Deloitte.
デロイト トーマツ

保険セクターの国際的な規制の動向

（Vol. 64, 2025 年 10 月～11 月）

MAKING AN IMPACT THAT MATTERS since 1845

保険セクターの国際的な規制の動向（2025 年 10 月～11 月）

内容

A: ESAs、EU の金融セクターにおけるビッグテックの活動状況を調査（10 月 1 日）..... 3

B: EIOPA、2026 年の監督上の優先領域を特定（10 月 1 日）..... 4

C: 印 IRDAI、保険不正にかかるガイドラインを公表（10 月 9 日）..... 5

D: FSB、AI の利用のモニタリングと脆弱性にかかる報告書を公表（10 月 10 日）..... 6

E: 豪 ASIC、集団投資スキームによる外部委託のレビューを実施（10 月 10 日）..... 8

F: FSB、金融危機以降の規制改革の中間報告を公表（10 月 13 日）..... 10

G: ESAs、2026 年の作業プログラムを公表（10 月 16 日）..... 11

H: 英 PRA、サイバーセキュリティ対応の好事例を公表（10 月 20 日）..... 12

I: NY 州 DFS、外部委託先の管理にかかるガイダンスを公表（10 月 21 日）..... 13

A: ESAs、EU の金融セクターにおけるビッグテックの活動状況を調査（10 月 1 日）

■ 欧州監督機構（ESAs。欧州銀行監督機構（EBA）、欧州保険・年金監督局（EIOPA）、欧州証券市場監督局（ESMA）から成る。）は、欧州連合（EU）におけるビッグテック企業の直接的な金融サービス活動の状況を取りまとめ、公表した。その主な内容は以下のとおり。

背景と目的	• ESAsは2022年、デジタル・ファイナンスにかかる欧州委員会（EC）からの助言の要請に対し、ビッグテック・グループの関連性の高まりと広範な顧客アクセスを理由として、EUの金融セクターにおけるビッグテック・グループのモニタリングを行う必要性を指摘した。 • ESAsは2023年、最初のモニタリング調査（exercise）を実施し[1]、その後も、金融セクター間におけるビッグテック・グループのモニタリングを改善することを目的として活動を継続することとした。 • 各ESAの監督者ボード（Board of Supervisors）のメンバーである監督当局で構成される欧州イノベーション・ファシリテーター・フォーラム（EFIF）を通じて実施された今回のビッグテック・モニタリング・エクササイズは、EUで活動するビッグテック・グループの子会社による金融サービスの直接的な提供の状況を把握するものである。本調査では、それらの子会社の認可等のステータス、提供しているサービス、顧客ベース、クロスボーダーのオペレーションなどの情報を収集した。 • なお、本調査は、上記の各当局が最善の努力ベースで提出したデータを用いて行われた。
対象	• 2025年のモニタリング調査の対象となったビッグテック・グループは、Alphabet、Amazon、Ant Group、Apple、Booking.com、ByteDance、Meta、Microsoft、NTT Docomo、Rakuten、Tencent、Uber、Vodafoneの13グループ。
ビッグテック・グループの活動の状況	• 上記の13のビッグテック・グループのうち11グループが、決済（payment）サービス、電子マネーの発行、保険の仲介を主とする金融サービス事業を営む子会社をEUに有している。 • 合計で20の子会社が、免許を取得して、もしくは、欧州決済サービス指令（PSD2）の適用除外を受けて事業を営んでいる。 • 8つのビッグテック・グループの10の子会社が、免許を取得してEUにおいて金融サービスを提供している。そのうち4社が電子マネー事業者として、3社が保険会社もしくは保険仲介者として、2社が決済事業者として、1社が銀行（credit institution）として免許を受けている。この状況は、2023年から変化していない。 • 5つのビッグテック・グループの11の子会社が、PSD2の適用除外を受けて、特定の決済サービスを提供している。そのうち1社は、保険仲介者としての免許も有している。
今後の対応	• ESAsは、ビッグテックのEUの金融セクターへの関連性のモニタリングを継続する。ESAsは、ビッグテックがEUにおける金融活動の規模をさらに拡大する可能性を認識しており、特に、クロスボーダーで領域横断的な（cross-disciplinary）監督上の連携に焦点を当てていく。 • ESAsの今後の取組みとして、①データの透明性の向上や監督当局間におけるデータの共有の

[1] 前回の調査の概要は、デロイト トーマツ「保険セクターの国際的な規制の動向（Vol. 44, 2024 年 2 月～3 月）」記事 A を参照。
https://www.deloitte.com/content/dam/assets-zone1/jp/ja/docs/industries/financial-services/2024/202403_ins_regulation.pdf

