第２６回原子力委員会定例会議議事録

１．日　時　　令和８年６月３０日（火）１４：００～１４：５９

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

恒藤審議官、井出参事官、中島参事官

４．議　題

（１）IAEA国際会議 Computer Security in the Nuclear World Securing the Future 参加報告

（原子力委員会委員　直井洋介氏）

（２）その他

５．審議事項

（上坂委員長）時間になりましたので、令和８年第２６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、畑澤参与はオンライン参加であります。

本日の議題ですが、一つ目がIAEA国際会議Computer Security in the Nuclear World Securing the Future参加報告、二つ目がその他であります。

それでは、事務局から説明をお願いいたします。

（中島参事官）一つ目の議題、IAEA国際会議Computer Security in the Nuclear World Securing the Future参加報告につきまして、原子力委員会、直井委員より御説明いただきます。

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、直井委員から御説明をお願いいたします。

（直井委員）それでは、資料に基づきまして、参加報告させていただきます。

初めに、全体概要ですけれども、この会議、５月１１日から１５日、オーストリア・ウィーンのＩＡＥＡで開催されまして、Ｃｏ－Ｐｒｅｓｉｄｅｎｔとして招聘されたので参加してまいりました。

この会議ですけれども、第１回目が２０１５年、第２回が２０２３年に開催されまして、今回の会議は第３回目に相当いたします。会議には８１か国、それから６国際機関から５３０名を超える参加者が３６の技術セッション、全体セッション、ポスターセッションなどに参加をいたしました。

開会セッションでは、グロッシーＩＡＥＡ事務局長の挨拶と、Ｃｏ－Ｐｒｅｓｉｄｅｎｔの挨拶等が行われまして、続いて基調講演が行われました。午後には、架空の国家アンシャールに対するサイバー攻撃を題材としたシナリオ形式のストーリーがビデオで展開され、その後で議論を行う全体セッションが持たれました。シナリオ形式のストーリーは、実際に発生した事案をベースにしたリアルな展開で、２日目から４日目までの全体セッションにおいても、より詳細なストーリー解説が追加のビデオで流されて、更に議論がなされました。

それから、技術セッションは、参加者の研究発表が以下の六つのテーマ別に複数の会場で並行して行われました。

それから、ライブのデモンストレーション、リアルタイムの対策の協議、実践的な学習をゲーム感覚で行って、コンピュータセキュリティの専門家との技術的交流を促進するイベント、Ｃｙｂｅｒ Ｖｉｌｌａｇｅというイベントでしたけれども、が技術セッションと並行して開催されました。

それから、最終日の閉会セッションでは、ＩＡＥＡの原子力安全・セキュリティ局のＤＤＧのカリーヌ・エルヴィウさんから閉会の挨拶と、Ｃｏ－Ｐｒｅｓｉｄｅｎｔを務めましたブラジルの原子力エネルギー研究所のイゾルダ・コスタさん、及び報告者よりテーマ別の成果のまとめと閉会挨拶を行い、会議は終了いたしました。

続きまして、個別の結果について御報告をいたします。

まず、開会セッションですけれども、冒頭グロッシー事務局長よりビデオメッセージにて、情報セキュリティとコンピュータセキュリティは、原子力安全・核セキュリティの根幹を成す柱であること。それから、新規原子力プロジェクトでは、計画段階からコンピュータセキュリティを考慮し、また、既設システムにおいて現在及び将来のサイバー脅威に対応できるようセキュリティ対策を更新しなければならないこと。それから、サイバー脅威は、国境を

超えるため、情報セキュリティとコンピュータセキュリティの強化には国際協力が不可欠であることなどが述べられました。

ここでちょっと御報告ですけれども、コンピュータセキュリティという言葉はＩＡＥＡがよく使っている言葉でございまして、基本的にはサイバーセキュリティと同義で使われております。

それから、Ｍｓ．エルヴィウＤＤＧから、ＩＡＥＡはコンピュータセキュリティの良好事例やインシデント情報を共有するためのＩｎｆｏｍａｔｉｏｎ ａｎｄ Ｃｏｍｐｕｔｅｒ Ｓｅｃｕｒｉｔｙ ｏｆ Ｐｒａｃｔｉｃｅ、これＣｙｂｅｒＣｏｐと省略するそうですけれども、これを立ち上げるということがアナウンスされました。

続きまして、Ｃｏ－Ｐｒｅｓｉｄｅｎｔのコスタさんから、コンピュータセキュリティはもはや補助的な機能ではなくて、原子力安全・セキュリティの中核を成す柱であって、回復力、そして国民の信頼を支える基盤となること、強固なコンピュータセキュリティがなければ、デジタル化の恩恵を十分に享受することはできず、リスクを、責任を持って管理することもできない。この国際会議で得た知識を組織内で活用すること、そして常に将来を見据え、強靭性を維持することの必要性を強調しました。

また、報告者より、物理的な侵入の痕跡が見えにくいサイバー攻撃では、共通の危機感を醸成することは難しいが、この会議はその危機意識を高め、協力関係を構築し、専門家ネットワークを構築する絶好の機会となること。それから、法的な規制枠組みは脅威やサイバー攻撃に対応していく必要があり、変化する状況に合わせて規制の枠組みも進化させていく必要があることを述べました。

