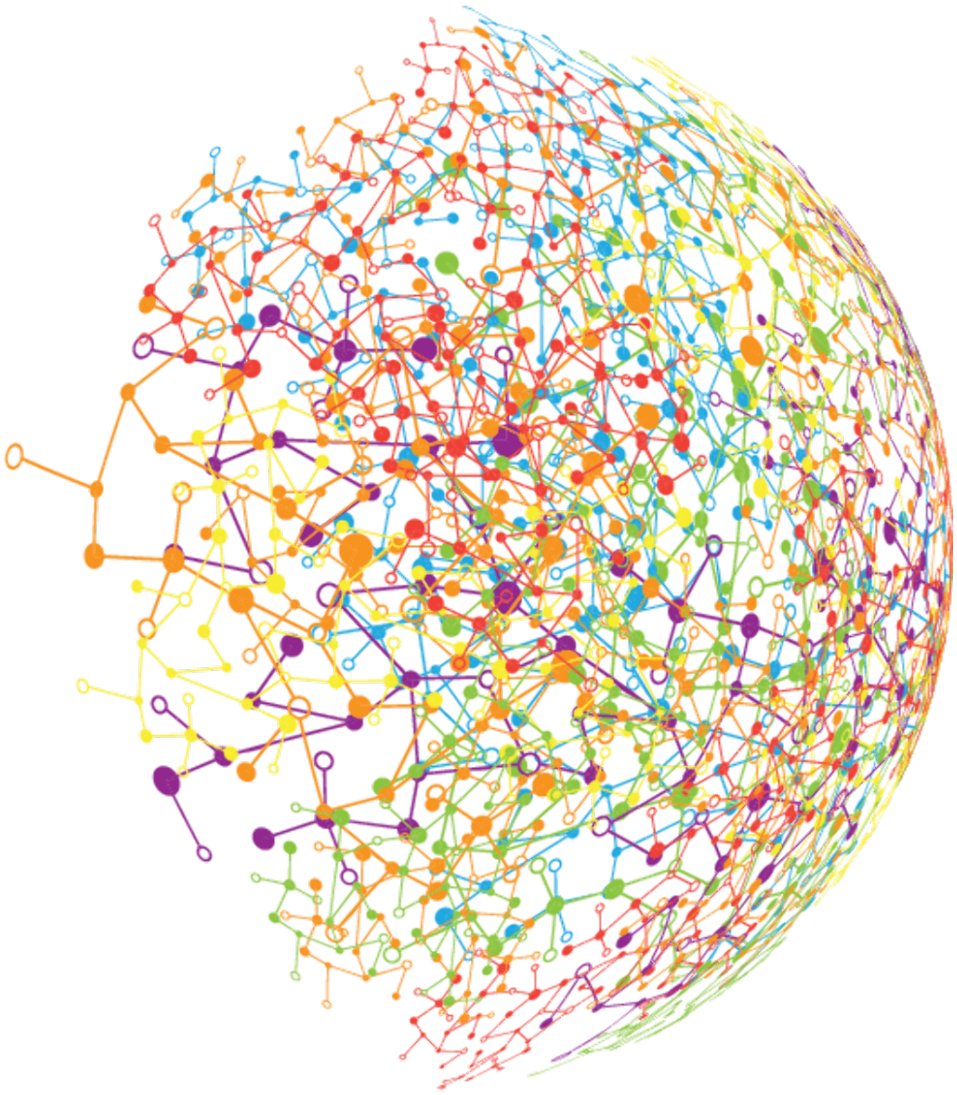
Deloitte.
デロイト トーマツ



金融機関のオペレーショナル・レジリエンス

MAKING AN IMPACT THAT MATTERS since 1845

欧州デジタル・オペレーショナル・レジリエンス法（DORA）からの示唆

2023 年 3 月

内容

1. オペレーショナル・レジリエンスにかかる金融規制・監督の動向

1.1 オペレーショナル・レジリエンスの重要性の高まり

金融機関および金融システムのレジリエンスの確保は、各国の監督当局の重要なマンデートの一つである。このことは、例えば、バーゼル銀行監督委員会（BCBS）が「金融安定の向上を目的とする、銀行の規制・監督とその実践の強化」を、保険監督者国際機構（IAIS）が「保険契約者の保護のための保険会社の実効的な監督の促進と金融安定への貢献」を、それぞれのマンデートやミッションとして掲げていることからも明らかである。

2008年の金融危機以降、監督当局は、危機の根本原因に対処し、金融機関、そして、金融システムのレジリエンスを確保するため、金融機関に対する資本規制の強化や破綻処理の枠組みの構築等に注力してきた[1]。前者には、BCBSによるバーゼルIIIの整備や、金融安定理事会（FSB）による「健全な報酬慣行に関する原則」の策定が、後者には、FSBによる「金融機関の実効的な破綻処理の枠組みの主要な特性」の公表とその実施状況の評価が含まれる。FSBは、2019年に公表したアニュアル・レポートにおいて、「これらの取組みは、レジリエントな金融システムの構築につながっている」、と評価している[2]。

こうした中、金融セクターを取り巻く環境は常に変化しており、現在では、「ファイナンシャル・レジリエンス」に加え、金融機関の「オペレーショナル・レジリエンス」の確保が、監督当局の優先課題の一つとなってきている。例えば、英国のイングランド銀行、健全性監督機構（PRA）、金融行為規制機構（FCA）は2018年、オペレーショナル・レジリエンスに関するディスカッション・ペーパーを連名で公表し[3]、「金融機関が提供する商品やサービスのオペレーションの中断は、消費者や市場参加者に損害を生じさせ、金融機関の存続可能性を脅かし、また、金融システムの安定を揺るがす可能性がある。」と指摘した。加えて、金融機関のオペレーショナル・レジリエンスを脅かす要因として、①フィンテックや人工知能、分散型台帳、暗号資産などの技術の革新、②アクセスの容易さや取引の高速化などの行動の変化、③変化の速さによって生じるスキルのギャップや陳腐化、④サイバー・インシデントやコスト削減のプレッシャーなどの環境の変化、⑤サードパーティや集中リスク、クロスボーダー化などのシステムの複雑化、を挙げている。

近年のパンデミックの中でその進展が大きく加速したデジタライゼーションも、オペレーショナル・レジリエンスを脅かす一因となる。例えば、クラウド・コンピューティングなどのビッグ・テック・サービスの利用は、金融機関のコスト削減、柔軟性、スケーラビリティ、標準化、安全性やオペレーショナル・レジリエンスの改善に寄与し得る。他方で、技術への一層の依存は、サイバー攻撃、金融サービスの提供構造の複雑化、一部のサービス・プロバイダーへの集中リスクなど、新たな脆弱性を生じさせ得る[4]こととなり、金融機関のオペレーショナル・レジリエンスに課題をもたらす。

1.2 各国・地域における規制・監督の動向

金融機関のオペレーショナル・レジリエンスの確保が監督上の重要な課題となる中で、規制や監督の枠組みの整備も始まっている。

グローバル

BCBSは、金融危機後の規制改革により、銀行の資本や流動性の健全性は高まったものの、パンデミックやサイバー攻撃、技術的な不具合など、オペレーションに関連するリスクへの耐性を強化する余地があるとして、2021年3月に「オペレーショナル・レジリエンスのための原則」を策定した。同原則は、オペレーショナル・レジリエンスを「中断を受けてもなお、重要なオペレーションを提供できる銀行の能力」と定義し、オペレーショナル・レジリエンスにかかる7つの原則（表1）

[1] Financial Stability Board 'Post-2008 financial crisis reforms' (last updated on 13 June 2022), https://www.fsb.org/work-of-the-fsb/market-and-institutional-resilience/post-2008-financial-crisis-reforms/.

