核セキュリティの動向：核物質防護条約改正レビュー締約国会議に向けて

日本原子力研究開発機構　福井　康人

1. はじめに

2022年も新年を迎えてIAEAも新しい予算年度になったが、現在、核セキュリティ[1]の関連で関係者の間で注目されているのは、2022年3月28日から4月1日の期間にウィーンで開催が予定されている核物質防護条約改正レビュー締約国会議である。この手の条約の意思決定機関の開催前には準備委員会が開催され、事前に手続事項や議題等について議論した結果が準備委員会報告書に纏められることが多い。しかしながら、かかる文書は締約国関係者限りの限定配布であり、直前にならないと公開されないことが多く、この会議の場合も同様である。他方で、その直前の関連する会合である今年の国際原子力機関（IAEA）総会では、関係しうると思われる資料が幾つか公開されている。例えば、核セキュリティ決議[2]、2021年核セキュリティ年次報告[3]、2022年－2025年核セキュリティ計画[4]、IAEA予算書の主要計画の原子力安全・核セキュリティ関連部分[5]等がIAEAホーム・ページに掲載されている他、核セキュリティ文書も新たに刊行されている。

ちなみに、核セキュリティ分野の代表的な条約としては、核物質の防護に関する条約（略称：核物質防護条約）及び同改正が挙げられる[6]。同条約は核物質の国際輸送時に防護を強化すること等を基本的義務として規定した条約として作成され、特にその後の改正により国内の使用、輸送、貯蔵中の核物質及び施設に対する防護に適用対象が拡大されたことにより核物質防護の基本的な条約になっている。それ以外では、核によるテロリズムの行為の防止に関する国際条約（略称：核テロリズム防止条約）が挙げられることもある[7]。もっとも同条約は核テロを未然に防ぐ条約であり、厳密には核物質防護の条約では

[1] 核セキュリティについて、日本の原子力規制委員会は、「核燃料物質、その他の放射性物質、その関連施設及び輸送を含む関連活動を対象にした犯罪行為又は故意の違反防止、検知及び対応」と定義している。
[2] IAEA Doc. GC (65)/9, September 2021, pp.1-9.
[3] IAEA Doc. GC (65)/10,30 July 2021, pp.1-35.
[4] IAEA Doc. GC (65)/24, 15 September 2021, pp.1-22.
[5] IAEA Doc. GC (65)/2, July 2021, pp.111-138.
[6] 核物質の防護に関する条約（核物質防護条約）（Convention on the Physical Protection of Nuclear Material）, 1456 UNTS 246(entered into force 8 February 1987); 改正核物質防護条約（2005 Amendment to the 1979 Convention on the Physical Protection of Nuclear Materials）（adopted on 8 May 2016）. なお、同条約改正の2021年11月末の締約国数は127か国（改正に必要な要件国数は核物質防護条約締約国の3分の2が改正を締結することが必要とされる。）
[7] 核によるテロリズムの行為の防止に関する国際条約（略称：核テロリズム防止条約）（International Convention for the Suppression of Acts of Nuclear Terrorism）, 2245 UNTS 89, (enter into force 7 July 2007).

ないものの、抑止効果が期待できる観点から、核セキュリティ関連条約として、上記の核物質防護条約及び同改正とともに挙げられることが多い。

これらの条約のうち、2016 年 5 月の核物質防護条約改正の発効から 5 年が経過したため、レビュー締約国会議が初めて開催される。当初はもう少し早い時期の開催も検討されていた。その後、コロナ対策もあり延期され、最終的に 2022 年 3 月末に開催されることとなった。

かかる次第もあり、冒頭の本節では議論の視点を明らかにする為にも、核物質防護条約の改正の経緯について簡単に回顧した上で、引き続き、核セキュリティ関連の動きを概観するため、本年の IAEA 総会決議を通してどのようなことが核セキュリティ分野で要請されているかを見てみる。次に、IAEA が今後中期的に何を実現しようとしているかを見るために 2022 年－ 2025 年核セキュリティ計画を概観する。更に、最近頻繁にサイバー攻撃が話題になる上に、2021 年 10 月に原子力施設のためのコンピューター・セキュリティ[8] 技術にかかる技術ガイダンス改定版[9] が刊行されたので概要を紹介した上で、レビュー締約国会議を念頭においての、筆者の考える核セキュリティ分野の課題について述べることとする。

先ず、元の核物質防護条約は締約国に対し、国際輸送中の核物質について警備員等による監視等の防護の措置が取られるようにすること、また、核物質の窃取等の行為を犯罪として、容疑者が刑事手続を逃れることのないように、それらの犯罪について自国の裁判権を設定し、容疑者を引き渡さない場合には自国の当局に事件を付託すること等を義務付けるものである[10]。その後、近年、核物質の不法取引及び核によるテロリズムの脅威に対する国際社会の認識が高まる中、現行条約の強化が求められるようになった。これを受けて、1999 年 11 月、IAEA において、元の条約の要否を検討するための非公式専門家会合が開催され、2001 年 5 月、現行条約の改正の要否を検討にするための非公式専門家会合が開催され、その後も調整が続けられた結果、2004 年 6 月、日本を含む 25 か国で作成した改正案が IAEA の事務局長に提出された。更に、IAEA 事務局長の招請により、2005 年 7 月 5 日から 8 日まで、88 の締約国及び欧州原子力共同体（EURATOM）が参加して条約改正会議が開催され、この条約が改正された[11]。

特にこの条約の意義としては、平和目的のために使用される核物質及び原子力施設の効果的な防護を世界的規模で達成するため、国際輸送中の核物質を防護することに加え、締約国の管轄下にある核物質及び原子力施設について防護の制度を確立すること、平和的目的のために使用される核物質及び原子力施設に関連する犯罪を世界的規模で防止するため、核物質の窃取等に加え、法律に基づく権限なしに行う核物質のある国への又はある国からの移動を犯罪とすること等について定めるものである。このように、核物質防護を世界的規模で強化するためには必要不可欠な条約であり[12]、IAEA においても核セキュリティ・シリーズ基本文書と共に重要視されている。

