第４７回宇宙安全保障部会　議事録

１．日時

令和４年４月２１日（木）　１４：００～１６：００

２．場所

中央合同庁舎４号館　１２０８特別会議室

３．出席者

（１）委員

青木部会長、片岡部会長代理、石井満委員、石井由梨佳委員、遠藤委員、久保委員、白坂委員、新谷委員、鈴木委員、中須賀委員、名和委員

（２）事務局

宇宙開発戦略推進事務局　河西局長、坂口審議官、藤重参事官

（３）関係省庁

内閣官房国家安全保障局　徳永内閣審議官

内閣官房内閣情報衛星センター管理部総務課 高橋課長

外務省総合外交政策局 宇宙・海洋安全保障政策室　倭島室長

経済産業省製造産業局宇宙産業室 伊奈室長補佐

防衛省防衛政策局戦略企画課　田邊課長

４．議事要旨

（１）議題（１）「令和３年度机上演習（ＴＴＸ）成果報告等」について、資料１に基づく内閣府からの説明の後、以下のような議論があった。

（○：委員からの質問・意見等　●：事務局、関係省庁からの回答等）

○石井満委員　質問というよりも意見になるかもしれませんが、私どもスカパーJSATとしましては、通信衛星の回線を提供している会社でございますが、主なお客様は、省庁様も含めまして、国内の重要インフラ、電力会社様、ガス会社様あるいはJR様とか、全てではないのですけれども、一般的なインフラ事業者様の最後の回線として御認識いただき、頼りにされていると認識しております。

今回の演習でそこまではやっていないと思いますけれども、私どもの回線あるいは衛星に障害があるときに、かつ、東日本大震災クラスの地震が起こっているといった状況においては、この中でいう宇宙システムを利用する重要インフラのお客様への影響が結構大きく出てくるのかなと思っています。次の、あるいは、次の次かもしれませんが、こういっ

た演習の中で、そういった東日本大震災クラスの地震が起きて通信衛星なり宇宙システムがメインの回線になっている状況、かつ、何らかの障害を起こるといった場合、私どもの重要インフラのお客様に大きな影響が出る、その辺の分析は十分したほうがいいと私どもは思っておりますし、こういったところでやることによってそこの認識が上がっていくことが大事かと思っております。

●藤重参事官　机上演習につきまして今石井委員からいただきました点でございますけれども、衛星通信に加えまして、地上の通信にも併せて障害が出ている状況は確かに十分あり得るところでございますし、また、その場合は非常に大きな影響が出ると思われますので、先生が御指摘のとおり、次の次も含めてということにはなるかもしれませんけれども、今年度、来年度の中でそういった視点も入れて社会的影響の分析や机上演習に反映していきたいと考えます。よろしくお願いします。

○中須賀委員　今の質問と非常に近いところなのですけれども、いわゆる１フェイルではなくて２フェイルの状況があまり予期されていないことでいつも大変なことになると思うので、２フェイルの状態でどういう体制をするかとか、その辺の情報の伝達をどうするかといった話はぜひやっていただければと思うところです。それが１点。

これの前提として、例えば、宇宙システム、宇宙のアセットがおかしくなったときに、各省庁が管轄する範囲内において、どういったところに連絡をしたり、あるいは、対策をしたりしなければいけないかという話は、省庁ごとにある程度まとまったというか、認識はされた上でこの机上演習をやられたのか、その辺を教えていただければと思います。いかがでしょうか。

●藤重参事官　まず、２フェイルの件につきましては、御指摘のとおりでございますので、どんどん勘案して進めていきたいと思います。

各アセットに何か起きた場合、各官庁の対策がまとまった状態であったかどうかというところにつきましては、官庁によってそれぞれございまして、各省庁が所管するインフラ単位の対処の要領についても整備・改善を続けていくように取り組んでまいりたいと思います。

○中須賀委員　もう１点だけ、いいですか。

もう一つは、いわゆるシナリオが完全に皆さんに公開されてどういうことが起こるかということが前もって分かる状況ではなくて、どこかで、いわゆるこのイベントをつくる人が皆さんに言わない状態であるイベントをつくって、見る側は今ある情報を使って何が起こったのかを判断してそれに対しての対策を取るということも多分必要になってくるのではないかと思うのですけれども、そういったことも計画されているのでしょうか。

