丙第３９１号証

AESJ-SC-TR005(ANX):2013

原子力安全の基本的考え方について
第Ｉ編　別冊
深層防護の考え方

標準委員会　技術レポート

2014年5月

一般社団法人　日本原子力学会

第Ⅰ編別冊「深層防護の考え方」の発刊にあたって

平成23年9月から日本原子力学会標準委員会の傘下に原子力安全検討会，原子力安全分科会を設け「原子力安全の基本的考え方について」を検討してきた。標準委員会は標準の制改定をその任務としているが，標準委員会発足当時から，「安全原則（基本理念）も整備されるべき」との活動方針を明示してきた。また，標準の策定の検討は，原子力安全の意味や目的などを常に念頭に置いて行うべきと考えて活動している。そこで，これを明文化し，活動の拠り所とすべきと考え，「原子力安全の基本的考え方について　第Ⅰ編　原子力安全の目的と基本原則」を平成25年6月に発行した。

このたびは，その議論中において特に重要であり，共通の認識が必要であるとして「深層防護の考え方」を取り出してとりまとめ，別冊として発刊するものである。福島第一原子力発電所事故の教訓としても，深層防護の適用は重要なものとして扱われている。しかし，深層防護は基本概念であり，その解釈と適用は諸外国においても議論を継続しているところである。そこで我が国の関係者が原子力発電所の安全確保・向上に資するために，深層防護に関して共通の基本認識を記載したものが必要と考え，IAEA，NRCなどの文献をまとめ，適用に際しての論点についても検討した。これを国内の関係者に広く共有し，深層防護の概念の適用に際して，関係者が拠り所とできるように，ワークショップなどを開催する予定である。

なお，引き続き，「原子力安全の基本的考え方について」は，第Ⅱ編「原子力安全確保のための基本的な技術要件」の策定を進めており，さらに関係学協会とも協働して規格・標準体系について検討を進めていく予定である。

平成26年3月

一般社団法人　日本原子力学会
標準委員会
委員長　　宮野　廣

原子力安全検討会
主査　　田中　知

深層防護とは何か

福島第一原子力発電所事故では，設計想定外の大きな津波により複数プラントの建屋設置エリア全域にわたって海水が浸水し，多くの安全上重要な設備が機能を喪失したため，炉心損傷事故（シビアアクシデント）が発生し，放射性物質が大量に周辺に放出されて多くの住民の方の長期間の避難が余儀なくされ，現在もその状態が続いている。

この事故の最大の背景要因として，IAEA 閣僚級会合報告書や NRC の NTTF 報告書等の多くの報告書において，深層防護の実践に不足があったとして，なぜ深層防護が原子炉の安全確保に有効に働かなかったのかについて多くの頁を割いて体系的に考察している。そして，新しく策定された我が国の規制基準の根幹にもリスクと深層防護の概念が導入されている。しかし，深層防護の概念は論理的で簡明である一方，その適用性が広く多様であるが故に，多重に層を設けることだけに注目してしまうなど，深層防護の正しい理解が不足している局面が見られる。また，深層防護は基本概念であるので，それだけでは安全性の向上の「万能薬」ではない。適用し，それを如何に改善していくか，に着目しなければならない。

そもそも，深層防護とは，人と環境を守るという原子力の安全確保の目的を達成するための方策を構築する考え方を定める基本概念であり，安全対策の妥当性を社会に説明し，信任いただくものである。具体的には，ハザード（原子力施設の場合には放射性物質）と防護すべき対象である人と環境の間に複数の層を置くことにより，特定のハザードが防護すべき対象にとって顕在リスクとならないように，すなわち，特定のハザードがもたらすリスクを許容できるレベルまで低減しようとすることにつながるものである。

深層防護の具体化を考える上でポイントとなる点は，①深層防護の目的（防護の対象），②深層防護で防ぐハザード（放射性物質），③望ましくない状態を決定，である。望ましくない状態の定義により，例えば，望ましくない状態を原子炉の状態の観点とするのか，公衆と環境への影響の観点とするのか，規制に使うために設計基準の観点にするのか，等によって複数の層の定め方は多様である。従って，層の数がいくつかというのは本質の問題ではなく，ハザードの質と規模，防護に係る不確かさ或いは知見の程度に応じて，深層防護を適切に実装することが重要である。

次に重要なのは，深層防護を用いて実効的に安全性向上を図る際にリスク評価，リスク管理を徹底することである。深層防護を用いて全体を俯瞰してバランスよく信頼性を強化し，真に質の高いロバストな原子力安全を確保するには，設計段階はもとより運転段階においても，最新知見や研究成果，事故の教訓等を活かすことにより，深層防護の適用になお残る不確実さへの対応が不十分ではないのかを絶えず問いかけ，継続的に改善する姿勢が大事である。そういった改善の効果を分析し把握し，安全目標に照らして効果的かつ効率的な改善を着実に進めていくことが重要である。

本書では，深層防護についての理解と深い洞察を持って，原子力関係者が安全確保対策に取り組んでいただけるように，日本原子力学会が刊行している「原子力安全の基本的考え方について 第Ⅰ編 原子力安全の目的と基本原則」（AESJ-SC-TR005）の別冊として，深層防護の考え方に関する共通的な認識と，それらに関する論点を纏めた。とり纏めにあたっては，原子力安全検討会 原子力安全分科会の深層防護ワーキンググループにおいて検討・整理が行われ，同分科会及び検討会において審議された。本書が基となって，原子力関係者の間のみならず社会との対話により深層防護の考え方に関して共通の認識が形成されるとともに，それぞれの分野への適用において活発な議論のもとに適切な実装がなされ，それらに関する活発な情報共有や意見交換が行われること，それによる安全確保に対する信頼が得られることを望んでいる。

平成 25 年 12 月
原子力安全分科会
主査　　山口　彰

目　次
（第Ⅰ編　別 冊　深層防護の考え方）

解　説

1. はじめに

本書は，日本原子力学会にて刊行している「原子力安全の基本的考え方について 第Ⅰ編 原子力安全の目的と基本原則」（AESJ-SC-TR005）の別冊として，深層防護の考え方について共通認識と論点をまとめたものである。

(1) 本書の目的

「原子力安全の基本的考え方について：第Ⅰ編 原子力安全の目的と基本原則」（AESJ-SC-TR005）では，基本原則を大きく 3 カテゴリー（「責任とマネジメント」，「人及び環境の防護」，「放射線リスク源の閉じ込め」）に分類しており，「深層防護の考え方」は，「放射線リスク源の閉じ込め」を実現し，原子力の安全を確保するための重要な概念である。

国内外において，これまでに深層防護の観点から様々な安全設計の方針が記述されてきた。それらはいずれも深層防護の概念に対して概ね一致した考え方によっている。しかしながら，福島第一事故が深層防護に対する取組みの不足に起因するものであることを踏まえ，今後，原子力安全を向上させていく上で，深層防護について原子力関係者が共通の認識を持って議論し，深層防護の概念を深化させていくことが，二度とこのような事故を起こさないようにするために極めて重要なことと考える。

本書では，

・そもそも原子力安全における深層防護とは何かということを共有化すること

・これまでの原子力安全への深層防護の具体的な適用を調査するとともに，必ずしも体系的に整理できてはいないものの原子力の安全確保に関する様々な事項と深層防護との関連に係る論点について整理することで原子力関係者間で論点が共有・認識され，深層防護の概念の適用が原子力の安全確保をより効果的なものにしていくための手段となる足掛かりとなること

を目的としている。従って本書では，具体的な防護レベルの数や深層防護概念の原子力施設への具現化の提案を行うものではない。

(2) 本書の構成

本書では，まず第 2 章において原子力安全における深層防護とはどういうものかについて論じ，各深層防護レベルを設定する際の考え方を提示することで，原子力安全における深層防護概念の考え方の共有化を図っている。

次に第 3 章では，論点とした事項について，3.1 節にて論点を展開する上で必要となる共通の認識をまとめるとともに，3.2 節にて具体的な論点の展開を行っている。

また，原子力施設への深層防護概念の適用とは直接は関係が無いものの，原子力安全の向上にとって必須である規制についても，深層防護の考え方をどう取り入れるべきかについて論じている。

2. 深層防護の考え方とは何か

2.1 深層防護の概念

「深層防護の考え方」とは，一般に，安全に対する脅威から人を守ることを目的として，ある目標をもったいくつかの障壁（以下「防護レベル」）を用意して，あるレベルの防護に失敗したら次のレベルで防護するという概念である。

この概念を適用して高い安全性を確保するためには，信頼性が高く，かつ共倒れしない防護レベルを，脅威に対して幾重にも準備しておく必要がある。すなわち，ある防護レベルがどんなに頑健であったとしても，単一の防護レベルに完全に頼ってはならず，一つの防護レベルが万一機能し損なっても次の防護レベルが機能するようにしなければならない。

こうした深層防護の概念は原子力に特有のものではないが[1]，原子力の利用においては，炉心に大量の放射性物質を内蔵している原子炉施設のように，人と環境に対して大きなリスク源が内在し，かつどのようにリスクが顕在化するかの不確かさも大きいという化学プラントや航空機などと同様の特徴があることから，不確かさに対処しつつ，リスクの顕在化を徹底的に防ぐために，深層防護の概念を適用することが有効と考えられている**【解説 1 参照】**。

なお，防護レベルの目標を達成するための手段（以下「防護策」）としては，物理的な障壁の他，例えば制御・管理や緊急時における対応手段といったものがある。

2.2 原子力安全のための深層防護

(1) 原子力安全の特徴

一般産業や社会的活動についても，我々の生活に影響を及ぼすリスクがあるという面では，原子力施設の場合と同じである。ただし，原子力施設は放射性物質を内蔵しているので，他の産業などが有するのと同種の危険があるだけではなく，放射線影響という原子力固有のハザードが存在する。さらに，万一，大量の放射性物質が放出される事故が発生した場合には，広範囲かつ長期間，人と環境に深刻な影響を及ぼすという特徴を持っている。特に，原子炉施設の場合は，福島第一原子力発電所事故のように，放射性物質が大量に放出されてしまうと，周辺住民の放射線影響を防ぐための避難や居住制限などの施策によって，生活への影響が出るなど社会的な影響が大きい。このような原子力固有の特徴を踏まえて，放射性物質の放出を抑制し，放射線影響の顕在化を徹底的に防ぐため，原子力安全を確保する取り組みが必要である。

このため，原子力安全の基本的な目的は，原子力の施設や活動に起因する放射線の有害な影響から人と環境を防護することであり，原子力施設の安全確保の目標は，人や環境に放射線の有害な影響を与えるような事故の可能性を確実にきわめて低いものとする

---

1 例えば，軍事用語では“縦深防御（じゅうしんぼうぎょ）”という。その意味は攻撃側の軍勢を停止させるのではなく，占領地を与えつつ時間を稼ぎ，遅延させることを目的とした戦略であり，対義語としては“水際作戦”がある（Wikipedia より）。

