サイバー空間の防衛力強化プロジェクト　政策提言

“日本にサイバーセキュリティ庁の創設を!”

2018年10月

公益財団法人　笹川平和財団
安全保障事業グループ

政策提言要旨

サイバー攻撃は、今や人類最大の懸案事項になりつつある。テロリストによるサイバー攻撃は、大規模自然災害に匹敵する被害を社会にもたらし、国家によるサイバー攻撃は、諜報活動、知財窃取、機能妨害、破壊行為、情報操作などにより私達の社会を脅かしている。サイバー攻撃の主体の多様化や攻撃手法の高度化により、今や狭義のサイバーセキュリティである「Security of Internet」＝インターネット（ネット空間）の安全確保のみならず、「Security of Cyberspace」＝サイバー空間（重要インフラなどのハードやネット空間とつながる人間といった社会層を含む）の安全確保、さらには「Security of Democratic Society」＝インターネット情報に左右される民主主義社会そのものの安全確保が世界的な課題となっている。サイバー攻撃は日々刻々と進化を続けており、その対応のためには、サイバー攻撃の検知、分析、判断、対処までを一元的かつ迅速に実施する必要がある。

このため、欧米先進国においては、政府がサイバーセキュリティに主導的な役割を果たすとともに、①サイバー攻撃に一元的に対応する体制整備、②サイバー脅威情報の収集及び重要インフラ事業者のサイバーインシデントの報告に関する法整備、③政府によるサイバーセキュリティ人材と産業の育成、が着々と進められている。これは、国家を背景としたサイバー攻撃の激化や国家レベルで開発されたサイバー攻撃ツールの拡散といった、日々増大するサイバー脅威への対応は民間の努力だけでは限界との認識が欧米各国で共有されていることによる。しかしながら、日本においては、サイバーセキュリティは基本的に民間企業の責任であるとされ、各省庁は所管の範囲内で最大限の努力をしているものの、縦割りによる対応には限界があり、人材育成・産業育成も不十分である。これでは重要インフラへのサイバー攻撃に的確に対応することも、政府の機密情報を守ることも、国民の生命と財産を守ることも困難である。

サイバー空間では、情報が自由にやりとりされ、国境に関係なくサイバー攻撃は行われるため、日本のサイバーセキュリティの強化は世界のサイバーセキュリティの強化に直結する。東京オリンピック・パラリンピックでのサイバーセキュリティのノウハウの蓄積は、世界各国のサイバーセキュリティ強化の礎となる。平和国家日本として、サイバーセキュリティの分野における国際貢献を進めるためにも、サイバーセキュリティ政策の抜本的強化が必要である。東京オリンピック・パラリンピックを２年後に控え、すべてのものがインターネットにつながるIoT社会、人工知能が社会に大きな影響を与えうるAI社会に備えるためにも、サイバーセキュリティの強化は国民の生命と財産を守る国家としての最優先事項である。政府は、サイバーセキュリティにおける政府の主導的役割を宣言するとともに、①サイバー攻撃に一元的に対応する「サイバーセキュリティ庁」を創設し、②サイバー攻撃に対処するための情報収集に必要な法整備を行うとともに、③サイバーセキュリティに欠かせない人材と産業の育成を進める必要がある。

【政策提言のポイント】

1.サイバーセキュリティ庁の設置
　サイバー攻撃に一元的に対応する実務機関として、現行の内閣サイバーセキュリティセンターを発展的に改編・強化して内閣府外局にサイバーセキュリティ庁を設置し、サイバー攻撃の検知、分析、判断、対処までを一元的かつ迅速に行うとともに諸外国のサイバーセキュリティ機関との連携を行う。

2.サイバー攻撃に対応するための法整備
　サイバーセキュリティ基本法を改正して「サイバーセキュリティ」の定義をより広義のものに見直すとともに、政府の主導的役割を明らかにし、併せてサイバー攻撃に対応するための関連法の一括改正を行う。また、政府によるプライバシー侵害を監視するための委員会を国会に設置する。

3.人材育成・産業育成のためのエコシステムの整備
　サイバーセキュリティ人材とサイバーセキュリティ産業を育成するため、サイバーセキュリティ特区を新設して技術開発と産業育成を行うとともに、初等教育から専門教育、社会人教育までの一元化されたサイバーセキュリティ教育体制を整備する。

欧米各国と日本のサイバーセキュリティ政策の比較表

	各国のサイバーセキュリティ政策	英	米	独	仏	日
体制整備	1．国家戦略に政府の主導的な役割が明記されているか	○	○	○	△	△
	2．様々なサイバー攻撃への対応が一元化されているか	○	○	○	○	×
	3．機動的なサイバー攻撃対応体制が整備されているか	○	△	○	○	×
法整備	4．政府によるサイバー脅威情報の収集を認める法律があるか	○	○	○	○	×
	5．重要インフラ事業者にサイバーインシデント報告義務があるか	○	△	○	○	△
	6．重要インフラ事業者にサイバーインシデント連絡担当者の必置規制があるか	○	△	○	○	×
	7．政府によるプライバシー侵害を監視する機関があるか	○	○	○	○	×
人材育成 産業育成	8．サイバーセキュリティ機関が実施する産業育成プログラムがあるか	○	○	△	△	△
	9．サイバーセキュリティ機関が実施する人材育成プログラムがあるか	○	○	△	○	△

目次

第１章　サイバー攻撃の現状

１．サイバー攻撃の現状

サイバー攻撃は、今や人類最大の懸案事項となりつつある。

世界経済フォーラム（World Economic Forum）が毎年１月に発表する世界のリスクに関する報告書“Global Risks Report 2018”[1]では、サイバー攻撃は自然災害に次ぎ最も危険なリスクとされている。また、マカフィー社と米国のシンクタンク戦略国際問題研究所（CSIS）によれば、2017年のサイバー攻撃の被害額は世界全体で最大6,000億ドル（約66兆円）に達するとされている[2]。これは、東日本大震災（被害額約17兆円）４回分の被害額に相当する。

電力や金融機関などの重要インフラへの脅威も高まっている。2015年12月には、ウクライナの電力システムへのサイバー攻撃により約22万人（東京都の渋谷区の人口に相当）に影響する大規模停電が発生した。2017年５月には、身代金型ウィルス WannaCry が世界150カ国に広がり、英国では国民保健サービス（NHS）のコンピュータが多数停止して医療サービスが行えなくなる病院も現れた。また、仮想通貨へのサイバー攻撃が国家やテロ組織により行われており、それらの重要な資金源となっているとの報道もある。

知的財産や国家機密に対するサイバー攻撃もある。2011年には防衛装備品等を製造する三菱重工業でサイバー攻撃による情報流出があったほか、本年４月には防衛省OBに対するサイバー攻撃が行われている。サイバー空間は陸海空宇宙に次ぐ「第５の戦場」と言われるように、軍事面での重要性も年々高まっており、米国、中国、北朝鮮等ではサイバー攻撃を専門とする部隊（サイバー軍）が相次いで創設されるなど、防衛面におけるサイバー攻撃への対応も必要とされている。

サイバー攻撃の被害は、経済的損失にとどまらない。米国の2016年の大統領選挙では、立候補者に対する「情報操作型サイバー攻撃」が行われた。偽ニュースの流布や、サイバー攻撃により窃取された機密情報が意図的に公開されるなど、サイバー攻撃は大統領選挙の最終結果に大きな影響を及ぼしたとされる。これに対して、米財務省は今年の３月15日にロシアの24団体・個人への制裁措置を発表している。

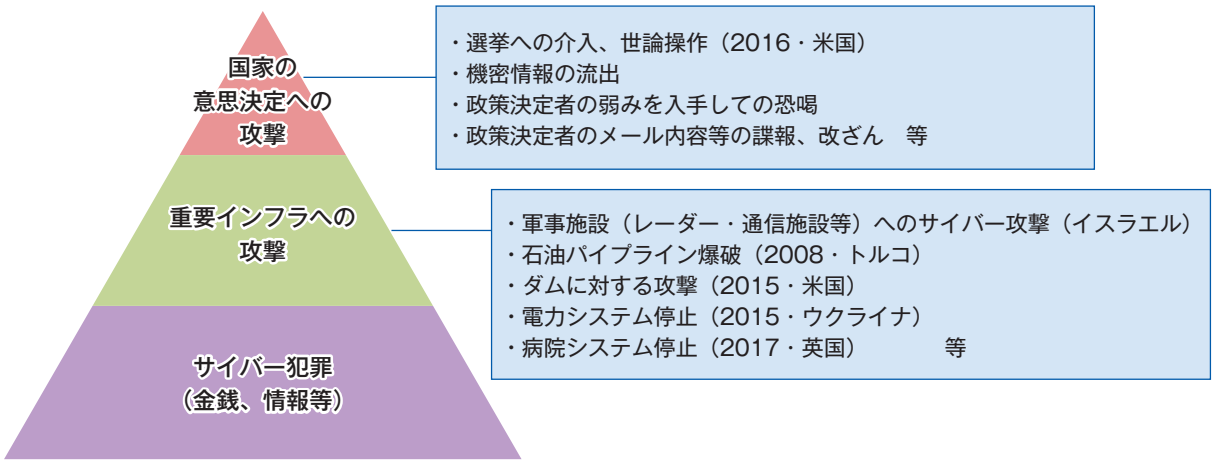
また、あらゆるものがネットに繋がるSociety5.0社会を目前にして、サプライチェーンリスクも深刻化しつつある。Society5.0社会に向けて、FinTechや取引を管理するEDI（Electronic Data Interchange：電子データ交換）システムなどが導入され始めているが、セキュリティデザインが必ずしも最初から考えられていないネットサービスも入り込みつつある。重要インフラである電気・ガスなどのエネルギー産業においても、自由化・競争が激化し、合理化のために標準的なICS（産業用制御システム）やEDIシステムが導入されつつある。米国では、2017年10月に国土安全保障省（DHS）と連邦捜査局（FBI）が、「ATP（高度で持続的な脅威）攻撃グループによる重要インフラを狙った攻撃」に対する警告を発していたが、天然ガスパイプライン事業者が利用するEDIに対するサイバー攻撃が明らかになっている。

サイバー攻撃は、諜報活動、知財窃取、機能妨害、破壊行為、情報操作を目的として、国家の

1　World Economic Forum, “The Global Risk Report 2018”, January 2018.
2　CSIS, “Economic Impact of Cybercrime-No Slowing Down”, February 2018.

戦略目的を達成し、意思を表示するツールとしても利用され始めている。サイバー攻撃の対象や手法は日々高度化・大規模化しており、幅広い分野についての一元的な情報収集と迅速な対処が求められている。

図1-1-1 さまざまなサイバー攻撃の脅威



※笹川平和財団作成

表1-1-2 国家が関与したとみられる主なサイバー攻撃事案

2007.4	エストニア政府、報道、金融機関を狙った機能妨害型サイバー攻撃
2008.8	グルジア紛争と関連して政府、金融機関を狙った機能妨害型のサイバー攻撃
2009.7	韓国政府、米国政府を標的とした機能妨害型サイバー攻撃
2010.8	イランの核施設の制御システムを狙ったStuxnetウィルス攻撃
2011.9	三菱重工等の防衛関連産業への標的型攻撃
2013.3	韓国、メディア、金融機関への機能妨害型攻撃
2014.3	ウクライナ通信事業者、政府への機能妨害型攻撃
2015.4	仏TV５（国際放送）がサイバー攻撃により放送停止
2015.5	日本年金機構への標的型攻撃により125万件の個人情報が流出
2015.12	ウクライナ東部の電力網に機能破壊型のサイバー攻撃で22万世帯が停電
2016.2	バングラデシュ中銀からサイバー攻撃によるSWIFT不正送金（8100万ドル）被害
2016.11	米国民主党全国委（DNC）に対するロシアによる情報窃取型攻撃
2016.12	ウクライナ首都の変電所へのサイバー攻撃により10万世帯が停電
2017.5	Wannacryランサムウェアが全世界に拡大
2017.6	Petya亜種ランサムウェアが全世界に拡大
2018.3	米国DHSとFBIが重要インフラのICSに対する攻撃を警告

※公開情報等を基に笹川平和財団作成

２. サイバーセキュリティとは何か

サイバー攻撃の多様化・高度化に伴い、サイバーセキュリティの定義は、インターネットやデジタルデータに限定された従来の定義から、社会層も含むより広義の定義へと変化している。

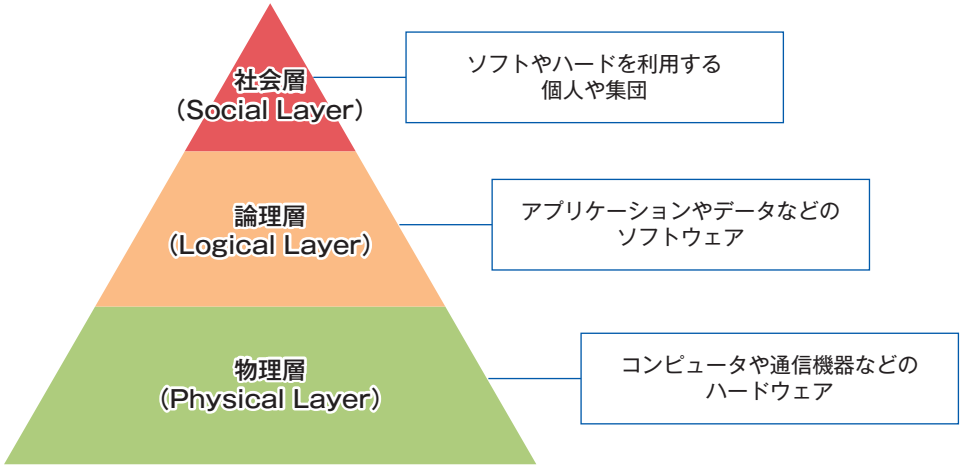
サイバー攻撃は情報窃取のようなインターネット空間での行為にとどまらず、重要インフラの

破壊のような現実社会に対する物理的な攻撃や、2016年の米国の大統領選挙のように民主主義システムに対する攻撃も含まれるようになってきている。このため、現在では、サイバーセキュリティの対象はソフトウェアだけでなく、ハードウェアやネットワークとつながる社会システムを含むものだと考えられている。元来、「サイバー」という言葉の語源となったノーバート・ウィーナーの「サイバネティクス」という考え方は、制御システムだけでなく人間社会を含むものであった。

NATO（北大西洋条約機構）のサイバー専門家が作成した国際的なサイバーセキュリティに関するガイドライン「タリン・マニュアル」の最新版（Tallinn Manual 2.0：2017年公表）では、サイバー空間はコンピュータやサーバー、通信機器などのハードウェア（物理層）、アプリケーションやソフトウェア（論理層）、ソフトやハードを利用する個人や集団（社会層）の三層からなると記述されている（図1-2-1）。

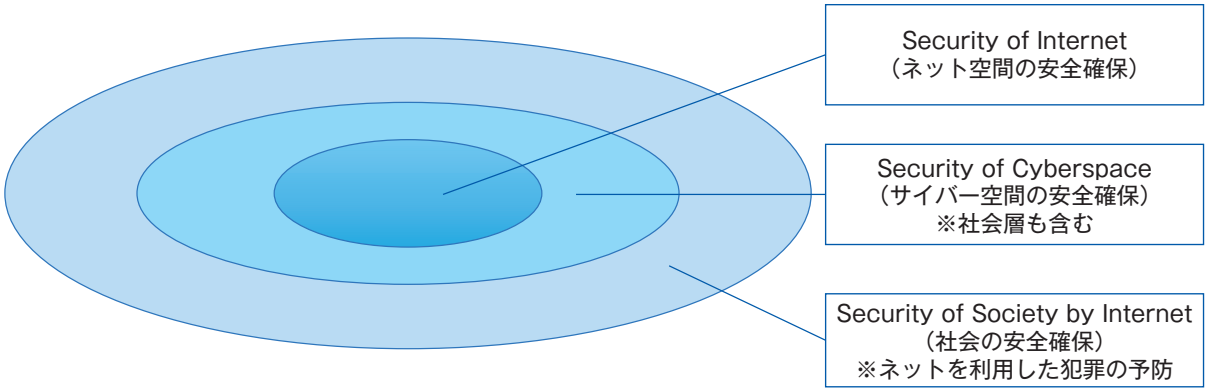
このようにサイバーセキュリティの定義の拡大により、サイバーセキュリティで守るべき領域は、従来のサイバーセキュリティ領域であった「Security of Internet（インターネットの安全確保）」だけでは不十分であり、社会層も含む「Security of Cyberspace（サイバー空間の安全確保）」やその外縁部に相当する社会全体に及んでいる（図1-2-2）。