●藤重参事官　すみません。説明が不十分でございましたけれども、昨年度の演習につきましても、シナリオはブラインドということで、このようなシナリオで用意はしましたけれども、実際のプレーヤーは、起きて、演習が終わって、反省会になるまでは、何が起き

ていたかということについては説明されないという状況で行ったところでございます。
○中須賀委員　要するに、その認識は正解だったのですか。
●藤重参事官　昨年度につきましては、大体合っていたという印象でございました。
○中須賀委員　分かりました。それもすごく大事で、僕らも衛星でよくそれをやるのですけれども、ぜひやっていただければと思います。ありがとうございました。

○石井満委員　これはオペレーターとしてということになってしまうのですけれども、今回の演習の中の仕組みで申し上げると、私どもは、運用事業者としてそういった問題を検知して、その検知した内容を、これは何々法に基づくのでこちらの省庁、これは何々法に基づくのでこちらの省庁と我々が仕分けをするような仕組みになってはいるのですけれども、それで私どもはやるのですが、あるレベル以上のものになると、我々のほうで選別するのではなくて､関係ある･なしにかかわらず全て一旦お渡しして御覧いただいたほうが、より網羅できることがあるのではないかと。例えば、このレベルで、衛星の全損とか、非常に大きな事象のときには、これはこちら、これはこちらと仕分けをするよりは、全体を見ていただくという意味で、全部をどなたかにというか、この場合ですと全省庁様に全てお渡ししたほうがいいのかもしれないという感じがしました。我々は、このタイミングでは恐らくお客様の対応でばたばたしているタイミングですので、そういった仕分けをするよりは全部の事象を各省庁様に全部一様にお渡ししたほうが、より早いし、抜けがないのかなという気はいたしました。
●藤重参事官　何か事態が起きたときにばたばたされているというところは十分理解できますし、また、どこがということを丁寧に仕分け切れるとは限らないということは全くおっしゃるとおりでございます。もちろん対応との関係でどれだけ資源配分できるかということはあると思いますけれども、複数の省庁に入れていただくことは当然ありがたいと思います。

○片岡部会長代理　御苦労さまでした。非常に年々よくなってきていると思いますし、これからさらに中身を充実して、参加するところも多くしたほうがいいと思うのですが、今回のサイバーのものは、名和さんが後でお話しになるかもしれませんけれども、ウクライナでサイバーのインシデントがあって、ViasatのKA-SATが大幅に20％ぐらいまでダウンして、これはウクライナ軍も使っていると。そのときに20％ダウンしたものをしばらく回復できない可能性が十分あると思いますので、それの対処をどうするのか。例えば、スカパーJSATさんの衛星がほとんど使えなくなりましたと。これは商業衛星ですけれども官も使っている、この状況をどうやって乗り越えることができるのかといったシナリオなども、今回のウクライナのこともサーチをして変えていく必要があるのかなという感じがします。
　国家安全保障局に質問なのですけれども、今回、こういう対応の考え方を御説明していただいたのですけれども、対応の基本ができても、どこもそうですけれども、きちんと演

習なり、フランスもAsterXという軍事演習を昨年から始めたのですよね。これをマニュアルにして対応する今回の机上演習みたいな、そういう方向は考えておられるのかどうかといったところを御説明いただきたいと思います。
●NSS　御指摘の点は重々承知をしておりまして、ここに整理しましたものは、あくまで情報の共有やどう情報を提供するかということであり、本当に大事なのは情報を政府として一体的に収集した後にどう対応するかというところだと認識をしています。これについては、今年度以降、訓練の中で取り組めるように、今、まさに調整中でありますので、御指摘の点を踏まえて、しっかりやっていきます。
○片岡部会長代理　その訓練は、何か新しくつくられるのですか。
●NSS　今調整していますものは、事態室で年間を通じてサイバーへの対応など様々な訓練を行っているのですが、その中で何かできないかということで調整しています。
○片岡部会長代理　そのサイバーインシデントの中に宇宙も含めた演習をNSSさんでやるということですか。
●NSS　まだ明確に決めているわけではないのですが、この後をどうしていくかというところも含めて、調整中です。
○片岡部会長代理　ぜひこちらの宇宙でやっている机上演習のものとか、恐らく、防衛省が、そのうち、防衛というか、軍事演習みたいなものを考えないとならない時期になると思いますので、全体を含めて、今後の方向について検討していただきたいと思います。
●NSS　分かりました。

