第２４回原子力委員会定例会議議事録

１．日　時　　令和８年６月１６日（火）１４：００～１５：４６

２．場　所　　中央合同庁舎第８号館６階６２３会議室

３．出席者　　原子力委員会

上坂委員長、直井委員、吉橋委員、青砥参与、畑澤参与、岡嶋参与、

小笠原参与

内閣府原子力政策担当室

井出参事官、中島参事官

ＮＴＴ株式会社

チーフ・サイバーセキュリティ・ストラテジスト　松原実穂子

４．議　題

（１）重要インフラへの攻撃事例とレジリエンスの教訓

（２）その他

５．審議事項

（上坂委員長）それでは、時間になりましたので、令和８年第２４回原子力委員会定例会議を開催いたします。

本日は、青砥参与、畑澤参与、岡嶋参与、小笠原参与に御出席いただいております。

なお、吉橋委員と畑澤参与はオンライン出席であります。

本日の議題ですが、一つ目が重要インフラへの攻撃事例としてレジリエンスの教訓、二つ目がその他であります。

それでは、事務局から御説明をお願いいたします。

（井出参事官）それでは、一つ目の議題でございます。重要インフラへの攻撃事例とレジリエンスの教訓ということで、ＮＴＴ株式会社チーフ・サイバーセキュリティ・ストラテジストの松原様に御説明を頂きます。

本件は、原子力利用に関する基本的考え方の３の４、国際協力の下で原子力の平和利用及

び核不拡散・核セキュリティの確保等を進めるに主に関連するものです。

それでは、松原様から御説明をお願いいたします。

（松原氏）皆様、こんにちは。ただいま御紹介にあずかりましたＮＴＴの松原実穂子でございます。それでは本日、「重要インフラへの攻撃事例とレジリエンスの教訓」と題しましてお話をさせていただきます。

私は、原子力の専門家ではないため、原子力そのものの安全性についての知見の共有はできません。原子力の供給には、通信、電力、金融、エネルギーを運ぶための運輸など様々な重要インフラの稼働が前提となります。ただし、自然災害やシステム障害、サイバー攻撃、あるいは戦争・紛争など有事の際のミサイルやドローン攻撃で施設そのものの破壊やそこで働いている人々の身に危険が及ぶことによって、重要インフラサービスに影響の及ぶときもあります。

そのため、原子力を含む私たちの日々の活動の下支えをしている重要インフラサービスに対して、今どのような攻撃が世界で行われているのか、その現状を踏まえた上で、私たち日本人と日本の組織がどういったレジリエンスの教訓を導き出せるのかについて、私なりの考えを共有させていただければと思います。

まずサイバーセキュリティについてお話しいたします。地政学的な緊張関係とサイバー攻撃はある程度相関関係があります。もちろん、地政学的緊張関係には関係なく、不正送金など、金銭目的に基づくサイバー犯罪はいつでも起こり得ます。ただサイバー犯罪に加えて、国家が相手の国の国力を落とすために、戦略的な目的を持って他国の経済、社会、安全保障が依存している重要インフラに業務妨害型のサイバー攻撃を仕掛けることもあるのです。

それから、自国の企業の市場競争力を高めるため、相手国の企業から最先端の技術情報などの知的財産情報を盗み取るためのサイバースパイ活動を国家が行うこともあります。

例えば、北朝鮮から日本の方向に向かってミサイルが発射されたとのニュースを私たちは時折目にしています。北朝鮮は今まで長い間、制裁下にあり、外貨を稼ぐことが非常に難しい。米国家情報長官室が毎年２月に出している報告書によると、北朝鮮は何とサイバー攻撃だけで毎年１０億ドル、日本円にして１，６００億円相当の外貨をサイバー攻撃だけで稼ぎ出しています。その外貨がミサイルや核の開発に使われ、私たちの地域の安定性にも影響を及ぼしているのです。

また、ウクライナとロシアの間では４年以上にわたって戦争が続いていますが、戦争開始前からサイバー攻撃は始まりました。

今年の２月末にアメリカとイスラエルへのイランへの攻撃が始まった以降、世界的にサイバー攻撃の数が相当増えたとの観測結果も出ています。

加えて、台湾有事の前哨戦と思われるサイバー攻撃が、少なくとも数年前から重要インフラに対して行われていることが確認されています。

こういった地政学的な緊張と関連したサイバー攻撃の場合、サイバースパイ活動は政府や軍需産業に対して行われることが多いのですが、業務妨害型のサイバー攻撃は重要インフラ企業に対して行われることが非常に多いです。

ただ、最初に申し上げましたように、サイバー攻撃自体は平時からも行われ、企業はサイバー攻撃の最前線に立たされています。しかし、一旦戦争、紛争など有事の段階に入ってしまうと、企業は、サイバー攻撃だけではなく、ウクライナで見られるように、ミサイルやドローンによる攻撃の対象にもなり得ます。

ただ、重要インフラ企業は社会経済活動と国家安全保障に大きな責任を持っている以上、２４時間稼働し、間断なくサービスを提供し続け、そのための規制が課せられています。だからこそシステム故障、自然災害、サイバー攻撃などのリスクに対し重要インフラ企業はかなりの対策を様々取っており、事業継続計画もほかの企業よりも相当細かく作っています。

ところが、戦時であろうが、紛争中であろうが、国民はあなたたちのサービスを必要としているからという理由で、絶対にサービスを止めてはいけないという平時の規制は、有事においても妥当かとの問題があります。一企業でミサイル防衛やドローン防衛はできるのでしょうか。今まで私たちが考えてこなかったような課題を突き付けたのが、４年以上前に始まったウクライナでの戦争です。

２０２２年2月２４日にウクライナへの全面軍事侵攻が始まり、その年の秋にウクライナの電力とエネルギーインフラに対するミサイルやドローン攻撃が激化しました。その結果、停電が多発するようになったのです。電力・エネルギーインフラはその後も攻撃を受け続けており、去年の夏以降は鉄道への攻撃も激化している状況にあります。

インフラに対する破壊行為が続いている結果、去年の１２月の時点で修理に必要な金額は、ウクライナのＧＤＰの３倍以上に相当する金額にまで膨れ上がっていると想定されています。しかし、ウクライナが今でも主権国家としての地位を維持し、そして残された国民が生活と経済活動を続け、国民の一部である兵士たちが戦い続けていくためにも、重要インフラサービスは必要不可欠です。それは危険地域でも誰かが残って職務を全うし、サービスを提供し続けること、そして危険地域にも赴き、壊されたインフラを直し続けることを意味します。

その結果、ウクライナでは、ごく普通の会社員が勤務中に負傷あるいは殉職する数が増えています。２０２５年の勤務中の負傷者は１，０００人以上、殉職者は２００人以上です。

どれだけウクライナの電力・エネルギーインフラへの攻撃が苛烈なものであったのかについては、２０２４年６月の段階で、火力発電能力の９０％、そして水力発電能力の４５％が喪失したという数字だけでも、十分伝わるのではないかと思います。

