サイバーセキュリティ戦略本部
第１回会合　議事概要

１　日時

平成27年２月10日（火）　17：00～18：00

２　場所

総理大臣官邸２階小ホール

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
高市　早苗	総務大臣
岸田　文雄	外務大臣
宮沢　洋一	経済産業大臣
中谷　元	防衛大臣
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
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)　安倍内閣総理大臣冒頭御挨拶

「サイバーセキュリティ戦略本部」の開催に当たり、一言、御挨拶を申し上げる。

サイバー空間は、経済成長やイノベーションを推進するために必要な場となっており、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、成長戦略を実現するためにも、必要不可欠な基盤である。

他方、最近の米国の映画配給会社や、韓国の重要インフラに対するサイバー攻撃に見られるように、サイバー空間における脅威は、ますます深刻化している。サイバー攻撃への対応は、正に国家の安全保障・危機管理上の重要な課題である。

こうした状況を踏まえ、先の国会において、我が国のサイバーセキュリティを抜本的に強化するため「サイバーセキュリティ基本法」が成立した。

本日、初会合となる「サイバーセキュリティ戦略本部」は、基本法によって、関係行政機関の施策を評価し、資料の提出を求める等の権限を付与された、名実ともに、我が国のサイバーセキュリティ分野の司令塔となるべき存在である。

まずはサイバーセキュリティ施策の基本的な方針について、新たな「サイバーセキュリティ戦略」を策定することとなるが、有識者の皆様には、その卓越した知見を存分に発揮していただくようお願いする。

2020 年には、オリンピック・パラリンピック東京大会が開催される。ロンドンの経験からいっても、大会の成功にはサイバーセキュリティの確保が必要不可欠である。こうした点も見据え、我が国のサイバーセキュリティに万全を期してまいりたいと考えている。

この本部が司令塔としての役割を十分に果たすことを期待し、私からの御挨拶とさせていただく。

(2)　討議

【決定事項】

- 本部の運営等について
- 重大インシデントの対応等について
- サイバーセキュリティ政策の評価等について

【討議事項】

- 新・サイバーセキュリティ戦略について
- サイバーセキュリティ対策を強化するための施策の評価（監査）の方針について

【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
- サイバーセキュリティ月間について

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。

○（小野寺本部員）サイバーセキュリティ基本法が成立し、施行されたことは、日本のサイバーセキュリティにとって画期的なことであり、非常に高く評価している。

先ほど総理からもお話があったが、2020 年のオリンピック・パラリンピックを控え、今後はここで決められた政策をどのように実行していくかが問題だと思っている。

先ほど事務局から説明があった資料４、新・サイバーセキュリティ戦略の主な検討課題について、検討課題自体は網羅的に書かれていると思っているが、私からはそれに関連し、３点申し上げたい。

１点目は、基盤的事項で指摘されている社会全体のセキュリティ意識及び日本におけるセキュリティ人材についてである。サイバーセキュリティの必要性は、ＩｏＴの進展等、対象とする範囲がますます広がると同時に、その影響範囲も非常に広がっている。大多数の国民が意識している、していないは別にして、ＩＣＴを利用しているが、残念ながらサイバーセキュリティに関する意識は、まだまだ低いと言わざるを得ない。

これまでにもいろいろな取組がなされ、一部ではその成果が上がってきている部分もあると思うが、諸外国に比べると遅いのではないかと思う。

その理由の１つは、サイバーセキュリティの基本となるＩＣＴ教育は、成長戦略の中で、プログラミング教育等という言葉で指摘されているが、現状では、教育課程の制度上で義務化されていないという点である。これからの社会では、ＩＣＴが新しいリベラルアーツだと認識しており、英国のように義務化を図っていく必要があるのではないかと思う。

その際、常に問題とされるのが、教える教員が不足しているという反論である。これはぜひお考えいただきたいのであるが、国立大学の 44 大学に教員養成課程があり、その定員は１万名を超えている。これから卒業する学生は、いわゆるデジタルネイティブと言われる世代で、教員養成課程でＩＣＴ教育を学ばせる体制を整えるだけで、年間１万名を超える教員が確保できるのではないかと思う。44 大学であれば、先進的な教育を行っている小中学校や、ＮＰＯ法人から教官を募れば、教官の確保もそれほど難しい問題ではないと思う。まず教員養成課程で学ぶ人たちに、ＩＣＴをきっちり教育する、この点をお考えいただきたい。

