原子力施設の妨害破壊行為に対抗する防護措置についての 新たな評価制度

板倉 周一郎^{1,*†}, 中込 良廣²

New Evaluation System for Antisabotage Physical Protection

Shuichiro ITAKURA^{1,*†} and Yoshihiro NAKAGOME²

¹Graduate School of Energy Science, Kyoto University, Yoshida-Honmachi, Sakyo-ku, Kyoto 606-8501, Japan

²Research Reactor Institute, Kyoto University, Kumatori-cho, Sennan-gun, Osaka 590-0494, Japan

(Received November 5, 2006 and accepted in revised form August 23, 2007)

The discussion on an appropriate level of physical protection has not been elaborated so far because of the confidentiality of its nature, thus resulting in a lack of consensus on this issue. In view of this context, a new system for the evaluation of antisabotage physical protection systems is proposed in this paper, in which we introduce openness to a certain extent in the process of the evaluation. The proposed system is composed of the following three elements; (1) establishment of an evaluation basis threat (EBT), which should be less strong but more likely to occur than the design basis threat (DBT); (2) employment of realistic standard scenarios in the process of evaluation; (3) disclosure of results of evaluation implemented based on the above EBT and standard scenarios. It is expected that this considerably open system will foment peace of mind among citizens as well as create a deterrent effect that would minimize the occurrence of sabotage on nuclear facilities.

KEYWORDS: *physical protection, evaluation, terrorism, sabotage, insider, INFCIRC225, design basis threat (DBT)*

I. 緒 言

一般に犯罪対策においては、「どこまで対策を強化すればよいのか?」という問に対する客観的な答, すなわち十分条件を示すことは困難である。「これで十分である」という説明を対外的に行うと, その情報をもとに不備な点を狙う犯罪者が現れる可能性が発生するからである。核物質および原子力施設を不法行為実施者から防護する措置(以下「核防護^{a)}」という。)においても, 個別の施設の防護水準についての情報は厳重に管理されている^{b)}。これは, 防護の内容やその水準について情報が明らかになれば, 妨害破壊行為を企図する者(以下「妨害破壊者」という。)を利用することになると考えられるからである。その結果とし

て, 当該施設が十分な水準で防護されているかどうかは, 規制当局と事業者以外の者にはわからないことになる。

核防護については, 国際原子力機関(IAEA)が策定したガイドラインである INFCIRC/225^{c)}において, 施設が内包する核物質の形態, 量に従い, 講じるべき具体的な防護

¹ 京都大学大学院 エネルギー科学研究科

² 京都大学 原子炉実験所(現 京都大学名誉教授)

* Corresponding author, E-mail: shuichiro.itakura@cao.go.jp

† 現在, 内閣府政策統括官(科学技術政策・イノベーション担当)付参事官(資源配分/国際政策担当)(Director for Resource Allocation & International Affairs, Bureau of Science and Technology Policy, Cabinet Office)

a) 日本では, 従来「核物質および原子力施設の物理的防護」の意味を表す用語として, 旧来の IAEA ガイドライン(INFCIRC/225)の表題に沿って, 「核物質防護」という用語を用いている。しかし, 最新の IAEA ガイドラインの表題に「施設」の防護が加わったことを踏まえ, 本報では, その点をより明確化するため, 敢えて「核防護」という言葉を用いることとした。

b) 原子力に関する情報公開については他分野と比べても取り分け要求が厳しい。しかしながら, 行政機関の保有する情報の公開に関する法律において, 「公にすることにより, 犯罪の予防, 鎮圧又は捜査, 公訴の維持, 刑の執行その他の公共の安全と秩序の維持に支障を及ぼすおそれがあると行政機関の長が認めることにつき相当の理由がある情報」については, 開示請求の対象外とできる旨が規定されていることから, 核防護に関わる情報は, この規定に基づき, 例外的に, 情報の開示が, 原則として行われていない。

c) 「INFCIRC」は, IAEA の文書番号である。1975年に策定された後, 順次改定が行われ, 現行のガイドラインは, INFCIRC/225/Rev. 4 である。

措置が詳細に示されている。しかしながら、その防護措置がなぜ必要か、さらには、そのような防護措置でなぜ十分なのかについての説明は INFCIRC/225 には示されていない。核原料物質、核燃料物質及び原子炉の規制に関する法律(以下「原子炉等規制法」という。)の下に構築される我が国の核防護制度においても、基本的には INFCIRC/225 に準拠して、その個々の防護措置を定めている。ここにおいても、講じるべき個別の措置が示されているのみであり、それが十分であることを示す根拠は示されていない。

本来各国の状況を勘案して設定されるべきセキュリティ対策において、個別の防護措置の必要性および十分性の説明の多くを国際機関の統一的なガイドラインに委ねている現行の核防護制度においては、講じられている核防護措置について、十分であると国民が納得して安心感を抱くことは難しいと考えられる。安心感が得られないことは、過剰な防護の要求にもつながる。

本報では、上記の問題意識の下、原子力施設に対する妨害破壊行為に対抗する防護^{d)}の水準について、一部の情報公開を導入しながら国民のコンセンサスを形成し、安心感を醸成する方策を提唱する。なお、核防護制度は、個々の国家で異なる警備制度を前提として、それぞれの国情に沿って整備・構築されることから、制度自体が各国で異なる。したがって、本報では、我が国における核防護制度のあり方に範囲を限って論じることとする。