○白坂委員　年を経るごとに進んできていることがすごくよく分かりました。ありがとうございます。
　２点あるのですが、１つが、先ほど片岡さんが先に言われたことに関連するのですが、今回、現状がこうなっているから何かが起きたときにこうやるという訓練がおこなわれた。それはどうするかを対応するということが一つはあると思うのですが、一方で、そもそもインフラとして現在の仕組みでは足りないというところ、つまり、国として重要インフラを何らかの事象が起きたときにちゃんと機能を確保するためには、例えば、別経路の何か違うものを用意しておかなければいけないとか、別のインフラの仕組み、代替を用意しておかないといけないとか、そういう今あるものをどう生かして使っていくかではなく、そもそものインフラそのものをアップデートしていく話があるのかどうかということが１点目です。
　２点目が、各省庁間とか部局間の相互理解が不足というものがあるのですが、そもそも全体がどうなっているか、何がどこにどう関係しているかということは、どなたかがちゃんと把握して、その上で、シナリオをつくるとか、オペレーションはこうあるべきみたいなことを考えられているのかということを教えていただきたい。この２点をお願いしたいと思います。

○青木部会長　時間の関係もありますので、鈴木委員に先に御質問いただいて、まとめてお答えいただきたいと思います。
○鈴木委員　私の場合、質問というよりも先ほどの片岡委員のお話の続きで、要は、今、白坂さんもおっしゃったような代替インフラ等の対処をどうするかというときに、恐らく、宇宙の場合、今回は少なくともステークホルダーが日本の中だけという前提になっているのですけれども、恐らく国際的なインプリケーションは必ずあるので、国際的なユーザーや対外的なアプローチをどうするのかということも含めて将来的には考えていく必要があると思いますので、NSSでの対処、事態室での対処と同時に、外務省とか、対外的な発信と対外的なコミュニケーション、対処等も含めて、令和４年度以降の机上演習に生かしていただければと思っております。
○青木部会長　ありがとうございます。
　事務局から、お願いいたします。
●藤重参事官　まず、こうなってしまったらというところで、インフラとして別の手があるかどうか、そもそもどうなのかという点につきましては、どちらでも気づきが出てくれば活用していきましょうというスタンスでやっているところでございます。
　全体の把握につきましては、少なくとも毎年度の演習を計画する中では、その演習のシナリオについてこういうところに影響が出てくるのではないかということは分析してつくっているところでございます。
　また、鈴木先生から御指摘がありました対外的なというところにつきまして、継続的にやっていく必要性は非常に関係省庁間でシェアされているところです。

（２）議題（２）「サイバーセキュリティ・ガイドラインについて」について、資料２に基づく経済産業省からの説明の後、次のような議論が行われた。
（○：委員からの質問・意見等　●：事務局、関係省庁からの回答等）

○新谷委員　これは事業者にとっても非常に有益なガイドラインだと思って、拝聴しておりました。ありがとうございます。
　３ページにこれをつくられた目的としてビジネス振興とサイバー攻撃による倒産等の経営リスクの軽減と書いてあるのですけれども、サイバー攻撃で実際に事業者の衛星が滅失してしまうということを言われているのか、あるいは、サイバー攻撃でサービスが提供できなくなって損害賠償請求を受けることを想定されているのか、両方かもしれないのですが、カスタマーから、サイバー攻撃があったということで損害が生じてしまった、サイバーセキュリティをきちんと事業者がやっていなかったのではないかということで損害賠償請求を受けることが考えられると思っています。そのときに、実際にこれを参考にしてもらう、自主的な対策を促す目的だと書かれていらっしゃるのですが、日本の判例法ですと、今、サイバーセキュリティのところは法律では追いかけ切れないので、アップデートをさ