2. IAEA 総会で採択された決議

（1）決議の読み方

IAEA 総会に限らず、決議は国連総会等に広く採択される会議文書である。このような決議は、例え

[8] IAEA は日本で頻繁に使用されるサイバー・セキュリティの意味で「computer security」を使う傾向があるものの、原語を尊重し、コンピューター・セキュリティにした。
[9] IAEA Doc. “Nuclear Security Series (NSS) No. 42-G Computer Security for Nuclear Security,” September 2021, pp.1-140.
[10]『核物質の防護に関する条約の改正の説明書』外務省、1 頁。
[11] Ibid.
[12] IAEA Doc. IAEA INFCIRC/225/Rev.5, June 2012, p.4, para.2.1.
核物質、原子力施設の物理的防護に関する核セキュリティ勧告（INFCIRC/225/Rev.5）IAEA 核セキュリティ・シリーズ 13 番によれば、国家の核セキュリティ体制の目的を核物質及びその他の放射性物質が関与する悪意のある行為から人、財産、社会及び環境を防護することにあるとした上で、国家の核セキュリティ体制の中核となる核物質防護体制の目的として以下の 4 点を挙げている。
①不法移転に対して防護すること。
②行方不明の核物質を発見、回収すること。
③妨害破壊行為に対して防護すること。
④妨害破壊行為の影響を緩和又は最小化すること

ば、国際機関の加盟国毎の分担金を決定する文書等を除いては一般的には立法的でない（即ち、法的拘束力を持たない）とされるが[13]、今年のIAEA総会でも合計17本の決議が採択されている[14]。また、標準的な決議は関連する決議の引用や当該決議の趣旨と目的を説明する前文パラ（preambular paragraph）と本文パラ（operative paragraph）からなり、概ね最終パラグラフは次回会合の議題に次回会期にその案件が取り上げられるように書かれ、また、決議によっては附属が添付される場合もある。

特に、本文を読み進める際に注意すべきはどのような動詞が使用されているかである。例えば、当該決議により加盟国又事務局に行動を慫慂する場合はencourageを、行動を求める場合はcall uponを、更にそのことを歓迎する場合はwelcomeを、留意することに留める場合はtake noteの表現を使用する。また、加盟国又は事務局に実施を要請する場合はrequestを使用するなど、概ね書き方が決まっている。なお、IAEAにも関連する北朝鮮制裁等の安保理決議ではdecideが使用されると、国連憲章第25条に基づいて法的拘束力を有することになるが[15]、IAEA決議の場合は余り見かけない。

因みに、この核セキュリティ決議（GC (65)/9）には、15のパラグラフで行動を求める（call upon）が、7つのパラグラフで要請（request）が使用されおり[16]、これらのパラで加盟国又は事務局に要請が行われている。もっとも、これらのパラグラフの中にはin a position to do so（本文パラ36後段）は「出来る国は協力する」という文言を入れてより多くの国に受け入れられるための文言の工夫である。また、加盟国の国内法令との関係を明確にするため、consistent with the national legislation and regulation（本文パラ41）の文言は、加盟国の法制度との整合性を確保するためである。他のパラにon a voluntary basis(本文パラ14) 等も義務的なものでなく任意性を強調する文言である。こうした定型の文言を適宜使いつつ、可能な限りコンセンサス採択を目指し、調整を進めて決議の文言を確定させてから、最終的に決議の採択を目指すことになる。

（2）核セキュリティ決議の概要

そのような観点から特に決議本文から、要請を求めるcall uponのキーワードを中心に今年の核セキュリティ決議の内容を概観する。先ず、核セキュリティの原則として、全ての各締約国の責任の範囲内で非常に実効的な核物質、放射性物質の使用時、輸送時に高度な核セキュリティが関連施設のみならず、そのライフサイクルにおいても、機微情報の保護を含めて、達成・維持されることが要請される（パラ2）。その上で、事務局に対しては2018年－2021年核セキュリティ計画を継続して実施し、2022年－2025年核セキュリティ計画を包括的且つ調整されて実施し（パラ3）、更に今後も4年毎にICONS会議を開催することが事務局に求められる（パラ6）。

また、未実施の加盟国に対して、権限ある当局又は法的枠組みを実施する当局の指定を要請、維持することを要請している（パラ7）[17]。その具体的な核セキュリティを強化する上で取るべき措置についても要請している（パラ8）[18]。他方で、加盟国に対してIAEAの活動を支援するために、必要な政治的、技術的、財政的な支援を提供して、二国間、地域及び国際的なレベルで多様なアレンジメントを通じて支援するとともに、核セキュリティ基金の支援に係るIAEA理事会決定を想起している（パラ9）。このことからIAEAが核セキュリティ関連拠出金を加盟国

---

[13] V. Lowe, “International Law (Clarendon Law) (Clarendon Law Series),” Oxford University press, 17 November 2007, p.91.
[14] IAEA Doc. GC（65）/RES/2021（DEC), December 2021, pp.1-141.
[15] 国連憲章第25条は「国際連合加盟国は、安全保障理事会の決定（decision）をこの憲章に従って受諾し且つ履行することに同意する。」と規定していることから、国連加盟国には法的拘束力を有するとされている。なお、かかる決議文の読み方は識者には「釈迦に説法」の感があるものの、幅広い層の読者の存在を考慮して説明を書いたもの。
[16] もっともcall uponは加盟国に対し、requestは事務局に対して特定の事項を要請する場合に使用することが多いが、その他の決議文では加盟国に対して強く要請する (urge) が使われることもある。
[17] ここでの「当局」は、核物質又は他の放射性物質の推進又は使用に係る事項を扱うその他の意思決定機関から全体又は部分的に独立して機能した意思決定機関であり、その責任を遂行するために権威又は必要な人的、財政的及び技術的なリソースを有すると同パラ後段で説明されている。
[18] 具体的には、核物質又はその他の放射性物質の利用、移転、生産、原子力の平和的利用に係る活動平和目的のための核物質の交換及び原子力エネルギーの平和利用を推進し、IAEAの技術協力プログラムのために確立された優先度を損なわないとする条件が課されている。

