参議院常任委員会調査室・特別調査室

論題	経済安全保障推進法改正案 －名古屋港でのサイバー事案を契機とした制度の見直し－
著者 / 所属	柿沼　重志 / 内閣委員会調査室
雑誌名 / ISSN	立法と調査 / 0915-1338
編集・発行	参議院事務局企画調整室
通号	465 号
刊行日	2024-4-12
頁	21-32
URL	https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/20240412.html

経済安全保障推進法改正案

― 名古屋港でのサイバー事案を契機とした制度の見直し ―

柿沼　重志
（内閣委員会調査室）

１．経済安全保障法の施行とサイバー攻撃からインフラを守るための取組等[1]

（１）経済安全保障推進法の施行

国際情勢の複雑化、社会経済構造の変化等に伴い、安全保障を確保するためには、経済活動に関して行われる国家及び国民の安全を害する行為を未然に防止する重要性が増大していることに鑑み、「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年法律第 43 号。以下「経済安全保障推進法」という。）が令和４年５月 18 日に公布され、同年８月１日から同法の一部が先行的に施行された（残りの規定についても段階的に施行されている[2]）。

[1] 以下、本稿は、令和６年３月 26 日の脱稿時点までの情報に基づき、執筆している。また、本稿におけるインターネット情報の最終アクセス日も同日である。
[2] ４つの柱のうち、第１の柱である重要物資の安定的な供給の確保及び第３の柱である先端的な重要技術の開

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及び④特許出願の非公開の４つの柱で構成されている[3]。

今般の改正案は、経済安全保障推進法の第２の柱である基幹インフラ役務の安定的な提供の確保に関するものであり、以下では同制度について見ていく。

ア　基幹インフラ役務の安定的な提供の確保に関する制度創設

特定社会基盤役務（基幹インフラ）の対象とすべき事業の考え方については、特定社会基盤役務基本指針[4]において「①国民生活又は経済活動が依存している役務[5]であって、その利用を欠くことにより、広範囲又は大規模な社会混乱を生ずるなどの経済・社会秩序の平穏を損なう事態が生じ得るもの」又は「②国民の生存に不可欠な役務であって、その代替が困難であるもの」とされている。また、特定社会基盤事業（基幹インフラ事業）は、経済安全保障推進法第 50 条第１項第１号から第 14 号で、「電気」、「ガス」、「石油」、「水道」、「鉄道」、「貨物自動車運送」、「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」の 14 分野が外縁として規定されている。さらに、それぞれの分野について、必要な範囲に細分化し政令で絞り込みが行われているほか、特定社会基盤役務基本指針において、「国家及び国民の安全と自由な経済活動のバランスに留意し、規制対象を真に必要なものに限定するとともに、事業者からの意見の十分な聴取を行うこと等により、それぞれの事業の実態等を十分に踏まえた制度整備及び運用を行うこととする」ことが示されている。

こうした制度創設の意義について、小林鷹之経済安全保障担当大臣（当時）は、「基幹インフラの分野については、2015 年に、ウクライナにおいて変電所に対するサイバー攻撃があって、大規模かつ長期にわたる停電が発生した事案を始めとして、世界各国においてサイバー攻撃の対象となる事案が増加している。また、基幹インフラ事業者が利用しているＩＣＴ機器が高度化している。それに伴って、サプライチェーンの過程で、その設備に不正な機能が埋め込まれる可能性が高まってきている。そうした意味で、リスクが高まっていると捉えている。この法案においては、基幹インフラ事業者による役務の安定的な提供が妨害されることを未然に防止するために、設備の導入等を行う前に政

発支援については、令和４年８月１日に施行。次いで、第２の柱である基幹インフラ役務の安定的な提供の確保は令和５年 11 月１日及び同年 11 月 17 日に施行されており、６か月間の経過措置期間の後、制度の運用開始の予定となっている（令和６年５月 17 日に制度運用開始の予定）。なお、「特許出願の非公開」は「公布の日から起算して２年を超えない範囲内において政令で定める日」に施行と規定されており、令和６年５月１日の施行が予定されている。

[3] 同法施行後の動向等については、柿沼重志・小林惇「経済安全保障推進法制定後の動きと今後の課題－経済的威圧に対抗するための体制構築に向けて－」『立法と調査』No.461（令 5.11）３～18 頁を参照。

[4] 経済安全保障推進法第 49 条第１項の規定及び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基本的な方針（令和４年９月 30 日閣議決定）に基づき、「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（特定社会基盤役務基本指針）」が令和５年４月 28 日に閣議決定された。

