新たな「サイバーセキュリティ戦略」について

内閣官房内閣サイバーセキュリティセンター　参事官　吉田（よしだ）　恭子（きょうこ）

1. はじめに

2018年7月27日、おおよそ3年ぶりとなる新たなサイバーセキュリティ戦略が閣議決定された。新しい戦略は、実空間との一体化に伴ってサイバー空間がもたらす恩恵と脅威を踏まえ、人工知能（AI）やIoT等による新たな価値の創出を支えるためのサイバーセキュリティの推進、国民・社会を守るための官民の任務保証、自由・公正かつ安全なサイバー空間の堅持等を支える施策について定めた、サイバーセキュリティに関する政府の基本的な計画となる。本戦略の策定に携わった立場から、本稿では、新たな戦略の背景にある基本的な考え方や戦略のポイントについてご紹介させていただく。

2. サイバーセキュリティ政策の推進体制

その前提として、我が国の政府全体のサイバーセキュリティ政策の推進体制についてご説明したい。政府の中でサイバーセキュリティ体制が構築される契機となったのが、2000年の各省庁のHP改ざんの事案である。この事態を受けて、同年2月に内閣官房に情報セキュリティ対策推進室が設置され、以後、国内外で各種サイバー攻撃が頻発・高度化していく中で、我が国のサイバーセキュリティ政策の大きな転換点になったのが、2014年に成立したサイバーセキュリティ基本法である。同法の制定によって政府の推進体制が法的に担保されることとなり、2015年1月にサイバーセキュリティ戦略本部が新たに設置された。内閣官房内閣サイバーセキュリティセンター（NISC）は当該本部の事務局としてその活動を支えている。

NISCの業務は、大きく分けると、①外部からのサイバー攻撃等に対して、政府関係機関の緊急対応能力強化を図るために整備されているGSOC（政府機関情報セキュリティ横断監視・即応調整チーム）に関する事務、②原因究明調査に関する事務、③監査等に関する事務、④サイバーセキュリティに関する企画・立案、総合調整、の4つを主たる所掌事務としている。

また、政府のサイバーセキュリティに関する予算は、2018年度当初予算が前年比約22億円増の約621億円、2017年度補正予算が約33億円となっており、厳しい財政状況の中で確実に措置されてきている。NISCにおいても、2020年東京オリンピック・パラリンピック競技大会に向けたサイバーセキュリティ対処調整センター構築のための措置等が講じられている。

3. サイバー空間と実空間の一体化に伴う脅威の深刻化

新たなサイバーセキュリティ戦略は、サイバーセキュリティ基本法に基づいて策定される2回目の戦略であり、2020年以降の目指す姿も念頭に置きつつ、サイバーセキュリティに関する我が国の基本的な立場と今後3年間の諸施策の目標と実施方針を国内外に示すものである。

また、今般の戦略は、2018年4月に発表された自由民主党サイバーセキュリティ対策本部の第1次提言の内容等を踏まえたものとなっている。

新たな戦略は、「1 策定の趣旨・背景」、「2 サイバー空間に係る認識」、「3 本戦略の目的」、「4 目的達成のための施策」及び「5 推進体制」という5つの章から構成されている（**図1**参照）。

第1章及び第2章の検討過程において、現在のサイバー空間の状態をどのようにとらえるべきかという点を踏まえつつ、その上で、我が国が目指すサイバーセキュリティの姿とはどのようなものかという点について、NISC内はむろんのこと、政府部内さらには外部の有識者の方々と多くの議論を重ねた。

3年前の戦略を策定した際のキーワードは「連接融合情報社会の到来」ということで、サイバー空間と実空間（フィジカル空間）が徐々に融合していくのではないかとの考えに基づいていたが、今般の戦略においては、サイバー空間と実空間が既に一体化しており、それによって経済社会や国民生活、すなわち我々の活動空間自体がますます拡張している状態であるとしている。具体的には、今ではAIやIoTをめぐる話題がメディアに登場しない日はなく、AIは第1次及び第2次のブームを経て、深層学習に支えられた第3次ブームの時期を迎えている。また、ネットワークにつながるIoT機器は2020年には約300億個に拡大する見通しとなるなど、その数は爆発的に増加している。これらの技術が様々

