Global

〔提　言〕

自主自律的な安全保障について

２０２５年３月

グローバル適塾　第２３期

安全保障グループ

目次

はじめに

2022 年、ロシアによるウクライナ侵攻は世界中に衝撃を与えた。以前から軍事的緊張状態にあったとはいえ、近代国家が隣国に戦争を仕掛けることを、多くの人々が信じていなかった。しかし、実際に戦争は勃発したのである。

ウクライナ侵攻は人道的悲劇であると同時に、世界経済にも大きな打撃を与えた。サプライチェーンの断裂、エネルギー価格の高騰、不安定な市場環境など、多くの企業の活動に困難をもたらした。特にエネルギー資源の多くを輸入に頼る日本にとって、その経済的影響は甚大であった。しかしながら、このような状況下においても、多くの日本人はこの出来事をどこか遠い国の話と捉え、「他人事」として自分たちの平和を当然視していたように思う。

今回の提言において、我々は、日本が位置する東アジア地域における、地域の安全保障について深く考察してきた。

東アジア地域は、地政学的に非常に重要な位置にある。特に日本は、その地理的条件から極めて戦略的な立場にある。日本は、太平洋を挟んで世界最大の経済大国でありアジア太平洋地域に強力な軍事プレゼンスをもつアメリカと接している。一方には、世界第 2 位の経済規模を持ち、経済的・軍事的に急速に勢力を拡大している中国があり、日本の安全保障に直結している。日本はこの二大国の狭間で、地理的にも経済的にも大きな影響を受ける立場にあり、絶えずバランスを取りながら外交・経済政策を進めていかなければならない。さらに、北朝鮮やロシアとも近接しており、世界のパワーバランスに大きく影響している国家に挟まれている日本は、厳しく複雑な安全保障環境に置かれている。

このような状況下において、国家レベルでは当然のように、安全保障政策が立案されている。しかし、その一方で、日本人である我々はそれを「自分事」として捉えられていただろうか。自国を取り巻く地域の情勢を正確に理解し、安全保障政策の内容を把握し、我々自身を守るに十分な安全保障政策だと納得していただろうか。それとも再び「他人事」の話として聞き流していなかっただろうか。

安全保障グループに所属した当初、我々も「安全保障」という言葉に漠然とした難しさを感じ、何か壮大で遠い存在のように捉えていた。しかし、神戸大学大学院の簑原教授からのリアルタイムな情勢を踏まえた講義、RIIPA（認定 NPO 法人インド太平洋問題研究所）を通した各国大使の講演、安全保障政策と直結する自衛隊や在日米軍との交流を経て、世界の安全保障情勢、そのなかの日本の立ち位置や現状を知るうちに、「安全保障とは我々自身の生活そのものであり、安全保障上の危機は常に私たちの身近に存在している」と認識するよう

になった。

特に台湾における海外視察は、安全保障問題を肌に感じる機会となった。台湾の人々と直接交流する中で、彼らが 100 年以上にわたり中国からの圧力を日常的に感じ、緊張感を持ちながら生活していることを知り、我々日本人が如何に平和に甘んじていたかを痛感した。さらに、台湾の人々からは、もし有事が発生した場合には日本が助けてくれるのではないかという期待を寄せられていた。その期待は経済的支援のみならず軍事的支援にも及び、日本がアジア地域の安定をもたらすと信頼されていたが、我々は本当にその信頼に応えられる状況にあるのだろうか。

平和と安全は決して当たり前に存在するものではない。我々は、安心して暮らせる社会を未来の世代に引き継いでいく義務がある。そのために、まさに今、自国の安全保障について正面から向き合い取り組まねばならない。

提言書作成にあたっては、国家レベルでの施策に留まらず、企業や個人レベルでもどのような安全保障施策に取り組むべきか、という視点で考察してきた。これは「安全保障を決して他人事にしない」という我々の決意であり、現場で働く企業人であり、日常生活を送る一般人である我々だからこその提言を生み出したいとの意志である。

この提言書が、単なる理論や政策の提言に留まらず、我々自身の手で安心して暮らせる豊かな未来を創り上げていくための第一歩となることを期待する。

第１章　日本の安全保障を取り巻く環境

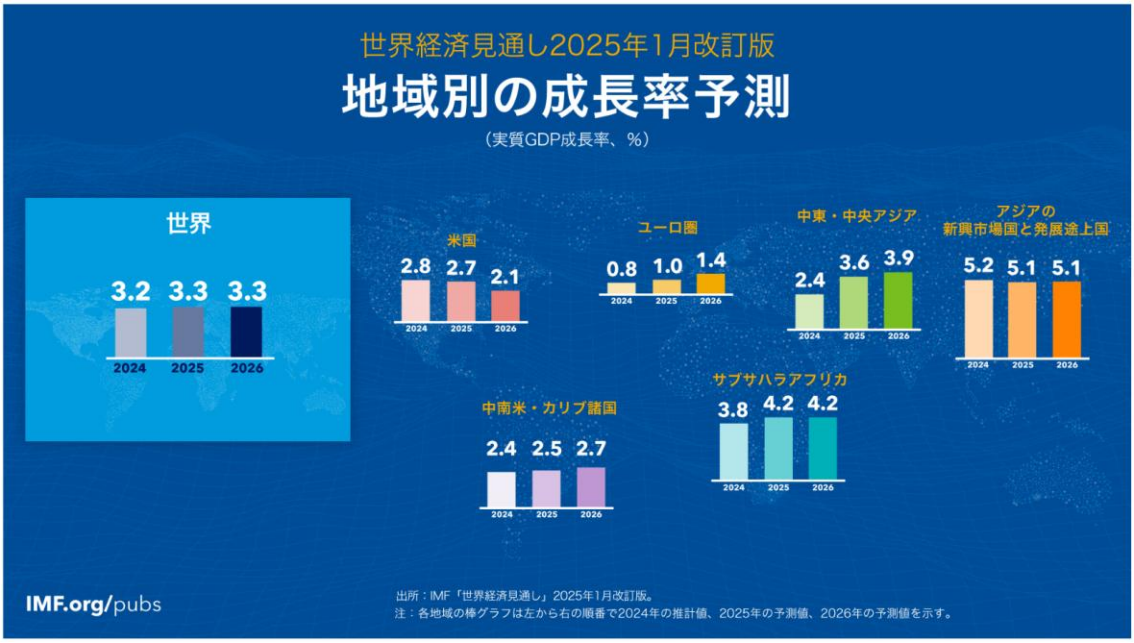
1.1 東アジアを取り巻く情勢

日本が位置している東アジアは、近年、経済的および地政学的な観点から国際社会に強い影響を及ぼしており、日本、中国、韓国といった経済大国や、著しく経済成長を遂げている東アジア諸国連合（ASEAN）が集まり世界経済を支える一方で、多様な価値観を持つ国家の存在が軍事的緊張を引き起こしており、グローバルなパワーバランスを変化させ、世界全体の軍事的緊張へとつながっている。

1.1.1 世界における東アジアの経済的重要性

東アジアは、世界の主要な経済圏の一つとしてグローバル経済に大きな影響力を持っている。2024 年の国際通貨基金（IMF）の予測によると、中国、日本、韓国、ASEAN 5 か国の名目 GDP 合計は 29.5 兆 US ドルに達し、これら 8 カ国だけで世界 GDP の約 25%を占めている。さらに、2025 年 1 月に発表された「世界経済見通し」（IMF）によれば、2025 年と 2026 年の実質 GDP に基づく世界経済の成長率が 3.3%と予測されている。一方で、インドを含むアジア新興市場国と発展途上国の成長率は 5.1%と世界平均を大きく上回っており、アジア地域の発展と成長が世界経済全体に大きな影響を与えている。

【図表 1.1.1-1】地域別の実質 GDP 成長率予測



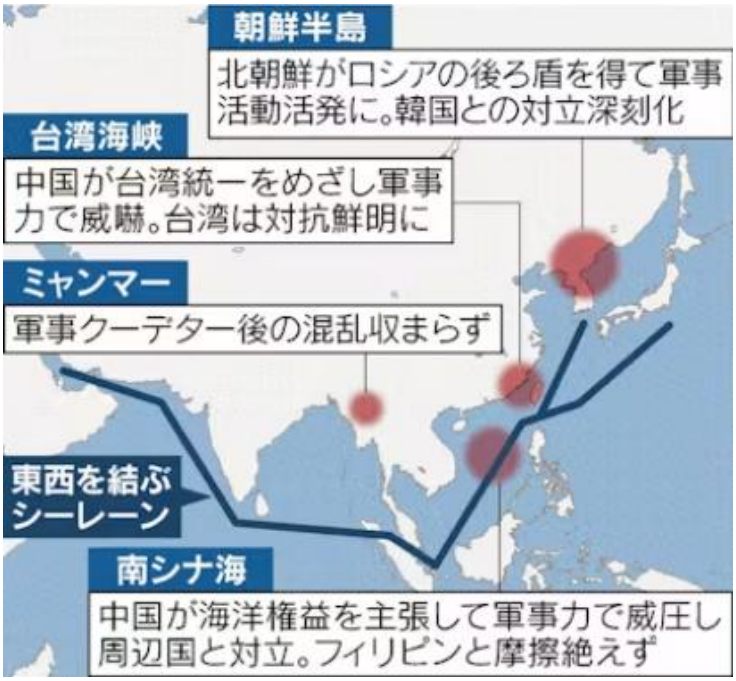
出典：IMF 世界経済見通し(2025 年 1 月)

これらの経済成長を支えている要因の一つが貿易である。特に中国の輸出額は 3 兆 US ドルを超え世界第 1 位となっており、第 2 位のアメリカの 2 兆 US ドルを大きく上回る（2023 年)。中国は「世界の工場」として呼ばれ、多様な製品をグローバル市場に輸出しており、アメリカやヨーロッパをはじめとする多くの国々は中国製品に依存しているという現状がある。また、日本や韓国も自動車やエレクトロニクス、ハイテク製品などの高付加価値製品をグローバル市場に輸出し、自国の経済成長の基礎としている。ASEAN 諸国も中国に次ぐ製造拠点としての地位を高め、急速に成長している。これらの東アジアの国々の貿易活動が、世界の産業活動や製品供給に大きく寄与していることは明らかであり、東アジアは世界のサプライチェーンの中心的な存在となっている。

1.1.2 世界における東アジアの地政学的重要性

東アジアは急速に成長・発展していると同時に、多様な価値観を持った国々が存在している。中でも、普遍的価値やそれに基づく政治・経済体制を共有しない国家が勢力を拡大してきており、経済力の増大はそのまま軍事力の強化となり、地域全体の軍事的緊張が増大している。また核兵器を含む強大な軍事力を有する国の存在や、歴史的な経緯を背景とする外交課題が複雑に絡み合い、複数の安全保障リスクを抱える地域である。

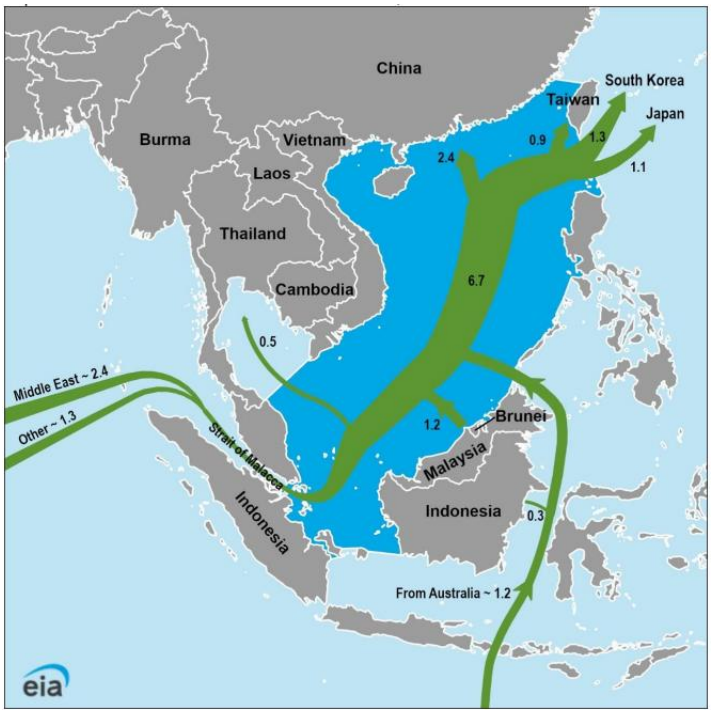
【図表 1.1.2-1】アジアに点在する主な安全保障リスク



出典：日本経済新聞(2024 年 11 月 22 日付)

特に、地政学的な観点から、東アジアはユーラシア大陸の東端に位置し、かつ太平洋を挟みアメリカと向き合う形で存在していることから、世界の安定と国際的な安全保障に大きな影響を及ぼしている。東シナ海、南シナ海、日本海などの海域を擁しているが、これらの海域には重要な海上交通路（シーレーン）が交錯しており、世界貿易の大部分がこれらの航路を利用している。例えば、南シナ海はアジアと中東・ヨーロッパを結ぶ主要な航路であり、世界総貿易額の約 25%がこの海域を通過していると推定される。特にエネルギー資源の輸送においては要所となっており、世界の海上石油輸送の 43%、液化天然ガス（LNG）輸送の 34%が南シナ海を経由している。南シナ海を通過したエネルギー資源は中国や韓国、日本などへ輸入され、各国の経済を支えている。

【図表 1.1.2-2】南シナ海における LNG 貿易量(兆立方フィート、2023 年)



出典：“Regional Analysis Brief: South China Sea” U.S. Energy Information Administration (2024 年)

この重要な海域の支配権を持つことは各国の経済成長と密接に結びつくことから、日本や韓国、アメリカなどの周辺国は航行の自由と開かれた海域の維持を主張している一方、中国や ASEAN 諸国は南シナ海の領有権を主張しており、地域の軍事的緊張が発生、グローバルな安全保障の課題をもたらしている。

次節以降では、東アジアの安全保障における主要プレーヤーである中国とアメリカについて、より深くその安全保障の方針と政策について述べる。

1.2 中国の安全保障に対する状況

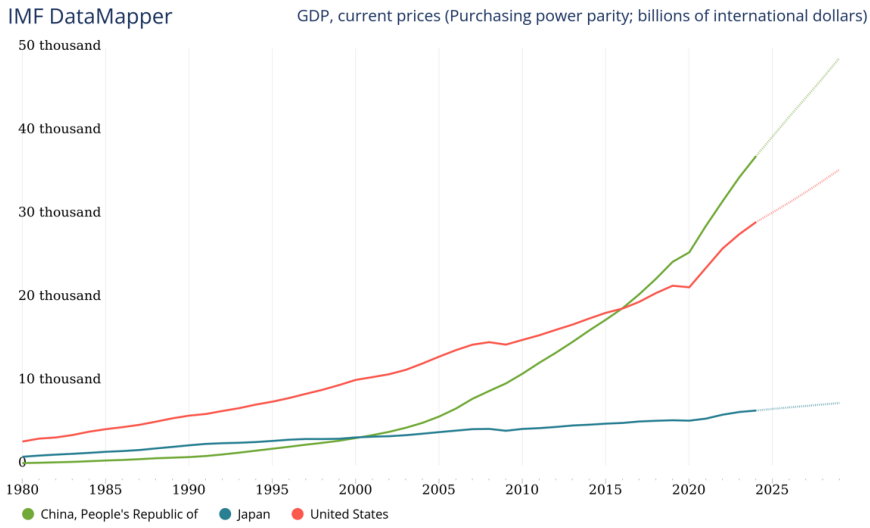
1.2.1 中国の国際社会におけるプレゼンス強化の政策

中国は急速な経済成長を背景に、国際社会におけるプレゼンスを強化するための積極的な政策を展開している。多くの国との間で経済協力やインフラ投資を通した密接な関係を構築したり、国防予算の増強や軍事技術の向上に取り組むことで、世界の舞台における中国の存在感を全方位的に高めている。

(1) 中国経済の発展

過去十数年にわたり、中国の経済成長は非常に高い水準を維持してきた。近年では、労働人口の減少、労働生産性の伸び悩み、不動産市場のバブルなどの影響により、その成長の勢いはやや鈍化してきているものの、名目 GDP ではアメリカに次ぐ世界第 2 位の経済大国である。さらに、各国の物価水準を調整した購買力平価 GDP では、2016 年より世界一の座を維持し続けており、中国の経済力は他国に対する競争力を一段と高めている。

【図表 1.2.1-1】購買力平価

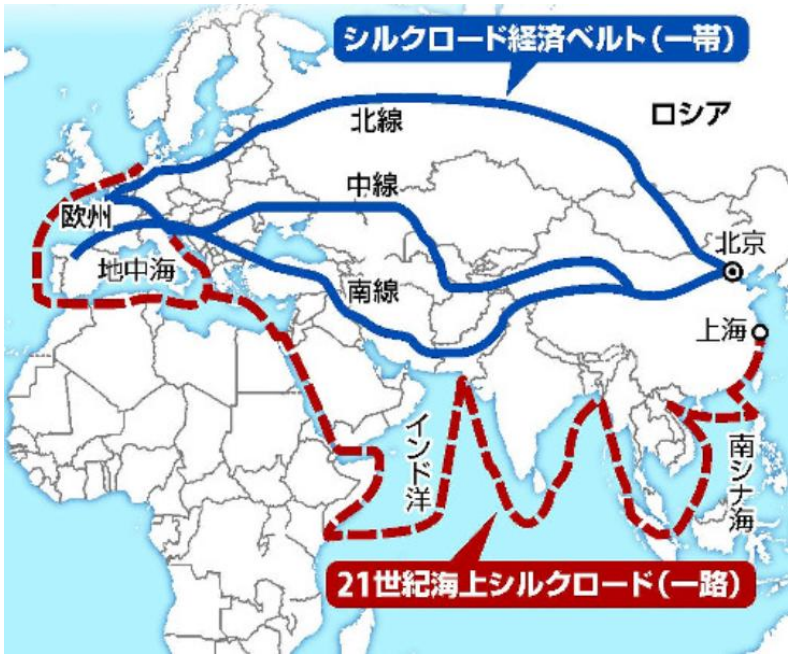


出典：“World Economic Outlook” IMF(2024 年 10 月)

この経済力を背景に、中国は広範囲にわたって国際投資を展開している。特に注目すべきは、2013 年に提唱された「シルクロード経済ベルトと 21 世紀海洋シルクロード」、通称「一帯一路」構想である。この壮大な構想は、アジア、アフリカ、ヨーロッパの国々を陸路と海路の両面から結びつけ、経済連携とインフラ開発を推進することを目的としている。提唱から約 10 年が経過した現在、その累計関与額は 1 兆 530 億 US

ドルに達した。2023 年時点において 149 か国がこの一帯一路プロジェクトに参加しており、2023 年には 212 件の契約が結ばれ、総額 92.4 億 US ドルの投資が行われた。この投資額は 2022 年から約 18%も増加している。これらは、中国の国際的地位向上と経済的影響力が急速かつ顕著に強化されていることを明確に示している。

【図表 1.2.1-2】一帯一路のイメージ図

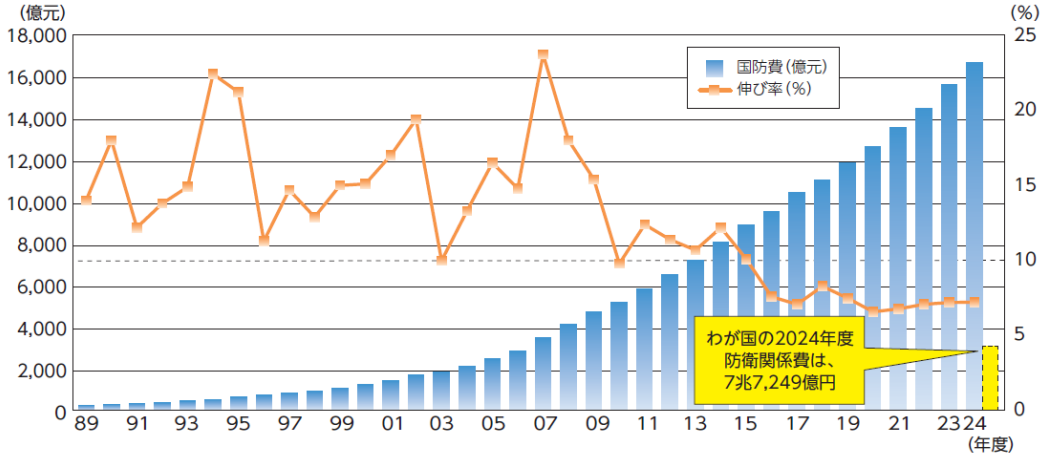


出典：読売新聞（2017 年 5 月 29 日付）

(2) 中国軍事力の質と量の拡充

中国は経済力の強化に伴い、軍事力の拡充にも力を入れている。中国の公表された国防予算は速いペースで増加しており、1994 年度からの 30 年間で約 32 倍に達している。2024 年度の国防予算は 1 兆 6,655 億元と発表されており、これは日本円に換算して約 36 兆円（2025 年 2 月為替レート）に相当する。この額は、日本の防衛関係費である 7 兆 7,249 億円の約 4.7 倍に相当する。

【図表 1.2.1-3】中国の公表国防予算の推移

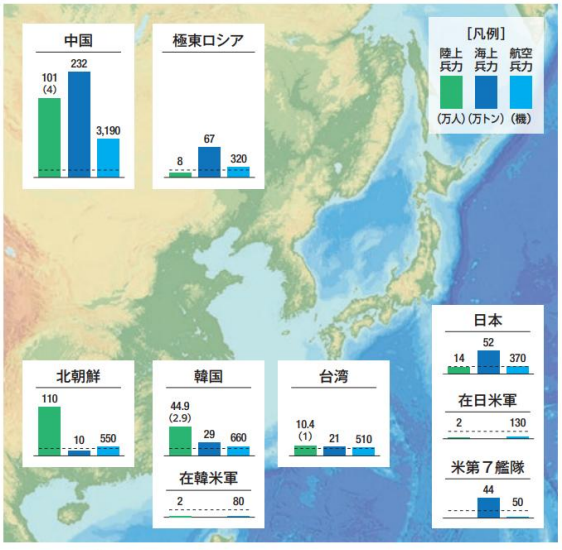


(注) 「国防費」は、「中央一般公共予算支出」(2014年以前は「中央財政支出」と呼ばれたもの)における「国防予算」額。「伸び率」は、対前年度当初予算比。ただし、2002年度の国防費については対前年度増加額・伸び率のみが公表されたため、これらを前年度の執行実績からの増加分として予算額を算出。また、16年度および18～24年度は「中央一般公共予算支出」の一部である「中央本級支出」における国防予算のみが公表されたため、その数値を「国防費」として使用。伸び率の数値は中国公表値を含む。

出典：令和 6 年版 防衛白書(2024 年)

特に習近平政権下では、大規模な軍備増強が進められており、核・ミサイル戦力の近代化・多様化・拡大や、海上・航空戦力を中心に、軍事力の質・量を大幅に強化している。特に海軍は、アメリカを上回る規模の艦艇を保有しており、世界最大とも指摘される。