	促進、②欧州オペレーショナル・レジリエンス法（DORA）の下でのモニタリングの拡充（重要なサードパーティ・サービス・プロバイダ（CTPPs）としての指定を含む。）、③デジタル市場法（Digital Markets Act）に基づくゲートキーパーの指定などの動向の注視、などが考えられる。

インプリケーション：ビッグテック企業による金融サービス・セクターへの参入が注視されている中、「欧州では、2023年からその状況に大きな変化はない」という今回の調査結果は興味深い。ビッグテック企業のCTPPsとしての指定を含め、欧州における今後の規制・監督の動向は注目に値する。

（参考）EIOPA 'Factsheet: 2025 Joint ESA stocktaking of BigTechs' direct financial services activities in the EU'

B: EIOPA、2026 年の監督上の優先領域を特定（10 月 1 日）

■ 欧州保険・年金監督局（EIOPA）は、2026年の監督上の優先領域（focus areas）と注力領域（areas for attention）を特定した。それぞれの概要は以下のとおり。

背景	• EIOPAは2024年3月、①保険会社および再保険会社の財務の頑健性、②混乱した（disruptive）環境における消費者の保護、の2つを、2024年から2026年のEU全域の戦略的な監督上の優先課題として特定した。 • EIOPAは、その2つの優先課題の中で、より具体的な優先領域を毎年公表しており、2025年には、①リスクの移転（リスクの移転のキャパシティと適切性を含む。）、②保険料に見合う保険契約の価値（Value for Money：VfM）の2つが優先領域として特定された。
2026年の優先領域と注力領域	• EIOPAは、2026年の優先領域および注力領域として、それぞれ以下の事項を特定した。 - 優先領域：①欧州オペレーショナル・レジリエンス法（DORA）、②サステナビリティ・リスク - 注力領域：①集団投資スキーム（collective investment undertakings：CIUs）にかかるソルベンシー資本要件（SCR）の計算、②保険金の支払い請求（デジタルを通じたものを含む。）における消費者の公正な取扱い
想定される主な監督上の活動	• DORA - ICTリスクの管理の枠組みの構築における取締役会（Administrative Management or Supervisory Board：AMSB）の関与の程度の評価（ICTリスクの管理の枠組みの目的適合性の評価を含む。） - 主なICT関連のインシデントのモニタリングとそれにかかる保険会社との積極的な対話 - ICTサードパーティ・リスクの管理の枠組みの評価 - 保険会社のデジタル・レジリエンス・テスティング・プログラムの評価 • サステナビリティ・リスク - ORSAにおいて報告されるサステナビリティ・リスクのマテリアリティ評価の品質と深度の評価 - 気候変動シナリオ分析の設計、信頼性およびORSAへの統合の評価

	- サステナビリティ・リスクの管理と投資の意思決定の整合性との一貫性の評価 - 商品の価値提供と適切な開示の観点からの商品設計と販売機能の評価 • CIUsにかかるSCRの計算 - 20%超をCIUsに投資している（再）保険会社のSCRの計算におけるルックスルー・アプローチの適用方法の評価 • 保険金の支払い請求における消費者の公正な取扱い - 保険金の支払い請求への対応に問題が認められた保険会社を対象とする、当該問題と商品設計やVfMとの関連性の評価

インプリケーション：優先領域の一つであるDORAに関し、日本でも金融庁の「金融分野におけるサイバーセキュリティに関するガイドライン」を受けて保険会社の取組みが進展しつつある中、欧州の保険会社のICTリスク管理にかかる（先進的な）取組みは、日本の保険会社に対して示唆を提供するものと考えられる。その意味で、欧州の好取組等にかかる情報が広く公表されることも期待される。

（参考）EIOPA 'Union-wide strategic supervisory priorities - focus areas for 2026'

C: 印 IRDAI、保険不正にかかるガイドラインを公表（10 月 9 日）

■ インド保険規制開発庁（IRDAI）は、保険不正のモニタリングの枠組みにかかるガイドラインを公表した。2026年4月に適用が開始される同ガイドラインの主な内容は以下のとおり。