に対して強く期待していることが分かり、多くのプロジェクトが具体的には核セキュリティ基金からの支出を想定している（次節の核セキュリティ計画関連の 3.（1）参照）。

また、具体的に踏み込んだ措置も要請されており、例えば、コンピューター・セキュリティについてはセキュリティと透明性のバランスを勘案しつつ、IAEA 核セキュリティ・シリーズ 23-G に定められているように規制から離脱した核物質又は他の放射性物質に係る情報を取り扱う適切なメカニズムを強化、改善するために取り組むとされている（パラ 20）。更に、IAEA が使用済みのものを含む放射線源に係るセキュリティについて継続した対話及び同分野の研究開発を進めることも支援を要請している（パラ 33）。また、事務局に対して、マンデートの範囲内で、締約国に対して技術的に可能且つ経済的で維持可能であり、加盟国の原子力技術における原子力及び放射化学上の選択肢を勘案して通知するとする（パラ 34）。また、加盟国に対して、安全で確実な保管場所及び使用されなくなった密封放射線源の処分方法については、このような線源が規制管理下にあることを確保することを要請し、更に、実現可能な限り、使用されなくなった放射線源を供給国に返還または可能な時にはこのような線源を再利用することも慫慂している（パラ 36）。また、各国の脅威評価に基づき、領域内での不法取引及びその他の違反行為、核物質の関連活動を対象にした活動や事件を防止、探知、対処、抑止する当該国の能力を改善、維持するとともに、関連する国際的な義務に合致させ、更に可能な場合にはこの点に関して国際的なパートナーシップと能力構築の向上を図ることが要請されている（パラ 37）。

また、その領域内の規制から逸脱した核物質及びその他の放射性物質を回収し、保全する努力を継続すること（パラ 40）、全ての加盟国に対して、国内法令に基づいて原子力施設での内部脅威を防止、検知、防護するための適切な措置を取ることを継続し、事務局は加盟国に対して、核セキュリティを強化するために内部脅威に対する更なる防止・防護措置を取ることにつき、要請に応じて加盟国に対して助言を行い、それは「施設における核セキュリティの目的のための核物質計量管理（核セキュリティ・シリーズ No.25 － G）」を含むとしている（パラ 41）。また、国内法令に従い、放射線源を使用する施設及び輸送中の内部脅威を防止、検知、防護するために適切な措置を取ることを継続して要請されている（パラ 42）。

以上、加盟国や事務局に対して要請されていることを中心に今年の核セキュリティ決議を概観したが、上記以外のパラで、例えば核物質の移転事案データベースの有用性についての言及、核セキュリティ情報マネージメントシステムにつき任意での利用を慫慂するパラに加えて、IPPAS（国際核物質防護諮問サービス）、INSServ（国際核セキュリティ諮問サービス）、INSSPs（統合核セキュリティ支援計画）等について言及したパラなどが盛り込まれている。このように、この決議を概観することにより、現時点で IAEA 及び加盟国が核セキュリティについてどのような状況にあり、更にどのような課題を抱えているかについて把握することが可能になる [19]。

3. 2022 年－ 2025 年核セキュリティ計画

（1）核セキュリティ関係予算

また、中期的に核セキュリティを実施する上でどのような課題を抱えているかについては、2022 年－2025 年核セキュリティ計画を読むことにより今後の大まかな方向性を知ることが出来る。では、その前提となる核セキュリティ関係予算はどのようになっているであろうか。IAEA も国連予算と同様に二か年予算制度（Biennium）になっており、2021 年 9 月の IAEA 総会で承認されたのは 2022 年－ 2023 年二か年予算である [20]。IAEA 予算は総計 6 つの主要計画（Major programme）から編成されており、核セキュリティは原子力安全・核セキュリティの主要計

[19] supra note 3.　本稿では解説しなかったが、前年の決議に基づき年次報告でも公表されている。
[20] IAEA 二か年予算は、①主要計画 1：原子力、燃料サイクル及び原子力科学。②主要計画 2：開発のための原子力技術、③主要計画 3：原子力安全及び核セキュリティ、④主要計画 4：原子力の検認、⑤主要計画：政策、マネージメント及び行政サービス、⑥主要計画 6：開発のための技術協力管理の 6 つの主要計画から構成されている。更に、下層に計画（programme）、小計画（sub-programme）、プロジェクトに階層的に作成され、整理番号と共に標記されている。

画 3 に含まれており、その中の計画 3.5 が核セキュリティ分野をカバーし[21]、これらは更に細分化されて小計画（Sub-programme）に分かれている。

具体的には小計画 3.5.1 の情報管理、小計画 3.5.2 の物質及び施設の核セキュリティ、小計画 3.5.3 の規制の管理を外れた物質の核セキュリティ、小計画 3.5.4 の国際協力の発展計画の 4 つの要素から構成され、更にそれぞれの小計画には具体的なプロジェクトとして必要となる予算が計上されている。そういう意味では核セキュリティは主要計画 3 の中でもその一部分を占めているにすぎず、2022 年予算は 6,567,000 ユーロであり、2023 年予算は 6,663,000 ユーロが通常予算にて賄われる予定である。加盟国からの拠出金、即ち核セキュリティ基金等により支弁されることが想定される非通常予算分が 2022 年予算では 28,674,000 ユーロであり、2023 年予算では 28,983,000 ユーロが未充当（unfunded）とされている。現下のコロナ禍による予算執行が困難な問題もある一方で、かかる資金不足を今後加盟国からの任意拠出金等で財源を念出する必要があり、こうした前提で 2022 年 -2025 年核セキュリティ計画全体を見ていく必要がある。

