仮　訳

保険監督者国際機構

保険セクターにおける
オペレーショナル・レジリエンスに関する
論点書

２０２３年５月

IAIS について

保険監督者国際機構（IAIS）は、200 を超える管轄区域からの保険監督者および規制者である任意のメンバーからなる組織である。IAIS の使命は、保険契約者の利益と保護のために、公正、安全かつ安定した保険市場を発展させかつ維持すべく、効果的でグローバルに整合的な保険業界の監督を促すこと、およびグローバルな金融安定に貢献することである。

IAIS は 1994 年に設立され、保険セクターの監督のための原則、基準および他の支援する資料の策定、ならびに、それらの実施を支援する責任を有する国際的な基準設定主体である。また、IAIS はメンバーに対して、保険監督および保険市場に関するメンバーの経験および見解を共有するための議論の場を提供する。

IAIS は、他の国際的な金融政策立案者および監督者または規制者の協会と自身の取組みを調整しており、また、世界的な金融システムの形成を支援している。特に、IAIS は、金融安定理事会（FSB）のメンバーであり、国際会計基準審議会（IASB）の基準諮問会議のメンバーであり、および保険へのアクセスに関するイニシアティブ（A2ii）のパートナーである。また、その結集された専門知識が認められ、IAIS は、G20 のリーダーおよび他の国際的な基準設定主体から、保険の論点のみならずグローバルな金融セクターの規制および監督に関する論点について、定期的に助言を求められている。

さらなる情報は、www.iaisweb.org を参照いただくか、LinkedIn で我々をフォローいただきたい：IAIS－保険監督者国際機構。

論点書は、特定のトピックの背景を提示したり、特定のトピックに関する現在の実務、実際の事例またはケーススタディを述べたり、および/または、関係する規制上および監督上の論点ならびに課題を特定したりするものである。論点書は主として説明的であり、監督者がどのようにして監督文書を実施すべきについて期待を生み出すことは意図していない。論点書は、基準策定の準備作業の一部を形成することが多く、IAIS による将来の作業のための提言を含むこともある。

保険監督者国際機構
c/o 国際決済銀行
CH-4002 Basel
Switzerland
Tel: +41 61 280 8090
www.iaisweb.org

本文書は、IAIS メンバーとの協議の上、オペレーショナル・レジリエンス・タスクフォースにより作成された。

本文書は IAIS のウェブサイト（www.iaisweb.org）上で入手可能。

コンテンツ概要

1 はじめに

1.1 目的と範囲

1. 本文書の目的は、新型コロナウイルスのパンデミック（以下「パンデミック」）時に得られた教訓を考慮しながら、保険セクターにおけるオペレーショナル・レジリエンスに影響を与える課題を特定し、監督者がこれらの発展にどのようにアプローチしているかに関する実例を提示することである。[1]本文書はオペレーショナル・レジリエンスが広範かつ発展途上の領域であるという認識のもと、重大かつ増加するオペレーショナル・リスクの原因であり、そのため監督者の関心を引くものであるとタスクフォースが考える領域に関する、オペレーショナル・レジリエンスについての 3 つの具体的なサブ・トピックに対応する：
   - サイバー・レジリエンス；
   - IT のサードパーティへの外部委託；および
   - 事業継続管理（BCM）。

2. 近年、IAIS はオペレーショナル・レジリエンスに関する他の資料を公表している（特にサイバー・レジリエンスに関するもの）。 IAIS は保険セクターのサイバーリスクのトピックを論点書（2016 年）と適用文書（2018 年）において検討した。これらの文書は、金融機関のサイバーセキュリティに関する特定の基礎的要素の認識、保険セクターにおけるサイバー侵害（cyber breach）のケーススタディ、および既存の有用な実務と指標に即したサイバーリスク枠組みに焦点を当てている。IAIS は 2020 年に、持続可能性のあるサイバーリスク引受市場の発展に向けた課題と監督上の検討事項を特定する、サイバーリスクの引受に関する報告書も公表している。これらの資料は、適切な場合には本文書の議論を補足するものとして考えるべきである。[2]

3. 本文書の情報は、IAIS の保険基本原則（ICPs）の見直し、基準設定主体（SSBs）によるオペレーショナル・レジリエンスに関連する既存文書のストックテイク、IAIS のメンバー外である専門家との直接的な関与―ラウンドテーブルを含む―および保険監督者間で共有された監督実務に関する情報から、情報提供を受けている。

1.2 保険セクターにとってのオペレーショナル・レジリエンスの重要性

4. デジタル時代は、サイバー上の脅威とテクノロジーへの依存の拡大によってもたらされる付随的なリスクと共に、数十年にわたって保険会社にとって現実のものとなっている。オペレーショナル・レジリエンスの概念は新しくないが、保険会社のデジタルシステムへの依存度の増加を考慮して監督体制を適応させることの重要性はより最近認識されるようになった。

5. パンデミックは、デジタルテクノロジーの利用、重要な事業部門のサードパーティへの外部委託、および予期せぬ出来事による通常の事業機能の中断により発生するリスクを考慮した、より包括的なオペレーショナル・レジリエンスの枠組みを企業が整備する必要性をさらに浮き彫りにした。こうした検討は短期的な課題に適用することができるが、検討により取締役会および上級管理職（現在と将来の両方）が重要な戦略目標としてオペレーショナル・レジリエンスに注目することができるようになる可能性もある。

6. パンデミックの拡大および、それに付随するリモートワークの幅広い普及に伴いサイバー攻撃は増加した。金融安定理事会（FSB）の報告によれば、金融機関に対するフ

---

[1] IAIS の 2022-2023 年ロードマップは、特に急速に発展する技術革新と、COVID-19 のパンデミックに起因する人々の働く場所・働き方の変化に照らして、オペレーショナル・レジリエンスを、監督上のますます重要な焦点領域として「ハイレベル目標 3 *監督上のグッドプラクティスの共有と監督上の課題の理解の促進*」に位置付けた。

[2] 保険セクターにおけるサイバーリスクに関する論点書（2016 年 8 月）；保険会社のサイバー・セキュリティの監督に関する適用文書（2018 年 11 月）；サイバーリスクの引受―持続可能な市場発展のための課題および監督上の検討事項の特定（2020 年 12 月）。

ィッシング、マルウェアおよびランサムウェアといったサイバー行為の件数は、2021 年 2 月に 1 週間あたり 5000 件未満だったところ、2021 年 4 月末には 1 週間あたり 200,000 件以上にまで増加した。[3]FS-ISAC（Financial Services Information Sharing and Analysis Center）による金融機関への調査により、事例の 45%で従業員の在宅勤務が仮想デスクトップ（VDI）／仮想プライベートネットワーク（VPN）プロセスを圧迫していたことも明らかになった。ハイブリッド勤務・リモート勤務への急速な移行は、IT システムにある種の新たな脆弱性を与え、アタックサーフェス（攻撃対象領域）を拡大するという点において、事業体のオペレーショナル・レジリエンスにリスクをもたらした。事例の 3 分の 1 では、長期の在宅勤務労働者についての IT-BCP が用意されていなかった。金融機関の 5 分の 1 は、そのネットワーク運用業務がパンデミック時に中断されたと報告している。[4]

7. SSBs と監督者は、パンデミック以前とパンデミック時の双方の期間に、概念的および構成の観点からオペレーショナル・レジリエンスに対応しようとしてきたが、おそらくパンデミックはこうした意識を向上させ、こうした懸念に対応する監督文書の策定を加速させた。

8. バーゼル銀行監督委員会（BCBS）は銀行の文脈において、オペレーショナル・レジリエンスを「ディスラプションの中で銀行が重要な業務を継続できる能力」と定義している。さらに、BCBS は「銀行は、オペレーショナル・レジリエンスを検討する際に、ディスラプションが起こりうることを前提とし、その全体的なリスク選好と、ディスラプションへの許容度を考慮に入れるべきである」と説明している。[5]有害な事象の防止は全体的な枠組みにおける不可欠な部分ではあるものの、この定義は、回避不能なディスラプションからの回復も同等に不可欠であるということを強化している。

9. 経済協力開発機構（OECD）は、オペレーショナル・レジリエンスの非常に広範な定義の策定において、その定義を「長期のストレス、変化および不確実性を前にして、家計、地域および国家がショックを吸収・回復するとともに、その構造と、生計を保つ手段を積極的に適応・変換する能力」であると明言している。[6]OECD の定義を踏まえれば、健全なオペレーショナル・レジリエンスの重要な要素とは、目標を達成し続けられるように枠組みの側面を更新・発展させることであると分かる。

10. 英国の金融監督当局は 2021 年に、オペレーショナル・レジリエンスを「会社、その会社のグループ、および金融セクター全体が、業務上のディスラプションを防止し、そうしたディスラプションに適応・対応し、回復し、さらには教訓を得る能力」と定義した。[7]英国のアプローチでは、レジリエンスは、保険会社のシステムやプロセス単独で考えるのではなく、重要な事業サービスに焦点を当てることで最も実効的に対応することができると考えられている。英国の政策は、保険会社が通常通り業務を行うことを妨げるようなディスラプションは時折発生するであろうこと、および、保険会社は、深刻だが起こりうる多様なディスラプションのシナリオを検討する必要があることを強調している。このアプローチでは、盲点が存在することにより、ショックやディスラプションが現実のものになるための実質的なステップとなり得ることを認められている。

11. 2020 年に米国では、連邦準備制度理事会、通貨監督庁、および連邦預金保険公社（以下、「各当局」）がガイダンスにおいてオペレーショナル・レジリエンスを「あらゆる災害によるディスラプションの中で、重要な業務と中核的な事業分野を含めた業務を遂行する能力」と定義した。各当局は、オペレーショナル・レジリエンスは、ディ