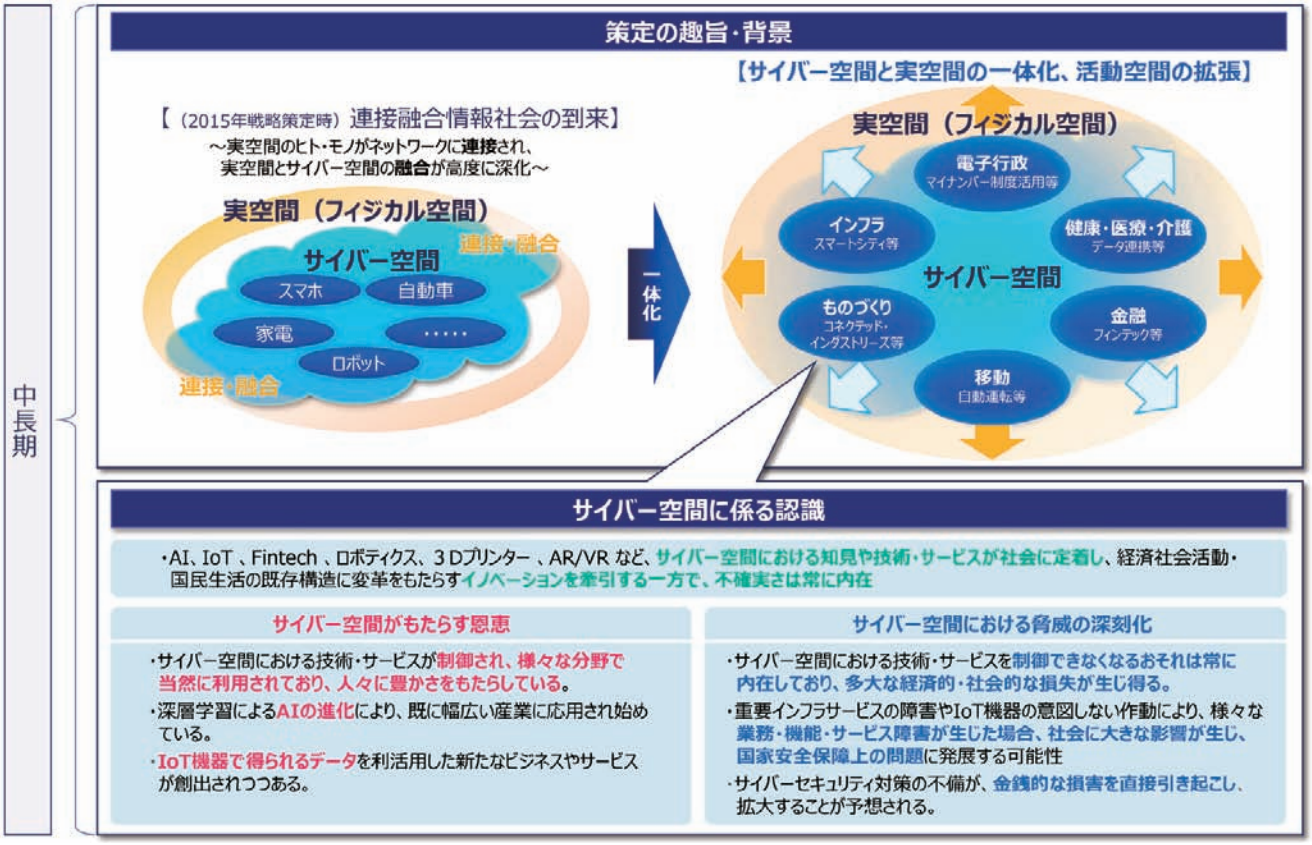
■図1. 新たな「サイバーセキュリティ戦略」及び「サイバーセキュリティ 2018」の概要

なサービスを生み出し、経済成長や国民生活の利便性向上を牽引している。

その一方で、サイバー空間と実空間の一体化を踏まえ、サイバー空間における脅威もまた深刻化・巧妙化している。すなわち、サイバー空間におけるAI、IoT、Fintech等の技術・サービスの定着はイノベーションを牽引する一方で、それらを制御できなくなるおそれを常に内在しており、誤った対処等により、多大な経済的・社会的損失が生じ得る状態となっている。また、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ずる可能性がある（図2参照）。

