西村あさひ法律事務所

新たな国家安全保障戦略の策定と経済安全保障·サイバー安全保障

独禁/通商·経済安全保障ニューズレター　2022 年 12 月 26 日号

執筆者:
E-mail✉ 桜田 雄紀　E-mail✉ 平家 正博
E-mail✉ 根本 拓

2022 年 12 月 17 日、新たな「国家安全保障戦略」[1]、「国家防衛戦略」及び「防衛力整備計画」(「国家安全保障戦略」を以下、「安保戦略」といい、「国家防衛戦略」「防衛力整備計画」とあわせて「安保三文書」と総称する。)が、国家安全保障会議及び閣議において決定された。

このうち、安保戦略は、我が国の安全保障に関する最上位の政策文書として位置づけられ、外交、防衛、経済安全保障、技術、サイバー、海洋、宇宙、情報、政府開発援助(ODA)、エネルギー等の我が国の安全保障に関連する分野の諸政策に戦略的な指針を与えるものとされる(安保戦略「I 策定の趣旨」)。また、「国家防衛戦略」は、自衛隊を中核とした防衛力の整備、維持及び運用の基本的指針である防衛計画の大綱に代わって、我が国の防衛目標、防衛目標を達成するためのアプローチ及びその手段を包括的に示すために策定されたものである(国家防衛戦略「I 策定の趣旨」)。「防衛力整備計画」は、2027 年度までに、日本への侵攻に対し、同盟国等の支援を受けつつ、これを阻止·排除できる防衛力を構築するため、防衛力の抜本的強化のための計画を定めるものである[2]。

安保三文書は、防衛体制の強化を中心に安全保障上に関する様々な事項について規定しているが、本ニューズレターでは、安保三文書のうち安保戦略に規定される事項のうち、特に企業に経済活動に影響を及ぼし得る、経済安全保障及びサイバーセキュリティの観点から着目すべきポイントについて、速報的解説を試みるものである[3]。なお、本ニューズレターでの以降の引用に係る項目は、特に断りのない限り、安保戦略の項目を意味している。

---

1 安保戦略は、2013 年 12 月 17 日にはじめて策定されたものであり(平成 25 年 12 月 17 日国家安全保障会議·閣議決定)、9 年ぶりの改訂が行われたものである。

2 2022 年 4 月 26 日付自由民主党政務調査会安全保障調査会「新たな国家安全保障戦略等の策定に向けた提言」(以下「4 月 26 日付自民党提言」という。)では、現行の「国家安全保障戦略」と「防衛計画の大綱」は、安全保障認識の点で重複する要素が多いため、「国家安全保障戦略」は戦略レベルでの、安全保障環境や国家安全保障の目標とその達成の方法の記述に重点を置き、「防衛計画の大綱」については、脅威対抗型の防衛戦略に焦点を置いた文書を策定すべき、としたうえで、米国の戦略文書体系との整合性も踏まえ、「防衛計画の大綱」に代わり、「国家防衛戦略」を新たに策定することとしている。また、現行の防衛計画の大綱の自衛隊の具体的な体制に関する記述及び現行の中期防衛力整備計画に代わる文書として、防衛力強化のための「防衛力整備計画」を策定することと、としている(同提言の「3文書のあり方」)。

3 なお、本ニューズレターでは紙幅の関係により割愛しているが、「国家防衛戦略」「防衛力整備計画」においては、防衛産業の生産基盤の強化として、防衛産業のサプライチェーンの強靭化、サイバーセキュリティ強化等が、防衛技術基盤の強化として、防衛装備庁の研究開発関連組織のスクラップ·アンド·ビルドを通じた新たな研究機関を創設等の様々な施策が掲げられている。

また、防衛装備の移転については、安保戦略及び「国家防衛戦略」において、安全保障上意義が高い防衛装備移転や国際共同開発を幅広い分野で円滑に行うため、防衛装備移転三原則や運用指針を始めとする制度の見直しについて検討することとされ、その際、三つの原則そのものは維持しつつ、防衛装備移転の必要性、要件、関連手続の透明性の確保等について十分に検討することとされている。また、「国家防衛戦略」及び「防衛力整備計画」では、防衛装備移転を円滑に進めるための、基金を創設すること等、いわば、防衛版の推進法ともいうべき施策が掲げられている。これらの各種施策については、今後も継続的に情報発信を行っていくことを検討したい。

