資料１

サイバーセキュリティ戦略（案）

資料１－１　「サイバーセキュリティ戦略（案）」の全体概要

資料１－２　次期サイバーセキュリティ戦略策定までの主要スケジュール（案）

資料１－３　サイバーセキュリティ戦略（案）

資料１－４　サイバーセキュリティ戦略案の作成に際しての高度情報通信ネットワーク社会推進戦略本部意見

資料１－５　サイバーセキュリティ戦略案の作成に際しての国家安全保障会議意見

「サイバーセキュリティ戦略（案）」の全体概要

資料１－１

中長期的

戦略期間

1　策定の趣旨・背景

１．１．　サイバー空間がもたらすパラダイムシフト（サイバー空間では、創意工夫で活動を飛躍的に拡張できる。人類がこれまでに経験したことのないSociety5.0へのパラダイムシフト）

１．２．　2015年以降の状況変化（サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会等を見据えた新たな戦略の必要性）

2　サイバー空間に係る認識

２．１．　サイバー空間がもたらす恩恵

・人工知能（AI）、IoT※などサイバー空間における知見や技術、サービスが社会に定着し、既存構造を覆すイノベーションを牽引。**様々な分野で当然に利用**され、人々に豊かさをもたらしている。

※：Internet of Thingsの略

２．２．　サイバー空間における脅威の深刻化

・技術等を**制御できなくなるおそれは常に内在**。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的な損失が生ずる可能性は拡大

3　本戦略の目的

３．１．　**基本的な立場の堅持**

（１）基本法の目的（２）基本的な理念（「自由、公正かつ安全なサイバー空間」）（３）基本原則（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携）

３．２．　目指すサイバーセキュリティの基本的な在り方

（１）目指す姿（**持続的発展のためのサイバーセキュリティ（「サイバーセキュリティエコシステム」）の推進**）（２）主な観点（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**）

4　目的達成のための施策

経済社会の活力の向上及び持続的発展

１．新たな価値創出を支えるサイバーセキュリティの推進

＜施策例＞・**経営層の意識改革の促進（「費用」から「投資」へ）**
・投資に向けたインセンティブ創出（情報発信・開示による市場の評価、保険の活用）
・セキュリティ・バイ・デザインに基づくサイバーセキュリティビジネスの強化

２．多様なつながりから価値を生み出すサプライチェーンの実現

＜施策例＞・**中小企業を含めたサプライチェーン（機器・データ・サービス等の供給網）におけるサイバーセキュリティ対策指針の策定**

３．安全なIoTシステムの構築

＜施策例＞・IoTシステムにおけるセキュリティの体系の整備と国際標準化
・**IoT機器の脆弱性対策モデルの構築・国際発信**

等

国民が安全で安心して暮らせる社会の実現

１．国民・社会を守るための取組
＜施策例＞・脅威に対する事前の防御（**積極的サイバー防御**）策の構築
・サイバー犯罪への対策

２．官民一体となった重要インフラの防護
＜施策例＞・安全基準等の改善・浸透（サイバーセキュリティ対策の**関係法令等における保安規制としての位置付け**）
・地方公共団体のセキュリティ強化・充実

３．政府機関等におけるセキュリティ強化・充実
＜施策例＞・**情報システムの状態のリアルタイム管理の強化**
・先端技術の活用による先取り対応への挑戦

４．大学等における安全・安心な教育・研究環境の確保
＜施策例＞・**大学等**の多様性を踏まえた対策の推進

５．2020年東京大会とその後を見据えた取組
＜施策例＞・**サイバーセキュリティ対処調整センターの構築の推進**
・成果のレガシーとしての活用

６．従来の枠を超えた情報共有・連携体制の構築
＜施策例＞・**多様な主体の情報共有・連携の推進**

７．大規模サイバー攻撃事態等への対処態勢の強化
＜施策例＞・**実空間とサイバー空間の双方の危機管理に臨むための大規模サイバー攻撃事態等への対処態勢の強化**

等

国際社会の平和・安定及び我が国の安全保障

１．自由、公正かつ安全なサイバー空間の堅持
＜施策例＞・**自由、公正かつ安全なサイバー空間**の理念の発信
・サイバー空間における法の支配の推進

２．我が国の防御力・抑止力・状況把握力の強化
＜施策例＞・国家の**強靭性の確保**（①任務保証、②我が国の先端技術・防衛関連技術の防護、③サイバー空間を悪用したテロ組織の活動への対策）
・サイバー攻撃に対する**抑止力の向上**（①実効的な抑止のための対応、②信頼醸成措置）
・サイバー空間の**状況把握の強化**（①関係機関の能力向上、②脅威情報連携）

３．国際協力・連携
＜施策例＞・**知見の共有・政策調整**
・事故対応等に係る国際連携の強化
・能力構築支援

等

横断的施策

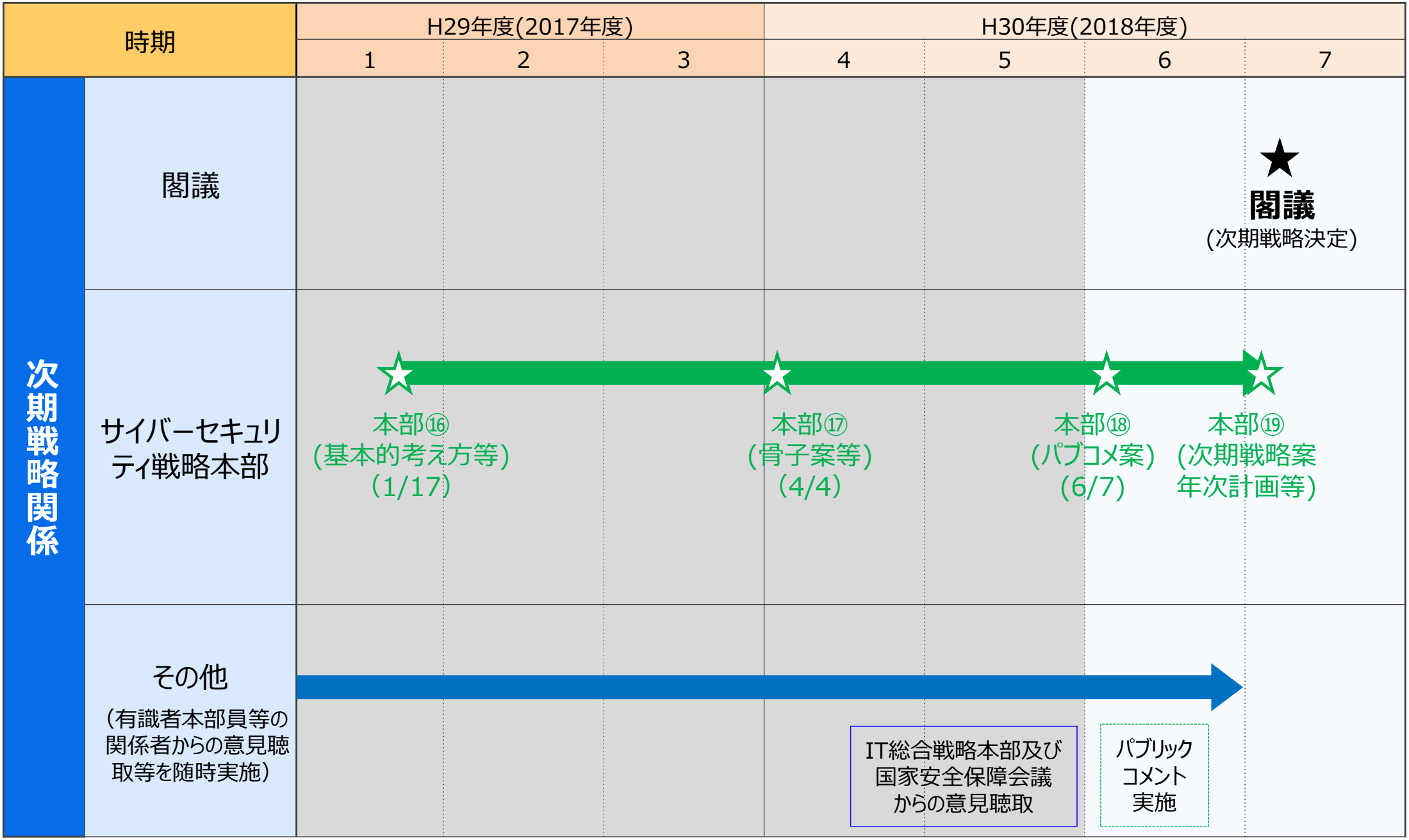
人材育成・確保	＜施策例＞**戦略マネジメント層の育成・定着**、実務者層・技術者層の育成（**高度人材**含む）、人材育成基盤の整備、**政府人材**の確保・育成の強化、国際連携の推進
研究開発の推進	＜施策例＞実践的な研究開発の推進（**検知・防御等の能力向上、不正プログラム等の技術的検証**を行うための体制整備）、**AI等**中長期的な技術・社会の進化を視野に入れた対応
全員参加による協働	＜施策例＞サイバーセキュリティの普及啓発に向けた**アクションプランの策定、国民への情報発信**（サイバーセキュリティ月間の充実等）、サイバーセキュリティ教育の推進

5　推進体制

本戦略の実現に向け、サイバーセキュリティ戦略本部の下、**内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化**を図るとともに、同センターが、各府省庁間の総合調整、産学官民連携の促進の要となる主導的役割を担う。また、危機管理対応についても一層の強化　等

次期サイバーセキュリティ戦略策定までの主要スケジュール（案）

資料１－２



資料１－３

（案）

サイバーセキュリティ戦略

平成 30 年＊月＊日

この戦略は、サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 12 条第 4 項の規定に基づき、国会に報告するものである。

目次

1. 策定の趣旨・背景

1.1. サイバー空間がもたらすパラダイムシフト

現代科学の知見を基礎としたデジタル技術の急速な進展により生み出された、インターネットを中核的な基盤とするサイバー空間は、民間を中心とする多様な主体[1]の自律的な取組により、グローバルな拡張・発展を続けてきた。

こうした発展を遂げた空間は、場所や時間の制約にとらわれず、国境を越えて、量・質ともに多種多様な情報・データを自由に生成・共有・分析することが可能な場であり、流通する場でもある。この空間で活動する主体は、誰もが他の主体と関わり合いながら、新たな価値を生み出していく可能性がある。

こうした特徴を持つサイバー空間は、技術革新や新たなビジネスモデルなどの知的資産を生み出す場であり、今後の経済社会の持続的な発展の基盤でもある。また、この空間は自由主義、民主主義、文化発展も支えている。この空間では、人間は創意工夫によって活動を飛躍的に拡張させることができる[2]。すなわち、サイバー空間は「無限の価値を産むフロンティア」である。我が国は、こうしたサイバー空間を堅持するため、採り得るあらゆる手段により、サイバーセキュリティに関する取組を行っていく。

今後、サイバー空間を前提とする人工知能（以下「AI」という。）などの計算機科学の知見の更なる進展により、新たな製品・サービスの創出が期待される。新たな製品・サービスの出現は、人々の日常の行動や生活環境を変えることにより意識の変化をもたらし、それが既存の手続、モデル、組織などの社会システムや産業構造の変革を促していく起点になる。これまで人類が経験してきた狩猟社会、農耕社会、工業社会、情報社会から「Society5.0[3]」へのパラダイムシフトが生じつつある中、今後のサイバーセキュリティの在り方についても、このような変革の潮流を俯瞰しながら、検討する必要がある。

1　サイバーセキュリティ基本法第16条において、「国、地方公共団体、重要社会基盤事業者、サイバー関連事業者等の多様な主体」と規定されている。サイバー関連事業者については、同法第７条で「サイバー関連事業者（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、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。以下同じ。）」と規定されている。

2　サイバーセキュリティ戦略（2015年９月）において、この特徴が社会に与えている大きな影響を、グーテンベルグの活版印刷が知の爆発を引き起こした歴史にたとえている。

3　狩猟社会、農耕社会、工業社会、情報社会に続く、人類史上５番目の新しい社会。新しい価値やサービスが次々と創出され、社会の主体たる人々に豊かさをもたらしていく。（出典：未来投資戦略2017（平成29年6月9日閣議決定））

1.2. 2015 年以降の状況変化

サイバーセキュリティ基本法[4](以下「基本法」という。)に基づき、サイバーセキュリティ戦略本部(以下「本部」という。)での検討を経て、2015 年９月に閣議決定されたサイバーセキュリティ戦略(以下「2015 年戦略」という。)は、３年間のサイバーセキュリティに関する施策の基本的な方針である。

2015 年戦略の策定後、官民データ活用推進基本法[5]や改正個人情報保護法[6]等のデータ利活用に関する一定の法的な基盤が整備された。また、政府は、サイバー空間とフィジカル(実)空間を高度に融合させることにより、経済的発展と社会的課題の解決を両立する人間中心の社会[7]を目指す方針を決定した。こうした中、現在、実空間においてセンサやデバイスを介して生成された大量のデータが、サイバー空間において集積・分析されている。そして、そのデータを活用することにより付加価値をつけた新たな製品やサービスが実空間で提供されるという循環が様々な分野で始まっており、進展している。もはや、サイバー空間と実空間が独立して存在するのではなく、相互に作用する状態が生じており、両者を分けて捉えることはできない。むしろ、サイバー空間と実空間は一体として進化を続ける有機的なものとして捉えるべきである。

こうしたサイバー空間と実空間の一体化に伴い、社会に豊かさがもたらされる可能性が飛躍的に高まる。一方で、悪意ある主体がサイバー空間を利用する機会も増大し、実空間での経済的・社会的な損失のリスクが指数関数的に拡大・加速することが予想される。

こうした中、経済社会が、人々に豊かさをもたらし、持続的に発展するためには、その基盤であるサイバー空間のサイバーセキュリティが確保されつつ、自律的・持続的に進化・発展していく必要がある。サイバー空間の脅威に対して、一部の国においては、国家が優越的な地位から管理・統制することを重視するという潮流が出てきている。しかしながら、国家によるサイバー空間の管理・統制を強めることは、このような自律的・持続的な発展の可能性を閉ざすことになる。全ての主体の自律的な取組により発展してきたサイバー空間を尊重し、連携・協調してサイバーセキュリティの確保に取り組む必要がある[8]。

4　平成26年11月６日成立。サイバーセキュリティという概念を法的に位置付け、各主体の責務などを明確化した。

5　平成28年12月７日成立。官民データの推進に関する基本理念等が定められた。

6　平成27年９月３日成立。平成29年５月30日全面施行。適切に匿名加工する前提で個人に関わるデータの利活用を進めるための整備が行われた。

7　Society5.0の内容(出典：科学技術イノベーション総合戦略2017(平成29年６月２日閣議決定)、未来投資戦略2017(平成29年６月９日閣議決定))

8　2015年９月に国連サミットで採択された「「持続可能な開発のための2030アジェンダ」、持続可能な開発目標(SDGｓ(Sustainable Development Goals))」は、持続可能な世界を実現するための17の目標を設定し、「誰ひとり取り残さない」社会の実現を目指すとしている。持続的な開発を目指すという点や、全ての主体が連携・協調して取り組むという点で、こうしたサイバーセキュリティの取組方針と共通点があると考えられる。

こうした認識の下、我が国は、2020 年東京オリンピック・パラリンピック競技大会（以下「2020 年東京大会」という。）等の国際的なイベントを控えていることを見据え、2020 年以降の目指すべき姿を念頭に置きつつ、サイバーセキュリティの基本的な在り方を明確にしたうえで、新たに取り組むべき課題を明らかにし、速やかに対策を実施することで、サイバーセキュリティ対策に万全を期していく。

