EUにおける デジタルレジリエンス強化の動き

EUは、金融業界のサイバーリスク等への強靭性を高めることを目的とする規制、DORAの2025年1月からの適用に向けた準備を本格化している。DORAは金融機関に加え、金融機関にICT サービスを提供するサードパーティも規制対象とする。金融機関は、ITガバナンスやリスク管理体制を再構築するとともに、信頼性の高いICTサービスを選択する必要がある。

デジタルレジリエンス強化を促す法規制

EUはサイバー攻撃の脅威を軽減し金融システム内の安定性を高めることを目的とした規制、デジタル・オペレーショナル・レジリエンス・アクト[1](DORA)の2025年1月からの適用に向けた準備を進めている。

DORAは、情報通信技術（ICT）関連のインシデントに対するレジリエンス強化を目的に、①ICTリスク管理、②ICTインシデント報告、③レジリエンステスト、④ICTサードパーティのリスク管理の4軸から構成される[2](図表)。

図表　DORAの求める主な要件

カテゴリー	概要
①ICTリスク管理	•企業戦略や目標に沿ったICTリスク管理の枠組策定（主要業績評価指標と主要リスク指標の策定を含む） •デジタルオペレーショナルレジリエンステストの実装方法に関する詳細説明 •ビジネス機能、プロセス、サードパーティの依存関係等をマッピングする包括的なビジネスインパクト分析実施 •脅威検知から対応、復旧、コミュニケーションまでの第一線の防衛線強化
②ICTインシデント報告	•ICT関連の重大インシデントに関する初報、続報、最終報告書を当局へ提出 •自社にとって重要な機能、重要なサードパーティ・プロバイダーを考慮し、インシデント対応計画をテスト •ICT関連インシデントの根本原因分析のタイムリーな実施、ステークホルダーへの報告
③レジリエンステスト	•すべての重要なICT機能について、脆弱性評価やシナリオに基づくテストを年に1回実施 •金融システムにおいて重要と判断された金融機関は、3年ごとに脅威ベースのペネトレーションテストを実施（重要な機能を提供するICTサードパーティ・サービスプロバイダーはペネトレーションテストに含める） •脆弱性に対処するための効果的な修復とフォローアッププロセスの確立
④ICTサードパーティのリスク管理	•契約段階に先立ってICTサードパーティ・サービスプロバイダーのコンプライアンスを検証するための効果的なプロセスの確立（契約に際し、出口戦略、監査、アクセシビリティ、セキュリティなどのパフォーマンス目標について交渉） •ICTサードパーティ・サービスプロバイダーの依存関係のマッピングと集中リスク評価の実施 •ICTサードパーティ戦略の定期的な見直し

（出所）DORAより、野村総合研究所抄訳

DORAの対象には、EUに所在する金融機関（銀行、証券会社、ファンド提供者、保険会社、決済処理業者等）だけでなく、金融機関にICTサービス（クラウドプラットフォームやデータ分析サービス等）を提供するサードパーティも含まれる（EUに拠点を置く日系金融機関、ICTサードパーティを含む）。また、金融機関のグループ内でICTサービスを提供する場合も、同規制の枠組みに従う必要があり、DORAの影響を受ける企業は金融機関だけで22,000社以上にのぼる。

サイバーセキュリティを強化するためのディレクティブやガイドラインは以前から複数存在したが[3]、DORAは分散したサイバーセキュリティ関連基準の重複やギャップの解消を目指した統一的な規制であるため、今後、国際標準のベンチマークとなる可能性がある。また、DORAは法的拘束力を持つ規制であり、違反した場合には金銭的ペナルティ（最大一日あたりグローバルでの前年売上高1%）が課される。

DORA対応のポイント

DORA遵守にあたり金融機関にとってチャレンジングな点として三点挙げられる。第一に、ICTリスク管理の範囲が非常に広範なことである。経営層は、自社のICT資産・情報、プロセス、システム間の相互関係、サードパーティへの依存関係を正確にマッピングすることが求められる。またDORAは金融機関に、ICTリスクに対するリスク許容度を定めた上で、明確なセキュリティ目標を設定することを求めている。

第二に、レジリエンステストの負荷が高いことである。DORAは、自社にとって重要な機能[4]を支えるシス

野村総合研究所　金融デジタルビジネスリサーチ部　©2024 Nomura Research Institute, Ltd. All rights reserved.