図1-2-1 Tallinn Manual 2.0（2017）によるサイバーセキュリティの対象



※Tallin Manual 2.0 を基に笹川平和財団作成

図1-2-2 安全確保領域の拡大



※笹川平和財団作成

しかしながら、日本のサイバーセキュリティの定義は、「情報の漏えい、滅失または毀損の防止」「情報システム及び情報通信ネットワークの安全性及び信頼性の確保」とされている（サイバーセキュリティ基本法第２条）。これは「狭義のサイバーセキュリティ」の定義であり、社会層を含むサイバー空間が想定されていない。今後も多様化・高度化するサイバー攻撃に的確に対応するためには、サイバーセキュリティ基本法第2条を改正し、サイバーセキュリティの定義に社会層を含めるとともに、さらにはネットを利用した犯罪予防にまで拡張する必要がある。

また、国民生活全体に影響を及ぼすサイバー攻撃も諸外国においては発生し始めているが、我が国では「国は、サイバーセキュリティに関する事象のうち我が国の安全に重大な影響を及ぼすおそれがあるものへの対応について、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」（サイバーセキュリティ基本法第18条）となっており、このような「大規模サイバー攻撃」に対応する責任主体が明確に定義されていない。「サイバー」の本来の意味合いからすれば、社会全体を守るためには、「大規模サイバー攻撃」に際しては、国（政府）が主導的に対応する必要がある。

表1-2-3 サイバーセキュリティ基本法第２条（サイバーセキュリティの定義）

（現行法の定義）	（本来あるべき定義）
（定義） 第2条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。	（定義） 第2条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されることにより、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が確保されていることをいう。

３. サイバー攻撃への対応のあり方

サイバーセキュリティ対策として、いわゆるPDCAサイクルの実施が求められるようになって久しいが、実際のサイバー攻撃では、非常に短期間に事象が推移する。このため、時間を要するPDCAサイクルではなく、サイバー攻撃の検知・分析・判断・対処を機動的に行うモデルとして、短時間の意思決定のために考案されたOODAループが注目されている。アメリカ空軍のジョン・ボイド大佐（1927-1997）は、朝鮮戦争の航空戦についての洞察を基盤にして、観察（Observe）- 情勢への適応（Orient）- 意思決定（Decide）- 対処（Act）のサイクルを素早く繰り返すことによって健全な意思決定が実現されるというモデルを提唱した。このモデルは、観察、情勢への適応、意思決定、対処の４つの活動の頭文字をとって「OODA（ウーダ）ループ」と呼ばれる（図1-3-1）。

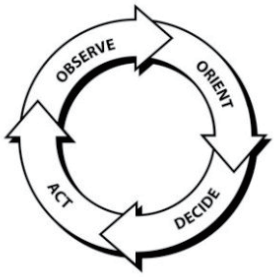
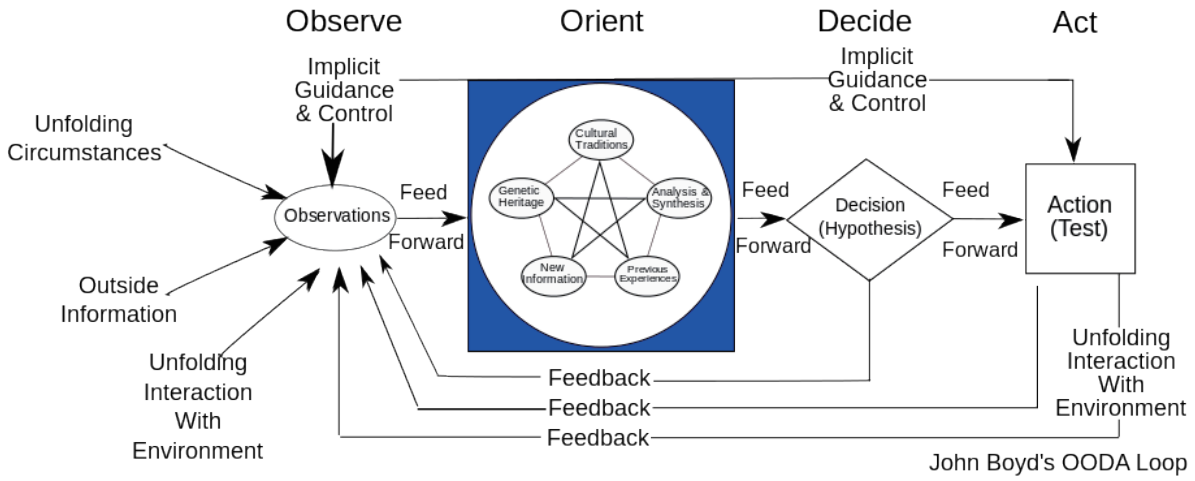


図1-3-1 OODA Loop

OODA ループは、より正確には以下の図1-3-2のとおりとなる。すなわち、観察から得た知見を基に情勢への適応（分析等）を行い、（仮説に基づき）対策を決定し、（試行的に）対処する。ここで重要なのは、現実の意思決定は不十分な情報に基づき行われることから、常に仮説と検証を繰り返し、対処の結果に応じて意思決定の修正を行う必要があることである。

OODAループは、コンパスやGPSのない時代の嵐の夜に、雲の隙間からときおり顔を出す星々を頼りに、舵を操作して目的地に向かう航海術に似ている。風や海流で船の方向が曲げられる夜間の外洋航海では、今見えている星がどの星かの仮説を立て、常に進路を確認していく必要がある。サイバー攻撃への対応についてもこれと同様に、①日々発生している日本や世界でのサイバー攻撃の検知（サイバー空間のモニタリング）、②日本に対するサイバー攻撃の影響や深刻度等の分析、③政府による対策の判断、④各主体による対処となり、日々進化する未知のサイバー攻撃に迅速に対応するには、刻々と移り変わる情勢を捉え、OODAループを迅速に回す対応が求められる。

図1-3-2 OODA Loop（詳細）



※ボイドの資料より

第２章　各国のサイバーセキュリティ政策

１. 各国のサイバーセキュリティ政策の概要

日々高度化・大規模化するサイバー攻撃に対応するため、世界各国はOODAループのモデルにほぼ近い形で検知・分析・判断・対処に係るサイバー攻撃への対応体制を構築し、政府主導による産業育成・人材育成を行っている。より具体的には、主に

１）サイバーセキュリティ機関へのサイバー攻撃対応の一元化

２）法律に基づくサイバー脅威情報の収集及び重要インフラ事業者のサイバーインシデントの報告義務化

３）サイバーセキュリティ機関が直接実施する産業育成・人材育成制度の整備

を進めている。

こうした各国のサイバーセキュリティの政策をモデル化すると、以下のようになる（図2-1-1）。以下の節では、欧米主要国のサイバーセキュリティ政策と日本のサイバーセキュリティ政策につき、その考察と比較を行う。（以下、各国のサイバーセキュリティ実務機関及びその傘下に存在する実働組織を２回目以降に表記する際は略称を用いる。）

図2-1-1 各国のサイバー攻撃対応体制・政策モデル

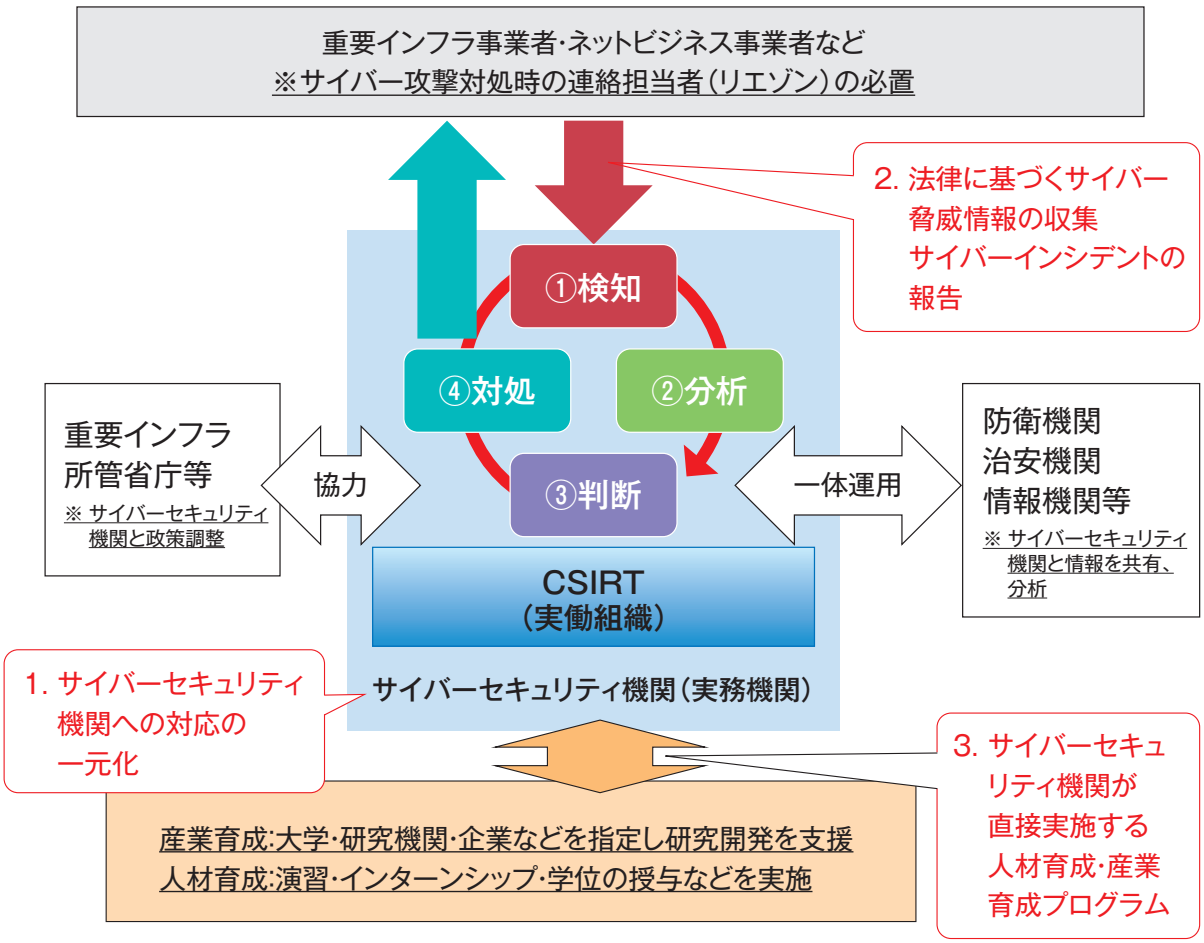


表2-1-2 欧米各国と日本のサイバーセキュリティ政策の比較

	各国のサイバーセキュリティ政策	英	米	独	仏	日
体制整備	1．国家戦略に政府の主導的な役割が明記されているか	○	○	○	△	△
	2．様々なサイバー攻撃への対応が一元化されているか	○	○	○	○	×
	3．機動的なサイバー攻撃対応体制が整備されているか	○	△	○	○	×
法整備	4．政府によるサイバー脅威情報の収集を認める法律があるか	○	○	○	○	×
	5．重要インフラ事業者にサイバーインシデント報告義務があるか	○	△	○	○	△
	6．重要インフラ事業者にサイバーインシデント連絡担当者の必置規制があるか	○	△	○	○	×
	7．政府によるプライバシー侵害を監視する機関があるか	○	○	○	○	×
産業育成 人材育成	8．サイバーセキュリティ機関が実施する産業育成プログラムがあるか	○	○	△	△	△
	9．サイバーセキュリティ機関が実施する人材育成プログラムがあるか	○	○	△	○	△

2. 英国のサイバーセキュリティ政策

（1）体制整備

英国政府は、2016年に「国家サイバーセキュリティ戦略2016-2021」（National Cyber Security Strategy 2016-2021）を公表し、英国のサイバーセキュリティに関し政府が主導的な役割を果たす（the Government will meet its responsibilities and lead the national response）ことを宣言した[3]。

この任務を担う英国のサイバーセキュリティ機関は、政府通信本部（GCHQ：Government Communications Headquarters）である。GCHQの前身は、コンピュータの父と呼ばれるアラン・チューリングが在籍した政府暗号学校（GCCS：ドイツの暗号エニグマを解読したことで有名）であり、1994年情報機関法（Intelligence Services Act）の2016年改正によってGCHQは国全体のサイバーセキュリティを一元的に担う行政機関として位置付けられている。GCHQには、下部組織としてサイバーセキュリティの実働組織であるNCSC（National Cyber Security Center）が2016年に設立されており、英国へのサイバー攻撃に半自動的に対応するActive Cyber Defense（ACD）プログラム等を展開している。

（2）法整備

政府によるサイバー脅威情報の収集については、2016年調査権限法（The Investigatory Powers Act 2016）により、GCHQに対し通信内容の監視を含む強力な情報収集の権限が与えられている。また、同法により収集されたサイバー脅威情報は、他情報機関であるSS（旧名称は

3　同戦略の前身である「The UK Cyber Security Strategy」（2011）では、民間企業や個人、政府など全ての人々が協同することとされており、政府の主導的役割は示されていない。（3.7“Achieving this vision will require everybody, the private sector, individuals and government to work together.”）

MI6)、SIS（旧名称はMI5）等の持つ情報と照合され、サイバー攻撃対処及び民間のサイバー攻撃対処の支援に用いられる。さらに、英国政府は、重要インフラ事業者に対し、2018年ネットワーク情報システム法（The Network and Information Systems Regulations 2018）に基づくサイバーインシデント報告や連絡担当者の配置を義務付けている。