---

[3] FSB、新型コロナウイルス感染症の世界的大流行に関する金融安定上の観点からの教訓：最終報告書（2021 年）

[4] 国際決済銀行（BIS）ブレティン、COVID-19 と金融セクターにおけるサイバーリスク（2021 年）

[5] BCBS、オペレーショナル・レジリエンスのための諸原則（2021 年）

[6] OECD、リスクおよびレジリエンス

[7] イングランド銀行、金融セクターのオペレーショナル・レジリエンス

スラプションに備え、適応し、耐え、回復するための充分な財務リソース・経営リソースと組み合わさった、実効的なオペレーショナル・リスク管理の成果物であると説明している。[8]

12. これらの定義をもとに、オペレーショナル・レジリエンスは、保険会社が現在利用している多様な実務と規律から生まれる成果物であると考えることができる。オペレーショナル・レジリエンスのある保険会社とは、重要な業務またはシステムに影響を与えることで通常の業務過程へのディスラプションを引き起こす可能性がある広範な事象の影響に直面し、耐え、軽減し、回復し、さらにはその教訓を得ることができる保険会社である。オペレーショナル・レジリエンスは、ディスラプションが起こる可能性があり、保険会社はこうしたディスラプションへの許容度を検討し、その業務上の枠組みを立案する際に考慮に入れるべきであるという仮定に基づいている。

1.3 論点書の構成

13. 本文書の**セクション 2** は、オペレーショナル・レジリエンスの広範なトピックと上述のサブ・トピックへの ICPs の一般的な適用可能性の概観を示している。これには、リスクの様相は変わり続けるということへの留意とともに、健全なオペレーショナル・リスク管理を原則として支援する ICPs の特定も含まれている。

14. **セクション 3.1 および 3.2** は、特に実効的なオペレーショナル・リスク管理に対する健全なガバナンスの重要性と、官民連携を含む情報共有による利益に焦点を当てながら、全般的な課題を概説している。

15. **セクション 3.3** では、監督者が利用可能な既存のツールおよび指標を含む、サイバー・レジリエンスを達成するために企業が確立する枠組みの質の評価に関する課題を検討している。監督者が保険会社のサイバー・レジリエンスを評価するために利用可能な適切なツールおよび指標を有することの重要性は、誇張しすぎることはない。2021 年にはサイバー攻撃が世界的に、ほぼすべてのカテゴリーで増加しており、ある情報源ではランサムウェア攻撃は 2020 年から 2021 年に 105%増加したことが示されている。[9]特に、既存のツールおよび指標がサイバー攻撃の発展途上の性質に対応しようとしている場合には、サイバー攻撃の増加は事業体のサイバー・レジリエンスの監督にリスクをもたらす。

16. **セクション 3.4** は、金融セクターの複雑性の増大と IT のサードパーティへの外部委託への依存を踏まえて、集中によって生じるリスクの評価に関連する課題を重大な問題として概説している。IT 関連部門の委託先サードパーティから保険会社にもたらされるリスクは、保険業界を含めて多くの業界で同様のものである。保険会社は、個人情報、財務情報および知的財産を含む大量の多様なデータを保有し取り扱っており、そのことは、ベンダーとの関係に関する保険会社のリスク管理と、集中によって生じるサードパーティ・リスクに関連する潜在的な脆弱性に対して、監督者と保険会社がどのように対応するかの重要性を高めている。

17. **セクション 3.5** では、パンデミックへの対応を含む今日の環境の実態に即すように BCM アプローチを発展させる必要性に関連した課題について述べている。ジョイントフォーラムは BCM を、「ディスラプションが発生した場合に特定の事業を維持または回復することができるようにするための、方針、基準、および手続を含む事業全体に関するアプローチである。その目的は、ディスラプションから生じる、業務上、財務上、法律上、風評上およびその他の重大な結果を最小化することにある」と説明している。[10]事業継続計画（BCP）は、「ディスラプションが発生した場合に組織の

---

[8] 米国連邦準備銀行、SR 20-24–オペレーショナル・レジリエンス強化のための健全な実務に関する省庁間文書（2020 年 11 月）

[9] ソニックウォール、2022 年ソニックウォール脅威レポート（2022 年）

[10] 業務継続のための基本原則－2006 年 8 月

事業を継続または復旧するために必要な手続およびシステムを規定する、書面による包括的な行動計画」と説明されている。[11]本論点書の目的上、BCM は BCP を含む包括的な概念として考える。オペレーショナル・リスクがパンデミック状況下でどのように発展したのか、および、その結果としてパンデミック時に得られた教訓は、BCM にとって重要である。広く普及したリモート勤務・ハイブリッド勤務のツールとテクノロジーの利用への依存により、パンデミックは、保険会社を含む多くの会社の従業員やステークホルダーとの関わりの持ち方を変えた。リモート勤務・ハイブリッド勤務は事業体に大きな柔軟性をもたらし、政府が義務付けたロックダウン後の（および一般的な）事業継続を促進した。しかしながら、ハイブリッド勤務・リモート勤務環境への移行の重要な点は、アタックサーフェスの拡大、テクノロジーへの依存、および IT サービスの外部委託に起因するリスクを理解し積極的に管理することである。

18. **セクション 4** は、―それまでのセクションで議論された見解に基づいて―保険監督者による将来の検討または更なる分析の恩恵を受ける可能性がある、サイバー・レジリエンス、IT のサードパーティへの外部委託および BCM に関連するリスクの多くの側面を概説する。

2 オペレーショナル・レジリエンスへの ICPs の適用可能性

19. ICPs は保険会社の監督のためのグローバルな枠組みを提供する。多くの場合、ICPs は具体的なテーマに沿ったリスクの課題に対応していないものの、新たなリスクおよびエマージングリスク、および／または保険セクターが直面している発達中のリスク―オペレーショナル・リスクを含む―への注意の高まりを監督者が特定・対応するための柔軟な基礎を提供している。このため、ICPs は保険会社のオペレーショナル・レジリエンスを確保するための基礎的な要素を特定する自然な出発点の役割を果たす。

20. 一般に、ICPs はオペレーショナル・リスクを含む多様なリスクに対応するような方法で起草されている。しかしながら、ICPs はオペレーショナル・レジリエンスという用語の範囲を説明していない。例えば、ICPs は IT システムの利用と外部委託に言及しているが、これらがどのように保険会社のオペレーショナル・リスク（サイバーリスクを含む）につながりうるかには具体的に対応していない。同様に、ICPs はサイバーリスクの特定と管理には言及しているが、サイバーリスク管理と、事業体の IT システムおよびプロセスの間のつながりは説明していない。

21. それでもなお ICPs は、これらの課題に対する監督上の対応の指針となり、オペレーショナル・リスクの視認性（visibility）を高めるための活動や戦略を包含し、重大なリスクの健全な管理と適切な内部統制の実施を求めている。これらのすべては、プロポーショナリティの課題に配慮しながら、より全般的で健全なオペレーショナル・リスク管理を促進するものである。

22. 保険セクターにおけるオペレーショナル・レジリエンスの監督と管理を支援するものとして特定されている ICPs には、以下が含まれる：

- ICP 4（免許付与）
- ICP 7（コーポレート・ガバナンス）
- ICP 8（リスク管理および内部統制）
- ICP 9（監督上のレビューおよび報告）
- ICP 10（予防措置、是正措置および制裁措置）
- ICP 12（市場からの撤退および破綻処理）
- ICP 16（ソルベンシー目的の ERM（統合的リスク管理））

[11] 業務継続のための基本原則－2006 年 8 月

- ICP 23（グループ全体の監督）
- ICP 24（マクロ健全性監督）

23. ICPs にはオペレーショナル・レジリエンスとの明確な相互作用があり、保険会社のオペレーショナル・リスクの健全な管理を支援する。とはいえ、ICPs は意図としてプリンシプルベースのレベルで設定されており、このためオペレーショナル・レジリエンス（および関連する用語）の定義やオペレーショナル・リスクの管理について具体的で詳細なガイダンスは含まれていない。

24. 近年の監督上の主要な発展は、オペレーショナル・レジリエンスを、成果物、すなわち、事業体がディスラプションの中で重要な業務を継続できる能力と考えるようになっていることである。オペレーショナル・レジリエンスは、ひいては事業体がどのように業務を遂行するかについての戦略的な背景を提供するとともに、財務上のレジリエンスおよび潜在的には金融安定性の主要な推進力となる。ICPs のプリンシプルベースな性質を足掛かりとして、成果物としてのオペレーショナル・レジリエンスの包括的な概念を検討すること、ならびに、この成果ベースのアプローチと、サイバー・レジリエンス、IT のサードパーティへの外部委託、および BCM の間のつながりを議論および／または規定することが有用となりうる。

25. ICPs のレビューによって、オペレーショナル・リスク管理の重要な要素としてのサイバー・レジリエンス、IT のサードパーティへの外部委託、および BCM（これらはセクション 4 で概説される要素の一部として検討されている）について、さらなる議論や支援文書策定の検討の必要な領域が多くあることが明らかになった。

3 主要な課題および監督上のアプローチ

26. 本セクションは、オペレーショナル・リスクが大きい・増加している領域に関連した、サイバー・レジリエンス、IT のサードパーティへの外部委託および BCM のサブトピックスにまたがる、保険監督者にとって包括的な課題を提示している。

27. これらのサブトピックスに関連するリスクは相互依存性および相互連関性があるため、個別に捉えるべきではない。保険会社のオペレーショナル・レジリエンスを管理するための統合的なアプローチを整備することは、事業体の業務上の実効性および効率性の向上につながりうる。

28. 例えば、保険会社は重要な IT サービスの提供をサードパーティに依存するかもしれないが、このことは、適切に運営すれば、保険会社のサイバー・レジリエンスを向上する可能性がある。クラウドのような先端テクノロジーの利用は、社内または旧来のテクノロジー・インフラおよびシステムと比べてサイバーセキュリティの効率化と向上につながりうる。しかしながら、サードパーティへの依存はサイバーリスクを高める可能性もある。金融セクターにおけるサードパーティのサイバーリスクマネジメントに関する G7 の基礎的要素で述べられているように、「サードパーティの脆弱性に起因するサイバーインシデントにより、不正行為やサービスのディスラプション、顧客または企業の機微（センシティブ）情報へのアクセスに至る可能性がある」。[12]サードパーティのサービスプロバイダーがアクセス可能なあらゆる機微情報または個人情報（顧客情報等）の観点において、これは特に保険会社にとって重要である。

