第１８回宇宙安全保障部会　議事録

１．日　時：平成２８年１１月１８日（金）１５：００～１６：３０

２．場　所：内閣府宇宙開発戦略推進事務局大会議室

３．出席者

（１）委員

片岡部会長代理、青木委員、折木委員、久保委員、山川委員

（２）事務局

高田宇宙開発戦略推進事務局長、高見宇宙開発戦略推進事務局参事官、行松宇宙開発戦略推進事務局参事官、松井宇宙開発戦略推進事務局参事官、守山宇宙開発戦略推進事務局参事官、佐藤宇宙開発戦略推進事務局参事官

（３）関係省庁等

内閣官房内閣サイバーセキュリティセンター　瓜生参事官

内閣官房国家安全保障局　萬浪参事官

４．議事次第

（１）重要インフラの情報セキュリティに係る行動計画について

（２）宇宙システム全体の抗たん性強化に関する基本的考え方(素案)について

（３）宇宙基本計画工程表の改訂について

（４）その他

５．議　事

（１）重要インフラの情報セキュリティに係る行動計画について

内閣府サイバーセキュリティーセンターより、資料１に基づき、抗たん性強化の議論のため重要インフラの情報セキュリティに係る行動計画について、説明を行った。当該説明を踏まえ、委員及び事務局から以下の意見・質問があった。（以下、〇意見等、●事務局等の回答）

〇２つあり、１つ目は、人材の観点で、これはマンパワーが多ければいいという話ではなくて、恐らく圧倒的な専門性を有しているようなリーダーが政府内にいることがすごく重要ではないかと思うが、そのあたり人材育成に関してそういったことはどのように取り組まれる予定なのか。もう一つは、重要インフラ所管省庁ももちろん重要なのだが、事案対処省庁に対する攻撃というのが、それが最後の砦だと考えている。そうすると、対処する省庁に対す

る攻撃にどう対処するかというところがもっと重要な気がしているが、そのあたりはどう考えているのかという話である。例えば防衛省で言うと、防衛装備庁の中の電子装備研究所でも緊急という意味で取り組まれていると思うのだが、そういったところも貢献しているのか。（山川委員）

●まず１番目であるが、今回、資料を用意できなかったが、セキュリティ人材については別のチームが人材育成という形で計画をつくっており、決定をしているが、その中に構造としては２つ。まずはおっしゃった政府部内できちんとした高度人材をつくるということで、キャリアパスをつくって、まさに政府の中で情報セキュリティができるような人材をつくって、パスをつくって、処遇をきちんとしようという話があり、民間の経営層の方と現場がすごく乖離しているので、橋渡し人材という言い方をしているが、きちんと下のことを上に伝えて、社として回れるような形をつくっていこうというのを計画として出している。これら２つを支えるための大学であるとか、いろいろなセキュリティ関係の企業なんかが、外からの人を受け入れて戻すみたいな全体構造で進めていこうという計画をつくっている。それに基づいて人材育成を進めていこうという形になっている。

２つ目だが、警察、防衛ということであるが、それぞれ熱心に組織を守るのもそうであるし、さらにそれを超えて取り組むという話もされていて、特に最近は、警察はすごくサイバーの専門チームをつくって自ら対処するとともに、いろいろな事案にも対処していることがあるし、防衛省にもいろいろなサイバー関係の体制もあると思っており、そういうところはそれぞれの組織がまさに専門性を高めてやっているのだと思う。（内閣サイバーセキュリティセンター）

○３ページのところについて教えて欲しいのだが、これは基本的にはセクターの事業者ごとのコンセンサスに基づくボランタリーなスタンダードというものを守っていくように政府が支援するということなのか、そして、そうであれば結構幅の広いものになるのか。ただし、その幅の中でこれはやらなければいけないという、実質的に拘束性のあるものが決まっているものなのか、その点のイメージというのはどういう感じなのか。（青木委員）

●結論から言うと、正にここに書いてあるとおり事業者が自主的にやるものが基本になっている。これは先程冒頭でサイバーセキュリティ基本法というものができたと申し上げたが、これは決して事業者を強制して何かさせるものではなくて、それぞれが頑張っていきましょうという、基本法は大体そういう精神論的なものを書くのであり、基本は事業者がやってもらうことになっており、この計画の最後の決定はサイバーセキュリティ本部なのだが、その下に専門調査会という会議があり、そこのメンバーが実は各セプターの代表、