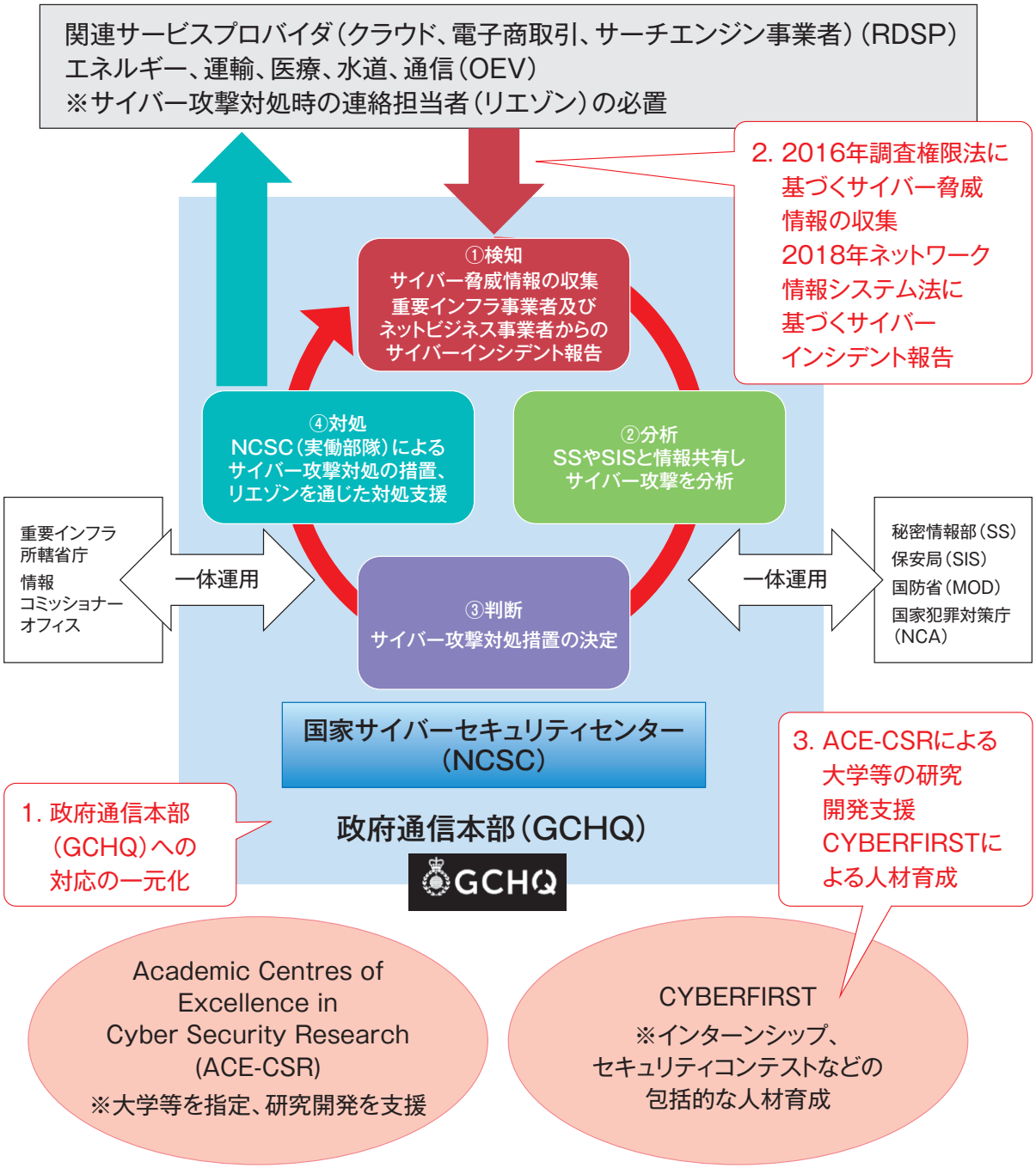
（3）産業育成・人材育成

サイバーセキュリティに係る産業育成や人材育成に関してもGCHQが一元的に実施しており、工学・物理科学研究会議（EPSRC）と共同で実施する大学や大学院の研究支援プログラムであるACE-CSRや、インターンシップやハッキングコンテスト等の総合的な教育・訓練を実施するCYBERFIRSTプログラム等が存在する。

表 2-2-1 英国のサイバーセキュリティ政策

英国のサイバーセキュリティ政策		
体制整備	1．国家戦略に政府の主導的な役割が明記されているか 「国家サイバーセキュリティ戦略2016-2021」（2016）において、政府が国家のサイバーセキュリティに関し主導的な役割を果たすことを明記	○
	2．様々なサイバー攻撃への対応が一元化されているか 同戦略によりサイバーセキュリティ関連機能をGCHQ内のNCSCに集中	○
	3．機動的なサイバー攻撃対応体制が整備されているか 検知・分析・判断・対処に係る体制整備を完了	○
法整備	4．政府によるサイバー脅威情報の収集を認める法律があるか 2016年調査権限法で法制化済み	○
	5．重要インフラ事業者にサイバーインシデント報告義務があるか 2018年ネットワーク情報システム法で義務化済み	○
	6．重要インフラ事業者にサイバーインシデント連絡担当者の必置規制があるか 2018年ネットワーク情報システム法で連絡担当者の配置を義務化	○
	7．政府によるプライバシー侵害を監視する機関があるか 議会に情報安全保障委員会（ISC）が設置済み	○
産業育成 人材育成	8．サイバーセキュリティ機関が実施する産業育成プログラムがあるか GCHQと工学・物理科学研究会議（EPSRC）が14の大学をAcademic Centres of Excellence in Cyber Security Research（ACE-CSR）に指定、研究開発を支援	○
	9．サイバーセキュリティ機関が実施する人材育成プログラムがあるか GCHQが、大学の講義を指定し学位を授与する等の包括的な教育プログラムであるCYBERFIRSTを実施	○

図2-2-2 英国のサイバー攻撃対応体制・政策モデル



（参考）
・GCHQの人員：5806人（2016年）
・GCHQの予算：29億ポンド（2015年、単年度、SIS・SSと共通）
・政府全体のサイバーセキュリティ予算：19億ポンド（2016～2021年）

３. 米国のサイバーセキュリティ政策

（１）体制整備

米国は、クリントン政権時代からサイバーセキュリティを国家安全保障上の重要な分野と位置づけており、オバマ政権時代にも2015年にサイバーセキュリティ法（Cybersecurity Act of 2015）を成立させ、2016年にサイバーセキュリティ国家行動計画（President's Cybersecurity National Action Plan : CNAP）を策定するなど、サイバーセキュリティ強化のための一連の政策を導入してきた。トランプ政権では2018年9月に米国国家サイバー戦略を発表し、さらにその方針を推し進め、連邦政府が国全体のネットワーク・システム・機能・データを守ることを明記した[4]。

米国のサイバーセキュリティ機関は、2002年国土安全保障法（Homeland Security Act）に基づき設置された国土安全保障省（Department of Homeland Security：DHS）である[5]。さらに、2015年サイバーセキュリティ法では、DHSと諜報機関との長きにわたる主導権争いを経て、DHSの情報共有のハブである国家サイバーセキュリティ通信統合センター（National Cybersecurity & Communications Integration Center : NCCIC, 2009年設立）が、実働組織として連邦政府と民間企業とのサイバーセキュリティ情報のゲートウェイ（窓口）となることが明記された。米国は防衛部門のサイバーセキュリティの能力が高く、産業・人材育成政策に関しても優れているものの、平時にサイバー攻撃に対応する義務的な枠組みの整備は進んでいない[6]。なお、現在（2018年10月末）、上・下院にてDHS内のサイバーセキュリティ部門を独立組織化しCISA（サイバーセキュリティ・インフラセキュリティ庁）に改組する法案が通過している。

（２）法整備

政府によるサイバー脅威情報の収集については、1978年外国情報監視法（The Foreign Intelligence Surveillance Act of 1978 : FISA）で法制化されている。しかしながら、米国は2013年の大統領令第13636号で重要インフラのセキュリティ強化の方針を打ち出したものの、重要インフラ事業者によるセキュリティ事故報告及び連絡担当者の配置は義務化されていない。ただし、DHSでは、サイバーセキュリティ法の一部である2015年サイバーセキュリティ情報共有法（Cybersecurity Information Sharing Act of 2015：CISA）に基づき、サイバー脅威情報共有システム（Automated Indicator Sharing : AIS）というサイバー攻撃に係る情報共有が自動で行われるシステムを運用している。（重要インフラ事業者が加入する法律的義務はないが、AISに加入している法人には、同システムの規定による報告義務がある）AISで共有された情報は、国家情報長官の下のサイバー脅威情報統合センター（Cyber Threat Information Integration Center : CTIIC）で分析され、DHSを通して民間と共有される仕組みとなっている

4　NATIONAL CYBER STRATEGY of the United States of America, White House, September 2018

5　DHSは、22の省庁を再編統合して創設された、規模的にも国防総省（Department of Defense : DoD）に次ぐ巨大組織（定員は24万人以上）。DHSの創設は国防総省及び国家安全保障会議（National Security Council : NSC）の設置（1947年）以来、50年ぶりの大規模な組織改革とされる。

6　2016年のロシアによる大統領選介入では、国防総省傘下の国家安全保障局（NSA）がサイバー脅威情報を把握していたが、NSAには平時の活動権限が無いため2016年大統領選では選挙システムのハッキングや世論操作を含むサイバー攻撃に対応することができなかったとされる。

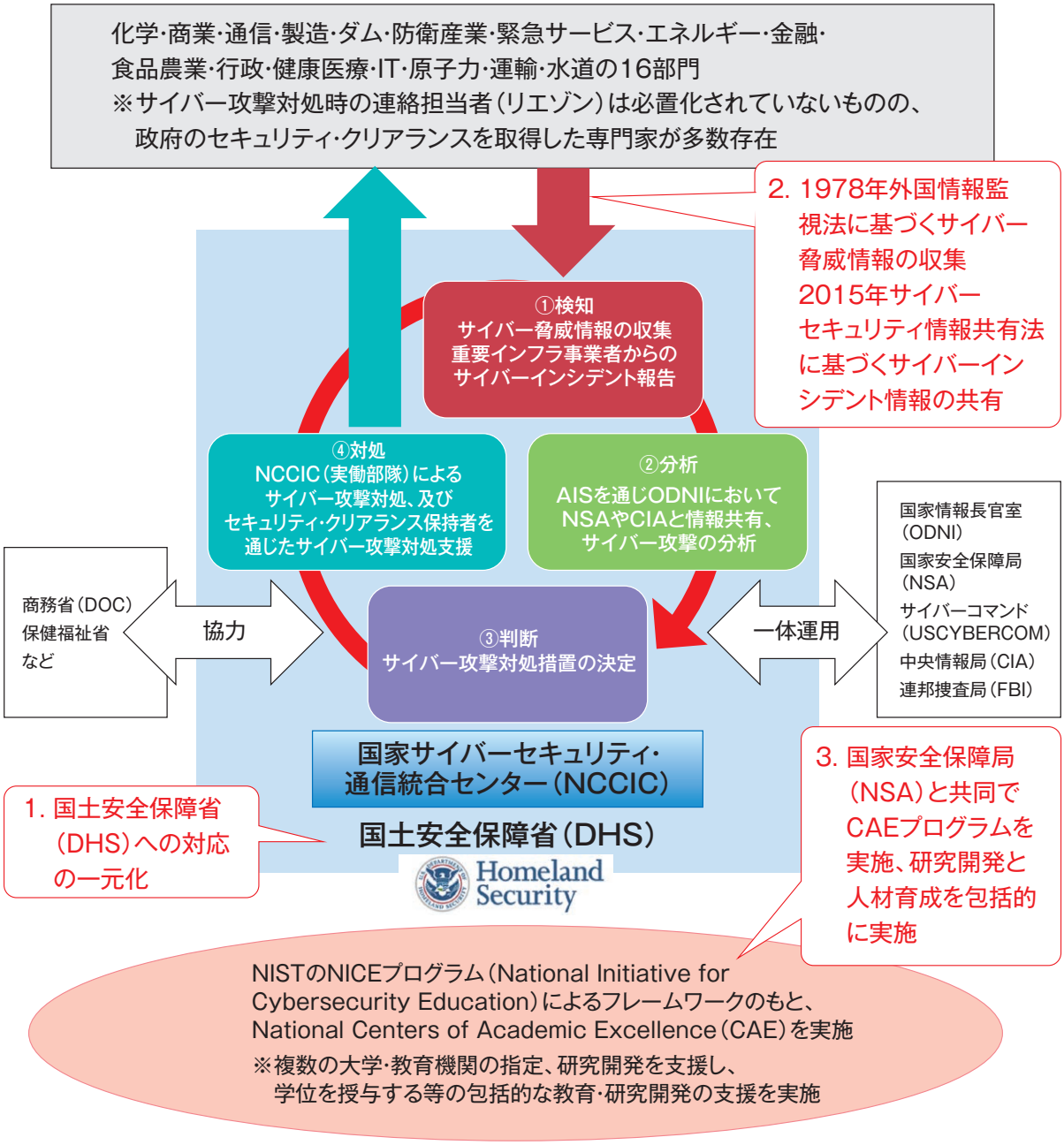
（3）産業育成・人材育成

産業育成、人材育成に関しては、NIST（国立標準技術研究所）の管轄する教育推進プログラムであるNICE（National Initiative for Cybersecurity Education）やDHSと国家安全保障局（NSA）が共同で多数の大学を指定し、研究開発、教育訓練を行うCAEプログラムを実施している。

表 2-3-1 米国のサイバーセキュリティ政策

米国のサイバーセキュリティ政策		
体制整備	1．国家戦略に政府の主導的な役割が明記されているか 「米国国家サイバー戦略」（2018）において、連邦政府が国全体のネットワーク・システム・機能・データを守ることを明記	○
	2．様々なサイバー攻撃への対応が一元化されているか 国土安全保障法（2002）で国土安全保障省（DHS）を設置 2018年10月末現在、DHS内部のサイバー部局（NPPD）をサイバーセキュリティ・インフラセキュリティ庁（CISA）に改組する法案が上・下院を通過済み	○
	3．機動的なサイバー攻撃対応体制が整備されているか 検知・分析・判断のプロセスに関しては体制整備を完了するも、サイバー攻撃対処時の重要インフラの連絡担当者の必置が行われていない。（ただし、セキュリティ・クリアランスを受けた民間人が多数存在し、連絡調整を行なっている場合が多数）	△
法整備	4．政府によるサイバー脅威情報の収集を認める法律があるか 1978年外国情報監視法で法制化	○
	5．重要インフラ事業者にサイバーインシデント報告義務があるか 2015年サイバーセキュリティ情報共有法（CISA）により、民間事業者が自主的にサイバーインシデントを報告した場合は、他の法律による罰則の適用を除外される（報告の義務は無し）	△
	6．重要インフラ事業者にサイバーインシデント連絡担当者の必置規制があるか 重要インフラ事業者への連絡担当者の配置は義務化されていないものの、政府のセキュリティ・クリアランスを受けた専門家が多数企業に在籍し、政府と連絡調整を行なっている。	△
	7．政府によるプライバシー侵害を監視する機関があるか 上院情報委員会（SSCI）、下院情報委員会（HPSCI）が政府の活動を監視	○
産業育成 人材育成	8．サイバーセキュリティ機関が実施する産業育成プログラムがあるか DHSと国家安全保障局（NSA）が共同で多数の大学をNational Centers of Academic Excellence（CAE）に指定し、研究開発を支援	○
	9．サイバーセキュリティ機関が実施する人材育成プログラムがあるか DHSと国家安全保障局（NSA）が共同で多数の大学をNational Centers of Academic Excellence（CAE）に指定し、学位を授与する等の包括的な教育支援を実施	○

図2-3-2 米国のサイバー攻撃対応体制・政策モデル



(参考)
・DHSのサイバー部門の人員:約700人(文民のみの数)(2018年)
・NSAの人員(一部の人員がNCCICへ出向):約30000人(2012年)
・DHSのサイバーセキュリティ予算:16億ドル(2017年)
・国防総省のサイバーセキュリティ予算:72億ドル(2017年)
・政府全体のサイバーセキュリティ予算:130億ドル(2017年)

４.ドイツのサイバーセキュリティ政策

（１）体制整備

ドイツは、サイバー空間におけるデータの安全性とその保証は、21世紀の最重要問題であるとの認識の下、サイバーセキュリティの確保のため2011年に「サイバーセキュリティ戦略」（Cyber Security Strategy for Germany）を公表した[7]。同戦略の中でドイツの経済・社会的繁栄を確保し促進するため、連邦政府がサイバー空間の安全に具体的な貢献を行うことを明確にし、政府が国全体のサイバーセキュリティに関する主導的役割を担うことを表明している。