脅威の深刻化の具体的な例として、国内では例えば、2018年1月に発生した仮想通貨の窃取を狙った攻撃が記憶に新しいところである。仮想通貨交換業者が保有していた仮想通貨が不正に外部に送信され、約580億円相当の金銭価値が消失した。海外では、2016年にバングラデシュの銀行がハッキングを受けて約8100万ドル（約91億円）が不正送金され、また、ウクライナの電力供給会社の変電所がサイバー攻撃を受け約1時間の停電が発生するという事案も発生している。同年9月には米国で、IoT機器に感染し史上最大規模のDDoS攻撃を仕掛けた新型マルウエア“Mirai”が登場し、防犯カメラや家庭用ビデオレコーダーなどを“踏み台”にしてインターネット関連サービス事業者のシステムが攻撃にさらされ、この時は日本のサービス事業者も影響を受けている。また、2017年5月に発生したランサムウェア「WannaCry」の感染により、英国では国民保健サービス関連システムが停止し、多数の病院で医療サービスが中断するなど、世界各国で被害が発生した。

また、2018年7月のサイバーセキュリティ戦略本部で決定した「サイバーセキュリティに係る年次報告（2017年度）」において、政府機関等に対するサイバー攻撃の傾向の分析結果を発表している。同報告によれば、前述のGSOCなど各種対応により攻撃件数自体は減少傾向にあるが、既知の脆弱性に対する攻撃等が減少する一方、脆弱性情報の公表直後の攻撃の増加や不審メールの巧妙化が確認されて



■図2.［1. 策定の趣旨・背景］及び［2. サイバー空間に係る認識］のポイント

おり、予断を許さない状況である。

このように、あらゆる機器、システム、サービスがネットワークでつながる現代社会において、ひとたびサイバー攻撃が発生して適切に対処できない場合には、多大な経済的・社会的損失をもたらすことになる。また、攻撃者は、ネットワークの最も脆弱なところを狙ってくることから、一部の組織・事業者だけがセキュリティ対策を講じるだけではもはや対処できない状況になっていることを前提に、対策を進めていくことが必要となっている。

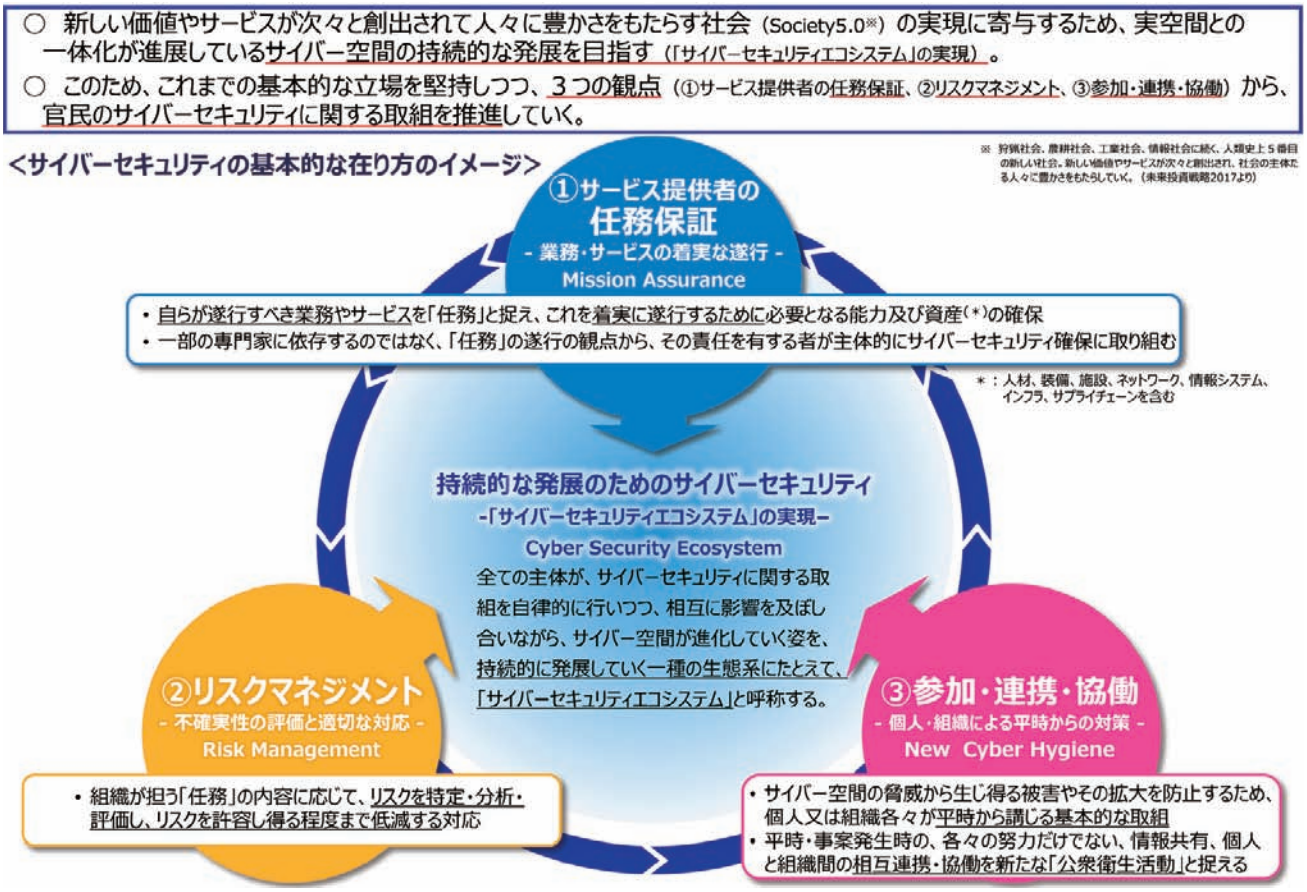
4. 新戦略のキーワードは「任務保証」、「リスクマネジメント」、「参加・連携・協働」