[5] 国民生活又は経済活動が依存している役務とは、国民生活や経済活動の維持に不可欠である役務等を指す。このような役務の安定的な提供に支障が生じた場合には、その態様及び程度によっては、広範囲又は大規模な社会的混乱を生ずるなどの経済・社会秩序の平穏を損なう事態が生じ、国家及び国民の安全を損なう事態を生ずるおそれがある。

府が事前にリスクを審査する制度を設けることとしている」旨の答弁を行っている[6]。

イ　現行制度のスキーム

現行制度のスキームは、以下のとおりである（図表１）。

図表１　現行制度のスキーム

（出所）「経済安全保障法制に関する有識者会議」分野別検討会合（基幹インフラ）資料（令和６年１月 29 日内閣官房）

まず、特定社会基盤事業者として指定を受けた事業者が主務省令で定められた設備の導入及び維持管理等の委託を行う場合には、事前に導入等計画書を届け出るとともに、事業所管大臣による審査を受けなければならないこととされている。禁止期間は、原則として、導入等計画書の届出を事業所管大臣が受理してから 30 日間とされ、また、同計画書を届け出た事業者は、同期間中は、当該計画に係る導入・委託を行うことができない。さらに、審査の結果、設備の導入等について、事業所管大臣が、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おそれが大きいと認めるときは、妨害行為を防止するために必要な措置（設備の導入等の変更・中止等）を勧告することができる。特定社会基盤事業者の指定基準は、特定社会基盤役務基本指針で示されており、事業規模又は代替可能性のいずれか又はその両方を考慮し、事業ごとの実態を踏まえて定めることとなっており、その指定は、①適正な競争関係を不当に阻害することがないように配慮すること、②中小規模の事業者の指定についてはより慎重に検討を行うことに留意して行うこととされている。なお、特定社会基盤事業者として指定を受けた事業者は 211 者となっている（令和６年２月 15 日現在）。

---

[6] 第 208 回国会衆議院内閣委員会議録第 11 号９頁（令 4. 3. 23）

また、特定社会基盤役務基本指針において、特定社会基盤事業の見直しに関する考え方については、「安定的な提供に支障が生じた場合に国家及び国民の安全を損なう事態を生ずるおそれがある事業は、技術の進展や社会経済構造の変化等により変わり得るものである。そのため、特定社会基盤事業は、これらの変化等を踏まえ不断に見直しを行うこととする」こととされている。

ウ　港湾に関する国会論議

令和４年３月 23 日の衆議院内閣委員会では、政府参考人から、「港湾については、輸出入貨物の 99.6％が港湾を経由しているので、物流の確保の観点から重要なインフラであると認識している。一方で、港湾等で使用される設備で、その機能に支障が出た際に船舶による物流に影響が生じ得るものとして、航路標識、荷役機械、海運事業者などが港湾施設使用の許可をオンラインで申請するためのシステムといったものが想定される。そのうち、航路標識については、原則として、海上保安庁が設置、管理をしており、国等の機関による調達については、ＩＴ調達に関する政府申合せ、これに基づき必要な措置を講ずることとしていることなどから、本法案の対象とはしていない。次に、荷役機械については、それぞれが独立して動作するものであり、仮に一部の荷役機械の運用に支障が生じたとしても、他の荷役機械による代替が可能であり、港湾の機能に大きな影響は生じないものと考えている。次に、施設使用許可のシステムについては、港湾施設使用の許可申請は、現状、約 60％が書面の持参、郵送、ファックスなど紙ベースで処理されていることから、仮に当該システムに支障が生じた場合であっても申請処理の大幅な遅延は見込まれないと認識している。したがって、港湾は、規制対象とすべき設備が具体的に想定されないので、今般、基幹インフラの対象事業には含めていない」旨の答弁があった[7]。

次に、同年４月 26 日の参議院内閣委員会、経済産業委員会連合審査会では、政府参考人から、「港湾が果たす役割は非常に重要ではあるが、現時点で規制対象とすべき設備が具体的に想定されないということで基幹インフラの対象事業に含めていない。他方で、本法案の成立後も、港湾のＤＸ等の進展を考えて、必要な取組について不断に検討を進めていく所存である」旨の答弁があった[8]。

（２）重要インフラと基幹インフラとの違い

重要インフラと基幹インフラとの違いについて、小林大臣（当時）からは、「重要インフラとは、国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものとされており、『サイバーセキュリティ基本法』（平成 26 年法律第 104 号）に基づき、官民が一丸となって重点的に防護する必要があるとの認識の下で指定されている。一方で、基幹インフラに関する制度については、国民生活及び経済活動の基盤となる役務の中でも、国民の生存に必要不可欠で代替困難なもの、又は、国民生活、経済活動が依存する役務で、その利用を欠くことに

