サイバーセキュリティ戦略本部
第８回会合　議事概要

１　日時

平成 28 年６月 13 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）

菅　　義偉	内閣官房長官
遠藤　利明	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担当大臣
河野　太郎	国家公安委員会委員長
高市　早苗	総務大臣
松本　文明	内閣府副大臣
黄川田 仁志	外務大臣政務官
北村　経夫	経済産業大臣政務官
藤丸　　敏	防衛大臣政務官
遠藤　信博	日本電気株式会社代表取締役会長
小野寺　正	ＫＤＤＩ株式会社取締役会長
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	日本大学大学院法務研究科教授
村井　　純	慶應義塾大学環境情報学部長・教授

萩生田 光一	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)　本部長冒頭挨拶

お忙しい中、早朝から御参集いただき、感謝申し上げる。

先般行われたG7伊勢志摩サミットにおいては、議長国である我が国が主導して「サイバーに関するG7の原則と行動」を取りまとめ、世界経済の成長と繁栄のためのサイバー空間の重要性、その前提としてのサイバーセキュリティ確保のための国際的な協力の必要性を改めて確認した。

そのような中で、我が国の施策にも注目が集まっている。今後は、特に、新産業の創出、人材育成のための環境整備、重要インフラ防護のための対策強化、さらに国際連携の強化に重点的に取り組んでいくことが必要である。

そこで、本日の会合では、サイバーセキュリティをめぐる昨年度の状況等を踏まえ、「サイバーセキュリティ戦略」に沿って今年度取り組むべき施策の具体的な内容、政府機関等におけるサイバーセキュリティ対策の基準等の見直し、こうしたことについて御議論いただき、方針を決定したい。

よろしくお願い申し上げる。

(2)　討議

【決定事項】

- サイバーセキュリティ政策に係る年次報告（2015年度）について
- サイバーセキュリティ2016（案）について
- 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の改定（案）について
- 国立研究開発法人情報通信研究機構の中長期目標の改正案に対するサイバーセキュリティ戦略本部の意見について

【報告事項】

- G7伊勢志摩サミットにおける取組等について
- 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取組について

上記について、事務局から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。

○（遠藤本部員）「サイバーセキュリティ政策に係る年次報告（2015年度）」の作成、大変感謝申し上げる。サイバーセキュリティに関して何が起き、何を目指して、それから、何を行っていったかが明確に記載されており、従来の報告に比べてさらに進化していると思う。

今日は２点お話を申し上げたい。まずは人材育成、２つ目が国際連携である。

人材育成については、いろいろな手法がとられており、足りない分を補おうとする努力がなされている。

まず１点目であるが、若年層の教育、それから、現在の足りない人材に対する教育の方法論、そして一旦教育を受けた人が、キャリアはどうあるべきなのだろうか、ということを既に相当気にしているという状況であり、若年層、現在の人材で足りない部分へ

の教育、キャリアパス、この３つをワンパッケージで考えることがとても重要であろう。

もう一つ、人材教育で必要なことであるが、先日ニュースにもなったが、17 歳の若い方が B-CAS という衛星放送の有料の番組を無料化するというプログラムをつくって捕まった。相当な能力のある方だと思う。今後若い方が能力をつけてくることは大変良いことであるが、一方で倫理観の問題が教育として明確にされないと、能力は高まっていくが、ちょっと間違った使い方をしてしまうと、その人たちに傷がつく。そういうことも含めて考えると、いかにこういう教育と倫理観を一緒に教育していくかということが重要になってきているということだと思う。

実は AI というのも今、非常に大きな力となってくるが、やはり AI の使い方に関しても倫理観をどうするのかということが非常に大きな問題になってくるため、この辺の倫理観に対する教育というものも必要であろう。

人材育成の３点目であるが、こういう教育の仕組みがしっかりできてくると、急速にレベルが上がってくる。ただ、私どもの会社でも品質という問題をみたときに、プロセスができ上がると一気にそのレベルが上がって、94%、96%ぐらいまで一気にレベルが上がってくるが、最後の３%、２%、この部分を上げていくためには一人一人の意識を高めなければならない。そういう意味では、一般にパソコンを使っている方々の意識を高める手法、これをもう一段意識しないと最終的な安全のレベルというのは上がってこないため、この辺の教育のあり方、また、意識の高め方ということも、教育の１つとして考える必要があろう。