目的	• 本ガイドラインの目的は、保険業界における不正リスクを実効的に抑止し、防止し、検知し、報告し、改善するための包括的な枠組みを構築すること。本ガイドラインは、保険セクターの不正に対するレジリエンスを高め、誠実なカルチャーを醸成し、保険契約者の利益を保護し、金融安定を確保し、また、国民の信頼を維持することを目指している。
定義	• 保険の不正（insurance fraud）とは、不正を働いている者もしくはその他の関係する者のために、不誠実な、もしくは、違法な手段によって利益を得ることを意図する作為もしくは不作為を言う。保険の不正には、以下のものが含まれる。 - 金銭の横領（misappropriation） - 意思決定、取引もしくは財務に関連する一つ以上の重要な事実を意図的に誤って伝え、隠し、また、開示しないこと - 責任、信頼される立場もしくは信認関係（fiduciary relationship）を濫用すること
不正の分類	• 保険会社は、以下の分類に従い、不正を抑止等するための適切な体制およびプロセスを構築しなければならない。 - 組織内の不正（役職員が関係する不正） - 販売チャネルの不正 - 保険契約者による不正（不正請求を含む）

	- 外部の不正（サービス・プロバイダ等の外部の者による不正） - その他の不正（上記の分類における一以上の不正の加害者間の共謀による不正）
不正リスクの管理の枠組み	• 保険会社は、不正をゼロにすることを目指し、自身のプロファイルに即した、適切な不正のリスクの管理の枠組みを設けなければならない。 • 保険会社のリスク管理委員会は、その枠組みの実効的な実施と監督に責任を有していなければならない。 • 不正リスクの管理の枠組みは、少なくとも、以下のものを含むものでなければならない。 - 取締役会によって承認された、反不正の方針 - 不正モニタリング委員会 - 報告の要件
サイバー	• 保険会社は、サイバーや新たな種類の不正（new age fraud）を防止するため、頑健なサイバーセキュリティの枠組みを構築し、また、インシデントのデータベースや顧客認証、アクセス管理等の不正リスク管理のための体制やプロセスを継続的にモニターし、強化しなければならない。
情報共有	• すべての保険会社は、保険情報局（Insurance Information Bureau：IIB）によって提供される不正モニタリング技術枠組み（Fraud Monitoring Technology Framework）に参加しなければならない。 • IIBは、業界のデータベースを通して、保険業界における脅威インテリジェンスにかかる情報をタイムリーに共有しなければならない。
販売チャネル	• 販売チャネルがその規模やリスク・プロファイルに応じた適切な不正リスクの管理の枠組みを構築することが重要である。
報告	• 保険会社は、関係する法令に従い、法執行機関等にインシデントを報告しなければならない。 • 販売チャネルが関係する不正の場合、保険会社は、遅滞なく、IRDAIに報告しなければならない。

インプリケーション：本ガイドラインのポイントの一つは、販売チャネルの不正リスクの管理にも言及していることであると考えられる。保険会社には、その販売チャネル（保険代理店などの仲介者を含む。）を含めた不正リスクの管理体制を構築し、そのリスクを管理することが期待される。

（参考）IRDAI 'IRDAI (Insurance Fraud Monitoring Framework) Guidelines, 2025'

D: FSB、AI の利用のモニタリングと脆弱性にかかる報告書を公表（10 月 10 日）

■ 金融安定理事会（FSB）は、「金融セクターにおけるAIの利用と関連する脆弱性のモニタリング」と題するレポートを公表した。同レポートは、AIの利用と関連する脆弱性について、金融監督当局が現在用いているモニタリングのアプローチを整理するとともに、モニタリングのための潜在的な指標について検討している。同レポートの（特に、モニタリングのための潜在的な指標にかかる部分の）主な内容は以下のとおり。

0：モニタリング指標全般	• AIの利用のモニタリングと関連する脆弱性の評価には、複数のソースからの指標を用いた、包括的なアプローチが必要となる。 • 以下の指標のうち、AIの利用にかかるものは、監督当局がAIの利用をモニタリングするために使い得る指標となる。その他の指標は、特定の脆弱性を評価するための指標の候補となり得る。
1：AIの利用	• AIの利用にかかる直接的なモニタリング指標には、以下のものが含まれ得る。 - 関連する側面（dimensions）でブレイクダウンした、金融セクターにおけるAIのユース・ケースのインベントリー（主な側面には、金融活動（トレーディング、融資、保険、決済等）、AIの種類（生成AI、AIエージェント等）、重要性の水準（中核となる事業ライン、重要なオペレーション、低リスクの内部プロセス等）が含まれる。） - AIを利用している金融機関のシェア（ユース・ケース、AIモデル、金融機関の規模別） - 金融機関のコホート別のAIの利用のパターンにかかる定性的なデータ（定性的な指標は、定量的な指標を補足し、主要なトレンドや共通の課題等を特定に資するものとなり得る。） • 直接的なデータを収集することが困難である場合、以下のような代替的な指標を用い得る。 - AI関連の特許の申請状況 - 金融機関におけるAI関連の役割のトレンド - AIにかかる投資の代理指標としての技術もしくは調査・開発予算
2：集中リスク	• AI関連のサードパーティへの依存度やサービス・プロバイダの集中のモニタリングには、以下のような指標を用いることができる。 - サードパーティが開示している、金融機関が利用するAIアプリケーションのシェア - サードパーティ・サービス・プロバイダによって提供されるサービスに影響する重要なサイバーやオペレーション上のインシデントにかかる、金融機関による監督当局に対する届出（脆弱性が金融機関の損失に波及し得る主要なチャネルのモニタリングに資する。） - 金融機関から取得したデータや情報に基づく、重要なAIサービスやサービス・プロバイダのリスト（registers） - 単一の、もしくは、密接に関係するAIサービス・プロバイダによってサポートされている重要なAIサービスの数 - 広く利用されているAIサービスの相対的なコストとパフォーマンス（AIサービスの代替可能性を評価するために用いることができる。）
3：市場の相関	• AIドリブンの市場の相関のモニタリングには、AIの利用が、集団行動（herding behaviour）、流動性の危機（liquidity crunches）、プロシクリカリティなどの市場のダイナミクスに与える影響を推計する指標が必要となる。そのための（代理）指標には、以下のものが含まれ得る。