[2] Financial Stability Board (2019) 'Implementation and Effects of the G20 Financial Regulatory Reforms', https://www.fsb.org/wp-content/uploads/P161019.pdf.

[3] Bank of England, Prudential Regulation Authority and Financial Conduct Authority (2018) 'Discussion Paper: Building the UK financial sector's operational resilience', https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf.

[4] Financial Stability Board (2022) 'FinTech and Market Structure in the COVID-19 Pandemic – Implications for financial stability', https://www.fsb.org/wp-content/uploads/P210322.pdf.

を示している[5]。

表1.　BCBSのオペレーショナル・レジリエンス原則

原則1：ガバナンス 銀行は、事業の中断が重要なオペレーションの提供に与える影響を最小限に抑えることを目的として、事業の中断に対応・適応し、また、それから復旧し、学習することができる、実効的なオペレーショナル・レジリエンスのアプローチを構築し、監督し、実践するため、既存のガバナンス構造を利用すべきである。	**原則5：サードパーティへの依存度の管理** 銀行は、重要なオペレーションの提供にかかるサードパーティやグループ内のエンティティ等との関係への依存度を管理すべきである。
原則2：オペレーショナル・リスク管理 銀行は、オペレーショナル・レジリエンスのアプローチに従い、外部および内部の脅威、ならびに、人員、プロセスおよびシステムにおける潜在的なリスクを継続的に特定し、重要なオペレーションの脆弱性を直ちに評価し、顕在化するリスクを管理するため、オペレーショナル・リスクの管理にかかる様々な機能を活用すべきである。	**原則6：インシデント管理** 銀行は、事業の中断に対する銀行のリスク・アペタイトと許容度に沿って、重要なオペレーションの提供を中断し得るインシデントを管理するための対応・復旧計画を策定し、実施すべきである。銀行は、生じたインシデントから得られた教訓を踏まえ、インシデント対応と復旧計画の継続的な改善を図るべきである。
原則3：事業継続計画とテスト 銀行は、事業の中断時に重要なオペレーションを提供する自らの能力を検証するため、事業継続計画を策定し、甚大な、しかしながら、生じ得るシナリオの下での事業継続テストを行うべきである。	**原則7：サイバーセキュリティを含むICT** 銀行は、重要なオペレーションの提供を完全にサポートし、また、円滑に行うため、定期的にテストされ、適切な状況認識を行うことができ、また、リスク管理と意思決定プロセスに対して関係するタイムリーな情報を提供できる、保護、検知、対応および復旧のプログラムに従う、サイバーセキュリティを含むレジリエントな ICT システムを確保すべきである。
原則4：相互関連性と相互依存性の把握 銀行は、重要なオペレーションを特定した上で、オペレーショナル・レジリエンスに対するアプローチと整合する、重要なオペレーションの提供に必要な内部および外部の相互関連性と相互依存性を把握すべきである。	

欧州

英国PRAは2021年3月、金融機関のオペレーショナル・レジリエンスにかかる新たな規制（Supervisory Statement）「オペレーショナル・レジリエンス：重要なビジネス・サービスに対する影響の許容度」を策定した[6]（※2022年3月に一部アップデートされた。なお、PRAは、同時期に、「アウトソーシングとサードパーティのリスク管理」にかかる規制[7]も策定している。）。2022年3月から施行されている同規制は、金融機関に対して、以下（表2）の事項を求めている[8]。

[5] Basel Committee on Banking Supervision (2021) 'Principles for Operational Resilience', https://www.bis.org/bcbs/publ/d516.pdf.

[6] Prudential Regulation Authority (2022) 'Supervisory Statement | SS1/21 – Operational resilience: Impact tolerances for important business services', https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss121-march-22.pdf?la=en&hash=ED32FF8608D88C585FD47B82F0C5FF0A3751E4EE.

[7] Prudential Regulation Authority (2021) 'Supervisory Statement | SS2/21 – Outsourcing and third party risk management', https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf?la=en&hash=5A029BBC764BCC2C4A5F337D8E177A14574E3343. 同規制の概要については、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. 9, 2021 年 3 月～4 月）」記事 H を参照されたい。https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/financial-services/ins/202104_ins_regulation.pdf

[8] 同規制の概要については、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. 9, 2021 年 3 月～4 月）」記事 G を参照されたい。

表2.　英国PRAのオペレーショナル・レジリエンス規制の概要

- 重要な事業サービス（important business services。金融機関が提供するサービスで、それらに中断が生じた場合、金融機関の安全性と健全性、もしくは、英国の金融安定にリスクをもたらすもの。）を特定すること。
- 特定されたそれぞれの重要な事業サービスについて、影響の許容度（impact tolerance。時間ベースの指標等で設定される、重要な事業サービスの中断に対して最大限許容できる水準。）を設定すること。
- 甚大で、しかしながら、生じ得る（severe but plausible）シナリオの下で、影響の許容度の範囲内で重要な事業サービスを提供可能であることを確保すること（改善策を策定すること、サードパーティの利用を実効的に管理すること、内外向けのコミュニケーション戦略を策定すること、を含む。）。
- 各重要な事業サービスを提供するために必要な人員、プロセス、技術、設備および情報を特定し、文書化すること。
- 甚大で、しかしながら、生じ得るシナリオを特定した上で、シナリオ・テストを実施すること。
- 重要な事業サービスや影響の許容度等について、取締役会の承認を得ること。

アイルランド中銀は2021年12月、「オペレーショナル・レジリエンスにかかる業界横断的なガイダンス」を公表し、その中で、オペレーショナル・レジリエンスを、①特定と準備、②対応と適応、③復旧と学習の3つの柱で整理している[9]。第1の柱では重要な（critical or important）事業サービスの特定や影響の許容度の設定、第2の柱では事業継続管理やインシデント管理、第3の柱ではPDCAサイクル等について、合計で15のガイドラインが示されている。

スイス連邦金融市場監督機構（FINMA）は2022年12月、オペレーショナル・リスクにかかる銀行向けの通達（circular）を全面的に改正し、「オペレーショナル・リスクとレジリエンスにかかる通達」として公表した（表3）[10]。同通達は、オペレーショナル・レジリエンスを「事業の中断時において、重要な機能を許容度の範囲内で復元する、金融機関の能力」と定義しており、金融機関に対して、重要な機能や事業の中断に対する許容度を特定すること、事業の中断時において重要な機能を提供可能であることをテストすること等を求めている。

表3.　FINMAのオペレーショナル・リスクとレジリエンスにかかる通達の構成

- オペレーショナル・リスク管理
  - 全般的なオペレーショナル・リスク管理
  - ICTリスク管理
    - ICT戦略とガバナンス
    - 変更管理（change management）
    - ICTオペレーション
    - インシデント管理
  - サイバー・リスク管理
  - 重要なデータ・リスクの管理
  - 事業継続管理
- オペレーショナル・レジリエンスの確保
- システム上重要な銀行の破綻処理と再建における重要なサービスの継続

欧州連合理事会は2022年11月、「デジタル・オペレーショナル・レジリエンス法（Regulation on digital operational resilience for the financial sector。一般にDORAと称される。）」を採択した。DORAについては、その内容を次章で概説する。

---

https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/financial-services/ins/202104_ins_regulation.pdf

[9] Central Bank of Ireland (2021) 'Cross Industry Guidance on Operational Resilience', https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp140/cross-industry-guidance-on-operational-resilience.pdf?sfvrsn=bd29921d_5.