(参考) 安保戦略の目次

1. 経済安全保障の観点から着目すべきポイント

- 安保戦略の中で、「経済安全保障」の定義が行われた。具体的には、「経済安全保障」は、「我が国の平和と安全や経済的な繁栄等の国益を経済上の措置を講じ確保すること」を意味することが明確化された[4]。また、日本が守り発展すべき「国益」については、「我が国の主権と独立を維持し、領域を保全し、国民の生命･身体･財産の安全を確保」することだけでなく、「経済成長を通じて我が国と国民の更なる繁栄」、「開かれ安定した国際経済秩序を維持･強化」、「自由、民主主義、基本的人権の尊重、法の支配といった普遍的価値」や「国際法に基づく国際秩序」の維持･擁護の概念を含むものとされた(II「我が国の国益」)。
- 安保戦略では、日本の自律性の向上、技術等に関する我が国の優位性、不可欠性の確保等に向けた必要な経済施策として、以下を含む措置を講じていくことを明らかにしている。

① 経済安保推進法[5]の着実な実施と不断の見直し、更なる取組の強化
② サプライチェーン強靭化について、特定国への過度な依存を低下させ、次世代半導体の開発･製造拠点整備、レア

[4] 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「経済安保推進法」という。）においては、「経済安全保障」の定義は置かれていないが、法案の審議の過程において、小林鷹之前経済安全保障担当大臣は、例えば、「国家そして国民の安全を経済面から確保すること」の説明をしていた(衆議院内閣委員会 11 号令和 4 年 3 月 23 日小林国務大臣答弁等)。今般、政府文書においても、明示的に定義されたものである。

[5] なお、経済安保推進法については、本事務所ニューズレター(経済安全保障推進法の内容と外国企業への影響、サプライチェーンの強靭化に係る支援対象物資(特定重要物資)の指定)や、雑誌 NBL 掲載の桜田雄紀「経済安全保障推進法 Q&A50 問」(NBL、1226(2022.09.15)号、1227(2022.10.01)号)等も参照されたい。

アース等の重要な物資の安定的な供給の確保等
③ 重要な物資や技術を担う民間企業への資本強化の取組や政策金融の機能強化等
④ 重要インフラ分野について、地方公共団体を含む政府調達の在り方の検討
⑤ 経済安保推進法の事前審査制度の対象拡大の検討等
⑥ データ・情報保護について、機微なデータのより適切な管理に向けた更なる対策
⑦ 情報通信技術サービスの安全性・信頼性確保に向けた更なる対策
⑧ 主要国の情報保全の在り方や産業界等のニーズも踏まえた、セキュリティ・クリアランスを含む我が国の情報保全の強化に向けた検討 [6]
⑨ 技術育成・保全等の観点から、先端重要技術の情報収集・開発・育成に向けた更なる支援強化・体制整備の検討
⑩ 投資審査や輸出管理の更なる強化の検討
⑪ 強制技術移転への対応強化の検討
⑫ 研究インテグリティの一層の推進の検討
⑬ 人材流出対策等について具体的な検討
⑭ 外国からの経済的な威圧に対する効果的な取組

- 本年 5 月に成立・公布された経済安保推進法関連又はこれに隣接するサプライチェーン強靭化に関わる取組(①②③⑤⑨)[7]や、「⑩投資審査や輸出管理」[8]「⑫研究インテグリティーの一層の推進の検討」といった、政府がこれまでも取り組んでおり、今後も継続的な取組が想定される項目に加えて、これまでの政府説明資料 [9]において、「経済安全保障」の問題としては、必ずしも言及されてこなかったと思われる「⑥機微なデータのより適切な管理の対策」[10]「⑦情報通信技術サービスの安全性・信頼性確保に向けた更なる対策」といったデータの管理や情報通信技術サービスに関する施策が「経済安全保障」の問題として明確に取り扱われていることは注目に値する。
- また、本年 9 月の G7 貿易相会合の共同声明においても、レベルプレイングフィールドの観点から懸念が示された強制的技