電力インフラで狙われてきたのは発電施設と変電所でした。原発の場合、原発施設の外に置かれているスイッチボード、開閉所に着弾、あるいは近くに破片が飛んできた際のリスクを懸念し、２０２４年に情報機関が原発の開閉所を守るための対策について呼びかけました。そこで初めて、原発で三つのレイヤーの防御策を取ることになったのです。

軍事侵攻前、ウクライナでは、電力・エネルギーがここまで徹底的に狙われ続けるなど誰も予想していませんでした。企業が単独でミサイル防衛やドローン防衛することは不可能です。しかし、ウクライナでは万が一戦争になり、企業が自分たちの身を自分たちだけで守り切ることは不可能な以上、どうするのかを考えていなかった。最後の最後まで守らなければいけない最重要インフラの選定も戦前にしていませんでした。選定が行われたのは、軍事侵攻が始まった後です。

しかも、最重要インフラを選定し、ミサイル防衛しても、そのためのミサイルは数が不足しています。積極的な防衛ができない以上、消極的な防御をするしかない。土嚢を積み重ねる、コンクリートの壁を造る、そしてより重要な施設は鉄筋コンクリートで更に守りを固めるという、三つのレイヤーの防御策を取ることになりました。

ただ、この防御策にも非常に問題があります。停電が多発している戦争中に重く、大きなものを製造し、運搬することが非常に難しい。

去年のエネルギー施設へのミサイル・ドローン攻撃だけでも６１２回ありました。１日に平均して2回ぐらいです。国連開発計画がウクライナの重要インフラ業種別被害を毎年算出しているのですが、２０２５年１２月の時点で、電力・エネルギーインフラの被害だけでＧＤＰの１３％以上に達しています。

これだけ破壊が続くと、直したくてもなかなか直せない。しかもウクライナの電力施設は旧ソ連時代に造られているため、パーツを輸出できる国が限られる。旧ソ連時代の発電施設がもう使われていないものの、良い状態で保存されており、それを解体してウクライナに送ることができるかどうか。でも、それも数が限られる。また、システムの中でも大きいものは。何階建ての建物に相当するサイズですので、簡単に運べない。

攻撃が続く中、地下化の試みも始まりましたが、やはり戦争中に工事は非常に難しい。国営の送電企業「ウクルエネルゴ」は１００か所近く変電所を持っていますが、今までに地下化できたのはそのうちの僅か１か所です。相当金額も掛かり、なかなか進みません。それでも何とか電力・エネルギーインフラ施設の人たちは稼働を続け、壊されたら何とかして直し続けようとしています。

ウクルエネルゴは７，０００人の社員を抱えている企業ですが、戦争開始後、早い段階で全国に１，０００人を修理のために展開していました。これはウクルエネルゴに限った話ではないですが、現在、全土で電力・エネルギーインフラの修理に従事しているウクライナの作業員数は１万５，０００人以上と言われています。

彼らは相当な危険にさらされており、ダブルタップ攻撃の対象にもなっていると言われます。一旦インフラが攻撃された後に、瓦礫の下に誰かが埋まっていないか助けるために消防や医療関係者、修理のための技術者たちが集まってきます。それを見計らってもう一度攻撃することをダブルタップ攻撃といいます。

火力発電所の場合、空襲警報が鳴っていても全員は待避できず、少なくとも２人はコントロールルームに残って火力の調整をしなければいけないのだそうです。想像してみてください。空襲警報が鳴り響き、ミサイルやドローンの飛来音が聞こえてくる中、他の同僚たちが地下の防空壕に潜っている間も最後まで残って作業を続けている人たちの気持ちを。ごく普通の会社員たちがインフラで今でも職務を全うし続けているのです。

ウクライナ最大の電力会社「ＤＴＥＫ」は。戦争が始まって３年の段階で修理を１万６，００１回実施したそうです。場合によっては、同じ箇所を１０回直しているそうです。１回、２回の破壊であれば、そこに住民の方が残っている限り絶対サービスを続けるのだという気持ちが維持できるかもしれません。しかし３回、４回、５回となれば、だんだん気持ちは萎えてくるでしょう。今日直しても明日また破壊されるかもしれないと考え始めたとき、現場の士気を維持するのは非常に難しい。

そして、ＤＴＥＫ１社だけでも、戦争が始まって３年の段階で社員の３００人以上が殺害されています。ＤＴＥＫのＣＥＯは海外メディアのインタビューに答えた際、戦争開始以降、朝一の仕事が前日に殺傷された社員たちの確認作業になったと語っています。

危険地域での修理作業は危険を伴うため、各企業はウクライナ軍か非常事態庁の許可を取ってからでないと、作業が行えません。今でも攻撃が続いているにもかかわらず修理作業が続いているということは、リスクを取って軍も政府も修理許可を出し、立入り許可を出され

た企業側もリスクを取って作業をしていることなのだと思います。

電力に加えて通信もなければ、経済活動と社会活動の維持が難しくなります。特に有事の際、自分たちの国で何が起きているのかを世界的に発信して理解してもらわなければ、国際支援を得ることも困難になります。

通信インフラは電力インフラほどではないものの、破壊をされています。国連開発計画の最新の統計値によると、去年の１２月時点で被害想定額はＧＤＰの１％相当です。しかも停電多発により、通信の維持が難しくなってきました。国内外に待避する国民の数が多いため、固定回線よりもモバイル回線の重要度が高まっています。その結果、ウクライナ政府は、ウクライナの通信事業者に対して、停電が長引いた際もモバイルサービスを維持するよう規制強化しました。

長時間停電してもサービスを提供するには、各基地局に大量の発電機と燃料を置かなければいけない。しかし、ミサイルやドローンの攻撃の対象になり得るのに、大量の燃料を備蓄すると大規模火災になり得る。しかも、発電機の購入や性能の良いバッテリーへの切り替えを進めれば、今までお付き合いしたことのないベンダーやサプライヤーとの取引をしなければならない。加えて戦時下で人手不足になっており、特に地方でメンテナンスの技術要員の確保が非常に困難になっている。

規制強化の必要はあるものの、規制を受ける企業側の負担が更に増しています。また、壊されたインフラの修理、復旧作業、あるいは停電対策は、企業負担で行われているため、企業の財政的状況は非常に苦しい。

電力、通信も大事ですが、経済・社会活動を続けていくためには、当然のことながら金融の下支えがなければ絶対長続きしません。ただ、停電が多発すれば、どうしても通信が不安定になり得、クレジットカード決済ができないかもしれない。それ故ウクライナでは、現金持参が推奨されています。現金を入手し続けるには、誰かが運ばなければいけない。

現金や燃料を入手し続けるため、運輸も重要です。これらの重要インフラサービスは相互依存関係にあり、どれが欠けても社会経済活動と安全保障の維持が難しい。

ウクライナには郵政公社と宅配サービス企業が１社、鉄道が１社あり、全てが攻撃の対象となってきました。

実は今年の４月の時点で、ウクライナ鉄道の従業員のうち１，０００人以上が殺害されています。勤務中あるいは前線で家族や国を守るために戦って命を落とした大切な仲間たちを悼み、去年１１月４日のウクライナ鉄道の従業員の日に、その方々の顔写真を集めた動画を