（2）2022 年－ 2025 年核セキュリティ計画

このように、2022 年－ 2025 年核セキュリティ計画はこうした予算前提の下で作成されており、2021 年 9 月 24 日に IAEA 総会前の IAEA 理事会で承認された後、事務局長はこの 2022 年 -2025 年核セキュリティ計画を理事会がテークノートし、加盟国に対して核セキュリティ基金への財政的貢献を呼び掛けている[22]。

その前提で、この計画書の内容を見ると、A．導入部分、B．背景、C．計画要素及び D．計画管理の 4 部から構成されており、C．については先述の予算書の主要計画 3 の構成に準拠している。

このため冒頭に述べられているように、「可能な限り全ての核物質及び他の放射性物質に係る実効的且つ包括的な核セキュリティを常に維持すること」[23]を目的としている。また、この計画は IAEA 総会で表明された加盟国の優先度のみならず、核セキュリティ・ガイダンス委員会（NSGC）の勧告の他、過去の 2018 年－ 2021 年核セキュリティ計画や統合核セキュリティ支援計画との整合性にも配慮されている。

こうした背景を基に、計画要素等を見てみると、これは予算書にも順序が異なるだけで同じことが書かれている。即ち、

> ①輸送時及び関連施設での平和的利用を含め、核物質及びその他の放射性物質のための国内核セキュリティ体制の確立、維持及び持続させるために各国を支援する。
> ②包括的核セキュリティ・ガイダンスの確立、要請に基づいて相互審査、諮問サービス、教育、訓練を含めた能力構築の推進を含めて実効的な核セキュリティを達成するための全世界的な努力に貢献する。
> ③関連する国際的な法的文書への加入並びに安全及びセキュリティについての行動規範及び核セキュリティを全世界的に向上させるためにその補完的なガイダンスへのコミットメントを推進する。
> ④ ICONS2020 の閣僚宣言を考慮し、IAEA 総会及び理事会の決定及び決議に対応するため、核セキュリティに関するコミュニケーションを通じて、可視化及び意識向上を進め、国際協力を推進し、促進する中心的な役割を果たす。

先ず、C.1 において優先度及び相互に関連する項目については、加盟国が確認し、IAEA が全世界的に核セキュリティにおける中心的な働きをすることとして 4 項目が特定されている。

これは、

> ①適切な国際的法的文書の普遍化を促進し、要請に応じて、加盟国が適切な国際的な法的文書に加入して、実施することを支援する。
> ②包括的な核セキュリティ・ガイダンスの出版

[21] 主要計画 3 は更に、4 つの原子力安全・核セキュリティ関連計画に細分化されており、そのうち計画 3.5 が核セキュリティ予算である。
[22] IAEA Doc. GC (65)/24, 15 September 2021, 表紙サマリー箇所。
[23] IAEA Doc. GC (65)/24, 15 September 2021, p.1 para.1

を行い、要請に応じて、加盟国による実施促進をするために支援する。
③民生用の核物質及び放射性物質の核セキュリティを確保する責任を履行する加盟国の努力を支援するための国際協力を促進する。
④核セキュリティの枠組みを世界的に強化し、重複を避けつつ、核セキュリティ分野のイニシアティブ、他の国際機関との協力を含め、核セキュリティ分野の国際的な活動を調整すること。

が優先事項及び相互関連事項として挙げられている。

ここで言う法的文書としては、核物質防護条約及び同改正を指しており、知見や良好事例の共有に資するものとして、研究拠点や各国に所在する核セキュリティ支援センターの活用を示唆している。統合核セキュリティ支援計画（INSSPs）、国際核物質防護諮問サービス（IPPAS）、国際核セキュリティ諮問サービス（INSServ）と言った業務は原子力安全等の他の分野にも関係するものであり、こうした相互関連性のある核セキュリティ関連事項は各計画と調整する必要があるとしている。

また、次に重要なのはC.2 情報管理であり、このプロジェクトの下で、

①核セキュリティ上の必要性及び優先度。
②事故及び不法取引についての情報共有。
③コンピューター・セキュリティ及び情報技術サービス。

の3点が挙げられている。これらは更にブレークダウンされて、詳細について述べられているが、特に注目されるのは、核セキュリティ計画を実施する上で、加盟国と緊密な協議や受益国との協力で他国を援助する場合に重要なことは、最も緊急性のある援助の実施に際して核セキュリティに関する情報の秘密の保護について特に留意すべきこととされている。

その前提で、情報共有及び情報交換については、例えば、核物質防護条約及び同改正の下でこれら両条約の締約国として義務として提供される情報、移転事案データベースや核セキュリティ支援センターネットワークを通じて提供される情報、国際核物質防護諮問サービス（IPPAS）良好事例データベースを通じて提供される情報がその対象になるものとして例示されている。

更に、情報・コンピューター・セキュリティと情報技術サービスは、各締約国の核セキュリティ能力の向上に重要であり、この分野のIAEAの業務は、締約国の要請に応じて、情報、ガイダンス、訓練を提供し、IAEAのプロジェクトを促進するため情報・コンピューター・セキュリティ関連プロジェクトについての調整された研究の手引及び管理を行うことが重要であるとされる。また、核セキュリティのためのコンピューター・セキュリティのIAEA核セキュリティ・シリーズの編纂をIAEAにおいて進めること、更に、そのための調査研究を進めること、更にはWEBベースのポータルサイトを提供し、侵入者追跡のための核セキュリティ情報技術の開発・維持・配備の支援等が提案されている。

