核セキュリティ確保の強化に向けて 事業者、規制当局、学会等間の透明性を確保した連携

日本原子力学会
核不拡散・保障措置・核セキュリティ連絡会

核不拡散・保障措置・核セキュリティ連絡会では、福島第一原子力発電所事故を契機に、我が国における核セキュリティ強化に向けた今後の課題について議論を重ねてきたが、このたび提言をまとめたので報告する；事業者自らが、核セキュリティの重要性についての認識を、組織の上層部から末端まで浸透させること、すなわち「核セキュリティ文化」の構築を図ることが必要である。また、核セキュリティ上重要な情報の秘密保持を進める場合、安全において重要とされる透明性とのバランスを図ることが重要であるが、それに関する制度設計と運用の検討を行うべきである。さらに、定期的に見直された設計基礎脅威(DBT)に伴う実効性のある性能試験・訓練の実施などの継続的な改善、及び次世代を担う人材の育成に際し核セキュリティの知識・経験をもたせること等が重要である。一方、規制当局、事業者、警察、海上保安庁、自衛隊など事案に応じた役割分担・相互連携協力および対応要領を明確にしていくこと、そして国家安全保障の中での核セキュリティの位置づけの検討が望まれる。放射性同位元素(RI)に対するセキュリティ強化においてRIの量や放射能強度に応じた等級別規制を取り入れること、内部脅威に対する人的管理面における信頼性確認の早期の導入、及び核鑑識対応体制の整備等、関連する法整備を進める必要がある。そして、原子力における3S(安全 Safety, 保障措置 Safeguards, セキュリティ Security)確保のための国側組織については、日本原子力学会、核物質管理学会等の関連学会が協力して、安全と核セキュリティの両者が、互いに他者で要求される規制要件を理解し、設計段階から両者融合した考え方を取り入れていくこと、現実的かつ実効性のある核セキュリティのための核物質の計量及び管理の検討、魅力のある研究分野とするためにも論文成果が発表できる環境を整え、業績を正当に評価する仕組みの検討等が求められる。

1. はじめに

2011年3月11日の東日本大震災に起因する福島第一原子力発電所の事故(以下、福島事故と略称)によって、いまだ多くの方々が避難生活を余儀なくされる等の困難な状況にあることは、原子力に携わってきた者として痛恨の極みである。福島事故は地震と津波による複合災害の結果として発生した事故であり、原子力安全の観点からの種々の課題に対する改善の議論が進められている。

核セキュリティの分野では、9.11の同時多発テロ事件発生を受けて米国NRCは、B.5.b(爆発や火災によって、プラントが大きく損傷した状況下での、炉心冷却、格納容器閉じ込め機能、使用済み燃料プール冷却能力維持・回復のための手引き)を定め、我が国にも情報共有を図った。日本国政府として、その重要性を強く認識し、政府と事業者が一体となって真剣かつ迅速に取り組むことができているれば、事故時の対応にも違いがあったとの観測がなされている。一方、福島事故によって明らかになった脆弱点が、テロ攻撃の標的となる可能性も否定できない。福島事故の反省を今後の種々の対策の実施に反映させるためには、原子力安全のみならず、核セキュリ

ティの側面を含めた対策を検討していく必要がある。

本連絡会では、上記の観点を基に、我が国の今後の核セキュリティについて考慮すべき基本的事項について議論し提言を取りまとめた。

2. 核セキュリティ強化への取組みと改善

(1) 核セキュリティに対する認識

核セキュリティとは、「核物質、その他の放射性物質、その関連施設及びその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行為の防止、検知、及び対応」を指す[原子力委員会原子力防護専門部会、2011]^{1,2)}。核セキュリティでは、核物質及び核物質を取り扱う原子力施設に対する防護である従来の核物質防護に加え、その他の放射性物質及びその関連施設へと防護を講じるべき対象が広がっている。

我が国では、核物質防護のみが議論されていた時期を含めて、原子力安全と同等の重要性の認識が核セキュリティに対して持たれているとは残念ながら言い難い。このことは、(1)上記のB.5.bへの対応の鈍さ、(2)原子力行政において、核セキュリティに実質的なイニシアティブをもつ体制がなかったこと、(3)原子力に関連する教育を担う大学において核セキュリティに関連する科目がごく最近までほとんど存在しなかったこと、(4)核物質防護管理者の専門性を確認する国家試験が存在しないこと等の事例が示している。核セキュリティを重視した人材育成を目標とする大学の取組については、徐々に進展して

Toward Ensuring Nuclear Security; Cooperation amongst plant operators, regulatory authorities, and related academic societies with assuring sufficient transparency: Nonproliferation, Safeguards, and Nuclear security Communication Group.