２つ目は国際連携である。御存じかもしれないが、エクスプロイトキットというものがはやっている。これは世界共通の攻撃プラットフォームと言ったら良いのであろうか、異なる分野、異なる攻撃者が同じプラットフォームを使って攻撃のプログラムをつくっているということであり、これが脆弱性を調べたり、ウイルス対策のソフトウエアを検知したり、また、マルウエア解析の環境を検知したりというようなプラットフォームである。

このプラットフォームが一般的に使われるようになるということは、世界共通的に攻撃パターンが似てくるということでもある。ということは、国際情報を早く共有することがサイバーセキュリティ上、今まで以上に非常に重要になってきており、他国でどのような攻撃を受け、我々はどのような状況をつくり込まなければいけないのかを、いかにリアルタイムに把握するか、ということが重要になってくると思う。

例としてイタリアのハッキングチームというサイバーセキュリティの会社で情報が盗まれ、１週間以内にエクスプロイトというプログラムにその部分が埋め込まれた。非常に早いタイミングで情報がプラットフォーム化されるということであり、そういう意味でもリアルタイム性を持った情報共有が国際的に必要であろう。このためのインターフェースの標準化も実は進んでいる。こういう中に日本が積極的に標準化に入っていくという努力が必要であろうと思い、この観点ではぜひ政府の力も借りながら、民間もこれに対して対応をしていければと思う。

○（小野寺本部員）２点申し上げる。

まず全体としては「サイバーセキュリティ政策に係る年次報告（2015 年度）」、「サ

イバーセキュリティ2016（案）」、これについては良い方向に行っているだろうと思っている。その中で年次報告について、資料１－１の１ページ目の政府機関等における情勢部分が一番良いと思うが、こういう状況にあるという広報をもっとやらないと、国民にはなかなか伝わらないのでないか。最近、サイバーセキュリティについては国民の関心も高まってはきていると思うが、実態がまだ知られていないというのが本当のところではないか。せっかくこのような立派な年次報告をつくられているので、こういうところをどのように広報していくか、是非お考えいただければと思う。

２点目は、遠藤本部員と一緒で、教育の話である。４月19日の産業競争力会議で総理からプログラミング教育の必修化をおっしゃっていただいた。私はこれは非常に影響が大きいと思っており、やっと必修でプログラミング教育が動き出すわけである。しかし、文部科学省に伺ったら2020年からと伺い、ちょっと待ってくださいと申し上げた。御存じのとおり、英国では本教育年度の９月からもう既に始まっている。それが2020年までというのはちょっとという気がしており、ここをどうスピードアップしていくか、是非お考えいただきたい。

それと、いつもそういうときに問題になるのは、教える教官がいないという話である。以前にも申し上げたが、国立大学の教員養成課程の卒業生が年間１万700人であり、２年くらいほとんど変わっていない。この人たちはいわゆるデジタルを最初からさわってきている人たちで、デジタルネイティブと言われる人たちである。こういう人たちにプログラミング教育のやり方を教え込むのは、正直言って30代、40代の教員の皆さんを再教育するよりずっと早いと思う。大学の教員養成課程でどう取り組むのかということを早急に決めていただければ、来年からでもそれは可能だと思う。卒業生が出てくれば、その人たちを中心に、若手の人になると思うが、プログラミング教育の実践が必修科目としてでき始めるのではないかと思うので、是非よろしくお願いしたい。

ここは遠藤本部員と一緒であるが、まさしくそのときに技術的な教育だけではなく、当然のことながらそれに対する考え方とか、そういう倫理観の養成も当然必要だと思うので、そこも御検討いただければと思う。

それから、先ほどG7の御報告もあったが、G7は問題なくいって成功だったと思う。これはNISCを中心とする皆さん方の努力の成果だと思っている。

問題は、G7の成果がオリンピック・パラリンピックにそのまま活きるかというと、これは全く性格が違うのではないかと思っている。特にG7のときには要人の警護とか、要人に対するアタックということでエリアも非常に絞られており、対象者数も限られていたが、先ほど資料６でも御説明があったとおり、オリンピックでは、運営システムそのものがダメージを受けるとか、もしくはそこに来ている観客の端末に対して全て攻撃をかけられるとか、攻撃のかけ方そのものがG7のときとは全く異なるのではないかと思っている。ここは専門家のNISCの方々は十二分に御理解されていると思うが、ただ、どうしてもG7の成果を活かしという書き方が強くなるものであるから、少し気になり、申し上げた。

