経済安全保障推進法で金融機関に求められる対応

金融調査部　金本 悠希

要　約

2022年5月11日、経済安全保障推進法が成立した。近年、インフラ企業を対象とするサイバー攻撃が多発しているため、経済安全保障推進法では、電気、通信、金融等のインフラサービスが安定的に提供されるよう、インフラ企業が重要設備（システムを含む）の導入等を行う場合に、政府が事前に審査する制度が導入された（2024年2月までに適用開始予定）。問題がある場合、導入等の方法の変更や中止が勧告・命令される。

本制度によりサイバー攻撃のリスクの低減が期待されるが、サイバー攻撃への対処には複数の防衛手段を取るなど、総合的なサイバーセキュリティ対策が重要である。さらに、インフラサービスに加え、米国の制度では保護の対象である、国民の機密個人データや先端技術等の保護・流出防止策についての検討も望まれる。

対象事業者の範囲等は今後政省令で決定される予定だが、対象となる可能性のある金融機関は、導入しようとしているシステムの設計・開発等に、サイバー攻撃を行っている主体と指摘されている中国・ロシア・北朝鮮の関係企業等が関わっていないか、調査しておくのが望ましい。

目　次

1章　はじめに
2章　基幹インフラ役務の安定的な提供の確保に関する制度
3章　米国の制度との比較
4章　我が国政府に求められる対応
5章　金融機関に求められる対応
6章　最後に

1章　はじめに

2022年5月11日、「経済政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」（以下、「経済安全保障推進法」）が成立した。経済安全保障推進法は、①重要物資の安定的な供給の確保、②基幹インフラ役務の安定的な提供の確保、③先端的な重要技術の開発支援、④特許の非公開の4分野で構成される。

これらのうち②は、基幹インフラサービスが安定的に提供されるよう、インフラ企業が重要設備（プログラムを含む）の導入等を行う場合に、政府が事前に審査してサイバーセキュリティを確保する制度といえ、多くのインフラ企業に影響が及ぶ可能性がある。ただし、本制度は2024年2月までに適用開始予定であり、2022年9月時点で政省令は定められておらず、制度の詳細は未定である。

本稿では、本制度の手続きについて、未定の部分については有識者会議の提言と国会での議論を参考にして解説し、米国の類似の制度から示唆を得る。最後に、政府と金融機関に求められる対応について検討する。

2章　基幹インフラ役務の安定的な提供の確保に関する制度

1．経済安全保障推進法制定の経緯

近年、米中対立などにみられるように、地政学的リスクが高まっており、安全保障を確保するために、外交・防衛だけでなく、経済的な側面からも対応する必要が生じてきている。そこで、日本政府は2021年11月に経済安全保障推進会議を立ち上げ、多岐にわたる課題のうち、法制上の手当てを講ずることによりまず取り組むべき分野として、以下4点が示された。

①重要物資や原材料のサプライチェーンの強靭化
②基幹インフラ機能の安全性・信頼性の確保
③官民が連携し、重要技術を育成・支援する枠組み
④特許非公開による機微な発明の流出防止

これを受け、「経済安全保障法制に関する有識者会議」（以下、「有識者会議」）が開催され、有識者会議は、2022年2月に「経済安全保障法制に関する提言」（以下、「有識者会議提言」）を公表した。経済安全保障推進法は、この提言を踏ま

図表1　重要インフラに対するサイバー攻撃事案

2013年3月	韓国	金融機関や放送局で、同時多発的にマルウェア感染によるシステム障害が発生。ＡＴＭの利用や一部放送業務に支障。
2015年4月	フランス	ＩＳＩＬ系とみられる「サイバーカリフ国」を名のるハッカー集団によるサイバー攻撃の影響で、フランスの国際放送局の放送が一時中断。
2015年12月	ウクライナ	電力会社がサイバー攻撃を受け、制御システムが不正に操作された結果、同国西部で数時間に及ぶ停電が発生し、約22万5,000人に影響。
2017年5月	我が国を含む約150か国	我が国を含む世界約150か国で発生した大規模ランサムウェア攻撃により、政府機関や医療機関、金融機関などの端末約30万台が感染。システムが停止し、業務に多大な影響。
2020年10月	インド	中央給電指令所や港湾施設等に対するサイバー攻撃によりムンバイで大規模停電が発生。
2021年5月	米国	米国最大の石油製品パイプライン事業者がランサムウェア攻撃を受け5日間操業停止。パニックによる買いだめでガソリンの売り切れが続出。

