第８２２号

令和５年11月１日

公益社団法人　安全保障懇話会
発行所　東京都新宿区若松町１８－３
電話　３２０２－８６３１　㈹

安全保障を考える

「重要インフラへの脅威の増大」への対応の一考察
－電力システムを題材として－

研究班　中　野　義　久

はじめに

昨年末に策定されたいわゆる「戦略三文書」及び５月に成立した「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（以下「経済安全保障推進法」という）」において、重要インフラに対する脅威の増大に対しては、外交・防衛政策に加え、経済政策が連携して対応することとされた[1]。また防衛省・自衛隊の役割として、重要インフラに対する攻撃には「実効的に対処」するとされている。重要インフラは、災害や事態対処において公益的な役割を担っているため、脅威の増大への対処のためには、様々な状況において脅威を排除してそれぞれのインフラとしての機能発揮を確保することが必要である。そのため、重要インフラへの脅威の増大に対して経済安全保障、外交と連携しつつ、防衛省・自衛隊の役割としての「実効的に対処」のあり方について考察することが必要である。

[1] 「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）3-6頁。また「サイバーセキュリティ基本法（平成二十六年）」において重要社会基盤事業に関するサイバーセキュリティの確保についても規定されている。

重要インフラは同法第 50 条において、「国民生活及び経済活動の基盤となる役務であって、その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もの」として 14 分野の特定社会基盤役務（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）が指定されている。その中でも「電力」はそれら重要インフラの多くの基盤でもあるため、安全保障上の重要な要素であると言える。このような観点から、本稿では「電力」を例として重要インフラへの脅威の対処を検討する。そのため先ず、電力システム[2]を取り巻く環境を明らかにした後、大規模停電に関する事例分析を通じて電力システムの安全保障上の脆弱性を案出し、これを踏まえて電力システムに対する脅威への外交・防衛・経済的手段による対処を考察する。なお、その対処の多くは電力システム事業者自らが平時において脆弱性の改善の観点から行うものであり、本稿においては当初、電力システムについて分析し、これに対して防衛省・自衛隊が連携して果たすべき役割について考える。

１　重要インフラとしての電力システムの位置付け

重要インフラは、防衛、経済そしてサイバーの観点から以下のような位置付けにある。先ず「国家安全保障戦略」によれば、「重要インフラへの脅威の増大」は、「従来必ずしも安全保障の対象と認識されていなかった課題」であったが、その「対応も安全保障上の主要な課題となってきている。」また「相対的に露見するリスクが低く、攻撃者側が優位にあるサイバー攻撃」による「重要インフラの機能停止や破壊、他国の選挙への干渉、身代金の要求、機微情報の窃取等は、国家を背景とした形でも平素から行われている」とされている。

その対応にあたって「国家防衛戦略」では、「大規模テロやそれに伴う原子力発電所を始めとした重要インフラに対する攻撃、地震や台風等の大規模災害」は「国民の生命・身体・財産に対する深刻な脅威であり、我が国として国の総力をあげて全力で対応してい

---

[2] 電力システムとは、電力を需要家（消費者）の受電設備に供給するための、発電・変電・送電・配電を統合したシステムであるが、我が国では、東京電力パワーグリッド（東京電力から分割発足）などの 10 社の「一般送配電事業者」がそれぞれ電力系統をもち、沖縄電力を除いた 9 社の電力は近隣のいずれかの電力系統と接続されるが、東西間で電気に 50Hz と 60Hz の二種類の周波数の違いがあるため、電力の融通には制約がある。

く必要がある」としている。そして「防衛省・自衛隊においては、抜本的に強化された防衛力を活用し、警察、海上保安庁、消防、地方公共団体等の関係機関と緊密に連携して、

◆大規模テロや重要インフラに対する攻撃に際しては実効的な対処を行い、

◆大規模災害等に際しては効果的に人命救助、応急復旧、生活支援等を行う」ため、「平素から関係機関と連携態勢を構築しておくことが必須」であり、「地方公共団体やインフラ事業者を含む関係機関と共に、各種計画等を踏まえつつ、その実効性を担保するために、総合的な訓練を実施する」としている。また

◆「サイバー領域においては、諸外国や関係省庁及び民間事業者との連携により、平素から有事までのあらゆる段階において、情報収集及び共有を図るとともに、我が国全体としてのサイバー安全保障分野での対応能力の強化を図ることが重要である」としている。

一方で経済安全保障の観点からは、①重要物資や原材料のサプライチェーンの強靭化、②基幹インフラ機能の安定性・信頼性の確保に関する制度整備がなされた[3]。電力は②の「特定社会基盤役務」として、安定的な機能発揮の確保のための設備の導入・維持に係るサプライチェーンリスクの低減・排除が規定されている。またその燃料の液化天然ガス(LNG)は①の「特定重要物資」とされて、入手先を分散させたり備蓄したりする動きを支援してサプライチェーンの強靭化を図り、安定供給を確保するとなっている。

また「サイバーセキュリティ戦略」では、重要インフラについて「任務保証」[4]を基礎として、更なるエンドユーザーへのサービスの確実な提供を意識したサプライチェーン全体の信頼性確保が求められている。

２　電力システムを取り巻く環境

上記の位置付けにある電力システムを取り巻く環境は次のように考えられる。

第一に、重要インフラ、特に電力システムに対する脅威は顕在化しつつある。現にロシアはウクライナに対する侵略ではサイバー攻撃のみならずミサイル攻撃等をもって電力

---

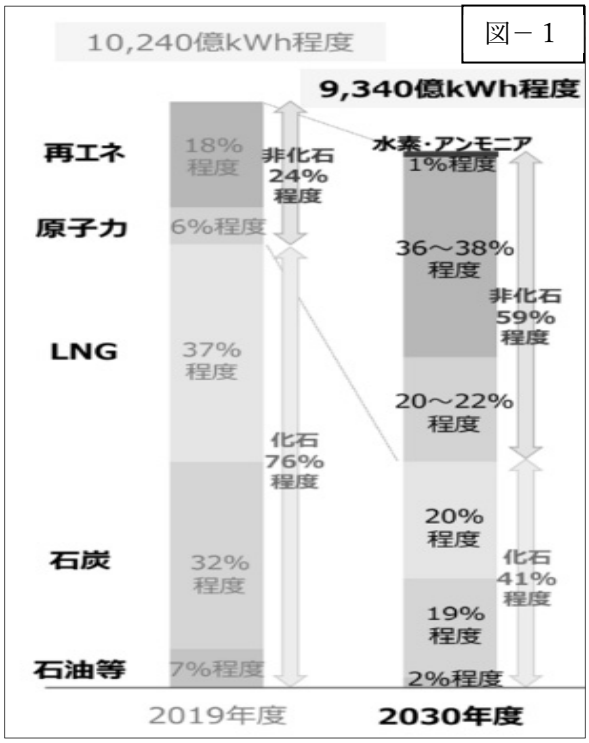
[3] 同法ではその他、③先端的な重要技術についての官民協力、④特許出願の非公開についても規定している。

