

2024 年 5 月 1 日

我が国のサイバー/情報セキュリティ政策の変遷 (重要インフラ編)

～今後の重要インフラに係るサイバーセキュリティ政策立案 において考慮すべき観点～

東海大学情報通信学部学部長・教授
三角 育生

1. はじめに

2022 年 12 月 16 日に国家安全保障会議及び閣議で決定された国家安全保障戦略(安保戦略 2022)¹⁾において、「サイバー攻撃による重要インフラの機能停止や破壊」等は、「国家を背景とした形でも平素から行われている」²⁾との認識が示された。そして、「サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」との方針が示された。具体的な施策として、「武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入」³⁾するとした。この様な方針は、従来からのサイバーセキュリティ領域における政策、例えばサイバーセキュリティ基本法に基づくサイバーセキュリティ戦略においては明示されたことはない。そして、安全保障論の観点からは、「縦割り行政の克服や抑止力の保有・行使の点で、かなり未発達な状態に陥っ」ていると、サイバーセキュリティ戦略の欠点として指摘されている⁴⁾。

サイバーセキュリティ政策は、サイバー安全保障分野の政策と、重要インフラ等に係るものなど、テクニカルな面において似ており、関連性の高い部分もある。しかし、サイバーセキュリティ政策は、安全保障政策⁵⁾とは目的、発展の経緯等について異なる流れにある。サイバーセキュリティ政策を安全保障政策の観点を主として捉えることが必ずしも妥当ではなく、その逆も然りであると考え。そこで、本稿では、重要インフラに係るものを対象として、サイバーセキュリティ領域における政策の変遷を概観し、政策推進にあたって重視されたとする点を抽出するとともに、サイバーに係る安全保障政策との関係を整理する。その上で、重要インフラに係るサイバーセキュリティ政策立案にあたって基本となる考え方は何か、それを前提としたときに今後のサイバーセキュリティ政策立案・実施にあたってサイバーに係る安全保障政策との関係で考慮すべき観点を示すことを目的とする。

2. 情報セキュリティ政策会議設置以前

2.1 重要インフラのサイバーテロ対策に係る特別行動計画

政府横断的な重要インフラに係る情報セキュリティ対策政策は、2000年12月15日に情報セキュリティ対策推進会議(対策推進会議)⁶によって取りまとめられた「重要インフラのサイバーテロ対策に係る特別行動計画」(特別行動計画)⁷にはじまる。特別行動計画では、重要インフラについて、「いわゆるサイバーテロの脅威により、国民生活や社会経済活動に重大な影響を与えと考えられる重要インフラ分野を、当面、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス(地方公共団体を含む。)」と定義した⁸。ここで、「いわゆるサイバーテロの脅威」とは、「高度な技術を有する犯罪者集団やテロリスト集団などが重要なネットワークを攻撃することによる、経済的な被害、混乱、死傷者等をもたらす脅威」⁹を念頭においている。こうした脅威に対して、「内閣官房を中心として、官民の緊密な協力の下、この計画の実施に努めること」としており、同「計画を指針として、自主的な取組の強化を図る」¹⁰ことなどによって政策を推進する手法をとった。

具体的な計画の内容は、被害を予防するため、民間重要インフラ・地方公共団体のセキュリティ水準の向上を図るべく、対策推進会議が決定した「情報セキュリティポリシーに関するガイドライン」等を参考とすることの促進や、政府からの情報提供・助言・指導等の支援の一層の推進などを行うとした。また、サイバーテロ対策に関する官民の連絡・連携体制の確立・強化や、民間重要インフラ事業者等において基幹を為す重要な情報システムに障害が発生した場合の対処手順の策定、緊急時対応計画の策定、緊急時における情報の連絡手順の明確化、警報情報の連絡といった官民連携によるサイバー攻撃の検知と緊急対処、人材育成・研究開発・普及啓発・法制度整備といった情報セキュリティ基盤の構築及び国際連携を図ることとした。

以上をまとめると、犯罪者集団、テロリスト集団といった攻撃者からのサイバー攻撃によって重要インフラ(7分野)における重要ネットワークや情報システムが障害を発生することを想定し、内閣の重要政策に関する基本的方針等について企画・立案・総合調整の事務を担う¹¹内閣官房が中心となり、国が防護、対処、連絡体制などについて任意の指針を示し、官民連携のもとで推進するというものであった。

2.2 情報セキュリティ基本問題委員会第2次提言

2005年4月22日、高度情報通信ネットワーク社会推進戦略本部(本部長:内閣総理大臣、IT戦略本部)情報セキュリティ専門調査会情報セキュリティ基本問題委員会が、「我が国の重要インフラにおける情報セキュリティ対策の強化に向けて」と副題をつけた第2次提言(2次提言)¹²をとりまとめた。2次提言は同年5月のIT戦略本部に報告され了承されている。

2次提言では、「重要インフラは、我が国の社会経済活動と国民生活を支える基本的なサービスを提供している」、「仮に、重要インフラで大規模な障害が発生するならば、さまざまな領域へ大きな影響を与えることが予想される」、「大規模な障害から重要インフラを防護するための取組みは、さまざまなリスクを勘案して行わなければならない」¹³との認識が示された。その上で、「重要イ

ンフラにおける情報セキュリティ対策」について、『重要インフラ』のサービスの維持・復旧を図ることを第一義的な目的とするとの視点が重要」であり、「その第一義的な目的を前提としながら、各事業において発生する障害（サービスの停止や機能の低下等）のうち、IT の機能不全が引き起こす障害（IT 障害）についての総合的な取組みとして位置づける」¹⁴という基本的な方針を示した。

特別行動計画ではサイバーテロ対策を中心としたものであったのに対して、2次提言は重要インフラの機能低下等を引き起こすような IT 障害への対策も含むとした点が新しい。その背景として、2003 年 3 月に、東京航空交通管制部にある飛行計画情報処理システムが 2 系統ともダウンし、20 分間、全国の空港から航空機が出発できなかったなどの影響が生じた事件¹⁵等が挙げられる。IT 障害であっても重要インフラのサービス途絶が社会経済活動に大きく影響する事象が認識されたためである¹⁶。

2次提言では、重要インフラの定義についても明確化を図った。すなわち、「重要インフラとは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下、または利用不可能な状況に陥った場合に、我が国の国民生活または社会経済活動に多大なる影響を及ぼすおそれが生じるものをいう」¹⁷とした。これは特別行動計画では、「いわゆるサイバーテロの脅威を前提とし、それによって重大な影響がある基盤を、対象とする『重要インフラ』として位置づけている。しかし、『重要インフラ』そのものの定義を行っておらず、入口と出口が逆転したかのような構造となってしまう」¹⁸ことから改めて定義したものである。2次提言では、防護の意義について、重要インフラの「事業において発生する障害を回避し、サービスを維持・復旧するための総合的な取組みを意味する。重要インフラの防護を充実することは、我が国の能力を保全し、ひいては安全保障・危機管理に資することになる」¹⁹としている²⁰。

具体的な対象分野には、特別行動計画における 7 分野に加えて、水道、医療、物流等を対象に含めるべく見直すとの方針を示した。水道は、豪州では既にサイバー攻撃によって未処理の汚水が下流河川に大量に放出されるなどの事案が実際に発生していたこと、飲み水の安全は、国民生活にとって重大であることが対象となった理由である。医療については、特別行動計画のフォローアップで分野追加への検討が明記されたことによる。物流も含めて、海外で対象となっていたものが念頭におかれて提言に盛り込まれた²¹。

2 次提言の特徴として、「重要インフラ相互間の依存性解析を行うなど、重要インフラ横断的な状況把握機能の強化」²²を新たに示したことを挙げられる²³。また、自然災害、物理的テロ等への対応における関係省庁等との連携の強化も提言している。

安全基準、ガイドラインについては、重要インフラ所管省庁及び重要インフラ事業者が協力をしつつ、分野ごとに IT への依存度や自然災害等の経験によりこれまで構築してきた総合的な対策の内容に基づき策定するとした。その位置づけは、「各事業法等の枠組みの下での、法的根拠に基づく強制基準、政府の策定する現行の事業法等に準じた性能規定からなる推奨基準及びガイドライン、並びに民間が自ら定める業界標準、さらに業界各事業者が技術基準等の仕様レベルで

の規定に関して自らの対処水準を定める自主基準・ガイドライン等の階層構造を念頭におく」²⁴べきと提言とした。

IT 障害に関する情報については、「①IT 障害の未然防止、②IT 障害の拡大の防止・迅速な復旧、③IT 障害の要因等の分析・検証による再発防止の 3 つの側面それぞれに資するものを適切に」官民、事業者間で共有することを重視した。その共有体制として、「重要インフラ事業者を主体とした「情報共有・分析センター」(ISAC : Information Sharing & Analysis Center)等の各重要インフラ内情報共有機構の創設を図る」²⁵ことなどが提言されている。さらに、官民の情報共有、連絡・連携のための仕組みが実際に有効に機能するように、類型化された脅威シナリオに基づく総合的演習の実施も提言した。

以上をまとめると、2 次提言は、重要インフラの定義を明確化し、防護の対象をサイバー攻撃起因のもののみならず非意図的要因、自然災害にまで広げて重要インフラサービスの維持・復旧を目指すものとしたこと、安全基準等の位置づけを業法等の下階層構造体系とすることを提言したこと、分野横断的な視点を持たせて、情報共有・連携、その有効性につき演習を通じて確認・改善する仕組みの提言など、その後現在に至るまで我が国の重要インフラ防護の政策の基本的なラインを提言したものであった²⁶。

3. 情報セキュリティ政策会議による政策

3.1 重要インフラの情報セキュリティ対策に係る行動計画(1 次行動計画)