本戦略は、こうした今後のサイバーセキュリティに係る我が国としての基本的な立場や在り方を明らかにするとともに、今後３年間の諸施策の目標及び実施方針を国内外に明確に示すことにより、共通の理解と行動の基礎となるものである。

2. サイバー空間に係る認識

AI、IoT[9]、Fintech[10]、ロボティクス、３D プリンター[11]、AR/VR[12]など、サイバー空間における知見や技術・サービスが社会に定着し、経済社会活動・国民生活の既存構造に変革をもたらすイノベーションを牽引しており、この結果、サイバー空間と実空間の一体化が進展している[13]。

本戦略の策定の前提として、こうしたサイバー空間がもたらす「恩恵」とこの空間における「脅威」の状況を的確に認識する必要がある。サイバー空間の知見や技術・サービスの恩恵を享受するためには、これらに常に内在している不確実さを制御することが不可欠であり、制御できない場合にはサイバーセキュリティに係る脅威が一気に高まるおそれがある。

2.1. サイバー空間がもたらす恩恵

サイバー空間における技術・サービスは、様々な分野で当然に利用されるようになってきている状況である。今後も、サイバー空間が持続的に発展することにより、人々に豊かさをもたらすことが予想される。

(1) サイバー空間におけるサービスの進展と社会への定着

我が国におけるインターネット利用者数が増加し、その普及率は上昇している[14]。また、デバイス面ではスマートフォンの個人保有率が大きく伸び[15]、インターネット利用率は増加している[16]。SNS の利用割合も伸びており[17]、サイバー空間上で簡単にコミュニケーションを行える環境が整った状況である。このようにサイバー空間におけるサービスが社会に定着していき、自由な情報の流通にとどまらず、多様なコミュニティの形成、情報共有が進んでいる。

経済活動においても、ネットショッピングや株取引・オンラインバンキングの利用

9 Internet of Thingsの略
10 Finance（金融）とTechnology（技術）を組み合わせた造語。ブロックチェーンやビッグデータ、AIといった新たな技術を活用し、多くが急速に普及したスマートフォンやタブレット等を通じて行われる革新的な金融サービス（出典：平成29年版　情報通信白書）
11 通常の紙に平面（二次元）的に印刷するプリンターに対して、３DCAD、３DCGデータを元に立体（３次元のオブジェクト）を造形する機器（出典：一般社団法人日本３Dプリンティング産業技術協会のWebサイト）
12 Augmented Reality/Virtual Reality（拡張現実/仮想現実）
13 2015年戦略では、「実空間のモノやヒトが、サイバー空間上の情報の自由な流通とデータの正確な通信により物理的な制約を超えて多層的につながる（連接する）ことで、実空間とサイバー空間の融合が高度に深化した社会、すなわち「連接融合情報社会」が到来しつつある。」としている。
14 インターネット人口普及率（2014年末82.8%→2016年末83.5%）（出典：平成29年版　情報通信白書）
15 スマートフォンの個人保有率（2014年末44.7%→2016年末56.8%）（出典：平成29年版　情報通信白書）
16 インターネット利用率（2015年末83.0%→2016年末83.5%（出典：平成29年版　情報通信白書）
17 代表的SNS（LINE、Facebook、Twitter、mixi、Mobage、GREE）の利用率※の推移（全体）（2014年末62.3%→2016年末71.2%）（出典：平成29年版　情報通信白書）※６つのいずれかを使用

が進んでいるとともに、Fintech、シェアリングエコノミー[18]の分野で新サービスが次々登場し、これらがイノベーションを牽引している。また、生産年齢人口の減少、地域の高齢化といった社会的課題に関連する医療・介護、福祉、教育等の分野における情報通信技術の活用も進展している。

(2) AIの劇的な進化

AIについては、昨今の計算機科学の知見が進展し、大量のデータが必要である機械学習の分野の研究が進展し、深層学習という手法が登場した。深層学習は、その登場により、AIの画像解析の精度を飛躍的に向上させ、製品の異常検知、ガンの診断、投資判断、翻訳等の精度を高め、経済社会において様々な機能の効率化・高品質化を加速させ、既に幅広い産業に応用され始めている。サイバーセキュリティにおいても、こうした可能性を持つAIは、例えば、マルウェアの自動検知などの対策の自動化に活用されつつある。

深層学習によるAIの進化は、機械・ロボットの世界でカンブリア爆発にたとえられるほどの変化をもたらすとの指摘[19]がある。深層学習では、従来の機械学習で人間が行う必要のあった識別・判断のための特徴量[20]の設計について、コンピュータが自ら特徴量を導き出すことができるようになり、これがAIの進化として着目されている。音楽、絵画、小説等の創作物や自動運転等のサービスにつながる出力（例：判定・判断・提案結果）について、人間が創作的な寄与をせずに、AIがこれらを自律的に生成する世界が現実的になりつつある。こうしたAIが権利侵害や事故を起こした場合の責任を誰が負うのかといった問題が生ずる可能性があることも指摘[21]されている。

こうしたAIの進展は、今後、AIを活用した全く新しい製品・サービスを出現させ、人々の日常の行動や生活環境を変えることにより、これまでの人間の物事に関する認識に変化をもたらし、それが既存の社会システムや産業構造の変革を促すことも予想される。

(3) IoTの進展

18　個人等が保有する活用可能な資産等を、インターネット上のマッチングプラットフォームを介して他の個人等も利用可能とする経済活性化活動（出典：平成29年版　情報通信白書）

19　「カンブリア爆発　５億4200万年前から５億3000万年前の間に突如として今日見られる動物の「門」が出そろった現象。古代生物学者アンドリュー・パーカーは、「眼の誕生」がその原因だったという説を提唱。ディープラーニングにより、見えるようになる。さらに次に何が起こるかを予想して動けるようになる。眼を持った機械が誕生する。機械・ロボットの世界でのカンブリア爆発が起こる。」（出典：平成29年２月３日日本経済再生本部第4次産業革命人材育成推進会議（第２回）資料１）

20　対象を認識する際に注目すべき特徴は何かを定量的に表すこと。ディープラーニング以前は人間の手で特徴量を設計していたが、ディープラーニングによって画像認識や音声認識などでコンピュータが自ら特徴量をつくりだすことが可能となった。（出典：平成28年版　情報通信白書）

21　知的財産戦略本部「新たな情報財検討委員会報告書」（平成29年３月）参照

センサの小型軽量化、低廉化が進み、全てのモノがネットワークにつながるIoTの爆発的な普及が進んでいる。家電、自動車、ロボット、スマートメーター等のモノの活用だけでなく、IoT 機器で得られるデータを利活用した新たなビジネスやサービスが創出されつつある。

具体的に、電子行政やスマートシティ、ものづくり、自動運転、金融、健康・医療・介護の分野[22]で生産性の向上やサービスの高付加価値化を進める動きがあり、そのサプライチェーン[23]の中でのデータ利活用が進むと予想される。また、サイバー空間を介して、分野を越えて協業を行ういわゆるオープンイノベーション[24]が進み、データを共有して分析することにより、人々に豊かさをもたらす新たなサービスが次々と創出される期待がある。

2.2. サイバー空間における脅威の深刻化

AI や IoT などの技術・サービスが人々に多くの恩恵をもたらす可能性がある一方で、こうした技術・サービスを提供する者がこれらを制御できなくなるおそれは常に内在しており、その場合には、逆に、多大な経済的・社会的な損失が生じ得る。サイバー空間と実空間の一体化が進展する中、こうした深刻な影響が生ずる可能性は指数関数的に拡大している。また、この空間は、場所・時間の制約を受けずに、悪意ある主体を含む全ての者が、新たな情報通信技術を悪用・濫用し、容易に活動できる場である。悪意ある主体とそのグループは、攻撃プログラムを含むデータや情報を容易に複製・流通させることが可能というデジタル技術の特性だけでなく、進展するAIやブロックチェーン[25]等の技術も柔軟に取り入れて自由に利用できる。このため、攻撃者には防御側と比べて非対称な優位性があり、特に、防御側の体制が従前の制度や技術体系を前提としている場合には、その優位性が高まると考えられる。

こうした中、実際に、IoT、仮想通貨を含むFintech、重要インフラ、サプライチェーンを狙った攻撃等[26]により、従来の情報漏えいに加えて、直接的な金銭被害、業務・サービス障害が国内外で生じ、経済社会の持続的な発展や国民生活の安全・安心等を脅かす

22　世界最先端IT国家創造宣言・官民データ活用推進基本計画（平成29年５月30日閣議決定）において、我が国が集中的に対応すべき、①経済再生・財政健全化、②地域の活性化、③国民生活の安全・安心の確保といった諸課題に対し、官民データ利活用の推進等を図ることで、その解決が期待される８つの分野（電子行政、健康・医療・介護、観光、金融、農林水産、ものづくり、インフラ・防災・減災等、移動）が重点分野として指定されている。

23　供給網。取引先との間の受発注、資材の調達から在庫管理、製品の配達まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと

24　組織内部のイノベーションを促進するために、意図的かつ積極的に内部の技術やアイディアなどの資源の流出入を活用し、その結果組織内で創出したイノベーションを組織外に展開する市場機会を増やすこと

25　ブロックチェーン技術のこと。電子署名とハッシュポインタを使用して改ざん検出が容易なデータ構造を持ち、当該データをネットワーク上に分散する多数のノードに保持させることで、高可用性及びデータ同一性等を実現する技術（出典：日本ブロックチェーン協会「ブロックチェーンの定義」）

26　バングラディシュ中央銀行がハッキングを受け、約8,100万ドルが不正送金。IoT機器に感染し史上最大規模のDDoS攻撃を仕掛ける新型マルウェア（Mirai）の登場（2016年９月）。ウクライナの国営電力会社に変電所へのサイバー攻撃（2016年12月）等

事例が生じている。また、国家の関与が疑われる大規模な事案も発生している。

今後、実空間との一体化が進展するサイバー空間において、官民のデータ利活用が更に進むと、IoT、サプライチェーン、オープンイノベーションの脆弱な部分を狙う動きや意図しない動きが発生する懸念は高まると考えられる。政府機関や重要インフラ事業者だけでなく、それ以外の事業者及び個人に対しても、深刻な影響が生ずる可能性が高まることが予想される。

(1) 業務・機能・サービス障害による社会への多大な影響

重要インフラサービスの障害やIoT機器の意図しない作動により、様々な業務・機能・サービス障害が生じた場合、社会に大きな影響が生じ、国家安全保障上の問題に発展する可能性もある。今後、サイバー空間と実空間の一体化が更に進めば、社会の機能障害、人命や生活へのリスクを含む国民の安全・安心、国家や民主主義の根幹をも揺るがす事態が生じるおそれもある。

(2) 情報の毀損及び漏えいによる競争力低下

IoTの爆発的な普及や、オープンデータ化が進む中、データを利活用した新たなサービスが増えていく。また、データの分析に当たってAIの活用が進む。深層学習に用いるデータはAIの性能に直結するものであり、データの重要性がますます高まる中、データの真正性[27]・完全性[28]が毀損されると、データを利活用したサービスの信頼が揺らぐことになる。

また、個人情報、営業秘密、価値あるデータを始めとした情報の漏えいは、損害賠償請求の対象となるおそれがあるだけでなく、組織・企業の社会的評価・信頼の低下を招くおそれがある。これらは、一度流出すれば取り返しがつかないものであり、組織・企業の競争力の低下に直接つながるものである。

(3) 金銭の窃取・詐取等の損害

サイバーセキュリティに関する基本的な対策の不備等により、仮想通貨交換業者への不正アクセスやビジネスメール詐欺で巨額の金銭的な被害が発生した事例が生じている。今後、経済社会がサイバー空間にますます依存していくことが想定される中、サイバーセキュリティ対策の不備が、金銭的な損害を直接引き起こし、拡大することが予想される。

27 ある主体又は資源が、主張どおりであることを確実にする特性
28 情報に関して破壊、改ざん又は消去されていないこと

3. 本戦略の目的

サイバー空間に係る現状認識の下、その将来像を視野に入れ、本戦略の目的として、以下のとおり、基本的な立場を堅持することや、こうした立場を踏まえて目指す「サイバーセキュリティの基本的な在り方」を示す。

3.1. 基本的な立場の堅持

我が国は、「基本法の目的」や 2015 年戦略で示した「基本的な理念」及び「基本原則」といった基本的な立場を堅持する。また、このような立場から、引き続き、悪意ある主体の行動を抑制し、国民の安全・権利を保障するため、政治・経済・技術・法律・外交その他の採り得る全ての有効な手段を選択肢として保持する。

(1) 基本法の目的

基本法は、「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に寄与すること」を目的としている[29]。本戦略においても、この３つの領域に政策目的を整理し、それぞれの目的に沿って、施策を推進することとする。

(2) 基本的な理念

基本法の目的に寄与するため、「自由、公正かつ安全なサイバー空間」を目指すこととし、この基本的な理念を堅持する。これは、サイバー空間で活動しようとする全ての主体が、正当な理由なく差別や排除されずに、表現の自由や経済活動の自由が保障され、情報・財産の窃取などの不正な活動を許さない安全な空間である。

(3) 基本原則

サイバーセキュリティに関する施策の立案及び実施に当たって従うべき基本原則については、2015 年戦略で掲げた「①情報の自由な流通の確保」、「②法の支配」、「③開放性」、「④自律性」、「⑤多様な主体の連携」の５つの原則を堅持する。

① 情報の自由な流通の確保

サイバー空間が創意工夫の場として持続的に発展していくためには、発信した情報がその途中で不当に検閲されず、また、不正に改変されずに、意図した受信者へ届く世界が作られ、維持されるべきである[30]。また、プライバシーへの配慮も引き続きなされるべきである。なお、情報の自由な流通で他者の権利・利益をみだりに害すことが

29 基本法第１条において、「この法律は、（中略）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。」と規定されている。

30 基本法第１条において、「情報の自由な流通を確保しつつ」と規定されている。

ないようにしなければならない。

② 法の支配

サイバー空間と実空間の一体化が進展する中、サイバー空間においても、実空間と同様に、法の支配が貫徹されるべきである。この空間では、国内においては法令を含む各種ルールや規範が適用されている。また、同様に、この空間では、既存の国際法が適用される。今後、サイバー空間が安全で信頼できる空間として持続的に発展していくためには、引き続き、既存の国際法の適用、規範の形成が不可欠である。

③ 開放性

サイバー空間が新たな価値を生み出す空間として持続的に発展していくために、多種多様なアイディアや知識が結びつく可能性を制限することなく、サイバー空間は全ての主体に開かれたものであるべきである。サイバー空間が一部の主体に占有されることがあってはならないという立場を堅持していく[31]。

④ 自律性

サイバー空間は多様な主体の自律的な取組により発展を遂げてきた。サイバー空間が秩序と創造性が共存する空間として持続的に発展していくためには、国家が秩序維持の役割を全て担うことは不適切であり、不可能である。サイバー空間の秩序維持に当たっては、様々な社会システムがそれぞれの任務・機能を自律的に実現することにより、悪意ある主体の行動を抑止し、対応する以外にはなく、これを促進していく[32]。

⑤ 多様な主体の連携

サイバー空間は、国、地方公共団体、重要インフラ事業者、サイバー関連事業者その他の事業者、教育研究機関、個人などの多様な主体が活動することにより構築される多次元的な世界である。こうしたサイバー空間が持続的に発展していくためには、これら全ての主体が自覚的にそれぞれの役割や責務を果たすことが必要である。そのためには、個々の努力にとどまらず、連携・協働することが求められる。国は、連携・協働を促す役割を担っており、その役割を果たすことができるように施策を推進していく[33]。