[7] 第 208 回国会衆議院内閣委員会議録第 11 号５頁（令 4.3.23）
[8] 第 208 回国会参議院内閣委員会、経済産業委員会連合審査会会議録第１号 17 頁（令 4.4.26）

よって広範囲若しくは大規模な混乱などが生じるものを提供する事業を対象とすることを基本としており、事業規模などの基準に該当する事業者が導入する重要設備を事前審査することから、規制対象となる事業者や設備が具体的に想定されない事業などは対象としていない。したがって、重要インフラと基幹インフラは、一部対象事業が異なるという関係になっている」旨の答弁があった[9]。

前述したとおり、港湾は、現行の経済安全保障推進法の基幹インフラの対象になっていない。また、港湾は、サイバーセキュリティ基本法の重要インフラ分野にも位置付けられてこなかったが、後述する名古屋港でのサイバー事案を受け、令和６年３月８日、「重要インフラのサイバーセキュリティに係る行動計画」が改定され、重要インフラ分野に港湾が追加された。なお、対象となるシステムの例として、コンテナの積卸し作業、搬入・搬出等を一元的に管理するターミナルオペレーションシステム（ＴＯＳ）が挙げられている。

（３）サイバー安全保障分野での対応能力の向上の必要性

「国家安全保障戦略」（令和４年 12 月 16 日国家安全保障会議決定、閣議決定）では、「サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」とされた[10]。また、同戦略では、能動的サイバー防御について、「武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する」とされた。

２．名古屋港の事案等を踏まえた基幹インフラ制度の見直し

（１）名古屋港におけるシステム障害の発生

令和５年７月４日に、名古屋港の５つのコンテナターミナル及び集中管理ゲートにおいて運用されている名古屋港統一ターミナルシステムが、大規模なサイバー攻撃を受けて３日間にわたり停止した。当該事案による影響は、①荷役スケジュールに影響が生じた船舶が 37 隻、②搬入・搬出に影響があったコンテナ約２万本（推計）とされ、名古屋港での物流に甚大な影響を及ぼした[11]。そして、名古屋港統一ターミナルシステムに障害を起こした原因は不正プログラム（ランサムウェア[12]）への感染であるとされている。

名古屋港の事案発生後の同月 14 日、高市早苗経済安全保障担当大臣は記者会見において、「物流確保の観点から港湾が果たす役割は大きく、経済安全保障の観点から非常に重要

---

[9] 第 208 回国会衆議院内閣委員会議録第 16 号 13 頁（令 4.4.6）

[10] 米国のハーバードケネディスクールベルファー科学国際問題センターの「国家サイバー・パワー・インデックス（National Cyber Power Index）」調査によると、日本の順位は 2020（令和２）年の９位から 2022（令和４）年は 16 位となっている。

[11] 名古屋港コンテナターミナルの機能が停止した３日間に支障が生じたコンテナ取扱貨物量は、停止した同３日間における我が国のコンテナ取扱貨物量の約 12％に当たる量であり、その間、多数の荷主のサプライチェーンが途絶し、経済に多大な影響が生じた。

[12] ランサム（身代金）とソフトウェアから成る造語であり、ランサムウェアに感染すると、端末内のデータが暗号化されて利用できなくなり、復号（復旧）の対価として身代金（ランサム）が要求される。

な役割を果たすものであり、経済安全保障推進法の基幹インフラの対象事業に追加するかも含めて検討したい」旨の発言を行った[13]。

次いで、同月 18 日、斉藤鉄夫国土交通大臣は記者会見において、「今般発生した名古屋港のコンテナターミナルのシステム障害を踏まえ、国土交通省では、港湾管理者、港湾運送事業者等に対し、改めてサイバーセキュリティ対策の徹底を図るよう、注意喚起を行った。また、同種事案の再発防止に向けて、早期に有識者等からなる検討委員会を立ち上げ、今般事案の原因究明とともに、必要なセキュリティ対策の整理・検討を行う予定である。制度面では、港湾機能の安定的な確保に向けて、サイバーセキュリティ基本法と経済安全保障推進法の２つの法令上の位置付けに港湾を追加するかも含めて、関係省庁等と連携し、必要な対応を検討していきたい」旨の発言を行った[14]。