29. 監督者は、サイバー・レジリエンスを達成するための保険会社の枠組みを評価する際にサードパーティである重要なサプライヤーへの依存がどのように特定されるか、および、こうした依存が重大な脆弱性をどの程度もたらしているかを検討するかもしれない。サイバー・レジリエンス評価にサードパーティを含めることにより、リスクの特定と、関連するリスク軽減戦略の実施が促進されうる。このことは、サードパーティによる評価への直接参加から、保険会社が自社のサイバー・レジリエンスの評価の

[12] G7、金融セクターにおけるサードパーティのサイバーリスクマネジメントに関する基礎的要素

際にサードパーティへの依存の影響を検討することまで、広範なアプローチを通じて達成されうる。

30. サイバー・レジリエンス、IT のサードパーティへの外部委託と BCM の間で重複するリスクも存在する。例えば、サイバーインシデントは事業継続性に影響を与える可能性があり、サードパーティへの攻撃に起因する可能性があるため、保険会社は、こうしたリスクの間のつながりを熟知している必要がある。サイバー・レジリエンス（事業体内の IT インフラと、外部委託された IT サービスの観点から）と BCM を統合することは、サイバーに関する検討事項が保険会社のより広範なオペレーショナル・レジリエンス枠組みにより適切に組み込まれるようにするうえで役立ちうる。

3.1 ガバナンスおよび取締役会の説明責任

31. ICPs は、保険会社が新たに発生したリスクを特定・対応し、変化する環境に適応することを可能にする、堅固なガバナンス構造の重要性を強調している。このことから、不充分なオペレーショナル・レジリエンス管理がもたらし得る潜在的に広範な影響は、オペレーショナル・リスクを保険会社の取締役会および上級管理職の適切な注意を必要とするような主要なリスクにまで高める。

32. 保険会社の取締役会と上級管理職は、業務上のディスラプションの影響を評価することができる堅固なガバナンス枠組みの策定を監視し、これらのリスクの影響を許容範囲内に留めるための適切な軽減戦略および措置の整備について監督する最終的な責任がある。一方で、上級管理職はレジリエンス計画の実効的な遂行を確保する責任がある。

33. 取締役会または上級管理職の個々のメンバーはオペレーショナル・リスク管理の専門性を有することを合理的に期待されてはいないものの、取締役会全体では、保険会社のオペレーショナル・レジリエンスに影響をもたらす意思決定を行う上級管理職に対して建設的な監視を行うために充分な知識、技術および経験を有するべきである。業務上のディスラプションは組織内に広範な影響をもたらしうるという認識の下、組織内の関連するグループに適切な研修を提供することにより、健全なオペレーショナル・レジリエンス枠組みの実施は促進されうる。

34. オペレーショナル・レジリエンスに対する、様々な期間にわたる深刻だが起こりうるリスクを特定し、その影響を分析するための枠組みがないことで、保険会社の全体的なオペレーショナル・レジリエンスを強化する能力が制限される可能性がある。同様に、主要な業務上の機能、事業サービスおよび事業分野を支援する人材、プロセス、テクノロジー、設備および情報を特定するためのプロセスが現在の枠組みにないこともまた、全体的なレジリエンスに影響を与えうる。

35. こうした枠組みの実効性に不可欠なものは、深刻だが起こりうるシナリオに起因する業務上のディスラプションに対して、保険会社が対応し回復する能力の実効性をテストするためのリスクベースのプロセスである。

3.1.1 パンデミックから得られた教訓

36. IAIS によって実施されたステークホルダーとの外部アウトリーチによれば、強力で実効的なガバナンス枠組みを持つ保険会社は、パンデミックによってもたらされた業務上のディスラプションを防止、適応および対応し、さらに回復し教訓を得るために有利な立場にあった。これは、保険会社がこの時期に行った意思決定および活動の多くは行政のような外部当事者から義務付けられたものであることを考慮に入れている（すなわち、ロックダウンおよび在宅指示）。オペレーショナル・リスクを特定し、対応するための強力な枠組みを持つ保険会社は、実効的な BCP の活性化、サイバー・レジリエンスを達成し報告するための健全な枠組みの維持、および重要なサードパーティとの関係の適切なモニタリングからの恩恵を受けた。

37. 外部アウトリーチにより、保険会社内の委員会が組織内の異なる専門領域からの代表者を有することが、パンデミックによってもたらされた業務上のディスラプションを管理するための包括的なアプローチを促進するために役立つことが強調された。

3.1.2 監督上のアプローチ

38. 多くの監督当局は現在、健全なガバナンス枠組みと、レジリエンスに関する措置の取締役会・上級管理職による充分な監視、および業務上のディスラプションに関連したリスクを軽減するための戦略を、保険会社が有しているという保証を求めている。[13] 監督当局は、この文脈において、以下に関する理解を助けるために事業体から（全てまたは部分的に）情報を得ている：

- 取締役会および上級管理職が、保険会社のオペレーショナル・レジリエンスに対する脅威に対応するための適切な知識、技術、専門性および責任を有しているか；
- 業務上のディスラプションの管理に関する役割および責任が、充分に明確で文書化されているか；
- 財務および非財務のリソースが、オペレーショナル・レジリエンスのアプローチをするように適切に配分されているか；
- 事業体内の職能上のグループが、その役割と責任、およびその業務または活動が互いにどのように相互作用を持ち影響するかに関する理解を含めて、オペレーショナル・レジリエンスに対する事業体のアプローチの明確な理解と実践を共有しているか；
- ディスラプションの中でサードパーティである IT 委託先ベンダーが業務を遂行できない場合に保険会社が講じるリスク軽減戦略・措置が適切か；
- 適切な文書化と、適切な水準の承認が、ガバナンスプロセスに含まれているか；ならびに
- オペレーショナル・レジリエンスのプロセスの文書化が、定期的に見直され、更新されているか。

3.2 情報収集・共有

39. オペレーショナル・レジリエンスの監視に関する実効的な監督戦略を立案する際の、保険監督者に対する重要なインプットは、事業体のオペレーショナル・レジリエンス枠組みや、保険セクターに影響を与える潜在的な脅威に関するものを含む、広範な情報へのアクセスを有することである。

40. 一部の監督者は、このような情報を収集する目的で、事業体のオペレーショナル・レジリエンス枠組みの実効性を理解するために企業の取締役会および上級管理職と積極的に関わりを持っている。オープンで建設的なコミュニケーション・チャネルを維持することもまた、監督者と保険会社の双方がオペレーショナル・レジリエンスに関連する新たに発生した潜在的懸念事項を理解する助けとなりうる。

41. 保険監督者間と、より広範な保険セクター内での実効的な情報共有もまた、監督者によるオペレーショナル・レジリエンスの監視と保険会社によるオペレーショナル・レジリエンスの管理の強化に役立つかもしれない。例えばサイバー脅威は、進化し、現在では複数の管轄区域、セクターおよび業界を頻繁に攻撃し、保険会社のオペレーショナル・レジリエンスに影響を与えている。国際通貨基金（IMF）が指摘しているよ

[13] 以下は ORTF メンバーからの 2022 年 5 月の情報収集活動から引用されている。

うに、「攻撃者は国境を越えた協力において当局が追随することが困難なほどの敏捷性を発揮する」。[14]

3.2.1 パンデミックから得られた教訓

42. パンデミックにより、事業体のオペレーショナル・レジリエンスを支援するための実効的な情報共有および官民連携の重要性が実証された。例えばパンデミックの初期には、一部の監督当局は、リモート勤務を行う従業員数、サービスの利用可能性の指標、および、パンデミックに関連する増加するリスクを軽減するために役立つと思われる内部統制枠組みにおけるあらゆる変更について、保険会社から頻繁にアップデートを受けることで利益を得た。同様に、パンデミック時に増大するオペレーショナル・リスクを管理する上で役立つと保険セクターにおいて考えられているアプローチについて、監督者が情報を共有することができる事例もあった。

3.2.2 監督上のアプローチ

43. オペレーショナル・レジリエンスに関する情報を適時かつ継続的に交換するための定期的なフォーラムが整備されている管轄区域も存在する。これらのフォーラムにより、現在の状況、リスクまたは脅威の原因、軽減のための戦略および措置、発生した事象と得られた教訓について、議論を行うことが可能となる。その参加が監督当局のみに限定されているか、または保険セクターを含んでいるかによって、異なるアプローチが用いられる。こうした情報共有のためのフォーラムは、技術の不足／研修の必要性に対する解決策や、特に危機的な状況下でコミュニケーションおよび協調をより適切に促進するための検知や情報発信のためにテクノロジーをどのように利用しうるかについて、検討するためのプラットフォームを提供する場合もある。

オペレーショナル・レジリエンスに関する情報共有を促進するために創設されたフォーラムの例：

ドイツ連邦金融監督庁（BaFin）

BaFin は情報交換のためのプラットフォームを提供する委員会を整備している。委員会は、監督当局、会社および関連する協会の代表者を含む専門家パネルで構成されている。委員会は VAIT（BaFin によって提案された、サイバーセキュリティに関連するトピックスを含む、保険引受における IT のための監督上の要件）の導入において業界を支援し、またこのプラットフォームは、匿名の監督監査の結果を議論するためにも用いられる。

英国健全性監督機構（PRA）および金融行動監視機構（FCA）

クロスマーケット・オペレーショナル・レジリエンス・グループ（CMORG）が整備されており、オペレーショナル・レジリエンスに関するセクター全体での集団的活動を指揮している。グループは、リテール、ホールセール、金融市場インフラ（FMIs）、および保険業界だけでなく、金融当局および国家サイバーセキュリティ・センターにもまたがる約 25 名のメンバーから構成されている。グループは、PRA および UK Finance の上級管理職が共同議長を務めている。CMORG は 3 つの中核的な目的を有している。それらは以下である：