（出所）公安調査庁「サイバー空間における脅威の概況 2022」

えて法案が策定され、国会での審議を経て 2022 年５月 11 日に成立した（同月 18 日公布）。

2．制度創設の背景

経済安全保障推進法で制定された４分野の制度うち、基幹インフラ役務の安定的な提供の確保に関する制度が創設された背景として次の点が指摘できる。

国民生活や経済活動は、電気、ガス、水道、通信、金融サービス等のインフラサービスを基盤に成り立っている。近年、地政学的緊張の高まりもあり、サイバー空間が国家間の争いの場となっており、我が国を含め、インフラ事業を対象とするサイバー攻撃事案が多数発生し、安全保障上の懸念となっている（前掲図表１参照）。このような事案の中には国家の関与が疑われるものもあり、例えば、2015 年 12 月のウクライナの電力会社へのサイバー攻撃について、欧米政府はロシア連邦軍参謀本部情報総局（ＧＲＵ）の関与が疑われるとしている。

このようなインフラサービスの提供に対して、サイバー攻撃などによって国外から妨害が行われることを防ぐため、インフラ事業者が設備を導入したり、設備の維持管理等を第三者に委託したりする場合に、政府が事前に審査する制度が設けられた。

3．本制度の手続

１）手続の概要

基幹インフラ役務の安定的な提供の確保に関する制度では、まず、政府が対象事業者を指定する。対象事業者は、電気、ガス、水道、通信、金融サービス等のインフラ事業のうち、その機能が低下した場合に国の安全が損なわれる基幹インフラ事業者が指定される。

対象事業者は、以下のいずれかを行う場合、原則として事前に政府に届け出なければならない。

> ①重要設備（ハードウェア・ソフトウェアを含み、クラウドサービスで提供される場合を含む）の導入
> ②重要設備の維持管理・操作の他の事業者への委託

事前届出がなされた場合、重要設備が基幹インフラサービスの安定的な提供に対する、国外からの妨害行為に利用される恐れが大きいかを、政府が審査する。審査の結果、その恐れが大きいと政府が判断した場合、導入等の方法の変更や中止を勧告・命令できる。

以上が原則的な手続きだが、審査を経て重要設備の導入等を行った後で、事後報告が求められたり、国際情勢の変化により一定の措置が勧告・命令されたりする場合もある。

２）対象事業者の範囲

事前届出の対象となる事業者は、経済安全保障推進法では「特定社会基盤事業者」とされている（法 50 ①）。特定社会基盤事業者は、その事業を所管する大臣である「主務大臣」（法 86 ②）が指定することができる（法 50 ①）。特定社会基盤事業者が指定された場合、名称等が公示される（法 50 ②）。

特定社会基盤事業者は、「特定社会基盤事業」を行う者のうち一定の基準に該当する者である。この特定社会基盤事業は、以下の事業のうち政令で定めるものとされ（法 50 ①）、電気、ガス、水道、通信、金融サービス等の基幹インフラ事業が該当し得る。

①電気事業
②ガス事業
③石油精製業・石油ガス輸入業
④水道事業・水道用水供給事業
⑤第一種鉄道事業
⑥一般貨物自動車運送事業
⑦国際的な貨物定期航路事業・不定期航路事業
⑧国際航空運送事業・国内定期航空運送事業
⑨空港の設置・管理事業、空港に係る公共施設等運営事業
⑩電気通信事業
⑪放送事業（基幹放送を行うもの）
⑫郵便事業
⑬以下の金融に係る事業
—銀行業（※）、保険業、取引所金融商品市場の開設事業・金融商品債務引受業・第一種金融商品取引業、信託業、資金清算業・第三者型前払式支払手段の発行事業、預金保険事業・農水産業協同組合貯金保険事業、株式等振替業、電子債権記録業
⑭包括信用購入あっせん事業（クレジットカード）