[10] Swiss Financial Market Supervisory Authority (2023) 'Circular 2023/1 Operational risks and resilience – banks', https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf?sc_lang=en&hash=1529FC7CCFD70F24BCC75C4D1B033ECF. 同通達の概要については、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. 30, 2022 年 12 月～2023 年 1 月）」記事 D を参照されたい。
https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/financial-services/ins/202301_ins_regulation.pdf.

アジア・パシフィック

シンガポール金融管理局（MAS）は2022年6月、事業継続管理（BCM）にかかるガイドラインを約15年振りに改正した[11]。新たなガイドラインは、金融機関に対して、①重要な事業サービスおよび機能を特定すること、②特定されたそれぞれの重要な事業サービスについて、サービスのリカバリー・タイム目標（SRTO）を設定すること、③リソース（人、技術、データ等）およびサードパーティへの依存度をマッピングすること、④BCMの方針、計画、手順等を策定し、アップデートし、準備状況をテストすること、⑤インシデント管理および危機管理を行うための態勢を整備すること、などを求めている。

オーストラリア健全性規制庁（APRA）は2022年7月、銀行および保険会社等を対象とするオペレーショナル・リスク管理にかかる健全性監督基準（案）を市中協議に付し[12]ており、今後、2023年初頭に最終化し、2024年から適用を開始することを予定している。同基準案は、主要な原則として、金融機関に対して、①オペレーショナル・リスクを実効的に管理すること、②甚大な事業の中断時において、重要なオペレーションを許容度の範囲内で維持すること、③サービス・プロバイダーの利用にかかるリスクを管理すること、などを求めている。

北米

米国では、連邦準備制度理事会（FRB）、通貨監督庁（OCC）、連邦預金保険公社（FDIC）が2020年11月、「オペレーショナル・レジリエンスの強化のための健全な実務」と題するペーパーを連名で公表した[13]。同ペーパーは、大規模で複雑な米国の銀行向けに、オペレーショナル・レジリエンスにかかる既存の規制やガイダンスをまとめたものである。その本編は、①ガバナンス、②オペレーショナル・リスク管理、③事業継続管理、④サードパーティ・リスク管理、⑤シナリオ分析、⑥安全でレジリエントな情報システム管理、⑦監視と報告、から成り、サイバー・リスク管理は別紙で整理されている。その他、米国財務省は、2023年2月に公表した「金融サービス・セクターのクラウド・サービスの利用」と題するレポートにおいて、クラウド等の新たな技術の利用が米国の金融サービス・セクターのオペレーショナル・レジリエンスに与える影響を評価することの重要性を認識している、と述べている[14]。

カナダ金融機関監督庁（OSFI）は、現在、オペレーショナル・リスク管理にかかるガイドライン（E-21）の改正を行っており、2023年春に同案を市中協議に付すことを予定している。OSFIは、オペレーショナル・レジリエンス、重要なオペレーション、事業の中断の許容度等の用語を定義しており、例えば、オペレーショナル・レジリエンスには、技術やサイバー・リスクに対するレジリエンスも含まれると整理している[15]。

[11] Monetary Authority of Singapore (2022) 'Business Continuity Management Guidelines', https://www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/bcm-guidelines/bcm-guidelines-june-2022.pdf.

[12] Australian Prudential Regulation Authority (2022 'Prudential Standard CPS 230: Operational Risk Management', https://www.apra.gov.au/sites/default/files/2022-07/Draft%20Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management.pdf. 同基準案の概要については、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. 25, 2022 年 7 月～8 月）」記事 G を参照されたい。

[13] Board of Governors of the Federal Reserve System (2022) 'SR 20-24: Interagency Paper on Sound Practices to Strengthen Operational Resilience', https://www.federalreserve.gov/supervisionreg/srletters/SR2024.htm.

[14] U.S. Department of the Treasury (2023) 'The Financial Services Sector's Adoption of Cloud Services', https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.

[15] Office of the Superintendent of Financial Institutions (2022) 'Operational resilience key definitions', https://www.osfi-bsif.gc.ca/Eng/fi-if/in-ai/Pages/20221206_let.aspx.

2. 欧州デジタル・オペレーショナル・レジリエンス法（DORA）の概要

欧州委員会は2020年9月、デジタル金融におけるイノベーションや競争を促し、また、そこから生じ得るリスクを低減することを目的とする、新たなデジタル金融パッケージを採択した。同パッケージは、①欧州のデジタル金融戦略、②暗号資産の規制案、③デジタル・オペレーショナル・レジリエンス法（DORA）案を含むものであった[16]。その後、DORAは2022年12月に最終化され、2025年1月17日から適用が開始されることとなっている。

2.1 DORA の全体像

DORAは、9章、64条から成り（表4）、共通した高い水準のデジタル・オペレーショナル・レジリエンスを確保することを目的として、金融機関のビジネス・プロセスをサポートするネットワークや情報システムの安全性にかかる要件を定めている。

DORAでは、デジタル・オペレーショナル・レジリエンスは、「金融機関が利用し、また、金融サービスの提供とその品質の継続的な提供をサポートする、ネットワークと情報システムのセキュリティに対応するために必要とされる様々なICT関連のケイパビリティを、直接的、もしくは、ICTサードパーティ・サービス・プロバイダー（以下、ICT TPSP）によって提供されるサービスの利用を通じて間接的に確保することにより、オペレーションの完全性と信頼性を構築し、保証し、レビューする金融機関の能力」と定義される。

DORAの適用対象は金融セクター広範にわたり、銀行（credit institutions）、投資サービス会社（investment firms）、決済サービス機関（payment institutions）、中央清算機関、保険会社、保険仲介者（insurance intermediaries）、信用格付機関等（同法では金融機関（financial entities）と総称される。）、様々な金融機関に適用される。なお、一部の要件については、例えば、零細金融機関（職員が10名未満で、年間の売上高やバランスシートの残高が2百万ユーロを超えない金融機関。）への適用は除外されるなど、その適用はプロポーショナリティ原則に従うこととなる。

以下では、DORAの5つの中核要素と考えられる、①ICTリスク管理の枠組みの構築と実践（DORA第2章）、②ICT関連のインシデントの管理、分類および当局への報告（同第3章）、③デジタル・オペレーショナル・レジリエンス・テストの実施（同第4章）、④ICTサードパーティ・リスクの管理（同第5章）、⑤重要なICT TPSPの監督（同第5章）、に焦点をあて、その内容を概説する。

[16] European Commission (2020) 'Digital finance package', https://finance.ec.europa.eu/publications/digital-finance-package_en.