ことである。

(2)原子力安全のための深層防護

原子力施設に限らず一般産業や社会的活動を含めて一般に，ある一つの対策が完璧に機能するのであれば，対策はそれだけで十分なはずである。一方，対策はある想定に基づいて考えられるため，その想定から抜け落ちる事項や人知が及ばない事項が存在することは否定できない。原子力施設の場合，人と環境を防護するにあたって，放射線や放射性物質が制御されずに環境中に放出される原因にも，それらが人と環境に影響を与えるまでの種々の現象にも，人知が及ばない振る舞いが存在しうる。すなわち，人と環境に影響を与えるまでの諸現象や対策やその対策の効果には不確かさが存在するため，一つの対策のみでは完璧な対策とはなり得ない（形あるものは必ず壊れるし，思うように動かない，対処できないこともある）。事前には充分と思われた対策でも思いがけない理由で失敗するかもしれないという不確かさの影響を考慮して，別の対策，次の防護レベルの対策と繰り返すことにより，人と環境に対する一連の防護策全体の実効性を高めることが必要となる。このように，一つの対策では防げないという不確かさを考慮して，放射線リスクから人と環境を護るための防護策全体の実効性（成功確率）を高めるために適用されるのが原子力安全のための深層防護の概念である。

(3)防護策の実効性を高めるための考え方

防護策全体の実効性を高めるために様々な対策がなされるが，この対策を多層とすることを基本的な考え方として，積極的な防護策を講じている（重要な戦略としている）。具体的な対策には，想定する事象に対して，複数の防護レベルでさまざまな手段を用意しておく，すなわち，設計基準事象という想定の中で対策することが基本であり，少なくともTMI事故までは，この設計基準事象を厳格に運用することで十分な安全性が確保できると考えられていた。一方，現実世界で発生する事故（特にシビアアクシデント）には，設計基準事象で想定したシナリオを逸脱する，多重故障やヒューマンエラー（特にコミッションエラー），外部事象が関与する場合がある。すなわち，定められた設計基準事象に対して備えるのみでは高い安全を達成するには十分ではない（現実の事故には完全には備えることはできない）と考えるべきである。このことは，設計基準事象の想定の不完全さに伴う不確かさを示すものであり，不確かさに対する備えを用意する，つまり，不確かさに備えて対策を多層とすることで，防護策全体の効果（成功確率）を高めることができる。放射線影響が抑制され，リスクが低く維持されるようになるように，対策を多層とすることが必要である。ここで，リスクの低減効果を評価するためには，目指すべきリスクの抑制水準（安全目標）やこれを満たすための性能目標といった指標が必要である。

(4)原子力安全を確保するための普遍的な考え方

以上のように，我々が最善を尽くし万全を目指して設計したシステムであっても，なおかつ安全を損なう事象が発生しうる可能性は排除できないとして，そのような不確かさにも適切に対応できるように対策をとる考え方が「深層防護の考え方」である。つまり，「深層防護の考え方」は，不確かさに対する備えであり，原子力安全を確保する上で，想定外は存在するということを考慮して事前に対策しておくために不可欠な考え方である。具体的な対策は，それぞれの原子力施設により異なるものとなりうるが，「深層防護の考え方」は原子力安全を確保するための普遍的な考え方となっている[2]。

2.3 防護レベルの設定の考え方

「深層防護の考え方」に基づく対策を有効なものとするためには，防護レベルの設定について次のような考え方が大切である。

(1)各防護レベルの信頼性

それぞれのレベルで最善を尽くすことで，初めて全体としての効果が期待されるものであって，他のレベルに依存して対策を考えるものではない。例えば，あるレベルの対策が十分になされているのだから次のレベルでは甘くても良いとか，逆に，次のレベルでの対策があるからこのレベルは甘くても良いといった考え方をとってはならない。また，他のレベルに依存して対策を考えるものではない。さらに，あるレベルの対策に欠陥があるから，次のレベルの対策が必要とされるのだというように理解すべきではない。各レベルの十分な対策を前提にして，あえてその効果が十分でなかった場合に備えて対策を多層にするという考え方である。現実に事故が起きた場合には，あるレベルの取り組みが不十分であったことが事後に分析されるが，事前の計画としては，可能な限りの知見を駆使して対策をとっておくという考え方である。各防護レベルの防護策の信頼性を高めることは，高い安全性を実現するためには不可欠な取り組みである。

深層防護の考え方を各防護レベルで効果的に適用するためには，確固たる安全文化を前提とした上で，適切な保守性を考えること，及び品質保証を，全ての防護レベルにおける全ての方策に適用することが前提となる**【解説 2 参照】**。また，各防護レベルの信頼性は，単なる設備設計の対応だけでなく，適切な立地の選定，製造，建設，試運転，運転及び保全，体制（組織，人員，力量）等を含めた対応により高められるものである。そして，運転経験をフィードバックすることは，不確かさが表出した例に学び防護策を

---

2 「改訂 原子力安全の論理」（佐藤一男）では，「・・・多重防護と言う考え方は，私たちの身近なところにも存在している。例えば，健康管理の原則がそれである。・・・まず必要なことは，・・・病気にならないように普段から気を付けることで，・・・次には，病気になりかかった時にこれを早期に発見して早期に治療することで，・・・第三レベルでは，・・・病院などの医療施設を充実しておくことである。」としており，深層防護の考え方は，一般に安全や信頼性確保の考え方として存在する。原子力利用の場合は，その影響が大きいため「深層防護の考え方」という用語を象徴的に用いていると考える。

強固なものとしていく継続的改善活動の重要な取り組みである。このように，深層防護の考え方を効果的に適用し防護策の信頼性を高めるためには，設備（ハード面）と運用（ソフト面）の両面からの取り組みが必要であり，運転経験に学ぶ活動が重要となる。

(2)各防護レベルの独立性

複数の防護レベルが全て機能しなかったときに，人或いは環境に対する有害な影響が引き起こされる。深層防護の考え方で不可欠な要素は，異なる防護レベルが，各々独立して有効に機能することである。そのため，ある防護レベルにおける設計，機能，対策等が，他の防護レベルのそれらにとって障害とならないようにしなければならない。ある防護レベルが他の防護レベルの機能失敗によって従属的に機能失敗することがないことを含め，各防護レベルが独立な効果を発揮するように設計を行うことが必要である。なお，防護レベルの設定の仕方によっては，独立な効果を発揮する具体的な対策が存在しなくなる場合もあり，深層防護の考え方が適切に適用できなくなる場合がある。また，各防護レベルの独立性を確保するためには，想定外がありうることを考慮して，全く異なる取り組み（例えば，設備や機器などのハードウェアだけに頼った対策だけではなく，マネジメントによる対策など）をとることも有効である。

(3)防護レベルのバランス

一方，各防護レベルが各々独立して有効に機能することが必要であるが，これは各防護レベルが相互に無関係に考えられるべきということを意味するものではない。防護策全体の性能を高めるためには，各レベルが適切な厚みを持ち，各レベルの防護策がバランスよく講じられ，あるレベルの防護策に負担が集中しないことが重要である。

(4)防護レベルでの不確かさへの対処

「深層防護の考え方」に基づく防護策が全体として有効に機能するためには，「効果が独立な防護レベルの設定」と「それぞれの防護レベルの信頼性」が必要な要素である。防護レベルの信頼性について，安全確保のための想定や具体的方法にはいずれも不確かさが含まれており，このため結果として，人と環境への放射線影響のリスクを完全にゼロとすることはできず，さらに，リスクを完全に把握して厳密に定量化することも不可能であるため，想定する条件に対して裕度を確保することによって，想定を超える条件に対しても頑健性が期待できるようにし，リスク並びにその不確かさに対処するという考え方がとられている。

(5)その他の留意すべき事項

ところで，「深層防護」という言葉が，多重障壁や物理的障壁といった狭い意味で受け取られる場合や，直接ハードウェアをイメージした意味でとらえていると見られる場合，

物理的障壁の数と認識している場合が見られるが，「「深層防護の考え方」とは，基本的な考え方であり，個別のハードウェアと直接的に対応するものではない」ことを強調したい。さらに，例えば「設計基準事象を深層防護の第三層」と表現するように，プラント状態と深層防護を関係づけるとらえ方も多く見られるが，これについても深層防護の考え方に基づいた対策の実現方法の一つである（一つにしか過ぎない）という理解が必要と考える。

防護策を具体化するためには，脅威となる事象やハザードを想定することが必要である。脅威となる事象やハザードは，その原子力施設への影響がそれぞれ異なるので，リスクの内容並びにリスクの不確かさに応じて，安全確保のために必要な防護レベルや個々の防護策は異なるものになりうる。

リスクの内容並びにリスクの不確かさについての認識は，運転経験や知見の蓄積とともに変化し，予測の不確かさも変化していく。知見の蓄積並びに洞察によって極力，排除する努力を継続することが必要である。リスクへの寄与が小さいことが明らかでない限り放置してはならず，リスクの定量化のための努力を継続するとともに，定量化が不完全な段階であっても合理的に実行可能な対策を検討することが必要である。合理的に実行可能な範囲は，技術の進展及び評価手法の進歩によって変化するものであって，このような変化を適切に取り込むことを含めて，継続的な改善が図られるべきである[3]。

防護レベルについては，これまでにもいくつかの分け方が提案されているが，基本的には，①ある防護レベルの維持及び②ある防護レベルが突破されたときの影響の緩和（もしくは次のレベルの維持）といった段階的な防護レベルで整理することができる。施設の特性に加えてリスクの内容や程度など，施設に想定される脅威やその程度によって，防護レベルの分け方や内容を設定することが適切であり，それぞれの施設によって設定される防護レベルは異なるものとなりうる。

[3] このような取り組みについて，同様な考え方が米国においても NUREG-2150 で提唱されている。

3. 深層防護の概念の具体的な適用と論点

第 3 章では深層防護の概念の具体的な適用，及び原子力安全に係る全ての人が共通の認識とすべき事項及び論点について検討・整理した内容を，原子炉施設を中心に記述する。

3.1 では，論点を展開する上で共通の認識とすべきと考えられる事項について述べ，3.2 では，具体的な論点について展開する。

3.1 深層防護の概念の適用と関連事項の整理

2.3 において深層防護の考え方に基づいた防護策が全体として有効に機能するためには，効果が独立な防護レベルの設定とそれぞれの防護レベルの信頼性が必要な要素であることを述べた。

ここでは，それぞれの要素の観点での適用とこれまでの認識を整理するとともに，深層防護と関連して検討した事項についても整理した。

3.1.1 防護レベルの設定に関する適用とこれまでの認識

防護レベルの設定に関連する事項のうち，原子炉施設に関する原子力安全確保の取り組みと防護レベルの関係，発生防止と影響緩和の考え方，多重の物理的障壁，及び内的事象・外的事象への適用に対する認識を示す。

(1)原子力安全確保の取り組みと防護レベルの関係

深層防護の防護レベルを，ある 5 つのレベルに設定した場合[4]，原子炉施設に関する原子力安全確保の取り組みと各防護レベルは，概ね以下のように関係付けられる。

- （第 1 のレベル）そもそもの発端となる異常や故障等のトラブルの発生を防止するために，実証された技術に基づいて十分余裕のある設計を行うこと，必要に応じ地震や飛来物等の個々の誘因事象に対する防護設計を行うこと，高い品質管理システムに基づいて保守管理を行うこと等が図られる。
- （第 2 のレベル）トラブルが起きた場合にそれを直ちに検知して対応することにより，それが事故に発展するのを防ぐため，運転パラメータがある許容範囲を超えた時に制御棒を自動挿入して原子炉を停止すること等が図られる。
- （第 3 のレベル）事故に備えて，その影響を緩和するため，例えば，原子炉冷却系の配管が破断し，冷却水が流出して炉心が空焚きになるような事故（冷却材喪失事故。Loss-of-Coolant Accident : LOCA）に対して非常用炉心冷却系（Emergency