（２）国土交通省における検討委員会の設置と同検討委員会での議論

国土交通省では、名古屋港で発生した事案の検証等を行うとともに、コンテナターミナルの運営に関する基幹的な情報システムに必要な情報セキュリティ対策、サイバーセキュリティ政策及び経済安全保障政策における港湾の位置付け等の整理・検討を行うため、令和５年７月 31 日、「コンテナターミナルにおける情報セキュリティ対策等検討委員会」が設置され、第１回委員会が行われた。その後も、同検討委員会は検討を進め、令和６年１月 24 日に「名古屋港のコンテナターミナルにおけるシステム障害を踏まえ緊急に実施すべき対応策及び情報セキュリティ対策等の推進のための制度的措置について」の取りまとめを公表し、名古屋港事案の検証が行われ、感染経路については、「保守用ＶＰＮ[15]を通じて物理サーバに攻撃者が侵入し、サーバ情報が暗号化されたものと考えられる一方で、ＶＰＮ経由以外での侵入の可能性についても否定することはできない」とされた。また、今回の事案における主な問題点として、①保守作業に利用する外部接続部分のセキュリティ対策が見落とされていたこと、②サーバ機器及びネットワーク機器の脆弱性対策が不十分であったこと、③バックアップの取得対象と保存期間が不十分であったこと、④システム障害時の対応手順が未整備であったこと等が示された。

さらに、同取りまとめでは、情報セキュリティ対策等の推進のための制度的措置として、「コンテナターミナルのＴＯＳはコンテナ単位の膨大な情報を処理するため、システムが停止した場合等においてマニュアルで代替することが困難なターミナルが生じると考えられ、その情報セキュリティ対策は極めて重要である」とした基本的考え方が示された上で、①「港湾運送事業法」（昭和 26 年法律第 161 号）の観点から、ＴＯＳの情報セキュリティ対策の確保状況を国が審査する仕組みの導入、②サイバーセキュリティ基本法の観点から、官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進、③経済安全保障の観点から、国として積極的に関与といった３点が示された。特に、③につ

---

[13] <https://www.cao.go.jp/minister/2208_s_takaichi/kaiken/20230714kaiken.html>

[14] <https://www.mlit.go.jp/report/interview/daijin230718.html>

[15] Virtual Private Network（仮想プライベートネットワーク）の頭文字を取った略語で、プライベートネットワーク間が、あたかも専用線接続されているかのような状況を実現する技術又はそのための機器を指し、秘匿性の高いデータを安全に通信するための仕組みである。

いては、経済安全保障推進法の趣旨も踏まえ、ＴＯＳを使用して役務を行う一般港湾運送事業[16]を同法の対象事業とすることが必要であると考えられるとされた。

（３）医療機関へのサイバー攻撃の発生

医療機関に対するサイバー攻撃については、令和３年 10 月に、徳島県つるぎ町にある町立半田病院においてランサムウェアを用いたサイバー攻撃により病院内のデータが暗号化され、電子カルテ等が利用不能になる事態が発生した。また、令和４年 10 月にも、地方独立行政法人大阪府立病院機構大阪急性期・総合医療センターにおいて、同様の事案が発生した。大阪急性期・総合医療センターの事案を受け、加藤勝信厚生労働大臣（当時）からは、令和４年 11 月 17 日の参議院厚生労働委員会において、「特に今回の大阪急性期・総合医療センターの事案では、委託先事業者を含む関係事業者のセキュリティがこれも一つ課題になっていたため、その管理体制を確認した上で、関係事業者とのネットワーク接続点を全て管理下に置き脆弱性対策を実施することを求めた。また、関係事業者を含め、今後Ｇ－ＭＩＳ[17]を用いた医療機関への調査も実施をしていき、その中で医療機関の対応状況も確認していきたいと考えている」旨の答弁があった[18]。

その後、令和５年４月 25 日には、日本医師会と警察庁サイバー警察局の間で、サイバー事案に係る被害の未然防止等を図るため、緊密な連携を実現すべく、覚書[19]が締結された。

そして、名古屋港の事案の発生後の令和５年８月 25 日の記者会見において、高市大臣からは、「港湾に加え、医療についても、国民の生命、また健康を守る医療機関がサイバー攻撃によって、その機能を失わないように対策を取ることは重要だと考えており、その分野を追加できるように検討をしてほしい旨を事務方に伝えている。国土交通省と厚生労働省において、システムの実態、サイバー攻撃があった場合の影響の程度を精査しているところであり、両省及びＮＩＳＣ[20]とも連携しながら検討していきたい」旨の発言を行った[21]ことを契機に、基幹インフラに医療を加える必要性について、検討が行われることとなった。