ウクライナ鉄道がＸの公式アカウントを通じて紹介しています。

その動画の顔写真をよくよく見ていただくと、ごく普通のシビリアンの格好の方も軍服の方もいらっしゃる。年齢層も様々で、男性も女性もいらっしゃることが見てとれます。ごく普通の人たちが、お客さんや物資をほかの地点に運ぶために仕事をしていただけにもかかわらず、命を奪われてしまったのです。

去年の夏から鉄道に対する攻撃が激化しており、その中でも特に狙われているのが鉄道に附属している変電所と路線の切替え地点です。鉄道の機能の停止期間をなるべく長引かせるために、そうした箇所が狙われているのではないかと言われています。鉄道の被害想定額は電力・エネルギーインフラや通信よりもかなり多く、ＧＤＰの２１％に相当しています。攻撃回数は今年３月までに５，０００回に達し、そのうちの１０％以上が今年発生しました。

先ほど鉄道で狙われがちなのが変電所と路線の切替え地点と申し上げましたが、まれに客車そのものが攻撃を受けることもあります。客車が攻撃された後、床が血の海になっているような写真も、地元のメディアやソーシャルメディアでは紹介されています。それでも尚、鉄道会社もほかの重要インフラサービスの従業員たちも仕事を続けているのです。

ウクライナではサイバー攻撃も行われてきましたが、戦争が長引けば長引くほど、重要インフラに対する業務妨害型サイバー攻撃の比重が下がり、むしろ殺傷能力・破壊能力の高いミサイルやドローン攻撃等の火力を使った攻撃が増えています。

ただ、有事の前には情報収集のためのサイバー攻撃が増加する傾向にあります。ウクライナでも、２０２２年２月に軍事侵攻が始まる前、サイバー攻撃が相当増えたとウクライナ側は主張しています。ウクライナの重要インフラへの業務妨害型サイバー攻撃も、戦争が始まる前から増えていきました。

他方、サイバー攻撃の増加に警戒感を抱いたウクライナ側が、これから更に烈度の高いサイバー攻撃が行われる可能性を予期し、サイバー防衛能力を高める準備期間が軍事侵攻前に与えられたのも事実だと思います。

日本が懸念すべきなのは、アジアで今後起こり得る事態であり、そのうちの一つ、憂慮すべきシナリオが台湾有事です。台湾有事の前哨戦と思われるサイバー攻撃が、数年前から観測されています。米国政府が２０２４年１月に発表したところによりますと、ボルト・タイフーンと呼ばれる中国政府系のハッカー集団が米国内の通信、エネルギー、交通、水道のインフラのネットワークの中に侵入していました。

ボルト・タイフーンの目的は、重要インフラのネットワークの中に潜み、有事の際に重要

インフラサービスを止めて、社会混乱を引き起こし、政治的な決断を遅らせ、そして軍の展開を抑止することなのではないかと言われています。

ボルト・タイフーンの侵入につきましては、米国内だけではなく、シンガポールとインドでも観測されたという報道が出ました。今のところ、台湾と日本国内の重要インフラのネットワークの中に侵入していたとの報道は出ていません。

ただし、去年の３月にポール・ナカソネ元米サイバーコマンド司令官が、琉球朝日放送のインタビューに答えられた際、ボルト・タイフーンが既に沖縄に入り込んでいるのではないかとの発言をされていました。繰り返しになりますが、現時点で日本の国内のネットワークにボルト・タイフーンが侵入したという報道は一切ありません。ただ、ナカソネ元司令官がそのような警告を出されたということは、私たちもそうしたサイバー攻撃が行われるかもしれないとの警戒感を高めておいた方がいいのではないかと思います。

現在の中東情勢を見ても、多くのサイバー攻撃の対象となっているのが重要インフラサービス企業です。今年の２月末以降、イラン、米国、イスラエル間で攻撃の応酬が続いていますが、イランからのサイバー攻撃の対象は、医療機関、医療機器メーカー、地下鉄、石油、ガス、水道、あるいはガソリンスタンドの貯蔵タンクの関連のシステムなど、重要インフラとなっています。やはり有事の際に重要インフラサービスがサイバー攻撃で狙われるのは、別にウクライナに限った話ではないということが中東情勢からも読み取れると思います。

今回の中東情勢で注目すべきなのは、重要インフラへのサイバー攻撃に加えて、民間のデジタルインフラへの物理的な攻撃です。今、ミュトスをはじめとして、日本国内でも非常にＡＩへの関心が高まっています。私たちの生活、経済活動、仕事においてＡＩの活用度合いはこれから加速度的に増えていくでしょう。ＡＩを使うには。大量のデータに常にアクセスできる環境が必要となります。つまり、データセンター、通信、電力がきちんと提供され続ける環境の維持が前提となるわけです。しかし今回の中東情勢では、紛争の当事国ではないＵＡＥとバーレーンにある民間のデジタルインフラがドローンによる攻撃を受けました。これは今までになかった傾向です。

例えば、３月１日にＵＡＥとバーレーンにあるＡＷＳのデータセンターにドローン攻撃が行われました。その結果、金融決済、タクシーやフードデリバリーなどのアプリサービスが現地で使えなくなったと報じられています。

その後、４月にも、バーレーンにあるアマゾンのクラウド施設に対する攻撃が行われました。ドバイにあるオラクルのデータセンターも攻撃を受けたとの報道も当初はありましたが、

ドバイ側がすぐに否定しています。

インフラに対するサイバー攻撃だけではなく、火力を使った攻撃がしかも当事国以外にも行われたのが中東情勢の新しいポイントです。

ウクライナでも、データセンターはミサイルやドローン攻撃の対象になってきました。それらの民間施設を民間だけでミサイルやドローンから防衛することはできません。

ウクライナ以外のほかの地域でも世界で緊張関係が高まっている中で、私たちの社会経済活動と安全保障がより依存するようになってきたインフラとデジタルインフラを守るために、私たちは何ができるのか問わなくてはならない。そして次に緊張関係が高まっていくのはどこなのかについて、私たち日本人も考える必要があります。

また、中東は日本企業も経済活動で依存している地域であり、デジタルインフラの安定性は、日本企業にとっても重要なポイントです。

最後にまとめです。ウクライナの場合、２０１４年のクリミア併合と２０２２年2月の軍事侵攻があるまでの８年間に、ロシアから複数回にわたり電力などの重要インフラサービスに業務妨害型のサイバー攻撃を受けてきました。非常に大きな被害を受けつつも、そこから教訓を導き出し、サイバー防衛能力の強化に成功しました。そして、２０２１年の秋にロシアからのサイバー攻撃が増加した後も、それを糧として気持ちを奮い立たせ、サイバー防御能力の向上に成功しました。