6 「⑧セキュリティ・クリアランスを含む我が国の情報保全の強化に向けた検討」に関しては、「経済財政運営と改革の基本方針 2022」(2022 年 6 月 7 日閣議決定)においては、「国際共同研究等における具体的事例の検証等を踏まえつつ、重要情報を取り扱う者への資格付与について制度整備を含めた所要の措置を講ずるべく検討を進める。」とされていた。

7 ②の「次世代半導体の開発・製造拠点整備」については、ポスト 5G 情報通信システム基盤強化研究開発事業等の政府の先端半導体開発に関する取組の一環であると考えられる。また、「⑤推進法の事前審査制度の対象拡大の検討等」については、推進法の基幹インフラ事業者の事前審査制度は、公布日から 1 年 9 か月以内の 2024 年 2 月までの施行が想定され、今後政令等の策定を通じて詳細が定められることが想定されるところ、制度が施行されていない段階において、「対象拡大の検討」が行われていることの趣旨は必ずしも明らかではない。もっとも、現在推進法に掲げられている電気、ガス、石油、水道、鉄道、電気通信、基幹放送、金融等の 14 のインフラ事業領域(推進法 50 条)以外のインフラ事業者に対しても、少なくとも中長期的には、制度の普段の見直しを通じて規制対象が拡大する可能性があることを示唆していると思われ、注目に値する。

8 本年 10 月 12 日に公表された米の National Security Strategy(国家安全保障戦略)においても、投資審査と輸出管理については、「投資審査、輸出管理、防諜のリソースを強化することにより、知的財産の盗用や技術移転の強要等技術的優位性を低下させる他の企てに対抗している。」「戦略的競争相手が米国と同盟国の安全保障を損なうために、米国と同盟国の基盤となる技術、ノウハウ、データを悪用できないようにしなければならない。そのため、我々は輸出管理及び投資審査の仕組みを近代化・強化し、また、戦略的競争相手が我々の国家安全保障を脅かす方法で投資や専門知識を利用することを防ぐため、対外投資の審査等的を絞った新しいアプローチを追求する」として触れられており、これらの施策が、安全保障の観点から重要な施策として位置付けられている。

9 例えば、前記の「経済財政運営と改革の基本方針 2022」(2022 年 6 月 7 日閣議決定)において、「経済安全保障の強化」として掲げられた各種施策(第 3 章 1(2))等。

10 2022 年 10 月 4 日付自由民主党政務調査会経済安全保障推進本部提言「わが国がめざす経済安全保障の全体像について～新たな国家安全保障戦略策定に向けて～」では、「データの管理に関する制度整備」として、情報の機密性に応じたクラウドサービスの利用に関する制度整備(国産クラウド育成を含む)、データのオーナシップに関する制度整備、輸出・投資管理対象の柔軟な見直しが挙げられている(同提言 5 頁)。

術移転の問題[11](⑪)や、同じ共同声明において深刻な懸念が示された貿易に関連する経済的威圧[12]の問題(⑭)について、今後政府において取組の検討が行われることが明らかにされている。

- なお、安保戦略に基づく施策は、国家安全保障会議の司令塔機能の下、戦略的かつ持続的な形で適時適切に実施されること、また、10 年の期間を念頭に置き、安全保障環境等について重要な変化が見込まれる場合には必要な修正を行うこととされており(VIII「本戦略の期間・評価・修正」)、上記の施策は、中長期的に実施が検討されていくことが想定され、必ずしも直ちに行われることを意味していないと思われることには留意する必要がある。