次に、C.3の物質及び施設については、組織的なインフラの構築を支援し、各国の適正、核物質及び施設の核セキュリティに関連する潜在的能力、専門的能力を向上させ、維持し、持続させることが求められている。C.3は、更に以下の4つの小計画に分割できる。即ち、

①全ての核燃料サイクルに対する統合核セキュリティ・アプローチ。
②核物質及び関連施設のセキュリティの向上。
③放射性物質及び関連施設セキュリティの向上。
④核物質及び放射性物質の輸送時の核セキュリティ。

先ず、廃棄物保管所、廃炉された原子炉、放射性物質及び関連物質を含む核物質及び関連施設のための統合核セキュリティ・アプローチについて、要請に応じて訓練や支援を提供したりするためのガイダンスが作成されている。また、核物質及び関連施設のセキュリティの向上については、IAEAは加盟国の要請に基づいて、同分野における助言を行うのみならず、加盟国により特定された核セキュリティ問題に対処するため、調整された研究プロジェクトを開始し、管理するとともに、加盟国の技術的能力を向上させることの支援が期待されている。

更に、放射性物質及び関連施設のセキュリティ同

様のプロジェクトが想定され、核物質及び放射性物質の輸送時の核セキュリティについても、上記2項目とほぼ同じ設計思想で書かれ、基本は同じである。このように見るとC.3に基づき冒頭の全ての核燃料サイクルに対する統合核セキュリティ・アプローチをベースに、核物質、放射性物質、輸送時の核セキュリティと言った個々の状況に併せて、プロジェクト形成を目指している。

最後にC.4の規制から外れた物質の核セキュリティであるが、加盟国から要請があり、適当な場合には、IAEAは規制外の核物質、その他の放射性物質による故意の犯罪又は不法行為の検知のための当該国のインフラ能力確立のために加盟国への支援を提供することが取り上げられている。更に、IAEAのINSServといった諮問サービスを含み、意見や良好事例の交換のような核セキュリティ回復措置についての機会を提供するものであり、

①規制の管理を外れた物質の核セキュリティ事案への対応体制。
②核セキュリティ検知アーキテクチャ。
③放射性物質を使った犯罪現場の管理及び核鑑識。

が該当するプロジェクトとしてあげられている。

ここでの具体的な検討項目としては、規制外の物質に対する組織的対応のインフラを確立し、国家及び適切な国際機関の間で、核物質及び放射性物質に係る事件の核セキュリティを確保すること、更には、同様に規制の管理を外れた物質の核セキュリティ事案対応体制の整備、実効的で維持可能な核セキュリティ体制の構築の支援について言及されている。

また、核セキュリティ検知アーキテクチャについても同じように核セキュリティ・シリーズのガイダンスの編集や訓練を加盟国に提供すること、特にこの項目は核物質の不法取引の撲滅といった犯罪防止の側面もあるので、各国の技術的知見を上げることを想定して項目があげられている。最後の放射性物質を使った犯罪現場の管理及び核鑑識についても、これらの基本的概念は非常に似ており、これが具体的なプロジェクトになった時点で、具体的な内容に差異が出てくるものと思われる。

また、C.5計画開発及び国際協力についてであるが、具体的なプロジェクト項目として、

①核セキュリティネットワーク及びパートナーシップに係る国際協力。
②人的資源開発のための教育・訓練計画。
③核セキュリティ・ガイダンス及び諮問サービスの調整。

が挙げられている。先ず、①の国際協力については、その中には2024年に予定されている次回の2024年の国際核セキュリティ閣僚会合（ICONS2024）を含めた様々な核セキュリティ関連会合の開催、マンデートの範囲内での情報交換会合、核セキュリティ支援センターネットワーク（NSSC）を補完、協力の調整、定期的な情報の交換会合を通じた活動を含めてプロジェクトが挙げられている。

更に、②の教育・訓練の関係では、核セキュリティ・ガイダンス等のIAEAの公式刊行物に基づいて教育・訓練プログラムが開催される原則が明らかにされ、同時に加盟国の実情に応じて訓練コースの内容を合致させるように微修正も示唆されている。また、核セキュリティ支援センターネットワーク（NSSC）を活用した、人材育成支援による情報共有の促進と言った点についても配慮するとされている。

最後に③の核セキュリティ・ガイダンス及び諮問サービスの調整について、核セキュリティ分野に限定しても、IAEA核セキュリティ基本文書、勧告文書、実施指針及び技術手引と階層化された多くの文書が作成されており、可能な限り最新の状態に保たれるように適時の改定も必要とされる。

最後のC.5計画管理については、D.1計画管理及びリソースについては最後の総括として簡潔にまとめられている。そもそも、この4年毎の核セキュリティ計画は毎年作成される年次報告と異なり、中期的な見通を明らかにする目的で2002年から作成されている[24]。特に資金面については、パラ74でこの計画の大部分の予算計画の実施のためには核セキュリティ基金への加盟国からの拠出金に依存し続けるだろうと予測している。以上の核セキュリティ計画

[24] IAEA Doc. GC (65)/24, 15 September 2021, p.1, para 2.

