平成２９年度

原子力の安全規制の最適化に関する研究

特重施設の保全の在り方について

平成３０年３月

一般社団法人　日本機械学会

イノベーションセンター　研究協力事業委員会
原子力の安全規制および対応にかかる調査分科会

動力エネルギーシステム部門
原子力の安全規制の最適化に関する研究会

Ⅰ　まえがき

本研究会では今年度、特定重大事故等対処施設（以下、「特重施設」という）の保全の在り方について検討を実施し、研究会意見として纏めた。但し、特重施設に関する一般的な情報を扱う上で、特重施設に関する資料、情報は一切開示、共有せずに議論を行うこと、特重施設に関する議論のために使用する資料、情報は開示制限を必要としないものに限定されるものの、特重施設のセキュリティ確保の重要性に鑑みそれらについても原則として開示せず、開示する場合は本研究会責任者の承認を得ること、を本研究会で申し合わせ、その旨を誓約書として作成した。

以上のような慎重な取り扱いを行って検討を進めた結果について、本報告書にまとめるとともに、日本機械学会ホームページに公開した。なお、上記にあるように、本検討結果については、開示について、本研究会責任者の承認を得ている事を付記する。

日本機械学会 原子力の安全規制の最適化に関する研究会

特重施設の保全の在り方について　研究会意見

●特重施設の規制要求上の位置づけ

「実用発電用原子炉及びその付属施設の位置、構造及び設備の基準に関する規則」第４２条（特定重大事故等対処施設）によると、特重施設はテロによる格納容器の破損を防止することを目的としており、海外がテロの予防に注力している（できる）のと比較すると、国内ではテロの影響を緩和する役割として特重施設が位置づけられていると考えられる。規制要求の点から特重施設の機能要求を整理すると、特重施設は SA(Severe Accident)設備のセーフティ機能の一部と同等の能力を有するものの、本来はテロ対策の一環として格納容器の破損を防止するセキュリティとしての機能を担う施設と解釈される。ただし、同規則３９条第１項第４号において特重施設は設計基準地震に対し一定程度の裕度をもって「重大事故等に対処するために必要な機能が損なわれるおそれがないものであること」を求められている。（４０条津波も同様）

１．特重施設の保安規定の在り方

1.1 管理運用について

セキュリティ機能としての位置づけなので、特重施設の保安規定は一式まとめたものを独立して作成し、非公開とすべきであると考える。PP(Physical Protection)規定の内容を踏まえ PP 設備に準じた運用管理とする。セキュリティを考慮し情報公開（プラント停止情報含む）につながるような措置は望ましくないと考える。

1.2 作成・記載方針について

特重施設用の保安規定において、現状の保安規定の内容と共通する部分は極力呼び込むことで対応し、特重施設固有のものは別冊扱い等新規に作成する（例として運転管理の条項）。

1.3 留意点

特重施設を既設設備に繋ぎこむ場合、経路とバウンダリの考えによって、既設または特重機器がセーフティとセキュリティの両方の機能を要求される場合が想定される。（例えば、既設配管の格納容器バウンダリ外側に特重施設配管を接続した場合、既設の隔離弁の作動は特重施設の機能を果たすうえで必要になることから、DBA(Design Basis Accident)としてのセーフティと特重としてのセキュリティ両方の機能を要求される。別の例では特重施設配管を格納容器バウンダリに接続した場合、特重施設配管上の最下流の弁は格納容器隔離弁の機能を要求されることから、セーフティ・セキュリティの両方の機能を要求されることになる。）

- 特重施設の要求のみが適用される場合

  特重施設用の保安規定には、後述する特重待機上の制限（LCS : Limiting Condition for Security）の逸脱、LCS 逸脱許容時間、特重施設の復旧完了時間を記載する。これ

により、セキュリティの要求は、特重施設用の保安規定で一元的に管理される。

- 特重施設と DBA 設備の両方の要求が適用される場合

  特重施設用の保安規定には、セキュリティの管理として、特重待機逸脱（LCS 逸脱）、LCS 逸脱許容時間、特重施設の復旧完了時間を記載する。一方、セーフティの管理（LCO(Limiting Condition for Operation)、AOT(Allowed Outage Time)等）は、現状の保安規定で規定されているためこれを呼び込むものとする。これにより、セキュリティの管理は特重施設用の保安規定、セーフティの管理は現状の保安規定で管理される。

  また、特重施設用の保安規定は上述した設備機器の運転管理と併せて、異常時の措置や緊急時の措置等の項目にセキュリティの視点を取り入れ、現状の保安規定とのインタラクションを意識した防災体制や教育訓練等ソフトウェア面を記載すべきと考える。