(2013年 1月15日 受理)

きており、その成熟が今後も期待される。

原子力安全に関しては、1986年のチェルノブイリ原子力発電所事故以降、安全文化(safety culture)の重要性が指摘され、我が国においても種々の取組が実施されてきた[原子力安全・保安院, 原子力安全基盤機構, 2007]⁹⁾。一方、核セキュリティに関しては、セキュリティ文化(security culture)について議論されるようになったのは、国際的に見てもごく最近のことである。安全文化に関する重要な報告書である INSAG-4[IAEA, 1991]⁴⁾が発行されたのが1991年であるのに対し、セキュリティ文化に関する IAEA の実施指針(implementing guide)[IAEA, 2008]⁵⁾が発行されたのが2008年であることから見ても、核セキュリティに対する取組が国際的にも遅れてきたことがうかがえる。

安全文化の醸成のための出発点は、安全を最優先するという認識を組織の上層部から末端に至るまで浸透させることであるが、核セキュリティにおいては、防護担当者に任せるべき事項であり、自身は当事者ではないという認識が強かったのではないと思われる。核セキュリティについても安全と同様に文化の醸成に向けた取組が必要である。原子炉等規制法が2012年3月に改正され、経営者責任が法令に規定されており、今後、上記に示す上層部から末端までの認識・情報の共有化が進められることが期待される。

(2) 秘密保持と周知のバランス

我が国においても、英国やフランスに再処理を委託していたプルトニウムの輸送時や、核物質防護条約の批准時、二国間原子力協力協定の締結及び改定時等には、核セキュリティに関連する詳細な検討が実施された。しかし、その検討内容は直接の関係者のみが知るところとなっており、広く一般的な議論とはなっていない。その背景には、核セキュリティに関連する機微な情報について、秘密保持が要求されるという制約があることが挙げられる。秘密保持が要求される理由は、核物質や原子力施設の全ての情報を公開すれば、テロ攻撃を企図している者に対して有益な情報を与えることになり、核セキュリティに対するリスクを高める結果となるからである。

2005年の原子炉等規制法改正によって、核物質防護に係る秘密について、罰則を伴う秘密保持が義務付けられた。しかし、核セキュリティに関連する情報を秘密情報として取り扱うためには、当該情報が核セキュリティの観点から秘匿を要するものであるかどうか十分に検証される必要がある。その際には、原子力基本法第2条が謳っている「自主・民主・公開」の平和利用三原則の一つである公開の原則も考慮し、秘密保持と周知のバランスを取る対策を検討すべきである。

秘密情報の範囲についても、画一的に定めるのではなく、職務上の「知る必要性(need to know)」や個人の信頼性の確認状況に応じて、情報ごとに対象者を何段階にも分けて定めるべきである。また、ある情報については、

時間の経過とともに、秘匿する必要性がなくなる可能性もある。その際には、情報秘匿の条件を適宜変更し、公開可能になった情報は順次公開すべきである。我が国では、原子力の分野のみならず、一般的に秘密保持の法的枠組の整備が十分には進んでいない。先行事例の蓄積が進んでいる諸外国の事例を参考にしつつ、制度設計及び運用の検討を行うべきである。また、秘密保持と情報共有とのバランスも重要で、効果的な核セキュリティ体制を確立するためには、他事業者における良好事例を事業者が共有して広く浸透させることが必要で、このために規制当局が積極的な役割を行うことが求められるだろう。

(3) 継続的改善と訓練

核セキュリティで考慮する脅威は、一定のものではなく、時間の経過とともに変遷する。したがって、脅威の変遷を反映した DBT の定期的な見直しが必要である。DBT の見直しに伴い、対抗するためのセキュリティ対策の実効性についても、想定した防護性能が発揮されるかどうかを性能試験の実施等によって実戦的に確認し、継続的に改善していくことが求められる。米国 NRC では、施設者に対し、シナリオを周知することなく仮想のテロリストと防護部隊との間での実地訓練(Force-on-Force 演習)を定期的に行うことを義務付けることにより改善が図られている。こうした継続的改善の実施のためには、防護システムや関連制度を長期的に見据えることができるように、核セキュリティを専門に担当する者が事業者や規制当局及び治安当局等に求められる。こうした点を考慮した人材育成・投与の検討が求められる。