II. 防護に関する一部情報開示のメリット

防護の内容やその水準について情報が明らかになれば、妨害破壊行為を企図する者は、その情報をもとに侵入方法や攻撃方法を検討できる。従来、このような考え方に立って、防護水準についての情報は厳重に管理されてきた。防護の能力の最大限のレベルが明らかになれば、まさに妨害破壊者側を利することになる。しかしながら、核防護は1つの措置で構成されるものではない。防護能力の限界まで余裕を保ちつつ部分的な情報開示をする場合、いい換えれば、「少なくともこの程度は満たしている」といった形で防護能力の一部の情報を示した場合は、必ずしも妨害破壊者側を利するとは限らないと考えられる。

具体的な事例としては、家屋への侵入に対する防犯対策において、防護性能の情報は我が国では積極的に公表されていることが挙げられる。警察庁等で構成される官民合同会議^{e)}が進めている防犯対策においては、ドア、窓、シャッターなどに用いられる建物部品の防犯性能を評価することを決定した¹⁾。その上で、一定の防犯性能があると評価

した建物部品を公表するとともに²⁾、共通標章を製品に貼付することとしている³⁾。検査基準についても、侵入窃盗の被疑者を対象とする調査⁴⁾において、「攻撃の開始から5分間⁵⁾以上人体が通過できる状態にならなかったと判定された試験体は、試験に合格したものとする。」と公表されている⁶⁾。「5分以上掛ければすべての侵入者があきらめるとは限らない。5分もちたえれば本当に十分なのか？」という懸念があるにも関わらず、具体的な防護能力を公表している。

セキュリティに関する情報を秘匿することは、絶対に守らなければならない原則ということではない。このことを踏まえ、以下本章では、核防護措置において、防護水準に関する情報を一部開示するメリットについて述べる。

1. 安心感の醸成

原子力安全の分野では、安心感を醸成するために、説明責任を果たすとともに情報を公開することは当然のこととされている。現行の原子力政策大綱⁶⁾においては、安全確保のための活動に係るコミュニケーションを行うべきこと、その中で情報提供を行っていくべきことが示されている⁸⁾。また、2007年3月に原子力委員会が発した「原子力の安全確保に関する透明性と信頼の確保について」と題する声明⁷⁾においても、「電気事業者の安全確保のためのシステム及びそのシステムに基づく活動が国民から信頼されるためには、(中略)安全確保に関する取組を国民や地域社会に対する説明責任を十分に果たしつつ着実に進め、その内容についての相互理解活動を進めていくことが必要と考えます。」と述べられている。これらの例に示されるように、安心感醸成のためには、単に基準に適合していることのみを示すだけではなく、行政当局または事業者が一部の情報を公開しつつ説明責任を果たすことが必要である。

原子力施設が不法行為に対してしっかりと防護されている、との安心感が国民の間に醸成されるためには、本来な

^{d)} 侵入窃盗の被疑者のうち、「侵入するのに時間が5分以上掛ければ侵入をあきらめる」と回答したものが約7割に上るとする調査結果が出ていることを参考に5分間という値が設定された。

^{e)} 原子力委員会が平成17年に策定した原子力政策大綱においては、「安全確保のための活動に係るコミュニケーション」について、次のように述べられている。「国、事業者等は、安全確保のための活動を的確に実行していることを立地地域や周辺地域の住民を含む国民に説明し意見交換して、相互理解の形成に寄与するリスクコミュニケーション活動を行う責任を有する。国は、安全審査の過程における安全審査書の公開と意見募集、行政処分に係る判断基準の制定・改定時における意見募集という取組を引続き重視していくべきである。また、国は、地域社会に対して、規制活動に関して一般のみならず個々具体的に、適宜に説明し、意見交換していくことが重要である。さらに、国は、住民安全の責任を有する地方公共団体に対して、安全規制に係る各種の判断基準等の制定・改定に関する適切な情報提供を行うとともに、規制活動状況を説明し、また、その意見等を求めて、共通理解を深めることが重要であり、引き続き努力を重ねていくべきである。」

^{d)} 核防護措置は、原子力施設に対して講じる措置と、輸送中の核物質に対して講じる措置があるが、本報では前者に焦点を当てて論じることとする。

^{e)} 「防犯性能の高い建物部品の開発・普及に関する官民合同会議」。警察庁、国土交通省、経済産業省の課長級メンバーと建物部品関係の民間団体の代表メンバーから構成される。

らば、原子力安全と同様に、行政当局または事業者が説明責任を果たし、情報を公開するべきであるが、核防護の場合、個別施設の防護水準についての情報は厳重に管理されていることから、国の規制がIAEAのINFCIRC/225に準拠していることをもって説明するしかない状況にある。IAEAは、原子力安全や保障措置の分野を始め、原子力の各分野で高い権威を有する存在であることは疑いない。しかしながら、核防護は、原子力安全や保障措置と異なり各国の国情に大きく依存することから、IAEAの示す核防護方策は強制力のない“ガイドライン”であるINFCIRC/225の策定に留まり、核防護に係る規制は各国の規制当局に委ねられている。各国の国情により異なる措置である核防護においてこそ、各国の行政当局が、積極的に説明責任を果たしていくことが求められるはずである。

安全・安心な社会を希求する国民の声が高まる昨今、核防護についても、一定限度内で部分的に情報を開示しつつ、核防護水準についての開かれた議論を行うことによって、初めて国民の安心感が醸成されるものと考えられる^{h)}。