31　高度情報通信ネットワーク社会形成基本法第３条において、「すべての国民が、インターネットその他の高度情報通信ネットワークを容易にかつ主体的に利用する機会を有し」と規定されている。

32　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」と規定されている。

33　基本法第３条第１項において、「サイバーセキュリティに対する脅威に対して、（中略）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。」と規定されている。

3.2. 目指すサイバーセキュリティの基本的な在り方

前述の基本的な立場を踏まえ、「サイバーセキュリティの基本的な在り方」として、以下のとおり、サイバーセキュリティの取組により目指す姿や、その取組を進めるに当たって求められる３つの観点を示す。

(1) 目指す姿

我が国は、「無限の価値を産むフロンティア」であるサイバー空間が持続的に発展し、新しい価値やサービスが次々と創出されて人々に豊かさをもたらす社会[34]の実現を目指している。

こうした社会の実現に寄与するため、サイバー空間は、全ての主体が新たな価値の創造に参画することで発展していくことが必要である。この発展を持続的に支えるためには、生物における免疫系のように、全ての主体が、サイバーセキュリティについて自らの役割を認識し、サイバーセキュリティに関する取組を自律的に行うことが求められる。

このような視点に立って、サイバーセキュリティの取組を進めるに当たって、以下のように取り組むこととする。

具体的には、３つの観点（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）からサイバーセキュリティに関する官民の取組を推進することとし、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というものである。

このように、全ての主体が、サイバーセキュリティに関する取組を自律的に行いつつ、相互に影響を及ぼし合いながら、サイバー空間が進化していく姿を、持続的に発展していく一種の生態系にたとえて、「サイバーセキュリティエコシステム」と呼称することとする。

(2) ３つの観点

① サービス提供者の任務保証

～業務・サービスの着実な遂行～

「任務保証」とは、企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保することである。その際には、一部の専門家に依存するのではなく、各々の組織の「任務」に該当する業務・サービスを遂行する観点から、その責任を有する者が主体的にサイバーセキュリティの確保に取り組

34 Society5.0の内容（出典：科学技術イノベーション総合戦略2017（平成29年６月２日閣議決定）、未来投資戦略2017（平成29年６月９日閣議決定））

むことが肝要である。

すなわち、これは、サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方である。

② リスクマネジメント

～不確実性の評価と適切な対応～

「リスクマネジメント」とは、組織が担う「任務」の内容に応じて、リスク[35]を特定・分析・評価し、リスクを許容し得る程度まで低減する対応をしていくことである。これは、サイバー空間に本質的にある不確実さから、不可避的に導かれる観点である。

リスクは、「目的に対する不確実さの影響」[36]と定義され、目的を設定して初めて測れるものである。したがって、リスクは、組織の目的によって、その評価や対応が変わってくるものである。また、リスクマネジメントは「リスクについて組織を指揮統制するための調整された活動」[37]と定義されており、リスクの特定・分析・評価という個別の活動を指すのではなく、組織を指揮統制して、組織が有する有限の資源を適切に分配し、リスクに対応していく一連の活動の全体を意味している。

各々の組織の「任務」に該当する業務・サービスを認識せずに、リスクを過小評価して、サイバーセキュリティに必要な資源を分配しなければ組織の存立そのものに関わるような事態を招くおそれがある。一方で、リスクを過大評価して、サイバーセキュリティに過剰に資源を分配すれば組織の業務・サービスの遂行と持続的な成長に支障が生ずることとなる。

このようなリスクマネジメントの考え方は、個人においても、サイバー空間の知見や技術・サービスを活用して恩恵を享受している以上、求められるものである。

恩恵の享受に当たっては、その前提となる技術・サービスを制御できなくなるおそれというリスクが発生するのが一般的である。その際、機械的な予測は成り立たず、完全なリスクの除去は不可能であることから、リスクの性格や影響の現れ方に応じて適切に対処し、その効用と比較してセキュリティリスクを許容し得る程度まで低減していくという課題への対処が求められる。

③ 参加・連携・協働

～個人・組織による平時からの対策と連携・協働～

35 プラス及びマイナスの両面がある不確実性を意味することに留意
36 国際標準化機構（ISO）の定義
37 国際標準化機構（ISO）の定義

「参加・連携・協働」とは、サイバー空間の脅威から生じ得る被害やその拡大を防止するため、個人又は組織各々が、平時から講じる基本的な取組である。サイバー空間で活動する主体は、誰もが、その恩恵として新たな価値を生み出す可能性があり、内在するリスクから発生する脅威にさらされる可能性がある。このような観点から、サービスを提供する組織だけでなく、個人においても、基本的な取組を平時から行う必要がある。

具体的には、不正プログラムからの防御、脆弱性の解消、認証における信頼性確保、個人情報の適切な管理等に関する対策が挙げられる。こうした取組は、実空間における公衆衛生活動や交通安全活動にたとえられる。

しかし、いつでもどこでもサイバー攻撃が生じるなど脅威が日常化していく中で、個々の努力による取組のみでは対応が困難であり、その取組を補強するため、組織を含む他者による積極的な助けも必要となる。

このため、皆が力を合わせて取り組むこと、すなわち協働が求められる。サイバー空間に関わる個人又は組織各々が、個々の努力で取り組むだけでなく、平時においても事案発生時においても、情報の共有を行い、個人と組織間で相互に連携・協働することをサイバー空間における新たな公衆衛生活動と捉えて、基本的な取組と位置付けていく必要がある。

我が国は、こうした基本的な取組を推進するため、官民連携で支援することが求められる。特に、国は、基本原則に掲げた「多様な主体の連携」の原則に基づき、連携・協働を促す役割を平時から積極的に担うことが求められる。

4. 目的達成のための施策

本戦略の目的を達成するため、戦略が寄与する政策領域ごとに、今後３年間に執るべき諸施策の目標や実施方針を示す。各施策は、前述の基本的な立場やサイバーセキュリティの基本的な在り方で示した３つの観点を踏まえたものであることが求められる。

4.1. 経済社会の活力の向上及び持続的発展

近年、企業においては、パソコン・スマートフォンを始めとするデジタル端末やインターネットの活用による業務の生産性の向上にとどまらず、経営改革や革新的なサービスの創出といった新たな価値を生み出す動きが進展している。サイバーセキュリティ対策をやむを得ない「費用」ではなく、こうした動きを支える基盤としての「投資」であると捉えて、一体的に取り組むことは、産業の成長及び国際競争力の強化につながり、我が国の経済社会の活力の向上及び持続的発展の観点から重要である。

4.1.1　新たな価値創出を支えるサイバーセキュリティの推進

サイバー空間と実空間の一体化が進展していく中で、企業が直面するサイバーセキュリティリスクは、これまで以上に高まっていく。こうした中、企業におけるサイバーセキュリティに対する問題意識は、一部の業種や大企業を中心として高まっている。今後は、全ての産業分野において、企業が事業継続を確固なものとしつつ新たな価値を創出していくためには、サイバーセキュリティに取り組む必要があるとの認識を広げ、取組を促進していく必要がある。

その際には、サイバーセキュリティに係るリスクは企業が直面する様々なリスクの一つであり、その対策をリスクマネジメントの一環として捉え、業種・業態等の状況に応じて、自然な形で対策が組織に浸透していくことが重要である。

(1)　経営層の意識改革

サイバーセキュリティ対策については、その取組自体が利益を生むものではないとの考え方が未だ支配的であると考えられる。この背景には、サイバー空間は自由に何の備えもなく利用できるものであり、散発的にしか起こらない、経営に対して影響が生じるような攻撃への対処は「費用」でしかないという考え方がある。しかしながら、サイバー空間の利用が急速に進展する中、自由であるがゆえに常に脅威が潜んでいるという認識に立って、そのための備えをすることが必須である。また、企業においては、サイバーセキュリティ対策の組織上の位置付けが明確になっていないと取組が進みにくいという側面がある。このため、経営層が、サイバーセキュリティ対策をやむを得ない「費用」ではなく、事業継続や新たな価値創出のために不可欠な「投資」であると捉えられるようにするため、経営層の意識改革が不可欠である。

具体的には、経営層は、取締役会等を通じたサイバーセキュリティに関する積極的な関与が期待されるとともに、リスクマネジメントのために必要となるサイバーセキュリティに関する一定の知識・能力を身につけることが求められる。その際、経営層に深い技術的な知識やスキルを期待することは必ずしも現実的ではない。このため、経営戦略、事業戦略におけるサイバーセキュリティのリスクを認識し、経営層の方針を踏まえた対策を立案し、実務者・技術者を指導できる人材（いわゆる「戦略マネジメント層」）を確保することが重要である。また、経営層は、自社の対策だけでなく、外部委託先やサプライチェーン全体を視野に入れ、リスクマネジメントとして相応しいレベルの対策ができるような体制を整備するとともに、株主等に対してサイバー空間を活用したビジネスの恩恵とリスクを説明できるようにする必要がある。

このような状況を踏まえ、官民が連携して、経営層に対してサイバーセキュリティ対策に関する説明や議論ができる人材を発掘・育成するとともに、経営層向けセミナー等を開催し、経営層の意識改革を促していく。また、国は、サイバーセキュリティに取り組む企業による宣言の促進や、類似の企業の対策状況と比較することで、自社に必要な対策を可視化するためのツールの整備など、経営層に分かりやすくサイバーセキュリティ対策を訴求するための施策を推進する。また、学会等と連携しつつ、企業がサイバーセキュリティ対策の実施において参照すべき法制度に関する整理を行う。

(2) サイバーセキュリティに対する投資の推進

企業がサイバーセキュリティに関わる取組を継続的に実施するためには、それに対応する経営上のインセンティブがあることが重要である。すなわち、財務的な観点を含め、サイバーセキュリティに係るリスクとその対策が可視化され、経営層がその現状を認識し、更に必要な具体的な対策を検討・導入するとともに、市場がその取組を企業価値の向上につながるものとして評価し、サイバーセキュリティに対する投資へのインセンティブが継続的に生まれる、という好循環が形成されることが望ましい。

このため、投資家を意識して、企業が積極的にサイバーセキュリティに関する取組について情報発信・開示を行うことが重要であり、国は、ベストプラクティスの共有やガイドラインを策定するとともに、情報発信・開示の状況についての継続的な把握・評価に取り組む。加えて、投資家が企業経営層のサイバーセキュリティに関する取組を評価できるような仕組みづくりを進めていくことも必要である。

また、企業に対するサイバーセキュリティの促進策について、サイバーセキュリティに対する投資のインセンティブが効果的に機能するよう、国はその活用状況をフォローしつつ、必要に応じて所要の措置を検討する。

このほか、サイバーセキュリティのリスクマネジメント手段の一つとして、保険の活用が広がっているが、サイバーセキュリティ対策の実施状況に応じて、適切に保険料が算定される仕組みにより、リスクへの備えに対するコストが明確になっていくため、投資が進めやすくなる可能性がある。こうした点を踏まえ、官民が連携してサイバーセキュリティにおける保険の活用を推進するための方策について検討を行う。

(3) 先端技術を利活用したイノベーションを支えるサイバーセキュリティビジネスの強化

企業が新たな価値を創出するためには、IoT、AI、VR、ブロックチェーン、次世代通信技術などの先端技術の利活用が不可欠となる場合が多い。一方、こうした技術の活用は、これまでになかった新たな脆弱性[38]を生み、それが悪用されることで想定外のリスクが発生する可能性がある。このため、リスクの想定を先取りし、サイバーセキュリティ対策をモノやサービス等を創出する過程において可能な限りあらかじめ組み込んでおくこと（セキュリティ・バイ・デザイン）によって、サイバーセキュリティに関する品質の高いモノやサービス等を実現することが期待される。また、こうした取組は、我が国のモノやサービス等に対する信頼の向上につながるだけでなく、我が国が目指す質の高いインフラの海外展開の推進にもつながるものである。

一方、企業がこのような取組を進めようとしても、サイバーセキュリティに関する専門性を有していないなどの理由により、容易に進められない可能性があることに加え、国際競争力の強化や真正性・信頼性の検証が困難なセキュリティ製品・サービスへの依存を回避する観点から、我が国において具体的な解決策を提供できるサイバーセキュリティビジネスの強化が必要である。

このようなニーズに応えるため、大企業のみならずベンチャー企業を含め、先端技術による新たな価値創出に向けたチャレンジを支えられるよう、官民が連携して、機動的に先端技術の利用に伴うサイバーセキュリティリスクの分析・明確化とそれに基づくガイドラインの策定や普及等に取り組む。また、こうした取組のために必要となる先端技術のリスク分析や脅威への対策に係る研究開発を推進する。これらの取組においては、セキュリティ・バイ・デザインの考え方を基本とすることが重要である。さらに、先端技術による新たな価値創出を目指す企業と、その先端技術の利用を支えるためのサイバーセキュリティ技術・サービスの供給者とのマッチングやサイバーセキュリティ技術・サービスの適切な評価に係る仕組みの構築等に向けた検討を行う。

加えて、我が国の高いサイバーセキュリティが確保されたモノやサービス等についての国際展開を促すため、トップセールスや展示会等を活用したアピールを行うほか、

38 脅威の発生を誘引するような人、モノ、サービス上の欠落点

サイバーセキュリティを理由とした自由貿易の障害となる措置を正当化する動きに対しては、国際的な連携の下、厳格に対処するなど、国際展開をしやすいビジネス環境の整備に取り組む。

4.1.2　多様なつながりから価値を生み出すサプライチェーンの実現

サイバー空間と実空間の一体化が加速的に進展する中、「Society5.0」の実現に向けて、グローバルな規模でこれまで取引がなかった異なる業種の企業間取引が生まれている。また、その取引自体が自動化されたものになるなど、従来のサプライチェーンを超えた多様かつ流動的な形態を見せている。そして、このような形態においては、サプライチェーンのつながりの端で起こったサイバーセキュリティの問題が、実空間、さらには、経済社会全体にこれまで以上に広く波及し、甚大な悪影響を及ぼすおそれがある。このようなリスクを認識し、サプライチェーン全体を俯瞰した取組を推進することが不可欠である。

(1)　サイバーセキュリティ対策指針の策定

サプライチェーンにおけるつながりが多様かつ流動的な形態になる中、サイバーセキュリティの確保を進めていくためには、サプライチェーン全体に対して、一貫性をもった必要な対策が実装されることが不可欠である。また、このような取組を通じて、モノやサービスに関わる品質が新たな価値を生み出すことが期待される。

具体的には、官民が連携して、サプライチェーンにおける脅威を明確化し、運用レベルでの対策が実施できるような業種横断的な指針を策定するとともに、その普及を図る。その際には、中小企業を含めた事業者が実際に対策を行いやすくするため、事業者の事情を踏まえた現実的に実施が可能な内容で、かつ、分かりやすいものとなるように十分に配慮する。また、事業者がリスクと対策費用のバランスを意識できるものとすることも重要である。

産業分野毎のサプライチェーンに関わるつながり方や守るべきもの、脅威の差異を意識しつつ、IoT 機器や組織等に求められる具体的な対応策を産業分野毎に示していく必要がある。さらに、サプライチェーンがグローバルに拡がる中で、我が国における対策指針に基づくサイバーセキュリティ対策がグローバルに認められるようにするため、海外におけるルール化の動きも反映する必要がある。

(2)　サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築

サプライチェーン全体としてのサイバーセキュリティを確保するためには、製造される機器、生成されて流通するデータ、それらを利用したサービス等のサプライチェーンの構成要素における信頼の確保が不可欠である。このため、それぞれの構成要素

