2023 年 7 月

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

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、国家安全保障戦略（2022 安保戦略）[1]が、国家安全保障会議決定・閣議決定された。同戦略「サイバー安全保障分野での対応能力の向上」の節で、「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」し、「能動的サイバー防御を含むこれらの取組を実現・促進するために、内閣サイバーセキュリティセンター（NISC）を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置する」方針が示された。そこで、今後の、サイバー安全保障政策の検討等に資するべく、我が国のサイバー／情報セキュリティ政策の司令塔機能の一角を担ってきた NISC が推進・実施してきた政策を中心に、我が国のサイバー／情報セキュリティに係る戦略及びそれらの策定・推進組織と根拠について概観・整理する。

2. サイバーセキュリティ基本法

2.1. 制定・改正の経緯

我が国のサイバーセキュリティ政策は、サイバーセキュリティ基本法[2]（CS 基本法）に基づき閣議決定されるサイバーセキュリティ戦略[3]によって、各省庁の関連施策が、総合的かつ効果的に総合調整され推進されている。CS 基本法は、国家の関与が疑われるものを含めたサイバー攻撃等の深刻化やオリンピック・パラリンピック東京大会への対応の必要性の高まりといったサイバーセキュリティを巡る情勢の変化を背景に、2014 年 11 月に議員立法により成立した。それ以前は、高度情報通信ネットワーク社会形成基本法[4](IT 基本法)22 条（高度情報通信ネットワークの安全性の確保等）の規定を踏まえて、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）の下に置かれた情報セキュリティ政策会議(議長：内閣官房長官。ISPC)によって、戦略又は基本計画が決定され、推進されていた。CS 基本法が制定されたことによって、サイバーセキュリティ政策の総合的な推進の法的基盤が確立されたことになる。

CS 基本法は、2016 年及び 2018 年に内閣から提出した同法の改正法案により、2度改正されている。2016 年の改正は、2015 年 5 月に発生した不正アクセスにより日本年金機構（JPS）から情報が流出した事件[5]が契機となった。事件当時、すなわち、CS 基本法制定当初は、同法に基づき内閣に置かれるサイバーセキュリティ戦略本部（本部長：内閣官房長官、CS 戦略本部）が行う原因究明調査の対象は、国の行政機関で発生した重大な事象に限られていた。このため特殊法人である JPS に対する調査を同法に基づき実施できないのではないかとの疑義が生じた。この点、本事件については、年金事務に関して JPS は厚生労働省と一体に運用していることから CS 戦略本部及び NISC は関与できるとして調査を実施した。しかし、こうした考え方が他の場合にも総じて適用できるわけではない。そこで、CS 基本法が改正され、原因究明調査や監査の対象が拡大され、独立行政法人や CS 戦略本部が指定する特殊法人・認可法人（指定法人）もカバーされるようになった[6]（2.3.参照）。

2018 年の改正は、その背景のひとつとして、2016 年改正において、衆・参議院において、2 年以内に CS 基本法の見直しの必要性について検討し、必要な措置を講ずるものとの附帯決議がなされていたことを挙げられる。2017 年 1 月から、CS 戦略本部で政策レビューが開始[7]された。その最中、2017 年 5 月にランサムウェア WannaCry の事件[8]が発生した。本事件での教訓として、政策レビュー結果において、被害拡大防止に資するべく官民、民民間で幅広く情報を迅速に共有することの必要性が改めて指摘された[9]。この指摘を踏まえて検討が進められ、2018 年 3 月、サイバーセキュリティ協議会（2.3.参照）を整備する CS 基本法の改正法案が閣議決定され、同年 12 月可決、公布された。

2.2. 定義

CS 基本法の特徴のひとつに「サイバーセキュリティ」という用語を法律用語として定めたことがある。基本的には、機密性、完全性、可用性を確保することで、情報漏えい、サイバー攻撃、内部不正等に対するものを含めて必要な措置全般が講じられ維持管理されていることを意味する[10]。サイバー攻撃への対応が喫緊の課題となる中、法令に定義することで、国民、企業、政府などにおいて、防御の重要性が強く意識され、この用語が浸透し、意識が高まることが期待された。カタカナの「サイバーセキュリティ」とした理由は、法令用語として漢字熟語を用いると見慣れない難解なものとなるおそれがあったこと、また、人の記憶や手書きのメモを通じて情報が漏えいしないようにすることは国際標準等で定義される「情報セキュリティ」の対象となりうるが、CS 基本法ではそうした行為を含まないことを明確にすることにあった[11]。その後、デジタル社会形成基本法[12]（デジタル基本法）をはじめ複数の法令で「サイバーセキュリティ」の用語が用いられ、また、組織名や政策などにおいても広く用いられるようになっている。

なお、2022 安保戦略で登場する「サイバー安全保障」という日本語の用語については、定義と明示した文はみられないが、「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の向上」とあるように国や重要イ

ンフラなどの安全の確保が念頭にあり、「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」することを含む概念である。従って、「機密性、完全性、可用性を確保」を意味する「サイバーセキュリティ」と重なる部分はあるが、それ以外の能動的な活動[13]も含む、より広い概念であると思われる。

CS 基本法は、重要インフラ事業者を意味する「重要社会基盤事業者」について、「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」と定義[14]している。具体的には、CS 戦略本部によって、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス」[15]、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」の 14 分野が特定されている[16]。

なお、これに類似する概念として、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[17]（経済安保推進法）50 条に規定する特定社会基盤役務（基幹インフラ役務[18]）がある。これは、「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」と定義され、「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 分野である。基幹インフラは、CS 戦略本部が特定する重要インフラ 14 分野とは多くは重複しているが、一部に異なる分野があることに注意が必要である。前者は「国家及び国民の安全を損なう事態を生ずるおそれ」、後者が「国民生活又は経済活動に多大な影響を及ぼすおそれ」があるかどうかによって決められていることが、両者の違いの理由の一つであると考える。

2.3. 組織

CS 基本法には、組織に関する規定がある。ひとつは、CS 戦略本部に関するものである。CS 戦略本部は、サイバーセキュリティを巡る情勢の変化を受け、政府において司令塔的な役割を担う ISPC の機能を強化し、各府省庁の情報共有、迅速な対応、連携などを図るべく、内閣に、我が国におけるサイバーセキュリティに関する施策の司令塔として設置された。CS 戦略本部は、国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティ対策の基準を作成し、その実施状況に関する評価（監査）[19]を行い、また重大事象に対する原因究明のための調査などを行う[20]。

指定法人には日本年金機構等が指定されている[21]。特殊法人には、例えば一部の JR グループ会社など民間会社と変わらないものなどもある。その様な法人は指定の対象とならない。それは、CS 戦略本部は、法人の業務と国の業務の体性、当該業務に係る保有情報の機微性やサイバー攻撃等による当該業務の国民生活・経済活動への影響、当該法人による自主的な対策の適

切性、NISC の技術的能力・知見の活用可能性といった要素[22]を踏まえて指定するからである[23]。

CS 戦略本部が監査や調査を行うには、必要な情報が行政機関から同本部に対して適時、着実に提供される必要がある。そのため CS 基本法で「本部に対し、サイバーセキュリティに関する資料又は情報であって、本部の所掌事務の遂行に資するものを、適時に提供しなければならない」と規定[24]されている。この規定があることにより、国の行政機関等に対して、監査の規定と相まって、CS 戦略本部が作成したサイバーセキュリティ対策の基準を事実上義務的に適用されると考えられる。

CS 戦略本部に関する事務は、内閣官房において処理し、内閣官房副長官補が掌理する[25]。これを踏まえて、内閣官房副長官補がセンター長を務める NISC が、監査等の CS 戦略本部に関する事務を実質的に行っている(3.3.参照)。2014 年 CS 基本法成立時の附則に、CS 戦略本部の事務処理を適切に内閣官房に行わせるために必要な法制の整備をすべき旨の規定があった(2016 年 CS 基本法改正時に削除。)。これを受けて内閣官房組織令により、NISC に係る規定整備が行われ、2015 年 1 月から、新体制の NISC が行政各部の情報システムに対する不正な活動の監視・分析、監査などの事務を、法的根拠をもって行うようになった。

CS 基本法に基づくもうひとつの組織はサイバーセキュリティ協議会[26](CS 協議会)である。サイバー攻撃などの事象に関し、早期段階でサイバーセキュリティの確保に資する情報を迅速に共有することにより、サイバー攻撃による被害を予防し、また、被害の拡大を防ぐことは重要である。しかし、被害を受けた企業・組織が情報を共有するにあたり、情報提供者の名が広がることで風評被害を受けるリスクや、機微な情報の提供が他の法令や契約に抵触するおそれがあった。このため CS 協議会に参加した者の守秘義務及び情報提供義務を法律事項としている[27]。CS 協議会は、不正プログラムの分析を行うなどして対策情報を作出する専門機関等からなるタスクフォースと、作出された対策情報を得て対策を実施する組織から構成される。庶務は NISC が務め、国内外の関係者との連絡調整といった一部の事務を一般社団法人 JPCERT コーディネーションセンター(JPCERT)に委託している[28]。2022 年 4 月 1 日時点で 300 を超える企業・団体等が参加している[29]。

2.4. 安全保障との関係

サイバーセキュリティに関する施策には、国家の関与が疑われるサイバー攻撃、重要インフラに対する大規模サイバー攻撃など我が国の安全に重大な影響を及ぼす事象への対応が含まれる。この点、CS 基本法立法時に、海外からのサイバー攻撃であっても、当初は攻撃の主体が判明しない。そのため、一義的には警察権による対応となり、国家の関与の疑いが生じた場合などには、CS 戦略本部が得たサイバーセキュリティ関連情報を国家安全保障会議(NSC)に逐次提供するなど、CS 戦略本部と NSC とが緊密な連携を図ることと整理した[30]。

こうした事象への対処にあたるには、警察庁、外務省、防衛省等の関係機関におけるサイバーセキュリティ確保のための体制整備が必要である。また、諸外国の例に鑑みても関係機関間の情報共有や連携が重要である。これらのことから、CS 基本法では、関係機関における体制の充実

強化並びに関係機関相互の連携強化及び役割分担の明確化を図るために必要な施策を講ずるものとするとの規定[31]が設けられている[32]。2022 安保戦略では、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置することとされており、政府における連携強化・役割分担の明確化等が図られるものと考える。