続いて、基調講演です。基調講演は、米国エネルギー省／国家核安全保障庁（ＤＯＥ／ＮＮＳＡ）副長官であるＤｒ．Ｍａｔｔｈｅｗ Ｎａｐｏｌｉさんから行われました。

ＮＮＳＡでは、２０２２年に「ＲＩ利用者のためのコンピュータセキュリティ・ベストプラクティス集」というものを作成していますけれども、今年度それを更新する予定であること。更新版では、ＲＩ使用施設に関連した最新のサイバー攻撃事例を追加して、サプライチェーンセキュリティへの対応の勧告を拡充する。サプライチェーンセキュリティに特に重点を置くのは、サイバー脅威はもはや自社が所有・運用するものを守るだけでなく、依存しているものを守ることにも及ぶからだ。それから、ＲＩの輸送に対する世界初のＧＰＳ位置偽装・電波妨害検知機能など、先端技術の活用を促進すべきだというような話。それから、サイバー攻撃は、物理的な攻撃の前兆となる可能性があって、インシデントの多くは、人的ミ

ス、認識不足、または訓練不足に起因していると。核セキュリティにおいては、システムが機能するかどうかを問うだけでなく、システムが信頼できるかどうかも問わなければいけない。それから、ベンダーの審査、技術試験と評価、サプライチェーンのリスク管理、入札や契約におけるコンピュータセキュリティ要件に関する適切な慣行を確立することは極めて重要だ。それから、ＩＡＥＡは、各国が信頼できるベンダー、コンピュータセキュリティ及び核物質防護を包括的な戦略に統合できるよう支援する上で、引き続き重要な役割を果たす。重要な意思決定には人間の関与が必要であり、敵対者もＡＩ対応ツールを使用することを想定する必要がある。それから、ＳＭＲは、将来のエネルギーの重要な一部であり、これらの設計に核物質防護と同様、コンピュータセキュリティを組み込むことは優先事項である。

それから、４番目の「架空の国家アンシャールに対するサイバー攻撃を題材としたシナリオベースの動画視聴と議論」です。

初日の午後のプレナリーでは、架空の国家アンシャールに対するサイバー攻撃を題材にしたストーリーがビデオで展開され、そのビデオのシーンを視聴した後に、投票アプリを利用して、会場参加者が質問に答えて、パネリスト、報告者もパネリストを務めましたけれども、がコメントをしていく形で議論が進められました。

シナリオは、実際に発生した事案等を参考に構成されていて、リアルで、臨場感のあるストーリーでありました。実際のサイバー攻撃や、大規模イベントで放射性物質をばらまくテロなどを経験したことのない参加者には、テロ対策や、関係者間の連携の重要性、テロ後の対応などを考える上で大変効果的な手法であると思いました。

また、２日目から４日目の午後の全体セッションにおいても、メインストーリーを更に深掘りする３本の動画、これはアンシャール原発へのサイバー攻撃、それから、グラ病院からＲＩを盗取するというストーリー、それから、大規模イベント会場でのテロ、このビデオがそれぞれ流されまして、会場参加者とスライドを使って対話形式で議論する形で進められております。

なお、このメインストーリーの概要につきましては、一番最後に参考資料にまとめております。

それから、５番目の「技術セッションのテーマ別のまとめ」でございます。

まず初めの①「原子力分野及びそれ以外の分野におけるコンピュータセキュリティの位置づけ」です。

これまで、コンピュータセキュリティ、核物質防護、安全、緊急時対応、そしてそれらの

運用というのは独立して発展してきたわけなのですが、原子力施設のデジタル化は、脅威の状況を根本的に変え、サイバーインシデントは、単なるＩＴ関連の事象として扱うことはできず、今日の脅威は複合的で、部門間の壁を取り払い、連携・協力して統合的に対策を考える必要があると。

組織は、攻撃経路のみに焦点を当てるのではなくて、サイバー攻撃事例の運用上及び安全上の影響をますます考えるようになっている。この変化は、事業を確実に運用することと原子力安全目標に直接的にコンピュータセキュリティを整合させるために極めて重要だ。

コンピュータセキュリティに関する専門知識は世界的に偏在していて、国際協力は不可欠である。ＩＡＥＡ、国際パートナーシップ、地域協力メカニズム、そしてコンピュータセキュリティを実践するコミュニティの役割は重要であり、デジタル時代に取り残される国がないように、国際協力の推進が重要である。

それから、②の「規制の枠組み」です。

デジタル化、先進原子炉、相互接続システム、クラウド技術、ＡＩ、そしてますます複雑化するサプライチェーンによって、規制環境は急速に変化しており、参加者は変化への適応性、リスク情報、そしてパフォーマンスに基づく規制モデルの重要性を強調しました。

目標は、変化する状況下でもシステム、組織、そして事業者が信頼できる安全な運用を維持できる対応力である。静的な規制では動的な脅威に対抗することはできない。

検査は規制当局にとって重要なツールの一つであって、規制が運用上の現実となる場になる。重要な課題は、法律や規制要件を真にリスクを低減する有意義な検査ガイドラインへと転換することにある。

これは容易ではなくて、以下の要素が必要となるということで、明確なコンプライアンス基準、客観的な証拠の収集、多分野にわたる専門知識、連携した検査と監査、そして、進化する脅威や新たな技術に対応できる適応性の高い手法。

もう一つの大きな懸念は、サプライチェーンリスクである。サプライチェーンは、今や戦略的なコンピュータセキュリティ領域となっている。ベンダー、ソフトウエアの依存関係、保守作業、あるいはデジタルサービスを通じて導入される脆弱性は、高度に成熟した施設でさえも弱体化させる可能性がある。

それから、３番目が、「コンピュータセキュリティと持続可能性のための能力・コンピテンシー管理」です。

技術だけでは原子力施設を安全に守ることはできず、コンピュータセキュリティ能力は持

続可能な人的能力に依存する。議論された有望な進展は、以下の訓練と演習の高度化が進んでいる点だということで、テーブルトップエクササイズ、それから、訓練用のシミュレーター、バーチャルリアリティーベースのゲーム化学習、物理環境とサイバー環境を組み合わせたハイブリッド演習、結果重視のシナリオ、そして、コンピュータセキュリティの専門家ではない人向けに設計された教育プラットフォーム。こういった分野で非常に進展が見られております。