（※）資金移動業が含まれる。また、信用金庫や信用組合等が銀行業を行う場合も含まれる。

一方、前述の「一定の基準」とは、使用する「特定重要設備」（後述）の機能が停止・低下した場合に、国家・国民の安全を損なう恐れが大きいものとして主務省令で定める基準とされている。この基準は、特定社会基盤事業者を比較的規模の大きい者等に限定する趣旨と推測される。有識者会議提言では、指定基準は、「利用者の数や国内市場におけるシェア等」の事業規模や、「地理的事情[1]や事業の内容の特殊性を含む」代替可能性を考慮して定めることとされ、中小規模の事業者を規制対象とすべきか、については「慎重な検討が必要」とされている。

3）対象設備の範囲

対象設備は、経済安全保障推進法では「特定重要設備」とされ、以下のように定義されている（法50①）。

特定社会基盤事業の用に供される設備、機器、装置又はプログラムのうち、特定社会基盤役務を安定的に提供するために重要であり、かつ、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の手段として使用されるおそれがあるものとして主務省令で定めるもの

特定社会基盤事業者は、導入等を行う設備が特定重要設備に該当する場合に事前届出が求められるが、特定重要設備に該当しなければ事前届出は不要である。

特定重要設備の具体的な範囲は主務省令で定められ、定義に「プログラム」とある通り、ハードウェアのほかソフトウェアも含まれる。また、有識者会議提言では、データセンターやクラウドサービス上にシステムを構築する場合も含めるべきとされている。

加えて有識者会議提言では、特定重要設備の範囲について、基幹インフラ事業の中心的なシステムのほか、「基幹インフラ事業において役務の安定的な提供に直結するような情報を扱うシステ

1）「特に、電気等の国民の生存にとって重要なインフラについては、一定地域において他の事業又は他の事業者による代替可能性があるか等の事情にも配慮する必要がある」とされている。

ム」も含むと考えられるとされ、その具体例として「オペレーション情報や重要施設のセキュリティ情報、銀行の預金情報等を扱うシステム」が挙げられている。

4）事前届出

（1）事前届出が必要な場合

特定社会基盤事業者は、以下のいずれかを行う場合、原則として、あらかじめ導入等計画書を主務大臣に届け出なければならない（法 52 ①）。

①他の事業者から特定重要設備の導入（※）を行う場合
②他の事業者に委託して特定重要設備の維持管理・操作（主務省令で定めるものに限る）を行わせる場合

（※）当該特定社会基盤事業者と実質的に同一と認められる者その他の政令で定める者が供給する特定重要設備の導入を行う場合は、原則として事前届出が不要（ただし、当該特定重要設備に当該政令で定める者以外の者が供給する特定重要設備が組み込まれている場合は事前届出が必要）。

事前届出を行わず、又は虚偽の届出をして導入等を行った場合、２年以下の懲役又は 100 万円以下の罰金が科される（又は併科される）（法 92 ①一）。

ただし、特定重要設備の導入等が緊急やむを得ない場合は、事前届出は不要である（法 52 ①）。具体的な範囲は主務省令で定められるが、有識者会議提言によると、災害時等が想定されている。この場合、事後届出が必要である（法 52 ⑪）。

加えて、以下のように、従来は事前届出の対象ではなかったが新たに対象となった場合において、その日から６カ月以内に特定重要設備の導入等を行った場合も事前届出は不要である（法 53）。

①新たに特定社会基盤事業者に指定された場合
②（法令の改正により）新たに特定重要設備に該当した場合
③（法令の改正により）新たに重要維持管理等に該当した場合

有識者会議提言を踏まえると、重要設備の導入は通常数年単位の時間をかけて検討、開発、製造等が行われるので、設備の導入等に急な変更が生じるといった混乱を回避するため、上記の経過措置が設けられたと考えられる。

（2）事前届出事項

事前届出事項（導入等計画書の記載事項）は下記の通りである（法 52 ②）。

①特定重要設備の概要
②特定重要設備の導入を行う場合、以下の事項
- 導入の内容・時期
- 供給者に関する事項（※１）
- 特定重要設備の一部を構成する設備、機器、装置またはプログラムであって、特定妨害行為（※２）の手段として使用される恐れがあるものに関する事項（※１）