がセキュリティ要件を満たした形で生成・流通されるよう、要件の明確化を図るとともに、その要件が満たされていることを確認等することにより信頼を創出する仕組みの構築が必要である。また、サプライチェーンにおける調達者が機器・サービス等の利用に際し、その信頼を確認できるよう、官民が連携して、信頼性が証明されている機器・サービス等のリストの作成と管理を行う仕組みの構築が必要である。さらに、これらがサプライチェーンのつながりにおいて、連続的な仕組みとなるよう、トレーサビリティ[39]を確認するための仕組みと、創出された信頼そのものに対する攻撃を検知・防御するための仕組みを検討する。

(3) 中小企業の取組の促進

中小企業は、サイバー攻撃により、金銭的な損害や信用の低下が生じた場合、経営に与えるインパクトが大企業と比べて大きい。また、中小企業が踏み台となって自社のみならず取引先までサイバー攻撃の影響が拡大することも懸念されている。一方、中小企業は、必ずしも高いサイバーセキュリティに関する知識やスキルを有しているとはいえず、サイバーセキュリティに対して十分な投資を行うことが難しいという事情を踏まえた上で、サイバーセキュリティ対策を推進する必要がある。

このため、国は、中小企業を対象として、安全な情報システムの利活用モデルの提示を含む理解しやすいサイバーセキュリティ対策の事例集を作成するとともに、サイバーセキュリティ保険の活用促進、中小企業がサイバーセキュリティに関するトラブル等について相談できる仕組みの強化を行う。また、官民が連携して、サイバーセキュリティに取り組んでいる中小企業が、それを自主的に宣言できる仕組みなどの可視化の取組を促進するとともに、インセンティブの仕組みとの連携により、効果的に中小企業のサイバーセキュリティを進めるための仕組み作りを行う。

4.1.3 安全な IoT システム[40]の構築

サイバー空間につながる様々なモノが急速に広がっており、経済社会の発展に不可欠なインフラとしてのサイバー空間に悪影響を及ぼし得る脆弱なモノ（機器）のサイバーセキュリティ対策が喫緊の課題となっている。また、セキュリティレベルや物理的安全性等の安全基準が異なる様々なモノ（IoT 機器）のつながりが拡大する中、こうしたつながりは、新たな脅威を生む可能性がある。このような状況を踏まえ、官民が連携して、安全な IoT システムの構築に取り組む必要がある。

(1) IoT システムにおけるサイバーセキュリティの体系の整備と国際標準化

39 追跡可能性

40 家電、自動車、ロボット、スマートメーター等のあらゆるモノがインターネット等のネットワークに接続され、そこから得られるビッグデータの利活用等により新たなサービスの実現が可能となるシステム

これまで、IoT システムのサイバーセキュリティ対策については、官民が連携し、ガイドラインの策定を始めとする安全な IoT システムの実現に向けた様々な取組を推進してきた。今後は、安全な IoT システムが価値を創出することに重点を置き、一定の整合性・一貫性をもって戦略的に取り組む必要がある。

このため、我が国がこれまで示してきた安全な IoT システムを実現するために求められるサイバーセキュリティに関する基本的な要素[41]に基づき、各主体の間で対策に係る基本理念、目標、方法、期限等についての共通認識の醸成と、各分野・各主体の役割や機能の明確化を図った上で、自律的にサイバーセキュリティに関わる取組を進めつつ、各主体が協働した取組を推進する。また、国は、こうした取組を促すため、官民の各主体が抱える課題[42]やそれぞれの取組について、全体像が俯瞰できる形で可視化するとともに、情報共有を行うための仕組みを構築する。さらに、IoT システムにおける価値創出の仕組みを、我が国の安全・安心といった強みを活かしながらグローバルな規模で展開し、安全な IoT システムの普及によって国際経済の発展に貢献するため、官民が連携の下、安全な IoT システムを実現するために求められるサイバーセキュリティに関する基本的な要素等の国際標準化に向けた取組を推進する。

(2) 脆弱性対策に係る体制の整備

IoT 機器に対するサイバー攻撃等の深刻化に対応するため、ネットワークの安全・信頼性を確保する観点で、産官学民及び民間企業相互間の連携と役割分担の下、対策を推進することが重要である。このため、官民が連携して、IoT 機器の脆弱性について、設計・製造、運用、そして破棄までのライフサイクル全体を見通したサイバーセキュリティ対策や、ネットワーク上の脆弱な IoT 機器の対策等のための体制整備が必要である。

ライフサイクルを見通した IoT 機器のサイバーセキュリティ対策については、それぞれの機器の利用方法やサイバーセキュリティ上の脅威、諸外国の検討状況や技術の進展の動向等を十分踏まえた上で、機器製造事業者、電気通信事業者、利用者等の各々の主体の相互理解と連携の下で取り組むべきである。その中で、官民が連携して、それぞれの IoT 機器について、その特性や利用方法等を踏まえつつ必要なサイバーセキュリティの要件を整理し、その要件を満たす IoT 機器の利用を推奨する。

また、ネットワーク上の脆弱な IoT 機器の対策については、パスワード設定に不備のある機器の調査・特定を行い、電気通信事業者において当該機器の利用者への注意

41 「安全なIoTシステムのセキュリティに関する一般的枠組」（平成28年8月、内閣サイバーセキュリティセンター）
42 IoTの分野個別の課題だけでなく、その範囲や定義、物理安全対策、責任分界点（既知の脆弱性への対応に関する製造者責任や運用者等の安全管理義務などインシデント発生時における各主体の責任を含む）やプライバシーの問題などの共通課題を含む。

喚起を円滑に行えるよう、所要の制度整備を着実に進める。また、対策の実施に当たっては、関係省庁等が一体となって、電気通信事業者、機器製造事業者等と連携して取り組む。

　将来的には、これらの我が国の対策をモデルとして、国際的な連携や標準化等を通じて海外に展開し、安全なネットワークの環境整備に貢献をしていく。

4.2. 国民が安全で安心して暮らせる社会の実現

国民が安全で安心して暮らせる社会を実現するためには、政府機関、地方公共団体、サイバー関連事業者、重要インフラ事業者、教育研究機関、そして国民一人一人に至るまで、多様な主体が連携して多層的なサイバーセキュリティを確保することが重要である。

特に、政府機関や重要インフラ事業者、事業者団体及び地方公共団体（以下「重要インフラ事業者等」という。）が提供する業務やサービスは、円滑な社会経済活動及び国民生活を支える基盤である。サイバーセキュリティに係るリスクを完全に除去することは不可能であるとの認識の下、リスクを許容し得る程度まで低減し、これらの業務やサービスが安全かつ持続的に提供されるよう、サイバーセキュリティの基本的な在り方で掲げた「任務保証」の考え方に基づく取組を推進していく。

また、我が国は、2019 年のラグビーワールドカップや 2020 年東京大会などの国際的・国民的な大会を控えており、悪意ある主体によるサイバー攻撃の誘因となることも予想される。2020 年東京大会等を円滑に実施するとともに、その後も見据え、各々の主体がそれぞれの役割を着実に果たし、皆で協力し合って対応していく必要がある。

4.2.1　国民・社会を守るための取組

サイバー空間の脅威の深刻化に伴い、多くの国民がサイバー犯罪に不安感を持つようになっており、社会全体におけるサイバーセキュリティへの危機意識は高まっている。このような状況を踏まえ、全ての主体が、自主的にセキュリティの意識を向上させ、主体的に取り組むとともに、連携して多層的にサイバーセキュリティを確保する状況を作り出していくことが不可欠である。

(1)　安全・安心なサイバー空間の利用環境の構築

サイバー犯罪・サイバー攻撃は複雑化・巧妙化しており、攻撃の種類も多種多様となっていることから、従来の受動的な対策だけでは対応しきれず、これまでよりも積極的な対策を行う必要がある。

このような状況を踏まえ、サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じる「積極的サイバー防御[43]」を推進する。具体的には、国は先行的防御を可能にするための脅威情報の共有・活用の促進、攻撃者の情報を集めるための攻撃誘引技術の活用、ボットネット[44]対策等、サイバー犯罪・サイバー攻撃による被害

43　サイバー攻撃に対して能動的に防御していく取組のこと

44　ウイルス感染等により攻撃者の自由に操られる状態となったパソコン等の機器（「ボット」と呼ばれる）を束ねたネットワークのこと。DDoS攻撃やスパムメールの送信等に悪用される。（出典：独立行政法人　情報処理推進機構「情報セキュリティ白書2017」）

を未然に防止できるような取組を推進する。

また、政府機関や重要インフラ事業者等が提供するサービスの全体の基盤となる信頼できる情報インフラの整備を促進する。このため、信頼性を評価するための検証や政府調達における運用改善等について検討を行う。

さらに、国民が仮想通貨取引を安全に利用できるよう、仮想通貨交換業者と連携し、対応を推進する。また、自動運転車やドローンについては、サイバー攻撃を受けて不正操作された場合には人命に影響を及ぼすおそれがあるため、かかる事態が生じないよう対策を推進する。特に、自動運転車については、国際場裡において国際基準策定の議論が進められており、引き続き議論を主導していく。

(2) サイバー犯罪への対策

サイバー空間が国民生活により身近なものとなる中で、世界規模のランサムウェア[45]感染被害や、国内の仮想通貨交換業者から多額の仮想通貨が不正に送信されたと見られる事案が発生するなど、サイバー犯罪が深刻な社会問題となっている。国民の安全と安心を守るためには、サイバー犯罪の実態把握、取締りを推進するとともに、関係機関・団体と連携し、国民一人一人の自主的な対策を促進するための広報啓発を行うほか、新たな手口のサイバー犯罪に対処できるよう、捜査能力・技術力の向上が不可欠である。

このため、国は、徹底した捜査活動や新たな捜査手法の検討、サイバー犯罪の被害を防止するための広報啓発活動等を推進する。また、高度な情報通信技術を用いた犯罪に対処するため、最新の電子機器や不正プログラムの解析のための技術力の向上、サイバー空間の脅威の予兆把握や脅威の技術的な解明のための総合的な分析を高度化すること等、情報技術の解析に関する態勢を強化する。さらに、民間事業者等の知見の積極的な活用や官民の人事交流を推進するとともに、情報の共有・分析、被害の未然防止、人材育成等の観点から、官民が連携したサイバー犯罪対策を推進する。

サイバー犯罪捜査等においては、サイバー空間における事後追跡可能性の確保が必要である。これには、関連事業者の協力や国際的な連携が不可欠であるため、必要な取組を行う。特に、通信履歴等に関するログの保存の在り方については、関係のガイドライン[46]を踏まえ、関係事業者における適切な取組を推進する。

45 データを暗号化して身代金を要求するマルウェア（malware。malicious softwareが短縮された語）
46 「電気通信事業における個人情報保護に関するガイドライン」の解説等

4.2.2　官民一体となった重要インフラの防護

重要インフラの防護については、重要インフラサービスを安全かつ持続的に提供するという「任務保証」[47]の考え方に基づき、「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」（以下「行動計画」という。）の５つの施策群[48]に基づいた取組を推進してきた。しかし、重要インフラ分野ごとに、サイバーセキュリティに関する意識や取組の進捗に温度差があるという課題がある。このような課題を解決するため、経営資源が限られ、サイバーセキュリティに十分な資源を割り当てることが難しい重要インフラ事業者等におけるセキュリティ対策のモデルに関する検討を含め、サイバーセキュリティに関する全体的な底上げを行う必要があり、各々の主体が自主的な取組を進めつつ、国も積極的な支援を行うことで、官民一体で取り組んでいく。

(1)　行動計画に基づく主な取組

重要インフラを防護するため、国は行動計画を策定・改定してきており、今後も引き続き、行動計画に基づく取組を推進していく。行動計画については、2020 年東京大会終了後に見直す予定であるが、社会動向の大きな変化等が生じた場合は、その前の時点においても、必要に応じて見直しを行う。

重要インフラ分野は、国民生活や社会経済活動に与える影響の度合いを考慮して、特に防護すべきという観点から指定しているものである。社会的情勢に鑑み、必要に応じて、重要インフラ分野や対象とする重要インフラ事業者等を拡大することにより、セキュリティの取組の輪を広げていき、面としての防護を強化していくとともに、情報共有の取組を更に促進し、情報共有体制を拡充していく。

また、重要インフラ防護の取組を推進するためには、重要インフラ事業者等の経営層の積極的な関与が必要不可欠であることから、サイバーセキュリティに関する意識を高めるように経営層への働き掛けを行いつつ、以下の取組を推進する。

①　リスクマネジメントの推進

重要インフラサービスは、サイバー攻撃発生時であっても安全かつ持続的に提供できるようにする必要がある。このため、重要インフラ事業者等は、事前のセキュリティ対策を講じるだけではなく、横断的かつ複合的なリスクを念頭に置いたリスクアセスメントの結果を踏まえ、「任務保証」の考え方を踏まえた事業継続計画[49]及び緊急時対応計画を策定することが重要である。こうしたリスクマネジメントの活動全体が継

47 「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」では「機能保証」としていたが、趣旨は「重要インフラ事業者等が果たすべき役割を確実に遂行することが重要」ということであり、ここで言う「任務保証」と同じ趣旨である。

48　安全基準等の整備・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、防護基盤の強化

49　BCP（Business continuity planning）

続的かつ有効に機能するよう、取組を推進する。

② 安全基準等の改善・浸透

重要インフラ事業者等における適切な対応を促進するため、国は、安全基準等を策定するための指針を浸透させる取組を行うとともに、データの管理の状況に関する調査や国際動向も踏まえた望ましいデータ管理の在り方を含め、業務の内容、組織の規模、システムの使用期間、国際競争力への影響等を考慮して安全基準等を改善する取組を継続的に推進する。また、安全等を維持する観点から、サイバー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など、制度的枠組みを適切に改善していく。

③ 深刻度評価基準

近年のサイバー攻撃の動向に鑑みれば、サイバー攻撃発生を検知した場合には、政府機関、重要インフラ事業者等の各々の主体の間で速やかに認識の共有を図り、迅速な対応の要否等の判断を行うことができるようにする必要がある。この実現に向けて、国民への周知による効果や影響に配慮しつつ、サイバー攻撃による重要インフラサービス障害等に係る深刻度評価基準を策定し、事案の深刻度を評価・公表することにより、様々な主体が冷静かつ適切な対応を行うことができるよう促していく。また、この基準がより良いものとなるように適時見直しを行っていく。

④ 官民の枠を超えた訓練・演習の実施

重要インフラ事業者等が、サービス障害発生時であっても適切に対応できるよう、そのような事態を想定した訓練・演習を実施し、能力向上を図ることが大切である。国や関係機関は、官民の枠を超えた様々な規模の主体の間での訓練・演習を引き続き実施し、必要に応じて対象の拡大や内容の改善を図るなど、発展させていく。

⑤ 制御系システムのセキュリティ対策

電力、ガス、石油分野等では、サービスを提供するために制御系システムを利用しているため、このシステムに不具合が生じると通常のサービスが提供できなくなり、国民生活に大きな支障が生じるおそれがある。制御系システムの特性を踏まえたセキュリティ対策が十分に行われ、サービスが安全かつ持続的に提供できるよう、制御系システムに関する人材育成を推進し、脅威情報の収集・分析・展開等を行っていく。

(2) 地方公共団体のセキュリティ強化・充実

地方公共団体が提供するサービスは、国民生活に密着しているものであり、そのサービスの提供に支障が出ると、地域の活動にも大きく影響が生じてしまう。中小規模の団体におけるセキュリティ対策については、個別に技術的な対策をとることには限界があるものの、まず、サービス障害や、人為的ミスによるマイナンバーを含む情報

