

「電気通信役務の安全・信頼性の確保に係るモニタリングの年次計画(令和7年度)(案)」に対する意見募集の結果及び回答
[募集期間:令和7年6月17日(火)～令和7年7月16日(水)]
意見提出者:計1件(法人0件、個人1件)

(意見提出者一覧)

個人(1件)

番号	意見提出者	提出意見	考え方	提出意見を踏まえた案の修正の有無
「電気通信役務の安全・信頼性の確保に係るモニタリングの年次計画(令和7年度)(案)」 全体				
1	個人①	<p>本計画において、令和7年度のモニタリング対象事業者が具体的に明記され、ガバナンスと電気通信設備の両面から多角的な確認を行う点が明確に示されていることを評価いたします。特に、過去の行政指導を踏まえた再発防止策の実施状況の確認や、仮想化技術、訓練状況、事故・ヒヤリハット事例の活用体制といった直近の環境変化を踏まえた重点確認項目が設けられていることは、実効性の高いモニタリングに繋がるものと期待されます。</p> <p>しかしながら、国民の電気通信役務に対する信頼を一層強固なものとするため、以下の視点についても、今後の計画策定やモニタリング実施においてご検討いただきたく、具体的に提案させていただきます。</p> <p>1. サプライチェーンリスク管理の強化と透明性の向上 本計画では、管理規程の実施状況及び遵守状況の点検において「委託先の状況を含む」とされていますが、電気通信サービスの提供においては、ハードウェア・ソフトウェアの供給、保守、運用等、多岐にわたるサプライヤーが関与しています。国際的なサプライチェーンの複雑化と地政学的リスクの増大を踏まえ、以下の点を重点的に確認し、その結果の透明化を図ることを提案します。</p> <ul style="list-style-type: none"> ・サプライヤー選定基準の厳格化と監査体制の確立: 主要なサプライヤーにおけるセキュリティ対策、品質管理体制、及び事業継続計画(BCP)の実効性について、事業者による評価・監査が適切に行われているか、より詳細な確認が必要です。特に、海外ベンダーからの調達における潜在的なリスク(国家主導のサイバー攻撃、情報窃取のリスク等)に対する具体的な対策を、各事業者がどのように講じているかをモニタリング項目に加えるべきです。 ・サプライチェーン全体の可視化とリスクアセスメント: 事業者が自身のサプライチェーン全体をどこまで可視化し、各層におけるリスクを定期的にアセスメントしているかを確認し、サプライチェーンの脆弱性マップを作成するなどの取り組みを促すことを提案します。 ・リスク情報の共有: 予期せぬサプライチェーン上の問題が発生した場合に、事業者間や政府と事業者間でリスク情報を速やかに共有する仕組みの有効性を確認し、必要に応じて改善を促すべきです。 <p>2. 組織文化とレジリエンス(回復力)の評価 事故の発生防止や早期復旧には、技術的な対策に加え、組織全体の意識や対応能力が不可欠です。ガバナンス確認において、以下の視点も追加し、事業者の組織的側面からのレジリエンス強化を促すことを提案します。</p> <p>安全文化の醸成と内部通報制度の有効性: <ul style="list-style-type: none"> ・従業員が事故やヒヤリハット事例をためらいなく報告できるような、風通しの良い安全文化が醸成されているか、そのための具体的な取り組み(例: 報奨制度、匿名での報告経路の確保)を確認すべきです。 ・内部通報制度が単に設置されているだけでなく、実際に機能し、通報内容が適切に経営層にまで届き、改善に繋がっているか、その実効性を評価する仕組みをモニタリング項目に加えることを提案します。 <p>危機管理体制と意思決定プロセスの実効性: <ul style="list-style-type: none"> ・大規模な障害発生時における経営層の迅速かつ適切な意思決定プロセス、特に情報収集、状況判断、指示系統の明確性について、定期的な検証や訓練(シナリオを共有しない訓練を含む)を通じて、その実効性を評価すべきです。 ・多様な専門性を持つ関係者(技術、広報、法務等)が連携し、的確な対応を取るためのクロスファンクショナルなチーム体制やコミュニケーション戦略についても確認を強化することを提案します。 <p>3. 技術革新への先行投資とリスク対応 本計画では仮想化技術に関連する取組状況を重点確認項目としていますが、電気通信分野における技術革新は日進月歩であり、AI、量子技術、5G/Beyond 5Gといった新たな技術の導入がサービス提供のあり方を大きく変えつつあります。これらの新技術がもたらす新たなリスクに対し、事業者がどのように対応しようとしているか、その先行的な取り組みもガバナンスの一部として評価することを提案します。</p> <ul style="list-style-type: none"> ・新技術導入に伴うリスクアセスメントの実施状況: 事業者が新たな技術を導入する際に、事前にその潜在的なリスク(セキュリティ脆弱性、予期せぬ障害発生の可能性、運用上の複雑性等)を評価し、適切な対策を講じているかを確認すべきです。 ・研究開発(R&D)への投資と技術者育成: 新たな脅威に対応し、サービスの安全・信頼性を将来にわたって確保するため、事業者が技術研究開発にどの程度投資し、次世代の技術者育成にどのように取り組んでいるかをモニタリング項目に加えることで、長期的な視点でのガバナンスを促すことを提案します。 </p></p>	<p>頂いた御意見は今後の参考とさせていただきます。</p>	<p>無</p>