[4] サイバーセキュリティ戦略(令和３年９月28日閣議決定)において示す、「企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方。」

インフラを集中攻撃し、変電所や原子力発電所を含む発電設備に被害を与えた[5]。加えて、「国際社会において急速に懸念が高まっている」中台情勢においても、台湾側の見積もりでは、中国は侵攻に際し戦略支援部隊が台湾軍の重要システムなどへのサイバー攻撃を実行すると考えられている[6]。

第二に、気候変動は全世界にとって重大な課題であるが、その対策の推進は電力システムに対する脅威を高めることにつながると考えられる。それは気候変動対策としての「脱炭素化」及び「電化」が進めば、電源としての電力システムの役割が高まっていくからである。脱炭素化の目標は 2030 年度において温室効果ガスを 2013 年度比で 46%削減、2050 年までにカーボンニュートラル実現である。そのため、温室効果ガス排出割合の高い電力部門では（図－1 参照）、2019 年現在と比較して、2030 年には省エネを一層進め（総発電量の抑制）、再生可能エネルギー（以下「再エネ」という）は倍増（約 4 割）するとともに、原子力については約 2 割まで拡大し、化石燃料による火力（LNG や石炭、石油等）は、その比率をほぼ半減させた電源構成となる[7]。また「脱炭素化」と同時にその電力を、EV 車への乗り換えやクーラーによる暖房のように、暮らしや経済活動に必要なエネルギー源として化石燃料から置き換える「電化」が進展する[8]。「電化」が進展すれば、電化された機械・施設等が増加し、その稼働に必要な電源を妨害するためのその供給源である電力への脅威が増加すると考えられるため、将来における電力システムへの脅威は増加する。

図－1



資源エネルギー庁作成

---

[5] 『日本経済新聞』2023 年 2 月 27 日。ロシア軍の攻撃対象は、当初は屋外にあり建屋などで守られていない変電所が中心であったが、被害の拡大を狙って、発電所へと攻撃対象を切り替えており、ウクライナ・エネルギー省によれば、２月時点で全体の 4 割に相当する電力設備・発電所が攻撃を受け、供給能力は半減した。

[6] 防衛省『令和 5 年版　防衛白書』92-94 頁。

[7] 資源エネルギー庁『第 6 次エネルギー基本計画』2021 年 10 月、33－41 頁。

[8] 産経新聞（電子版）「温室効果ガス実質ゼロへ「電化」加速　電源の「脱炭素化」と一体で」2021 年 3 月 28 日 08:00。

第三に、電力システムには、安定供給のためには、今後再エネの増加を考慮しても、日々の複雑な電力のバランス維持が必要である。発電の過程では天候気象を始め刻一刻と変化する条件を整合させる微妙な調整が必要であり、これが大規模停電の要因ともなる。それは電気の供給と需要が常に一致していないとその周波数が乱れ（同時同量の原則）、それを整合しないと電気の供給を正常におこなうことができなくなり、安全装置の発動によって発電所が停止し、場合によっては大停電におちいる危険があるからである。一方、再エネは天候等によって太陽光や風力の出力に変動があるため、柔軟な出力調整が可能である火力発電がそれを補うベースロード発電機能として、電力の需給バランスの調整を担わざるを得ない。今後再エネが増加しても、火力発電のこのような役割は引き続き必要である[9]。

以上のように電力システムは従来から経済活動の基盤であったが、現在その脅威は顕在化しているとともに、将来もさらに増大が予想される。さらにその発電機能は今後、再開が拡大する原子力発電を加えつつ、当面は火力発電が電力バランス調整機能としての役割を果たしてゆく。これらの条件を踏まえ、以下においては、大規模停電等の事例を検討して、電力の安定供給の確保が安全保障に及ぼす影響を考える。

3　電力システムの脆弱性と安全保障への影響

電力システムによる安定的な電力供給を考える上で、電力の安定供給の構成要素は、①発電設備の十分な確保（KW）、②送配電ネットワークの送電能力と強靭性確保、③燃料の十分な確保（KWh）である[10]。よって以下では①、②に関係する事例とともに、地域的な観点から電力供給の影響の最も大きい関東エリアでの大規模停電の可能性も併せて検討する[11]。

（1）　北海道胆振東部地震に伴う大規模停電（図－2 参照）

北海道胆振東部地域で最大震度 7 の地震が 2018 年 9 月 6 日 3 時 7 分に発生したが、これにより北海道全域において、3 時 25 分、日本で初めてとなる大規模停電（ブラックア

---

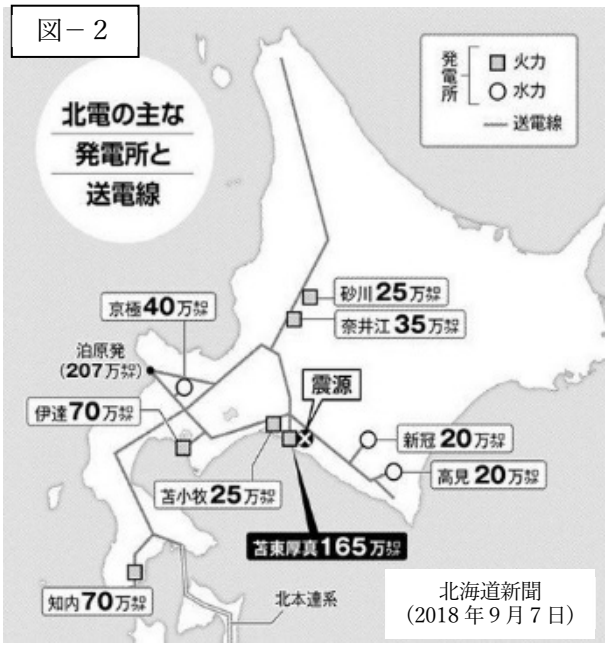
[9] 原子力発電は、経済性及び安定的な発電能力からベースロード電源とされ、今後の拡大が期待されている一方、技術的及び安全性の懸念の声もある。