２点目は、全般的事項で指摘されている、多様な主体間の役割分担にかかる事項である。サイバーセキュリティ基本法は、その性格上、国の機関に対し、重大インシデント等への対応が明確に定められており、基本法の骨格であると思う。一方、サイバー攻撃自体は、政府関係に限らず、個人を含むあらゆる組織が対象となり得る。攻撃者は、脆弱性の高い組織、部分を攻撃するが、その影響は攻撃された組織にとどまらず広範囲に及び、これは常識になってきている。この点からも、今まで以上に組織間の連携が重要になってきている。

先ほど総理からもお話があったが、米国における映画配給会社のように、重要インフラに指定されていない民間企業に対しても、重大な攻撃が行われる時代に入ってきている。これまで想定されていない一般企業についても、重大インシデントが発生した場合の通報、連絡系統の整備及びその対応方針を定めておく必要があると思う。そのためには、各種業界の団体等にサイバーセキュリティを自らの業界の問題として考えてもらえる仕組み、例えば重要インフラで整備されつつあるＩＳＡＣのような組織づくりが重要

になってくるのではないかと思う。

最後に、現在、いわゆるセキュリティソフトウェアは、ほとんどが外国企業のものであるが、これらの企業は、いわゆる中堅企業であり、我が国でも、これからこれらの企業に追いつくことは不可能ではないと思う。サイバーセキュリティで重要になっているセキュリティソフトウェアについて、産業振興の面からも、日本のセキュリティソフト会社をどのように育てていくかを検討する必要がある。

同時に、産業界にとっても非常に大きな問題として、ブラックボックス化されたデバイス、モジュールが海外から輸入されている例がかなり増えてきている。残念ながら、ブラックボックス化されたデバイス、モジュールがどのようにセキュリティに対して影響があるかということは、わかっていない。このような問題も含めて、どのように考えていくか、本部において検討を続けていく必要があるのではないかと思う。

○（中谷本部員）私から４点申し上げる。

第一に、サイバーセキュリティ基本法が成立し、このたび、サイバーセキュリティ戦略本部ができて、国内の体制は大きく整ってきたと評価できる。

その上で、今後、一層力を入れていく必要があるのは、サイバー外交であり、また、世界に率先して、サイバー空間の法秩序を構築し、強固なものにすることだろうと思う。サイバー外交の展開については、自由と民主主義という価値観を同じくする諸国とのサイバー分野での協力の強化はもちろんのこと、サイバーセキュリティについて、人材、技術、資金が不足する途上国へのキャパシティビルディングを一層進めることも、また重要であると考える。サイバー空間の法秩序形成をリードすることは、国際社会における法の支配、国際連携取組方針にまさに合致するものであると考える。

第二は、安全保障法制の中でサイバー攻撃をどう位置づけるか、その明確化のための検討が必要であると考える。さまざまな種類や強度のサイバー攻撃を、国際法上及び国内法上、どう分類し、それぞれに対してどのようなサイバー分野及び非サイバー分野での反応をとり得るかを明確化する必要があると考える。この主題は、ＮＳＣとサイバーセキュリティ戦略本部が連携して検討を進めることが望ましいと思う。

北朝鮮の関与が疑われる米国の映画配給会社へのサイバー攻撃や、ネットを駆使したイスラム国なるテロ集団の報道に鑑みると、早急に検討することが必要であると思う。

第三に、サイバー保険についてである。報道によると、政府はサイバー保険の普及を後押しするための基準づくりを検討するということであるが、これは企業にサイバー攻撃への備えを強化するよう促すものであって、大いに結構なものだと思う。

ただし、サイバーセキュリティ対策の自主努力が大前提であって、保険はあくまでそれを補完するにとどまるものであるから、サイバー保険の制度設計にあたっては、個々の企業のサイバーセキュリティ対策の努力や成果の度合いを、例えば保険料率等に十分反映させる必要があると考える。この点からも、企業のサイバーセキュリティ対策の強化が重要であり、政府が評価基準の作成を開始したことは、有意義であると考えている。