ドイツのサイバーセキュリティ機関は内務省傘下の連邦情報セキュリティ庁（BSI）である。BSIは旧西ドイツにおいてソビエト連邦及び旧東ドイツへの情報活動を担当した連邦情報局（BND）から切り離された機関であり、国全体のサイバーセキュリティに対し一元的な役割を担い、重要インフラ事業者の監査・サイバーインシデント報告対応・サイバー攻撃対処及びサイバー攻撃対処支援を行っている。また、関係する情報機関や捜査機関との連携体制が整備されており、BSI内に設置された実働組織であるサイバーディフェンスセンター（NCAZ）を通じてBND、国防省、連邦警察（BPOL）、連邦憲法擁護庁（BfV）等とデータの共同利用を行なっている。ドイツはサイバーセキュリティ機関が他の行政機関と共同でサイバー攻撃に対応する体制整備を他国と比べ早期に進めている特徴がある。

（２）法整備

政府によるサイバー脅威情報の収集に関しては、郵便・通信・メールの秘密制限法（G-10法）及び連邦情報局法（BND法）により法制化され、主に連邦情報局（BND）が担当している。同法により収集されたサイバー脅威情報は連邦情報セキュリティ庁内に設置されたサイバーディフェンスセンター（NCAZ）において連邦情報セキュリティ庁と共有される。また、重要インフラ事業者のサイバーインシデント報告及び連絡担当者の設置についてはITセキュリティ法により義務化されている。（違反時の罰則有り）

（３）産業育成・人材育成

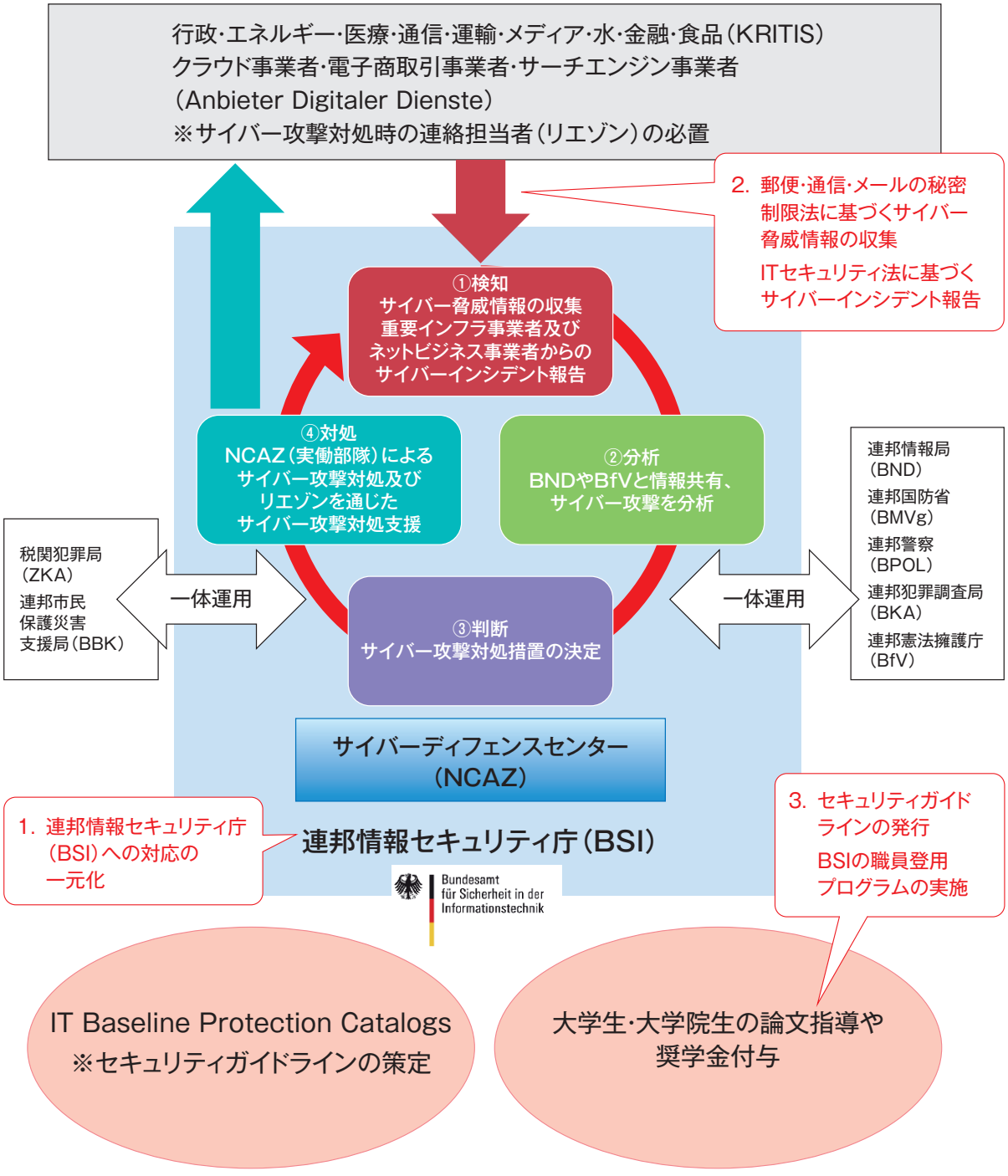
産業育成、人材育成については主に連邦教育・研究省（BMBF）が実施しており、BSIが直接実施するものは産業政策に関してはセキュリティ製品の基準を定めるITベースラインプロテクションカタログの作成、人材育成に関しては大学や大学院の学生に対し奨学金を給付しBSIの職員を確保、などとなっている。

7　Cyber Security Strategy for Germany, Federal Ministry of the Interior, February 2011

表 2-4-1 ドイツのサイバーセキュリティ政策

ドイツのサイバーセキュリティ政策		
体制整備	1．国家戦略に政府の主導的な役割が明記されているか 2011年国家サイバーセキュリティ戦略において連邦政府の国全体のサイバーセキュリティへの具体的な役割を明記	○
	2．様々なサイバー攻撃への対応が一元化されているか 2009年に連邦情報セキュリティ庁法（BSI act）により連邦情報局（BND）の一部門を分離、連邦情報セキュリティ庁（BSI）を設置	○
	3．機動的なサイバー攻撃対応体制が整備されているか 他国に先んじて早期に検知・分析・判断・対処に係る体制整備を実施。	○
法整備	4．政府によるサイバー脅威情報の収集を認める法律があるか 郵便・メール・通信の秘密制限法（G-10法）及び連邦情報局法（BND法）により法制化	○
	5．重要インフラ事業者にサイバーインシデント報告義務があるか 2015年にITセキュリティ法により義務化	○
	6．重要インフラ事業者にサイバーインシデント連絡担当者の必置規制があるか 2015年にITセキュリティ法により必置化	○
	7．政府によるプライバシー侵害を監視する機関があるか 議会監督委員団（PKGs）が政府の活動を監視	○
産業育成 人材育成	8．サイバーセキュリティ機関が実施する産業育成プログラムがあるか BSIはITシステムの標準化を行うIT Baseline Protection Catalogsを発行	△
	9．サイバーセキュリティ機関が実施する人材育成プログラムがあるか BSIは大学生・大学院生の論文指導・奨学金給付を行い職員の確保を実施	△

図 2-4-2 ドイツのサイバー攻撃対処体制・政策モデル



（参考）
- BSIの人員：約800人（2018年）
- BNDの人員（一部がNCAZに出向）：約6500人（2012年）
- BSIの予算：1.1億ユーロ（2017年）
- BNDの予算：8.3億ユーロ（2017年）
- 政府全体のサイバーセキュリティ予算：N/A

５. フランスのサイバーセキュリティ政策

（１）体制整備

フランス政府は2015年に国家デジタルセキュリティ戦略を発表[8]し、サイバー空間におけるフランスの基本的な利益のため、防衛力を確保することを明記し、防衛主導で国全体のサイバーセキュリティを実施することを表明している。

フランスのサイバーセキュリティ機関は、首相府傘下の国家サイバーセキュリティ庁（ANSSI）である。ANSSIは1947年当時植民地であったアルジェリアに存在した技術暗号部（DTC）を起源としており、2009年に現在の国家サイバーセキュリティ庁の形となった。ANSSI内に設置された実働組織である情報システムセキュリティセンター（COSSI）はフランス軍内のサイバー防衛部隊であるCALIDと共同でサイバー攻撃への対応を行っている。

フランスは国全体のサイバーセキュリティ政策を調整する機関である国家防衛・安全保障事務総局（SGDSN）が国防省とANSSIの両者を管轄しているため、全体として防衛主導が色濃い。ドイツに比べやや体制整備が遅れているものの、人材育成プログラムを充実するなどして能力の向上に注力しており、ANSSIの人員は急速に増加している。

（２）法整備

政府によるサイバー脅威情報の収集に関しては、2015年にインテリジェンス法により法制化されており、主に対外治安総局（DGSE）が実施しており、この法律によって収集されたサイバー脅威情報はANSSIと共有され分析される。また、重要インフラのサイバーインシデント報告及び連絡担当者の設置は2014年-2019年軍事計画法（LPM）により義務化されている。（違反時罰則有り）

（３）産業育成・人材育成

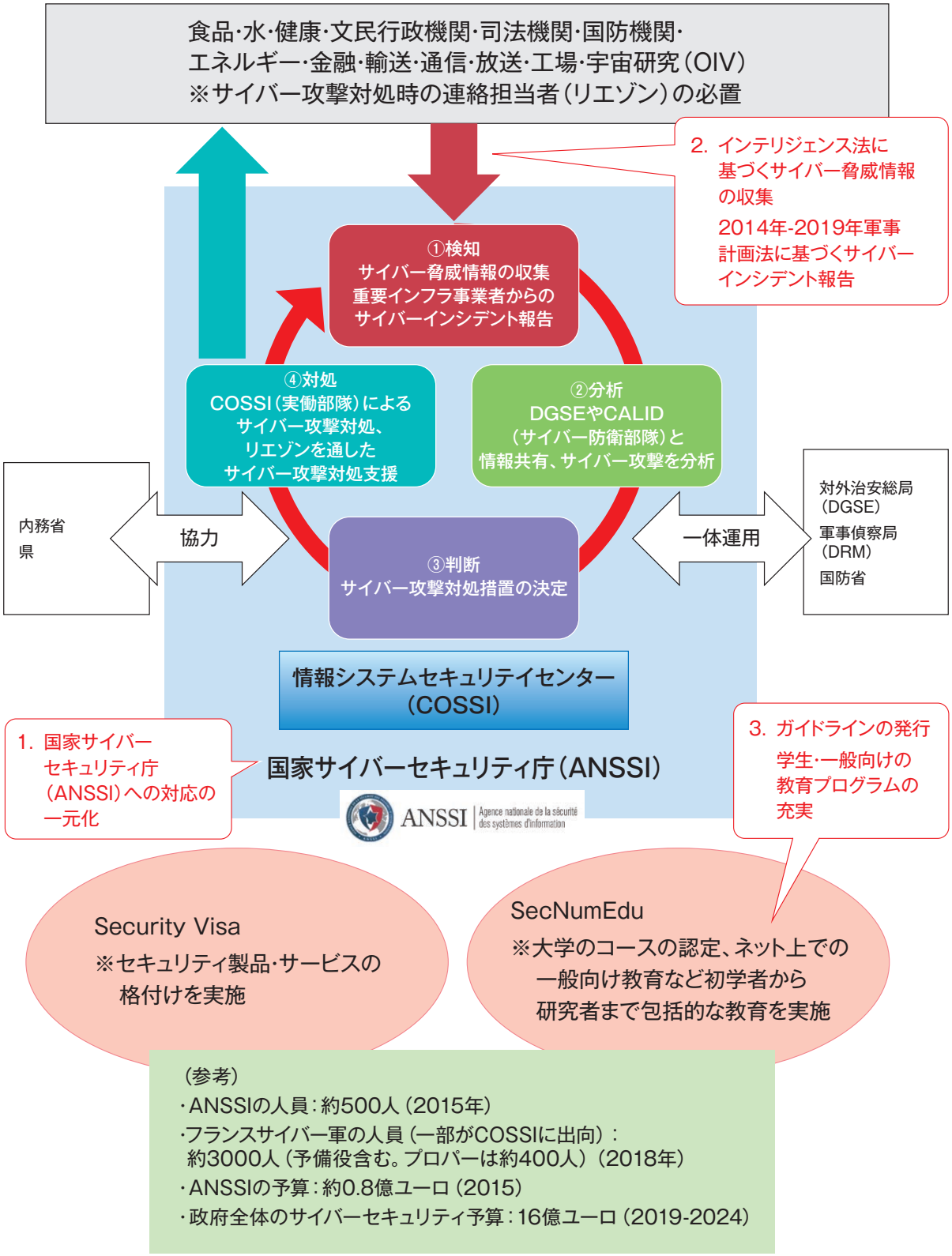
フランスは特に人材の確保・リテラシー教育に注力しており、人材育成プログラムであるSecNumEduには複数のサブプログラムが存在し、大学や大学院の講義を認定し学位を授与する専門的なカリキュラムだけでなく、セキュリティ教育を受けていない一般国民にもWebベースで遠隔で教育が受けられるサービスであるSecNumAcademyなども実施されている。また、産業育成に関してはセキュリティ製品やサービスの認定を行うSecurity Visaが発行されている。

8　FRENCH NATIONAL DIGITAL SECURITY STRATEGY, PREMIER MINISTRE, October 2015

表 2-5-1 フランスのサイバーセキュリティ政策

フランスのサイバーセキュリティ政策		
体制整備	1．国家戦略に政府の主導的な役割が明記されているか 2015年国家デジタルセキュリティ戦略において国全体のサイバーセキュリティのために防衛力を確保することを記載	△
	2．様々なサイバー攻撃への対応が一元化されているか 2009年に国家サイバーセキュリティ庁設置法により国家サイバーセキュリティ庁（ANSSI）を設置	○
	3．機動的なサイバー攻撃対応体制が整備されているか ドイツに1年ほどの遅れをとるも、検知・分析・判断・対処に係る体制整備を着実に実施。	○
法整備	4．政府によるサイバー脅威情報の収集を認める法律があるか 2015年にインテリジェンス法により法制化	○
	5．重要インフラ事業者にサイバーインシデント報告義務があるか 2014-2019年軍事計画法（LPM）により義務化	○
	6．重要インフラ事業者にサイバーインシデント連絡担当者の必置規制があるか 2014-2019年軍事計画法（LPM）により必置化	○
	7．政府によるプライバシー侵害を監視する機関があるか 議会情報技術監督委員会（CNCTR）が政府の活動を監視	○
産業育成 人材育成	8．サイバーセキュリティ機関が実施する産業育成プログラムがあるか ANSSIはセキュリティサービスの標準化を行うSecurity Visaを発行	△
	9．サイバーセキュリティ機関が実施する人材育成プログラムがあるか ANSSIは一般国民のリテラシー教育や学生のサイバーセキュリティ教育を総合的に行うSecNumEduを実施	○

図 2-5-2 フランスのサイバー攻撃対応体制・政策モデル



６.日本のサイバーセキュリティ政策

（１）体制整備

日本は2018年サイバーセキュリティ戦略において、サイバーセキュリティ基本法の理念に基づき、多様な主体の連携を重視するサイバーセキュリティを目指すとしており、各府省庁及び民間の自主的な努力に重点を置いている。各省庁は所管の範囲内で最大限の努力をしているものの、縦割りによる対応には限界が見えてきている。

日本のサイバーセキュリティ機関は、内閣官房サイバーセキュリティセンター（NISC）である。我が国では内閣法第12条により内閣官房の役割は「企画及び立案並びに総合調整に関する事務」と規定されているため、NISCは各府省庁の施策の調整と行政機関及び一部の独立行政法人・特殊法人・認可法人の情報システムのモニタリングのみ（NISCの実働組織である政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）が実施）を行っており、国全体のサイバーセキュリティを守る実務は行っていない（国や治安を守る自衛隊や警察庁、人命を守る消防庁、海を守る海上保安庁のような実働組織がない）。日本のサイバーセキュリティ政策は民間主導に力点を置いており、政府の体制整備は進んでいない。