事業者の代表の方と有識者と各省庁が揃って、これをやっていこうと合意をする会であり、それぞれ事業者がこれ位のことだったら自ら取り組んでいこうというのを合意し、自らやってもらうというスタンスのものである。
そうすると、参加した方々が最低これ位できるかなとか、こうしなければいけないなというのを、なるべく明確にして計画という形で示して、これに基づいてやっていこうという形になる。そのため、ある程度幅が広くなるというか、まさにセプターであれば凄い熱心なセプターと、そうでないセプターも幾つかあるのだが、少なくともそういうセプターという組織をつくって共有をするという行為はやっていこうとしている。さらに共有の深度というか、幅はそれぞれまちまちなのだが、ある程度の形はつくろうというものが集まったのがこの計画だと認識してもらえばと思う。（内閣サイバーセキュリティセンター）

〇では、その評価は誰が行うのか。ここは適切であろうとか、努力が必要であろうという評価はその後どこが行い、どういう是正措置のようなものが求められるのか。（青木委員）

●基本は自主的な評価になる。従って別に国とか省庁が規制するものではなくて、もしあるとすると先ほど申し上げた業法というのがあって、それは例えば電力であれば電力が供給できなかったときの電気事業法に基づいた指導みたいなものが出て、それは例えばサイバーが原因でおこる停電かケーブルが焼けたことで起こる停電かは関係なく、停電をしたらそれに対する指導というのが発生し、そういうものはあるけれども、ただサイバーのことで何かしら省庁が指導することは、今のところは余りないと思う。（内閣サイバーセキュリティセンター）

〇今の話の続きになるかもしれないが、リスク評価も多分何段階かあって、一番厳しいリスクになってきたときに、本当に事業者主体に任せていいのかどうかという統制の問題があると思う。そこのところは書き込みできないのかもしれないが、今後オリンピック等の様々なイベントがあるので、その点のところの体制整備が必要なのではないかというのがちょっと感じており、ましてや官公庁に対する統制もそんなに厳しくできないし、民に対してはもっと厳しくできないと思うのだが、そこは物すごいジレンマを感じている。（折木委員）

●正にそういう意見はいろいろなところから聞いており、そうすると新たな法制というか、そういうオリンピックのための事業者はこうしなければならないといった形をしっかり決めて、それでやらないとなかなか何もないところで強制というのは難しいのかなというのが現状であり、まさにおっしゃるとおりであり、オリンピックの関係でそういう特別な法律が必要ではないかと

いう議論になれば、そういうことが起こる可能性はある。（内閣サイバーセキュリティセンター）

〇この前みたいな新座の事故みたいなものは、あれは例えばサイバーなのか単なる延焼なのかという判断はどこがするのか。事業者が国に報告するという形か。（折木委員）

●そのとおり。結局、我々は停電が起きたので電気事業法上は経済産業省に報告をしてということで、恐らくきちんと原因を解明した上でということになると思っており、その中で恐らくそれがサイバー原因だとなってくると、警察署だけではなくて我々にも提供してもらい、それを分析するなりして他の所に警戒情報を出すのだが、そういう形の動きになるのかなと思っている。（内閣サイバーセキュリティセンター）

〇もう一点は、情報セキュリティという観点から今の宇宙政策を眺めたときに、どういうことをやればいいか。私なんかは本当に素人だが、そういう観点で宇宙を見たときに何かコメントはあるか。（折木委員）

●15ページ目に重要インフラ事業者以外と右側に欄が書いてあり、宇宙ではないが、この前、富山大学で核融合の技術が狙われたというのがあるので、ああいった先端技術は確実にサイバー攻撃で入手しようと思っているので、例えば我が国が持つ宇宙の技術が非常に進んでいるので、明らかにそういうところにアタックをして技術を盗んで、それを使っていろいろなことをしようという人たちがいるかもしれないなというのもあるし、あと安全保障上のことで言うと、GPSの情報が実は非常に重要で、実際にあれがアタックされてやられると非常に重要な問題が起きるというのもあり、それも宇宙だと思うが、そういったことはあるのかなと思っている。（内閣サイバーセキュリティセンター）

〇２ページの下にいろいろ安全基準とか情報共有とか演習とか、いろいろフルに言っている。どれもこれも必要だということなのだろうが、よりこれで効果が上がっているなという対策はどういうものか。（高田事務局長）