3. 総合的な情報セキュリティ政策推進体制の整備・強化

府省庁によるサイバーセキュリティ／情報セキュリティに係る政策の総合調整は、企画・立案・総合調整を担う内閣官房が行っている。その体制整備・強化の変遷をまとめる。

3.1. 情報セキュリティ対策推進会議／内閣官房情報セキュリティ対策推進室

1999 年 9 月 17 日、情報セキュリティ政策について、政府全体として総合的な対策の推進を図るため、内閣官房長官決裁により、内閣に情報セキュリティ関係省庁局長等会議（議長内閣官房副長官(事務)）を設置した。同会議は、ハッカー（コンピュータに不正なアクセスを行う者）対策等の基盤整備、いわゆるサイバーテロ対策など、官民のコンピュータシステムを違法・不正行為から守るための対策全般（情報セキュリティ政策）を広く検討するものであった[33]。2000 年 1 月 21 日に「ハッカー対策等の基盤整備に係る行動計画」[34]を決定したが、その直後(1 月 24 日)に、旧科学技術庁の Web ページが改ざんされる事件が発生した。その後も中央省庁の web ページが、外部からの不正アクセスによって改ざんされる事件が続いた[35]。

こうした情勢もあり、政府は、ハッカー、サイバーテロ対策について、コンピュータ西暦二千年問題における経験も活かしながら、抜本的な対策強化を図るべく、高度情報通信社会推進本部[36]（IT 推進本部。本部長：内閣総理大臣）の下で、全省庁が密接に連携し、また、民間有識者の知見も得ながら、総合的に施策を推進していく体制を整えた[37]。すなわち、2000 年 2 月 29 日、官民における情報セキュリティ対策の推進を図ることを目的に、本部長決定によって、IT 推進本部の下に、情報セキュリティ対策の推進に関し専門的かつ優れた見識を有する者から構成される情報セキュリティ部会と、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情報セキュリティ対策推進会議（対策推進会議）を設置した[38]。また、同日、内閣総理大臣決定によって、内閣官房に情報セキュリティ対策推進室（対策推進室）を設置した[39]（対策推進室は 2004 年時点で 18 名の体制[40]）。その後、2001 年 1 月に IT 戦略本部が設置されると、同本部の下に、対策推進会議が位置づけられ、また、情報セキュリティ対策の推進に関し学識経験を有する者で構成する情報セキュリティ専門調査会が置かれた[41]。

対策推進会議は、各省庁がリスク分析を踏まえて情報セキュリティポリシーを整備し実施することなどを内容とする情報セキュリティポリシーに関するガイドラインを策定し、各省庁における実施状況を対策推進室が評価するなど、電子政府の情報セキュリティ確保のための活動を行った。また、情報通信、金融、航空、鉄道、電力、ガス及び政府・行政サービスの7分野について、それぞれ対策のガイドラインを策定し、官民での連絡体制の整備を行うことなどを内容とする重要インフ

ラのサイバーテロ対策に係る特別行動計画の策定、推進などを行った。

2002 年には、電子政府や民間重要インフラ事業者等の情報システムへのサイバーテロなどの国民生活に重大な影響を与えるおそれのある情報セキュリティに係る事案に対し、各府省庁における情報セキュリティ対策の立案に必要な調査・助言を行うため、官民のコンピュータセキュリティ専門家で構成される緊急対応支援チーム(NIRT)を、対策推進室に設置した[42]。さらに、2004 年 4 月には、内閣官房の対策推進室に、民間の専門家に委嘱して、情報セキュリティ対策についての助言・支援を行う情報セキュリティ補佐官を置いた[43]。

3.2. 情報セキュリティ政策会議／内閣官房情報セキュリティ政策センター

2004 年 7 月、IT 戦略本部は、個人情報をはじめとした重要情報漏えい事件や国民生活・経済活動を支える重要インフラにおける情報システム障害事件の発生などを背景に、情報セキュリティ専門調査会の下に情報セキュリティ基本問題委員会を設置した。同委員会がまとめた第 1 次提言(2004 年 11 月)を受けて、12 月 7 日、IT 戦略本部は、政府としての情報セキュリティ政策に関する基本戦略の策定・推進などを行う体制として情報セキュリティ政策会議(ISPC)を設置すること、また、政府全体としての情報セキュリティ対策の統一的・横断的な総合調整機能の強化などを行う体制として情報セキュリティセンターの設置の方針を決定[44]した。同決定を受けて、ISPC は、2005 年 5 月 30 日、IT 戦略本部の下に設置された。ISPC は、情報セキュリティ政策に関する基本戦略（中長期計画及び年度計画）の策定、同戦略に基づいた政策の事前・事後評価、情報セキュリティ対策に係る政府統一的な情報セキュリティの基準の策定、同基準に基づく評価の結果を踏まえた各府省庁の情報セキュリティ対策に対する勧告の実施等の機能を有し、我が国の情報セキュリティに関する問題の根幹に関する事項を決定するものである[45]。

ISPC は、当初、内閣官房長官が議長を、情報通信技術担当大臣が議長代理、そして、国家公安委員会委員長、防衛庁長官、総務大臣及び経済産業大臣の6名の国務大臣と、IT 戦略本部長から審議に参画することを委嘱された民間有識者 6 名から構成された[46]。その後、2013 年度から外務大臣が構成員として加わり[47]、また、2014 年から民間有識者構成員は 7 名[48]となった[49]。ISPC の下に重要インフラ専門調査会、技術戦略専門委員会、人材育成・資格制度体系化専門委員会（2011 年 7 月に、普及啓発・人材育成専門委員会に改組[50]）などの専門委員会が置かれ、また、対策推進会議は ISPC の下に情報セキュリティ対策推進会議（CISO 等連絡会議）として置かれた。

内閣サイバーセキュリティセンター（NISC）の前進である内閣官房情報セキュリティセンター（旧 NISC）は、2005 年 4 月 25 に設立された。上述の決定を受けたものである。同時に、対策推進室に置かれた情報セキュリティ補佐官は旧 NISC に移った[51]。

旧 NISC は、内閣官房副長官補（安全保障・危機管理担当）をセンター長、内閣審議官2名を副センター長とした組織であった。旧 NISC は、①情報セキュリティ政策に関する基本戦略（中長期計画・年度計画）の立案、②政府機関の総合対策促進（政府統一的な安全基準の策定・評価）、③政府機関の事案対処支援、④重要インフラの情報セキュリティ対策などを主な機能とし、これら

を担当する内閣参事官、事務官、民間人材（当初 35 名程度の[52]）からなる体制であった。旧 NISC 設置当初、その本格稼働を 2006 年度からと予定し、2005 年度中は喫緊に取り組むべき課題（第 1 次中長期計画の策定、政府統一的な安全基準の策定・評価、事案対処における対応能力の強化）に取り組んだ。例えば、「政府機関の情報セキュリティ対策のための統一基準(2005 年項目限定版)」（政府統一基準）[53]を 2005 年 9 月 15 日に、ISPC で決定、同日その解説資料を旧 NISC が発行。その後、同年 12 月 13 日に、政府統一基準(2005 年 12 月版(全体版初版))[54]を ISPC 決定、その解説資料を旧 NISC が発行するなど、緊急性の高い業務から先行して着手し、全体を整備していくかたちで 2006 年度本格稼働に向けた取組みを行っていた。

重要インフラの情報セキュリティ対策については、重要インフラ専門委員会で検討が進められ、2015 年 12 月 13 日に最初の行動計画[55]が ISPC により決定された。その後、4回全体的な見直しが行われ現在の第5版に至っている。

旧 NISC におかれた体制として重要なもののひとつに政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）[56]がある。これは、横断的な情報収集、攻撃等の分析・解析、各政府機関への助言、各政府機関の相互連携促進及び情報共有を図る[57]ためのチームである。また、それをサポートする GSOC システムは、政府全体に横断的に対応するもので、府省庁等の情報システムと外部との通信を府省庁等に設置したセンサーを用いて監視するもの[58]である。2007 年度に整備を行い、2008 年 4 月から 8 時間／日の限定的な監視の運用を開始、2009 年 1 月から 24 時間／365 日の本格運用を開始した。GSOC システムは、これまで 3 回更改[59]されている[60]。

また、情報セキュリティ緊急支援チーム（CYMAT[61]）も NISC に置かれた体制のひとつである。2011 年 9 月、我が国の重工業等に対するサイバー攻撃事件が発生[62]し、標的型攻撃の脅威が顕在化、社会的に認識された。標的型攻撃は、巧妙化な手法を用いて特定の組織を標的に執拗に攻撃を行う。標的型攻撃への対応は、単独の組織で対応するのは困難な状況となってきた。そのため、CISO 等連絡会議に分科会を設置し、集中的に検討を行い、官民連携の在り方について方針[63]をまとめた。その方針の一つに、インシデントに機動的に対応するための政府機関の各組織内 CSIRT の整備に加え、他の府省庁の CSIRT 要員などによる支援体制の整備があった。これを受けて、2012 年 6 月 29 日、政府として一体となって迅速・的確に対応すべき事態が発生した際に、組織の壁を越えて連携し、被害の拡大防止等について機動的に支援を行うため CYMAT が NISC に設置された[64]。これは、各府省庁から派出された職員に内閣官房の併任辞令を発令し構成し、平素から研修・訓練等を行う体制である。

緊急時の初動体制では、現場レベルからの情報集約の全過程から収集された情報等を突合し、その危険性等を早期に把握し、その後の措置方針を決定する体制が不可欠である。そのための仕組み、とりわけ要員の熟度を維持することが重要であるが、そのためにも常日頃から計画的に人材発掘・育成・訓練が重要である。また、個々の案件で情報収集・報告に漏れがないよう、他の部署の担当者を臨時応援で派遣したり、補充したりする体制が重要である。CYMAT には、こうした目的達成のための戦略的意義があった[65]。

3.3. サイバーセキュリティ戦略本部／内閣サイバーセキュリティセンター

サイバーセキュリティ戦略本部(CS 戦略本部)及び内閣サイバーセキュリティセンター(NISC)は、CS 基本法全体が施行された 2015 年 1 月 9 日に設置された。CS 戦略本部の下に、重要インフラ専門調査会、普及啓発・人材育成専門調査会、CISO 等連絡会議などが置かれた。NISC は、旧 NISC の体制・機能を強化・充実させた(2015 年 6 月の時点で 120 名体制[66])もので、CS 戦略本部の所掌事務を常設の事務局的組織として処理するとともに、内閣官房組織令に規定される行政各部の情報システムに対する不正な活動の監視及び分析などの業務を実施する。