③特定重要設備の重要維持管理等を行わせる場合、以下の事項
- 委託の内容、時期・期間
- 委託の相手方に関する事項（※１）
- 委託の相手方が再委託する場合、再委託に関する事項（※１）

（※１）具体的内容は主務省令で定められる。
（※２）「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」と定義されている。

5）政府による審査

事前届出がなされた場合、主務大臣が審査を行う。審査期間は原則として 30 日以内だが、最長４カ月以内まで延長可能である。審査期間中は、特定社会基盤事業者は導入等を行うことができない（法 52 ③④）。

審査は、特定重要設備が、我が国の外部から行われる特定妨害行為、つまり、基幹インフラサービス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恐れが大きいか否かが判断される（法 52 ⑤）。特定妨害行為の具体的な内容については、2023 年５月までに閣議決定される基本指針で明確化される見込みだが、国会での審議によると「サイバー攻撃などの電磁的な方法」のほか、「物理的な方法」によるものも含まれる見込みである。さらに、例として、以下のような行為が想定されている[2]。

◇外国政府などが特定重要設備の供給者からその設備の脆弱性に関する情報の提供を受けて、その脆弱性を利用してウイルスに感染させること
◇外国政府などの指示を受けて、特定重要設備の供給者がその設備にあらかじめ不正プログラムを埋め込んで、そのプログラムによって設備を停止させること
◇重要維持管理などの委託を受けた者が外国政府などの指示を受けて、その委託を受けた重要維持管理などの業務を放棄することで設備の機能を失わせること

審査の結果、特定重要設備が特定妨害行為に利用される恐れが大きい場合、主務大臣は、導入等の方法の変更または中止を勧告できる（法 52 ⑥）。勧告を受けた事業者は、勧告を応諾するか否か、主務大臣に通知しなければならない（法 52 ⑦）。勧告を応諾しない旨通知した場合で、正当な理由がない場合、主務大臣は導入等の方法の変更または中止を命令できる（法 52 ⑩）。命令に違反した場合、２年以下の懲役又は 100 万円以下の罰金が科される（又は併科される）（法 92 ①四）。

6）導入後の変更の事後報告

事前届出と審査を経た上で特定重要設備の導入を行った後でも、一定の場合、主務大臣に事後報告が求められる場合がある。具体的には、特定社会基盤事業者は、事前届出を行った特定重要設備の導入を行った後に、一定の変更（具体的内容は主務省令で定められる）を行った場合は、遅滞なく変更の内容を主務大臣に報告しなければならない（法 54 ④）。

7）導入等の後の勧告・命令

事前届出を行い審査を経た上で特定重要設備の導入等を行った後でも、国際情勢の変化等により、一定の措置の勧告・命令がなされる場合がある。具体的には、特定重要設備の導入等を行った後、国際情勢の変化その他の事情の変更により、特定重要設備が特定妨害行為の手段として使用され、又は使用される恐れが大きいと認めるに至ったときは、主務大臣は以下の行為を勧告・命令できる（法 55 ①③）。

◇特定重要設備の検査・点検の実施
◇維持管理等の委託の相手方の変更
◇その他必要な措置

事前届出の場合、問題があるときは、導入等の方法の変更や中止が求められ得るのに対し、事後

2）2022 年３月 25 日 第 208 国会衆議院内閣委員会における小林経済安全保障担当大臣（当時）の発言参照。

的な勧告・命令は、特定重要設備の検査・点検の実施等とされ、事前届出の場合と比べて事業者への負担に配慮されているといえる。

8）今後のスケジュール

本制度に関する今後のスケジュールは以下の通りである。

◇（時期未定）：政省令案（特定社会基盤事業・特定重要設備等）の公表・確定
◇2023/5/17までの政令指定日：基本指針の策定
◇2023/11/17までの政令指定日：対象事業者の指定開始
◇2024/2/17までの政令指定日：事前届出の開始

