03

リスク管理

経済安全保障推進法改正と金融機関の対応

経済安全保障に関する「官民協議会」の創設により、参加が必要な金融機関は厳格な情報管理態勢構築が求められる。また、継続検討事項となった「データセキュリティ」については法制化を待たず、欧米規制を参考に、個人データの取扱いや委託先管理など、早期の準備に着手すべきだ。

近年の厳しい安全保障環境や地政学的な緊張の高まりの中、安全保障上の観点から国家として守るべき対象が経済分野まで広がるようになり、2022年5月に経済安全保障推進法[1)]が公布された。公布から4年が経過し、金融機関に影響のある「基幹インフラ役務の安定的な提供の確保に関する制度」（以下、基幹インフラ制度）は、2024年5月に運用が開始され、丸2年が経過した。内閣府の公表資料によれば、2024年度に、金融分野で全体のおよそ4割にあたる386件の届出・政府審査が実施されており、その実績を踏まえて内閣府、金融庁の解説書等[2)]が順次微修正されている。

経済安全保障推進法の附則で公布後3年を目途に法改正することとなっており、この作業のため2022年7月より有識者会議にて検討が進められ、2026年1月に「経済安全保障の更なる推進に向けた提言」（以下、提言書）がまとめられた。提言書をベースとした法律案が3月19日、閣議決定。2026年特別国会での審議を経て、可決・公布される見込みとなっている。

本稿では、法律案及び提言書から金融機関にとって重要な「官民協議会」と「データセキュリティ」について解説する。

もうひとつの官民協議会の創設

国家が守るべき対象を経済分野にまで拡大する為には、その担い手である民間との連携が重要である。提言書では、官民連携の枠組みとして官民協議会の創設が提言され、法律案にも盛り込まれた。官民協議会でのテーマは、顕在リスクへの対応、潜在リスクの分析および平時・有事の対策の点検となっているが、とくに影響が大きいのは、「情報の取扱い」である。

官民協議会では、政府保有の機微情報が民間に連携されることを想定し、協議会の構成員は国家公務員と同等の罰則を伴う守秘義務を負う。先行するサイバー対処能力強化法[3)]の官民協議会は、2026年10月1日に創設される予定だが、この官民協議会でも、政府保有の機密情報（サイバー攻撃の背景情報等）が共有されるため、必要に応じセキュリティ・クリアランス[4)]の取得が求められる。今回の経済安全保障推進法の官民協議会では、セキュリティ・クリアランスへの言及はないが、今後の国会審議の中で、議論される可能性があると考えている。機微情報の連携は有意義ではあるが、ただ守秘義務により情報伝達に制約が生じるため、担当部署を明確にし、情報管理態勢とその活用方法を検討する必要がある。

経済安全保障における「データセキュリティ」

提言書はデータセキュリティに関し、民間保有データの流出等が国家及び国民の安全を害するおそれがあることから、重要インフラに関するデータ及び機微な個人データの保護の在り方について国が責任もって対処するとしている。特に機微な個人データについては、個人の権利利益の保護を目的とした個人情報保護法があるが、安全保障の観点からの法制・制度は存在しない。検討が進む欧米制度と比較すると漏洩・改ざん・滅失等に対して、データの保有者と保存・処理先の体制は十分とはいえない状況にある。個人情報保護法との重複感は否めないが、そのバランスに留意した制度設計が求められる。

上記に関連し、個人情報に関するデータの保有者と保存・処理先であるデータセンター・クラウド事業者等の

野村総合研究所　金融ITイノベーション事業本部 事業企画室　

NOTE

1) 正式名称は、「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」。
2) 「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説」および「金融分野における経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説」。
3) 正式名称は、「重要電子計算機に対する不正な行為による被害の防止に関する法律」。
4) 「重要経済安保情報の保護及び活用に関する法律」における適正評価。
5) Network and Information Systems Directive 2022/2555
6) PART 202—ACCESS TO U.S. SENSITIVE PERSONAL DATA AND GOVERNMENT-RELATED DATA BY COUNTRIES OF CONCERN OR COVERED PERSONS
7) Cybersecurity & Infrastructure Security Agency
8) SECURITY REQUIREMENTS FOR RESTRICTED TRANSACTIONS E.O. 14117 Implementation
9) 本提言書で医療分野の追加が提言され、結果、16分野になる予定。
10) Digital infra structureおよび、ICT service management (business-to-business)
11) Critical Third-Party Provider

実態把握が課題として取り上げられている。具体的な記述はないが、データセンター・クラウド事業者の政府による直接監督も検討の視野に入っているようである。

いずれにせよ、データセキュリティについては、有識者会議でも議論が尽くされていないとして結論を見送っており、現時点では詳細まで踏み込めないが、有識者会議の中では、「機微な個人データの管理」は米国の大統領令14117を、「データセンター・クラウドサービスの規律」は、米国の情報通信技術・サービスサプライチェーン保護規則、欧州のNIS2指令[5]、英国のNIS規則等が例示されており、これら欧米の制度がヒントになろう。

欧米のデータセキュリティ制度

米国大統領令14117は最終規則[6]が2025年10月に施行されている。最終規則は、閾値以上の機微な個人データへのアクセスを伴う特定の取引・契約を、懸念国（中国（香港、マカオ含む）、キューバ、イラン、北朝鮮、ロシア、ベネズエラ）や懸念国の影響下にある者との間で禁止又は制限している。この機微な個人データには、金融データ（閾値は10,000件以上）が含まれるが、データ自体の売買取引は禁止され、機微な個人データを直接アクセスするベンダー契約、雇用契約も制限される。

雇用契約の具体的な例として、懸念国の市民権を持ち、主な居住地が懸念国である社員との雇用契約は制限される。また、ベンダー契約の例では、本社が懸念国の場合、米国企業のデータセンターとのベンダー契約が制限される。ここでの“制限”とは、組織的な措置、アクセス制御の実装、データのマスクなどを含む米サイバーセキュリティ・インフラセキュリティ庁（CISA[7]）のセキュリティ要件[8]を満たすことだが、このセキュリティ要件を満たさない場合は、そもそも例示した雇用契約、ベンダー契約は結べないことになる。厳しいハードルと言えよう。

NIS2指令では、エネルギー、金融等のほかに、日本の基幹インフラ制度の対象分野[9]ではないデータセンター・クラウドサービス分野[10]も規制されている。各国で差はあるが、提供サービス内容や規模に応じて当局が指定もしくは企業自ら登録した場合、対象となる。対象となった事業者は、当局から直接監督される。

NIS2指令では、金融機関も監督の対象だが、金融に特化した制度のデジタル・オペレーショナル・レジリエンス法（DORA）が優先される。DORAでは、金融機関を規制するだけでなく、金融機関向けクラウドサービスをCTPP[11]として指定し、金融当局が直接監督する。両制度とも施行済みだが、二重の枠組みでの具体的な運用方法について未定の部分も多く、欧州のベンダーにヒアリングすると、まずはDORA対応に注力しているようである。

「データセキュリティ」については、2026年特別国会での審議は見送られているため、準備期間は1年以上ある。政府では、個人情報保護法との整理や、欧州に倣った金融機関に特化した制度を作るか等の検討が進むと思われるが、米国の大統領令14117、欧州のNIS2指令とDORA等を参考に、準備に着手しないと間に合わない恐れもある。

Writer's Profile

堤 順 Jun Tsutsumi
金融ITイノベーション事業本部　本部付
シニアチーフエキスパート
専門は金融向けGRC
focus@nri.co.jp