

パラ	和文	英文
総論	<p>・ 全体的に、記述してある内容は正しい方向性であると考えます。</p> <p>しかしながら、Cyber security risks は保険会社固有の課題ではなく、保険会社以外の金融機関等に対するガイドラインや規制との整合性を保持し、重複を回避する必要があることから、金融機関向けの汎用なガイドラインをベースとした検討を行う方が妥当。業界固有の重要なリスクがない場合には、AP の分析のとおり、現行 ICP にもその要素は含まれており十分である。仮に不足がある場合でも、これを補う修正対応が適切と考えます。</p> <p>また、今回の AP の内容を受けても、保険業界固有のガイドラインや規則を策定する必要があるか否かは不明確であり、保険会社固有の規則を設ける場合には、その合理的な理由を明示する必要があると考えます。</p> <p>・ 本 AP の Recommendation におけるコメント内容は、導入文（例えばパラ 48 や 81）は may の表現が使用されていることから、ベストプラクティスとして記載されている趣旨であると考えますが、一方で後続の文章にはほぼ全て should や must の表現が使用されており、バランスを欠く。should や must の表現は may や would に変更し、監督者や保険者が重要性に応じて裁量を持てる記載にすべきと考えます。</p>	<p>We, the General Insurance Association of Japan (GIAJ), believe that what the Draft Application Paper on Supervision of Insurer Cybersecurity (hereinafter referred to as "AP") describes is going in the right direction. However, against the background of cybersecurity risks not being issues particular to insurers, we think it is more appropriate to consider potential insurance-specific guidelines and rules based on comprehensive guidelines for the whole financial sector so that their integrity in relation to sector-wide guidelines and regulations is maintained and unnecessary duplication is avoided.</p> <p>If there are no significant or industry-specific risks, the current ICPs which already encompass the issues presented by cyber risks should be sufficient for the supervision of insurer cybersecurity. If the current ICPs are found to be insufficient, we believe it is appropriate to revise the ICPs to make up for the shortfall.</p> <p>In any case, we are still not convinced that the insurance industry needs to develop its own guidelines or rules even after taking into consideration the contents of the AP. Therefore, when developing rules particular to insurers, the IAIS should clearly express its rationale.</p> <p>Judging by the fact that the introductory statements in the "Recommendation" section of the AP often use the word "may", such as in paragraphs 48 and 81, we understand "Recommendations" to mean "best practices". Additionally, almost all of the sentences in the latter part of the document use the words "should" or "must", which therefore indicates a lack of balance. We believe that the words "should" and "must" should be replaced with "may" and "would" so that supervisors and insurers can exercise discretion in accordance with the materiality of the issue.</p>

48.d	<p>取締役会と経営陣の間の役割や責任の配分は、取締役会の責任において、サイバーセキュリティーフレームワークの実効性を高める目的に資するよう、保険会社の裁量を許容すべきである。</p>	<p>It is the responsibility of the insurer's Board to appropriately define the respective roles and responsibilities of itself and its management so that its cybersecurity framework is effective. Therefore, the insurers' discretion should be allowed on this point.</p>
81.a	<p>3.1 48-d コメント同様</p>	<p>See our comment on 48.d.</p>
81.b	<p>同上</p>	<p>See our comment on 48.d.</p>
81.d	<p>・ 3.1 48-d コメント同様</p> <p>・ 人材の確保については、それぞれの国の事情によって難易度が高いケースがあることも鑑み、以下の通り修文を行うべき。</p> <p>d. An insurer's Board and senior management should cultivate awareness of and commitment to cybersecurity. The Board and senior management should make the effort to include members with skills appropriate to their oversight and management roles with respect to the risks posed by cyber threats. In addition, the Board and senior management should promote a culture that recognizes that staff at all levels have important responsibilities in ensuring the insurer's cybersecurity and lead by example.</p>	<p>See our comment on 48.d.</p> <p>Considering that it could be difficult in some countries to secure members with appropriate skills, this paragraph should be revised as follows:</p> <p>d. An insurer's Board and senior management should cultivate awareness of and commitment to cybersecurity. The Board and senior management should make the effort to include members with skills appropriate to their oversight and management roles with respect to the risks posed by cyber threats. In addition, the Board and senior management should promote a culture that recognizes that staff at all levels have important responsibilities in ensuring the insurer's cybersecurity and lead by example.</p>
81.f	<p>senior executive が independence を保有すべきとあるが、1.3 のプロポーシヨナリティに則り、当該保険者の事業規模、複雑性、事業特性などに応じた統治形態が容認されるものと理解している。</p>	<p>Although this paragraph alludes to the independence of the roles of senior executives, we understand that various forms of governance are allowed depending on the insurers' scale of business, complexity, and the characteristics of its business in accordance with the principle of proportionality stipulated in section 1.3.</p>
103.e	<p>管理が必要な要素を台帳によって管理するにあたって、その形式については、単一の台帳に情報を網羅する方法をすべての保険者に対し一律に求めるのではなく、保険者が適切と判断した管理手法が容認されるべきであるため、本項は以下の通り修正されるべき。</p>	<p>As for managing elements and forms of the inventory, management techniques that insurers judge appropriate should be allowed rather than uniformly requiring all insurers to encompass all the information into a single inventory. Therefore, this paragraph should be revised as follows:</p>