コンピュータセキュリティは、もはやコンピュータセキュリティ専門家だけのものではなく、運用担当者、エンジニア、規制当局者、緊急対応要員、核物質防護の専門家、経営幹部、調達担当者、そして政策立案者までもが、サイバーレジリエンスの維持において重要な役割を担っている。したがって、将来の労働力は多分野にわたる専門知識を持つ人材でなければならない。また、継続的な専門能力開発と、専門家が経験、教訓、実践的な導入戦略を共有できる実践コミュニティへの強い支持も表明されました。

もう一つの議論されたテーマは、持続可能性であり、持続可能なコンピュータセキュリティには以下の要素が必要だということで、長期的な投資、組織的な知識の保持、人材育成パイプライン、学術及び官民連携、そして継続的な適応。

コンピュータセキュリティは、一度きりのプロジェクトではなく、継続的かつ持続的な能力であって、この能力が組織文化の一部になることで、安全文化とセキュリティ文化を統合した強力なコンピュータセキュリティ文化が、デジタル化が進む原子力システムにおける信頼維持に不可欠となる。

４番目の「脅威とリスク」です。

サイバー脅威は急速に進化していて、加盟国が新たな原子炉を設計し、また、既存施設を近代化するに当たり、原子力施設のライフサイクル全体を通して、サイバーリスクを継続的に理解、評価、優先順位付けし、そして対処する必要がある。

複数のセッションで、現在の対策は依然として事後対応型である一方、脅威の状況はますます適応性、知識、相互関連性を高めていることも述べられました。

効果的なコンピュータセキュリティは、技術、運用、そして人的側面を組み合わせることに依存しており、最初の攻撃はしばしば人間の弱点を悪用するため、意識向上とセキュリティ文化の構築が効果的な対策の一つになります。

会議では、脅威インテリジェンスと運用フィードバックを通じて継続的に進化する、専用のインシデント対応能力と適応性セキュリティオペレーションセンターの重要性も強調され

ました。

参加者は、現実的なサイバー演習とレジリエンス検証を支援できるハイブリッドセキュリティフレームワーク、アクティブ防御メカニズム、それから、高精度テスト環境の必要性も強調されました。

この文脈におきまして、ＩＡＥＡのＣｏｏｒｄｉｎａｔｅｄ Ｒｅｓｅａｒｃｈ Ｐｒｏｇｒａｍで開発されたアシェラ原発シミュレーター、これはサイバー攻撃の実習訓練が行えるシミュレーターです。これは、コンピュータセキュリティのグローバルな能力向上を支援するツールとして認識をされました。

それから、もう一つの主要テーマは、ＡＩの責任ある導入です。ＡＩは新たなリスクをもたらしますが、防護のために依然として有効であること。複数の講演者が、ＡＩ導入に当たって以下の重要性を強調いたしました。

人間が関与する意思決定、ｈｕｍａｎ ｉｎ ｔｈｅ ｌｏｏｐ、それから、セキュリティアーキテクチャの透明性、ＡＩシステムの説明可能性、それから、ＡＩ導入のための厳格なガバナンス。

特に安全性が極めて重要なシステムにおいては、人間が関与する意思決定の必要性が繰り返し強調されました。

また、普及拡大を阻む幾つかの課題として、既存のＯＴシステム、規制の不確実性、データ品質の限界、ＡＩによる意思決定への信頼性などが挙げられました。多層防御、設計段階からのセキュリティ、厳格なアーキテクチャ、アクセスコントロール、そして強固なセキュリティ文化は、従来型の脅威とＡＩを活用した脅威の両方に対して有効である。

重要な点としては、効果的なコンピュータセキュリティでは、遠隔測定技術の増加や自動検出だけに頼ることはできず、状況に応じた対応が重要で、例えば、内部脅威の早期発見には、行動や作戦上の意味を解釈できる統合された人的・サイバー的運用能力が不可欠となる。

将来のコンピュータセキュリティは、強靭で説明可能、かつ先見性のある防御能力を実現するため、技術、人、組織、そしてガバナンスの各側面を統合する必要がある。

それから、５番目の「設計段階からのコンピュータセキュリティ」です。

コンピュータセキュリティは、原子力施設の概念設計段階から開始し、運用ライフサイクル全体を通して統合され続ける必要があります。参加者は、コンピュータセキュリティはもはやシステム導入後に適用される追加機能やコンプライアンス対策として扱うことはできない。むしろ、コンピュータセキュリティは以下の要素に直接組み込まれる必要がある。

プラント設計や計装制御システム、核物質防護システム、運用手順、及び人事のセキュリティプログラム。

会議で議論された重要な概念的転換の一つは、従来の「ＩＴセキュリティ」アプローチからコンピュータセキュリティを考慮したエンジニアリングへの移行でありました。このアプローチによって、コンピュータセキュリティ関する意思決定は、技術的なチェックリストだけでなく、物理的な安全性への影響や運用上の回復力要件に基づいて行われることになります。

提起された重要な点の一つは、規制当局と事業者がセキュリティ・バイ・デザインの原則とコンピュータセキュリティを考慮したエンジニアリング手法への理解を深めるべきであるという点です。

参加者は、この分野における規制上のギャップが依然として存在し、コンピュータセキュリティに関する考慮事項をエンジニアリング及び規制の実践に直接統合するためのさらなる取組が必要であると指摘がなされました。

参加者は、市販品活用時の標準化された評価ツールや、コンピュータセキュリティ対策の評価と検証を改善するための方法論についても発表しました。また、脆弱性管理は、核物質防護、計装、制御システムのライフサイクル全体を通して継続的なプロセスでなければいけないことが強調されました。