このような現状認識の下、第3章「本戦略の目的」では、今後、我が国としてどのようなサイバーセキュリティの姿を目指すのかということを議論し、打ち出している。

この点について、サイバーセキュリティありきではなく、サイバーセキュリティにしっかり取り組むことによってサイバー空間の持続的な発展を図り新しい産業やサービスが創出される「サイバーセキュリティエコシステム」の実現を目指すというのが基本的な考え方となっている。セキュリティ至上主義になってしまうと、最も確実な防御策はそもそもネットにつなげない、情報通信技術を活用しないということになりかねないが、それはもはや現実的な対処ではない。政府は、「Society 5.0」という、実空間とサイバー空間を高度に融合させたシステムにより、経済社会と社会的課題の解決を両立する人間中心の社会を目指しており、データ主導社会の到来に伴い、サイバー空間を利用することと守っていくことは表裏一体として進めていく必要がある。

このため、新たな戦略では、サービス提供者の「任務保証」、「リスクマネジメント」、「参加・連携・協働」という3つの観点でサイバーセキュリティの対策を進めていく必要があるとしている（図3参照）。

1つ目がサービス提供者の「任務保証」である。これは、官民問わず、全ての組織が、自らが遂行すべき業務・サービスを「任務」と捉え、その着実な遂行を目指す、そのために必要となる能力及び資産を確保するという考え方である。その際には、一部の専門家に依存するのではなく、「任務」の遂行に責任を有する者が主体的にサイバーセキュリ



■図3.［3. 本戦略の目的（目指すサイバーセキュリティの基本的な在り方等）］のポイント

ティの確保に取り組むことが重要である。

2つ目の観点が「リスクマネジメント」である。これは、不確実性の評価とそれに基づいて適切な対応を行うということである。サイバー攻撃のリスクは決してゼロにはならないとの認識を持った上で、事前にそのリスクを特定・分析・評価し、リスクを許容し得る程度まで低減していくということが重要となる。

そして、3つ目の観点が「参加・連携・協働」である。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には、個人やそれぞれの組織・企業が、平時から基本的な対策をしっかり講じていくことが重要となる。その上で、各々の努力だけでは十分に対処できない部分については、情報を共有したり、官民で連携するなどの相互連携・協働を図る必要がある。このような活動は、いわばサイバー空間における新たな公衆衛生活動としてとらえることもでき、今後、その重要性が高まっていくと考えられる。