【図表 1.2.1-4】東アジアにおける主な兵力の状況(概数)(2022 年度)



(注)1 令和5年版防衛白書をもとに作成。
2 在日・在韓米軍の陸上兵力は、陸軍および海兵隊の総数を示す。
3 ( )は海兵隊の兵力で内数。
4 日本は、実勢力を示す。
5 - - - - - は、1976年の日本の実勢力の水準を示す。

出典：令和 6 年版 防衛白書(2024 年)

さらに近年では、サイバー戦力や宇宙戦力の強化も進めている。中国は、「ネットワーク空間と宇宙空間は各方面の戦略的競争の新たな要害の高地（攻撃ポイント）」であるとし、これらの空間における情報優勢を獲得することが重要であると表明している。敵対国への情報収集や諜報活動、インフラへの攻撃といった攻撃的サイバー作戦を実施する部隊が設置されていると言われ、中国軍全体のサイバー作戦能力を強化しているとみられる。また、宇宙領域においても軍事目的にも利用可能な人工衛星の数を急速に増加させ、軍事作戦遂行能力の強化を図っていると考えられる。

1.2.2 中国の東アジアへの進出

歴史的に中国はアジアにおける文化・経済・軍事の中心国であり、世界の列強のひとつでもあった。しかし、19 世紀から 20 世紀初頭にかけてのアヘン戦争、日清戦争、義和団事件などを経て、大国の地位を徐々に失ってきた。その後、中国はアジアおよび世界の支配的な地位を再び取り戻すため、強いナショナリズムと復興意識のもと、「中華民族の偉大な復興」という壮大な目標を掲げ、具体的な取り組みを進めている。その一つが、中国の東アジアへの進出であり、これには大きく 2 つの理由がある。

1 点目は、海洋路の安全確保による安定的な経済成長である。中国は経済活動やエネルギー輸入の多くを海上貿易に依存しており、海上交通路の安全確保が極めて重要である。特に南シナ海は中東からのエネルギー輸送の主要ルートであり、中国の経済成長において生命線となる海域である。この地域を支配下に置くことは、安定的な経済成長を維持するうえで不可欠である。さらに南シナ海の海底には豊富な石油や天然ガス資源が存在するとされており、これらの資源へのアクセス権を確保することも経済発展に寄与する。

2 点目は、地政学的な包囲を防ぎ、中国の国際的なプレゼンスを高めることである。中国は、アメリカを中心とした西側諸国とその同盟関係国である日本や韓国、フィリピン、オーストラリア、インドといった国々に囲まれている。第一列島線（日本列島、台湾、フィリピン）を起点に中国の防衛範囲を確立し、中国沿岸部への直接な脅威を軽減させることは重要である。同時に、第二列島線（グアム、パラオ、パプアニューギニア）を目指して防衛ラインを外洋に前進させることで、特にアメリカの影響力が強いアジア太平洋地域において、中国の影響力を拡大することができる。これにより、中国の国際的な地位を大幅に向上させ、アメリカと肩を並べる二大強国となり世界の支配権を持つ可能性がある。

【図表 1.2.2-1】逆さ地図に見る中国海洋進出と第一列島線、第二列島線

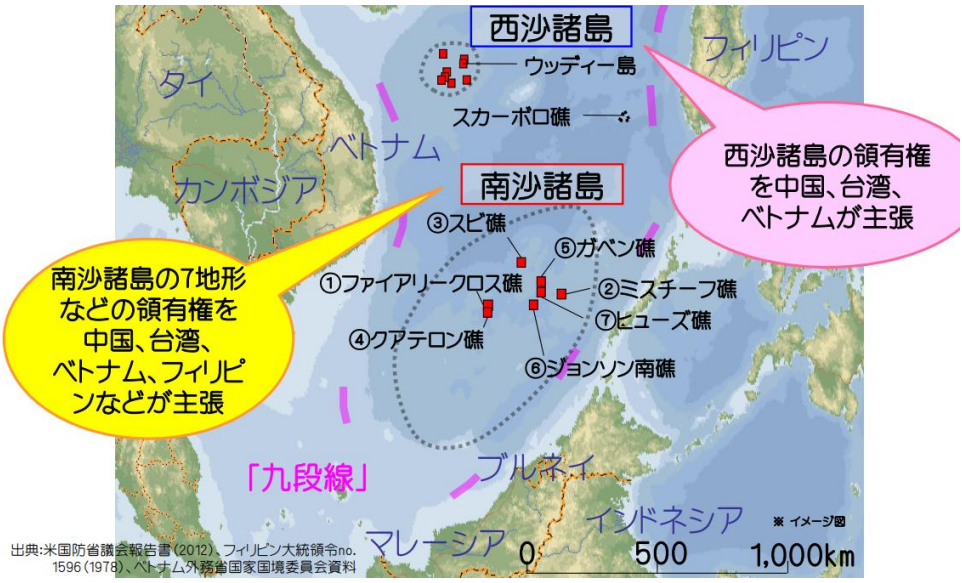
出典：産経新聞（2019 年 1 月 1 日付）

このような背景から、中国の東アジアへの進出は世界中の関心を集めている。本提言においては、具体例として、南シナ海の南沙諸島（スプラトリー諸島）及び台湾海峡における中国の活動について述べる。

（1）南沙諸島（スプラトリー諸島）における中国の活動

南沙諸島は南シナ海の中部に位置する多くの無人島および岩礁群であるが、前述の通り重要な海上交通路であること、また豊富な石油や天然ガス資源があるとされており、中国、台湾、フィリピン、ベトナム、マレーシア、ブルネイなど複数の国が領有権を主張している。

【図表 1.2.2-2】南シナ海情勢全体図



出典：防衛省 南シナ海情勢（中国による地形埋立・関係国の動向）（2024 年 9 月）

中国は 1950 年代より「九段線」と呼ばれる境界線を設定し南シナ海の領有権を主張し続けている。特に 2014 年以降、南沙諸島にある 7 つの地形（ファイアリークロス礁、クアテロン礁、他）を急速かつ大規模に埋め立てて人工島を建設、インフラの整備を行った。2016 年、国際仲裁裁判所はフィリピンが提訴した南シナ海問題に関する判決において、中国が主張する「九段線」の根拠となる歴史的権利を否定し、中国の埋め立て活動の違法性が認定されたが、中国はこの判決を受け入れる意思がないことを明確にしており、空港や港湾、レーダー・通信施設、砲台などの軍事設備を建設、中国の軍事拠点化を強力に推進している。

【図表 1.2.2-3】中国による南沙諸島の急速な埋立と軍事拠点化

出典:CSIS Asia Maritime Transparency Initiative(写真含む)/ 2016年及び2017年米国防省議会報告書 /Google Earth(長さ)、各種報道

出典：防衛省 南シナ海情勢（中国による地形埋立・関係国の動向）（2024 年 9 月）

これらの人工島周辺では中国海軍や中国海警局の艦船が頻繁に巡回しており、南シナ海全域に対する中国の領有権を主張、周辺国や国際社会に対して力の誇示を行っている。フィリピン軍の輸送船に対して中国海警局の船が接近し放水砲を用いて妨害活動を行うなど、挑発的行動が散見されており、こうした中国の軍事的行動に対して、ベトナムやフィリピンなどの東南アジア諸国、アメリカをはじめとする国々からの反発が高まっている。

【図表 1.2.2-4】中国海警局によるフィリピン船への放水

出典：日テレ NEWS NNN(2023 年 11 月)

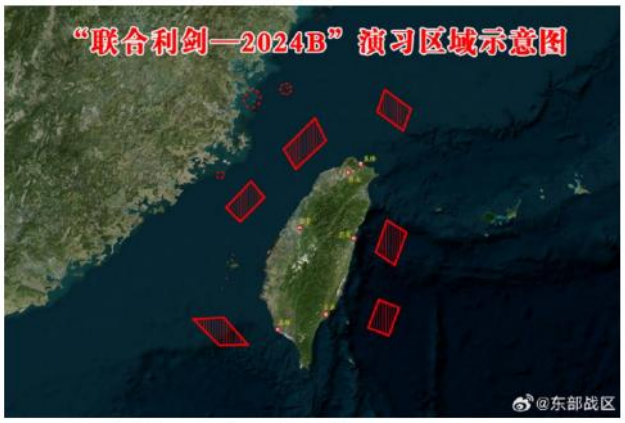
アメリカは南シナ海における「航行の自由作戦（Freedom of Navigation Operations)」を展開し、実際に南沙諸島周辺の海域において米海軍の駆逐艦を航行させることで国際法にて認められた「航行の自由」を主張、国際法の遵守と国際的な海上秩序の維持に対する強いメッセージを発信している。

(2) 台湾海峡における中国の活動

台湾海峡は、中国大陸と台湾島の間に位置する約 130ｋｍの海域であり、非常に重要な戦略的要所である。この海峡は南シナ海と東シナ海を結ぶ重要な海上交通路であり、中国は台湾海峡を支配することで、地域の影響力を高めることができる。

また、1949 年の中国国内共内線終結以降、台湾海峡を挟んで中国と台湾は対立と緊張を繰り返してきた。中国政府は、台湾は中国の一部であるとの「一つの中国」原則を堅持しており、台湾島を再統一しようとする意図を常に持っている。直近では 2024 年 10 月、頼清徳・台湾総統による「中華人民共和国と中華民国は互いに隷属しない」「中華人民共和国には台湾を代表する権利はない」との演説に、中国は強く反発。同月 14 日、中国人民解放軍は台湾をほぼ取り囲む形で大規模な軍事演習を実施、空母を含む 125 機を投入するなど武力行使もちらつかせ、以降は中国海警局による台湾島の周回パトロールを実施するなど強硬な姿勢を鮮明にしている。

【図表 1.2.2-5】中国による台湾周辺での軍事演習区域と周回パトロール



東部戦区が公表した演習区域のイメージ図
（演習区域の具体的な座標等は明らかにしてない）

海警局が公表したパトロールのイメージ図

出典：防衛省 中国の台湾周辺における軍事演習について（2024 年 9 月）

1.3 アメリカを中心とした世界の東アジア安全保障政策

1.3.1 アメリカの東アジアに対する安全保障政策

第二次世界大戦後、冷戦期におけるアメリカの東アジアに対する安全保障政策は、ソ連の軍事的脅威を封じ込めることに重点を置いていた。アメリカは日米安全保障条約や米韓相互防衛条約などの二国間協定を通じて強固な軍事同盟網を構築し、共産主義の拡散を防ぐことを最重要課題としていた。

冷戦の終結後、ソ連の脅威が消滅すると、アメリカの安全保障政策は経済的繁栄と地域の安定に重点を移したかと思われた。1990 年代初期には、中国が市場経済に移行して国際秩序に統合されることを期待され、アメリカにより中国を支援するような動きも見られた。しかし、中国の経済が急成長し、軍事面でも急速な近代化を遂げると、その影響力の増大に対する懸念が高まり、アメリカは次第に中国を東アジアにおける安全保障政策の中心的懸念として認識するようになった。その契機となったのは 1995 年から 1996 年にかけて行われた、中国の台湾海峡における連続的ミサイル発射実験である。これは台湾に対して威嚇行動を取ったものであるが、アメリカは 1979 年に制定された「台湾関係法」に基づき、台湾の安全保障と防衛を支持していたため、このミサイル発射実験はアメリカに対する挑発行為と見られ、米中関係は急速に緊張状態となった。

その後、2001 年の 9・11 同時多発テロ発生により「テロの戦い」へと安全保障上の課題が大きく転換した際、中国はテロとの戦いに協力する姿勢を見せ、2000 年代前半まで両国は「建設的な協力関係」を築いていた。

しかし2000年代後半になると、リーマンショックによる米経済が衰退したことを背景に、前述の通り、中国が南シナ海や東シナ海における領有権問題に強硬な姿勢を示すようになった。この中国の軍事的活動に対して、アメリカは東アジアの軍事バランスに重大な影響を及ぼすとの懸念を抱き、オバマ政権下の 2011 年には、「アジア・リバランス政策（Asia Rebalance Policy)」が打ち出され、東アジア地域の同盟国との安全保障協力の強化、グアムやオーストラリアへの軍事配備の増強といった軍事的プレゼンスの強化、および環太平洋パートナーシップ協定（TPP）の推進による経済連携の強化を通じて、中国の影響力を抑制し、アメリカのパワーバランスの維持に努めてきた。

1.3.2 トランプ政権下での東アジアの安全保障政策

アメリカの東アジア政策は、冷戦終結後一貫して中国の台頭を警戒しつつ地域の安定を図るものであったが、第一次トランプ政権が対中強硬姿勢を明確にしたことにより、東アジアの安全保障の構図が大きく変化することとなった。

2017 年に就任した第一次トランプ政権の安全保障政策は「アメリカ第一主義（America First)」を掲げて展開された。トランプ政権は、対中強硬路線を打ち出し、経済、技術、軍事の面から中国に対して厳しい対抗策を取った。2018 年、長年の貿易赤字を是正するべく、中国からの輸入品に対して 25%と大幅な関税の引き上げを実施。それに対して中国も報復措置として同等の関税をアメリカ製品に課すなど、米中両国間の貿易関係は急速に緊張し、世界経済にも大きな影響を及ぼした。加えて、トランプ政権は米国内の雇用を守るために、パリ協定や TPP から離脱した。

さらにトランプ政権は国防予算の大幅な増額を推進し、2018 年の国防予算は前年より 10%増加され、老朽化した軍備の更新や新技術の導入が進められた。具体的には F-35 戦闘機の導入や新型選管の建造、サイバーセキュリティ対策の強化などが挙げられる。自国の国防予算の増加と同時に、トランプ政権は同盟国に対する圧力も強めた。NATO 加盟国に対しては、防衛費を GDP の 2%以上に増やすことを強く求め、日本や韓国にも駐留米軍の費用分担を増やすように要求、これらの政策はアメリカの負担を減らし、同盟国自身が防衛の責任をより多く担うよう求めるものであった。実際のところ、アメリカが文書上で防衛する義務を負う同盟国は少なくとも 51 カ国に駐留する 14 億人以上おり、これはアメリカの人口の 4 倍以上に相当する。同盟国への防衛費の増額要求は、アメリカが過度に他国防衛に費やしている資源を削減する意図があった。

【図表 1.3.2-1】アメリカの条約同盟国

出典：Defense Priorities Foundation(2022 年 10 月)

しかし、このような「アメリカ第一主義」の政策は、ときにルールに基づく国際秩序を軽視しており、孤立主義的な外交と紙一重である。同盟国に対する防衛費増額の要求や多国間協定からの離脱は、アメリカと同盟国との関係に緊張をもたらし、関係の弱体化につながった。さらに、パリ協定や TPP からの離脱は、中国が国際的な影響力を拡大する余地を与える結果となり、東アジアにおいて中国が主導権を握りやすい状態を生み出した。

2025 年に発足した第二次トランプ政権においても、これら第一次トランプ政権での「アメリカ第一主義」を基軸とした安全保障政策が継続されることが見込まれる。元々、アメリカの東アジアにおける安全保障政策は、世界最強であるアメリカとのアジア各国による二国間同盟を主軸にパワーバランスを保ってきた。しかし 2000 年代以降はアメリカの相対的な国力が低下し、QUAD（日米豪印戦略対話）や IPEF（インド太平洋経済枠組み）などの多国間枠組みを発展させることで、東アジアのパワーバランスを保持し続けてきた。

もし第二次トランプ政権が第一次と類似の孤立主義的な外交政策を続けた場合、東アジアにおける安全保障環境が複雑化することが懸念されるトランプ大統領は選挙戦を通して、アメリカの要求に応じて防衛費の引き上げを行ってきた日本や韓国、台湾の同盟パートナーに対しても更なる防衛費・軍事費の支出を要求すると発言したり、自助努力を行わない同盟国の防衛に対してアメリカは関与しないという姿勢をちらつかせるなどしている。これらの動きは同盟国を疲弊させ、アメリカと同盟諸国の関係性が弱体化、東アジアにおけるアメリカのプレゼンスをさらに低下、地政学的バランスの崩壊を招く可能性がある。日本、韓国、台湾における安全保障環境は悪化して緊張感が高まり、さらに相対的に国力が劣るフィリピンの場合は、南シナ海におけるフィリピンの防衛線が後退する可能性もある。東アジアへの進出を画策している中国にとって、南沙諸島や台湾海峡での武力行使・実効支配のまたとないチャンスになり得る。

1.3.3 ロシアや北朝鮮の東アジア安全保障政策

ロシアと北朝鮮は、東アジアの中で中国とのつながりが強い国々である。

ロシアは、東アジア地域において他国領土への積極的な侵攻を行うような安全保障政策を採用しているわけではないが、中国と同様、東アジアにおけるアメリカのプレゼンスが高まることを好ましく思っていない。中国との大規模な合同軍事演習を定期的に開催するなど、中国との戦略的パートナーシップを進展させることで、自国の東アジアにおける影響力強化を狙っている。

北朝鮮は、主に国家存続と体制維持を中心に安全保障政策を構築している。自国の安全保障を強化するために核武装と弾道ミサイル開発を進めることで、アメリカや日本、韓国への軍事的抑止力を誇示している。北朝鮮の安全保障政策は主に防衛的であり、他国の領地への進出などは行っていないが、韓国や日本に対して軍事的威嚇行動をとるなど、地域の安全保障環境の不安定化の一因となっている。

1.3.4 欧州・カナダの東アジア安全保障政策

欧州やカナダは地政学的には東アジアから離れた位置にあるものの、東アジアにおける安全保障政策にも積極的に関与する姿勢を見せている。

欧州連合（EU）はウクライナをめぐるロシアとの対立に対応するために多くのリソースを投入している一方で、2021 年 4 月に「インド太平洋戦略」を策定、日本や ASEAN 諸国などの東アジア諸国との連携を強化している。これは、EU がインド太平洋地域における最大の投資国で主要な開発パートナーであり EU の経済成長に重要な地域と考えていることや、欧州の対外貿易の約 40%が南シナ海を通過しており同地域の不安定化が共通の懸念であることが背景にある。

カナダもアジア太平洋の安定は世界の平和や安全保障の確保に不可欠であると考え、2022 年 11 月に「インド太平洋戦略」を発表した。この戦略は、抽象的な目標ではなく、10 年間にわたって 23 億カナダ･ドルの予算を計上し、5 つの柱に対して具体的な目標と予算が設定された点が画期的であり、カナダの外交政策における重要な転換点で、東アジアにおけるカナダの役割を強化することが期待されている。

1.4 有事の定義

本節では、本提言書における「有事」の概念とその適用範囲について明確にしたい。有事とは、国家が重大な脅威に直面し、通常の生活や経済活動が損なわれる事態を指すが、現代社会において脅威は広範囲に存在している。

最も狭義の有事の定義は、日本への直接な武力攻撃である。具体的な例としては、沖縄や

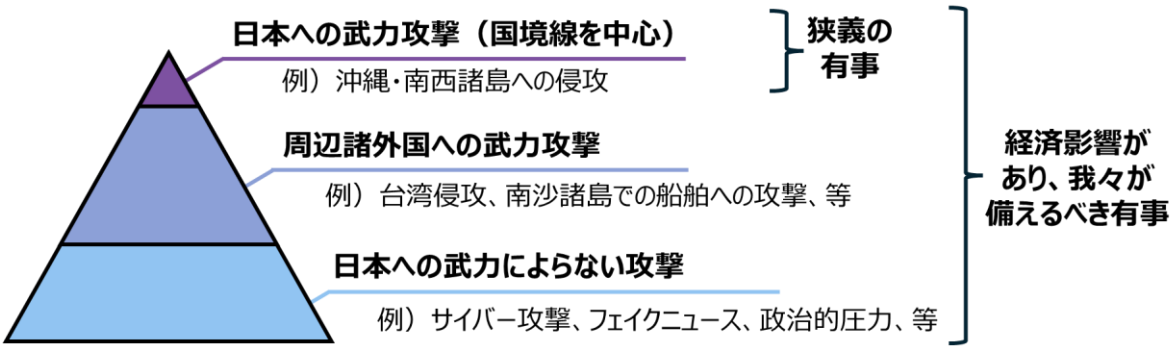
南西諸島への侵攻が挙げられる。このような事態は、国家の安全保障に直接的な影響を与え、国民の生命や財産に甚大な被害を及ぼす。我々塾生自身、安全保障について学ぶまでは有事とはこの狭義の有事だけを指すと考えていた。

しかし、現代社会における有事の範囲はこれだけに留まらない。次のフェーズとして考えられるのは、周辺諸外国への武力攻撃である。例えば、台湾への侵攻や、南シナ海の諸島への攻撃、ウクライナ侵攻などがこの有事に該当する。これらの事態は日本国土への直接的な攻撃ではないが、物理的な近接性や経済的な結びつきから日本に間接的な影響を及し、日本経済や安全保障に重大な問題を引き起こす。

さらに最も広義で最も現代に起こりうる有事として、武力に依らない攻撃も有事に包含される。サイバー攻撃、フェイクニュースの拡散、政治的圧力などがこれに該当する。サイバー攻撃によって重要なインフラが麻痺すれば経済活動の停止を引き起こし、フェイクニュースや情報操作で社会の不安を煽ることも、国家の安定を揺るがす脅威となりうる。

本提言書においては、これら全てを「有事」であると定義し、以降の章にて有事に対する提言を述べる。

【図表 1.4-1】本提言における有事の定義



1.5 まとめ

日本を取り巻く安全保障環境は、経済的、地政学的な側面から急速に変化しており、重要性と複雑性が増している。特に東アジア地域は、中国の台頭と軍事力の増強、アメリカの安全保障政策の変動、そして ASEAN 諸国の成長といった要因が重なり合い、地域全体で大きく変動している。

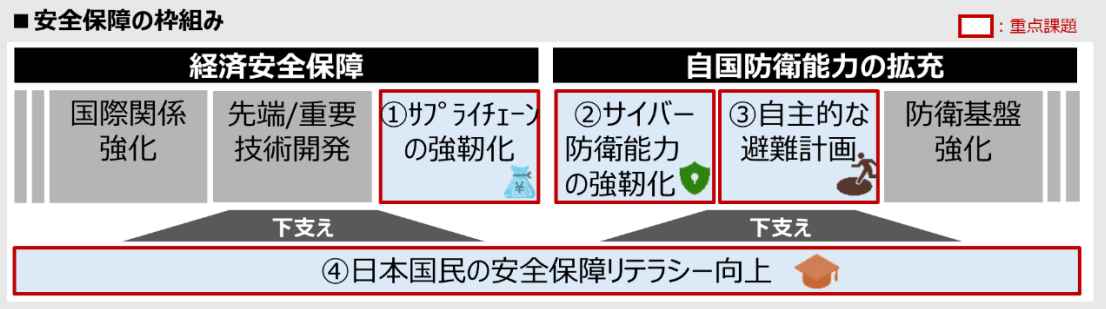
中国の積極的な領有権主張や南シナ海、台湾海峡での軍事行動は、東アジアの軍事的緊張を高めており、日本を含む周辺諸国にとって大きな脅威となっている。加えて、アメリカの「アメリカ第一主義」と東アジアに対する安全保障政策の揺らぎは、日本をはじめとする同盟諸国の安全保障を一層不安定にさせている。