漏えいに対してしかるべき対策を講じる必要がある。

こうした中、現行の国と地方の役割分担を背景に、国による直接の関与[50]が他の機関に比べて限定的な中で、高いセキュリティレベルを確保する必要があるため、セキュリティに関するガイドラインを更新する。また、業務の円滑化を考慮しつつ、業務用ネットワークのセキュリティレベルを確保するとともに、セキュリティ人材の確保・育成及び体制の充実を支援する取組を推進する。

加えて、官民の認証連携について、利便性とセキュリティのバランスが取れたものとなるよう、環境整備を進めていく。

4.2.3 政府機関等におけるセキュリティ強化・充実

各政府機関においては、統一的な基準を踏まえた情報セキュリティ対策が講じられるとともに、当該基準に基づいた監査や、不正な通信の監視等の取組等を通じて、政府機関全体としての対策の水準の向上が推進されてきており、引き続きこれら取組を継続することが必要である。サイバーセキュリティ基本法の改正[51]により、独立行政法人及びサイバーセキュリティ基本法に基づく指定法人（以下「独立行政法人等」という。）に対する取組の枠組みが、政府機関に対するものと同様に拡充されたが、今後、独立行政法人等の多様な業務形態を踏まえ、その特性に応じた効果的な情報セキュリティ対策を進めていくことも重要な課題となる。

複雑化・巧妙化しているサイバー攻撃に対しては、引き続き攻撃を前提とした多層防御や、サプライチェーンリスクへの対応を強化するとともに、新たな技術を活用し、従来の攻撃側優位の状況を改善するための取組を進めることが求められる。

政府機関及び独立行政法人等（以下「政府機関等」という。）における行政サービスの円滑な遂行は極めて重要な責務であり、システムへの投資を行う際には所要の IT 投資とセキュリティ関連投資を一体的に行うことが不可欠である。このような状況を踏まえ、政府の IT 投資の効率化によって得られた原資をセキュリティにあてるなどセキュリティ関連投資の充実とともに、上記の情報セキュリティ対策を強化していくことが重要である。

(1) 情報システムのセキュリティ対策の高度化・可視化

脅威が深刻化しているサイバー攻撃に対して、これらへの対処能力の向上に加え、被害の未然防止や、仮に被害が発生した場合にも、その拡大の防止や極小化を行うこ

50 技術仕様の統一・監査等
51 平成28年４月15日成立。国による不正な通信の監視・監査・原因調査等の対象を拡大

とを目指し、新たな防御技術を活用し、より効果的な取組を行う。

① 情報システムの防御能力の向上と状態の把握

政府機関等において、プログラムが動作するエンドポイント（端末等）においてマルウェアの挙動を検知することにより、被害の未然防止及び拡大防止に取り組む。IT資産管理の自動化により、情報システムの状態をリアルタイムに把握し、ソフトウェアの脆弱性への迅速な対応を可能としていく。また、全政府機関を対象としたデータ保護により、事案が発生した際にも情報を漏えいさせない取組を図る。さらに、様々な機器で発生する事象やアカウント管理情報を組み合わせて脅威を分析することにより、検知が困難な攻撃を発見する対策について検討する必要がある。この対策を効率的に行うためには、情報の分析に係る作業等の自動化を見据えたシステムを構築する必要がある。

② 政府機関等における横断的な連携の高度化による被害の発生・拡大の防止

政府機関等において、予防・検知・復旧・対処の各段階において端末等でのマルウェアの監視やIT資産管理の自動化について、導入状況等を踏まえつつ、これらから得られる情報をGSOC[52]に適切に共有するなど、政府機関等とGSOCによる効果的かつ効率的な連携の高度化による横断的な対応の発展を目指す。

(2) クラウド化の推進等による効果的なセキュリティ対策

各府省庁において情報の特性に応じて適切な情報システムの形態を選択するとともに、政府全体としてセキュリティ施策を効率的・効果的に実施できるよう、システムの構築と運用の集約及びセキュリティ水準向上の利点を活かすことができる、政府プライベートクラウドとしての政府共通プラットフォームへの移行を含むクラウド化を推進する。クラウド化の推進に当たっては、安全性評価など、適切なセキュリティ水準が確保された信頼できるクラウドの利用を促進する方策について検討を進める。

また、インターネット接続回線については、統一基準においてその接続口の統合・集約化を求めてきた。政府機関のインターネット接続口の適切な集約を更に推進することは、運用及びセキュリティ対策上、非常に効果的であるため、政府共通ネットワーク及び政府共通プラットフォームと連携しつつ、境界監視ポイントの集約を含め、必要な検討を行う。

(3) 先端技術の活用による先取り対応への挑戦

近年、普及してきた情報システムの基盤の中には、サイバー攻撃に対する高い耐性を有するものがある。こうした新しい設計思想の下で誕生した情報技術について、政

52 Government Security Operation Coordination teamの略。政府機関情報セキュリティ横断監視・即応チーム

府機関等における活用の可能性を検討し、ベストプラクティスの蓄積を図り、防御側優位に向けた転換を目指す。

(4) 監査を通じたサイバーセキュリティの水準の向上

サイバーセキュリティ基本法に基づき、政府機関等に対して実施する監査において、組織横断的な分析により抽出される傾向や課題を政府機関等全体にフィードバックし、更なるサイバーセキュリティの水準の向上を促す。また、効率的な情報システムの状態の把握に係る取組に沿って整備される各政府機関における IT 資産管理情報を活用し、効果的かつ効率的に監査を実施することを目指す。

(5) 組織的な対応能力の充実

事案対応を行うチーム[53]を中心に、各政府機関等の事案対応能力や情報セキュリティに係る知識を向上させる。また、政府機関等に対するサイバー攻撃の発生に備え、各府省庁の知見・技能を有する職員から構成される機動的な支援が可能な体制（情報セキュリティ緊急支援チーム[54]）の強化を図るため、要員の対処能力の向上のための研修等を充実する。

4.2.4 大学等における安全・安心な教育・研究環境の確保

大学及び大学共同利用機関等（以下「大学等」という。）は、多様な構成員によって構成され、多岐にわたる IT 資産、多様なシステムの利用実態を有する。このような大学等の特性を踏まえ、安全・安心な教育・研究環境を確保するためには、大学等において自律的にサイバーセキュリティ対策を行うとともに、大学等の連携協力によるサイバー攻撃への対応体制の構築や情報共有等を国が積極的に支援することが重要である。

(1) 大学等の多様性を踏まえた対策の推進

大学等の経営層は、自らサイバーセキュリティ対策の重要性を認識したうえで、サイバーセキュリティ対策を経営上の重要課題と位置付け、対策を推進するための計画等に基づき自律的かつ組織的に取り組むとともに、フォローアップを実施することによりサイバーセキュリティ対策を一層推進する必要がある。

こうした取組に当たっては、様々な教育・研究を実施している大学等の多様性を踏まえつつ、守るべき IT 資産を特定し、サイバーセキュリティリスクの評価を行い、リスクに応じて重点的に実施するべきマネジメント面・技術面における対策を検討することが求められる。また、事案に適切かつ迅速な対処をするための能力の向上に向け

53 CSIRT (Computer Security Incident Response Team)
54 CYMAT (Cyber Incident Mobile Assistant Team)

た取組や、これらの対策を組織的かつ着実に実施するための体制についても検討する必要がある。

国は、大学等に対して、サイバーセキュリティに関するガイドライン等の策定・普及、リスクマネジメントや事案対応に関する各層別研修及び実践的な訓練・演習の実施、事案発生時の初動対応への支援を通じて、大学等における自律的かつ組織的な取組を促進する。

(2) 大学等の連携協力による取組の推進

大学等は、共通の情報基盤を利用しており、共通性が見られるサイバーセキュリティ上の課題を有している。こうした大学等の実態を踏まえたサイバーセキュリティ対策の強化が重要であり、各々の相互協力による取組の一層の促進が求められている。

このため、学術情報ネットワークを運営する機関は、国立大学及び大学共同利用機関と連携し、サイバー攻撃を観測・検知・分析するシステムを構築し、情報提供を行うとともに、監視能力の機能維持・強化及び戦略マネジメント層の育成に向けた共同研究や技術職員への研修を実施する。

さらに、国は、大学等の事案対応体制を強化するため、複数の大学等の事案対応を行うチームにおいてサイバー攻撃に関する情報や共通課題、事案対応の知見等を共有するための取組を支援する。

4.2.5 2020 年東京大会とその後を見据えた取組

オリンピック・パラリンピック競技大会は、世界中から多数のアスリート、要人、観客等が集まり、国際的にも最高度の注目を集めて開催される行事であることから、サイバー攻撃のターゲットとなるおそれがある。

過去の大会を振り返ると、ロンドン大会では、大会の運営には影響はなかったものの、膨大な数のサイバー攻撃があったとされるほか、リオデジャネイロ大会においても平昌大会においても、相当数のサイバー攻撃が行われ被害を受けたとの報道がある。2020 年東京大会においても、過去の大会以上のサイバー攻撃が予想され、その特性上各種サービス分野にまたがるような攻撃も想定される。このため、次により 2020 年東京大会のサイバーセキュリティの確保及びその後を見据えた施策を推進する。

また、2020 年東京大会後も各種施策は適用範囲を拡大して引き続き推進し、整備した仕組み、その運用経験及びノウハウはレガシーとして、以降の我が国の持続的なサイバーセキュリティの強化のために活用していく。

(1) 2020 年東京大会に向けた態勢の整備

引き続き、「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推進本部」の下の「セキュリティ幹事会」で決定された基本戦略に基づき大会の安全に関する情報の集約等の取組を進めるとともに、物理的なセキュリティとの連携も考慮してリスク源を分析し、その結果を踏まえたリスクシナリオの検討を含め、大会運営に影響を与える可能性のある重要サービス事業者等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分野横断的なリスクを含めた各種リスクへの対策を促進する。また、関係府省庁、大会組織委員会、東京都、競技会場のある地方公共団体、重要サービス事業者等、大会関係組織間でサイバーセキュリティに係る脅威情報を共有するとともに、事案発生時に大会関係組織が皆で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（政府オリンピック・パラリンピック CSIRT)」の構築を推進し、緊密に連絡調整を図るための態勢を整備する。

(2) 未来につながる成果の継承

2020 年東京大会の態勢整備のための各種施策を引き続き推進し、整備した仕組み、その運用経験及びノウハウは、レガシーとして、2020 年東京大会以降の我が国の持続的なサイバーセキュリティの強化のために活用していく。また、構築した「サイバーセキュリティ対処調整センター」を、サイバー攻撃等に対してオールジャパンで力を合わせて対処するための調整役・調整窓口（ナショナル CSIRT）として活用し、サイバーセキュリティの基本的な在り方でも掲げた「リスクマネジメント」の手法については、広く全国の事業者等に適用できるよう整備・普及を促進していく。

4.2.6 従来の枠を超えた情報共有・連携体制の構築

本来、サイバーセキュリティの確保は、保有する情報資産の価値、情報通信技術の利活用の状況等を踏まえ、各組織が自主的に取り組むものである。一方、攻撃態様の変化により、自組織のみでサイバー攻撃への効果的な対策を講じることには限界が生じてきている。このため、他の組織との連携を重視する意識が官民ともに着実に広がっており、行政機関や重要インフラ事業者に限らず、幅広い主体が情報共有に取り組み始めている。

サイバー空間と実空間の一体化が進展し、サイバー空間と密接に関連する分野が一層増加する中、サイバーセキュリティに資する情報の共有に取り組むべき分野や関係者の範囲は、更に広がり続けることが予想される。

そのため、サイバーセキュリティの基本的な在り方で掲げた「参加・連携・協働」

の観点から、各主体との緊密な連携の下、国は ISAC[55]を含む既存の情報共有における取組の推進を支援するとともに、新たな役割を果たしていく必要がある。

(1) 多様な主体の情報共有・連携の推進

情報共有に取り組む主体の増加に伴い、情報の集約・分析や各主体との迅速な調整を担う役割の重要性が増している。一方で、共有した情報が適切に取り扱われず、社会的評価・信頼の低下を引き起こすおそれがあることから、自らが保有する情報の共有に各主体が積極的に取り組むことができないという課題がある。

これを踏まえ、情報共有に十分な知見を有する専門機関を含む官民の多様な主体が、安心して相互にサイバーセキュリティ対策に資する情報の共有を図るための新たな体制を構築する。その際、基本原則に掲げる「自律性」の観点から、各々の主体の自主性を尊重することが重要である。このような取組を進めることで、官と民、業界、国内外といった枠を超えた情報の共有・連携を推進していく。

また、官民で既に複数組織されている情報共有体制において、関係者の更なる負担が生じることのないよう、各々の特色や役割を踏まえて、連携や統合について検討していく。

(2) 情報共有・連携の新たな段階へ

新たな情報共有体制を構築するに当たって、多様な主体が信頼関係を構築し、連携して積極的に情報提供に協力する者ほど恩恵を享受できる仕組みを検討していく。

他者との連携・協働のレベルが高まるほど、情報共有体制に参加するメリットが高まるため、まずは国から率先して自ら保有している情報を適切に提供していくとともに、各主体が自ら保有する情報を共有するなどして積極的に貢献できる環境を整備する必要がある。また、寄せられる情報に対して、処理の自動化を推進するなどして、適切かつ迅速な分析や、各々の主体が真に必要とする情報の共有を実現していく。

このような取組により、サイバーセキュリティを高めるためには双方向の情報共有が不可欠であるとの認識を社会に広く醸成していく。さらに、我が国の情報共有の仕組みを発展させつつ、国際社会との戦略的な連携を視野に入れることも肝要である。官民や業界といった従来の枠を超えて、各々の主体が共存・発展していくことのできる関係を構築できるよう、国は各主体と緊密に連携し、環境整備に積極的に取り組んでいくことで、サイバーセキュリティに関する情報共有・連携が新たな段階へ移行し

55 Information Sharing and Analysis Centerの略。サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織。分析した情報はISACに参加する会員間で共有され、各々のセキュリティ対策に役立てられる。（出典：サイバーセキュリティ2017（平成29年８月25日））

ていく。

4.2.7　大規模サイバー攻撃事態等への対処態勢の強化

海外では、サイバー攻撃による大規模な停電や金融機関の一部機能停止といった事案が発生し、国民生活に多大な影響を与えている。サイバー空間と実空間の一体化が進展している中、我が国においても、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。また、大規模なサイバー攻撃については、通常、関連性の薄い分野のサービスが同時多発的に被害を受けることも想定されるところであり、係る脅威から国民・社会を守るためには、国が一丸となってサイバー空間の脅威への危機管理にも臨む必要がある。

実空間とサイバー空間の双方の危機管理に臨むために、実空間とサイバー空間の横断的な対処訓練・演習を実施するとともに、当該訓練・演習を通じてサイバー攻撃への対処態勢の強化を図る。加えて、サイバー攻撃に関する分析に係る人材の育成や官民連携の枠組みを通じた情報共有、インターネット観測の高度化を推進し、サイバー空間における情報収集・分析機能及び緊急対処能力の向上を図る。

4.3. 国際社会の平和・安定及び我が国の安全保障への寄与

自由、公正かつ安全なサイバー空間は、国際社会の平和・安定及び我が国の安全保障に寄与するものである。

全ての主体に開かれ、自律的で、自由な情報の流通が保障されたサイバー空間は、技術革新の源泉であり、民主主義の基盤である。サイバー空間は、産学官民の多様な関係者による技術革新や発明、取組を通じて発展してきた。国家による過度な統制は、サイバー空間の自律的・持続的な発展を阻害する。サイバー空間の健全な発展のためには、多様な主体の協力により、自由な情報の流通が確保され、開放的・自律的なサイバー空間を堅持する必要がある。