- 金融セクターのレジリエンスに対するリスクを特定すること；
- セクターのオペレーショナル・レジリエンスを向上するためのソリューションを策定すること；ならびに、
- 知識を共有すること。

[14] IMF スタッフ・ディスカッションノート、サイバーリスクと金融安定性—結局は小さな世界（2020 年）、8 頁

CMORG は専門家のサブ・グループによって支援されている。これらのサブ・グループは、セクターのためにオペレーショナル・レジリエンスの向上を設計、管理、実行する。これらのグループが実施する作業は自主的なものである。サブ・グループの議長は、CMORG の活動を議論し、さらなる協調の恩恵を受けうる領域を特定するために、定期的に会合を行っている。

44. 加えて、保険会社のオペレーショナル・レジリエンスに影響を与える事項に関するアップデートを公衆に開示すること、または監督者に直接報告することを求めている当局もある。こうした報告に基づいて、現在の状況、所見、およびテーマに沿ったレビューの報告書、ならびに保険会社のオペレーショナル・レジリエンスに関するベストプラクティスを公表する監督当局もある。

45. オペレーショナル・レジリエンスに関する監督枠組みについて、監督者は以下を含む広範な情報を収集する可能性がある：

- 深刻だが起こりうるシナリオが許容範囲にもたらす潜在的な影響についての事業体による評価を含む、保険会社による主要な業務上の機能、事業サービスおよび事業分野を特定するための枠組みおよび手法；
- サードパーティのサービスのディスラプションの場合の保険会社の業務に対する潜在的な影響を含む、保険会社の外部当事者への依存度；
- 重要なサービスを代替のベンダーに交代することの実行可能性、業務上の影響およびコスト、ならびに予測される課題についての、事業体による評価；
- 発生した業務上のインシデント（サイバーインシデントを含む）および得られた教訓；
- 脆弱性の特定を含む、ディスラプションが保険会社にもたらしうる業務上の影響についての評価、および、保険会社が影響を許容範囲内に留める能力についての保険会社によるテスト／自己評価；
- 深刻だが起こりうる広範なシナリオに対して、復旧活動の責任を負うチームの構成、および、重要な業務の復旧に要する時間；
- オペレーショナル・レジリエンスのベストプラクティスに関して行われた研修、および特に期待、ならびに機能が低下している期間における役割と責任についての報告；
- 保険会社とそのサードパーティ・サービスプロバイダーによって実施された共同の BCP テスト／評価についての報告；ならびに
- 必要な場合に、オペレーショナル・レジリエンスに関する潜在的なリスクおよび課題を取締役会および上級管理職に報告／エスカレーションするためのプロセス。

46. 保険監督当局間、保険セクター内、および当局と保険会社間でのオペレーショナル・レジリエンスに関する情報共有による利益はよく知られているが、こうした取組みは現在では限定的なようである。この関連で、監督カレッジは監督上の協力と情報共有のための枠組みを提供しうる。IAIS が特定した、実効的な情報共有に対する潜在的な障壁には以下が含まれる：

- 共通のタクソノミーが無いために、監督者が管轄区域を越えて実効的にコミュニケーションをとることが困難になり、オペレーショナル・レジリエンスの傾向、ギャップおよび機会についての集約的な見方を得ることも困難になる可能性；
- 事業体または管轄区域間での情報共有を制限または阻止する、データ保護およびプライバシーに関する法律（顧客保護のために整備されたもの等）についての懸念；

- 公式なクロスボーダーの情報共有活動を組織し実行することの複雑性とコスト；
- 監督当局がその法律上の義務により、関連する情報を獲得／共有することができないこと；ならびに
- 情報が企業の統制への追加的な監視または法的リスクにつながるかもしれないという懸念または認識によって生じる、監督者との情報共有に対する企業のためらい。

3.3 サイバー・レジリエンス

47. 保険会社はデジタルテクノロジーの利用に大きく依存しており、パンデミック時、事業体はリモート勤務に移行したためこの依存は加速した。その結果、保険会社が増大するサイバーリスクに耐え反応することができるサイバー・レジリエンスを達成するための健全な枠組みを事業体が整備していることへの注目が高まった。

48. FSB は、サイバー・レジリエンスを「サイバー上の脅威とその他の関連する環境上の変化を予測し、それに適応すること、および、サイバーインシデントに耐え、それを抑制し、迅速に回復することにより、組織がその使命を継続して果たす能力」と定義している。[15]近年、公的セクターと民間セクター双方の国際機関、国家的組織、業界団体がサイバー・レジリエンスに関連する複数の枠組みおよびガイダンスを策定・公表しており、実効的なサイバー・レジリエンス体制の原則に関する全般的な合意の形成につながっている。[16]2018 年に IAIS は、G-7 Fundamental Elements of Cyber Security for the Financial Sector を土台とした、保険会社のサイバーセキュリティの監督に関する適用文書を公表した。[17]この適用文書は、事業体が自社のサイバーセキュリティ戦略および運営の枠組みを設計および導入するための基礎的要素（building blocks）を提示している。

49. 監督者にとっての主要な課題は、比例的かつリソースを効果的に用いた方法（a proportionate and resource effective way）で、保険会社がサイバー・レジリエンスを達成するために確立した枠組みが実効的かつ堅固であるという安心を、どのようにして得るかということである。とりわけ課題となるものとしては、サイバーリスクが絶えず進化し拡大しているために、事業体／セクターのサイバー・レジリエンスに対する潜在的な脅威について先を見越した予測を体系的に行うことが困難であること、またこのことから、広く合意され、標準化された、先を見越した指標が完全には開発されていないという問題がある。このことは、サイバー攻撃に起因して起こりうる将来的なディスラプションに対する事業体の脆弱性を監督者が評価する能力に課題を提示している。

50. 保険業界の外部の専門家と行った直接的な意見交換により、サイバー・レジリエンスの監督に対して画一的なアプローチを規定することは適切ではない一方で、監督上の調整を拡大することは有益となりうることが明らかになった。特に、参加者はサイバー・レジリエンスのテスト要件を相互に認識していないことは、国際的に活動する保険会社に対する要件の重複または不整合につながりうると指摘した。

51. さらに、保険会社のサイバー・レジリエンスを達成するための枠組みを評価するためのアプローチに一貫性がないことは、サイバー上の脆弱性が検知されずに、保険会社の安定性と完全性が脅かされ、より広範な金融セクターへ波及するリスクをもたらすことにつながりうる。保険会社のサイバー・レジリエンスを評価するためのベストプラクティスに関するより大きな合意がない場合には、監督当局間でのアプローチの相互認識と情報共有は困難なままである。この点については EU の TIBER (Threat Intelligence Based Ethical Red Teaming)枠組み（セクション 3.3.2 を参照）のような、一定の進展もみられる。

52. 以下は、サイバー・レジリエンスを達成するために保険会社が確立した枠組みの質を監督者が評価する際に直面する 2 つの主要な課題をさらに詳しく示している。

---

[15] FSB、サイバー用語集（2018 年）

[16] FSB、サイバーセキュリティにおける規制・ガイダンス・監督上の慣行に関するストックテイク報告書（2017 年）

[17] G7 の金融セクターのサイバーセキュリティに関する基礎的要素および金融セクターのサイバーセキュリティの効果的な評価に関する基礎的要素を参照。

3.3.1　サイバー・レジリエンスを評価するためのアプローチの整合性

53. 監督者にとっての主要な課題は、サイバー攻撃の変化する性質と事業体が新たなテクノロジーを採用するスピードの双方についていくことができる、サイバー・レジリエンスのモニタリングのための最も実効的なツールおよびアプローチを特定することである。テスト形式や監査のような、最も一般的に用いられている監督手法の一部は、特定の時点での保険会社のサイバー・レジリエンスについて価値あるスナップショットを提供する。しかしながら、絶えず進化する・新たに発生したサイバーセキュリティ上の検討事項が、事業体のすべてのプロセスに完全に一体化され、その全体的な情報通信テクノロジー（ICT）のライフサイクルに組み込まれることを確保することは監督者にとって困難である。

54. 現在、監督者はモニタリングに関して幅広いアプローチを展開している。例えば監督者は、保険会社が定期的に（多くの場合、年次で）社内のサイバーセキュリティのテスト、評価または監査を実施することを求めるかもしれない。これには、保険会社のサイバー・レジリエンスを達成するための枠組みの有効性、システム、および統制の実効性の分析、ならびに主要な機能、事業サービスおよび事業分野を支援するためのスキルを備えたリソースの利用可能性についての分析も含まれるかもしれない。保険会社はさらに、これらの評価の結果を監督者に報告し、特定された脆弱性または誤りを是正することが求められるかもしれない。

55. 保険会社のサイバー・レジリエンスを評価するための整合的なされたアプローチを有することは、特に保険会社が、管轄区域を越えて事業活動を行うサードパーティ・サービスプロバイダー（例えばクラウド）と関わりを持つ際に有用となりうる。保険会社のサイバー・レジリエンスを評価するための監督上のアプローチの例には、報告されたインシデントの分析、質問状、立ち入り検査および継続的な監督上の関与が含まれる。国際決済銀行（BIS）は、これらの実務では「財務リスクに匹敵する定量的な指標やリスク指標、例えば標準化された定量的な指標を生み出すことはほとんどない」と特定している。[18]

56. 限定的ではあるものの、定量的な指標が現在でも存在している場合には、それらは保険会社のサイバー・レジリエンスを達成するための枠組みの各部分を評価するうえで有用となり得ると当局は指摘する。指標およびデータは、固有リスクおよび残余リスク、リスク管理枠組みの成熟度、ならびに潜在的な集中によって生じるリスクの特定を監督者が理解することを支援しうる。いくつかの管轄区域では、フォワードルッキングな指標を含むより多くの指標を開発するための作業が行われており、他のセクターでの進捗を活用できる可能性がある。一般的に利用可能な指標には以下が含まれる：

