな設備については、**著しい高負荷時の挙動検証についても実施を求めていくことが必要ではないか。**

ご議論頂きたい事項

- 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**ではないか。
- 当該基準は、設備の基準になることから、技術基準で求めていくべきではないか。

（参考）著しい高負荷時の動作検証に関する事業者調査の結果

■ 著しい高負荷時の挙動検証状況（単一選択式、回答事業者数183、無回答4）



論点⑥　データ蓄積型設備への定期監視

検討事項⑥

- 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はないか。

検討の視点

- 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が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はないか。
- 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ではないか。

ご議論頂きたい事項

- 電気通信回線設備の設置事業者等に対して、「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**することが適当ではないか。
- 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については、当該定期的な監視・点検の対象から除くことが考えられるのではないか。

論点⑦　訓練

検討事項⑦

- 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。具体的な訓練について、制度化に向けた検討が必要ではないか。

検討の視点

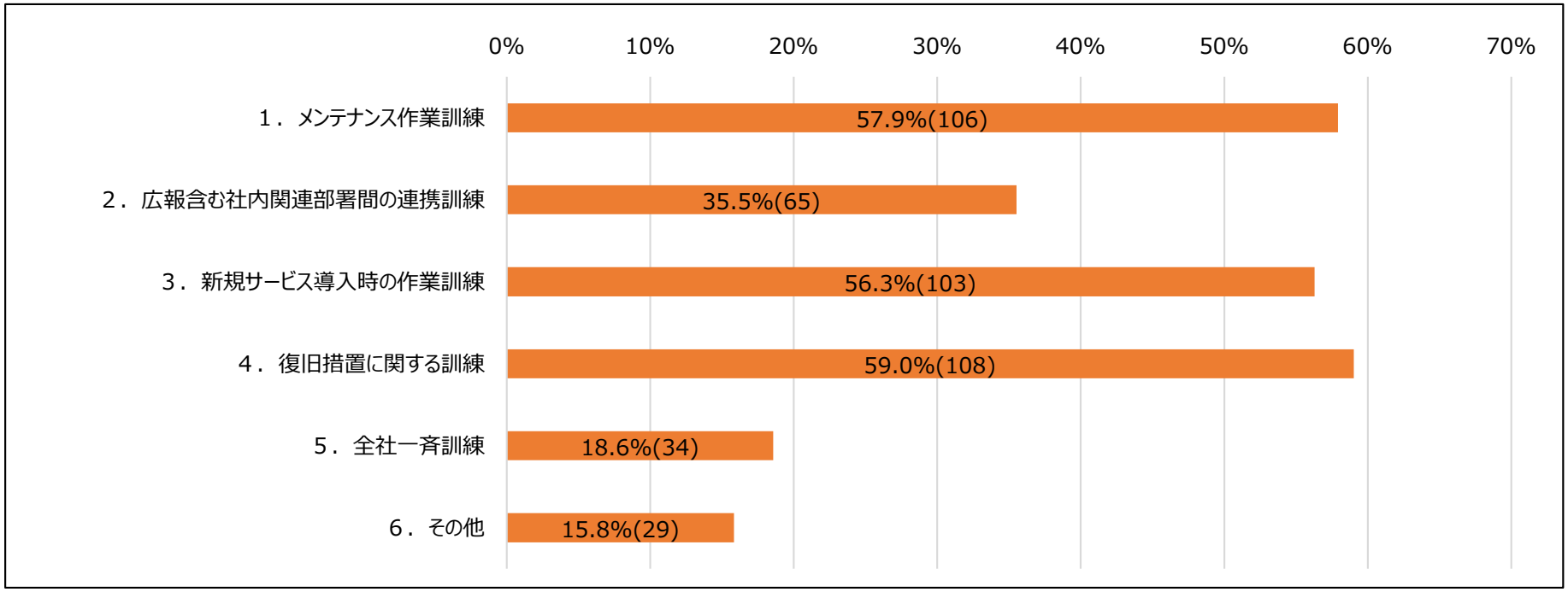
- 現行制度では、電気通信事業法施行規則第29条第１項第3号ロで管理規程への記載を求めている事項として、「事業用電気通信設備の設計、工事、維持及び運用に従事する者に対する教育及び訓練等の実施に関すること。」が規定されているが、**訓練の詳細については求めていない。**
- 電気通信回線設備を設置する事業者等に対するアンケート調査によると、「メンテナンス作業訓練」が57.9%、「広報含む社内関連部署間の連携訓練」が35.5%、「新規サービス導入時の作業訓練」が56.3%、「復旧措置に関する訓練」が59.0%、「全社一斉訓練」が18.6%となっている。
- 少なくとも、事故の発生・長時間化の防止に資する「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ではないか。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ではないか。
- また、自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べきではないか。