2005 年 4 月に内閣官房情報セキュリティセンター(旧 NISC)が設置され、2005 年 5 月に IT 戦略本部の下に情報セキュリティ政策会議(議長:内閣官房長官、ISPC)が設置された。ISPC 及び旧 NISC は、喫緊の課題となっていた中期計画や政府機関の情報セキュリティ対策のための統一基準の策定・決定を行った²⁷。並行して、重要インフラの情報セキュリティ対策について、重要インフラ専門委員会で検討が進められた。そして、2005 年 12 月 13 日に最初の行動計画である「重要インフラの情報セキュリティ対策に係る行動計画」(1 次行動計画)を ISPC が決定した²⁸。

その決定プロセスについては、まず、ISPC が 2005 年 7 月 14 日の初会合で、特別行動計画の改定に向けた検討、安全基準・ガイドラインの策定・見直し等の取組及び同基準等に基づく点検等の推進、ISAC の創設支援及び分野横断的演習等を通じた重要インフラ防護体制の検証を進めることを決定した²⁹。その後、2005 年 9 月 15 日の第 2 回 ISPC 会合で、2 次提言を踏まえ、「重要インフラの各事業において発生する『IT 障害』から重要インフラを防護し、重要インフラ事業者の事業継続性を確保するため、特別行動計画及びこれに基づく取り組みを発展・強化させた新たな行動計画をとりまとめる」ことを決定³⁰した。同決定に基づき、ISPC の下に優れた見識を有する者(重要インフラ事業者となりうる者、その業界団体や学識経験者等)から構成される重要インフラ専門委員会を設置³¹し、1 次行動計画の検討が進められ、上述のとおり同年 12 月に ISPC が決定したものである。

1 次行動計画の内容は、基本的には 2 次提言を踏まえたものとなっている。対象分野は、「情

報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」及び「物流」の10分野とした。国民生活や社会経済活動に重大な影響を及ぼさないようIT障害から防護し、事業継続の取組強化を促すべく、それぞれの分野に属する者から、重要インフラ事業者等³²として電気通信事業者、銀行等を指定し、それらのネットワークシステム、勘定系システムなどを防護の対象とした³³。安全基準等については、内閣官房が「重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針」（安全基準等策定指針）³⁴を策定し、それを踏まえて、それぞれの事業分野が、必要又は望ましい対策の水準を安全基準等に明示することとした。

情報共有体制については、情報共有のみならず、自身が所属する産業分野に属するメンバー間で、セキュリティ強化策の実装・展開までやるべきとの考え方から³⁵、ISACではなく、CEPTOAR（Capability for Engineering of Protection, Technical Operation, Analysis and Response：セプター）と呼ばれる体制の整備を進めることとした。同時に、分野横断的な情報共有の場として、セプターの代表で構成される重要インフラ連絡協議会（CEPTOAR-Council）の創設もされることとなった。

加えて、重要インフラの情報セキュリティ確保では重要インフラ分野間の相互依存性の認識とレジリエンスの評価が必要であることから、相互依存性解析を行うこととした。また、想定される脅威シナリオ類型をもとに毎年度重要インフラ所管省庁・重要インフラ事業者等・セプター等の協力を得て分野横断的な演習を行うこととされた（実施状況については4.3を参照。）。

以上をまとめると、1次行動計画は、2次提言を踏まえて、対象を10分野とし、政府が示した指針等を踏まえた業界の事情にあった安全基準等の業界による整備、自主的な情報共有・セキュリティ対策実装体制の強化、相互依存性解析³⁶及び分野横断的演習を柱とする内容を整備したもののといえる。

3.2 重要インフラの情報セキュリティ対策に係る第2次行動計画（2次行動計画）

2009年2月3日、ISPCは、1次行動計画を改定し、重要インフラの情報セキュリティ対策に係る第2次行動計画（2次行動計画）³⁷を決定した。1次行動計画決定後に、重要インフラ事業者等におけるITの利活用がさらに広がったこと、サービス利用者においても、ITを利用したサービスに触れる機会が増えていることなど社会におけるIT依存度の高まりから、重要インフラ事業者等の自主的な取組みを充実させることが求められたこと³⁸が改定の背景である。

2次行動計画は、「『重要インフラ事業者等のサービスの維持』のためのIT障害の予防的対策と、『IT障害発生時の迅速な復旧等の確保』のためのIT障害の事後的対策の両方について、必要な対策を広く具体化」³⁹したものとなっている。このアプローチは、2次行動計画と同時にISPCによって決定された第2次情報セキュリティ基本計画⁴⁰において「『事故前提社会』への対応力強化」を一つの計画推進の観点にしていることと整合的であるといえる。

2次行動計画は、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「共通脅威分析」、「分野横断的演習」及び「環境変化への対応」の5項目を、その柱とした。「安全基準等の整備及

び浸透」では、安全基準等策定指針を原則3年に1度の頻度で改定を行い、継続的に安全基準等の改善を図るとした。「情報共有体制の強化」では、内閣官房、重要インフラ所管省庁、セプター、重要インフラ事業者等において各々が整備している情報共有に係るルールの整合を図るなどとした。「共通脅威分析」では、重要インフラ分野に共通に起こりうる脅威が何であるかを把握するための分析などを行うとした。「分野横断的演習」では、脅威に関する最新動向を踏まえた演習シナリオによる演習を継続的に実施するとした。「環境変化への対応」では、社会環境、技術環境等の状況が変化するため、情報セキュリティ対策の有効性を保ち続けるべく、「広く国民に対しての広報公聴活動、当事者間のリスクコミュニケーション、国際連携等を通じて、関係主体各々が」、「環境の変化を察知する能力の向上に努めること」⁴¹とした。

以上をまとめると、2次行動計画は1次行動計画を継続・発展させるかたちで、予防的対策と事後的対策の両方をバランスさせて促進することを目指すものであった。

3.3 重要インフラの情報セキュリティ対策に係る第3次行動計画(3次行動計画)

2014年5月19日、ISPCは、重要インフラの情報セキュリティ対策に係る第3次行動計画(3次行動計画)⁴²を決定した。

3次行動計画は、2次行動計画の評価結果を踏まえ、また、「東日本大震災発災時のシステム障害、データ滅失等への対応において得られた知見等の活用に加え、刻々と変化する社会環境・技術環境、近年の複雑化・巧妙化するサイバー攻撃の趨勢への適切な対応を反映」⁴³すべく、策定されたものである。

ここで、東日本大震災への対応において得られた知見等とは、事業継続計画(BCP)の重要性や石油製品の供給の重要性などである。BCPの議論の背景には、「東日本大震災の震源域は1,000キロメートル以上にわたり」、「東京・大阪間の400～500キロメートルの距離だと両方被災をする可能性がゼロではないため」、「バックアップが同じリスク要因によって倒れることがないようにすべき」というものである。また、「石油製品の輸送が途絶すると、通信基地局などの機能も止まって」しまうが、「東日本大震災の際、太平洋側の石油製品の輸送ができなくなり通信基地局が1日半」「ストップする事態に陥」ったこともその背景にある⁴⁴。

重要インフラ事業者の分野については、上述のような背景事情を受けた検証を行い、従来の10分野に加えて新たに「石油」、「化学」、「クレジット」の3分野が追加され、全体で13分野となった。クレジットは、情報システムが障害に至った場合の影響として、処理するサービス提供の価値及び規模の観点から大きいと加えられた。「化学」は、情報システムが障害に至った場合の影響として、制御が困難な状態において生じ得るリスクが大きいと考えられたため加えられた。「石油」は、「化学」と同じ理由に加えて、既存の重要インフラ分野における情報システムに与える影響も考慮されて追加されている⁴⁵。

3次行動計画では、5つの柱として「安全基準等の整備及び浸透」、「情報共有体制の強化」、「障害対応体制の強化」、「リスクマネジメント」及び「防護基盤の強化」が置かれた。

「安全基準等の整備及び浸透」は従来からの取組をさらに深めたものである。

「情報共有体制の強化」は、柱としては従来からあるところ、3次行動計画では、内閣官房（事態対処・危機管理担当）、重要インフラ所管省庁、セプター、重要インフラ事業者等との連携による大規模IT障害対応時の情報共有体制が明記された⁴⁶。また、新たに「情報連絡・情報共有について」を別添として設け、災害防止に結び付ける目的の活動であるヒヤリハット⁴⁷に係る情報の共有についても行うこととした点に特徴がみられる。

「障害対応体制の強化」は、新たな柱に見えるが、これは、従来からの「分野横断的演習」に加えて、物理的な要因によるIT障害への対応や、各分野のセプターと重要インフラ所管省庁との間の情報共有体制の強化を図るセプター訓練を通じて、「重要インフラ全体の防護能力の維持・向上を図る」ことを明確化し、重要インフラ事業者における体制強化の取組として束ねたものである。

その上で、新たに柱の一つとして位置づけられたものとして、「リスクマネジメント」がある。これは、「国民に対する重要インフラサービスの安定的供給や事業継続等といった事業目的の達成に向け」、「情報セキュリティに係るリスク源から導き出されるリスクに対する包括的なマネジメントを行う必要性」⁴⁸の高まりから打ち出されたものである。「重要インフラ事業者等におけるリスク評価手法等に基づく情報セキュリティ対策の重点化を目的に、第2次行動計画の『共通脅威分析』及び『リスクコミュニケーションの充実』（『環境変化への対応』の一施策）を包括的に捉え直し、各重要インフラ事業者等が主体的に行うリスクマネジメントに係る施策を新たに実施」⁴⁹するとした。「リスクマネジメントは各重要インフラ事業者等がそれぞれにおいて主体的に実施」される。一方で、重要インフラサービスは相互に関連しているものであり、「共通的なリスクマネジメントの考え方や用語による情報共有及び議論」が必要である。そこで、「国際的にも標準的なリスクマネジメントの考え方やそこで利用される情報セキュリティに関わる用語の定義等を利活用することが望ましい」としている⁵⁰。

