経済安全保障推進法「事前審査」を通じてBCPの実（じつ）も取る

経済安全保障推進法の成立に伴い、「国外から行われる役務の安定的な提供を妨害する行為」（主にサイバー攻撃）のリスクに関して、審査が行われる。各企業は、審査に向けた準備を進めるとともに、この制度施行をBCP再点検の契機と捉え、危機からの対応力を維持、向上させていくことを推奨したい。

経済安全保障推進法の成立

2022年5月、「経済安全保障推進法」（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」）が成立した。本法律ではわが国の安全保障の確保に関する経済施策として4つの施策を掲げている。第2の柱である「基幹インフラの安全性・信頼性の確保」は、金融事業者への影響が大きい規制強化策である。

図表1　経済安全保障推進法における4つの施策

<1>	<2>	<3>	<4>
サプライチェーンの強靭化への支援	基幹インフラの安全性・信頼性確保	先端技術開発における官民協力	特許出願の非公開

（出所）内閣府の資料

「特定妨害行為」を防ぐための予防策

本施策は、基幹インフラの重要設備が国外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「特定妨害行為」を防止するため、重要設備の導入及び維持管理等について「事前審査制度」を創設するという主旨のものである。基幹インフラ14事業のうち、特定社会基盤役務の提供を行うとして政令で定めた事業を「特定社会基盤事業」とし、中でも特に主務省令で定める基準に該当する「特定社会基盤事業者」は、特定重要設備の導入または重要維持管理の委託に際して、「導入等計画書」を主務官庁に提出しなければならない。

図表2　本施策で定める重要インフラ事業 14分野

情報通信	ガス	石油	水道	鉄道
貨物自動車運用	外航貨物	航空	空港	電気通信
放送	郵便	金融	クレジットカード	

（出所）内閣府の資料

計画書に含める内容は、国が定める共通事項と、主務省令で定める個別事項とに分かれる。前者では、設備の概要や導入/委託計画等が審査対象であり、設備の導入/委託時点で国外からの脅威が入り込むのを未然に防ごうとする「予防策」と言える。

サイバー攻撃対策としてより実効性のある審査に

「特定妨害行為」とは具体的に何か。事前審査制度は、重要設備の導入時に不正なソフトウェアが埋め込まれることや脆弱性が放置されることによる外部からの妨害行為、つまり主にサイバー攻撃によって有事の際に誤作動を起こされる事態を想定している。そのため、設備を指定することで、設備の供給者や部品の出所を詳らかにする。

しかし昨今、IT技術の進歩とともにサイバー攻撃も巧妙化、多様化しており、どこまで詳細に設備の情報を集めればリスクに対応できているとは言い切れない。すべての脅威を「予防策」だけで防ごうとするには限界がある。

思うに、経済安全保障推進法は法律自体としては攻撃に対する予防という建付けになっているが、わが国の安全保障政策の一環として捉えるならば、その運用につい

ては受け身だけの「予防策」に終始すべきではない。そのため、事前審査の計画書の一部にBCPを含めることで、本法律の実効性をさらに高めることができるのではないかと考える。仮にサイバー攻撃を受けたとしても、適切なBCPの発動によって、特定社会基盤役務の安定的な提供を保つことができる。

今後金融庁によって経済安全保障推進法が具体化される中、国のサイバー攻撃対策の司令塔である内閣サイバーセキュリティセンター（NISC）のガイドラインが参考にされると予想する。経済安全保障推進法の「基幹インフラ」、NISCの「重要インフラ」は、それぞれ対象を14分野に定めており、いずれにも金融分野は含まれる。

NISCの「重要インフラのサイバーセキュリティに係る行動計画」では、重要インフラを取り巻くリスクに対して、リスクを許容範囲に留めること、また障害体制の整備・強化と適切な対応、迅速な復旧を行うことにより強靭性を確保することで、安全かつ持続的な提供の実現を目指すとしている。

サイバー攻撃を含むあらゆるリスクへの対策としては、「予防策」に加えて、万が一防ぐことができなかった時にどのように対処するのか、重要サービスを停止させることなく維持継続するために何を準備しておけばよいのか、といった「レジリエンス策」が不可欠であることが分かる。

また、既にBCPを策定している企業であっても、地震やパンデミックといった特定の原因事象に対してのみ適用される従来のBCPでは、昨今の環境変化、拡大する情報セキュリティリスクに対応しきれない。それらの脅威に対応していくためには、情報セキュリティリスクもBCPの一部として組み込むべきだろう。

2024年の制度施行に向けて

金融庁においては、2022年7月に経済安全保障室が発足した。事前審査に関する詳細情報はいまだ公表されていない。国会答弁では、米国のように、使用してはいけない製品や事業者等を公表するといったブラックリスト的アプローチは取らないとされているが、企業としては予見性の観点から、審査基準の一定の開示はしてもらいたい。一言で設備の概要といっても、委託先や機器一覧、委託先経営者、実質的所有者、再委託先再々委託先…と多岐にわたる。当局としても、膨大な審査物件から審査を行うのは至難の業だろう。「予防策」の審査は一定の範囲に留め、「レジリエンス策」であるBCPを審査物件に加えそちらに重心を置いた方が、実効性を担保しつつも双方の負荷を抑えることができるのではないか。

企業にとっては、この度の事前審査制度は相応の負担になることが予想されるが、これをBCP再点検の契機と捉えてほしい。制度施行に向けて、「予防策」の準備と同時に、BCPにサイバー攻撃の概念を取り入れる等といった「レジリエンス策」の検討を進め、危機からの対応力を維持、向上させていく活動を推奨したい。

Writer's Profile

斎藤 亜美 Ami Saito
金融ガバナンスプラットフォーム企画部
コンサルタント
専門はBCP、システムリスク、証券業務
focus@nri.co.jp