れていくガイドラインに従って、当該事業者であれば必ず守らなければいけないというラインを守っていなかった場合には過失が認定されるとなっていると理解しております。このガイドラインだと、最後のほうに少し御説明があったのですが、３段階になっていまして、shallとshouldとmayとなっていて、このmayのところは当該この専門のこういうことをやっている事業者の立場に立って高いセキュリティレベルということと理解しております。shallは、今、申し上げたように、裁判所に持っていかれたときに、これを守っていなかったらさすがに過失が認定されるよねという範囲なのかなと思っています。間のshouldがあるので、これは個別判断なのかなとは思うのですけれども、こういったことが出ることで、事業者が、自分たちの身を守る、やれる限りのことはやっていたのに攻撃を受けたと主張できるのか、やるべきこともやっていなかったので損害賠償請求を受けても仕方ないのかという判断にできると思っております。

これは欧米にもいろいろあるということなのですが、欧米のものと比べてこの粒度はどうなのかということが、１点、お伺いしたい点です。欧米よりも厳しいのか。ほかの業種の場合には、３ページの左側にあるNISTが出しているものに従ってやっている事業者、ここをウオッチしている事業者はとても多いと思うのですが、本件に関しては、日本独自のものなのか、それともこちらを非常に参考にしたようなものになってshallとshouldとmayになっているのか、その粒度のところをお伺いしたい。アップデートも、海外は頻繁にアップデートをしていますが、それと同じようにされていくのかという２点をお伺いできればと思います。お願いします。

○青木部会長　すみません。時間がかなり押していますので、質問とコメントを集約してからお答えいただこうと思います。ほかに、御質問、コメントはございますでしょうか。石井委員、お願いいたします。

○石井満委員　今の話に若干かぶりますけれども、対象として、私どもは衛星の事業者になるのですけれども、衛星を製造する人といった方も対象になっているのですが、まさにこれが提供する範囲を知りたいと思っています。私どもの衛星は、国内メーカーのものもありますが、海外から買ってくる例も多数ございまして、それは、我々からすると、ブラックボックスと言うと言い過ぎですけれども、ある程度はブラックボックス化されていますので、ここまでの管理ができないことは十分ありまして、海外から買ってきた場合に、我々としては、地上設備は当然セキュリティを担保するのですが、衛星部分まで見られませんという可能性があるのですが、その点はどうなのかということを質問させていただきたいと思います。

○青木部会長　ありがとうございます。ほかにございますでしょうか。

鈴木委員、お願いいたします。

○鈴木委員　今回、観測衛星を中心にガイドラインをつくられたということなのですけれども、例えば、想像しにくいのですけれども、将来的には有人システムとか、とりわけ、通信もそうですけれども、恐らくここで示されたリスクシナリオやリスクの考え方以上の

いろいろな問題点があるのではないかと思われます。特に、地球観測の場合、例えば、データ利用に関する設備にかなり重点を置かれるかと思うのですけれども、恐らく、通信の場合は、特にダイレクト・トゥ・ホームみたいなものだとこうした設備は逆にバイパスされるのに対して、今度は衛星運用設備の重要性が重点化されると思いますし、有人はやや極端な例なので置いておくとしても、今後、こうしたリスクシナリオを考える上で恐らくそうした衛星の機能ごとにいろいろなリスクの在り方が変わってくる可能性はありますので、どちらかというと、リクエストですけれども、将来的には、省庁の壁を越えて、観測衛星以外のところでもぜひこういったことを進めていただければと考えております。

○青木部会長　オンラインには挙手が見えませんので、経済産業省様から御回答をお願いいたします。

●経済産業省　まず、欧米との比較についてですが、イギリスのガイドラインやアメリカのガイドラインを参考にしながら開発をしておりますので、基本的には彼らが書いているようなものはおおむね取り込むような形で書いているつもりではございます。むしろイギリスもアメリカも宇宙システム特有の対策は十分にはまだ記載ができているようには見えておりません。今回開発したガイドラインはサブシステムごとに分けて整理をして書いておりますので、ひょっとしたら我々のガイドラインのほうがサブシステムごとの対策については記載が多いかもしれません。いずれにせよ、こういったセキュリティガイドラインはアメリカや欧州の規格とインターオペラビリティーを取ってくるということが非常に重要になりますので、今年度、早めに英訳をしまして、アメリカやイギリスの関係機関とも議論をして、うまく合わせていきたいということは考えているところです。

