サイバーセキュリティ戦略本部
第２回会合　議事概要

１　日時

平成27年５月25日（月）　８：30～９：30

２　場所

総理大臣官邸４階大会議室

３　出席者（敬称略）

安倍　晋三	内閣総理大臣
菅　義偉	内閣官房長官
山口　俊一	情報通信技術（ＩＴ）政策担当大臣
山谷 えり子	国家公安委員会委員長
西銘 恒三郎	総務副大臣
中山　泰秀	外務副大臣
山際 大志郎	経済産業副大臣
原田　憲治	防衛大臣政務官
遠藤　信博	日本電気株式会社代表取締役執行役員社長
小野寺　正	ＫＤＤＩ株式会社代表取締役会長
中谷　和弘	東京大学大学院法学政治学研究科教授
野原 佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
林　紘一郎	情報セキュリティ大学院大学教授
前田　雅英	首都大学東京法科大学院教授
村井　純	慶應義塾大学教授
加藤　勝信	内閣官房副長官
世耕　弘成	内閣官房副長官
杉田　和博	内閣官房副長官
谷内 正太郎	国家安全保障局長
西村　泰彦	内閣危機管理監
遠藤　紘一	内閣情報通信政策監
髙見澤 將林	内閣サイバーセキュリティセンター長
古谷　一之	内閣官房副長官補

４　議事概要

(1)　本部長冒頭挨拶

前回２月の会合において、安倍総理から、新たなサイバーセキュリティ戦略の策定について指示があった。本日はその戦略（案）について御議論をお願いする。有識者の皆様には、戦略（案）の起草に御協力いただき、感謝申し上げる。

先月４日には、フランス放送局に対するサイバー攻撃によって、当局のテレビ放映システムが機能停止するという事件が発生した。重要インフラである報道機関へのこうした行為は決して許されるものではない。サイバーセキュリティは危機管理、安全保障の上からも、また我が国経済の成長を推進する上からも必要不可欠なものになっている。特に、2020 年のオリンピック・パラリンピック東京大会を見据えたときに、こうした多角的観点からしっかりとしたサイバーセキュリティ戦略を策定するということは極めて大事であると考える。皆様においては、今回の会合でも活発な御討議をお願いしたい。

(2)　討議

【決定事項】

・　サイバーセキュリティ戦略（案）について
・　サイバーセキュリティ対策を強化するための監査に係る基本方針について
・　重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針等について

【報告事項】

・　NISC と関係機関との協力について
・　政府のサイバーセキュリティに関する予算について

上記について、事務局より資料に基づき説明が行われるとともに、本部員より意見が述べられた。

○（中谷本部員）私から５点申し上げる。

第一に、近年、国際社会における法の支配が特に重要視されているが、その中でも我が国にとって特に重要なのが海洋とサイバーである。それは、この二つの分野において、力による一方的な現状変更や秩序破壊を目指す国外の勢力が残念ながら存在するからにほかならない。この意味で、今回のサイバーセキュリティ戦略（案）において、サイバー空間における国際的な法の支配の確立がしっかりと書き込まれ、国際的な規範形成と規範実現の積極的な推進がうたわれたことを高く評価したい。

第二に、国際的な連携について述べる。まず、同盟国である米国について、４月 27 日の「日米防衛協力のための指針」でサイバー空間に関する協力が明記されたことは日米双方の安全保障にとってはもとより、アジア太平洋地域や国際社会全般のサイバー環境にとっても重要な意義を有する。また、戦略（案）にもあるとおり、価値観を同じくする欧米諸国とは最先端の共同プロジェクトを、途上国にはキャパシティビルディングを引き続き積極的に推進していくことが重要である。同時に、サイバー問題について何らかの懸念のある国との間でも信頼醸成措置を進めることが重要であり、いわばテー

ラーメードのサイバー外交が求められていると思われる。

第三に、特にこのサイバーセキュリティの分野では、政府の方針を正しく英語で発信することが、透明性の向上の観点からも、また、サイバー外交を主導する観点からも重要であり、今回の戦略（案）もパブリックコメントを経て採択された際には、できるだけ早く英訳を公表することが望ましい。また、サイバーセキュリティ基本法についても、まだ英訳の仮訳が公表されていないのであれば、可能な限り早く英訳を作成して公表することが望ましい。

第四に、重要インフラの対象に化学、クレジット、石油が新たに指定されたことは良いことであるが、ほかにも例えば航空は入っていても空港は入っていないとか、上水道は入っていても下水道は入っていないなど、重要インフラと考えられるにもかかわらず指定されていない分野があると思われる。抜け穴が生じてしまうことがないように包括的にカバーできる体制を一刻も早く整えるべきであり、関係業界の御理解をお願いしたい。