5番目の柱である「防護基盤の強化」は、他の4つの柱を支えるものである。その内容は、広報公聴活動、国際連携及び規格・標準及び参照すべき規程類の整備である。

3次行動計画の特徴として、経営層の役割を明確化している点を挙げられる。すなわち、重要インフラのサービスの持続的提供、そのためにIT障害の発生を可能な限り減らし、IT障害発生時の迅速な復旧を図るという重要インフラ防護の目的を達成するために、経営層のリーダーシップによるリスクマネジメント、経営資源の継続的確保、障害対応体制の検証・改善といったことが強調されている。そして、経営層に訴求するように、3次行動計画の中で簡潔に記載されたページを用意した⁵¹。こうした経営層の役割の明確化は、業界団体からの要望を受けたものであった⁵²。

3.4 小括

ISPCのもとで旧NISCが事務局となり推進した重要インフラの情報セキュリティ対策は、IT戦略本部了承の2次提言を踏まえて、重要インフラサービスそのものの維持・復旧を目的とし、重要インフラ事業者の事業継続などを重視するものとなった。そのための情報セキュリティ対策というこ

とで、サイバー攻撃に起因するもののみならずバグ等の非意図的要因や自然災害に起因する IT 障害も対象としていることが、それまでの特別行動計画のもとで進められた情報セキュリティ対策とは異なる点である。また、重要インフラ相互間の依存関係を分析し、分野横断的な演習を開始したことなど、分野横断的なアプローチとなった。加えて、3 次行動計画からはリスクマネジメントの手法の導入、経営層の役割の明確化なども図られ、より組織的な取組を推進するようになった点は、その後の政策の方向付けしたものとなっている。なお、安全保障との関係については、2 次提言において重要インフラの防護が「安全保障・危機管理に資すること」になると副次的効果を指摘していたものの、1 次から 3 次までの行動計画において、明示的な記述はない。

4. サイバーセキュリティ基本法制定後の政策

重要インフラ事業者は、サイバーセキュリティ基本法(2014 年 11 月 12 日施行。以下「基本法」という。)第 3 条において、「重要社会基盤事業者」として、「国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者をいう」と定義された。これは、従来からの基本計画や行動計画におけるものと基本的に同じである。そして、同法第 6 条で、「重要社会基盤事業者は、基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする」と、重要インフラ事業者の責務が示された。重要インフラの行動計画については、基本法に基づき設置されたサイバーセキュリティ戦略本部(本部長:内閣官房長官。以下「CSHQ」)が、同法第 26 条第 5 号の事務として決定している。

4.1 重要インフラの情報セキュリティ対策に係る第4次行動計画(4 次行動計画)

2017 年 4 月 18 日、CSHQ は、「重要インフラの情報セキュリティ対策に係る第4次行動計画」(4 次行動計画)⁵³を決定した。同計画は、基本法に基づく初めてのサイバーセキュリティ戦略⁵⁴(2015 年 9 月 4 日閣議決定。以下「2015 戦略」という。)を踏まえて策定されたものである。情報通信技術(IT)と制御システム等の運用技術(OT)との融合、IoT(Internet of Things)システムの普及といった環境変化や、2020 年東京オリンピック・パラリンピック競技大会(以下「TOKYO2020」)の開催を控えて重要インフラを取り巻くリスクが高まるなか、それまでの対策のさらなる強化・改善を目指したものであった。

4 次行動計画の柱は、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「障害対応体制の強化」、「リスクマネジメント及び対処態勢の整備」及び「防護基盤の強化」の5つである。これらは、基本的⁵⁵に 3 次行動計画の骨格を継続したものとなっている。「安全基準等の整備及び浸透」では、2016 年 9 月に電気事業法に係る省令でサイバーセキュリティに関する規定が整備された⁵⁶ことなどもあり、「情報セキュリティ対策を関係法令等における保安規制として位置付ける」分

野を広げるなどの方針⁵⁷が示された。「情報共有体制の強化」及び「リスクマネジメント及び対処態勢の整備」については、後述する。「障害対応体制の強化」は、分野横断的演習の質的改善などである。「防護基盤の強化」では、行動計画として初めて「国の安全等の確保の観点からの取組」として「安全保障」が言及された⁵⁸。

4 次行動計画の特徴として、「機能保証」という考え方を導入した点を挙げられる。「機能保証（任務保証）」の考え方は、2015 戦略で、「業務責任者（任務責任者）がシステム責任者（資産責任者）と重要インフラや政府機関の機能やサービスを全うするという観点からリスクを分析し、協議し、残存リスクの情報も添えて経営者層に対し提供し総合的な判断を受ける『機能保証（任務保証⁵⁹）』の考え方に基づく取組⁶⁰として示されたものである。2015 戦略を踏まえて策定された 4 次行動計画では、これを「各関係主体が重要インフラサービスの防護や機能維持を確約することではなく、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うこと⁶¹と説明した。

2015 戦略では、「機能保証」を、ミッションを達成するためのリスクマネジメントの考え方として示したものであったが、行動計画ではプロセスについての責任の位置づけに変えたように見える。その理由としては、重要インフラ事業者と顧客との関係で、「保証」が 100%のレベルのサービスを確約するというように誤解されることへの懸念が惹起され、重要インフラ事業者によるサービス契約の実態などを踏まえるように記述を修正したためと考えられる。いずれにせよ、重要インフラサービスの安全かつ持続的な提供の実現を重要インフラ防護の目的⁶²としている点には変わりはない。

4 次行動計画では、3 つの重点的な取組方針を示している。まず、重要インフラ事業者等における先導的取組の推進を挙げた。これは、他の重要インフラ分野からの依存度が高く、かつ、比較的短時間の重要インフラサービス障害であってもその影響が大きくなるおそれのある重要インフラ分野（例：電力、情報通信、金融）では、主要な事業者において相対的に高度な対策を自主的に実施している実態がある。この実態を踏まえ、当該事業者の取組をさらに強化・推進するとともに、当該重要インフラ分野内の他の事業者や他の重要インフラ分野にも自主的な取組を広めていく施策を進めるというものである。

2 つ目は、4 次行動計画の期間中に TOKYO2020 の開催をはじめ多数の国際的イベントが予定されていることから、情報共有体制の強化を含めて TOKYO2020 等を念頭に置いた施策を推進することである。例えば、情報共有体制について所管省庁を経由して内閣官房に提供する仕組み（業法等に基づき所管省庁に報告されたら、基本法及び CSHQ の決定⁶³に基づき所管省庁の長は CSHQ に報告する仕組み。事務は内閣サイバーセキュリティセンター（NISC）が行う。）がある。しかし、法令等によって義務付けられていないヒヤリハットによる障害情報については、それを所管省庁に報告することで所管省庁からの指導等につながるのではないかと懸念が払しょくできない状況にあった⁶⁴。そこで、法令等で義務付けられていない情報はセプター事務局経由で匿名化等を行ったうえで所管省庁に報告することも可能⁶⁵とされている。

また、2 つ目の取組方針の一環として深刻度に係るものもある。重要インフラサービス障害につ

いては深刻度に応じて影響範囲や対処行動が異なることから、関係者間での認識の共有を図り、迅速で効果的な情報共有を実現すべく、重要インフラサービス障害に係る深刻度の判断基準の例を示すこととした。2018年7月に、「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準」⁶⁶がCSHQによって決定されている。この深刻度の考え方は、2016年に米国政府で示されている⁶⁷が、こうした動向が背景にあるといえる。

3つ目はリスクマネジメントを踏まえた対処態勢整備の推進である。2017年1月にNISCから公表された「2020年東京オリンピック・パラリンピック競技大会のサイバーセキュリティの確保に向けたリスク評価資料」⁶⁸を基に重要インフラ事業者向けに作成しなおした「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」⁶⁹を2018年4月に公開した。また、事業継続計画及び緊急時対応計画（コンティンジェンシープラン）の策定等による重要インフラ事業者等の対処態勢の整備を図るとした。

4次行動計画は2回改訂されている。1回目の改定は、2018年7月に、14番目の重要インフラ事業者分野として「空港」が追加されたもの⁷⁰である。4次行動計画策定時に、対象範囲の見直しを継続的に行うとしていた。そして、空港については、「関係企業による自主的な取組として情報共有等に係る枠組み（空港SIG: Special Interest Group）が構築されるに至っている」と記された⁷¹。継続的見直しのなかで、関係企業等との調整がついた結果「空港」が追加されたものである⁷²。2回目の改定は、4次行動計画期間中に、重要インフラ「分野によっては、安全基準等の名称等の変更や法改正に伴う条ずれが生じたりしていることから、行動計画を一部改定」したものである⁷³。

4.2 重要インフラのサイバーセキュリティに係る行動計画（5次行動計画）

2022年6月17日、CSHQは、「重要インフラのサイバーセキュリティに係る行動計画」（5次行動計画）⁷⁴を決定した。本行動計画は、COVID-19禍のなかでのデジタル技術活用の加速、国際情勢・地政学の変化、TOKYO2020の開催等の大きな環境変化を背景として2021年9月に閣議決定されたサイバーセキュリティ戦略（2021戦略）⁷⁵を踏まえて策定されたものである。