---

4 「福島第一原子力発電所事故に関するセミナー」報告書（2013 年 3 月，日本原子力学会）では，原子力発電所についての深層防護は，一般には次の 5 つのレベルからなるとされている，としている。
第 1 のレベル：異常・故障の発生防止
第 2 のレベル：異常・故障の「事故」への拡大防止
第 3 のレベル：「事故」の影響緩和
第 4 のレベル：「設計基準を超す事故」への施設内対策
第 5 のレベル：「設計基準を超す事故」への施設外対策

Core Cooling System : ECCS）を用意しておくこと，また，放射性物質の環境への放出を防ぐために頑丈で気密性の高い格納容器を用意しておくこと，格納容器が内圧によって破損するのを防止するために格納容器冷却系を用意すること等が図られる。これらの方策は，施設及び設備の安全設計及び安全評価のために想定する設計基準事象（後述）に基づいて用意される。

- （第 4 のレベル）設計基準[5]を超すような事故状態になった時に備えて，それがシビアアクシデントになるのを防止するための対策（フェイズ１の AM），シビアアクシデントになってしまったあとにその影響を緩和するための対策（フェイズ２の AM）が用意される。
- （第 5 のレベル）放射性物質又は放射線の異常な放出或いはそのおそれがある場合に，周辺住民の健康を防護する等のため，防災対策が図られる。

本事項に関連する論点として，各防護レベルの有効性が独立であるということをどのように考えるかについて，3.2 に記載する。

(2)発生防止と影響緩和

一旦事故が発生すると，その進展に従い対策を実施する上で現象論的な不確かさを含む様々な不確かさを扱わなければならなくなる。したがって，取扱う不確かさが小さい事故の発生防止策をまず考え，その上で事故の発生防止策が喪失することを想定して事故の影響の緩和策を講じることによって，人と環境に対する防護策全体の実効性をより効果的に高めることができる。

発生防止と影響緩和の考え方は，例えば立地の選定においては発電所の安全性に影響を及ぼす自然現象がないことの確認が発生防止として，人口密集地帯からの離隔を求めることが影響緩和として適用される。また，運転においては，発生防止と影響緩和の考え方を適用した設計が適切に機能するための対応が求められる。

すなわち，発生防止と影響緩和の考え方は，設計のみならず原子炉施設に係る様々な取り組みに適用される考え方である。

(3)多重の物理的障壁

深層防護の概念の具体的な適用という捉え方がされているものとして，発電用原子炉施設における多重の物理的障壁の使用（燃料ペレット，燃料被覆管，原子炉冷却材圧力バウンダリ，格納容器）がある**【解説 3 参照】**。これらの物理的障壁の健全性を確保するための冗長かつ多様な独立した動的，静的システムの設計も多重の物理的障壁の使用に関する深層防護の具体的な適用に含まれている。

---

[5] ここでは，design criteria を満足するための設計上の想定条件（design basis）を言う。

(4)内的事象への適用に対する認識

例えば内的事象であるLOCAに対して原子炉冷却材圧力バウンダリを確保する，冷却を維持する，及び閉じ込め機能を維持するというように，設計基準事象に対しては，深層防護の概念を適用して多段に備える安全設計がされ，このような対策が有効に機能しない場合でも炉心損傷や格納容器破損が発生しないよう，代替注水などのアクシデントマネジメントが整備されてきた。

一方，圧力容器底部破損などの設計基準を超える内的事象については，原子炉冷却材圧力バウンダリが喪失すると同時に冷却機能も喪失するため，深層防護の概念を適用した複数の防護レベルが同時に無効になる。このような事象に対しては，そもそも発生しないよう品質管理による発生防止，LBB（Leak Before Break）の概念による検知などの信頼性が高い発生防止対策が可能であり，対策を考える上で評価上の足切りがされてきた。深層防護が不確かさに備えるための概念であることから，対策の信頼性が十分高く，その対策で不確かさに対処できれば，やみくもに後段の防護レベルを設定する必要がない場合もありうる。

(5)外的事象への適用に対する認識

外的事象（自然現象）に関しては，予見し得る自然現象に対して，安全確保上重要な機器が必然的に失われること（システマティック・フェーリュア）の可能性を，無視できるほど低くしており，換言すれば，自然現象に関しては，各自然現象のある強度レベルに対する防護策をとることで共通的に設備が故障することを防止し，残る偶発故障に対して内的事象の中で取り込んで考えるという整理がなされていた。また，内的事象，外的事象の区別は無いが，IAEAではクリフエッジ効果について言及されていた。すなわち，ある強度レベルまでの外的事象に対しては，深層防護の概念に基づき対策することになっていたが，その強度レベルを超える外的事象に対する具体的な取り組みについては，これまで明確にされていなかった**【解説4参照】**。

本事項に関連する論点として，設計基準を超える外的事象に対してどのように取り組むべきかについて，3.2に記載する。

3.1.2 各防護レベルの信頼性に関する適用とこれまでの認識

各防護レベルの信頼性に関連する事項のうち，安全裕度の深層防護上の位置付け，多重性，多様性，独立性及び単一故障基準の深層防護との関係，安全重要度分類の意義，人的過誤への対策，及びシビアアクシデント対策に対する認識を示す。

(1)安全裕度の深層防護上の位置付け

安全設計で要求される基準（例えば燃料被覆管温度や格納容器圧力に係る基準）は，安全上必要なシステムや物理的障壁が喪失した場合に実際に損傷するレベル（温度，圧

力等）に対して余裕を持って設定される。これは，機器等の設計において，システムや物理的障壁のふるまいを予測する際に十分に考慮されない現象や事象進展に対して余裕をみておくためである。安全裕度（safety margin）は，このように設計において現象や事象進展の不確かさに対して備えるための工学的アプローチであり，深層防護の概念を適用して各防護レベルの信頼性を高めるためには不可欠の要素である。

(2)多重性，多様性，独立性，及び単一故障基準

安全設計において，安全機能を有する構築物，系統及び機器は，その安全機能の重要度に応じて，十分に高い信頼性を確保し，かつ，維持することが求められる。例えば，原子炉施設を止める，冷やすといった機能を有する重要度の特に高い安全機能を有する系統については，機器のランダム故障に対して信頼性を有するための多重性や，設備共通に係る機能喪失要因に対して信頼性を有するための多様性を求めるとともに，それらが独立して有効に機能するように独立性が要求される。ただし，これまでの取り組みでは，何に対しての多様性なのか，明示的な議論はなされてきていなかった。

多重性とは，同一の機能を有する同一の性質の系統又は機器が二つ以上あることであり，多様性とは，同一の機能を有する異なる性質の系統又は機器が二つ以上あることである。そして，独立性とは，共通要因によって同時にその機能が損なわれないよう，二つ以上の系統又は機器が，想定される環境条件及び運転状態において，物理的方法その他の方法によりそれぞれ互いに分離することである。

すなわち，多重性は，安全設計において，ランダム故障に対するある防護レベルの信頼性を高めるための手段であり，多様性は共通の環境要因に対して防護レベルの信頼性を高めるための手段である。そして独立性は，物理的分離等により共通要因に対する防護レベルの信頼性を高めるための手段である。このうち多重性については，系統・機器の信頼性を十分に確保した上で，設計上の最悪の故障を１つ考える（単一故障基準を採用する）ことにより，その適切性が確認される[6]。

深層防護の概念との関係を整理すると，多重性，多様性，独立性は，深層防護の概念に基づいた安全設計において，ある防護レベルの信頼性を高めるための手段であり，このうち独立性は多重性，多様性が効果を発揮するための前提条件である。そして単一故障基準は多重性の適切性を確認するための１つの手段である。

本事項に関連する論点として，各防護レベルの有効性が独立であるということと安全設計における多重性，多様性，独立性との関係をどのように考えるかについて，3.2 に記載する。

---

[6] SECY-77-439 "Single Failure Criterion" において，次の記述がある。" The Single Failure Criterion , as a design and analysis tool, has the direct objective of promoting reliability through the enforced provision of redundancy in those systems which must perform a safety-related function."

(3)安全重要度分類の意義

各防護レベルの信頼性を高めるための対策を具体化する際には，原子炉施設に存在する様々な構築物・系統・機器の中から原子力安全を確保する機能を見落とさず，それらに焦点を当てて重要度分類を行うことによって，原子力安全の重要度に応じた信頼性を確保する取組みが可能となる。すなわち，重要度分類の目的は，安全確保に必要不可欠な機能を見極めて安全確保の努力を最適配分することである。重要度分類は，人と環境への有害な放射線影響を防ぐ観点から設定される深層防護の防護レベルの信頼性を確かなものにするため，原子炉施設から放出される放射性物質を抑制する観点から定義されるものである。

(4)人的過誤への対策

また，完全に自動化された原子力施設であって，かつ，異常時に運転員の操作を禁止する施設でないかぎり，何らかの形で運転員の操作が必要となる。人間はミスをするものである（to err is human）ことを踏まえた安全設計や運転員の力量維持が求められる。

例えば，駆動源喪失や故障が発生した場合においても，常に安全側にその機能が作用するように設計する（フェイルセーフ），駆動源喪失や故障が発生した場合においても，常にその状態を維持するように設計する（フェイルアズイズ），間違った操作をしようとしても操作出来ないように設計する（フールプルーフ）などがあり，これらにより防護レベルの信頼性が高められる。

(5)シビアアクシデント対策

シビアアクシデントに対しては，これまで我が国では，既存設備を有効活用してリスクを低減する対策を講じてきた。防護レベルの信頼性を確保するために講じられる措置は本来的に，必要な機能と信頼性を満たすものであれば恒久設備，可搬式設備のいずれでも良く，その両者を組み合わせたものでも良いはずであるが，シビアアクシデントに対して可搬設備を活用するという取り組みが我が国ではこれまでなかった。すなわち，我が国では，シビアアクシデント対策の信頼性を担保すべくアクシデントマネジメント手順の整備とその教育・訓練がなされてきたが，運転員による恒設設備での対応が主であり，緊急時対応要員がプラント対応に主体的に関与するような，想定していない困難な状況でも柔軟に対応することを意識してマネジメントするという取り組みがなされていなかった。

本事項に関連する論点として，深層防護の概念と設計での対応が求められる範囲との関係をどのように整理すべきかについて，3.2 に記載する。

3.1.3 関連事項の整理

防護レベルの設定や防護レベルの信頼性に直接関係しないものの，深層防護と関連して検討した事項について整理した。

(1)設計基準事象

原子力の施設と活動について具体的な防護対策を設計する場合には，ある「想定」に基づいて事故シナリオを考え設計基準事象を設定する。この設計基準事象（DBE：Design Basis Event）は，これによって現実に起きる可能性のある多様な事故群，或いは事故シーケンス群をカバーし，包絡されている（envelope）という考え方をとる。我が国においてDBEは歴史的な変遷を経て安全評価審査指針類に規定されるような現在の形になっている。

本事項に関連する論点として，深層防護の概念と設計での対応が求められる範囲との関係をどのように整理すべきか，及びこれに関連して，設計で要求される条件が満たされているかを確認するための設計評価やその許容基準のあり方について，3.2に記載する。

また，設計基準事象を整理する上で，欧米で議論されている Design Extension Conditions (DEC)とは何か，DEC をどのように考えるかについて，論点として 3.2 に記載する。

(2)深層防護と安全目標との関係

信頼性の高い防護レベルが複数存在することで，防護レベル間の従属性が大きくないとの前提があれば，全体として高い安全性が得られる。

しかし，深層防護の概念を適用した対策により許容基準への適合性の確認は可能であるが，どの程度の安全性が達成されるかは保証がなく，安全性のレベルの尺度として安全目標が必要となる。