5. 経営層の意識改革、官民の任務保証、グローバルな対応のための諸施策

第4章の「目的達成のための施策」は、経済界・産業界との関係が深い「経済社会の活力の向上及び持続的発展」、国民生活に直結する重要インフラなどを守る「国民が安全で安心して暮らせる社会の実現」、グローバルな対応を示した「国際社会の平和・安定及び我が国の安全保障への寄与」、そしてこれら全体を支える人材育成・確保や研究開発推進等の「横断的施策」の4つの柱から構成されている。

まずは1つ目の柱である「経済社会の活力の向上及び持続的発展」のポイントについて、経済界・産業界においては、「サイバーセキュリティ対策はリスクマネジメントの一環」という認識の下で取組みを進めていくことが重要であるとしている。災害対策をはじめとして事業を遂行する上では各種のリスクが存在する中、とりわけサイバーセキュリティに関して経営層の方々は社内外の専門家に対策を一任する傾向が見られるが、このような状況を変えていく必要がある。

既に大企業は一部の産業分野においては経営層がリーダーシップをとってサイバーセキュリティ対策に取り組む動きが見られるが、事業の規模や分野を問わず、経営層の意識改革を進め、自身が組織のリスクマネジメントをリードしていくといった意識の下で対策に取り組んでいくことが重要となる。この点について、2018年3月に「経団連サイバーセキュリティ経営宣言」が公表されるなど、経済界における積極的な取組みが始まっており、今後も官民で連携していくことが必要となる。また、企業におけるセキュリティ投資を進めることも重要である。例えば、政府においては今年度から「コネクテッド・インダストリーズ税制」を設け、事業者のセキュリティ対策の強化と生産性向上の取組みを支援している。

次なるキーワードが「サプライチェーン」である。今、米国でも議論が進んでいるが、大企業に端を発する供給網のどこかでサイバー攻撃が発生するとその影響が全体に及ぶおそれが高いため、サプライチェーンにおけるセキュリティ対策をどのように構築していくのかが問われることになる。この課題について、政府においては、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作成する予定となっている。また、サプライチェーンには中小企業が入ってくるので、その取組みの底上げを進めていくことも重要である。その1つの方策として、我が国においても広がりを見せ始めているサイバーセキュリティ保険が有効であると考えられ、官民が連携して、そのような取組みを広げていくこととしている。

また、全てのモノがネットワークにつながってきている中、安全なIoTシステムの構築も欠かせない。具体的には、パスワード設定に不備のあるIoT機器の調整を行い、電気通信事業者の協力の下で当該機器の利用者を特定し設定変更を促す取組みや、IoTシステムにおけるセキュリティの体系整備と国際標準化等を進めることとしている。

2つ目の柱である「国民が安全で安心して暮らせる社会の実現」は、「国民・社会」「重要インフラ」「政府機関」「大学」「2020東京大会」「従来の枠を超えた情報共有・連携体制」「大規模サイバー攻撃への対処態勢強化」の7つの項目によって構成されている。最初の3つの項目は、これまでの戦略にも入っていたが、あとの4つの項目については、最近の状況や2020年東京大会を控えていることを踏まえ、今般の戦略で新たに盛り込んだ事項となる。ここでは、政府機関、地方自治体、重要インフラ事業者、大学等、それぞれの組織が必要な対策を実施しつつ、多様な関係者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り、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、「任務保証」の考え方に基づく取組みを推進していくということが基本的なコンセプトとなっている。

そして、この柱のキーワードの1つは「積極的サイバー防御」である。これは、攻撃が実際に発生してからそれに対処するという受け身の体制ではなく、サイバー攻撃に対して能動的に防御していくという考え方である。例えば、攻撃の予兆情報等を関係者で共有して対策を講じるといったこともその1つの対応と言えよう。

また、重要インフラの防護に関しては、電力・ガス・通信等の13分野に加え、2018年7月に、新たに空港の分野が加わり、計14分野となった。各分野の所管省庁と関係機関が連携しながら、「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」に基づいて施策を進めていくこととなっている。具体的には、業務内容や組織の規模等を考慮した安全基準等の継続的な改善や官民の枠を超えた様々な規模の主体間での訓練・演習の実施、脅威情報の共有等が挙げられる。さらに、2018年7月には「重要インフラサービス障害等の深刻度評価基準」が発表された。これは、サイバー攻撃により発生した重要インフラ障害等が国民社会に与える影響の深刻さを、NISCが評価・公表することにより、事業者、政府機関、国民等がその深刻さに関する共通の理解を得て、冷静かつ適切な対応を行えるようになることを目的とする取組みであり、初版として決定したものとなる。