設計段階からのセキュリティ確保には、複数の分野にわたる連携が必要で、コンピュータセキュリティは、単なるサイバー問題として孤立した状態であってはならず、分野間の連携と統合が不可欠である。

このような多分野にわたる統合は、デジタル技術が運用においてより大きな役割を果たす先進原子炉やＳＭＲの登場に伴い、特に重要となる。参加者は、コンピュータセキュリティに関する懸念事項をプラント及び計装制御設計に直接統合するための共同ガイダンスの必要性と協力の強化を推奨いたしました。コンピュータセキュリティを最初から統合しておかないと、後々レジリエンスを実現することが著しく困難かつ高コストになることが明確に示されました。

それから、最後、６番目、「新しいデジタル技術がコンピュータセキュリティに与える影響」です。

新しいデジタル技術の影響に係るセッションでは、イノベーションとセキュリティのバランスを取るという課題に焦点が当てられました。これらの議題を通して一貫して伝えられた

のは、イノベーションはコンピュータセキュリティの敵ではなく、多くの場合、イノベーションはレジリエンス、検知、運用状況把握を強力に促進する要因となり得るということです。

同時に、参加者は原子力施設におけるデジタルトランスフォーメーションは避けられないものであり、戦略的に監視、自動化、効率化、そしてサイバーレジリエンスの向上に有益であると認識しました。

しかしながら、新たなデジタル機能は、新たなコンピュータセキュリティリスク、依存関係、そして攻撃対象領域をもたらします。そのため、これらの技術を単なるＩＴアップグレードとしてではなく、厳格なガバナンスと設計段階からのセキュリティ確保を必要とする統合されたサイバーフィジカルシステムとして扱う必要があることが強調されております。

また、自律システム、スマートセンサーネットワーク、ドローンベースの技術は、潜在的に有用なツールとして認識されたものの、参加者はこれらのシステムには、無線インターフェース、リモートアクセス経路、クラウドへの依存、セグメンテーションなどの点に細心の注意を払う必要があると強調しました。

最後に、会議参加の所感を述べさせていただきます。会議全体を通じて得られた大きなメッセージとしては、以下の５点であると考えます。

まず、コンピュータセキュリティをめぐる脅威は大きく変化をしていて、事業者も規制当局もこれに適応することが重要であるということ。

それから、２点目は、コンピュータセキュリティ、ＩＴセキュリティ、核物質防護、安全、緊急時対応など、部門間の壁を取り払って、統合的にサイバー攻撃に対する対策を考える必要があるという点。

それから、３点目は、ＡＩを含む最新のイノベーション技術は注意すべき点に留意して積極的に活用するべきであるという点。

それから、４番目として、専門家の育成・非専門家への教育を含め、コンピュータセキュリティ人材の育成は極めて重要である。

それから、５番目として、情報・教訓の共有、人材育成など、国際協力はコンピュータセキュリティを確保する上で不可欠になるという点です。

それから、仮想の国、アンシャールを舞台にしましたサイバー攻撃のストーリー展開と議論は、テロ攻撃の経験のほとんどない参加者に臨場感を持って疑似体験をさせる非常に良く練られたプログラムでありました。このデモンストレーションは、核セキュリティ文化の醸成にも役割を果たしたと思います。

それから、研究発表以外にも実際のセキュリティ機器のデモンストレーションや、サイバービレッジのような企画も参加者の意識づけや能力開発、人的ネットワークの構築に大いに役立ったというふうに感じました。

将来の原子力環境は、間違いなくデジタル化され、より相互接続され、より複雑化いたします。したがって、私たちの共通の課題は、イノベーションに抵抗することではなく、イノベーションが安全、セキュリティ、レジリエンス、そして信頼を弱めるのではなく、強化することを確実にすることであると思います。

次回のこの会議は、２０３０年に開催される予定であるということでした。

報告以上でございます。

（上坂委員長）直井委員、ありがとうございます。

６月１６日の定例会議において、ＮＴＴの松原氏から、重要インフラへの攻撃事例とレジリエンスの御説明がありました。本日はまさにＩＡＥＡ中心のそれに対する対策の会議の報告であったと認識します。

それでは、４０分をめどに質問、質疑を行いたいと存じます。

吉橋委員からお願いしたいですが、聞こえますか。

（吉橋委員）はい、聞こえます。

私の声、大丈夫でしょうか。

（上坂委員長）大丈夫です。

（吉橋委員）直井委員、ＩＡＥＡへの御出張お疲れさまでございます。

また、大変詳細な会議の御報告もありがとうございます。

この会議は、コンピュータセキュリティに関する国際会議で、サイバー攻撃を題材として非常に様々な議論がなされたということでした。先ほど上坂委員長からもありましたように、最近聞いたお話ですと、物理攻撃よりもまずサイバー攻撃が始まって、気づいたときにはもう遅いということもあるということがあり、更に最近のＡＩの発展も著しくて、コンピュータセキュリティは非常に重要で、これは社会全体でちゃんと意識して、勉強して、対策、対応していく必要があるのではないかと感じております。

その中で質問なのですが、今回５３０名を超える参加者があったということで、この問題、色々と規制当局であったり、先ほどの社会全体で考えていく必要があると申しましたが、今回のこの出席者は企業の方、電力の方、規制当局の方、どのような立場の方が多く参加されていたのでしょうか。

（直井委員）御質問ありがとうございます。

冒頭スライドを使って会場の投票システムで、あなたの仕事は何ですかという問いをしたときに、５０％を超える人が規制当局というふうに回答していまして、それ以外は研究機関とか、それから事業者、そういうような回答でした。だから、メインは規制当局者が半分ぐらいを占めていたということです。