安全目標は，原子力安全を確保するために講じた措置によって達成しうる原子力利用に伴うリスクの抑制水準を示すものであり，公衆の日常生活に伴うリスクとの関係で定めるものである。一方，性能目標は，原子力施設が安全目標に適合しているかを判断する目安となる水準を示すものであり，性能目標の指標と目標値は原子力施設の種類や特性によりソースタームの大きさやタイミングに大きな違いがあれば，その違いに応じて適切に定められるものである。すなわち，安全目標は原子力施設の種類や特性によって異なるものではないが，性能目標は異なりうる。

原子力施設の安全確保には深層防護の概念が採用されていることを踏まえると，防災など原子力施設の外側の防護レベルの機能を適切に仮定することによって，例えば原子炉であれば重大な炉心損傷が発生する確率や格納容器から大量の放射性物質が放散される事象が発生する確率などを安全目標に対応する性能目標として定めることができる。

このように安全性のレベル，いわば深層防護の十分さは，リスク評価を行い安全目標

や性能目標に照らし合わせることにより確認することができる[7]。ただし，不確かさの要因の一つである"unknown unknowns"（未知の未知）の事柄はリスク評価では考慮されないことから，リスク評価により示される安全性のレベルは真のレベルではないことに留意が必要である。

本事項に関連する論点として，深層防護の概念を適用した対策による安全性のレベルを確認するための評価のあり方について，3.2 に記載する。

3.1.4 論点とする項目のまとめ

3.1.1 から 3.1.3 で述べた事項に関連して論点とする項目を以下にまとめる。

- 設計要求範囲と設計評価に関する整理（3.1.2(5)，3.1.3(1)と関連）
- Design Extension Conditions (DEC) の持つ意義（3.1.3(1)と関連）
- 各防護レベルの独立な有効性（3.1.1(1)，3.1.2(2)と関連）
- 設計基準を超える外的ハザードに対する取組み（3.1.1(5)と関連）
- 深層防護の有効性評価（3.1.3(2)と関連）

3.2 深層防護の概念の理解のための論点

ここでは，3.1.4 で示した論点について示す。また，欧米の安全規制や IAEA における深層防護に関する議論に関連し，原子力安全規制の中での深層防護をどのように考えるのかについても合わせて示す。

3.2.1 設計要求範囲と設計評価に関する整理

設計基準事象(3.1.3(1))やシビアアクシデント対策(3.1.2(5))に関連する論点として，設計要求範囲や設計評価及び評価における許容基準のあり方について考察した。

(1)設計要求範囲に関する整理

欧州と米国において，深層防護に関する報告書が最近提出されている。欧州 WENRA からは RHWG Report として "Safety of new NPP designs", March 2013 が，米国 NRC からは NUREG-2150 "A Proposed Risk Management Regulatory Framework", April 2012 が提出されており，それぞれの中で深層防護と設計要求範囲の関係についても整理されている。

欧州 WENRA での深層防護を適用した規制体系においては，深層防護のレベルを５段階に設定しており，第１のレベルを「異常な運転と故障の予防」，第２のレベルを「異常

[7] リスクは，望ましくない状態の発生可能性とその影響の大きさで定義されるため，望ましくない状態をどのように定義するかでリスクの表し方は変わりうる。安全目標に関するリスクについては，公衆の日常生活に伴うリスクとの関係で望ましくない状態が定義され，性能目標に関するリスクについては，原子力施設の種類や特性との関係で望ましくない状態が定義される。そのため，安全目標と性能目標は密接な関係があるが，これらに対する安全性のレベルを確認するためのリスク評価ではリスクの表し方（指標）は異なる。

な運転と故障の制御」，第３のレベルを「急速な炉心溶融状態への進展の防止」と「放射性物質の放出制限」としており，第４のレベルを「炉心溶融状態下での状態制御」と「サイト外影響制限」と定義している。第５のレベルは緊急時対応である防災となっている。また，第３のレベルで対処すべき状態として，旧来からの設計基準事故・事象に対応するレベル（3.a）に加えて多重故障状態（3.b）を含めることとし，一方，炉心溶融を伴う事故は炉心溶融以前とは本質的に異なる現象を伴うため，第４のレベルで取り扱うことを提唱している。設計要求範囲は防災のレベルを除く深層防護の各レベルに亘る一連の構成としており，例えば IAEA での深層防護の考え方における設計基準範囲(Design Basis Conditions)と設計拡張状態(Design Extension Conditions)に区分するような体系とはなっていない[8]。

米国 NRC のこれまでの規制体系においては，設計要求範囲は主に許認可（License）範囲と認識されており，単一の起因事象による旧来からの設計基準事故・事象に基づく範囲を指すことが多いと考えられるが，対応手順などを含む規制プログラム全体の範囲は深層防護のレベル全域に及んでいる。新設炉においては，旧来からの設計基準事故を超える範囲で確率論的リスク評価を行い安全評価書に含めることが既に規則化されており，これに合わせて設計要求範囲や許認可の範囲も拡張して認識されてくることも考えられる。さらに NUREG-2150 では，深層防護の考え方を自らの意思決定プロセスに取り入れ，今までの事象分類の見直し・再構築による規制のあり方について今後再検討することが提唱されており，設計要求範囲も今後変遷していくことが考えられる。

欧州 WENRA のように深層防護の全レベルを一貫して設計要求範囲とすることは，規制の体系として一つのあるべき姿であろうが，米国 NRC のように規制当局の意思決定プロセスに深層防護の考え方を取り入れていくこともあり方の一つであろう。また，旧来からの設計基準事故・事象においては，起因事象の発生頻度が極低頻度と考えられる場合には，除外することが許容されてきた。これに対して，例えば NUREG-2150 での事象分類の見直し・再構築においては，設計基準を超える外的事象への対処も含まれており，今まで想定外としていた事象も考慮の対象となるものが出てこよう。このような事象では，事故シナリオを予め想定しておくことが難しいことも考えられ，対処の方策としてレジリアンス[9]などの新たな提案もなされてきている。

(2)設計評価に関する整理

旧来からの設計基準事故・事象に基づく設計においては，単一の起因事象を定義し，

---

8 参照「3.2.2 Design Extension Conditions (DEC) の持つ意義とは何か」

9 レジリアンスの定義として「極度の不利な状況に直面しても，正常な平衡状態を維持することができる能力」（Bonanno.G）があり，レジリアンス・エンジニアリングの視点では，レジリアンスを，「変化や外乱の前，途中，後でシステムが自分の機能を調整し，それによってシステムが想定内，想定外，いずれの状況に対しても必要な動作を維持することができる能力」とする捉え方がある（日本原子力学会誌 Vol55,No.8(2013)）。

その事象を主に許容基準（Acceptance Criteria）内に収束させることが求められてきた。これらの許容基準は，例えばスクラムの速度や非常用炉心冷却系の容量などの根拠となっており，このため設計評価としてはプラント挙動解析による現象の把握が必要となることから，決定論的な手法が主に採用されてきたと考えられる。また，これらの設計評価は一般に許認可要件となっていたことから，許容基準に関するパラメータに対して保守性を有することが要求されてきた。例えば米国 NRC は NUREG-2150 において設計評価の保守性に関する OECD/NEA の整理を参照しており，プラント挙動解析では保守性の要因を許認可マージン（Licensing Margin）と評価マージン（Analytical Margin）とで整理している。これによると，許認可マージンは余裕を含めた許容基準の設定として，評価マージンはプラント挙動の包絡性として分析されている。ここから保守性に関する要因としては，許認可要件であることの他にも，評価に関する事象の不確かさを補うこと，場合によっては当時の計算機環境により簡易であるが保守側となる計算モデルを採用してきたことなどが考えられる。対して昨今では，事象の不確かさについては LOCA 時の挙動実験などを経てより確度の高いモデルが開発されてきており，計算機環境についても進歩してきているので精緻なモデルを採用できる状況にあり制限は緩和されてきている。また，最適評価手法による解析結果群を統計的に処理することで事象の不確かさを見積もることも可能になってきており，国内においてもこのような統計的安全評価の実施基準が既に用意されている[10]。このように，最近では旧来からの設計基準事故・事象における設計評価においても一律に保守的な解析を行う必要性は低減してきており，プラント挙動解析などでの評価マージンは解析側に取り込める状況にもあると考えられる。この場合には，保守性の主な要因は許認可マージンになってくるものと考えられる。

一方，旧来からの設計基準事故・事象を超える範囲においては，主に複数故障の組合せによる事象などが対象となるため，そのような多様な故障の組合せによりどのようなプラント状態に陥るのか，その重要性はどの程度かを分析する必要がある。このためには，多様なプラント状態を分析できるシーケンス解析を行い，その発生頻度や影響度合いを把握できる確率論的リスク評価などの確率論的な手法が適している。また，対象とするプラント状態における原子炉や格納容器内の物理現象では不確かさも大きくなることから，徒に保守性を有することが必ずしも現象理解に繋がらないことが考えられる。このような事象では，最適評価手法に基づく現実的な評価と不確かさを把握することで事象進展の広がり捉えることができ，現実的な現象理解に至るものとなる[11]。

これらに対して，欧州 WENRA のように深層防護の各レベルを一貫して設計要求範囲とする場合には，旧来からの設計基準事故・事象とそれを超える範囲で区分することではなく，対象とする事象や許容基準に応じて決定論的手法と確率論的手法，或いは保守的評価手法と最適評価手法を組み合わせる考え方になってきている。

---

10 AESJ-SC-S001:2008「統計的安全評価の実施基準:2008」日本原子力学会

11 参照「3.2.5 深層防護の有効性評価 (1)有効性評価のあり方」

(3)許容基準のあり方について

設計評価の保守性に関する OECD/NEA の整理における許認可マージンは，主に許容基準の設定にあり，例えば「大規模な炉心の損傷防止」を目的として，より厳しい「炉心燃料の被覆管損傷防止」を許容基準に採用することなどがある。欧州・米国とも旧来からの設計基準事故・事象における設計評価では，このような保守的な許容基準を継続することを基調としているように見受けられるが，欧州 WENRA においては，旧来からの設計基準事故・事象を超える範囲に対して，より現実的な条件設定も許容している。例えば WENRA の深層防護第 3 のレベルは「急速な炉心溶融状態への進展の防止」を目的としているが，その内の旧来からの設計基準事故・事象に相当する 3.a では保守性を有する許容基準として，炉心燃料の被覆管損傷防止（例えば被覆管温度と酸化率）を，これを超える事象に相当する 3.b では目的そのものである，急速な炉心溶融状態への進展の防止（例えば被覆管温度）を許容基準とすることもできる。このような設定とすることにより 3.b に適合する設備や方策の範囲が拡大し，実質的な安全性の向上に繋げることができるものと考えられる。

国内においても，設計評価や許容基準のあり方に関して深層防護をどう適用していくか，今後とも検討されることが望まれる。

3.2.2 Design Extension Conditions (DEC) の持つ意義とは何か

IAEA の最新の設計技術要件 No.SSR-2/1 [文献8)]では，design basis accident を越える事故に対する従来の呼称"beyond design basis accident"に変えて，新しく"design extension conditions(DEC)"という呼称を与えている。SSR-2/1 にはその理由は述べられていないため，ここでそのように呼称が変えられた理由・意義について，米国,欧州における深層防護の考え方の変遷から考察する。