第五に、民間企業による情報セキュリティリスクの開示を推進することが重要であることは言うまでもないが、民間企業自身にインセンティブを与える意味でも、格付会社が格付に当たって、情報セキュリティ対策を評価基準に加えるようになるとよいのではないかと思っている。

○（野原本部員）私から４点申し上げたい。

１点目は、サイバーセキュリティ対策の推進には、民間の力をいかしたセキュリティ産業の育成が極めて重要であるということ。いろいろな組織でのセキュリティ対策推進には三つの要素が重要と思う。

一つ目は、今回のサイバーセキュリティ戦略（案）にもある、トップの意識改革や組織体制の整備等、セキュリティマインドを持った企業経営、組織運営の推進である。これはサイバーセキュリティ関連の産業あるいは事業から見ると、潜在ユーザーのニーズ喚起に当たると思う。

二つ目は、セキュリティ関連の製品サービスを提供する環境の整備である。これが正にセキュリティ産業の育成、振興であり、一つ目で言ったニーズ喚起のユーザーニーズに応じたサービス提供環境を整備するということに当たると思う。

三つ目に重要なのは、セキュリティ人材の育成である。IPA によれば、24 万人ほどがスキル不足または人数そのものが不足していると推計されており、それだけの多数の人を急ぎ育成しなくてはならない状況にある。セキュリティ産業に従事する人材だけでなくユーザー組織内人材の育成が急務であり、戦略（案）にもあるとおり、セキュリティ実務者、企業のセキュリティを含むリスクマネジメントを担う経営層、それらを橋渡しする橋渡し人材が、育成すべき企業内人材として重要だと考えられている。

これらユーザー組織の啓蒙、セキュリティ関連産業の振興、人材育成という三つそれぞれが、鶏と卵の密接な関係にありつつ推進されていかなければならないと思う。セキュリティマインドを持つ企業が増えてニーズが喚起されても、関連ビジネスが育っていなければ環境整備はできないし、企業組織内人材を含めて人材育成することができなければ産業も育たず環境整備もできない。その意味で、人材育成はとても重要であり、かつ

24 万という大人数の育成が必要である。今回の戦略（案）では、大学等の高等教育機関を通した教育施策が中心に書かれているが、社会人育成も急務である。民間サービス事業による育成、振興の拡充も重視していただきたい。

それ以外にもセキュリティ産業の育成は極めて重要である。サイバーセキュリティ関連産業というと、セキュリティ製品のベンダーやフォレンジックス、ネットワーク監視事業者などを想定しがちであるが、先ほど述べた人材育成サービスやコンサルティングなどのジャンルも含め、幅広い事業を関連産業として振興、育成することが重要と思う。今回の戦略（案）に記載されている、政府系のファンドによるサイバーセキュリティ分野への集中的な投資だけでなく、関連サービスが育成、充実されるような様々な施策をさらに検討していただきたいと思う。

以上が１点目である。

２点目は、IoT 社会、技術の進化に対応した柔軟な環境整備をしていただきたいということである。申すまでもなく、IoT 社会に入って自動運転、ドローン、スマートシティ、ウェアラブルデバイスなどあらゆるものがネット接続されると、これまでスタンドアロンでの利用を前提につくられていたものがオープンプラットフォームに接続されるようになる。また、従来、サイバー空間に縁遠かった事業者もデータ収集や通信を行うようになるなど、一つのサービスをつくり上げるためにさまざまなプレーヤーがかかわる環境が増えていく。IoT システム全体をセキュリティ・バイ・デザインで構築、運営することは非常に難しいが、一方、やり過ぎて新たな事業サービスの芽を摘み取ってしまうことのないよう、バランスに十分留意しながら進めてもらいたい。

３点目は、ネットによる海外へのサイバーセキュリティ関連の情報発信を強化していただきたいということである。サイバーセキュリティ戦略は、今回初めて日本語版と英語版を同時に公開することになっており、グローバル化対応として素晴らしいと評価している。しかしながら、例えばNISC サイトの英語ページなどを見ると、ネットによる英語での情報発信は極めて不十分と思う。これを機会にサイト運営や海外への情報発信のための人材や予算を十分確保し、しっかり情報発信をする体制をつくっていただきたい。

最後４点目。今後、この戦略（案）に基づき具体的施策を策定していくわけであるが、個々の施策を並べた場合にばらばらでなく、戦略全体がしっかりそのとおりに実現されるよう策定していただきたいと思う。