	- 広く利用されている訓練済みのモデルを利用している金融機関の数、その特性、および、教育に用いられるデータのソース - 特定のユース・ケースにおけるAIの利用と資産価格のボラティリティの間、もしくは、資本市場のセグメントにおける相関との間の関係の分析的な測定 - 主要な市場におけるAIモデルの自律性の水準にかかる情報
4：サイバー	• AIに固有のサイバーの脆弱性を追跡するための指標には、以下のものが含まれ得る。 - 金融セクターを対象としたAI関連のサイバー攻撃の数 - AIに関連する組織内のサイバー・インシデントの数 - サードパーティ・サービス・プロバイダに影響を与えるAI関連のサイバー・インシデントの数 - サイバー防御（cyber defence）のためのAIのユース・ケース
5：ガバナンス	• AI関連のモデル・リスク、データの品質、ガバナンスにかかる脆弱性のモニタリングのための指標には、以下のものが含まれ得る。 - 金融機関のモデル・インベントリーにおけるAIモデルのシェア - AIのモデル・リスクの管理やガバナンスに関連する監督上の発見事項のトレンド - AIシステムにおける自動化された意思決定の程度
6：金融不正	• AIドリブンの金融不正や偽情報のモニタリングのための指標には、以下のものが含まれ得る。 - AIドリブンの金融不正の数、および、そうした不正にかかる定性的な情報（金融機関の検知の手法等） - 偽情報キャンペーン - AI不正や偽情報に関連する顧客の苦情

インプリケーション：FSBがその報告書の中で示した指標は、一義的には、監督当局がそのモニタリングにおいて利用を検討することが想定されている。他方で、金融機関は、これらの指標を、内部管理の高度化において参照し得るものと考えられる。

（参考）FSB ‘Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector’

E: 豪 ASIC、集団投資スキームによる外部委託のレビューを実施（10 月 10 日）

■ オーストラリア証券投資委員会（ASIC）は、登録を受けた集団投資スキーム（Managed Investment Scheme）を運営する免許を受けた主体（Responsible Entity：RE）のオフショアのサービス・プロバイダ（OSPs）の利用にかかるレビューを実施し、その結果を公表した。その主な内容は以下のとおり。

レビューの概要	• 本レビューは、特に、リスク管理体制（サイバーセキュリティ・リスクやレジリエンスにかかるOSPsの監督やモニタリングの枠組みを含む。）の十分性に焦点を当て、REsによるOSPsの利用、および、それに関連するリスクの管理の実態を調査するもの。

