

内航海運業法施行規則等の一部を改正する省令案
に関するパブリックコメントの募集結果について

国土交通省では、令和7年2月10日から令和7年3月12日まで、内航海運業法等の一部を改正する省令案についてパブリックコメントを実施し、広く国民の皆様からの御意見を募集いたしました。

その結果、本件に関して、4件の御意見が寄せられました。

お寄せいただいた御意見の概要とそれに対する国土交通省の考え方を別紙のとおりとりまとめましたので公表します。

皆様方の御協力に深く御礼申し上げるとともに、今後とも国土交通行政の推進に御協力いただきますよう、よろしくお願い申し上げます。

1 実施方法

- (1) 募集期間 令和7年2月10日（月）～令和7年3月12日（水）
- (2) 周知方法 電子政府の総合窓口（e-Gov）に掲載
- (3) 意見提出方法 電子メール及び郵送

2 意見数

提出意見数 4件（4名）

3 問い合わせ先

国土交通省総合政策局情報政策課

電話番号 代表：03-5253-8111（内線28123）

直通：03-5253-8333

御意見の概要及び国土交通省の考え方

No.	御意見の概要	国土交通省の考え方
1	<p>内航海運業者です。</p> <p>弊社運航船の現状では、外部とインターネットにより接続されている運航関連機器やエンジン関連機器はありませんので、安全管理規程への追加は不要と考えます。</p> <p>一方、将来的に自動運航船を運航する場合には、サイバーセキュリティ対策が必須と考えられますので、業種ではなく、対象となる装備や機器名を明確にして、それに該当する場合に限定した対応を希望します。</p>	<p>内航海運分野に関し、国土交通省としましては、今後とも、皆様のご意見も踏まえながら、実効性の高い制度としてまいりたいと考えております。</p>
2	<p>■ 1. 改正の背景について</p> <p>「事業法体系でのサイバーセキュリティ対策に係る監督措置について、国が各事業者の保有する重要なシステムを把握し、国・事業者の情報交換等により、これを適切に行えるよう、必要な規定を整備していく方針としたところである」とあります。</p> <p>セキュリティの性質上、事業者より国に報告する「重要なシステム」に関する内容に関しては、「行政機関の保有する情報の公開に関する法律」第 5 条第四号（不開示情報）に規定している「公にすることにより、犯罪の予防、鎮圧又は捜査、公訴の維持、刑の執行その他の公共の安全と秩序の維持に支障を及ぼすおそれがある」に該当するものとして取り扱っていただきたく存じます。</p> <p>■ 2. 改正の概要について</p> <p>「鉄道事業における安全管理規程に、電子計算機（その機能が停止し、又は低下した場合に輸送の安全の確保に多大な影響を及ぼすおそれが生ずるものに限る）に係るサイバーセキュリティの確保に関する事項を記載することとする」とあります。</p>	<p>1. 情報公開法の適用に当たっては、個別具体の判断となっておりますが、一般論としては、サイバーセキュリティの維持に支障を及ぼすおそれがある事項については、情報公開法上の不開示情報となる余地があるものと考えております。</p> <p>2. 鉄道分野に関し、国土交通省としましては、制度の運用について鉄道事業者の皆様からご意見を頂戴する場をいただいたところであり、今後とも、皆様のご意見も踏まえながら、実効性の高い制度としてまいりたいと考えております。</p>

	<p>鉄道事業法施行規則の改正内容や対象となる電子計算機に関しては、趣旨及び各事業者の実態と乖離しないよう、事業者との認識合わせをお願いします。</p>	
<p>3</p>	<p>(該当箇所)</p> <p>現下の情勢に鑑み、特定国等を背景とする攻撃等を防御するのに十分な水準のサイバーセキュリティを事業者横断的に確保する必要がある、事業法体系でのサイバーセキュリティ対策に係る監督措置について、国が各事業者の保有する重要なシステムを把握し、国・事業者の情報交換等により、これを適切に行えるよう、必要な規定を整備していく方針としたところである。</p> <p>(意見)</p> <p>弊社においては「航空分野における安全ガイドライン」に従い対策を行っている。これは企業の実施すべき対策であることから行っているが、法案化された時の懸念は以下の通り。</p> <ul style="list-style-type: none"> ・罰則は定義されるのか？セキュリティ対策というレベルにおいて、ウイルス対策ソフトのみの導入だとほぼ防御できない。このレベルは条文上対策はしているが、実際には効果がない。こういう場合の罰則判定は？ ・EDR が推奨されているが、昨今の Living off the Land 攻撃においては、ほぼ EDR は無価値であり、結局、「プロセスの Zero-Trust 化」か「セキュリティ稼働体制が十分にある会社」しか守れない。こういう場合に罰則規定は適用されるのか？ ・監督措置とあるが、監査がはいるのか？その基準などは定義できるのか？ 	<p>今般の省令改正にて、「その機能が停止し、又は低下した場合に国民生活又は経済活動に重大な影響を及ぼすおそれが生ずる者であつて電子計算機（その機能が停止し、又は低下した場合に航空運送事業の遂行に著しく支障を及ぼすおそれが生ずるものに限る。）を使用する者として国土交通大臣が定める要件に該当する者」においては、航空運送事業における事業計画の記載事項に、当該電子計算機に係るサイバーセキュリティの確保に関する事項を記載することが必要となります。航空法第 108 条第 1 項の規定により事業計画の遵守の義務が課せられるところ、当該義務に違反していると認められる場合に航空法第 108 条第 2 項の規定に基づく国土交通大臣が行う命令に違反したときは、罰則の対象となります。</p> <p>また、事業計画に定められた事項の遵守状況について、報告徴収や監査等により確認をしていく方針としています。</p> <p>必要となる対策レベルや事業計画に記載を求める事項については、現在検討を進めているところ、いただいたご意見については、検討の参考とさせていただきます。</p>