最後に、サイバーセキュリティに関連する教育についてである。サイバーセキュリティ関連教育は、従来は理系が中心であったが、文系においても、法学、政治学、経済学を初めとする各分野においてサイバーセキュリティを検討することはとても重要であると

いうことを、情報セキュリティ政策会議の構成員を１年ほど務めるなかで、実感した次第である。

大学に籍を置くものとして、今後、私自身は、専門の観点からいろいろと行いたいと思うが、政府においても、教育について一層の確保等をお願いできればありがたく思う。

○（野原本部員）先ほど総理からもお話があったが、日本を取り巻く政治的、経済的、社会的環境変化、すなわち東京オリンピック、周辺国との関係、新興国各国のＩＴ化の進展、経済振興の状況を考えても、今後、日本をターゲットにしたサイバー攻撃、サイバーテロが発生する可能性は大きく、しっかり備えなければならないと感じる。

そして、そうした環境変化だけではなく、ＩｏＴの時代になると、ウェアラブルデバイス、自動運転、ドローン、スマートシティというように、これまで以上にさまざまなものがインターネットにつながれるようになる。その結果、サイバー空間にこれまで縁遠かったようなプレイヤーもデータを集め、交信するようになるし、１つのサービスをつくり上げるのに様々なプレイヤーがかかわらなければならない、という環境もこれから増えていくと考えられる。今回の新・サイバーセキュリティ戦略は、こうした変化を踏まえて検討する必要があると思っている。

資料４の３ページの検討課題の中に、「『サイバー空間』はどのような性質の空間として発展していくと考えるか」という記載があった。サイバー空間というと、国境がなく、距離や場所が自由で、物理的に見えなくてといったサイバーの部分が強調されるが、これもリアルな生活空間の１つだと思う。その点もしっかり考えながら、サイバーセキュリティ対策を考えていかなくてはならないと思う。

その具体的な方法について、２点、申し上げたい。

１つ目は、資料６、あるいは資料７の予算のところにも書かれているが、引き続き内閣官房の機能の強化は大変重要だと思っている。サイバーセキュリティといっても、政策的な面の分析、サイバー攻撃の脅威の情勢分析、そして、技術面での状況の分析と、いろいろな側面があり、それによって必要とされる人材の専門性が全然違う。必要な専門的人材を確保し、質の高い人材を集める体制をつくることが重要だと思う。現在の官僚の方々の給与・処遇で、そういう人材を集められるのかを考えて、必要に応じて処遇等も考えながら、十分な体制をつくっていくことが重要だと思う。

そして資料６では、ＮＩＳＣとＪＰＣＥＲＴ／ＣＣやＩＰＡ等の関連機関との関係を強化するという話があり、これも基本的なことだが、非常に重要な体制整備だと思っている。その結果、シームレスに連携されることも重要であるが、インシデントを起こした企業等があちこちに何度も報告しなければいけないことにならないよう、スムーズな連携体制をきちんとつくっていく必要があると思っている。

最後に、こうしたサイバーセキュリティ対策をすることは、行政のアクションだけではなくて、サイバーセキュリティ産業として、しっかり民の力を活用して育成していくことも重要だと思う。

先ほどからお話が出ている人材育成についても、ＩＴリテラシー教育についても、民によってなされるべきだし、ウイルス対策や企業に対する支援、マネジメントといったサービス、派遣等の事業についても、幅広いサービス事業が考えられるので、こうした

サイバーセキュリティ産業をしっかり創出していくことにも関与できればと思っている。

○（林本部員）まずサイバーセキュリティ戦略本部が設置され、それに合わせて事務局が大変たくさんの資料を整備されたことに敬意を表したい。

特に私が注目しているのは、従来、日本の情報セキュリティと言われている分野では、Plan、Do、Check、Actのうち、PlanとDoにかなり力が入り、Check、Actにはなかなか手が回らなかった懸念があった。その意味で、今回出された資料のうち、政策の評価や監査の方針のところでこの点がカバーされており、私も同感するところである。

（情報セキュリティ政策会議の会合で）前回、私は、新しい組織になるのであれば基本事項の総点検から始めるのが良いのではないかと発言した。今日は（サイバーセキュリティ戦略本部の）第１回会合であるので、特に企業におけるサイバーセキュリティ対策をもう一度見直す観点で、コメントさせていただく。