3. 核セキュリティ対応体制の整備

(1) 役割分担と責任の明確化

核セキュリティの観点からは、核物質の盗取や原子力施設に対する妨害破壊行為等の核セキュリティ事案が発生しないようにするための事前の防止措置、核セキュリティ事案発生時の検知、通報及び行為の遅延等の措置、盗取された核物質等の発見及び奪還措置、放射線影響が発生した場合の緩和及び最小化等の事後的な対応措置等、広範な事項が要求される。

上記のような広範な事項は、事業者(輸送の場合の運送事業者等を含む)と規制当局のみで対応できるものではない。近年、核セキュリティ強化のために多くの対策が事業者要求されているが、現行の法的枠組の下では、事業者が対処できる範囲には限界がある。銃火器での武装が許されている警察や海上保安庁等の治安当局を含め、各々の役割分担と責任を明確化する必要がある。また、関係各機関が具体的な対応要領を持ち、相互の緊密な連絡協力体制を構築しなければならない。その際には、国際的犯罪が増加していることを踏まえ、国際的に通用する対応要領が整備されることが求められる。また、事前の想定を超えた事態に柔軟に対応できるように、状況に応じた対応を可能にする補完的資料を準備することが重要である。

(2) 国家安全保障の中での核セキュリティ

核セキュリティで考慮するのは主に潜在的な脅威者についての詳細な記述である DBT に対する対応であり、有事の際の原子力災害(武力攻撃原子力災害)に対する対応は国民保護法の下で実施されることになっている。しかし、両者の間の連続性の確保の問題や、対応態勢の円滑な移行の問題については、十分な議論がなされ、共通の理解が得られているとは言い難い。その前提として、国家安全保障の中で核セキュリティをどう位置付けるかについて、議論と関係者間での認識の共有が必要である。また、核セキュリティにおける有事の際の、省庁等関係組織間の協力体制、分担、リーダーシップについても、新原子力規制庁を中心に早急に再検討がなされる必要がある。

(3) 放射性同位元素(RI)に対するセキュリティ強化

核セキュリティの特徴は、従来の核物質防護では核物質のみに焦点を当てていたのに対し、放射性物質のばらまきや放射線の発散を伴う妨害破壊行為を踏まえて、核物質ではない RI 等の放射性物質を含めたセキュリティを考慮する点である。RI は放射線障害防止法によって規制されているが、現在の放射線障害防止法では、セキュリティに関しては簡単な規定しか定められていない。

α 核種や β 核種は比較的遮蔽が容易であるが、裏を返せば不法所持の検知が難しいということになる。また、核物質よりも放射線強度が高い RI は数多く存在することから、放射性物質のばらまきや放射線の発散を伴う妨害破壊行為の観点からは、核物質に準じたセキュリティ対策が適切に講じられるような規制強化が図られるべきである。

一方、RI の規制については、医療関係者等の原子力事業者ではない多くの者が関係する。したがって、一律の規制を実施するのではなく、RI の量や放射線強度に応じて等級別取組(Graded Approach)に基づいた規制が必要である。

(4) 内部脅威対策

内部脅威とは、「原子力施設の内部で働く従業員等による不正行為等により生ずる脅威」を指す[総合資源エネルギー調査会原子力安全・保安部会原子力防災小委員会, 2005]。内部脅威対策として、①内部脅威者が不正行為等に及ぶのを物理的に阻止する物的防護、②内部脅威者の枢要区域への侵入の排除及び破壊工作に用いる工具や核物質の不法持ち出し等を阻止する出入管理、③潜在的な内部脅威者の組織及び区域からの排除、行動観察等を通じた不正行為等の抑止を目的とした人的管理という3つの手法がある[総合資源エネルギー調査会原子力安全・保安部会原子力防災小委員会, 2005]⁶⁾。