2. 防護水準についてのコンセンサス形成

2001年9月11日の米国同時多発テロ(以下「9・11テロ」という。)以降のテロリズムの脅威の高まりの中、原子力施設の防護の強化が国際的な要求となり、IAEAにおいても核セキュリティ強化の取り組みが精力的に進められている。原子力のみならず、テロリズムの対象となる可能性の高い枢要かつ大規模なインフラストラクチャー、いわゆるクリティカル・インフラストラクチャー全般に対する防護措置への関心が世界的に高まっている。公共輸送機関、エネルギー供給事業にみられるようにクリティカル・インフラストラクチャーを運営する組織も民間機関である場合が多い。脅威の設定自体は、取り扱う情報が機微であるため公的機関が担うが、これに対応する防護策は民間機関側に委ねられることが多い。このような状況下において、セキュリティ対応に関する民間機関側の情報不足に起因する過剰負担感が深刻になっており、これを解決するために民間機関と公的機関との間の“情報共有に基づく協力”が重要であるとの認識が、国際的にも共有されつつある⁸⁾。

セキュリティに関する論調の多くは、脅威の大きさ、強さについて公的機関側から警鐘を鳴らすものが多い。公的機関と民間機関の両者間の対話に基づき、かつ国民も交えて防護の水準についての一定程度のコンセンサスが形成さ

れないことにより、その国の実情を超えた過敏かつ過剰な対応をしなくて済むことが期待される。我が国の現状としては、脅威の強さについての警鐘が鳴らされるたびに部分的な防護措置強化が行われ、時間の経過とともに人々の関心が低下した時点で目立たぬように防護水準がもとに戻されている。

防護水準の目安となるものとしては、INFCIRC/225の最新版であるINFCIRC/225/Rev. 4において導入が勧告された設計基礎脅威(DBT)が挙げられる。INFCIRC/225/Rev. 4は、DBTを「核物質防護システムの設計及び評価に対し、核物質の不法移転又は妨害破壊行為を企てようとする内部者及び/又は外部敵対者の特性及び性格」として定義した上で、これをもとに原子力事業者は核防護措置を設計し、国はこれを評価することが勧告されている。このことを受けて、我が国の核防護制度においても、政府の規制当局がDBTを設定し、これに基づき事業者が核防護措置を講じるよう義務付けるとともに、核物質防護規程ⁱ⁾の遵守状況を規制当局が検査する制度を導入するため、原子炉等規制法が2005年に改正された。しかしながら、防護水準を決める上での基礎となるDBTは非公開とされ^{j)}、また遵守状況検査における検査の基準自体も非公開とされている。DBTが非公開である以上、上述のように過敏・過剰な対応になる恐れがある。

INFCIRC/225/Rev. 4の勧告に基づき、評価が導入される結果、防護水準についてのコンセンサスが評価を通じて形成されとの考え方もあろう。原子力安全の分野では、原子力安全委員会による安全審査が、公開された安全審査指針に基づき、事業者と一次規制官庁以外の立場の専門家により行われており、透明性が高いといえる。一方、核防護においては、この点について、次に述べるような課題がある。

一般的に、達成目標の設定のためには、達成したことが明確となる基準が必要であり、可能ならば定量的な概念の導入が望ましい。核防護システムの評価における定量的概

^{h)} 原子炉等規制法体系下に設計基礎脅威(DBT)を導入するための法改正を行うに先立って原子力委員会が議論をした際にも、「適切なDBTであることを確認するために、リスクアセスメントを実施したほうが良い。公開の場で議論できるのは限られた内容になるので学識経験者による委員会など、第三者の判断を入れる仕組みを用意しておく方法もある。」との意見が、原子力委員会委員長から示されている(2004年11月9日第43回原子力委員会議事録)。

ⁱ⁾ 原子炉等規制法に基づき、核物質防護措置が必要な事業所ごとに事業者が定め、主務大臣に提出し、認可を受けることを義務付けられている規定。防護業務従事者の職務および組織、防護区域の設定ならびに巡視および監視、防護区域の出入管理、核燃料物質の管理、防護のために必要な設備および装置の整備および点検、連絡体制の整備、情報管理、教育訓練、緊急時対応計画等に関することなどを定めることとなっている。

^{j)} 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報告「原子力施設における核物質防護対策の強化について」によれば、「DBTには、核物質防護システムの構築の前提となる機微情報が含まれることから、その内容は秘密扱いとし、一般には開示しないことが適当である。」との考え方が示されている。また、文部科学省研究炉等安全規制検討会報告書「試験研究用原子炉施設等の安全規制のあり方について」によれば、「DBTを始めとする脅威情報や、原子力施設における具体的な防護情報などは、核物質防護の水準を保つ上で、国、事業者等における情報管理の徹底が必要不可欠である。」とされている。

念の導入については、具体的には、タイムライン分析や脅威到達時間評価といった手法が取られている^{9,10)}。これらの手法は基本的には同じものと考えられており、施設への攻撃に対する防護能力を測定する基本的なアプローチとして、米国エネルギー省などで以前から開発が進められてきたものである^{k)}。分析の目的は、外部からの不法侵入者が破壊対象に到達するまでの所要時間が、外部支援部隊(我が国においては、警察警備当局)が到着するまでに要する時間を超えるよう、不法侵入者の侵入行為を遅延させる能力を有する核防護措置および態勢であるか否かを評価することである。具体的な手法としては、早期に検知する確率を算出するものであり、侵入者の想定経路上のいくつかのポイントで検知が失敗する確率を掛け合わせて、全体の検知失敗の確率を導出することにある¹¹⁾。この分析手法は、想定される脅威、攻撃シナリオを網羅的に捉えることを前提としていることから、対象施設が複雑になるに従い、分析手法は複雑なものとなり、誤差・不確定要因の拡大は避けられない。一方、インサイダ(内部脅威者)のような機械的に算定し難いリスクや、9・11テロ以降に新たに考慮に入れざるを得なくなった、いわゆる自爆テロによる事案も生じてきていることから、ある特定施設の防護措置全体の評価を行うには、定量的なアプローチだけでは不十分な状況になってきている。このことから国民の安心感醸成のためには、防護対策について、定量的評価のほかに、心理的側面を含む定性的な評価を加えて総合的に評価することが重要になろう。定性的な評価に当たっては、具体的には複数の核防護や犯罪心理学分野の専門家から構成される組織による多角的な分析および評価が有効となるであろう。