    - 利用可能性―1か月のうちでサービス／ソフトウェアが利用可能な時間の割合として測定される（すなわち、1か月の利用可能性 99.9%）。
    - 目標復旧時間（RTO）－サービスの中断からサービスの復旧までの間の許容可能な最長遅延時間を指す。これは、サービスが利用不可能となる許容可能な期間を決定する。
    - 目標復旧時点－最後のデータ修復時点からの許容可能な最長時間を指す。これは、最後のデータ修復時点からサービスの中断までの間の許容可能なデータ損失を決定する。

3.3.2　サイバーの専門知識の供給

57. 多くの監督当局は、技術の不足により、サイバー・レジリエンスの監視プログラムの開発の課題に直面している。サイバー・レジリエンスを評価するために求められる技

[18] BCBS、サイバー・レジリエンス―多様な実務（2018年）

術は需要が高く、適切に資格を満たすスタッフは著しく不足している。このことは、サイバー・レジリエンスの分野において、固有の技術および専門性を必要とする特定の領域が存在し、これらの専門技術に対する需要が供給を上回っていることにより悪化している。

58. 英国の労働市場におけるサイバーセキュリティの技能に関する報告書は、「英国内の事業のうち大きな割合が、そのサイバーセキュリティを管理するために必要な専門的技能、インシデント対応の技能およびガバナンスの技能を有するスタッフを依然として欠いている」と推定している。[19]このことは、監督当局および企業が同様に技術のあるスタッフを求めてセクターをまたいで競い合っており、専門家を集め雇うことの困難さを高めていることを浮き彫りにする。

59. 技術不足による結果の一つは、サイバー・レジリエンスに対する監督枠組みの発展がサイバー攻撃のますますの高度化に後れを取るかもしれないということである。監督当局は、既存のスタッフへの内部の研修の展開、認証プログラムの創設、および国家のサイバーセキュリティ当局間での知識共有の促進を含めて、サイバーの専門家の雇い入れと保持を強化するために多様なツールを展開していると述べている。

3.3.3 パンデミックから得られた教訓

60. サイバーリスクの動的な性質は、パンデミック時に前面に押し出された。多くの管轄区域が、高度で攻撃的なランサムウェア攻撃の著しい増加を経験した。同時に、リモート勤務を促進するためのリモートアクセス・テクノロジーの利用の増加により、IT システムに新たな脆弱性が露呈した。リモート勤務の促進のために、保険会社が急速に大規模な IT トランスフォーメーション・プログラムを必要としたことで、この脅威は増幅された。こうしたトランスフォーメーションはそれ自体がディスラプションの原因となる可能性がある。旧来の IT システムから新たなテクノロジーへの大規模で複雑な転換は必然的にアタックサーフェスを拡大し、そのため、適切に管理されず充分にテストが行われなかった場合には、保険会社のサイバーリスクへのエクスポージャーを増加させる可能性が高い。外部の専門家との協議からのフィードバックに基づけば、脅威者が事業体の脆弱性に付け込むために人工知能のような新たな形態のテクノロジーを利用することから、多くの専門家は、サイバー攻撃の複雑性が今後、高まる可能性が高いことに同意している。

システミックなサイバー攻撃の事例：Log4j の脆弱性

Log4j はインターネット上のアプリケーションおよびサービスが利用しているオープンソースのログ記録ライブラリである。Log4j の最近発見された脆弱性は、保険会社がそのサプライチェーン上で修正しなければ、サイバー犯罪者またはハッカーがシステムに侵入し、パスワードとログイン情報を盗み、データを引き出し、ネットワークを悪意のあるソフトウェアに感染させることを許す可能性がある。米国と欧州の当局は、その他の管轄区域とともに、最近この困難な脅威に対応している。米国サイバーセキュリティ・インフラストラクチャセキュリティ庁は、リスク軽減のためのツールおよびリンク、ならびに企業ネットワーク内の脆弱性の特定に役立つユーティリティへのリンクを含めた、企業が事象に対応するうえで役立つ情報を広く配布した。欧州レベルでは、この不具合がもたらす潜在的な波及効果は十分に重要であると考えられ、異なる当局間で調整された情報交換が行われた。

[19] イプソス報告書

3.3.4 監督上のアプローチ

61. IAIS の管轄区域が採用したサイバー・レジリエンスを向上するためのアプローチの一部の例を以下に概説する：

欧州連合（EU）2018 年 TIBER-EU

欧州連合内では、TIBER-EU (Threat Intelligence Based Ethical Red Teaming)の枠組みが開発されている。TIBER-EU のガイドラインに基づき、各国が独自に導入している。様々な EU 加盟国がこれまでに TIBER 枠組みを導入している。TIBER-EU およびその国家的導入は、テスト要件の調整と相互認識を確保するために役立つ。また、EU デジタル・オペレーショナル・レジリエンス法（DORA）は IT のオペレーショナル・レジリエンス・テストのための欧州の共有された原則を確立することをねらいとしている。

英国 CBEST

英国 CBEST はサイバー攻撃のシミュレーションを用いて規制者が事業体と協力するための枠組みを提供する。これにより、事業体のサイバーセキュリティ統制上の人材、プロセスおよびテクノロジーに対する攻撃の影響を、事業体が検討することができる。CBEST のねらいは、事業体の防衛力をテストし、その脅威インテリジェンス能力を評価し、外部および内部に端を発する広範なサイバー攻撃を事業体が検知・対応する能力を評価することである。英国当局は、現在のサイバー上の脅威に基づいて模擬攻撃を実施している。これらには、脅威者が事業体に攻撃するために取りうるアプローチ、および、事業体のオンライン情報を悪用する方法などが含まれている。認可を受けたサービスプロバイダーが、法的、倫理的、道徳的制約の中でシミュレーションを実施する。活動の目的は、事業体の重要な事業サービスを遂行するシステムおよびプロセスの守秘義務、誠実性および／または利用可能性が損なわれうるかを評価することである。

机上演習

全米保険監督官協会（NAIC）は、財務省の「ハミルトン」プログラムの支援のもと、米国の各州および連邦の監督者、法執行機関および当局者と協力して、サイバーインシデントへの対応と復旧を検討するための保険会社および監督者との机上演習を促進している。これは、潜在的な脅威に対する早期／事後の対応を支援する主要な手法を議論することにより、保険会社および監督者のサイバー対応プログラムを強化することをねらいとしている。これらの演習は、監督者および保険業界がこれらのインシデントに実効的に対応する能力をテストするための有用な手段である。演習はサイバーセキュリティ事象（すなわち、ランサムウェア、インサイダー脅威等）を模して行われ、サイバーインシデントが保険会社や保険セクター全体に与える可能性のある影響について参加者間で対話を実施する。これらの演習は、ステークホルダーが、事象が発生した際のコミュニケーションへの期待を明確化するうえで役立ち、選択したリスク軽減実務の重要性を強調するための機会を監督者にもたらす。

62. 加えて、サイバー・レジリエンスを達成するための保険会社の枠組みの質を評価するための以下のツールおよびテクニックが（単独で、または組合せで）監督者によって用いられている：

- 自己評価の質問状—保険会社がサイバー・レジリエンスを達成するためのその枠組みの質の自己評価を実施することを伴っており、その回答は事業体のサイバー・レジリエンス能力および脆弱性のスナップショットを提供する。
- 脆弱性評価—悪用可能な既知の脆弱性を点検する自動スキャンによってシステムおよびプロセスのセキュリティの脆弱性を特定・評価し、最終的にはリスク・エクスポージャーに関する報告を行うことをねらいとする。テストは一般に定期的に行われる（オンサイトまたはオフサイトの評価の際に実施されるかもしれない）が、その頻度は、問題となるシステムおよびプロセスの性質によって異なる可能性がある。
- サイバーインシデント報告—監督当局に対するミクロレベルのデータの報告は、特に報告要件が標準化されている場合に、より広範なシステミックな脅威の概観を形成するうえで役立ちうる。
- シナリオベースのテスト—深刻だが起こりうるサイバー攻撃のシミュレーションを含む、広範なシナリオに対する事業体のサイバー・レジリエンスをテストする。これにより、企業は、検知、対応、復旧、および関連するガバナンスの取り決めやコミュニケーション計画に組み込まれた仮定を試行することができる。シナリオベースのテストは、机上演習またはシミュレーションの形をとりうる。
- レッドチーム演習—管理された環境で敵の視点を導入するためにレッドチームを使用し、内部および外部の依存関係に挑戦する事業体を含む—。レッドチームは、事業体の緩和制御における、可能性のある脆弱性と実効性をテストするために役立つ。レッドチームは、保険会社自身の従業員および／または外部の専門家（いずれの場合もテストされる部門から独立した者）から構成されるかもしれない。
- 脅威ベースのペネトレーションテスト—G7 は「コントロール下において、実在の攻撃者の戦術、テクニック、手順をまねることにより、金融機関のサイバー・レジリエンスを侵害しようとする試みである。これは、特定の脅威情報（threat intelligence）に基づき、金融機関の職員、プロセス、テクノロジーに焦点を当て、予見や業務への影響を最小限に抑えたものである」と定義している。[20]

3.4 IT のサードパーティへの外部委託

63. 保険会社が事業プロセスまたは機能の外部委託に関連するオペレーショナル・リスクを特定する具体的な要件が、多くの規制枠組みに含まれている。その結果、適用可能なリスク管理プロセスが一般に保険会社によって実施されている。しかしながら、監督上の要件と保険会社のリスク管理プロセスの双方の発展が進んでいない領域は、サードパーティ・サービスプロバイダーによる企業への不可欠な IT サービスの提供に関連した、集中によって生じるリスクの継続的な管理である。

64. 集中によって生じるリスクはいくつかの異なるレベルで生じる可能性がある：

- 多くの企業が特定のサービスについて一社または数社のサービスプロバイダーを利用する、一つもしくは複数の管轄区域の、保険セクターもしくはより広範な金融サービスセクター全体；
- 複数の事業体もしくは部門が、同一もしくはいくつかの、内部もしくは外部のサービスプロバイダーが提供するサービスに依存している、より大規模な保険会社またはグループ；
- サードパーティ・サービスプロバイダーが利用する下請け業者；および／または
- グローバルなレベル、または多くのサードパーティ・サービスプロバイダーおよび／もしくは下請け業者が所在する地域レベル。