表4.　DORAの構成

第1章：総則

- 第1条　主題
- 第2条　適用範囲
- 第3条　定義
- 第4条　プロポーショナリティ原則

第2章：ICTリスク管理

- 第5条　ガバナンスと組織
- 第6条　ICTリスク管理の枠組み
- 第7条　ICTシステム、プロトコルおよびツール
- 第8条　特定（identification）
- 第9条　保護（protection）と予防（prevention）
- 第10条　検知（detection）
- 第11条　対応（response）と復旧（recovery）
- 第12条　バックアップの方針と手順（procedures）、復元（restoration）と復旧の手順と手法
- 第13条　学習と高度化
- 第14条　コミュニケーション
- 第15条　ICTリスク管理のツール、手法、プロセスおよび方針のさらなる調和
- 第16条　簡素なICTリスク管理の枠組み

第3章：ICT関連のインシデント管理、分類および報告

- 第17条　ICT関連のインシデント管理のプロセス
- 第18条　ICT関連のインシデントとサイバーの脅威の分類
- 第19条　主な（major）ICT関連のインシデントの報告と重大な（significant）サイバーの脅威の自主的な通知
- 第20条　報告の内容とテンプレートの調和
- 第21条　主なICT関連のインシデントの報告の一元化
- 第22条　監督上のフィードバック
- 第23条　銀行等の決済関連のインシデント

第4章：デジタル・オペレーショナル・レジリエンス・テスト

- 第24条　デジタル・オペレーショナル・レジリエンス・テストの実施のための一般的な要件
- 第25条　ICTツールとシステムのテスト
- 第26条　脅威ベースのペネトレーション・テスト（TLPT）に基づくICTツール、システムおよびプロセスの先進的なテスト
- 第27条　TLPTの実施者のための要件

第5章：ICTサードパーティ・リスクの管理

- 第28条　一般的な原則
- 第29条　エンティティ・レベルでのICT集中リスクの予備的な評価
- 第30条　主要な（key）契約条項
- 第31条　重要な（critical）ICT TPSPの指定
- 第32条　監督枠組みの構造
- 第33条　リード監督者のタスク
- 第34条　リード監督者間のオペレーション上の協調
- 第35条　リード監督者の権限
- 第36条　域外におけるリード監督者の権限の行使
- 第37条　情報提供の要請
- 第38条　一般的な調査
- 第39条　検査
- 第40条　日常の監督
- 第41条　監督を行うための条件の調和
- 第42条　監督当局によるフォローアップ
- 第43条　監督の手数料
- 第44条　国際的な協力

第6章：情報共有の取決め

- 第45条　サイバーの脅威にかかる情報とインテリジェンスに関する情報共有の取決め

第7章：監督当局

- 第46条　監督当局
- 第47条　関係当局等との協力
- 第48条　当局間の協力
- 第49条　金融セクター内の協力
- 第50条　行政処分と改善策
- 第51条　行政処分と改善策を課すための権限の行使
- 第52条　刑事罰
- 第53条　通知義務
- 第54条　行政処分の公表
- 第55条　職務上の守秘義務
- 第56条　データ保護

第8章：　委任法

- 第57条　委任

第9章：経過および最終規定

- 第58条　レビュー条項
- 第59条～63条　関連する規制の改正
- 第64条　施行と適用

2.2 中核要素 1：ICT リスク管理

ICTリスク管理は、①特定、②保護と予防、③検知、④対応と復旧、⑤高度化、⑥コミュニケーション、というプロセスで実施する。

2.2.1 ガバナンスとICTリスク管理の枠組み

デジタル・オペレーショナル・レジリエンスを高い水準で実現するため、金融機関には、ICTリスクの効果的な管理を確保するガバナンスと統制の枠組みを整備するとともに、全社的なリスク管理の枠組みに統合されたICTリスク管理の枠組みを構築することが求められる。ICTリスクは、「ネットワークや情報システムの利用に関して、顕在化した場合には、デジタルもしくは物理的な環境に悪影響を生じさせることを通じて、ネットワークや情報システム、技術に依存するツールやプロセス、オペレーションやプロセス、あるいは、サービスの提供の安全性を脅かし得る、合理的に特定可能な状況」と定義される。

ICTリスク管理の枠組みは、すべての情報資産やICT資産、関係するすべての物理的なコンポーネントやインフラストラクチャを適切に保護するために必要な戦略、方針、手順、ICTプロトコルおよびツールを提供するものとなる。金融機関には、ICTリスク管理の枠組みの実効性を確保するための手法等を示す「デジタル・オペレーショナル・レジリエンス戦略」を策定することが求められる。それには、例えば、①ICTリスクに対する許容度（tolerance level）の設定と影響の許容度（impact tolerance）の分析、②情報セキュリティの目標（KPIsなどの指標を含む。）の設定、③ICT関連のインシデントを検知するためのメカニズムの整備、④デジタル・オペレーショナル・レジリエンス・テストの実施、⑤開示が求められるICT関連のインシデントが発生した際のコミュニケーション戦略の策定、などが含まれる。

金融機関のICTリスク管理の枠組みの整備と運用に最終的な責任を負うのは、その経営陣である。経営陣には、例えば、①データの可用性、信頼性、完全性および機密性が高い水準で維持されることを確保するための方針を策定し、②ICTに関連するすべての機能について役割と責任を明確にするとともに、それらの機能の実効性を確保するガバナンスの取決め（governance arrangements）を設け、③デジタル・オペレーショナル・レジリエンス戦略を策定および承認し、④ICTの事業継続方針、対応および復旧計画を承認し、監督し、また、その実施状況を定期的にレビューし、⑤ICT TPSPから提供を受けるICTサービスの利用の取決めに関する方針を承認する、などが求められる。

2.2.2 事業機能および情報・ICT資産の特定

ICTリスク管理の最初のステップは、事業機能（business functions）および情報・ICT資産の洗出しである。事業機能について、金融機関は、ICTリスク管理の枠組みの一環として、ICTのサポートを受けているすべての事業機能、役割および責任、それらの機能をサポートしている情報・ICT資産、ならびに、それらの役割や依存関係を特定し、文書化しなければならない。また、金融機関には、他の金融機関との間のエクスポージャーを含む、ICTリスクのすべてのソースを特定するとともに、ICTのサポートを受けている事業機能、情報・ICT資産に関係するサイバーの脅威やICTの脆弱性を評価することが求められる。

情報・ICT資産に関して、金融機関は、すべての情報・ICT資産（リモート・サイトやネットワーク・リソース、ハードウェア設備にかかるものを含む。）を特定し、重要なものをマッピングしなければならない。また、金融機関は、それらの資産の構成（configuration）や相互依存関係もマッピングする必要がある。さらに、金融機関は、ICT TPSPに依拠しているすべてのプロセスを特定し、文書化するとともに、重要な機能（critical or important functions）をサポートするサービスを提供しているICT TPSPとの相互関係を特定しなければならない。その他、金融機関には、すべてのレガシーICTシステムのICTリスクの評価を行うことも求められる。