これらの変化は、グローバルなパワーバランスに深い影響を与えると同時に、日本の安全

保障に大いなる影響を与えており、日本国民は「既に有事に巻き込まれている」といっても過言ではない状態にある。

戦後最も複雑で厳しい安全保障環境において何が必要なのだろうか？という問いを立て議論を重ねた結果、安全保障グループでは「日本および我々による自主自律的な安全保障対策が必要」との結論に達した。今まさに戦後から続く安全保障政策の大きな転換点に立っており、危機が差し迫った現状においては国家による安全保障だけに頼るのではなく、我々は自らの安全を守るために立ち上がる必要があると感じている。より具体的な安全保障対策に落とし込むための議論を行い、様々な角度から対策の方向性を探り検証した。その中で、今回我々の提言においては以下の 4 点を重要課題と設定し、企業人の立場から実行性を重視した提言を行う。

【図表 1.5-1】取り組むべき安全保障対策と、重点 4 課題



次章より、各課題について背景と現状課題、提言内容について詳細に述べる。

第２章 サプライチェーンの維持と強靭化

サプライチェーンとは、製品やサービスが最終消費者に届くまでの一連の流れのことをいう。この流れには、原材料の調達から生産、流通、販売、廃棄やリサイクルまでのすべてのプロセスが含まれるが、単に製品やサービスを届ける仕組みというだけでなく、経済、社会、そして安全保障に直結する重要なシステムでもある。

安全保障におけるサプライチェーンの重要性は、国家や社会の安定を維持するために不可欠な資源、製品、サービスの供給を確保する役割にある。グローバル化が進む中で、サプライチェーンの信頼性は、国家の安全保障に直接的な影響を及ぼす。

また、そのサプライチェーンの維持と強靭化にむけ有効な施策を立案し実行することが、今後の日本の持続可能な成長を実現するものと考える。

本章では、安全保障におけるサプライチェーンの重要性の認識と、我々経済界が、国、企業など様々なステークホルダと共に連携しながら実現をめざす、サプライチェーンの強靭化に向けた具体的施策について述べる。

2.1 背景

2.1.1 グローバル化とサプライチェーンの複雑化

近年のグローバル化は、これまでの単なる世界の一体化からさらに進化し、技術の進化、地政学的な分断、環境意識の高まりといった新しい要素を伴い、多様化・複雑化してきた。例えば、原材料を南米から調達し、アジアで加工し、北米や欧州で販売するといった、各国が比較優位に基づいて生産活動を行うことで、効率的なサプライチェーンが構築された。またそれに伴い、企業は人件費の安い地域に生産拠点を移すことでコスト削減を追求し、さらに、国際輸送網（海運、空輸）が整備され、迅速で安価な物資輸送が可能となった。

一方、このように各国や企業が効率性や経済的メリットを追求した結果、世界のサプライチェーンは長大化し、また、一部の国同士の依存関係が増加したことで、外部リスク（自然災害、パンデミック、地政学的緊張など）の影響が大きくなった。

複雑化した現代のサプライチェーンは、効率性と安全保障の両立を求める新たな段階に入っていると言える。

2.1.2 安全保障におけるサプライチェーンの役割

現代社会において、安全保障におけるサプライチェーンは、国家や企業が直面するリスクを軽減し、社会的・経済的安定を維持するうえで極めて重要である。

サプライチェーンはエネルギー、通信、食料、水道、医療など、国家の重要インフラを支える基本的な仕組みであり、このインフラが途絶すると社会が混乱し、国家安全保障に深刻な影響を及ぼす。また、兵器、装備、通信技術など、国防に必要な物資や技術の安定供給を確保するためにも、信頼できるサプライチェーンが必要となる。しかし、前述のとおり近年は自然災害やパンデミック、地政学リスク（紛争や制裁など）、サイバー攻撃などの影響により、サプライチェーンが脅かされた事案が多発している。もはや、安全保障分野におけるサプライチェーンは、単なる物流だけではなく、経済、技術、外交を含む包括的な役割を担っている。

2.1.3 直近の地政学リスク（ウクライナ侵攻）の影響

ロシアによるウクライナ侵攻は、全世界のサプライチェーンに多大な影響を及ぼした。この紛争により引き起こされた影響は以下のとおりである。

【図 2.1.3-1】ロシアのウクライナ侵攻よる影響

	分野・地域	影響
世界的影響	エネルギー供給	ロシアは世界最大のエネルギー供給国の一つであることから、侵攻後、各国からの制裁や輸出制限によりエネルギー価格が急騰した。また、石炭などの代替需要が増加し、アジアや他地域でエネルギー市場が混乱した。
	食料供給	ウクライナとロシアは世界の穀物供給において主要な役割を担っており、小麦、大麦、ひまわり油の輸出大国である。侵攻によりこれらの供給が途絶え、特に中東やアフリカ諸国で深刻な食料危機が発生した。
特定分野への影響	金属・鉱物資源	ロシアとウクライナは、アルミニウム、ニッケル、パラジウム、チタン、ネオンガス（半導体製造に不可欠）などの供給源である。侵攻とロシアに対する各国の制裁により、これらの材料の供給が不安定化した。
	医療・医薬品・医療機器	医療従事者が戦闘に巻き込まれたこと医療環境が逼迫しただけでなく、物流の混乱や戦闘の影響で、戦闘地域への医療物資の供給や国際的な人道支援スピードが遅延した。また、ロシアとウクライナは医療機器の製造に必要な希少金属（例：チタン、ニッケル、ネオンガス）の主要な生産地であり、これらの供給が滞ったことで、医療機器の製造と供給に影響が出た。
地域ごとの影響	ヨーロッパ	エネルギー危機により、冬季の暖房問題や電力価格の上昇が発生した。また、ロシアからの供給停止により、再生可能エネルギーや液化天然ガス導入が急加速した。
	アフリカ・中東	ウクライナ産小麦への依存が高い国々で深刻な食糧不足となった。また、政情不安が増幅し、社会不安の引き金となるケースもあった。
	アジア	日本や韓国など、多くの国がエネルギー価格の高騰に苦しんだことで、サプライチェーンの多様化やロシア依存の低減を模索した。

このように、ロシアによるウクライナ侵攻は、エネルギー、半導体、医療、食料を中心に幅広い範囲でサプライチェーンに大きな影響を及ぼした。安全保障におけるサプライチェーンは、国家や社会の基盤を支える重要な役割を担っており、特に現代のグローバル化された経済では、サプライチェーンの脆弱性が多くの分野に影響を与えるため、強靭性を高めるための政策や技術的アプローチが求められている。

2.2 サプライチェーンの重要性

2.2.1 経済的影響

サプライチェーンは、製品やサービスの流れを支える基盤として機能することで、需要・供給のバランス、企業成長、雇用創出、価格変動などのリスク管理、技術改革など、様々な経済的影響を及ぼしている。

【図 2.2.1-1】サプライチェーンが及ぼす経済的影響

#	経済的影響	詳細
1	需要と供給をつなぎ市場を機能させる	生産者と消費者を結び付け、適切に管理することで、経済の安定に不可欠な需要と供給のバランスをとり、市場の均衡を維持する。
2	企業の生産性と競争力を向上させる	サプライチェーンを最適化・強化することで、在庫管理の効率化、物流の最適化、調達コスト削減と、より迅速で低コストな商品提供が可能になり、企業競争力が高まる。
3	雇用を創出し、経済成長を促進する	多くの業界・職種に関わり雇用を生み出す。また、製造業や流通業が活発になることで、消費が促進されGDPの成長につながる。特に、グローバルサプライチェーンの発展により、各国の経済が相互に依存し、世界経済全体の発展に繋がる。
4	リスクを管理し、経済の安定性を支える	分散化・多様化されたサプライチェーンであれば、特定の国や地域での災害・政治問題などが発生しても、他のルートから供給を確保できる。また、商品の安定供給を可能にすることで、急激な価格変動を防ぎ、インフレやデフレのリスクを軽減できる。
5	技術革新を促進し、持続可能な成長を実現する	サプライチェーン管理にはAI、IoT、ブロックチェーンなどの先端技術が活用されており、経済全体の効率化につながっている。また、持続可能なサプライチェーン（Green Supply Chain）により、CO_2排出削減やエシカルな消費の促進が可能になる。

2.2.2 国家安全保障との関連性

サプライチェーンは経済活動だけでなく、国家安全保障とも密接に関係している。特に、軍事・インフラ関連やハイテク技術を含む重要物資（半導体、エネルギー、レアアースなど）のサプライチェーンの重要性は高いことから、慎重な管理が求められる。

自然災害やパンデミック、地政学的リスク、サイバー攻撃などの影響でサプライチェーンが途絶えると、軍事能力や経済活動が大きなダメージを受けるため、各国はサプライチェーンの強靭化を急いでいる。

(1) 日本における軍需物資のサプライチェーン強靭化

軍需物資は、武器・弾薬に留まらず、燃料・電子部品・航空機・軍服など、戦争や国防に不可欠な物資を含む。例えば、戦闘機やミサイル制御用 IC など数多くの軍需物資に使われている半導体は、台湾有事が勃発した場合、TSMC に被害が及ぶことで供給網の混乱が予想されるため、TSMC は熊本に工場を設置し、半導体供給を安定化させようとしている。

(2) 日本におけるインフラ関連のサプライチェーン強靭化

電力・通信・輸送などの基幹インフラは、戦時や有事の際にも継続的に運用する必要があり、各国はその安定供給を確保するためにサプライチェーンの強靭化を図っている。例えば、地政学リスクの顕在化により、海運が途絶することで天然ガス（LNG 等）の供給確保が困難になる可能性があることから、オーストラリア・アメリカ・マレーシアからの調達を強化している。

日本だけでなく、各国も安全保障上のリスクを顕在化させず、安定供給を実現するため、リショアリング（国内生産）、フレンドショアリング（友好国との連携）、サプライチェーンの分散化といった施策を講じ、国家の安定と成長を確保しようとしている。今後、地政学リスクや技術革新の進展に応じて、各国のサプライチェーン戦略も変化していくため、日本も柔軟な対応が求められる。

2.2.3 社会的安全性の確保

サプライチェーンは社会的安全性を保つためにも重要な役割を担っており、ひとたび機能しなくなると、人々の心理面・社会面のネガティブな反応を発端とした行動により、市場混乱・治安悪化へとつながる。そして最終的には国家の安全保障まで脅かされる。

【図表 2.2.3-1】社会不安の直接的な原因と影響

#	社会不安の直接的な要因	影響
1	生活必需品（水、食料、医療品など）の不足	市場価格の高騰やパニック買いが発生し、暴動、略奪の原因となる。また、衛生環境の悪化、感染症のリスクが高まりや、慢性疾患を持つ人々にとっては命にかかわる問題となる。
2	エネルギー（電力、燃料など）の遮断	通信・交通・医療機関の機能が停止し、経済活動や生活が混乱するだけでなく、物流や輸送手段が機能しなくなり、物資の配送が滞る。さらには、失業者が増え、インフレが進行し、経済活動そのもの混乱が生じる。

【図表 2.2.3-2】社会不安のメカニズム

#	段階	影響
1	初期段階	企業やメディア、SNSを通じて供給途絶が徐々に認識され、人々は不安を感じ、「このままだと生活が困るのではないか」という心理的ストレスが増大する。
2	拡散段階	人々は物資の買い占めに走り、市場から商品が消える。また、SNSやメディアを通じて誤情報が広がると、パニックが増幅し社会不安が拡大する。更に、あらゆる物資の価格高騰による経済的混乱が発生する。
3	臨界段階	必需品を手に入れるために暴動や略奪や、政府への抗議やデモ活動が激化し、警察や軍・自衛隊などが介入することで鎮静化を図るなどの混乱が発生する。

これらの事象は、新型コロナウイルス（COVID-19）のパンデミックの際などにも、実際に発生した。今後、同様の事態が発生した際には、この社会不安の連鎖を断ち切るために、サプライチェーンの強靭化を図り、事前の備蓄、情報管理、社会的レジリエンスの向上が不可欠である。

2.3 サプライチェーンの脅威と課題

2.3.1 自然災害・パンデミック

自然災害やパンデミックの影響で、生産拠点や物流網が停止し、原材料や部品、製品の供給がストップすると、企業の生産活動が停止し、市場に商品が不足する事態が発生する。

2011 年の東日本大震災の際は、複数の自動車メーカーの工場が被災し、世界的な部品供給不足が発生したり、港湾や鉄道が寸断され国内外への輸送が停止するなどした。また、2020 年にアメリカ・カリフォルニアで発生した山火事により電力供給が停止し、シリコン

バレー周辺の工場の稼働が制限され、一部操業停止にまで至り、製品の配送が滞った。

新型コロナウイルス（COVID-19）のパンデミックは、全世界のサプライチェーンに壊滅的な影響を与えた。世界的な自動車部品の生産拠点である中国・武漢の工場がロックダウンにより部品供給が停止した結果、自動車メーカー（ホンダ・日産・フォルクスワーゲンなど）が操業停止となった。また、人員不足や検疫強化によって、海運、陸上輸送、航空貨物にも大きな混乱を招き、世界中の物流・輸送網の機能を大幅に低下させた。

2.3.2 地政学リスク

地政学リスクには、各国が自国の利益を追求することで発生する貿易摩擦、国際法を無視した軍事活動などに対する制裁、台湾有事などの領土問題解決のための軍事的緊張などが挙げられる。

(1) 貿易摩擦のリスクと事例

貿易は単なる経済活動ではなく、外交政策の重要な手段の一つでもある。貿易関係を通じて国際協力を強化することができる一方で、制裁措置や関税政策により政治的な影響を及ぼす手段としても利用される。そのため、貿易は経済と外交の両面で国家戦略の要となる。

2025 年 2 月、アメリカは第二次トランプ政権が生まれて間もなく、中国からのほぼ全ての輸入品に対して 10%の追加課税を課し、カナダおよびメキシコからの輸入品に対しても 25%の関税を課す方針を示した。それに対し中国もアメリカからの石炭や液化天然ガスなどの輸入品に対し最大 15%の追加関税を課し、報復することを発表した。

トランプ政権による関税措置は、アメリカの貿易赤字削減や国内産業の保護を目的としているが、世界的なサプライチェーンや各国経済に多大な影響を及ぼす可能性がある。

(2) 制裁のリスクと事例

制裁は、特定の国や企業、個人に対する政治的・経済的な圧力を目的として、様々な状況において発動される。

ロシアによるウクライナ侵攻においては、アメリカ、EU、日本などが、ロシアへの経済制裁として、国際金融ネットワーク（SWIFT）からの排除、ロシアからのエネルギーの輸入制限などを発動した。その結果、ロシア向け貿易が大幅に縮小し、エネルギー価格が高騰し、市場が混乱した。

2018 年にはイランが核合意（JCPOA）から離脱し、経済制裁を強化した結果、イランの石油輸出が大幅に減少し、エネルギー価格が変動した。

これら国際紛争や軍事侵攻による状況の他、北朝鮮の核・ミサイル開発加速の宣言のような安全保障上の脅威が強まった場合、新疆ウイグル自治区の事例のように特定の国や政府が人権侵害や弾圧を行った場合、知的財産権の侵害や産業スパイ行為を特

定の国や企業が行った場合など、様々な状況において制裁は発動され、それに伴いサプライチェーンに大きな影響を与える。

(3) 軍事的緊張のリスクと事例

軍事的緊張は、物流の混乱、原材料不足、価格上昇、技術輸出規制などを通じてサプライチェーンに大きな影響を与える。

ロシアのウクライナ侵攻後における、経済制裁によってロシア産のエネルギー・穀物の貿易停止などにより、各国への供給が途絶えたことは前述のとおりであるが、台湾有事が勃発した場合においても、サプライチェーンには大きな影響を与えることは必至である。

台湾の TSMC は世界の先端半導体生産の約 90%担っており、同社の生産が停止すると、各産業に大打撃が及ぶことは明白である。また台湾周辺の海域（台湾海峡）は世界の貿易の約 25%が通過する重要なシーレーンであり、中国軍による海上封鎖や戦闘が発生すると、貿易が停滞する。さらに、中国産のレアアース・リチウム・コバルトなどの資源が輸出制限される可能性がある。

2.3.3 サイバー攻撃のリスクと事例

サイバー攻撃による情報漏洩やシステム停止は、サプライチェーンの供給分野に深刻な影響を及ぼす。ハッキングやランサムウェア等によるサイバー攻撃で、システム障害が発生したことを発端に、自動車会社などの製造ラインが停止するなど、サプライチェーンに大きな影響を及ぼす事案が多数発生している。詳細は第 3 章「サイバー防衛能力の強靭化」にて記載する。

2.3.4 特定国や企業への過度な依存の問題

特定の国や企業への過度な依存は、これまで述べてきたリスクの顕在化によって、サプライチェーンが途絶された場合、経済、企業、消費者に多大な影響を及ぼす。

(1) 特定国への過度な依存のリスク

特定の国に原材料や製造工程を依存している場合、貿易制裁・関税・紛争・政治対立などの影響を大きく受ける。まず原材料において、ヨーロッパはロシアの天然ガスに依存していたため、ロシアのウクライナ侵攻時に貿易制裁が発動された際には、供給停止でエネルギー危機が発生した。また、世界のレアアースの約 60%は中国産でありほぼ独占状態にある。2010 年には中国がレアアース輸出を制限し、世界的に価格が高騰するという事態も発生した。

次に、製造工程において中国は 2021 年時点、世界全体の製造業付加価値の約 30%を占めている。これは、2012 年の 22.5%から大幅な増加を示しており、中国が世界最大

の製造業大国としての地位を維持・強化していることを示している。今後、中国において様々なリスクが顕在化することで、世界中のサプライチェーンに多大な影響を及ぼすことは明白である。

(2) 特定企業への過度な依存のリスク

特定の企業が市場を独占している場合、その企業のトラブルが直接サプライチェーンに影響する。Apple や NVIDIA などのハイテク企業は、半導体製造を TSMC に依存しており、もし、TSMC が台湾有事により攻撃・被害に遭えば、世界の IT 製品が生産不能になる。

また、世界中の多くの企業が Amazon Web Services（AWS）を活用している。AWS がダウンすると、企業のシステムや EC サイトなどが停止するなどの事例が過去に数回発生している。

このように、近年、自然災害・パンデミック、地政学的対立やサイバー攻撃などによるサプライチェーンの脅威は多様化・複雑化しており、実際にそれらのリスクが顕在化した事案が多数発生している。また、特定の国・企業への過度な依存は、サプライチェーンの脆弱性を高めることにつながる。

これらを踏まえ、国や企業は、サプライチェーンの強靭化に向け、リスク分散と柔軟な対応力を持つことが求められている。

2.4 サプライチェーンの強靭化に向けた施策

2.4.1 多様化（リスク分散）

サプライチェーンの多様化とは、調達・生産・物流の拠点を複数の国・地域・企業に分散することで、一つの供給元への依存を減らし、自然災害・パンデミック・地政学リスク・サイバー攻撃などのリスクを最小限に抑えることである。以下は、各企業が実際に行っている施策である。

(1) 供給元の多様化（マルチソーシング戦略）

単独のサプライヤーではなく、複数の企業から調達したり、特定の国ではなく地域ごとに調達先を分散させることにより、複数の供給元を確保することをマルチソーシング戦略という。トヨタの半導体不足対策として 3～6 ヶ月分の部品在庫を確保する戦略や、Apple が iPhone 製造拠点を中国からインドやベトナムに分散するなどの施策がこれにあたる。

(2) 生産拠点の分散（チャイナ・プラスワン戦略）

世界の工場と呼ばれる中国だけに生産活動を依存せず、他の国にも生産拠点を広げることをチャイナ・プラスワン戦略という。東南アジア諸国や中南米、インドなどに

生産拠点を移行、拡大する企業が増えており、ホンダやパナソニックなどがベトナムに進出している。

(3) 近隣国・自国での生産

地理的に近い国での生産（ニアショアリング）や自国内での生産（リショアリング）で、リスクを低減する戦略である。日本は国内での半導体・電池生産を強化しており、TSMC の熊本工場の設置はその一環である。また、アメリカにおいては、CHIPS 法（CHIPS for America Act）により国内半導体産業への投資拡大を支援する枠組みもある。

2.4.2 代替供給源の確保

代替供給源の確保に関しては、各国や企業は様々な取り組みをしている。ここでは、日本政府が経済的威圧に屈しない経済システム構築の一環として、資源開発や産業関連インフラの整備を通じて代替供給源の確保を推進している内容を示す。

(1) 重要物資の安定供給確保

石油・天然ガス、銅、レアメタルなどの重要鉱物資源の安定供給を確保するため、同志国との協調を含めた資源外交を進め、海外での上流開発を推進している。また、液化天然ガス（LNG）の安定供給を確保するため、政府は企業が長期契約を締結しやすくする支援策を検討している。具体的には、国内外での貯蔵タンクの確保や、需要が予想を下回った場合の余剰分を市場で転売できる枠組みの構築などが含まれる。

(2) 産業関連インフラの整備

サプライチェーンの途絶リスクを踏まえ、従来の輸送手段・ルートを代替・補完するための調査や実証を通じ、国際物流の多元化・強靭化に取り組んでいる。また、重要物資の安定供給や企業の競争力向上に資するサプライチェーンの強靭化および関連インフラの整備に対して、公的金融機関を通じた支援を行っている。

(3) 国際的な連携と協力

透明で強靭かつ持続可能なサプライチェーン構築に向けて、同志国との政策協調を強化し、グローバルサウス等との連携の輪を広げている。また、官民の戦略的対話を通じて、研究開発、産業人材、産業インフラ、ファイナンス、データセキュリティ、サイバーセキュリティなどの分野で国際的な枠組みを構築している。

2.4.3 戦略的備蓄（必需品や戦略物資の国内備蓄）

2023 年度の農林水産省の発表によると、日本の食料自給率は 38%であり、備蓄状況は 4～5 カ月分、小麦は 2～3 カ月分である。また、資源エネルギー庁によると、エネルギー自給率は 12.6%で、備蓄状況は石油が約 8 カ月分、石炭が約 1 カ月分、天然ガス（LNG など）

が約 3 週間分である。

農林水産省は、食料の国内農業生産の増大、安定的な輸入の確保、そして備蓄の適切な運用を基本方針として掲げている。国内農業生産額は 2000 年の 113.2 兆円から 2022 年には 114.2 兆円と増加している一方、安定的な輸入の確保、備蓄の適切な運用については、進捗状況が公開されていない。

総じて、農林水産省は食料安全保障の強化に向けた取り組みを進めているが、課題も存在し、引き続き施策の効果的な実施と検証が求められている。

資源エネルギー庁は、石油危機以降、国家備蓄と民間備蓄を組み合わせた石油備蓄制度を構築し、安定供給の確保に努めている。その結果、石油備蓄の増強などを実施して成果を上げたとされている。一方、天然ガス（LNG など）は需要が増加しているにも関わらず、具体的な施策や進捗状況についての詳細な情報は公開されていない。また、新たな取り組みとして、エネルギー自給率の向上と化石燃料依存度の低減をめざし、再生可能エネルギーの導入が推進されている。政府は、2040 年度までに再生可能エネルギーの電源構成比率を 40～50%に引き上げる目標を掲げている。