[10] 竹内純子『電力崩壊』日経 BP、2022 年 45 頁。

[11] ③については後述する。

ウト）が発生した。その結果、最大約 295 万戸が停電し、復旧に数日を要したが[12]、本事例からは以下の点が重要である。

図－２



第一に、大規模地震による一ヶ所の発電所の停止がきっかけとなり、北海道の夏の日の出前の需要の低い時間にもかかわらず、北海道全土のブラックアウトを招いたことである。本事象は、地震による苫東厚真発電所の停止を直接要因として、電力システム全体の供給不足となった。道央に位置し発電需要の約半数を担っていた苫東厚真発電所（165 万 KW／総需要 308 万 KW）は地震の直接の影響を受け、2、4 号機（合計 116 万 KW）が停止した。これに他の水力や風力発電の停止が加って供給不足になったため、一部の地域で負荷遮断（地域的な停電による需要抑制）により需給を保つ努力をした。このような 18 分間の電力供給努力にもかかわらず、最終的には苫東厚真発電所 1 号機も停止し（34 万 KW）、北海道全域がブラックアウトとなった。

第二に、ブラックアウトからの復旧には数日（約 45 時間）を要した。通常の停電からの復旧のためには、停電エリア外部からの電気の供給で発電機を起動し、その電源供給の下、安定的に復旧するが、ブラックアウトからの復旧の場合には、ブラックスタートと呼ばれる特別な方法が必要となる。具体的には、地域内で発電機能を喪失しているため、ブラックスタート機能（始動のための電源の必要のない水力発電など）が付いた一部の発電機から、少しずつ周囲の発電機を起動させ、周波数を一定にしつつ供給と需要（停電解消）の拡大を進めていくため、綿密かつ長時間にわたる操作を要する。海外で発生した事例においても、状況は異なるものの復旧まで 11 時間から 26 時間程度を要している。

（２） 2019 年千葉台風被害（図－3 参照）

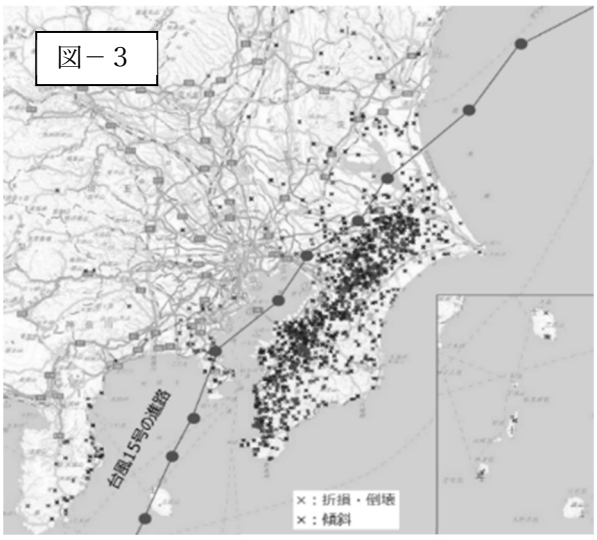
2019 年 9 月に上陸した台風 15 号は、電力システムの送配電機能に大きな被害をもたらした。特に千葉市では最大瞬間風速 57.5m/s を観測する記録的な暴風となり、停電被害は

[12] 本事例については、事実関係を「平成３０年度北海道胆振東部地震に伴う大規模停電に関する検証委員会最終報告(2018 年 12 月 19 日)」に基づく。

最大約 93 万戸で、千葉県を中心に停電が長期化し、その復旧には近年の停電被害の中では最大の約 280 時間を要した[13]。

本事例からは、広域にわたる配電設備の損傷による広域停電では、被害状況把握及びそれに基づく復旧の適格な見積もりが困難であったため、対処に時間を要したことが言える。そのため電力会社の発表では停電が解消しているエリアでも、個別の地域や住居などでは停電が解消されていないところがあるとして、いわゆる「隠れ停電」と報道された。

図－３



資源エネルギー庁作成

（３） 2022 年初の電力需給ひっ迫警報発令

2022 年 3 月 21 日に東京電力ホールディングスと東北電力管内において、初めての「電力需給ひっ迫警報」が発令され、広く節電が要請された。その原因は、①3 月 16 日の福島沖地震等による発電所の停止及び地域間連系線の運用容量低下、②真冬並みの寒さによる需要の大幅な増大、③悪天候による太陽光の出力大幅減のため再エネ出力不足、④冬の高需要期（1・2 月）終了に伴う発電所の計画的な補修点検による需要急増への対応の制約であった[14]。最終的には各種の電力供給増加策の他、大幅な節電（電力需要抑制）により、前日の見積もり以下の需要をまかなうことになったが、本件からは以下の点が重要である。

第一に、関東エリアでも大停電が発生する可能性があるということである。首都東京を中心とするエリアの電力需要は、4,800 万 KW とブラックアウトを発生させた北海道の 308 万 KW の十倍以上の規模であるが、それでも地震などの負の条件による一部の発電能力の停止などと、天候、気象の影響での予想外の需要・供給の増減の複合により、大規模な停電を発生させる可能性があると言える。

---

[13] 本事例については事実関係を、資源エネルギー庁『「台風」と「電力」～長期停電から考える電力のレジリエンス（2020 年 1 月 23 日）』に基づく。

[14]本事例については、「2022 年 3 月の東日本における電力需給ひっ迫について）」（資源エネルギー庁）2022 年 4 月 25 日に基づく。

第二に、電力ひっ迫の原因として、電力自由化による構造的な要因による電力の供給力低下を挙げる声もある[15]。これは電力自由化以降、発電事業者の経済合理的な判断の下で採算性が悪化する火力発電所は順次廃止されていたため、発電自体が供給力の低下傾向にある電源に依存し続ける状況となっているからである[16]。