以上です。

（吉橋委員）ありがとうございます。

また、その参加者なのですが、日本からはどれぐらいの参加者があって、日本からはどういった方が御出席されていたのでしょうか。

（直井委員）はい、ありがとうございます。

規制庁さんから７名か８名おられたと思います。それからあと、ＪＡＥＡから何名かおられました。ということで、１０数名参加していました。

以上です。

（吉橋委員）ありがとうございます。

今日の御報告の中でも連携というキーワードが幾つか出てきたかと思うのですが、今のお話、参加者を聞いていても、規制当局が一番多いと。ただ、実際は事業者だったり、この対策をしていかないといけないところが沢山あるかと思います。そういう意味では日本はかなり遅れているなと感じて、もっと関係各所に知ってもらえるといいのかなと思うのですが。

今回のこの題材とされていた仮想の国のアンシャールを舞台にしたこのビデオですね、非常に私も興味があるのですが、これは各国の人材育成の教材として公開されるというようなことはないのでしょうか。

（直井委員）おそらくビデオは公開しないのではないかと思いますが、非常に出来がいいので、できればそういうふうにしてもらいたいという提案はＩＡＥＡに対してしていきたいと考えています。

（吉橋委員）ありがとうございます。

多分先ほどお伝えしたように、日本国内かなりこういった問題遅れていると思います。今後更にこのサイバーセキュリティの問題出てくるかと思いますので、こういう世界的な人材育成の取組ということで、是非日本であったり、世界中で取り入れてもらえるといいなというふうに私は感じました。

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、参与から御質問や御意見を伺います。

青砥参与から御意見を頂ければと思います。

（青砥参与）直井委員、吉橋委員からもありましたように、国際会議への出張、御苦労さまでした。

また、かなり詳細な情報を共有いただき、ありがとうございます。

色々多面的な内容がサイバーセキュリティについて議論されていて、そうした中で最も色々と考えさせられるのは、例えば開会のセッションでサイバーセキュリティはもはや補助的な機能ではなく、原子力安全・セキュリティの中核を成す柱であるとして、原子力安全・セキュリティの中核だと言い切っているところ。あるいは、技術セッションで幾つかのテーマの中で関連した議論がなされていて、直井委員も総括の中に挙げられましたように、ＩＴ関連の事象として単純に扱うことはできず、脅威は複合的で部門間の壁を取り払って、連携・協力して統合的に対策を考える必要があるとしていること。更には、デザインの中で設計段階からサイバーセキュリティを組み込んでいく、これらを規制と共有していくというか対応していくという話合いがなされたことを考えますと、一番やはり気になるのは、こういう議論の中でなぜＣＩＳＯのポジションが議論されないのか。もっと言いますと、ＣＩＳＯって今、割と軽く扱われているような気がしていまして、各プラントにおけるＣＩＳＯのプロ化ですとか資格の対応ですとか、あるいは教育、教育の話もあったのですが、一般的な教育ではなく、管理責任者としての人材を育てていく。彼が中心となってプラントのサイバーセキュリティを見ていくというようなそういう動きについて議論があったのか。あるいは今後の趨勢としてそういう議論に入っていこうとしているのかについて、もしお分かりでしたらお話しいただきたいと思います。

（直井委員）貴重な御質問と御意見ありがとうございます。

確かにＣＩＳＯの育成ですとか教育ですとかは極めて重要で、今回のこのビデオを使った中にも、アンシャール原子力発電所のＣＩＳＯが辞任するというフェイクビデオが流れます。そういった意味でＣＩＳＯというのは、サイバーセキュリティを達成する上で、対策を達成していく上で重要な役割を負うのですが、あまりこの会議でＣＩＳＯの教育に特化したような教育プログラムですとかという話はなかったと思います。

（青砥委員）是非そのあたりも、各国が様々な段階にある、情勢にある中で、統一的なサイバーセキュリティの在り方ですとか、対応の機能の在り方、人間の役割の在り方に責任を持たせるという意味で是非必要かと思います。もし機会がありましたら是非そのような進言をし

ていただきたいと思います。

（直井委員）ありがとうございます。

この国際会議のときにＩＡＥＡ側からアナウンスされました、冒頭申し上げましたけれども、ＣｙｂｅｒＣｏｐという、これはどういうプラットフォームかといいますと、まさにＣＩＳＯなど実務責任者がサイバーセキュリティ関連の情報を共有するような場にするという予定です。こういったプラットフォームが今後ＣＩＳＯを育成する上では非常に重要な役割を果たすのではないかなというふうに考えています。

今後ともＩＡＥＡに対してはそういった進言をしていきたいというふうに思います。

ありがとうございました。

（上坂委員長）畑澤参与からも御意見を頂ければと思います。聞こえますでしょうか。

（畑澤参与）はい。聞こえております。ありがとうございます。

直井委員におかれましては、重要な会議に出席されて、大変貴重な情報を共有していただきまして、ありがとうございました。

今回は、ＩＡＥＡが主催するということで、核関連のサイバーセキュリティという側面が大きかったと思いますけれども、恐らくそのサイバーセキュリティというのは他の重要な分野でも同じように今大きな問題になっているのではないかと思います。

私は医療の分野におりますけれども、医療機関の中の情報に対するサイバーセキュリティ、サイバーアタックが最近頻発しておりまして、これに対しては、いかに対応するかというのを医療機関の中では情報共有しています。今回のＩＡＥＡで行われた核の分野のように、包括的に、それから深く何が問題で、どういう解決方法を、しかもネットワークを組んで行わなければならないということは、医療など他の分野ではなかなかまだできていないことだと思うのです。