の概要を踏まえると、具体的なプロジェクトを円滑に進める為には核セキュリティ基金への各国からの任意拠出金を確保することが非常に重要であり、中長期的には通常予算内で再配分を検討する際には、核セキュリティの重要性に鑑み、実施優先度を明確にして検討する必要があることが分かる。また、決議で要請されたことを踏まえて、この4か年計画を念頭に、下記4. のサイバー攻撃対策を含めて、各プロジェクトを具体化する必要がある。

4. サイバー攻撃対策

前回のICONS2020でも日本の代表であった若宮外務副大臣が核セキュリティの直面する脅威として「サイバー攻撃」及び「内部脅威」を取り上げたが[25]、各論の最後に特にサイバー攻撃との関連で、本年9月に改定版の出た「原子力施設のためのコンピューター・セキュリティ」に係る核セキュリティ・シリーズ（No.17-T）について、紹介しておきたい。同文書は技術ガイダンスとして編集されており、そこは基本的な概念の説明に留めている。

グロッシーIAEA事務局長も前文で、「IAEA核セキュリティ・シリーズ」は核セキュリティに係る独自の責任を果たそうとする国を支援するために、核セキュリティのすべての側面についての国際的なコンセンサスを提供するものである。」と位置付けている。更に、「核セキュリティはその国の責任であり、IAEA核セキュリティ・シリーズは核セキュリティに関する国際的な法的文書を補完し、（核物質防護条約等の）締約国が義務を果たすことを援助するための世界的な参照されることが期待される」ともしており、セキュリティ・ガイダンスは、各国に対して法的拘束力を有しないが、広く適用されている。」と説明している[26]。

因みに、類似の文書も刊行されており、『核セキュリティのためのコンピューター・セキュリティ』[27]が2021年10月に刊行されている。IAEAのサイトの説明によると、このガイドは各国が核セキュリティ制度におけるコンピューター・セキュリティを強化することを支援するために刊行されている。核セキュリティ制度を弱体化させることなく、デジタル技術の利便性を確保して、サイバー上の脅威から保護し、検知するとともに対処することを目的としている。コンピューター・ベースのシステムは我々の生活においても重要な役割を果たし、それが原子力及び関連する関係の技術であっても相違はない。これらのシステムは原子力産業においても実効的で、安全且つ保護された施設の操業のみならず、核物質や放射性物質の使用、保管、輸送する際の活動に必要であるとする。

こうした鍵となる役割のため、かかるデジタル・システムはテロリストや破壊者の標的となりうる。彼らは施設のデジタル・システムの潜在的な脆弱性を悪用しようとして、無許可のアクセス、操業の停止、更には施設の破壊、核物質や放射性物質の窃取さえも行おうとする。こうした行為に対しても、これらのシステムを保護し、サイバー攻撃から施設を防護し、破壊行為の防止のみならず、例えば、システムが稼働するように物理的防護や検知制度を稼働させることにより、他の核セキュリティの分野を強化するとしている[28]。この本書は本文が60頁に満たない分量で、核セキュリティ実現のためにはコンピューター・セキュリティには何が政策的に必要かと言うような基本理念を中心に書かれている[29]。

同文書の構成は、先ず、総論的な内容に3章分が、

[25] 拙稿『核セキュリティ対策；サイバーセキュリティの側面から見て』190号、209頁、下注4参照。

[26] IAEA doc. “Technical Guidance on Computer Security at Nuclear Facilities (IAEA Nuclear Security Series No. 17-T), “September 2021, pp.1-140. なお、その前にグロッシー事務局長の前文と目次があり、当該部分は前文の第一段落と第三段落に出ている。
URL: https://www.iaea.org/publications/14729/computer-security-techniques-for-nuclear-facilities

[27] IAEA doc. “Computer Security for Nuclear Security (IAEA Nuclear Security Series No. 42-G), September 2021, pp.1-40. なお、Implementing guideは基本文書に基づくrecommendationをどう実施するかの方針、technical guidanceはさらにその技術的な指針との総意がある。

[28] “Now Available: IAEA Guidance on Computer Security for Nuclear Security, “ URL: https://www.iaea.org/newscenter/news/now-available-iaea-guidance-on-computer-security-for-nuclear-security

[29] 例えば、同書の章立ては、第1章導入部、第2章概念と文脈、第3章国家の役割と責任、第4章権限ある当局と事業者の役割と責任、第5章コンピューター・セキュリティ戦略の確立、第6章コンピューター・セキュリティ戦略の実施、第7章コンピューター・セキュリティ計画の実施、第8章コンピューター・セキュリティの持続というように、政策担当者向けに解説している。

具体的なリスク管理等に5章分が割り当てられている。即ち、前者には第1章が導入、第2章が基本的な概念と関係、第3章がコンピューター・セキュリティに関する一般的考察が挙げられている。他方で、第4章が施設のコンピューター・セキュリティ・リスク管理、第5章がシステム･コンピューターセキュリティ・リスク管理、第6章施設のライフサイクルにおける一定の段階の間の施設及びシステムのコンピューター・セキュリティ・リスク管理、第7章コンピューター・セキュリティ計画の諸元、第8章は防御的なコンピューター・セキュリティの構成とコンピューター・セキュリティ措置の例が挙げられている。

では具体的に主要部分を見てみると、先ず全体を総括説明する第1章が重要である。最初に、一般的な核セキュリティの説明が行われた上で、原子力施設におけるサイバー攻撃により、施設に物理的なダメージを引き起こしたり、セキュリティ関連又は安全関連システムを無力化し、機微な原子力情報に無許可でアクセスしたり、核物質の許可を得ない取り出しにつながることが起きかねない。このためにコンピューター・セキュリティは原子力施設では核セキュリティ及び原子力安全を保護するために死活的重要性を有するとされている[30]。更にその上で、機微なデジタル資産（sensitive digital assets, SDAs）[31]の概念を定義して、保護の対象にしている。

