経済安全保障推進法の事前審査非対象金融機関のリスク管理

経済安全保障推進法によって外部委託先を含めたリスク管理措置に関連する規制は強化される方向にある。経済安全保障推進法の事前審査非対象の金融機関でも、国際的なサードパーティリスク強化の動きもあり、品質管理・委託先審査・業務継続策の再点検が必要となるだろう。

経済安全保障推進法における非対象金融機関の扱い

2023年11月17日、経済安全保障推進法[1]の事前審査対象企業として、金融機関では59社が指定され、6か月の経過措置後の2024年5月の制度運用開始に備え事前審査の準備を進めている。本稿では、今回指定されなかった非対象金融機関が今後、留意すべき点について海外の動向等も踏まえ考察する。

2023年4月28日に経済安全保障推進法に基づき閣議決定された「特定妨害行為の防止に関する基本指針」（以下、基本指針）[2]において、「特定妨害行為」を「特定重要設備の導入又は重要維持管理等の委託に関して行われる我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為」と定義している。金融庁は、この「特定妨害行為」を防止できるかの観点で事前審査することとしている。

基本指針では、「特定妨害行為の例に関する事項や、望ましいリスク管理措置の例等の特定妨害行為の防止に資する情報」について「内閣総理大臣及び事業所管大臣は、指定基準に該当しない者や設備供給に関わる幅広い者等に対しても適切な情報提供等を行う」とし、関係者との円滑な連携を促しており、非対象となった金融機関も経済安全保障推進法の埒外にあるわけではない。

サードパーティリスクに注目する海外規制当局

経済安全保障推進法では、特定重要設備の供給者とその委託先をリスク管理措置の対象とし、これら供給者・委託先（サードパーティ）も事前審査の対象としている。

他方、海外においても、サードパーティに対するリスク管理が注目され、2023年12月4日には、金融安定理事会（FSB）が、「サードパーティリスクの管理とオーバーサイトの向上：金融機関と金融当局のためのツールキット」を公表した。本ツールキットには、バーゼル銀行監督委員会（BCBS）[3]、証券監督者国際機構（IOSCO）[4]、保険監督者国際機構（IAIS）[5]が公表した資料が例示されており、それぞれ若干の差異はあるものの、サイバー攻撃による妨害行為に対するオペレーショナル・レジリエンス（業務の強靭性・復旧力）を主なテーマとしている。中でも、BCBSは、2023年11月に公表した「オペレーショナル・レジリエンスのための諸原則及び健全なオペレーショナル・リスク管理のための諸原則の改訂の適用状況に関するニューズレター」の中で、「本レターは新たな当局監督のガイダンスや期待を示すものではない」としながらも、「各国の適用状況を引き続きモニタリングする」としている。

IT要員の一部を委託先から提供を受ける特殊な労働市場環境にある日本の「委託先」と欧米諸国における「サードパーティ」とは必ずしも一致するものではないが、委託先・サードパーティを含めたリスク管理における制度が、国際的な枠組みの中で強化される方向である。

非対象金融機関が対応すべきリスク管理措置

海外規制をきっかけに強化されると見込まれる委託先・サードパーティを含めたリスク管理に関連する国内規制を見据え、現時点では経済安全保障を意識していない事前審査の非対象金融機関においても、対象金融機関が準備している経済安全保障対応のうち次に挙げる3点

NOTE

1) 正式名称、「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) 正式名称、「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針」。
3) 公表資料（「オペレーショナル・レジリエンスのための諸原則」および「健全なオペレーショナル・リスク管理のための諸原則の改訂」2021年）」。
4) 公表資料（「アウトソースのための諸原則」2021年）。
5) 公表資料（「保険セクタにおけるオペレーショナル・レジリエンス公表資料」2022年）。

について再点検することを提案したい。

【悪意のあるコード混入を考慮した品質管理】

ITシステムの品質管理はシステム障害の未然防止策の根幹であり、これまでも最大限の努力がなされてきた。しかしながら、それはあくまでも「不作為：ミス」への対応であり、社員、委託先を含めたIT要員に悪意を持つ者が含まれる可能性は考慮されていない。もし、社内のIT部署に、悪意を持つ者が含まれる可能性を考慮して品質管理するように指示すれば、現場からは「できない」と返ってくるだろう。もし（特定妨害行為に該当する）悪意を持ってコードを作られれば、見つけるのが極めて困難だからである。

しかし、システム開発工程の中に、悪意のあるコードがないかの観点でのチェックプロセスを組み入れ、そのチェックプロセスを社内外の事案をもとに継続的にバージョンアップできれば、完全ではないものの十分に効果は期待できる。

【外部の主体者からの影響を考慮した委託先審査】

これまでも、金融機関では一定の委託先審査を実施している。それは、もっぱら委託先企業の財務の健全性や反社会的組織との関係を考慮したものである。

経済安全保障推進法では、事前審査の提出資料として役員の国籍・生年月日、5%以上の議決権保有者の国籍の提出を求めている。また、「同盟国・同志国に対する妨害行為に関与したとの指摘はないか」、「外国政府との取引高が25%以上の場合、どの政府と取引しているのか」を考慮することを求めており、国内関連法規では外国為替及び外国貿易法が例示され、国際的に受け入れられた基準ではOECD外国公務員贈賄防止条約が例示されている。

対象金融機関では、自社の委託先審査をこれら事前審査の水準に高めることになる。非対象金融機関においても、社内の委託先審査を、審査対象と審査の考慮点を拡大して、「外部の主体者からの影響」を考慮した審査プロセスに見直すことが求められる。

【サイバー攻撃を危機事象に加えた業務継続策】

経済安全保障推進法では、サイバー攻撃を受けた場合でも、役務を安定的に提供し続けるための事業継続策が求められている。これまで、業務継続策は自然災害やパンデミックを中心に準備し、サイバー攻撃に関してはCSIRT（Computer Security Incident Response Team）によるインシデント管理の整備や脆弱性診断など専門組織を作り対応していても、必ずしも、業務継続策とサイバー攻撃を融合した活動をしていない企業もある。

この2つを融合させて、業務継続策の危機事象にサイバー攻撃を加え、かつサイバー攻撃の対象を委託先にも拡大して、委託先経由で、インターネットに接続のないITシステムもサイバー攻撃を受けることを想定した業務継続策を作りなおす必要がある。

将来強化されるであろう規制の観点からも、また経済安全保障本来の目的からも、非対象金融機関でも、品質管理、委託先審査、業務継続策の既存の枠組みに、わが国の外部から行われる妨害行為という新たなリスクを認識して再点検する必要があるだろう。

Writer's Profile

堤 順 Jun Tsutsumi

金融リスク管理部長
専門は金融向けGRC
focus@nri.co.jp