それで、今回直井委員がおっしゃられたことは、核セキュリティの分野だけではなく~~そ~~、他の重要な分野も、考えなければいけない共通した方法論であったり方向性であったり、含んでいると思うのですけれども、それについてはいかがでしょうか。どのようにお考えでしょうか。

（直井委員）どうも畑澤先生、ありがとうございます。御質問ありがとうございます。

今回の会議のビデオの中でも病院で使っているＲＩを盗取するという事例が出てきて、その中でも議論したのですけれども。やはり医療機関というのは原子力施設に比べますとサイバーセキュリティ対策の陣容も、それから施設の設備も桁違いに脆弱だというような議論が

なされて、やはりそういったところも対策を格上げしていかなきゃ駄目だというような議論はなされました。

それで、今回、参加された半分以上の方が規制当局の方でした。全世界で見ますと原発を持っているのは３０か国ぐらいで、参加者は今回８１か国からですから、残りの５０か国ぐらいはＲＩしか使っていない国になります。ＲＩを使うというところは基本的には病院がメインになってくるというので、今回の会議の中ではそういう医療関係の施設においてもＲＩの防護だとかサイバーセキュリティの重要性というのが、クローズアップされたのではないかというふうに思います。それで、今後もしっかりやっていかなきゃいけないということだったと思います。

今回基調講演したＤＯＥのＮＮＳＡの副長官の話では、ＲＩを使っている現場でのサイバー攻撃の実例についての事例集を改訂版に含めるという話でしたので、そういった情報は今後病院関係者にも有益に使える情報となるのではないかと思いました。

（畑澤参与）大変ありがとうございます。

医療機関の中でもサイバー攻撃に対する対応が必要だという認識はできていると思うのですけれども、病院の中にその専門家を雇用して対策に当たるということはなかなかできていなくて、病院のスタッフの中でコンピュータの得意な方をそういう役職に就けて対応しているというのが現状です。

ですから、直井委員の今回の報告の中にもありましたように、人員を育成する、コンピュータに対して十分理解できている人と、また医療について知識がある、経験がある二つの分野の能力を兼ね備えた人材の育成というのが非常に重要だというふうに思いました。

それで、もう一つは、あとはそういう専門職ができた場合の組織におけるコストですね、コストをどういうふうに確保するかというのも非常に重要な点ではないかと思うのですけれども、そういう人材を育成した場合のコスト、雇用をどういうふうに担保するかということは議論になったのでしょうか。

（直井委員）ありがとうございます。

具体的に病院のサイバーセキュリティの体制としてこういうふうにしたらどうかみたいな具体的な話はなかったと思うのですが、やはり病院でサイバーセキュリティを強化するためには、しっかりと脅威を理解してもらわなくてはならず、そういった意味ではＤＯＥが作っている事例集で、こんな事例がある、あんな事例があるということが明確になれば、それをもって予算要求をするというようなことができるのではないかというふうに思います。

それから、ＩＡＥＡのサイバースドルフには核セキュリティのためのトレーニングセンターが設置されておりまして、そこでサイバーセキュリティの訓練もできるようにするというような話もあって。また、全世界には日本もＪＡＥＡがＩＳＣＮというセンターを持っていますけれども、そういった人材育成、トレーニングしたりする、提供したりする地域のネットワークみたいなのが出来上がっていて、サイバー攻撃に対する教育をするというようなコースも出てきておりますので、そういったものを使って陣容の育成に当たるということができるのではないかというふうに思います。

以上です。

（畑澤参与）ありがとうございます。

恐らく、核セキュリティの分野ではこのサイバーセキュリティというのが、直接的に脅威になりますので、一番その必要性は高いと思うのですけれども、是非このサイバーセキュリティというのは、それ以外の分野でも非常に重要なことだと思いますので、この会議の内容を是非社会に広く知っていただきたいな、というのが直井委員の御報告を聞いて感じたことでございました。

是非この先端的な取組を他の分野にも知っていただくような形で広報していただければいいなというふうに思いました。

どうもありがとうございました。

畑澤は以上です。

（上坂委員長）ありがとうございます。

それでは、岡嶋参与から御意見を頂ければと思います。

（岡嶋参与）直井委員、どうもお疲れさまでした。会議への参加。それから、非常に上手く、詳細にまとめていただきまして、ありがとうございます。

お話をお聞きして、これまでの委員や参与からの御質問等々の内容も含め、気になっている点があります。それは、まず、開会セッションのところです。ここでいうと第２パラグラフのところです。エルヴィウＤＤＧがアナウンスしたということで、コンピュータセキュリティの良好事例やインシデント情報を共有するためのそういうものを立ち上げるという話だったのですが、具体的にこのアクションというのはいつ頃から始まるとか何かそういうような話はあったのでしょうか。

（直井委員）ありがとうございます。

既にどういうものをつくるというのを紹介するウェビナーを、この７月だったと思います

が、申込みがもう既に始まっていたと思うので、そういった場でオープンになってくるのではないかなと思います。

今回のこの国際会議の中では詳細なこんなものをつくるというような提案はなく、恐らく開催されるウェビナーの中で情報共有されると思います。

（岡嶋参与）こういう事例というのは非常に早く進んでいきますので、どうしても後追いになりがちかと思います。そういう点で早く立ち上げて、早くこういうことで共有化を図っていくということが、僕は一つの重要ポイントではないかと思って聞いていました。

（直井委員）はい、おっしゃるとおりかと思います。

（岡嶋参与）それからもう一つは、この架空の国家アンシャールに対するサイバー攻撃とシミュレーションといいますか、デモンストレーションというのか、どちらか分かりませんけれども、それに関してです。資料後ろにあるシナリオを見ると、なかなか今の、どう言えばいいのだろう、映画を見ているような感じがするようなシナリオになっているのですが。ほぼ現実的な状況の映画を見ているような感じがします。こういう教材というのは、今後、関係者の間で、例えば人材育成とかそういうところでこういうものが使われていくと考えられるのでしょうか。この会議だけでの紹介だけではあまりにももったいないような気がします。その辺のところは何かお話があったのでしょうか。

