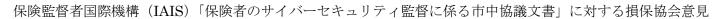


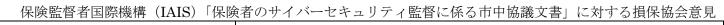
保険監督者国際機構(IAIS)「保険者のサイバーセキュリティ監督に係る市中協議文書」に対する損保協会意見 ハ°ラ 和文 英文 ・全体的に、記述してある内容は正しい方向性であると考える。 We, the General Insurance Association of Japan (GIAJ), believe that 総論 しかしながら、Cyber security risks は保険会社固有の課題ではなく、保険会社 what the Draft Application Paper on Supervision of Insurer 以外の金融機関等に対するガイドラインや規制との整合性を保持し、重複を回 Cybersecurity (hereinafter referred to as "AP") describes is going in the 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 right direction. However, against the background of cybersecurity risks 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 not being issues particular to insurers, we think it is more appropriate to 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 consider potential insurance-specific guidelines and rules based on 合でも、これを補う修正対応が適切と考える。 comprehensive guidelines for the whole financial sector so that their 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 integrity in relation to sector-wide guidelines and regulations is 定する必要性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 maintained and unnecessary duplication is avoided. には、その合理的な理由を明示する必要があると考える。 If there are no significant or industry-specific risks, the current ICPs which already encompass the issues presented by cyber risks should be ・本 AP の Recommendation におけるコメント内容は、導入文(例えばパラ 48 sufficient for the supervision of insurer cybersecurity. If the current ICPs や 81) は may の表現が使用されていることからも、ベストプラクティスとし are found to be insufficient, we believe it is appropriate to revise the ICPs て記載されている趣旨であると考えるが、一方で後続の文章にはほぼ全て to make up for the shortfall. 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 In any case, we are still not convinced that the insurance industry needs 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 to develop its own guidelines or rules even after taking into consideration る記載にすべきと考える。 the contents of the AP. Therefore, when developing rules particular to insurers, the IAIS should clearly express its rationale.

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.



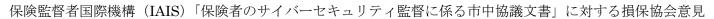
<u>SO</u>	NPO
18 d	取締役会と経り

40.1	「「大型」とは、「大型」というしまり、「大型」とは、「大型」とは、「大型」というしましまり、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしき、「大型」というしまり、「大型」というしまり、「大型」というしまり、「大型」というしい、「大型」は、「大型」は、「大型」は、「大型」というしい、「大型」は、「しき、「大型」は、「しい、「しき、「大型」は、「しい、「し、「、「しき、「しい、「しき、「しい、「しい、「しい、「しい、「しい、「しい、「しい、「しい、「しい、「しい	T
48.d	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	It is the responsibility of the insurer's Board to appropriately define the
	ーセキュリティーフレーワークの実効性を高める目的に資するよう、保険会社の	respective roles and responsibilities of itself and its management so that
	裁量を許容すべきである。	its cybersecurity framework is effective. Therefore, the insurers'
		discretion should be allowed on this point.
81.a	3.1 48-d コメント同様	See our comment on 48.d.
81.b	同上	See our comment on 48.d.
81.d	・3.1 48-d コメント同様	See our comment on 48.d.
	・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	Considering that it could be difficult in some countries to secure members
	ることも鑑み、以下の通り修文を行うべき。	with appropriate skills, this paragraph should be revised as follows;
		d. An insurer's Board and senior management should cultivate
	d. An insurer's Board and senior management should cultivate awareness of	awareness of and commitment to cybersecurity. The Board and senior
	and commitment to cybersecurity. The Board and senior management should	management should make the effort to include members with skills
	make the effort to include members with skills appropriate to their oversight	appropriate to their oversight and management roles with respect to the
	and management roles with respect to the risks posed by cyber threats. In	risks posed by cyber threats. In addition, the Board and senior
	addition, the Board and senior management should promote a culture that	management should promote a culture that recognizes that staff at all
	recognizes that staff at all levels have important responsibilities in ensuring	levels have important responsibilities in ensuring the insurer's
	the insurer's cybersecurity and lead by example.	cybersecurity and lead by example.
81.f	senior executive が independence を保有すべきとあるが、1.3 のプロポーショナ	Although this paragraph alludes to the independence of the roles of
	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	senior executives, we understand that various forms of governance are
	が容認されるものと理解している。	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.
103.e	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	As for managing elements and forms of the inventory, management
	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	techniques that insurers judge appropriate should be allowed rather than
	 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	uniformly requiring all insurers to encompass all the information into a
	の通り修正されるべき。	single inventory. Therefore, this paragraph should be revised as follows;
L		



SO	N	PO

	The inventory should may encompass hardware, software platforms and	The inventory may encompass hardware, software platforms and
	applications, devices, systems, data, personnel, external information systems,	applications, devices, systems, data, personnel, external information
	critical processes, and documentation on expected data flows, based on the	systems, critical processes, and documentation on expected data flows,
	management method deemed appropriate by the insurer.	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。	We assume it is immensely difficult to literally "integrate" identification
	→「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。	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	As each insurer may have a different perception of "cyber events
	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	considered unlikely to occur or have never occurred in the past", we
	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。	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	Penetration tests are usually carried out by a limited number of (mainly
	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	IT) departments. We would like to have a clearer view of how "the tests
	メージかを確認したい。	which could include wider business stakeholders" will be carried out.



SO	N	PO

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	We would like to more clearly understand the objective of the rule
	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。	"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	We would like to know the intention behind the IAIS requiring insurers
	たい。	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	As long as the necessary responsibilities with regard to stakeholder
	割を明確にすることで足りると考える。	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	We would like to make sure that insurers have the discretion as to
	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	whether to participate or not in FS-ISAC or Financials ISAC Japan,
	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	taking into account their judgment of the necessity to enhance the
	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	effectiveness of their cybersecurity. We also would like to make sure that
	V' _o	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、現実は機能を持つことも難	This paragraph assumes that an insurer's cyber threat intelligence
	度は高いことを指摘したい。	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.



保険監督者国際機構(IAIS)「保険者のサイバーセキュリティ監督に係る市中協議文書」に対する損保協会意見

198.g

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。

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.

以上