NISC の機能がうまく働いた例として、2015 年 5 月に発生した JPS からの不正アクセスによる情報流出事件への対応を挙げられる。この事件は、JPS に対して不審メールが送付され、同メールに添付されるなどした不正プログラムを起動させたことにより、不正アクセスを許してしまい大量の個人情報が流出したというものである。事件の経緯は、まず、NISC の GSOC が、不正プログラムが動作する際に発信する不審な通信を検知ししたことに始まる。検知の事実は、厚生労働省を通じて JPS に伝えられた。しかし、JPS では対応が間に合わず、結果として個人情報が流出してしまい、警察によって流出したデータが現実に確認された。情報流出が確認されたことは厚生労働省から NISC に報告され、すぐに NISC は CS 戦略本部長である内閣官房長官に報告、長官はすぐに内閣総理大臣に報告している。

NISC は初動として 4 つのことを行った。すなわち、①厚生労働省等が行う対応を支援するための CYMAT 派遣、②内閣官房副長官(事務)を議長とする CISO 等連絡会議の開催、③原因究明調査チームの設置、及び④厚生労働大臣に対して CS 基本法に基づく資料提供を求め、勧告に向けた検討の開始であった。

CS 基本法は、全面的に施行されたばかりであったが、将来にわたり法律に基づく資料提出(義務)や勧告が適切に運用されるためには、立法時の問題意識を関係者がよく理解している法律施行後の早期に前例が作られることが大切であるといえる。本件について、NISC 勤務経験のある専門家の招集を含めて原因究明調査チームを NISC に設置し、資料提出を求めた。そして、警察の協力も得るなど関係省庁との密接な連携のもと、同年 8 月 20 日に報告書をとりまとめ、公表し、その結果を踏まえて CS 戦略本部長が厚生労働大臣に対して勧告をしたことなど、早期に前例がつくられた[67]。

本事件が立法事実となり前述のとおり CS 基本法改正が行われた。CS 戦略本部の所掌事務として、監査、原因究明調査の業務を独立行政法人・指定法人に拡大した。これらの業務を行うにはリソースが必要である。そのため、監視も含めて一部の事務について、法定で独立行政法人情報処理推進機構(IPA)に委託している[68]。NISC と IPA との間で密接な連携が図られるようになり、NISC 内部の体制もさらに強化・充実された。

また、本事件は、改めて政府内部でサイバーセキュリティや情報化人材育成強化の必要性が認識された契機ともなった。行政機関が全体としてキャリアパスなども含めて IT やサイバーセキュ

リティ人材の確保・育成を計画的に取組むこととしたとともに、2016 年度に各府省庁に、サイバーセキュリティ・情報化審議官等を設置した[69]。

オリンピック・パラリンピック東京競技大会（TOKYO2020）に向け、政府等とし全体の方針を検討等する体制としては、2014 年 4 月に全閣僚を構成員とする 2020 年オリンピック・パラリンピック東京大会等に関する閣僚会議が設置された。同会議の下に関係省庁による「セキュリティ幹事会」及び NISC 副センター長を座長とする「サイバーセキュリティワーキングチーム（WT）」が設置された[70]。この体制によって、セキュリティ対策に係る基本的な考え方や対策の方向性を示す「2020 年東京オリンピック競技大会・東京パラリンピック競技大会に向けたセキュリティ基本戦略」の決定や改訂を行っている[71]。

TOKYO2020 に向けた具体的な取組みとして、大会開催に向けて事前にリスクマネジメントを行うこと、また、開催期間中などにおける対処体制の整備という2つの柱がある。リスクマネジメント（継続的リスク評価）は、TOKYO2020 の運営に不可欠な電力、情報通信等の重要サービス事業者や競技会場におけるサイバーセキュリティ上のリスク評価及びそれにより明確となる各種リスクへの対策を促進するものである[72]。

こうしたオペレーショナルな取組みを行うため、NISC 内に TOKYO2020 準備の体制が組織された。2016 年の G7 伊勢志摩サミットでは関係省庁などでの連絡体制を整備し、また、NISC は開催会場への要員派遣などを行った。こうした NISC による G7 対応の取組みは、TOKYO2020 の体制と一体的に行われたものであり、その経験は TOKYO2020 の準備に反映された[73]。

また、2019 年ラグビーワールドカップへの対応も、TOKYO2020 準備体制と一体的に行われた。すなわち、2019 年 4 月、関係組織間でサイバーセキュリティに係る脅威情報の共有と事案発生時に関係組織が力を合わせて対応するために国が調整役となるための組織である「サイバーセキュリティ対処調整センター（対処調整センター）」が設置され、情報共有プラットフォームシステムの運用を含めて対応を行った[74]。

TOKYO2020 は COVID-19 の影響によって 2021 年に延期されたが、大会開催中、NISC は対処調整センターを運用し、インシデント対処等に 24 時間対応可能な態勢を構築・運用した。また、TOKYO2020 組織委員会（組織委）との円滑な連絡調整を行うための職員を組織委へ派遣している。TOKYO2020 期間中は、関係組織 Web サイトの閲覧障害等のインシデントが複数確認・報告されたが、TOKYO2020 運営に影響を与えるインシデント等を発生させずに大会を無事に終えた[75]。

TOKYO2020 を契機に得られた経験を、レガシーとして活かすべきと指摘されている。その経験とは、サイバーセキュリティ上のリスクへの対策の促進のために推進してきたリスクマネジメントや、関係機関等における相互の信頼関係を築き、サイバーセキュリティに係る脅威・インシデントに対し関係機関等が自律的に未然対処及び事案対処ができるよう対処調整センターを構築し、運用したといったことである。具体的には、インシデント対処に係る助言や支援を行うことができる情報セキュリティ関係機関、被害組織の事業所管省庁、治安機関等の関係組織と緊密に連携して対応に当たったこと、個別のインシデント対処のみならず、被害情報等を総合的に分析し、分析結果か

ら明らかになった攻撃者等に関する情報の発信、指令サーバのテイクダウンを始めとする対処に係る企画、支援を行うなどの積極的なサイバーセキュリティ対策の推進などである。これらの経験は、2021 年に閣議決定された CS 戦略において示された「ナショナルサート機能の強化」についての検討に連動すべきと指摘されている[76]。

4. 情報セキュリティ／サイバーセキュリティ戦略

ISPC が設置された以降は、政府の全体的・横断的な情報セキュリティ／サイバーセキュリティに係る戦略は、ISPC・CS 戦略本部／NISC によって企画・立案、推進・実施されている。それ以前は、IT 戦略本部の下の情報セキュリティ専門調査会が政策的事項を、また、対策推進会議及び対策推進室が対策的事項をまとめていた。ISPC が設置されたことにより、戦略的目標が示され、政策的・対策的事項が総合的に調整され、推進されることになった。以下に、ISPC／CS 戦略本部によって取りまとめられた戦略について背景・概要をまとめる。

4.1. ISPC による戦略

4.1.1. 第 1 次情報セキュリティ基本計画

第 1 次情報セキュリティ基本計画（1 次計画）[77]は、2006 年 2 月 2 日、ISPC によって決定された。本計画は、IT 戦略本部情報セキュリティ基本問題委員会第 1 次提言及び第 2 次提言（重要インフラ等に係る提言）[78]を受けて検討され、策定された 3 年計画である。同計画は、経済大国としての我が国の持続的な発展、IT を利活用してより良い国民生活を実現し及び IT 起因の脅威を十分考慮した安全保障の確保[79]を目指して、IT 基盤を新に依存可能で強固なものとすることが情報セキュリティの役割であるとした。そして、我が国の高品質、高信頼性、安全・安心という強みに基づく「セキュリティ立国」の思想に基づき世界最高の高度情報通信ネットワーク社会に見合った取組みを実施し、真に「情報セキュリティ先進国」になることを理念として持つものである。そのための基本目標は、「IT を安心して利用可能な環境」の構築（IT 基本法 22 条の具体化）、利便性とセキュリティの両立、「新しい官民連携モデル」の構築である。ここで「新しい官民連携モデル」とは、IT 社会を構成するあらゆる主体が情報セキュリティ問題への重要性についての共通認識の下、自らの責任を自覚しながら、それぞれの立場に応じた適切な役割分担の下で対策を実施することをいう。

1 次計画では、各主体が政府機関・地方公共団体、重要インフラ、企業及び個人に分類され、それぞれの計画内容が示されている。

政府については、2008 年度までに政府機関統一基準のレベルを世界最高水準のものとしすべての政府機関においてその水準の対策を実施することを目指す。そのために IPv6、国家公務員身分証 IC カード、暗号、生体認証等の新規機能の導入などを含む次世代の電子政府構築に向けて政府全体の業務・システムの基盤となる共通的なプラットフォーム構築の検討を行うことなどとしてた。また、地方公共団体については 2006 年 9 月を目処に情報セキュリティ確保に係るガイ

ドラインを見直し、2006 年度末までに地方公共団体間の情報共有体制整備を目指すとしていた。

重要インフラ[80]については、サイバー攻撃などの意図的要因に起因する障害以外の IT 障害への対策についての検討が不足しており、官民の情報共有体制が十分に構築されていないなどの問題を抱えている。そこで、政府は、2009 年度初めには、重要インフラにおける IT 障害の発生を限りなくゼロにすることを目指し、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」の策定、各重要インフラ分野における情報共有・分析機能（CEPTOAR[81]）の整備、重要インフラ連携協議会の創設促進、相互依存性解析の実施、分野横断的な演習の実施などを行うとした。

企業については、情報セキュリティ人材の確保・育成が十分でないという問題を抱えている。そこで、2009 年度初めには、企業における情報セキュリティ対策の実施状況を世界トップクラスの水準を目指し、情報セキュリティの観点からコーポレートガバナンスとそれを支える内部統制の仕組みの構築・運用を促進するとした。そのため、企業の情報セキュリティ対策が市場評価に繋がる環境整備、企業における情報セキュリティ対策担当者のモチベーション維持のための取組みなどをするとした。

個人については、情報セキュリティ教育の強化・推進、情報セキュリティの日の創設などによって情報セキュリティのリテラシー向上を支援し、政府が 20009 年度初めには IT 利用に不安を感じる個人を限りなくゼロにすることを目指すとした。

また、横断的な情報セキュリティ基盤の形成として、抜本的な技術革新の実現を目指すグランドチャレンジ型の研究開発・技術開発に取り組むとととともに、人材育成・確保、国際連携・協調の推進、犯罪取り締まり・権利利益の保護・救済を推進することとした。そして、1 次計画の推進体制として、旧 NISC について、横断的な情報セキュリティ問題に関する国際 POC(Point of Contact)としての機能を含めて政府全体の中核としての機能の強化を目指すとした。