（直井委員）これは、ミッションインポッシブルみたいな映画になっていまして、トータルすると４０分ぐらいの動画なのですね。スポンサーがイギリスとカナダと韓国と、それからアメリカとＥＵなのですけれども、相当のお金がかかっているのではないかなと思います。それで、やはりそういう教材は非常に貴重なので、使えるようにしてもらいたいなというふうには思っていて、実際にお金を出したアメリカの担当者を存じ上げておるので、その彼にちょっと相談してみようかなというふうに思っています。

ありがとうございます。

（岡嶋参与）是非我が国もそうですけれども、こういうことを扱っているセンター等があるという話ですから、その辺を通して教材とともに人材育成に充てていくというのは一つ大きな効果があるかと思います。

私からのコメントとしては以上です。

（上坂委員長）ありがとうございます。

それでは、小笠原参与から御意見を頂ければと思います。

（小笠原参与）直井委員、どうもありがとうございました。大変充実して、かつ中身のある国

際会議だったと思います。

直井委員の方から、最後に、会議参加の所感として５点挙げておられますけれども、いずれももっともなことで、政府のサイバーセキュリティに関する対応も大体こういったラインに沿って今強化されているのではないかというふうに理解しております。去年はサイバーセキュリティ基本法が改正されまして、能動的なサイバー防御の法的な基礎が置かれ、また官民一体となって取り組むという、我が国においてもそういった法整備が進められていると思いますので、まさに時宜を得たＩＡＥＡ側のインプットではなかったかと思います。

特に強く印象を受けましたのが、参考資料として直井委員がつけてくださっている架空の国家アンシャールに対するサイバー攻撃を題材としたシナリオ、ストーリーということで、今お話がございましたけれども。これを拝見していますと、直井委員が所感でおっしゃっている色々な部門間の壁を取り払って、統合的にサイバー攻撃に対する対策を考える必要があるということがよくビジュアライズして分かるような組立て方になっていると思います。サイバー攻撃と共に、実際のフィジカルな、あるいはキネティックな攻撃が同時並行して行われており、更に、言論空間における色々な偽情報等を発信して社会不安を醸成するといった多面的な攻撃が有機的に組み立てられて行われているということです。これは非常によく分かりますし、また、教育的な効果があるのではないかと思います。

これは原子力委員会の所掌ではないかもしれませんけれども、サイバーセキュリティは今後非常に重要になってきます。やはり司々で色々と専門でやっておられますので、こういった統合的に色々な側面から実際にどういう攻撃が行われるかということを想定して、そういった準備の段階から関係の司々の省庁がこういったシナリオに基づいて色々と対応を考えられることは、日本においても非常に有意義ではないかというふうに思いました。

私から以上、コメントだけですが。

（上坂委員長）ありがとうございます。

では、上坂から意見を述べさせていただきます。

現在、世界の原子力発電所にとってサイバー攻撃が最も差し迫った脅威の一つであると思います。最近でも、大手飲料メーカーが甚大なサイバー攻撃を受けまして、まだ影響を受けているというようなことを伺っております。

それに対する対策の、ＩＡＥＡ中心の国際会議なのですが、やはり人材育成といいますか、そういう体制をしっかりつくっていただきたいなと思うのです。先ほど青砥参与からＣＩＳＯ、最高情報セキュリティ責任者の話がありました。原子力発電所には原子炉主任技術者が

いまして、国家資格者でいまして、現在こちらが全ての安全とセキュリティをみているということなのですね。ところが、今日の御説明のように、サイバー攻撃が非常に甚大になっているということを考えると、並列のような形でＣＩＳＯがいてもよろしいのではないかなと。

実は、１５年ほど前に、原子力学会の教育委員会で、原発にセキュリティ主任がいるのではないかという議論しました。すぐにそういう資格をつくるのは大変だから、技術士にセキュリティ教育をして、このＣＩＳＯ相当になっていただけないかなというような議論もしておりました。

それで、吉橋委員からもコメントがありましたが、是非これの教育を水平展開して、世界でやっていただきたいと思うのです。セキュリティに関してＩＮＳＥＮという、インターナショナルニュークリアセキュリティエデュケーショナルネットワークがあります。本当に今日の内容や、アンシャール国家のビデオですね。こういう教材をＩＮＳＥＮのような、ＩＡＥＡ発信の教育プログラムに入れていただいて、世界で共有できるといいかなとも思うのです。いかがでございましょうかね。

（直井委員）どうもありがとうございます。

おっしゃるとおりで、大学での教材としてサイバーセキュリティを教える教材として、ＩＡＥＡのコーディネーテッドリサーチプロジェクトで御紹介しましたけれども、いわゆるサイバーセキュリティのシミュレーターですね、シミュレーターを使った教育がもう既に実際の大学院で適用されている例がございまして、そういった例でインセン（ＩＮＳＥＮ：Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｎｕｃｌｅａｒ Ｓｅｃｕｒｉｔｙ Ｅｄｕｃａｔｉｏｎ Ｎｅｔｗｏｒｋ）でもＩＡＥＡ内で共有はされているのだと思います。

ということで、そういった意味では教育にサイバーセキュリティも含めた形でというのはこれからのトレンドじゃないかなというふうに思います。

一方で、なかなかそういう教育をするには、そもそも先生がいないというようなコメントも結構聞きました。それで、やはり専門のそういうサイバーセキュリティのコントラクターといいますか、専門家と契約をしてサイバーセキュリティを見てもらう、人材を育成してもらうということもあり得ると思います。それからサイバーインテリジェンスですか、現在のサイバー攻撃の動態を理解した上で対策まで進展させるというようなサイバーインテリジェンスの会社も出てきていて、そういったところを上手く使うということもあると思います。御紹介でした。