（４）「経済安全保障法制に関する有識者会議」における検討

令和５年 12 月 20 日には、「経済安全保障法制に関する有識者会議[22]」基幹インフラに関する検討会合（第１回）が開催され、物流の安定提供の観点から、コンテナターミナルにおいて荷役作業を行う一般港湾運送事業者は基幹インフラ事業者となることが想定されう

---

16 荷役又は船社の委託を受けて、委託者に代わって貨物の受け渡しを行い、受渡行為に先行又は後続する船内荷役、はしけ運送（自走できない特殊な港運船を使って、貨物船と物揚場との間の貨物の荷役作業を行う事業）、沿岸荷役、いかだ運送を一貫して行う事業のこと。

17 Ｇ－ＭＩＳ（医療機関等情報支援システム：Gathering Medical Information System）とは、全国の医療機関から稼働状況、受診者数、医療機器や医療資材の確保状況等を一元的に把握、支援するシステムである。

18 第 210 回国会参議院厚生労働委員会会議録第６号 23 頁（令 4.11.17）

19 <https://www.npa.go.jp/policies/disclosure/notice/document/cyber/R050426.pdf>

20 ＮＩＳＣとは、内閣サイバーセキュリティセンターのことであり、内閣官房に設置され、政府のサイバーセキュリティ政策に関する総合調整を行っている。

21 <https://www.cao.go.jp/minister/2208_s_takaichi/kaiken/20230825kaiken.html>

22 経済安全保障推進法の施行その他必要な事項について意見を聴くために設けられた会議であり、内閣官房長官決裁を根拠とする。

るほか、当該事業者が利用するＴＯＳに支障が生じた際、役務の安定提供が困難となりうることから特定重要設備[23]に該当しうるため、①港湾運送事業については、一般港湾運送事業を基幹インフラの対象事業に追加する方向で検討する一方、②港湾管理者等の行う業務については、特定重要設備の対象となるシステムが想定されないことから、基幹インフラ制度の対象としない方向で検討することが確認された。

一方で、①医療（個々の医療機関）については、基幹インフラ事業者として指定される者や、特定重要設備の対象となるシステムが想定されないことから、基幹インフラ制度の対象としない方向で検討すること、②医療ＤＸに関するシステムについては、基幹インフラ事業者として指定される者や、特定重要設備の対象となるシステムが想定されないため、基幹インフラ制度の対象としない方向で検討することが確認された[24]。なお、同会議では、厚生労働省から「医療機関に対してはサイバーセキュリティ基本法の枠組みの中で省令等改正をし、同法の下、サイバーセキュリティ対策のガイドラインにどの程度準拠しているのか立入検査を行う等、対応状況を確認しつつ、平時から対策を高めることが予防につながると考えている」旨の発言のほか、「経済安全保障推進法の対象に医療機関を含めるかどうかという点に関し、有識者を交えた検討会等は行われていない。同法の基本指針[25]に則り、省内で整理をしたところである」旨の発言があった[26]。

その後、令和６年１月 29 日に「経済安全保障法制に関する有識者会議」が開催され、港湾運送事業について一般港湾運送事業を基幹インフラの対象事業に追加すること及び医療については医療ＤＸの進展を見据えて将来的に検討することを政府に提言することが決定された。

（５）「経済安全保障推進会議」における総理指示

令和６年１月 30 日には、「経済安全保障推進会議[27]」において、岸田内閣総理大臣から「基幹インフラについては、昨年の名古屋港における事案を踏まえ、経済安全保障推進法の対象事業に一般港湾運送事業を追加することが必要である。また、医療に関して、医療ＤＸの進展に合わせて引き続き検討することが必要である」との発言があった。その上で、岸田総理大臣から高市大臣に対して、「基幹インフラに一般港湾運送事業を追加する経済安全保障推進法改正案を早急に取りまとめ、与党との調整を進め、今通常国会への提出に向け、準備を加速する」旨の指示が行われた[28]。

---

[23] 経済安全保障推進法第 50 条第１項において、事業所管大臣は、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定められている。

[24] ただし、今後開発されるシステム（「医療ＤＸ推進に関する工程表」（令和５年６月医療ＤＸ推進本部決定）に基づく、電子カルテ共有サービスやクラウドベースの電子カルテ（標準型電子カルテ）等）の機能によっては、そのシステムがサイバー攻撃等を受けた場合に影響が広範囲に及ぶ可能性もあり、基幹インフラ制度の適用について引き続き検討とされた。