○（林本部員）新たなサイバーセキュリティ戦略の草案が短時間でできたことを喜ばしく思っている。前回会合で私が述べた意見の趣旨をいかしていただいた点があることを感謝し、基本的にはこの草案を支持したい。しかし、ここまではPDCA の Plan の部分であり、今後進める Do、Check、Act のほうがより重要ではないかと思っている。そのような視点から４点ほど意見を述べたい。

１点目として、この５原則を国際的に貫いていくには、外交以外の担当者も含めた多面的な努力をするべきと思う。その意味では、英訳も有効であり、さらに、控え目で発言が少ないという日本人のイメージを払拭するほどに、あらゆる場を通じてこの原則を訴えていくべきと思う。戦略（案）の 29 ページにある「（５）国際的な人材育成」とも連動して実行されることを期待している。

２点目は企業行動の規律とその実施方法に関してである。戦略(案)11 ページの「（１）経営層の意識改革」に、「サイバーセキュリティを経営上の重要課題として取り組んでいることが市場や出資者といったステークホルダーから正当に評価される仕組みや資金調達等の財務面で有利となる仕組みの構築」という表現がある。これは以前の本会合で私も発言した、財務諸表にセキュリティに関する記述を加え、ある種の対外的な約束とすることと同じか、少なくとも類似の仕組みだと思われるので大変期待している。ただし、実行に当たってはあくまでも企業の自主性を第一義とすべきと思う。これは中谷本部員御発言にもあったが、私も同趣旨のことを考えていた。

３点目は、監査の留意事項に関してである。サイバーセキュリティ基本法の制定によって戦略本部にセキュリティ監査をする権限と責任が与えられた。今回もその基本方針が付議されているが、これは非常に大切な機能である。我が国では PDCA のうち Plan と Do は忘れないが、Check と Act が忘れられがちなことが、私はかねがね気になっていた。会社の役員も、取締役に比して監査役は脇役であるとの印象を持たれていることが否めない。確かに監査は地味であり、また自分の欠点を他人に指摘されることは誰にとっても大喜びではない。しかしながら、失敗から学ぶことがインシデントを避ける最大の武器である。年１回の健康診断と同様、民間企業も喜んで監査を受け、その結果を日常業務にいかすことが期待されるので、その意味では NISC あるいは政府機関が手本を示していただきたい。その際には、助言型に徹するとともに、人材も含め監査対象者の気持ちがわかるような対応が必要であると思う。

４点目は、教育、特に初等中等教育に関してである。私も大学院に属しているので、人材育成の項には絶えず注目している。今回も網羅的であると同時にバランスよく整理されていることを評価している。中でも特に注目しているのが、戦略（案）35 ページにある「初等中等教育段階における教育の充実」である。なぜなら、IT は進歩が速いため、教科書や指導要領を整える間もなく現実の事態が先に行ってしまう。子供たちは指導を受けることがなくとも、時の流れについていくことはできるが、それが問題をはらんだものでも意識することは少なく、一方で、親や教師は未経験の事態にどう対応すべきか戸惑ったままということが頻繁に起きる。子供の対応力は柔軟性の表れであり、これを抑え込むことは得策でないが、倫理観が全体に揺らいでいる中、何をしてよいか、何をしてはいけないのかが不分明なまま、旧世代が驚くような事件が頻発することになる。大げさに言えば、現在の教育制度は工業社会の人材を育成するために最適化を図ってきたので、情報社会には少し違った新しい視点が必要なのかもしれない。今後、この戦略を実施する過程で問題点を洗い出し、より高次の視点からの議論につなげていただければと思う。

○（前田本部員）サイバーセキュリティの戦略（案）については、短期間で非常にうまくまとめていただき、優れた内容になっている。途中いろいろ意見を申し上げたが、基本的に異存はない。

３、４点ほどコメントをさせていただく。

発展の途中段階ということであったかもしれないが、以前この戦略本部は「情報セキュリティ政策会議」と呼ばれていた。一方、先週 21 日に、邦人殺害テロ事件の対応に関す

る検証委員会検証報告書がこの官邸の場で出たことについて、素晴らしいと思うとともに、見るべきポイントがいろいろあると思う。私たちから見ると、やはり情報収集がまだまだ足りておらず、組織や方法の面で充実させなければならない。この戦略本部との関連で言えば、サイバーの視点からの情報収集が何よりも大事である。