以上です。

（上坂委員長）ありがとうございました。

直井委員と吉橋委員と共に参加した２月１６、１７日にありましたＪＡＥＡのＩＳＣＮ、原子力人材育成・核不拡散・核セキュリティ総合支援センターと、ＷＩＮＳ、ワールドインスティテュートフォーニュークリアセキュリティの共催の核セキュリティセミナーがありました。そこではやはり同じようにビデオ視聴演習がありました。ここでも内部の職員がぼや騒ぎを起こすという、セキュリティと安全が融合した事案でありました。

それから、こういう例えばＩＳＣＮ、それからＷＩＮＳですね。世界共同のセミナーとかで、非常に厳しいサイバー攻撃の事例を教育する。そしてだんだんと標準化してＩＮＳＥＮで教材つくっていく。そんなシナリオもあるかと思いますけれども、いかがでございましょうか。

（直井委員）詳細は伺わなかったのですけれども、サイバーセキュリティトレーニングコースというものを今ＩＡＥＡでも、アメリカですとか韓国ですとか、それからＥＵ等も入って開発をしていまして、それを地域のニュークリアセキュリティサポートセンターなどで展開していくというような計画を聞いております。また、ＩＳＣＮでももう既に規制庁の検査官といいますか、を育成するためのトレーニングコースなどを規制庁とともに開発して適用するというような報告もありまして、だんだん増えてきているのではないかなというふうに思います。

それから、国際会議で非常にいいなと思ったのは、国際会議ですので学術的な研究発表がなされる中で、規制当局側と事業者が意見交換を行えるというところが非常によかったなというふうに感じていまして、それはＩＳＣＮがこの２月に上坂委員長と吉橋委員共に行きましたウィンズのワークショップ、そこでも同じテーブルで電力事業者と規制当局の人が一緒に議論するというような機会になっています。そういう機会は情報の共有といいますか、何をお互い考えているかというのを知る上では貴重なよい機会だなというふうに思いました。

以上です。

（上坂委員長）そのようなサイバーセキュリティ、そこには当然ＡＩの活用が入ってくると思います。その対策の教育プログラム。それからＣＩＳＯのようなポストができ、そしてまたグループもできますと、若手の人材投入された組織になると思うのですよね。

今若手はこういうＡＩに非常に興味があって、当然彼らは功罪も知っています。このＡＩ、サイバーセキュリティというのは非常に若手人材育成にもいい分野と思いました。

それから、６月１９日に、日本原子力学会の安全部会がフォローアップセミナーを行いま

して、これは福島事故のフォローアップセミナーだったのです。その総合討論で私が安全とセキュリティの対策の融合の重要性を指摘しました。そうしたところ、次回のフォローアップセミナーはセキュリティが取り上げられるということでございました。

また、これは先週の金曜、６月２７日に、日本技術士会の原子力・放射線部会の講演会で、前原子力規制委員の伴氏が特別講演で、安全文化とそれから放射線防護の講演をされました。その後の質疑の中でも、私、安全文化とセキュリティ文化の融合の必要性を指摘したところでございます。

それから、先ほど来話題に上がっている、ＪＡＥＡ、ＩＳＣＮとＷＩＮＳでの核セキュリティセミナーなのですが、あのドラマはセキュリティと安全が融合した事案でございました。

ところが、私、研究炉施設に長く勤務したので、規制庁の訓練を受けるのですが、安全訓練とセキュリティ訓練が別々の実施なのです。ですから、それが一緒になった訓練はまだやってないのですね。ＪＡＥＡ、ＩＳＣＮとＷＩＮＳのドラマ演習で、近くのテーブルに規制庁の若い方がいました。一緒の訓練やるべきじゃないですかと言ったところ、現在検討中ですということでしたので。

今回のＩＡＥＡ会議にも直井委員からかなり多くの規制の方が出席されているということです。サイバーセキュリティの教育プログラムも今後進むということです。是非安全とセキュリティの一緒の対策。そして教育、訓練を期待するところであります。

例えば一般セキュリティ業界ですと、安全とセキュリティがかなり同義に近い形で使われています。我々もセキュリティ検索すると、安全、安心とか出てきて、本当に安全とほぼ同義で使われているようなところがあるのです。原子力ではこの安全対策、安全文化とセキュリティ対策、セキュリティ文化というのが現状あまり融合されていないということがあるので、今後融合が非常に重要なかと。

今日の直井委員の報告の中にも、安全とセキュリティという並列した表現がいっぱいあったと思うのですよね。今後、冒頭原子力発電所にとってサイバー攻撃が最も差し迫った脅威の一つだと思います。是非安全とセキュリティの調和、融合。それによる教育と体制づくりを是非ＩＡＥＡ中心に、日本ではＪＡＥＡのＩＳＣＮ中心に対策、教育、人材育成のプログラムをつくっていっていただきたいと思う次第でございます。

いかがでしょう。

（直井委員）ありがとうございます。そのとおりだと思います。

今回の会議でも繰り返し述べられていたのは、ブレークダウンサイロという、要は縦割り

をなくせということで、それがまず大前提で、その上で対策を統合して考えるということかと思います。そういった形で人材育成の方も取り組んでいくということが必要だと思います。ＩＳＣＮの方にはその旨伝えていきたいというふうに思います。

ありがとうございました。

（上坂委員長）ありがとうございました。

議題１は以上でございます。

次に、議題２について、事務局から説明をお願いいたします。

（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７月８日水曜日、１４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。

御発言はないようですので、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－