○（中谷本部員）４点申し上げる。

第１に、伊勢志摩サミットにおいて採択された「サイバーに関するG7の原則と行動」

において、「我々は、国連憲章を含む国際法がサイバー空間において適用可能であることを確認する。」、「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、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。」と明記された。このことはG7の結束を示すにとどまらず、サイバー空間における法の支配と慣習国際法の結晶化にとって非常に重要な意義を有するものであり、高く評価したい。

第２に、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の改定は、全ての独立行政法人及び指定法人における適切な情報セキュリティ対策のために不可欠であると考える。指定法人は施行後に本戦略本部において決定するものと理解しているが、個人情報の保護など適切な情報セキュリティ対策のために積極的に対応していく必要があると考える。また、独立行政法人や指定法人のクラウドサービスの利用に際しては、機微に係る情報は国内に留保して、国外のクラウドサービスには委ねないこと、クラウドサービス契約においては準拠法は日本法とし、裁判管轄は日本とするよう対応すること、がとりわけ必要であると考える。

第３に、NICT において研究開発成果を最大化するための業務に、サイバーセキュリティに関する演習が加えられることを歓迎したい。演習は最善のサイバーセキュリティ対策であり、今回の業務追加は、国の機関や重要インフラによる実践的なサイバーセキュリティ対応にとって非常に有意義であると考える。

第４に、南アフリカの銀行が発行したクレジットカード情報などを悪用して、コンビニの多数のATMから合計20億円近くが不正に引き出されるという非常に深刻な事件が発生してしまった。ATM とクレジットカードのセキュリティの脆弱性は、残念ながら嘆かわしいと言わざるを得ない。セキュリティ対策の抜本的な強化を大至急行うことが不可欠であると考える。

○（野原本部員）３点申し上げる。

まず１点目は、伊勢志摩サミットで会議の運営に支障をきたすようなことがなく、無事対応できたということで本当に良かった。皆さんの周到な準備の賜物だと思う。2020年東京オリンピック・パラリンピック競技大会に向けてやるべき対応は大きく違うと、先ほど小野寺本部員からもコメントがあったが、大会関連のシステムや政府機関、重要インフラ等を含めて、幅広い領域に対してリスクを再度検討し、しっかり取り組んでいただきたい。

２点目であるが、今年度の施策である「サイバーセキュリティ2016（案）」をしっかりと拝見した。よくバランスがとれた施策群がつくられていると思うので、これをしっかり実施していただきたいが、例えば重要インフラの各業界については、固有の対策が少ないのではないかと感じている。重要インフラを守る取組について本文の項目を読んだが、大半の項目は各業界に共通の対策をしっかりやりますというような対策の列挙になっており、業界に固有の施策としては、例えばクレジット決済端末のIC対応化100％を実現する、といったものが注目されるくらいである。金融業界だけを見ても、このほかにもオンラインバンキングの不正送金であるとか、コンビニATMからの不正引き出し

等、広域プラットフォーム化の話も先ほど出たが、産業化するサイバー攻撃によってさまざまな課題が出てきている。それらに対して、それぞれの業界特有の課題を解決する施策がもっと検討され、追加されるべきなのではないか。

３点目は、サイバーセキュリティ産業の育成、振興についてである。冷静に考えると我が国の状況というのはなかなか厳しいところであるが、それゆえに戦略的に賢く施策を展開していく必要があると思う。関連産業の育成・振興については、政府系ファンド等の活用を始め、いくつか施策が記載されているが、その内容は極めて貧弱だと思う。

海外の状況、例えば米国やイスラエルの状況を見ると、膨大な軍事予算と日々攻撃にさらされている実戦経験を通して、軍や情報機関のニーズに対応した高度な技術や人材が養成されており、その技術や人材が民間に流れるというような好循環が生まれていて、それがサイバーセキュリティ産業を進化させているというようなエコシステムが機能している。