今回の軍事侵攻以降、ウクライナのサイバー防衛能力の高さについて様々な国から非常な大きな驚きをもって受け止め、尊敬の言葉もよく聞かれるところです。

ただ一旦有事になれば、サイバー攻撃だけでは終わらないかもしれない。重要インフラサービスの重要性が有事において高まる中、その機能を最後まで維持しなければならないのに、企業だけでは火力を使った攻撃から自分たちの身を守ることができない。ではその機能をどうやって続けていくのか、国全体としての事業継続計画をどうするのか、軍や政府はどのようにして火力による攻撃からの防御機能を提供するのか。しかし、国としての包括的な事業継続計画をウクライナは平時のうちに作っておかなかった。

今年日本は、１２月までに安保三文書の改定をすることになっています。国家防衛戦略では重要インフラに関する記述が限られており、「重要インフラに対する攻撃に際しては実効的な対処を行い」とありますが、実効的な対処が何かについては具体的な法律は作られてきませんでした。

唯一の例外が去年５月に成立した能動的サイバー防御関連法です。重要インフラに対する

国家安全保障を脅かすような重大なサイバー攻撃に対して、日本が国家として対応するための非常に重要な法律です。この法律の成立は日本の安全保障上、非常に意義があります。しかし、有事になったときにサイバー攻撃だけで終わらないかもしれない中、サイバー攻撃以外での「実効的な対処」で何をするのかについては、これから安保三文書の中で議論する必要があると思います。前回の安保三文書のときと異なり、日本を含めて、世界中がこれだけＡＩを含めたデジタルインフラへの依存度を増していく中、デジタルインフラを含めた重要インフラをどう守るのか問わなければならないでしょう。

デジタルインフラを回していくためには、電力が必要不可欠です。その電力の中には原子力も含まれ、原子力委員会の皆様の御知見が非常に重要になってくると思います。

サイバー攻撃だけでなく、ドローンを使ったデジタルインフラへの攻撃も行われるようになっているため、今後ほかの地域でどのような攻撃の組合せ方があるのかについて、日本が学び、備えを固めていく上で教訓を得るべきです。

今までどのような攻撃がインフラに行われてきたのか、それぞれの攻撃に対して国や企業がどういった備えを事前にしており、どれがうまくいき、どれが失敗したのかにつきましては、拙著と「Ｖｏｉｃｅ」最新号に記しています。参考にしていただければ幸いです。

有事になったときに戦いますかという質問に対し、他国と比べて日本人は「はい」と答える割合が非常に少ないとの世論調査があります。「戦う」の意味の捉え方が、おそらく日本と他国で違うのではないかと考えています。

軍事侵攻下で殉職されたウクライナ鉄道の従業員の方々の写真を見ていただければ、あの方々にとって「たたかい」は必ずしも武器を手に取った戦いだけではなく、生活と経済を回し続け、残っていらっしゃる方々を支え続けるために職務を全うする「闘い」も含まれることがお分かりいただけると思います。闘いは、当事者意識をどの場面に求めるのかです。

どのようにして職務を全うし続け、そこにいらっしゃる方々に対して必要なものを提供し続けていくために、自分がどういう役割を果たしていけるのか。「たたかい」を再定義し、行動に移し込んでいくことは、いわゆる軍事や安全保障だけではなく、日本の経済安全保障のレジリエンスにも私は貢献すると思います。それが日本人の強みである「和」を更に高め、日本の安全・安心に寄与していくでしょう。

御清聴ありがとうございました。

（上坂委員長）重要インフラ、世界のインフラへのサイバー、そして付随するハード的な攻撃の最新の状況と、またそれに対するレジリエンスに対する御提言を頂きました。

それでは、委員会の方から質問させていただきます。４０分をめどに行いたいと思います。それでは、直井委員からお願いいたします。

（直井委員）どうも松原様、なかなか聞くことのできないお話をお聞かせいただきましてどうもありがとうございます。

まず、武力攻撃が、いわゆる武器を使った破壊活動だけじゃなくて、前哨戦としてのサイバー攻撃で重要インフラがやられるとか、そういうような形で、またドローンを使った攻撃も含めて戦争の形が変わってきているというようなこと。その中でやっぱり重要インフラである原子力発電所なんかのサイバー攻撃からしっかり守っていかなきゃいけないというようなことを痛感した次第でございます。

それで、先月なのですけれども、ＩＡＥＡでサイバーセキュリティに関わる国際会議が開催されまして、参加をしてきました。それで、この公開の場での国際会議でサイバー攻撃に備えた対策に関する研究成果の発表ですとか、そういうのを聞いていて感じましたのは、比較的オープンな場でこういうサイバーセキュリティ対策が議論されるというようなことで、いわゆるセキュリティといいますと、基本的に情報を外に出さないというのが原則になっている中、ちょっとサイバーセキュリティの国際会議で受けた印象としては、何かしっかり情報共有しているぞというような感じをしまして、それで恐らくそういう情報共有をすることがサイバー攻撃に対処する、防衛をする意味でも信頼性を高めるとか、意味があるんじゃないかというふうに私は感じたのですけれども、サイバーセキュリティの専門家として松原様がどういうお見立てであるか、サイバーセキュリティに関してそういう私が感じた印象についてどういうふうにお感じになるかというところをお話しいただけますでしょうか。

（松原氏）サイバーセキュリティ対策については、国際協力を議論する会議では必ず取り上げられるトピックになってきたと思います。私たちの活動や業務を遂行する上で絶対にデジタル技術は欠くことができません。デジタル技術を安全・安心に使うために、サイバーセキュリティは両輪として必ず確保しなければいけない。自分たちの業界がどこにあるとしても、サイバー攻撃がこれだけ増えてきますと、自分たちがどういう対策を取っていくのか様々な悩ましい問題が発生する。限られたリソースをどこに配分しなければいけないのか、人材をどうやって確保するのか、悩みは大体皆さん共通していらっしゃいますので、オープンに議論することになったのは非常に良いことだと思います。

ただ、ここがうまくいかないという部分をオープンにしてしまうと、その情報がサイバー攻撃に悪用されてしまうこともあり得ます。非常に具体的な技術的機微情報については必ず

しもオープンな場では出さずに、別のクローズドの場で議論していると思います。

（直井委員）ありがとうございます。

日本の場合はどちらかというと、本当に情報を外に出さないというところを中心に考え過ぎちゃって、何か閉塞感みたいなのがある、セキュリティ担当者に。そんな印象を私は受けていまして、サイバーセキュリティの国際会議で非常に活発な議論がなされていて、そういう情報を共有しながら一緒に対策を考えていくというところは、非常に前向きでいいんじゃないかなというふうに私は感じました。

それから、中東情勢とか、それから台湾有事の前哨戦のお話ございました。それで、既にサイバー戦が展開されているというお話だったのですけれども、これらは余り報道をされていないのではないかなと、国民は余り知らないのではないかなと思うのですけれども、いかがでしょうか。

（松原氏）それはどちらのケースでしょうか。

（直井委員）どういうふうにお感じになられていますでしょうか。もう国民には十分に伝わっているというふうにお考えでしょうか。

（松原氏）２年前に米国政府がボルト・タイフーンによる米重要インフラサービスへの侵入と米国政府によるサイバー攻撃の食い止めについて発表した際、日本語のメディアでもかなり報じられていました。しかしその後は日本でボルト・タイフーンについて余り報じられていないため、一般の方の間での認知度はそこまで高くはないかもしれません。