情報セキュリティ政策会議が発足した初期においては、市場経済である以上いろいろなプレイヤーがいるが、民間の占める割合が高いという観点で民主導の色が濃かったのではないかと思う。しかし、次第にサイバーセキュリティにはナショナルセキュリティに関連する公的な機能があることがわかり、政府への期待、あるいは官民連携への比重が高まったものと理解している。しかし、依然として民の占める部分は大きい。これについて企業規模の面から再度見直す必要があるのではないかと思う。端的に言って、中小企業対策と大企業対策を分けて、それぞれについて、以下のようなことを検討いただければと思う。

中小企業に関しては、ＩＴにかかわる人材の分布が日米で大きく違っていることに配慮が必要である。経済産業省の資料によると、ＩＴ人材がユーザー企業にいるのか、それともサービスを提供しているベンダー企業にいるのかを比較をすると、米国では７対３でユーザー企業のほうに多く、逆に日本は１対３でベンダー企業に多くいるという。つまり米国では、ユーザー企業自体がＩＴ人材を抱えて対策をしているのに対し、日本ではＩＴ業務がアウトソースされてベンダーに奪われているか、あるいはＩＴ人材そのものの絶対数が不足しているのでベンダーに頼んですらいない、ということでもあると思う。日本においてこのような人材分布の偏りがある以上、身の丈に合ったセキュリティを考えるしかないと思う。

特に2020年が１つのターゲットイヤーだとすると、これに間に合わせる時間は余りない。私も、長期的にはユーザー企業に人材が配置されるように努力することは必要だと思うが、当面はＩＴ企業にテコ入れすることがより効果的だと考える。

他方、大企業に関しては、２つの点が気になっている。

１つは、委託先の管理であり、委託先のセキュリティレベルが自社内におけるものと同じレベルにあるか、ということである。従来は企業間に濃淡があったと思われ、情報漏えい等は委託先で起こる事例も目立っていたと思う。しかし、大手通信教育会社の不幸なケースが警鐘となり、大企業においては、社内教育と外部委託を区別せず同じレベルのセキュリティを確保しておく動きが高まっていると思うし、クラウドサービス導入を志向すればますますそうならざるを得ないと思う。

日経新聞の昨年夏の調査によると、有価証券報告書において情報管理に関するリスク

を開示する企業は60％を超えたと言われている。このように、同社の事件が、「災い転じて福となす」になればと期待している。

次に気になるのが、子会社、関連会社の管理問題である。特に海外子会社、その中でもさらに海外の会社をM&A等で取得した場合の管理である。今やグループ経営が当たり前になり、子会社、関連会社は社内に準じて管理されていると思われているが、必ずしもそうでもないように思う。特にM&Aで販路や事業を拡大した場合、それに合わせたセキュリティ管理は、口で言うほど易しいものではないと思う。買収された企業にも独自の風土があり、ましてや文化的な背景を異にする事業を行うとなれば、ローカライズが必要である。そこで、グローバルなセキュリティポリシーと現地が実運用するセキュリティマネジメントとの間に、微妙な差を生むことは避けられないと思う。

しかも、今後の成長市場が東南アジア等であるとすれば、そこには独自の風土があることにも留意しなければならない。私たちの研究結果によると、東南アジアには欧米のドライな企業風土とは違った濃密な人間関係があり、そこで機密情報を意図せずに共有してしまうというリスクが高いことがわかっている。このような点に配慮が必要である。

米国の映画配給会社のケースは、ケーススタディとしては、非常に有効だと思う。管理を強化しろという面からは、同社の親会社も大変であろうが、もっと何とかならないのかという指摘もあり得ると思う。しかし、逆に同社だから、あの程度で済んだという見方もあると思う。具体的に、親会社のグローバル経営は非常に長い歴史を持っており、取締役と執行役員を分離して、既に長い歴史がある。さらにグローバル情報セキュリティポリシーを全社統一で定めており、その関連として、グローバル情報セキュリティスタンダードを定めているようである。