重要インフラにおいて、「一部分野において、環境変化に起因するサービス障害がすでに発生」し⁷⁶、重要インフラサービス障害のリスクは、「サイバー攻撃だけではなく、自然災害、人的要因等の多岐にわたり、特に、適切な組織管理がなされれば防げたサービス障害が目立ち始め」、「システム間の連鎖が進み、サービス障害による影響が大規模化する傾向にある」こと⁷⁷が、5次行動計画策定にあたって重視されている。この点は、柱の構成において、「障害対応体制の強化」が第一に位置付けられたことにも表れているといえる。5次行動計画の「障害対応体制の強化」では、特に、組織統治の一部としてのIT障害対応体制が強調された。具体的には、サイバーセキュリティに関する体制は、経営層の義務として構築が求められる内部統制システムの一部といえるとしていること、会社法における役員等の責任が生じる場合があることなどを指摘している。「経営層、CISO、戦略マネジメント層、システム担当者等の組織全体及びサプライチェーン等に関わる事業者における役割と責任を明確にした上で、サイバーセキュリティの専門的・技術的な問題点と、経

営層が抱えている事業運営の問題点を融合させることが必要である」⁷⁸と示し、「しかしながら、経営層がサイバーセキュリティの専門的な知見を必ずしも有するとは限らないため、サイバーセキュリティの知見を有する人材を経営層に取り込むという、より実効的、現実的な選択を示し」⁷⁹たものとなった。また、官民一体となった障害対応体制、情報共有体制の強化として安全保障の観点からの取組強化の方針が示された⁸⁰。

5 次行動計画においても5の柱が示されており、先述した「障害対応体制の強化」に続き、2番目が「安全基準等の整備・浸透」、以下、「情報共有体制の強化」、「リスクマネジメントの活用」及び「防護基盤の強化」となっている。「リスクマネジメントの活用」は、「障害対応体制の強化」を具体化するためのものとされている。その内容は、「重要インフラ事業者等がリスクマネジメントに的確に取り組むためには、まず自組織の特性（プロファイル）を把握し、さらに自組織に適した防護対策については、計画、実施、評価・改善を繰り返し、継続的な取組（プロセス）を推進することが求められる」⁸¹としている点が特徴的である。自組織に適した防護対策を実現するにあたり、プロファイルを重視する考え方は、米国立標準技術研究所（NIST）が策定した「サイバーセキュリティフレームワーク（CSF）」⁸²を参考としているといえる。すなわち、CSF では「組織のリスクを明確にするためには、組織が提供するサービスの特徴や組織がどうありたいのかといった組織の特性（プロファイル）を当初に明らかにする必要」⁸³あるとしているからである。

2024 年 3 月、5 次行動計画は、15 番目の重要インフラ分野として「港湾」を追加するべく改定⁸⁴された。これは、2023 年 7 月に、サイバー攻撃によって名古屋港コンテナターミナルにおいてシステム障害が発生し約 3 日間にわたりコンテナ搬入出作業が停止したことを受けて、国土交通省が「コンテナターミナルにおける情報セキュリティ対策等検討委員会」を設置⁸⁵し、重要インフラ分野に「港湾」を追加する方向で検討する旨を最終とりまとめに記載したことなどを踏まえたものである。

4.3 分野横断的演習

分野横断的演習は、2006 年度から現在に至るまで毎年度実施されてきている。1 次行動計画を受けて、初回は 2007 年 2 月に東京の会場にて、首都圏の重要 IT 関係施設で IT サービス停止等が発生し、決済機能等の低下等、複数分野に波及・影響したという想定での官民における連携・情報共有の枠組み等を検証すべく机上演習を行った⁸⁶。その後、官民連携体制の機能・実効性向上を図るべく分野横断的演習は継続され、例えば、2008 年度（12 月実施）には、参加者に IT 障害の発生原因を知らせない等の現実に近い状況で、起こった現象に関する関係者間の情報共有により原因を特定し、サービスの維持・早期復旧、事業継続等を行っていく演習を実施している。2 次行動計画期間中は、重要インフラ事業者における事業計画等の実行性の確認・問題点抽出を目標とし、広域停電、大規模通信障害、重要インフラ複合障害、情報セキュリティインシデントなどをテーマに演習を行った⁸⁷。

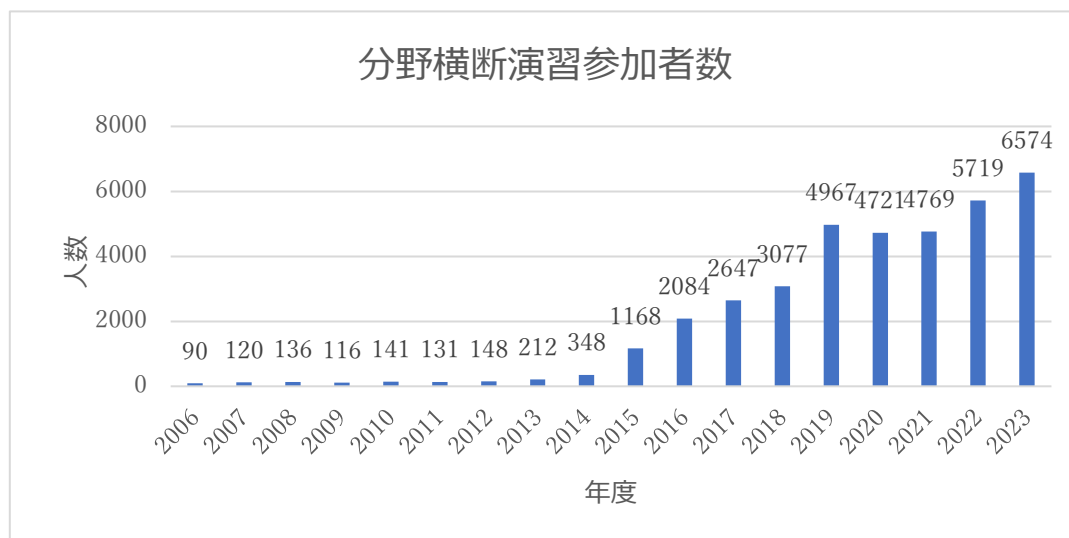
3 次行動計画のもとでは、重要インフラ全体の防護能力の維持向上を図るため、事業者等による情報セキュリティ対策の実施及び実効性確認等を通じた障害対応能力の向上を目指すことを

目標とした。2014 年 12 月実施の演習では、IT 障害対応に関する能力向上及び検証を目的とする他の演習・訓練との連携を強化することにより、重要インフラ全体の防護能力の維持・向上を図るべく、首都圏以外の事業者等参加を促進し、また、自職場からの参加を充実させた⁸⁸。2015 年及び 2016 年の 12 月に実施された演習では、演習内容を2部制にし、標的型攻撃やランサムウェア攻撃を受けたときの情報共有体制の実効性検証、DDoS 攻撃等を受けたときの事業継続計画の発動などについて演習した⁸⁹。

4 次行動計画のもとでは、「機能保証」の考え方を踏まえた演習となったが、2017 年 12 月実施の演習内容は 2016 年度の延長上のものとなっている。演習の結果、気づきの点について、2018 年 1 月に意見交換会を行って演習参加者等と共有するなどの取組も行った。2018 年度の演習では、TOKYO2020 をも視野に入れたシナリオ(サービス障害に関するレピュテーションリスクへの対応等)による演習を実施⁹⁰した。その後の演習も、TOKYO2020 に向けて最大限に活用することとして開催⁹¹することとした。しかしながら、2020 年に発生した新型コロナ禍の影響で、2020 年及び 21 年の 12 月に実施した演習は集合会場での演習を行わず自職場(テレワークを含む)から参加する形式に変更してランサムウェア攻撃への対応などをテーマに実施することとなった⁹²。2022 年 12 月に実施した演習では、集合会場と自職場等(テレワークを含む)のハイブリッド形式として、ランサムウェア攻撃、サプライチェーン攻撃及び Emotet に対する対応について確認するなど重要インフラ事業者等の障害対応体制に対してその有効性の検証⁹³を行った。

5 次行動計画のもとでの演習は、2023 年 12 月に集合会場と自職場(テレワーク含む)のハイブリッド形式で、机上演習を実施した。その内容は、演習シナリオとして、「最新のサイバー情勢等を踏まえ、インシデント対応における経営層の参画や取引先等を含むサプライチェーンリスク対策を踏まえた状況付与を実施」した。また、「重要インフラ事業者等間の平時からの情報共有体制の構築を促進」するべく「演習当日の集合会場において、演習参加者等同士が有識者も交えて対面で意見交換を行う座談会を開催している⁹⁴。

参加者数の推移(図1参照)をみると、1 次及び 2 次行動計画の期間中の演習参加者は百数十名規模が続いた。3 次行動計画の期間となり、重要インフラの分野が追加され、また、会場を東京に加えて大阪を加え、自職場からの参加も可能としたことから、参加者数は、2014 年度は三百名規模となった。これが 2015 年度には一千名を超える規模となった。その背景には、2015 年 5 月に発生した不正アクセスによる日本年金機構からの情報流出事件があると考えられる。同事件の結果、サイバーセキュリティ対策の重要性が広く認識されるようになった結果といえよう。さらに、2017 年度からは福岡会場も置かれるようになった。こうしたこともあり、順調に参加者数は増加している。加えて、2019 年度からは TOKYO2020 の演習としても最大限に活用した。



(NISC の分野横断的演習に係る結果の資料から作成)

図 1 分野横断的演習参加者数の推移

分野横断的演習への参加者数は大きく増加してきているが、これは NISC による演習方法の充実や、事業者におけるサイバーセキュリティ対策の重要性についての認識の一層の高まりなどの結果であると考えられる。