信頼性確認とは、「不正行為等に及びそうな人間(要注意人物)をあらかじめ把握するための情報の収集と分析」を指す[総合資源エネルギー調査会原子力安全・保安部会原子力防災小委員会, 2005]。信頼性確認は、人的管理対策の一つであり、米国や英国等の諸外国ではすでに

整備・運用がなされている。INFCIRC/225/Rev.5においても、核物質又は原子力施設に係る機微情報を取り扱う者や枢要な施設・設備にアクセスする者を対象とした信頼性確認の実施が勧告されている。我が国においても、信頼性確認についての議論は行われてきた[総合資源エネルギー調査会原子力安全・保安部会原子力防災小委員会, 2005]が、基本的人権との関係や、制度の実効性確保の難しさ等もあって、2013年1月現在においても導入はなされていない。

一方、INFCIRC/225/Rev.5が対象とする核物質及び原子力施設に係る分野における信頼性確認の導入を目指して、具体的な制度についての議論を開始するべきという提言がなされた[原子力委員会原子力防護専門部会, 2012]。基本的人権は憲法上保証された権利であり、信頼性確認の導入は容易ではないと考えられるが、可能な限り早期な導入を目指した議論の進展が期待される。また、信頼性確認は、セキュリティ上重要な職務に就いている者への処遇等と関連付ける等、信頼性確認が必要とされる者にとっても動機付けがなされるような施策が必要である。

(5) 核鑑識への対応

2010年4月、米国ワシントン DC で開催された、核セキュリティサミットでは、我が国は核鑑識の技術開発に関連する国際協力を行うことが声明に記載されている。また、2012年の第2回核サミットでのソウルコミュニケにおいて、核鑑識の能力を構築、強化するための国際協力及びIAEAとの協力がうたわれた。サミットにおける合意及び我が国首脳による国際的なコミットメントを踏まえ、現在、我が国でも核鑑識技術を確立し国際的に共有していくために、核鑑識技術確立に向け取り組んでいる⁷⁾が、鑑識活動を実質的に有効なものにするためには、技術開発だけでなく的確な対応体制を構築することが不可欠である。例えば、国境などで核物質が確保された場合や核テロやダーティボムによるテロが発生した場合を想定し、関係機関の連携による的確かつ迅速な協力・対応体制の整備が求められる。また、核物質・放射性物質分析結果と、一般的(伝統的)な鑑識分析結果との効果的なリンクなど、全体を一元的に扱い解析評価するための体制作りも求められる。さらに、今後、核鑑識機能をより有効なものにするためには、上述の体制整備とともに、法整備についても取り組んでいくことが重要と考える。商業的規模で核燃料サイクルを有する我が国としては、核の鑑識に関しても国際的に大きな役割を担うべく、的確な体制確立が強く望まれる。

(6) 法律や規則の充実

以上のような対策を実行的に確保するためには、その基礎となる法令の整備が必須である。INFCIRC-225 rev 5及び福島第一原子力発電所の事故の教訓を反映する核セキュリティを含めた核物質防護強化のための原子炉等規制法の改正が、2012年3月に行われた。今後、法令改正

を受けての各事業者による具体的な展開が重要である。

なお、未整備部分の信頼性確認制度の確立は、原子力分野だけでなく国全体としてのバランスある制度づくりが望まれる。

4. 3S 確保に向けた国と関連学会との連携

(1) 安全要件とセキュリティ要件の調整

現行の原子力施設設置時の審査は、主として安全の観点から実施されていることから、安全要件とセキュリティ要件が相反的である状況が生じる可能性がある。相反的な場合の例としては、内部脅威等への対策として建屋内を区画分けして出入管理することが、事故時等の建屋内の設備へのアクセスや建屋外への避難の遅れにつながる事が挙げられている[原子力委員会原子力防護専門部会, 2012]。安全要件とセキュリティ要件が相反的な場合には、安全の担当者とセキュリティの担当者の双方が相互の要件に対する理解を深め、妥協点を見出す努力が求められる。