[20] G7、脅威ベースのペネトレーションテストに関する基礎的要素

65. サードパーティのサービスの規模、種類および重要性に応じて、集中によって生じるリスクがシステミックとなる可能性が理論上は存在するかもしれず、そのため、金融機関によるリスク管理のみならず、集中によって生じるサードパーティリスクの監督の枠組みおよび実務を発展させることが重要である。

66. サードパーティ・サービスプロバイダーは世界中で、異なるセクターにまたがって営業することが多い。これらのサードパーティ・サービスプロバイダーに由来する集中によって生じるリスクへの対応は、業界と複数国の監督者、およびサードパーティ・サービスプロバイダーの間での調整されたアプローチを必要とするだろう。

67. 特にテクノロジーの利用に関連して、（保険を含む）金融セクターの複雑性が増大しているために、パンデミック時を含む過去数年にわたって集中によって生じるサードパーティリスクは増加している。[21]規制対象でない下請け業者の利用と、重要なサービスを提供するための複雑なサプライチェーンへの依存度の高まりも、過去数年間は明白になっており、このことはリスクを規制の範囲から外れさせる可能性がある。[22]

68. サードパーティサービスの利用による利益には、イノベーションの加速、顧客にもたらされる結果の向上、コストの削減、拡張性、およびオペレーショナル・レジリエンスの向上が含まれる。しかしながら、これらの利益は、重要なサービスを外部委託することで個々の保険会社、より広範な市場、そして金融安定全体にもたらされるリスクと天秤にかけられるべきである。とはいえ、集中によって生じるリスクは市場における競争の不在や代替性の欠如から頻繁に生じるため、保険会社がこのリスクの性質に単独で対応する能力は限定的かもしれない。[23]

69. クラウドの利用は、個々の事業体、セクターおよびグローバルなレベルで集中によって生じるリスクをもたらすかもしれないサードパーティの IT サービスの一例である。[24]クラウドのディスラプション、またはクラウドに保管された情報への不適切なアクセスは、業界にまたがる広範なシステム上のディスラプションにつながりうる。集中によって生じるリスクをもたらすかもしれない、保険会社が利用することが多いサードパーティのサービスのその他の例には、年金支払・給付管理プロセス、投資運用、請求処理および顧客からの問い合わせの処理が含まれる。保険金請求の管理と損害査定プロセスもまた、サービスの提供に求められる専門性の高さから、集中によって生じるリスクが存在する典型的な非 IT 分野の例である。

3.4.1 パンデミックから得られた教訓

70. 保険セクターによるパンデミックへの対応は、サードパーティ・サービスプロバイダーおよび委託業者がどのように保険会社のレジリエンスの向上に貢献することができるかを明らかにした。実効的かつ適時にリモートワークに移行できたのは、多くの場合、IT サービスプロバイダーの利用によるものだった。これらのプロバイダーはまた、金融機関が顧客にサービスを提供し、より広範な経済における他のセクターを支援する能力にも貢献した。

71. パンデミックはまた、保険会社のデジタル・トランスフォーメーション計画の進展にも刺激を与えた。サードパーティは、より安全性が高く、レジリエンスがあり、かつ、旧来のシステムに依存する場合がある金融機関自身の既存のテクノロジー・ソリューションよりも柔軟性があるような、テクノロジー・ソリューションを提供する能力を有していると考えられることが多かった。

---

[21] FSB、アウトソーシング・サードパーティに関する規制・監督上の論点（2020 年）

[22] 例えば、アーンスト・アンド・ヤング、パブリック・クラウドの導入により保険会社はどのように変化しうるか（2021 年）を参照。

[23] 例えば、アクセンチュア、クラウドによる保険会社に対する 5 つの利益（2019 年）を参照。

[24] 米国財務省、金融サービスセクターによるクラウドサービスの採用、セクション 6.4

72. とはいえ、パンデミックはまた地理的集中に関連するリスクも浮き彫りにした。これは同一の地理的領域内で多数の契約を締結している事業体に関連しており、サービスの提供について当該領域内で単一または二、三のプロバイダーに依存することにつながる。こうした状況は特に、低コストの管轄区域にサービスセンターを有する大規模な保険グループに当てはまるかもしれない。

3.4.2 監督上のアプローチ

73. 集中によって生じるリスクを検討するための要件は管轄区域間で異なる。多くの場合、保険会社はサービスプロバイダーの最初の選定時に集中によって生じるリスクを検討することを求められるが、継続中のモニタリングおよびリスク評価のプロセスの中でこのリスクの検討が求められる保険会社も、少数だが存在する。

74. 複数の管轄区域にまたがる複数の金融機関に対して同一のサードパーティ・サービスプロバイダーが提供するサービスについて単一の事業体が有する視認性は限定的であることから、既存の金融監督枠組みにはサードパーティおよび委託業者によってもたらされるシステミックリスクの特定と管理について本質的な制約がある。このことは、大規模で支配的なサービスプロバイダーに対して単一の金融機関が有する影響力が限定的であることによって悪化するかもしれない。こうした制約は、外部委託されたサービスプロバイダーの内部で生じた保険会社のサイバー・レジリエンスおよび BCM に対するリスクを保険会社が軽減する能力にさらに影響を与える。

75. 加えて、規制の範囲外にとどまっているサードパーティ・サービスプロバイダーもいるため、監督当局が保険会社によって提供されるサービスのレジリエンスを直接的にモニター、管理する能力も限定的である。

76. 伝統的な監督上のアプローチは、サードパーティのサービスおよび外部委託に関連するリスクの管理について保険会社の要件と期待を定義する監督当局に依存している。しかしながら、個々の事業体には、集中によって生じるシステミックリスクを実効的に評価・管理する能力について本質的な制約があり、規制の範囲外にとどまっているサービスプロバイダーもいることから、監督当局の影響力もまた限定的である。

77. 多くの監督当局は、サードパーティに委託されたサービスについての情報を提供することを保険会社に求めているか、求める予定である。こうした情報収集により、監督当局は将来的に、例えば、情報収集活動の進展に伴ってより正確に集中によって生じるリスクを特定することができる可能性がある。とはいえ、収集された情報をより有用にするために、報告の定義と要件の整合性について改善が必要である。特定の管轄区域はサードパーティ・サービスプロバイダーについての法令および／または指針を推進しており、その例には EU の DORA や英国大蔵省の政策綱領が含まれる。

78. 集中によって生じるリスクはまた、マルチクラウド／マルチベンダー・アプローチおよび出口戦略／ポータビリティ戦略の導入のような、新たなリスク管理実務を通じても部分的に対応することができる。それでも、こうした解決策の採用に関連してコストや業務上の複雑性が生じる可能性もある。

3.5 事業継続管理

79. 保険セクターは、多様なシステム、参加者およびサービスプロバイダーの間の多くの相互連関性および相互依存性から成り立っている。保険会社またはそのあらゆるサービスプロバイダーの活動における業務上のディスラプション、悪化または中断は、その被保険者および他のパートナーに対するコミットメントを果たす能力を脅かしうる。これらの相互連関性および相互依存性、ならびにセクターの複雑な機能を踏まえて、保険会社が、業務上のインシデントの際の事業継続性を確保するために健全かつ慎重な経営実務を採用することは不可欠である。

80. BCM は、自然災害、停電、通信障害、コンピュータの故障、データ漏洩、テロリズムおよびパンデミックのような、保険会社の重要な活動に脅威を及ぼす可能性が高い主要な業務上の事象の特定から始まる。特定プロセスは、事業体の業務に対する業務上のインシデントの影響を保険会社が評価することができるようにし、重要な事業活動の継続性を確保するための必要な軽減措置を実施するための、最初の重要なステップである。

81. 健全な BCM 枠組みには一般に、確立された事業継続計画、明確な責任を負った熱心で競争力のある人材、ならびに、計画、実施、テスト、実績評価、レビューおよび継続中の改善に関連した多様な管理プロセスが含まれる。保険会社はその計画に基づき、ディスラプションに対応し、商品およびサービスの納品または提供を再開および／または復旧する。講じられる措置は、事業体の事業継続の目標ならびに、ディスラプション後に保険会社が受容しうる、または受容しない可能性があるリスクの量および種類と整合的であるべきである。

82. 健全な BCM 枠組みは、保険会社がディスラプション時の業務遂行能力を確保するために役立つ。それにより、保険会社が戦略目標の達成に貢献することが可能になり、保険会社の信頼性と評判を保護および強化する。それは、関連当事者の期待を考慮に入れ、保険会社が成功する能力に対する彼らの信頼を構築しながら、ディスラプションの間も実効的であり続けるための能力を向上させ、ディスラプションの直接的・間接的なコストを削減することのために役立つ。

83. BCM のベストプラクティスは、変化する運営環境に沿って、またパンデミックへの対応として発展している。BCM の以下の側面は、IAIS によるさらなる分析および／または監督当局間の協調から恩恵を受ける可能性がある課題として認められている：

BCM とリスク管理の統合

84. 業務上のディスラプションが増加するなかで、オペレーショナル・レジリエンスの概念は実効的なリスク管理の主要な成果として浮上してきた。その結果、健全な BCM の確立から、BCM 実務の、他の関連するリスク関連実務への統合と機関の全体的なオペレーショナル・レジリエンスへの整合化に焦点が移っている。例えば、保険会社の重要な業務およびあらゆる主要な内部／外部依存性（サードパーティの BCP を含む）の文脈の中で、保険会社がどのように BCM を検討する必要がありうるかの検討に価値があるかもしれない。BCM と全体的なオペレーショナル・レジリエンスの間のつながりは、サードパーティのリスク管理と同様に、保険会社がその BCM 枠組みから追加的な恩恵を受けることができるようにする可能性がある。BCM 枠組みがサイロ化されている場合、特にサードパーティおよび／または外部委託取決めによって提供される IT サービスに関しては、これは恐らく事業継続性に対する阻害要因となる。