4.4 小括

CSHQ のもとで推進されてきている重要インフラ対策は、ISPC のもとで推進されたものと同様に、重要インフラ事業者自らの取組として実施されるべく、重要インフラ事業者、所管省庁及び関係者との検討・協議・合意を経て、重行動計画をとりまとめるという形で進められてきている(行動計画の柱の推移は図2を参照)。同時に、基本法その他の法令との関係の明確化も図られてきている。

1次行動計画 1. 安全基準等 2. 情報共有体制の強化 3. 相互依存性解析 4. 分野横断的演習	2次行動計画 1. 安全基準等の整備・浸透 2. 情報共有体制の強化 3. 共通脅威分析 4. 分野横断的演習 5. 環境変化への対応	3次行動計画 1. 安全基準等の整備・浸透 2. 情報共有体制の強化 3. 障害対応体制の強化 4. リスクマネジメント 5. 防護基盤の強化	4次行動計画 1. 安全基準等の整備・浸透 2. 情報共有体制の強化 3. 障害対応体制の強化 4. リスクマネジメント、対処体制の整備 5. 防護基盤の強化	5次行動計画 1. 障害対応体制の強化 2. 安全基準等の整備・浸透 3. 情報共有体制の強化 4. リスクマネジメントの活用 5. 防護基盤の強化
---	---	---	---	--

図2 重要インフラ行動計画の柱の推移

重要インフラ防護の目的も従来と同様に、サイバー攻撃のみならず自然災害や非意図的な要因によるものも含めて IT 障害による重要インフラ事業者のサービスへの影響を抑えることにある。具体的対策の策定にあたっては、重要インフラ事業者及びその経営層などが認識・理解・実施で

きるようにされており、例えば、リスクマネジメントについては事業者の理解のレベルに応じて導入できるように作りこまれてきた。また、分野横断的演習も、会場・参加形態を拡充などしてきている。

法令等との関係については、サイバーセキュリティ対策を法令等における規制として位置付けが開始された。また、インシデントの情報について、法令等により所管省庁経由で内閣官房に伝えられる枠組もできた。一方で、法令等に基づかないヒヤリハットに関するものについては、セプターを介して匿名化して所管省庁を経由し内閣官房に伝達するなど、事業者の懸念を払しょくするようなものとなっている。

安全保障との関係については、基本法 1 条に「サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする」とされ、それを踏まえた 2015 戦略で安全保障に関連する柱が設けられた後に策定された 4 次行動計画で言及が始まった。5 次行動計画でも、情報共有体制の強化が言及されている。

5. 経済安全保障・国家安全保障政策との関係

5.1 経済安全保障政策との関係

安保戦略 2022 によると、経済安全保障とは、「日本の平和と安全や経済的な繁栄等の国益を経済上の措置を講じ確保すること」⁹⁵である。経済安全保障に係る政策のうち、重要インフラのサイバーセキュリティ政策に関連するといえるものとして、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律(令和 4 年法律第 43 号。経済安保推進法)における基幹インフラ役務の安定的な提供の確保が挙げられる。

基幹インフラ役務とは、経済安保推進法第 50 条で規定される「特定社会基盤役務」を指し、その定義は、「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」である。電気、ガス、石油、水道、鉄道、貨物自動車運送、外航貨物、航空、空港、電気通信、放送、郵便、金融、クレジットカードの 14 分野が同法によって特定されている。そして、具体的事業者の指定基準を事業所管大臣が省令で定め、該当する者を告示する。指定対象とする設備等も各大臣が省令で規定する⁹⁶。なお安保戦略 2022 において、対象拡大の検討を進める⁹⁷としているが、基幹インフラの分野に「港湾」の追加が予定されている⁹⁸。

これら分野の多くは行動計画で定める重要インフラの分野と同じである。分野に係る定義を比較すると、重要インフラと基幹インフラは、いずれも「国民生活及び経済活動の基盤」である点は同じである。しかし、その機能や役務に支障が生じたときに、前者は「国民生活及び経済活動への多大な影響」があるもの、後者は「国家及び国民の安全を損なう事態を生ずるおそれ」があるものであり、この点で両者は異なるものとなっている。

基幹インフラに係る制度は、経済安保推進法第三章「特定社会基盤役務の安定的な提供の確

保」において「事前審査制度」が規定される。具体的には、基幹インフラ役務を提供する事業者は、重要設備の導入・維持管理等の委託に関する計画書を事前に届出なければならない。計画書には、対象となる設備の概要、導入時期のほか、設備の供給者（代表者・住所・代表者の国籍など）や、「重要設備に悪意のあるコード等が混入していないかを確認するための受入検査その他の検証体制が構築されており脆弱性テストが導入までに実施されること」などのリスク管理措置についての資料が含まれる⁹⁹。そして、政府の審査の結果、重要設備が国外から妨害する行為の手段として使用されるおそれ大きいと認めるときは、妨害行為を防止するため必要な措置（重要設備の導入・維持管理等の内容の変更・中止等）の勧告がなされる。この義務は罰則によって担保される。このように義務的・規制的なものが基幹インフラ事業者には課されている。この点は、事業者と政府との間で合意に基づく任意の制度（基本法上では責務が示されている）や施策の対象となる重要インフラ事業者の地位とは大きく異なっている。

懸念する事態については、基幹インフラに関しては、経済安保推進法第 50 条で規定されるように「我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為の手段」が前提にある。そして、そのような妨害の行為には、サイバー攻撃などの電磁的な方法によるものだけでなく、爆発物を仕掛けるなど物理的な方法によるものも該当しうるとする¹⁰⁰。これらの点は、サイバー攻撃のみならず自然災害、非意図的な原因も含めた IT 障害によるサービスへの影響を想定した重要インフラに関する政策とは異なるものである。

5.2 国家安全保障政策との関係

サイバー関連で重要インフラに係る安全保障政策として、安保戦略 2022 において、能動的サイバー防御の実施のために必要なもののひとつとして「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の取組を進める」措置の実現に向けた検討が明記されている¹⁰¹。ただし、ここでいう情報共有¹⁰²が義務的なもの又は任意なもののいずれであるかについては、安保戦略 2022 の文言からは明らかではない。義務的なものであるとすれば、法整備が必要であるところ、能動的サイバー防御の実現に向けた法整備については、現時点（2024 年 4 月 30 日現在）では検討段階にあるものと考えられる¹⁰³。

そこで、本件について考察してみるため、諸外国における政府へのインシデント情報の伝達に係る制度の例をみる。EU では Network and Information Security (NIS) 2 指令¹⁰⁴ によって、構成国は 2024 年 10 月 17 日までに、エネルギー、運輸、銀行等の基幹サービス事業者や郵便・宅配、デジタルプロバイダーなどの重要なサービス事業者に対して、重大なサイバーインシデントが発生したときには 24 時間以内に早期報告、72 時間以内にインシデントの重大度・影響・侵害の兆候などについての初期評価を行うための報告の義務付けなどを規定した国内法を施行することになっている¹⁰⁵。シンガポールにおいても、サイバーセキュリティ法に基づき、重要インフラ事業者はサイバーインシデントが発生したときにはサイバーセキュリティ長官に報告する義務がある¹⁰⁶。米国で

は、2022 年 3 月に重要インフラのサイバーインシデント報告法(CIRCIA)がバイデン大統領により署名された¹⁰⁷。CIRCIA により対象とされる事業者は、対象となるサイバーインシデントがあった場合とランサムウェアの支払いをした場合にサイバーセキュリティ・インフラストラクチャ・セキュリティ庁(CISA)に報告することを義務付けられる¹⁰⁸。CISA は報告義務の範囲、手続き等を定めるプロセスを進めているところである。

これらの動向から考えるに、能動的サイバー防御政策「政府への情報共有」に係る検討においても、義務的なものが目指されると推測される。ただし、重要インフラを含む民間企業等においては、通常、「インシデント対応現場では、いかに被害を把握し業務を正常な状態に戻すかということが最優先であり、限られたリソースの中で、同時並行／複数の外部とのやりとりを行うことは大きな負担」¹⁰⁹となることに注意が必要である。また、政府へ共有された情報は、政府から、効果的に他の民間事業者等に情報共有され、被害拡大防止・再発防止、被害事業者支援などに活かされることが期待される。

6. 重要インフラに関するサイバーセキュリティ政策についての考察

6.1 重要インフラのサイバーセキュリティ政策についての考察

ここまで、我が国の重要インフラに係るサイバーセキュリティ政策について、その変遷と、安全保障政策との関係を概観した。重要インフラに係るサイバーセキュリティ政策については、事業者等との調整が順調に進み分野が拡大してきていること、分野横断的演習参加者が順調に増加していることなどからみて、事業者におけるサイバーセキュリティに対する意識は高まってきており、政策効果が妥当に高まっていると考えられる。このことを踏まえて、重要インフラに係るサイバーセキュリティ政策立案・実施にあたって重視されてきたことであって引き続き基本とすべきと考える点について指摘したい。

- ① 重要インフラのサイバーセキュリティ政策は、引き続きサイバー攻撃のみならず、非意図的要因、自然災害が原因となる IT 障害によるものも含めて対策を講ずることが求められる。2 次提言・1 次行動計画から継続されている政策の基本的な姿勢である。基本法において「機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼす」ことから守ることを明記されていること、すなわち国民生活及び経済活動の視点からすれば、要因に関係ないことから明らかである。
- ② 重要インフラ事業者自らの意思による機能の停止・低下を防ぐ努力を促すような環境整備や信頼関係に基づく政策が重要である。この点、法令等に基づくサイバーセキュリティ関連規定の整備もなされている。しかし、法令等に基づく義務的な取組は、基準に該当するかどうか判断材料になってしまう。法令等に基づかないヒヤリハットの情報共有などもハインリッヒの法則にかんがみて大切であるところ、こうした活動を促進するためには、政府と事業者間での信頼関係や、事業者自ら、その重要性を理解することが重要である。分野横断的演習の活用や、経営層に訴求するようナスクマネジメント等の説明、話法などは引き続き重要になろう。