3章　米国の制度との比較

1．米国の制度の概要

米国では、2019年5月15日にトランプ前大統領が、国家緊急経済権限法に基づいて、「外国敵対者」との情報通信技術・サービス（ＩＣＴＳ）に関する取引を一定の場合に禁止する大統領令[3]に署名した。これに基づいて、2021年1月19日、商務省が大統領令を実施するための規則（以下、「商務省規則」）[4]を公表し、同年3月22日に発効している。

本制度では、米国企業・米国人が、「外国の敵対者」の影響下にある者が設計・開発等を行ったＩＣＴＳの調達、輸入、設置等を行う場合（または行った場合）、関係省庁が審査を行う。「外国の敵対者」として、具体的に、中国（香港を含む）、ロシア、北朝鮮、イラン等が明示されている。

我が国の制度と異なり、対象事業者が事前届出を行う義務は定められておらず[5]、当事者から取得した情報等に基づいて、商務長官の判断や関係省庁の要請により審査が開始される。審査の結果、問題がある場合は、ＩＣＴＳ取引の禁止や、リスク軽減措置を取ったうえで実施することが求められる。

2．審査対象

米国の制度では、審査対象は、2021年1月19日以後に開始・完了した、以下のＩＣＴＳの取得、輸入、導入等[6]（以下、「ＩＣＴＳ取引」）とされている（商務省規則§7.2、§7.3（a）（4））。

①重要インフラ事業者（※1）が使用するＩＣＴＳ
②通信（※2）関連のＩＣＴＳ
③100万人超の米国人の機密個人データ（※3）を保持するホスティングサービス等に不可欠なＩＣＴＳ
④米国人に100万個超販売された家庭用通信・モニタリング機器
⑤100万人超の米国人が使用する接続・通信ソフトウェア
⑥先端技術（※4）に不可欠なＩＣＴＳ

（※1）化学、商業施設、通信、重要製造業、ダム、防衛産業基盤、緊急サービス、エネルギー、金融、食料・農業、政府施設、ヘルスケア・公衆衛生、情報技術、原子力、輸送システム、上下水道システム、およびその下位分野の事業者が該当する。

3）「情報通信技術・サービスのサプライチェーンの安全性の確保に関する大統領令」（EO13873）。
4）「情報通信技術・サービスのサプライチェーンの安全性の確保に関する暫定最終規則」。
5）第2回の有識者会議（2021年12月28日）の資料4によると、「商務省は、事業者の予見可能性を担保する観点から、事前承認制度案を検討中」とされている。
6）ソフトウェアのアップデート等が含まれる。

（※２）ワイヤレス・ローカルエリア・ネットワーク、モバイルネットワーク、衛星通信、アクセスポイント、コア・ネットワーキング・システム等が該当する。
（※３）個人の財務データ、健康保険関連のデータ、健康状態に関連するデータ、Ｅメール等の電子的情報通信、個人の地理的位置情報データ、生体認証データ、遺伝子情報等が含まれる。
（※４）ＡＩ・機械学習、量子暗号、量子コンピューター、ドローン、自律システム、応用ロボティクスが該当する。

3．政府による審査

米国の制度では、商務長官は、当事者から取得した情報等に基づき、以下①と②を審査する（商務省規則§7.2、§7.4、§7.103（b）（c））。

①以下の「外国の敵対者」の影響下にある者（※）が設計・開発等に関わったＩＣＴＳが含まれるか
―中国（香港を含む）、ロシア、北朝鮮、イラン、キューバ、ベネズエラ（マドゥロ政権）
②ＩＣＴＳ取引が以下のいずれかに該当するか
（a）米国のＩＣＴＳの設計、製造、運用等に対して妨害・破壊行為といった不当なリスクを及ぼすもの
（b）米国の重要インフラ・デジタル経済のセキュリティに不当なリスクを及ぼすもの
（c）米国の安全保障や米国民の安全に受け入れられないリスクを及ぼすもの