これらの施策を通じて、日本は食料やエネルギーの安定供給と安全保障の強化を図っている。しかし、それらの施策は万全とは言えず、もし今、日本が有事に巻き込まれた場合、必需品や戦略物資の国内備蓄だけによる安定供給の保証はない。昨今の国際情勢が目まぐるしく変化する状況下において、日本は柔軟かつ迅速な対応が求められている。

2.5 サプライチェーン強靭化に向けた提言

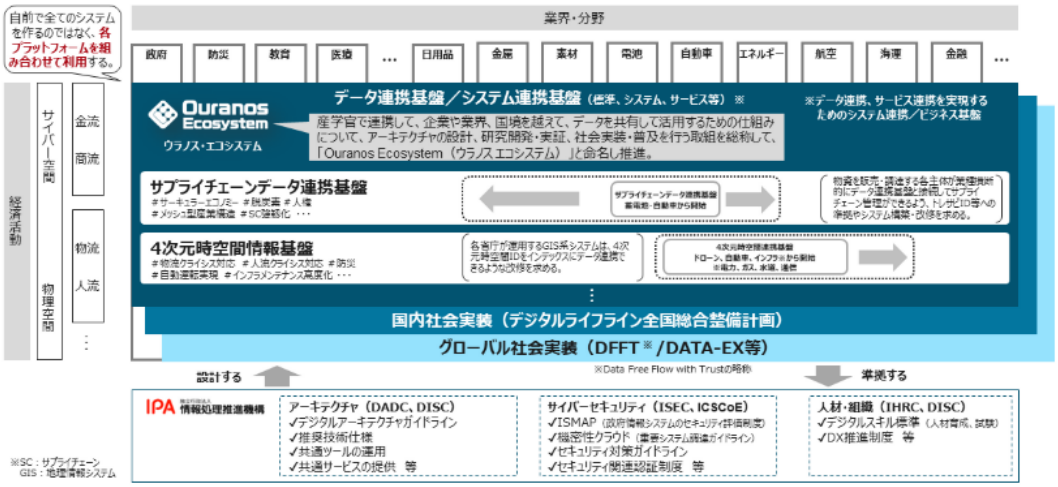
2.5.1 テクノロジー活用(他業種間データ連携プラットフォームによる監視と最適化

これまで述べてきたように、グローバル化が進む中で、サプライチェーンは複数の国や企業、業種を跨いで構築されており、これを適切に監視・最適化することはリスクを早期に検知し迅速な対応をすることと、国家および企業の競争力を維持するために不可欠である。

我々は以下のとおり、政府や企業などが連携し、テクノロジーを活用したデータ連携によるサプライチェーンの監視と最適化の有効な施策として、「ウラノス・エコシステム」を有事対応に活用することを提言する。

ウラノス・エコシステムは、経済産業省が人手不足や災害激甚化、脱炭素への対応といった社会課題を解決しながら、イノベーションを起こして経済成長を実現するため、企業や業界、国境を跨ぐ横断的なデータ共有やシステム連携の仕組みとして構築した。

【図表 2.5.1-1】ウラノス・エコシステムの概要



出典：経済産業省 Ouranos Ecosystem（ウラノス・エコシステム）

経済産業省とともに共同構築に参画している、独立行政法人情報処理推進機構（IPA）は、ウラノス・エコシステムについて、以下のとおり説明している。

・様々なシステムを連携し、すべての利用者が共通のデータを利用できるようにすることで、低コストで効率的な業務を実現する。
・各企業が自社のデータ主権を守りながら、他社とのデータの共有や活用によって、国際的な法規制やルールへの対応など、経営上のリスクを回避するための仕組みとして寄与する。

ウラノス・エコシステムは、有事対応を前提に構築されたものではない。しかし、システムの構想や利用目的自体が、有事対応へと十分に活かすことが出来ると我々は想定している。有事対応としてのサプライチェーンの監視と最適化にむけ、有効となる様々な機能と、我々がイメージするその活用例は下表のとおりである。

【図表 2.5.1-2】ウラノス・エコシステムの機能一覧と活用例

機能名	機能概要	活用例
分散管理台帳技術（DLT）	取引データを改ざん不可能な形で記録し、供給網の透明性を確保。	- 食品の生産・流通履歴を記録し、品質管理や偽装防止を実現。 - 半導体の供給経路を可視化し、不正流通を防ぐ。
スマートコントラクト	条件を満たした際に自動実行されるプログラムで契約や取引を効率化。	- 医薬品供給契約を自動化し、緊急時の優先供給を確保 - エネルギー取引を自動化し、需要に応じた最適配分を実現。
AIによるリスク分析	需給予測や供給網の脆弱性を分析し、最適なシナリオを提示。	- IoTリアルタイム監視食料供給リスクを分析し、事前に備蓄を最適化。 - 半導体供給のリスクシミュレーションを行い、バックアップルートを確保。
IoTリアルタイム監視	センサーやGPSを活用し、物流や生産環境をリアルタイム監視。	- 冷蔵医薬品の輸送時、温度異常を即座に検知・通知 - エネルギー供給網の状況をリアルタイムで監視し、障害発生時に即対応。
トレーサビリティ管理	サプライチェーン全体の追跡・監査を強化し、透明性を確保。	- 医薬品の原材料から最終製品までの流通経路を記録 - 食品の生産地情報を消費者に提供し、安全性を証明。
デジタルID認証	取引相手の信頼性を保証し、不正アクセスやサイバー攻撃を防止。	- 需給予測システム医療機関間のデータ共有をセキュアに実現 - 半導体供給網の関係者認証を厳格化し、不正取引を防止。
需給予測システム	AIを活用して供給と需要のバランスをリアルタイム分析し、最適化。	- 有事の際の食料・医薬品の需要をシミュレーションし、適正配分を実施。 - エネルギー供給網で再生可能エネルギーの利用最適化を支援。
緊急時バックアップ計画	災害・戦争・パンデミックなどのシナリオを想定し、供給網を維持する計画を作成。	- 主要生産国の供給停止時に代替ルートを即座に発動 - 天候不順時の食料不足を想定し、事前に代替供給網を確保。
自動在庫管理	スマートコントラクトとIoTを組み合わせ、備蓄品の数量・使用期限を自動管理。	- 半導体部品の在庫が一定量を下回ると自動発注 - 医療品の備蓄期限を管理し、期限切れ前に使用・補充。
グローバル供給網連携	各国の企業・政府機関とデータを連携し、有事に迅速対応。	- 国際的な半導体供給網と連携し、生産・流通状況をリアルタイム共有 - 医薬品供給網のデータを各国と共有し、パンデミック時に即時供給。

有事対応のためのプラットフォームには、迅速な意思決定を支援するための「データの一元化とリアルタイム監視」、サイバー攻撃やインフラ障害が発生しても耐えられる「分散型システム」、供給元の信頼性確保のための「トレーサビリティと追跡機能」、高度な分析が可能となる「AI とデータ分析」が必須要件である。

ウラノス・エコシステムは、それらを具備していることから、我々が考える有事におけるサプライチェーン監視と最適化のためのプラットフォームとして活用することは有効であると考える。

2.5.2 国際連携（ウラノス・エコシステムの活用範囲拡大）

ウラノス・エコシステムを有事対応におけるサプライチェーンの監視と最適化のために有効活用するうえで、国内産業間の連携だけではなく、各国と連携した活用は極めて重要であると考える。以下にその活用例を示す。

- 分散型台帳と AI を活用し、各国の生産・流通状況をリアルタイムで監視・分析し、リスクの高い供給元を特定のうえ、バックアップ供給網を同盟国間で構築する。
- 有事発生時、供給ネットワークの切り替えには時間がかかり、必要な物資が確保できない場合、スマートコントラクトで「有事プロトコル」を設定し、特定の条件が発生すると、自動的に代替供給ルートが作動させる。また、IoT と AI を組み合わせたリアルタイム物流管理により、同盟国間で緊急物資を即時配分が可能となる。
- 防衛産業において、アメリカ、日本、EU の安全な兵站管理ネットワークを構築するため、トレーサビリティ管理とデジタル ID 認証により、信頼できる供給網を確立する。

その他、日本・アメリカ・EU 間で、最先端技術の共同管理体制を構築するうえで、サプライチェーンに関わる重要技術を分散型管理台帳で保護し、敵対国への技術流出を防ぐなどの経済安全保障の観点でも活用できると想定される。

また、ウラノス・エコシステムを利用し、各国間とシームレスに連携する上では、統一された国際基準・規格に則った枠組みが必要である。この点においても、各国との協議を進め、本構想の実現性を高めていく必要がある。

2.6 結論・まとめ

2.6.1 安全保障上の要点の再確認

サプライチェーンは経済的影響だけでなく、安全保障とも密接に関わっており、その強靭化は、国家や企業の競争力、リスク管理、持続可能性など、あらゆる側面に影響を与えるため、極めて重要な施策である。

以下のとおり、サプライチェーンの強靭化の重要性を改めて整理する。

・必需品、軍需物資やインフラ関連の重要物資の供給確保
・社会的安全性の確保
・自然災害やパンデミック、地政学的リスク、サイバー攻撃、経済的要因などのリスクに対するレジリエンス向上

2.6.2 提言内容の要約

サプライチェーンの強靭化を推進するには、リスクの分散・デジタル化・セキュリティ対策・政府支援・国際協調など様々な要素と具体的なアクションが求められる。その中でも我々は、テクノロジーを活用した新たな施策を有効策として提言する。

【図表 2.6.2-1】提言内容

#	提言内容	詳細
1	ウラノス・エコシステムの有事向け活用	経済産業省が、企業や業界、国境を跨ぐ横断的なデータ共有やシステム連携の仕組みとして構築。各産業を跨いだサプライチェーンの維持や強靭化に役立つことが想定されるが、これを有事向けにも活用する。
2	ウラノス・エコシステムの有事向け活用のための国際連携	有事におけるサプライチェーン維持や強靭化に向け、主に同盟国、同志国との連携を強化することと、シームレスなデータ連携を実現するため、適用する国際基準・規格を決定する。

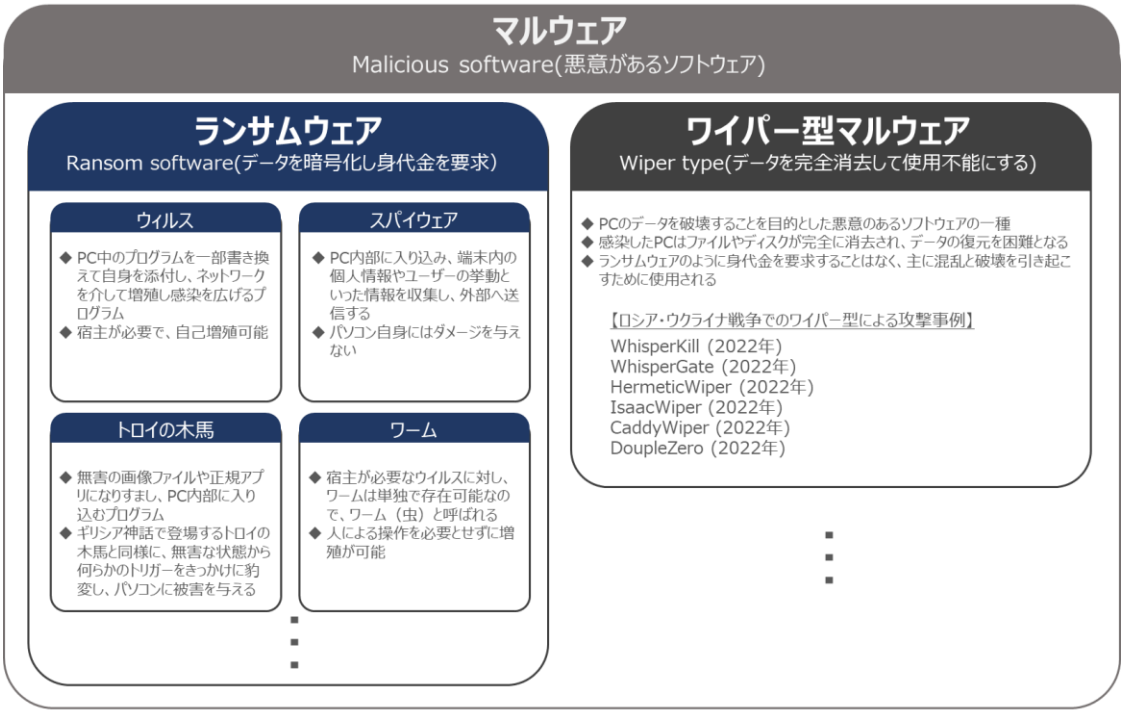
本提言内容については、経済産業省の担当者と会話をしており、充分に実現性はあるとの感触を得ている。今後、具体的な議論を重ね、我々の提言の有効性を訴求しつつ、経済界として日本の安全保障に貢献できることを模索していく。

第３章 サイバー防衛能力の強靭化

近年、サイバー攻撃の脅威は増大しており、武力攻撃の前からフェイクニュースの拡散などを通じた情報戦が展開されるといった、目的遂行のために軍事的な手段と非軍事的な手段を組み合わせるハイブリッド戦が、今後さらに洗練された形で実施される可能性が高い。SNS でのインフルエンサーなどを媒体としたフェイクニュースの流布による攻撃対象の政府の信頼低下・社会の分断を企図した情報戦への懸念が高まっており、ランサムウェアのようなサイバー攻撃も増加している。

本章では、ロシア・ウクライナ戦争や台湾におけるサイバー攻撃の事例を踏まえ、日本の現状と課題を分析し、国、企業、個人が協力してサイバー防衛能力を強靭化するため国、企業、個人が果たすべき役割と対応策について述べる。

【図表 3-1】マルウェアの定義と主な区分



3.1 背景

3.1.1 電磁波・宇宙・サイバー領域の重要性

現代の戦争では、陸海空の伝統的な三領域に加え、電磁波・宇宙・サイバーといった新たな領域の重要性が増している。電磁波領域においては通信や GPS 信号を妨害するためのジャミング[1]やレーダーの無力化、宇宙領域においては衛星を利用した情報収集や偵察、サイ

1 ジャミング（jamming）は、レーダー波に対する妨害のことで電波妨害装置によって行われる。

バー領域においては重要インフラへの攻撃に加え、SNS を利用した情報操作やフェイクニュースの拡散による社会の分断が懸念される。

これらの新領域は、軍事作戦の遂行において不可欠な要素となり、これらの領域での優位性が戦局に大きな影響を与える。新興技術の発展により、これらの領域を重視した防衛戦略が求められている。

電磁波領域においては、行動の自由を確保することが戦略的に求められており、2020 年の米国防省の「電磁スペクトラム優勢戦略[2]」は、電磁波による通信やデータ伝送を確保することが新たな戦闘環境における優位性をもたらすとしている。

宇宙領域においては、2007 年に中国、2021 年にロシアが、それぞれ自国の人工衛星に対する破壊実験を実施し、スペースデブリ[3]が多数発生したことで他国の人工衛星に対する衝突リスクが高まることが懸念されている。

また、サイバー領域においては、悪意ある国家や組織によるエネルギー・水道・情報通信・交通・医療といった重要インフラへの攻撃が増加しており、戦時下はもとより平時における経済・情報の混乱をきたすことが懸念されている。

3.1.2 現代の安全保障における脅威の多様化と技術進化の影響

ロシア・ウクライナ戦争は、新領域の戦争が現代の安全保障において重要であることを示す具体的事例となった。

(1) 電磁波領域の挑戦

電磁波領域では、2022 年以降のウクライナ紛争においてロシアはウクライナの通信システムを破壊するため、ジャミング技術を利用し、情報通信の混乱を引き起こした。ウクライナは西側諸国から提供された先進的な電子戦システムを駆使し、一定の成功を収めているものの、依然としてロシアの電子戦能力に対抗するには課題が残る状況にある。

(2) 宇宙領域における戦略的役割

宇宙領域では、ロシアの空爆やサイバー攻撃により、ウクライナの通信インフラは大きな打撃を受け、ウクライナ市民や政府機関は情報の発信や受信が困難となり混乱が生じた。このような危機的な状況が生じた一方で、スペース X 社のスターリンクは、地球低軌道に配置された数百の衛星を利用しインターネット接続を提供したことで、ウクライナの市民や軍はリアルタイムでの情報共有を継続でき、ロシアの侵攻に対抗するための重要な情報源となった。

2 電磁波領域における優位を確保し、あらゆる作戦を成功させるための戦略。
3 宇宙空間に漂っている人工衛星やロケットの残骸、それらから発生した破片。

(3) サイバー領域

ウクライナは侵攻以前からロシアによる継続的なサイバー攻撃に直面していた。侵攻前の 2022 年 1 月 14 日にはウクライナ政府機関の約 70 の公式ウェブサイトが一斉に乗っ取られた。この攻撃には、強力なワイパー型マルウェアが使用されウクライナにおける重要なデータの破壊が行われたことが Microsoft 社の報告により明らかとなっている。

一方でウクライナは 2014 年のクリミア併合以降、ロシアからのサイバー攻撃の脅威に晒されてきたことから、今般の侵攻に先んじてアメリカや EU 諸国との連携を強化し、サイバー攻撃に関する情報共有を行っていた。これにより、ウクライナはサイバー攻撃の兆候やリスクを早期に察知し、攻撃の 1 週間前からデータをクラウドにアップロードするなど、データレジリエンスの向上によりロシアのサイバー攻撃による影響を低減させることに成功した。

このように、新領域におけるリスクは、技術の進化と相まって、国家にとって新たな脅威となることに疑いの余地はない。一方で、技術の進化は、新たな国家防衛の手段となり得る可能性もあり、これらの領域におけるリスクを適切に評価し、効果的な対策を講じることが、持続可能な安全保障体制の構築に繋がるものと考えられる。

3.1.3 本章の目的

これまで述べてきたように現代の安全保障環境において、電磁波、宇宙、サイバーの各領域の重要性についての認識は高まっている。日本においても、電磁波領域では陸上自衛隊の電子作戦隊の新編や航空自衛隊のスタンドオフ電子戦機[4]の開発、宇宙領域では航空自衛隊宇宙作戦群の新編や部隊の拡充などが進められている。サイバー領域においても、自衛隊サイバー防衛隊の新設が行われていることに加え、経済安全保障推進法の制定などにより、企業や個人の役割が一層重要視されるようになった。

これら新領域の中でも特にサイバー攻撃は、国家を対象としたものから個人や企業を対象としたものまで多岐にわたり、重要な経済情報や機微情報の窃取、システムの破壊などが行われており、国家安全保障に加え経済活動に対する大きな脅威となっている。

電磁波や宇宙領域における安全保障に対する対策は、主に国家レベルの取り組みに依存することが多いが、サイバー領域においては企業や個人が主体的に関与できる環境が整っており、企業や個人が実践的な対策を講じることが安全保障に寄与するための有効な手段となるものと考えられる。このため、本章は企業や個人のサイバー領域における具体的な対策と役割を明確に提言することで、各企業・個人ひいては国家全体としての安全保障の強化に寄与することを目的とする。

4 強力な電波妨害によって敵のレーダー施設などを無力化し、自衛隊の航空作戦の遂行を支援する機体。

3.2 日本におけるサイバー領域の現状と課題

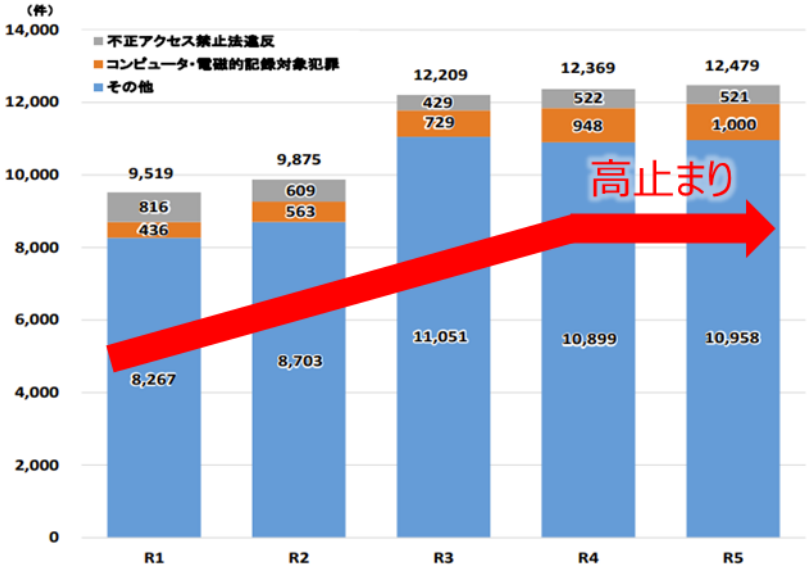
3.2.1 攻撃手法の多様化と高度化

日本においてもサイバー空間における脅威は年々増加しており、特にフィッシング詐欺やランサムウェア攻撃などが広がっている。2024 年版情報通信白書によると、サイバー攻撃関連の通信数は急増しており、サイバー攻撃関連の通信数が約 6,197 億パケットに達し、2015 年と比較して 9.8 倍に増加した。このような状況の中、警察庁は 2022 年にサイバー特別捜査隊を設置するなどの対策を講じているが、サイバー空間は急速に進化しており、サイバー犯罪の検挙状況は、2021 年以降、約 12,000 件/年と高止まりしている。警察による抑止や捜査だけでは完全な防御が難しく、企業や個人が自ら主体的に対策を講じることが不可欠であると言える。

【図表 3.2.1-1】サイバー攻撃関連の通信数の推移

出典：令和 6 年版情報通信白書（2024 年）

【図表 3.2.1-2】サイバー犯罪の検挙件数の推移

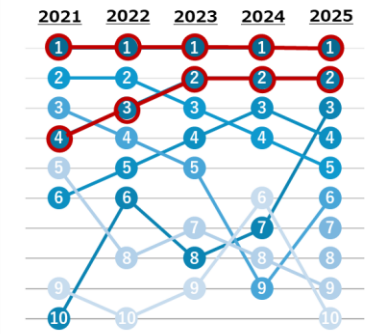


出典：令和 5 年におけるサイバー空間をめぐる脅威の情勢等について（2023 年）

3.2.2 主要な被害事例とその影響

また、日本国内に着目しても企業や組織がサイバー攻撃の受けており、特にランサムウェア攻撃やサプライチェーンの弱点を悪用した攻撃は、深刻な被害を被っている。下記例に挙げられるように医療やサプライチェーンといった事業において攻撃を受けた場合、国民の生活の基盤を揺るがすことになることから、その影響範囲は、単なる個別の企業に留まらず、社会全体の麻痺といった広範囲に及ぶことが懸念される。

【図表 3.2.2-1】情報セキュリティ 10 大脅威



順位	脅威
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	システムの脆弱性を突いた攻撃
4位	内部不正による情報漏えい等
5位	機密情報等を狙った標的型攻撃
6位	リモートワーク等の環境や仕組みを狙った攻撃
7位	地政学的リスクに起因するサイバー攻撃
8位	分散型サービス妨害攻撃（DDoS攻撃）
9位	ビジネスメール詐欺
10位	不注意による情報漏えい等