商用原子力発電における深層防護原則は，1960 年代からすでに原子力安全確保（原子力利用に起因する放射線災害を防止すること）のための基本的な考え方[文献9)]とされていた。深層防護原則といえば現在では IAEA の 5 つのレベルの防護概念が有名であるが，そのように概念整理がなされたのは 1980 年代後半の IAEA INSAG-3 [文献10)]においてである。しかしながら，それ以前からも深層防護については多様な側面から捉えた考え方が表明されており，必ずしも統一された概念があるわけではない。文献 2)によれば，（特に 1970 年代前半まで）深層防護概念は，概ね

(1)事故を起こす確率が低くなるように設計・運転する

(2)プラントの擾乱に備えた保護システムを装備する

(3)想定事故に対し影響を緩和する工学的安全設備を装備する

という 3 つの防護レベルの文脈で語られているが，その 3 つのレベルそのものを指して defense-in-depth と呼ぶ考え方（Internal Study Group, AEC, 1969）もあれば，(1)の防護レベルを確実にする物理的な多重障壁のことを defense-in-depth と呼んだり（Clifford

Beck, then Deputy Director of Regulation, Joint Committee on Atomic Energy Hearings, 1967)，或いはその多重障壁を防護する手段を defense-in-depth と呼ぶ[文献 11)]など，微妙にズレのある複数の考え方があったとされている。また，上記 3 つのレベルには「一般公衆の（放射線）防護」が陽には含まれていないが，TMI2 事故以降になると，

(1′)（保守的設計余裕による）事故発生防止

(2′)事故の検知と収束

(3′)一般公衆の防護

という 3 つのレベルを defense-in-depth と呼ぶ考え方が出てきている[文献 12)]。いずれにせよ，深層防護の意味については，概ね類似はしながら微妙に細部の異なる考え方が示されているが，重要なのは共倒れのない高い信頼性を持つ複数の手段で備えるという「概念」である。

大部分の既設原子力発電所では，上記(1)～(3)の考え方がその安全設計に反映されていると考えられる。安全設計の design basis（安全設計上の想定条件）としては，想定起因事象（大 LOCA，反応度事故，給水喪失過渡事象など）に対し，いかなる単一機器（又は単一サブシステム）が機能喪失しても炉心健全性と炉心冠水を維持できる（一般公衆に被害を及ぼさない）ように設計すること，すなわち単一故障基準（single failure criterion）を満足するように造り込むことが要求されている。この単一故障基準は深層防護の一構成要素である冗長信頼性を定性的に確認する手段であり，このような design basis の範疇で設計する限り原子力プラントの安全性はそれにほぼすべて包絡されるという論理であったと考えられる。

この論理は，適切な品質保証の元（米国では 10CFR50 Appendix B にて規制）で設備が維持されるならば，「複数機器の同時機能喪失（共通原因故障）」，「炉心冠水の失敗による著しい炉心損傷」は発生確率が低く実際にはありえない，ということを暗黙の前提にしていると考えられる。しかしながら，実際の運転実績では共通原因故障の発生頻度が想定以上に高く，design basis の範疇で必ずしもプラントの安全性が包絡されるわけではないことがわかってきた。典型的な例として，米国等では全非常用交流電源の同時機能喪失である SBO（Station black out），原子炉保護系の同時機能喪失である ATWS（Anticipated transient without scram）は，信頼性評価実績と発生影響を考慮すると安全重要度が極めて高いと判断され，深層防護の観点からこれら beyond design basis の事象に対しても事業者に設計上の対策を要求する規制要件（SBO: 10 CFR 50.63, 1988, ATWS: 10 CFR 50.62,1984）が課されるようになった（本来であれば，単一故障よりも厳しい同時機能喪失（共通原因故障）を新たに design basis として再定義する選択肢もあったはずであるが，実際は従来の design basis が変更されることはなかった）。また，同様にして，beyond design basis 事象への対応が重視され，事業者の自主活動として AM（Accident management）策が整備されるようになった。

このような状況について，福島第一事故の 1 ヶ月前 2011 年 2 月に発足した NRC のリ

スクマネジメントタスクフォース（RMTF, G. Apostolakis NRC 委員主査）の報告書[文献2)]では，

- Design basis に運転経験や新しい知見が反映されていない。Beyond design basis 事象に対して設計対応を規制要求しているにも関わらずこれを design basis としていないのには矛盾がある。
- Beyond design basis 事象への対応に規制要件と事業者自主対応が混在しているのは一貫性を欠いている

という問題点を指摘し，これを「パッチワーク」であったと評価している。そこで RMTF では，"Risk-Informed and performance-based defense-in-depth protections"というキーワードで特徴づけられる，論理的・体系的かつ首尾一貫した安全規制体系を構築することを提唱した。この新しい体系においては，design basis の範疇は "adequate protection category"として従来の規制対応を継続するが， beyond design basis の範疇については "design-enhancement category"と位置づけ，これに対してコストベネフィットを考慮しつつリスク評価に基づいて規制対応することとしている（なお，この対応を越える部分は "residual risk category"と呼ぶ)。

RMTF 報告書では，WENRA の Reactor Safety Reference Levels [文献18)]，或いは IAEA の Draft Safety Guide DS-414 [文献14)]（現在の No.SSR-2/1）の検討状況を引用しながら，この"design-enhancement category"について"design extension conditions"とほぼおなじ概念であると注記している。欧州では，1990 年代から，新型炉において，従来の design basis で対処していなかった複雑な事故シーケンスやシビアアクシデントに対し，これらを"design extension conditions"と呼んで（EUR,1998）[文献15)]，シビアアクシデント防止・緩和の設計対策を行う研究が進められていた[文献16),17)]。このことから，1990 年代～WENRA，IAEA の上記文献発行時期 2008～2010 年前後に，欧州規制機関では"design extension conditions"という概念を用いて beyond design basis 事象に対しても設計対応を要求しようという議論が行われていたと考えられ，その議論を反映した形で NRC の "design-enhancement category" という概念が生じたものと推察される。

年代を少し遡って IAEA の旧設計技術要件である No.NS-R-1 [文献18)]では，プラント状態の分類において，beyond design basis の事故状態を，炉心損傷に至らない事故状態と炉心損傷に至る事故状態との 2 つに分類している。それ以前は，事象を design basis の状態に抑えれば炉心損傷に至らず，design basis を超えればシビアアクシデントに至る，というある意味単純な分類であったが，No. NS-R-1 では，beyond design basis 事象に対しても炉心損傷防止対策をとるという状況が明示された。No. NS-R-1 にはまだ "design extension conditions"という概念はなく，beyond design basis 事象に対しては，アクシデントマネジメント（AM）策によって炉心溶融防止或いは炉心溶融後の放射性物質の放出防止を図る，という考え方であった(Glossary のプラント状態の図には，beyond design basis accidents に対して accident management と記載されている)。

No. NS-R-1 の改訂版である No. SSR-2/1(2012)では，本項冒頭で述べたように "beyond design basis"に替えて新たに "design extension conditions" (DEC) という呼称が与えられた。DEC は，従来の beyond design basis 事象に対しても，予め設計で対処しておくために設定されたものである。実際的にどのような事象にするかは，PRA の知見，最適評価手法などによって特定される。No.SSR-2/1 には，DEC に対して AM 策により対処すべしとの記述はなく，No. NS-R-1 と違って beyond design basis 事象に対して，より設計での対処を重視する考え方になっていると考えられる。また，WENRA の Safety Objectives，new NPP designs [文献5),19)]では，IAEA の No. SSR-2/1 を更に発展させ，新設炉の design basis を従来既設炉の design basis よりも拡大させている。その主な特徴は以下の 2 点である。

- 複数機器同時故障に対しても炉心損傷防止を可能とする設計（レベル 3 の防護条件を旧 design basis の単一故障から複数機同時故障まで拡大）
- 著しい炉心損傷が発生しても格納容器外への放射性物質放出を低く制限する設計（design basis の防護目標を従来のレベル 3 からレベル 4 に拡大）

最近では，No.SSR-2/1 の改訂議論が始まっており，その改訂ドラフト DS-462 [文献20)]では，プラント状態"design extension conditions"を炉心溶融前と溶融後（シビアアクシデント）の 2 つの状態に明確に分類するとともに，DEC を越える状態は "(a) Conditions practically eliminated" とすることを定めている。ここで "practically eliminated" とは，「物理的にあり得ないか又は高い信頼性を持って極めて発生しにくいと考えられ，実質的に考慮から排除される状態」を意味する。従って，No.SSR-2/1 の改訂議論では，"design basis" に対してだけなく "design extension conditions" の事象に対しても，実質的に考慮不要な状態しか残らないような範囲まで，設計での対応を考慮しておく，という考え方に進みつつあるのではないかと考えられる。

以上のことから，深層防護概念の変遷と，NRC における RMTF 報告書での議論，IAEA 設計技術要件の改訂議論，WENRA の安全目的の内容を併せて考えると，DEC ("design extension conditions" (欧州，IAEA)，或いは "design-enhancement category" (米国)) の意義は次のような点にあるのではないかと考えられる。すなわち，原子力プラントの安全確保において，従来，設計ではなくアクシデントマネジメントで対応していた "beyond design basis" 事象に対し，これを工学的判断や決定論的・確率論的評価，最適評価を用いて DEC として捉え直すことによって設計で対処することを考え，それによる residual risk が実質的に考慮から排除できるようにする。簡単に言えば，DEC とは，重大事故に対して，従来のようなアドホックなやりくり（マネジメント）での対処から，予め考慮した設計での対処へとシフトしていこう，という考え方の現れではないかと思われる[12]。

---

[12] 東京電力（株）では，福島原子力事故の教訓から，深層防護の各層（防護レベル）における重要な安全機能（「異常発生防止」，「止める」，「冷やす」，「閉じ込める」）が，外的事象に顕著な共通原因で

3.2.3 各防護レベルの有効性が独立であることの一考察

原子力安全確保の取り組みと防護レベルの関係(3.1.1(1))や多重性，多様性，独立性及び単一故障基準(3.1.2(2))に関連する論点として，各防護レベルの有効性が独立であるということをどのように考えるか，また，各防護レベルの有効性が独立であるということと安全設計における多重性，多様性，独立性との関係をどのように考えるかを考察した。

2.3 において，防護レベルの基本的な分け方を，ある防護レベルの維持，及びある防護レベルが突破されたときの影響の緩和と整理した。このことは，ある防護レベルが突破されたときの影響の緩和は，次の防護レベルの維持と同様の意味であることから，深層防護の基本的な考え方は，ある防護レベルの維持のみと考えることができる。

このような整理に基づくと，例えば 3.1 で述べたような，実証された技術に基づく設計や高い品質管理システムに基づく保守管理等により異常や故障等のトラブルの発生を防止する対策と，異常や故障等のトラブルの検知や原子炉停止機能等により事故に発展するのを防止する対策は，工学的に違った切り口からのものであり，有効性が独立であると考えることができる。

一方，例えば設計基準を超すような事故状態になった場合の対策が，事故に対して ECCS 等の工学的安全施設を用意する対策と同等の考え方（例えば恒設代替設備の要求）に基づいていれば，これらは同じ切り口の対策となり，工学的安全施設の機能が無効になると同時に恒設代替設備の機能が無効となるような脅威に対しては有効性は同等（独立性は低い）と考えられる。ただし，恒設代替設備の多様性や設置場所（位置的分散）などの工夫によって，工学的安全施設等との共通要因故障の可能性を低減できれば，全体としてのリスク低減には寄与することに留意が必要である。

