重要性を増すサードパーティ・サイバーセキュリティ・リスク管理

金融機関のサードパーティ・サイバーセキュリティ・リスク管理（TPCRM）が重要課題となっている。2025年1月に適用された欧州の規制枠組みは、わが国の金融機関がTPCRMを強化する上で参考にすべき点も多い。しかし、その適用に際しては、システム開発形態の違い等、内外の慣行の違いを踏まえることが重要である。

TPCRM規制の国際的な潮流

デジタル技術の進展により金融機関のITシステム依存度が高まる中、外部事業者への業務委託も拡大している。各国の金融規制当局は、サードパーティ・サイバーセキュリティ・リスク管理（以下、TPCRM）の整備を急いでいる。その1つのポイントは、サプライチェーンを通じたサイバーセキュリティ・リスクの脅威への対応である。この国際的な潮流は、バーゼル銀行監督委員会が公表した「オペレーショナル・レジリエンスのための諸原則」（2021年）により加速化した。わが国では、本文書の公表を受け、金融庁が2023年に「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」を策定、公表した。

欧州DORAのTPCRM規制

一方、欧州連合（EU）では、TPCRM強化によるレジリエンス向上を目的として、「デジタル・オペレーショナル・レジリエンス・アクト（以下、DORA）」を法制化し、2025年1月から適用を開始している。DORAは金融分野のICTリスクに特化した法律であり、わが国のICTに関する法規制である「経済安全保障推進法」や「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（以下、サイバーセキュリティガイドライン）」と類似している。しかし、TPCRMという観点からは、わが国の法規制よりも進んでおり、参考となる点が多くあると考える。

DORAは、条文と欧州監督機構（以下、ESAs）[1]が策定する標準仕様（RTS[2]、ITS[3]）により構成されている。RTSは、条文をより具体化して定めたものであり、ITSは、実務的な手順や標準化されたテンプレート類を定めたものである。

条文は、全9章から構成され、各章に紐づく形でRTSとITSが策定されている。図表は、第2章から第5章の概要と、それらに関連する主要なRTS、ITSの抜粋を整理したものだ。

TPCRMに関連する規定は、第2章から第5章に横断的に存在するが、主に第5章「ICTサードパーティのリスク管理」に集約されている。一方、第2章から第4章には、金融機関がICTリスクを管理する上で遵守すべき規定がまとめられている、その中には、サードパーティ管理に関連する規定も含まれる。

なかでも第4章「レジリエンステスト」は重要である。DORAでは、ESAsによって脅威主導型侵入ペネトレーションテスト（以下、TLPT）の実施対象となる金

図表　DORAの構成

DORA条文		主要RTS・ITS
第2章	ICTリスク管理（第5条～第16条）	ICTリスク管理フレームワークに関するRTS
第3章	ICTインシデント報告（第17条～第23条）	ICTインシデント分類基準に関するRTS
		重大ICTインシデント報告に関するRTS・ITS
第4章	レジリエンステスト（第24条～第27条）	TLPTに関するRTS
第5章	ICTサードパーティのリスク管理	ICTサードパーティとの契約に関するRTS
	第1節 ICTサードパーティのリスク管理（第28条～第30条）	情報登録簿に関するITS
		サブコントラクトに関するRTS
	第2節 重要なICTサードパーティの監督体制（第31条～第44条）	合同審査チーム（JET）に関するRTS

（出所）DORAを基に野村総合研究所作成

NOTE

1) ESAs：European Supervisory Authorities。欧州銀行監督局（EBA）、欧州保険・企業年金監督機構（EIOPA）、欧州証券市場監督局（ESMA）から構成される。
2) RTS：Regulatory Technical Standards
3) ITS：Implementing Technical Standards
4) CTPPs：critical ICT third-party service providers
5) RTS、ITSに詳細に記載されている。
6) 再委託、再々委託などのn次委託をすべて含む。

融機関が指定されている。対象金融機関にサービスを提供するサードパーティは、それに従う必要がある。TLPTの詳細な実施要件はRTSに定められている。

TPCRM規定を集約した第5章は、「（1）ICTサードパーティのリスク管理」と「（2）重要なICTサードパーティの監督体制」の2節で構成されている。（1）は、金融機関を主たる実施主体とした規定、（2）は、重要なICTサードパーティ（以下、CTPPs[4]）に対する監督当局による直接監督に関する規定である。この直接監督の仕組みは、わが国にはまだ導入されていない。

「（1）ICTサードパーティのリスク管理」には、以下の3つの重要なポイントが規定されている[5]。第一に、「サードパーティ依存関係の管理と情報登録」である。DORAでは、金融機関にICT関連サードパーティの依存関係を管理し、すべての契約情報を情報登録簿に記録し、監督当局に報告する義務が課されている。金融機関が提出した情報登録に基づき、ESAsはCTPPsを指定し、直接監督下に置くプロセスとなっている。なお、ITSには、この情報登録に関する標準テンプレートが定められている。

第二に、「ICTサードパーティとの契約の管理」である。サードパーティのICTサービスを利用する際の、ガバナンス態勢、契約ライフサイクル全体の管理プロセス、デューデリジェンスやモニタリングなどサードパーティに対する対応が細かに定められている。

第三に、「再委託[6]の管理」である。サードパーティの再委託先全体に対するリスク管理態勢として、サードパーティとの契約時における再委託先に関する明確な条件や責任範囲、および契約に明記すべき条項などが、細かく定められている。

適用の留意点

わが国も、経済安全保障推進法とサイバーセキュリティガイドラインによって、DORAのおおよそが網羅されている。しかし、前項で述べた通り、レジリエンステスト実施対象金融機関の指定、監督当局によるサードパーティの直接監督、サードパーティ情報の登録、サードパーティとの契約や再委託に関する管理など、わが国では規定化がまだ十分に進んでいないものもあり、今後、サードパーティリスク管理の高度化を図るうえで参考になる点も多い。

一方、DORAにおけるサードパーティの定義は、「サードパーティ・サービス・プロバイダー」であり、主にSaaS等を想定している。しかしわが国では、サービス・プロバイダーに加え、SIによる開発委託も重要な委託形態として併存している。これは、欧日金融機関の慣行の違いによるものである。このためDORAをわが国のSI開発管理に適用する際には留意が必要と考える。

わが国の金融機関がDORAに限らず先進的なTPCRMの適用する際には、システム開発形態に限らず、内外の慣行の違いを考慮した上で、真に必要な点を抽出し、採用することが肝要である。

Writer's Profile

斎藤 亜美 Ami Saito
金融リスク管理部
シニアコンサルタント
専門はBCP、システムリスク、証券業務
focus@nri.co.jp