刑事法学者としての立場から発言させていただく。世界中が、刑事捜査の手法として、ネットを使って情報を集めている。国によっては、捜査においてソフトウェアの送り込みやバックドアを用いて中を見るようなことをしており、これを合法化する法律が出始めている国もある。日本も同様にせよという意味ではなく、いろいろな意味でサイバーから情報を収集できる人材をいかに育てていくか、もう少し幅広の人材育成が必要だということと思う。これは、林本部員の御議論と全く重なるものであり、最後に申し上げる話に通じるものでもある。

今回の戦略（案）で私が一番高く評価しているのは、サイバー空間を悪用する国際テロ組織への対処を記載したということであり、非常に重要である。イスラム過激派組織が、いろいろな過激思想を広げたり、テロの実行を呼びかけたりすることを、インターネットを活用して行うことで、テロ組織と関係ない人間が動いたり、資金が膨大に集まったりする可能性もある。これへの対処をいかに実効性あるものにしていただけるかに注目していきたい。

先ほどの官房長官のお話にもあったように、オリンピックの対応として、公衆無線LANやSIMカードなどインターネット利用環境整備は非常に大事であるが、我々刑事法学者の感覚としては、それを悪用したなりすましなど、悪意ある犯罪活動の温床になる可能性があると考える。ここについても今回の戦略に基づいて関係省庁が連携し、ぜひ必要な対策を講じていただきたい。

最後に、今回の戦略（案）にも出ている、サプライチェーン、特に調達における問題について申し上げる。以前に遠隔操作や何かで述べたが、国の用いる情報漏えい防止ソフトウェアは、外国のものを使っている。外国の力を借りざるを得ないのは確かであるが、企業から情報がとられている可能性があったらどうするか。これについては、オウム真理教事件を思い出していただきたい。開発能力が非常に優れている宗教団体が製造したソフトウェアのほうが低価格かもしれない。

今の政府調達は、価格・費用面で判断するので、安ければよいとなりかねない。しかし、安全保障、国民の安心・安全の視点で考えるべきである。特にセキュリティ関係に関してはもう一歩進むべきである。調達先企業の役員の情報や国籍などを調べることのガイドラインはあるが、政府としてはもう半歩前に出て、なるべくそのようなことをさせる方向に進んでいくことが望ましい。国際化の時代ではあるが、あらゆる国と平等にという問題でも安ければよいという問題でもないということである。

そのためには、日本製のソフトウェア開発が必要である。それゆえ、人材が大事であると先ほど申し上げた。情報を集める検索ソフトウェアは、既に特定企業が独り勝ちしているが、日本の優秀な知能を結集して、もう一歩進むべきである。検索エンジンだけの問題ではなく、本当の意味でのサイバーの人材育成はそこにあるのではないか。ぜひ村井本部員を始めとして御尽力をお願いしたい。

○（村井本部員）先週アメリカへ行った際、シンギュラリティの新しい映画を見た。世界一の独占的検索エンジン企業の社長が、ひそかに美女のAI分析のロボットを造って、という話であり、もうすぐ日本でも公開されると思う。ポイントは、基本的にはウェブ上の文字の分析が前提ということである。この映画も、最近の他のシンギュラリティに関する映画と同様、対象の分析により好みの女性などをわかりながらアプローチをして恋に落ちていくというようなことである。この中で言語の分析、音声の認識、自動翻訳といった文字をどのように処理していくかが知性で、AIであり、これで非常に大きく育っているのがその会社である。

一方、今、日本の中で私がとても残念に感じるのは、「あの会社にはどうしてもかなわないから他のことをやりましょう」と、アカデミズムでさえ言うことである。それは間違っていると思う。ある海外検索エンジン企業の音声自動認識は、日本語をきちんと認識できる。また、日本の地図の位置情報サービスがある。これは日本人がやっている。日本語の翻訳や分析は日本人でなければできない。つまり、優秀な学生が海外企業に行っているということである。

これまでであれば、今、前田本部員の御発言にあったように、我が国の企業に勤めて働いてほしいということであろう。人材がいないとよく言うが、いる人材はそのような海外企業にとられているという側面もある。それだけではなく、我々の責任もある。これをどのように変えるかについては二つあると思う。一つは、日本の企業が、非常に面白い新しいチャレンジをしていく産業をこの国で興していくことだと思う。そこに行って活躍したい優秀な人材は、皆頑張って勉強して日本の企業に勤めるようになると思う。つまり日本の産業が、新しい技術の時代に伸び伸びと新しい産業をつくっていける体制づくり、これが大事だということが１点。

もう１点は、今までは文字を分析していたが、IoTというのはデータであるということ。至る所のセンサーから出てくる数字の分析には言語の壁がない。したがって、私たちにとってゲームチェンジのチャンスである。つまり、IoT時代、センサー時代になって、変わったゲームをどう捉えるかが、新しい技術の時代に我が国がどのようできるかということである。