2.2.3 保護、予防および検知

洗い出された事業機能や情報・ICT資産について、それらを保護し、リスクの顕在化を予防し、潜在的なリスクを検知できる必要がある。金融機関には、特に、重要な機能をサポートしているICTシステムのレジリエンス、継続性および可用性を確保し、また、高い水準のデータの可用性、信頼性、完全性および機密性を維持するため、ICTセキュリティ・ポリシー、手順、プロトコルおよびツールを整備することが求められる。

データや情報・ICT資産に関し、金融機関は、ICTリスク管理の枠組みの一環として、①データや情報・ICT資産の可用性、信頼性、完全性および機密性を保護するためのルールを定めた情報セキュリテ

ィ・ポリシーを策定し、②情報・ICT資産への物理的もしくは論理的なアクセス権限にかかる方針、手順および統制を設け、③ICTの変更管理にかかる文書化された方針、手順および統制を整備しなければならない。

検知の観点からは、金融機関には、異常な（anomalous）活動を迅速に検知し、潜在的にマテリアルな単一障害点を特定するためのメカニズムを整備し、それらを定期的にテストすることが求められる。なお、それらのメカニズムは、複層の統制を可能にし、ICT関連のインシデント対応のプロセスを発動するアラートの閾値や基準を定義するものである必要がある。

2.2.4 対応と復旧

顕在化したリスクに対応し、BAUへの速やかな復旧を可能にする体制が構築されていることも必要である。金融機関は、ICTリスク管理の枠組みの一環として、全社的な事業継続方針の不可欠な（integral）構成要素となる、包括的なICTの事業継続方針（ICTの対応および復旧計画を含む。）を整備しなければならない。その上で、金融機関には、①金融機関の重要な機能の継続性を確保し、②すべてのICT関連のインシデントに速やかに、かつ、効果的に対応し、③計画を遅滞なく発動し、④予備的な影響、損害、損失を見積り、⑤コミュニケーションおよび危機管理のアクションを提供することなどを目的として、策定したICTの事業継続方針を実践することが求められる。

また、金融機関には、特に、外部委託されている重要な機能について、ICTの事業継続計画を策定し、定期的にテストすることのほか、甚大な事業の中断の事業影響度評価（BIA）を行うことが求められる。BIAでは、内外のデータやシナリオ分析を利用し、事業の中断の潜在的な影響を、定量的および定性的な基準によって評価する。

さらに、金融機関は、包括的なICTリスク管理の一環として、すべての機能をサポートしているICTシステムにかかるICTの事業継続計画やコミュニケーション計画を定期的にレビューするとともに、その実効性をテストしなければならない。事業継続計画や対応・復旧計画のテストには、サイバー攻撃やメインと予備システム間のスイッチオーバーのシナリオを含めることが求められる。

2.2.5 バックアップ、回復および復旧の手順

金融機関は、最小限のダウンタイムや中断、損失でICTシステムとデータを回復するため、対象となるデータやそのバックアップの頻度を特定したバックアップ・ポリシー、回復・復旧の手順や手法を策定し、文書化するとともに、それらを定期的にテストしなければならない。加えて、金融機関には、それらのバックアップ・ポリシーや手順に従って起動されるバックアップ・システムを設けることや、ビジネス・ニーズを満たすことができる予備の（redundant）ICTケイパビリティを維持することが求められる。なお、各機能について設定されるリカバリー・タイムやリカバリー・ポイント目標は、それぞれの機能の重要性や市場の効率性に与え得る影響を考慮したものである必要がある。

2.2.6 管理態勢の高度化

金融機関は、脆弱性やサイバーの脅威、ICT関連のインシデント（特に、サイバー攻撃）に関する情報を収集するとともに、それらがデジタル・オペレーショナル・レジリエンスに与え得る影響を分析することができるケイパビリティを有している必要がある。そうしたケイパビリティを確保するため、金融機関には、ICTセキュリティ・アウェアネス・プログラムやデジタル・オペレーショナル・レジリエンス・トレーニングの研修をすべての役職員について必修化することが求められる。

2.2.7 その他

ICTリスク管理のツール、手法、プロセスおよび方針のさらなる調和を図るため、①ICTセキュリティ・ポリシー、手順、プロトコルおよびツールに含まれる項目、②アクセス権限に関する事項、③異常な活動の検知のためのメカニズム、④ICT事業継続方針に含まれる項目、⑤ICT事業継続計画のテストの詳細、⑥ICT対応・復旧計画に含まれる事項、⑦ICTリスク管理の枠組みのレビューに関する報告の内容とフォーマットなどは、別に策定される規制上の技術的基準において規定される（2.8を参照）。

2.3 中核要素 2：ICT 関連のインシデントの管理、分類および報告

インシデント管理は、①ICT関連のインシデントの管理のプロセスの構築、②インシデントの分類、③監督当局への報告と通知、の3つのステップで構成される。

2.3.1 ICT関連のインシデントの管理のプロセス

金融機関は、ICT関連のインシデントを検知し、管理し、通知するため、インシデントの管理のプロセスを構築しなければならない。そのプロセスは、①早期警戒指標を含み、②優先度や甚大さ、影響を受けたサービスの重要性に応じて、インシデントを特定し、追跡し（track）、記録し（log）、分類するための手順を整備し、③発動が必要な役割と責任を、インシデントの種類やシナリオに応じて整理し、④役職員、外部のステークホルダーおよびメディアに対するコミュニケーション、顧客に対する通知、内部のエスカレーションの手順等にかかる計画を定め、⑤主なインシデント（その影響度や対応方針、インシデント後に新たに設けられる統制を含む。）が関係する役員に報告されることを確保し、⑥影響を低減し、サービスの提供をタイムリーに再開することを確保するものでなければならない。

2.3.2 ICT関連のインシデントとサイバーの脅威の分類

金融機関は、ICT関連のインシデントを分類し、その影響を評価しなければならない。評価に際しては、①影響を受ける顧客や取引の数や風評リスクを生じさせる可能性、②インシデントの継続期間（サービスの中断時間を含む。）、③影響を受ける地理的な範囲、④可用性、信頼性、完全性、機密性の観点からのデータの損失、⑤影響を受けるサービスの重要性、⑥コストや損害などの金額的な影響、などの観点を勘案することが求められる。サイバーの脅威については、金融機関には、自身が提供する商品やサービスの取引や顧客数等の観点から、その重大性を分類することが求められる。

2.3.3 ICT関連のインシデントとサイバーの脅威

主なICT関連のインシデントの報告について、金融機関は、定められた期間内に、①第一報、②中間報告（インシデントの状況に大きな変化があった場合等）とその後のアップデート、③最終報告（根本原因の分析が完了し、実際の影響額が判明した時点）を、関係する監督当局に提出しなければならない。これらの報告は、監督当局がインシデントの重要性（criticality）を判断するために必要な情報を提供するものでなければならない。なお、金融機関は、これらの報告をTPSPに委託できるものの、規制の遵守については金融機関が全責任を負うこととなる。

重大なサイバーの脅威にかかる監督当局への通知は、任意となる。金融機関は、それが金融システムや金融サービスの利用者、顧客に関係すると考える場合、その脅威を関係する監督当局に自主的に通知することができる。