また、たまたま同社の前身は、米国文化の一翼を担ってきており、これが作用して、米国が同社を守ってくれた面があったと思うが、その他の日本企業がこういう対応を受けられるかというと、そうは思えない。

先日中東で起きた人質事件では、関係の皆様は大変御苦労されていると思うが、今後、社員情報を出すということにも注意しなければならない。

なお、以上申し上げたことをさらに進めると、将来的には情報セキュリティ報告といったことを法的に義務化すべきだ、という意見もあり得るかと思う。ただ、米国の証券取引委員会でも2011年にガイドラインをつくったが、現在、法的な義務化はしていない。日本もガイドライン的な導入が有効なのではないかと考える。

○（前田本部員）学者として、意見を一言述べさせていただく。

戦略本部に改組されたことは、今までから見ると大変大きな前進であったと思う。ＮＩＳＣが重大インシデントを調査する権限を広く持つようになったことは非常にすばらしく、大事なことで、内閣官房組織であることから実質的な機能を持つところとして非常に重要だと思う。ただ、政策とのバランスでいうと、具体的な問題が起こったときの対処関係、例えば警察庁とのバランス、調和を考えることは、十分に考慮されていると思うが、大事だと思う。

刑事訴訟法、法的な観点からすると、ログの保存の問題がある。これは刑事訴訟の運用という狭い範囲だけではなく、対テロ対策や、国際関係という観点からも考える必要

がある。今回のテロのような問題が起きた際、お互いにログがどうなっているのかを聞かれて、日本はログをとっていないと言えるのか、日本がその国に致命的なダメージを与えたのに、我々はログをとらない国ですと言えるのか、ということである。今までコスト等いろいろな理由を言ってきたが、国際的にはもう通用しなくなるのではないかと思う。

それから、ＪＰＣＥＲＴ／ＣＣ等との連携は非常に重要である。後で申し上げる将来の方向性との関係でポイントになってくるのは、情報をいかに守っていくか、日本の安全をいかに確保するか、ということ。テロ対策その他の観点からいうと、サイバーセキュリティの情報に関しては、機微なものが非常に含まれており、クリアランスの観点、どこの誰が見て良いかという観点が重要である。両者は車の両輪であり、ばらばらにやっても機能しないわけであるが、いかに信頼関係を持ってその範囲で協力していくかということが重要になってくる。

先ほど小野寺本部員が教育の問題を指摘されていたが、私が所属する大学はサイバー問題の不祥事があり、私の個人情報等も出てしまい、セキュリティ管理ができていないと言われている。当大学の運営費の一部は税金で賄われており、それが犯罪のネタにされている。ここでは文科省の問題はほとんど出てこないのであるが、やはり重要インフラうんぬんというとき、大学のあり方も考えなければいけない問題だと思う。

最後に、サイバーセキュリティ戦略本部がどのように変わっていくかの将来的な展望の方向性について個人的な意見を述べる。これまで、重要インフラをいかに守るか、民の生活をいかに守るかということに取り組んできたが、今回の風刺画に関するテロ等一連のものを見ていると、情勢は大きく変わっている。一言で言うと、戦後の日本の憲法の中で何よりも大事だと言ってきた表現の自由や通信の秘密というものの根本的な考え方が、ほころび始めた、瓦解が始まった、という感じがする。もっと大事なものがあり、そのバランスを考える必要がある。国によって表現の自由は違い、守るべきものが違う。北朝鮮の一件もあるが、日本に同様のことが起きたら、どう考えるのか。

そのようなことから考えると、政府が言われるとおり、記録を集めることは何よりも大事である。そのときに、サイバーテロの発生は情報を合法的に収集することができる最大の場となる。ただ、人材がいない。サイバーが安全な社会であることを保障することは大事であり、それは変わらないが、サイバーに絡む社会で生活している国民を守るためには、半歩前に出る状況がいずれあるのではないか。守れば良いというよりは、悪い動きに対して、合法の範囲で、政府の力で情報を集めてよく知る。そのような方向で、半歩でも進めれば良いと思う。

○（村井本部員）日本の良いところについて、意見を申し上げる。

資料４の５ページを見ていただくと、ここに「各国のサイバーセキュリティ戦略等について」という記載がある。ドイツの戦略の項の備考欄を見ていただくと「『Industrie4.0』（インダストリー4.0）として、ＩｏＴによる製造業の技術革新を提唱」とある。これがドイツの政策であり、ドイツのサイバーセキュリティ戦略である。