なお、重要インフラ及び個人に係る取組み目標で「限りなくゼロにすることを目指す」という表現がある。これは、最初の基本計画であったため、情報セキュリティの世界ではリスク源は次々に出現するものの目標については高く示すべきと考え、「目指す方向」の究極の目標値としてゼロとしたというものである。ただし、必ずリスクは残るため、それは漸近線のような意味で、リスクが存在することを前提にして対策を考えていく必要があるという趣旨で「限りなくゼロを目指す」となっている[82]。

具体的な戦略的政策の推進にあたっては、1 次計画に基づき、各年度において年次計画が策定され、それを担当府省庁による実施状況を毎年度評価するかたちで行うこととされた。

2007 年度の年次計画では、政府全体として戦略的に国際協調・貢献に取組むための基本方針・具体策を検討することが盛り込まれた。そして、ISPC は、2007 年 10 月 3 月に、経済関係の進化が進むアジア地域のビジネス環境向上に向けた協調・貢献の推進、情報セキュリティに係る新しい諸権利に係るグローバルな検討・議論への貢献等を内容とする「我が国の情報セキュリティ分野における国際協調・貢献に向けた取組み」[83]を決定した。

4.1.2. 第 2 次情報セキュリティ基本計画

第 2 次情報セキュリティ基本計画（2 次計画）[84]は、2009 年 2 月 3 日、ISPC によって 3 年計画として決定された。1 次計画の下で情報セキュリティ政策は着実に推進された。しかし、IT 利活用が一層広がったともに、ボットネット、標的型攻撃などの脅威の高まりや PtoP ソフトウェア利用に起因する情報流出の頻発といった情勢変化を受け、2 次計画は、1 次計画を継続しつつもさらに発展させたものとなっている。1 次計画を発展させた考え方として、「（1次計画の下で）「追求された水準は、時として絶対的な無謬性の追求と言っても過言ではない水準であった。情報セキュリティに係るリスクの状況にかんがみると、このような水準の事前対策を実現することは、現実には容易でない。実現可能性や、結果を追求するためのコストとのバランス、情報セキュリティの確保と引換え（トレードオフ）になり得る利便性とのバランスの観点を考慮する必要」と示した点がある。そして、2次計画の下では、事故が生じ得ることを前提とした形での対応力を強めること、すなわち「事故前提社会」への対応力強化を実現するとした。「『事故前提社会』では、脅威によってリスクが現実のものとなり得る事態を想定し、リスクを予見・予防するとともに、生じる損害や障害を極力小さくするべく、対処の手立てなどを検討するというリスクマネジメント手法が重要となる」、すなわち、守りのセキュリティから攻めのセキュリティへと転換するものとなっている[85]。2 次計画では、1次計画における政府・地方公共団体、重要インフラ、企業、個人、そして横断的な情報セキュリティ基盤の形成という構造が維持され、施策の内容も基本的に承継されている。

2 次計画では、現在のサイバーセキュリティ政策においても重要な論点となるものが複数提示されている。例えば、設計段階からセキュリティを作りこむ開発手法の普及と定着を図ること、すなわち、セキュリティ・バイ・デザインの推進がその一つである。また、情報システムの設計、資材調達、生産、供給に係る一連の過程（サプライチェーン）がグローバル化・複雑化していることを受けて、製品・サービスの品質検証が困難な状況にあるため、政府等による情報システムの調達に際して、安全保障上の懸念が生じるおそれがあることを指摘している。

2 次計画により国際連携・協力の具体的な活動が一層推進された。その例として、我が国とASEAN が共同議長を務める日・ASEAN 情報セキュリティ政策会議がある。第 1 回会合は 2009 年 2 月に東京で開催された。そして、2010 年 3 月にタイで開催された第 2 会合で、地域で共通する情報セキュリティ上の課題について議論を深め、日・ASEAN における情報セキュリティに関する協力事項を定めた「連携枠組み」を採択した[86]。その後も、日・ASEAN の連携・協力は継続しており、政策会議やワークショップの開催、ASEAN 加盟国とのサイバー演習及び机上演習の実施などを行ってきている[87]。

4.1.3. 国民を守る情報セキュリティ戦略

2010 年 5 月 11 日、ISPC は、「国民を守る情報セキュリティ戦略」（国民を守る戦略）[88]を決定した。同戦略は、2 次計画策定後、2009 年 7 月に米韓における大規模サイバー攻撃事態が発生したほか、大規模な個人情報漏えい事案の発生も後を絶たないことなどが策定の背景としており、

2次計画を包含する 4 年間(2010 年度から 2013 年度)を対象とした包括的なものとの位置づけである。大規模サイバー攻撃等、我が国の安全保障・危機管理に影響を及ぼしうるサイバー攻撃から国民を守るため、平素からの取組みを強化するとともに、サイバー攻撃事態が発生した際に有効に対処できる体制を整備することなどが新たに追加された中核事項となっている。リスクが発生した時点でその都度対応するといった対処療法的な対策ではなく、IT 進歩が著しいなか問題の根本的な解決をもたらす情報セキュリティ対策の検討などを戦略的に行うことなど、より能動的に取組む体制の実現を目指したものとなっている。

国民を守る戦略は、2 次計画策定から 1 年 3 か月で策定されており、また、2009 年 9 月 16 日に自民党から民主党に政権が交代していることから、政権移行との関係があるのではないかとの疑問がある。この点、2 次計画において十分とは言い切れなかった大規模攻撃対応体制について、その強化の方針は、政権交代以前から検討開始されており、情報セキュリティは実務政策性が強いことから、政権交代があってもその方針は変わらなかった[89]というのが実態である。従って、政権交代が、短期間で新たな補完的戦略が ISCP で決定されたことの理由にあったというものではない。

4.1.4. サイバーセキュリティ戦略(2013 年版)

2013 年 6 月 10 日、ISCP は「サイバーセキュリティ戦略」[90](CS 戦略 2013)を決定した。「サイバーセキュリティ戦略」としたのは、従来の情報セキュリティ確保のための取組みはもとより、広くサイバー空間に係る取組みを推進する必要性と取組姿勢を明確化するためである[91]。CS 戦略 2013 は、IoT(Internet of Things)の登場・普及により、サイバー空間と実空間の「融合・一体化」の進展、サイバー空間を取り巻く「リスクの深刻化」、「甚大化するリスク」といった環境の変化を受けて、情報の自由な流通の確保、深刻化するリスクへの新たな対応、リスクベースによる対応の強化、社会的責務を踏まえた行動と共助を基本的な考え方に置いたものとなっている。そして、国、重要インフラ事業者等、企業・教育研究機関、一般利用者や中小企業及びサイバー関連事業者(インターネットサービスプロバイダー、ハードウェア・ソフトウェア開発者等)といった各主体の役割を示した。

政府機関に関する取組みとして、政府情報システムのクラウド化やサプライチェーン・リスクへの対応強化といった情報及び情報システムに係る情報セキュリティ水準の一層の向上、GSOC や CYMAT の体制強化といったサイバー攻撃への対処態勢の充実・強化などを行う。また、重要インフラ分野においては、制御系機器・システム等の調達・運用における国際標準に則った評価・認証導入の在り方の検討、秘密保持契約に基づく情報共有体制の深化などを図る。さらに、一般利用者等についてはサイバーハイジーンを国民運動とするための取組みを行うなどを通じて、「強靱な」サイバー空間の構築を図ることとした。サイバー防衛に関しては、サイバー空間は、自衛隊等による情報収集、攻撃、防御といった様々な活動がその中で行われる、陸・海・空・宇宙と並び得る新たな「領域」であり、サイバー防衛隊(仮称)の新編等による体制整備、高度の専門性を有し

た人材の安定的な確保や高度な研究開発などサイバー空間における自衛隊の能力・態勢強化などが示された。

また、サイバーセキュリティ産業の活性化や研究開発、人材育成を通じて、「活力ある」サイバー空間の構築をするとした。情報の自由な流通の確保、法の支配といった価値観を共有する国・地域とのパートナーシップ等外交を通じるなどして、「世界を率先する」サイバー空間の構築をするとしている。

CS 戦略 2013 によって、戦略の推進体制に関して、専門職員の採用、育成といった人事管理による人材の確保や権限等の必要な組織体制を整備することにより、2015 年度を目途として NISC を「サイバーセキュリティセンター」(仮称)に改組することが決定された。この改組の方針を含めて CS 戦略 2013 のキーワードは、CS 基本法の内容と方向性が近い。CS 戦略 2013 決定と CS 基本法が与党内で検討が開始された時期は同時期であり、法案検討初期に、一定程度、参考にされたものと思われる。

2013 年 10 月 2 日、ISCP は「サイバーセキュリティ国際連携取組方針」[92]を決定した。これは、CS 戦略 2013 が決定されたことなどを踏まえ、サイバーセキュリティ分野における国際連携・共助に関する我が国の基本方針や重点取組分野等を整理し、国内外に示すものである。情報共有体制の強化、サイバー犯罪への適切な対応、サイバー安全保障における協力体制の確立などによるサイバー事案への動的対応の実践、CSIRT 構築支援や運用能力の開発支援など動的対応に備えた「基礎体力」の向上、サイバーセキュリティに関する国際的なルール作りへの積極的貢献などを取組み内容とする。地域的な取組みについては、我が国企業による投資の増加等を踏まえ、特に ASEAN との関係を重視している。

4.2. CS 戦略本部による戦略

CS 基本法施行後、CS 戦略は同法に基づき CS 戦略本部により案が作成され、これまで 2015 年、2018 年及び 2021 年に閣議決されている。

4.2.1. CS 戦略(2015 年版)

CS 基本法に基づく最初の CS 戦略(CS 戦略 2015)[93]は、2015 年 9 月 4 日に閣議決定された。2015 年 5 月 25 日に CS 戦略 2015 の意見招請プロセスに付す案が CS 戦略本部によって了解された。その後直後に JPS 事件が発生し、同事件について NISC によって実施され原因究明調査の報告書(2025 年 8 月 20 日付け)を踏まえた CS 戦略案の内容の見直しも行われたため、9 月の閣議決定となった。

CS 戦略 2015 の構造は、目的や基本原則などを示す総論と、目的達成のための施策として、経済社会の活力の向上・持続的発展、国民が安全で安心して暮らせる社会の実現、国際社会の平和・安定及び我が国の安全保障という 3 つの柱と、その基盤となる研究開発、人材育成・確保といった横断的施策から成る。

本戦略では、サイバー空間を、「国境を意識することなく自由にアイディアを議論でき、そこで生

まれた知的創造物やイノベーションにより、無限の価値を産むフロンティア」である人工空間と説明した。これはサイバー空間における脅威の深刻化が進むなか、サイバー空間の安全確保には民間による積極的な投資が重要であり、民間の投資意欲を高める表現を採ったものといえる[94]。