主なICT関連のインシデントが発生し、顧客の財務上の利益に影響を及ぼしている場合、金融機関は、それに気付いた後に遅滞なく、インシデントおよび講じている施策について顧客に情報を提供しなければならない。重大なサイバーの脅威の場合、金融機関は、潜在的に影響を受ける顧客に対して、顧客が採ることを検討できる適切な保護措置にかかる情報を提供する必要がある。

2.4 中核要素 3：デジタル・オペレーショナル・レジリエンス・テスト

デジタル・オペレーショナル・レジリエンス・テストには、①原則、すべての金融機関が実施すべきテスト、②監督当局が指定する金融機関のみが実施する脅威ベースのペネトレーション・テスト（TLPT）、の2つがある。

2.4.1 ICTツールとシステムのテスト

ICT関連のインシデントに対応するための準備状況を評価し、デジタル・オペレーショナル・レジリエンスにおける弱点、不足およびギャップを特定し、また、改善策を速やかに実施するため、金融機関は、ICTリスク管理の枠組みの中核要素の一つとして、健全で包括的なデジタル・オペレーショナル・レジリエンス・テスト（DORT）プログラムを構築しなければならない。同プログラムは、脆弱性評価やスキャン、オープン・ソース分析、ネットワーク・セキュリティ評価、ギャップ分析、物理的セキュリティ評価、質問表やスキャン・ソフトウェア、ソース・コード・レビュー、シナリオベースのテスト、互換性テスト、パフォーマンス・テスト、E2Eテスト、ペネトレーション・テストなど、適切なテストを

行うことが可能な手法やツールを含むものである必要がある。

DORTは、内部もしくは外部の独立した者によって行われる。金融機関は、内部の者がテストを行う場合、十分なリソースを割り当てるとともに、テストの設計や実行フェーズを通じて利害の相反が生じないことを確保しなければならない。また、金融機関は、テストにおいて発見されたすべての事項の優先度を決め、分類し、改善を図るための手順と方針を設けるとともに、すべての特定された弱点、不足あるいはギャップが完全に解消されることを確保するための内部検証のメソドロジーを策定しなければならない。なお、重要な機能をサポートしているすべてのICTシステムやアプリケーションについては、少なくとも年次でテストが行われる必要がある。

2.4.2 脅威ベースのペネトレーション・テスト（TLPT）

金融機関は、少なくとも3年ごとにTLPTを実施し、その結果の概要（発見事項や改善策等）を監督当局に提出しなければならない。TLPTを実施すべき金融機関は監督当局によって指定される。その指定は、①影響度（金融機関のサービスや活動が金融セクターに与える影響等）、②金融安定に対する懸念（金融機関のシステム上の重要性等）、③特定のICTリスクのプロファイル、金融機関のICTの成熟度あるいは関係するテクノロジーの特性、を評価した上で行われる。

金融機関は、重要な機能やICTサービス（外部委託されている重要な機能をサポートしているものを含む。）をサポートしているすべての関係する基盤となるICTシステム、プロセスおよび技術を特定しなければならない。その上で、金融機関は、重要な機能のうちどの機能をTLPTの対象とする必要があるかを評価する必要がある。TLPTの範囲を決定するその評価の結果は、監督当局による検証に従うこととなる。

各TLPTは、金融機関の複数もしくはすべての重要な機能を対象として、そのような機能をサポートしている本番システム上で実施される必要がある。また、ICT TPSPがTLPTの範囲に含まれる場合、金融機関は、当該TPSPのTLPTへの参加を確保するために必要な措置を講じる必要がある。TLPTの実施者について、TLPTは、専門性や独立性等にかかる一定の要件を満たす外部の者によって行われることが想定されている。内部の者を利用する場合には、金融機関は、監督当局の承認を受けることに加え、3回に1回は外部の者を用いる必要がある。

なお、①TLPTの対象を特定する要件の閾値、②内部の者の利用を統制する要件や基準、③TLPTの範囲（重要な機能等の範囲）、テストのメソドロジーやアプローチ、および、テストの結果、終了・改善段階に関する要件等は、別途規制上の技術的基準として定められる（2.8を参照）。

2.5 中核要素 4：ICT サードパーティ・リスクの管理

DORAにおけるICTサードパーティ・リスクの管理は、①戦略の策定、情報一覧の作成および集中リスクの評価、②ICT TPSPのモニタリング、③重要なICT TPSPの監督、の3つの柱で構成される。（なお、本稿では、監督当局が主として対応する③を、中核要素5として整理している。）

2.5.1 ICTサードパーティ・リスクの管理の主要な原則

ICTサードパーティ・リスクは、ICTリスク管理の枠組みの中の不可欠な要素の一つである。金融機関には、ICTサードパーティ・リスクに関する戦略を採択し、定期的にレビューすることが求められる。その戦略は、ICT TPSPから提供を受ける、重要な機能をサポートするICTサービスの利用に関する方針を含むものでなければならない。また、金融機関には、ICT TPSPから提供を受けるICTサービスの利用に関するすべての契約上の取決めにかかる情報一覧を作成し、アップデートすることが求められる。監督当局の要請を受けた場合、金融機関は、同一覧におけるすべての情報を提供できる必要がある。

監督当局への報告に関して、金融機関は、ICTサービスの利用に関する新たな取決めの数、提供を受けているICTサービスと機能等について、少なくとも年次で監督当局に報告する必要があるほか、重要な機能をサポートするICTサービスの利用を計画している場合には、その旨をタイムリーに報告しなければならない。

ICTサービスの利用に関する契約上の取決めを締結する前に、金融機関には、①契約上の取決めが重要な機能をサポートするICTサービスの利用に関係するものであるか否かを評価し、②契約上の取決めにかかるすべての関係するリスク（ICTの集中リスクを含む。）を特定し、評価し、③契約を予定しているICT TPSPのデュー・ディリジェンスを行うこと等が求められる。その上で、金融機関は、適切な情報セキュリティ基準を遵守しているICT TPSPとのみ、契約上の取

決めを締結できる。契約上の取決めが重要な機能に関係するものである場合、金融機関は、契約の締結前に、ICT TPSPが最新かつ最も高水準の情報セキュリティ基準を利用しているかどうかを十分に考慮しなければならない。

契約の終了の観点からは、金融機関は、①ICT TPSPによる関係法令や約款の重大な違反、②提供を受ける機能のパフォーマンスに変化が生じ得る事象の発生、③ICT TPSPのリスク管理の脆弱さ、④契約上の取決めの要件が監督当局による金融機関の実効的な監督を妨げること、等を理由として、ICTサービスの利用にかかる契約上の取決めを解除できることを確保しなければならない。

重要な機能をサポートしているICTサービスの場合、金融機関は、出口戦略を用意しておく必要がある。出口戦略は、ICT TPSPにおける障害（failure）の可能性や提供を受けているICTサービスの品質の低下等、ICT TPSP側で生じ得るリスクを勘案したものでなければならず、また、金融機関は、それらの事由が生じた場合に事業を継続できるよう、適切なコンティンジェンシー施策を有していなければならない。さらに、金融機関は、自らの事業活動を中断させず、規制上の要件の遵守を妨げず、顧客に提供するサービスの継続性と品質に不利益をもたらすことなく、契約上の取決めを終了できる必要がある。その他、金融機関には、ICTサービスやデータの移行が安全かつ完全に行われるよう、代替的なソリューションを特定するとともに、移行計画を策定しておくことも求められる。