（２）法整備

各省庁は、サイバーセキュリティを高めるために所管の範囲内で最大限の努力をしている。例えば、総務省は所管の電気通信事業法における「通信の秘密」ガイドラインを積極的に見直しており、「約款による規定を当事者の同意とみなし、通信の秘密の侵害に当たらない」というところまで来ている。また、情報通信研究機構（NICT）法も改正され、IoT機器の脆弱性調査を合法的にNICTが行えることになった。また現在、官民情報共有のための「サイバーセキュリティ協議会」の設置を規定したサイバーセキュリティ基本法の改正案が国会に上程されており、2020年の東京オリンピック・パラリンピックを前に、早期の成立が望まれている。

しかしながら、所管別の各省庁縦割りによる対応には限界が見えてきている。重要インフラのサイバーセキュリティは、各府省庁が既存の業法（特定の業種の営業に関する規制の条項を含む法律）における安全基準の設定や事業者に対する指示・命令を行っているものの、基本的には物理的な障害が発生した場合の所管省庁に対する事故報告義務しかなく、顕在化しないサイバー攻撃の被害について行政は把握できない。（他国のような具体的手続きを含む立法はされていない）

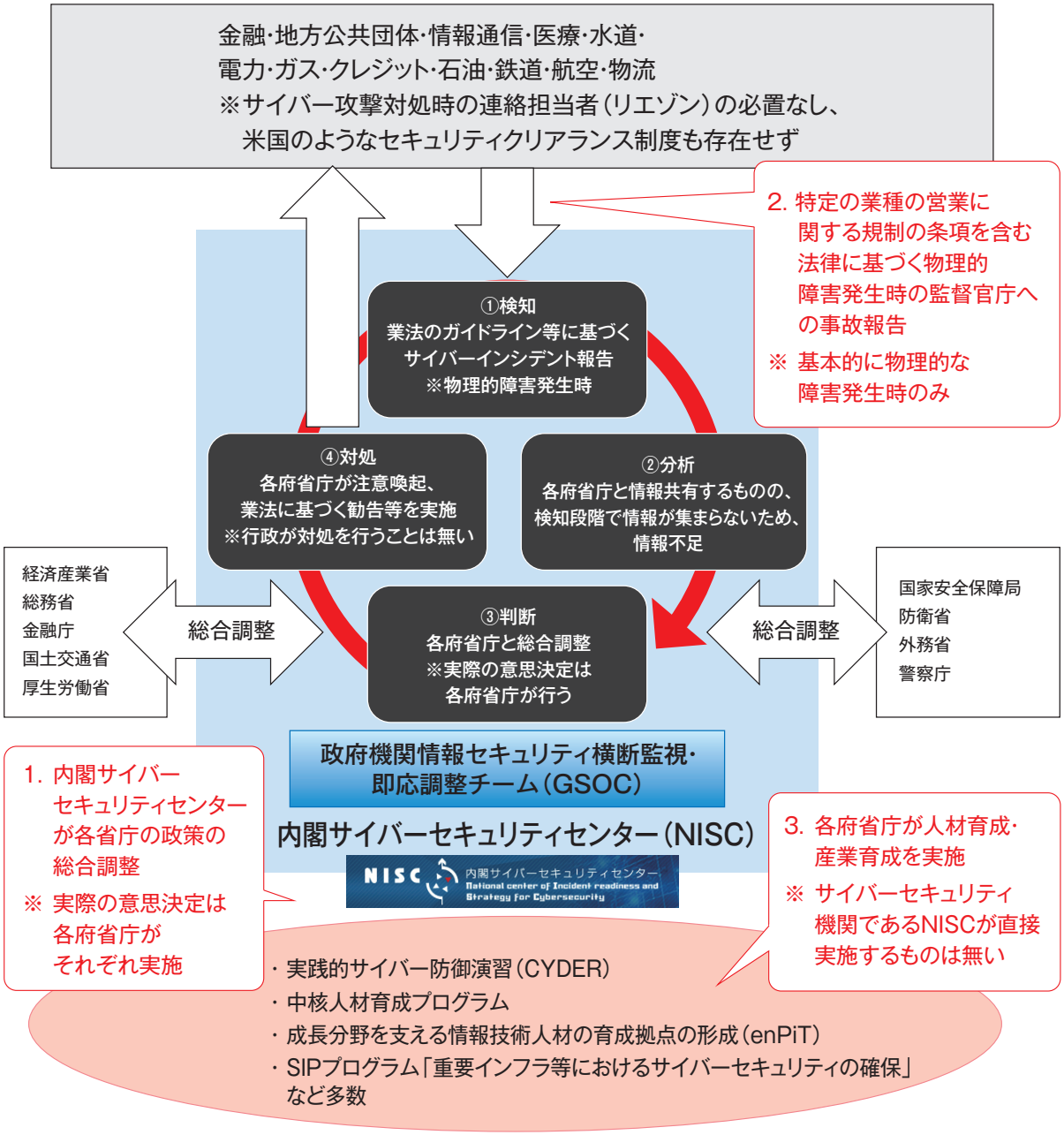
（３）産業育成・人材育成

産業育成、人材育成に関しても各省庁がそれぞれ実施しており、各国のようなサイバーセキュリティ機関が直接実施する産業育成プログラムや人材育成プログラムは存在しない。

表 2-6-1 日本のサイバーセキュリティ政策

日本のサイバーセキュリティ政策		
体制整備	1．国家戦略に政府の主導的な役割が明記されているか サイバーセキュリティ基本法第３条第２項において、「サイバーセキュリティに関する施策の推進は、国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促す」としており、サイバーセキュリティ戦略2018もその立場を踏襲	△
	2．様々なサイバー攻撃への対応が一元化されているか 2015年に内閣官房組織令（政令）により内閣サイバーセキュリティセンター（NISC）が設置されたが、その役割は各省庁の連絡・調整等に限られている	×
	3．機動的なサイバー攻撃対応体制が整備されているか 検知・分析・判断・対処の全てに体制整備の遅れ。	×
法整備	4．政府によるサイバー脅威情報の収集を認める法律があるか なし	×
	5．重要インフラ事業者にサイバーインシデント報告義務があるか 既存の業法のガイドライン・安全基準の改定により一部義務化（基本的にサービス障害発生時のみ報告義務）	△
	6．重要インフラ事業者にサイバーインシデント連絡担当者の必置規制があるか なし	×
	7．政府によるプライバシー侵害を監視する機関があるか なし	×
産業育成 人材育成	8．サイバーセキュリティ機関が実施する産業育成プログラムがあるか NISCが基本方針を定め、各府省庁が実施しているため、NISCが直接実施するプログラムはない	△
	9．サイバーセキュリティ機関が実施する人材育成プログラムがあるか 同上	△

図 2-6-2 日本のサイバー攻撃対応体制・政策モデル



（参考）
・NISCの人員：102人（2016年度）
・自衛隊サイバー部隊の人員：150人（2018年度）
・NISCのサイバーセキュリティ予算：約50億円（2018年度）
・自衛隊サイバー部隊の予算：約50億円（2018年度）
・政府全体のサイバーセキュリティ予算：727.5億円（2018年度）

第３章　日本のサイバーセキュリティ政策の課題

１. 体制整備

(1) 政府の主導的な役割が不足

サイバー攻撃は知的財産の流出、個人情報の漏洩だけでなく、国民の社会生活や経済的繁栄に対して深刻なダメージを与える可能性があり、社会のデジタル化に伴いその脅威は日々深刻化している。このため欧米各国では、サイバーセキュリティに関し政府が主導的な役割を果たす旨をサイバーセキュリティ戦略に明記する方向にある。

しかしながら、日本では、各府省庁、各民間事業者、各個人が自主的にサイバーセキュリティの確保を推進することとされており、重要インフラに対する国家支援のサイバー攻撃や、国の安全保障に係る大規模サイバー攻撃への対応も、原則的には民間企業の責務となっている。

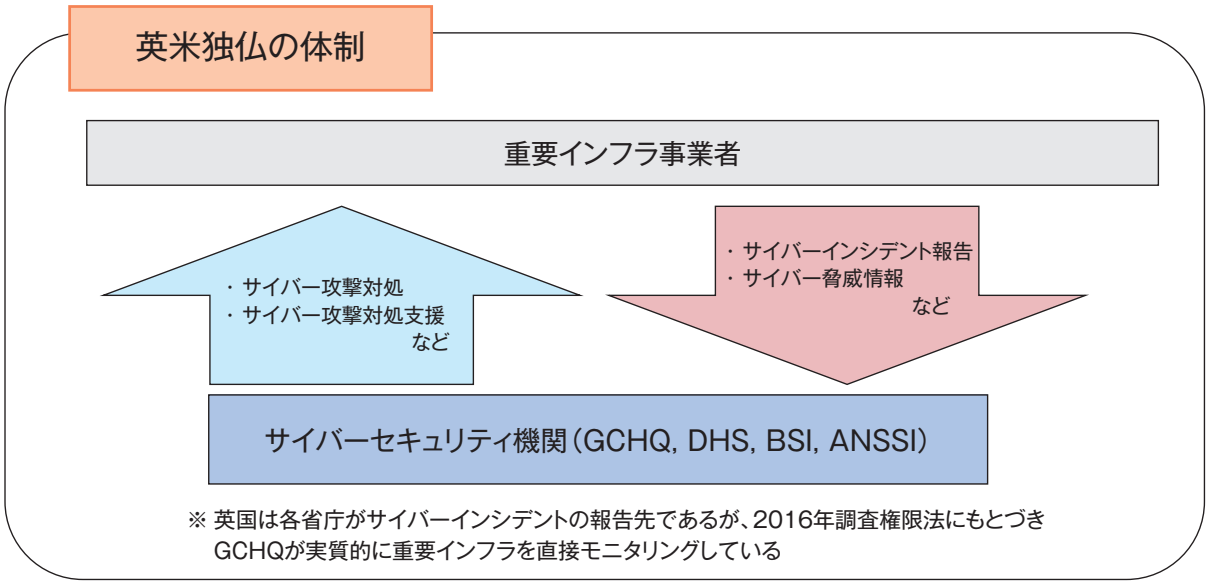
	各国のサイバーセキュリティ政策	英	米	独	仏	日
体制整備	国家戦略に政府の主導的な役割が明記されているか	○	○	○	△	△

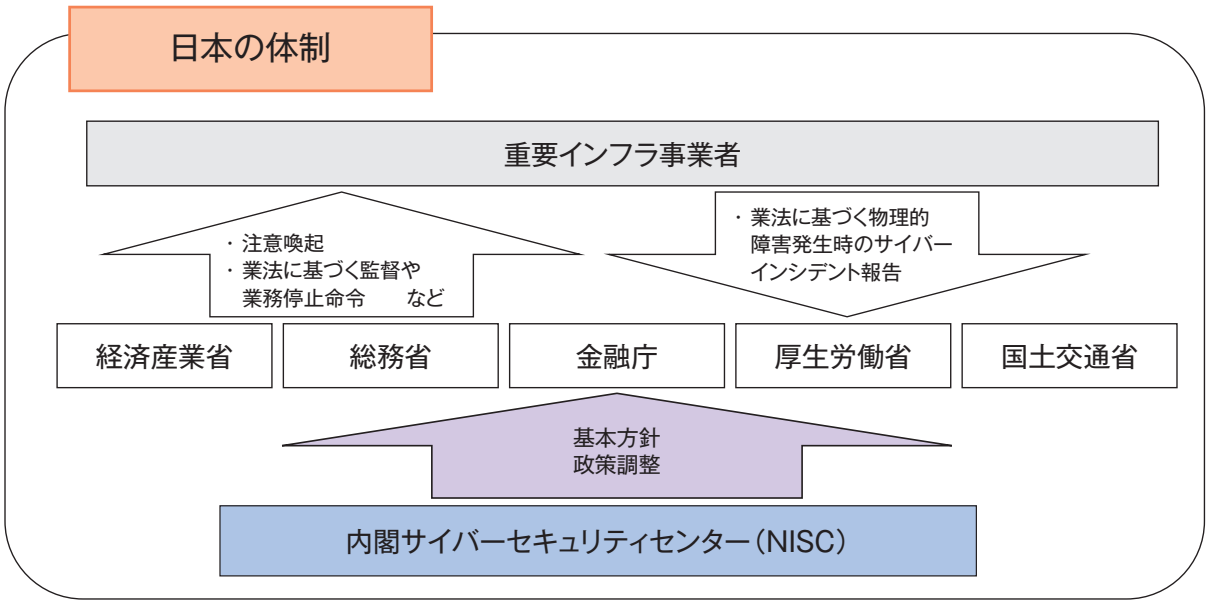
国名	国家戦略、命令、基本法の内容
英国	・国家サイバーセキュリティ戦略2016-2021 第4章OUR NATIONAL RESPONCE 「政府の最も主要な責務は他国からの攻撃から国を守り、市民と経済を損害から守ることと、我々の利益を守り基本的な権利を保障し犯罪者に司法的措置を取るための国内・国際的フレームワークを整備することである。」
米国	・米国国家サイバー戦略（2018年）前文ドナルド・トランプ大統領 「米国の国家安全保障を守り、米国市民の繁栄を推進することが私の最優先事項である」
ドイツ	・ドイツ国家サイバーセキュリティ戦略（2011年）Basic principles of the Cyber Security Strategy 「連邦政府はサイバー空間をセキュアにするために具体的な貢献をし、以ってドイツの経済・社会的繁栄を保持することを目標とする。」
フランス	・フランス国家デジタルセキュリティ戦略（2015年）第1章OBJECTIVE 「フランスはサイバー空間における基本的権利の防衛力を確保する。これは重要インフラのデジタルセキュリティを強化し、経済に不可欠な業者のデジタルセキュリティに全力を尽くすものである。」
日本	・サイバーセキュリティ基本法第３条第２項（基本理念） 「サイバーセキュリティに関する施策の推進は、国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促すとともに、サイバーセキュリティに対する脅威による被害を防ぎ、かつ、被害から迅速に復旧できる強じんな体制を構築するための取組を積極的に推進することを旨として、行われなければならない。」 ※サイバーセキュリティ戦略2018にて上記立場を踏襲

(2) 中央一元化された実務機関が無い

欧米各国には、GCHQ、DHS、BSI、ANSSIのような国全体のサイバーセキュリティを確保する実務機関が存在する。一方で、NISCは、行政システムのサイバーセキュリティに関する助言等は行うものの、それ以外については各府省庁の施策の総合調整を行うこととされている。このため、日本のサイバーセキュリティ政策については、①意思決定や対応のスピード、②海外サイバーセキュリティ機関との実務的な連携、③行政担当者の専門性、などに課題がある。

	各国のサイバーセキュリティ政策	英	米	独	仏	日
体制整備	様々なサイバー攻撃への対応が一元化されているか	○	○	○	○	×





２. 法整備

（１）政府によるサイバー脅威情報の収集の法制化がされていない

欧米各国は、プライバシーの保護を図りつつ、一定の条件のもとで合法的に行政がインターネットサービスプロバイダーからサイバー攻撃やその前兆等のサイバー脅威情報を収集できる法的枠組みを整えている。

しかしながら、日本では、サイバー脅威情報の収集に関して、通信傍受法に該当する場合を除き、ケースごとに電気通信事業法による違法性阻却事由があるか否かを判断しなければならないため、事前にサイバー攻撃を検知することが困難となっている。

	各国のサイバーセキュリティ政策	英	米	独	仏	日
法整備	政府によるサイバー脅威情報の収集を認める法律があるか	○	○	○	○	×

国名	サイバー脅威情報の収集に係る法律
英国	2016年調査権限法
米国	1978年外国情報監視法
ドイツ	郵便・メール・通信の秘密制限法及び連邦情報局法
フランス	インテリジェンス法
日本	-