CS 戦略 2015 の目的は、「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」[95]に寄与することとした。そして、基本原則として、「情報の自由な流通の確保」、「法の支配」、「開放性」、「自律性」及び「多様な主体の連携」を挙げた。サイバー空間について、国家主権を強調する中国、露等の立場と、領土内の情報通信インフラなどに対する主権の他は国家の関与を極力控えて情報の自由な流通の確保や表現の自由を重視する米欧の立場が激しく対立するようになっていたなか、我が国は、CS 戦略 2015 の基本原則を明確にすることによって、米欧の立場と同じくすることを国際的に表明したといえる[96]。

CS 戦略 2015 の実践にあたって強調された考え方のひとつに「機能保証」がある。これは、米国国防省の“Mission Assurance”[97]の考え方、すなわち、あらゆる環境・条件下で、組織の任務遂行に重要な機能にとって不可欠な能力や資産の持続性・回復力を守り、保証するプロセスを、我が国の民生分野に応用したものといえる。サイバーセキュリティは、しばしば、それ自体が目的化することがある。しかし、組織は、その任務・業務を効果的に遂行するために ICT を導入する。組織には、サービス提供などの任務を全うする責任があり、組織の任務を安全かつ着実に遂行できるよう、サイバーセキュリティを検討すべきであることについて強調したものといえる[98]。

各論については、1 つめの柱、経済社会の発展に係る施策としては、IoT システムの安全・品質などを高めること、セキュリティマインドを持つよう経営層の意識改革を促進すること、セキュリティに係るビジネス環境を整備することなどを挙げた。2 つめの柱、安全安心な社会実現に係る施策としては、サイバー犯罪から国民や一般の企業などを守ること、重要インフラ事業者・地方公共団体に係る取組み、さらに国の機関のサイバーセキュリティ強化を図ることなどを示した。特に、政府機関・独法等に関する取組みは、JPS 事件の経験を踏まえ、防御策の強化を強調している。3 つめの柱、安全保障等は、2013 年に決定された国家安全保障戦略[99]においてサイバーセキュリティの方針が示され、サイバーセキュリティ政策の中で安全保障の重要性が一層高まったこともあり柱として位置付けられたといえる。警察や自衛隊を始めとする対処機関の能力を質的・量的に向上、先端技術の活用・防護等による我が国の安全の確保と、国際場裡におけるサイバー空間における国際的な法の支配の確立に向けた積極的取組みやキャパシティビルディングへの協力などの施策から構成される。横断的施策として、人材育成・確保に関しては、サイバーセキュリティの圧倒的な人材不足が従来から指摘されていたところ、2014 年に ISPC によって決定された人材育成に係るプログラム[100]を踏まえて、突出した能力を有しグローバルに活躍できる人材の発掘・育成・確保のみならず、サイバーセキュリティについて経営層を事業戦略企画・実施や企業リスク管理の観点から支え、かつ、実務者層をリードできるような両者の層の間の人材層の育成を強調したものとなった[101]。

なお、CS 戦略 2015 期間中の 2017 年 1 月から、CS 戦略本部は「2020 年及びその後を見据えたサイバーセキュリティの在り方について」（中間レビュー）の議論を開始した。その中で、重要インフラ等に関する取組みの強化[102]として、障害・事故、脅威情報の総合的な情報共有（バーチャル脅威情報集約センター構築）等の検討を行った。同年 5 月に WannaCry 事件が発生したが、（重要インフラのみならず広く）情報を迅速に共有することで被害拡大防止に資する可能性があったことなどが指摘された。これを受け、同年 7 月、CS 戦略本部は、官民が一体となって効果的な情報連携体制を構築するための制度整備を実施する情報共有・連携ネットワーク（仮称）の構築・運用を含む「中間レビュー」を決定[103]した。同決定を踏まえて検討が進められ、サイバーセキュリティ協議会の設置に係る CS 基本法改正が行われた[104]。

4.2.1. CS 戦略（2018 年版）

CS 戦略 2015 を改定した新たな CS 戦略(CS 戦略 2018)[105]は、2018 年 7 月 27 日に閣議決定された。これは、人工知能(AI)が劇的に進化し、また、サイバー空間と実空間の一体化が進んだなかで、重要インフラ事業者以外の者が顕著な被害を受けた 2017 年の WannaCry 事件などの経験を踏まえて、より多くの者による協働の重要性[106]や、より多くの者への情報発信などの重要性が認識されたなかで策定された戦略である。

CS 戦略 2018 の目的や基本原則は、短期間で変わるものではなく、CS 戦略 2015 と同じである。そして、戦略立案や推進におけるサイバーセキュリティ政策の在り方として、3つの観点、すなわち①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働という点から、サイバーセキュリティに関する官民の取組みを推進することし、サイバー空間における安全・安心と経済発展を両立させ、信頼できるサイバー空間が自律的・持続的に進化・発展することを目指すこととした。①の任務保証は CS 戦略 2015 における機能保証と同じことを意味しているが、Mission Assurance の考え方を明確に伝えるべく、本戦略では、そのまま日本語とした用語となっている。

CS 戦略 2018 の構造も、CS 戦略 2015 の構造を踏襲している。すなわち、総論に続く各論は、経済社会の発展、安全安心な社会、安全保障等の 3 本柱と、その基盤としての横断的施策から構成される。「経済社会の発展」の柱では、経営層の意識改革、サイバーセキュリティ投資の促進、価値創造プロセスのサプライチェーンや中小企業に対する取組みなどが強調された。

「安全安心な社会」の柱では、攻撃者の情報を得るために攻撃誘引技術の活用や、ボットに感染するリスクが高い弱いパスワード設定の IoT 調査等の活動を念頭に「積極的サイバー防御」の考え方を打ち出した。また、大学等の先端技術・機微技術の防護や、WannaCry 事件などの経験も踏まえて、多様な主体間での情報共有・連携体制を強調した。さらに、実空間において発生する事案の原因がサイバー攻撃にあることも将来十分にあり得るため、「大規模サイバー攻撃事態等への対処態勢の強化」についての節を設けた。加えて、CS 戦略 2018 の期間中に TOKYO2020 が開催されるため、そのための取組みの節も設けられた。

「安全保障等」の柱については、CS 戦略 2018 案過程で、NSC から「我が国は、悪意のあるサ

イバー活動に対して、同盟国・有志国とも連携し、政治・経済・技術・法律・外交その他の取り得るすべての有効な手段と能力を活用し、断固とした姿勢・対応をとる」という意見が CS 戦略本部に出された。これを受けた記述が、安全保障等の柱において記述されている。その具体的な実施例としては、外交的な非難[107]などを行っている[108]。

横断的施策については、人材育成に関して、経営層・実務者層の間の層を「戦略マネジメント層」と呼ぶようになり、その育成・定着を、実務者層の育成・定着等とともに方針が示された。研究開発については、AI、ブロックチェーンなどの先進的技術を用いたサイバーセキュリティ確保などが示されている。普及啓発について CS 戦略 2015 では安全安心な社会の柱における国民に係る施策として位置付けられていたが、CS 戦略 2018 では、横断的施策の一つとして「全員参加による協働」の施策となった。

4.2.1. CS 戦略（2021 年版）

2 度目の改正が図られた CS 戦略(CS 戦略 2021)[109]は、2021 年 9 月 28 日に閣議決定された。CS 戦略 2021 は、リモートワークなどが急速に広がった COVID-19 によるニューノーマルや TOKYO2020 開催を経験し、2021 年 9 月 1 日にデジタル庁が発足した後に決定されたものである。サイバー脅威については、CS 戦略 2018 期間中に、国内外でランサムウェアの被害が顕著となった。また、中国・ロシア・北朝鮮において、軍をはじめとする各種機関のサイバー能力の構築が進められて地政学的緊張が高まってきている。その様ななかで、国家が背景にいる可能性の高いサイバー攻撃事件に対して、我が国として外交的な非難を実施し、また、中国人民解放軍を背景に持つサイバー攻撃グループが関与した可能性が高いサイバー攻撃の事件[110]も経験している。

こうしたことを背景として、CS 戦略 2021 では、目的、基本原則については、従来の CS 戦略におけるものを維持しつつ、目的達成のための施策として、～Cybersecurity for All～デジタル化の動きと呼応し「誰一人取り残さない」サイバーセキュリティの確保に向けた取組みを進める考え方を基本とした。CS 戦略 2018 では「全員参加による協働」の考え方がしめされており、「for all」ではなく「by all」のようにも思われる。この点、CS 戦略 2021 では、「for all」としているが、従来からの意味での「by all」の重要さは変わっていない。CS 戦略 2021 では、「全員が自らの役割を主体的に自覚してサイバーセキュリティに取り組む」という考え方を「for all」の概念に含むことを示している。新たに参画してくる主体を守るとともに、自らの役割を主体的に自覚してサイバーセキュリティに取り組むこともあわせた形で「for all」という言葉が用いられたものである[111]。なお、一般社団法人日本経済団体連合会も、「Cybersecurity for All に加えて誰もが主体的に危機意識を持って取り組む(Cybersecurity by All)が重要」[112]としている。

CS 戦略の施策の主たる対象としては、従来から政府機関や重要インフラなどがあった。CS 戦略 2021 では、新たにサイバー関連事業者、そして重要技術を保有する主体も重要ドメインとして位置づけ、政府として一元的に対応していくこととしている[113]。

CS 戦略 2021 の構造は、従来の CS 戦略と同様に、総論に続き、各論として「経済社会の発展」、

「安全安心な社会」、「安全保障等」の 3 本柱と、その基盤としての横断的施策を置いた。「経済社会の発展」では、製品・サービスのデジタル化が進む中で、サイバーセキュリティ自体が企業価値に直結する営為になってきていることから、セキュリティ・バイ・デザインをはじめ、DX with Cybersecurity の考え方などを強調している。サプライチェーンの信頼を高める取組みも重視している。

「安全・安心な社会」については、自助・共助による自律的なリスクマネジメントが進むような環境づくりを国が推進する。新たなサイバーセキュリティの担い手との協調(クラウドサービスへの対応)などを行う。また、国として重大なサイバーセキュリティ事件が発生したときに適切に対応できるような仕組みとして、包括的なサイバー防御の総合的な調整を担うナショナルサート(CSIRT/CERT)機能等を強化することとしている。2023 年の主要国首脳会議(G7 サミット)、2025 年の日本国際博覧会 (expo2025)が我が国で開催されるが、大きな国際イベントはサイバー活動も活発になる傾向があるので、それに向けた体制強化において TOKYO2020 の経験を役立てていくことになる[114]。