	<p>上記の質問はあるものの、パブリックコメントということもあり、以下をコメントする。</p> <p>(1) 法案化されて、その後、ガイドラインなどの工程を踏まえると、鉄道・航空・空港・物流・港湾などの業務特性を踏まえて事業者側に過度な負担にならないような法案・ガイドライン作りを切望する。</p> <p>(2) 航空会社は航空機の運航を担っているが、滑走路は空港施設で運営され、発着の指示は国交省から行われ、運航中の無線通信は衛星通信業者含む各通信事業者が担い、出発前の燃油補給事業者による給油など、業界を超えた官民連携・民民連携によって運航が可能であるため、航空会社のみならず、関連のサプライチェーンに関する対応も検討してもらいたい。ここを解決せねば、弊社単独でセキュリティ対策を実施しても限界が生じる。</p> <p>(3) 本法案成立にあたっての NIST などの海外フレームワークとの関連性があれば、お示しいただきたい。</p>	<p>(1) 事業者の実情も踏まえつつ、サイバーセキュリティの確保に資する実効性の高い取組となるよう制度を構築してまいりたいと考えております。</p> <p>(2) 今般の省令案においては航空等の4分野について措置をしているところ、サプライチェーンを含めた対応については弊省所管以外の分野も含まれるところかと存じますので、今後の運用に当たって、参考とさせていただきます。</p> <p>(3) 御指摘の海外フレームワークの指すところが必ずしも明らかではないですが、今般の省令案については、「NIST サイバーセキュリティフレームワーク」に直接紐付く形で作成したものではありません。いずれにせよ、今後、各分野における制度の運用にあたり、海外の取組等を幅広く参照しながらアップデートを図っていくこととなります。</p>
4	<p>(該当箇所) 航空法施行規則関係 (第2条関係)</p> <p>(意見)</p>	<p>必要となる対策レベルや事業計画に記載を求める事項については、現在検討を進めているところ、いただいたご意見については、検討の参考とさせていただきます。</p>

1. 必要となるサイバーセキュリティ対策のレベルについて

事業計画の記載事項に「サイバーセキュリティの確保に関する事項」が追加されることにより、対象となる各事業者には一定のセキュリティ対策が求められることになる。

しかし、対象となる定期航空運送事業者は、事業領域、事業規模、地域特性、対象市場などが異なっており、サイバーセキュリティ事故に対するリスクや発生時の社会的影響は一律ではない。

仮にこれらの特性に鑑みることなく特定の事業者において過度な対応が求められることになった場合、事業者によっては業務上の制約や負担が生じかねず、航空輸送サービスの提供そのものに影響が及ぶことも懸念される。

したがって、対象となる事業者や必要となる対策のレベルについては、事業者毎の特性を十分に考慮し、それらに応じて必要かつ十分なものとするのが肝要である。

2. 事業計画に記載を求められる内容について

サイバー攻撃の動向は近年ますます多様化・高度化しており、これらに対する対策の技術もまた日進月歩である。各事業者はこのような変化の激しい環境において、事業環境なども考慮しつつ、日々柔軟にサイバーセキュリティリスクに対応することが求められているのが現状である。

このような状況の中、航空法令にて認可が必要とされている事業計画への記載内容として過度に個別具体的かつ詳細なものが求められた場合、認可手続きに時間を要することによって最新動向への柔軟な対応を阻害し、セキュリティ対策に遅れが生じることが懸念される。

したがって、記載項目については航空輸送サービスのセキュリティ面での安全性を担保するに足る最小限のものにとどめ、また、記載内容についても一定の柔軟性を担保すべく概要や方針のレベルとすることが

	必要である。	
--	--------	--

(以上)