司法府、裁判の関係ですけれども、国が出したガイドラインに従わなければ必ず裁判で勝つか負けるかというところは決まっていないと認識しています。過去に、IPAが出した文書に従っていなかったことなどを理由に、義務を怠っていたことが認められた判例があったということは認識しておりますけれども、どこまでやっていれば裁判で有利になるのかというところは、ケースバイケースと認識しています。

経営リスクとして何を考えているかというところについては、名和委員から御指摘いただき、倒産等の経営リスクという文言を入れております。宇宙以外の分野において実際にサイバー攻撃の影響で損害が生じて倒産に陥ったケースがあったということで、それぐらい危険なことだということがちゃんと分かるように記載をしました。宇宙分野においてどういう経営リスクを想定するのかということは、おっしゃったとおり、いろいろあると思っていまして、損害賠償請求の場合もあると思いますし、宇宙システムそのものが使えなくなることによる損害もあると思います。その辺りは、リスクシナリオの中でいろいろ想定を置いているところです。

適用範囲について、海外の物品の購入等まで適用がされるのかというところですけれども、各論になってしまって恐縮なのですけれども、12ページの衛星本体の高いセキュリティレベルが求められる場合の基本対策事項として、ｆにサプライチェーンに対するセキュ

リティ対策を記載しております。近年、サプライチェーン攻撃などという言われ方もしますけれども、外から買ってきて入れた、物品、システム、ソフトウエアなどが脆弱性になって、ここを入口にして攻撃を受けるようなこともございますので、サプライチェーン全体でセキュリティ対策を取っていくことが非常に重要になってきていると認識しております。非常に高いセキュリティレベルを求める場合には、こういった外から買ってくるものは、ソフトウエア等々も含めて、セキュリティ対策について検討していく必要があると考えています。

最後に、有人や通信衛星といった分野について、少々リスクシナリオや対策等も異なってくるのではないかということは、おっしゃるとおりと思っております。それゆえ、御指摘いただいたとおり、省庁の壁を越えて、政府全体として、本件について、経産省だけではなく、関係省庁と一緒に取り組んでいきたいと考えております。

（３）議題（３）「昨今の情勢におけるサイバー事象の趨勢について」について、資料３に基づく名和委員からの説明の後、議論が行われた。

（４）議題（４）「軌道利用のルール作りに関する中長期的な取組方針」について、資料４に基づく内閣府からの説明の後、次のような議論が行われた。
（○：委員からの質問・意見等　●：事務局、関係省庁からの回答等）

○片岡部会長代理　今後の長期的な方向で、答えられる範囲で結構なのですけれども、STMはどうなのでしょうか。今、航空機でICAOやFAAのルールづくりが行われたのですけれども、将来的にはそういうICAOみたいな形のルールが構築されていくと考えられているのか、そういう方向に日本が持っていこうとするのかどうかといったところを教えていただきたいのですけれども。
●藤重参事官　まず、日本につきまして申し上げますと、国際組織をつくっていくべきだという議論は必ずしもこれまで政府部内の検討では出てきていないところでございます。また、国際組織以前の問題として、STMに関わるルール全体について、一つのまとまった枠組みといいますか、組織には当たらないけれども法的な枠組みがどうこうというところも、正直、具体的に明示した議論はこれまでしてきていないところでございまして、この取組方針案にあるとおり、特に重要だと思われる地球周回軌道の周辺で、少なくともこの分野ぐらいルールがあったほうがいいですよねというところまでしかやっていないところでございます。国際的にも、どこかの国が具体的に宇宙交通管理に関して国際機関を打ち出しているというところは、すみませんが、把握していないところでございます。

○鈴木委員　このタスクフォースにかかる前の軌道上のルールづくりに関わって、今の片岡委員の質問と今後の方針についても、いろいろと議論はありましたけれども、１つ、ICAO

