

欧州DORA適用後の 金融業界の状況

EUでは2025年1月にDORAの適用が開始されたことを受けて、金融機関が当局に対し、レジストリー（ICTサードパーティサービスに関する契約情報登録簿）を提出した。サイバーレジリエンスに関する取り組みも着実に前進しているようだ。

レジストリー対応が本格化

金融業界のサイバーレジリエンスを高めることを目的としたデジタル・オペレーショナル・レジリエンス・アクト（DORA）の適用が2025年1月にEU域内で開始された。これを受けてEU域内の金融機関およびICT事業者は「ICTリスク管理」「インシデント報告」「ICTサードパーティリスク管理」「レジリエンステスト」「情報共有」の五つの要件を遵守することが求められる。なかでも負荷が大きいICTサードパーティリスク管理とレジリエンステストについて施行後1年の対応状況をまとめた。

まず、ICTサードパーティリスク管理についてだが、金融機関は毎年監督当局に「ICTサードパーティサービスに関する契約情報登録簿（Register of Information、以下、レジストリー）」を提出することが求められる。レジストリーはICTサードパーティサービス・プロバイダーとのすべての契約を体系的に記録・更新するもので、金融機関の外部委託リスクや集中リスクを測る上で重要なデータである¹⁾。加えて金融監督当局が金融機関にとって重要な機能を提供するICT事業者をクリティカル・サードパーティ・プロバイダー（CTPP）として指定する際の重要な判断材料となる²⁾。

金融機関にとって、このレジストリーのためのデータ整備は大きな作業を伴うものであった。金融機関はクリティカルで重要な機能を支えるICTサービスかどうかを一つ一つ確認し、代替可能性はあるか、再委託先はどこか、同一プロバイダーへの集中がないかといった判断が必要となる。数百社のICT事業者に委託している金融機関では、複数のソースから異なるフォーマットのデータを収集してレ

ジストリーに入力する必要がある、レジストリーとデータの整合性をとることも容易ではない。金融業界の対応の難しさから、一部の国の金融監督当局はレジストリーの提出期限を複数回延期せざるを得ないほどであった。

野村総合研究所によるヒアリングや公開情報を踏まえると、欧州におけるサードパーティリスク管理は着実に前進している。DORA対応にあたってサードパーティリスク管理やITセキュリティ管理を統合した社内横断の新たな部門を設立し、サイバーレジリエンスや事業継続に関して四半期レベルで議論する金融機関も見受けられた。CISOおよびCIO主導のもとで経営層レベルがすべてのICTサードパーティリスク契約のデューデリジェンスに関わることも少なくない。またサードパーティ管理はエクセルでの手作業に依存するケースが少なくないが、グループ内に独自のデータベースを構築し、レジストリー提出前に何回もエラーチェックを行って、データ精度の向上に取り組む金融機関もあった。

準備が進むTLPT

次にレジリエンステストに関しては大手金融機関に対し脅威ベースのペネトレーションテスト（TLPT）を少なくとも3年に1回実施することが求められている³⁾。DORAに準拠したモデルであるEU TIBER⁴⁾は2025年初にアップデートされたばかりであるため、DORAベースのTLPTの実施はまだ模索が続いているが、大手金融機関では本格的な準備が始まっている（図表）。

INGではCISO配下に40名以上のペンテスターを擁するチームを配備し、Nordeaではサイバーセキュリティ部門にテストベンダーのモニタリングやセキュリティコ

NOTE

- 1) レジストリーは15のテンプレートから構成され、契約内容、ICT サービス毎のサプライチェーン、データ所在、重要な機能を支えるICTサービスの代替可能性等を記載する必要がある。
- 2) DORA ではレジストリーのデータをもとに、欧州監督当局 (ESA) がどのICT事業者が金融機関に重要な機能を提供しているかを判断し、CTPPを指定するため、データ品質は非常に重要である。
- 3) EU TIBER (DORAに対応したTLPTモデル) では、本番環境のもとで3週間のレッドチームテストを実施することが求められる。
- 4) 出所) European Central Bank "TIBER-EU Framework updated to align with DORA (2025年2月)"
<https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews250211.en.html>
- 5) コントロールチームとは、金融機関内でテスト全体の計画と管理を担う中核チームを指す。プロジェクト管理、リスク管理、調達、関係者間のコミュニケーションを含むすべてのプロジェクト管理関連事項を担当する。
- 6) DORAの規制技術水準 (RTS) にはICTサードパーティサービス・プロバイダーのロケーションに関連するリスクが記載されている。
- 7) 金融安定理事会 (FSB) による「2026年の作業計画」にはオペレーショナル・レジリエンスが含まれる。