「安全保障等」については、信頼性のある自由なデータ流通(Data Free Flow with Trust: DFFT)や 5G セキュリティ等国際的な取組みの進展を踏まえた我が国の基本理念に沿う国際ルールの策定といったサイバー空間におけるルール形成を行っていく。また、自衛隊及び米軍の活動が依拠する重要インフラ及びサービスの防護のため共同演習等の着実な実施、防衛省・自衛隊におけるサイバー関連部隊の体制強化等のサイバー防衛能力の抜本的強化をするとした。また、抑止として、一定の場合には、サイバー攻撃が日米安全保障条約第 5 条の規定の適用上武力攻撃を構成し得ることを確認したこと、我が国への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力も活用すること、サイバー攻撃に関する非難等の外交的手段や刑事訴追等の手段も含めて対応することなど、これまでより具体的な内容が示された。

横断的施策については、AI や量子技術といった先端的な研究開発を進める。また、人材育成において、DX with Cybersecurity を推進していく上で、内外のセキュリティ専門人材との協働等が円滑に行われることが重要である。経営層や、企業・組織内で DX を推進するマネジメントに関わる人材層をはじめとして、IT やセキュリティに関する専門知識や業務経験を必ずしも有していない様々な人材に対して「プラス・セキュリティ」知識が補充されるべく施策を推進することとした[115]。

5. まとめ

我が国における情報セキュリティ／サイバーセキュリティ(以下、まとめて「サイバーセキュリティ」と記述する)に係る政策、特に戦略とその推進体制、その基礎となる CS 基本法について概観した。これらを俯瞰してみると、戦略、組織等に変遷について特徴がみられるが、それらのいくつかの例を次にまとめる。

① サイバーセキュリティ対策からより広い領域の戦略に

2005 年以前は、政府や重要インフラにおけるサイバーセキュリティ対策の推進と、IT 政策の一環としてのサイバーセキュリティの戦略的な政策の立案が、それぞれの場で検討されていた。2005 年に ISPC と旧 NISC が設置されたことにより、サイバーセキュリティ対策と政策的戦略が一体的に検討され方向付けられるようになった。この点は、オペレーショナルな施策と戦略的施策とを一体的に取組めることの相乗効果を得られる利点があるといえる。例えば、2015 年の JPS 事件を受けて、GSOC システムの強化を含む政府のサイバーセキュリティ対策強化や人材育成・確保などを内容とする CS 戦略を策定し、その後 GSOC システムの強化を図ったことや政府全体における人材育成・確保の方針を定めて着実に人員強化するようになったこと[116]はその一例である。

サイバーセキュリティ政策については、2000 年代初期から、侵害されたときの経済社会への影響の大きさから、対策の指針、基準等を定めるなど政府機関及び重要インフラを重点的な対象として対応してきている。官民連携、官民情報共有、民間の知見活用を重要する点も、対策推進室の時期から変わらない。一方、政府・重要インフラ・民間企業などにおいて IT の利活用の幅が広がり、また、新たなサービスや技術の登場に合わせてその政策範囲も拡大してきた。例えば、2005 年以降、企業の経営層の役割りの重要性を従前よりも強く指摘し、ガバナンスなどを強調する政策や、人材育成の強化などを、サイバーセキュリティ政策対象は広がりを見せている。また、クラウド、IoT、AI など新たな技術やサービスを対象とした政策もその社会における普及の度合いなどに応じて、内容も充実させてきている。

② サイバーセキュリティ推進者（supplier）主導から利用者（consumer）主導に

2005 年の戦略文書（1 次計画）以来、いかに経営層を意識づけるか、重要インフラ事業者における行動を促進するかなど、サイバーセキュリティ推進者(supplier)の視点からの政策・施策が中心にあった。戦略の推進者・実施者も、主として旧 NISC などのサイバーセキュリティ部局であった。安全保障とサイバーセキュリティに係る事項もサイバーセキュリティ推進者の視点からの内容であった。

しかし、政府、企業などさまざまな分野で DX が進み、組織の IT 依存度の高まりに伴うサイバーリスクの増大がみられ、サイバーセキュリティのサービスの利用者（consumer）である個別の政府機関においてサイバーセキュリティ対策をより積極的に推進するようになっている。また、State Sponsored のサイバー攻撃を含めてサイバー脅威が安全保障に係る問題として深刻化するなか、サイバーに関わる機能の Consumer である安全保障関係者が主導的になってきた。例えば、CS 基本法成立後は CS 戦略本部が NSC からの意見を受けて CS 戦略を決定するようになり、その内容は安全保障当局の方針を反映している。

サイバーセキュリティ推進組織の在り方についても、従来は、IT 戦略本部や CS 戦略本部の決定によってサイバーセキュリティ推進組織の形を決めてきた。しかし、今般、安保戦略 2022 によっ

てサイバー安全保障の推進体制として NISC の発展的改組の方針が示された。本来 IT やサイバーセキュリティはテクニカルなツールであるため、企業活動、重要インフラサービスなど含めて、ツールを利用する主体となる者が、サイバーセキュリティ政策に意見・要求を示すことがあるべき姿であると考えられる。まさに、安全保障の領域から大きな方針が示されたわけである。

③ 重心が置かれるサイバーセキュリティ政策・施策の変動性

限られたリソースの中でサイバーセキュリティ政策・施策についての重心の置き方の提示は重要である。これまでのサイバーセキュリティに係る戦略や、そこに示される政策・施策の変遷をみると、この重心の置き方に変動性がみられるものがある。

例えば、1 次計画(2006)では、サイバー攻撃への緊急対応能力の強化も言及しているが、戦略の基底には、政府統一基準による底上げを図り世界最高水準を目指すことなど、我が国のサイバーセキュリティ水準を引き上げるための予防的・管理的な面に重点が置かれているように見える。これが、国民を守る戦略(2010)では、大規模攻撃対応体制が不十分であるとして、その強化を図ること、すなわち事後対応に重点がシフトしたように見える。CS 戦略 2015 では、戦略目標を達成するための施策を示す各論で経済社会の発展、安全安心な社会実現、安全保障等の順で柱が建てられ、GSOC の強化など発見的な取組みも示されているが、全体的には、ガバナンスや機能保証などの予防的・管理的な面に重点が置かれている。CS 戦略 2018 では、改めて大規模サイバー攻撃への危機管理に係る節を設けた。このように、予防的・管理的な面と、発見的・事後対処的な面の重心の置き方には変動性がみられる。両者はいずれも重要な取組みであり、適切なバランスが図られる必要があるが、社会的に意識され実施される施策にはその時々の情勢や人々の意識、それまでの取組みの蓄積状況などを受けて、必要な補正がなされるものである。そうした点が、戦略の重点の置き方に影響したものといえよう。

また、個別の施策をみると、例えば緊急対応を支援する体制については、2002 年に NIRT が対策推進室に置かれた。2008 年に旧 NISC のもとに GSOC の体制が整えられると、システムによる監視といった側面が強くなる。その後、現実に支援に行く体制が改めて置かれたのは 2012 年の CYMAT となる。こうした支援体制の重要性は、迅速かつ有益な情報提供をはじめとする被害組織に対する有益な活動を実質的にできているかによるところが大きい。この点は、重要インフラにおける情報共有や、サイバーセキュリティ協議会における活動でも同様で、情報共有体制への参加者や被害組織にとって有益な活動や迅速な情報が提供されかがポイントとなる。そのため、例えば、活動や情報を提供する組織としての知見・経験を着実に積み重ね、随時、支援などできる体制を維持する取組みがなされているとは考える。しかし、支援体制を構成する要員が持つ知見・経験については、異動などの影響を受ける。また、組織の活動についての継続的な見直しなどあり、支援体制、情報共有体制などが変化してきていることも事実である。こうしたことにより変動性がみられるものと考えられる。

以上のようにまとめた戦略、組織等の変遷の特徴を踏まえ、今後の戦略や政策の企画立案にあたって、いくつかの留意すべき事項が考えられる。

① 範囲が広がるサイバーセキュリティに係る戦略の検討にあたって:

今後とも、新たな技術の登場・普及、適用範囲の拡大、データの利活用は進展していく。このため、新たな技術の動向、その適用状況、開発現場の実態などを把握し、その技術の本質やメカニズムを踏まえてサイバーセキュリティ上の課題を洗い出したうえで、戦略を検討する必要があろう。

② サイバーセキュリティ利用者主導の戦略・政策推進にあたって:

サイバー安全保障については主導する主体が意志をもって推進できる。一方、一般の市民や中小企業などは、サイバーセキュリティ政策企画立案・実施者に対して集団としての意見・要求を示すことが難しいので、この点については、特段の配慮が必要になろう。

③ 重点の置かれる戦略・政策の変動性について:

戦略・政策の立案にあたっては、新たなテーマ、課題に直面したときに、過去においても類似した／本質が同等の課題に取り組んでいる可能性があることに注意が必要であろう。その場合には、過去の課題への取組み成果を評価した上で、新たなテーマ等への対応が求められよう。このため、戦略・政策の検討にあたっては、過去から将来にわたり、より中長期的視点をもって見直し、検討、企画・立案、実施が必要であると考える。

---

[1] 内閣官房「国家安全保障戦略について」(https://www.cas.go.jp/jp/siryou/221216anzenhoshou.html (2023 年 3 月 20 日閲覧))

[2] 平成 26 年法律第 104 号

[3] サイバーセキュリティ基本法 12 条。

[4] 平成 12 年法律第 144 号。デジタル社会形成基本法により廃止された。

[5] 2015 年 5 月 28 日、外部から送付された不審メールに起因する不正アクセスにより、JPS が保有している個人情報の一部(約 125 万件)が外部に流出したことが判明した事件。

[6] 三角育生、「サイバーセキュリティ基本法制定・改正の経緯」、日本セキュリティ・マネジメント学会誌 2020 年、Vol.34、No.1、p28-34。

[7] 2016 年 10 月から翌年 2 月にかけて、未来投資会議の下の第 4 次産業革命・イノベーション会合にて、「重要インフラに係る制度整備が必要」といった問題意識が示されているなかで検討が進められていた。

[8] 我が国を含む世界約 150 か国以上、数十万台の端末等で感染が確認された事件。我が国では、重要インフラ事業者ではない大手企業における顕著な被害が観測された。

