IAEA 国際会議
Computer Security in the Nuclear World
- Securing the Future -
参加報告

令和８年６月 30 日
原子力委員会　委員　直井　洋介

１．全体概要

2026 年 5 月 11 日～15 日、オーストリア・ウィーンの IAEA で開催された International Conference on Computer Security in the Nuclear World - Securing the Future –（CyberCon26）に Co-President として招聘され参加した。この国際会議は第 1 回目が 2015 年に、2 回目が 2023 年に、今回の会議は第 3 回目である。会議には 81 か国、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した。

開会セッションでは、グロッシーIAEA 事務局長のあいさつと Co-President のあいさつ等が行われ、続いて基調講演が行われた。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、その後議論を行う全体セッションが持たれた。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、さらに、議論がなされた。

技術セッションは、参加者の研究発表が以下の 6 つのテーマ別に複数の会場で平行して行われた。

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
② 規制の枠組み
③ 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
④ 脅威とリスク
⑤ 設計段階からのコンピュータセキュリティ
⑥ 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

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い、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 が技術セッションと並行して行われた。

最終日の閉会セッションでは、IAEA 原子力安全・セキュリティ局の DDG カリーヌ・エルヴィウより閉会挨拶と、Co-President であるブラジル原子力エネルギー研究所のイゾルダ・コスタ及び報告者より、テーマ別の成果のまとめと閉会挨拶を行い会議は終了した。個別の結果概要は以下のとおり。

開会セッション（IAEA HP より）

２．開会セッション

冒頭、グロッシー事務局長よりビデオにて、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、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も現在およ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、サイバー脅威は国境を越えるため、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た。

Ms. エルヴィウ DDG（原子力安全・核セキュリティ局）より、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 Information and Computer Security of Practice（CyberCop）を立ち上げることがアナウンスされた。

続いて Co-President のコスタ氏より、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、原子力安全・セキュリティの中核を成す柱であり、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見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、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た。

３．基調講演

米国エネルギー省/国家核安全保障庁 (DOE/NNSA)副長官 Dr. Matthew Napoli より、基調講演がなされた。NNSA 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」を作成し、今年更新予定である。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、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である。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である。サイバー攻撃は、物理的な攻撃の前兆となる可能性があり、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。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はなく、システムが信頼できるかどうかも問わなければならない。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である。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、およ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。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に、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。

４．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

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（Slido）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た）がコメントをしていく形で議論が進められた。シナリオは、実際に発生した事案等を参考に構成されており、リアルで、臨場感のあるストーリーであった。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。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さらに深掘する 3 本（アシェ

ラ原発へのサイバー攻撃、グラ病院からの RI 盗取、大規模イベント会場でのテロ）のビデオがそれぞれ流され、会場参加者と Slido を使って対話形式で議論する形で進められた。なお、メインストーリーの概要は「参考資料」にまとめた。

５．技術セッションのテーマ別まとめ

① 原子力分野およ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

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は、独立して発展してきたが、原子力施設のデジタル化は、脅威の状況を根本的に変えた。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。

組織は、攻撃経路のみに焦点を当てるのではなく、サイバー攻撃事例の運用上およ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である。

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おり、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。

② 規制の枠組み

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り、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 1 つであり、規制が運用上の現実となる場である。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である。これは容易ではなく、以下の要素が必要となる。

- 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。

③ 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

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である。

- テーブルトップエクササイズ、
- 訓練用のシミュレータ、
- VR 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。

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い。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た。

もう一つ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である。

- 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、
- 学術連携、
- 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る。この能力が組織文化の一部となることで、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 脅威とリスク

サイバー脅威は急速に進化しており、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あたり、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である。

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型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、高精度テスト環境の必要性も強調した。この文脈において、IAEA の CRP(Coordinated Research Program)で開発されたアシェラ原発シミュレータ（サイバー攻撃の実習訓練が行えるシミュレータ）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された。

もう一つの主要テーマは、AI の責任ある導入である。AI は新たなリスクをもたらすが、防護のために依然として有効である。複数の講演者が、AI 導入にあたって以下の重要性を強調した。

- 人間が関与する（human in the loop）意思決定、
- 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(explainability)、
- AI 導入のための厳格なガバナンス（継続的な検証）。

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た。また、普及拡大を阻むいくつかの課題として、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、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に、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。

⑤ 設計段階からのコンピュータセキュリティ

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る。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、
- 計装制御システム、
- 核物質防護システム、
- 運用手順、
- および人事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った。このアプローチにより、コンピュータセキュリティに関する意思決定は、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。

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ある。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および規制の実践に直接統合するためのさらなる取り組みが必要であると指摘した。

参加者はまた、市販品(COTS)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を発表した。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ならないことが強調された。

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、特に重要になる。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およ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た。

⑥ 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

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を当てた。これらの議論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ある。

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

とが強調された。

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が、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ことが強調された。

６．会議参加の所感

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。

① コンピュータセキュリティを巡る脅威は大きく変化しており、事業者も規制当局もこれに適応することが重要である。
② 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い、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。
③ 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。
④ 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。
⑤ 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。

仮想の国、アンシャールを舞台にしたサイバー攻撃のストーリーの展開と議論は、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った。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。研究発表以外にも実際のセキュリティ機器のデモや、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おおいに役立ったと感じる。