3. 犯罪抑止の効果

一般的に、犯罪防止対策を講じていることをアピールすることにより、一定の犯罪抑止効果が期待できるとされる。身近な例でいえば、街中での監視カメラの設置が挙げられよう。繁華街などで目立つ場所に監視カメラを設置した結果、犯罪件数自体が減少することが確認されている¹²⁾。別の例として、各地で盛んになっている地域における防犯対策の取り組みでは、住民が日常生活で学校周辺などの街中を歩く際に、「地域安全パトロール中」と書かれた腕章を着用する取り組みや、同様の事項を記載したパネルを取り付けた自転車を日常生活で用いるなどの取り組みが行われている^{13,14)}。

また、警察庁関係機関が侵入犯罪者を対象として実施した調査結果では、「犯行をあきらめた要素」として、2つまでの複数回答で31%が「セキュリティシステムの存在」

を、9%が「防犯看板」を挙げている¹⁵⁾。まさに、防犯していることのアピールが犯罪抑止力を発揮することの証左といえよう。また、本章冒頭に述べたように、家屋への侵入に対する防犯対策においても、我が国では、防護性能の情報は積極的に公表されている。

これらの例に示されるように、強い信念をもった確信犯による妨害破壊行為を除いて、意図的な妨害破壊行為に対しては、最大能力を示さないようにした上で防犯能力をアピールすることは、妨害破壊行為の抑止効果につながるといえるであろう。

上記のような開かれた議論を通じて評価の内容を公表していくことにより、国民の安心感を醸成するだけでなく、副次的に妨害破壊者に対する抑止効果を生み出すことが期待できる。この点は従来見過ごされがちであった重要な点であると考えられる。

III. 一部の情報開示を前提とする新たな評価制度

1. 評価組織の構築と基本方策

第II章で述べた核防護に対する国民の安心感醸成のために重要となる分析・評価については、その基本は、以下の3つの方策よりなるものとする。

- (1) 評価基礎脅威(Evaluation Basis Threat : EBT)の設定および開示
- (2) 現実的な評価用妨害破壊行為シナリオの構築
- (3) 評価結果と内容の開示

この評価は、一部の限定された情報を開示することを前提としたものとし、専門家集団による公的かつ中立的な第三者機関(以下「第三者機関」という。)が行うものとする。本報では、この機関において行われる評価を「第三者評価」と呼ぶ。

次節にて、これらの方策の具体的な内容を述べる。

2. 基本方策の詳細

(1) 評価基礎脅威(EBT)の設定および開示

EBTの設定およびそれに基づく防護措置は、原子炉等規制法及び関係法令等に従って実施される。これとは別に、第三者評価のための脅威として、開示を前提として、第1図で位置付けられるEBTを新たに設定する。これは、「評価のために規制当局以外の第三者機関が設定する標準的な脅威であって、想定し得る最大規模の脅威よりも脅威の強度は低い、『発生する可能性がある』と合理的に推定される脅威」と定義する。EBTは、定義に示すとおり、あくまでも評価の実施を目的として導入するものである。

ここで、開示を前提とするEBTを設定するに際しては、それが規制当局の設定するDBTよりも低い脅威であることが必要条件となる。EBTは公開されている情報を通して決められるものとし、DBTよりも脅威の程度が低

^{k)} タイムライン分析の手法としては、米国エネルギー省が開発した計算コードであるSAVIおよびEASI、ならびにそれらをもとに日本で開発されたESOPなどのシステムが知られている。

第1図 EBTの設定手法の例

いことを規制当局が確認した上で、第三者評価のために使用されるものとする。

(2) 現実的な評価用妨害破壊行為シナリオの構築

EBTに基づき、評価のために単純化された妨害破壊行為シナリオ(以下「標準評価シナリオ」という。)を構築し、防護上の重要な箇所を特定することにより、評価の対象を限定する。妨害破壊者が、原子力施設の防護措置について有する情報の量は、施設者側に比べて少ないと考えられる。標準評価シナリオは、一般人が通常想定し得るレベルのものと位置付けていることから、シナリオ自体の一部を開示することに支障はないと考えられる。なお、EBTとしてインサイダの存在を考慮した場合には、インサイダからの事前の情報入手を前提としたシナリオを構築することも必要となる。この場合においても、施設の脆弱な点が明らかにならないよう留意しつつ、シナリオを構築・開示するよう努めることになる。

また、DBTのような高いレベルの脅威によるテロが発生することは稀であるため、現実感が湧き難く緊張感の維持には必ずしも効果的とはいえないが¹⁾、現実性が高いと推定されるシナリオの下、模擬部隊投入による実践的訓練を実施した場合には、事業者における高い緊張感の維持が期待できるであろう。

(3) 評価結果と内容の開示

EBTと標準評価シナリオに対応する防護措置について、評価を行った上、その結果を開示することになる。開

示するに当たっては、目標を達成していることが前提となる。成果内容を公表することにより、実際にはより高いレベルで厳重に防護されていることを間接的に示すことになる。これは、施設周辺公衆や国民に対する信頼感・安心感の醸成が期待できるだけでなく、第II章で述べたとおり、テロ行為自体に対する抑止効果を生み出すことにつながると考えられる。