（２）重要インフラのサイバーインシデント報告が義務化されていない

欧州各国は、国民の社会生活にとって不可欠な重要インフラがサイバー攻撃を受けた場合、その報告義務を重要インフラ事業者に対して課している。重要インフラ事業者に対する法的な報告義務を課していない米国は、AIS（Automated Indicator Sharing）という政府と民間企業がサイバー攻撃情報を自動的に共有するシステムを整えている。

しかしながら、日本では重要インフラ事業者に対するサイバー攻撃の報告義務が法的に課せられておらず、サイバー攻撃が潜在化したままとなってしまう。

	各国のサイバーセキュリティ政策	英	米	独	仏	日
法整備	重要インフラ事業者にサイバーインシデント報告義務があるか	○	△	○	○	△

国名	サイバーインシデント報告に係る法律
英国	2018年ネットワーク情報システム法
米国	2015年サイバーセキュリティ情報共有法
ドイツ	ITセキュリティ法
フランス	2014-2019年軍事計画法
日本	既存の業法のガイドライン等に規定（基本的にサービス障害時のみ）

（3）重要インフラ事業者にサイバー攻撃対処時の連絡担当者（リエゾン）がいない

重要インフラ事業者は、国民の社会生活にとって死活的な役割を果たしていることから、様々な事態に即時対応できるような事業継続計画（BCP）が求められる。このため、欧州各国は重要インフラ事業者に連絡担当者を必置化し、サイバー攻撃に即時対処できる体制が整備されている。

しかしながら、日本では重要インフラ事業者に連絡担当者が必置化されておらず、重要インフラへのサイバー攻撃が発生した場合に現場で行政との連絡に当たる担当者が存在せず、対処が不可能で被害が甚大化する可能性がある。

	各国のサイバーセキュリティ政策	英	米	独	仏	日
法整備	重要インフラ事業者にサイバーインシデント連絡担当者の必置規制があるか	○	△	○	○	×

国名	連絡担当者の必置に係る法律
英国	2018年ネットワーク情報システム法により重要インフラ事業者（OEV）と関連サービスプロバイダ（RDSP）に連絡担当者を必置化
米国	-（セキュリティ・クリアランス保持者が多数存在）
ドイツ	ITセキュリティ法により重要インフラ事業者（KRITIS）と関連サービスプロバイダ（Anbieter Digitaler Dienste）に連絡担当者を必置化
フランス	2014-2019年軍事計画法により重要インフラ事業者（OIV）に連絡責任者を必置化
日本	-

（4）行政のプライバシー侵害を監視する機関が無い

欧米各国は、行政がサイバー攻撃への対応のために必要のない情報を集め国民のプライバシー侵害を行うことを未然に防ぐため、議会に第三者委員会としてプライバシー侵害を監視する組織を設置している。一方で、日本は行政のプライバシー侵害を監視する機関が存在せず、政府がサイバー攻撃への対応にあたって権力を恣意的に濫用することを抑止する枠組みが不十分である。

	各国のサイバーセキュリティ政策	英	米	独	仏	日
法整備	政府のプライバシー侵害を監視する機関があるか	○	○	○	○	×

国名	政府のプライバシー侵害の監視を行う機関
英国	議会情報安全保障委員会（ISC）
米国	上院情報委員会（SSCI）、下院情報委員会（HPSCI）
ドイツ	議会監督委員団（PKGs）
フランス	議会情報技術監督委員会（CNCTR）
日本	-

３. 産業・人材育成

（１）NISCが直接実施する産業育成の枠組みが無い

各国のサイバーセキュリティ機関は産官学連携の協定に基づき、研究機関や大学の研究開発を支援するか、あるいは製品やサービスを認定する枠組みを整備している。日本も、内閣府の行うSIPプログラムなど先進的な産業育成の枠組みを整えているが、それぞれの省庁がサイバーセキュリティの専門官庁でないため、専門性の高い産業育成を行うことが難しい。

（２）NISCが直接実施する人材育成プログラムが無い

各国は、サイバーセキュリティ機関が集約された教育プログラムを実施している。日本は総務省の実施する実践的サイバー防御演習（CYDER）、経産省の実施する産業サイバーセキュリティセンターの中核人材育成プログラム、文部科学省の実施する「成長分野を支える情報技術人材の育成拠点の形成（enPiT）等、各府省庁が幅広い分野での教育プログラムを実施しているものの、一貫した教育フレームワークが存在せず、体系的な人材育成が遅れている。

	各国のサイバーセキュリティ政策	英	米	独	仏	日
人材・産業育成	サイバーセキュリティ機関の実施する産業育成プログラムがあるか	○	○	△	△	△
	サイバーセキュリティ機関の実施する人材育成プログラムがあるか	○	○	△	○	△

国名	産業育成プログラム	人材育成プログラム
英国	・Academic Centres of Excellence in Cyber Security Research （実施主体：GCHQ・EPSRC）	・CYBERFIRST （実施主体：GCHQ）
米国	・National Centers of Academic Excellence （実施主体：DHS・NSA）	
ドイツ	・IT Baseline Protection Catalogs （実施主体：BSI）	・BSIが大学等からの職員登用プラグラムを実施
フランス	・Security Visa （実施主体：ANSSI）	・SecNumEdu （実施主体：ANSSI）
日本	・SIPプログラム「重要インフラ等におけるサイバーセキュリティの確保」 （実施主体：内閣府・経済産業省）	・実践的サイバー防御演習（CYDER） （実施主体：総務省） ・中核人材育成プログラム （実施主体：経済産業省） ・成長分野を支える情報技術人材の育成拠点の形成（enPiT） （実施主体：文部科学省） など23の制度が存在

第４章　政策提言
～ 日本にサイバーセキュリティ庁の創設を！～

１. 日本にサイバーセキュリティ庁の創設を！

（１）サイバーセキュリティにおける政府の主導的役割の明確化

日本では、サイバーセキュリティ基本法に「国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促す」とあるとおり、国民の自発的な取組が中心とされ、セイバーセキュリティ戦略2018でもその立場が踏襲されている。しかしながら、第２章で述べたように、世界各国のサイバーセキュリティ国家戦略においては政府の主導的な役割が明記されており、国民の社会生活に多大な損害をサイバー攻撃が与えるようになった現状では、サイバーセキュリティを確保する上で、政府の主導的な役割が不可欠となっている。

国家を背景としたサイバー攻撃の激化や国家レベルで開発されたサイバー攻撃ツールの拡散といった、新次元のサイバー脅威への対応は、もはや民間の努力だけでは限界に達しつつある。例えば英国では、2011年の「国家サイバーセキュリティ戦略」において、民間のサイバーセキュリティ能力の底上げを図ることで、中小のビジネスも含む国全体のセキュリティ確保を行おうとしたが、2016年のサイバーセキュリティ戦略策定にあたってレビューを行なったところ、民間部門だけではセキュリティの向上が見込めないことが明らかになった。そのため2016年の「国家サイバーセキュリティ戦略」では、積極的サイバー防御も含め、政府が主導的にサイバーセキュリティを確保することを明確にした。また、国家を背景とした攻撃事例の増加を受け、米国でも2016年の大統領政策指令41号（PPD-41）で、サイバーインシデントに対して、連邦政府の役割と責任を明確化している。

このような先進国のサイバー攻撃に対する政府の主導的な役割の拡大を考慮するならば、我が国もサイバーセキュリティ戦略のなかで「国（政府）の主導的役割」を明記すべきであり、これに伴い、サイバーセキュリティ基本法においても、第３条「理念」及び第４条「国の責務」に政府の主導的な役割を明記する必要がある。

サイバーセキュリティ基本法（現行法）	サイバーセキュリティ基本法（改正案）
（理念） 第３条　サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による情報の自由な流通の確保が、これを通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要であることに鑑み、サイバーセキュリティに対する脅威に対して、国、地方公共団体、重要社会基盤事業者（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。以下同じ。）等の多様な主体の連携により、積極的に対応することを旨として、行われなければならない。 （中略） ６　サイバーセキュリティに関する施策の推進に当たっては、国民の権利を不当に侵害しないように留意しなければならない。	（理念） 第３条　サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による情報の自由な流通の確保が、これを通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要であることに鑑み、サイバーセキュリティに対する脅威に対して、国、地方公共団体、重要社会基盤事業者（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。以下同じ。）等の多様な主体の連携により、積極的に対応することを旨として、行われなければならない。 （中略） ６　サイバーセキュリティに関する施策の推進に当たっては、国民の権利を不当に侵害しないように留意しなければならない。 ７　サイバーセキュリティに関する施策の推進は、我が国の人口、産業その他の社会経済情勢の変化を踏まえ、サイバー攻撃による被害の発生を常に想定するとともに、被害の最小化及びその迅速な回復を図ることを旨として、行われなければならない。 ８　サイバーセキュリティに関する施策の推進は、サイバー攻撃に備えるための措置を適切に組み合わせて一体的に講ずること並びに科学的知見及び過去の被害から得られた教訓を踏まえて絶えず改善を図ることを旨として、行われなければならない。 ９　サイバー攻撃による被害の発生直後その他必要な情報を収集することが困難なときであつても、できる限り的確に被害の状況を把握し、これに基づき人材、物資その他の必要な資源を適切に配分することにより、人の生命及び身体を最も優先して保護すること。また、被害が発生したときは、速やかに、施設の復旧及び被害者の援護を図り、被害からの復旧を図ること。
（国の責務） 第４条　国は、前条の基本理念（以下「基本理念」という。）にのっとり、サイバーセキュリティに関する総合的な施策を策定し、及び実施する責務を有する。	（国の責務） 第４条　国は、前条の基本理念（以下「基本理念」という。）にのつとり、国民の生命、身体及び財産をサイバー攻撃から保護する使命を有することに鑑み、組織及び機能の全てを挙げてサイバーセキュリティに関し万全の措置を講ずる責務を有する。 ２　国は、前項の責務を遂行するため、サイバー攻撃の予防、サイバー攻撃への応急対策及び被害からの復旧の基本となるべき計画を作成し、及び法令に基づきこれを実施するとともに、地方公共団体及び民間企業等が実施するサイバー攻撃対策につき、勧告し、指導し、助言し、総合調整を行ない、その他適切な措置をとらなければならない。

（2）サイバーセキュリティ庁の創設

サイバーセキュリティにおいて政府が主導的な役割を果たすため、第２章で概観したように、欧米各国では一元化されたサイバーセキュリティ実務機関が設置されている。しかしながら、我が国においては、サイバーセキュリティの実務を担う一元的な機関が存在していない。

現行では内閣サイバーセキュリティセンター（NISC）であるが、内閣官房組織令で定められているのは「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」、「行政各部におけるサイバーセキュリティの確保に関し必要な助言、情報の提供その他の援助に関すること」、「行政各部の施策に関するその統一保持上必要な企画及び立案並びに総合調整」などであり、実務としては、行政機関と一部政府関連法人の情報システムの監視のみを行っており、国全体のサイバーセキュリティを守る権限は与えられていない。また、サイバー脅威情報を分析し、その対処を行う十分な人数の実働部隊も存在していない。NISCの役割は各省庁の総合調整機関であり、緊急時の指揮命令権限もなく、所掌範囲も行政機関（及び独立行政法人）までであり、重要インフラ等は対応の対象となっていない。

高度化・巧妙化するサイバー攻撃に迅速に対応するためには、我が国でも一元化されたサイバーセキュリティ実務機関の創設が必要である。火災や事故に対して消防庁・自治体消防局の消防士が対応しているように、海洋における遭難・事故・事件に対して海上保安庁の海上保安官が対応しているように、国内の事件・事故に関して警察庁・都道府県警の警察官が対応しているように、サイバー空間においても、サイバー空間で「泳げる」技術と資格を持った専門家が対応する必要がある。

そのためには、現行のNISCを発展的に改編・強化する形で、内閣府外局として新たに「サイバーセキュリティ庁」（Cyber Security Agency：CSA）を設置すべきである。「サイバーセキュリティ庁」は、国民の生命、身体及び財産をサイバー攻撃から保護する責務を一元的に担う行政機関となる。

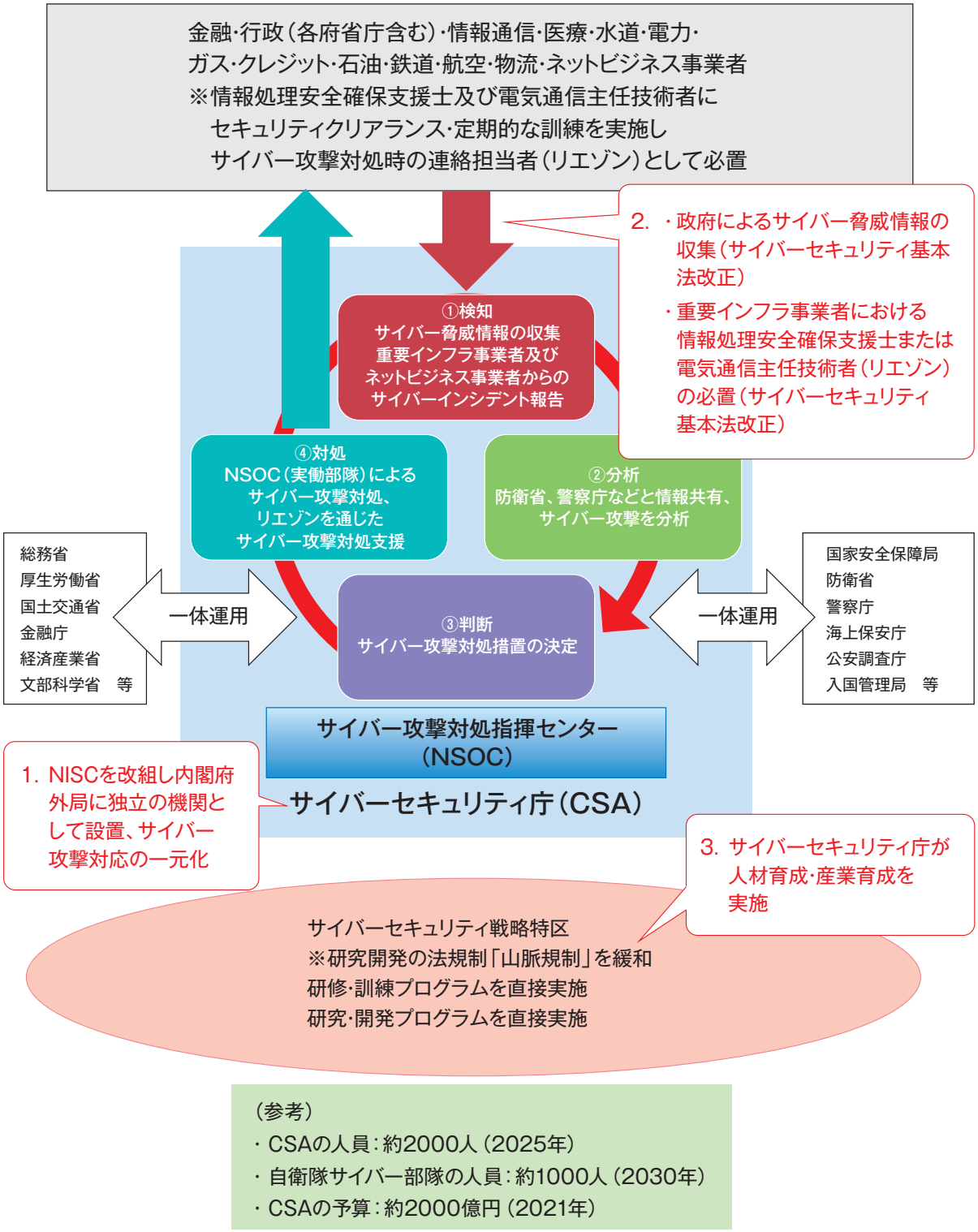
この新設されるサイバーセキュリティ庁では、現行では各機関にまたがっているサイバー空間全体の情報収集、サイバー攻撃の検知・分析を情報分析室に一元化するほか、情報分析室によるサイバー脅威情報の分析を踏まえ、行政機関や重要インフラ等へのサイバー攻撃への対処も「サイバー攻撃対処指揮センター（NSOC）」で統一的に行える能力を持たせる。特にこのNSOCの下には、サイバー空間で「泳げる」能力をもった専門家からなる対応の実働部隊を複数配置し、同時多発的なサイバー攻撃に対しても対応できるだけの複数の部隊を持たせることが望ましい。