[9] CS 戦略本部、「2020 年及びその後を見据えたサイバーセキュリティの在り方について」(https://www.nisc.go.jp/pdf/policy/kihon-s/csway2017.pdf (2023 年 3 月 26 日閲覧))

[10] 岡村久道編、『サイバーセキュリティと法律』、商事法務、2019 年 12 月、p12-14。

[11] 三角育生、「サイバーセキュリティ基本法制定・改正の経緯」、日本セキュリティ・マネジメント学会誌 2020 年、Vol.34、No.1、p28-34。

[12] 令和 3 年法律第 35 号。33 条（サイバーセキュリティの確保等）参照。

[13] 例えば、Cyber Exploitation といったものが含まれる可能性が否定されないと思われる。

[14] CS 基本法 3 条 1 項。
[15] 「政府・行政サービス」は、重要インフラ事業者“等”としてまとめられている。
[16] 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 17 日）」（https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf (2023 年 3 月 20 日閲覧)）
[17] 令和 4 年法律第 43 号、
[18] 内閣府、「経済安全保障推進法の概要」（https://www.cao.go.jp/keizai_anzen_hosho/doc/gaiyo.pdf (2023 年 3 月 20 日閲覧)）
[19] CS 基本法 31 条 1 項 1 号。
[20] CS 基本法 26 条 1 項
[21] NISC「サイバーセキュリティ基本法第 13 条の規定に基づきサイバーセキュリティ戦略本部が指定する法人(2016/10/21 CS 戦略本部決定)」（https://www.nisc.go.jp/pdf/council/cs/shiteihojin.pdf (2023 年 3 月 27 日閲覧)）
[22] 第 190 回国会衆議院内閣委員会議事録第 10 号（2016/3/30）平井たくや委員の質問に対する政府参考人説明参照。
[23] 三角育生、「サイバーセキュリティ基本法制定・改正の経緯」、日本セキュリティ・マネジメント学会誌 2020 年、Vol.34、No.1、p28-34。
[24] CS 基本法 33 条 1 項
[25] CS 基本法 35 条
[26] CS 基本法 17 条
[27] 三角育生、「サイバーセキュリティ基本法制定・改正の経緯」、日本セキュリティ・マネジメント学会誌 2020 年、Vol.34、No.1、p28-34。
[28] CS 基本法 31 条 1 項 2 号。
[29] NISC「サイバーセキュリティ協議会について」（https://www.nisc.go.jp/pdf/council/cs/kyogikai/kyogikai_gaiyou.pdf (2023 年 3 月 27 日閲覧)）
[30] 第 186 回国会衆議院内閣委員会議事録第 23 号（2016/6/11）関芳弘委員の質問に対する平井たくや委員の答弁参照。
[31] CS 基本法 19 条
[32] 三角育生、「サイバーセキュリティ基本法制定・改正の経緯」、日本セキュリティ・マネジメント学会誌 2020 年、Vol.34、No.1、p28-34。
[33] 国立国会図書館 Web Archiving Project サイト（WARP）内 NISC「情報セキュリティ関係省庁局長等会議の設置について」（https://warp.da.ndl.go.jp/info:ndljp/pid/8245066/www.nisc.go.jp/active/sisaku/0917kyokutyou.html (2023 年 3 月 20 日閲覧)）
[34] WARP/NISC「ハッカー対策等の基盤整備に係る行動計画」（https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/active/sisaku/0121actionplan.html (2023 年 3 月 20 日閲覧)）
[35] JPCERT/CC「インターネットセキュリティの歴史第 5 回」（https://www.jpcert.or.jp/tips/2007/wr071801.html (2023 年 3 月 20 日閲覧)）
[36] 同本部は、IT 戦略本部の前身にあたり、1994 年に設置されたもの。
[37] WARP/NISC「ハッカー・サイバーテロ対策に関する体制の整備について」（内閣総理大臣発言要旨）（https://warp.da.ndl.go.jp/info:ndljp/pid/8245066/www.nisc.go.jp/active/sisaku/0222souri.html (2023

年 3 月 20 日閲覧))

[38] WARP/NISC「情報セキュリティ対策推進会議の設置について」(https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/conference/suisinkaigi/0229suisinkaigi.html (2023 年 3 月 27 日閲覧))

[39] WARP/NISC「内閣サイバーセキュリティセンター(NISC)とは」(https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/about/details.html (2023 年 3 月 20 日閲覧))

[40] WARP/NISC「情報セキュリティ基本問題委員会第 1 次提言」(https://warp.da.ndl.go.jp/info:ndljp/pid/998223/www.nisc.go.jp/conference/kihon/teigen/pdf/1teigen_hontai.pdf (2023 年 3 月 28 日閲覧)) p10 参照。

[41] WARP/IT 戦略本部「IT 戦略本部（第 1 回）2001 年 1 月 22 日開催」(https://warp.da.ndl.go.jp/info:ndljp/pid/1165057/www.kantei.go.jp/jp/singi/it2/dai1/1gijisidai.html (2023 年 3 月 28 日閲覧))

[42] WARP/NISC「情報セキュリティ対策推進会議」(https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/conference/suisinkaigi/index.html (2023 年 3 月 27 日閲覧))

[43] 首相官邸「e-Japan 戦略 II 加速化パッケージ」(https://www.kantei.go.jp/jp/kakugikettei/2004/040206ejapan.pdf (2023 年 3 月 27 日閲覧))

[44] WARP/NISC「IT 戦略本部決定『情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて』について」(https://warp.da.ndl.go.jp/info:ndljp/pid/11688280/www.nisc.go.jp/conference/kihon/teigen/press.html (2023 年 3 月 28 日閲覧))

[45] WARP/NISC 「IT 戦略本部決定 情報セキュリティ政策会議の設置について」(https://warp.da.ndl.go.jp/info:ndljp/pid/11688280/www.nisc.go.jp/press/050530seisaku-press.html (2023 年 3 月 28 日閲覧))

[46] WARP/NISC「情報セキュリティ政策会議の設置について」(https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/conference/seisaku/pdf/050530seisaku-press.pdf (2023 年 3 月 20 日閲覧))

[47] WARP/NISC「情報セキュリティ政策会議第 33 回会合 議事要旨」(https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/conference/seisaku/dai33/pdf/33gijiyoushi.pdf (2023 年 3 月 27 日閲覧)) 及び「情報セキュリティ政策会議第 34 回会合 議事要旨」(https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/conference/seisaku/dai34/pdf/34gijiyoushi.pdf (2023 年 3 月 27 日閲覧)) を参照。

[48] CS 戦略本部の民間有識者が 2019 年度から 8 名になっている。

[49] WARP/NISC「情報セキュリティ政策会議第 37 回会合 議事要旨」(https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/conference/seisaku/dai37/pdf/37gijiyoushi.pdf (2023 年 3 月 27 日閲覧)) 及び「情報セキュリティ政策会議第 38 回会合 議事要旨」(https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/conference/seisaku/dai38/pdf/38gijiyoushi.pdf (2023 年 3 月 27 日閲覧)) 参照。

[50] WARP/NISC「普及啓発・人材育成専門委員会の設置について」(https://warp.da.ndl.go.jp/info:ndljp/pid/11688280/www.nisc.go.jp/conference/seisaku/jinzai/dai1/pdf/

shiryou01.pdf (2023 年 3 月 28 日閲覧))

[51] JCIC「日本のサイバーセキュリティ政策史 第 3 回」(https://www.j-cic.com/pdf/report/Participating-the-Start-up-of-NISC.pdf (2023 年 3 月 27 日閲覧))

[52] WARP/NISC「内閣官房情報セキュリティセンター(NISC)の設置について」(https://warp.da.ndl.go.jp/info:ndljp/pid/998223/www.nisc.go.jp/press/pdf/nisc_press.pdf (2023 年 3 月 28 日閲覧))

[53] NISC「政府機関の情報セキュリティ対策のための統一基準(2005 年項目限定版)」(https://www.nisc.go.jp/pdf/policy/general/2siryou04-3d.pdf (2023 年 3 月 28 日閲覧))

[54] NISC「政府機関の情報セキュリティ対策のための統一基準(2005 年 12 月版(全体版初版))」(https://www.nisc.go.jp/pdf/policy/general/k303-052.pdf (2023 年 3 月 28 日閲覧))

[55] WARP/NISC「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/12213293/www.nisc.go.jp/active/infra/pdf/infra_rep.pdf (2023 年 3 月 28 日閲覧))

[56] Government Security Operation Coordination Team

[57] WARP/NISC「２００８年度の情報セキュリティ政策の評価等」(https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/active/kihon/pdf/sjeval_2008.pdf (2023 年 3 月 28 日閲覧)) p4 参照。

[58] 三角育生、「大規模 IT セキュリティインデント対処の政策的影響」、日本セキュリティ・マネジメント学会誌　2020 年、Vol.34、No.2、p22-28。

[59] 2008 年 4 月に第 1 期、2013 年 4 月に第 2 期、2017 年 4 月に第 3 期、2021 年 4 月に第 4 期 GSOC システム運用開始。

[60] NISC「サイバーセキュリティ 2022(2021 年度年次報告・2022 年度年次計画）」(https://www.nisc.go.jp/pdf/policy/kihon-s/cs2022.pdf (2023 年 3 月 28 日閲覧)) p20 参照。

[61] Cyber Incident Mobile Assistance Team

[62] WARP/NISC「三菱重工業等に対するサイバー攻撃事案について」(https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/conference/suishin/ciso/dai3/pdf/s2.pdf (2023 年 3 月 28 日閲覧))

[63] WARP/NISC「情報セキュリティ対策に関する官民連携の在り方について」(https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/conference/suishin/ciso/dai4/pdf/1-1.pdf （2023 年 3 月 28 日閲覧))

[64] WARP/NISC「情報セキュリティ緊急支援チーム（CYMAT）設置について 」(https://warp.da.ndl.go.jp/info:ndljp/pid/12213293/www.nisc.go.jp/press/pdf/cymat_press.pdf (2023 年 3 月 28 日閲覧))

[65] JCIC「日本のサイバーセキュリティ政策史 第 2 回」(https://www.j-cic.com/pdf/report/Building-a-Crisis-Management-System-in-Turbulent-Times.pdf (2023 年 3 月 28 日閲覧))

[66] 第 189 回国会衆議院内閣委員会第 13 号(平成 27 年 6 月 10 日)近藤洋介委員の質問に対する菅義偉内閣官房長官答弁参照。なお、その後も、JPS 事件を踏まえ、また、TOKYO2020 対応などのために NISC の体制は強化・充実されている。