このような設計思想に基づき、同書は他の関連文書と合わせて、各国で実施されることが期待されている。更に、パラ1.5は「物理的保護、原子力安全、及び核物質計量管理のために使用されるコンピューターをベースとするシステムはセキュリティ侵害に対して、脅威評価又は設計ベースの脅威に応じて、保護されなければならない（例えば、サイバー攻撃、操作、改ざん、偽造等）」とされている。即ち、コンピューター・セキュリティに付随する内部脅威についても認識されており、こうした観点からの実施が期待されている。このように、コンピューター・セキュリティの観点からは、原子力施設での他のデジタル資産の保護についても考慮する必要がある。

また、同書が対象としているのは規制官庁のみならず、他の権限ある当局、原子力施設の従事者、機器販売業者、更には契約者や役務提供者も対象としている[32]。これは推察するに、核セキュリティもコンピューター・セキュリティも専門性が高いため、守秘義務を掛けた上で専門業者に外注したりすることが現実問題としてあるため、そのようなルートから狙われないように、関係者しうる者は全てこのような問題を理解した上で、業務に従事してもらうことが強く期待されている。

次に基本的概念では核セキュリティとコンピューター・セキュリティが具体的に何を指すかについて定義されている。即ち、核物質、その他の放射性物質、関連施設、関連活動、若しくは他の場所又は主要な公共行事、戦略的場所、機微情報、及び機微情報資産を含む、核セキュリティ上の脅威による潜在的に悪用される物体が核セキュリティ上の標的になるとされた上で、核セキュリティ措置についても定義されている[33]。他方で、コンピューター･セキュリティについては、コンピューターをベースとするシステムに関連して実施され、重要な施設を支援し、又は核セキュリティ及び原子力安全（例：デジタル資産）に関連するシステムに関係するとされている。その上で、コンピューター･セキュリティはサイバー攻撃、セキュリティに影響しかねない人間による作為乃至は不作為から防護する技術及びツールを提供するものと理解されている[34]。

また、これも一般的に実施されていることではあるが、階層アプローチが頻繁に使用され、コンピューターのセキュリティ・レベル、セキュリティ・ゾーンに区分して運用することも重要視されているが、最近の傾向を踏まえて、用語の定義が増加している。例えば、施設機能は操作するため及び行政的な（あるいは組織的な）機能を含むとするもので、これは多様なコンピューターの操作方法が実際には使用されることを踏まえると係る定義が必要となる。また、

[30] IAEA doc. Technical Guidance on Computer Security at Nuclear Facilities, p.1 para1.4. 42-G は implementing guide、17-T は技術指針なので、より技術的な解説。
[31] Ibid, 脚注によれば、SDA とは、「コンピューター・ベースのシステムの部分または全体となる機微情報資産」と定義されている。
[32] Ibid. 2. paras 1.9, 1.10
[33] Ibid. P.4, paras. 2.2-2.3
[34] Ibid. P.4, para. 2.4

設置場所や操作場所の関係で、現地 (on-site)、他の場所（off-site）乃至はクラウドをベースとするシステム等の区別も使用されている。これは簡単に見えて、特にクラウドの場合は業者選定の際に条件を慎重に吟味しないと、重要なデータが国外等にあるサーバーに蔵置されたりすると、セキュリティ上も万が一暗号システムが破られた場合にデータが窃取されることが起きる可能性があり、是正措置と言っても国外に実際のデータがあると現実には管轄権の関係で対応が制限される。

また、同手引が示唆している追加的な基準で興味深いのは、コンピューターのセキュリティ・ゾーンの定義である。第一に組織的な責任の問題で、これは他の部署が管理するゾーンが自分のゾーン内にある場合に、両者が協力関係にないと折角のゾーン区分がセキュリティ・ホールになりかねず、他の部分の操作により自分のゾーンが影響を受けて、システムが停止、データの損失が起きるといった予期しない事態が発生する可能性もある。第二に、システムの冗長性を維持するためには、ゾーンの区分は維持される必要があるということである。これは言うまでもないが、冗長性を維持するために例えば記憶装置上で頻繁にデータの書き換えが行われ、区分が勝手に変更されるとデータの統一性が失われかねず、保管してあるデータに再アクセスできなくなる可能性もあるからである。

他にも興味深い点が多く含まれているものの、紙面の都合で代表的な点しか紹介できないので、興味がある方は是非本書をお読み頂きたいが、コンピューター･セキュリティのリスク管理で、例えば、システム設計をする際には、必ず様々なタスクをこなす部分と、シャットダウンの機能を分けることは重要であるとされ、さらには、理想的には一機能に対して一つのシステムを割り振ることもリスク管理として推奨されているが、これも修復が簡単になるのみならず、安定したサーバーの管理には望ましい方法である。そのほかにも有益な概念的な原子力施設ごとにゾーンを切るといったモデルのみならず、原子力安全とのインターフェイスについても言及されており、冒頭の 2 章だけでも有益なモデルが示されている。

5. 結びにかえて

以上、2021 年の IAEA 総会に提出された公開文献等を中心として、近未来を含めての核セキュリティの現状乃至は近未来の姿を明らかにすることを試みたが、今後の核セキュリティ分野の課題としては、2022 年 3 月末に予定されているレビュー締約国会議を念頭に置いて如何なる課題が考えられるであろうか。当然のことながら、5 日間の会期期間のうち、通常の意思決定機関の会議の手続事項として議長等の選出や各国代表団の演説に加えて、成果文書の採択に向けての交渉が裏舞台で行われて、最終日には各国代表団が努力して最終的には採択されるのが通例である。

筆者は一研究者の立場から、特に核セキュリティ決議、2022 年－ 2025 年核セキュリティ計画、及び核セキュリティ計画コンピューター・セキュリティ関連文書から考えられるのは、上記に述べたことを踏まえると、以下の 3 つの課題が重要であると考えている。即ち、①サイバー攻撃等やドローン等新たな技術の脅威への対応、②各国との更なる国際協力の増進、③核セキュリティの財政面を含めた実施体制の強化の 3 点の課題が重要であると考えている。もっとも、公開されている IAEA 文書を見ても多種多様な問題提起が行われているので、この 3 点に限定されないのは明らかであるものの、紙面の制約もあり特にこの 3 点を強調したい。