妨害破壊者は、妨害破壊活動を行うに当たり、失敗すれば組織が摘発され、以後活動が行い難くなるなどの、妨害破壊者側にとっての一定のリスクを負うことになる。情報セキュリティの突破能力の誇示自体を目的とするハッカーなどの愉快犯を除けば、テロ組織はなんらかの社会的メッセージを発することを目的に妨害破壊行為を行う。成功する可能性が高いと考える妨害破壊行為を、妨害破壊者側が社会的メッセージ発信の手段として選択することは当然のことであり、社会的メッセージを発するという目的が達成できるならば、妨害破壊の対象として当該施設に関わる必然性はない。したがって、妨害破壊者としては、より防護の手薄な別の放射性物質使用施設を標的として選ぶことも可能であるし、また、反原子力のメッセージを発することを目的としない場合には、原子力施設の破壊以外の他の手法によるテロも選択肢として採り得る。いい換えれば、妨害破壊者からみて施設の防護能力が高いと認識されればされるほど、当該施設に対する妨害破壊行為実施の意欲がそがれることになる。当該施設の防護能力の高さをアピールすることにより、一般の防犯対策と同様に、テロに対する抑止力を得ることは十分期待できると考えられよう。

3. 法令に基づく規制体系と第三者評価との関係

現在、法令に基づきDBTを基準として、事業者は核物質防護規定に基づき必要と判断される高いレベルの防護措置を講じることとされている。法令に基づき規制当局が行

¹⁾ 一般的な傾向として、セキュリティに関しては、高い警戒感を維持することは容易ではない。強度の脅威が発生した直後は、高い警戒意識が働くが、そのような強度の脅威による犯罪が発生することは稀であり、時間とともに警戒感が薄れていく。卑近な例でいえば、登下校時の小学生が殺害される事件が発生すると、その直後は父兄が付き添い登下校を行うが、時間が経つとともに負担感が増えて警戒レベルを下げようとの動きがみられるのはその典型である。

う核物質防護規定の遵守状況検査は、事業者が高いレベルの防護措置を目指していること自体をチェックすることによって、想定し得る最高レベルの脅威である DBT に基づき設計された防護措置全般が正しく機能していることを検査するものと解釈することができる。一方、本報で提唱する第三者評価は、現実には発生しやすいと推定される脅威のもとに構築されたシナリオに沿って、デモンストレーションを兼ねて評価を行うものである。第三者評価は DBT のレベルの脅威を対象とするものではないため、評価内容は開示されることとなる。これらの関係を第 2 図に示す。

IV. 安心感醸成のための評価制度の具体像および考察

1. 評価基礎脅威 (EBT)

IAEA によれば、DBT は、1) 脅威の程度に応じたリソースの配分を可能とする、2) 脅威の想定をリスクや被害と結び付ける、3) 個々の施設に特有のものとして想定される、としている。さらには、脅威の評価に当たっては、「誰が (Who)」、「何故 (Why)」、「能力 (Capabilities)」、「戦術 (Tactics)」、「支援 (Support)」が含まれるべきであるとされる¹⁶⁾。経済産業省の報告書によれば、「仮想敵 (テロリスト、不満をもつ従業員等)」、「人数」、「戦術 (偽りの証明証を用いて警備システムを突破する偽計等)」、「不法行為 (警備システムを突破する公然とした実力行使等)」、「隠密 (検知システムを破って密かに施設に侵入等)」、「能力 (防護システム等に関する知識、襲撃のスピード、武器・爆薬・道具等の所持等)」が、DBT の具体的なイメージとして示されている¹⁷⁾。

本報で提案した EBT も、上記の DBT と同様の内容であるが、脅威の強さが DBT とは異なるものである。その具体像については、以下のような類推により導出できると考えられる。

(a) 他分野における事例からの導出

原子力以外の分野における過去の我が国での妨害破壊行為の事例に即して、同規模の組織力・破壊力による妨害破壊行為が発生するとして想定。

(b) 外国の事例からの導出

外国における妨害破壊行為を企図している集団と深いつながりをもつ集団が我が国にも存在することが公知の事実となっている場合などにおいて、外国における脅威と同等の脅威が我が国にも存在するとして想定。

(c) 新たに明らかになった事実・事態からの導出

例えば次の例にみられるように、新たに明らかになった事実に基づき、脅威が推定できる場合：

- a) クリティカル・インフラストラクチャーを対象とする妨害破壊行為の実施を綱領に掲げる反社会的集団の出現
- b) 国内の反原子力活動団体の活動の実力行使への傾斜傾向が顕著になった場合

これらの場合においては、当該団体の声明内容、これま

での活動実績等の公開情報から脅威の程度を想定。

EBT については、我が国の国情を勘案した上で、現実的な脅威として設定されることになるが、主としてサブナショナルな組織の最大規模を想定することが妥当と考える。例えば、オウム真理教団や、広域暴力団のレベルの脅威の存在、また、近年の状況として、一般市民の不法な銃器保持等が考えられる^{m)}。インサイダについては、米英仏の各国は DBT のレベルではインサイダの脅威を想定している¹⁸⁾。現実的な脅威として EBT を我が国の国情に照らして設定するに際しては、オウム真理教団の一連の事件に際して、原子力メーカから情報の流出があったことに鑑みれば、EBT のレベルであってもインサイダの関与を想定することは妥当であろう。特に、原子力施設への破壊攻撃を実施する場合、我が国初の事例となることから、防護の状況などの内部情報を全く入手しないで攻撃を行うリスクよりは、インサイダによる幫助を確保する方が、妨害破壊者にとってリスクはるかに小さくなると考えられ、妨害破壊者側は、インサイダの幫助を確保するよう努力することとなると考えられる。すなわち、妨害破壊者側からみれば、「インサイダを確保できた原子力施設を標的にする」と考える方がむしろ自然であるといえよう。