これに対して日本においては、そういう状況を生むというのはなかなか難しいわけで、これらのサイバーセキュリティ先進国に勝てるような先進技術を開発するとか、セキュリティ産業を育成しグローバル競争に打ち勝つというのは、容易なことではないと思う。それでも育成、振興していくということであれば、こうした状況を踏まえて戦略的に賢い施策を展開していく必要がある。

例えば思いつきではあるが、研究開発や実証実験の場合は、日本でもサイバー攻撃に反撃するような技術の開発や実験ができる環境をつくる等、より有効な施策を検討していくべきではないかと思う。

○（林本部員）今回の議題、決定事項を見ると、これは大変実務的な面が強いのであるが、セキュリティは元来、基本に忠実に実行することに意義があるので、このようなルールを定めて日常業務を淡々とこなすことが大切だということを再確認した。また、ルーチン化は一朝一夕で整備できるものではなく、長い年月をかけた関係者の御努力でここまでまとめることができたのだなという印象を持ったので、決定事項には賛成である。

しかし、資料を通読した中で、「サイバーセキュリティ政策に係る年次報告（2015 年度）」の別添４に重要インフラの資料があるが、その中に重要インフラ事業者等における情報セキュリティ対策に関する取組の評価みたいなものがあり、俗に言われる PDCA、Plan、Do、Check、Act のうち、P はほぼ実施されているが、D はかなり心もとなく、C と A は余り取り組まれていないというデータが目についた。日ごろから私もどうもこうではないかと思っていたところと符合するところがある。

そこで、基本をさらに徹底するには何が必要かということを考え、一応の体制が整った現時点では、強いところをさらに強くすることも大事であるが、弱いところを補強するほうが肝要かと思い、その点について６点ほど、ある種のギャップを埋めるという視点から申し上げたい。

第１は、中央省庁間にもあるギャップである。NISC とそれぞれの官庁の関係を見ても、所掌業務とセキュリティの相関度が高いところから低いところまで、官庁間にかなりの差があると思う。これは私の直感ということではなく、同じく年次報告の中に別添１として各省庁ごとに御自身の自己評価のような形でステートメントがつけられているが、

それを見ても濃淡があるなということは推測できる。もちろん秘匿すべきものは秘匿しなければならないので、その面で隠れていることはあると思うが、やはり濃淡はあると思う。しかし、今やセキュリティは全ての組織の問題になっているため、相関度が低いからといって気を抜くことはできない。そこで、今後はあらゆる手段を尽くして相対的に弱い官庁の底上げということが必要ではないかと思う。

第２は、中央と地方のギャップである。両者とも重要インフラの 13 分野の分類では、政府・行政サービスとしてまとまっているが、一括りにできるような一律なものではないと思う。例えば治安の面でいくと、体感治安が地域によって異なるとすれば、それに応じて高低があってもいいということはあるかもしれないが、サイバーの世界では地理は意味を持たないことになるので、ある種、統一が必要ではないかと思う。

第３は、民間における重要インフラ事業者の間にあるギャップである。重要インフラの横断連携など、これまでの対策は成功しつつあると思うが、いざ事が起きたときの体制とかレジリエンスの面では、演習を通じて実力を把握し、逐次レベルアップを図る必要があると思う。今回の案にも経済産業省が制御系システムの人材育成策を挙げられているようで、それはそれで評価できるが、このような視点を重要インフラ全体に投げかける必要があろうかと思う。

第４は、大企業と中小企業の差である。この差は上記の３つのギャップを上回るほど大きいかと思う。自前でできるところは自前でやっていただければ良いのであるが、手が回らない企業の助けになるような手段を工夫する必要がありそうである。しかもそうしたある種、小さい企業がサプライチェーンの上では重要な役目を果たしているということがあり得る。

第５は、世代別のデジタル対応であり、これは通常、高齢者をどうするかという問題もあるが、逆に若手に対してどういう施策が必要かという問題がある。この点については既に遠藤本部員、小野寺本部員が発言されたが、私もほとんど同じことを考えていた。