●先ほども申し上げたが、２番目の情報共有体制が一番まずは効果があるのかなと思っており、それがうまくいっているかどうかのチェックができるのが、真ん中の演習とか訓練でチェックしていくというのがいいのかなと感じており、それが大体できてくると両脇に移るというか、主に公的なことで言うと安全基準につながってきちんとやりましょうとなり、各事業者の中でいくとリスクマネジメントをやっていきましょうという形になると思うので、まずは情報共有から始めて広げていくというのがいいのではないかと思っている。（内閣サイバーセキュリティセンター）

〇この演習のときに、演習のシナリオとか、そういう場をつくってしまうのも

プロ集団が必要だと思うのだが、NISCの場合はそういうプロ集団というのはセキュリティーカンパニーみたいなところを使うのか。（高田事務局長）

●シナリオづくりについては一部、外注もしている。（内閣サイバーセキュリティセンター）

○地理院のシステムはどうなっているのか。（高田事務局長）

●政府のシステムはNISC自体が政府のシステムを見ている。政府機関と独立行政法人はNISCが責任を持って見る形になるのだが、それ以外の民間になってしまうと今だとカバーはされていないので、困ったときには今でもいろいろな情報セキュリティの対処をする業者であるとか、JPCERTと呼ばれている公的な対処機関があるので、そこに相談してもらい、個別で対処するという形になる。（内閣サイバーセキュリティセンター）

○先ほどから青木委員、折木委員からあったが、非常に重要なインフラがやられる、宇宙で言えばGPSがシャットダウンしてしまうとPNTが入ってこない、それから、衛星通信が大規模にやられて、社会インフラシステムが部分的ではなくて大規模に機能障害を起こすとき、この対策をやっていなかったですというのが一番問題になる。そのシステムでポイントになるところ、本当に核心になるところ、重要インフラのノードみたいなところには強制力をある程度持たせておかないと、官庁は強制力を持たせて多分やれると思うが、民間企業に対してもそういったことをNISCの方でもある程度考えているのか。（片岡部会長代理）

●我々内閣府、内閣官房は総合調整の機関であり、各省庁の方とか民間の方がやるべきだとなってきたところで、全体を調整してやりましょうかというような形になるので、余り上から国家権力的にどうというのは、なかなか動きづらい組織にはなっている。（内閣サイバーセキュリティセンター）

○基本的には宇宙も多分同じような仕組みになる気がする。今後とも引き続き連携のほうをよろしくお願いする。（片岡部会長代理）

（２）宇宙システム全体の抗たん性強化に関する基本的考え方(素案)について

事務局より、資料２に基づき、宇宙システム全体の抗たん性強化に関する基本的考え方について、説明を行った。当該説明を踏まえ、委員及び事務局から以下の意見・質問があった。（以下、○意見等、●事務局等の回答）

○４ページの対象とする脅威・リスクという部分に関する表現である。①の敵対行為等と②の宇宙デブリの衝突や自然現象等に分けてあり、①はこれでわかる。これは考え方なのかもしれないが、宇宙デブリの衝突であるとか人工衛星同士の衝突というリスクと、自然現象によるリスクというのは対処法も

異なる部分があって、少し性質が違うものではないかという気もする。従って例えば衛星の衝突やデブリに対するものであればSSAの能力の向上によるとか、人工衛星の機能向上でうまく衝突を回避する方法が考えられる。自然現象であるとまた少し違うのではないか。宇宙天気予報などを充実させたり、ということはあっても、脅威に対処する方法も違うのではないかと考える。ただし、分類の基準は考え方にもより、対処方法の異同をきちんと知っているわけでもないので迷うところでもあるけれども、疑問に思ったところである。（青木委員）

●ただいま指摘を受けた点については、ここでは対象とする脅威・リスクで、それを前提に対策を3.2.3で脆弱性評価に従って検討していくということで、必ずしも１対１では対応していないものであるが、その脅威の性格が違うという点について、少しここでわかるように工夫してみたいと思う。（松井参事官）