さらに、政府機関等におけるセキュリティ強化・充実についても、2018年7月に改定された「政府機関等の情報セキュリティ対策のための統一基準群等」に基づき、新たな技術を活用し、情報システムのセキュリティ水準の向上を進めるとともに、その確認を通じて、従来の攻撃側優位の状況を改善すること等を盛り込んでいる。

2020年東京大会との関係では、2018年2月～3月、平昌オリンピック・パラリンピック競技大会が開催された。同大会の準備期間中は約6億件、大会期間中は約550万件の攻撃が発生した。2020年東京大会の開催まで2年弱となる中、我が国は、この間のサイバー空間の発展状況等も見据えながら、対策を取っていくことが必要となる。そのために必要となる、官民の多様な主体が相互に連携し、施策の推進に係る協議会の創設等を措置するためのサイバーセキュリティ基本法の一部を改正する法律案を先の通常国会で提出したところである。

次に、3つ目の柱である「国際社会の平和・安定及び我

が国の安全保障への寄与」については、「自由、公正かつ安全なサイバー空間の堅持」、「我が国の防御力・抑止力・状況把握力の強化」、「国際協力・連携」という3つの項目から構成されている。特に、今回の戦略では、2つ目の「我が国の防御力・抑止力・状況把握力の強化」というコンセプトを明確に打ち出した点に特徴がある。具体的には、自衛隊をはじめとする防衛関係機関の任務保証や、先端技術を有する組織ではその防御に努める必要がある。また、ひとたびサイバー攻撃を受けたならば、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全ての有効な手段と能力を活用し断固たる対応をとることとしており、このような活動により攻撃そのものを抑止していくことが大事であるという考え方に基づくものである。このような観点から、サイバー攻撃に関する脅威情報を、立場を同じくする有志国間で積極的に共有することも進めていく取組みも重要である。

6.「戦略マネジメント層」の人材育成を

最後に、4つ目の柱である「横断的施策」のうち、特に人材育成について触れたい。

サイバーセキュリティの推進に当たって、我が国における大きな課題になっているのがサイバーセキュリティ人材の確保・育成である。とりわけ、これからはいわゆる「戦略マネジメント層」、すなわち、これまで橋渡し人材と言われてきた層の人材を企業においてどのように育てていくかが問われている。先に述べたように、経営層がセキュリティの意識を持つことはもちろん重要であるが、経営層が専門的なことの全てを把握することは困難である。一方で、実務者層の人材は技術や現場の対応に特化しているため、その間を円滑につなぐべく、自らの組織のビジネス戦略を踏まえた上で、ある程度の権限を持ってサイバーセキュリティに関する対策の企画立案ができる人材層が必要であり、また育てていく必要がある。このような認識の下、NISCでは、2018年5月に「サイバーセキュリティ人材育成取組方針」を策定したところである。本方針においても、戦略マネジメント層の育成・確保が重要とする一方、組織におけるかかる人材層の定着を課題として掲げており、今後、政府全体で取り組んでいくことが重要である。

そのほか、新たな戦略では、横断的施策の1つとして、実践的な研究開発の推進やサイバーセキュリティに関する普及啓発の必要性についても触れている。普及啓発の関係では、今後、アクションプログラムの策定等に取り組むこととしている。また、NISCでは、サイバー攻撃の事案やそれに関する各種情報をSNSで随時発信しているところである。

7. NISCを中心とする関係機関の一層の能力強化を

最後に、戦略の最終章となる「推進体制」の章において、NISCを中心に関係機関の一層の能力強化を図るとともに、各府省庁間の総合調整及び産学官民連携の主導的役割を担うこととされている。また、各府省庁の施策が着実かつ効果的に実施されるよう、必要な予算の確保と執行についても言及されているところである。今後、NISCにおいては、関係の皆様方のご指導・ご協力をいただきながら、本戦略に基づく諸施策が着実に実施され、戦略の目的が達成されるよう取り組んでまいりたい。