具体的な組織の形態については、図4-2-2及び図4-2-4のとおりであるが、全体の規模としては、日本の経済規模や英国のGCHQ、ドイツのBSI、フランスのANSSIなどの例を勘案すると、最終的に2000人規模、年間予算2000億円程度の組織が必要である。

図4-2-1 サイバーセキュリティ庁（CSA）の業務

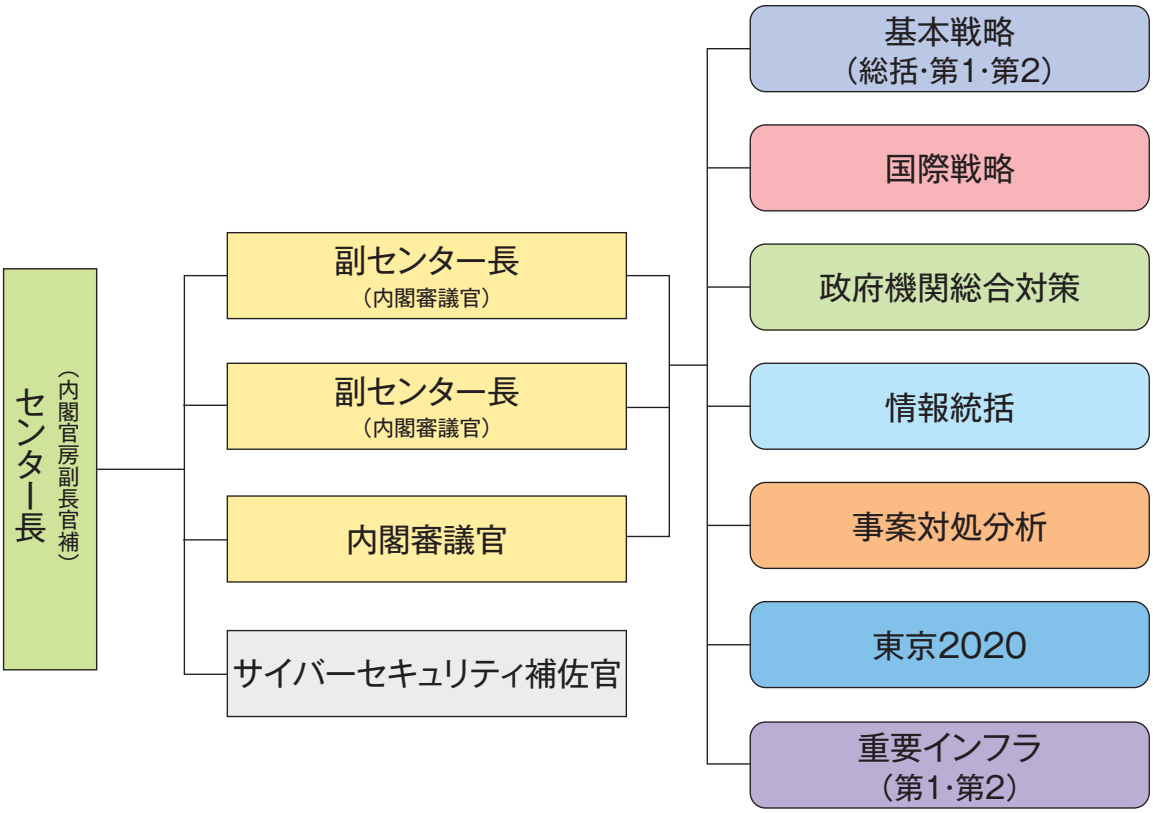
サイバーセキュリティに係る業務	現状	新体制
サイバーセキュリティ戦略の策定・推進	サイバーセキュリティ戦略本部 （NISCが事務局）	サイバーセキュリティ戦略本部 （CSAが事務局）
国家の重要資産の特定とサイバーセキュリティリスクの評価	NISCが一部実施	CSA
政府・独立行政法人・重要インフラの情報システムの防御 （対外基準の策定、対策の評価・勧告等）	NISC・IPA	CSA
サイバー空間全体の全体の情報収集（サイバー脅威情報の収集）及びサイバー攻撃の検知・分析	NISC-GSOC （政府と独法のみ） IPA、NICT、JPCERT、ISAC	CSAが全体をコーディネート
政府・独立行政法人に対するサイバー攻撃への対処・復旧支援	NISC-CYMAT	CSA
重要インフラに対するサイバー攻撃への対処・復旧支援	-	CSA
諸外国のサイバーセキュリティ庁との連携 国際協力の推進	NISC、各府省、外務省	CSAが一元窓口
サイバー武力攻撃への対応	官邸対策室 防衛省	官邸対策室 防衛省、CSA
サイバーテロへの対応	官邸対策室 （NISCは担当せず）	官邸対策室 （CSAも参加）
サイバー犯罪の取り締まり	警察庁	警察庁 （CSAも捜査に協力）
サイバーセキュリティ産業の振興及び国際競争力の強化	経産省、総務省	CSA
サイバーセキュリティ研究・開発の推進	総務省、経産省、文科省	CSA
サイバーセキュリティ人材の確保	文科省、経産省、総務省	CSA
サイバーセキュリティ教育及び学習の振興	文科省、NISC	CSA
デジタルゲリマンダー（サイバー世論操作）への対処	総務省	CSA

図4-2-2 サイバーセキュリティ庁設置後の日本のサイバー攻撃対応体制・政策モデル



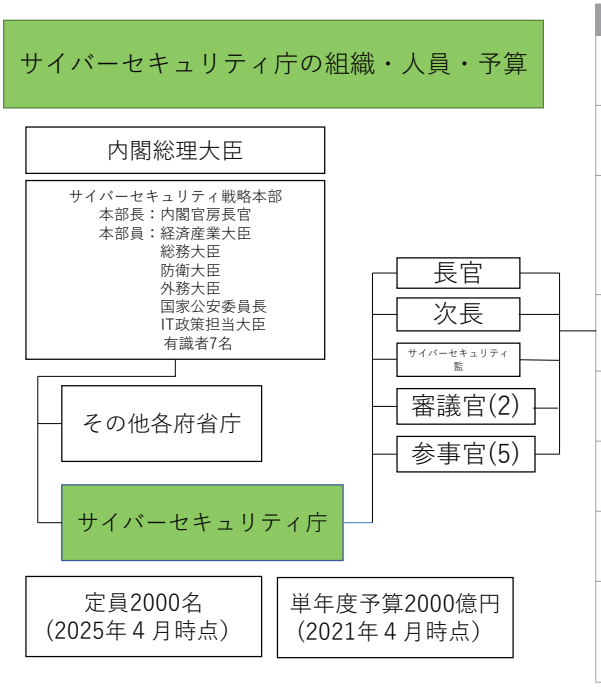
（参考）
- CSAの人員：約2000人（2025年）
- 自衛隊サイバー部隊の人員：約1000人（2030年）
- CSAの予算：約2000億円（2021年）

図4-2-3 現行の内閣サイバーセキュリティセンター（NISC）の組織



出典：「内閣サイバーセキュリティセンター（NISC）の組織体制」
（内閣サイバーセキュリティセンターのホームページ　最終閲覧日:2018年10月26日）
https://www.nisc.go.jp/about/organize.html

図4-2-4 サイバーセキュリティ庁（CSA）の組織・人員・予算



課員(定員)	主たる業務（抜粋）
総務課(50名)	総務、人事、予算、会計、機構・定員、メディア・広報・報道対応、政策関連の情報発信、国会連絡
情報部(350名) (情報分析室300名)	・サイバー空間の情報収集・加工・分析 ・ダークウェブ、ディープウェブの状況把握 ・国際連携
事案対処部(1150名) (サイバー攻撃対処指揮センター (NSOC)1100名)	・サイバー攻撃対処指揮センター(NSOC)を所管 ・サイバー攻撃への対処、復旧支援 ・重要インフラの横断監視 ・サイバー脅威情報の発信、サイバーインシデント情報の発信 ・各府省庁CERTとの連携
社会基盤防護部(150名) (鑑査室100名)	・サイバーセキュリティ基本法の監査を所管 ・国の重要資産の特定とリスクアセスメント ・部内移動設備・物理施設の維持管理
戦略企画課(50名)	・サイバーセキュリティ戦略本部の事務を所管 ・サイバーセキュリティ戦略の策定・推進 ・各府省庁との政策総合調整
通信管理課(50名)	・部内情報システム管理 ・官民情報共有システムの維持管理 ・部内通信設備・衛星の維持管理
人材開発部(100名) (サイバーアカデミックセンター50名)	・サイバーアカデミックセンターを所管 ・サイバーセキュリティ人材の育成、獲得 ・教育カリキュラムの策定、推進
研究開発部(100名) (R &Dセンター50名)	・サイバーR &Dセンターを所管 ・サイバーセキュリティ産業の育成・推進 ・政策評価 ・部内情報システム、暗号、ツールの開発

サイバーセキュリティ庁設置法（案）

（趣旨）
第１条　この法律は、サイバーセキュリティ庁の設置並びに任務及びこれを達成するため必要となる明確な範囲の所掌事務を定めるものとする。

（設置）
第２条　内閣府設置法（平成11年法律第89号）第49条第３項の規定に基づいて、内閣府の外局として、サイバーセキュリティ庁を設置する。
２　サイバーセキュリティ庁の長は、サイバーセキュリティ庁長官（以下「長官」という。）とする。

（任務）
第３条　サイバーセキュリティ庁は、サイバーセキュリティ基本法（平成26年法律第104号）第2条の基本理念にのっとり、国民の生命、身体及び財産のサイバー攻撃からの保護に関する事務を行うことを任務とする。
２　前項に定めるもののほか、サイバーセキュリティ庁は、同項の任務に関連する特定の内閣の重要政策に関する内閣の事務を助けることを任務とする。
３　サイバーセキュリティ庁は、前項の任務を遂行するに当たり、内閣官房を助けるものとする。

（所掌事務）
第４条　サイバーセキュリティ庁は、前条第１項の任務を達成するため、次に掲げる事務をつかさどる。
一　サイバーセキュリティ戦略の策定・推進
二　国家の重要資産の特定とサイバーセキュリティリスクの評価
三　政府・独立行政法人・重要インフラの情報システムの防御
　（対策基準の策定、対策の評価・勧告等）
四　サイバー空間全体の情報収集
五　サイバー攻撃の検知・分析
六　政府・独立行政法人・重要インフラに対するサイバー攻撃への対処・復旧支援
七　諸外国のサイバーセキュリティ機関との連携
八　サイバーセキュリティに係る国際協力の推進
九　サイバー武力攻撃への対応の支援
十　サイバーテロへの対応の支援
十一　サイバー犯罪の取締りへの協力
十二　サイバーセキュリティ産業の振興及び国際競争力の強化
十三　サイバーセキュリティに係る研究開発の推進
十四　サイバーセキュリティ人材の確保
十五　サイバーセキュリティ教育及び学習の振興
２　前項に定めるもののほか、サイバーセキュリティ庁は、前条第２項の任務を達成するため、行政各部の施策の統一を図るために必要となる事項の企画及び立案並びに総合調整に関する事務（内閣官房が行う内閣法（昭和22年法律第５号）第12条第２項第２号に掲げる事務を除く。）をつかさどる。
３　前２項に定めるもののほか、サイバーセキュリティ庁は、前条第２項の任務を達成するため、内閣府設置法第４条第２項に規定する事務のうち、前条第１項の任務に関連する特定の内閣の重要政策について、当該重要政策に関して閣議において決定された基本的な方針に基づいて、行政各部の施策の統一を図るために必要となる企画及び立案並びに総合調整に関する事務をつかさどる。

（資料の提出要求等）
第５条　長官は、サイバーセキュリティ庁の所掌事務を遂行するため必要があると認めるときは、関係行政機関の長に対し、資料の提出、説明その他必要な協力を求めることができる。

図 4-2-5 サイバーセキュリティ庁と他組織の規模の比較

	定員	予算	任務
海上保安庁	13,994人 （2018年度）	2,112億円 （2018年度当初）	・治安の確保 ・領海警備 ・救難救護 ・海洋調査 ・国際協力など
警察庁	7,902人 （2018年度） ※警察官は全国26万人	3,168億円 （2018年度当初） ※都道府県予算を含めると約3.7兆円	・市民生活の安全確保 ・犯罪捜査 ・警備 ・交通規制 ・国際捜査共助など
消防庁	169人 （2018年） ※消防士は約16万人 消防団員は約85万人	143億円 （2018年度当初） ※市町村消防費2.7兆円	・消防防災 ・救急救助 ・火災予防 ・国民保護など
サイバーセキュリティ庁	2,000人 （2025年度）	2,000億円 （2021年度）	・リスク評価・予防 ・サイバー攻撃の検知・分析・判断・対処 ・産業育成・人材育成 ・国際連携など

（3）サイバーセキュリティ賦課金の創設

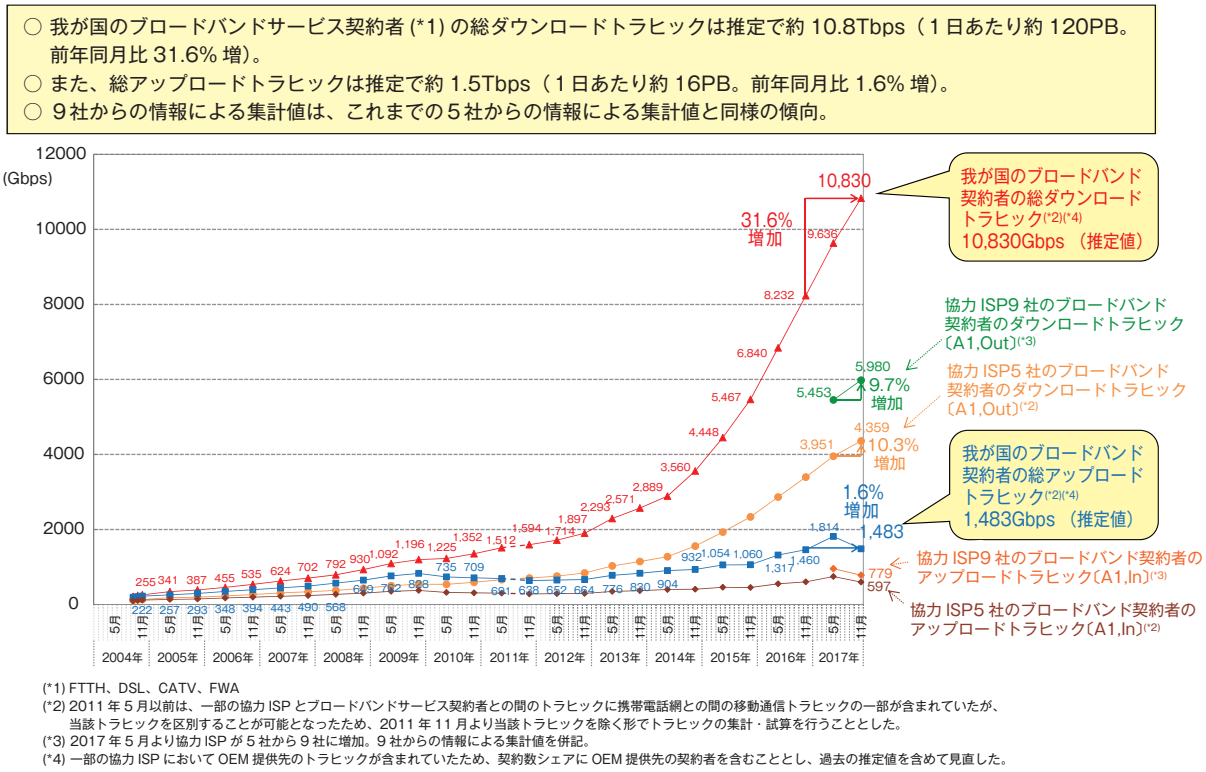
増分主義に基づく、現行の行政予算の組み替えという発想のもとでは、「サイバー空間」という新たな、かつ急速に広がり続けるドメインを守ることはできない。IoT社会が到来しSociety5.0となる時代においては、情報流通の基盤整備とセキュリティを新たな発想で行う必要がある。