BCM 枠組みの範囲の拡大とテスト

85. BCM が過去に考えられていたよりも広範な事象および事業運営を含むようにどのように拡大されうるかについての検討に価値がある可能性もある。例えば、ビジネス・インパクト分析（BIA）およびリスク評価が実施される際には、BCP における利用可能性の検討の必要性が、重要な事業サービスのための情報の信頼性と完全性の損失による結果の検討にまで拡大される可能性がある（情報セキュリティ／サイバー予防は、より広範な BCP と統合的リスク管理（ERM）に統合される可能性がある）。BCP はまた、保険会社が多くの従業員または主要な人員の損失にどのように対応するかについても検討する可能性がある。

「ニュー・ノーマル」での BCM の適応

86. パンデミック以前は、多くの機関の事業継続戦略は短期的な影響シナリオへの対応に焦点を当てていた。パンデミック時に不充分と認められた継続性の仮定は、その BIA の結果および各保険会社の必要性とリソースに応じて、多くの事業継続戦略において、

一部の既存のプロセスの重要性の見直しと異なる時間軸（例えば、即時、短期、中期および長期）の採用につながっている。IMF によれば、「金融規制主体および会社は、古典的な事業継続計画および災害復旧計画から、攻撃によって通常の業務へのディスラプションが起きても重要なサービスを継続することへ、焦点を移す必要がある。レジリエンスには、企業および金融規制主体の指導者、ならびにその取締役会メンバーからの賛同が必要である。会社は、システミックな影響をもたらしうる深刻だが起こりうるインシデントに備える必要がある。監督者は、不利なシナリオを検討し、個別と全体の双方でその危機管理計画をテストするように、業界に対して求めるべきである。」[25]

87. ハイブリッドな就労制度はより恒久的な特徴となるかもしれないが、実務上ではリモート勤務方針は企業ごとに大きく異なる可能性がある。様々な理由から、スタッフが家で勤務することができる時間の量を制限する取決めを検討している企業もあるかもしれない。管轄区域の法的枠組みを満たすために、やがて導入されることになる就労制度に応じて、雇用契約の調整の可能性が予見されうる。

88. このことは、既存の（パンデミック以前に用意された）または最近改定された BCP が変わらず目的に適合しているか、または大きな追加的改定を必要としているかについて問題を提起している。その結果、監督者が事業継続戦略の変更によって発生したリスクをどのように管理すればよいか、ならびに、新たな就労制度が発展し続ける中で保険会社がこれらのリスクを特定、分析および集約するための手続きを実施しているかどうかを検討することは価値があるかもしれない。

3.5.1 パンデミックから得られた教訓

89. 過去数年における以下の進展は、保険会社が健全な BCM 枠組みを整備していることの重要性の向上に貢献している：

- 保険会社内およびセクターをまたいだデジタル・トランスフォーメーション、およびその結果としての保険会社の重要な活動およびプロセスに対する変更；
- 多くの従業員が家から勤務する、「どこからでも」勤務する、またはハイブリッド（家とオフィスの組み合わせ）環境で勤務する、「再設計された」職場；
- 一時的なディスラプションへの短期的な注目から、多様な時間軸（例えば、即時、短期、中期および長期）にわたる事業のレジリエンスの検討への移行；
- 回復までの時間と回復の水準に関する、また保険会社からの実効的なコミュニケーション—すなわち、ディスラプションの発生、回復の進展、および、顧客が引き続きサービスを受けられることを確保するための軽減措置、およびサービスが回復した際の通知—についての顧客の期待の高まり；
- それぞれの水準のサイバー／事業継続リスクおよび多様な BCM 枠組みを有する、複数のサードパーティおよび下請け業者の利用；ならびに
- サイバー攻撃への脆弱性を含む、脆弱性の増加。

90. 外部の専門家との方向性を持った協議に基づけば、これらの進展はパンデミックと同時に発生しているものの、これらのテーマはパンデミック以前にも存在していた。しかしながら、これらの進展の多くはパンデミックの経験からより急速に重要性を増したことが一般に認識されていた。

[25] IMF、サイバー脅威に立ち向かうことは、金融機関のより優れた保護措置の緊急の必要性を意味する（2022 年）

3.5.2 監督上のアプローチ

91. 監督者は、BCM に関連して、変化したリスク環境に対応するための措置を講じている。政策および／または監督上の作業（オンサイトおよびオフサイトの調査を含む）は、以下を含む広範な領域に焦点を当てているが、それらに限定されない：

- パンデミック時と、保険会社のハイブリッド勤務環境への転換に伴って発生したリスクに基づく BCP の改善；
- トップの姿勢の設定、BCM に関する戦略的な方向性の設定およびそのオペレーショナル・レジリエンスのための実行、ならびにリスク許容度に関するステートメントの策定のための、取締役会および上級管理職による支援の重要性；
- 相互に連関する部門に関連した事業継続リスクを特定し、縦割りを最小化するための、事業部門間での BCM システム要件の統合；
- 重要な事業サービスに関する完全な知識および、戦略的投資決定と日々の事業運営の間の重要な相互連関性に関する完全な知識の確保に役立てるための、脆弱性評価の幅広さと頻度の向上；
- データのバックアップ、深刻だが起こりうるシナリオの利用、災害復旧枠組み、およびテスト結果から得られた教訓を取り入れることを含む、BCP の堅固で定期的なテスト；
- 適切なコミュニケーションおよび危機管理の能力；
- BCM に対する期待を、保険会社における外部委託ソリューションにまで拡大すること；
- BCM が動的なリスク管理ツールであるようにするための、BCM プロセス全体の定期的な見直し；ならびに
- BCM に関する継続中の発展／リスクについて議論するための事業体との定期的なタッチポイント。

4　見解の総括および可能性のある IAIS の将来の焦点領域

92. 以下のセクションは—本文書で議論された見解に基づいて—サイバー・レジリエンス、IT のサードパーティへの外部委託および BCM に関連するリスクの多くの主要な側面を総括し、IAIS と保険監督者による将来の検討または更なる分析の恩恵を受ける可能性がある多様なトピックスを概説している。

情報共有

93. 情報共有のためのメカニズムを促進すること、または既存の情報共有メカニズムを活用することにより、新たに発生したリスクについて保険セクターと保険監督者に新たな理解がもたらされ、業務上のインシデントとシステミックリスクを集合的に検知し対応する能力の向上を含めて、軽減戦略および軽減措置の開発に情報が提供されるかもしれない。これには、サイバー・レジリエンス、IT のサードパーティへの外部委託および BCM に関連する幅広い課題についてのベストプラクティスに関する情報共有が含まれうる。この目的のために活用されうる、情報共有のための既存の IAIS のメカニズムが存在するかもしれない。

94. 保険会社間と監督者間、およびより広範な保険セクター全体での情報共有を促進するために、オペレーショナル・レジリエンスに関連する定義および専門用語をどのようにしてより適切に擦り合わせることができるかを検討することが有用となりうる。このことは、異なる概念を指す同一の用語を意図せず用いること、または異なる用語を用いることを最低限に抑えるために役立ちうる。このことはまた、関連する課題を議論・理解するためのより整合的なアプローチの開発において、管轄区域を支援するかもしれない。

95. 本セクションの残りの部分は、サイバー・レジリエンス、IT のサードパーティへの外部委託および BCM の各領域について、更なる情報共有および検討の恩恵を受ける可能性がある主要なトピックスの具体例を示している。

サイバー・レジリエンス

96. セクション 3.3 で概説された見解に基づけば、更なる検討から恩恵を受ける可能性があるサイバー・レジリエンスに関連する領域には、以下が含まれる：

- 保険会社のサイバー・レジリエンスを達成するための枠組みの品質を評価するための指標とツール、および新たな、または発展しているテクノロジーの利用に関連する新たなサイバーリスクについての議論。これはまた、保険セクターのサイバーインシデントの報告に関する実務と発展についての情報の共有にも役立つように拡大されうる。こうした情報の共有は、脅威者が利用する最新のアプローチ、およびサイバーリスク・インシデントの適時の検知と対応を促進する新たに発生したテクノロジーまたはツールのような、急速に変化するサイバーリスクの状況について、保険セクターが最新情報を入手することを支援する可能性がある。
- 保険会社が、クラウド・コンピューティングのような新たなテクノロジーをますます利用していることに伴う、サイバー・レジリエンスに対する大規模な IT トランスフォーメーションの影響の分析。
- 保険会社のサイバー・レジリエンスを達成するための枠組みの、開発、監督上の評価、および実施のための積極的、整合的かつ比例的なアプローチ（consistent and proportionate approaches）、ならびに、保険会社がサイバーインシデントを保険監督者にエスカレーションするためのアプローチの開発。後者は、「サイバーインシデント報告—既存のアプローチとより広い範囲での収斂に向けた今後のステップ」についての FSB の作業[26]を、保険会社についての追加的な検討とともに

[26] FSB、サイバーインシデント報告—既存のアプローチとより広い範囲での収斂に向けた今後のステップ（2021 年）

活用する可能性がある。この提案はまた、欧州システミックリスク理事会（ESRB）からの、サイバーインシデントに対する各国の対応を調整するための専用メカニズムの創設の要求とも整合的であるかもしれない。[27]