（4） 大規模停電の要因と安全保障への影響

ここまでの検討から、ベースロード電源の計画外の機能停止、送配電網の広域にわたる被害からの復旧の遅延などが大規模停電を引き起こす要因であったと言える。ここから安全保障上の重要性としては、電力の安定供給は需要に応じた日々の微妙な出力バランス調整を基礎としているため、例えば、高需要期終了後の発電所の計画的な補修点検期間中（3 月や 9 月など）に、時期外れの猛暑や寒波に対応するため急遽発電量の増加を図った数個の発電所が何らかの原因で突然停止した場合、対処を誤ると最悪の場合には関東エリアであっても大規模な停電が発生する可能性があると言える。そしてその場合は、ブラックアウトにより電源喪失した電力システムを復旧するには数日を要するため、その間は通信・金融を始めとする他の重要インフラの機能発揮も制限され、国民生活そして安全保障に重大な影響を及ぼす。

4 電力システムへの脅威とその対処

ここまで電力システムの安定供給の条件について検討したが、以下においては、電力システムへの脅威について具体的に考察しその対処の方向性を検討する。安定的な電力供給を妨げる安全保障上の具体的脅威としては、(1)事前の予測が困難な大規模災害、(2)サイバー攻撃や大規模テロやそれに伴う原子力発電所を始めとした重要インフラに対する攻撃、(3)そして国際安全保障環境の悪化等による LNG 途絶の恐れであり、それらに対する外交、

---

[15] 2020 年 3 月、電力システム改革として発送電分離がなされた。これは従来地域独占で供給されていた電力分野に競争原理を導入することで、①電力の安定供給、②電気料金の抑制、③需要家（消費者）の選択肢や事業機会の増加を目的としたものである。

[16] 資源エネルギー庁『エネルギー基本計画』17 頁。また電力供給力の確保の観点から、自由化前は、地域独占と規制料金により費用回収が保証された旧一般電気事業者が、需要に合わせて必要となる発電設備や燃料を計画的に確保していたが、自由化後、発電設備を自ら保有しない小売事業者の参入に伴い、短期的な取引をベースとした競争の中で、採算性の悪化する火力発電の停止が進展し、新規投資も停滞している。実際に、石油火力は 2014 年度から 2019 年度までの 5 年間で約 1,000 万kW 減少しているなど、経年火力の休廃止が進んでいることに加え、直近の需給見通しでは安定供給に最低限必要とされる予備率の確保が不透明となるなど、供給力の低下に伴う安定供給へのリスクが顕在化している。94-5 頁。

防衛、経済的手段を検討する。

（1） 地震や台風等の大規模災害への対処

◇ 電力システムの脆弱性の改善

大規模災害等に際しては、災害対策基本法における「指定公共機関」として、いかに早期に必要な電力供給を回復し救援活動に貢献するかが、災害という脅威への対処の目的である。そのために電力システムは、地震に対する耐震基準を保有する火力発電所等[17]の整備や BCP（事業継続計画）の策定による災害時の体制をもって、平素からのレジリエンスの充実を図る。さらに事業者相互の連携によって、被災地域の電力供給をカバーし復旧を支援する観点から、地域間で電力を融通する「地域間連携線」の増強による融通電力の増加の他、各地域間での「災害時連携計画」による相互の応援の準備や応急復旧のための設備の復旧方法および設備仕様の標準化を進めている。

また地方自治体とは、送電線の非常災害時の障害物除去ための協議も進める他、自衛隊との連携として、過去の非常災害時において、地方自治体からの要請にもとづく自衛隊の派遣により倒木等の除去等が加速し復旧に貢献したことに鑑み、平時から意見交換や訓練を実施している[18]。

加えて電力システム事業者は、原子力災害対策特別措置法における「原子力事業者」としての地位を持つ場合もあり、各種の規制基準に基づく安全対策をとりつつ原子力発電所の逐次の再開を進めているが、大規模災害等においては、原子力災害の発生または拡大の防止を図る。

◇ 防衛省・自衛隊の役割

地震や台風等の大規模災害には、「国の総力をあげて全力で対応」して、迅速に救援活動にあたるために、防衛省・自衛隊は、ライフラインに係る重要インフラとの災害時の連携の必要性についての認識の下、災害情報共有や復旧支援のための協定を結んでその態勢を整備している。電力システムに対しては、電力の早期復旧を支援することが期待され、今

---

[17] 被災により人命に重大な影響を与える可能性のある設備（ダムや LNG や油タンクなど）を「耐震性区分Ⅰ」として、直下型または海溝型地震に起因する「高レベルの地震動」に耐えると共に、それ以外の「区分Ⅱ」でも、著しい供給障害が生じないよう整備しており、一般的な地震動（震度５程度）に対して問題となる設備がないことが確認されている。松崎加那絵「エネルギー業界の備えと課題を分析」『エネルギーフォーラム』No.825、2023 年９月、17 頁。

[18] 一般送配電事業者 10 社（北海道、東北、東京、中部、北陸、関西、中国、四国、九州、沖縄）『災害時連携計画』4 頁。

後その実効性の向上が必要である[19]。加えて「防衛力整備計画」では、「原子力発電所が多数立地する地域等において、関係機関と連携して訓練を実施し、連携要領を検証するとともに、原子力発電所の近傍における展開基盤の確保等について検討の上、必要な措置を講じる」とされているように、原子力災害時の対処は各関係機関の参加する訓練を通じて実効性の向上が必要である。さらにその成果は、有事の対応においても活用可能である。

（2） サイバー攻撃及び大規模テロやそれに伴う原子力発電所を始めとした重要インフラに対する攻撃への対処

ロシアのウクライナへの侵略では、電力システムがサイバー及びミサイル等によって攻撃を受けるとともに偽情報の拡散による混乱の拡大など、重要インフラに対する脅威は複合化しているが、まず対処すべき脅威は次のように考えられる。平時からグレーゾーンまでも含め、攻撃主体としての露見を避けつつ「機微情報の窃取」や「重要インフラの機能停止や破壊」による相手国国民の士気の低下を狙ったサイバー攻撃。これには 2015 年 12 月の厳冬の時期に、キーウを含むウクライナ東部の住民 22.5 万人に停電の影響を与えたサイバー攻撃がある[20]。

また武力攻撃開始に際し、「重要インフラの機能停止や破壊」により社会的な機能を麻痺させ相手国の戦意低下および戦力発揮を妨害して、短時間に軍事目的を達成するために奇襲的に行うサイバー攻撃がある。例えば、ロシアはウクライナ侵攻当日には政府機関等に対する大規模な DDoS 攻撃を行った他、金融、農業、緊急事態対応サービス、人道支援、エネルギーなどの幅広い重要インフラに対して「ワイパー」と呼ばれる破壊型ウイルスによるサイバー攻撃を行ったとされる[21]。また DDoS 攻撃を受けた銀行では ATM が停止したが、数時間の使用不能の後に復旧された後でも、未だ停止しているとのフェイクニュースが拡