	• 本レビューは2段階に分けて行われた。フェーズ1では、REsによるOSPsの利用の実態を把握するため、30のREsを対象としてレビューを実施した。フェーズ2では、その対象を10のREsに絞り込み、より深度ある調査を行った。
外部委託されているサービス	• REsがオフショアに外部委託している主なサービスは、投資のプロセスの管理と監督、ならびに、ファンドのポートフォリオ、カストディ、ファンドの管理（fund administration）および取引の処理にかかるサービス（transaction processing services）の管理である。 • 事業機能の外部委託の程度は、運用資産の額と比例している傾向が見られる。例えば、レビューの対象となったREsのうち、少なくとも1つ以上の事業機能をオフショアに外部委託している割合は、運用資産の額で上位20％に入る6つのREsについては100％、中位40%では33%、下位40%では58%であった。
主なリスク	• REsによるオフショアへの外部委託にかかるリスクには、以下のものが含まれる。 - 外部委託されたタスクや事業機能に対するコントロールを失うリスク（それは、自身もしくは顧客の情報の機密性を保護するREsの能力を阻害し得る。） - 外国の法律に従うOSPsが、オーストラリアの法律と相容れない要件を遵守すること、もしくは、REsのデータに対するコントロールやアクセスを失うことによる、データやテクノロジー（特に、顧客情報の保護）に関連するリスク - 事業機能や外部委託されたタスクがオフショアで行われる場合、オーストラリアの事業にかかるデータの侵害やサイバー・インシデントの実効的な検知や管理に関連するリスク - 消費者や市場参加者を害し得る、サービスに対するオペレーションの中断のリスク（オフショアのインフラストラクチャーは、本国のそれと比べ、信頼性が低い可能性がある。）
好取組の事例	• 今回のレビューにおいて発見された好取組には、以下のものが含まれる。 - デュー・ディリジェンスのプロセス：契約締結前および契約締結後に継続して、OSPのケイパビリティを評価するためのプロセスを文書化している。 - 継続的なパフォーマンスのモニタリング：サービスの水準を評価するための指標を明確に定義し、文書化している。 - サービス・レベル・アグリーメント（SLA）：それぞれのOSPと、法的拘束力のある文書化された契約を締結している。 - サイバー・リスクへの対応：組織的なリスク・レジスターの一部として、OSPのサイバー・リスクを文書化し、モニターしている。 - データ・プライバシー：機密情報を管理するためのOSPのコントロールを定期的に評価している。 - 事業の継続：OPSsに対して、高リスク・シナリオに対する対応の戦略を文書化し、定期的な災害復旧テストを行うことを求めている。

インプリケーション：一般的に、オフショア（国外）のサードパーティ・サービス・プロバイダの管理には様々な障壁があると考えら

れるところ、サードパーティ・リスク・マネジメント（TPRM）の文脈におけるクロスボーダーでの監督当局間の連携の重要性も増してくるものと考えられる。

（参考）ASIC 'Review of offshore outsourcing – Responsible entities'

F: FSB、金融危機以降の規制改革の中間報告を公表（10 月 13 日）

■ 金融安定理事会（FSB）は、グローバルな金融危機以降に合意された規制の実施状況にかかる中間報告書を公表した。同報告書の主な内容は以下のとおり。

バーゼルIII	• バーゼルIIIについては、完全な実施の期限を後ろ倒しにすることはグローバルの金融システムにとっての重大なリスクであるとの懸念をいくつかのFSBメンバーが表明している中、その包括的なパッケージの完全な実施に向けた取組みは続けられている。 • 実施時期の後ろ倒しを単にタイミングの問題であるとすることは、その重要性を危険に晒すこととなる。規制の策定から実施までのサイクルが15年を超える場合、そのことは、制度における機敏性（agility）の欠如を強調する。 • バーゼル銀行監督委員会（BCBS）の提言の実施のタイムラインの延期は、ノンバンク金融仲介（NBFIs）の急速な成長とその銀行システムとの潜在的に重大な関係など、FSBが懸念する脆弱性と密接に関連している。
TBTF	• グローバルにシステム上重要な銀行（G-SIBs）の指定のためのメカニズムと、それと関係する「大きすぎて潰せない（too-big-to-fail：TBTF）」問題にかかる改革は、概ね実践され、実効的にモニターされている。総損失吸収力（total loss-absorbing capacity：TLAC）規制は、グローバルの金融システムの安全を補完する重要な施策となっている。
破綻処理の枠組み	• システム上重要な金融機関（SIFI）の監督の枠組み一般、および、主要な特性（Key Attributes）にかかる実施上の課題（issues）は、引き続き存在する。2023年3月に救済された銀行の事案を受けて、スイスが自国の規制・監督の枠組みを改正するための検討を開始したことは注目すべきであり、また、賞賛に値するものであるが、グローバルな金融危機後にそのような大きな危機を経験することは、理想的な状況とは言えない。 • TBTFのリスクを低減するため、各国・地域による、より包括的で実務的な主要な特性の実施の実現に向けてFSBが重要な役割を果たすことも合わせ、さらに積極的なアプローチが採られることが望ましい。
NBFI改革	• NBFIにかかる取組みは、グローバルな金融危機後の取組みと直近5年における取組みの二段階に分けて進展している。 • 第一段階の取組みは、伝播（spillover）の緩和、MMF、証券化、証券金融取引（securities financing transactions）、その他のノンバンク金融機関、の5つの領域にかかるものである。これらの領域の改革は進展しているものの、領域によって、また、国・地域によって、そのスピードには差がある。 • FSBは、2020年3月の市場の混乱からの教訓をもとに、MMF、オープンエンド型のファンドの流動性ミスマッチ、NBFIのレバレッジ、マージン・コールにかかる流動性の準備、の4つの領域に焦点