ご議論頂きたい事項

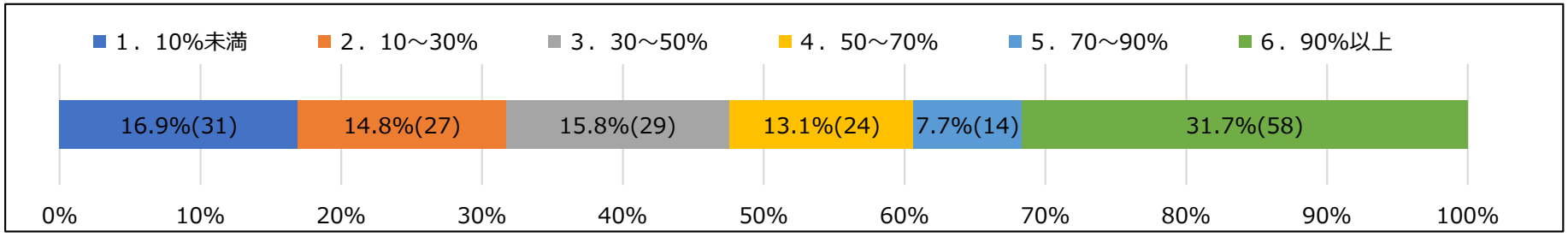
- 電気通信回線設備の設置事業者等に対して、事故の発生・長時間化の防止に資する**「メンテナンス作業訓練」、「復旧措置に関する訓練」については、管理規程を通じて、実施を求めていく**べきではないか。
- また、「安信基準」により、①**「広報含む社内関連部署間の連携訓練」、「全社一斉訓練」、シナリオ共有しない訓練等、効果的な訓練についても実施を推奨**するとともに、②復旧措置の訓練等も含め、**自社及び運営委託会社の「全ての保守運用員」を対象にこうした訓練の実施を推奨**していくべきではないか。

（参考）訓練に関する事業者調査の結果

■ 安全管理関係の実施訓練内容（複数選択式、回答事業者数183、無回答4）



■ 保守運用人員における年間訓練実施者の割合（複数選択式、回答事業者数183、無回答4）



論点⑧　ヒューマンエラー防止対策

検討事項⑧

- 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はないか。

検討の視点

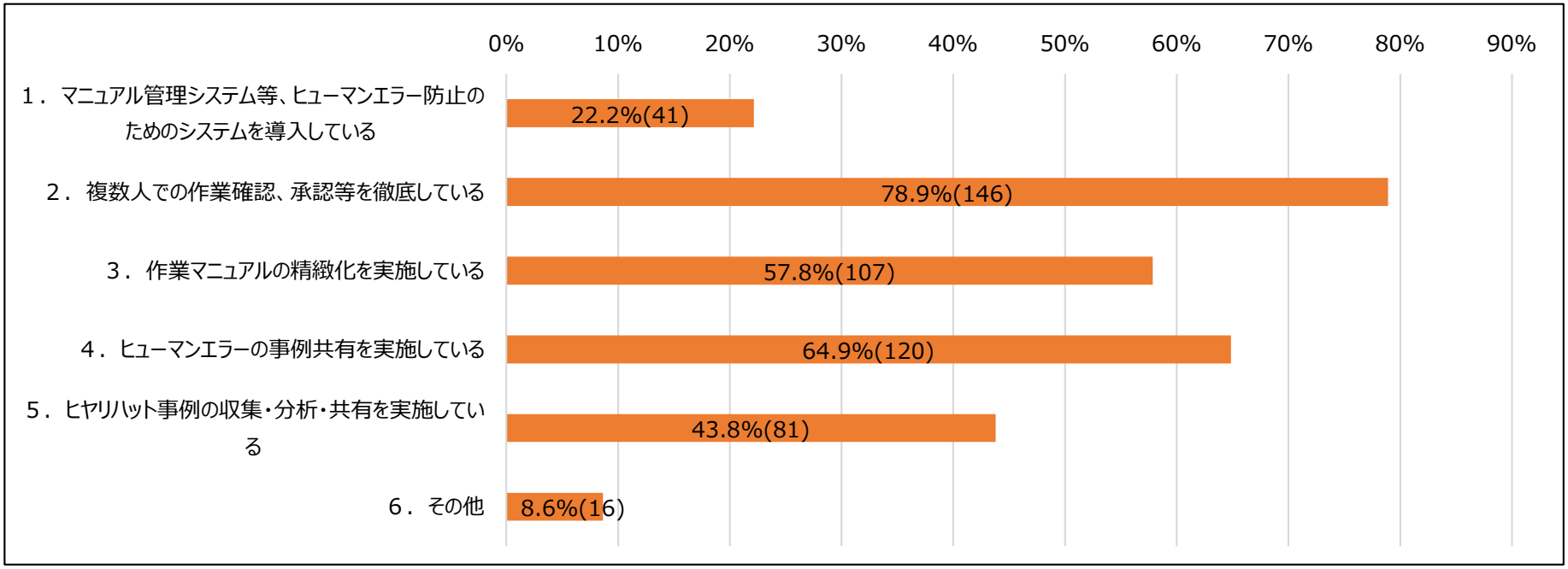
- 電気通信回線設備を設置する事業者等に対するアンケート調査によると、「ヒューマンエラー防止のためのシステムを導入」が22.2%、「複数人での作業確認、承認等を徹底」が78.9%、「作業マニュアルの精緻化を実施」が57.8%、「ヒューマンエラーの事例共有を実施」が64.9%、「ヒヤリハット事例の収集・分析・共有を実施」が43.8%となっている。
- ヒューマンエラーが原因で重大な事故に至る事案が少なくないことに鑑みると、ヒューマンエラーの防止策について、具体的な対策を含め、対策を求めていくべきではないか。