[67] 三角育生、「大規模 IT セキュリティインデント対処の政策的影響」、日本セキュリティ・マネジメント学会誌　2020 年、Vol.34、No.2、p22-28。

[68] 三角育生、「サイバーセキュリティ基本法制定・改正の経緯」、日本セキュリティ・マネジメント学会誌

2020 年、Vol.34、No.1、p28-34。

[69] NISC「サイバーセキュリティ人材育成総合強化方針」（https://www.nisc.go.jp/pdf/policy/kihon-1/jinzai_kyoka_hoshin.pdf）

[70] NISC「サイバーセキュリティ政策に係る年次報告(2014 年度)」（https://www.nisc.go.jp/pdf/council/cs/dai03/jseval_2014.pdf (2023 年 3 月 31 日閲覧)）p23 参照。

[71] NISC「東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ対策の結果等を踏まえた今後の取組方針」（https://www.nisc.go.jp/pdf/council/cs/dai32/32shiryou04.pdf (2023 年 3 月 31 日閲覧)）

[72] NISC「2020 年東京オリンピック・パラリンピック競技大会に向けた取組」（https://www.nisc.go.jp/pdf/council/cs/dai08/08shiryou06.pdf (2023 年 3 月 31 日閲覧)）

[73] NISC「G7 伊勢志摩サミットにおける取組等」（https://www.nisc.go.jp/pdf/council/cs/dai08/08shiryou05.pdf (2023 年 3 月 31 日閲覧)）

[74] NISC「2020 年東京大会に向けた取組状況について」（https://www.nisc.go.jp/pdf/council/cs/dai22/22shiryou07.pdf (2023 年 3 月 31 日閲覧)）

[75] NISC「東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ対策の結果等を踏まえた今後の取組方針」（https://www.nisc.go.jp/pdf/council/cs/dai32/32shiryou04.pdf (2023 年 3 月 31 日閲覧)）

[76] NISC「東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ対策の結果等を踏まえた今後の取組方針」（https://www.nisc.go.jp/pdf/council/cs/dai32/32shiryou04.pdf (2023 年 3 月 31 日閲覧)）

[77] NISC「第 1 次情報セキュリティ基本計画(セキュア・ジャパンの実現に向けて)」（https://www.nisc.go.jp/pdf/policy/kihon-s/bpc01_ts.pdf (2023 年 3 月 28 日閲覧)）

[78] NISC「第 2 次提言(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)」（https://www.nisc.go.jp/pdf/policy/kihon-s/teigen/2teigen_hontai.pdf (2023 年 3 月 28 日閲覧)））

[79] 関係機関がその体制を強化しつつ連携して我が国の安全保障を確保することが重要としている。

[80] 2005 年に「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 分野を対象として決定した。2014 年に「化学」、「クレジット」及び「石油」を追加、さらに、2018 年に「空港」が追加された。

[81] Capability for Engineering of Protection, Technical Operation, Analysis and Response

[82] JCIC「日本のサイバーセキュリティ政策史 第 3 回」（https://www.j-cic.com/pdf/report/Participating-the-Start-up-of-NISC.pdf (2023 年 3 月 27 日閲覧)）

[83] NISC「我が国の情報セキュリティ分野における国際協調・貢献に向けた取組み」（https://www.nisc.go.jp/pdf/policy/kokusai/international_approach.pdf (2023 年 3 月 28 日閲覧)）

[84] NISC「第 2 次情報セキュリティ基本計画(IT 時代の力強い「個」と「社会」の確立に向けて)」（https://www.nisc.go.jp/pdf/policy/kihon-s/bpc02_ts.pdf (2023 年 3 月 28 日閲覧)）

[85] JCIC「日本のサイバーセキュリティ政策史 第 4 回」（https://www.j-cic.com/pdf/report/The-History-of-Japan-Cybersecurity-Policy-4.pdf (2023 年 7 月 17 日閲覧)）

[86] NISC「2009 年度の情報セキュリティ政策の評価等」（https://www.nisc.go.jp/pdf/policy/kihon-s/sjeval_2009.pdf (2023 年 3 月 28 日閲覧)）

[87] NISC「サイバーセキュリティ 2022(2021 年度年次報告・2022 年度年次計画)」（https://www.nisc.go.jp/pdf/policy/kihon-s/cs2022.pdf (2023 年 3 月 28 日閲覧)）

[88] NISC「国民を守る情報セキュリティ戦略」(https://www.nisc.go.jp/pdf/policy/kihon-s/senryaku.pdf (2023 年 3 月 28 日閲覧))
[89] JCIC「日本のサイバーセキュリティ政策史 第 2 回」(https://www.j-cic.com/pdf/report/Building-a-Crisis-Management-System-in-Turbulent-Times.pdf (2023 年 3 月 28 日閲覧))
[90] NISC「サイバーセキュリティ戦略(世界を率先する強靭で活力あるサイバー空間を目指して)」(https://www.nisc.go.jp/pdf/policy/kihon-s/cyber-security-senryaku-set.pdf (2023 年 3 月 28 日閲覧))
[91] 情報セキュリティではなくサイバーセキュリティとすることは、CS 基本法の定義を参照すると、従来よりも対象とする範囲が狭まるようにも思われ、この点は、議論があるところである。しかし、この時期、自由主義圏の各国ではサイバーセキュリティに係る戦略が策定されるようになったことが影響したといえる。(例：EU の National Cyber Security Strategies、英国の The UK Cyber Security Strategy 2011-2016、米国の The Comprehensive National Cybersecurity Initiative)
[92] NISC「サイバーセキュリティ国際連携取組方針(j-initiative for Cybersecurity)」(https://www.nisc.go.jp/pdf/policy/kihon-s/InternationalStrategyonCybersecurityCooperation_j.pdf (2023 年 3 月 28 日閲覧))
[93] NISC「サイバーセキュリティ戦略(2015/9/4 閣議決定)」(https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku.pdf (2023 年 3 月 28 日閲覧))
[94] 三角育生、「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 2021 年、Vol.34、No.3、p39-46。
[95] CS 基本法 1 条に示された目的の順。なお、安全保障に係る活動を実践するにはサイバー空間の情勢を把握することなどが必要で、その観点から、我が国の ICT 産業が国際的に競争力をもち、国内にデータを獲得する機会が高まるように経済社会の発展を促進することは安全保障の観点からも重視されたともいえる。
[96] 三角育生、「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 2021 年、Vol.34、No.3、p39-46。
[97] US Department of Defense「Mission Assurance Strategy, Apr 2012」(https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf (2023 年 3 月 28 日閲覧))
[98] 三角育生、「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 2021 年、Vol.34、No.3、p39-46。
[99] 内閣官房「国家安全保障戦略 (2013/12/17 閣議決定)」(https://www.cas.go.jp/jp/siryou/131217anzenhoshou/pamphlet_jp_en.pdf (2023 年 3 月 28 日閲覧))
[100] NISC「新・情報セキュリティ人材育成プログラム」(https://www.nisc.go.jp/pdf/policy/kihon-1/jinzai2014.pdf(2023 年 3 月 28 日閲覧))
[101] 三角育生、「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　2021 年、Vol.34、No.3、p39-46。
[102] 2016 年 10 月から翌年 2 月にかけて、未来投資会議の下の第 4 次産業革命・イノベーション会合にて、(欧州におけるインシデント報告義務化などを背景に)「重要インフラに係る制度整備が必要」といった問題意識が示される中で検討が進められたものである。
[103] NISC「2020 年及びその後を見据えたサイバーセキュリティの在り方について」(https://www.nisc.go.jp/pdf/policy/kihon-s/csway2017.pdf (2023 年 3 月 28 日閲覧))
[104] 三角育生、「サイバーセキュリティ基本法制定・改正の経緯」、日本セキュリティ・マネジメント学会

誌　2020 年、Vol.34、No.1、p28-34。

[105] NISC「サイバーセキュリティ戦略(2018/7/27 閣議決定)」(https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2018.pdf (2023 年 3 月 28 日閲覧))

[106] 2018 年の CS 基本法改正案はすでに閣議決定(2018 年 3 月)されていることも、協働が基本的在り方に位置づけられている背景にあるといえる。

[107] 例えば、外務省「中国を拠点とする APT10 といわれるグループによるサイバー攻撃について(2018 年 12 月 21 日外務報道官談話)」(https://www.mofa.go.jp/mofaj/press/danwa/page4_004594.html (2023 年 3 月 28 日閲覧))

[108] 三角育生、「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　2021 年、Vol.34、No.3、p39-46。

[109] NISC「サイバーセキュリティ戦略(2021/9/28 閣議決定)」(https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf (2023 年 3 月 28 日閲覧))

[110] 2021 年 4 月に警視庁が中国共産党員の男を被疑者として東京地方検察庁に書類送致した事件

[111] JCIC「日本のサイバーセキュリティ政策史 第 1 回」(https://www.j-cic.com/pdf/report/The-History-of-Japan-Cybersecurity-Policy.pdf (2023 年 3 月 28 日閲覧))

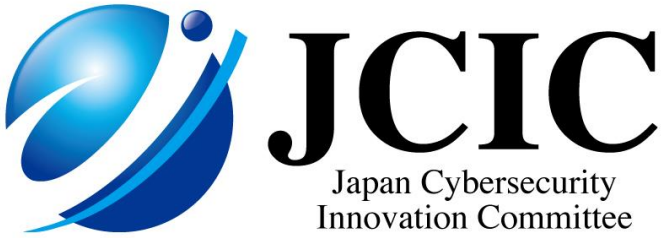
[112] 一般社団法人日本経済団体連合会「全員参加によるサイバーセキュリティの実現に向けて」(https://www.keidanren.or.jp/policy/2021/062_gaiyo.pdf (2023 年 5 月 6 日閲覧))

[113] JCIC「日本のサイバーセキュリティ政策史 第 1 回」(https://www.j-cic.com/pdf/report/The-History-of-Japan-Cybersecurity-Policy.pdf (2023 年 3 月 28 日閲覧))

[114] JCIC「日本のサイバーセキュリティ政策史 第 1 回」(https://www.j-cic.com/pdf/report/The-History-of-Japan-Cybersecurity-Policy.pdf (2023 年 3 月 28 日閲覧))

[115] NISC「サイバーセキュリティ戦略(2021/9/28 閣議決定)」(https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf (2023 年 3 月 28 日閲覧))

[116] CS 戦略本部「サイバーセキュリティ人材育成総合強化方針」(https://www.nisc.go.jp/pdf/policy/kihon-1/jinzai_kyoka_hoshin.pdf (2023 年 4 月 24 日閲覧))



[本調査に関する照会先]

JCIC 事務局　info@j-cic.com