中東のデジタルインフラに対するドローン攻撃につきましては、朝日新聞の五十嵐編集委員が詳しい記事を書いていらっしゃいました。ただ、それ以外にサイバー攻撃やデジタルインフラへの攻撃という切り口でまとまった情報が日本語で見られるところは、あまりないので、そうした観点で中東情勢を見ていらっしゃる方は限られているかもしれません。

（直井委員）ありがとうございました。私からは以上です。

（上坂委員長）それでは、吉橋委員、聞こえますか。

（吉橋委員）はい、吉橋です。私の声、聞こえますでしょうか。

（上坂委員長）大丈夫です。

（吉橋委員）松原様、本日は大変貴重なお話ありがとうございます。ちょっと今日は現地に行けずに大変失礼いたします。

先ほど最後の戦い方の意味ということでは、少しはっとさせられた気がします。どうしてもこういった色んな情勢ありますと、武器を持つのか、逃げるのか、守るのかというような

ことが最初に頭に来てしまいますけれども、この当事者意識ということを最初の方の御説明にもあったような、自分たちの責任ですか、やらなければいけないことを守るということも戦いの意味の一つであるということは、非常にはっとさせられました。

また、先ほど直井委員が御質問された内容にしましても、多少なりともニュースですとか、今回のこういった攻撃のお話に関する情報は入ってくるわけですけれども、物理的攻撃の前に数多くのサイバー攻撃があって、現在も今、台湾等でそういったサイバー攻撃、サイバースパイ活動が行われているということについて知らないことも多く勉強させていただきました。本当にありがとうございます。

それで、色んな攻撃がある中で、この修理費がどういったところから捻出されていたんだろうということが気になったのですがウクライナの場合や、ほかの情勢ももし分かるようでしたらお聞きしたいと思います。国ではなく、やはり企業そのものが修理をして、修理の費用を捻出していくという認識でよろしいでしょうか。

（松原氏）コメントと御質問どうもありがとうございました。

ウクライナでは基本的に各重要インフラ企業が、修理や停電対策の費用を捻出しています。ただし戦争・紛争時に顧客の数は増えず、ただでさえ財政状況が厳しい中、出費だけが増えていくので、当然のことながら、その企業だけで全部を捻出するのが難しくなります。

例えば最初に説明したウクライナ最大の民間電力会社「ＤＴＥＫ」の社長やその他の大手の重要インフラ企業の社長は、自社がどのようにインフラサービスを維持しているのか大きな国際会議で教訓を共有し、国際支援を要請することで資金を募っています。

（吉橋委員）ありがとうございます。

ということは、今の御説明を聞く前は、もしかしたら優先順位みたいなものが国の中であるのかなということを思ったりもしたのですけれども、今日のお話ですと、もちろん電力がなければ通信もできない。逆を言うと、通信が止まってしまったら、どこにどういう電力を使ったらいいかと。全部総合的に関係してくるので、優先順位なんていうものも付けられないのだろうなと思いましたので、どのような手順で修繕をやっていらっしゃるんだろうということを思いました。

そういった意味でも、最後のスライドで平時の備えで軍と規制当局、それから企業の連携ということがあったかと思いますが、こういった問題に対して日本というのは、先ほど直井委員もおっしゃったように、少し閉鎖的という、各省庁だったり各企業は閉鎖的で、もう少し水平展開といいますか、皆がある程度情報を共有したりすることも重要かなとは思うので

すけれども、松原さんはその辺りどういうふうに思われるでしょうか。

（松原氏）それはおっしゃるとおり、各業種の専門家の方々が知見を寄せ集めることによって、国としての包括的な事業継続計画を作ることが重要だと思います。これだけ各業種で専門化が進んでいきますと、全てについて理解している人はいないからです。

原子力の安全担保についてはその専門家、重要インフラの具体的なミサイル防衛の仕方については、自衛隊や軍事の専門家に相談しなければならない。

ウクライナや中東で現実に起きていることをまず知っていただいた上で、日本で今後起こり得る有事のシナリオはどういうものなのかを考えなければいけない。日本は予算が無尽蔵にあるわけではないため、いつ起きるか分からず、どういった形でどこまで地域的に影響が及ぶか分からない有事の可能性に対して、リソースを費やすのは難しいかもしれない。しかし少なくとも、ヨーロッパや中東でこうしたことが起きている以上、日本として今後の事業継続計画を国として作っていくためにはどうすればいいのかは練らなければいけない。特に今年、安保三文書改定を１２月までに行うことが決まっており、原子力を含め、皆様の御知見が非常に重要になってくると思います。

（吉橋委員）ありがとうございます。

私としましては、原子力の安全をどうやって守るのかということを優先に考えるわけですけれども、ただその中で色んな方のやはり意見を聞きながら、今おっしゃられたように、世界でこういうことが起きているということをちゃんと認識していかないといけないということは、今日本当によく認識させていただきました。大変勉強になりました。

私からは以上になります。ありがとうございます。

（上坂委員長）それでは、参与からも御質問と御意見を伺います。青砥参与からお願いいたします。

（青砥参与）なかなか本当に聞けないというか、余り耳にも目にもできないような内容で、非常に興味深く、言い方がいいかどうか分からないですが、聞かせていただいてよかったと思います。

私からの質問は１点で、この重要インフラのレジリエンスを高める、あるいはこの日本ではどうしていくかという話をされました。それを高めるのに、国際的な連携というか、ネットワークというようなものがあったら、それはどのような有効性を持つのかについて、今回、たくさん触れられたウクライナの例などで、もし御存じであれば、若しくはお考えがあれば、少し加えていただけないでしょうか。

というのは、今日のお話の中では、そうした国際的なネットワークや連携が、こうした大きな問題に色々と対応するに当たって、どのように効果を持っているのかといった内容が少し抜けていたような気がしたので、お願いします。それが重要インフラのレジリエンスにおいても、国内で様々な連携やＢＣＰですか、事業継続計画を作るにしても、その周辺を守るために、一国ではできない内容についてはどうしていくのかについてのヒントになるように思います。

（松原氏）平時のウクライナでは、万が一、全面軍事侵攻になった場合に重要インフラをどう物理的な攻撃から守るのかについて計画を全く立てていませんでした。戦争が始まってから初めて、土のうを集め、鉄筋コンクリート製の構造物の建設が必要となりました。しかし物資や資金が足りず、米国際開発局（ＵＳＡＩＤ）が相当資金と物資の援助を行ったのです。

ただＵＳＡＩＤは去年解体されてしまいました。日本の国際協力機構（ＪＩＣＡ）はその前からウクライナのエネルギー業界に蛇籠を提供していたのですが、ウクライナの重要インフラへの支援を一層増やそうとしています。でも、ＵＳＡＩＤの完全な代替にまではなっていません。