また、資料１－１のチャートは、どの国のサイバーセキュリティのチャートよりよくできている。経済が左、安心・安全が真ん中、国際社会の平和が右にあり、この三つ鼎（みつがなえ）で議論しているのが良いところである。グローバル経済で成長しないと国の関係で勝てず、真ん中に安心・安全がある。安心・安全については、以前も述べたとおり、この国ほど安心で信頼性のあるサービスを提供する国はない。この国の国民ほど電車の遅延に文句を言う国民はいない。このようなマーケットを持っていることはとても強い。信頼性のあるサービスをサイバー空間に提供すれば、セキュリティは必然的に高まる。したがって、そういう意味では私たちにはアドバンテージがある。安心・安全を中心としたこのチャートの意味は、そこにあると思う。

オリンピック・パラリンピック東京大会も同様である。そのときまでに、適切なタイミングで安心・安全なサイバースペースというものをどのように使い、維持・発展できるかという目標設定にちょうどよいと思う。私も含めてしっかりと人材、技術の未来をきちんとつくっていくべきだと思う。

○（遠藤本部員）村井本部員の御発言は、日本の企業がしっかりするようにとのお叱りであると思った。

私は、サイバー空間というものを少し違う観点からレビューしながら、今回の戦略（案）について少しコメントをさせていただく。

サイバー空間は、価値を生むことができる空間と捉えるべきだと私は思う。例えば、私ども地球上の人間それ自体の人口問題というものは非常に大きな問題として捉えるべきである。30年間で世界の人口は1.3倍になり、その中で都市部に住む人たちは1.8倍になる。そうなると、エネルギーが1.8倍、食料が1.7倍、水も1.6倍必要になり、限られた資源をどのように有効に使うか、また、1.8倍のエネルギーが必要ということは、電力ネットワークをもう一個造りなさいということを意味しており、どのように有効なネットワークにするのかということが、非常に大きな課題である。

一方、日本は人口が70%、60%になるという課題があるが、その場合にも60%、70%の税金で、今のインフラをどうやって維持するのか。人口も少なく、税金も少ない。警察官も60%、70%になるかもしれない。それで安全をどのように守るのかという話に必ずなる。そのときにICTは非常に大きな力を発揮する。サイバー空間で価値を生んでその部分を補うということが絶対的に必要になる。そういう意味でサイバー空間をどうやってうまく使うか、一方で価値を生み出すサイバー空間をどうやって守るか。これが、我々が本当に真剣に取り組まなくてはならないアイテムであろうと私は思っている。

そういう観点で今回、サイバーセキュリティ戦略（案）をまとめていただいているが、サイバー空間の認識が非常に明確になっており、戦略の目的、基本原則、さらにはそれに対する施策が出ている。今、村井本部員が述べられたように３つの視点からつくられているという観点でも、サイバー空間というものを大きな視点で俯瞰をした形でまとめていただいていることは非常にありがたく、バランスの良いまとめ方になっていると思う。

その中でもう一つ、本部員皆さんがコメントされているが、国際社会の平和と安定という観点から、この戦略を英語でほかの国にも知っていただき、日本の方向感をお見せすることは非常に重要なことと思う。日本の国が主体的にすべきことを行っても、海外と連携してしっかり情報交換をしない限りは、世界の安定を求めることができないからである。

この４月に、インターポール、インターナショナル・ポリスが、シンガポールにIGCIというブランチをつくった。トップの総局長には、日本の警察庁の方がおいでいただいている。私もオープニングのイノベーションセレモニーのとき、プレゼンターとして、プライベートセクターから１人呼んでいただいた。というのも、弊社がここのサイバーセキュリティのシステムを全部入れており、３年間継続的にメンテナンスを含めてフォローすることになっている。いずれにせよ、日本がいろいろなところでこのようなリーダーシップをとっていくということが絶対的に必要で、この戦略とともに積極的な我々のサイバーセキュリティに対するリーダーシップをどうやって発揮していくかが、今後の重要なポイントになってくるのではないかと思う。