社会のあらゆる場面でサイバー空間の利用が加速的に進み、サイバー空間と実空間の一体化が進展することにより、人権、プライバシー、犯罪・テロ、国家安全保障など、実空間の問題が、サイバー空間に持ち込まれ、課題となっている。これら課題に対応し、安全・安心を確保するための取組をサイバー空間についても進める必要がある。サイバー攻撃は容易に国境を越え、また、国家の関与が疑われる事案も出てきているため、サイバー空間の安全・安定の確保のためには、法の支配の推進、サイバー攻撃に対する防御力・抑止力・状況把握力の向上、国際協力・連携を進める必要がある。この際、サイバー空間の自律的・持続的な発展を阻害しないように留意しなければならない。

我が国は、自由、公正かつ安全なサイバー空間を堅持するため、国際場裡において我が国の立場を発信し、既存の枠組みを活用し、我が国の安全を確保するための取組を行い、国際連携を進める。

4.3.1 自由、公正かつ安全なサイバー空間の堅持

グローバル規模で自由、公正かつ安全なサイバー空間を実現するため、国際場裡においてその理念を発信し、サイバー空間における法の支配の推進のため、積極的な役割を果たしていく。

(1) 自由、公正かつ安全なサイバー空間の理念の発信

我が国は、自律的・持続的に発展するサイバー空間のエコシステムを維持するため、情報の流通の規制などの国家による管理・統制ではなく、多様な主体が連携・協働してサイバーセキュリティの確保に取り組むことにより、サイバー空間の安全を確保することを目指す。

こうした日本型のサイバーセキュリティの基本的な在り方を国際場裡において発信するとともに、サイバー空間の発展を妨げるような国際ルールの変更等を目指す取組に対しては、同盟国・有志国、民間団体等と連携して対抗する。

この際、インターネットの資源管理に関する議論と、人権、プライバシー、犯罪・テロ、国家安全保障等のサイバー空間の利用に関して生じる問題についての議論は分けて考えなければならない。サイバー空間の利用に関して生じる問題については、既存の枠組みの存在を前提とした議論を進める必要がある。

(2) サイバー空間における法の支配の推進

国際社会の平和と安定及び我が国の安全保障のため、サイバー空間における法の支配を推進することが重要である。

サイバー空間においても、国際連合憲章を始めとする既存の国際法が適用される。我が国は、この立場から、既存の国際法の個別具体的な適用の在り方、規範の形成・普遍化についての議論に積極的に関与する。また、これまでに明らかにされた責任ある国家の行動規範[56]について、着実な履行・実践を通じ普遍化を進める。そうした規範を国際社会に広げ、国家実行を積み重ねていくことで、規範に反する行動を抑止する。

サイバー犯罪対策では、警察庁及び関係省庁が連携して、サイバー犯罪に関する条約、刑事共助条約、ICPO[57]等の枠組みを活用した国際機関、外国法執行機関、外国治安情報機関等との間における国際捜査共助や情報交換等による国際連携をさらに推進する。

こうした取組により、法の支配を推進し、国際社会の平和と安定及び我が国の安全保障を実現する。

4.3.2 我が国の防御力・抑止力・状況把握力の強化

サイバー空間における安全保障を取り巻く環境は、厳しさを増している。政府機関、重要インフラ事業者、先端技術を有する企業・学術機関等への攻撃や、民主主義の根幹を揺るがしかねない事例も発生している。さらに、それらの中には国家の関与が疑われる事案も存在する。

以上の状況を踏まえ、サイバー攻撃から我が国の安全保障上の利益を守るため、サイバー攻撃に対する国家の強靱性を確保し、国家を防御する力（防御力）、サイバー攻撃を抑止する力（抑止力）、サイバー空間の状況を把握する力（状況把握力）のそれぞれを高めることが重要である。

これら安全保障に係る取組に関しては、内閣官房国家安全保障局による全体取りまとめの下、防御は内閣サイバーセキュリティセンターを中心として官民を問わずすべ

56 2015年第４会期国連サイバー政府専門家会合（UNGGE）報告書、2015年G20アンタルヤ・サミット首脳宣言、及び2017年サイバー空間における責任ある国家の行動に関するG７（ルッカ）宣言　等

57 International Criminal Police Organizationの略。国際刑事警察機構

ての関係機関・主体、抑止は対応措置を担う省庁、状況把握は情報収集・調査を担う機関が、平素から緊密に連携して進める。また必要な場合には、国家安全保障会議で議論・決定を行う。

(1) 国家の強靱性の確保

① 任務保証

政府機関は、国民生活や経済社会を守り、支える任務を有しており、その機能停止は、安全保障上の重大な懸念事項である。政府機関の任務遂行は、重要インフラその他の社会システムを担う事業者のサービスに依存している。また、これら事業者自身も、国民や社会に不可欠なサービスを提供するという重要な任務を有している。

我が国の安全保障に関係する政府機関の任務遂行を保証するため、また、国民や社会に不可欠なサービスを提供するため、政府機関及び重要インフラ事業者等におけるサイバーセキュリティの確保を推進する。特に、防衛当局である防衛省・自衛隊においては、サイバー攻撃対処を行う部隊の能力を更に向上させ、自らの活動が依存するネットワーク・インフラの防護を引き続き強化するとともに、自衛隊の任務保証に関連する主体との連携を深化させていく。

② 我が国の先端技術・防衛関連技術の防護

先端技術は、経済的な優位性を保障するだけでなく、安全保障上も重要な国家的資産である。宇宙関連技術、原子力関連技術、セキュリティ技術、防衛装備品に関する技術等、我が国の安全保障上重要な技術を扱う事業者及び関係省庁における人的要因によるリスク軽減も含めたサイバーセキュリティ対策を強化する。特に防衛産業が取り扱う技術情報等は、それが漏洩・流出した場合の我が国の安全保障上の影響が大きいため、安全な情報共有を確保する仕組みの導入、契約企業向けの新たな情報セキュリティ基準の策定、契約条項の改正等の取組を行う。これらについて、官民連携の下、下請け企業等を含めた防衛産業のサプライチェーン全体に適用することを前提とした検討を行う。

また、先端技術情報を保護する観点から、国立研究開発法人や先端的な技術情報を保有する大学等における対策を促進する。

③ サイバー空間を悪用したテロ組織の活動への対策

サイバー空間は、個人や団体が自由に情報をやり取りし、自らの考えを述べる場を提供するものであり、今や民主主義を支えているものの一つである。他方、テロ組織が、過激思想の伝播や示威行為、組織への勧誘活動、活動資金の獲得等の悪意ある目的でサイバー空間を利用することは防止しなければならない。このため、表現の自由を含む基本的人権を保障しつつ、サイバー空間におけるテロ組織の活動に関する情報

の収集・分析の強化その他の必要な措置を国際社会と連携して実施する。

(2) サイバー攻撃に対する抑止力の向上

① 実効的な抑止のための対応

国際連合憲章を始めとする国際法は、サイバー空間において適用される。そして伊勢志摩サミットにおいてG7首脳が確認したとおり、一定の場合には、サイバー攻撃が国際法上の武力の行使又は武力攻撃となり得る[58]。また、G7 ルッカ外相会合において確認したとおり、悪意のあるサイバー攻撃等武力攻撃に至らない違法行為に対しても、国際違法行為の被害者である国家は、一定の場合には、当該責任を有する国家に対して均衡性のある対抗措置及びその他の合法的な対応をとることが可能である[59]。

以上の認識を踏まえ、我が国は、悪意ある主体の行動を抑止し、国民の安全・権利を保障するため、国家の関与が疑われるものも含め、我が国の安全保障を脅かすようなサイバー空間における脅威について、同盟国・有志国とも連携し、脅威に応じて、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、断固たる対応をとる。

適切な対応を適時にとれるよう、内閣官房を中心とした関係省庁の連携体制を強化し、政府が一体となって組織・分野横断的な取組を総合的に推進する。また、法執行機関、自衛隊を始めとする関係機関の能力強化を進める。

② 信頼醸成措置

サイバー攻撃を発端とした不測の事態の発生や悪化を防止するため、国家間の信頼を醸成する。サイバー攻撃は、匿名性・隠密性が高いことから、意図せず国家間の緊張が高まり、事態が悪化するリスクがある。このように偶発的、不必要な衝突を防ぐため、国境を超える事案が発生した場合に備え、国際的な連絡体制を平素から構築しておくことが重要である。また、二国間・多国間の協議における情報交換、政策対話等を積極的に行うことを通じ、透明性を高め、国家間の信頼を醸成する必要がある。各国と協力し、サイバー空間の問題を調整するメカニズムについても検討する。

(3) サイバー空間の状況把握の強化

---

58 G7伊勢志摩サミット　サイバーに関するG7の原則と行動（2016年５月）「我々は、一定の場合には、サイバー活動が国際連合憲章及び国際慣習法にいう武力の行使又は武力攻撃となり得ることを確認する。また、我々は、サイバー空間を通じた武力攻撃に対し、国家が、国際人道法を含む国際法に従い、国際連合憲章第51条において認められている個別的又は集団的自衛の固有の権利を行使し得ることを認識する。」

59 サイバー空間における責任ある国家の行動に関するG７（ルッカ）宣言（2017年４月）「紛争の予防及び紛争の平和的解決のため、国際法が武力攻撃に至らない違法行為（悪意のあるサイバー活動を含み得る。）に対する国家の対応のための枠組みを提供していることに留意する。国際違法行為の被害者である国家は、一定の場合には、その違法行為について責任を有する国家に国際的な義務を遵守させるために、当該責任を有する国家に対して均衡性のある対抗措置（ICTを介して実施する措置を含む。）及びその他の合法的な対応をとることができる。」

① 関係機関の能力向上

深刻化するサイバー攻撃の脅威を抑止していくためには、対応力の強化に加え、攻撃者に責任を負わせるために、サイバー攻撃を検知・調査・分析する十分な能力が求められる。このため、関係機関の情報収集・分析能力を質的・量的に向上させる。高度な分析能力を有する人材の育成・確保、サイバー攻撃を検知・調査・分析等するための技術の開発・活用等あらゆる有効な手段について幅広く検討を進める。また、カウンターサイバーインテリジェンスに係る取組を進める。

② 脅威情報連携

国の関与が疑われるサイバー攻撃、非政府組織等による攻撃等多様な脅威に的確に対処し、抑止するため、政府内関係省庁及び同盟国・有志国との国内外の情報連携が不可欠である。同盟国・有志国との間で、脅威情報の共有を推進する。また、内閣官房を中心とした政府内の脅威情報共有・連携体制を強化する。

4.3.3 国際協力・連携

サイバー空間においては、事象の影響が容易に国境を越えることから、海外で生じたサイバー事案は常に我が国にも容易に影響を及ぼす可能性がある。世界各国との政府・民間様々なレベルで協力・連携することにより、サイバー空間の安全を確保し、もって国際社会の平和・安定及び我が国の安全保障を図る。

このため、様々な国際的な議論に積極的に貢献し、サイバー問題に関する情報の共有や意識の統一に向けて取り組む。また、外国との知見・経験の共有を進め、具体的な協力・連携関係を構築し、実際の行動につなげる。また、国際場裡で我が国の立場を主張できる官民の人材を確保し、育成する。

(1) 知見の共有・政策調整

サイバーセキュリティに関する二国間の協議や国際会議を通じ、互いのサイバーセキュリティ政策や戦略、体制の情報交換を行い、我が国のサイバーセキュリティ政策立案に生かしていく。また、我が国とサイバーセキュリティに係る基本的な考え方を共有する戦略的パートナー国との二国間で、サイバーセキュリティ施策に関する協力・連携を強化する。

(2) 事故対応等に係る国際連携の強化

サイバー攻撃の情報や脅威情報を平時から共有し、事故発生時に連携対処できるよう、CERT[60]間連携を強化する。また、国際サイバー演習への参加や共同訓練等を通じて、連携対処能力の向上を図るとともに、事故発生時に適切に国際連携しながら対処する。

60 CERT (Computer Emergency Response Team)。コンピュータセキュリティインシデントに対応する活動を行う組織

(3) 能力構築支援

国際的な相互依存関係が進む現在、我が国の平和と安全は我が国一国のみでは確保できない。我が国の安全保障の確保に寄与するためには、全世界的に連携してサイバーセキュリティ上の脆弱性を低減し、撲滅を目指していくことが肝要である。

このような観点から、世界各国におけるサイバーセキュリティの能力構築を支援することは、対象国の重要インフラ等に依存する在留邦人の生活や日本企業の活動の安定を確保し、当該国の健全なサイバー空間の利用の進展を促すのみならず、サイバー空間全体の安全の確保と直結しており、ひいては我が国を含む世界全体の安全保障環境の向上に資する。

2016 年に公表した基本方針[61]に基づき、様々な政策手段を活用し、開発途上国における能力構築支援を積極的に実施していく。

61 「サイバーセキュリティ分野における開発途上国に対する能力構築支援（基本方針）」（平成28年10月サイバーセキュリティ戦略本部報告）

4.4. 横断的施策

「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」の３つの政策目標を達成するためには、その基盤として、横断的・中長期的な視点で、人材育成や研究開発に取り組むとともに、サイバー空間で活動する主体としての国民一人一人が、サイバーセキュリティに取り組むような全員参加による協働を推進していくことが重要である。

4.4.1　人材育成・確保

「Society5.0」の実現に向けて新たな価値が創出されていく中、サイバー攻撃の脅威は広がっており、一部の専門家がサイバーセキュリティの確保に取り組むのではなく、それぞれの役割を遂行する観点から、主体的に取り組むことが求められる。

こうしたパラダイムシフトにより生じる将来を見据えつつ、各々の組織の「任務」の遂行や個人の安全な利用を支える観点から、サイバーセキュリティの確保に取り組む各人材層において保有すべき知識や技術の水準を明確化することが求められる。その上で、教育等を通じ、資格・評価基準等によって可視化された確かな知識と実践力を備えた人材が、適切な処遇を受け、更に実務経験を積み重ねることにより、人材の需要と供給が相応されるといった好循環の形成が必要である。

このため、産学官が連携して人材の需要や人材育成施策に関する情報共有等の連携を図りつつ、人材育成・確保を強化していく。その際、イノベーションを推進する観点から、人材の多様性の確保を推進していくことが重要である。

(1)　戦略マネジメント層の育成・定着

企業経営においてサイバーセキュリティ対策を進めていくためには、それが単に技術的な課題にとどまらないことから、専門家や実務者任せにすることは適切ではない。経営層が示す経営戦略や事業戦略の下、組織がマネジメントすべき様々なリスクの一つとして、業務やサービス等を実現するために必要なサイバーセキュリティに係るリスクを認識し、事業継続と価値創出に係るリスクマネジメントを中心となって支える立場として、社内外の実務者・専門家を活用・指揮しつつ、対策や事案への対応を実践する役割を果たしうる人材が求められている。このため、こうした役割を担う層を「戦略マネジメント層」と位置付け、経営層の理解の促進を含め、産業界と連携しつつ、その定着を図る。

また、業種や業態によっては、文化や慣習などの違いにより、業務やサービス等を実現するための既存のマネジメントに対し、サイバーセキュリティ対策を組み込み、実践することに困難を伴う場合がある。このため、多様なビジネスとそのマネジメン

トの実態があることを踏まえつつ、戦略マネジメント層向けの実践的な教材の開発や、指導者の発掘・育成も含め、学び直しプログラムの実践を推進する。

(2) 実務者層・技術者層の育成

戦略マネジメント層が示す方針を踏まえ、システムの企画や構築・運用時における対策等を実践する実務者層や技術者層については、これまで官民において、教育プログラムや資格・試験、演習の実施などの様々な取組が行われてきた。