[25] 本稿１．（１）で示した特定社会基盤役務基本指針を指す。

[26] 「経済安全保障法制に関する有識者会議」基幹インフラに関する検討会合（第１回）議事要旨

[27] 令和３年 11 月 19 日に創設された会議であり、議長は内閣総理大臣。

[28] 第６回経済安全保障推進会議議事要旨

３．改正案の概要

（１）特定社会基盤事業として定めることができる事業の追加

特定社会基盤事業に一般港湾運送事業を追加する。つまり、前出の図表１中で示されている14事業に一般港湾運送事業を追加する。なお、一般港湾運送事業における特定重要設備として想定しているのは、ＴＯＳである（主務省令で定める予定）。

（２）附則

改正案の附則では、①公布の日から起算して１年６月を超えない範囲内において政令で定める日から施行する旨の「施行期日」及び②政府は、施行後３年を目途として、この法律による改正後の規定の施行状況を勘案し、必要があるときは、当該規定について検討を加え、必要な措置を講ずる旨の「見直し規定」がそれぞれ定められている。

４．改正案の論点と基幹的なインフラをサイバー攻撃から守るための課題

令和５年７月の名古屋港の事案や同年11月の米国ペンシルバニア州水道局へのサイバー攻撃を始め、国内外で基幹的で重要な役割を果たすインフラをターゲットにしたサイバー攻撃が続出しており、その中でもランサムウェアによる被害は甚大である[29]。

令和６年２月、我が国を始め世界各国の企業等に対してランサムウェア被害を与えている攻撃グループ「LockBit（ロックビット）」について、サイバー特別捜査隊等が欧州刑事警察機構（ユーロポール[30]）等との国際共同捜査を推進した結果、関係国捜査機関が、同グループの一員とみられる被疑者２名を逮捕するとともに、同グループが使用するサーバ等のテイクダウン（機能停止）を実施したとされる。なお、この事案では、我が国のサイバー特別捜査隊[31]が、ランサムウェアによって暗号化された被害データを復号するツールを独自開発し、令和５年12月に同ツールをユーロポールに提供しており、令和６年２月、世界中の被害企業等の被害回復が可能となるよう、ユーロポール等と共に警察庁において、同復号ツールについて情報発信し、その活用を促す旨の発表を行ったとされる[32]。

以下では、本法律案の論点と基幹的なインフラをサイバー攻撃から守るための課題について若干の考察を行う。

（１）対応が後追いとなるリスク

インシデントの発生後、事後的に対象事業を追加する仕組みで十分かといった点については、令和５年12月20日の「経済安全保障法制に関する有識者会議」基幹インフラに関す

---

[29] トレンドマイクロ株式会社の調査では、令和５年に国内企業が公表したランサムウェアの被害数は 63 件で過去最多、ランサムウェア被害にあった国内企業の過去３年間の累計被害額は平均で１億 7,689 万円になったとされる（『日経クロステック』（株式会社日経ＢＰ、令 6.1.10））。

[30] 欧州連合（ＥＵ）の法執行機関であるが、捜査権限はなく、加盟国間の情報交換の促進や収集した情報の分析等が主な任務である。

[31] 重大サイバー事案への対処を担う国の捜査機関として、警察庁の地方機関である関東管区警察局に令和４年４月に設置された。なお、令和６年度予算（警察庁）では、サイバー特別捜査隊のサイバー特別捜査部への格上げと、増員による体制強化を柱とするサイバー対策費として 49 億 6,200 万円が計上されている。

[32] 警察庁「令和５年におけるサイバー空間をめぐる脅威の情勢等について」（令 6.3.14）

る検討会合（第１回）で、委員から「基幹インフラ事業・事業者に指定されていない事業・事業者がサイバー攻撃を受け、そうした事業者にも影響が及ぶことは十分に考えられるのではないか。そのような場合を想定すると、インシデントが発生したことを受けて事後的に特定社会基盤事業を追加するような、ボトムアップのアプローチだけではなく、トップダウンのアプローチが求められるのではないか。基幹インフラについては、政府において、誰から何を買ってはいけないのかを把握すべく情報力を強化し、トップダウンでリスクの高い製品を示すような仕組みを併せて構築しなければ、いたちごっこになりかねない。今のままでは事業者のみの負担が重くなり、効果が上がらないのではないかと懸念する」旨の意見が表明されている[33]。こうした指摘も踏まえ、ＮＩＳＣ、国家安全保障局、警察庁等が連携して、海外でのサイバー攻撃での事例を適宜モニターし、基幹インフラの対象になっていない事業の設備へのサイバー攻撃を認知した場合には、我が国においても基幹インフラの対象に追加すべきか早急に検討するような仕組みを構築すべきであろう。