最後の第６は、以上の５点とやや視点が変わるが、国内対策と国際関係の問題である。セキュリティ対策は国際的な協調なしでは十分でないことが知られており、中谷本部員から御発言があったように、伊勢志摩サミットはその面では大きな一歩だと思う。しかし、世界は情報の自由な流通を信ずる国々と、それよりも国家主権を重んずる国々に分断されている。このギャップを埋めるのは容易ではないと思うが、片方で情報共有とか捜査協力あるいは標準化活動などの現場レベルで協力を続けるとともに、伊勢志摩サミットに続いて政策協調の国際会議などで日本が提案するような努力が継続的に必要かと思う。

○（前田本部員）初めに、去る５月９日に奈良先端科学技術大学院大学の山口教授が亡くなられた。山口教授は長く我が国の情報セキュリティ、特に NISC に大変な貢献をされて、現在の NISC があるのは、もちろん多くの方のお力なのであるが、山口先生のお力は非常に大きかったと思う。私個人も非常に多くの御教示をいただいたので、ここで謹んで哀悼の意を表したい。

私は犯罪とテロという観点からお話をさせていただきたい。

まず第１点は、人材育成に関しての方針を前に進めるという議論は全く異存のないと

ころである。しかし、そのときに私が一番感じるのは、先ほどの小野寺本部員の話にもつながるのかもしれないが、これまではサイバーの専門家をつくるという意識があった。もちろん今でもそうなのであるが、ただ社会全体を国民目線で見ると、リアルな普通の社会とサイバー空間がどんどん融合してきて、スマホ抜きの学校生活といったものは若い人の生活では考えられず、ある程度の歳の我々も同様かもしれない。そうした中では、余りサイバー犯罪、サイバーテロに特化するというよりは、リアルな社会とサイバー空間のつながりを重視していかないと、国民から見て安心安全に対応できていないことになるのではないか。

先日、小金井で芸能活動を行っている女子学生が刃物で刺される殺人未遂事件があった。我々はストーカー対策などをずっとやってきているわけであるが、あそこでネットの視野が足りなかったという指摘が強く来ている。それはもちろんそのとおりかもしれないが、今の段階では学ぶべき点は２つある。

一つはネットを使ってもっとそういう情報を集めておけば対応できたので、事件が起きてからでは遅い、起こらないように何とかする、そのためには情報収集を行うということ。しかしそのときにネット、サイバーの世界の情報の集め方に対して、まだまだ国として対応が十分できていないのではないかと、いずれ国民からも強い指摘が出てくると思う。

もう一つは、去年１年間で大変NISC も御苦労された日本年金機構の個人情報流出事案の問題がある。これは起こる前に潰さなければいけない、情報を集めなければいけないということもあるが、やった犯人を捕まえる、今まだ捜査は継続していると思うが、やった人間を捕まえて潰していくという方向でのサイバー空間に対する力の強化も国民は望んでいるのだと思う。そのための人材養成も非常に重要になってきている。

その意味で国民から見て非常に関心があるということの象徴というか、中谷本部員、野原本部員からも発言があったが、南アフリカの銀行口座であれだけお金が瞬時に抜かれていく。これは国民から見たら不安を覚える。それに対応するために、銀行としては、システム部門では磁気テープではなくてICにしなければいけないなど、いろいろな技術論はあるが、犯人の一部検挙が始まっているようにやはりたどっていってきちんと捕まえることが非常に重要である。

第２点は、これも先ほどから何回も発言されているが、NISC の国際化対応である。捜査機関はICPO などいろいろ取り組んでいるが、国全体として国際連携のできる組織で国際化に対応していかなければならないと思う。

課題ばかり申し上げたが、伊勢志摩サミットは100 点に近かったと思う。サイバー攻撃も懸念されていて、それを見事に封圧した。もちろん御指摘のように2020 年東京オリンピック・パラリンピック競技大会も質が違う攻撃が考えられるのであり、それに対応していかなければいけないが、この経験を踏まえてさらに前に進むことは十分可能である。そのためにはNISC を軸に、各省庁間の連携をさらに進めていくことが重要だと思う。

○（村井本部員）１点目は、技術の発展や展開とサイバーセキュリティあるいはリスクとの関係は同期をしていかなければならないという点である。IoT やAI、家庭の中でのテレビなど、技術は大変発展をしている。そして領域としても、例えば今、農業機器はロ