---

[19] 防衛省・自衛隊においても以下の認識を持っている。「ライフライン断絶について、都市部において高密度に整備されている電力、ガス、上・下水道、工業用水道、通信施設等のライフライン施設は復旧が困難な地下に埋設されているものが多く、大規模震災等が発生し断絶した場合、復旧に困難を伴い、広く、長期にわたり被災者の生活を始め、経済・社会活動に甚大な被害をもたらすおそれがある。そのため大きな被害の発生が見込まれる地域については、自治体、関係機関との連携の下、あらかじめ被害想定を見積もっておく必要がある。また、人命救助・応急医療支援、避難支援、消防・消防支援等各々の活動に関し、関係機関との間で役割分担等を始めとする連携要領について認識の共有化を進めておく必要がある」、防衛省「都市部、山間部及び島しょ部の地域で発生した災害並びに特殊災害への対応について」『防衛省防災業務計画』、令和５年３月、2-3 頁

[20] ICS Alert “Cyber-Attack Against Ukrainian Critical Infrastructure,”(Cyber-Attack Against Ukrainian Critical Infrastructure | CISA

[21] 松原実穂子『ウクライナのサイバー戦争』新潮社、2023 年、8 月、52-6 頁。

散され、社会の混乱と不安をあおる攻撃もあった[22]。

さらに武力行使後も引き続き、電力供給の妨害によって通信を遮断し、国際的な情報発信の妨害や国民のさらなる混乱を生起させるため、火力攻撃などと連携したサイバー攻撃も行われている。ロシアは戦争の初期段階でミサイル攻撃や「ワイパー」によって電力インフラを攻撃しその供給能力を半減させるとともに、ウクライナの通信インフラも攻撃し国家のデータセンターも破壊した。そのため電力や通信技術者は国内の通信ネットワーク確保や基本的なデータの保護を、火力による破壊とサイバー攻撃そして停電との三重苦の中で継続した[23]。加えて原子力発電所やダムには、電力システムの機能妨害の他、損傷による放射能漏えいや水害への威嚇や地域利用妨害などの直接的効果を狙って攻撃が行われていると考えられる。

このように物理的被害も発生させるサイバー攻撃が平素から行われ、さらに武力行使後もミサイルや砲爆撃など物理的な攻撃と表裏一体になり、電力、通信、エネルギー、交通・輸送などの重要インフラに被害を及ぼすと同時に、偽情報などを拡散し不安をあおり、システムの機能の修理・維持を妨害している。そのため対処にあたっては、サイバー攻撃の脅威に対しては平素からの重要施設のシステムの脆弱性の改善を、ミサイルなどの物理的な攻撃への脅威に対しては関係機関の連携による効率的な脅威の排除を、そして偽情報への迅速かつ的確な対応を重視することが必要である。

ア　サイバー攻撃対処

サイバー攻撃に対しては、政府としての対処のための体制構築や、システム・セキュリティの強化などの具体化とともに、人的要素の充実も必要である。「国家安全保障戦略」では民間・政府間のサイバー攻撃に関する状況共有や対処調整を含むサイバー安全保障の政策を一元的に総合調整する組織の設置などの体制の整備とともに、相手のサイバー空間の利用を妨害する能力の強化が記されている。またシステム・セキュリティの観点からは、「防衛力整備計画」では「境界型セキュリティのみでネットワーク内部を安全に保ち得るという従来の発想から脱却し」、「ゼロトラストの概念に基づくセキュリティ機能の導入を検討する」としている。

◇ 電力システムの脆弱性の改善

上記を受けて、電力システムのセキュリティに関しては、システムの中心である発電機

---

[22] 同上、42頁。

[23] 同上、48頁。

能において以下を重視して対処する必要がある。第一に、「制御システム」をその防護の主体とする。「制御システム」は、電力の発電から送配電までの工程において具体的に操作を制御していることから、「サイバーセキュリティ戦略」では、重要インフラ事業が防護すべき対象となる重要システムとして「電力制御システム」を指定し、その機能が妨害された場合には、電力供給の停止や電力プラントの安全運用に対する支障が生じるとしている[24]。前述のロシアのサイバー攻撃によるウクライナに対する 2015 年の停電は、標的型メールなどで業務端末にウイルスを感染させ、そこから制御システムに侵入し直接操作により電力供給を停止させたと分析されている[25]。そのため、電力システムに関しては、制御システムと外部ネットワークとは分離することが規定されている[26]。これにより外部からのサイバー攻撃の影響の可能性を低下させ、仮に制御システム自体がウイルスに感染しても、他の発電所などのシステムへの横展開による感染被害の拡大の恐れは少ない[27]。

第二に、従来外部との接続がないとして安全と考えられていた制御システム等においてもサイバー攻撃が確認されているため[28]、サプライチェーンに起因する脅威への対処も必要とされている。それは発電所などの施設に用いられる設備の導入やメンテナンス等に当たる事業者がウイルス等を仕込んだり、場合によっては内部の人員による過失または故意のウイルスへの感染により、いざという時に誤作動を起こす恐れがあるからである。そのため「経済安全保障推進法」では、基幹インフラ機能の安全性・信頼性の確保のため、重要な設備、機器、装置又はプログラムなどの特定社会基盤役務に不可欠な設備を「特定重要設備」として指定する。そして導入する設備や維持管理を委託する業者などについて事前審査を義務付けると共に、重要設備の導入では設備の概要や供給者それに部品などを、また維持管理の委託をする場合は委託相手や再委託の概要などがチェックされる。

◇ 防衛省・自衛隊の役割

サイバーの分野における防衛省・自衛隊の対応としては、上記の技術的な対処に加え、平素からの政府・民間の各機関の連携による情報共有に基づく対処が必要である。そのた

---

[24] サイバーセキュリティ戦略本部『重要インフラのサイバーセキュリティに係る行動計画』2022 年 6 月、47-51 頁。

[25] ICS Alert, ibid.

