2024年10月16日
一般社団法人日本損害保険協会 経営企画部国際業務室

IAIS市中協議文書「オペレーショナルレジリエンスの目標に関するアプリケーションペーパー」に意見提出

日本損害保険協会(会長：城田 宏明)は、保険監督者国際機構(IAIS)が2024年8月8日から10月11日にかけて市中協議に付した「オペレーショナルレジリエンスの目標に関するアプリケーションペーパー（AP）(※1)」に対する意見を提出しました。

当該意見は、添付1をご参照ください。

１．市中協議の概要

- IAISはこれまでに、金融機関のサイバーセキュリティの基礎的な側面に関するイシューズペーパー(IP)(※2)（2016年公表）およびAP（2018年公表）、オペレーショナルレジリエンスに影響を与える問題を特定し、監督アプローチの事例を示すIP（2023年公表）を作成してきた。策定中の2025年-2029年戦略計画も、デジタルイノベーション・サイバーリスクを戦略テーマに含んでいる。
- 本APは、オペレーショナルレジリエンスの監督アプローチの策定・強化に関して監督者を支援するための、健全かつ一貫性のある基盤の提供を目的として、保険セクターのオペレーショナルレジリエンスに関する目標を示している。なお、本APは新たな要件を定めるものではなく、既存の監督文書の適用を明確にするものである。
- IAISは、「目標」に関連する監督実務を示す「ツールキット」について、2025年前半に市中協議を実施した後、「目標」および「ツールキット」の両要素を単一のAPに統合することを予定している。

２．損保協会意見(抜粋)(詳細は添付1ご参照)

- 本APは、新たな監督上の目標を定めるものではなく、既存の保険基本原則（ICP）の規定をオペレーショナルレジリエンスの着眼点からまとめたものと理解している。オペレーショナルレジリエンスに関する問題は確たる解があるわけではなく、引き続き、IAISでの検討状況を保険会社に対しても適宜共有いただきたい。
- 用語「オペレーショナルレジリエンス」が各所で多用されているため、本APにおいても再定義（または再掲載）し、明文化していただきたい。

当協会は、IAISにおける国際保険監督基準策定の議論に積極的に参加しており、今後も市中協議等に際して本邦業界の意見を表明していきます。

(※1)アプリケーションペーパー

IAISの監督文書(ICP、ComFrame等)の特定のテーマに関して、原則や基準の一律な解釈や適用が難しい場合に、事例やケーススタディの提供を目的に作成される文書。助言や具体例、推奨、事例などを含む。

(※2)イシューズペーパー

トピックの背景、現行取組み、ケーススタディ等を提供し、規制・監督上の論点・課題を特定することを目的に作成される文書。監督者が文書の内容を実施することは期待されていないが、基準策定に向けた準備として作成されることが多く、IAISによる今後の作業に関する推奨を含む場合がある。

SONPO

添付１

保険監督者国際機構（IAIS）「オペレーショナルレジリエンスの目標に関するアプリケーションペーパー」に係る損保協会意見

番号		損保協会意見（和文）	損保協会意見（英文）
1	アプリケーションペーパーに関する一般的なコメント	本 AP は、新たな監督上の目標を定めるものではなく、既存の ICP の規定をオペレジの着眼点からまとめたものと理解している。オペレーショナルレジリエンスに関する問題は確たる解があるわけではなく、引き続き、IAIS での検討状況を保険会社に対しても適宜共有いただきたい。 2024 年後半のツールキット開発および監督実務に関する AP のドラフティングにおいても、引き続き一貫性のある対応をお願いしたい。	We understand that this application paper does not establish new supervisory objectives, but rather summarizes existing ICP provisions from an operational resilience perspective. As there is no definitive solution to the issue of operational resilience, we ask that the IAIS continue to share the status of its deliberations on this topic with insurers as appropriate. We ask for continued consistency in the development of the draft Toolkit and the drafting of the AP regarding supervisory practices in late 2024.
2	セクション 1「はじめに」に関する一般的なコメント	従来の AP には、「AP は新たな基準や期待を設定するものではなく、既存の基準の実施を支援するための補助資料である」といった文言が記載されていると認識している。本 AP 本文にもその旨を明記していただきたい。	We are aware that the existing APs contain language such as "APs do not set new standards or expectations, but provide supporting material to assist in the implementation of existing standards". We request that it be clearly stated in this AP as well.
10	パラグラフ 7 に関するコメント	用語「オペレーショナルレジリエンス」が各所で多用されているため、本 AP においても再定義（または再掲載）し、明文化していただきたい。	As the term "operational resilience" is used extensively in various parts, it should be redefined (or reposted) and clarified in this AP.
11	パラグラフ 8 に関するコメント	2024 年後半の監督実務の策定においても、新たな要件等を追加するのではなく、地域や法域を考慮したプロポーショナルなアプローチが取られることを期待する。	We expect that a proportional approach will be adopted in the development of supervisory practices in late 2024, taking into account regional and jurisdictional circumstances, rather than adding new requirements, etc.
31	パラグラフ 20 に関するコメント	オペレーション上の影響・混乱は必ずしも「定量化」できるとは限らないため、1 ポツ目の「定量化する」は「把握する」とするか、「定量化できないことがあること」を付記すべきである。	Since operational disruption/impact is not always quantifiable, we suggest replacing "Quantifies" in the first bullet point with "Understands" or additionally describing that there are cases where it is impossible to quantify maximum disruption/impact.