と宇宙の決定的な違いは、ICAOは、領空という地理的なコントロールのメカニズムがある前提があって、もちろん領空でない部分も飛行機が飛ぶわけですけれども、ある種の空間的な管理が前提になっている組織で、ルールのインプリメンテーションが恐らく違うということは多分大きなポイントになるかと思っています。

もちろん国際的な組織がつくれればいいのですけれども、これまで、いろいろな国際組織の管理、特にITU、既に静止軌道の管理についてはITU方式というのもあるので、そういったことを想定しながら考えていくことも一つの方向性ではあるというところまでは認識をしておりますけれども､最終的に日本が中心となって国際的なルールづくりをする際に、そうしたきっちりとした国際組織まで想定できない状態であるというところから、先ほどの藤重参事官の回答のような、個々のルールづくりから進めていくという方針になっているのだろうという理解をしています。以上、補足です。

（５）議題（５）「その他」において、内閣衛星情報センターより民間衛星の利用を含めた今後の方針･取組等について､防衛省より資料５－１～２に基づき､次期防衛衛星通信、コンステレーションを活用した通信に関する検討等についてそれぞれ説明を行った後、次のような議論が行われた。（○：委員からの質問・意見等　●：事務局、関係省庁からの回答等）

○片岡部会長代理　防衛省に、幾つかコメントと意見というか、衛星通信について、こういう方向だと思うのですが、アメリカの空軍は、Advances Battle Management Systemをつくっていますので、これとの連接をどうするかというのは将来のキーポイントになりますので、これも含めて
ぜひ検討していただきたいと。

衛星コンステレーションは、経済安全保障で光衛星通信をやっていますが、それとのタイアップをされるのかどうかといったところを教えていただきたい。

CSpOは、参加する方向で、ぜひ早急に参加してほしいのですけれども、何か障害はあるのかどうかといったところを教えていただきたいのですけれども。

●防衛省　米国のJADC2について、どういう利用形態があるのかという点について、防衛省としてこれから検討していきたいと考えております。

通信衛星コンステレーションを導入する場合の光通信の組み合わせ方について、防衛省で基本的にはサービスを買ってくるという形を考えております。既に低軌道であればスターリンク､中軌道でもO3bといった民間の通信コンステのサービスが展開されておりますので、独自にスペックを定めて日本の光通信技術を利用するという形での通信サービスの購入は、今の時点では考えてございません。

CSpOに加入するということにつきましては、いろいろな国が加入に向けて手を挙げていると承知しておりますので、現構成国の７か国の中で加入する順番をお決めいただくしか

ないものかと考えております。
　以上です。
○片岡部会長代理　何か具体的に障害があるとか、そういうことはないのですか。
●防衛省　恐らくないと思います。
○片岡部会長代理　衛星通信コンステレーションは、要は、スターリンクとか、経済安全保障で進んだ国内の衛星コンステレーションができれば、それを利用するという前提ですということですね。衛星コンステレーションを活用した通信ということは、商業衛星通信のコンステレーションを使うということを前提にされているということですね。
●防衛省　防衛省として、衛星コンステレーション技術を使ってやるべきことは幾つかあろうかと思います。通信やミサイル防衛あるいは、その観測もあろうかと思います。そのうち、通信に限って申しますと、既に民間サービスが出てきている中で、重畳的に国独自のものを打ち上げる必要はないのではないかと現在は考えています。
○片岡部会長代理　防衛省が独自に上げるということは考えていないということですね。ありがとうございます。

○鈴木委員　１点質問ですけれども、次期防衛通信衛星に関するところで、きらめき後継機なのですが、現在は運用自体はスカパーJSATさんがやられていて、いわゆるPFIの方式でやられているのですが、こういういわゆる調達形態というか、運用方式を継続されるのかどうか、これはイエス・ノーのクエスチョンなのですけれども。
●防衛省　次期防衛通信衛星につきまして、PFI方式を継続するかどうかというのはまだ具体的な検討に至っておりません。まずは、どういう通信衛星を持つべきかということのコンセプトを固めた上で、その次の段階での検討になろうかと考えております。
以上