出所) https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024_53_Final_report_DORA_RTS_on_subcontracting.pdf, https://eur-lex.europa.eu/eli/reg_del/2024/1773/oj/eng

図表 大手金融機関の取り組み例

取り組み	ING	ABN AMRO	Deutsche Bank	Nordea
サードパーティリスク管理	- サイバー/サードパーティリスク管理への投資継続を明記 - 非金融リスク課題はイシューマネジメントシステムに記録。オーナー、リスク分類、改善期限、完了基準、証跡に基づくクローズ確認で管理	2025年コントラクトマネジメント機能を新設、サプライヤー契約やリスク管理を中央管理 - サードパーティリスク管理の一部を第三者に委託。4種類の質問票を使い、Tierに応じてサプライヤーが1つ以上の質問票に回答	2025年12月にサードパーティリスク管理AIを導入。ベンダー証跡文書を統制フレームワークに照らし分析、人間が最終判断	- サードパーティ、アウトソーシングを含むリスクを契約締結前、契約期間中、退出時に特定・評価・管理 - サードパーティ関連リスクをリスクアペイトとリスクリミット内に保つ
TLPT	Global CISO配下のオフェンシブセキュリティ CoEが40人のペンテスターを擁し、TLPT推進を担う	- オフェンシブセキュリティエキスパートがアタックシミュレーションやパープルチームング等を担う - ペンテスターおよびレッドチームングの人材募集中	包括的なセキュリティテストの一部として、レッドチームングおよびTLPTを実施	サイバーセキュリティ部門のオフェンシブテストチームがレッドチームエクササイズに参加。ベンダーの監督、ブルーチームとのパープルチームング、セキュリティコントロールテスト等を行う

(出所) ING、ABN AMRO、Deutsche Bank、Nordea HPを基に野村総合研究所作成 (2026年6月時点)

ントロールテスト等を担う専門のチームを設置している。

本番環境での実施においては、顧客への影響に配慮し、コントロールチーム⁵⁾を最少人数に絞ってテストを監視し、経営層への直接的なエスカレーションを構築するほか、事前合意した範囲以外のクリティカルな影響が懸念される場合は必要に応じて介入することも検討しているようだ。加えてTLPTの実施が必須ではない一部の中小金融機関においても、自主的に外部テスターを活用して定期的にテストを実施しているケースもあるようだ。最近ではデジタルバンクでもTLPTを実施しているという。

経営レベルでのレジリエンス意識の高まり

こうした取り組みに加え、地政学リスクの高まりを背景に、経営レベルでレジリエンスの重要度レベルは一段と上がってきている。DORAにおいてもICTサードパーティおよび親会社の所在地やデータ保存地に関するリス

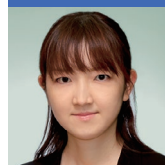
ク評価、第三国・制裁リスクの確認、代替先の確保等がテーマとなっている⁶⁾。

ロシアや中国の情勢を踏まえ、毎月地理的エクスポージャーを国家および企業レベル双方でサードパーティの集中リスクを精査し、ロケーション戦略の見直しを図る動きもある。米国のクラウドやAIサービスへの過度な依存が懸念される場合には、あえてEU域内のサービスを採用する

金融機関もみられる。出口戦略としては、インフラ全体の停止に備えて電子データ保管庫 (e-vault) やソースコードのエスクローサービスを導入する動きも広がっている。こうした取り組みはどの顧客サービスにもいかなる影響ももたらさないという強い経営層の意思に基づくものである。

DORA遵守にあたり、欧州の金融機関は「オペレーショナル・レジリエンスを高めることが、顧客や自社ビジネスを守ることにつながる」という強い意識のもとで、リソースおよびコストをかけた対応を進めている。オペレーショナル・レジリエンスの高度化は各国間で連携が進み、レベル感を合わせる方向にある⁷⁾。日本においても同様の高いレベルでの取り組みが期待される。

Writer's Profile



小野 亜樹 Aki Ono
金融ビジネス企画部
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