将来の原子力環境は、間違いなくよりデジタル化され、より相互接続され、より複雑化する。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。

次回の同会議は 2030 年に開催される予定である。

（以上）

（参考資料）

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のストーリー概略

（第１幕）

アンシャールでは地域国際競技大会(Major Public Event)が計画されていた。この大会会場で放射性物質をばらまくテロ攻撃を計画する集団 Radionuclide Liberation Front（RNLF)によってさまざまな攻撃がしかけられる。

大会３週間前にアンシャールにあるアシェラ原子力発電所の主任制御システムエンジニア（CSE）のノアが、混雑している街中のカフェでノートパソコンを用いて作業をしていた時、近くでテークアウトのコーヒーを持ち出そうとした女性が急に倒れる。ノアは女性を助けに自席を離れたすきに、近くで同じように作業をしていた男（RNLF のテロリスト）がノアの PC に USB を差し込みサイバー攻撃の起点を作る。RNLF のテロリストはノアが気づく前に USB を抜き去り、その場を立ち去る。ノアはこれに全く気付かない。

（第２幕）

アシェラ原発の HP には、発電所の最高情報セキュリティ責任者（CISO）が、もはや発電所のセキュリティを確保する責任を果たすことができないとして、この職を辞任するとの動画が流される。これは RNLF によるディープフェイク画像であり、この画像を起点に、原発反対派や環境活動家、さらには国外からも反響が寄せられ、地域国際競技大会直前にアンシャールでは社会不安が引き起こされる。

一方、ディープフェイク画像を流された CISO と自宅テレワーク中のノア（CSE）がやり取りを始める。CISO はノアに対し、アシェラ原発への制御システムへの安全な遠隔接続を許可し、アシェラ発電所の運転状況を確認させる。しかしこの接続でテロリストのアシェラ原発制御システムへの侵入を許してしまう。また、ノアの PC の Web カメラ画像がテロリストとつながり、テロリストによるノアの画像の配信を許してしまう。

CISO は、自身の辞任の動画はフェイク動画であることを対外的に発表。同時に、アシェラ原発は安全に運転されていることも発表。しかし、アシェラ原発の中央制御室では、メインのモニター画面が真っ暗になるなどの異常が発生する。

（第３幕）

CISO のフェイク動画やアシェラ原発中央制御室でのメインモニターの異変など RNLF の発電所ネットワークへの侵入事件に端を発し、インフルエンサー、反原子力活動家や環境活動家がネガティブな発信を行い、アシェラ原発への反対運動が爆発的になっていく。一方のアシェラ原発側も、流出したノア（CSE）の Web カメラ画像が本物であることを確認し、また、テロリストらが、アシェラ原発の５層あるコンピュータセキュリティレベルの第３層まで侵入してきたことを確認する。３層までの侵入では、発電所の運転には影響はなかったが、運転員達はパニックになり、すでに、RNLF の広範囲な不安定化工作は成功を収めていた。アンシャールの原子力規制当局は、原子力関係者すべてに警戒を指示する。

（第４幕）

一方、アンシャールのグラ病院では、人材不足に悩む人事部門の担当者がスタッフの採用支援を行うAIエージェントの無料トライアル、実はこれはRNLFが仕掛けたわなで、これをクリックしたことにより、RNLFにグラ病院のコンピュータネットワークへの侵入を許してしまう。RNLF はこの侵入により、病院内の放射線モニターの警報設定値をかさ上げし、その後の病院への侵入で RI を盗取しても警報が鳴らないように細工を施した。しかし、病院側がすでに導入していた AI ベースの OT（Operation Technology）監視システム（IT ソリューションツール）によって、外部からの意図的なかさ上げ設定の変更を検知するとともに、その旨を警察に通報する。その後、RNLF のテロリスが病院に侵入して RI の盗取を試みるが、すでに、

警戒に当たっていた警察にテロリストは逮捕される。

一方、アシェラ原子力発電所では SNS での呼びかけを受け数百人の過激派活動家がアシュラ原子力発電所の完全停止を要求して発電所に集結する。

（第５幕）

アンシャールのシャパシュ原子力研究所から放射性廃棄物（Cs-137）の輸送が行われる。輸送車と護送車の隊列で研究所を出発するが、途中で輸送車のエンジンが不調になり、修理のためにロードサービスを呼ぶ。すでに、この輸送は RNLF に監視・追跡されており、輸送車のエンジンの不調も RNLF によって事前に仕組まれていた。ロードサービスへの連絡は RNLF に繋がってしまう。ロードサービスを装う RNFL のメンバーは、輸送車の修理をするふりをして、輸送車に積載されていた放射性廃棄物の盗取に成功する。

（第６幕）

シャパシュ原子力研究所からの放射性廃棄物輸送時に RI の盗取に成功した RNLF のテロリスト達は、放射性廃棄物を国際競技場会場で拡散させるため、その廃棄物を搭載したドローンをピックアップトラックに載せてイベント会場に向かう。イベント会場の上空では、放射線検知器を積んだヘリコプターが市内を上空から監視している。ヘリコプターは、ピックアップトラックから高い放射線を検知し追跡する。ピックアップトラックはイベント会場の近くのスーパーマーケットの駐車場に停車し、荷台から放射性廃棄物を搭載したドローンを下す。ドローンを飛ばそうとしたその時に、警察が駆け付けテロリストたちを逮捕する。