	を当て、さらなる取組みを進めてきている。直近では、その焦点は、流動性管理の品質の評価から、レバレッジの利用の実態把握へとシフトしてきている。NBFIのレバレッジにかかる政策措置は2025年7月に提言されたところであり、それらの実施状況のモニタリングは今後行われることとなる。
OTCデリバティブ	• OTCデリバティブ市場改革のための政策措置の実施は、FSBメンバー国・地域において十分に進展しているものの、例えば、包括的な取引報告や中央清算もしくはプラットフォーム取引にかかる規制の枠組みなど、完全な実施にまでは至っておらず、そのギャップはなかなか埋まらない状況にある。
今後の対応	• 全体的に、G20の金融改革の推進において大きな進展が認められているものの、最近の傾向は、実施のペースが鈍化していることを示唆しており、そのことは、将来の危機に対する金融システムのケイパビリティを脆弱なものとし得る。 • 近年では、暗号資産などの新たな領域が拡大してきているものの、合意された規制の完全な実施を行わず、新たな優先事項に目を向けることは避けるべきである。

インプリケーション：「合意された規制の完全な実施を行わず、新たな優先事項に目を向けることは避けるべきである」というメッセージは注目に値する。他方で、そのことは、国際規制の一貫した実施の難しさを示すものであると考えられる。

（参考）FSB 'G20 Implementation Monitoring Review: Interim report'

G: ESAs、2026 年の作業プログラムを公表（10 月 16 日）

■ 欧州監督機構（ESAs。欧州銀行監督機構（EBA）、欧州保険・年金監督局（EIOPA）、欧州証券市場監督局（ESMA）から成る。）は、共同委員会（Joint Committee：JC）としての2026年の作業プログラムを公表した。同作業プログラムにおいて特定された主な領域は以下のとおり。

オペレーショナル・レジリエンス	• JCは、デジタル・オペレーショナル・レジリエンスについて、欧州デジタル・オペレーショナル・レジリエンス法（DORA）に基づく新たな監督の枠組みの実効的な運用および監督上のコンバージェンスにかかる作業に焦点を当てる。予定されている主な取組みは以下のとおり。 - EUの金融セクターにICTサービスを提供している重要なサードパーティ・プロバイダ（CTPPs）を指定 - 指定された個々のCTPPにかかる年間および複数年の監督計画の策定 - DORAの一貫した実践を確保するための、監督上のコンバージェンスの推進 - ESAsの新たな機能であるインシデント報告および危機時の協力（crisis coordination）の推進
消費者保護とイノベーション	• JCは、銀行、保険、年金および証券の商品およびサービスに対する消費者の信頼、ならびに、それらの領域における消費者の保護を強化する。予定されている主な取組みは以下のとおり。 - パッケージ型のリテールおよび保険ベースの投資商品（packaged retail and insurance-based investment products：PRIIPs）規制（PRIIPs Regulation）にかかる、重要情報文書（Key Information Document：KID）の簡素化にかかる規制上の技術的

	な基準（RTS）の策定 - 金融教育にかかる好取組を共有するためのワークショップの開催
サステナブル・ファイナンス	• JCは、引き続き、サステナブル・ファイナンスを主要なテーマとして位置付ける。本領域で予定されている主な取組みは以下のとおり。 - サステナブル・ファイナンス開示規則（SFDR）のレビューの結果を受けた作業（技術的な監督上の基準の策定等） - ESGリスクのストレス・テストの実施に関するハイレベルな原則にかかるガイドラインの策定
リスク評価	• ESAsは、引き続き、金融安定に対する主要なリスクと脆弱性の分析を行う。
証券化	• JC証券化委員会は、EU証券化規則（Securitisation Regulation：SECR）の実施における監督上のコンバージェンスを促進する。

インプリケーション：本作業プログラムは、欧州におけるクロスセクターでの優先課題を示すものであるとみなすこともできる。オペレーショナル・レジリエンスや消費者保護が金融セクターにおける優先課題として特定されていることは、注目に値する。

（参考）EIOPA '2026 Work Programme of the Joint Committee of the European Supervisory Authorities'

H: 英 PRA、サイバーセキュリティ対応の好事例を公表（10 月 20 日）

■ 英国健全性監督機構（PRA）は、イングランド銀行（BoE）および英国金融行為規制機構（FCA）と共同で、「実効的な実務：サイバーへの対応（response）と復旧（recovery）のケイパビリティ」と題するサイバーセキュリティ対応にかかる事例集を公表した。同事例集の主な内容は以下のとおり。