２番目はIoTである。先ほど申し上げたようにサイバー空間は、価値をつくり出すと

ころである。リアルの世界フィジカルの世界からデータが入り、そのデータをベースにサイバー空間でつくり上げた価値をリアルまたはフィジカルの世界に持っていく。それがIoTの基本であるが、ソフトウェアだけではなくハードウェアが絡んでくる。この点において、いわゆるサイバー空間を守るというだけでなく、ハードウェアと一体となって安全性を守ることが必要である。特に、インフラストラクチャーのところに絡んでくるため、ソフトウェアとハードウェア一体で安全性を守ることができないとインフラに大きな影響を与え、先ほど菅官房長官がおっしゃったように放送機器にダメージを与えるというような問題に絡んでくる。よって、今後は、サイバー空間だけではなく、IoTを考えたときにはハードウェアも含めたコンプレックスが一体となった安全性の守り方ということを今後模索していく必要があり、そのためには非常にスピードが速い領域に入ってくるため、この戦略をベースに年次計画をつくり、PCDAを細かく回していくことが必要であろうと考える。

３番目は人材の問題である。いろいろ言われているが、絶対的にソフトウェアの人材が不足している。どのように人材を育て上げていくかという観点は、一つは地方創生と絡めながら人材を育て、地方で就職先も探していくような形をどこかでとれるというのも一つのポイントではないか。実は地方に工場を持っていくというような雇用のありようがだんだんなくなってきており、一方でソフトウェアの人材が足りないということがある。かつ、サイバーの領域は、必ずしも人が一箇所に集まって仕事をしなくても、ばらばらにいてリモートで仕事ができるという仕事の領域でもあるわけで、これをうまく地方再生の一つとして使える可能性は十分にあるのではないか。いずれにしても、人の育て方というのは幅広く考え、日本の中でつくり上げていくことが必要であると思う。

○（小野寺本部員）今回の戦略（案）は、非常にうまくまとまったのではないかと思う。

私がこの中で一番気に入っているのは出だしの部分である。今までどうしてもサイバー空間、我々にとってはインターネットの部分が大きいわけであるが、この部分に対する影響の大きさに対する理解が今まで非常に少なかったと思う。インターネットは検索するだけのような格好になっており、これが日本人のサイバーセキュリティに対する意識を低くとどめていた大きな理由の一つではないかと思っている。その意味では、「グーテンベルクの活版印刷」を引き合いに出し、今、世の中が大きく変わっていることを最初にしっかり書き込んだということが非常に良いと思っている。

その点で言えば、先ほどから出ている教育の問題について、例えばある新聞がつくったと言われる「交通戦争」という言葉によって、交通安全教室なり教育なり、そういう方向でどんどん意識付けされてきたのではないかと思う。残念ながら現状では、ネット社会の教育問題というのは、ほとんど初等中等教育ではまだ触れられていない。これが非常に気になるところである。初等中等教育の中で、まずはサイバーセキュリティ、サイバーセキュリティというと語弊があるが、まずネットの空間というのがどういうものか、ある意味非常に楽しいものであるということをまず子供のうちに植えつけ、興味を引いた上でサイバーセキュリティの方向に持っていかないと、ただ締めつけるだけにしてしまうと大変なことになるのではないかと危惧している。現在、一部で既に始まっているが、初等中等教育の段階からネットの楽しさ、ICTを使ったときの楽しさというも

のを勉強させている仕組みが一部で出ている。ここをもっと広げていくことによって、まずは日本人の教育の ICT に対する知識の基盤をつくっていく必要があるのではないかと思っている。

２点目として、今回、IoT を全面に出していただき、これは非常に結構だと思っている。セキュリティ・バイ・デザインという言葉もここに出てきているが、産業界から見たときにセキュリティ・バイ・デザインで設計していくのは当然のこととして、遠藤本部員も述べられていたように標準化が一つ非常に重要である。恐らくデファクト標準になるのだと思うが、この標準化の部分を早く日本がとらないと、結果的にどうしても海外のものが主体にならざるを得なくなるのではないかと危惧している。

そういう意味は、日本の得意とするモノのほう、先ほど遠藤本部員も述べられたように、ソフトウェアだけではなくてハードウェアの関連が必ず出てくる部分である。幸いなことに、まだハードウェアは日本が強いところがかなり残っている。この強いところと今まで弱いと言われていたソフトウェアの部分、ここをうまく結びつけて標準化に持っていくことによって IoT での世界標準をとれれば、日本の産業にとって非常に大きなことになるのではないかと思っている。

３点目であるが、今回セキュリティの中でマネジメント監査とペネトレーションテストを非常に重視して書き込んでいただき、これは非常に重要だと思っている。ただ、先ほどから話題に上っている PDCA サイクルに関連することになるが、マネジメント監査やペネトレーションテストは、ある意味一時的なものである。監査やペネトレーションテストをする時期、それだけの対応になりかねないのではないかという危惧の念を抱いている。