脅威の強さについては、上記のような情勢分析による定性的な考察とあわせ、定量的な考察を加えた上で EBT を設定する必要がある。例えば、以下のような手法が考えられる。第 1 図に示すように、脅威側が企図する妨害破壊活動の規模が大きければ大きいほど脅威側は強力な態勢で臨むと考えられることから、妨害破壊の規模は脅威の強さに対する単調増加関数 (第 1 図の破線) とみなすことができるⁿ⁾。他方、妨害破壊行為の成功の可能性は、妨害破壊の規模が大きくなるにつれて、一般的には原子力施設の内奥に侵入する必要性も増すことから、成功が困難になると考えられる。この考え方を前提とすれば、妨害破壊行為成功の可能性は、企図する妨害破壊行為の規模に対して単調減少の関係にあり、脅威の強さに対しても、単調減少となる (第 1 図の二点鎖線)。妨害破壊の防止効果は、妨害破壊行為が成功する可能性 (成功確率) とその被害規模の積で表される妨害破壊の期待値に比例すると考えられる^{o)}。こ

^{m)} 警察庁発表の「平成18年の犯罪情勢」によれば、平成18年度の銃器使用事件の認知件数は366件、うち拳銃使用件数は189件に上っている。

ⁿ⁾ 強い脅威をもって、小さい規模の破壊活動を実施することもあり得るが、ここでは、単純化のため、保守的な立場に立って、脅威はその能力で可能な最大の妨害破壊行為を実施するものと仮定する。

^{o)} 図の二点鎖線で示される成功確率は、妨害破壊行為を実行に移した後に成功する可能性であるから、実際のリスクはこの積に、妨害破壊者が妨害破壊行為に着手する可能性を乗じたものになる。ここでは単純化のため、この数値を1、すなわち年当たり1回、妨害破壊の企てが実行に移されるものと仮定しているが、これは、我が国で妨害破壊行為が実行に移された事例がないことに鑑みれば十分保守的な仮定であると考えられる。

第2図 法令に基づく規制体系と第三者評価制度との関係

の値は、通常、第1図で示すように極大点をもつことになる⁹⁾。

本報で提案している評価の主たる目的は、安心感の醸成である。この目的に沿って行う評価の基礎となるEBTを設定するに当たって留意すべきことは、国民に対し、最も起こりそうな妨害破壊行為に関して、十分な対応ができることを具体的に示すことが肝要である。具体的には、第2図の実線曲線の極大点を超えた領域にEBTを設定することが効果的と考えられる。加えて、評価に際して、第三者機関は、EBTのレベルを当該レベルに設定した理由を明らかにすることが重要である。

2. 標準評価シナリオ

上記のEBTを想定した上で、標準評価シナリオを設定する。標準評価シナリオ構築に際しては妨害破壊者側の視点に立って考えることが必要となろう。標準的なシナリオの構築に際しては、個別の施設ごとに、規制当局、事業者、第三者専門家などを交えて検討を行うことにより、多角的に分析した上で構築する必要があるが、一般論として、例えば次のものが考えられる。

(a) 妨害破壊行為着手の前提条件として、成功の可能性

がある程度見込めること

失敗した場合、犯罪組織が強制捜査等の対象となり、次なるチャレンジがし難くなると考えられる。

(b) 必ずしも当該施設に対し関心をもつ者、および/または実行時期への関わりをもつ者に限らないこと

妨害破壊者にとって、社会へのメッセージを発することが主目的であり、当該施設を破壊することは、そのための手段に過ぎないと考えられる。

(c) インサイダによる幫助があること

外部から侵入する妨害破壊者を原子力施設内部に居るインサイダが幫助する方策が考えられる。

3. 評価結果の開示

第三者評価の結果は、評価報告書の形で取りまとめることとし、その内容は次のとおりとする。

(a) 評価に際して設定したEBT

(b) 評価に用いた標準評価シナリオ

(c) 評価の結果

開示される評価結果については、結果を導き出した理由の詳細は記載しないこととし、評価を実施した第三者機関が公開する。

上記の評価の結果の開示により、十分強いレベルのEBTに対して具体性をもったシナリオを提示した上、複数の専門家が、当該施設が十分に防護されていることを表明することになる。評価結果の開示は、十分な防護水準を達成しているとの結果が出るのが前提となる。万一達成していない場合は、結果を開示するのではなく、必要なら

⁹⁾ 単調減少関数 f と単調増加関数 g の積で表される関数 h については、その一次微分 h' は、 $h' = (fg)' = f'g + fg'$ となる。ここで、 $f > 0, g > 0, f' < 0, g' > 0$ である。 f および g が、それぞれ下限値が0に収束する場合であって、 f' および g' が有限値を取るならば、 $f'g + fg' = 0$ となる点が存在することから、関数 h は極大点をもつといえる。

ば施設の運転を停止することも視野に入れて改善措置を講じなければならない^{q)}。したがって、評価作業そのものは非開示で、しかも評価を行っていること自体も秘匿して行う必要がある。

