強化されるデジタル・オペレーショナル・レジリエンス

バーゼル銀行監督委員会は2024年4月「バーゼルコアプリンシプル」を12年ぶりに改訂し、オペレーショナル・レジリエンスを重要項目として追加した。欧州金融業界でもサイバー攻撃や情報通信技術に係るリスクに鑑み「デジタル・オペレーショナル・レジリエンス」強化に向けた法規制施行の準備が進んでいる。日本の金融業界は、内外の法規制の動向に注視が必要だろう。

オペレーショナル・レジリエンス項目の追加

バーゼル銀行監督委員会は2024年4月、「バーゼルコアプリンシプル（実効的な銀行監督のためのコアとなる諸原則）」を約12年ぶりに改訂した[1)]。コアプリンシプルは、銀行の健全性規制・監督の枠組みに関するグローバルな事実上の最低基準として機能し、監督当局及び銀行の自己評価のための基準として活用されている。29の基本原則（監督当局向け13、銀行及び監督当局向け16）から成り、各原則に10程度の評価基準が付随している。今般、基本原則25「オペレーショナルリスク」が「オペレーショナルリスク及びオペレーショナル・レジリエンス」と改題され、大幅な加筆が行われた[2)]。

「オペレーショナル・レジリエンス」とは、金融機関が想定外の事象が起きた際にもサービスを継続する能力、もしくは速やかに回復する能力を指す。具体的にはパンデミック、サイバー攻撃、自然災害など想定外の事象が起きた際に、その影響を耐性度内に収めるレジリエンスを意味する。

コアプリンシプルの中で、監督当局は銀行に対して、重要な業務を中断させるインシデントやその重要性の報告を含め、オペレーショナルリスクに影響を与える事態に関し、適切な報告メカニズムを常に有するよう求めている。また監督当局が、潜在的な脆弱性、例えば共通サービスへの依存、支払・決済業務のサービスプロバイダーの障害、地政学リスクを定期的に特定することを明示している。監督当局が集中リスクや潜在的なシステミックリスクに対する危機感を高めていることが窺われる。金融庁も2023年6月、「主要行等向けの総合的な監督指針」の中でオペレーショナル・レジリエンスにかかる評価項目を追加しており、日本の金融機関にとってもオペレーショナル・レジリエンスを高めることは不可避の状況となっている。

EUにおけるデジタル・オペレーショナル・レジリエンス強化

EUと英国ではオペレーショナル・レジリエンスの議論の中で特に、サイバーセキュリティやシステムリスクに対するレジリエンスを高めることに焦点を当てる「デジタル・オペレーショナル・レジリエンス」規制施行への準備を進めている。

EUではデジタル・オペレーショナル・レジリエンス・アクト（DORA）が2023年1月に発効され、2025年1月の施行に向けて、監督当局および金融業界による準備が進んでいる。DORAの目的は金融業界全体のサイバー関連リスクに対するレジリエンスを高めることである。金融機関（22,000社以上）およびICT事業者を含め、幅広い企業が対象だ。DORAはコンセプチュアルで汎用性が高い設計であるため、①具体的にどのような基準を満たせばDORAに準拠したことになるのか、②各金融機関の規模や複雑さ、リスク特性や業務の性質等に応じて、どのように規制が適用されるかという「比例原則」の論点については検討の余地が残っている。

欧州金融監督当局（ESAs[3)]）は規制上の技術標準（RTS）と、事業体が実装する必要がある技術標準（ITS）を2024年中に策定予定だ。2024年1月には第一弾としてICTリスク管理フレームワークに関する3つのRTSと、アウトソーシング登録に関する1つのITSの

NOTE

1) 「バーゼルコアプリンシプル」は、1995年のメキシコ通貨危機を契機に、新興国経済における健全性確保のための強固な基準の必要性が認識されたことを受け、バーゼル銀行監督委員会によって1997年に初版が公表された。初版公表以降、2006年、2012年に改訂が行われている。コアプリンシプルは、適用範囲が広く、非バーゼル銀行委員会のメンバー法域内の銀行や国際統一基準行ではない銀行も対象であるため、日本の国内基準行も範囲となる。出所）日銀レビュー「バーゼルコアプリンシプルの改訂」（日本銀行 金融機構局 2024年5月）。
2) バーゼル銀行監督委員会は2021年3月に「オペレーショナル・レジリエンスの諸原則」を公表しており、当該内容を踏まえた加筆が行われている。
3) 欧州監督機構（European Supervisory Authorities：ESAs）を指し、欧州銀行監督機構（EBA）、欧州証券市場監督局（ESMA）、欧州保険・年金監督局（EIOPA）から構成される。
4) 出所）ESAs publish first set of rules under DORA for ICT and third-party risk management and incident classification | European Banking Authority (europa.eu)
5) 基準として、1.影響を受ける重要なサービス、2.クライアント・金融カウンターパート・取引、3.データ損失、4.風評被害、5.期間とサービスのダウンタイム、6.地理的な広がり、7.経済的影響が挙げられている。
6) 金融サービス市場法（2023）の改正により第18条および19条に追加する形で、CTPレジームを構築した。
7) サイバーリスク、環境リスク、継続企業としての財務的存続性に関わるリスク、地政学的リスク、リーガル、レピュテーションリスク、インサイダーリスクなどが挙げられている。