ＩｏＴ（Internet of Things）は、ＰＣやスマートフォンだけではなく、デバイス等々がインターネットにつながっていき、それが製造業の技術革新に結び付くという考え方

であり、これは日本が非常に強い分野である。例えばスマートシティや、制御系、エネルギーマネジメント、家電といったものがインターネットにつながってきちんと動いていることに関しては、日本は圧倒的に先端な国である。ＩｏＴという新しい世界の安心・安全をつくっていくのは、日本の役割になるのである。

もう一つ、同資料の１ページ目を見ていただくと、これまでいろいろな事件が起こっているが、ほとんどが間違いや、事故、やり忘れといった穴を突かれている。つまりサイバー空間のクオリティの問題なのである。

先ほど挙げた製造業や制御系、サービスといったものの品質管理については、日本は非常に強い。クオリティアシュアランスに関するリーダーシップは、日本の産業がずっととってきた。今、ＩｏＴの時代にサイバー空間の品質管理という視点で考えると、日本には大変大きな責任がある。安心で安全なサイバー空間には高い品質管理が必要であり、これをつくっていけるリーダーは、やはり日本だと思う。

インターネットを知らない人もサイバー空間を自然に使っているというのがＩｏＴの時代である。日本には高い品質で保たれるサイバー空間をつくっていくという、大変大きな役割・責任がある。

もう１点、資料６にＮＩＳＣとＪＰＣＥＲＴ／ＣＣ、ＩＰＡとのパートナーシップについて記載されており、大変良いことだと思う。ここで皆さんと共有しておきたいのであるが、今、ＪＰＣＥＲＴ／ＣＣが世界の中で大きなメッセージを出している。サイバーグリーンというコンセプトである。ＪＰＣＥＲＴ／ＣＣ、つまり日本のＣＥＲＴからのメッセージが、インターネットの世界だけでなく、サイバーセキュリティの世界で、大変大きな輪をつくり始めている。

そのコンセプトとは、グローバルな空間であるサイバー空間において、各国がどのように安全な空間をつくっているかという指標をつくろうというものである。ここでいう安全とは、サイバー空間で安心して経済活動を行えるか、ということであり、各国毎にこれを指標化しようという動きが、サイバーグリーン運動である。

その中で、先ほどのお話と結び付けると、日本はものすごくランキングの高い国になるだろうと思われる。ポイントとなるのは、安心・安全なクオリティの高いサイバー空間をつくる技術力、あるいは品質管理の力である。こういうものが今、サイバーセキュリティをつくっていく上で大変重要になってきており、日本は大変大きな経験も実力もある。そういった形の結び付きも考慮してサイバーセキュリティを考えていくことも重要ではないかと考えている。

○（山口情報通信技術（ＩＴ）政策担当大臣（副本部長））

先ほど来話があったように、パソコンや携帯電話のみならず、あらゆるものがインターネットにつながる、いわゆるＩｏＴ社会が到来しつつある中、国民の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が必要不可欠であると考えている。

ＩＴ政策を担当する大臣として、今後はサイバーセキュリティ戦略本部とＩＴ総合戦略本部の緊密な連携を図りつつ、政府全体のＩＴ戦略を着実に推進していきたいと考えている。

○（山谷国家公安委員会委員長）サイバー空間の脅威が深刻化する中、サイバーセキュリティ戦略本部の下、政府一丸となってサイバーセキュリティを強化することは、極めて重要であると認識している。

特に重大インシデント発生時の原因究明は、警察による捜査と調和し、政府全体としての迅速な被害拡大の防止に資するものとなる必要があると考えている。

様々な事案対応等を通じて、警察が培った実践的対処能力と知見を生かし、引き続き内閣サイバーセキュリティセンター等と連携の上、我が国のサイバーセキュリティの確保に貢献するよう、警察庁を督励していく。

また、原因の究明には、ログが保存されていることが必要である。これは、サイバー攻撃等が容易に国境を越えて行われることを踏まえると、我が国の安全保障上の観点からも重要なものであると考えている。今後ともログの保存のあり方について、関係省庁間において十分に検討が進むことを期待する。