- ③ 重要インフラ事業者のサイバーセキュリティ対策についての柔軟な政策企画・立案・実施体制が重要である。重要インフラの対象分野は、当初の 7 分野から 15 分野まで増加してきた。新たに追加する過程では、業界との間の調整、事業者における対応体制の整備などのプロセスが進められてきている。そして、任意の取組として整ったところから追加されている。また、重要インフラ事業者におけるデジタル化の進展、サイバー攻撃の洗練度など常に変化しており、これらに対応した政策の立案・実施も求められる。こうした取組は、法令等に基づく比較的硬直的なものよりも、随時、柔軟に取組める体制とした方が有利である。引き続き、こうした柔軟な体制の維持が重要になろう。

6.2 重要インフラに関する安全保障政策との関係についての考察

次に、今後の重要インフラに関するサイバーセキュリティ政策立案・実施にあたって、安全保障政策との関係から、考慮すべき観点を指摘したい。

- ① サイバーセキュリティ政策と安全保障政策とはテクニカルに似ており密接に関連する部分もある¹¹⁰が、本来的には異なる政策分野である。特別行動計画・行動計画の経緯を見ても、安全保障の用語が明記されるようになったのは、基本法が施行され、それを踏まえて策定された 4 次行動計画以降である。同法に基づく戦略において、「国際社会の平和・安定及び我が国の安全保障への寄与」という柱¹¹¹があるが、これは「寄与」である。これらが示すことは、安全保障政策、とりわけ、防衛については、サイバーセキュリティ政策ではなく、防衛政策において方針が示されるべきもの¹¹²ということである。サイバーセキュリティ自体が手段であることからしても明らかであるが、サイバーセキュリティ政策から目的が異なる安全保障政策に対して変更を加えるものではない。なお、サイバーセキュリティ政策には、6.1①や基本法における重要インフラの定義からも明らかなように、安全保障政策以外のものも含まれるため、安全保障政策の観点から、サイバーセキュリティ政策が大きく変更されるようなことが生じる場合には注意が必要であることについても言うまでもない。
- ② 重要インフラ事業者に求める義務的事項と任意の政策のバランスと連携が重要である。経済安全保障推進法においては、基幹インフラ役務の提供者に義務的な事前審査制度を創設した。サイバーのみならず物理的な手段も含め、国家・国民の安全を損なう事態を引き起こしかねない妨害行為に対する対策であり、義務的な措置に当然の理由がある。そして、罰則で担保する制度であるため、その適用範囲の外縁・基準は法令により明確化されている。ただし、その結果、適用範囲外のもの、基準に至らないものについては、有益な措置であっても義務的制度的対象にはならない。サイバーセキュリティ政策については、6.1②及び③で述べたように、任意の措置、柔軟な対応が求められるところ、関連政策当局が常に対等に連携して、義務的事項と任意の政策のバランスを図ることが重要であると考ええる。
- ③ 重要インフラ事業者に負担を求める事項に関して負担の軽減策の考慮が必要である。例えば、経済安全保障推進法第 49 条第 4 項に、「指針の案を作成するときは」、「経済活動に与

える影響に配慮しなければならない」とある。今後、重要インフラ事業者に対して政府への情報共有を求めるにあたり義務的な制度を含めて現状よりも厳しいものとする場合にも、事業者の経済活動等に与える影響に配慮が求めらよう。この点、安全保障の目的を達成するためには、目的自体が棄損されるような制度内容の緩和は望ましくない。一方で、事業者の実質的な負担を軽減することを検討することが重要であると考えるところ、サイバーセキュリティ政策当局側での貢献は有益であろう。例えば、事業者において、インシデントからの復旧に注力でき、負担となる同時並行／複数の外部とのやりとりを軽減するべく、サイバーセキュリティ当局への伝達をすれば、当該当局が関係部局に情報を展開するなど、ワンストップ化を実現するなどは一案である。また、事業者がインシデントの報告をすることで、政府から充実したサイバーセキュリティ対策の支援を受けられるといったメリットを与えることも、実質的な負担軽減策になると考えられる。

安全保障の構図を覆すような国際情勢の変化がみられるなか、重要インフラによるサービスの提供機能の維持について、関係者・関係当局からの関心はますます大きくなると考える。デジタル化が進展するなか、国内外からのサイバーに関わる懸念も一層高まっていく。その際、懸念を受けて対策の実施、情報共有などについての政策を立案・実施するにあたっては、重要インフラ事業者が主として民間であることを踏まえ、経営者が利害関係者に説明責任を果たせるものであることが重要である。サイバーセキュリティ政策分野において、適切に政策が立案・実施され、官民での信頼関係をより強める取組が継続されていくことを期待する。

¹ 内閣官房「国家安全保障戦略(令和4年12月16日国家安全保障会議・閣議決定)」
(<https://www.cas.go.jp/jp/siryou/221216anzenhoshou.html>) (2024年3月30日閲覧)

² 安保戦略 2022 p7

³ 安保戦略 2022 p21

⁴ 松村昌廣「我が国のサイバーセキュリティ戦略の欠点と展望」、総務省学術雑誌「情報通信政策研究」vol.5、no.2、p73-94(https://www.soumu.go.jp/main_content/000787278.pdf) (2024年3月30日閲覧)

⁵ 安全保障政策の範囲について、国家安全保障会議が審議する事項に関係するものを想定した(国家安全保障会議設置法第2条参照)。

⁶ 内閣官房副長官(事務)を議長とし各省庁の局長級を構成員とする会議体
(<https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/conference/suisinkaigi/0229suisinkaigi.html>) (2024年3月30日閲覧)

⁷ 内閣サイバーセキュリティセンター「重要インフラのサイバーテロ対策に係る特別行動計画関連資料」(<https://www.nisc.go.jp/pdf/council/seisaku/ciip/dai1/1sankosiryou2.pdf>) (2024年3月30日閲覧)

⁸ 特別行動計画 p5

⁹ 特別行動計画 p4

¹⁰ 特別行動計画 p3

-
- ¹¹ 内閣法第 12 条第 2 項参照
- ¹² 内閣サイバーセキュリティセンター「情報セキュリティ基本問題委員会関連 2005 年 4 月 22 日第 2 次提言」(https://www.nisc.go.jp/pdf/policy/kihon-s/teigen/2teigen_hontai.pdf) (2024 年 3 月 30 日閲覧)
- ¹³ 2 次提言 p9
- ¹⁴ 2 次提言 p10-11
- ¹⁵ 内閣府「平成 14 年度交通事故の状況及び交通安全施策の現況 航空管制情報処理システムの障害について」(https://www8.cao.go.jp/koutu/taisaku/h15kou_haku/genkyo/topics7.html) (2024 年 3 月 30 日閲覧)
- ¹⁶ JCIC「日本のサイバーセキュリティ政策史第 6 回 サイバーセキュリティ対策黎明期の重要インフラ防護」(<https://www.j-cic.com/pdf/report/The-History-of-Japan-Cybersecurity-Policy-6.pdf>) (2024 年 3 月 30 日閲覧) p4
- ¹⁷ 2 次提言 p10
- ¹⁸ 2 次提言 p10
- ¹⁹ 2 次提言 p10
- ²⁰ サイバー攻撃による IT 障害のみならず非意図的要因による IT 障害、自然災害による IT 障害をも防護の対象とするものであるから、改めて定義をすることは当然であったと考える。
- ²¹ JCIC「日本のサイバーセキュリティ政策史第 6 回 サイバーセキュリティ対策黎明期の重要インフラ防護」p3
- ²² 2 次提言 p31
- ²³ Critical Infrastructure Information Act (2002) の § 673(a)(1) において、情報公開法等の例外として、重要インフラ事業者から自発的に政府機関に提供された情報が規定されており、提出を受けた政府機関による当該情報の利用方法のひとつとして相互依存性分析が含まれていることが影響した可能性が考えられる。
- ²⁴ 2 次提言 p35
- ²⁵ 2 次提言 p37
- ²⁶ 2 次提言では、「情報システムやネットワークの構築後に情報セキュリティを勘案することは困難であり、重要インフラにかかわるシステムの設計段階で情報セキュリティを組み入れることが強く望まれる」と指摘しており、その後、政策的において重視されるセキュリティ・バイ・デザインの考え方も示したことも注目される。
- ²⁷ 経緯等については、JCIC「我が国のサイバー/情報セキュリティ政策の変遷 組織・戦略編」(<https://www.j-cic.com/pdf/report/The-History-of-Japan-Cyber.pdf>) (3 月 30 日閲覧) を参照。
- ²⁸ NISC(国会図書館 web アーカイブプロジェクト)「重要インフラの情報セキュリティ対策に係る行動計画」(https://warp.da.ndl.go.jp/info:ndljp/pid/998223/www.nisc.go.jp/active/infra/pdf/infra_rt.pdf) (3 月 30 日閲覧)
- ²⁹ NISC(国会図書館 web アーカイブプロジェクト)「早期に着手すべ政府統一的・横断的課題」(<https://warp.da.ndl.go.jp/info:ndljp/pid/998223/www.nisc.go.jp/conference/seisaku/dai1/pdf/1siryoku5.pdf>) (2024 年 3 月 30 日閲覧)
- ³⁰ NISC(国会図書館 web アーカイブプロジェクト)「重要インフラの情報セキュリティ対策に係る基本的考え方の概要」(<https://warp.da.ndl.go.jp/info:ndljp/pid/998223/www.nisc.go.jp/conference/seisaku/dai2/pdf/2siryoku05.pdf>) (2024 年 3 月 30 日閲覧)
- ³¹ NISC(国会図書館 web アーカイブプロジェクト)「重要インフラ専門委員会の設置について」