また、前述したとおり、令和４年３月及び同年４月の政府参考人による国会答弁では、現時点では港湾を基幹インフラに加える必要性はないとしていたが、翌令和５年７月に名古屋港の事案が発生し、港湾のＴＯＳがサイバー攻撃で機能不全に陥り、物流に甚大な影響を被った。港湾施設へのサイバー攻撃の事例は、世界的には名古屋港の事例が初めてではなく、平成29年６月に海運世界最大手のデンマークのマースクの17のコンテナターミナルがサイバー攻撃を受けた事例が存在する。国土交通省や国家安全保障局、ＮＩＳＣ等は、こうした事例の分析を行い、政策に反映すべきではなかったのか。この点については、政府内で十分な検証が行われるべきであり、今後の教訓とすべきであろう。

（２）迅速な対応の必要性

基幹インフラに事業を追加する場合には、経済安全保障推進法上も、企業活動に与える影響の大きさに鑑み、政令等の下位法令の改正で柔軟に対応可能といった形とするのではなく、法改正を必要とする建付けになっている。そして、改正案の附則では、公布の日から起算して１年６月を超えない範囲内において政令で定める日から施行する旨の「施行期日」が規定されている。

政府が事業者に丁寧な説明を尽くすことは不可欠であり、そのための一定の周知期間は必要ではあるが、施行までの期間にまた港湾を狙ったサイバー攻撃が起きないとも限らず、そうした意味では可能な限り、迅速な対応が求められているのではないか。また、医療に関して基幹インフラに追加することは引き続き検討とされているが、まずは個別医療機関の体制整備を着実に進めるとともに、障害時の地域連携の仕組みの整備等について、厚生労働省と各地方公共団体が推進することを速やかに検討していく必要があろう。

（３）他の関連制度も含めた大きな文脈の中で運用する必要性

経済安全保障推進法の第３章は、サイバー攻撃の危険性といっても重要設備等の導入又

---

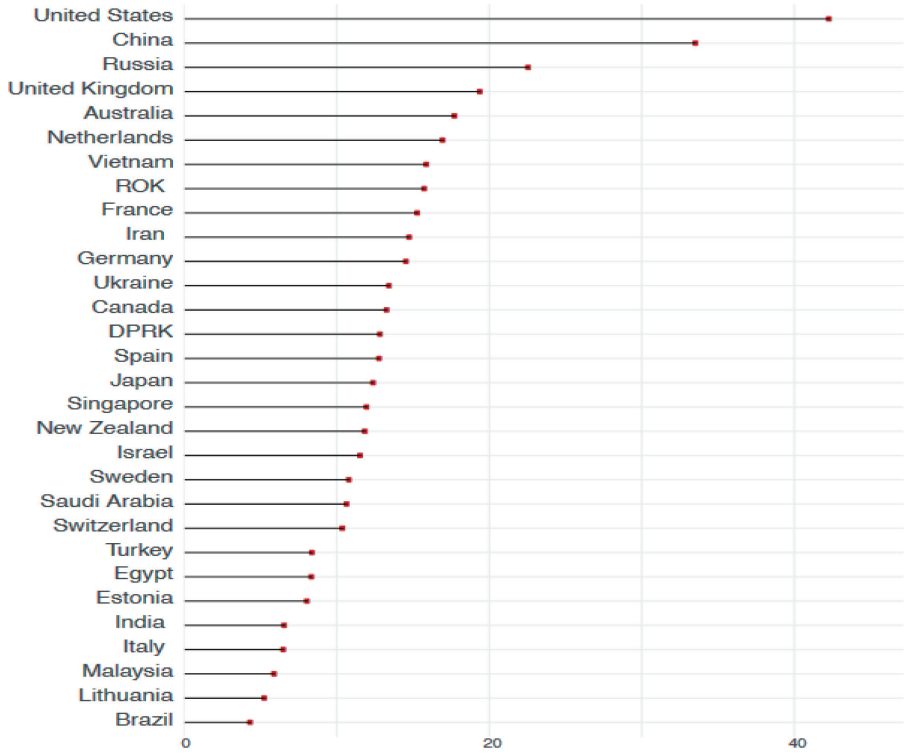
[33] 「経済安全保障法制に関する有識者会議」基幹インフラに関する検討会合（第１回）の議事要旨を参照。