2. サイバーセキュリティの観点から着目すべきポイント

- 「経済財政運営と改革の基本方針 2022」(2022 年 6 月 7 日閣議決定)においては、サイバーセキュリティについては、「経済安全保障」に関する項目としては、「国際情勢の変化等を踏まえたサイバーセキュリティの確保に向けた官民連携や分析能力の強化について、技術開発の推進や制度整備を含めた所要の措置を講ずるべく検討を進める」とされ、経済安全保障の問題としても掲げられてきたが、安保戦略においては、「我が国を全方位でシームレスに守るための取組の強化」の一環として、食料安全保障、エネルギー安全保障、経済安全保障と同様に、経済安全保障の問題とは独立した別途の重要な項目として整理された。そのうえで、「サイバー安全保障」に関する政策は、経済安全保障、安全保障関連の技術力の向上等、サイバー安全保障の強化に資する他の政策との連携を強化することとされた。
- これらの「サイバー安全保障」に関連する施策のうち、注目に値するのは、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」を導入すること、及びその実施のための、体制を整備することとされたことである[13]。
- 安保戦略では、能動的サイバー防御の実施のための体制整備として、以下の①から③までを含む必要な措置の実現に向け検討を進めることとされている

① 重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業

---

11 共同声明の中では、「我々は、既存のツールをより効果的に用いるとともに、非市場的な政策及び慣行に対する適切な新しいツールやより強力な国際ルール及び規範を開発し、公平な競争条件の実現に向けた我々の努力を維持し、更に推進する。我々が共有する懸念には、あらゆる形態の強制技術移転...といった不公正な慣行が含まれる。」と述べられている。なお、強制技術移転の問題は、2017 年以降、米国による通商法 301 条に基づく調査及び対抗措置の発動、米国及び EU による WTO 協議要請、日米欧三極貿易大臣会合等で、継続的に問題提起がなされている。

12 共同声明の中では、「貿易関連の経済的強制力の行使に深刻な懸念を抱いている。経済安全保障、多国間貿易システムにおける自由で公正な貿易、世界の安全保障と安定を損ない、国際的緊張を悪化させる。経済的強制の試みと闘うために、我々は、G7 首脳のコミットメントを再確認し、協力を強化し、経済的強制に対処するための協調的アプローチを模索する。」こととされている。なお、EU は、2021 年 12 月に、経済的威圧に対抗する措置を講ずることを認める規則案が公表するとともに、2022 年 12 月 7 日に、中国のリトアニア産品に対する輸入規制等について、WTO パネル設置を行っている。また、米国で 2022 年 12 月 23 日に成立した国防授権法 2023 年(National Defense Authorization Act for Fiscal Year 2023)に基づき、中国の経済的威圧についての政府横断のタスクフォースを設置し、日本を含む同盟国との連携しながらこれに対抗していくことが想定されている(同法案 Section 5514)。

13 「国力としての防衛力を総合的に考える有識者会議」(2022 年 9 月 22 日付けの内閣総理大臣決裁により設置)の 2022 年 11 月 22 日付報告書(以下「有識者会議報告書」という。)では、サイバー攻撃については、被害を受けてから対処するのではなく、それを未然に防ぐための能動的なサイバー防御(アクティブ・サイバー・ディフェンス)が必要とし、具体的には、我が国全体のサイバー安全保障分野での対応を一元的に指揮する司令塔機能を大幅に強化するなどし、能動的なサイバー防御を実施できるような新たな制度を設けるべきとしている(2(4))。

また、4 月 26 日付自民党提言では、「アクティブサイバー・ディフェンス」について、「一般に、受動的な対策にとどまらず、反撃を含む能動的な防御策により攻撃者の目的達成を阻止することを意図した情報収集も含む各種活動」と説明するとともに、サイバー攻撃を通じて、武力攻撃に至らない侵害を受けた場合の対応については、特に、サイバー分野においては、攻撃側が圧倒的に有利なことから、攻撃側に対する「アクティブ・サイバー・ディフェンス」の実施に向けて、不正アクセス禁止法等の現行法令等との関係の整理及びその他の制度的・技術的双方の視点、インテリジェンス部門との連携強化の観点から、早急に検討を行う、としている(戦い方の変化(4))。

者等への対処調整、支援等の取組を強化する等の取組を進める。

② 国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を進める。

③ 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について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする。