[26] 経済産業省『自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン』2022 年 4 月、25 頁。

[27] この場合でも、特定の条件下、複数の発電所が個別かつ同時攻撃を受けた場合は大規模な停電発生の可能性はある。

[28] サイバーセキュリティ戦略本部、20 頁。

め「国家安全保障戦略」では「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、政府から民間事業者等への対処調整、支援等の取組を強化するなど」としている。しかしながら各企業は日々の業務を通じてサイバーの分野では、「ランサムウエアによる被害」を最も重視しているため[29]、被害を受けてもその事実や身代金支払いに関する情報を政府と共有することや、政府との迅速かつ密接な情報共有には経営上抵抗があると予想される。一方でランサムウエアは従来、「身代金の要求」の目的で使われると考えられていたが、ウクライナ侵攻においてロシアはこれを、システムの「機能停止や破壊」のためにも使用していることから[30]、今後は平素の段階における国家としての関与も一層必要となると考えられる[31]。そのため次のような平素からの防衛省・自衛隊を含む政府機関との連携を検討しなければならない。

先ず、政府としてサイバー安全保障の政策を一元的に総合調整する中で、武力攻撃以前の段階での民間の重要インフラに対するサイバー攻撃を能動的サイバー防御でいかに対処するかについての具体化が焦眉の急である[32]。すなわちサイバー安全保障分野での対応能力の強化を図るためには、民間システムのすべてを常に監視・防衛することは妥当ではないものの、民間の重要インフラに対してサイバー攻撃をおこなう相手に、新たに強化される自衛隊サイバー防衛隊等のサイバー関連部隊をもって、平素の段階からのサイバー偵察や能動的サイバー防御などを選択的に行う態勢整備が必要である。その枠組みの下、自衛隊サイバー防衛隊は、民間の重要インフラ事業者と必要な情報共有を平素から行い、脅威の現状を共有するとともに、脅威側システムの脆弱性の解明や各種のオプションを策定しておくことが可能になると考えられる。

またサイバー攻撃能力を担う国家としての人材の育成には時間を要することや二重三重の対策によっても人的要素による感染の恐れは排除できないことを踏まえると、システ

---

[29] 独立行政法人　情報処理推進機構　「情報セキュリティー10 大脅威 2023－組織向け脅威」（https://www.ipa.go.jp/index.html、（2 位）サプライチェーンの弱点を悪用した攻撃、（3 位）標的型攻撃による機密情報の窃取、（4 位）内部不正による情報漏えい、（5 位）テレワーク等のニューノーマルな働き方を狙った攻撃

[30] 松原、32 頁。

[31] 米国は、2021 年5月の石油パイプラインへのランサム攻撃を受けて、すでに示していた指示に加えて、制御システム等が完備すべき技術的対策や対処計画について大統領指示を発出した。The White House, FACT SHEET: Biden Administration Announces Further Actions to Protect US Critical Infrastructure, July,2021

[32] 米国の「国家サイバー戦略」では、重要インフラの防衛を第一の柱としている。The White House, National Cybersecurity Strategy, March,2023

ムを守りかつ活用するサイバー分野での人的要素の教育・訓練や活用のためにも平素からの連携が重要である。

イ　大規模テロやそれに伴う原子力発電所を始めとした重要インフラに対する攻撃への対処

電力システムに対する攻撃の脅威の中で、国際テロ対策の国内での対策の徹底の対象として「国家安全保障戦略」では「原子力発電所等の重要な生活関連施設の安全確保」と明記しており、これは平成 25 年版での「原子力関連施設の安全確保等」と比較して、「断固とした姿勢」を示している。なぜなら安全確保が必要とされた「生活関連施設」とは、国民保護法で武力攻撃災害への対処のため安全確保（第 102 条）が必要とされる十種類の広範な施設であり、テロ対策の対象が大幅に拡大していることを表すからである[33]。これを受け、電力システム事業者及び防衛省・自衛隊それぞれの対処における役割は次のように考えられる。

◇ 電力システム事業者の対処

テロ等の脅威に対しては、電気システム事業者が保有する地位に応じたそれぞれの役割を行う必要がある。経済安全保障上の重要インフラとしての電力システム事業者は、①武力攻撃事態においては「指定公共機関」として有事において公益的事業を営む法人である他、②国民保護の観点からは発電所・変電所等を保有して安全確保措置が必要な「生活関連施設の管理者」であり、③加えて武力攻撃原子力災害においては「原子力事業者」である。そのため、①としてはあらゆる事態においても電力供給力確保のための措置をとると同時に、②の地位として、電力システムの脅威に対する施設の警戒・監視・通報等の安全確保措置を、そして③としての核物質防護や核物質の放出、汚染拡大防止のための「応急対策（国民保護法第 105 条 7）」を行う。

この際、次のような課題の検討が必要である。第一に脅威への対処については、現在すでに③の原子力発電所の防護に関して関係機関との連携に基づく役割分担をもって行われているが[34]、国際テロ対策の強化の観点からは、今後いかに②に関して充実するか。また第

---

33 電気、ガス、水道、鉄道、電気通信、放送、港湾、空港、河川、危険物質等の取扱所（下線部は経済安全保障推進法で指定されていない項目）国民保護法施行令第 27 条

34 原子力事業者としては、故意の航空機衝突などによる大規模な損壊でも原子炉を安全に停止することができる中央制御室の代替として「特定重大事故等対処施設」を整備するハード面での対策をとる。警戒は警察が一義的に担任しテロに対しては高度な制圧能力をもつ特殊部隊（SAT）を投入する体制を整え、海上保安庁とも連携し、テロ発生時や警察力では対応できないと認められた場合に備え、自衛隊との間で共同訓練を実施している。「原子力総合パンフレット 2022 版」日本原子力文化財団 www.jaero.or.jp/sogo/detail/cat-04-05.html

二に、原子力施設に対するテロ対策として義務付けられた施設は、現在の安全保障環境下、ミサイルや航空攻撃への対処には適していないとの問題点への対応[35]。

◇ **防衛省・自衛隊の役割**

重要インフラへの脅威への対処において防衛省・自衛隊が果たすことが期待される役割は、時間的、地域的またその範囲が拡大しているため、上記の問題点を考慮しつつ、「抜本的に強化された防衛力」をもって効率的に対応することが必要である。「国家安全保障戦略」では「原子力発電所等の重要な生活関連施設の安全確保対策」に関し、「武力攻撃事態のほか、それに至らない様々な態様・段階の危機にも切れ間なく的確に対処できるようにする」とし、さらに「総合的な防衛体制強化の一環として、自衛隊・海上保安庁による国民保護への対応」をあげている。これは前述のように、安全確保の範囲や対象は、これまでの原子力発電所に加え、場合によっては、ガス、水道施設、駅、海底ケーブル引き上げ地点などまで含み、それらが所在する地域まで拡大していると言える。さらにその防護においては、平素からグレーゾーンを含めたシームレスな対応の中での役割が改めて必要とされた。すなわち、防衛省・自衛隊に期待されている役割としては、Ⓐ原子力発電所を含む重要インフラへのテロ等の脅威への対処のための警戒・監視や施設の防護等、またⒷ避難・誘導に加え、武力攻撃に伴う被害の局限による国民保護の充実、そして現在の問題点であるⒸミサイル等による重要インフラへの直接攻撃への対処などについて、平時から有事までシームレスに対応することである。このような役割の実行にあたり、限られた人的基盤の中、優先順位をもって対応することは当然として、強化された防衛力の活用の観点から以下の点を重視することが重要である。