〇では事務局の方でどうしたらいいのか、検討して欲しい。（片岡部会長代理）

〇イメージで言うと②の中に人造的に発生したものと、天然のものと、数字的に言うと②－１と②－２みたいな違いがあるのではないかということか。（高田事務局長）

〇そうである。（青木委員）

〇３点あり、まず５ページ目の4.1②の将来の脅威・リスクを考慮した抗たん性の維持・強化ということで、強化という言葉を入れていただき感謝している。しかし、その文章を見ると保持となっているので、何となく対応していないような気がするので、ぜひ文章のほうにも「強化する」、違う言葉でもいいが、その雰囲気が出るようにして欲しいというのが１点目である。

それから、戻って３ページの2.3の抗たん性と信頼性の部分の一番上である。予見という言葉に重点を置いて記述している文章かと思うのだが、予見することができない、そういったものを検討する抗たん性とは異なる。だから何を言おうとしているのかがちょっとわからなかった。例えば予見することが可能なものに関しては含めるのか含めないのかという意味なのか。（山川委員）

●この点については、先ほどの3.2.2の対象とする脅威・リスクという点で説明している通り、この抗たん性の議論の中で対象としているのは主に敵対行為であるとか、スペース・デブリ、太陽フレアという現象がある。他方でいわゆる一般的に対応される信頼性、部品の信頼度を上げるとか、そういった議論のところは必ずしも全部対象にはならないのだろうというのをうまく書き分けようとしているところである。その１つの考え方として、部品というかシステムの信頼性というのは、あらかじめ設計段階においてこの程度のもの

であるというのを考えた上で対策していくことを、予見と管理という形で示したかったところである。（松井参事官）

〇その後の信頼性の部分とつながっているということであれば、段落を分けないほうがいいのではないかと思う。文言はお任せする。

３つ目であるが、その同じページの我が国の抗たん性、赤い四角で抗たん性（Space System Resilience）と書いてあって、下のところのシステム自体の抗たん性は単にレジリエンスと書いてあって、何か違うような気がしていて、下にシステムと書いてあればわかるが、上のほうは同じ文言が出てきて、例えば下はSystem Resilienceにして、上をSpace Domain Resilienceにする等より広い範囲なのだという意味が分かるように、分かりやすくした方が良いのではないかと思う。（山川委員）

〇先程のNISCのお話に近いが、宇宙のものも抗たん性強化政策を打って整備をして、何か起こったときに回復するところを目指すのだが、オペレーションの観点で誰がその脅威を全体として評価をして、機能回復等をどこが指示するのか。そういったことはここ（内閣府）ではなく、衛星センターでもなく、多分NSSでもないだろう。だからそれを全体として何か起こったときに誰が責任を持って対応していくのか。そこは今の抗たん性の議論の中に入るのか入らないのか、あるいは違う項目なのか分からないのだが、先程のNISCのお話を聞いてみて疑問に思ったところである。（折木委員）

〇抗たん性をこれからいろいろ整備して、運用することになるだろう。アメリカみたいに宇宙軍等がとかが統括してやるのだったら話は分からなくもないが、米国でも民と官があって、課題もあるようだ。アメリカでも、空軍の方は空軍の担当するところだけでやっているので、当面は恐らく機能区分ごとでそれぞれの宇宙システムを管理しているところが責任を持って対処するような形になる。ただ、複数絡んだ時に、ではどこがヘッドでオペレーションするのか、ということについては、多分アメリカではJICSpOCというのが今後整備されていくのだろう。（片岡部会長代理）

〇日本も整備するのは良いのだけれども、そこのオペレーションをどうするかを考えなければいけない。（折木委員）

〇課題である。先程の重要インフラとかGPSとかの問題ではなくて、金融とか情報通信などの社会インフラシステムに衛星が入り込んで、絡んでしまっているから、そこのところを調整するところがない。会社との調整。宇宙の観点で調整するところがない。今後の検討課題である。最後の５の主な取り組み。ちょっと大き過ぎるのかもしれない。（片岡部会長代理）

●それが出来上がるのを待っていたら進まないので、中の議論ではボーイング社がやっているようなスコアリングはなかなかやり方もわからないし、何が

しか評価手法を借りてくるようなことはしないといけないと思っている。それでシステムを持っている人が自前の環境で一旦責任をとってやっていくといったが「分権型」というか、「分掌型」でもまずは進めないといけないと考える。ただ、本当は折木委員のおっしゃるとおり、やがてはそういうことも考えていかないといけない。（高田事務局長）