（※）「外国の敵対者」の所有、支配、命令又は司法権の対象となる者。

上記②を判断する際に考慮する要素として、以下の事項が明記されている（商務省規則§7.103（c））。

◇ＩＣＴＳの性質と特徴（機能、用途、市場シェア等）
◇「外国の敵対者」がＩＣＴＳの設計等に及ぼす影響（※）の性質と程度
◇「外国の敵対者」を含む取引関係者の言動
◇ＩＣＴＳ取引の脅威の有無、脆弱性の性質
◇ＩＣＴＳ取引が以下の事項に与える損害の深刻さ
―米国人の健康・安全、重要インフラ、機密データ、経済、外交政策、自然環境、国家の重要機能
◇ＩＣＴＳ取引が実際に損害を発生させる可能性

（※）「外国の敵対者」による所有、支配、命令又は司法権が及ぶこと。

審査の結果、問題がある場合は、商務長官は関係省庁と協議の上、審査の終了（ＩＣＴＳ取引の許容）、ＩＣＴＳ取引の禁止、リスク軽減措置を取ることを条件に許容、のいずれかを決定する（一次決定。商務省規則§7.105（b））。

一次決定に対して、取引当事者はその取り消しや軽減措置を求めることができる（商務省規則§7.107）。商務長官は当事者の要求を検討し、再度関係省庁と協議の上、ＩＣＴＳ取引の許容、禁止、リスク軽減措置を取ることを条件に許容、のいずれかを最終決定する。取引を禁止する場合、最終決定の内容が連邦官報で公表される（商務省規則§7.109（a）（f））。

4．日米制度の比較

日米の制度を比較すると、我が国の制度では基幹インフラサービスの安定的な提供の確保が目的とされているのに対し、米国の制度は、重要イン

フラのセキュリティに加えて、通信全般、米国人の機密個人データ、先端技術も保護の対象とされている。

このような制度の趣旨の違いのため、審査対象の範囲も、米国の制度の方が広い。我が国の制度では、審査対象は基幹インフラ事業者の設備（システム）のうち重要なものに限られるが、米国の制度では、インフラ事業者が使用するもの以外でも、通信に関連するＩＣＴＳ、米国人の機密個人データを扱うサービスのＩＣＴＳや先端技術に不可欠なＩＣＴＳも対象とされている。

インフラ事業者による設備の導入等に関する審査に限っても、審査対象の範囲は米国の方が広いといえる。例えば、我が国の制度では、中小規模の事業者は基本的に対象事業者から除外される見込みだが、米国の制度では中小規模の事業者であることを理由に審査対象から除外することとはされていない。

加えて、米国の制度では、ソフトウェアのアップデートもＩＣＴＳ取引として審査対象となり得るのに対し、我が国の制度ではソフトウェアのアップデートは設備の導入等に該当せず、事前届出・審査の対象ではないと考えられる。

このような違いが生じている背景として、我が国の制度では、規制によって事業者の経済活動を過度に制約しないよう配慮しているためと考えられる。

4章　我が国政府に求められる対応

1．制度の明確化

経済安全保障推進法の基幹インフラ役務の安定的な提供の確保に関する制度については、制度の対象となる基幹インフラ事業者や対象となる設備の範囲は、今後政省令で明確化される予定である。特に、対象となる基幹インフラ事業者は、主務大臣に指定された場合は公示されるため、誰の目から見ても明らかになる。

一方、審査基準は、前述の通り、特定重要設備が、我が国の外部から行われる、基幹インフラサービス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恐れが大きいか否かとされている。

この審査基準について、有識者会議の検討においては、「我が国の外部にある主体の意図や我が国の外部にある主体と特定重要設備の供給者等との関係性などを考慮することが考えられる」[7]という意見もあったとされる。ただし、上記の「我が国の外部」について、米国の「外国の敵対者」のような具体的な国名は明示されない見込みである[8]。

審査基準については、基本指針で明確化される見込みである。対象となる基幹インフラ事業者が審査で承認されるか否かの見通しが立てられるよう、可能な限り具体的な基準が示されることが望ましい[9]。