4. 第三者評価の実施による安心感の醸成の考察

心理学において「感情」の構造についての研究を行った戸田^{19,20)}は、「不安」を、個人にとって重要な事柄についての脅威を感じている状況において、予測の「不確実性」が大きいために、行動や情報処理の妨げになっている場合に生じる感情として定義し、「不安」は「恐れアージ^{r)}」を発動させるべきか否か不確実である状態において、不確実度を低減させるために環境についての情報探索行動を生起させる機能をもつとしている。この考え方に立てば、核防護においても、人々が漠然ともつ不安感は、情報の不足に起因するといえてよい。また、情報不足によって生じる不安は、当該事象を自己がコントロールしているという意識(以下「コントロール感」という。)の欠如が関係していると考えられている。情報の不足によって不安が生起・増幅した場合には、単に情報を提供するだけでは不安はさほど解消しないであろう。不安を感じている人々に対して、当該事象についてコントロール感をもつことができる情報とは、望ましい状況を得るための方法についての情報である²¹⁾。吉川²²⁾は、能動的に情報取得した結果知識がある状態になった能動型安心への移行のプロセスとして捉えている^{s)}。

そもそも、「安心」という概念については、吉川²³⁾が主張するように合意された定義はないが、ここでは、文部科学省が設置した「安全・安心な社会の構築に資する科学技術政策に関する懇談会」がまとめた報告²⁴⁾に、一例として提示された「人が知識・経験を通じて予測している状況と大きく異なる状況にならないと信じていること、自分が予想していないことは起きないと信じなにかあったとしても受容できると信じていること」という定義を採用す

る。本報で提案した一部の情報開示を含む第三者評価の結果、「規制当局が検査をしているから問題がない」とする従来型の一方的かつ断片的な情報提供だけではなく、第三者評価の過程で用いられるシナリオや、それに対する第三者の判断のプロセスをわずかでも住民・国民が共有することにより、核防護においても、上述の「自分が知識・経験を通じて予測している状況」を形成し、能動型安心につながるものと考えられる。

原子力安全の分野では、リスクの受容を円滑に進める観点から、リスクコミュニケーション^{u)}に関する研究が発展している。リスクコミュニケーションに関する木下のモデルでは、対象に関するベネフィット情報と対象に関するリスク情報の双方を情報の送り手が提示するというフェアな情報提供を前提として、情報の送り手と受け手がともに考えていく態度(木下はこれを「共考」と呼ぶ。)によりリスクコミュニケーションが成立すると説く²⁵⁾。この考え方を踏まえれば、上記の第三者評価の結果の開示とは、リスク情報とベネフィット情報の提供を核防護の分野において行うことに相当するものといえよう。すなわち、EBTとそれに基づく標準評価シナリオの提示はリスク情報の提供に該当する。また、評価の結果発せられる「当該施設の防護は十分な水準を満たしており、この施設が稼動することにより原子力の平和利用に伴う便益が享受できる」というメッセージが、ベネフィット情報に該当する。

なお、リスクコミュニケーションにおいて伝達すべき情報に関しては、松本²⁶⁾が原子力発電のリスクを例として行ったアンケート調査の結果、リスク情報とベネフィット情報に加えて「安全対策情報」を伝えた方が、情報の「送り手に対する信頼」は高いことが示され、原子力発電におけるリスクコミュニケーションでは「安全対策情報」が必要であることが認められた。これを核防護に当てはめると、ある程度の防護対策情報は開示することはメリットがあるということになる。その一方で、松本らの調査では、実際にパンフレットで「安全対策情報」を含めて情報を伝達した場合、原子力発電に反対の人については「リスク情報に対する信頼」を低下させ、その影響から「情報に対する信頼」を低下させていることも、同時に明らかとなった。このことを核防護に当てはめると、防護対策の詳細の情報を提供することは、かえって不安感を増大させる可能性がある、ということになる。核防護措置の評価結果の開示内容をどの程度具体性を帯びたものにするのが安心感を得る上で適切か、という点については、今後、アンケート調査の実施などを通して慎重に検討していくことが必要となるといえよう。

^{q)} DBTに基づき事業者において核防護措置が適切に講じられていれば、このような事態は起こり得ないはずである。

^{r)} 戸田は、感情は進化の過程において獲得した原始社会の環境に適応するための心的ソフトウェアであるとの立場から、感情を状況に応じた問題解決のプログラムであるとして「アージ(urge)」と呼んでいる。戸田によれば「恐れアージ」とは明確な危険が発見されたとき知覚した場合に即座にそれまでのすべての行動や思考を強制終了させて、ただ逃げろという行動のみを実行させる心的ソフトウェアである。(リスク学事典(2000))。

^{s)} 吉川らは、「能動的安心」に対峙する状態として「無知型不安」を定義し、加えて「無知型安心」および「能動型不安」を定義している(吉川 *et al.* (2003))。この考え方に立てば、現行の核防護措置は、「規制当局がしっかり検査している」と信じて安心した状態、すなわち無知型安心の状態にあるが、ひとたび9・11テロのような事態に直面すると能動型不安となり過剰防護を求める傾向に陥る。このような状況を回避するために、日頃から情報開示を伴う一定のシミュレーションを行い、能動的安心を目指すことが重要であるといえよう。

^{u)} 吉川によれば、「リスクコミュニケーション」とは、「単にリスクについての正確な情報だけでなく、リスクのある問題について多くの人々の合意を得るためのコミュニケーションの過程」と定義されている。