米国には CDM（Continuous Diagnostics and Mitigation 継続的診断及び対策）という概念があるようである。これを見ると「All system scanned within 72 hours」と記載されている。要するに、国にある全てのシステムを 72 時間以内にスキャンし、プログレスレポートをすると書かれている。日本には CDM 的な概念がまだ弱いような気がしており、ここは正に今からのところであるので、今回の戦略の中に書き込むというより、今後どのように日本に考え方を取り込んでいくのかということになるのだと思う。

そのときに NISC の指導力、責任について、今の法律上は、どうしても国の機関もしくは地方自治体まで、要するに政府関係がメインにならざるを得ないというのは仕方がないと思うが、民間との連携を深めていかないと CDM 的なことは当然できないのだと思う。そういう意味で民間との連携をどう強めていくか。強制ではないのだろうと思うが、その中で民間の協力を得られるような体制、また、民間が協力しやすいような体制、これをどうやってつくっていくか、一つ大きな課題ではないかと思う。

もう一つは、IoT を含めた今後の技術開発に絡むところで、重要インフラ関係では当然のことであるが、研究開発について今まで後手であったのを、先手という格好でプロアクティブに進めようということになっている。幸いなことに今、AI がどんどん進んできて、しかもビッグデータの解析もかなり進んできている。このサイバーセキュリティの中に、今からの技術である AI、ビッグデータの技術をうまく取り込むことによって、世界でも先端的な分析、解析、この技術が日本としてつくれるのではないかと期待している。そういう意味で、プロアクティブな対応を可能とするための技術、この開発に日

本全体で是非取り組んでいただきたいと思う。

○（山口情報通信技術（ＩＴ）政策担当大臣（副本部長））いろいろと有効な大変素晴らしいお話を聞かせていただき、また、いろいろと御尽力をいただいており感謝申し上げる。

私は、先月エストニアを訪問し、国民IDを初めとするITの積極利活用について取組状況を視察した。IT政策を担当する大臣として、IT利活用の一層の深化を図っていくためには、サイバーセキュリティの確保と同時に国民の皆様方の御理解は不可欠であると再認識したわけであるが、我が国においても、今ちょうど国会審議中のマイナンバー制度の推進によって、国民生活のさまざまなシーンにおける利便性の向上が期待されている。行政の効率化あるいは国民生活の利便性向上と合わせ、セキュリティについても新たなサイバーセキュリティ戦略を踏まえてしっかりと担保をして、国民の皆様方の御理解を得ながら着実に進めていきたい。

○（山谷国家公安委員会委員長）サイバー空間の脅威については、平成26年中のインターネットバンキングに係る不正送金事犯の被害額が過去最多となるなど、サイバー犯罪が多発するとともに、海外ではISILの賛同者とみられる者がサイバー攻撃によって国際放送を停止させるなど、サイバー攻撃も多発しており、サイバー空間の脅威はますます深刻化している。

本日の議題である新たな戦略や施策の方向性を踏まえ、警察もその役割を十分に果たしていくことができるよう、引き続き警察を指導していく。

また、サイバー犯罪等に対する事後追跡可能性の確保に必要なログの保存については、その取組が進みつつある。本件に御尽力いただいた皆様に、この場をお借りして深く感謝申し上げるとともに、引き続き御協力をお願いいたしたい。

○（西銘総務副大臣）総務省では、本年１月から省内の有識者会議で検討を実施し、先日５月22日、サイバーセキュリティ政策推進に関する提言を取りまとめたところである。総務省としては、この提言を踏まえ、サイバー防御演習（CYDER）の知見を生かして演習基盤を拡充し、東京五輪大会を想定した大規模なサイバー演習を実施することで、実践的なセキュリティ人材の育成を図っていく。

また、サイバー攻撃関連情報の組織横断的な共有も必要。情報共有組織（ISAC）の国内での設置は、通信と金融の２分野にとどまっており、NISCとも連携してTelecom-ISACの体制強化とその横展開に努め、提言の具体化に取り組んでいく。

○（中山外務副大臣）国内外を問わず、あらゆる分野でサイバー空間への依存度が高まっている中、ルールを無視する一部国家、また、ルールを持たないテロリスト等が関与する各種脅威への対応は喫緊の課題である。私自身、シリアにおける邦人拘束事案において現地で指揮に当たったが、その際、従来型の物理的なテロにITというハイテクの利用を融合させ、インターネット等を通じて瞬時に距離に関係なくテロの恐怖を個々人に届けるというISILによる卑劣な犯罪行為を実感した。

４月に行われたサイバー空間におけるハーグ会議においても、こうしたテロリズムとハイテクの出会い等の問題意識を提起するとともに、日本の取組を説明した。

本日議論されたサイバーセキュリティ戦略（案）は、政府が一体となってサイバー政策に取り組む上で極めて重要な施策である。策定後には実施に加え、積極的に対外発信する所存である。