NOTE

1) 「デジタルオペレーショナル・レジリエンス」とは、ICTサービスの運用が中断されても企業がサービスの継続性と品質を保証し続ける能力を指す。
2) 情報共有（サイバー脅威に関する情報を金融機関間で共有）についても項目として記載することを推奨。
3) 類似ガイドラインとして、EBAによる“Guidelines on ICT and security risk management（2019年）”や、ISO27001が挙げられる。
4) 金融機関にとって「重要な機能」とは、金融機関の財務実績、そのサービスおよび活動の健全性または継続性を著しく損なう機能、またはその機能の中断、欠陥、または失敗が金融機関の認可の条件および義務の継続的な遵守を著しく損なう機能を意味する。
5) 具体例として、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レビュー等が挙げられる。
6) アドバンストテスト（脅威主導型ペネトレーションテスト、TLPT）は、システミックな重要性と成熟度が一定の閾値以上の企業に課されるテストで、少なくとも3年毎の実施が求められる。
7) European Supervisory Authoritiesの略称で、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。
8) 2022年に施行された「経済安全保障推進法」とDORAは、サイバー攻撃への対応強化を目的とする点では類似しているが、相違点もある。「経済安全保障推進法」は電気、ガス、水道、鉄道、金融等が対象分野で、政府が対象企業を指定し、対象企業がITシステム等を導入する際、その導入計画を政府自らが事前審査する。一方でDORAは主に金融分野を対象とし、金融機関が自社にとって重要な機能を支えるシステム等を特定する。また、想定するリスクが、テロのみならず、電源障害やITシステムの停止までと広範なため、より多様なシナリオの想定が必要。

テムおよびアプリケーションについて、少なくとも年一回、適切なテスト[5]を実施することを求めている。テストで脆弱性が認められた場合には、修復とフォローアップを通じて「完全に対処」することを求めるため、テストを実施しただけでは不十分だ。また、これまでのレジリエンステストにない試みとして、ICTサードパーティ・サービスプロバイダーをより厳格なアドバンストテスト[6]に含めることを求めている。

第三に、金融機関はICTサービス利用に際し、事前に、集中リスクや再委託かどうか等を含め、複数の要素を加味した評価が求められることだ。また、利用するICTサードパーティ・サービスプロバイダーが最高水準の情報セキュリティ基準を満たしているかのみならず、重要な機能を提供するか否かを判断し、重要な機能を提供している場合には代替手段や出口戦略を用意しなければならない。

新たな概念「クリティカルサードパーティ」

DORAでは、特定のICTサービス利用の集中がもたらす潜在的なシステミックリスクを踏まえ、金融機関にとって特に重要なICTサービスや機能を提供する「クリティカルサードパーティ・プロバイダー（CTP）」を金融監督当局が直接監督することになっている。欧州金融監督当局（ESAs）[7]によって、金融サービスへの影響（利用している金融機関の数や資産等）、重要性（システム上重要な金融機関 SIFIsへの依存度等）、機能の重要性、代替可能性等を勘案した上でCTPが指定され、年次でリストが更新される。

各監督当局（EBA、EIOPA、ESMA）は、CTPに指定されたサードパーティに対して、情報開示要求や立入調査を行う権限をもち、指示に従わない場合は業務停止を求めることができる。金融機関側は、CTPがもたらすICTリスクの影響を定量化し、脅威ベースのレジリエンステストを年次ベースで実施し、脆弱性を解消するための対策を講じなければならない。なお、英国でも同様に金融監督当局によるCTPのモニタリング対応に向けた準備が進められている。

求められる透明性の高いICTサードパーティ管理

DORA自体が日本の金融機関や企業に直接影響することはないものの、G7諸国は「金融セクターにおけるサードパーティ・サイバーリスク管理のためのG7基本的要素」など、類似の方針をフォローすることを表明しており、デジタルレジリエンス強化はグローバルレベルの共通アジェンダとなっている。

日本の金融業界においても、オペレーショナルレジリエンス強化やITガバナンスの高度化が求められる中で、経済安全保障推進法への対応[8]も進められている。デジタルインフラの欠陥や脆弱性は、ITに限った問題ではなく、経営層を巻き込んだ企業全体の問題である。金融機関は、ガバナンスやリスク管理体制を再構築するとともに、透明性の高い評価軸をもとに信頼性の高いICTサービスを選択することが求められる。

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