IT のサードパーティへの外部委託

97. セクション 3.4 で概説された見解に基づけば、更なる検討から恩恵を受ける可能性がある領域には、以下が含まれる：

- 集中によって生じるクロスボーダーなリスクの特定における監督者間の国際的な協力を向上する目的で、可能な限り、（例えば、重要なサービス、外部委託、サードパーティ等といった）IT のサードパーティへの外部委託に関連する用語の報告上の定義と要件を調整すること。[28]
- 以下を含む、監督者が用いる実務および手法に関する情報を交換すること：
  - 特に回復活動に関して、集中から生じるリスクがサイバー・レジリエンスと BCM 枠組みに与える影響。これは特に、複数の保険会社がその顧客とその他のステークホルダーへの事業とサービスを継続する能力を妨げる可能性がある、広く利用されるサービスプロバイダーから発生したインシデントの潜在的な影響を軽減するために重要である。
  - 業界内で広く利用される重要なサードパーティを特定するために役立つ、各管轄区域内のサードパーティ・サービスプロバイダーの一覧を開発するための監督上のアプローチ；
  - 「IT のサードパーティリスクおよび外部委託」の管理から、システミックな依存性全般およびあらゆる外部委託取決めとサードパーティ取決めから生じるリスクの検討（依存性管理）への、焦点のシフトに関するアプローチ；
  - サービスおよびリソースの相互連関性と相互依存性のマッピングを可能にすることを目的とした、重要な活動（および重要となりうる活動）を構成する要素の特定、および、こうした活動の利用者の特定のための指針。こうしたマッピング活動の開発は現在、一部の管轄区域の監督当局間で議論されている。
- 大規模な保険会社がマルチベンダー戦略とプロバイダー間のデータポータビリティの取決めと環境の導入を検討することによる影響を調査すること。しかしながら、これらは特により小規模の事業体に対しては複雑でコストのかかるツールであることが認識されている。

事業継続管理

98. ICPs は、保険会社の事業のレジリエンスの確保に関連したプロセスおよび活動を支援するハイレベルな原則を設定しており、これは健全な BCM を幅広く支援する。それでもなお、事業のレジリエンスと BCM の関連を明らかにすることは、BCM の概念が短期的なディスラプションに関するものに留まらない議論にまで拡大されることが確実に理解されるようにするために有用であるかもしれない。

99. 以下を含む、ベストプラクティスおよび監督者が用いる手法についての情報の交換にも価値があるかもしれない：

- 特に、縦割りを排除し、サイバーリスクと IT のサードパーティへの外部委託リスクに起因するディスラプションの影響を BCM 枠組みが考慮していることを確保するために、BCM を他の関連するリスク管理機能に継続的に統合する必要性に

[27] ESRB、システミックなサイバーリスクの軽減（2022 年）

[28] FSB、外部委託およびサードパーティとの関係に関する規制上および監督上の課題：ディスカッション・ペーパー（2020 年）。IAIS はこの領域において、FSB による継続中のセクターをまたいだ作業に関与している。

関して、セクターが BCM のベストプラクティスの発展にどのようにアプローチしているか；

- BCM の範囲は、過去に考えられていたよりも広範な事象および事業運営に拡大される可能性がある。事業体が、深刻だが起こりうるディスラプションに耐える能力を発揮するために、堅固で定期的な事業継続活動およびテストの範囲の中で、一連のシナリオおよびステークホルダーの拡大もまた検討される可能性がある。；ならびに
- パンデミック時に発生した勤務環境の変化に鑑みて、既存の（パンデミック以前に用意された）または最近改定された BCP が変わらず目的に適合するためにどのように発展したか、または発展する予定であるか。

Annex 1： SSB の公表文書のストックテイクからの主要な洞察

オペレーショナル・レジリエンスに関連する利用可能な基準と支援する資料についての現在の状況を理解することをねらいとして、IAIS は既存の SSB の公表文書のストックテイクを実施した。この付属文書の後には参考文献一覧が記載されており、レビューされた広範な公表文書を提示している。以下は、サイバー・レジリエンス、IT のサードパーティへの外部委託および BCM についてストックテイクから得られた主要な教訓を詳述している。

サイバー・レジリエンス

1. サイバーセキュリティ・リスクは増加しており、サイバーインシデントは、保険会社が事業を行う能力を損ない、商業上のデータと個人情報の保護を侵害し、信頼を傷つける可能性がある。
2. 保険会社のサイバーセキュリティ枠組みは、その業務上のセキュリティと、保険契約者のデータの保護の双方（例えば、保険会社がサイバーセキュリティ・インシデントを予測し、検知し、耐え、抑制し、復旧する能力を維持・促進する能力）を、支援し促進するべきである。
3. 公的セクターと民間セクター双方の複数の国際機関、国家的組織、業界団体が保険監督に関連するサイバーセキュリティの枠組みおよび指針を開発しており、整合性に対する利益はあるものの、画一的なアプローチは、異なる地理、事業構造、監督上のアプローチ等にまたがって存在する固有の複雑性に対応しないだろう。
4. サードパーティが保険会社にもたらすリスクの重大性は、その保険会社との取引関係の重要性と必ずしも整合的であるとは限らない。保険会社は、サードパーティからもたらされる、またサードパーティにもたらすサイバーリスクを特定すべきである。

IT のサードパーティへの外部委託

5. クラウド・コンピューティングにおける集中によって生じるリスクの評価は初期段階にあり、保険会社のクラウド・コンピューティングの利用に対する監督者の期待は、明確化と、クロスボーダーな協力の恩恵を受ける可能性がある。このことは、クロスボーダーな外部委託とクラウドソーシングがより一般的になっている時代において、現在の多国間 MoU が目的に適合しているかどうかについて、さらに問題を提起している。
6. 外部委託された業務の再委託（フォースパーティ・リスク）は、IT のサードパーティへの外部委託に関連するリスクと同様のリスクをもたらしながら増加中である。
7. 重要な外部委託の取決めをカバーする契約に適用される準拠法の特定における監督者の役割と、外部委託された業務に関して保険会社の統制機能が十分であることの確保に監督者がどのようにして有用に貢献しうるかは、さらなる明確化が必要だろう。
8. 特にクロスボーダーな、IT のサードパーティへの外部委託に関して、データ保護法制と金融監督の間の相互作用については、さらなる議論と明確化が必要だろう。

事業継続管理

9. パンデミックにより、伝統的な災害復旧計画が失敗した領域が露呈し、新たな可能性と課題が特定された。それは、デジタル・セキュリティの準備をより広範な ERM と BCM に統合することの必要性をさらに明らかにした。
10. 現在の BCM アプローチは、少なくとも以下の要素に注目することで恩恵を受ける可能性がある：大規模なリモート勤務のためのインフラの促進とセキュリティ強化；職場における適切な制限を伴う物理的なアクセスのためのプロセスの開発；ならびにヘルス・サイエンスについての外部パートナーシップの策定と包含。

11. 事業継続活動は、広範な、深刻だが起こりうるシナリオの下で実施され、スタッフのオペレーショナル・レジリエンスに対する意識を高める。

12. ベストプラクティスについての情報共有を促進するフォーラムは、システミックなオペレーショナル・リスクに関して有益であろう。これは特に、重要なITのサードパーティ・サービスプロバイダーの事業継続性と災害復旧メカニズムに対する脅威への事業体の脆弱性をどのように評価・軽減しうるかに関連する。

参考文献

1. BIS ブレティン、*COVID-19 と金融セクターにおけるサイバーリスク*（2021 年）
2. BIS アメリカ事務所（2022 年）、*パンデミック時とパンデミック後の中央銀行における事業継続計画*
3. イングランド銀行、*金融セクターのオペレーショナル・レジリエンス*
4. BCBS、*サイバー・レジリエンス—多様な実務*（2018 年）
5. BCBS、*オペレーショナル・レジリエンスのための諸原則*（2021 年）
6. カーネギー国際平和基金、*金融システムをサイバー脅威からより適切に保護するための国際的戦略—サイバーセキュリティ・ワークフォースの挑戦*（2020 年）
7. 欧州システミックリスク理事会（ESRB）、*システミックなサイバーリスクの軽減*（2022 年）
8. FSI インサイト、*クラウドの規制と監督：保険会社向けの新たな健全性アプローチ*（2018 年）
9. FSB、*サイバーセキュリティにおける規制・ガイダンス・監督上の慣行に関するストックテイク報告書*（2017 年）
10. FSB、*サイバー用語集*（2018 年）
11. FSB ディスカッション・ペーパー、*アウトソーシング・サードパーティに関する規制・監督上の論点*（2020 年）
12. FSB、*サイバーインシデント報告—既存のアプローチとより広い範囲での収斂に向けた今後のステップ*（2021 年）
13. G7、*金融セクターにおけるサードパーティのサイバーリスクマネジメントに関する基礎的要素*
14. G7、*金融セクターのサイバーセキュリティに関する基礎的要素*
15. G7、*金融セクターのサイバーセキュリティの効果的な評価に関する基礎的要素*
16. G7、*脅威ベースのペネトレーションテストに関する基礎的要素*
17. IAIS 論点書、*保険セクターにおけるサイバーリスク*（2016 年）
18. IAIS 適用文書、*保険会社のサイバーセキュリティの監督*（2018 年）
19. IAIS 文書、*サイバーリスクの引受—持続可能な市場発展のための課題および監督上の検討事項の特定*（2020 年）
20. IMF *スタッフ・ディスカッションノート、サイバーリスクと金融安定性—結局は小さな世界*、ディスカッションノート No. SDN/20/07（2020 年 12 月）
21. IOSCO 協議文書、*外部委託の原則*（2020 年）
22. ISO 27002　情報セキュリティ統制（予防）
23. ISO 27035 情報セキュリティインシデントの管理（インシデント発生後）
24. OECD、*リスクおよびレジリエンス*
25. ソニックウォール、*2022 年ソニックウォール脅威レポート*（2022 年）
26. ジョイントフォーラム（BCBS、IOSCO、IAIS）、*金融サービスにおける外部委託*（2005 年）

27. ジョイントフォーラム（BCBS、IOSCO、IAIS）、*事業継続のためのハイレベル原則*（2006 年）

28. 米国連邦準備銀行、*SR 20-24—オペレーショナル・レジリエンス強化のための健全な実務に関する省庁間文書*

29. 世界経済フォーラム、*組織の存命のためにサイバー・レジリエンスは不可欠である。思慮にとんだ報告がその構築に役立つ*（2020 年）

30. 世界経済フォーラム、*サイバー・レジリエンスと報告*（2020 年）

31. 世界経済フォーラム、*サイバー・レジリエンスの原則とツール*（2017 年）