出典：IPA（情報処理推進機構）「情報セキュリティ 10 大脅威 2025」を基に作成

(1) 医療機関におけるランサムウェアによる被害事例

2022 年 10 月、大阪府内の医療機関 A がランサムウェアによる被害を受けた。この攻撃は、当該医療機関の給食事業委託先企業 B 社のサーバーを介して行われ、電子カルテシステムや診療データを含むサーバーに感染を拡げ、データを暗号化した。この結果、当該医療機関は医療情報にアクセスできなくなり、外来診療や各種検査の停止、緊急の医療を必要とする患者への対応に影響が発生した。本事例おける復旧に要した時間は約 2 ヶ月にも及び、その間の収益損失はもとより、地域医療の維持に深刻な影響を及ぼした。この事例では、B 社のサーバーの脆弱性や漏洩した ID・パスワードが攻撃の入り口となったが、この他、情報資産の棚卸しと把握の未実施といった組織的課題、セキュリティに関する知識を有した人材の不足といった人的課題、RDP 通信[5]の常時接続が許可されていたことや、管理者権限のパスワードが共通であったことなど技術的課題が明らかとなった。

5 RDP（Remote Desktop Protocol）通信。ユーザーは離れた場所からコンピューターを制御および操作できる。

(2) 自動車メーカーにおけるサプライチェーンの弱点を狙われた被害事例

2022 年 2 月、日本国内の自動車メーカーC 社のサプライチェーンの一部である D 社がサイバー攻撃を受けた。この攻撃により、C 社は必要な部品を確保できず、C 社の国内全 14 工場で 28 ラインが一時停止せざるを得ない事態が発生し、1.3 万台以上の生産に影響を及ぼす事態となった。本事例では、D 社の子会社が独自に特定外部企業との専用通信に利用していたリモート接続機器に脆弱性があったことが原因とされているが、根本的には、サプライチェーンの脆弱性に起因している。C 社は効率的な受注・発注・生産の観点から極めて高度な管理体制を構築していたが、同社のサプライチェーンは約 6 万社から構成されており、一部の企業のセキュリティが疎かであると、全体に波及するリスクを孕むことを示唆することとなった。

3.2.3 他国における事例と日本への影響

他国に目を向けるとサイバー攻撃に国家が関与しているとの報道も散見される。

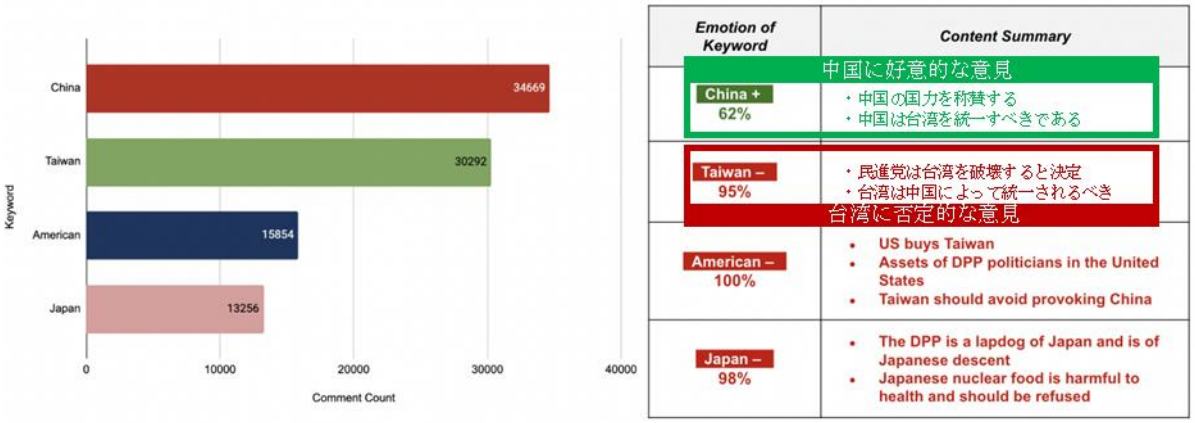
(1) アメリカ

アメリカでは 2024 年 11 月、中国系ハッカー集団ソルト・タイフーンがアメリカの通信ネットワークに侵入し、安全保障を担当する高官や政治家の携帯電話から数千人分の通話記録やテキストメッセージを流出させる事例が発生した。また、2024 年 12 月 30 日には、米財務省が中国政府系の組織による攻撃を公表し、米財務省の職員のコンピューターが侵入され、内部文書が盗まれ、数カ月間にわたり通信ネットワークを監視し、多数の通話やテキストメッセージの情報を収集していた可能性が示唆されている。

(2) 台湾

台湾 AI ラボが 2024 年に実施した調査によると、TikTok で拡散された中国関連のコンテンツの 62%は中国に好意的であり、台湾に言及するコンテンツの 95%は否定的だった。2024 年 1 月に総統に選ばれた民進党の賴清徳氏に対する否定的なメッセージが多く見られたとしている。

【図表 3.2.3-1】TikTok における世論操作が疑われる事例



出典：台灣人工智慧實驗室レポート（2024 年 4 月）

直近では、2025 年 1 月、台湾の国家安全局は、台湾政府機関に対する昨年のサイバー攻撃が 1 日平均 240 万回に達し、前年の平均 120 万回から倍増したと発表した。発表によれば、これらの攻撃の大半は中国のサイバー部隊によるものであり、特に通信、輸送、防衛分野が標的となった。中国はサイバー攻撃への関与を否定しているが、中国によるサイバー攻撃の一部は台湾周辺での軍事演習に合わせて行われており、交通機関や金融機関のウェブサイトへのサイバー攻撃が実施されている。

これら事例からも中国は他国に対し、政府機関・インフラへのサイバー攻撃、SNS を利用したフェイクニュースの拡散あるいは自国への好意醸成による相手国社会の分断など、自らの有利な状況創出を画策していることが疑われる。

2025 年 2 月 7 日、石破首相はトランプ大統領と対談し、宇宙関連でのパートナーシップの継続、AI や安全かつ強靭なクラウドサービス等、二国間における新技術を含む、サイバー空間での安全保障協力の拡大でも合意するなど、日本はアメリカと密接に連携しており、また、台湾とも民間企業におけるサイバー防衛連携を中心に交流セミナーを開催するなど友好な関係にあるが、アジアにおける地政学的な緊張が高まる中、中国との関係は複雑であり、領土問題や経済摩擦を背景に、日本もサイバー攻撃や情報操作の標的となっている可能性は高く、サイバー領域における対策は急務である。

3.3 サイバー防衛の課題

3.3.1 法制度の整備状況について

このようにサイバー領域における安全保障環境の重要性は高まっているものの、現在、日本において有事にこれら脅威を能動的に排除する環境は整っているとは言えない。それは、

有事判定基準に起因している。日本において有事判定は主に武力攻撃事態法、重要攻撃事態法、国民保護法、自衛隊法に基づいて行われるが、これらの法令は、国家の防衛および国民の保護を目的としており、武力攻撃を前提とした規定が中心に据えられているからである。

【図表 3.3.1-1】有事判定にかかる各法令に定める基準

適用法令	条文	概要
武力攻撃事態法	第2条	「武力攻撃事態」とは「武力攻撃が発生した事態又は武力攻撃が発生する明白な危険が切迫していると認められるに至った事態」を指す。
重要攻撃事態法	第1条	「そのまま放置すれば我が国に対する直接の武力攻撃に至るおそれのある事態等我が国の平和及び安全に重要な影響を与える事態に際し、合衆国軍隊等に対する後方支援活動等を行う」ことを定める。
国民保護法	第1条	「武力攻撃事態等において武力攻撃から国民の生命、身体及び財産を保護し、並びに武力攻撃の国民生活及び国民経済に及ぼす影響が最小となるようにすることの重要性に鑑み」
自衛隊法	第76条	「内閣総理大臣は、外部からの武力攻撃に際して、わが国を防衛するため必要があると認める場合には、国会の承認を得て、自衛隊の全部又は一部の出動を命ずることができる」

サイバー攻撃が武力攻撃に当たり得るかについては議論の余地があり、日本政府も国会答弁においてサイバー攻撃が武力攻撃に当たり得るとの見解は示しつつも、個別具体的のその判断をするとの見解であり、一様に判断することは困難である。

【図表 3.3.1-2】サイバー攻撃が武力攻撃に該当し得るかについての国会答弁

	回答者	概要
第201回国会（2020年）	河野防衛大臣	「現代社会の中では、社会全体のサイバー空間への依存度というのが非常に高くなってきていると思います。また、サイバー攻撃の態様も高度化、巧妙化してきているわけで、例えば、物理的手段による攻撃と同様の極めて深刻な被害が発生し、これが相手方によって組織的、計画的に行われている場合には、武力攻撃に当たり得ると考えております。」
第208回国会（2022年）	岸田内閣総理大臣	「特定のサイバー攻撃が武力攻撃に該当するかどうかについては、実際に発生した事態の個別具体的な状況に即して、政府が全ての情報を総合して客観的、合理的に判断することとなるため、一概にお答えすることは困難である。 また、どの時点で我が国に対する武力攻撃の発生、すなわち武力攻撃の着手があったと見るべきかについては、その時点の国際情勢、相手方の明示された意図、攻撃の手段、態様等によるものであり、個別具体的な状況に即して判断する必要があることから、一概にお答えすることは困難である。なお、政府としては、サイバーセキュリティ戦略（令和三年九月二十八日閣議決定）を踏まえ、サイバー攻撃に対する防御力、抑止力及び状況把握力を向上させるとともに、我が国の安全保障を脅かすようなサイバー空間における脅威に対しては、同盟国・同志国とも連携し、政治、経済、技術、法律、外交その他のとり得る全ての有効な手段と能力を活用し、断固たる対応をとることとしている。」

このように、現行の法律は主に肉体的な武力攻撃を前提としており、サイバー攻撃をどのように武力攻撃として認めるかについては、明確な基準が欠如しているため、政策決定が難しい現状がある。2025 年 2 月 7 日、サイバー対処能力強化法案及び同整備法案が閣議決定された。同法案は官民連携の強化や攻撃者のサーバー等への侵入・無害化等の対策を講じることとしており、昨今のサイバー環境の複雑化や社会経済構造の変化に対応するために必

要なものではあるが、その適用要件は「我が国及び国民の安全を損なうおそれのある重大な事態」となっており、どういった事態がこれに該当するか、また通信の秘密といった国民の権利と同法案の実効力をどのように両立させるかはより深い議論を要することとなる。

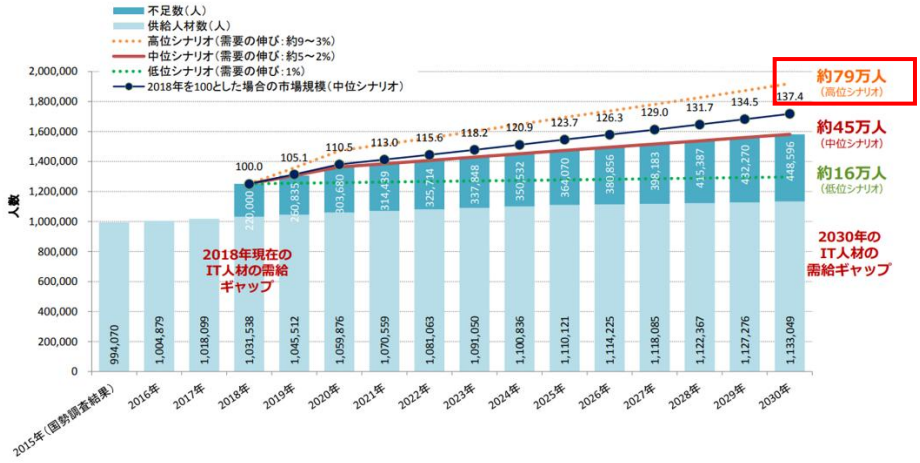
従って、日本おいては法制度の拡充や議論は必要としつつも、これと並行して、民間企業の主体的な取り組みが極めて重要であり、自主自律的なサイバーセキュリティ基準の導入や技術の革新が求められる。

3.3.2 技術的課題と構造的課題

企業や組織においては、システムの脆弱性管理が不十分であることも多く、各組織は、最新の脆弱性情報を把握し、適切なパッチ適用を行う体制が整っておらず、攻撃者による既知の脆弱性を利用した侵入を看過する事態となっており、適切なセキュリティ対策が必要である。また、事前の準備やシミュレーションの不足もあり、サイバー攻撃発生時の迅速かつ効果的に対応できていない事例も多く、これにより、被害の拡大や情報漏洩が発生し、企業の信頼性やブランド価値が損なわれる可能性が高まるものと考えられる。

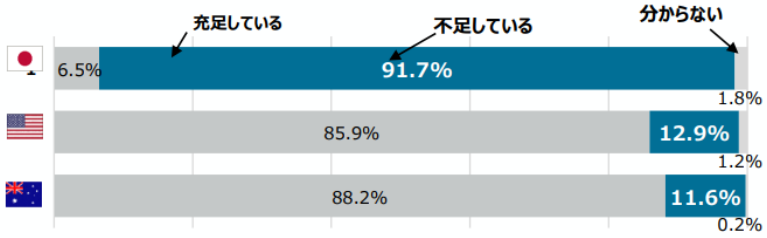
これらの背景として IT 人材の不足が挙げられ、2030 年までに最大 79 万人程度不足すると予測されている。これに対し、総務省は、NICT（情報通信研究機構）と連携し、「CYDER」や「SecHack365」といったプログラムを通じて人材育成の取り組みを進めているが、これらの取り組みだけでは、業界全体の人材不足を解消するには不十分である。

【図表 3.3.2-1】IT 人材の供給動向の予測と平均年齢の推移



出典：みずほ情報総研 IT 人材需給に関する調査報告書（2019 年 3 月）

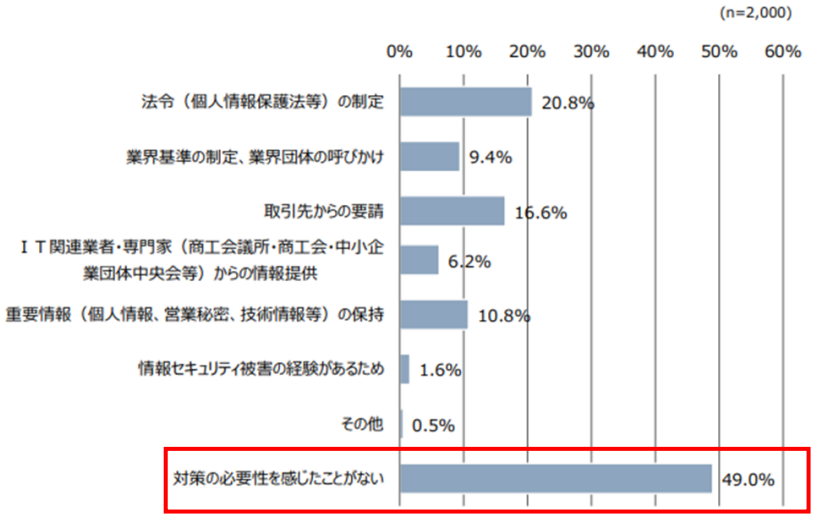
【図表 3.3.2-2】IT セキュリティ人材の不足状況



出典：NRI セキュア 企業における情報セキュリティ実態調査 2023（2024 年 3 月）

これら課題の原因は様々考えられるが、その一端は企業（経営層・従業員）の認識の低さにあるものと考えられる。多くの企業、とりわけ中小企業では、サイバーセキュリティに対する投資が限られており、専門人材の採用には十分な経済的余裕がない。その結果、セキュリティ対策が後手に回り、リスクが増大している。また、経営層を含む多くの人々がサイバーセキュリティの重要性を十分に認識していないことも問題を深刻化させている。

【図表 3.3.2-3】情報セキュリティ対策の必要性を感じた理由



出典：三菱 UFJ リサーチ＆コンサルティング 中小企業における情報セキュリティ対策の最新動向（2024 年 5 月）

日本の教育機関においても、サイバーセキュリティ分野に特化したカリキュラムや研修プログラムが不足しており、多くの学生が実務に必要なスキルを習得できないまま卒業し、就業するため企業従業員における認識も十分には醸成されていない状況にある。

総務省が推進するセキュリティ・ネクストキャンプなどの取り組みはあるものの、その受講者数は依然として限られており、国家的な制度設計に依らない民間企業としての取り組みの重要性は増している。

3.4 サイバー防衛における提言（国への提言）

3.4.1 サイバー攻撃の無害化に係る制度の整備

サイバー対処能力強化法案が閣議決定され、今後、発動条件や国民の権利保護との調和について議論が深められるものと想定されるが、同時に同法案の実効性の担保についても対策が講じられることが望まれる。同法案では我が国及び国民の安全を損なうおそれのある重大な事態には、警察・自衛隊による無害化措置を講じることとしているが、先に述べたサイバー犯罪の検挙件数の高止まりなど、現状では対応人員が不足しているものと想定される。このようなことから、サイバーセキュリティ分野での人材不足を補うため、大学や専門学校との連携を強化し、サイバー防衛に特化した教育プログラムを設けることが求められる。また、警察や自衛隊においても、サイバー攻撃に対応できる技術者を増やし、実践的なトレーニングを実施する機会の創出を期待したい。

3.4.2 平時・有事を全方位で守るための法整備

サイバー攻撃は多くの場合、組織の脆弱性を突く形で行われ、結果として大規模なデータ漏洩や経済的損失を引き起こしているが、政府機関や企業は、これらの脅威に対して単独で対処することは難しく、官民連携を強化し、情報共有の体制を確立することが不可欠である。民間企業が直面するサイバー脅威に関する情報を迅速に収集・分析し、サイバー攻撃の兆候を早期に察知する体制を整備することが重要である。サイバー対処能力強化法案の実効性担保のためには通信情報の監視を行う際の国民の理解を醸成、運用に関する具体的な基準や指針を明確化し、国民や関係機関に対して透明性のある説明を行うことで、信頼性を高めることを求めたい。

3.5 サイバー防衛における提言（企業への提言）

3.5.1 セキュリティ対策の強化と教育

企業におけるサイバー防衛能力の向上には、経営層および従業員のサイバーセキュリティリテラシーを向上させ、定期的な教育プログラムの実施が不可欠である。企業は、セキュリティを経営の重要な要素として位置付け、従業員全体にその意識を浸透させる必要がある。

一方で、これまで述べてきたようにサイバーセキュリティは被害の実態を予測しづらいことに加え、対策には費用を要することから人的・金銭的投資が憚られることが想定される。そのため国や行政からの一方通行な通知・連絡のみでは主体的に自分事として捉えることが難しく、有識者を通じた双方向の意見交換、理解醸成が不可欠であるものと考えた。

我々はその一助を担うべく、企業に対するセキュリティ意識の醸成に取り組むこととし、

専門的な知見を有する Trend Micro 社とコンタクトを取った。同社は経済産業省が主催する産業サイバーセキュリティ研究会に参画、企業や専門家と連携し、サイバー攻撃の脅威に対する効果的な対策の議論を通じ、産業界全体のセキュリティ対策の強化を推進するなど、日本における有数のサイバーセキュリティ企業である。また、「世界サイバーリスクレポート」を公表し、全世界を対象としたサイバーリスクの状況をスコア化しており、日本の組織がサイバーリスクに対して継続的に対策を講じているスコアは他国と比べて低く、企業規模別にリスク指標を分析すると、1 万人以上の従業員を抱える企業が最も高いリスクレベルであることを示していることや、脆弱性の判明からパッチ適用までに 1 カ月以上も要しており大企業においてもサイバーリスクの管理が不十分であることについて警鐘を鳴らしている。

そこで、同社と日本の企業が対策すべきサイバーセキュリティに関する意見交換を行い、まずはグローバル適塾会員企業向けの勉強会を開催することでサイバーセキュリティについて考えを深めるきっかけを作ることとした。この勉強会で各企業が取り組むべき事項について明確化し、従業員一人ひとりがサイバー防衛に対する意識を高め、自らの役割を理解し実行に移すきっかけとなることが期待される。

3.5.2 サプライチェーンを含む重要情報資産の特定、リスク評価および対策

企業はまず、自社の情報資産に対するリスク評価を実施し、脆弱性を明確にすることが求められる。これに基づき、対策を策定し、実際の攻撃に備えた訓練を行うことが重要である。具体的には、サイバー攻撃の兆候を早期に発見し、迅速に対応するための仕組みを構築することが必要である。

受動的なセキュリティ対策では不十分であり、多層防御を取り入れ、ファイアウォール[6]、侵入検知システム、コンピューターやスマートフォンといったエンドポイント[7]へのセキュリティなどを組み合わせることで、攻撃に対する耐性を高めることができる。これらの防御策を講じることで、企業のセキュリティの強化につながる。

各企業には定期的なセキュリティ監査を実施し、その結果に基づいて対策を見直すことで、常に変化するサイバー攻撃の脅威に対応できる体制を維持することを期待したい。

6 ファイアウォール（Firewall）。不正アクセスや未許可の通信からネットワークやコンピューターを守るセキュリティシステム。
7 コンピューター ネットワークに接続してそのネットワークとの間で情報を交換する物理的なデバイスのこと。

3.6 サイバー防衛における提言（個人への提言）

3.6.1 個人情報管理

個人としては、自らが使用する電子機器やネットワークのリスクを見直す必要がある。

同志国以外で製造されている機器については、バックドア[8]が組み込まれている可能性があり、個人情報（氏名や電話番号に加え、銀行口座やクレジット番号など）が流出することでの個人的な経済損失はもとより、バックドアで侵入した端末を踏み台として、他のシステムへの侵入を試みたり、マルウェアを拡散させるおそれがある。

そのため、各個人は電子機器等の安全性を評価し、必要な対策を講じることが求められる。これにより、個人情報の漏洩や不正アクセスのリスクを低減し、サイバー攻撃の影響を最小限に抑えることができる。また、セキュリティソフトの導入や定期的なパスワードの変更など、日常的な管理を徹底することが重要である。

3.6.2 情報の適正利用

また、個人は、受け取る情報を多面的かつ客観的に捉える姿勢が求められる。フェイクニュースが横行する現代において、自らの判断で情報を精査し、信頼性のある情報源からの情報を優先することが必要である。情報を適正に利用することで、サイバー空間における混乱を避け、社会全体の情報セキュリティ向上に寄与することができるものと考える。

3.7 結論・まとめ

3.7.1 サイバー防衛の重要性の再認識

サイバー防衛は、現代の安全保障環境においてますます高まっている。サイバー攻撃は国家、企業、個人に対して多様な形で脅威をもたらし、その影響は経済活動や社会の安定にまで及ぶ。特に、ランサムウェアやサプライチェーン攻撃などの手法は、組織の機能を麻痺させ、広範な被害を引き起こす可能性がある。これに対抗するためには、国、企業、個人が一体となってサイバー防衛能力を強靭化させることが不可欠である。