背景と本レポートの位置付け	• オペレーショナル・レジリエンスは、BoE、PRA、FCAにとって、優先度が高いテーマの一つである。サイバーの脅威が高まり、また、サードパーティへの依存度が高まる中、金融機関は、レジリエンスを維持するため、戦略的でダイナミックなアプローチを採る必要があることを認識している。 • 本レポートは、BoE、PRAおよびFCAが、その他のシステム上重要な金融機関（Other Systemically Important Institutions）および金融市場インフラ（financial market infrastructure：FMIs）のオペレーショナル・レジリエンスにかかる自己評価において認識した、サイバーセキュリティ対応にかかる実効的な実務を取りまとめたものである。 • 本レポートを公表する目的は、金融機関に対してこれらの実務の検討や実施を慫慂することにある。金融機関の取締役会は、本レポートを、事業を継続するために必要な保証の水準、サイバーにかかるテスティングの妥当性、サイバーセキュリティ・リスクの定量化等の、オペレーショナル・レジリエンスにかかる議論を活発に行うための材料として用いることができる。
事例1：甚大なサイバーの被害への対応	• 最も成熟した金融機関は、価値、量、重要な活動、エンドユーザー、決済（payments）の手段など、期間（duration）に留まらない影響の許容度（impact tolerance）の指標を検討している。それによって、これらの金融機関は、消費者の被害、市場の清廉性、自身の安全性と健全性、金融安定に対するリスクを低減するために提供する必要があるサービスの水準をより正確に認識している。 • 金融機関が金融市場の秩序的な機能を支える重要な事業サービスを特定している場合、多

	くの金融機関は、より広範なシステミックな影響を反映した影響の許容度を定めている。 • 最も実効的である金融機関の自己評価は、すべての顧客、カウンターパーティ、規制当局およびより広範なステークホルダーをカバーする、事前に定義された危機コミュニケーション計画を含んでいる。金融機関は、また、サイバー攻撃中および攻撃を受けた後のコミュニケーション能力（capabilities）のレジリエンスを確保するためのテストを行っている。
事例2：甚大なサイバー攻撃からの復旧	• 金融機関は、自身のレジリエンスのケイパビリティを強化するため、多様な施策を講じている。それらには、以下のものが含まれる。 - 重要なデータの改ざん不可能なバックアップ（immutable back-ups）からの復元、および、重要な（important）事業サービスを支える重要な（critical）アプリケーションや中核となるインフラストラクチャーの再構築 - 外部のアクターが金融機関の本番環境（production environments）に不正アクセスすることを非常に困難にするために設計された、分離され、隔離された、第三の（tertiary）設備の利用
事例3：重要なサードパーティにおけるインシデントへの対応	• サードパーティが重要な事業サービスの提供をサポートしている場合、最も成熟した金融機関は、それらのサードパーティのレジリエンスのケイパビリティが自身のインフラストラクチャーに対して期待するレジリエンスのケイパビリティと同等であることを積極的に確保している。そのような水準の保証が得られない場合、影響の許容度に留まるため、以下の様な代替措置を検討している。 - サードパーティ・サービス・プロバイダに対して、自身のケイパビリティを構築することを求める - 別のサードパーティ・サービス・プロバイダもしくは自身のシステムに切り替える（fail over）ための能力（ability）を開発する - サードパーティ・サービス・プロバイダにおけるデータの喪失や破壊の後にサービスを復旧するケイパビリティを構築する • 実効的なレジリエンスのケイパビリティは、明確に定義された役割と責任、組織内の適切な階層における意思決定、レジリエントなコミュニケーション戦略を含む、より広範なインシデント・レスポンスの枠組みに内包される。
結論	• 金融機関は、サイバーの脅威に対応する取組みを進めてきているものの、さらなる高度化の余地がある。BoE、PRA、FCAは、金融機関に対して、エンド・トゥ・エンドの対応や復旧のプロセスの文脈におけるレジリエンスのケイパビリティへの投資を検討することを慫慂する。

インプリケーション：英国においても、あらためて、サードパーティ・サービス・プロバイダ（TPSPs）の管理の重要性が指摘されている。日本の金融機関には、こうした国際的な流れを受け、TPSPsの管理の強化に向けた取組みを推進することが期待される。

（参考）PRA ‘Effective practices: Cyber response and recovery capabilities’