(<https://warp.da.ndl.go.jp/info:ndljp/pid/998223/www.nisc.go.jp/conference/seisaku/ciip/dai1/pdf/1siryu1.pdf>) (2024 年 4 月 27 日閲覧)

³² 「等」は、「政府・行政サービス(地方公共団体を含む)」を指す。

³³ 1 次行動計画 p1 を参照した。

³⁴ 最初の安全基準等策定指針は、2006 年 2 月に ISPC により決定された。
(https://warp.da.ndl.go.jp/info:ndljp/pid/998223/www.nisc.go.jp/active/infra/pdf/tgc01_sf.pdf)
(2024 年 4 月 27 日閲覧)その後、行動計画が改定されることなどを踏まえて、数次の改定が重ねられ、現在は、2023 年 7 月にサイバーセキュリティ戦略本部によって決定された「重要インフラのサイバーセキュリティに係る安全基準等策定指針」
(<https://www.nisc.go.jp/pdf/policy/infra/shishin202307.pdf>) (2024 年 4 月 27 日閲覧)が最新のものとなっている。

³⁵ JCIC「日本のサイバーセキュリティ政策史第 6 回 サイバーセキュリティ対策黎明期の重要インフラ防護」p5

³⁶ 例えば、NISC「静的相互依存性解析の総括について」(2007 年 12 月)
(<https://warp.da.ndl.go.jp/info:ndljp/pid/8833367/www.nisc.go.jp/conference/seisaku/ciip/dai12/pdf/12siryu05.pdf>) (2024 年 4 月 27 日閲覧)、
「2012 年度重要インフラの共通脅威分析に関する調査の結果について」(2013 年 3 月)
(<https://warp.da.ndl.go.jp/info:ndljp/pid/8833367/www.nisc.go.jp/conference/seisaku/ciip/dai31/pdf/31sankousiryu05.pdf>) (2024 年 4 月 27 日閲覧)といった調査報告があり、「同時多発型 IT 障害時の重要システム復旧の迅速さに対するベンダ対応への依存度は、分野や重要システムの特徴により違いがあるものの、重要システムにはベンダへの外部依存性が存在することが確認できた」などの結論が示されている。

³⁷ NISC(国会図書館 web アーカイブプロジェクト)「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」
(https://warp.da.ndl.go.jp/info:ndljp/pid/998223/www.nisc.go.jp/active/infra/pdf/infra_rt2.pdf)
(2024 年 3 月 30 日閲覧)

³⁸ 2 次行動計画 p3-4

³⁹ 2 次行動計画 p5

⁴⁰ NISC「第 2 次情報セキュリティ基本計画」(https://www.nisc.go.jp/pdf/policy/kihons/bpc02_ts.pdf) (2024 年 3 月 30 日閲覧)

⁴¹ 2 次行動計画 p20

⁴² NISC(国会図書館 web アーカイブプロジェクト)「重要インフラの情報セキュリティ対策に係る第 3 次行動計画」
(https://warp.da.ndl.go.jp/info:ndljp/pid/8930005/www.nisc.go.jp/active/infra/pdf/infra_rt3.pdf)
(2024 年 3 月 30 日閲覧)

⁴³ 3 次行動計画 p1

⁴⁴ JCIC「日本のサイバーセキュリティ政策史第 7 回 すべての人が「自分ごと」として向き合える行動計画を【前編】」p2(<https://www.j-cic.com/pdf/report/The-History-of-Japan-Cybersecurity-Policy-7-1.pdf>) (公開日の 2024 年 5 月 25 日に閲覧、URLを追記)

⁴⁵ 3 次行動計画 p8

⁴⁶ 3 次行動計画 p18-19

⁴⁷ 厚生労働省「安全衛生キーワード:ヒヤリハット」
(https://anzeninfo.mhlw.go.jp/yougo/yougo26_1.html) (2024 年 4 月 21 日閲覧)参照。

⁴⁸ 3 次行動計画 p23

⁴⁹ 3次行動計画 p23

⁵⁰ ISO31000(リスクマネジメント規格)を直接に言及せず、「国際的にも標準的なリスクマネジメントの考え方」といった表現となった背景は、当時は事業者によってリスクマネジメントの考え方などに様々な意見があったことに起因する。JCIC「日本のサイバーセキュリティ政策史第7回 すべての人が「自分ごと」として向き合える行動計画を【前編】」p5 参照。

⁵¹ 3次行動計画 p11-12 参照。

⁵² JCIC「日本のサイバーセキュリティ政策史第7回 すべての人が「自分ごと」として向き合える行動計画を【前編】」p3 参照。

⁵³ NISC(国会図書館 web アーカイブプロジェクト)「重要インフラの情報セキュリティ対策に係る第4次行動計画(2017年4月18日サイバーセキュリティ戦略本部決定)」
(https://warp.da.ndl.go.jp/info:ndljp/pid/11001539/www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf)
(2024年4月15日閲覧)

⁵⁴ NISC「サイバーセキュリティ戦略(2015年9月4日閣議決定)」
(<https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku.pdf>) (2024年4月15日閲覧)

⁵⁵ 3次行動計画との違いは、「リスクマネジメント」に「対処体制の整備」が追加された点である。

⁵⁶ 経済産業省「電気関係報告規則及び電気設備に関する技術基準を定める省令の一部を改正する省令について」
(https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2016/09/280923-1.html) (2024年4月15日閲覧)

⁵⁷ 4次行動計画 p12

⁵⁸ 4次行動計画 p23-24。

⁵⁹ US Department of Defense “Mission Assurance Strategy”
(https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf) (2024年4月15日閲覧)を参考にして2015戦略で取りまとめた考え方。

⁶⁰ 2015戦略 p15

⁶¹ 4次行動計画 p5

⁶² より詳しく記述すると「自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現すること」である。

⁶³ NISC(国会図書館 web アーカイブプロジェクト)「サイバーセキュリティ戦略本部資料提供等規則(2015年2月10日CSHQ決定、2016年10月12日一部改定)」
(https://warp.da.ndl.go.jp/info:ndljp/pid/10217953/www.nisc.go.jp/conference/cs/pdf/teikyou_kisoku.pdf) (2024年4月21日閲覧)

⁶⁴ NISC(国会図書館 web アーカイブプロジェクト)「サイバーセキュリティ戦略本部 重要インフラ専門調査会 第9回会合 議事概要」p11
(<https://warp.da.ndl.go.jp/info:ndljp/pid/10357242/www.nisc.go.jp/conference/cs/ciip/dai09/pdf/09gijigaigyau.pdf>) (2024年4月21日閲覧)

⁶⁵ 4次行動計画 p46

⁶⁶ NISC「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準(初版)」
(https://www.nisc.go.jp/pdf/policy/infra/hyouka_kijun_shohan.pdf) (2024年4月27日閲覧)

⁶⁷ DHS “NCCIC CYBER INCIDENT SCORING SYSTEM”
(https://www.cisa.gov/sites/default/files/publications/NCCIC_Cyber_Incident_Scoring_System.pdf) 及び 28th Annual First Conference “Evaluating National Level Cyber Risk, the DHS Approach

Mark Bristow (DHS/ICS-CERT, US) のセッション

(<https://www.first.org/conference/2016/program/#evaluating-national-level-cyber-risk-the-dhs-approach>) を参照 (2024 年 4 月 21 日閲覧)

⁶⁸ NISC (国会図書館 web アーカイブプロジェクト) 「2020 年東京オリンピック・パラリンピック競技大会のサイバーセキュリティの確保に向けたリスク評価資料一式」

(<https://warp.da.ndl.go.jp/info:ndljp/pid/10310121/www.nisc.go.jp/materials/index.html>) (2024 年 4 月 18 日閲覧)

⁶⁹ NISC (国会図書館 web アーカイブプロジェクト) 「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書 (第 1 版)」

(<https://warp.da.ndl.go.jp/info:ndljp/pid/11095919/www.nisc.go.jp/materials/index.html>) (2024 年 4 月 18 日閲覧)

なお、現在は、NISC から「機能保証のためのリスクアセスメント・ガイドライン 1.0 版 ～社会経済を支えるサービスを提供する事業者等による自律的なリスクマネジメントに向けて～、リスク評価資料一式」が公表されている

(<https://www.nisc.go.jp/policy/group/cyber/policy.html>) (2024 年 4 月 18 日閲覧)

⁷⁰ NISC (国会図書館 web アーカイブプロジェクト) 「平成 30 年第 19 回サイバーセキュリティ戦略本部会合 (平成 30 年 7 月 25 日) 重要インフラの情報セキュリティ対策に係る第 4 次行動計画 (改定)」

(<https://warp.da.ndl.go.jp/info:ndljp/pid/11133232/www.nisc.go.jp/conference/cs/index.html>) (2024 年 4 月 21 日閲覧)

⁷¹ 4 次行動計画 (当初のもの) p24

⁷² 国土交通省「空港・空港ビルの重要インフラ化作業状況 (H29.11.30 現在)」

(<https://www.nisc.go.jp/pdf/council/cs/ciip/dai13/13shiryoku05.pdf>) (2024 年 4 月 27 日閲覧)

⁷³ NISC「重要インフラの情報セキュリティ対策に係る第 4 次行動計画の改定 (案) について」

(<https://www.nisc.go.jp/pdf/council/cs/dai23/23shiryoku02.pdf>) (2024 年 4 月 21 日閲覧)