一旦戦争・紛争になると、製造能力と経済機能がかなり落ちるため、その代替となる機能を国際支援でどうやって得続け、なおかつ物資の運搬手段を確保していくかが大切です。

ウクライナ上空を飛行機は飛んでいないので、ウクライナは鉄道を使っています。一方島国の場合、鉄道による海外からの物資運搬ができないため、ウクライナから教訓を学べず、独自に考えなければいけません。

ウクライナに対する全面軍事侵攻が２０２２年２月に始まって以降、欧米のサイバーセキュリティ業界の有志が立ち上がり、ウクライナの重要インフラ企業とサイバーセキュリティ庁にサイバー攻撃に関するインテリジェンスを提供してきました。このようにして、様々なレイヤーでウクライナのレジリエンスに対する国際協力が続けられています。

（青砥参与）ありがとうございます。

その辺りも含めて色々な議論の際にネットワークというか、国際的な連携がどんな有効性を持つのか。特に今お話にあったように、何度か繰り返し強調されているように、平時におけるネットワークの在り方とか、今言われた重層性だとか、その辺りの議論がうまくいくように是非指導していただければと思います。ありがとうございました。

（上坂委員長）畑澤参与、聞こえますでしょうか。

（畑澤参与）はい、聞こえております。

今日は大変貴重なお話を聞かせていただきまして、ありがとうございました。重要インフラへの戦時・有事のときの攻撃とその対策ということで、実際どういうことが起こっているか、本当に生々しく聞かせていただきました。

私は医療の分野に身を置いておりまして、医療機関へのサイバー攻撃というのが大変増えてきております。これは平時に起こるわけですけれども、病院の機能が停止してしまうと、患者さんへの直接の影響がありまして、大変患者さんには御迷惑を掛けてしまうわけです。人の命に直結するようなことがすぐ起こってしまいます。

この有事の際の事例というのは今日聞かせていただきましたけれども、医療機関へのサイバー攻撃の事例というのは集積されているものなのでしょうか。もしそういうことが集積されていて、共有できれば、大変医療機関が個別に対応する、若しくは何か標準的な対応策を考える上で非常に役に立つと思うんですけれども、いかがでしょうか。

（松原氏）御質問ありがとうございます。

５年前に徳島の半田病院がランサムウェア攻撃を受け、しばらく外来患者の受付ができなくなってしまいました。この事件を受け、日本の厚生労働省は医療機関のサイバーセキュリティ対策に危機感を持ちました。その１年後に今度は大阪の病院でもランサムウェア攻撃があり、しばらく医療活動に支障が出ています。厚生労働省は、どのようなサイバーセキュリティ対策を取るべきかについて医療機関に対しガイドラインを出しました。

海外に目を転じても、６年前にランサムウェア攻撃を受けたドイツの病院が、高齢の女性患者の受け入れができなくなり、別の病院に搬送しなければいけなくなりました。この患者は、治療の遅れによって亡くなっています。

米国の病院が７年前にランサムウェア攻撃を受け、それを知らなかった女性の方が出産のためにその病院に行って、赤ちゃんを生みました。へその緒が赤ちゃんの首に絡まって生まれたのですが、医療システムが全てダウンしていたため、必要な医療行為を行えず、その赤ちゃんに重い障害が残ってしまい、後日亡くなってしまいました。

これは裁判になり、裁判で母親側が勝てば、ランサムウェア攻撃によって死亡した初めての事例になるとして注目を集めました。

医療機関や医療機器メーカーに対する業務妨害型のランサムウェア攻撃については、人命に関わってくるため、結構注目されていると思います。

（畑澤参与）ありがとうございます。

今やはり多くの病院では、日本で発生した事例に対処するために、厚生労働省の指導もあ

って、院内にそのようなセキュリティの専門家を置くような体制を取っています。

そのときに一番問題になるのは、やはり医療機関ですので、サイバーセキュリティの専門家を雇用して防御態勢を作るということはなかなか難しい状況で、実際には病院の中に勤務している方の中で、ＩＴに堪能な方を集めて対策を練るというふうなのが主流になっています。

ですから必要なのは、やはりサイバーセキュリティ、医療機関でも必須だと思いますので、そういう方の人材育成であるとか、人材が一番重要ではないかと思いますし、また、サイバーセキュリティの専門家、ＩＴの専門家だけではなくて、プラス医療をよく知っている方とのグループというか集団が対応に当たるのがいいのではないかなというふうに思っているのですけれども、その考え方についてはいかがでしょうか。

（松原氏）大きな病院ですと、サイバーセキュリティに特化した人材を雇う余裕がおありかもしれませんが、中小の病院や小型クリニックでは、サイバーセキュリティ専門人材を雇い、日々起こっているサイバー攻撃に対処していくのはリソース面で非常に難しいと思います。

医療機関だけに限った話ではありませんが、中小の企業や組織の場合は、サイバー攻撃を監視してもらい、万が一感染し、被害が出た際にいち早く駆け付けてもらって対処してもらうサービスの外注をしていくしかないと思います。外部の知見を借りるにしても、まずは経営者がリスクの存在を認識し、そのリスクが経営だけでなく、医療機関の場合は人命に関わりかねないことを知っていただき、投資していただくことが最初の一歩となります。

経営者に問題を認識していただけるよう、是非お力を貸していただければと思います。

（畑澤参与）よく分かりました。どうもありがとうございました。

畑澤の方は以上です。

（上坂委員長）それでは、岡嶋参与、お願いいたします。

（岡嶋参与）どうも御説明ありがとうございました。

平和ぼけしているというのか、こういう状況をお伺いしていて、本当に今すぐにでも対応しないといけないものも多々あるのだろうなと思いながら聞いていました。今の畑澤参与の質問にも関連なのですけれども、今日のお話で重要インフラのレジリエンスという最後のお話において、平時の備えというのがありました。平時の備えというのは、言わば関係者間で連携して、事業計画を継続して作っていくというお話だったと思います。今のお話では、それを企業の経営者側がまず理解することとおっしゃっていたのですが、要はそれをどこまで浸透させるのか、その危機感といいますか、そういうものをどの程度、どの範囲まで共有す

るべきなのか。

次に目指すべき国の形とおっしゃったところの戦いの再定義を考えると、言わば国民レベルで考える必要があるだろうと思います。その間をどういうふうに埋めていくべきなのか、あるいはどう考えていかないといけないのか、というのが一つの大きなポイントではないかと私は思いつつ聞いていました。もし何かその辺のところでお考えがあれば、教えていただきたいと思っています。

例えば、国民レベルで見ると、先月でしたか、内閣情報会議の設置とかという話のところでも、これに関連する話だろうと思うのですが、国会の中では議論されているのですが、それでは国民レベルでどれぐらいそれが浸透しているのかというと、私は何となくニュースでは聞くけれども…という程度であり、国民としてはちょっと離れたところにあるような気がします。また、つい二、三日前には、ＡＩに関して片山大臣だったと思いますが、ミュトス５が使えるようになったとおっしゃっていました。一方、昨日だったか、アメリカで公開できませんという話になって、さあこれからどうするんだという話もあると思うのです。