ボット化され、あらゆるデータを農地から集めて新しい農業をつくろうとしているし、病院では医療のデータがいろいろな分析に供され、健康な社会をつくるために利用されている。これは内閣の立場から言うと、全ての分野の全ての大臣の管轄において、新しい技術を使い新しい日本をつくっていくという方向に一斉に動いているのである。それら新しい技術のサイバーセキュリティを考える上で、どのようなリスクがどこにあるかということを、全体を見通して考えられるのは内閣なのである。

これまでは、情報は特定の分野が専門であろうと思われていたが、あらゆることで情報が品質、安全、そしてそうしたものを追求しながら発展していくということが日々起こっており、そこからリスクの変化が起こる。このリスクの変化に対応するのがサイバーセキュリティの話である。IoT や AI の時代において大変な勢いで変わっているため、新しいアプローチをきちんと考えて、発展していく日本と、そこで生まれてくる新しいリスクに対応する。この体制をつくっていく必要がある。

研究、アカデミズムとしてそれはできると思うが、そのような体制に必要な人材をつくらなければならないということがあり、これは大学として我々も頑張っていく。

ここで課題として共有しておきたい人材の分野が２つある。１点目は、経営者のトップマネジメントが、今申し上げたような IT による変化をどのように捉えているかということ。そこに新しいリスクが生まれてくるため、経営者の理解を促進していくということを、例えば経団連であるとか、経済界の中で大変大きな動きとして考えていただく必要があると思う。

２点目は地域である。地域の IT 化が大変な勢いで進んでいくと思う。このことは地方を活性化するために必要である。このとき特に中小企業が情報化で発展をしていくというプロセスは進むと思うが、その際にこの情報のリスクというものを伝えられる人材をどのようにして地方で確保するかということがある。この２点は大変大きな課題として残っており、残りの部分は大学を中心につくっていくことができると思うが、その部分は政府として検討しなければならないと考えている。

また、今回、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取組の説明があった。私は、アトランタオリンピックと長野オリンピックでは、IBM と組んでずっと情報システムの準備をしていた。その際は、日本 IBM としっかり連携することで全ての情報システムの仕組みがわかった。今度の東京オリンピックでは、情報システムを担うのはフランスのアトスという会社であろう。時計は全てオメガである。セイコーでもシチズンでもない計時をする。計時というのはデータの一番の中心である。そうすると大変重要だと思うのであるが、資料６で示された体制をつくっていただいて、遠藤大臣のリーダーシップで進んでいくと思うが、技術から考えると私は長野より日本が入りにくい状態だと思う。ロンドンのときもブリティッシュテレコムが全てのサイバーセキュリティを一手に見られた。では東京オリンピックではどのようにしたら一手に見られるかということが課題となるが、このチームの構造だと前回までのオリンピックとは状況が異なるのではないか。それだけに資料６でお示しいただいた体制が大変重要なことになってくると思う。お示しいただいて良かったと思うが、そのことを是非考えていただきたい。

最後に、この資料６の４ページに記載があるオリンピック CSIRT について、これをつ

くろうということが第６回会合で決められた。そのことが書いてあるのだが、併せて「政府CSIRT」として、「NISC を中心に、政府機関、重要インフラ事業者、セキュリティ関連組織等の情報共有・対処体制の確立」するとも書いてある。経済産業省も全ての経営組織にはCSIRT をつくろうというガイドラインを出している。ただ、CSIRT とは何なのか本当に理解されているのか。日本年金機構の事案ではCSIRT がうまく動いていたかどうかが重要なポイントで、そこが反省点だと言うほど重要なものである。もはや CSIRT という言葉を略号として政府の文書に記載するのはやめてはいかがか。CSIRT では理解されないであろう。これはComputer Security Incident Response Team のことで、世界中でやるべきことは決まっており、一般名詞である。一般名詞をどうしてアルファベットで残さないと政策ができないのかということは、そろそろ考えたほうが良い。私も協力するので、きちんとわかりやすい日本語の名前にしたほうが良いのではないかと思う。