○（高市総務大臣）総務省では、サイバーセキュリティ基本法の成立を受けて、東京五輪を見据えた新たな情報セキュリティ対策の検討に着手している。４月ごろを目途に、新たな情報セキュリティ対策の方向性を取りまとめる予定であるので、政府全体の戦略の策定に積極的に貢献していきたいと思う。

また、総務省では、政府機関や重要インフラ事業者等を対象とした、実践的サイバー防御演習ＣＹＤＥＲを実施中である。本日、参考資料として、１枚お配りしている。

この演習の実施で得たノウハウを活かし、３月には全省庁が競うサイバーセキュリティ訓練をＮＩＳＣと共同で実施予定である。このような取組を通じて、我が国全体のサイバーセキュリティの向上に貢献していく。

○（岸田外務大臣）昨年11月には、米国の映画配給会社がサイバー攻撃を受ける等、サイバーセキュリティは、国家の安全保障にかかわる重大な問題である。

５年後のオリンピック・パラリンピック東京大会の前に、来年には先進国首脳会議を控えており、我が国としても早急に対応を進めることが必要である。

外務省としても、関係国との連携、サイバー空間における国際的なルールづくり、あるいは信頼醸成の促進、さらには途上国に対するＯＤＡ等を活用した能力構築支援の取組を一層積極的に進めていく。

○（宮沢経済産業大臣）先ほどの報告事項にもあったとおり、また、今、何人かの本部員の方からも触れていただいたが、このたび、経産省が関係する２つの機関が内閣サイバーセキュリティセンターとの間で協力覚書を結んでいる。これを受け、経産省としても、当本部を中心とした効果的な対策実施に協力していく。

新・サイバーセキュリティ戦略については、サイバー空間の大部分が民間企業により構成されていることから、民間における対策が重要となる。また、オリンピック・パラリンピック東京大会に向けて、官民連携により、セキュリティ対策に万全を期していくことが必要である。

このため、まず重要インフラ企業について、国がイニシアティブをとって対策を強化する方策を検討していく。

さらに中小企業を含めた一般企業の対策強化に向けて、第三者認証の活用等による促進を検討していくことが重要である。

また、人材育成や研究開発といった基盤的分野においても、底上げに向けた取組強化を検討していく。

○（中谷防衛大臣）防衛省としては、サイバー空間を取り巻くリスクは深刻化しており、サイバー空間の安全策の強化は、我が国の安全保障並びに危機管理の観点からも不可欠であると認識している。

また、サイバー空間で高度化をする脅威に適切に対応することは、自衛隊の任務遂行においても、サイバー空間を安定的に利用していく上でも不可欠であると思う。

今般のサイバーセキュリティ基本法の成立、またサイバーセキュリティ戦略本部の新設を機に、サイバーセキュリティの一層の強化に向けた政府全体の取組に対して、防衛省・自衛隊としても最大限の努力を行っていく所存であり、国民の負託に応えるべく、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。

⑶　決定事項の決定等

決定事項８つにつき、案のとおり決定した。

また、新たなサイバーセキュリティ戦略について、本会合での本部員意見に加え、サイバーセキュリティ基本法の規定に基づくＩＴ総合戦略本部、及び国家安全保障会議からの意見聴取を踏まえて戦略案を起草し、次回会合で議論を行うこととした。

⑷　本部長締め括り挨拶

本日は、限られた時間にもかかわらず、大変有意義な意見をいただき、まことに感謝申し上げる。

サイバー攻撃の脅威が深刻化する中にあって、安全なサイバー空間を確保することは極めて重要である。

こうした中で、サイバーセキュリティ基本法が制定され、政府においても政策の企画・立案、さらにサイバー攻撃への対処の両面において司令塔機能の強化を図ったところである。

今後は戦略本部とこれを支える内閣サイバーセキュリティセンターが司令塔となり、政府一丸となって取り組んでいくので、各府省においても、それぞれの役割を一層積極的に果たすようお願いする。

また、有識者本部員の皆様におかれては、新たなスタートを切る戦略本部の取組について、今後とも一層の協力を賜ることをお願いして、挨拶とする。

－　以上　－