この辺も含めると、国民ってどれぐらい危機感を持っているのかということも含めて考えると、今、私がお尋ねしたようなところというのが大事なポイントになっているだろうという気がしています。それゆえ、その辺のところをちょっと教えていただければと思います。

（松原氏）国民の危機意識を一般化してお答えするのは非常に難しく、人によって異なると思います。一方、ウクライナでどのようなサイバー攻撃やドローン・ミサイル攻撃が重要インフラ企業に行われているのか、中東でも重要インフラに対して、いかなる攻撃が行われているのか、防衛省を経て現在ＮＴＴという重要インフラ企業で働いており、必ずしも安全保障や軍事の専門家ではない私に話をしてほしいとの講演のご依頼が日本全国で増えています。それを鑑みますと、一般の企業レベルでも様々な地域でも関心が高まっているのでしょう。

確かに、国家情報会議の設置や安保三文書の改定は、私たちの日々の生活から非常に遠く感じる方もおられるかもしれない。一方、安保三文書の改定や国家情報局の設置への反対の声が特に身の回りで聞こえてこないことを考えると、関心を持っていない人もおられるのかもしれませんが、必要性を感じられている人たちも増えているのではないかと思います。

私がお話をさせていただいている企業経営者や一般の方々は、日本の置かれている状況や今後の有事の可能性、有事の日本への影響について情報収集したいと考えていらっしゃるようです。そうしたことに関心を持たれる方が増えてこられたからこそ、私の話に耳を傾けてくださる方々も増えてきたのではないかと思っております。

（岡嶋参与）分かりました。事実そうなのだろうとは思いますが、何となくどこかで、まだ国民レベルで見たときに、そんなに関心があるとは思えないでいます。

例えば、この前のビール会社のような状況になったら、なかなか入手できないということを実感して、初めて理解するような状況だと私は思いますし、先ほどの病院でもそうだと思うのですが、何かそういうことが起こらない限り理解しにくいものです。ましてや「たたかい」という言葉になってしまうと、ちょっとその言葉自身もそうですが、気になっており、理解というところがどういうふうにおこなわれるのか。もし、理解されていかないと、対応ができていかないのではないかと思います。そういう点でちょっとお伺いしたいと思います。

（松原氏）具体性のない掛け声だけでは、全く響かないと思います。例えば、自分たちの業種で攻撃が起きているということ、外来の患者さんの受入れが病院でできなくなってしまったこと、自分の好きなブランドの飲料が入手できなくなってしまったことなど、身近に感じられる話が非常に響くと思います。去年のアスクルに対するランサムウェア攻撃では、インフルエンザの季節にもかかわらず、医療機関や高齢者施設への医療物資の輸送にも影響が出てしまいましたので、危機感を持たれた方は多かったのではないでしょうか。

身近なところで起きた実例がどのような意味を持つのか、教訓とともに発信活動すると、意識が変わり、具体的な行動に移っていくのではないかと思います。

（岡嶋参与）分かりました。どうもありがとうございました。

（上坂委員長）それでは、小笠原参与、お願いいたします。

（小笠原参与）松原先生、本日は大変貴重なお話をありがとうございました。私は前職で外交官で軍縮ですとか国際安全保障の会議を担当しておりましたので、本日色々と御説明いただいたことは非常に貴重な情報だと思って伺っておりました。

御指摘があったとおり、まさに今年新たに安保三文書が改定されるということで、これは非常に重要なものになると思います。前回の国家安全保障戦略は２０２２年１２月だったので、ウクライナ侵攻がその年の２月に起こったので、それからまだ間もない時期でした。ウクライナでどういう戦い方が行われたのか、それからまた今回のイラン戦争でどういった戦い方が行われたのかということを十分消化しないで、前の国家安全保障戦略は、あと国家防衛戦略もできていると思いますけれども、今回新たに作るものは、本日色々お話しいただきましたけれども、こういった経験を踏まえて、そういったものを反映した形で日本がいかにして日本の安全保障、防衛を遂行していくのかということを判断していく必要があろうかと思います。

前回の国家安全保障戦略、非常に重要なところは、経済安全保障、特に平時の経済安全保障がいかに重要であるかということに光を当てたところが一つの非常に大きな付加価値だったと思っています。

今回、松原様より色々とお話をしていただいて、私が思いましたのは、次の国家安全保障戦略、そこに書かれるかどうかは別にして、日本としてやはり重視しなければいけない課題というのは、有事における経済です。経済界と、産業界と、それから国防部門との連携をどうやって確保していくのかという問題、これが非常に重要になってくるのではないかと思います。

ウクライナで我々が学んだのは、なかなか戦争が終わらないと、終わらない戦争に突っ込んだときに、兵站及びアミュニシオンをどうやって維持・確保していくかということが非常に重要だということが我々ウクライナから学んだ大きな一つの教訓ではないかと思います。

それのみならず、インフラをいかにして守るかということを超えて、例えば戦時にキネティックな攻撃が始まりますと、実際に戦場で武器が使えなくなるといったような場合、日本の自衛隊独自に別に武器を造っているわけではないですから、その武器を調達先の企業に直してもらったりとか、あるいはそれを修復してもらったりという必要が出てきますけれども、そういったところに民間企業の方がいらしてくださるのかどうか。そういったことも含めて、有事の際の民間企業と、それから国防を担う国家の機関との関係をどういうふうに整理するのかということが今非常に重要になってくるのではないかと思います。

国家防衛戦略で「重要インフラに対する攻撃に対しては実効的な対処を行」う、と書かれているということですが、国防戦略ですので、手の内を全部明かすわけにはいかないので、今までこういう書き方でも我々国民も満足していたのではないかと思いますけれども、これだけ武力紛争に巻き込まれる恐れが高くなってくると、国民もやっぱりこれではなかなか満足できないと思うんです。今後は重要インフラを担う原子力産業界も含めて、電力事業者なんかも含めて、有事の際にそういった国防に対する重要なインフラサービスを提供する企業たちが、どういった役割を演じるのか、どういった義務を負うのか、あるいはインセンティブを与えられるのかといったようなところについて、重要な課題になってくるのではないかと思います。

もう一つ、ウクライナから特に学ぶことのできる原子力発電に関する重要な教訓というのは、ザポリージャ原発みたいに敵対勢力に原子力発電所そのものを制圧されてしまって、そこを拠点にして、単に電力の供給が滞るということのみならず、そこから放射能汚染を広げ

るような脅威を国内に与えてしまう、そういった拠点を与えてしまうという、これをいかにして防圧するかというようなことがウクライナから我が国の原子力事業者並びに政府が学ばなければいけない、非常に大きなポイントではないかと思います。

原子力のことは御専門ではいらっしゃいませんけれども、最後の点について何か御意見があれば伺いたいと思います。

（松原氏）ありがとうございます。

国家防衛戦略を含め安保三文書は、戦略レベルの話ですので、余り事細かに何をするのかについては書き込めないでしょう。それでも、実効的に何をするのかについては、法律やガイドラインに落とし込むことはできると思います。