SONPO

保険監督者国際機構（IAIS）「オペレーショナルレジリエンスの目標に関するアプリケーションペーパー」に係る損保協会意見

		「あらかじめ定義された」とあるが、これは各事業会社が個々に”許容範囲”を定義するという理解であっているか。	The second bullet point: Regarding "pre-defined", we would like to clarify this means that each entity defines its own "tolerances".
32	セクション 2.2.3 に関するコメント	深刻だが妥当なシナリオを用いたシナリオテストの重要性について同意する。他方で、オペレーショナルレジリエンスに影響を与える要因は様々なものが考えられることから、網羅的にシナリオを用意することは容易ではない。シナリオテストはオペレーショナルレジリエンス向上のひとつの手段にすぎないため、網羅的なシナリオを用意するのではなく、蓋然性および重要性が真に高いシナリオに厳選して実施すべきである。	We agree on the importance of scenario testing with severe but plausible scenarios. On the other hand, it is not easy to prepare exhaustive scenarios because there are many possible factors that can affect operational resilience. Scenario testing is only one of various ways to improve operational resilience, and therefore, instead of preparing exhaustive scenarios, only those scenarios that are truly probable and important should be carefully selected for implementation.
36	セクション 2.2.5 に関するコメント	NIST（National Institute of Standards and Technology）等一般的なフレームワークに照らし、「保護・検知・対応・復旧」に加え、まず冒頭に「特定」があるのが妥当である。	In light of the NIST (National Institute of Standards and Technology) and other general frameworks, it is appropriate to have "identification" before "protection, detection, response, and recovery".
37	パラグラフ 23 に関するコメント	・パラ 23 に記載の内容は、全般的に粒度が細かく、また、箇条書きで様々な切り口が並列されており、どのような対応が求められているのか、わかりにくい。たとえば 1 点目について、数多くセキュリティ対策の切り口が存在する中で当該分類を選択した意図はなにか。国際的に使われているスタンダードを参照しているのであれば、出典を明記し「例えば、●●を参考にすると以下のようなアプローチが考えられる」といった記載とすることを提案する。 ・一般的に人/ポリシー/技術による対策が有効とされる。本パラグラフの記載が例示である前提のもとで、ポリシーの観点を追加してもよいのではないか。	- Paragraph 23 in general is very detailed. In addition, various perspectives are described in parallel in bullet points, making it difficult to understand what kind of response will be required. For example, regarding the first bullet point, what is the intention of selecting these categories among many security measures? If internationally used standards are referred to, we suggest clarifying the source and adding a sentence such as "For example, the following approaches could be considered with reference to...". - Generally, measures by people/policies/technologies are considered to be effective. Based on the premise that this

			paragraph is intended to provide examples, we suggest adding a policy perspective.
41	パラグラフ 25 に関するコメント	・「明確な復旧目標」とは RPO（Recovery Point Objective）や RTO（Recovery Time Objective）など、保険者が適切と考えるものを設定するものという理解に相違ないか。 ・第三者の BCP テストの検証主体が保険会社とはならないのではないか。「テスト結果の確認」が本文脈上、検証と同義であるか？	- Regarding "clear recovery objectives", is it correct to understand that insurers are to set RPO (Recovery Point Objective), RTO (Recovery Time Objective), etc., which they consider appropriate? - Insurers are not supposed to validate testing of the BCPs of third parties. In this context, is "confirmation of test results" synonymous with "validation"?
42	セクション 2.2.8 に関するコメント	管理（Manage）ではなく、監理（Oversee）ではないか。（パラ 26 の 2 点目にも管理のサポートとある）	We suggest replacing "manages" with "oversees". (The second bullet point also mentions "Supports effective management...".)
51	パラグラフ 30 に関するコメント	情報共有によって、業界全体のレジリエンスを高めることは重要である。一方で、オペレーショナルレジリエンスに関連する事項は、サイバー攻撃者へのヒントにもつながるため、ステークホルダーとの連携・透明性のあるコミュニケーションにあたっては、必要に応じて対象を限定し、慎重に対応すべきである。 パラ 30 の 1 ポツ目を以下の通り修文することを提案する。 ・保険会社のオペレーショナル・レジリエンス・アプローチに関して、機密保持に留意しつつ、業界、第三者および第ｎ者のサービス提供者、政府、非政府組織、保険契約者などの関連する利害関係者と協力する。	Paragraph 30 (first bullet point): It is important to enhance the resilience of the entire industry through information sharing. On the other hand, because matters related to operational resilience could also provide useful hints to cyber attackers, the scope of stakeholders should be carefully limited as necessary when collaborating and transparently communicating with them. Therefore, we suggest adding "taking into account confidentiality" at the end of the sentence.