第一にⒸに関し、武力攻撃事態におけるミサイル攻撃対処に加え、グレーゾーンにおける重要インフラに対するミサイル攻撃の恫喝に対処すること。原子力発電所を含め重要インフラは、ミサイル攻撃により経済的、物的及び精神的にも多大な被害を生み、都市などの人口密集地同様、重要な価値を構成しているため、攻撃の恫喝にさらされた場合に、国民の継戦意思に影響を与え、国家の意思決定を左右する恐れがある。これまでは原発等へのミサイル対処のために、拠点防空のため全国に配置されている PAC-3 を機動的に移動・

---

[35] 原子力規制委員会の更田豊志委員長は 9 日の衆院経済産業委員会で、日本国内の原発がミサイル攻撃を受けた場合、「放射性物質がまき散らされることが懸念される。現在の設備で避けられるとは考えていない」との見解を示した。東京新聞（電子版）2022 年 3 月 9 日 19 時 26 分。

展開するとしてきた[36]。今後は、統合防空ミサイル防衛能力の一環として BMD の能力向上による多様な対空脅威に対処するとともに反撃能力を保有する。これによりミサイル攻撃の効果を無効化できる能力とともに、攻撃者が被るコストとリスクを高めることを通じた攻撃を抑止する手段の重層化が期待でき有効である[37]。

第二にⒶに関し、広域において、時期も、目標も、敵も不明な状況で奇襲的に行われるテロ攻撃に対し、それを早期に把握し、予め最小限の被害で対処する方策の立案に必要な、平素からの警戒・監視及び情報分析能力の強化。テロ対処においては、無人アセットを活用した情報収集に基づき、フィジカル空間のセンサから得るビッグデータを AI が解析し、その解析結果がフィジカル空間にフィードバックされ、状況不明なグレーゾーン事態において脅威側が発する兆候を検知し、それが対処能力を超える前に排除することが可能になることが期待される[38]。これらの情報収集・処理能力の向上により、平時か有事かの不明な状況下、軍事・非軍事も不明なテロ攻撃の兆候を察知して、脅威対象をあぶり出し早期対処することが可能となる。

第三に、Ⓑに関して平素からの防災を中心とする訓練を通じて武力攻撃時の安全確保への適正な信頼感を醸成した国民保護体制の構築。原子力防災等の目的で展開地域を活用して行う平素からの訓練は、それを通じて、部隊の正しい姿を実際の行動で明示し、地域社会を含む内外に安心感を与え、重要インフラの脅威への対処のための地域の理解と協力につながる[39]。

これと同時に、偽情報等の拡散を含めた情報戦に対応しつつ、地域を含む国内外の信頼性を確保し、平素からの協力体制の構築が必要である。特に情報戦の観点からは、あらゆる事象において、真偽ないまぜのニュースや動画等により、相手国政府への信頼低下を狙

---

[36] 防衛省「令和 5 年版防衛白書」、303－4 頁。また浜田靖一防衛相（当時）は 2022 年 10 月 13 日衆院外務、安全保障などの連合審査で、原発へのミサイル攻撃に対する防護を強化するため、全国 24 部隊に配備している地対空誘導弾パトリオット(PAC3)の配置転換も含め、迎撃態勢の見直しを検討する考えを示した。東京新聞（電子版）「『原発狙われるリスク』ミサイル迎撃態勢を検討と浜田防衛相　立地県に PAC3 配備も　衆院連合審査会」2022 年 10 月 13 日 19 時 48 分。

[37] 松村五郎『対日ミサイル攻撃の脅威にどう立ち向かうか』「安全保障を考える」第 804 号、安全保障懇話会、令和 4 年 5 月、7－8 頁。

[38]住田和明『超スマート化による領域保全能力の向上＝ 国境離島の保全を中心とした一考察 ＝』「安全保障を考える」第 795 号、安全保障懇話会、令和 3 年8月、13 頁。

[39] 産経新聞（電子版）2022 年 3 月 8 日「福井県知事、ロシア軍の原発攻撃で自衛隊配備を要請」
防衛省によれば、自衛隊は 2012 年以降、各地の原発の敷地において、警察との共同実働訓練を行っている。防衛省、前掲書、304 頁。

った情報の拡散がなされると考えられる。ウクライナにおいては、ロシアの侵攻と同時にゼレンスキー・ウクライナ大統領の国民に向けた降伏を呼びかける偽動画が拡散されたが、同大統領が即座に国民の前に出て否定したように、虚偽の情報に対して迅速に責任ある者が反論することが効果的である。防衛省においても、偽情報などのファクト・チェックなどの情報戦対処能力を整備することとしており[40]、部隊レベルにおいても平時・有事を問わず、SNS などを活用して偽情報を否定し正しい姿を発信することを通じて信頼性を確保する能力の充実が望まれる。

以上述べたように、重要インフラへの脅威は、サイバー領域、テロ攻撃を含む火力による物理的領域そして認知領域において増大しているため、その対処にあたってはそれぞれの脅威に対処するとともに、総合的な効果を発揮することが必要である。

（３） LNG の安定的確保

電力システムに必要なエネルギー安全保障の観点からは、「国家安全保障戦略」では、資源国や供給源の多角化や調達リスク評価の他、再生可能エネルギー等による自給率向上と開発などを通じて同盟国等と連携しつつ「有事にも耐え得る強靭なエネルギー供給体制を構築する」として、良好な外交関係に基づく経済的手段を中心とするサプライチェーンの供給源確保の方策が強調されているが、電力システムのエネルギーとして必要な LNG については以下の点から、その輸送の安全確保及び備蓄の実効性について検討する必要がある[41]。