先ず、新たな技術の脅威への対応については、上述のサイバー攻撃と言ったことがあげられる [35]。日本では富士通や三菱電機と言った企業を狙った攻撃が発生している他 [36]、原子力規制庁も被害にあって

[35] 具体的な事例については、NTI 等が調査結果を公表している他、拙稿『核セキュリティ対策：サイバーセキュリティの側面から見て』CISTEC ジャーナル、190 号、pp.208-218. 参照。
[36] 富士通『プロジェクト情報共有ツールへの不正アクセスについて（第三報）』2021 年 9 月 24 日、URL: https://pr.fujitsu.com/jp/news/2021/09/24-3.html;三菱電機『不正アクセスによる情報流出について』2021 年 10 月 22 日、URL: https://www.mitsubishielectric.co.jp/news/2021/1022.pdf

おり[37]、新たな脅威となっている。それ以外でも、フランスではドローンにより原発へ空中からの侵入事案が起きており[38]、日本国内においてもドローンの使用は飛行禁止区域の指定により、類似の事件について理論上は発生しないことになっている[39]。しかしながら、簡単に高性能のドローンが一般にも購入可能であり、故意による大型航空機の衝突その他のテロリズムも想定した国内法が施行されているものの、今後より強力なドローンが開発されないか関連動向等にも留意することが肝要であろう。

第二点目の各国との更なる国際協力の増進については、そもそもの核セキュリティの実施について、条約改正前文２に「原子力の平和的利用のための国際協力を推進し、原子力技術の移転を促進することを確信し」とあり、その必要性は言うまでもない。しかしながら、改正第 2 条 3 項において、「締約国内において防護の制度を確立し、実施し及び維持するすべての責任は当該締約国が負う。」と規定しており、核セキュリティの制度もこのような規定の下に実施されるので、最後は各国の自己責任で実施することが条約上も規定されている。さらに、核セキュリティの性質上、各原子力施設での設計や設備と言った情報が外部や同一組織内の職員であっても漏れると問題を惹起しかねない。万が一情報漏洩が起きると予期せざる「内部脅威」になりかねないので、こうしたことから国際協力の必要性は理解しうるものであるものの、核セキュリティの脆弱点になりかねない。

このため、特に開発途上国や核セキュリティ措置を巡る国際協力や情報共有については研修・訓練と言った場合も含めて慎重に対応せざるを得ない面もある。具体的な機微情報交換となると各加盟国のクリアランスを受けた有資格者間等で行うことが想定されるものの、基本的概念についての技術等知見の移転や核セキュリティ上有益な経験の共有は、特に途上国やかなり進んで国であっても核セキュリティを強化する上で必要である。その観点から、新たに開設されるサイバースドルフの核セキュリティ訓練センターのみならず、JAEA の ISCN（核不拡散・核セキュリティ総合支援センター）のようなところでは、例えば、最近はやりのヴァーチャル・リアリティを利用することや仮想の施設を事例に挙げて、受講者は現場に行かずとも状況の疑似体験も可能になり、秘密の保護に配慮しつつ知見の伝達が可能になるので、こうした訓練手法や研修施設の活用は有益であると思われる。

最後の核セキュリティ実施体制の強化であるが、特に財政面の強化が求められていうように思われる。上記 3.（1）で核セキュリティ関連予算を概観したが、十分な任意拠出が行われないと実施が不可能になるプロジェクトが生じる可能性もある。もっとも、通常予算案の編成には昨今の厳しい経済事情を反映して、実質ゼロ成長（Zero real growth）等の原則が適用されることが多いが[40]、基本的にはプロジェクトの実施等を確実にするためにも、各国からの任意拠出金を確実に回収できることが重要である。

以上、公開文書を基に特に核物質防護条約改正第 1 回レビュー締約国会議を念頭に置いて、2021 年 9 月に開催された IAEA 総会の文書等を基に、核セキュリティ関係の見通し等を見た上で 3 点の提案をさせて頂いた。第 1 回レビュー締約国会議は核物質防護条約改正発効後に最初に実施されるということもあり、その準備過程では試行錯誤も少ないと思われるものの、規制当局や事業者を含む各国関係者のみならず IAEA 等の核セキュリティに関係するステークホルダーが共に協力して最終的に成功裏に開催されることが期待される。

---

[37] 不正アクセス事案に関する報告（中間報告）（概要）、原子力規制庁、2021 年 5 月。URL: https://www.nsr.go.jp/data/000352786.pdf.
[38] Greenpeace fait s'écraser un drone sur un bâtiment de la centrale nucléaire du Bugey, Ouest France, 3 Juilet 2018, URL: https://www.ouest-france.fr/environnement/greenpeace/greenpeace-fait-s-ecraser-un-drone-sur-la-centrale-nucleaire-du-bugey-5860783. リヨン郊外にある Bugey 原発敷地の飛行禁止区域にドローンを飛ばし、使用済み核燃料の貯蔵プール建屋外壁にドローンを命中させる事件が発生。
[39] 警察庁、「小型無人機等飛行禁止法関係」。いわゆるドローンは、日本では航空法（昭和 27 年法律第 231 号）、重要施設の周辺地域の上空における小型無人機等の飛行の禁止に関する法律（平成 28 年法律第 9 号。以下「小型無人機等飛行禁止法」という。）の２つの法律で規制されている。URL: https://www.npa.go.jp/bureau/security/kogatamujinki/index.html
[40] supra note 5, p.1. IAEA 事務局長は通常予算につき次期二か年予算においては、実質ゼロ成長（Zero real growth）を提案している。