# 経済安全保障推進法が想定するリスクの再確認と新たな課題

経済安全保障推進法の運用が開始され1年が経過した。従前のITガバナンスの枠組みでは十分でない事項が含まれており、改めて、新たなリスクとして再確認する必要がある。また、ISMAP認証クラウドの扱いやネットワーク機器への対応などの新たな課題も浮上している。

2024年5月に経済安全保障推進法[1](以下、経済安保法）の運用が開始されて1年が経過した。特定社会基盤事業者[2]として指定された金融機関は、特定重要設備を「導入」（もしくは大規模更改）と「維持管理」の委託契約締結（もしくは更新）する場合に、「導入等計画書」を届出、審査を受けてきた。いずれの場合も、概ね、これまで金融庁と対話を続けたITガバナンス[3]の枠組みに沿って、リスク管理態勢を整備したものと思われる。

しかし、経済安保法関連の「基本指針」[4]に「基幹インフラの重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されることを防止する」とあり、近年の状況から「国家を背景とした（意思を持った）妨害行為」に対する事項が必要であることから、既存のITガバナンスの枠組みでは十分でない事項が含まれる。ここでは、審査実績の多い「維持管理」の分野から主だった留意すべき項目を分析する。

## 経済安保法の広範囲にわたるリスクの確認を

経済安保法の対象は広くサプライチェーンを含めた関係者となっている。そのなかで妨害行為に加担する者がいないかどうかをチェックするというものである。これは既存のITガバナンスの枠組みにはない新たなリスクを想定したものである。これに着目して3点ほど指摘したい。

**①設計書に関するリスク管理態勢**

既存のITガバナンスでは、メンテナンス効率の低下や品質の劣化をリスクとして、設計書の版管理や更新権限の管理が求められてきた。また、システム障害を即時に対応することから考えれば、最新かつ正確な設計書は、障害対応を行う者から、いつでも広く閲覧できる方が望ましい。しかしながら、経済安保法では、IT体制のなかに妨害行為を企図する者が居るという仮定に立つ必要があるため、いつ、だれが、何の理由で閲覧したかを管理する必要がある。さらに、閲覧できる者も極力限定的にしておく方が望ましい。

**②監視カメラ等に関する取り扱い**

既存のITガバナンスにおける監視カメラ等の役割は、承認・申請されていない箇所への不正なアクセスがないことの確認と設置されていることによるけん制機能等である。一方、経済安保法では、国内外の過去の具体的な事案を基に、監視カメラ等にバックドアが仕込まれ、不正に情報を入手されたり、外部からの攻撃で映像記録が停止されたりしないよう、購入時に監視カメラ等の供給者の所在国及び法制度を確かめ、欧米各国の制裁リストに含まれていないことなどを確認する必要がある。

また、他社のデータセンターを利用する場合においては、データセンター選定の際、これらの情報提供は重要な選定要件となる。

**③委託の相手方等の従事者に対するリスク評価**

既存のITガバナンスでは、委託の相手方等の維持管理の従事者に対するリスク管理は、本人であることの確認、その本人の権限と行為が合致しているかの確認が中心であった。経済安保法では、さらに一歩踏み込んだ内容となっている。特定社会基盤事業者は、委託の相手方等との間で、作業従事者の所属・専門性の情報を入手できることを契約で締結する必要がある。情報提供の意図は、当然、入手した情報を基にリスク評価することを促したものである。経済安保法では、政府が委託の相手方等の役員、株主の国籍情報を入手し、「外部の主体から

**NOTE**

1) 「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」(令和4年法律43号)。
2) 事業所管省庁において特定社会基盤事業者として指定した者は以下の通り。
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_jigyousya.pdf
3) 「金融機関のITガバナンスに関する対話のための論点・プラクティスの整理」参照。
https://www.fsa.go.jp/news/r4/sonota/20230630/02.pdf
4) 「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」参照。
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/doc/kihonshishin2.pdf
5) 「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」。

強い影響がないか」を考慮事項として審査しているが、金融機関においては、委託の相手方（企業）だけではなく、作業従事者個々人についても、同様に扱う考慮事項と考えるべきだろう。

## 浮上してきた今後の課題

スタートの初年度を終え、態勢を整えるなかで制度上の課題も何点か浮上している。

**①ISMAPについて**

特定社会基盤事業者が、特定重要設備を構成する設備として、ISMAP認証を持つクラウドサービスを導入する場合、政府はすでに、ISMAP制度によって評価済みとして、重複を避け、「導入」の審査を省略可能としている。一方、「維持管理」の審査ではこの省略規定がない。ISMAP認証のクラウドサービスが、特定重要設備の一構成設備を担う場合、クラウドサービスが「維持管理」に当たるかどうかという議論である。

クラウドサービスを「維持管理」と位置付ければ、そこでのリスク管理措置や再委託先の相手方等の情報を届け出る必要がある。しかし、通常のクラウドサービスにおいて、それらの情報をサービス提供先には開示されていない。「導入」の審査と同様に省略を可能とすればこの問題は生じないものの、いまのところどうなるのかまったく不透明である。ISMAPでの審査が、「維持管理」の審査の省略に足るものかが吟味されるものと思われる。

**②運用状況の評価について**

経済安保法の審査では、リスク管理措置の整備状況を審査対象とし、整備されたリスク管理措置を確実に運用しているかまでは審査の対象としていない。

これは、これまでの金融行政により、金融機関では当然適切に運用するであろうという当局との信頼関係が前提となっている。通常の内部監査の枠組みや監査法人の保証報告書の枠組みなどを活用し、運用状況を確認することで対応可能となろう。

**③ネットワーク機器について**

金融業界での審査対象となる構成設備は、「業務アプリケーション」「サーバ」「OS」「ミドルウェア」の4種類となっている。しかし、「ネットワーク機器」については、制度開始前には検討されていたと推察されるが、最終的には当時の14業種（現時点では15業種）から一律に、構成設備から外された。

2025年5月23日に公布された能動的サイバー防御法[5]では、特定社会基盤事業者は、特定重要設備（本法では、“重要電子計算機”）のインターネット接続部分のネットワーク構成図を提出する必要がある。そのため、経済安保法の制度変更を待たずとも、届出の準備は必要である。この1年で、官民双方で経済安保法の知見が蓄積された。また、能動的サイバー防御法も公布され、地政学的緊張への備えは拡充しつつある。こうした環境変化も踏まえ特定社会基盤事業者は、たんに制度対応とだけ考えるのではなく、新たなリスクへの備えとして、積極的に対応することが求められる。また、経済安保法非対象金融機関に対しても蓄積された知見を展開することが、金融業界として有益と考える。

## 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