このように，防護レベルの有効性が独立かどうかということは[13]，3.1 で述べたような多重性，多様性，独立性により信頼性を確保すること（各防護レベル内の信頼性）と合わせて議論することが重要である。なお，それぞれに用いられる「独立性」の具体的な方策は，その目的（レベル間またはレベル内の信頼性）により異なり得る。

また，可搬設備の活用は，工学的安全施設等（恒設，自動起動）とは異なった切り口（可搬，手動操作）となるため，可搬設備を活用する時間余裕があるような脅威に対しては有効性が独立であると考えることができる。しかしながら，可搬設備を活用することが必ずしも防護レベルの有効性が独立になるとは限らず，防護レベルを脅かす脅威の

喪失することを防ぐために，従来の多重性による信頼性確保から，多様性や位置的分散を重視した信頼性確保にシフトし，深層防護を強化することを原子炉安全確保の基本方針の１つとしており，同一の層内で更に信頼性を向上させるために設計ベースを超える分類の対策を設定することで，複数の多様な対応手段の選択肢を確保するとしている。この設計ベースを超える分類を，設計拡張状態，DEC (Design Extension Condition) と呼んでおり，従来から欧州で定義している DEC とは異なるものである。
参考文献：「福島原子力事故の総括および原子力安全改革プラン」(2013 年 3 月 29 日，東京電力（株))

[13] 各防護レベルの独立性の考え方は 2.3 で述べている。なお，“independent effectiveness” とは，「ある防護レベルの failure が，他の防護レベルの failure を引き起こさない（他の防護レベルに依存しない (independent)）」という意味である。

特性と対策の組み合せに応じて，各防護レベルの有効性が独立であるかどうかは変わりうると考えるべきであろう。

3.2.4 設計基準を超える外的ハザードに対する取組み

3.2.1で述べた設計要求範囲（設計基準事故・事象に基づく設計範囲）を設定することにより，必然的にそれを超える領域（beyond design basis）が存在することになる。また，3.2.2で述べたように，beyond design basis事象について，リスク評価や最適評価を用いてDECとして捉え直し設計で対処した場合においても，きわめて頻度の低い事象やこれまでに経験のない事象に関しては知識の不完全性による限界があることから，やはりそれを超える領域（beyond design basis）の存在を否定することはできない。したがって，深層防護を適用することによって，そのいずれにも対応できるようにしておくことが重要である。特に，地震や津波を始めとする自然事象に加えて，テロや航空機衝突などの外的人為事象など，設計基準を超える外的ハザードに対しては，設計基準に対する対策は機能を失うことから，当該ハザードの特質を踏まえた異なる質の対策が必要である。すなわち，当該ハザードの影響を受けない設備の設置（ハード）もしくは，アクシデントマネジメントによる柔軟な対応（ソフト）が効果的と考えられる。例えば航空機衝突への対応として，欧州では離隔や残留熱除去システムなどハード面での対策を要求している例がある一方，米国では炉心冷却や格納容器及び燃料プール冷却の機能を維持又は復旧することを目的としたガイダンスや方策の策定・実施を求めている。

航空機衝突に限らず，設計基準を超える津波などの外的ハザードが発生した場合には，恒設の設備が共通的に機能を喪失する可能性が高まる。したがって，対策を施すにあたっては，喪失した機能の回復の可能性を高め，それにより環境中への放射性物質の早期大量放出はもとより，有意な影響を生じるような規模の放出を防止することができるよう，事象進展を遅らせることも質の異なる対策として効果的である。このような場合は，多様な状況に柔軟に対処できる能力（例えば，代替策としての設備の準備や復旧能力）を重視した対策として，基本的には可搬設備や汎用品を活用した代替策等を用意することが有効と考えられるが，事象進展が速く，可搬設備では対応が困難な場合においては恒設設備が必要となることもある。いずれにしても，どのようなハード面もしくはソフト面の設備・対策をどう組み合わせるかについては，ハザード毎の特性に応じて決定することが重要である。また，効果的なリスク低減を図るため，リスク評価を実施し，対策の有効性を確認することも重要である。

また，設計基準を超える外的ハザードに見舞われた場合においても，冷静かつ迅速に，持ちうるリソースを活用することによって有効かつ実効的な対策を行うことが求められるが，こうした対応が実施可能かどうかは，実際の施設についての細部にわたる知識，多様な異常状態における原子炉施設の挙動に関する理解，緊急時における個人並びに組織の対処能力などに大きく依存する。したがって，原子炉設置者等は常々，運転経験や

外的事象等についての最新知見に基づいたリスク評価を行い，各プラント固有の事項を十分に理解した上で，対応のための手順を整備し，十分な訓練を行っておく必要がある。

3.2.5 深層防護の有効性評価

ここでは，深層防護と安全目標の関係(3.1.3(2))に関連する論点として，深層防護の概念が適切に適用されプラントのリスクが適切に抑制されていることを確認するための有効性評価に関して検討する。深層防護の有効性を測る方法，特に定量的に測定する方法については，必ずしも確定された共通認識が得られていないと考えられることから，あるべき姿に関して決定論的手法／確率論的手法或いは保守的評価手法／最適評価手法の関係を含めて考察し，合わせてリスク評価の意義について整理する。

(1)有効性評価のあり方

旧来からの設計基準事故・事象の範囲においては，許容基準を満足することを確認する観点から，これまで主に決定論的な手法が使用されてきた。これを超える範囲においては，多重故障の領域に入り多様な事象が対象となることもあり，事故シーケンス毎の現実的な姿を捉える観点から，これまで主に確率論的な手法が使用されてきた。ここで，設計基準事故・事象では代表事象を選定していること，リスクの一因子である確率の概念がないこと，設計基準を超える領域が実質的にリスクを支配することから，深層防護の有効性を観るには適当ではないと考えられる。また，深層防護のレベルが進むにつれ一般的には事象の発生頻度は小さくなり，その分事象が有する不確かさも大きくなることから，事象を特定して評価する決定論的手法の適用には限界も生ずると考えられる。このようなことから，深層防護の有効性を評価するには，基本的には多くの事故シーケンスや不確かさが扱える確率論的手法がより適するものと考えられる。

また，深層防護のレベルが進むにつれ，一般的には対応策としてのマネジメントの比重が大きくなる。マネジメントの実施にはその場，その場での判断も必要となり，適切な判断のためには事前に現実的な状況の推移を知識ベースとして把握しておくことも重要となる。さらに，多様な事象を扱う場合には保守性のとり方によってはある事象や現象に偏った情報になる可能性もあり，現実的な状況と乖離する場合も考えられる。このような状況に対処するためには，不確かさがあることを意識しつつ可能な限り現実的な評価とすることが求められ，最適評価手法を採用していく必要があろう。

不確かさの要因についてはこれまで幾つか分析されているが，最も扱いに留意すべきことの一つに“unknown unknowns”（未知の未知）の事柄がある。例えば米国NRCのNUREG-2150では，深層防護の考え方に基づく自らの意思決定プロセスを提示しており，その中の「審議」(Deliberation）の過程において，“unknown unknowns”に対する配慮を含む，低頻度で複雑な事象における不確かさと感度に対する検討を求めている。このような検討に基づくリスク情報は，深層防護の有効性を測る上でも常に認識しておくべ

き事項であろう。

(2)リスク評価の意義

従来の決定論的な安全評価では，事象想定や設備の状態，人間信頼性など一定の包絡性を考慮した条件を所与のものとして設定し，安全性のレベルが基準に適合しているかを評価しており，現状の安全性のレベルや安全性を向上させる上での重要なシナリオ・設備を把握することができない。

一方，リスク評価において，現実的に発生しうる様々な状態を考慮し，その状態の生起性を確率で表現することで，安全性のレベル，不確かさやクリフエッジ性を含めたリスクプロファイルを把握することができる。すなわち，リスク評価は，深層防護の十分さと安全性に対する不確かさを把握することに有効なツールであり，原子力施設の安全性の能力を知る重要な手法である**【解説5参照】【解説6参照】**。

リスク評価が深層防護の十分さと安全性の不確かさを把握することに有効なツールである一方で，自然現象を起因としたリスク評価など，ハザードによってはその評価手法が確立していないものがある。また，確立している評価手法においても，改良の度合により成熟度が異なる。したがって，評価の結果として示される数値の信頼性は，評価の対象とするハザードにより異なる。

リスク評価の際は，このような評価手法の限界を認識し，評価手法の成熟度に応じたリスク評価を実践し，安全性向上に活用しながらより良いリスク評価にしていくことが重要である。

また，極端に発生頻度が低い，或いは予見することができないために，安全性を向上させるための対象として考慮されない事象は存在し続ける。例えば PRA (Probabilistic Risk Assessment) は一般にイベントツリーやフォールトツリーを用いて論理的に事象を網羅するアプローチであり，“unknown unknowns”（未知の未知）の事柄は考慮されない。安全性を向上させる上ではリスク評価にも限界があり，そのような事象に対しては，定量的な発生頻度の評価結果ではなく，防護策が無効になることを想定して対策を展開する，守るべきものから逆に辿って対策を展開するなどの安全性を高める取り組みが重要となる。

深層防護の概念を適用した安全確保策はリスク評価を通じて強化され，リスク評価を通じて強化された安全確保策は，さらに深層防護の概念を適用した取り組みにより強化される。深層防護の概念の適用とリスク評価の活用は，安全性を高める上でこのように相補性がある。

3.2.6 原子力安全規制の中で深層防護をどのように考えるか

深層防護は原子力安全を確保するための基本的戦略概念であるので，安全規制における規制要件ではその考え方が抽象的なまま要求されるのではなく，特に事業者に対して

は，安全な炉停止に必要な「止める」「冷やす」「閉じ込める」の 3 機能について深層防護の考え方を反映した具体的な設計や運用などが要求される。深層防護の反映の形としては，IAEA の 5 つの防護レベルに対応した事象発生防止/検知・事象影響緩和・放射性物質閉じ込めに係る設計がオーソドックスな形として理解されているが，それだけでなく，閉じ込め物理障壁の多重化，各防護レベル内における安全関連機能の多重化・多様化，設計・施工・検査・品質保証を一体とした機能性維持方策など，各防護レベルの信頼性を確保する手段も深層防護の反映の形とみることができる。

安全設計の規制要件においては，一つの想定起因事象に対していかなる機器の単一故障（人的過誤を含む）を仮定しても炉心健全性が確保されるように設計せよという，いわゆる「単一故障基準」が，深層防護を確認する手段として要求されている。単一故障基準要件が暗黙の前提としているのは，「安全機能の多重故障の発生確率は極めて小さく事実上起こり得ないので，単一故障基準を満足している限り著しい炉心損傷も事実上起こり得ない」という工学的判断である。以前の IAEA のレベル 3 の防御目標が「起因事象＋単一故障の design basis 内に抑える」となっているのもこの暗黙の前提に依拠していると考えられる。しかしながら，実際には，TMI2 事故，ブラウンズフェリー火災等の経験，或いは交流電源の信頼性評価や Salem1 での原子炉保護系不動作などの運転経験から，安全機能の多重故障は従来想定していたより起こりやすいことが明らかとなっている。そのため，米国 NRC では，多重故障の可能性とその影響の甚大さに鑑み，深層防護の観点から，（TMI2 事故教訓としての）シビアアクシデントにおける水素制御対策，火災防護や全交流電源喪失 SBO 対策，想定過渡時スクラム失敗 ATWS 対策の規制要件化を行ってきた。一方，かつて我が国では，福島第一炉心溶融の一因となった長期 SBO 対策の不備について，送電線の信頼性や非常用電源の信頼性が極めて高いため長期 SBO は起こり得ないとして，対策の規制要件化を見送ってしまったが[14]，深層防護の基本に立ち返れば，設備機能の信頼性が高くてもなお当該機能喪失への対策を規定しておくべきであったはずである[15]。そういう意味で，我が国では深層防護の概念が民間にも規制にも十分に浸透していなかったということになる。