3.7.2 提言の要約と実行の重要性

提言として、まず国に対しては、サイバー攻撃に対する法制度の整備と官民連携の強化が求められる。企業に対しては、セキュリティ対策の強化と従業員教育の徹底、サプライチェーンを含む情報資産のリスク評価と対策が重要である。個人に対しては、個人情報の適切な管理と情報の適正利用が求められる。これらの提言を実行することにより、サイバー攻撃に

8 コンピューターやサーバー、システム・アプリケーションなどに不正侵入するための入口。

対する防御力を高め、被害を最小限に抑えることが可能となる。

【図表 3.7.2-1】提言内容

対象	提言内容	詳細
国	法制度の整備と官民連携の強化	➢ サイバー攻撃に係る官民の情報共有、サイバー攻撃の無害化に係る制度の整備 ➢ サイバー攻撃には平時・有事の境がないため武力攻撃事態に至らない段階から我が国を全方位で守るための制度（法整備等）の策定
企業	セキュリティ対策の強化と社員教育の徹底	➢ 企業によるサプライチェーンを含む重要情報資産の特定、リスク評価の実施 ➢ リスクを低減させる対策（サイバーセキュリティ対策）の実施
個人	個人情報の適切な管理と情報の適正利用	➢ 有事における敵対国で作られた電化製品・情報機器、ネットワーク機器等の見直し、アプリケーションシステムの見直し ➢ 情報を批判的に評価する

3.7.3 将来展望と更なる技術革新への期待

今後、技術革新がサイバー防衛の新たな手段となることが期待される。AI やブロックチェーン技術[9]の進化により、より高度なセキュリティ対策が可能となり、サイバー攻撃に対する防御力が一層強化されることは間違いなく、これらを有効活用することにより、持続可能な安全保障体制の構築が進み、社会全体の安定と発展に寄与することが望まれる。

9 多数の参加者に同一のデータを分散保持させる仕組みで、改ざんが非常に困難であることが特徴。

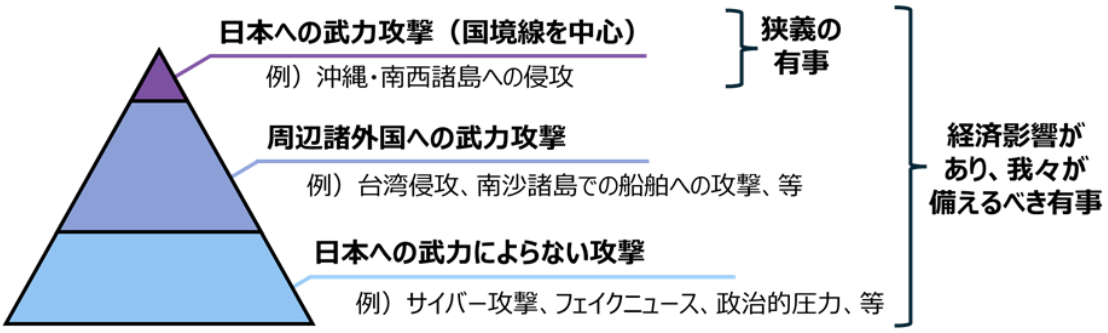
第４章 武力攻撃に巻き込まれた時に備えた自主的な避難計画

本提言では経済影響などを含めた広義での有事に関して取り上げているが、本章においては武力攻撃を想定した対策について述べる。安全保障においては、武力攻撃も想定して国民一人ひとりが備えることによって安全保障に対するリテラシーを向上することが必要であると捉えている。その結果として、諸外国から日本を捉えた際、安全保障に対する意識の高さを警戒され、対外的な抑止力になると考えるからである。

武力攻撃に関しては、日本本土や沖縄・南西諸島への武力攻撃のみならず、海外で巻き込まれた際も想定して考える必要がある。近年では日本人が海外を訪れる機会も多く、年間1,300万人が海外を旅行し（2024年推測）、129万人が海外へ在留している（2024年10月現在）等、日本人口の 11.6%が海外を訪れており、海外で巻き込まれることも十分あると言える。

では、実際にどのような武力攻撃に巻き込まれる可能性があるのだろうか。次節にて考察する。

【図表 4-1】本提言における有事の定義（再掲）



4.1 想定される武力攻撃

4.1.1 台湾有事の可能性

中国の習近平国家主席は、台湾の統一を中華民族の偉大な復興の不可欠な要素と位置づけ、3期目入りを決めた2022年10月の党大会で台湾統一を目標に掲げ「武力行使の放棄は約束しない」と明言した。前年2021年3月20日の米下院軍事委員会では、当時の米インド太平洋軍司令官が6年以内に中国が台湾に武力侵攻を行う可能性があると証言し、また2023年2月2日、米中央情報局（CIA）長官がワシントンでの講演で、習近平国家主席が「2027年までに台湾侵攻を成功させる準備を整えるよう、人民解放軍に指示を出した」ことを情報として把握していると述べたことで、専門家の間では2027年に台湾有事が起こるのではないかとの見立てがある。

現時点で習近平国家主席が台湾へ侵攻する決断をしているわけではなく、今後の第 2 次

トランプ政権の動向にも左右されると推測されるが、2027 年は習近平国家主席の 4 期目続投の節目であり、長期政権を実現するためには軍事力を使ってでも台湾の統一をめざす可能性が指摘されている。

4.1.2 台湾有事では何が起こり得るのか

台湾有事は、単なる軍事衝突に留まらず、サイバー攻撃、経済制裁、情報戦、そして国際的な軍事的対立に発展する可能性がある。

初期段階では軍事行動を表面化させず、情報戦や経済制裁、サイバー攻撃を中心に台湾の機能を弱体化させると考えられる。具体的には政府機関への攻撃として台湾国防部、外交部、総統府などへのハッキングやシステムダウンを実行、また電力や通信会社等への攻撃により停電やインターネット障害を発生させ、混乱を引き起こすことが想定される。

次に銀行や証券取引所のシステムを麻痺させて台湾経済の安定を揺るがせた上で、情報操作として「台湾政府が降伏した」「アメリカは台湾を見捨てた」などのフェイクニュースを SNS やメディアで拡散し、パニックを誘発する。

さらに次の段階では、経済封鎖・貿易制限として台湾向けの輸出入を制限し、経済的圧力をかけ台湾経済に打撃を与えることが想定される。海上封鎖として中国海軍が台湾周辺を封鎖し物資の輸入を妨げ、航空封鎖として中国軍機が台湾周辺を飛行し、国際線の運航を妨害する可能性がある。

外交的な圧力や封鎖によっても台湾が降伏しない場合、最終的に中国は本格的な武力侵攻を開始する可能性がある。港や空港への攻撃により台湾への物資供給を遮断し補給を困難にし、台湾の空軍基地や防空システムを破壊して航空優勢を確保、さらには総統府・政府機関へ攻撃し台湾政府の指揮系統を混乱させると考えられる。またさらには陸上侵攻を行い主要都市での戦闘など市街戦となる可能性もあり得る。

現時点で具体的に武力攻撃が発生しているとは言えないが、「3.2.3 他国における事例と日本への影響」で述べた通り、実際に台湾政府機関に対するサイバー攻撃が倍増、大半が中国のサイバー部隊による攻撃だったとしている。台湾国家安全局の報告書によると、中国によるサイバー攻撃の一部は台湾周辺での中国の軍事演習に合わせて行われ、すでに中国による台湾有事に向けた動きが始まっていると言える。

4.1.3 台湾有事が起こった場合の日本への影響

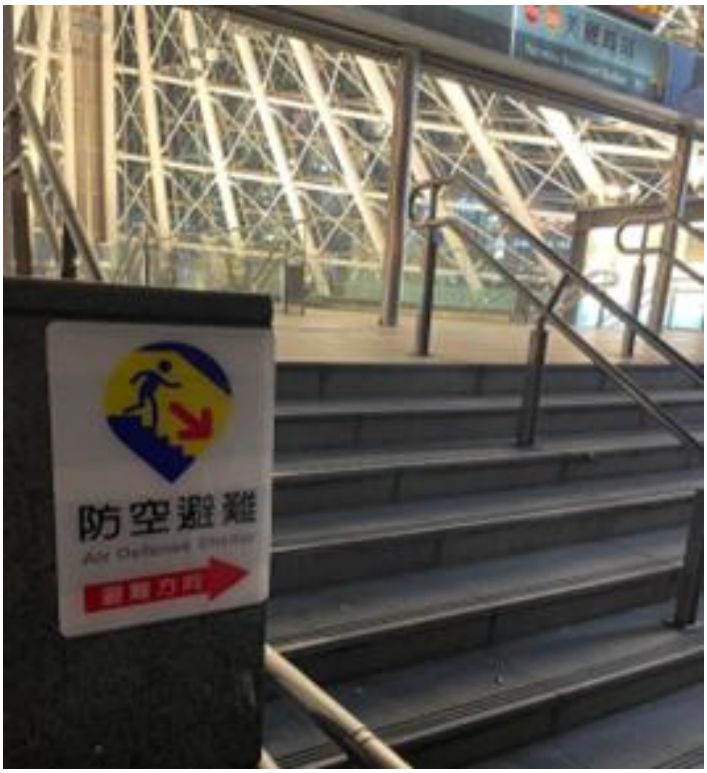
万一、実際に台湾有事が起こった際、日本にはどのような影響が出るか。

まずは、台湾現地で影響を受ける可能性が考えられる。現在在留邦人は 2.1 万人（2023 年 10 月外務省調べ)、旅行者などを含むとその数はさらに増え、これら多くの邦人が巻き込

まれることとなる。

台湾では緊急避難先として全土に 10.5 万か所のシェルターを整備し、収容能力は計約 8,600 万人としている。台湾の人口は 2,342 万人であり十分な収容が可能となっている。シェルターは駅や大型競技場などの公共施設以外に、行政が指定する 5 階建て以上の工場、6 階建て以上のマンションや商業ビルなどへの設置が義務づけられており、シェルターの設置場所が分かるアプリも提供されているため初めて台湾を訪れる人にも認識は容易である。

【図表 4.1.3-1】台湾の駅に設置されているシェルター案内（23 期安全保障 G 撮影）



一方で、シェルターは通常時は駐車場などを兼ねている場合もあり、食料や水などの備蓄設置に関する義務はなく、一時的な避難に留まると想定される。また、邦人の本格的な日本への避難に関しては具体的には示されておらず、2022 年 12 月 29 日付 日本経済新聞記事によると「邦人全員を台湾から退避させるには『現行の輸送能力では 1 カ月はかかる』状況」とされている。我々が 2025 年 1 月に台湾を訪れ台湾有事に関して現地の方々とディスカッションを行った際には、「万一、台湾有事が起こった際は台湾では自国防衛に専念しており、外国人の避難は各国に任せることになるのではないか」という声もあり、緊急避難に関する計画の策定が必要と考える。

次に、台湾現地の在留邦人だけでなく日本への直接の影響も考えられる。2021 年 12 月に安倍晋三元総理が「台湾有事は日本有事」であると述べたように、台湾有事は対岸の火事ではない。それは、もし台湾有事が発生した場合、日本は米軍支援の有無にかかわらず巻き込

まれる可能性が高いと考えることができるからである。理由として、中国は台湾侵攻時に米軍の介入を警戒し、沖縄・横須賀などの在日米軍基地や自衛隊基地を攻撃目標に含める可能性があることが挙げられる。

また台湾有事の戦域が台湾周辺だけでなく東シナ海や西太平洋にも及び、日本周辺の海域にも浮遊機雷等が流れ込む可能性や、中国が台湾侵攻と同時に尖閣諸島を占領する可能性もある。

このように日本が望む望まないに関わらず、近隣諸国における有事に巻き込まれる可能性は大いにあると言える。

4.1.4 日本への武力攻撃の可能性

最後に、日本における有事の可能性について考察する。現時点では日本への武力攻撃は具体的には考えにくいが、本項で日本を取り巻く情勢を踏まえ改めて確認する。

日本の安全保障環境は、中国の台頭、北朝鮮の核・ミサイル開発、ロシアの動向など多方面において不安定要因が多くなってきている。

中国とは前節で述べたように危険性が高まっている中、北朝鮮は核実験を継続して行い、ICBM（大陸間弾道ミサイル）の開発を加速させるなど軍事強化を図っており、見過ごすことは出来ない存在になってきている。

またロシアのウクライナ侵攻において、日本も対ロシア制裁を実施したこと等を踏まえ日露関係は悪化、北方領土問題の交渉は停滞しており、ロシアは日米の軍事連携を警戒し中国との関係強化を模索している。またロシアと北朝鮮も関係強化されており、2024年12月、北朝鮮の金正恩総書記はロシアのプーチン大統領に書簡を送り包括的戦略パートナーシップの強化を確約。さらに、北朝鮮はロシアのウクライナ侵攻を支援するため、数千名の兵士をロシアに派遣していると報告されている。

これらの世界情勢により、日本の周辺では軍事力を強化した近隣諸国の影響が拡大しており、またそれらの国々が連携を強化しているため武力攻撃の対象となる可能性を考慮した備えについて、ますます必要性が高まってきている。

次節以降で、日本の国民保護法を踏まえ日本で有事が起こった場合の対応策について述べる。

4.2 国民保護法の定めと日本の避難計画の実態

国民保護法（正式名称：武力攻撃事態等における国民の保護のための措置に関する法律）は、2004年に成立した法律である。2001年アメリカでの同時多発テロや北朝鮮による弾道ミサイル発射等により、日本の安全保障に対する国民の関心が高まるとともに、大量破壊兵器の拡散や国際テロ組織の存在が重大な脅威となっており、こうした状況の下、日本に対す

る武力攻撃に対処できるよう必要な備えをするため、有事法制の整備が進められた。

2003 年には武力攻撃事態法が成立し、国家の防衛を目的とし、政府・自衛隊・地方自治体がどのように武力攻撃に対応するかを定められた。2004 年の国民保護法は、日本が武力攻撃を受けた場合や大規模テロが発生した場合に、政府・地方自治体・住民がとるべき対応を明確にしたものであり、避難、救援、治安維持、インフラの確保などを円滑に行うための法的枠組みを整備している。

【図表 4.2-1】武力攻撃事態法と国民保護法の比較

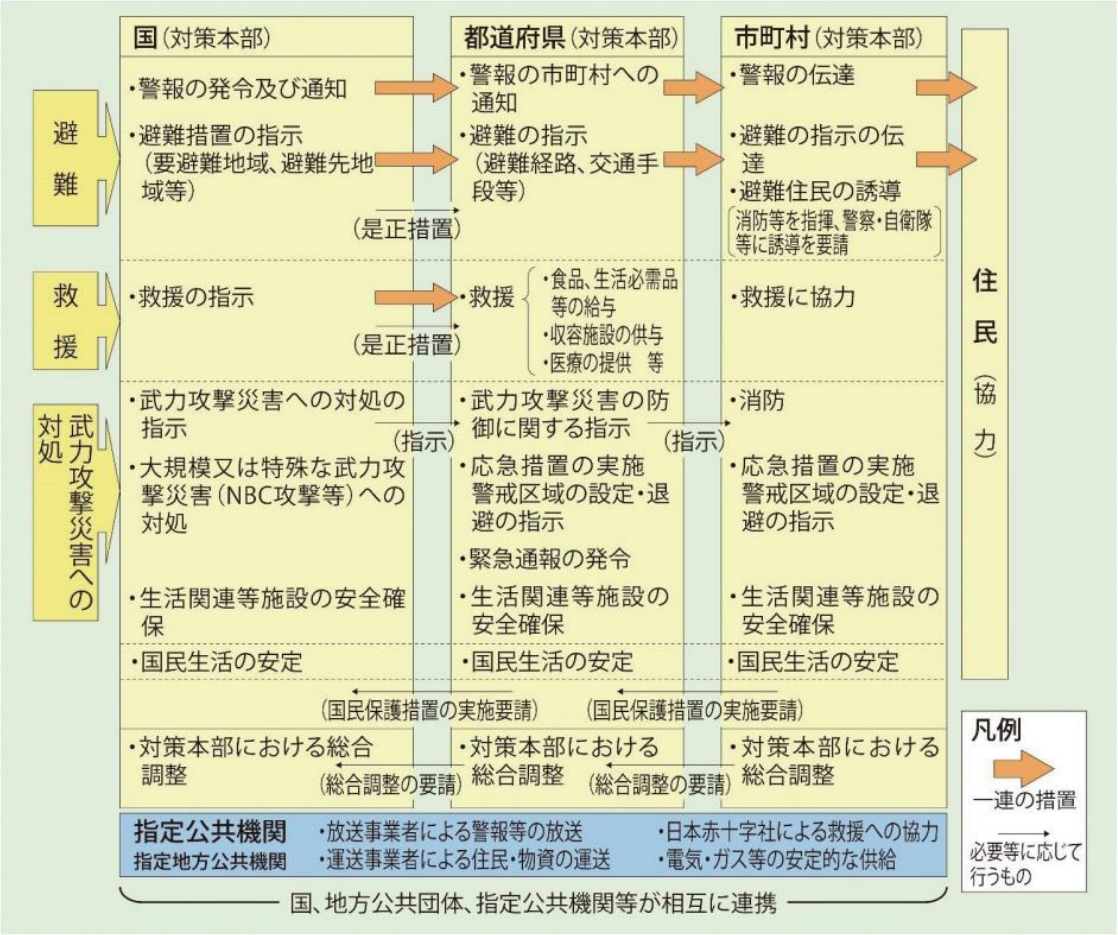
項目	武力攻撃事態法	国民保護法
目的	国の防衛と武力対応	国民の避難、保護
対象	自衛隊、政府、自治体の武力対応	住民の避難、救助、治安維持
適用される事態	武力攻撃事態、武力攻撃予測事態など	武力攻撃、テロ、ミサイル攻撃など
具体的な内容	・自衛隊の出動 ・防衛出動の指示 ・政府の対応方針の決定	・住民の避難計画 ・物資、医療支援 ・自治体の避難誘導

4.2.1 国民保護法の定め

国民保護法を理解するうえで、まず認識しておきたいことは、国民の保護は国・地方自治体が担うものであり、自衛隊の役割は別となっていることである。

国民保護法における具体的な措置は、自衛隊による国民の保護ではなく、あらかじめ政府が国民の保護に関して定めた基本指針や、各府省および地方公共団体にて定めた国民の保護に関する計画に基づき、国・都道府県・市町村などの地方自治体が連携して対処することとなっている。

【図表 4.2.1-1】避難・救援・武力攻撃災害への対処等の国民保護措置



出典：令和 6 年版 消防白書（2025 年）

自衛隊の役割に関しては、自衛隊法第 76 条第 1 項に防衛出動について定められており、「内閣総理大臣は、外部からの武力攻撃（外部からの武力攻撃のおそれのある場合を含む。）に際して、わが国を防衛する必要があると認める場合には、国会の承認を得て、自衛隊の全部又は一部の出動を命ずることができる。ただし、特に緊急の必要がある場合には、国会の承認を得ないで出動を命ずることができる」とされ、また第 88 条において「第七十六条第一項の規定により出動を命ぜられた自衛隊は、わが国を防衛するため、必要な武力を行使することができる」と定められている。

このように、自衛隊は有事の際には防衛のために出動するものである。我々日本人は、日本が有事に巻き込まれた際にも自衛隊に任せておけばいい、という漠然とした考えが浸透しているのではないか。災害時などの自衛隊の活動を目にすることも多く、いざ有事の際にも頼ることができると考えている人も多いと推察する。だが実際には、自衛隊は侵害排除を第一優先として活動することとなるため、救援・避難に関しては自治体と連携として国民自身が行動する必要があると認識するべきである。

4.2.2 自治体の避難計画

本項では実際に自治体はどのような避難計画を策定しているのか確認する。2004 年国民保護法の施行に伴い、都道府県及び市町村は国民保護計画を作成することが義務付けられた。東京都の国民保護計画でも、「武力攻撃事態」「大規模テロ等」の事態を想定して策定されており、平素より備えを行うと示されている。

【図表 4.2.2-1】東京都の定める事態

事 態	事 態 類 型
武力攻撃事態	① 着上陸侵攻 ② ゲリラ・特殊部隊による攻撃 ③ 弾道ミサイル攻撃 ④ 航空攻撃
大規模テロ等 (緊急対処事態)	① 危険物質を有する施設への攻撃（ガス貯蔵施設等） ② 大規模集客施設等への攻撃（駅、列車、劇場等） ③ 大量殺傷物質による攻撃（炭疽菌、サリン等） ④ 交通機関を破壊手段とした攻撃（航空機による自爆テロ等）

出典：東京都「国民保護計画」解説冊子

また有事の際には、東京都知事は市区町村長を通じて避難を指示することとしている。指示の内容は避難準備の時間的余裕などにより異なり、特に、島しょ部における避難は交通手段が制約されることを考慮し、早めに全島民を本土へ避難させることも併せて明示されている。

しかしながら下表の通り、武力攻撃が起こった際、時間的余裕がない場合の避難はまず個人それぞれが自身で近隣の安全な場所へ避難することとなっている。また東京都の国民保護計画には前述の通り「指示の内容は避難準備の時間的余裕などにより異なり」と示されており、多くの国民が経験したことのない不測の事態の中で状況に応じた避難指示が出ることになる。

【図表 4.2.2-2】東京都の定める避難指示

出典：東京都「国民保護計画」避難の指示（2024 年 11 月）

実際にその場の状況に応じた避難判断や、フェイクニュースなども錯綜し混乱する中で示される避難指示の情報を得た上での行動は、個人の抱える環境や事情、情報リテラシーにも影響されると想定する。このため、各自治体が国民保護計画を策定するだけでなく、国民が各自治体の国民保護計画を理解し、まずは自身で避難の判断を行う必要性があることを理解するべきである。

4.2.3 自治体の避難訓練

国民が各自治体の国民保護計画を理解し、有事の際に実際に自身で実行するためには避難訓練が効果的であると考える。避難訓練は、緊急時に適切な行動を選択し被害を最小限に抑え、混乱を防ぐ効果が期待でき、何より住民の危機意識向上および有事の際に助け合える関係構築も可能となる。また計画通りに避難が進むか確認し問題点を洗い出し、行政や関係機関が協力した実践的な対応を確認することができる。

実際に、台湾からわずか 110 キロの位置にある沖縄県与那国島では 2022 年 11 月に弾道ミサイル発射を想定した住民保護訓練を実施している。また沖縄県石垣市でも 2024 年 2 月に住民保護訓練、さらに同年 9 月には有事の際の全島避難を想定した初の模擬訓練を実施し、住民が避難する際に必要な手続きなどを実際に行い動線や所要時間の検証を行った。

しかしながら政府は、台湾有事で沖縄を取り巻く状況が悪化した場合、南西諸島から避難が必要となるのは観光客も含めて 12 万人にも上ると想定している。避難計画について策定の協議を始めているが、輸送船・輸送機の確保、具体的な受け入れ先の決定など課題は残っており、避難訓練が行きわたるのはまだ先のことと考えられる。また与那国島に関しては、一時的に住民が避難するシェルターの整備をめざしているが、現時点では計画段階である。

国は国民保護法、自治体は国民保護計画を策定し有事の対策を行っているが、実際には国民それぞれが考え行動することが必要である。その認識を国民一人一人に持たせるような有事に備えた避難訓練などの活動は充分とはいえず、そもそも自治体の国民保護計画の認知すら行き届いているとは言えないのではないだろうか。