外務省としては、本年２月の第１回戦略本部以降、関係省庁とともに新たにオーストラリア、ロシアと二国間協議を実施している。本年４月末の米国との「２＋２」の会合においては、新たな日米防衛協力のための指針、いわゆるガイドラインを発表した。サイバー空間に関する協力を規定している。これにより、情報共有や重要インフラ防護等についても、日米両国が協力することを確認した次第である。

外務省としては、サイバー分野における情報収集、インテリジェンスを一層強化するとともに、積極的平和主義の立場から自由、公正かつ安全なサイバー空間の確保のために、引き続き積極的な取組を進めていく。

○（山際経済産業副大臣）本日、御説明のあった新たなサイバーセキュリティ戦略（案）にあるとおり、あらゆるものがネットワークにつながっていくことにより、ビッグデータの利活用等の新たなビジネスチャンスが生まれる一方、新たな企業経営上のリスクともなる。

例えばネットワークでつながるビジネスパートナーからの情報漏えいのリスクや、サイバーセキュリティ対策が不十分な企業がサプライチェーンから外されるといった事態も予想される。こうしたリスクに対応するために経営層のリーダーシップによるサイバーセキュリティ経営の推進及び外部からの評価のための枠組みの構築、サイバー攻撃の手口や対策に関する情報を官民で共有するネットワークの一層の拡充等が重要であると考えている。今回のサイバーセキュリティ戦略（案）でも、その内容を盛り込んでいただいている。

また、事務局からの報告にもあったとおり、当省関係の産総研がNISCとの協力覚書を締結したところであり、経産省としても関係省庁との連携の下、セキュリティ対策を着実に取り組んでいく

○（原田防衛大臣政務官）自由、公正かつ安全なサイバー空間の創出・発展は、我が国の安全保障並びに危機管理の観点からも必要不可欠である。また、先般改定された日米ガイドラインにおいても、日米両政府によるサイバー空間に関する協力の重要性及び組織強化について言及されるなど、国際社会全体における安全保障上の喫緊の課題である。今般のサイバーセキュリティ戦略（案）には、こうした我が国の安全保障や国際社会に対する貢献の観点からの取組のあり方や、政府機関やインフラの機能保証、自衛隊の任務保証の観点からも、国全体としての対策強化の方向性をしっかりと示したことは、極めて重要と認識している。

防衛省・自衛隊としても、自由、公正かつ安全なサイバー空間の創出・発展のため、官民一体となった取組に対して最大限の協力を行うとともに、自衛隊のサイバー攻撃対処能力の強化に向け、引き続き積極的に取り組んでいく。

(3)　決定事項の決定等

決定事項４件につき、案のとおり決定した。

また、サイバーセキュリティ戦略（案）は、一般からの意見募集手続を本日から６月８日までの約２週間実施する。その結果を踏まえ、次回会合において戦略（案）を最終決定することとした。

(4)　安倍内閣総理大臣締め括り御挨拶

サイバー空間における安全の確保、すなわちサイバーセキュリティは、さまざまな分野でのITの利活用を進め、成長戦略を実現するために必要不可欠な基盤であるだけでなく、国家の安全保障、危機管理にとって極めて重要な課題である。2020年のオリンピック・パラリンピック東京大会を成功させるためにも、我が国のサイバーセキュリティに万全を期す必要がある。

このたび、各委員の精力的な検討、御尽力により、新たな戦略（案）が取りまとめられたことに改めて感謝、御礼を申し上げる。

本戦略（案）は、今後のサイバーセキュリティ政策の羅針盤となるものであり、あらゆるものがインターネットに接続され、実空間とサイバー空間が高度に融合した社会、すなわち連接融合情報社会が到来しつつあるとの認識の下、セキュリティはコストではなく安全な製品、サービスをつくり、企業価値や国際競争力を高めるための投資であるという大胆な発想の転換を打ち出した。また、我が国の安全保障を戦略の大きな柱の一つに据えた。サイバー空間が第５の安全保障空間と言われる中、国境を超えた高度なサイバー攻撃を含め、あらゆる事案に適切に対処できるよう、我が国の能力をこれまで以上に強化していかなければならない。

今後はこの新たな戦略（案）を具体化し、目標を着実に達成していく必要がある。そのため、サイバーセキュリティ基本法に基づき設置されたこの戦略本部が司令塔となり、関係各位が緊密に連携し、省庁、官民の垣根を越えて実効ある取組を着実に前に進めていくことをお願いしたい。

－　以上　－