	The inventory should may encompass hardware, software platforms and applications, devices, systems, data, personnel, external information systems, critical processes, and documentation on expected data flows, based on the management method deemed appropriate by the insurer.	The inventory may encompass hardware, software platforms and applications, devices, systems, data, personnel, external information systems, critical processes, and documentation on expected data flows, based on the management method deemed appropriate by the insurer.
103.g	「統合」を狭義の意味で実現するのは難易度が非常に高いと想定される。 →「関連付けた管理を実施すべき」という解釈が許容されるべき。	We assume it is immensely difficult to literally "integrate" identification efforts with other relevant processes in a narrow sense. Therefore, insurers should be allowed to interpret this paragraph as “insurers should manage identification efforts in association with other relevant processes”, such as acquisition and change management, in order to facilitate a regular review of its list of critical business processes, functions, individual and system credentials, as well as its inventory of information assets to ensure that they remain current, accurate and complete.
103.q	・通常発現しないと考えられるイベントや、過去に発現しなかったイベントのとらえ方は保険会社により異なると思われるため、考慮すべきイベントのレベル感や内容について保険会社の裁量が確保されることを確認したい。	As each insurer may have a different perception of “cyber events considered unlikely to occur or have never occurred in the past”, we would like to make sure that the judgment of cyber threats to be considered is left to the discretion of each insurer.
133.f	「cyber threat intelligence programme」を明確化していただきたい。	The definition of the “cyber threat intelligence programme” should be clarified.
133.n	「advanced threat agent capabilities」の定義について解説頂きたい。	We would like to have a detailed definition of “advanced threat agent capabilities”.
133.o	3.1 48-d コメント同様	See our comment on 48.d.
133.s	ペネトレーションテストは通常 IT 部門を中心に限られた範囲で実施する。“wider business stakeholders”を含めて実施するペネトレーションテストとはどんなイメージかを確認したい。	Penetration tests are usually carried out by a limited number of (mainly IT) departments. We would like to have a clearer view of how “the tests which could include wider business stakeholders” will be carried out.

160.e	当該規律の目的を明確化したい。大規模インシデント時の外部リソース枯渇リスクを避けるために外部と事前に契約締結を求めているものか。	We would like to more clearly understand the objective of the rule “insurers should plan to have access to external experts”. Does it require insurers to conclude some kind of contract with third-parties in advance of a large-scale or industry-wide event to avoid the risk of losing access to external resources?
160.f	レスポンスプランについて、関連当局と事前調整まで求める意図を教示いただきたい。	We would like to know the intention behind the IAIS requiring insurers to consult and coordinate with relevant authorities regarding their response plan. This requirement seems too prescriptive.
160.h	コミュニケーションのために「a specific team」を配置する必要はなく、各人の役割を明確にすることで足りると考える。	As long as the necessary responsibilities with regard to stakeholder communications are clarified, we do not think insurers need to have “a specific team” in place for all stakeholder communications.
198.a	198 パラグラフについて、FS-ISAC または金融 ISAC に参加するかどうかについての判断は、保険会社自身が、そのサイバーセキュリティの実効性を高めるうえでの必要性等に照らしつつ、自己の責任で適切に行うものであること、および当該必要性の有無および程度についても比例の原則が適用されること、を確認したい。	We would like to make sure that insurers have the discretion as to whether to participate or not in FS-ISAC or Financials ISAC Japan, taking into account their judgment of the necessity to enhance the effectiveness of their cybersecurity. We also would like to make sure that the principle of proportionality is applied with regard to their decision on the necessity of such participation.
198.d	脅威分析の機能があるものとして記述されているが、現実には機能を持つことも難度は高いことを指摘したい。	This paragraph assumes that an insurer’s cyber threat intelligence operations are a given. However, we would like to point out that in reality it is difficult to even have a department that deals with cyber threat intelligence operations.
198.e	同上	See our comment on 198.d.
198.f	同上	See our comment on 198.d.

198.g	<p>業務委託関係にあるような第三者のサービスプロバイダーとの間でサイバーセキュリティフレームワークに関する"bilaterally"の情報交換を行うことは、当方側のセキュリティやガバナンス上のリスクをさらけ出すことそのものであり、セキュリティ上危険な状態に陥る可能性があるため、現実的ではないと考える。</p>	<p>We think that exchanging information “bilaterally” on their cybersecurity framework with third-party service providers is unrealistic. Such exchanges would be no different from exposing an insurer’s security and governance risks, and would put insurers in greater danger with regard to their cybersecurity.</p>
-------	--------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

以 上