⁷⁴ NISC「重要インフラのサイバーセキュリティに係る行動計画」

(https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf) (2024 年 4 月 21 日閲覧)

⁷⁵ NISC「サイバーセキュリティ戦略 (2021 年 9 月 28 日閣議決定)」

(<https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf>) (2024 年 4 月 21 日閲覧)

⁷⁶ 2019 年に複数自治体を利用するクラウドサービスのシステム障害、2020 年の大手通信キャリアの電子決済サービスにおける利用者範囲拡大に伴うリスク増加に十分対応できていなかったため不正送金が発生して一時的にサービス停止、2021 年に重要インフラ事業者等が利用する業務委託先に対するランサムウェア攻撃が発生といったことが背景にあるとされる。JCIC「日本のサイバーセキュリティ政策史 (第 5 回): 結果を保証する『重要インフラのサイバーセキュリティに係る行動計画』」(<https://www.j-cic.com/pdf/report/The-History-of-Japan-Cybersecurity-Policy-5.pdf>) (2024 年 4 月 21 日閲覧) p5 参照。

⁷⁷ 5 次行動計画 p7

⁷⁸ 5 次行動計画 p11

⁷⁹ JCIC「日本のサイバーセキュリティ政策史 (第 5 回): 結果を保証する『重要インフラのサイバーセキュリティに係る行動計画』」p6。

⁸⁰ 5 次行動計画 p14-15

⁸¹ 5 次行動計画 p23

-
- ⁸² NIST “Cybersecurity Framework V1.1(April 2018)”(<https://www.nist.gov/cyberframework/csf-11-archive>) (2024 年 4 月 21 日閲覧)
- ⁸³ JCIC「日本のサイバーセキュリティ政策史(第 5 回):結果を保証する『重要インフラのサイバーセキュリティに係る行動計画』」p6-7。
- ⁸⁴ 「重要インフラのサイバーセキュリティに係る行動計画(2024 年 3 月 8 日改定 CSHQ 決定)」(https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2024.pdf) (2024 年 4 月 21 日閲覧)
- ⁸⁵ 国土交通省「コンテナターミナルにおける情報セキュリティ対策等検討委員会について」(https://www.mlit.go.jp/kowan/kowan_mn2_000006.html) (2024 年 4 月 21 日閲覧)
- ⁸⁶ NISC(国会図書館 web アーカイブプロジェクト)「重要インフラ分野における分野横断的演習(机上演習)の実施について」(<https://warp.da.ndl.go.jp/info:ndljp/pid/998223/www.nisc.go.jp/conference/seisaku/dai10/pdf/10siryou06.pdf>) (2024 年 4 月 27 日閲覧)
- ⁸⁷ NISC(国会図書館 web アーカイブプロジェクト)「2013 年度重要インフラの分野横断的演習に関する調査」の結果について」(<https://warp.da.ndl.go.jp/info:ndljp/pid/8655428/www.nisc.go.jp/conference/seisaku/ciip/dai36/pdf/36siryou05.pdf>) (2024 年 4 月 27 日閲覧)
- ⁸⁸ NISC(国会図書館 web アーカイブプロジェクト)「2014 年度 分野横断的演習について」(<https://warp.da.ndl.go.jp/info:ndljp/pid/8930005/www.nisc.go.jp/conference/seisaku/ciip/dai38/pdf/38siryou02.pdf>) (2024 年 4 月 27 日閲覧)
- ⁸⁹ NISC(国会図書館 web アーカイブプロジェクト)「2015 年度 分野横断的演習について」及び「2016 年度 分野横断的演習について」(<https://warp.da.ndl.go.jp/info:ndljp/pid/9979139/www.nisc.go.jp/conference/cs/ciip/dai05/pdf/05shiryou05.pdf>) 及び(<https://warp.da.ndl.go.jp/info:ndljp/pid/10341577/www.nisc.go.jp/conference/cs/ciip/dai10/pdf/10shiryou05.pdf>) (2024 年 4 月 27 日閲覧)
- ⁹⁰ NISC(国会図書館 web アーカイブプロジェクト)「分野横断的演習について」(<https://www.nisc.go.jp/pdf/council/cs/ciip/dai16/16shiryou06.pdf>) (2024 年 4 月 27 日閲覧)
- ⁹¹ NISC「2020 年オリパラ東京大会に向けた分野横断的演習のあり方について」(2019 年 1 月 17 日)(<https://www.nisc.go.jp/pdf/council/cs/ciip/dai17/17shiryo08.pdf>) (2024 年 4 月 27 日閲覧)
- ⁹² NISC「2020 年度分野横断的演習について」(<https://www.nisc.go.jp/pdf/council/cs/ciip/dai24/24shiryou04.pdf>) (2024 年 4 月 27 日閲覧)及び「分野横断的演習の実施結果について」(<https://www.nisc.go.jp/pdf/council/cs/ciip/dai28/28shiryou04.pdf>) (2024 年 4 月 27 日閲覧)
- ⁹³ NISC「2022 年度分野横断的演習について」(<https://www.nisc.go.jp/pdf/council/cs/ciip/dai32/32shiryou03.pdf>) (2024 年 4 月 27 日閲覧)
- ⁹⁴ NISC「2023 年度 分野横断的演習の実施結果について」(<https://www.nisc.go.jp/pdf/council/cs/ciip/dai36/36shiryou03.pdf>) (2024 年 4 月 27 日閲覧)
- ⁹⁵ 安保戦略 2022 p26 参照
- ⁹⁶ 内閣府「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度について(2024 年 4 月 19 日)」p2,5(https://www.cao.go.jp/keizai_anzen_hosho/doc/infra_gaiyou.pdf) (2024 年 4 月 25 日閲覧)
- ⁹⁷ 安保戦略 2022 p27 参照
- ⁹⁸ 2024 年 1 月 30 日の経済安全保障推進会議(議長:内閣総理大臣)第6回会合において、「港

湾については、港湾運送の役務の安定提供の確保を図るため、特定社会基盤事業として定めることができる事業に一般港湾運送事業を追加する改正法案の準備を進める」とこととされた。

(https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo/dai6/gijisidai.html) (2024 年 4 月 21 日閲覧) 参照。

⁹⁹ 内閣府「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度について(2024 年 4 月 19 日)」p13

¹⁰⁰ 内閣府「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説」 p7-8 (https://www.cao.go.jp/keizai_anzen_hosho/doc/infra_kaisetsu.pdf) (2024 年 4 月 21 日閲覧)

¹⁰¹ 安保戦略 2022 では、能動的サイバー防御として、政府への情報共有等のほか、国内の通信事業者が役務提供する通信に係る情報を活用して攻撃者による悪用が疑われるサーバ等を検知するための所要の取組や、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにすることを進めるとしている。

¹⁰² 「政府への情報共有」と記述されているが、これは、重要インフラ事業者など民間事業者から政府へと情報伝達の向きがあるように見えることに注意が必要である。

¹⁰³ 例えば、自由民主党デジタル社会推進本部サイバーセキュリティに関する PT「サイバーセキュリティ対策の更なる強化に向けた提言 ～「常時有事」の脅威に立ち向かうサイバーレジリエンスの確立へ～」(2024 年 4 月 23 日)では、「我が国のサイバー安全保障の確保に万全を期す観点から法制度の整備、運用の強化に向けた検討の具体化を図ることを強く求める」としている。
(<https://www.hirataku.com/uploads/66307d48e25c673069a03ee5.pdf>) (2024 年 4 月 30 日閲覧)

¹⁰⁴ NIS 2 Directive 第 23 条 “Reporting obligations” 参照。(<https://eur-lex.europa.eu/eli/dir/2022/2555>) (2024 年 4 月 21 日閲覧)

¹⁰⁵ NIS2 指令を受けた構成国内法が施行されるまでは、基づく基幹インフラ事業者のインシデントの影響報告が義務付けられている従来からの NIS 指令が有効。

¹⁰⁶ シンガポール・サイバーセキュリティ法 14 条参照。(<https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312>) (2024 年 4 月 21 日閲覧)

¹⁰⁷ CISA “Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)”
(<https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia>) (2024 年 4 月 21 日閲覧)

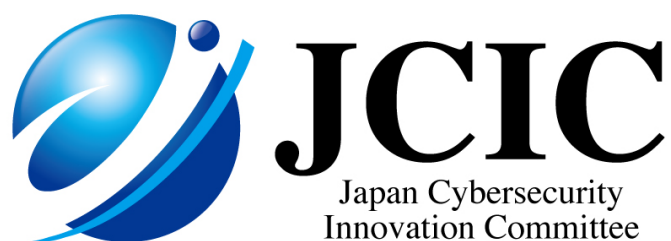
¹⁰⁸ Critical Infrastructure Information Act では政府に対する任意の情報提供であったが、本法によって、義務的なものとなる。

¹⁰⁹ NISC「サイバー攻撃被害に係る情報の共有・公表ガイダンス」p26 参照。
(https://www.nisc.go.jp/pdf/policy/kihon-2/kyogikai_guidance2022.pdf) (2024 年 4 月 21 日閲覧)

¹¹⁰ 5.1 で述べたようにサイバーセキュリティ政策における「重要インフラ」と、経済安全保障政策における「基幹インフラ」の多くは重複しており、懸念される攻撃手段への対策には、サイバーセキュリティ政策における防護の手法とテクニカルには同じである。

¹¹¹ 2021 戦略 p29-34

¹¹² 三角「我が国のサイバーセキュリティ戦略策定の背景」日本セキュリティ・マネジメント学会誌 Vol.34, No.3, p39-46 (2020)



[本調査に関する照会先]

JCIC 事務局 info@j-cic.com