「Ｖｏｉｃｅ」の７月号に寄稿いたしましたが、例えば、有事の際に自衛隊と民間企業がどのような協力をするのか定めた自衛隊法の１０３条には、防衛企業や重要インフラ企業が含まれていません。有事のときにどう経済を回し続けていくのか。誰かが残って経済を回し続ける場合、その人たちの身の安全を確保するために何が国としてできるのかについても、自衛隊法や規制の見直しを含め、具体的な計画づくりが必要ではないかと思います。

（小笠原参与）ありがとうございます。

（上坂委員長）それでは、上坂から幾つか意見を述べさせていただきます。まず平時についてですが、先日、ビットコインの金融不正で犯人が見付かって、国籍がロシア人だったようで、アメリカの警察が逮捕して拘束したのです。ただロシアとアメリカとの他件含めた人質交換交渉で帰ってしまったということがあって。ただ、一応犯人は逮捕したということで。

そうしますと、今日お話の中で北朝鮮の話もありました。それから、有事でない平時ということでしょうか、２０１６年から２２年の間でのロシアからウクライナ社会インフラへのサイバー攻撃が頻発したということで。こういうのはもう明らかに国際犯罪だと思うのですが。これ平時としたら、どうして国際社会は犯人を逮捕できないのでしょうかと。

（松原氏）サイバー犯罪を行った人が必ずしも国内にいるとは限らず、むしろ国外にいることが多いかもしれないため、犯人を特定できたとしても手続が複雑になります。逮捕をして身柄を送ってもらうには、外交上・経済上の駆け引きなど様々な複雑な要素が絡んできます。それゆえに、なかなか身柄の確保が難しいのです。

（上坂委員長）やっぱり国際関係が。

（松原氏）そうですね、国際関係がありますので。

（上坂委員長）分かりました。

それから、原子力に関しては、平時のセキュリティですと原子炉等規制法の規制があります。こちらに関して原子力規制庁、それから警察を中心とした国で、あと事業者で対策を作っていくということです。

そして、有事に関しては、ウクライナ、ロシア、それからイラン、ＵＡＥでも原発への攻撃がありました。ただ、我々のネットワークで伺っている範囲では、建屋にミサイルやドローンが当たる、あるいは敷地内に落下した程度だと。

それで、この定例会議でも国際人道法の視点から、有事の原子力セキュリティのお話をしていただいたことがあります。私が伺ったところ、国際人道法を、最低限ですね、放射性物質が周辺に拡散する実態は招いていないという状況で、キープされているようだと。

ですから、とにかく今、原子力に関する有事というのは起きている最中で。それに対して、ＩＡＥＡが有事のセキュリティの七つのシナリオ、それからザポリージャ原発に関する安全の５つの原則を出して、監視もしてくれているということで。その状況を見て早く停戦していただきたいと。

そして、その上で有事の核セキュリティというのができていく。国際的な力でね、というふうに考えていますが。今日のお話を一般の方々に理解していただき、また学生にも教えていくということを考えた場合、有事の話ですと、まさに国際的なネットワークと、あと国が全面的に出てくる必要があって、そして情報を得ていくと。

それから、平時であれば民間、あるいは公的な組織レベルで各自皆さん、サイバーセキュリティに対する対策を練っていらっしゃる。そういう情報は先ほど直井委員がおっしゃったように、国際会議でも共有されているということです。そういう情報は得られると。

そういう現状の対策の体系を少しずつ作っていって、そういうものを一般の方や学生たちに周知していくと。そういうふうな教育の方向でよろしいでしょうか。

（松原氏）そうです。講演で参加者の方に関心を持っていただけるのは、やはりご自分の業種に関連するお話が出てきたときです。ご自分の業種そのものではなくても、取引のある業種や依存度の高い業種、なおかつそれが生々しい話であればあるほど、人ごとではないと思っていただけるようです。

ただし、ウクライナや中東も戦闘が継続中であるため、情報が必ずしも全部出そろっておらず、話の裏付けが必ずしもできないのが難しいところだと思います。

（上坂委員長）分かりました。例えば、平時の原子力のセキュリティといいますと、直井委員が日本原子力開発機構の核不拡散・核セキュリティ総合支援センターのセンター長だった。

もうこちらが世界の教育の拠点になっています。とても高品質な教育コンテンツもありまして、それで大学に来て講義していただくか、私がお借りして講義とか。そういう教育もできたのです。

ですから、原子力安全ですと、もう多くの機関が、原子力規制委員会中心に安全体系を作っています。そういう教材で教えることができるのです。

今、安全の教育レベルに、セキュリティがだんだん追いついてきているという状況なのです。これは平時のセキュリティです。今日お話ししていただいたのは有事です。これを非常に難しいでしょうけれども、なるべく自分ごとと感じられる人から教育していくと。そういう方に対して情報を与えていくのかなとは思うのですけどね。有事のセキュリティ。そういうのもだんだんと、体系化と教育を考えていかなければいけないと思うのですけどね。

（松原氏）私が、ウクライナの電力・エネルギー業界のニュースを見て導き出す教訓と、皆様のような原子力の専門家から見て読み解ける教訓は、おそらく異なるはずです。民間の電力会社「ＤＴＥＫ」や国営の電力供給会社「ウクルエネルゴ」は、それぞれ別に国から言われたからというだけではなく、自発的に土のうの設置など消極防御策を取っているだけでなく、ＣＥＯが積極的に海外のカンファレンスに行って、必要なファンディングも得ています。

ザポリージャの原発も保有している国営企業「エネルゴアトム」では去年、汚職が見付かりました。この会社は、国から何回言われても、３レイヤーの消極防御どころか、最初の段階の消極防御のための発注すら非常に遅れていました。ウクルエネルゴが第１段階の消極防御を９０％終えた段階で、エネルゴアトムは発注もしていなかったのです。これを見ますと、企業任せでいいのか、それとも一律的に規制をかけ、政府から資金を出して防衛策を取ってもらうようにするべきなのか議論が必要ではないかと思います。

そこのさじ加減やウクライナで取っている原子力の安全対策は、原子力という特定の業界についてよくご存じの皆様がお読みになれば、日本にとって必要かどうかお分かりになられると思います。知見を持った方による教訓の読み解きが必要と考えます。

（上坂委員長）早く有事が終わって、情報が公開されて、我々としても勉強したいと思います。

それでは、どうも御説明ありがとうございました。議題（１）は以上でございます。

説明者におかれましては、大変恐縮ですけれども、御退席の方をお願いいたします。

（松原氏　退室）

（上坂委員長）次に、議題（２）について事務局から説明をお願いします。

（中島参事官）今後の会議予定について御案内いたします。

次回の定例会議につきましては、令和８年６月２３日火曜日、１５時から、場所は中央合同庁舎８号館６階６２３会議室、議題については調整中であり、原子力委員会ホームページなどによりお知らせいたします。

（上坂委員長）ありがとうございます。

その他、委員から何か御発言ございますでしょうか。

御発言ないようですので、これで本日の委員会を終了いたします。お疲れさまでした。ありがとうございました。

－了－