こうした知識や技術の水準を高める取組は、引き続き強化を図っていく必要があるが、実務者や技術者が戦略マネジメント層に対して貢献できるよう、日々進化する情報通信技術や制御システムの技術、これらに対するサイバー攻撃について理解を深めることはもとより、経営層の方針を理解しつつ、他の専門人材と円滑にコミュニケーションをとりながらチームの一員として対処ができるようにすることが重要である。このため、実務者層・技術者層向けの育成プログラムにおいては、戦略マネジメント層が示す概念的・抽象的な考えを理解し、それを具体化するとともに、様々な関係者と円滑なコミュニケーションができるような学び直しによるスキルの開発や実践的な演習が必要である。

さらに、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・確保も引き続き行っていく。例えば、サイバー攻撃に対する防御方法、攻撃手法も含む対処法、情報を収集して分析評価を行う方法の体系化を含む研究を通じ、グローバルに切磋琢磨する機会を広げ、対策を検討できる能力の育成を引き続き推進する。

(3) 人材育成基盤の整備

中長期的な情報通信技術の進化を見据え、応用分野であるサイバーセキュリティの土台となる基礎原理の理解を促し、論理的思考力や概念的思考力の育成を充実させる必要がある。このため、サイバーセキュリティや情報通信技術に関する基礎的な内容については、産学官が連携して、知識・技術体系やそれに基づくモデルカリキュラムの在り方の検討を行う。

また、サイバーセキュリティや情報通信技術について若年層の教育を強化するため、初等中等教育段階では、小学校段階から必修としたプログラミング教育など、発達の段階に応じてコンピュータなどの情報通信技術の原理や仕組みなどを理解し、プログラミング的思考といった論理的思考力を育てるなど、教育課程内で情報活用能力の育成に着実に取り組む。さらに、こうした情報活用能力の育成に関する履修項目が、教員養成課程において着実に盛り込まれるようにするとともに、教員の研修を充実させる。その際、必要に応じて産業界などの人材の活用も柔軟に進めることが重要である。加えて、近年、若年層によるサイバー犯罪が発生していることから、情報モラル教育

も重要な課題である。

さらに、将来、高度なサイバーセキュリティ技術を持つ人材となることが期待される若年層向けに、教育課程外の地域や企業・団体等において、産業界などの人材の能力を柔軟に活用しつつ、自由にサイバー関連ツール、機器を用いて興味を持って学べる機会が豊富に用意されるような環境整備を進める必要がある。同時に、こうした自己実現の環境整備は、倫理教育と併せて実施することで、若年層による興味本位のサイバー犯罪などの防止に効果があると考えられる。また、産学官連携により、大学・高等専門学校等の高等教育段階における情報技術人材の育成を引き続き推進する。

(4) 各府省庁におけるセキュリティ人材の確保・育成の強化

政府機関における統一的な方針に基づき、セキュリティ対策を専任で担う「サイバーセキュリティ・情報化審議官」による司令塔機能の下、各府省庁におけるセキュリティ人材の着実な確保・育成を継続して進めていく。各府省庁の人材確保・育成計画に基づき、定員の増加による体制整備、レベルに応じて知識・能力を高められる研修や高度なセキュリティ技術者を活用した演習、適切な処遇の確保等について、着実に取り組むとともに、毎年度、計画の見直しを行い、一層の取組の強化を図る。

(5) 国際連携の推進

サイバーセキュリティの問題への対応がグローバルな規模で求められていることを踏まえ、我が国のサイバーセキュリティ人材の育成においても、国内で完結するのではなく、可能な限りグローバルな規模で切磋琢磨できるようにすべきである。このため、人材育成に取り組む大学や公的機関等のプログラムについて、国際的な基準に照らして一定の基準があると認められるものを認定し、共同演習の実施や単位互換の認定など海外の人材育成を行う組織との間での様々な連携を促すための仕組み作りを主要国との連携の下で進める。

加えて、海外におけるサイバーセキュリティ人材育成にも貢献をするため、我が国におけるサイバーセキュリティの人材育成等によって得られた知見を活かし、海外におけるサイバーセキュリティ人材の能力構築に貢献する。

4.4.2 研究開発の推進

実空間とサイバー空間が一体化していく中、サイバー空間におけるイノベーションの進展とそれに対するサイバー攻撃の脅威を踏まえた、実践的なサイバーセキュリティの研究開発が必要である。併せて、中長期的な技術・社会の非連続的進化を視野に入れた対応も必要である。

(1) 実践的な研究開発の推進

IoT、AI など様々な情報通信技術の組合せによって革新的製品やサービスの創出が期待されている。高いレベルのセキュリティ品質を備えた安全・安心な製品やサービスを提供していくことは、我が国の産業の成長、国際競争力の向上を目指していく上で不可欠である。

一方で、こうした技術の活用は、これまでになかった新たな脆弱性を生む可能性がある。このため、AI、ブロックチェーンなどの先進的な技術を用いたサイバーセキュリティ確保の技術、製品・サービスを構成するシステムの中に組み込むセキュリティ技術や、その組み込みの方法に関する実践的な研究開発について重点的に取り組む。特に、サプライチェーンにおける価値創出のプロセスにおける信頼の創出や証明、トレーサビリティ（追跡可能性）の確保とこれらに対する攻撃の検知・防御に関する研究開発を進めるほか、機器に組み込まれた不正なハードウェアやソフトウェアを効率的に検出する技術開発、プラットフォームにおいて利用者の意図しない動作を生じさせるおそれがあるときにもデータや情報の真正性・可用性・機密性を確保するための研究開発を行う。

また、我が国が、サイバー攻撃に対する検知・解析能力を含むサイバー空間の状況把握能力を高め、防御等の対処能力や強靭性の確保等サイバー空間における安全保障の確保にも資する研究開発を推進する。具体的には、政府機関や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃活動を把握することや、ネットワーク上の脆弱な IoT 機器の調査のための広域ネットワークスキャンの軽量化を目指した研究開発等を進める。こうした研究開発の実施においては、セキュリティを運用する現場のサイバー攻撃に関する知見をいち早く共有することによって、その知見を研究開発に活かすとともに、研究開発の成果をいち早くセキュリティを運用する現場で活かすといった好循環のサイクルを形成することが重要である。このため、セキュリティ運用を行う事業者と、国の研究機関等とのリアルタイムでの情報共有を推進する。

さらに、政府機関や重要インフラ事業者等のシステムに組み込まれている機器やソフトウェアについて、必要に応じて、不正なプログラムや回路が仕込まれていないことを検証できる手段を確保することが重要である。このため、国が中心となって、必要な技術的検証を行うための体制の整備を図るとともに、そのために必要となる研究開発に取り組む。加えて、計算機技術の発展（例：量子コンピュータ、AI）を意識した暗号技術など安全保障の観点から国として維持することが不可欠な基盤技術についても研究開発を推進する。

加えて、これらの技術的な研究開発にとどまらず、例えば、サイバーセキュリティに関する法令解釈の明確化等、サイバーセキュリティ対策における制度上の課題に関

する調査・研究を推進する。

これらのサイバーセキュリティの研究開発の取組については、その成果の普及や社会実装を推進する。また、海外のイベント等への積極的な参加等を通じ、国際的な情報発信を行いつつ、我が国と基本的な価値観を共有する有志国との間で、共同研究の実施や研究成果の国際標準化等の研究開発に係る官民の国際連携の強化を図る。

(2) 中長期的な技術・社会の進化を視野に入れた対応

実空間とサイバー空間が一体化していく中、AI や VR といった情報通信技術の進展によって、個々人の異なる価値観を承認しながら、多様な体験を、それらが形成されるプロセスを含めて共有することが実現できるようになってきている。こうした技術が人間にもたらす大きな変化の中で、中長期的には、現在の社会システムや倫理の常識が未来において根本的に変化し、これまでの技術進歩を外挿して、サイバーセキュリティの研究開発を考えるアプローチには限界が来る可能性がある。新しい価値を創出していくためには、実空間とサイバー空間との一体化が進む現状から将来を見据え、行為主体としての人間を含むエコシステムとの視点から社会全体を設計していくような新しいアプローチが必要となっていくことが考えられる。このため、中長期を視野に入れて、サイバーセキュリティと、法律や国際関係、安全保障、経営学等の社会科学的視点、さらには、哲学、心理学といった人文社会学的視点も含めた様々な領域の研究との連携、融合領域の研究を促進する。その際、科学技術を始め各種研究開発の成果が人間社会に悪影響を及ぼすものであってはならないということは言うまでもない。

4.4.3 全員参加による協働

スマートフォンを始めとする端末や公衆無線 LAN の普及によって、国民一人一人が、サイバー空間につながり、多大な恩恵を享受している。IoT の進展によって、今後、その動きは加速していく。一方で、サイバー攻撃の脅威が広がる中、安全・安心にサイバー空間を利用していくためには、実空間における防犯対策や交通安全対策と同様に、サイバー空間で活動する主体としての国民一人一人がサイバーセキュリティに対する意識・理解を醸成し、サイバー空間における様々なリスクに対して対処できることが不可欠になっている。

サイバーセキュリティに対する意識・理解を広く醸成していくためには、国による従来の普及啓発の取組だけでは限界がある。むしろ、国は、地域、企業、学校など様々なコミュニティの自主的な活動を尊重しつつ、各々の関係者が、お互いの役割分担の下で、連携・協働をできるような仕組みを構築し、その仕組みを下支えしていくというかたちでリーダーシップを発揮していく必要がある。

このため、内閣サイバーセキュリティセンターが中心となって、産学官民の関係者が円滑かつ効果的に活動し、有機的に連携できるよう、国は、サイバーセキュリティの普及啓発に向けた総合的な戦略及び具体的なアクションプランを策定するとともに、必要な情報発信や国民からの相談対応を行う。また、産学官民の様々なコミュニティの代表が参加する協議会の場を活用しながら、関係者による実践を推進していく。さらに、サイバーセキュリティに関する国民一人一人の理解を促すための集中的期間として、「サイバーセキュリティ月間」のさらなる充実を図るとともに、国民向けのわかりやすい解説書の作成・普及や、学校教育を通じて、情報モラル教育の一部としてのサイバーセキュリティ教育を推進する。

スマートフォンやパソコン等の機器の製造・販売事業者、通信キャリアやインターネットサービスプロバイダー等の通信事業者は、セキュリティに配慮した製品・サービスの提供や、利用者への説明、相談への対応などを通じて、利用者がサイバーセキュリティの取組を適切に実施できるよう対応することが期待される。このため、国においては、必要に応じて、これらの事業者や関係団体等の取組が促進される環境を整備するとともに、利用者のニーズや利用形態等を踏まえつつ、サイバーセキュリティの確保に資するガイドラインの整備とその着実な実施を推進する。

5. 推進体制

サイバーセキュリティの確保を通じて、情報通信技術及びデータの利活用を促進[62]し、経済・社会活動の基盤とする[63]こと、我が国の安全保障を万全のものとする[64]ことは、従来からの我が国政府の方針である。

この方針の下、政府においては、関係機関がそれぞれの機能を果たし、政府一体となったサイバーセキュリティ対策を推進することが肝要である。このため、内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化を図るとともに、同センターにおいては、本戦略に基づく諸施策が着実に実施されるよう、本戦略を国内外の関係者に積極的に発信しつつ、各府省庁間の総合調整及び産学官民連携の促進の要となる主導的役割を担うものとする。また、危機管理対応についても一層の強化を図る必要がある。とりわけ、2020 年東京大会を控える中、産学官民における参加・連携・協働の枠組みを構築し、サイバーセキュリティの確保に向けた取組の着実な履行が重要である。

本部は、サイバーセキュリティに関する重要事項については高度情報通信ネットワーク社会推進戦略本部と緊密な連携により対応する。加えて、必要に応じて、重大テロ対策本部など危機管理体制と情報共有・連携する。さらに、本部は安全保障に関わる問題については国家安全保障会議の緊密な連携により対応し、内閣官房国家安全保障局による全体取りまとめの下、関係省庁が連携して対応する。

また、本部は、本戦略で示された方向性に基づき、各府省庁の施策が効果的に実施されるよう、経費の見積もり方針を定め、政府としての最適な予算の確保と執行を図る。さらに、情報収集・分析機能の強化や、サイバー攻撃の速やかな検知・分析・判断・対処を一体的サイクルとして行う機能を有する体制の整備に向けて、官民連携を促進する。

今後、本部は、本戦略を的確に実施するため、３年間の計画期間内において、各年度の年次計画を作成するとともに、その施策の進捗状況を検証して、年次報告として取りまとめることとする。また、サイバー空間に係る情勢や技術動向が非連続的に変化することもあり得ることから、必要が生じた場合には、計画期間に縛られることなく、機動的な見直しを実施することとする。

62　世界最先端IT国家創造宣言・官民データ活用推進基本計画（平成29年５月30日閣議決定）は、「データ利活用の促進に当たっては、個人情報やプライバシーの保護、サイバーセキュリティ対策、知的財産権の在り方、データの品質や信頼性・安全性の確保、AI、ロボット時代の倫理の在り方など、同時並行的に対策を講じておくことは言うまでもない」としている。

63　未来投資戦略2017（平成29年６月９日閣議決定）は、「あらゆる場面で快適で豊かに生活できる超スマート社会、Society5.0では、安全なサイバー空間の確保が経済・社会活動の重要な基盤」としている。

64　国家安全保障戦略（平成25年12月17日閣議決定・国家安全保障会議決定）は、「情報の自由な流通による経済社会やイノベーションを推進するために必要な場であるサイバー空間の防護は、我が国の安全保障を万全とするとの観点から、不可欠」としている。

資料1－4

別紙

サイバーセキュリティ戦略案の作成に際しての
高度情報通信ネットワーク社会推進戦略本部意見

「ＩＴ新戦略の策定に向けた基本方針」（平成 29 年 12 月 22 日高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議決定）は、「ＩＴを活用した社会システムの抜本改革」により、ＩＴを最大限活用した簡素で効率的な社会システムの構築を目指すこととしている。具体的には、行政サービスの 100%デジタル化、行政保有データの 100%オープン化及びデジタル革命の基盤整備を通じた「行政サービスのデジタル改革断行」や、この取組の横展開による「民間部門のデジタル改革、ＩＴ・データ活用ビジネスの推進」及び「地方のデジタル改革」を行うとしている。

このような「ＩＴを活用した社会システムの抜本改革」をはじめ、サイバー空間の利用によって新たな価値を創出し、社会課題を解決するにあたっては、サイバーセキュリティの確保が大前提である。こうした観点から、ＩＴ利活用とサイバーセキュリティの双方のバランスを取りつつ、両者のレベル向上を図ることが重要であり、サイバーセキュリティとＩＴ利活用はいわば車の両輪でなければならない。

悪意ある主体によるサイバー空間における脅威が深刻化し、我が国の安全保障・危機管理や国際的な競争力に影響を及ぼすおそれが生じている現下の状況において、「世界最先端 IT 国家創造宣言・官民データ活用推進基本計画」に基づくデータ利活用のための基盤整備等を盛り込んだＩＴ新戦略を推進していく上で、サイバーセキュリティの強化の重要性が増している。

以上の観点から、内閣サイバーセキュリティセンターは、内閣官房情報通信技術（ＩＴ）総合戦略室との緊密な連携により、サイバーセキュリティ戦略を着実に推進するとともに、各府省庁とも連携して政府の情報セキュリティ投資を適切なものとすべく、今後とも、政府一体で対策を図ることとされたい。また、サイバーセキュリティ戦略に基づいた施策の実施に当たっては、これまで実施してきた各施策の成果を検証した上で、サイバーセキュリティ対策の実施機関等に対して、より具体的な取組みを提示し、施策の実効性を高めることに努めていただきたい。