はその維持管理等の委託を通じた妨害行為という相当程度限定されたリスクを想定するものであり、サイバー攻撃全般への対応は本法単独では不十分である。令和３年９月28日に閣議決定された「サイバーセキュリティ戦略」の実施やサイバーセキュリティ基本法に基づく重要インフラに関する障害対応や情報共有体制の強化等の実施と補完関係に立つと考えられ、他の関連制度も含めた大きな文脈の中で運用する必要があるのではないか[34]。

（４）サイバー安全保障分野での対応能力を高める必要性

「国家安全保障戦略」では、「サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」ことが掲げられたものの、現時点ではそれは目標にとどまっていると思われる。例えば、米国のハーバードケネディスクールベルファー科学国際問題センターの「国家サイバー・パワー・インデックス（National Cyber Power Index）」調査によると、日本の順位は2020（令和２）年の９位から2022（令和４）年は16位となっている。なお、同調査の2022年の１位は米国、２位は中国、３位はロシアとされている（図表２）。

図表２　「国家サイバー・パワー・インデックス」（2022年）



（出所）HARVARD Kennedy School BELFER CENTER for Science and International Affairs “National Cyber Power Index 2022”

我が国のサイバー安全保障分野での対応能力を高めていくためには、ＮＩＳＣ、警察庁

[34] 川島富士雄「経済安全保障推進法の制定と一部施行」『法学教室』No.508（令5.1）48頁。

等の組織がそれぞれ能力の向上を図るとともに、そうした機関が効果的かつ緊密に連携して、国家としての対応能力を高めていくことが求められているのではないか。

「国家安全保障戦略」では、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるための具体的な方策として、能動的サイバー防御の導入が掲げられ、令和５年１月31日に、内閣官房に「サイバー安全保障体制整備準備室」が設置されたが、現時点では未整備のままである。能動的サイバー防御の導入に向けては、日本国憲法第21条２項に規定される「通信の秘密」との関係で懸念があるとされるほか、「電気通信事業法」（昭和59年法律第86号）や「不正アクセス行為の禁止等に関する法律」（平成11年法律第128号）では、通信の監視や知り得た秘密を他人に伝えたり、相手の許可なくサーバやシステムに侵入したりすることを禁じていることから、通信の秘密の保護の在り方、権限の濫用を防ぎプライバシーを確保するための方法等の緻密な議論が求められる。ただし、通信の秘密については、令和６年２月５日の衆議院予算委員会で、内閣法制局長官から、「通信の秘密はいわゆる自由権的、自然的権利に属するものであるということから最大限に尊重されなければならない。その上で、通信の秘密についても、憲法第12条及び第13条の規定からして、公共の福祉の観点から必要やむを得ない限度において一定の制約に服すべき場合があると考えている」旨の答弁が行われており[35]、今後の動向を注視する必要があろう。

また、サイバー安全保障分野での対応能力を高めるために不可欠なのは専門人材の育成である。例えば、中部電力パワーグリッドでは、独立行政法人情報処理推進機構（ＩＰＡ）に従業員を派遣して育成したり、北大西洋条約機構（ＮＡＴＯ）などの国際的なサイバー防御演習に参加したりして最先端のスキルを身に付けた人材を育てているとされる[36]。こうした企業による取組を政府としても支援できるような枠組みを検討すべきではないか。

さらに、ランサムウェア等によるサイバー攻撃は、攻撃する側が一箇所を狙ったとしても、サプライチェーンを通じて、複数業種と経済安全保障に打撃を与え得る[37]。こうした点に配意した官民の緊密に連携した取組が求められる。

（５）セキュリティ・クリアランス制度創設がもたらす影響

今常会では、経済安保関係の情報保全を目的としたセキュリティ・クリアランス制度を創設するための「重要経済安保情報の保護及び活用に関する法律案」（閣法第24号）が提出されている。同法案における重要経済安保情報の対象は、サプライチェーンと基幹インフラ等に関する情報とされている。今後、こうした情報に関係する我が国企業や同企業の従業者がセキュリティ・クリアランスを取得することで、国際的な共同研究に参画できることにつながる環境が整っていけば、そうした研究の成果も得て、基幹インフラのサイバー攻撃からの耐性強化に資することも期待できるのではないか。

（かきぬま　しげし）

---

[35] 第213回国会衆議院予算委員会議録第３号（令6.2.5）
[36] 『日刊工業新聞』（令6.1.8）
[37] 『産経新聞』（令6.3.14）