7）2022年3月23日 第208国会衆議院内閣委員会の小林経済安全保障担当大臣（当時）の発言参照。
8）2022年3月25日 第208国会衆議院内閣委員会において、小林経済安全保障担当大臣（当時）は「特定の国や企業を名指しする、いわゆるブラックリスト」は「設けないことを考えております」と発言している。
9）有識者会議提言は、「制度の運用に当たっては、（･･･）政府が規制対象となるインフラ事業者からの相談を事前に受け付ける仕組みを設けるべき」（p.27）と提言されており、実際上、事前相談において審査で承認されるか否かの感触を得ることができるのではないかと考えられる。

2．さらなる対策の検討

1）総合的なサイバーセキュリティ対策

本制度により、基幹インフラ事業者がサイバー攻撃に脆弱なシステムを導入するリスクが低減することが期待される。しかし、「サイバー攻撃のリスクに対処するためには、１つの防衛手段では全く足りず、多層防御を行うことによりサイバー攻撃を防ぐ」[10]ことが重要と指摘されている。

さらに、事業者によるシステム的な多層防御（複数の防御策）に止まらず、政府によるサイバー攻撃自体への対応を含む、総合的なサイバーセキュリティ対策を推進することが重要と考えられる。

政府によるサイバー攻撃自体への対応に関して、サイバーセキュリティに関する施策の基本的な方針を定めた「サイバーセキュリティ戦略」（2021 年９月閣議決定）では、以下のようにサイバー攻撃に対する防御力・攻撃力・状況把握力の強化に取り組む方針を示しており、これらの取組みによりサイバー攻撃自体への対応が強化されることが期待される。

◇サイバー攻撃に対する防御力の向上
　―防衛省・自衛隊におけるサイバー防衛能力の抜本的強化、自衛隊・米軍のインフラ防護の演習等の実施
　―先端技術・防衛産業等のセキュリティ確保のための官民連携・情報共有等の強化
◇サイバー攻撃に対する抑止力の向上
　―相手方によるサイバー空間の利用を妨げる能力の活用や外交的手段・刑事訴追等を含めた対応の活用、日米同盟の維持・強化
◇サイバー空間の状況把握力の強化
　―全国的なネットワーク・技術部隊・人的情報を駆使したサイバー攻撃のさらなる実態解明の推進

2）国民の機密個人データや先端技術等の保護

経済安全保障推進法では基幹インフラサービスが対象とされているが、前述の通り、米国の商務省規則では、国民の機密個人データや先端技術等の保護・流出防止も図られている。経済安全保障推進法とは別の制度として整備することも考えられるが、我が国においても、国民の機密個人データや先端技術等の保護・流出防止が求められる[11]。

サイバーセキュリティ戦略においては、これらの課題について下記のように取り組み方針が示されている。我が国企業に対するサイバー攻撃が相次いでいることも踏まえ、さらなる取組みの必要性について、引き続き検討することが望まれる。

◇国民の個人情報の保護
　―サイバー攻撃等から個人情報を保護する有効な安全管理措置について、適時適切に情報提供を行う
　―保有・管理する主体である民間企業、大学等におけるセキュリティ対策に資する情報共有を促す取組を強化
◇先端技術・防衛関連技術の防護
　―（特に防衛産業について）新たな情報セキュリティ基準の策定や官民連携の一層の強化等
　―重要インフラ事業者や先端技術・防衛関連技術産業、研究機関といった関係事業者と

10）有識者会議提言脚注５（p.19）参照。
11）商務省規則は、商務長官に対して「必要に応じ、本制度の適用について国際的なパートナーと調整および情報共有を行う」ことを求めている。また、日米の政府間では、日米経済政策協議委員会（いわゆる経済版「２＋２」）において、経済安全保障等について協議されている。

国の一層の情報や脅威認識の共有および連携を図る

5章　金融機関に求められる対応

前述の通り、経済安全保障推進法の対象業種には、以下の金融業のうち、政令で定められるものが含まれる。銀行・証券会社・保険会社に加え、下記に該当する金融機関のうち、一定の事業規模の者が対象事業者に指定される可能性がある。

銀行業（※）、保険業、取引所金融商品市場の開設事業・金融商品債務引受業・第一種金融商品取引業、信託業、資金清算業・第三者型前払式支払手段の発行事業、預金保険事業・農水産業協同組合貯金保険事業、株式等振替業、電子債権記録業