我が国では、道路、電源開発、港湾整備、空港整備などのインフラ整備に関しては特別会計で行ってきた歴史がある。また、現在でもエネルギー対策や食料の安定供給、自動車安全などの国民の安心と安全に関わる分野については、特別会計がそれぞれ残されている。例えば道路の整備は、受益者負担の原則に基づき、ガソリン税や自動車重量税からなる道路特定財源制度によって実施されてきた。インフラの整備が整い、行政改革も相まって、これらの特別会計は整理されてきたが、サイバーの分野はまったく状況が異なる。国民生活の基盤となるインフラも安心・安全を担保するサイバーセキュリティも不十分だからである。また、民間が負担するサイバーセキュリティのコストも年々上昇しており、この一部を公的に負担する道を拓く時期に来ている。

サイバーセキュリティ庁を最終的に2000人規模、年間予算2000億円程度の組織にすることを前提とし、Society5.0時代の情報基盤のインフラをある程度公的に整備することを考えれば、受益者負担の原則に基づき、情報基盤安全環境整備賦課金制度を設けるべきである。情報基盤を利用する国民のみならず、経済活動を情報基盤に依拠する企業や、情報基盤を使ってサービスを提供するGAFA（Google, Amazon, Facebook, Apple）など海外のIT企業にも負担を求める。当グルー

プの試算では、インターネットの通信料に１ギガビットあたり１円の賦課金を課すことで、年間4000億円程度の予算の確保が可能になると見込まれる。

Society5.0時代には、自動車などを含めあらゆるものが高速でネットに繋がることが必要となる。そのためには、全国津々浦々に5Gの高速移動体通信網の整備が必要とされる。基盤整備と同時に、ネットに繋がったすべての機器の安全を確保することが、Society5.0時代の喫緊の課題となっており、これを同時に解決する手段として、情報基盤安全環境整備賦課金の導入は有効である。



(*1) FTTH、DSL、CATV、FWA
(*2) 2011 年 5 月以前は、一部の協力 ISP とブロードバンドサービス契約者との間のトラヒックに携帯電話網との間の移動通信トラヒックの一部が含まれていたが、当該トラヒックを区別することが可能となったため、2011 年 11 月より当該トラヒックを除く形でトラヒックの集計・試算を行うこととした。
(*3) 2017 年 5 月より協力 ISP が 5 社から 9 社に増加。9 社からの情報による集計値を併記。
(*4) 一部の協力 ISP において OEM 提供先のトラヒックが含まれていたため、契約数シェアに OEM 提供先の契約者を含むこととし、過去の推定値を含めて見直した。

出典：「我が国のインターネットにおけるトラヒックの集計結果（2017年11月分）」
（2018年２月27日　総務省 総合通信基盤局　電気通信事業部 データ通信課）
http://www.soumu.go.jp/main_content/000535404.pdf

（我が国の一日当たりのブロードバンドサービス契約者の総ダウンロードトラヒック）
＝約120（ペタバイト：PB）
（我が国の一日当たりのブロードバンドサービス契約者の総アップロードトラヒック）
＝約16（PB）
（我が国の一年当たりのブロードバンドサービス契約者の総トラヒック）=（120（PB）+16（PB））×365（日）=49,640（PB）=49,640,000,000（ギガバイト: GB）
=397,120,000,000（ギガビット: Gbit）
電力における固定価格買取制度（FIT）と同様にインターネットの通信量に1ギガビット当たり1円の賦課金を課せば、
年間397,120,000,000円＝約4,000億円の予算確保が可能
国民1人当たり一様に負担するとなれば年間3,200円であるが、海外大手IT事業者など大口の利用者の負担が大きく、一般的なスマホユーザー向けのデータ定額プラン（月々5GBのプラン）であれば賦課金は月々40円程度に留まる。（5（GB）×8=40（Gbit））
これは、各世帯の年間の電話通信料約12万円と比べても非常に少額に収まる。

（単位：円）

（年）	2010	2011	2012	2013	2014	2015	2016	2017
電話通信料	110,771	111,372	111,906	112,453	113,775	117,720	120,392	122,207
（うち）固定電話通信料	30,853	30,806	30,429	29,354	27,536	26,414	24,086	21,957
（うち）移動電話通信料	79,918	80,566	81,477	83,099	86,239	91,306	96,306	100,250
消費支出	3,027,938	2,966,673	2,971,816	3,018,910	3,017,778	2,965,515	2,909,095	2,921,476
消費支出に占める電話通信料の割合（%）	3.66%	3.75%	3.77%	3.72%	3.77%	3.97%	4.14%	4.18%

出典：「平成 30 年版情報通信白書」（総務省）
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/pdf/n5200000.pdf

２. サイバーセキュリティのための情報収集に関する法整備を！

（１）サイバー脅威情報収集能力強化のため通信ログのモニタリング

サイバー攻撃に適切に対応するためには、サイバーセキュリティの実施機関がサイバー攻撃の兆候を事前に検知する必要がある。このため、英国・米国・ドイツ・フランスの各国では、通信ログを保存し、必要に応じて令状などにもとづきサイバーセキュリティ実施機関へ提供することが法律で義務付けられている。

我が国においては、電気通信事業法のガイドラインにおいて、概ね1年を上限としてログの保存を認めるとされているが、例えば中国の人民解放軍の軍人をサイバー攻撃の犯人として訴追した米国の事案においては、数年にわたるログ情報が訴追状の中で証拠として提示されている。

したがって、我が国においても、各国と同様に、数年にわたり通信ログを保存し、必要に応じて令状などに基づきサイバーセキュリティ実施機関へ提供することを通信事業者に義務付けることにより、サイバー攻撃の事前検知及び追跡等を行う必要がある。

（2）国会におけるプライバシー侵害監視委員会の設置

サイバーセキュリティのためのモニタリングは、プライバシーとの関係で各国とも慎重に行われている。行政傍受の濫用を防ぐために、各国ではプライバシー侵害監視委員会という形でバランスを取っている例が多い。

先に述べたように、英国・米国・ドイツ・フランスの各国は、行政によるプライバシー侵害を監視するため議会に委員会を設置し、恣意的な権力濫用を防止している。

このため、我が国においても、行政がサイバー脅威情報の収集を行うにあたり、行政における情報の取り扱いのチェックのため、第三者によるチェック体制を整備するべきである。また、行政のこうした情報収集活動によるプライバシー侵害を抑止するため、サイバーセキュリティ庁の活動に関する情報公開制度も整備すべきである。

（3）重要インフラ事業者のサイバーインシデント報告の義務化

サイバー攻撃に対応するためには、どのような攻撃を現在受けているのかをほぼリアルタイムに近い形で把握する必要がある。我が国においては、かかる攻撃に関する情報共有は任意での共有になっており、また現行法においては、重要インフラ事業に対し事業法（電力事業法、ガス事業法等）においては所管官庁に対するサイバーインシデント報告が義務化されていない。

一方、英独仏３か国においては、ECのNIS指令（2016年7月制定・2018年6月施行）により、重要インフラ事業者に対しサイバーインシデントをサイバーセキュリティ機関へと報告することがNIS指令施行前に既に罰則付きで法制化・義務化されている。

他方、米国においては、CISA（サイバーセキュリティ情報共有法）により、DHS（国土安全保障省）による情報提供システム（AIS）への民間事業者のインシデント報告が義務付けられているが、強制加入規定及び罰則規定がないためすべての重要インフラ事業者をカバーできていない。

これらの実例を踏まえ、我が国においては、英独仏３か国に倣い、重要インフラ事業者に対しサイバーインシデントのサイバーセキュリティ庁への報告を（違反に対する罰則付きで）義務化すべきである。これによって、サイバー攻撃に対応するOODAループの第一段階である、①日々発生している日本や世界でのサイバー攻撃の検知（サイバー空間のモニタリング）を行うことが可能となる。

（4）重要インフラ事業者における情報処理安全確保支援士又は電気通信主任技術者の必置化

迅速かつ適切なサイバー攻撃への対応のためには、重要インフラ事業者におけるサイバーセキュリティ庁との24時間対応の窓口が必要であり、英独仏は重要インフラ事業者にサイバーセキュリティ庁の窓口となる連絡担当者（リエゾン）の配置を義務化している。

我が国においても、サイバーセキュリティ庁からサイバー攻撃に係る情報を受け取り、現場で迅速な対処を行うため、24時間対応の窓口設置を法制化する必要がある。サイバー攻撃への対応においては、機密保持が義務付けられておりサイバー攻撃対処能力の高いセキュリティ専門家が必要であるが、我が国においては、2017年に情報処理安全確保支援士（情確士）制度が発足しこうした有資格者が育成されていることから、重要インフラ事業者の情報システム管理者に情確士の配置を義務付けるべきである。

また、サイバー攻撃への対応や研究開発に当たる専門家は国家の安全保障に関わる機密情報、

企業の重要な顧客情報や知的財産等を取り扱うため、適正に情報を扱う人物であることを担保する必要がある。そのため、情報処理安全確保支援士、サイバーセキュリティ庁においてサイバーセキュリティ業務に携わる者、研究開発に携わる人物については、過去の犯罪歴や国籍、負債の有無、クラッキング活動をしていないか等のセキュリティ・クリアランスを確保できるよう法制化が必要である。

このような制度の導入に合わせて、情報処理安全確保支援士（情確士）に１級、２級、３級などの段階的資格認定を施し、クリアランスの資格を認定したものは１級に認定するなどして、機微な情報を取り扱う資格を持たせるとともに、サイバーセキュリティ関連の正当業務行為（研究のためのウィルス保有や脆弱性調査など）を許可するのも一案であろう。

３. 政府が主体となった産業育成・人材育成を！

（１）サイバーセキュリティ庁を中心とした研究開発環境の整備

重要インフラの保護をはじめとする日本の安全保障のため、また知的財産を守り日本の産業の健全な育成を図るためにはサイバーセキュリティ産業の育成が不可欠である。ちなみに、イスラエルは、研究開発拠点である「サイバースパーク」をテルアビブに設立するなど、政府主導でサイバーセキュリティ産業の育成を行い、既に世界的なサイバーセキュリティ企業が多数誕生している。

このため、我が国においても、同様のサイバーセキュリティ産業の育成を政府主導で最優先に行うべきである。実施にあたっては、ヒト・モノ・情報の集積とこれを可能とするための規制緩和が必要となる。

具体的には、前者については、起業から国際展開まで企業の成長を包括的に支援するためサイバーR&Dセンターの設置（サイバーセキュリティ庁が所管）、企業が安心して製品開発ができる環境を整えるためのサプライチェーンの認証・チェック、国産OS（汎用、脆弱性調査用）の開発と政府への実装等を行う。

後者については、日本においてサイバーセキュリティ産業が発展するためには、「岩盤規制」ならぬ「山脈規制」（何重にも重なる様々な法律による規制）の適用除外が必要であり、大幅な規制緩和が不可欠となっている。しかしながら、情報関係の規制緩和は、実際に社会に与える影響が予測しがたいことから、ヒト・モノ・情報が集積している首都圏近郊にサイバーセキュリティ戦略特区を創設し、試行的な規制緩和（個人情報保護法、不正競争防止法、電気通信事業法、不正アクセス禁止法、マルウェア作成罪の適用除外など）を行い、産業育成を図ることとする。

（２）一元化されたサイバーセキュリティ教育プログラムの提供

不足するサイバーセキュリティ人材の育成のためには集約的かつ長期的視野に立ったカリキュラムが不可欠であり、第2章で見たとおり各国は一貫したサイバーセキュリティ教育フレームワーク及び教育カリキュラムを整備して人材育成に取り組んでいる。また、教育機関の単位認定をサイバーセキュリティ庁と大学が共同で実施し、サイバーセキュリティ人材の学位（certificate）授与を行っている。

このため、我が国においても、一貫したサイバーセキュリティ教育フレームワーク及び教育カリキュラムをサイバーセキュリティ庁及び関係省庁で策定し、大学と共同で学位授与及び資格認定（情確士）を行うべきである。

おわりに

サイバー空間では、国家が関与するサイバー攻撃が激しさを増しつつあり、我が国のサイバー防衛に関する体制・組織の整備は焦眉の急となっています。サイバー空間は、通常の安全保障と異なり、平時における空間の状況把握・分析・判断・対処が重要になっており、各国では軍や情報機関と密接に連動する形で、国を挙げたサイバーセキュリティ体制が構築されています。

笹川平和財団では、2016年度から我が国のサイバーセキュリティにおける様々な課題をテーマに、国内の有識者の方々にご参集いただき、「サイバーセキュリティ研究会」を開催してまいりました。すでにその研究成果の一端は、月例のサイバーセキュリティセミナーの形で、一般に公開してきております。

今般、「サイバーセキュリティ研究会」における有識者の方々の議論を踏まえ、我が国のサイバー防衛に関する体制・組織の整備のあり方として、「サイバーセキュリティ庁を創設すべきである」という本政策提言を、笹川平和財団安全保障グループとして取りまとめさせていただきました。

本政策提言の策定にあたり有益なコメントを頂戴した皆様方に、この場をお借りして深く感謝申し上げます。特に、伊東寛先生、田中達浩先生、土屋大洋先生、名和利男先生、西正典先生、山崎文明先生、湯淺墾道先生、また、お名前をあげることは控えますが、ご指導賜りました有識者の先生方に深く御礼申し上げます。

今回の提言はサイバーセキュリティの側面に光を当て、「サイバーセキュリティ庁の創設を！」という結論とさせていただいております。しかしながら、Society5.0時代を迎える今日、サイバーセキュリティを確実に担保するには、最初から「セキュリティ・バイ・デザイン」の発想で次世代通信基盤を考える必要があり、さらに、政府のITシステムの調達についても最初からセキュリティを念頭に一元的に行う必要があります。将来的には、この「サイバーセキュリティ庁」を、セキュリティのみならず、通信基盤、政府のITシステム調達、サイバーセキュリティを一元的に行う独立した行政庁である「国家サイバー庁」に発展させていくことが、残された課題であると認識しております。

なお、本政策提言の内容の責任は、執筆いたしました笹川平和財団安全保障グループにございますことは、言うまでもないことであります。

本政策提言が、我が国のサイバー空間の安全構築の一助となれば幸いであります。

2018年10月

笹川平和財団安全保障事業グループ

［サイバー空間の防衛力強化プロジェクト　事務局］

佐分利　応貴　　笹川平和財団安全保障事業グループ　グループ長
大澤　　淳　　笹川平和財団安全保障事業グループ　プロジェクト・コーディネーター
下條　　秋太郎　笹川平和財団安全保障事業グループ　アシスタント・プロジェクト・コーディネーター
西嶋　　典子　　笹川平和財団安全保障事業グループ　アシスタント

政策提言　“日本にサイバーセキュリティ庁の創設を!”

2018年10月発行
発行者　公益財団法人　笹川平和財団
〒105-8524　東京都港区虎ノ門1-15-16　笹川平和財団ビル
Tel. 03-5157-5430　URL https://www.spf.org

笹川平和財団