単一故障基準に基づく design basis を維持するのみでは，炉心健全性確保に十分ではないことが明らかになってから，欧米の安全規制や IAEA の設計技術要件では，炉心健全性確保を目的とする防護レベル 3 の条件を多重故障への対処まで拡張するようになっ

---

14 なお，我が国では，米国の SBO 規則 10CFR50.63 のような SBO 対策の規制要件化はされなかったが，「試みに米国の RG1.155 に基づいて我が国の原子力プラントを評価した場合，＜中略＞我が国の代表的な原子力プラントの SBO に対する原子炉の耐久能力は，＜中略＞米国 NRC の SBO 規則に対する条件を満たしている」とされている（「原子力発電所における全交流電源喪失事象について」原子力安全委員会 原子力施設事故・故障分析評価検討会 全交流電源喪失事象ワーキング・グループ，平成 5 年 6 月 11 日）。

15 我が国での造語「前段否定」はこの文脈でのみ用いられる。佐藤一男「改訂 原子力安全の論理」2006 によれば，それぞれの防護レベルで最善を尽くし，前段の防護レベルが堅牢だからといって後段の防護レベルを手加減してはいけない，また，前段レベルが不十分だから後段レベルが必要なのではない，という深層防護の基本的考え方を我が国の言葉で別表現したものである。「それぞれの防護レベルで最善を尽くす」の意は「前段否定」の中に含意されており，厳格な前段否定や厳格でない前段否定があるわけではない。

たと考えられる（例えばIAEAの旧設計基準NS-R-1(2001)に記載されている新設炉のプラント状態には，旧design basis（単一故障基準）を越える事態（多重故障）に対しても炉心健全性を確保する状況が想定されている）。ただし既存炉に対してはすでに従来のdesign basisで設計されているため，それを超える部分（beyond design basis，IAEA SSR-2/1ではdesign extension conditions）に対する対応の一部を“アクシデントマネジメント”として規制要件化している（米国NRCのSBO規則，ATWS規則など）。欧州では，新設炉に対しては，当初からdesign basisのハードルを高めた設計要件を志向している。すなわち，多重故障に対しても防護レベル3の炉心健全性が確保されるような設計とし，さらにレベル3が失敗して炉心溶融となってもその後の閉じ込め措置が可能な装備を持つ設計を要求する考えである（WENRA，“Safety Objectives for New Power Reactors,”（2009），WENRA，“Report Safety of new NPP designs,”（2013））。

以上のような欧米の原子力規制の動きを見ると，これまでの運転経験・知見の蓄積に応じて深層防護の概念を再考し深化させているように思われる。3.2.2で見たような，“design extension conditions”（欧州，IAEA），“design-enhancement category”（米国）を設定することによって重大事故への設計対処を強化する方向性はその現れと言えよう。特に，注目すべき点は，その深層防護の再考・深化の議論が，福島第一事故を契機に始められたのではなく，それ以前から行われていたということである。一方，我が国では，平成22年12月2日旧原子力安全委員会決定「原子力安全委員会の当面の施策の基本方針について」の中で今後の活動の一つとして「原子力安全の基本的考え方の提示」を挙げており，関連して福島第一事故の1ヶ月前に開始された「当面の施策の基本方針の推進に向けた外部の専門家との意見交換『安全確保の基本原則に関すること』」において深層防護の議論も開始された。事故直前の2回の会合（第1回2月16日，3月2日）における深層防護の議論については，IAEA安全原則SF-1や設計技術要件ドラフトDS-414（当時，現在のNo.SSR-2/1），WENRAの安全原則等を題材に，IAEAと我が国との考え方の相違（防護レベルの分類解釈や「層」の数など），新しく登場したDEC概念の解釈，シビアアクシデントの防護レベル内での位置づけ，等，国内外の現状分析が開始されたばかりで，欧米のように深層防護概念の深化とそれに基づいた安全性向上の展望を議論するまでには至っていなかった[16]。今後は，欧米の議論の仕方を参考に，深層

[16] 我が国ではIAEAの深層防護の「level」を，語感の異なる「層」と翻訳して議論しているため，その語感に引きずられて無用の議論を生んでいると思われる。典型的なものは，「炉心損傷は第3層に入れるか第4層に入れるかあいまいで多様な考え方がある」というような議論である。深層防護でいう防護「level」はいわゆる「防御線」であり，当然ながら防御線を破られる前後でプラント状態が変わる。すなわち，プラント状態を分かつ線が防護レベルである。そういうイメージを念頭に置いて考えると，欧米の深層防護レベルの議論はどれも「防護レベル3が成功すれば炉心健全性が確保され，失敗すれば炉心健全性が失われるので放射性物質閉じ込めを目的とする防護レベル4が発動される」という文脈になっていることがわかる。この場合，「炉心損傷は防護レベル3か4か？」という議論にはなりえない。日本では，「層」の語感が例えば地層のような個々の厚みのある層が相接して並んで入る状況を連想させるため，この語感に引きずられて「プラント状態＝防護層」のようなイメージが生まれ（実際，旧原安委や旧原子力安全・保安院の深層防護関連資料には，通常運転状態，設計基準内事故状態，設計基準超事故状態，・・・などのプラント状態にそれぞれ深層防護第1層，第2層，第3層，・・・を当てはめている図がある），そこから「炉心損傷は第3層に入れるか第4層に入れるか」という擬似問題が生じているように思われる。

防護の観点から安全規制の包絡性等に不備・矛盾がないか，如何にすれば不備・矛盾が解消できるか，というような，具体的な安全性向上に結びつく実効的な規制施策の議論を進めていくべきであろう。

4. まとめ

原子力安全の基本的な目的は，原子力の施設や活動に起因する放射線の有害な影響（放射線リスク）から人と環境を防護することであり，不確かさに対する備えである深層防護の概念が重要となる。

本書では，「2.深層防護の考え方とは何か」において，原子力安全のための深層防護の概念（一つの対策では防げないという不確かさを考慮して，放射線リスクから人と環境を護るための防護策全体の実効性（成功確率）を高めるために適用されるもの）を明示し，その際重要となる深層防護における各防護レベルの設定について，その信頼性，独立性（有効に機能すること），レベル間のバランスやそれぞれのレベルでの不確かさに対する備えについての考え方を示した。

深層防護の概念に基づく方策は必ずしも設備や機器などのハードウェアに留まらず，組織や人の力量に係るマネジメントなどのソフトウェアや安全文化に基づいた行動規範など多様なものが含まれる。また，対象とするリスクの内容並びにリスクの不確かさについての認識も，運転経験や知見の蓄積とともに変化していく。常に最新の技術レベルや運転経験，知見を取り入れ，考慮すべき不確かさやそれに対する備え（方策）を継続的に改善することで初めて，安全を効果的に向上させることが可能となる。

次に「3.深層防護の概念の具体的な適用と論点」では，設計要求範囲と設計評価に関する整理や Design Extension Conditions(DEC)の持つ意義等，現時点における主要な論点について関連事項の整理を行い，論点や考え方を取りまとめた。また，安全を達成するために規制が果たす役割は大きい。原子力安全の確保において放射線リスクの低減が重要である以上，規制もまた深層防護の概念に基づく考え方が重要となる。そこで本書では，論点の一つとして，これまでの我が国の規制と深層防護概念との関連（深層防護の概念の適用に対する対策や検討）や最近の欧米の動向を整理し，より高い安全を確保するための規制のあり方に関する方向性を示した。

深層防護の概念は必ずしも固定されたものではなく，時代とともに深化させている。今後も継続して，原子力関係者の間で深層防護の概念の深化ならびに具体的な適用を図ることが，より高い安全を達成するために極めて重要である。

5. 解 説

解説 1：深層防護の考え方について

米国 NRC 発行の NUREG-1860 においては，深層防護の考え方は不確かさに対する備えであるとしており，原子力施設において異常や事故等が発生した場合に被害を防止・緩和するために安全裕度を含む一連の手段を用いることによって不確かさを取扱うために用いられる NRC の安全思想の要素であるとしている。

IAEA の基本安全原則である SF-1 においては，深層防護は事故の影響と緩和の主要な手段として，以下のように記述されている。「深層防護は，それらが機能し損なったときに初めて，人或いは環境に対する有害な影響が引き起こされ得るような，多数の連続しかつ独立した防護レベルの組み合わせによって主に実現される。ひとつの防護のレベル或いは障壁が万一機能し損なっても，次のレベル或いは障壁が機能する。適切に機能する場合，深層防護は，単一の技術的故障，人為的或いは組織上の機能不全だけでは有害な影響につながる可能性がないこと，また，重大な有害影響を引き起こすような，機能不全が組み合わせで発生する確率が非常に低いことを確実にする。異なる防護レベルの独立した有効性が，深層防護の不可欠な要素である。」

また，「軽水炉発電所のあらまし（改訂第 3 版）」では，「人的過誤や人間の思考の未熟性等も考慮して，安全確保対策が高い信頼性を持って目的を達成できるように取込まれている安全設計の考え方が「深層防護」である」としている。

なお，深層防護の考え方について，現時点でも様々な議論が継続されており，この考え方を厳格に定義することは難しいとされている。例えば，米国 NRC の福島第一事故の報告書である「21 世紀における原子炉安全強化に関する勧告」では，以下の記述（INTRODUCTION（P3）より引用）がある。

The Task Force has found that the defense-in-depth philosophy is a useful and broadly applied concept. It is not, however, susceptible to a rigid definition because it is a philosophy. For the purposes of its review, the Task Force focused on the following application of the defense-in-depth concept：・・・

解説 2：深層防護の概念を効果的に適用するための前提条件

IAEA の INSAG-10 では，深層防護の効果的な実行のために全てのレベルにおける全ての措置に適用する前提条件として，以下のように適切な保守性を考えること（conservatism），品質保証及び安全文化があるとしている。

（保守的な考え方）

INSAG-10 で定義する最初の 3 つの防護レベルにおいて，保守的な考え方が広く適用されている。立地の選定，設計，建設，試運転及び運転に対し，保守的な仮定がなされている。また，改善に伴う変更に対するレビュー，経年劣化の評価，定期的な安全評価と緊急時計画の策定，並びに規制審査とそれに続く許認可交付判定においても，適切な保守的仮

定と安全裕度が考慮される。レベル 4 と 5 においては，最適推定による検討の重要性が高まる。

（品質保証）

各防護レベルは，設計，材料，構造物，系統と機器，運転と保全の品質が信頼できる場合にのみ有効となりうる。品質保証プログラムによって，（立地評価，運転系統と安全系統の設計，障壁の設計，変更設計及び安全解析を含む）安全設計が確実にされる。また，品質保証プログラムによって，設計の意図が実際のプラントで達成され。プラントが意図された通りに運転され，設計された通りに保全されることを確実にすることができる。

（安全文化）

各防護レベルに影響を与える活動に関係する組織と個人は，強固な安全文化を醸成する義務を負う必要がある。事業者と政府機関，並びに設計，製造，建設，保守，試験，供用期間中検査，及び緊急時の介入に関係する組織は，適切な要件を満足しており，適切な方法を使用していることを確実にしなければならない。