（※）資金移動業が含まれる。また、信用金庫や信用組合等が銀行業を行う場合も含まれる。

金融機関が提供する主なインフラサービスとして、銀行等が提供する資金決済サービスや、証券会社が提供する取引所を中心とした証券取引サービスが挙げられる。仮に審査の結果、システムの導入の中止等が命令された場合、インフラサービスの提供に支障をきたし、それを利用している顧客の取引に影響が生じる可能性がある。

そのため、本制度の対象事業者となった場合、導入しようとしているシステムが審査の対象となるか、審査で承認されるかを事前に把握しておくことが望ましい。

審査対象となるシステムの範囲については、有識者会議提言を踏まえると「銀行の預金情報等を扱うシステム」は対象とされる見込みである。

審査で承認されるかに関して、前述の通り、「我が国の外部にある主体の意図や我が国の外部にある主体と特定重要設備の供給者等との関係性など」が考慮される可能性がある。「我が国の外部にある主体」について具体的な国名等は明示されない見込みだが、サイバーセキュリティ戦略では、サイバー攻撃等を行っているとみられる主体として中国・ロシア・北朝鮮が明記されている。

前述の通り、米国の制度では、審査の際、ＩＣＴＳの性質と特徴、ＩＣＴＳ取引の脅威の有無、脆弱性の性質に加え、「外国の敵対者」がＩＣＴＳの設計等に及ぼす影響の性質と程度、つまりＩＣＴＳの設計等に「外国の敵対者」の所有、支配、命令又は司法権がどのように及んでいるか、また、どの程度及んでいるか、等を考慮するとされている。

これらを踏まえると、対象事業者に指定される見込みのある金融機関は、今後導入を予定するシステムに関して、システムの設計等に中国・ロシア・北朝鮮などに関連する個人・企業がどの程度関わっているかなどをあらかじめ調査しておくのが望ましいだろう。

調査の際、ソフトウェアについては、我が国でも普及が目指されている「ソフトウェア部品表（ＳＢＯＭ；Software Bill Of Materials）」を利用することが考えられる。これは、特定の製品に含まれるすべてのソフトウェアコンポーネント、ライセンス、依存関係を一覧化したものであり、ソフトウェア開発者についての情報を得ることができる。

ただし、ソフトウェア部品表では、ソフトウェア開発者の株主構成や最終親会社、開発担当者の国籍等の情報は得られないと考えられる。これらを確認する場合は、ヒアリング等で個別に確認する必要がある。

なお、多くの金融機関はシステム開発をシステム開発業者に委託していると考えられ、その場合、これらの確認作業は実際上、システム開発業者が行うことになるだろう。

金融機関への影響としては、顧客が経済安全保障推進法の対象となることによる間接的な影響も考えられる。例えば、銀行が顧客に貸出を行っているときに、その顧客が経済安全保障推進法の適用対象となり、対応コストのためその経営に影響があった場合、貸し倒れのリスクが発生するといった影響も想定される。しかし、対応コストのため経営に影響が及ぶ可能性は高くはないと考えられ、このようなケースは限定的だろう。

6章　最後に

経済安全保障推進法の基幹インフラ役務の安定的な提供の確保に関する制度は、2024年2月までに手続きが開始する予定である。

制度の対象となる可能性がある事業者は、自社が対象となった場合にどのような影響があるか、あらかじめ準備しておくことが望ましい。

今後、基本指針の案や政省令案が公表され、パブリックコメントが実施される予定である。案の内容が、自社にとって対応可能か確認し、必要であれば案に対して意見を提出することも検討すべきだろう。

我が国の制度では、国家・国民の安全と事業者の経済活動の自由とのバランスが考慮され、事業者にとって過大な負担とならないよう制度整備や運用がなされる見込みである。

しかし、我が国においても、サイバー攻撃によってインフラサービスの提供が停止するような事態が生じれば、将来的に規制が厳格化される可能性も考えられる。対象となる事業者は、引き続き規制の動向に注視しておく必要があるだろう。

[著者]
金本 悠希（かねもと ゆうき）

金融調査部
主任研究員
担当は、税制、会計制度、
金融商品取引法、金融規制