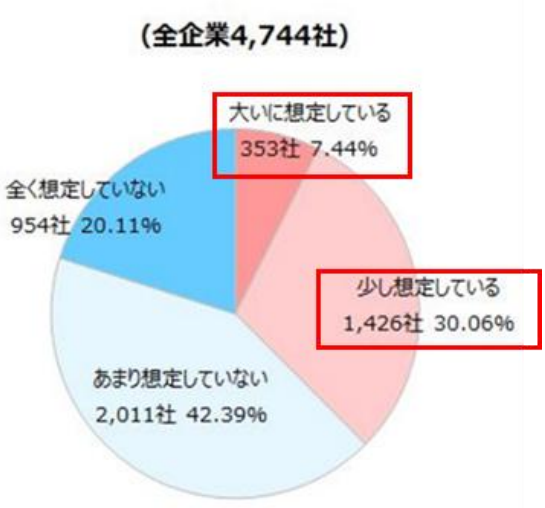
4.2.4 企業の避難計画

次に、もし武力攻撃に巻き込まれるような事態が平日日中に起こった際、企業に勤める人は企業の指示に従うことが考えられる。では企業はどのような対応を取るのだろうか。

東京商工リサーチは 2024 年 2 月、インターネットで台湾有事に関するアンケート調査を実施（回答 4,744 社）。結果として、台湾有事を想定している企業は約 4 割（37.5%）に上るものの、何らかの対策を講じている企業は 23.9%に留まる。

【図表 4.2.4-1】台湾有事の想定状況

Q1. 中国と台湾の緊張関係が高まっています。貴社は「台湾有事」を想定していますか？（択一回答）

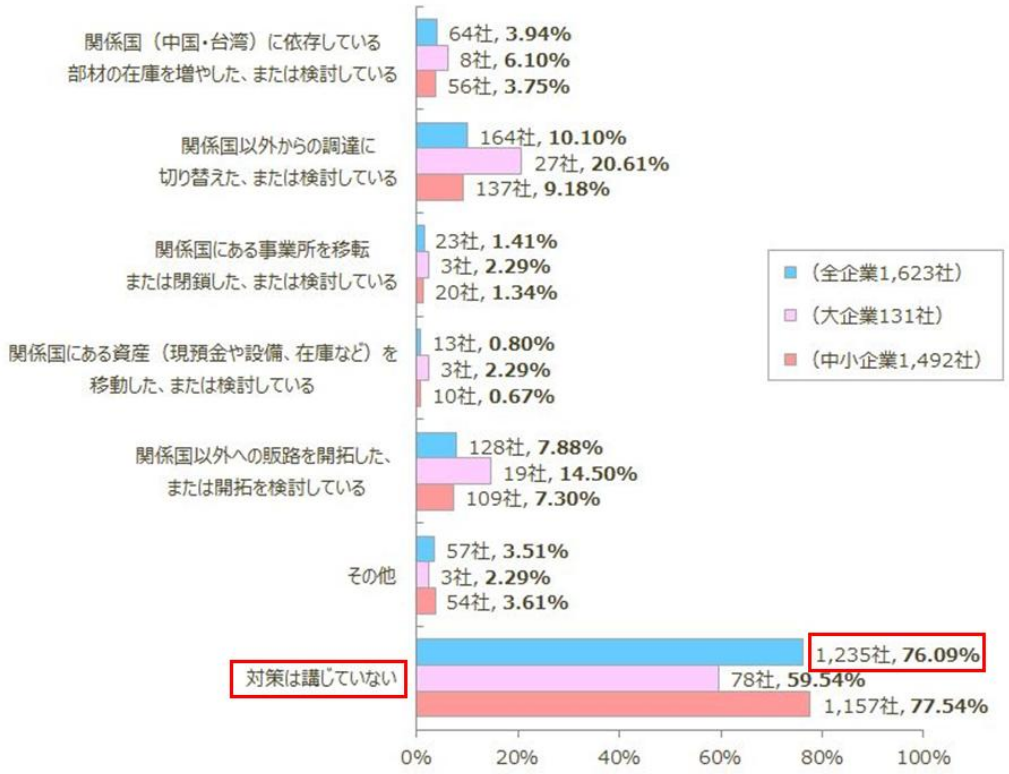


出典：東京商工リサーチ「企業の台湾有事の想定」アンケート調査（2024 年 2 月）

【図表 4.2.4-2】台湾有事の対策状況

Q2.Q1 で「大いに想定している」「少し想定している」と回答された方に伺います。

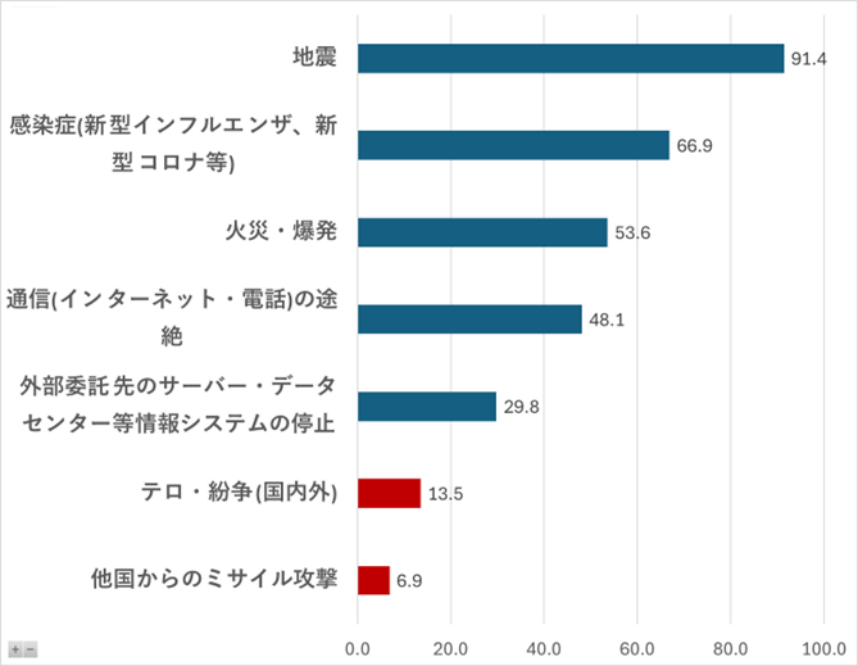
なんらかの対策は講じていますか？（複数回答）



出典：東京商工リサーチ「企業の台湾有事の想定」アンケート調査（2024 年 2 月）

また台湾有事に限定せず、日本国内も含めた有事に関する企業の BCP に関しても同様の状況である。内閣府の行った「令和 5 年度企業の事業継続及び防災の取組に関する実態調査」において、BCP 策定率は大企業で 76.4%、中堅企業で 45.5%と一定程度の策定を行っていると言える。しかしながら BCP で重視しているリスクに関して、紛争やミサイル攻撃の考慮は企業規模問わず 10%前後であり、ほとんど物理的な有事に係るリスクは未考慮である。

【図表 4.2.4-3】重視しているリスク



出典：内閣府「令和 5 年度企業の事業継続及び防災の取組に関する実態調査」を基に作成（2024 年 3 月）

これら企業の BCP は、事業継続のために重要なサプライチェーンなどに関しては考慮されているが、武力攻撃を考慮した上で現地で巻き込まれる従業員の安全確保・避難についての対策は見受けられない。

我々が自身の身を守るためには、各自治体のみならず、自身が所属する企業の BCP は有事も踏まえた計画となっているか、なっていない場合は BCP の見直しを行うなど、従業員および経営幹部ともに現在のうちから確認しておくことは、安全保障に関する意識醸成および万一有事が起こった際の有効な手段である。

4.3 自主的な避難計画における提言

避難計画は単に危機が起こった際の対策だけでなく、安全保障に関するリテラシー向上および諸外国に対する抑止力につながるものであり、安全保障の重要な取り組みであることから、避難計画に対して企業・個人に対して提言を行う。

4.3.1 避難計画における提言（企業への提言）

現在、日本において有事に関する危機感は高くなく、必要性を高く感じていないと想定され、企業の有事に備えた避難計画を含めた BCP は策定が十分であるとは言えない状況である。ただし、ウクライナ侵攻について大半の人々が想定外であったように、昨今の情勢によ

り日本を取り巻く環境は大きく変わってきている。

万一に備えた対策を検討することは多くの予算をかけずに行えることも多く、杞憂に終わっても大きな損失にはならないと想定するため、まず検討し始めることが重要であると考える。

海外で巻き込まれた場合には、現地に在籍する従業員の当面をしのぐ備蓄確保、どの機関と連携すべきか、現地在住の家族構成の把握を含めた避難計画の立案・周知・訓練などを行い、日本で巻き込まれた場合には、所属する自治体との連携や備蓄確保、従業員の避難計画などを策定、こちらも周知・訓練を行う必要がある。これらは災害時の対策とも連動することが多いと推察するが、それに加え、サイバー攻撃やフェイクニュースなどに惑わされずに情報連携するツールや手段の検討、また影響期間を短期・中期・長期の期間別に対策のシミュレーションを行っておくことは非常に有益であると考える。

4.3.2 避難計画における提言（個人への提言）

国や自治体、企業における避難計画があっても、それを受け取る個人の認識がなく、いざ有事の際に行動できないことは大いに考えられる。有事に巻き込まれる場所も時間帯も予測できない中、自身の所属する自治体・企業に頼ることができる状況下であるか想定はできない。このため、各個人が有事に巻き込まれた際の対応を検討しておく必要がある。

海外で巻き込まれた場合には、まずは情報確保が必須である。例えば旅行前に外務省の海外安全ホームページの確認を行い、また「たびレジ」に登録しておくことで安全情報をメール受信でき、万一の際に安否確認や支援を受け取ることができる。また予備の食料など余裕をもって確保しておくことも対策として考えられる。

日本で巻き込まれた場合に備えては、自身の自治体の国民保護計画を知る、自宅での備蓄を行う、電子機器が使えない場合に備えた現金の確保や、自治体の避難訓練に参加する必要がある。また日本でも旅行先で有事に巻き込まれた場合のシミュレーションと対策も必要であると考える。

4.4 結論・まとめ

台湾有事や北東アジアの地政学的リスクを考慮すると、日本も有事に巻き込まれる可能性は十分に考えられる。

その際、自衛隊は防衛活動が主な任務となるため、避難や救助は自治体と住民の主体的な対応が求められる。国・自治体の国民保護計画を理解して実行し、機能させるためには自治体の努力だけでなく、企業・個人レベルでも有事に備えた計画を策定し、日頃からのサイバー攻撃やフェイクニュースに関する意識を高めた行動、また安全保障リテラシーの向上が重要である。

【図表 4.4-1】提言内容

	提言内容	詳細
企業	・国内有事の避難計画を含むBCPを策定 ・海外や他拠点における有事の従業員等の安全確保を規定化	国内においては避難計画・備蓄準備・自治体との連携を準備。 海外においては在外邦人の行動計画等の立案、周知、訓練を実行する。 これらは短期/中期/長期と期間別に在外邦人/現地従業員の対応SIMが必要
個人	有事に巻き込まれた際の対応を検討	自治体の対策案を知る・備蓄準備・現金の確保を行い、避難訓練を実施する。 旅行先で有事に巻き込まれた場合のシミュレーションと対策を行う

第５章 安全保障リテラシーの向上に向けた取り組み

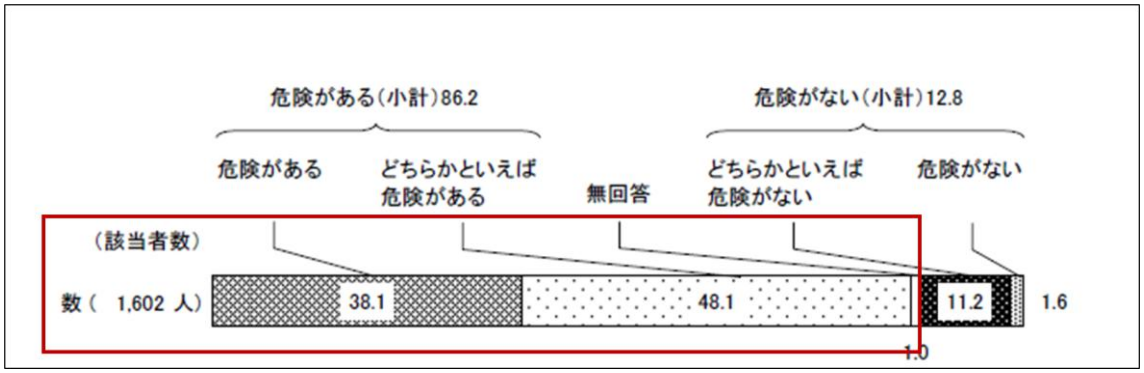
これまで「サプライチェーン維持・強靭化」「サイバー防衛能力の強靭化」「自主的な避難計画」について論じてきたが、本章では安全保障対策の下支えとなる日本国民の安全保障に対するリテラシー向上に向けて、主に若年層に対する教育の観点から提言する。日本国民の防衛意識は、北朝鮮のミサイル発射や中国の軍事力増強、ロシアのウクライナ侵攻など、近年の国際情勢の変化に伴い、徐々に高まってきてはいるものの、日常生活で積極的に論じられる機会は未だ少ない。これは戦後から続く社会的背景や教育の影響であり、一朝一夕に意識を変容することは難しい。「戦争」や「防衛」に対して比較的忌避感が少ないと考える若年層のリテラシーを向上し、大人へと波及することでリテラシーの向上につなげることが必要であると考える。

5.1 日本国民の防衛意識

5.1.1 安全保障に対する日本国民の認識

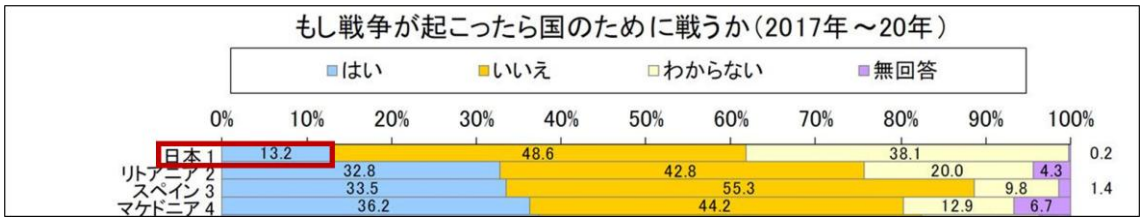
我々は「他人事」として自分たちの平和を当然視していたが、日本全体ではどのような認識か確認する。昨今の国際情勢を踏まえて、有事に巻き込まれる危険性を多くの日本国民は感じている。その一方で、戦後教育の影響や日米同盟があることにより、戦争自体が対岸の火事と捉えている側面があり、防衛意識については諸外国と比較しても非常に低い水準であるといえる。そのような背景もあり、世界価値観調査による「もし戦争がおこったら国のために戦うか」という問いに対して、「戦う」と答えた日本国民は僅か 13.2%という状況である。

【図表 5.1.1-1】日本が有事に巻き込まれる危険性認知



出典：内閣府 自衛隊・防衛問題に関する世論調査（2022 年 11 月）

【図表 5.1.1-2】戦争が起こった際に戦わないと答えた日本人



出典：プレジデントオンライン（2022 年 6 月）

5.1.2 認識の要因①「歴史的背景と社会的価値観」

防衛意識が希薄となっている要因の一つは、歴史的・社会的そして教育的な背景が複雑に絡み合った結果、日常生活や教育の場でそもそも安全保障や防衛の議論が十分になされていないということが上げられる。

第二次世界大戦後に「日本国憲法に戦争放棄と軍隊不保持を謳う第 9 条」が盛り込まれた。この条項は、戦争の悲惨さを経験した日本国民にとって、平和を維持するための重要な条項であるが、一方で戦争や軍事に対する忌避感を日本国民に強く植え付ける結果となっている。

「戦後の平和教育」では、平和主義が強調され、戦争の悲惨さや平和の重要性が教えられてきた。特に、学校教育においては、戦争の悲惨さを伝えることが重視され、防衛意識の醸成が後回しにされている傾向がある。また、戦後に制定された教員の「政治的中立」の徹底により、教育の場で深く戦争や防衛について深く議論されることがない。

多くの日本国民は、国の防衛について教育の場で取り上げるべきと考えているものの、そのような背景のもと、現在まで教育の場で積極的に取り上げる状況には至っておらず、文部科学省が掲げる学校教育目標においても、戦争・防衛に対する内容は特段記載がない状況である。

【図表 5.1.2-1】国の防衛について教育の場で取り上げる必要があるか

（2）国の防衛について教育の場で取り上げる必要があることの考え

問 12. あなたは、国の防衛について教育の場で取り上げる必要があると思いますか。（○は 1 つ）

	令和 4 年 11 月
取り上げる必要がある（小計）	89.3%
・取り上げる必要がある	47.8%
・どちらかといえば取り上げる必要がある	41.4%
取り上げる必要はない（小計）	9.3%
・どちらかといえば取り上げる必要はない	6.6%
・取り上げる必要はない	2.7%

出典：内閣府 自衛隊・防衛問題に関する世論調査（2022 年 11 月）

【図表 5.1.2-2】安全教育目標

幼稚園	日常生活の場面で、危険な場所、危険な遊び方などが分かり、安全な生活に必要な習慣や態度を身に付けることができるようにする。また、災害時などの行動の仕方については、教職員や保護者の指示に従い行動できるようにするとともに、危険な状態を発見したときには教職員や保護者など近くの大人に伝えることができるようにする。
小学校	安全に行動することの大切さや、「生活安全」「交通安全」「災害安全」に関する様々な危険の要因や事故等の防止について理解し、日常生活における安全の状況を判断し進んで安全な行動ができるようにするとともに、周りの人の安全にも配慮できるようにする。また、簡単な応急手当ができるようにする。
中学校	地域の安全上の課題を踏まえ、交通事故や犯罪等の実情、災害発生のメカニズムの基礎や様々な地域の災害事例、日常の備えや災害時の助け合いの大切さを理解し、日常生活における危険を予測し自他の安全のために主体的に行動できるようにするとともに、地域の安全にも貢献できるようにする。また、心肺蘇生等の応急手当ができるようにする。
高等学校	安全で安心な社会づくりの意義や、地域の自然環境の特色と自然災害の種類、過去に生じた規模や頻度等、我が国の様々な安全上の課題を理解し、自他の安全状況を適切に評価し安全な生活を実現するために適切に意思決定し行動できるようにするとともに、地域社会の一員として自らの責任ある行動や地域の安全活動への積極的な参加等、安全で安心な社会づくりに貢献できるようにする。

出典：文部科学省「「生きる力」をはぐくむ学校での安全教育」を基に作成（2019 年 3 月）

5.1.3 認識の要因②「安全保障環境と原体験不足」

次に大きな要因となっているのが、アメリカとの安全保障条約への依存である。憲法 9 条による武力放棄のため、日本は長年アメリカの軍事力に依存しており、自国の防衛に対する意識が低下している。日本国民が「有事の際に戦わない」という意識を持っているのも、何かあればアメリカが防衛してくれるという意識が根底にあるものと推察される。

また、原体験が不足しているということも大きく影響している。日本は中国やアメリカなどに挟まれた地理的特徴はあるが、島国のため他国からの侵略を受けにくいということもあり、第二次世界大戦以降、諸外国からの侵略や戦争に巻き込まれるといったことが起こっていない。周囲を海に囲まれているため、直接的な軍事的脅威を感じにくいという側面もある。

加えて日本では、徴兵制を採用していないため、徴兵制を通じた軍事訓練や、国防の重要性を直接体験する機会が不足している。現在世界では 60 か国以上の国々が徴兵制を採用しており、徴兵制度を採用している国の多くが国民の防衛意識が高くなっている傾向にある。

【図表 5.1.3-1】徴兵制度導入国一例

国名	徴兵年齢	期間	もし戦争が起こったら国のために戦うか	備考
日本	-	-	13.2%	徴兵制度なし
韓国	18歳～30歳	約18～22か月	67.4%	男性のみ徴兵、女性は志願制
スイス	18歳以上	約4か月	59.9%	男性徴兵、女性は志願制
フィンランド	18歳以上	約6～12か月	74.8%	男性のみ徴兵
ノルウェー	18歳～44歳	約12～15か月	87.6%	男女ともに徴兵
ロシア	18歳～27歳	約1年	68.2%	男性のみ徴兵
エジプト	19歳～34歳	約1～3年	83.9%	男性のみ徴兵
トルコ	18歳～40歳	約12～15か月	76.4%	男性のみ徴兵
マレーシア	18歳以上	約3か月	79.0%	男女ともに無作為選抜制
タイ	21歳以上	約2年	67.7%	男性のみ徴兵、くじ引きで選抜

出典：公務員総研「世界主要各国の徴兵制についてまとめ」を基に作成（2022 年 5 月）

5.2 日本国民の意識変容

日本国民の防衛意識の希薄さは第二次世界大戦以降から長年にわたり蓄積されたものであり、一朝一夕では解決できない問題である。

一方で混迷を極める国際情勢において、これまでのように長期的な平和が続くとは断じきれない状況でもあり、時間はかかるかもしれないが、我々は安全保障に対するリテラシーの向上に向けて、一歩ずつ取り組む必要性を感じている。

5.2.1 子供から始める意識変容

リテラシーの向上は、一朝一夕では解決できない問題であるため、我々は子供から防衛意識を向上させることが有効ではないかと考えた。とりわけ、一定程度物事の分別がつく義務教育の最終段階である中学生をターゲットとすることが効果的であると思われる。子供は、将来の社会を支える重要な存在であり、また大人と比較して、比較的柔軟に物事を受け入れられるためである。教育の場を活用した安全保障リテラシー向上の取り組みが子供から安全保障に対する地盤を築いていき、大人へも波及させていくことを目指す。それらを実現することによって、我々が中長期的に目指す日本社会は、「子供とニュース（政治・経済・世界情勢）を分かり合える、話し合える環境」の構築である。

5.3 安全保障リテラシー向上に向けた提言

安全保障リテラシーの向上に向けて、我々は学校教育において「本質を見抜ける力の醸成」

「有権者教育のさらなる充実」が必要であると考える。

まず一点目の「本質を見抜ける力」は日本の安全保障・防衛を考えるにあたり、最も重要な能力であると考えている。これまで述べたように、現代の国際情勢は非常に複雑で、多くの要因が絡み合っており、地政学的な対立、経済的な競争、テロリズム、サイバー攻撃など、多岐にわたる脅威が存在する。これらの脅威の要因を理解し、本質を正確に見抜くことで、適切な対応策を講じることができる。また、抑止力の効果的な運用においても、重要な力である。抑止力を効果的に運用するためには、相手国の意図や能力を正確に評価することが重要であり、相手意図を過小評価したり、誤解したりすると、抑止が失敗し、紛争が発生するリスクが高まる。それは、外交についても同様である。安全保障は一国だけで達成できるものではなく、他国との協力が不可欠である。効果的な外交を展開するためには、相手国の立場や利益を正確に理解することが重要となる。このように安全保障を考えるうえでは、一つの事象を一側面だけで判断するのではなく、その裏にある意図や本質を見抜くことが極めて重要である。