2.5.2 ICT集中リスクの予備的な評価

金融機関は、契約上の取決めにかかるすべての関係するリスクを特定し、評価する際、重要な機能をサポートするICTサービスにかかる契約上の取決めの締結が、①容易に代替可能でないICT TPSPとの契約となるか否か、②同一もしくは緊密なICT TPSPと複数の契約を締結することとなるか否か、を考慮しなければならない。契約上の取決めが重要な機能をサポートするICTサービスと関係するものである場合、金融機関には、当該TPSPの破綻時に適用される倒産法の規定、および、金融機関のデータの速やかな回復の観点において生じ得る制約を十分に考慮することも求められる。

重要な機能をサポートするICTサービスが再委託される可能性がある場合、金融機関は、再委託のベネフィットとリスクを比較考量しなければならない。また、金融機関は、再委託や再々委託が提供を受けるサービスの金融機関自身による十分なモニタリングや監督当局による金融機関の実効的な監督に与える潜在的な影響を評価する必要がある。

2.5.3 主要な契約条項

金融機関およびICT TPSPのそれぞれの権利と義務は、文書において明確にされなければならない。ICTサービスの利用に関する契約上の取決めに含まれるべき事項として、①ICT TPSPから提供を受けるすべての機能とICTサービスにかかる明確かつ完全な記述（再委託の可否を含む。）、②機能やICTサービスが提供され、また、データが処理される国・地域、③データ保護の観点からの可用性、信頼性、完全性、機密性に関する条項、④ICT TPSPの破綻時や契約上の取決めの終了時等において、金融機関によって処理されるデータへの容易にアクセス可能なフォーマットでのアクセス、復旧、返却を確保する条項、⑤サービス・レベルの記述、⑥ICTインシデントが生じた場合のコスト負担の方法、⑦ICT TPSPが金融機関の監督当局や破綻処理当局に協力する義務、⑧契約上の取決めを終了する権利と事前の通知期間、⑨ICT TPSPが金融機関のセキュリティ・アウェアネス・プログラムやデジタル・オペレーショナル・レジリエンス・トレーニング研修に参加する条件、等が列記されている。

重要な機能をサポートするICTサービスの利用に関する契約上の取決めは、上述のものに加え、①サービス・レベルの完全な記述（合意されたサービス・レベルが満たされない場合において、金融機関による実効的なモニタリングやタイムリーな改善策の実施を可能にする、合意されたサービス・レベルの範囲内における定量的および定性的なパフォーマンス指標に基づくアップデートや改正を含む。）、②金融機関に対する通知期間および報告義務、③ICT TPSPが事業コンティンジェンシー計画を実践、テストし、また、金融機関によるサービスの提供に対して適切な水準の安全性を確保するICTセキュリティ施策、ツール、方針を策定する要件、④ICT TPSPがTLPTに参加する義務、⑤ICT TPSPのパフォーマンスを継続的にモニタリングする権利（金融機関や監督当局によるアクセス、検査、監査にかかる制限の無い権利等を含む。）、⑥出口戦略（義務的で十分な移行期間の設定等を含む。）、等を含むものでなければならない。

2.6 中核要素 5：重要な ICT TPSP の監督の枠組み

2.6.1 重要なICT TPSPの指定

欧州監督機構（ESAs。欧州銀行監督機構（EBA）、欧州保険・年金監督当局（EIOPA）、欧州証券市場監督局（ESMA）から成る。）は、金融機関にとって重要なICT TPSPを指定し、また、指定したそれぞれの重要なICT TPSPについてリード監督当局（Lead Overseer）を定めなければならない。指定の基準は、①関係するICT TPSPが大規模なオペレーション上の障害に直面した場合における、金融サービスの提供の安定性、継続性もしくは品質に与えるシステミックな影響、②関係するICT TPSPに依拠している金融機関のシステム上の重要性（個々のTPSPに依拠しているシステム上重要な金融機関（systemically important institutions: SIIs）の数やSIIsとその他の金融機関との相互依存関係）、③重要な機能にかかる金融機関の同一のICT TPSPへの直接的・間接的な依拠、④ICT TPSPの代替可能性の程度、の4つである。

ESAsは、重要なICT TPSPとして指定した者に対して、その旨を通知し、また、重要なICT TPSPに指定された者は、その旨を、サービスを提供する金融機関に通知する。第三国に設立されたICT TPSPが重要なICT TPSPとして指定された場合、当該者がその指定後12か月以内にEU域内に子会社を設置する場合には、金融機関は当該者のサービスを利用できる。なお、他の金融機関に対してICTサービスを提供している金融機関、金融グループ内のICT TPSP、一国のみで活動している金融機関に同国のみでICTサービスを提供しているICT TPSP等は、重要なICT TPSPとして指定されない。

EUレベルでの重要なICT TPSPのリストは、ESAsによって作成・公表され、年次で更新される。欧州委員会は、指定の基準にかかる詳細を定める委任法を2024年7月17日までに採択し、それ以降、指定が行われることとなる。

2.6.2 リード監督者の権限

リード監督者は、担当する重要なICT TPSPについて、①すべての関係する情報および文書の提出を要請し、②調査（investigations）および検査（inspections）を実施し、③勧告を行い、④改善策の提出を要請する権限を有する。重要なICT TPSPがリード監督者の要請に応じることができない場合、リード監督者は、当該TPSPに対して、弁明の機会を付与した上で、要請が満たされるまでの間（ただし、6か月を超えない。）、当該TPSPの前年の売上高の日次平均の1%に相当する金額までの金銭の支払い（penalty payment）を日次ベースで科すことを決定しなければならない。なお、その処分が科された旨は、原則公表される。

2.6.3 情報提供の要請、調査および検査等

リード監督者は、重要なICT TPSPに対して、その職務を遂行する上で必要なすべての情報を任意もしくは義務として提供することを要請することができる。

リード監督者は、必要な場合、重要なICT TPSPの調査や立入検査を行うことができる。リード監督者は、重要なICT TPSPの監督に必要な金額を、当該TPSPに請求しなければならない。その金額の決定方法は、2024年7月17日までに欧州委員会が委任法で定めることとなる。

2.7 サイバー関連の情報共有

2.7.1 情報共有の取決め

金融機関は、自身のデジタル・オペレーショナル・レジリエンスを強化することを目的としており、信頼できる金融機関のコミュニティ内で行われ、また、情報共有の取決めに従って行われる場合、サイバーの脅威や脅威インテリジェンスに関する情報（侵害指標、戦術、技術、手順、サイバー・セキュリティ・アラート、コンフィギュレーション・ツール等）を他の金融機関と相互に交換できる。金融機関は、情報共有の取決めに参加する場合、その旨を監督当局に通知しなければならない。

2.8 監督基準等の策定

DORAは、ESAsに対し、いくつかの規定について、その詳細な基準案を規制上の技術的基準（Regulatory Technical Standards: RTS）や実施上の技術的基準（Implementing Technical Standards: ITS）として作成し、欧州委員会（EC）に提出するよう要請している（表5。なお、市中協議の時期は、ESAs等の公表資料[17]による。）。