○（遠藤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担当大臣（副本部長））
サイバーセキュリティ戦略本部による原因究明調査等の範囲を独立行政法人や特殊法人等に拡大することなどを盛り込んだサイバーセキュリティ基本法の改正案が、本年４月に成立した。今後は改正法の円滑な施行に向けて、政府として全力で取り組んでいく。
また、先月のG7 伊勢志摩サミットにおいては、関係府省庁が連携してサイバーセキュリティ確保のための取組を推進しており、会合の運営に支障をきたすようなサイバーセキュリティ関連事象はなかったところである。
サイバーセキュリティの確保は、2020 年のオリンピック・パラリンピック東京大会の成功の条件である。まずは、G7 伊勢志摩サミットにおける取組結果をしっかりと総括した上で、今、話があったように小野寺本部員あるいは野原本部員、村井本部員からの御指摘を踏まえながら、東京オリンピック・パラリンピック競技大会における取組に反映していく。
引き続き、重要インフラ防護など各種重要な課題は多くあるため、サイバーセキュリティ戦略本部の副本部長として政府全体のサイバーセキュリティの強化に向けて全力で取り組んでいく。

○（河野国家公安委員会委員長）伊勢志摩サミットに関するサイバー対策においては、関係省庁あるいは重要インフラ事業者を始め、専門家の皆様、さまざまな皆様に御協力、御支援をいただき、本当に無事に終えることができたこと、改めて感謝申し上げる。まだ関係閣僚会議がいくつか残っているため、最後までしっかりやりたい。
小野寺本部員から、サミットとオリンピックは少し違うのではないかという御指摘をいただいたが、我々も、限定されたサミットの警備と、多くのお客様が海外から来るオリンピックは全く別物と考えなければならないと思っているため、引き続きサイバー空間をしっかり守っていくということをオリンピック・パラリンピックに向けてやっていきたい。警察もこれからしっかり情報収集、分析あるいは各国と連携をして対応をしていきたいと思うところ、引き続きの御指導、御鞭撻をお願い申し上げたい。

○（高市総務大臣）サイバー防御演習については、本日のサイバーセキュリティ戦略本部

の御意見を踏まえ、NISC や関係府省と連携するとともに、地方自治体をはじめとして対象や規模を大幅に拡大し、演習の抜本的強化にしっかりと取り組んでいく。

次に、本年４月に香川県で、G7 情報通信大臣会合を実に 21 年ぶりに開催した。G7 各国、EU、OECD など ICT 分野のリーダーと最新の ICT やサイバー空間に関する課題について議論を行った。特に、サイバーセキュリティに関しては、サイバーセキュリティのリスク、脅威及び脆弱性に対処する取組において、国際協力、能力開発及び官民連携を強化するよう努めること、サイバーセキュリティへの脅威を軽減するための人材育成の重要性、について合意した。

また、IoT への対応として、「IoT 推進コンソーシアム」において経済産業省と総務省が連携し、IoT システム・サービスの供給者・利用者を対象とした「IoT セキュリティガイドライン」を取りまとめ、現在、パブリックコメント中である。

NICT のサイバー攻撃観測網（NICTER）では、IoT に対する攻撃が観測全体の約４分の１を占めることが判明した。IoT のセキュリティ対策は喫緊の課題であり、ガイドラインを踏まえ、早急に対策を行っていく。

本日の本部員の皆様の御意見を受けて、意見を申し上げる。

先ほど申し上げた情報通信大臣会合でも、「AI の開発原則」を初めてたたき台として日本から提案した。今後、OECD などでも積極的に取り上げられていくと思う。また、開発途上国への ICT 投資の推進についても合意したが、本日の本部員の御意見を伺っていて、国際貢献をする際にも、インフラの整備だけではなく、セキュリティ、モラル教育、こういうものをセットにしていかなければならないということを痛感した。

国内でのプログラミング教育、モラル教育は非常に大事であるが、これまで Wi-Fi 環境の整備は、どちらかといえば観光地や防災拠点を中心に行ってきた。まだまだ学校の Wi-Fi 環境の整備率は低いため、文部科学省と協力しながらしっかりと対応をやっていきたい。

野原本部員からも御発言頂いたが、重要インフラ対策も各業界特有の、かつ、多様なタイプの攻撃への備えとなるメニューを考えなければならない。NICT の中長期目標変更案の中にも受講者に応じた演習内容の多様化を入れており、しっかり掘り下げていきたい。