以上を踏まえた上で、閣サ第 494 号により意見聴取のあったサイバーセキュリティ戦略案については異存ない。

資料１－５

サイバーセキュリティ戦略案の作成に際しての国家安全保障会議意見

情報システムや情報通信ネットワーク等により構成されたグローバルな空間であるサイバー空間は、社会活動、経済活動、軍事活動等のあらゆる活動が依拠する場となっている。

「国家安全保障戦略」（平成 25 年 12 月 17 日閣議決定）において、サイバー問題を我が国がとるべき国家安全保障上の戦略的アプローチの一要素と位置付けているとおり、サイバー攻撃からサイバー空間を守り、その自由かつ安全な利用を確保することは、我が国の安全保障上重要である。

以上の観点から、サイバーセキュリティ戦略案の作成に際し、内閣サイバーセキュリティセンターは、国家安全保障局と密接な連携を図るとともに、以下の視点を十分に踏まえられたい。

１．サイバー空間に関する現状認識

サイバー空間における安全保障を取り巻く環境は、以下のとおり一層深刻化している。またサイバー空間の秩序を自国に有利に作り変えようとする国家の動向にも留意が必要である。サイバー攻撃は、今そこにある危機であるとの認識を持ち、安全保障の根幹となる極めて重要な課題として、サイバー空間における安全保障の確保に取り組む必要がある。

（１）国家主体が関与する(States and state-sponsored)サイバー攻撃の発生

個人や犯罪集団によるサイバー犯罪にとどまらず、政治的、経済的、社会的目的等により、国家主体が関与する形(States and state-sponsored)で、政府機関・政府関連機関、重要インフラ、先端技術を有する企業・学術機関等への攻撃が戦略的に行われ、民主主義制度の根幹を揺るがしかねない事案も発生している。

（２）安全保障上重大な攻撃の発生

電力、通信、金融、医療機関等、その機能停止が国民生活に多大なる影響を及ぼしかねない重要インフラへの攻撃、サイバー攻撃による宇宙関連技術、原子力関連技術、防衛装備品に関する情報等の我が国の安全保障上重要な情報の窃取、政治目的の攻撃等、重大な攻撃が発生している。

（３）国家安全保障上の活動を妨げる攻撃の発生

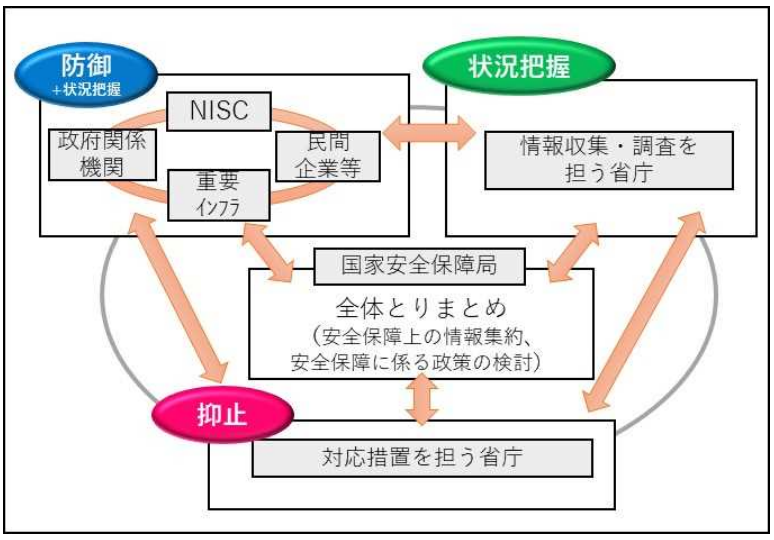
諸外国において軍事活動の一環としてサイバー攻撃を行う動きが出てきており、仮にサイバー攻撃により自衛隊の重要なシステムの機能が停止した場合、我が国の防衛の根幹に関わる問題が発生する可能性がある。自衛隊の部隊の指揮統制及び通信の維持、自衛隊・在日米軍等の任務保証等、我が国の安全保障上の活動を妨げることを目的としたサイバー攻撃に対する対処が必要である。

2．サイバー空間における安全保障の確保に関する目標と役割

上記の状況を踏まえ、サイバー攻撃から我が国の国家安全保障上の利益を守るため、以下の取組を進める。

（1）サイバー攻撃に対する国家の強靱性を確保する。【防御力】
（2）サイバー攻撃に対する抑止力を向上させる。【抑止力】
（3）サイバー空間の状況を把握する能力を強化する。【状況把握力】

上記の取組に関しては、内閣官房国家安全保障局による全体取りまとめの下、防御は NISC を中心として官民を問わずすべての関係機関・主体、抑止は対応措置を担う省庁、状況把握は情報収集・調査を担う省庁が、平時から連携し対応する。また必要な場合には、国家安全保障会議で議論・決定を行う。



3．サイバー空間における安全保障の確保のための取組

サイバーセキュリティとは、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[1]。このた

[1] サイバーセキュリティ基本法第二条

め、サイバーセキュリティは主として防御が中心の概念ではあるが、サイバー攻撃に対する抑止力の向上やサイバー空間の状況を把握する能力を強化することは、広義の意味で我が国のサイバーセキュリティの確保につながるものである。新たなサイバーセキュリティ戦略では、防御を中心としつつも、抑止や状況把握を含めた、以下を含む施策を推進することが望ましい。

（１）サイバー攻撃に対する国家の強靱性の確保

サイバー空間に係る安全保障の確保のためには、国家の関与が疑われるものを含むサイバー攻撃から、政府機関、重要インフラ等の任務・機能を保障するなど、サイバー空間の防護のための取組を一層強化し、我が国自身の強靭性を確保していくことが肝要である。

○　政府機関・重要インフラ等の防護

政府機関は、国民生活や経済社会活動を守り、支える任務を有しており、その機能停止や、政府機関が有する機密情報に対する情報窃取は、厳として回避しなければならない。また、重要インフラその他の社会システムを担う事業者は、政府機関の任務遂行はもちろん、国民生活や経済社会活動に不可欠なサービスを持続的に提供するという重要な任務を有している。したがって、こうした重要インフラその他の社会システムを担う事業者のサイバーセキュリティの確保は、我が国の安全保障上、極めて重要な課題である。

そのため、政府機関の任務を保証する観点から、自らが保有するネットワーク・インフラの防護の強化、政府機関の行政遂行上必要な社会システムに対するサイバーセキュリティの確保等、政府機関の対策を強化する。特に、安全保障上の活動を担う要である防衛省・自衛隊については、その活動が依存するネットワーク・インフラの防護の強化や、自衛隊の任務保証に関連する主体との連携の深化を図る等、任務保証等に重点的に取り組む。また警察、自衛隊を始めとする対処機関の能力を質的・量的に向上させる。

重要インフラに関しては、情報共有、人材育成、リスク評価、技術基準、サプライチェーン等を含め、制御系システムを含む重要インフラ防護の対策を強化する。さらに宇宙関連技術、原子力関連技術、セキュリティ技術、防衛装備品に関する技術等、我が国の安全保障上重要な技術に関して、サイバー情報窃取への対策を強化する。

○　安全なサイバー空間の構築

あらゆるモノがインターネット等のネットワークに接続され、新たな価値を創造する IoT（Internet of Things）が急速に進展する一方、IoT 機器を踏み台

としたサイバー攻撃等が深刻化している。また、諸外国では、通信ネットワークを構成する機器や端末等に関して、安全保障上の懸念を指摘する動きもある。安全なサイバー空間の構築に向けて、IoT 機器の脆弱性対策を含む IoT セキュリティ対策、国が中心となって技術的な検証を行うための体制整備等、必要な対策を進める。

○　積極的サイバー防御

サイバー空間における攻撃者は、その手口を常に変化させ続けている。サイバー空間は、その構成上、脆弱性が内在しているものであるという現実を認識した上で、被害が発生してから対応するのではなく、先手を打って必要な政策を展開することが必要である。サイバー空間のサイバー脅威情報（CTI: Cyber Threat Intelligence）[2]を活用した先行的なサイバーセキュリティ対策、通信事業者間における攻撃情報の共有・活用の促進など、積極的サイバー防御[3]に向けた取組を進める。また、サイバー空間における安全保障の基本的な方針として、同盟国・有志国との間での積極的サイバー防御に関する政策調整に努める。

○　国際連携の推進

サイバー空間における脅威は容易に国境を超えることから、一国のみで自らの平和と安定を守ることには限界があり、国際社会が連携・協力して対応していくことが重要である。同盟国・有志国と密接な連携がとれるよう、二国間サイバー協議を軸としつつ、政府内における各機関と各国のカウンターパートとの日常的な情報共有・政策調整のための連携体制を強化する。また日本を含む世界全体へのサイバー攻撃によるリスク低減のため、開発途上国における能力構築支援についても積極的に実施していく。

○　研究開発の推進

サイバー攻撃は日々進化し高度化・複雑化しており、その変化に対処・対応していくため、創意と工夫に満ちたサイバーセキュリティ技術を生み出すための充実した研究開発の推進が不可欠である。サイバー攻撃に対する強靱性の確保、サイバー安全保障に資する科学技術、国家安全保障の観点から国として維持することが不可欠な科学技術（暗号技術、サイバー空間の基盤となる通信技

---

[2] サイバーセキュリティに関する様々な情報をつなぎ合わせることで導かれる脅威等に関する情報のこと。このような情報をセキュリティ対策に活用することで、先行的な防御が可能となることが期待される。

[3] サイバー攻撃に対して能動的に防御していく取組のこと。

術・通信機器技術、機器等の信頼性検証技術等）について、研究開発を推進する。

（２）サイバー攻撃に対する抑止力の向上

現在、サイバー空間では、国家の関与が疑われるものを含め、組織的かつ周到に準備された高度なサイバー攻撃の脅威が増大している。このような中、サイバー空間における安全保障を確保するためには、サイバー攻撃に対する対応力を強化し、悪意のある者の行動を抑止することが必要である。

○　実効的な抑止のための対応

我が国は、G7 伊勢志摩サミットで宣言されたとおり、国際連合憲章を含む国際法は、サイバー空間において適用可能であるとともに、一定の場合には、サイバー活動が国際連合憲章及び国際慣習法にいう武力の行使又は武力攻撃となり得ると認識している。また、G7 タオルミーナ・サミットにおける宣言（ルッカ宣言）のとおり、紛争の予防及び紛争の平和的解決のため，武力攻撃に至らない違法行為（悪意のあるサイバー活動を含み得る。）に対して、国際違法行為の被害者である国家は、一定の場合には、その違法行為について責任を有する国家に国際的な義務を遵守させるために、当該責任を有する国家に対して均衡性のある対抗措置（ICT を介して実施する措置を含む。）及びその他の合法的な対応をとることが可能であると認識している。

我が国の安全保障を脅かすようなサイバー空間における脅威から国民の安全・権利を守り、悪意のある者の行動を抑止するためには、脅威に応じて、様々な対応措置を進めていくことが必要である。

以上の認識を踏まえ、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。

また、上記の対応をとる観点から、法執行や国際ルールの活用等を含め、警察、外務省、自衛隊を始めとする関係機関の能力強化、対応措置の実施に必要な国内の体制の強化（サイバー空間の状況把握、関係府省庁間の連携等）、協調行動の実施に必要な有志国との連携体制の強化・拡大（情報共有体制、政策協調体制等）を進める。

○　国際連携・信頼醸成措置

サイバー攻撃には、匿名性・隠密性等の特性があることから、意図せず国家間の緊張が高まり、被害国との間でエスカレーション等が生じるリスクもある。また国を超えるインシデントが発生した場合の、様々な階層における国際

的な連絡体制を平素から構築しておくことが重要である。このように偶発的な衝突を防ぐとともに国家間の信頼を醸成する見地から、各国と情報交換、政策対話、交流などを進める信頼醸成措置を推進する必要がある。

我が国は、これまでも、信頼醸成措置として、米国、オーストラリア、英国、フランス、インド、イスラエル、エストニア、ロシア、EU、ASEAN 等との協議・対話、日中韓等の 3 か国の枠組みでの協議・対話等の多国間の協議など、二国間・多国間の取組を実施してきている。今後は、上記以外の国との協議・対話も更に積極的に進めていく。また、諸外国と協力し、サイバー空間の問題を調整する国際的メカニズムについても検討していく。

○　法の支配の推進

サイバー空間に関しては、既存の国際法の適用のあり方等について我が国を含む諸国とは異なる意見を持つ国も存在する。そのため、既存の国際法の適用に関する議論の継続と並行して、まずは自発的な拘束力のない規範を国際社会に広げ、国家実行を積み重ねていくことで、そうした規範に反する行動を国家がとることを抑止することを目指していくことが重要である。国際的な規範を普遍化し、実行していくことは、悪意のある者を国際的に容認しないことを意味し、我が国の安全保障と世界の平和に寄与するものである。我が国は、サイバー空間の一層の安定性確保のため、G7、国連等の場において、日本の立場を明確にしつつ、引き続きサイバー空間における法の支配の推進を主導していく。

（３）サイバー空間の状況把握の強化

サイバー攻撃に対する国家の強靭性の確保並びに抑止力の向上を実現する前提として、官民や国の枠を超えあらゆる関係機関・主体の連携を通じて、国民生活・経済社会活動に影響を与える可能性のあるサイバー空間に関する事象を各機関が適切に把握するとともに、然るべき対応措置を採るために敵対的活動を検知・調査・分析し、攻撃元を把握する能力を強化することが必要である。

○　防御のための状況把握

サイバー攻撃は複雑・巧妙化し続けており、多様な脅威に的確に対処するためには、各主体が連携してサイバー攻撃の可能性がある障害情報を共有し、攻撃の兆候を含む状況を早期に認識・把握することが必要である。このため、戦略的かつ迅速な情報共有を図るとともに、通信事業者間でサイバー攻撃の発信元となる電気通信設備の情報を共有する制度の整備や、インシデント情報共有・分析機能を有する組織である ISAC（Information Sharing and Analysis

Center）を金融、ICT、電力等以外の分野にも拡大するなど、官民間・民民間における一層の情報共有の拡充を進める。

○　抑止のための状況把握

サイバー空間における敵対的活動を検知・調査・分析し、攻撃者を追い込むことなくして、サイバー空間における抑止力を効果的に高め、我が国の平和と安全を維持することは困難である。このため、具体的に以下の取組を進める。

① 捜査・調査機関の能力向上

高度化・複雑化するサイバー攻撃の脅威を抑止していくためには、対応力の強化に加え、サイバー攻撃を検知・調査・分析する能力の一層の向上が求められる。捜査・調査機関の能力を質的・量的に向上させ、情報収集・情報分析能力を強化する。またその役割を十分に果たすため、人材育成・確保、最新技術の導入・習得、諸制度の見直し等、あらゆる有効な手段について、幅広く検討を進める。

② 検知・調査・分析等に資する技術の開発・活用

隠密性が高く攻撃者優位と言われるサイバー空間を、平和で安全な空間にしていくために、プライバシーの保護等の人権にも配慮しつつ、悪意のあるサイバー攻撃に対する透明性を高めていくことが必要である。我が国の先端技術の力を結集して、サイバー空間における敵対的活動を検知・調査・分析等するための技術の開発・利用を推進する。

③ 情報連携

悪意のあるサイバー活動を抑止し、調査・追跡していくためには、政府内関係省庁及び同盟国・有志国等との国内外の情報連携が不可欠である。政府内の情報共有体制の強化、外国政府機関とのサイバー脅威情報（CTI）の共有等、サイバー攻撃に対する対応能力向上のための情報連携を進める。

（了）