I: NY 州 DFS、外部委託先の管理にかかるガイダンスを公表（10 月 21 日）

■ ニューヨーク州金融サービス局（NYDFS）は、サードパーティ・サービス・プロバイダ（TPSPs）の利用に関連するリスクに対

応するためのサイバーセキュリティ・ガイダンスを発出した。同ガイダンスの主な内容は以下のとおり。

TPSPsの評価	• 金融機関は、TPSPを選定する際、そのTPSPが当該金融機関の情報システムおよび非公開情報（NPI）にもたらすサイバーセキュリティ・リスクを評価しなければならない。 • 金融機関の方針と手順は、それらのリスクの評価の方法（TPSPに求められる最低限のサイバーセキュリティの基準を含む。）およびTPSPのサイバーセキュリティの実務とコントロールを評価するための手順を含むものであるべきである。 • 金融機関は、システムへのアクセス、データの重要度、所在地、提供を受けるサービスの重要性等の要素を勘案し、リスクに応じてTPSPsを分類すべきである。 • 金融機関は、各TPSPによってもたらされるリスクを低減するため、個社別でリスクベースの計画を策定すべきである。金融機関がTPSPsのデュー・ディリジェンスを実施する際に検討すべき項目には、以下のものが含まれる。 - 情報システムおよびNPIに対するアクセスの種類と程度 - 業界内におけるTPSPの評判 - TPSPが策定および実施しているサイバーセキュリティ・プログラムの水準 - TPSPから提供を受けるサービスの重要性と他のTPSPsへの代替可能性 - TPSPが再委託先を選定し、モニタリングするための実務 • 金融機関は、契約しようとしているTPSPsによって提供される情報の入手、レビューおよび検証の方法を検討すべきである。
契約	• 金融機関が策定する、デュー・ディリジェンスおよび契約にかかる文書化された方針は、TPSPがアクセス可能なデータや情報システムの重要性に応じた、リスクベースのものでなければならない。 • 金融機関がTPSPsとの契約において含めることを検討すべき事項には、以下のものが含まれる。 - アクセス・コントロール - データの暗号化 - サイバーセキュリティにかかるインシデントの報告 - データの所在地と転送の制限 - 再委託 - データの共有と契約終了時のデータの取扱い • 金融機関は、必要に応じて、AIの利用可能性（金融機関のデータをAIモデルの訓練に利用することの可否を含む。）にかかる条項を設けることを検討すべきである。
モニタリングと	• 金融機関のTPSPにかかる方針は、TPSPsの定期的な評価について規定していなければならな

監督	い。 • TPSPにかかるリスク管理の手順は、TPSPのサイバーセキュリティ・プログラムが金融機関のサイバーセキュリティにかかる期待と整合していることを確認するために設計された監督のプロセスと統制を含むべきである。 • 金融機関は、TPSPsの継続的なモニタリングと監督のための方針と手順を策定し、実施すべきである。 • 金融機関は、脆弱性の管理にかかるアップデートを要請し、パッチングの実務を評価し、特定された不足の改善を確認すべきである。重要な、もしくは、未解決のリスクは、金融機関のリスク評価において文書化され、内部のリスク・ガバナンスの枠組みの中で、適切にエスカレーションされるべきである。 • 金融機関は、例えば、代替システムやプロバイダへの変更など、サードパーティ・リスクを、自身のインシデント・レスポンスおよび事業継続計画に統合すべきである。
契約の終了	• 金融機関は、TPSPとの契約を終了しようとする際、TPSPの金融機関の情報システムへのアクセスを遮断しなければならない。 • 金融機関は、安全で秩序だった契約の終了を確保するため、重要なサービスにかかる移行計画を策定すべきである。 • 契約の終了後、すべての義務が履行されており、アクセスが適切に遮断されていることを確認するため、最終的なリスクのレビューを実施すべきである。

インプリケーション：（記事Hにかかるインプリケーションを参照）

（参考）NYDFS ‘DFS Acting Superintendent Kaitlin Asrow Issues New Cybersecurity Guidance to Address Risks Associated with the Use of Third-Party Service Providers’

執筆者

小林 晋也／Shinya Kobayashi
マネージングディレクター
ファイナンシャルサービシーズ
デロイト トーマツ リスクアドバイザリー合同会社

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ リスクアドバイザリー合同会社、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT 弁護士法人およびデロイト トーマツ グループ合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従いプロフェッショナルサービスを提供しています。また、国内約 30 都市に 2 万人超の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト（ www.deloitte.com/jp ）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTL および DTTL の各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTL はクライアントへのサービス提供を行いません。詳細は www.deloitte.com/jp/about をご覧ください。

デロイト アジア パシフィック リミテッドは DTTL のメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける 100 を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、最先端のプロフェッショナルサービスを、Fortune Global 500®の約 9 割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促進することで、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来 180 年の歴史を有し、150 を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約 46 万人の人材の活動の詳細については、（ www.deloitte.com ）をご覧ください。

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301