- 安保戦略では、さらに、能動的サイバー防御を含むこれらの取組を実現・促進するために、内閣サイバーセキュリティセンター(NISC)[14]を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置するとされるとともに、これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備、運用の強化を図るとされた[15]。しかし、「能動的サイバー防御」が今後いかなる形で実現するかは不明ではあり、また、通信の秘密等国民の権利侵害に対する懸念を払しょくすること[16]や、不正アクセス禁止法等の現行法令との関係の整理等も必要となることから、今後、これらの法制度の整備、運用の強化を注視していく必要がある。

3. 今後の展望

上記 1 及び 2 で見てきたとおり、安保戦略では、経済安全保障及びサイバー安全保障という、企業活動にも広く影響を及ぼし得る各種の施策を掲げている。2022 年は、日本では経済安保推進法が成立し、経済安全保障という言葉が定着する等、ロシアのウクライナ侵攻にはじまりサプライチェーンの供給の遅延や途絶が生じたこともあいまって、企業が経済安全保障を我がこととして認識せざるを得ない、いわば経済安全保障元年ともいうべきな年であった。2023 年には、経済安保推進法の重要物資の安定供給確保支援制度や、重要技術の研究開発支援が本格化するとともに、基幹インフラ事前審査等の制度が確定していくことが見込まれる。今後、関係する企業としては、制度運用が本格化するこれらの経済安保推進法上の制度について、対応を検討する必要があるだけでなく、安保戦略で掲げられた、今後 10 年のスパンの中で、法律やソフトローの整備が予想される事項についても、継続的な情報収集を行っていく必要がある。まさに「グローバリゼーションと相互依存のみによって国際社会の平和と発展は保障されないこと」が明らかになった今、「戦後最も厳しく複雑な安全保障環境下」にあることを認識しつつ(I「策定の趣旨」IX「結語」)、これらの安保戦略に掲げられた施策について、企業として必要な対応の要否や、場合によっては、所管官庁との間での必要な議論・確認をしていく必要があろう。

以上

---

14 現状では、NISC については、内閣官房組織令(昭和 32 年政令第 219 号)において、概要、次の事務を行うこととされており(同第 4 条の 2)、少なくともサイバー安全保障分野の政策を「一元的」に総合調整する権限は付与されていないようである。

① 情報通信ネットワーク又は電磁的記録媒体を通じて行われる行政各部の情報システムに対する不正な活動の監視及び分析に関すること。

② 行政各部におけるサイバーセキュリティの確保に支障を及ぼし、又は及ぼすおそれがある重大な事象の原因究明のための調査に関すること(内閣情報調査室においてつかさどるものを除く。)。

③ 行政各部におけるサイバーセキュリティの確保に関し必要な助言、情報の提供その他の援助に関すること。

④ 行政各部におけるサイバーセキュリティの確保に関し必要な監査に関すること。

⑤ ①～④に掲げるもののほか、行政各部の施策に関するその統一保持上必要な企画及び立案並びに総合調整に関する事務のうちサイバーセキュリティの確保に関するもの(国家安全保障局、内閣広報室及び内閣情報調査室においてつかさどるものを除く。)

15 サイバーセキュリティ関連の法律としては、サイバーセキュリティ基本法(平成 26 年法律第 104 号)が存在しているが、これを改正する形で制度整備を行うか、或いは新法が想定されているかは現時点では明らかではない。

16 有識者会議報告書においても、「制度の検討に当たっては、その対象が安全保障にかかわるものに限ることを明確化にし、通信の秘密等国民の権利侵害に対する懸念を払しょくすることが必要となる」とされている(2(4))。

当事務所では、クライアントの皆様のビジネスニーズに即応すべく、弁護士等が各分野で時宜にかなったトピックを解説したニューズレターを執筆し、随時発行しております。N&A ニューズレター購読をご希望の方は N&A ニューズレター　配信申込・変更フォームよりお手続きをお願いいたします。また、バックナンバーはこちらに掲載しておりますので、あわせてご覧ください。

本ニューズレターはリーガルアドバイスを目的とするものではなく、個別の案件については当該案件の個別の状況に応じ、日本法または現地法弁護士の適切なアドバイスを求めていただく必要があります。また、本稿に記載の見解は執筆担当者の個人的見解であり、当事務所または当事務所のクライアントの見解ではありません。

西村あさひ法律事務所　広報室　E-mail