最終案が公表された[4]。その中で「重大なICT関連インシデント」かどうかを判断するための7つの分類基準のリスト[5]や、各基準の詳細な重要性の閾値が具体的に示された。当該基準は欧州における改正ネットワーク及び情報システム指令（NIS2）や欧州決済サービス指令（PSD2）との平仄がとられており、今後金融業界におけるデファクトスタンダードとなる可能性がある。また、DORAへの準拠は大手金融機関中心に進められているが、「比例原則」が具体化すれば、中小金融機関でもレジリエンス強化の準備が一気に進む可能性がある。

英国におけるデジタル・オペレーショナル・レジリエンス強化

英国ではイングランド銀行（BoE）、金融行為規制機構（FCA）、健全性監督機構（PRA）が2018年に共同で、「オペレーショナル・レジリエンスの原則」を公表し、オペレーショナル・レジリエンスの議論を先導してきた。英国の銀行業界における特定ICTサービスの利用が集中している状況を踏まえ、2023年に法改正を行い[6]、監督当局が金融セクターにサービスを提供する重要なサードパーティ（CTP）を直接監督下におく「CTPレジーム」を法制化した。監督当局の勧告のもとで、財務省が2024年中にCTPの指定を行い、2025年の施行を目指している。

英国CTPレジームは、DORAと比較していくつかの相違点がある。第一にサービス単位で対象が選定されること、第二にDORAに比べてCTPに対して実践的なレジリエンス基準が示されていること、第三に想定するリスクがDORAに比べて具体化されていることだ[7]。

英国のICT事業者の多くは欧州でも事業を行っているため、グローバルな潮流はEUのDORAに収斂していくと思われる。しかしながら英国CTPレジームが求めるレジリエンス基準は、金融機関にとってICT事業者を選定する際に大いに参考になるだろう。

デジタル・オペレーショナル・レジリエンスは、サイバーセキュリティ対策やサードパーティリスク管理を包含する重要な論点である。日本の金融業界は国際協調の流れに鑑み、内外の法規制の動きに注視が必要だろう。

図表　EU DORA、英国CTPレジームの比較

	EU DORA	英国CTPレジーム
対象	**金融機関、ICT事業者の両方** •「企業」単位で監督	**ICT事業者** •「サービス」単位でCTPを監督
監督当局	欧州銀行監督機構（EBA）、欧州証券市場監督局（ESMA）、欧州保険・年金監督局（EIOPA）	イングランド銀行（BoE）、金融行為規制機構（FCA）、健全性監督機構（PRA）
CTPの指定手順	欧州監督機構（ESAs）が、監視フォーラムの勧告に基づき指名 •委任法に則り、**広範な基準**（システムへの影響、重要性、代替性等）に基づき指定	BoE、FCA、PRA勧告のもと、**財務省が指定** **•2つの明確な基準**（重要性、集中度）に基づき指定
CTPに課される基準	**特定の基準は課さない** •CTPが金融機関へもたらす可能性のあるICTリスクを管理するための、包括的で健全・効果的な規則・手順・メカニズム・取り決めを持っているか、等を検査で評価	**最低限のレジリエンス基準を当局が設定** •関連サービス特定とリソースマッピング、リスクの特定と管理、レジリエンステスト、監督当局対応力、継続性プレイブックの開発 等
金融機関に課される基準	金融機関がICTとの契約に盛り込むべき「一般原則」（場所、SLA、査察権等）をルール化	提案されていない
罰則	**前事業年度グローバル売上高1%を日割で支払**（最長6か月）	**違反の公表と失格**（英国企業へのサービス提供制限・停止・契約禁止）

（出所）各種資料より野村総合研究所作成

Writer's Profile

小野 亜樹 Aki Ono
金融デジタルビジネスリサーチ部
エキスパートコンサルタント
専門はリテール金融
focus@nri.co.jp