二点目の「有権者教育のさらなる充実」については、民主主義の日本において自らの意思を反映させる貴重な方法が選挙であるためである。2014 年の国政選挙と比べ、2021 年の国政選挙では若年層世代を含め、投票率は改善しているものの、依然として低調な水準が続いている状況である。

【図表 5.3-1】衆議院議員選挙における投票率の推移

(%)

年	S.42	S.44	S.47	S.51	S.54	S.55	S.58	S.61	H.2	H.5	H.8	H.12	H.15	H.17	H.21	H.24	H.26	H.29	R.3
回	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49
10歳代																		40.49	43.23
20歳代	66.69	59.61	61.89	63.50	57.83	63.13	54.07	56.86	57.76	47.46	36.42	38.35	35.62	46.20	49.45	37.89	32.58	33.85	36.50
30歳代	77.88	71.19	75.48	77.41	71.06	75.92	68.25	72.15	75.97	68.46	57.49	56.82	50.72	59.79	63.87	50.10	42.09	44.75	47.13
40歳代	82.07	78.33	81.84	82.29	77.82	81.88	75.43	77.99	81.44	74.48	65.46	68.13	64.72	71.94	72.63	59.38	49.98	53.52	55.56
50歳代	82.68	80.23	83.38	84.57	80.82	85.23	80.51	82.74	84.85	79.34	70.61	71.98	70.01	77.86	79.69	68.02	60.07	63.32	62.96
60歳代	77.08	77.70	82.34	84.13	80.97	84.84	82.43	85.66	87.21	83.38	77.25	79.23	77.89	83.08	84.15	74.93	68.28	72.04	71.38
70歳代以上	56.83	62.52	68.01	71.35	67.72	69.66	68.41	72.36	73.21	71.61	66.88	69.28	67.78	69.48	71.06	63.30	59.46	60.94	61.90
全体	73.99	68.51	71.76	73.45	68.01	74.57	67.94	71.40	73.31	67.26	59.65	62.49	59.86	67.51	69.28	59.32	52.66	53.68	55.93

出典：総務省 国政選挙の投票率の推移について（2021 年）

5.3.1 本質を見抜ける力の醸成

本質を見抜ける力を醸成する具体的方法を検討するにあたって、中学校の生徒らが社会の諸問題について意見を交わす「社会討論会」を企画・実行している飯島知明教諭にヒアリングを行った。飯島教諭は多面的・多角的な視点を身に着けることが大事との観点で NIE[10]

10 Newspaper in Education。学校などで新聞を教材として活用する教育活動。

に積極的に取り組んでおり、同様にNIEを重視している中学校に声をかけ、複数の中学校と12 年にわたり社会討論会を実施している。社会討論会はこれまで「集団的自衛権の是非」「日本のエネルギー（原発再稼働の是非)」「戦後70年の節目に考える日本の安全保障（憲法改正の是非)」等のテーマで討論を行っており、学生同士で闊達な意見交換が行われている。

討論会・ディベートは、単にその情報を受け取るだけでなく、その情報の信頼性や妥当性を評価する必要があり、例えば、ある主張が提示された場合、その根拠や証拠を検討し、矛盾点や弱点を見つけ出す必要がある。また、異なる視点を理解し、受け入れることが求められるため、反対の立場を取る相手の意見を理解し、その上で自分の意見を再構築することで、柔軟な思考が促進される。本質を見抜く力を醸成するにあたり、この「社会討論会」や「ディベート」が有効であると考えた。

【図表 5.3.1-1】社会討論会の様子

出典：産経ニュース（2024年8月29日付）

実際に我々も社会討論会に参加したが、それぞれの中学校の生徒が社会問題に対して時間をかけて考察し、独自の観点で提言を実施していた。提言の内容が示唆に富んだものであったことに加え、その提言に対して別の切り口での意見や、深堀するための質問等、お互いの理解が深まる討論を展開していた。

討論会の中で我々からも安全保障に関して現在の国際情勢と日本が置かれている状況について発表を行った。興味を持って聞いていただき、「台湾有事が実際に行った場合の対応をどうするのか」「日本が有事に巻き込まれた場合、本当に自衛できるのか」等の鋭い質問があった。今回参加していた中学生は、特に日常生活で安全保障や防衛については触れていないと思うが、これまで社会討論会で侃侃諤諤の議論を行ってきたことで、受け入れる素地が培われていたと推察される。

このような場で安全保障をテーマとした発表が「安全保障について知ってもらう」非常に

有意義な機会であると認識した。来年度以降も本社会討論会は継続実施予定であるため、グローバル適塾生も継続的に参加・発表できる枠組みを作成することを検討している。

【図表 5.3.1-2】社会討論会塾生参加の様子（2025 年 2 月 2 日実施）

一方で社会討論会の継続に向けては課題も存在している。飯島教諭は社会討論会をボランティアで実施しているが、昨今教育の過重労働が社会問題化している現状もあり、本取り組みを担う次世代の人材不足が懸念されている。また、本取り組みを大阪府ひいては全国に展開するとしてもボランティアの協力のみでは限界がある。さらに、社会討論会を実施するにあたっては一定程度の社会問題に対する知識が必要となるが、先ほど述べたように過重労働が問題視されている中、自己研鑽を行う時間も限られている現状がある。

社会討論会やディベートについては安全保障の観点以外でも、子供にとって有意義な教育課程である。論理的批判思考の育成やコミュニケーションスキルの向上、そして社会的責任の向上にもつながる。これらの取り組みを教諭の自発的なものとして終わらせるのではなく、国・自治体が主体となり、全国に展開するべきである。多忙を極める教諭が本取り組みを行うための体制整備も必要であり、必修科目に組み込む等の対応も必要であると考える。

5.3.2 有権者教育のさらなる充実

前述したように、我が国日本において、政治家になる方法以外で自分自身の意思を国家に反映させる唯一の方法は選挙であり、日本の安全保障・防衛の在り方については選挙によって決まるといっても過言ではない。各党においても安全政策については必ず政党の方針を

定めており、選挙を始めとする政治に正しく向き合うことで安全保障に対するリテラシーも向上すると考える。そのためには教育の場において責任ある有権者として判断できる力を養う必要があり、既存政党の成り立ちや各政党の主義主張等のより踏み込んだ内容の教育の実施を行うべきと考える。

そこで今回、我々は安全保障に力を入れている自民党 大阪８区支部長である高麗啓一郎氏にヒアリングを行った。日本国民の安全保障に対しての現状や教育現場の在り方について現状を知ることができ、選挙公約だけでは見えない政策背景や安全保障に対する考え方を深く理解することが出来た。安全保障のリテラシー向上に向けては、草の根活動の重要性や日本が抱えている課題（憲法９条の在り方等）についてしっかりと議論をする場を醸成することが必要とのご示唆も頂いた。有権者教育の重要性を認識するとともに、このように政治家との直接の対話を行うことも効果の高い手段であると感じた。

【図表 5.3.2-1】自民党 大阪８区支部長ヒアリングの様子

諸外国においては、教育学校教育の一環として、政治教育が充実しており、選挙前には模擬選挙の実施や、今回我々が行ったように政治家と若年層が直接対話できるイベント等を実施し、若者への選挙に対する意識向上、政治への関心を高めている。これらの取り組みは日本でも取り入れることができる部分があると考える。

【図表 5.3.2-2】各国の取り組み

国名	取り組み内容
スウェーデン	学校での政治教育の充実、政党による若者向けイベントの開催
ノルウェー	学校や地域コミュニティでの政治討論会の開催
オーストラリア	投票の義務化、学校での選挙教育プログラム
カナダ	選挙管理委員会による教育プログラム

日本の教育では、戦後の「平和教育」の系譜の中で、国際協力や国際平和を希求するベクトルで構成されており、また教諭の政治的中立性の観点が根付いているため、教科書への既存政党の主張等の掲載は難しい。また、政党については選挙結果により変更となるため、教科書を都度変更することは現実的に不可能である。

そのため、教科書による政治教育の実施ではなく、新聞を活用した教育（NIE）の実施や既存政党の主張をまとめた資料等を活用した有権者教育を行うことを提言する。学校教育の中で政治に対する関心を高め、政治を「大人の問題」として捉え、自分事ではないという若年層の意識を変容させる。

教諭毎に独自の資料の作成や NIE を実施するとなると相応の負担となるため、マスメディアが主体となり、題材の提供を行うことが効果的であると考える。現在グローバル適塾 23 期・安全保障グループメンバーが出版社にアプローチを行っており、例えばひと月に一度有権者教育の題材（今月の政治トピックスや各政党の主張等）を発行できる仕組みを作成できないか検討中である。

5.3.3 結論・まとめ

安全保障のリテラシー向上は一足飛びに行うことはできない。学校教育の場で安全保障に関する取り組みを実施することで、日本全体のリテラシー向上に繋がると我々は確信している。そのために、今回提言した社会討論会やディベート、有権者教育の実施が行いやすい環境作りを我々も引き続き検討・実施していく考えである。

安全保障のリテラシー向上に向けては様々なアプローチ方法があると思うが、今回の提言によって、少しでも「子供とニュース（政治・経済・世界情勢）を分かり合える、話し合える環境」が構築され、安全保障が当たり前に語られる日本となることを切に願う。

【図表 5.3.3-1】提言内容

#	提言内容	詳細
1	本質を見抜ける力の醸成	• 新聞を活用した教育（NIE）の全国的な展開。 • 現在茨木市の教員が中心となって行っている “社会討論会” の必修化
2	有権者教育のさらなる充実	• 新聞を活用した教育（NIE）の実施 • 既存政党の主張をまとめた資料等を活用した有権者教育の実施

終わりに

2025 年 1 月 20 日、第二次トランプ政権が発足した。

第二次トランプ政権は、アメリカ第一主義を一層強固なものとし、国際的な安全保障環境に大きな影響を与え、また米中関係の緊張も深まるものと想定される。トランプ政権は「中国は我々の最大の競争相手である」とし、安全保障政策においても対抗姿勢を強化することが示唆される。この結果、南シナ海や台湾周辺の軍事的緊張が高まり、地域の不安定化を招くおそれがある。さらにトランプ政権は、アメリカ中心の外交政策を継続し、国際的な協力よりもアメリカの利益を最優先する姿勢を鮮明にしている。これにより、世界秩序は一層不安定化し、各国の安全保障に新たな課題を引き起こすことが懸念される。

貿易政策においては、トランプ政権は保護主義的な傾向を強化することを明らかにしており、対中強硬姿勢の一環としての中国に対する追加関税を課し、これに反発した中国は対米報復関税を発動するなど貿易戦争の緊張はより高まっている。

さらには、第二次トランプ政権は普遍的価値を共有しているはずのカナダにまで追加関税を課すことを明言した（本提言を執筆している 2025 年 2 月現在、両国間取引により左記追加関税は適用延期となっている）。本来、アメリカとカナダは歴史的な同盟国であり、互いに強固な経済的関係を築いているにもかかわらず、トランプ政権のこのような保護主義的な政策は両国間の関係に亀裂を生じさせる可能性がある。この経済的圧力を外交手段とする手法は、その他各国にも用いられることが想定され、各国との同盟関係の信頼性が揺らぐこととなり、安全保障政策への影響が懸念される。

日本に対しては、防衛費負担の増額および自衛隊の強化や防衛費の増加要求に加え、貿易政策においても圧力がかかると予想される。日本製品に対する関税の引き上げを示唆することも考えられ、日本企業はアメリカ市場での競争が厳しくなり、サプライチェーンの再考を迫られることになる。

また、サイバーセキュリティに関しても国家間連携は重要性を増しており、日本では、総務省が主導し、二国間・多国間の協力を強化するための取り組みを進めている。トランプ政権も国際的なサイバーセキュリティの強化を重視しており、その結果として日本に対してもアメリカ主導のサイバー防衛体制への参加を求める可能性があり、これらに向けた情報共有や共同訓練が重要となる。このように、米中間の緊張が高まる中においての国際的な連携強化は不可欠であり、日本は自国のサイバー戦略を見直すことが求められる。

我々は、本提言において自主自律的な安全保障対策の重要性について述べた。この提言は、第二次トランプ政権の発足を受け、混迷を深める世界情勢において、日本の安全保障を向上させるのみならず、国際的な安定と秩序の確立にも寄与するものであると考えている。

我々はグローバル適塾での学びを終えたのちも企業人として安全保障に貢献できる活動を続けていくが、国家、企業、国民各位にも、本提言の内容を真摯に受け止め、実行に移し

ていただきたい。

　各自が積極的に行動することで、より良い未来を築き上げ、我々の安全保障環境が一層強化されることを祈念してやまない。

謝辞

本提言を策定するにあたり、半年間を通じて多大なご指導・ご助言を賜った神戸大学大学院法学研究科 簑原俊洋教授に心より感謝申し上げます。また、談論風発講座の開講時に安全保障に関するご講話を賜った三紀ホールディングス㈱ 杉野利幸代表取締役社長をはじめ、我が国を取り巻く安全保障環境やその対応状況についてご講話を賜った自衛隊大阪地方協力本部 深草貴信本部長、国内フィールドワークでの意見交換をご快諾頂いた陸上自衛隊第 15 旅団、海上自衛隊第 5 航空群、航空自衛隊南西航空方面隊、自衛隊沖縄地方協力本部、在日米軍キャンプフォスター、沖縄経済同友会の皆様、掃海艇の乗船体験に我々を受け入れて下さった海上自衛隊阪神基地隊の皆様、海外フィールドワークでの意見交換先をご紹介いただいた台北駐大阪経済文化弁事処ならびに我々を受け入れて下さった国防安全研究院、米国在台湾協会、日本台湾交流協会、台湾日本関係協会、能率集團、中國鋼鐵股份有限公司の皆様、救難飛行艇のご紹介・工場見学をお受けいただいた新明和工業㈱の皆様、その他ご講話や意見交換にお時間を割いてくださった全ての方々に深謝の意を表します。

最後に、塾生を支えて頂いたグローバル適塾運営協議会 山本香主任調査役及び、事務局の皆様、そして、グローバル適塾参加という機会を与えて下さった塾生各々の企業の皆様に深くお礼申し上げます。

参考文献・参考資料

【参考文献】

- ◆ 本郷和人・簑原俊洋『「外圧」の日本史 白村江の戦い・蒙古襲来・黒船から現代まで』朝日新書,2023 年
- ◆ 簑原俊洋『大統領から読むアメリカ史』第三文明社,2023 年
- ◆ 松田康博、福田円、石井正文、本松敬史、沈明室、黒﨑将広、尾上定正、小原凡司河上康博、武居智久、西山淳一、兼原信克『「台湾有事」は抑止できるか:日本がとるべき戦略とは』勁草書房,2024 年
- ◆ 喬良、王湘穂『超限戦 21 世紀の「新しい戦争」』KADOKAWA,2020 年
- ◆ 防衛省『令和 6 年版防衛白書』
- ◆ 外務省『令和 6 年版外交青書』

【参考資料】＜参考 URL の閲覧期間は、2024 年 10 月～2025 年 2 月＞

《第 1 章》

- ◆ 国際通貨基金　世界経済見通し 2025 年 1 月改定版　地域別の成長率予測（2024 年 12 月）
  https://www.imf.org/ja/Publications/WEO/Issues/2025/01/17/world-economic-outlook-update-january-2025
- ◆ 日本経済新聞　「アジア安保、米関与で維持」拡大 ASEAN 国防相会議　衝突抑止へ中国とも対話_2024 年 11 月 22 日付（2024 年 12 月）
  https://www.nikkei.com/article/DGKKZO84962360R21C24A1PD0000/
- ◆ U.S. Energy Information Administration　南シナ海における LNG 貿易量（2025 年 1 月）
  https://www.eia.gov/international/content/analysis/regions_of_interest/South_China_Sea/south_china_sea.pdf
- ◆ 国際通貨基金　購買力平価（2024 年 12 月）
  https://www.imf.org/external/datamapper/PPPGDP@WEO/CHN/USA/JPN
- ◆ 読売新聞　中国「一帯一路」会議から見えてきたもの_2017 年 5 月 29 日付（2024 年 10 月）
  https://www.yomiuri.co.jp/fukayomi/20170525-OYT8T50024/2/
- ◆ 産経新聞　中国、海洋覇権へ「列島線」突破狙う　米国、海軍力増強で対応_2019 年 1 月 1 日付（2024 年 12 月）
  https://www.sankei.com/article/20190101-5OLSKFKTUNNLDJY6PO6PSGDZ44/
- ◆ 防衛省　南シナ海情勢(中国による地形埋立・関係国の動向)（2024 年 11 月）
  https://www.mod.go.jp/j/surround/pdf/ch_d-act_b_2023.pdf

◆ 日テレ NEWS NNN　南シナ海で中国海警局の船が“放水”フィリピン側が映像公開（2024 年 10 月）
https://news.ntv.co.jp/category/international/b9c6e513d46141158454ee32a1378924

◆ 防衛省　2024 年 10 月の中国による台湾周辺での軍事演習について（2025 年 1 月）
https://www.mod.go.jp/j/surround/pdf/ch_exchange_202409.pdf

◆ Defense Priorities Foundation　誰が味方で、なぜそれが重要なのか（2025 年 1 月）
https://www.defensepriorities.org/explainers/who-is-an-ally-and-why-does-it-matter/

《第２章》

◆ 日本経済新聞　TSMC 熊本工場が量産開始　国内半導体供給網の整備進む_2024 年 12 月 27 日付（2025 年 1 月）
https://www.nikkei.com/article/DGXZQOUC274RZ0X21C24A2000000/

◆ トヨタ　トヨタ取り巻く主要論点　株主質疑（2024 年 11 月）
https://toyotatimes.jp/toyota_news/shareholders_2022/002.html

◆ 農林水産省　令和 5 年度食料自給率（2024 年 12 月）
https://www.maff.go.jp/j/zyukyu/zikyu_ritu/attach/pdf/012-9.pdf

◆ 経済産業省　第 7 次エネルギー基本計画（2025 年 1 月）
https://www.enecho.meti.go.jp/committee/council/basic_policy_subcommittee/2024/067/067_006.pdf

◆ 経済産業省　Ouranos Ecosystem（ウラノス・エコシステム）（2024 年 12 月）
https://www.meti.go.jp/policy/mono_info_service/digital_architecture/ouranos.html

《第３章》

◆ Microsoft　ウクライナにおけるロシアのサイバー攻撃活動の概要（2024 年 12 月）
https://www.microsoft.com/ja-jp/security/security-insider/intelligence-reports/special-report-ukraine

◆ 総務省　サイバー攻撃関連の通信数の推移（2024 年 12 月）
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/pdf/00zentai.pdf

◆ 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（2025 年 1 月）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

◆ 情報処理推進機構　情報セキュリティ 10 大脅威 2025（2025 年 2 月）
https://www.ipa.go.jp/security/10threats/10threats2025.html
◆ 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　調査報告書（2025 年 2 月）
https://www.gh.opho.jp/pdf/report_v01.pdf
◆ ウォールストリートジャーナル　中国系ハッカー、米政府関係者の通話記録入手か（2024 年 12 月）
https://jp.wsj.com/articles/china-hack-enabled-vast-spying-on-u-s-officials-likely-ensnaring-thousands-of-contacts-c86bf125
◆ ブルームバーグ　米でサイバー攻撃被害広がる、財務省にも侵入－中国政府が支援の疑い（2025 年 2 月）
https://www.bloomberg.co.jp/news/articles/2025-01-01/SPDR70T0G1KW00
◆ 経済産業省　IT 人材育成の状況等について（2025 年 1 月）
https://www.meti.go.jp/shingikai/economy/daiyoji_sangyo_skill/pdf/001_s03_00.pdf
◆ 経済産業省　中堅・中小企業のセキュリティ人材の現状・課題（2024 年 12 月）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/cyber_human/pdf/003_03_00.pdf
◆ 三菱 UFJ リサーチ&コンサルティング　中小企業における情報セキュリティ対策の最新動向（2025 年 2 月）
https://www.murc.jp/wp-content/uploads/2024/05/seiken_240516_01.pdf
◆ 台灣人工智慧實驗室　情報操縦者の足跡とその手法（2025 年 2 月）
https://ailabs.tw/zh/tw_press/

《第４章》

◆ 外務省　海外在留邦人数調査統計（2024 年 12 月）
https://www.mofa.go.jp/mofaj/files/100436737.pdf
◆ 日本経済新聞　台湾、シェルター10 万カ所整備（2024 年 12 月）
https://www.nikkei.com/article/DGKKZO67257680Y2A221C2EA1000/

◆ 内閣府　令和 5 年度 企業の事業継続及び防災の取組に関する実態調査（2025 年 1 月）
https://www.bousai.go.jp/kyoiku/kigyou/pdf/chosa_240424.pdf
◆ 消防庁　避難・救援・武力攻撃災害への対処等の国民保護措置（2025 年 1 月）
https://www.fdma.go.jp/publication/hakusho/r6/items/part3_section1.pdf
◆ 東京都　避難の指示（2025 年 1 月）

https://www.bousai.metro.tokyo.lg.jp/taisaku/torikumi/1000063/1000418.html
◆ 東京商工リサーチ　「企業の台湾有事の想定」アンケート調査（2024 年 12 月）
https://www.tsr-net.co.jp/data/detail/1198405_1527.html

《第５章》

◆ 内閣府　日本が有事に巻き込まれる危険性認知（2024 年 10 月）
https://survey.gov-online.go.jp/r04/r04-bouei/gairyaku.pdf
◆ プレジデントオンライン　もし戦争が起こったら国のために戦うか（2024 年 11 月）
https://president.jp/articles/-/58391?page=1
◆ 文部科学省　安全教育の目標（2024 年 12 月）
https://www.mext.go.jp/component/a_menu/education/detail/__icsFiles/afieldfile/2019/04/03/1289314_02.pdf
◆ 公務員総研　世界主要各国の徴兵制についてまとめ（2025 年 1 月）
https://koumu.in/articles/220512a
◆ 総務省　衆議院議員総選挙における年代別投票率（抽出）の推移（2024 年 12 月）
https://www.soumu.go.jp/main_content/000255967.pdf
◆ NIE（Newspaper in Education）（2025 年 1 月）
https://nie.jp/about/

グローバル適塾　第２３期　安全保障グループ　名簿

塾生

尾 上 和 也	有限責任あずさ監査法人
大塚三智子	株式会社ＮＴＴドコモ
田 窪 遼 也	大 阪 ガ ス 株 式 会 社
田 口 幹 也	株 式 会 社 大 林 組
吉 山 麻 子	ダイキン工業株式会社
大 西 宏 典	東洋テック株式会社
山 本 潤 一	株式会社日立製作所
福 島 健 吾	株式会社ミライト・ワン
森　田　健	鹿 島 建 設 株 式 会 社
小 宮 大 輔	株式会社りそな銀行

学会担任講師

簑 原 俊 洋	神戸大学大学院法学研究科 教授

事務局

市 原 真 人	グローバル適塾運営協議会 事務局長
山　本　香	グローバル適塾運営協議会 主任調査役