〇少し関係しているかもしれないが、５の今後の主な取り組みに関係するが、今後のイメージだが、この後は各省庁とか、あるいは政府、民間それぞれのところで頑張ってくださいという感じになるのか、それともまもう少しこの辺が優先課題なので、ここの続きの部分で、この辺は特に重点的にやっていくというようなものが例えば４つ、５つとか示されることになるのか。（久保委員）

〇多分、事務局が考えていると思うが、脆弱性評価とか、演習とかそういうものをやって優先課題を決めていくパターンも出てくるのではないかと思う。（片岡部会長代理）

〇今の段階では課題、やらなければいけないことが物凄く一杯あって大変である。そんな一度にできるわけではないということもあるので、どこか大事なところから少し作業の手順みたいな、この辺はともかく急ぐので、緊急性とか重大性も大きいので、何かあるのかなという感じはする。（久保委員）

〇それは今後決めていかないとならない、先導するプロジェクトみたいなものがあるとNISCも良いと言っていたので、まさしく宇宙でも先導するプロジェクトがあると非常に良いような気がする。（片岡部会長代理）

●この資料の最後の５番目のところに、今後の主な取り組みというのを示しており、これは正にこれから早急に取り組むべき事項をこの中に反映していきたいと思っており、この部分はまずは前半の部分を固めて、次のステップで表現させていただきたいと思っている。（松井参事官）

●何となく今の段階で内部的にはNISCのいろいろな対策を参考にしながら、次回、方向性を並べられればなと思う。（高田事務局長）

〇国際協力による抗たん性強化の実現の中に、国際規範構築とか何が、もし入れられるようだったら検討を。大きな枠組みでは抑止力に繋がると思うのだが、国際規範の中で、こうこうこういうことはやらないようにというルールづくりをすることも抑止力の向上に繋がり、抗たん性に繋がる、もし入るようだったら検討して欲しい。（片岡部会長代理）

（３）宇宙基本計画工程表の改訂について

事務局より、机上配布資料１に基づき、宇宙基本計画工程表について、説明を行った。当該説明を踏まえ、委員及び事務局から以下の意見・質問があった。（以下、〇意見等、●事務局等の回答）

〇SSAのフランスとの協力というのは、具体的に何か決まっている事項はあるのか。（片岡部会長代理）

●これは日仏政策対話でSSAについて取り上げていこうということで、日本側の方が現時点でいろいろ学びが多いのだけれども、情報交換していこうという。（高田事務局長）

〇そういうレベルで話が進んでいるということですね。（片岡部会長代理）

〇先程NISCの方が連携しましょうと３回ぐらいおっしゃったと記憶しているのだが、そのあたりは抗たん性のところに入れるとしたら、そこに入れるのかなと思う。これはコメントである。

それと、宇宙基本計画工程表の資料に今回入っていないが、測位衛星信号への妨害対策という部分に関しては、これはどういう扱いになっているのか。ジャミングの件である。（山川委員）

●今回の中には示していないが、今回の改訂の方向では、ジャミングというのは引き続きまた検討していくということで進めさせていただければと思っている。（松井参事官）

〇この部会が適当なのか。（高田事務局長）

●基盤部会で進める。どちらがメーンかというのは。（松井参事官）

〇確か両方に出ていたのだが。（山川委員）

●後で改めて確認をしたいと思う。（松井参事官）

〇項目の45のところである。ガイドラインの一部合意とかあるが、元々COPUOSは民生のことだけをやることになっているので、本当は安保の話ではないのだが、安保の方にも入ってきているというところだと思う。それを広義に考えて入れていいのであれば、多分、他の項目のところには入っているのだが、UNISPACE+50の文書づくりが進んでいるので、それも29年度以降というところに入れることができるのではないかと思う。多分、他の項目のところにUNISPACE+50という言葉があるので書いてはあるのだが、同時に元々は、長期持続性のガイドラインの話はこの部会というよりは産業の方だったと思うので、両方に跨ることとして書けると思う。（青木委員）

●御指摘は検討したいと思う。（松井参事官）

〇今、いただいた御意見については、工程表の改訂作業の中で検討させてもらう。

なお、宇宙システム全体の抗たん性強化に関する基本的考え方はまだ素案であるが、素案と工程表の改訂については本日の議論を踏まえて修正して、12

月上旬に宇宙政策委員会に報告することになっており、修正を含めて本部会の対応については部会長代理に一任いただければと思っているが、よろしいか。（片岡部会長代理）

（一同、同意）

以　上