人的過誤が防御を危険に陥れる潜在的な可能性を含むものである一方，人的な対応は安全運転に必須なものであり，また，専門性と安全文化は，職員が信頼性のある運転をすることや初期段階で異変を検知・防止することを確実にすることに寄与する。さらに，十分な時間と情報があれば，十分に計画されていなかったために機械的に対応することで制御することができない状況においても建設的に対応することができる。優れた人的対応をとるためには，高度な能力と，広範な運転状況に対するシミュレータ訓練を含むトレーニングが必要となる。

なお，保守的な考え方における，レベル 4 と 5 での最適推定による検討の重要性についてはその理由が示されていないが，考察すると，保守的な考え方を適用したレベル 3 までの対策がうまく機能しなかった場合，それらの対策がどのように機能しなかったかによりその後の事象進展の仕方は多数存在するため，レベル 4 以降において有効な対策をとるためには，より現実的に事象進展を把握することが必要となることから，最適推定による検討が重要になるということと考えられる。

解説 3：深層防護と多重障壁の関係

米国 NRC の「21 世紀における原子炉安全強化に関する勧告」では，深層防護は放射性物質の放出に対する多重障壁アプローチの思想とともに NRC が使ってきた思想としており，NUREG-1860 では，過去の深層防護の適用でよく知られているのが多重の物理的障壁の使用（燃料，被覆管，原子炉冷却材圧力バウンダリ，格納容器）としている。

また，IAEA の INSAG-12 では，防護のレベルと物理的障壁（燃料マトリクス，燃料被覆管，一次冷却材バウンダリ，閉じ込め）は深層防護の構成要素としている。

以上から，多重障壁は，その考え方については深層防護の考え方とともに原子力安全を

確保するために用いられる考え方の 1 つであり，具現化された多重障壁は深層防護の考え方に基づく対策の一部を構成するものである。すなわち，深層防護と多重障壁は原子力安全の観点から密接に関連するものの，同義ではない。

解説 4：設計における外的事象への深層防護の適用

IAEA の INSAG-10 では，深層防護の概念は，内的事象及び外的事象に対してバリア（燃料マトリクス，燃料被覆管，原子炉冷却材圧力バウンダリ，格納容器）の健全性を防護することに適用するとしている。第一のレベル（通常運転からの逸脱と故障の防止）は内的事象及び外的事象に対する防護の最初の基準を規定するものであるとし，第三のレベル（設計基準内での事故の制御）では外的事象によるシステムの共通原因故障の防止を求めている。

また，IAEA の NS-R-1 では，発電所の設計要件として，設計条件とすべき外的事象を決めることを要求しており，炉心及び原子炉容器内にある内部機器は，設計基準の外的事象に対して想定される静的及び動的荷重に耐えられるよう設計・設置することを求めている。

なお，IAEA の INSAG-12 では，システム設計における配慮によりクリフエッジ効果を防止することが示されている（INSAG-3 でも同じ記載）。

一方，わが国において，これまでの原子力安全委員会の耐震指針では，「耐震設計上重要な施設は，敷地周辺の地質・地質構造並びに地震活動性等の地震学及び地震工学的見地から施設の供用期間中に極めてまれではあるが発生する可能性があり，施設に大きな影響を与えるおそれがあると想定することが適切な地震動による地震力に対して，その安全機能が損なわれることがないように設計されなければならない。」とし，耐震設計方針として，例えば S クラス施設については，基準地震動による地震力に対してその安全機能が保持できることを要求していた。

また，同指針において，津波に関しては地震随伴事象に対する考慮として扱っており，「施設の供用期間中に極めてまれではあるが発生する可能性があると想定することが適切な津波によっても，施設の安全機能が重大な影響を受けるおそれがないこと。」としていた。

このような安全確保の考え方に関連し，「原子力安全の論理」（佐藤一男）では，自然現象に対する対策例として，地震に対しては地震力に耐えられるように建造する，津波に対しては十分に高い所に施設を配置する，台風に対してはそれによる地すべりや山崩れなどについて防止対策を厳重に行うとしている。そして，これらの対策の目標は，「予見し得る自然現象に対して，安全確保上重要な機器が必然的に失われること（これを「システマティック・フェーリュア」と呼んでいる）の可能性を，無視できるほど低くするということである」としており，自然現象については，あるレベルの防護策をとることで共通的に設備が故障することを防止し，残る偶発故障に対して内的事象の中で取り込んで考えるという整理がなされている。

以上から，設計基準の外的事象に対しては，国内外ともに深層防護の概念に基づき対策

することになっているが，設計基準を超える外的事象に対する具体的な取り組みを明確にしたものはこれまでには見受けられない。

なお，複数の防護レベルが同時に喪失することに対して，例えば平成24年に当時の原子力安全・保安院から示された新たなシビアアクシデント対策規制の基本的な考え方において，複数の防護レベルが無効になっても包括的な放射性物質拡散抑制対策や防災を含む対策を用意しておくなどの考え方が示されている**【添付資料**参照**】**。

解説5：リスク評価と深層防護の関係

米国NRCのNUREG-2150では，リスク情報を活用したパフォーマンス・ベースの深層防護（Risk-informed and performance-based defense-in-depth）を特徴付ける1つとしてリスクを挙げており，リスク評価は深層防護の適切さを測るための有効な手段としている。この中では，リスク評価により以下がもたらされるとしている。

- 原子炉施設の安全性を脅かす多様なハザードを評価するための体系的なアプローチ。
- 特定されたハザードに対する原子炉施設の設計・運転の能力を特徴付けるための論理的な手法。
- ハザードとそれへの対応の失敗の組み合わせによる影響を評価するための手法（従来のアプローチでは限定的で定型化した事故シナリオが考慮されるところ，数千の現実的な事故シーケンスが調査される）。
- ハザードの発生頻度と対応の失敗確率，及び失敗することによる影響を評価するためのモデル。頻度と確率は定量的に評価することができる。
- リスクに寄与する事故シーケンスの順位，構築物，系統，機器（SSC）の順位。
- 事故シーケンスとSSCの順位を通じた，リスク上本当に重要なものに焦点を当てるために必要なリソース配分をするためのリスクマネジメントへの貴重な情報。

また，リスク評価の1つであるPRAは，設計や運転が安全目標を満足していることを確実にするために，プラントのリスクプロファイルを評価するために使うことができ，さらに，あるバリアが喪失，もしくはある設計値（例えば溢水レベル）を超えることで炉心損傷や放射性物質の環境中への放出に直接結びつくような潜在的なクリフエッジ効果を特定することができるとしており，PRAは深層防護をより定量的に特徴付けする機会をもたらすものとしている。

解説6：ストレステストの意義

ENSREG（European Nuclear Safety Regulators Group）のストレステスト仕様によれば，ストレステストは深層防護のロジック（起因事象，安全機能喪失，シビアアクシデント）に基づき選定した防止策・緩和策を確認するものであり，プラントの安全機能に影響しシビアアクシデントを引き起こすような極端な自然事象において，防御ラインが次々に喪失したと仮定して，クリフエッジ効果などを確認するものである。

このようにストレステストは外部事象に対するプラントの脆弱性を増すような潜在的な問題を同定し，それを改善する必要があることを示すものであり，原子力施設の安全性の能力を知る手法として重要である。

参 考 文 献

1. 全 般

1) 「改訂 原子力安全の論理」佐藤一男，日刊工業新聞社，2006年
2) NUREG-2150, "A Proposed Risk Management Regulatory Framework", USNRC, April 2012.
3) 「福島第一原子力発電所事故に関するセミナー」報告書，2013年3月，日本原子力学会
4) SECY-77-439, "Single Failure Criterion", USNRC, August 1977.
5) "Safety of new NPP designs", WENRA RHWG Report, March 2013.
6) 「会議報告『2013年春の年会』倫理委員会セッション報告」，日本原子力学会誌 Vol.55, No.8 (2013)
7) AESJ-SC-S001:2008「統計的安全評価の実施基準:2008」日本原子力学会
8) IAEA Safety Standards, Specific Safety Requirements, No. SSR-2/1, "Safety of Nuclear Power Plants: Design", Vienna, 2012.
9) J.N.Sorencsen, "Historical Notes on Defense in Depth", Memorandum to ACRS members, USNRC, 1997.
10) IAEA INSAG-3, "Basic Safety Principles for Nuclear Power Plants", Vienna, 1988.
11) WASH-1250, " The Safety of Nuclear Power Reactors (Light Water-Cooled) and Related Facilities", U.S.AEC, 1973.
12) R.J. Breen, Deputy Director of EPRI's Nuclear Safety Analysis Center, "Defense in Depth Approach to Safety in Light of the Three Mile Island Accident", Nuclear Safety, Vol. 22, No.5, Sept.-Oct. 1981.
13) "WENRA Reactor Safety Reference Levels", WENRA RHWG, January 2008.
14) IAEA DS-414, "Draft-Safety of Nuclear Power Plants: Design", Vienna, September 2010.
15) The European Utility Requirements for LWR nuclear power plants, 1998.
16) Gian Luigi Fiorini, *et.al.* "The Current CEA/DRN Safety Approach for the Design and the assessment of Future Nuclear Installations", 7th ICONE, Tokyo, 1999.
17) Gianfranco Saiu, *et.al.* "European Passive Plant Program Preliminary Safety analysis to Support System Design", 7th ICONE, Tokyo, 1999.
18) IAEA NS-R-1, "Safety of Nuclear Power Plants: Design", Vienna, 2000.
19) "Safety Objectives for New Power Reactors Study", WENRA RHWG, December 2009.

20) IAEA DS-462, "Amendments to GSR Part 1, NS-R-3, SSR-2/1, SSR-2/2 and GSR Part 4 – Draft 5", Vienna, July 2013.
21) 「福島原子力事故の総括および原子力安全改革プラン」東京電力株式会社, 2013年3月29日
22) 10CFR50.63 "Loss of all alternating current power", USNRC, June 1988.
23) RG1.155 "Station Blackout", USNRC, August 1988.
24) 10CFR50.62 "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants", USNRC, June 1984.
25) 「原子力発電所における全交流電源喪失事象について」原子力安全委員会 原子力施設事故・故障分析評価検討会 全交流電源喪失事象ワーキング・グループ, 平成5年6月11日

2. 解 説

26) NUREG-1860, "Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing", USNRC, December 2007.
27) IAEA SF-1, "Fundamental Safety Principles", Vienna, 2006.
28) 「軽水炉発電所のあらまし」改訂第3版, 原子力安全研究協会, 2008年
29) "Recommendations for Enhancing Reactor Safety in the 21st Century; The Near-Term Task Force Review of Insights from the Fukushima Dai-Ichi Accident", USNRC, July 12, 2011.
30) IAEA INSAG-10, "Defence in Depth in Nuclear Safety", Vienna, 1996.
31) IAEA INSAG-12, "Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev.1", Vienna, 1999.
32) IAEA NS-R-1 "Safety of Nuclear Power Plants: Design", Vienna, 2000.
33) 「原子力安全の論理」佐藤一男, 日刊工業新聞社, 1984年
34) NUREG-2150, "A Proposed Risk Management Regulatory Framework", USNRC, April 2012.
35) "EU Stress Tests specifications", ENSREG, 31 May 2011.

AESJ-SC-TR005(ANX):2013

日本原子力学会標準委員会

原子力安全の基本的考え方について
第Ⅰ編　別冊　深層防護の考え方

2014年5月20日　初版　第1刷発行

発行所　一般社団法人　日本原子力学会
（〒105－0004）東京都港区新橋2－3－7
（新橋第二中ビル3階）
電話（03)3508-1263；FAX (03)3581-6128