施設設置後に安全要件とセキュリティ要件が相反的である状況が生じた場合には、その解決に困難を伴うおそれがある。したがって、施設の設計段階からセキュリティ要件も考慮に入れる考え方(security by design)が重要であり、諸外国の動向も視野に入れつつ、我が国も議論を深めていく必要がある。security by design については、国際的な議論もまだ成熟しているとは言えない状況であるが、IAEA 事務局長の核セキュリティに関する諮問委員会(AdSec)が、基本的な考え方をまとめた AdSec 文書を2013年6月をめどに発刊することを計画しており、議論が深まれば、施設の設置許可要件に取り入れることも検討すべきである。他方、核セキュリティ対策と原子力安全対策とのシナジーにも注目すべきである。万が一、核セキュリティ事象が起こって、放射能放散という事態になれば、核セキュリティのために、固有な危機対応計画と防災計画が必要とされると考えるよりも、安全分野での防災対策が即発動される必要があると考える。

(2) セキュリティのための核物質の計量及び管理

核セキュリティのための核物質の計量及び管理は、内部脅威者による盗取の抑止及び検知を支援する対抗手段として検討が進められている。現在 IAEA では、核セキュリティのための核物質の計量及び管理のガイダンスの出版準備中の状況にある。核セキュリティの観点からの核物質の検知限界や検知時間等について決める必要性が生じる可能性がある。一方、我が国では、核セキュリティの観点からの核物質の計量及び管理を担当する行政機関は、原子力規制庁になると思われるが、本手段の導入に当たっては、保障措置のための計量管理と核セキュリティのための計量管理は、目的が全く違うので(保障措置は1SQ(有意量)の転用を転換時間に対応する探知時間で探知すれば良いのに対し、核セキュリティの場合は、より少量の核物質を頻繁に探知できるようにしなければならない。)、両者の計量管理が別々に導入されるの

でなく、互いに相補的に導入され、事業者に過度な負担がかかることのないように、実効性と必要性を考慮した議論を踏まえた導入の検討が必要である。

(3) セキュリティ分野の人材育成

核セキュリティ対策を確実に実施していくためには、関係者が核セキュリティに関する十分な知識と経験を有していなければならない。しかし、実際の核セキュリティ事案で経験を積むことを想定した教育訓練のプログラムはありえない。したがって、核セキュリティに関連する多くの分野の知見を取り入れられるような人材育成方法を検討すべきである。原子力関係者には、セキュリティに関連する基礎知識が十分ではない場合が多い一方で、治安当局の関係者には、原子力に関連する基礎知識が十分ではない場合が多い。両者がそれぞれの知識を共有できるような教育訓練が重要である。その際には、机上の学習のみならず、実戦的な演習プログラムを取り入れるべきである。

また、人材育成という観点では、これからの世代を担う若い世代にとって、核セキュリティに関する業務が魅力的なものにならなくてはならない。核セキュリティについての国家資格を作り処遇等と関連付ける、論文等の成果が発表できる環境を作る等、業績を正に評価するための施策が重要である。

5. 終わりに

福島第一発電所事故後に、原子力事業者側と規制側それぞれにおいて徹底した安全確保への取組が求められることとなった。一方、欧米各国に比べると実施経験が乏しい我が国の核セキュリティについては、今後、事業者、規制側組織、研究開発機関、及び関連学会等の間で、それぞれの役割を確認するとともに有機的な連携を図っていくことが、何よりも必要である。このために当連絡会は微力ながら連携強化の一翼を担うべく今後も努力していきたいと考えている。

本稿は、核不拡散・保障措置・核セキュリティ連絡会の総意としてまとめたものである。

(執筆担当：谷 弘、稲村智昌(電中研)、

久野祐輔(原子力機構・東大)、鈴木美寿(原子力機構))

— 参 考 文 献 —

- 1) 原子力委員会原子力防護専門部会、核セキュリティの確保に対する基本的考え方、(2011)。
- 2) 原子力委員会原子力防護専門部会、我が国の核セキュリティ対策の強化について、(2012)。
- 3) 原子力安全・保安院、原子力安全基盤機構、規制当局が事業者の安全文化・組織風土の劣化防止に係る取組を評価するガイドライン、(2007)。
- 4) IAEA, Safety Culture, (1991)。
- 5) IAEA, Nuclear Security Culture, (2008)。
- 6) 総合資源エネルギー調査会原子力安全・保安部会原子力防災小委員会、原子力施設における内部脅威への対応について、(2005)。
- 7) 久野祐輔、桜井聡、堀雅人、核鑑識技術の確立にむけて、原子力学会誌(ATOMOS), Vol.53, No. 4, 21-25(2011)。