また、欧州委員会は、2028年1月17日までに、重要なICT TPSPの指定基準や重要なサイバーの脅威の任意ベースでの通知の妥当性、第三国に本拠を有する重要なICT TPSPや第三国のICTサービス提供者への再委託の取扱い等についてレビューを行い、その結果を欧州議会および理事会に報告することとなっている。

表5. 今後策定が予定されている主な監督基準等

主な項目	種類	市中協議	ECへの提出
ICTセキュリティ・ポリシー、手順、プロトコルおよびツールの詳細（DORA第15条）	RTS	2023年6月	2024年1月17日
主なICT関連のインシデントや重大なサイバーの脅威の分類基準（18条）	RTS	2023年6月	2024年1月17日
主なICT関連のインシデントの報告の内容、各報告のタイミング、重大なサイバーの脅威の通知の内容（20条）	RTS	2023年11月	2024年7月17日
主なICT関連のインシデントの報告と重大なサイバーの脅威の通知のための標準様式、テンプレートおよび手順（20条）	ITS	NA	2024年7月17日
TLPTにかかる各種要件（26条）	RTS	NA	2024年7月17日
情報一覧のテンプレート（28条）	ITS	2023年6月	2024年1月17日
ICT TPSPから提供を受ける重要な機能をサポートするICTサービスの利用に関する方針の詳細（28条）	RTS	2023年6月	2024年1月17日
重要な機能をサポートするICTサービスの再委託にかかる評価項目（30条）	RTS	2023年11月	2024年7月17日

17 European Banking Authority, European Insurance and Occupational Pensions Authority, European Securities Markets Authority and Joint Committee of the European Supervisory Authorities (2022) 'Joint ESAs public event on DORA, technical discussion', https://www.esma.europa.eu/sites/default/files/2023-02/Joint_ESAs_DORA_event_-_ESAs_slides.pdf.

3. 考察

オペレーショナル・レジリエンスの確保は、金融機関にとって必ずしも新たな課題ではない。特に、ICTの分野では、そのセキュリティの確保などの観点から、継続的に取組みが行われてきているところである。日本においても、金融機関は、金融情報システムセンター（FISC）の「金融機関等のコンピュータシステムの安全対策基準」などを参照しつつ、ICTシステムの安全対策を実施してきている。

他方で、「必ずしも新たな課題ではない」ことは、「従来通りの対応を継続していくことで十分である」ということを意味しない。ICT関連のインシデントやサイバーの脅威が金融機関のオペレーション（さらには、金融システムの安定）に与え得る影響がより大きなものとなってきていること、また、それが故に、金融安定理事会（FSB）やバーゼル銀行監督委員会（BCBS）などの国際的な監督基準の設定主体や、英国、欧州、オーストラリア、カナダ、シンガポール等の主要な国・地域における監督当局が、オペレーショナル・レジリエンスにかかる規制・監督を強化する方向で取組みを進めていることなどから、オペレーショナル・レジリエンスの確保は、金融機関にとって「経営アジェンダ」となっている。

今般、DORAが、指令（Directive）や監督基準ではなく、法律（Regulation）として策定されたことも大きな意味を持つ。そうしたアプローチの是非には異なる意見があると推察されるものの、少なくとも、欧州の金融機関にとって、オペレーショナル・レジリエンスの確保は、喫緊の経営アジェンダとなった。そのことは、金融機関の経営陣のリードや関与が不可欠になったことを意味する。

日本の金融機関は、DORAをどのように捉えるべきであろうか。日本の金融機関の多くはDORAの影響を直接的に受けることは無いと考えられる。他方で、「グローバルや日本においても将来的に求められることとなるオペレーショナル・レジリエンスの水準」として、DORAをベンチマークに自身の現状を把握し、高度化を進めていくことは有益であると考えられる。特に、①ICTリスク管理の枠組みの構築と実践、②ICT関連のインシデントの管理および分類、③デジタル・オペレーショナル・レジリエンス・テストの実施、④ICTサードパーティ・リスクの管理など、DORAの中核要素について、金融機関の経営陣がAs IsとTo Beを認識することは重要であろう。その際、外部の専門家を活用することも選択肢の一つとなる。

監督当局にとっては、金融機関のオペレーショナル・レジリエンスを実効的に監督できるケイパビリティを高めていくことが課題の一つとなろう。金融庁は2022年12月、「オペレーショナル・レジリエンス確保に向けた考え方（案）」と題するディスカッション・ペーパーを公表し、現時点における金融庁としての考え方や今後の監督の進め方を提示した[18]。金融機関におけるベスト・プラクティスの探求を実質的に促していくためには、監督当局と金融機関との間における「深度ある対話」が不可欠である。

国としての対応も必要になる可能性がある。DORAは、金融機関にとって重要なICT TPSPを指定し、重点的に規制・監督を行っていく、というアプローチを採用している。同様のアプローチは、英国においても検討されている。英国PRAは、2022年7月に公表したディスカッション・ペーパー「オペレーショナル・レジリエンス：英国の金融セクターにとっての重要なサードパーティ（CTP）」において、「マテリアリティと集中」の観点からCTPを指定し、CTPが満たすべき最低限のレジリエンス基準を示している[19]。金融危機の後には、金融監督当局がグローバルなシステム上重要な金融機関（G-SIFIs）を指定することとなった。他方で、CTPの指定や監督は金融監督当局の権限のみでは対応できないことも想定されることから、関係当局間の連携が重要となろう。

以上

注：本稿における意見は、執筆者の私見であり、執筆者が所属する組織の公式な見解を示すものではない。

[18] 金融庁（2022）「ディスカッション・ペーパー：オペレーショナル・レジリエンス確保に向けた基本的な考え方（案）」, https://www.fsa.go.jp/news/r4/ginkou/20221216-2/01.pdf.

[19] Prudential Regulation Authority (2022) 'DP3/22 – Operational resilience: Critical third parties to the UK financial sector', https://www.bankofengland.co.uk/prudential-regulation/publication/2022/july/operational-resilience-critical-third-parties-uk-financial-sector.

執筆者

小林　晋也／Shinya Kobayashi
有限責任監査法人トーマツ
リスクアドバイザリー事業本部
リスク管理戦略センター
マネージングディレクター

Shinya Kobayashi
Managing Director
Center for Risk Management Strategy (CRMS)
Risk Advisory
Deloitte Touche Tohmatsu LLC

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 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 コーポレート ソリューション合同会社を含む）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、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約 30 都市に約 1 万 7 千名の専門家を擁し、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、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、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、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務、法務などに関連する最先端のサービスを、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し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、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 175 年余りの歴史を有し、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 415,000 名の人材の活動の詳細については、（ www.deloitte.com ）をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、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”）が本資料をもって専門的な助言やサービスを提供するものではありません。皆様の財務または事業に影響を与えるような意思決定または行動をされる前に、適切な専門家にご相談ください。本資料における情報の正確性や完全性に関して、いかなる表明、保証または確約（明示・黙示を問いません）をするものではありません。また DTTL、そのメンバーファーム、関係法人、社員・職員または代理人のいずれも、本資料に依拠した人に関係して直接または間接に発生したいかなる損失および損害に対して責任を負いません。DTTL ならびに各メンバーファーム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す。

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301