ご議論頂きたい事項

- 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、（管理規程において）対策を義務付ける**べきではないか。
- 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**するべきではないか。

（参考）訓練に関する事業者調査の結果

■ ヒューマンエラーを防ぐための取組内容（複数選択式、回答事業者数185、無回答2）



論点⑨　利用者への周知広報

検討事項⑨

- 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はないか。

検討の視点

- 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、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。今後は、総務省において、本取りまとめを踏まえ、年度内を目途にガイドラインの策定が行われる予定。
- 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はないか。

ご議論頂きたい事項

- 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、**「電気通信事故検証会議　周知広報・連絡体制WG」の取りまとめを踏まえた取組についても言及を求める**ことが適当ではないか。

（参考）周知広報・連絡体制WG　取りまとめの概要

✓近年、社会のデジタル化が進展しており、通信障害が社会全体に与える影響も増大。このため、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」を開催**しており、**1月27日（金）に報告書が取りまとめられた。**

✓今後は、**総務省において、本取りまとめを踏まえ、年度内を目途にガイドラインの策定を行っていく予定。**

電気通信事故検証会議　周知広報・連絡体制WG　取りまとめ案のポイント

※電気通信分野では、NTT持株、NTT東西、NTTドコモ、NTTコミュニケーションズ、KDDI、ソフトバンク、楽天モバイルの８者

① **電気通信事業者を広く対象。「指定公共機関※」には、一部高い内容を求める。**

② 対象とする事案は、**軽微な事故及び障害を除き、役務の提供に影響が生じた事故及び障害（自然災害含む）**

③ 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**。指定公共機関以外もこれに準じて対応。

④ 利用者へ周知すべき内容は、**事故の発生日時、影響を受ける地域・サービス、影響の具体的内容、原因、復旧見通し等に加え**、「**代替的に利用可能な通信手段とその利用方法**」等についても周知。

⑤ 通信障害情報等は、**平時よりトップページのわかりやすい位置及び大きさで常時掲載。**事故時は、深夜早朝を除き、少なくとも**１時間ごとに更新**、災害時においては、地図を通じたエリア障害情報を含め概ね１日３回以上更新。

⑥ 障害発生時には、初報も含め**報道発表資料等で問い合わせ先を掲載。**

⑦ 情報伝達手段として、自社ホームページ、SNS等に加え、例えば、販売代理店におけるデジタルサイネージの活用、報道機関への情報提供、放送事業者による字幕表示等を通じた周知を可能とするための放送事業者へ情報提供（Lアラートへの登録発信含む ） 等が考えられる。

⑧ 指定公共機関は、**総務省に対しては原則30分以内に連絡、緊急通報受理機関、MVNO/FVNO、他の指定公共機関に対しては、初報の公表後速やかに連絡。**指定公共機関以外もこれに準じて対応。

（参考）構造的な問題への対処のイメージ(案)

サービスの信頼性確保のための対策

※赤字が新たに検討する主な規律

設備故障リスク対策

- 設備管理の方針
- 設備の設計・維持・運用
- 情報セキュリティ対策
- ソフトウェアの信頼性確保
- ふくそう対策　　等

③ 設備におけるリスク管理・リスクの洗い出し
④ 冗長切替え不能時等の対処
⑤ 著しい高負荷時の動作検証（技術基準）
⑥データ蓄積型の設備への定期監視

人的リスク対策

- 法令遵守
- 統括管理者・責任者等の職務
- 組織内外の連携
- 教育・訓練の実施　　等

⑦ メンテナンス訓練等、訓練の具体化
⑧ ヒューマンエラー防止対策
⑨ 周知広報WGとりまとめを踏まえた取組

電気通信設備統括管理者による管理等

(委託先含む)対策を実行する態勢等（ヒト,モノ,カネ,組織等）

①管理規程の実施に係る保守運用態勢等の点検

経営層によるガバナンス

②事業者による点検結果へのモニタリング

外部モニタリング

（ガバナンス等へのモニタリング、設備ベースのモニタリング）