○（松本内閣府副大臣）「世界最高水準の IT 社会」の実現を目指す我が国において、サイバーセキュリティの強化は極めて重要である。

IoT や AI の更なる進化、マイナンバー制度の普及など、IT 政策の推進においては、利用者の安全安心の確保の観点から、政府機関だけでなく、民間においてもセキュリティの確保が不可欠である。

先月 20 日に閣議決定した「世界最先端 IT 国家創造宣言」の改定においても、官民のセキュリティ対策の強化に引き続き努めることとしている。

また、創造宣言の重点テーマの１つである「情報システムの運用コスト削減」により得られた成果を、セキュリティ対策の強化にも活用していきたいと考えている。

今後も IT 総合戦略本部とサイバーセキュリティ戦略本部が緊密に連携しつつ、情報セキュリティを踏まえた IT 政策を推進していきたい。

○（黄川田外務大臣政務官）G7 伊勢志摩サミット及び G7 広島外相会合においては、内閣サイバーセキュリティセンターや関係府省庁等との協力により、会議運営に支障を来すような事案は確認されなかった。外務省としても、今後ともサイバー攻撃対処のために関係者間で緊密な連携を図っていく。

サミットでは、長官の冒頭挨拶のとおり、G7 で一致して情報の自由な流通の重要性や、サイバー空間における法の支配の強化も含めた力強いメッセージを出すことができた。

また、サイバーセキュリティに関する G7 作業部会の設置も決定された。この作業部会、ワーキンググループを通じて、サミットの成果を実効性のある G7 の協力関係につなげていく。

遠藤本部員より御指摘のあった国際社会における情報共有の強化にもしっかりと取り組んでいきたい。

国連や G20 といった国際的な議論の場において、引き続き法の支配や信頼醸成の促進に向けた議論を加速化させていく。さらに、ODA 等を活用した関係国の能力向上支援についても、関係府省等と連携しつつ、引き続き積極的な取組を図っていく。

○（北村経済産業大臣政務官）先の国会においてサイバーセキュリティ基本法と併せて、情報処理の促進に関する法律が成立した。IPA を通じ、独立行政法人等のサイバーセキュリティの対策強化に貢献していく。

その上で、経済産業省の今後の取り組みを３点挙げたい。

１つ目に、サイバーセキュリティ対策の必要性について、事業者の認識を喚起する。

２つ目に、規制やガイドラインなどの制度整備、サイバーセキュリティ保険などのインセンティブのあり方について検討する。

３つ目に、各本部員から御指摘があった人材育成について、サイバー演習や脆弱性の検証などを行うことにより、実践的な能力を持った人材の育成を担う新組織について、来年度半ばを目途に設立すべく、今月より検討を開始する。

こうした取組の結果、サイバーセキュリティ対策を担う企業が国内で次々と誕生し、やがてそれが一大産業として成長していくことを目指し、引き続き NISC の御指導の下、官民で連携してサイバーセキュリティ対策の強化に取り組んでいく。

○（藤丸防衛大臣政務官）昨年度はサイバー攻撃の脅威が顕在化し、政府に対するサイバーセキュリティ確保の取組への期待は、これまでになく高まっているものと考える。

特に成功裏に終えることができた伊勢志摩サミットに続き、我が国では 2020 年東京オリンピック・パラリンピック競技大会を始めとする大規模な国際的行事が開催される予定であり、サイバーセキュリティに万全を期する必要がある。

「サイバーセキュリティ 2016（案）」においては、防衛省、自衛隊が今年度に取り組む具体的な取り組みも記載されており、国民の期待に応えるべく、各省庁とも協力しサイバーセキュリティの向上に取り組んでいく。

(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。

「サイバーセキュリティ2016（案）」及び「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の改定（案）」は、本日より一般からの意見募集手続を実施し、その結果を踏まえ、次回会合において最終決定することとした。

(4)　本部長締め括り挨拶

本日は皆さんから大変活発な御意見、貴重な御指摘をいただき、感謝申し上げる。今後しっかり対応させていただきたい。

本日、報告があったとおり「サイバーセキュリティ政策に係る年次報告(2015年度)」、そして「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の改定」の意見募集案等が取りまとめられた。厚く御礼を申し上げる。

政府としては、これらの決定に基づき、サイバーセキュリティの強化に着実に取り組んでいく。

今後とも、有識者の皆様には、よろしく御指導お願い申し上げる。

－　以上　－