V. 結 語

従来、セキュリティに関する議論は、開かれた議論が馴染まないとされ、「専門家の議論」に委ねられてきた。議論に参加していない部外者には、脅威の大きさと防護対策強化の必要性を主張するテロリズム研究者の警鐘のみが強調され、現場の実務経験に基づく現実的な議論がみえ難い。しかし、実際に起こるのは、最大規模の脅威ではなく、「確実に成功すると妨害破壊者側が考える」ものがほとんどであるとみられる。9・11テロをテロリストが実行したのは、破壊規模が大きいからというより、当時、自爆テロの成功率が非常に高かったからであろうと考えられる。テロ対策を考える際には、このことにもっと目を向けるべきであろう。「成功しそうもない」と妨害破壊者側が思えば、妨害破壊行為自体の発生確率は低くなるものと考えられる。したがって、関係者のみの議論では不十分であり、適切な防護水準についてのコンセンサス形成を踏まえて、高い防護能力のアピールがなされることが必要と考えられる。

本報では、このような考え方に立って、核防護の水準についてのコンセンサスと安心感を醸成することを目指す新たなアプローチとして、第三者評価を行いながら一定程度の情報開示をすることが有効である、との考え方を示した。その上で、評価基礎脅威(EBT)の設定、標準評価シナリオの構築、そして評価結果と内容の開示という3つの方策からなる新たな評価の枠組みを提案した。

本報で試みに行った推論にならって多様な視点からの議論が行われることにより、脅威の大きさと防護強化の必要性を啓発するだけになりがちな核防護論から一歩進めて、現実的な防護対策とその水準についての議論が発展して、社会的なコンセンサスが形成されるとともに、安心感が醸成されることを示した。

本報の執筆に当たっては、神田啓治京都大学名誉教授ならびに神田名誉教授および中込の主催するエネルギー政策研究会の参加各位から、貴重な御示唆を頂戴した。心より感謝申し上げる。

— 参考文献 —

- 1) 防犯性能の高い建物部品の開発・普及に関する官民合同会議, 防犯性能の高い建物部品の開発・普及の今後の在り方 (2004).
- 2) 防犯性能の高い建物部品目録, 財全国防犯協会連合会 WEB サイト (<http://www.cp-bohan.jp/>)
- 3) 官民合同会議による「防犯性能の高い建物部品」の共通標準について, 警察庁 WEB サイト (<http://www.npa.go.jp/>)

- safetylife/seianki22/bouhan.pdf) (2004).
- 4) JUSRI レポート別冊第17号防犯環境設計ハンドブック [住宅編], 財都市防犯研究センター.
- 5) 防犯性能の高い建物部品の開発・普及に関する官民合同会議, 建物部品の防犯性能の試験に関する規則 (2003).
- 6) 原子力委員会, 原子力政策大綱, 22 (2005).
- 7) 原子力委員会, 原子力の安全確保に関する透明性と信頼の確保について [平成19年3月19日] (2007).
- 8) Forum Report on *Critical Infrastructure and Continuity of Services in an Increasingly Interdependent World*, Geneva, Switzerland, 28-29 Oct. 2003, 6 (9/72), (http://www.gcsp.ch/e/publications/Security_Challenges/CIP/Con_Proceedings/CIP.pdf)
- 9) 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核物質防護対策の強化について, 7 (2004).
- 10) 文部科学省研究炉等安全規制検討会, 試験研究用原子炉施設等の安全規制のあり方について, 文部科学省 WEB サイト (http://www.mext.go.jp/b_menu/shingi/chousa/gijyutu/004/torimatome/04112501.htm) (2004).
- 11) 板倉周一郎, 中込良廣, “核防護システムの評価の視点からみた核防護制度の課題,” 日本原子力学会和文論文誌, 5[2], 136-151 (2006).
- 12) 警察庁, 平成14年警察白書, 84 (2002).
- 13) 防犯ボランティア活動事例, 財全国防犯協会連合会 WEB サイト (<http://www.bohan.or.jp/index2.htm>)
- 14) 目黒区の取組, 東京都目黒区役所 WEB サイト (<http://www.city.meguro.tokyo.jp/anzen/torikumi.htm>)
- 15) 住まいの防犯110番, 警察庁 WEB サイト (http://www.npa.go.jp/safetylife/seianki26/theme_c/c_b_3.html)
- 16) R. Hoskins, “IAEA Material Security Programme (Threat Assessments),” *IAEA Symposium on International Safeguards: Verification and Nuclear Material Security*, Vienna, Austria, Oct. 29-Nov. 2 (2001).
- 17) 前掲 9), 5 (2004).
- 18) 前掲 9), 20 (2004).
- 19) 戸田正直, “不安—感情のアーシ理論にもとづく一解釈,” 心理学評論, 23, 262-268 (1980).
- 20) 戸田正直, 感情一人を動かしている適応プログラム, 東京大学出版会, 65-66 (1992).
- 21) 土田昭司, 情報不足が生み出す不安, リスク学事典(日本リスク研究学会編), TBSブリタニカ, 288-289 (2000).
- 22) 前掲 1).
- 23) 吉川肇子, 白戸 智, 藤井 聡, 他, “技術的安全と社会的安全,” 社会技術研究論文集, 1, 1 (2003).
- 24) 安全・安心な社会の構築に資する科学技術政策に関する懇談会(座長: 中島尚正 放送大学教授, 東京大学名誉教授), 安全・安心な社会の構築に資する科学技術政策に関する懇談会報告書, 7 (2004).
- 25) 吉川肇子, リスクとつきあう, 有斐閣選書, 162-164 (2003).
- 26) 松本隆信, 塩見哲郎, “原子力発電のリスクコミュニケーションにおける安全対策情報の効果—受け手側の評価—,” INSS J., 財原子力安全システム研究所, 11, 34-49 (2004).