第一に、LNG は現在、発電の燃料構成の４割を、都市ガスのほぼ全量を占め、海上輸送に依存することから、交易路に関する物的安全保障についての検討が必要である[42]。「国家安全保障戦略」においては、「シーレーンにおける脅威に対応するための海洋状況監視、他国との積極的な共同訓練・演習や海外における寄港等を推進し、多国間の海洋安全保障協力を強化する。また、海上交通の安全を確保するために、海賊対処や情報収集活動等を実施する」と平素からの取組を重視している。今後は LNG の具体的な海上交易路に応じた

---

40 防衛省、309 頁。

41 石油及び LP ガスは、1975 年以来「石油備蓄法」により国家、民間備蓄が規定されている。

42 経済産業省『可燃性天然ガスに係る安定供給確保を図るための取組方針』令和５年１月、３頁。またダニエル・ヤーギン（米国を中心に世界で最も影響のあるエネルギー問題の専門家）の言葉として、エネルギー安全保障は３つの側面が必要としている。すなわち、第一に、資産・インフラ、サプライチェーン、交易路が守られるといった物的安全保障、第二に、エネルギー供給源を開発し、採算が取れ、契約で保証される形で実物を確保できるといったエネルギーアクセスの確保、第三に、インフラへの長期的な投資と供給途絶等の非常事態に協調して対応する国家政策からなる体系の成立である。前掲書、３頁。

安全確保の実効性を検証することが必要であると考えられる。

第二に、「経済安全保障推進法」では第 7 条において、LNG が「特定重要物資」として指定され、その特性に応じた要領で備蓄が行われるため、今後の実効性の確認・向上が必要である。途絶リスクが顕在化している LNG は、有事の際にも供給途絶が生じることのないようにするために、余剰の在庫を抱えることを目的として、国による一定の支援の下、「戦略的余剰 LNG（SBL: Strategic Buffer LNG）」の確保を目指す[43]。また LNG は、石油のような長期間のタンク備蓄には適さないため、陸上タンクによる備蓄ではなく、流通する在庫「流通在庫」として通常のトレーディングの中で余剰を確保しておき、需給ひっ迫等が生じ、政府が認める時には指定した国内事業者へ販売することとしている[44]。この際のその所要を「流通在庫」で賄うことになるが、状況に応じた在庫の配分の決定要領や実際に流通在庫がタイムリーに到着するかなどは今後の検討となる。

以上のように LNG の安定的な確保は電力供給、そして安全保障上の需要な要素であるため、その特性に応じた備蓄などは今後の実行段階での検証・検討が必要である。

おわりに

ロシアのウクライナ侵略において見られるように、重要インフラに対する脅威は現実化しており、その脅威はサイバー攻撃によるシステムの機能破壊とミサイル攻撃などによる物理的破壊と表裏一体であるとともに、偽情報の拡散等により認知領域にも影響を与え、インフラを扱う技術者を含めた国民の不安や政府への不信感を醸成して重要インフラの安定的な機能発揮を妨害している。我が国においても、重要インフラは国民の安全に大きな影響を及ぼす役割を果たしており、外交、防衛、経済的な方策をもって一体的に対処する必要がある。

本稿においては、その一つである電力システムについて検討した。防衛省・自衛隊として電力システムへの脅威の増大に対処するためには、大規模災害においては電力の早期復旧の支援を、またサイバーを含む大規模テロなどの脅威に対しては、抜本的に強化された防衛力を活用して関係機関との密接な連携に基づく平時から有事までのシームレスな対

---

[43] 2023 年 12 月から 2 月の 3 カ月に対応する SLB として当面は最低 1 カーゴ／月（6～7 万 t 級タンカーで約 5,000 万世帯の一日分の電力に必要な LNG を積載）づつの確保を目指す。経済産業省 11－19 頁。

[44] 前掲書、12-18 頁。また LNG は、マイナス 162 度以下の低温で輸送・貯蔵する必要があり、それによっても例えば 2.5 万トンのタンクに貯蔵した場合逐次蒸発し、約一年で全量が消失する。

応を、さらにLNGの安定供給の検証などを、重要インフラ事業者の機能維持努力と整合させることが必要である。さらに今後の課題としては、防衛省・自衛隊が果たすべき役割について、関係機関やインフラ事業者とさらに連携して具体化するとともに、平時を基準としている各種の法体系に基づく各機関の行動を、いかにグレーゾーンを含む事態にシームレスに対応できるかを検討していくことである。最後にこの観点から、以下の提言をもって結言としたい。

第一に、重要インフラ側及び防衛省・自衛隊側においてそれぞれ相手の安全保障上の位置付けと機能について共通理解を構築すること。経済安全保障の観点では、平素の自由かつ公正な競争が行われる経済活動を前提として最小限の規制を原則とするため、有事を基準とした防衛力による安全保障との平素からの接点は限定的であり、シームレスな対応に問題を生じやすい。一方で、防衛省・自衛隊関係者の14分野の重要インフラについての理解は必ずしも十分でなく、重要インフラ関係者の有事における防衛省・自衛隊の行動に関する理解も多くはない。そのためにも、平素からの連携態勢を構築し、共通理解と訓練を通じた役割分担の実効性を確認しておくことが重要である。

第二に、平素の連携は災害への共同した対処要領を検討することを基礎として逐次拡大充実させていくこと。民間企業ではステークホルダーに対する責任として、安全、サイバー、コンプライアンスなどが重視される傾向にあり、災害における被害極限と役割遂行に関する危機管理等の充実を重視していることから、地方公共団体や警察・消防など関係機関とともにその役割の検証が可能な総合的な訓練は、効果的であると考えられる。そしてこれまで都道府県、市町村との平素からの連携には、自衛官の経歴を有する防災官が防災訓練や災害派遣等の調整において自衛隊の運用についての知見を活用して重要な役割を果たしてきた経緯がある。重要インフラ事業においても、現在ではすでに、電気、情報通信、郵便、金融、クレジットカードなどの関係事業においてそれらの人材が携わっている。平素からの連携強化のため、今後はそれら人材の活用・拡大も望まれる。

【筆者プロフィール】

中野　義久（なかのよしひさ）

１９８７年防衛大学校卒業（国際関係論）
同年陸上自衛隊入隊
第５施設団長、大阪地本長
防衛研究所副所長
第１０師団長を歴任し、２０２２年退官
コロンビア大学大学院国際学修士