２．特重施設待機逸脱（LCS 逸脱），逸脱時に要求される措置とその許容時間，復旧完了時間の考え方等

※以下の考え方は安全上の要求を満足していることを前提とする。

2.1 特重待機逸脱の考え方

セーフティの思想から規定された現在の LCO の運用をそのまま特重施設の運用に適用すると、特重施設が不適合等により待機逸脱（特重待機逸脱）したときに対外的に逸脱宣言することとなり、これはセキュリティ上望ましくない。よって、現行の LCO とは異なる特重待機逸脱の考え方（LCS 逸脱の考え方）を新たに設定する必要があると考える。また、特重待機逸脱はセーフティではなくセキュリティ上の問題であるので、逸脱時の措置の結果としてプラント停止することは情報統制上からも不適切であると考える。

2.2 逸脱時に要求される措置とその許容時間

運転中保全等、特重施設を計画的に待機除外する場合、待機除外によるセキュリティレベルへの影響評価を行い、レベルの低下を保障する手段を講じる必要がある。

また、特重設備機器の故障等計画外の待機逸脱が発生した場合、安全機能ではなくセキュリティレベルの改善が必要であることから、プラントを停止するのではなく計画時と同様レベルの低下を保障する手段を速やかに講じる必要がある（例えば可搬の SA 設備による待機等）。この時、可搬の SA 設備の待機状態が確立できない場合は、警備の増強／警察・機動隊等への連絡や監視の増強等によるセキュリティレベル改善措置も考えられる。また、特重施設待機逸脱時には、その重要度に応じて NRA(Nuclear Regulation Authority)への報告も考慮する。なお、LCS 逸脱許容時間は極力早期のセキュリティレベル改善が望ましいことから「速やかに」と定義し、具体的な措置内容は、PP の思想（PP の重要度の考え方を含む）やプラクティスに則り事業者個別に設定するものであると考える。また、逸脱時への対応に備えて、教育・訓練等の充実も必要と考える。

2.3 特重施設の復旧完了時間の考え方

前述の通り、特重施設の待機逸脱（LCS 逸脱）が許容される時間はセキュリティレベルの確保を可能な限り早急に達成する必要があるので、“速やかに”と定義されるべきである。

一方、故障や保全のために待機除外している特重施設を復旧完了させるまでの時間を考える時、2.2 節の措置が完了した時点でセキュリティレベルの確保・維持がなされていることから機能的には問題ないので、復旧完了時間に対する制限は特にない。ただし、非常時体制でセキュリティレベルを維持し続けることは事業者にとって負荷が高いこともあり、早期に復旧完了し本来の特重施設待機状態に戻すことを目指す。

2.4 懸案

- LCO（運転上の制限）の単語を用いると従来の LCO の考え方を強く引きずるため、特重待機上の制限（LCS：Limiting Condition for Security）という表現としたが、この表現で良いかどうか議論が必要。

表　現状および特重施設用の保安規定の関係※

※以下の考え方は安全上の要求を満足していることを前提とする。

	現状の保安規定	特重施設用の保安規定
記載方針	従来と同様	現状の保安規定と共通する内容は呼び込むことで対応し、特重施設固有の内容は特重施設用の保安規定で扱う
公開の是非	公開	非公開（PP 規定に準じる）
記載対象設備	運転上の制限(LCO)を満足するための設備(特重施設として追設されたもののうち、LCO の対象となる設備も含む)	特重施設の機能を要求される設備（既設設備のうちで特重施設の機能を要求される設備を含む）
記載事項例	セーフティ機能の観点から LCO，逸脱時に要求される措置，AOT 等の管理項目を記載 （セーフティの管理）	セキュリティ機能の観点から LCS（Limiting Condition for Security），逸脱時に要求される措置，LCS 逸脱許容時間，復旧完了時間等の管理項目を記載（セキュリティの管理）
運用上の制限	従来と同様、原子炉の状態について LCO が設けられる	特重施設の待機状態について、例えばセキュリティ上の制限（LCS）を新たに設ける。
逸脱時に要求される措置	セーフティ機能として必要な措置を講じる。	セキュリティレベルの低下を保障するため可搬の SA 設備の待機や警備の増強／警察・機動隊等への連絡等、ハード面に加えソフト面での措置をとる。

	現状の保安規定	特重施設用の保安規定
逸脱の宣言及びプラント停止の是非	LCO 逸脱の宣言および、条件によりプラントを停止させる	セキュリティ上の観点から、LCS 逸脱を宣言すること、および逸脱時の措置の結果としてプラント停止することは情報統制上から不適切。ただし、重要度に応じて NRA への報告を考慮する。
許容待機除外時間の考え方	炉心損傷確率に応じた AOT を設定する	セキュリティの改善は速やかに実施されるべきであるので「速やかに」と定義する。
設備機器の復旧までの時間	AOT の間に復旧できない場合は基本的にプラントを安全停止する。	セキュリティレベルが維持されるのであれば復旧完了時間の制限はないが、早期復旧完了を目指す。
留意点	●DBA/SA 設備と特重施設の両方の要求が適用される設備については、セーフティ面の管理は従来の保安規定に記載し、セキュリティ面の管理は、特重施設用の保安規定に記載する。	
	●特重施設用の保安規定には、異常時の措置や緊急時の措置等の項目にセキュリティの視点を取り入れ、現状の保安規定とのインタラクションを意識した防災体制や教育訓練等ソフトウェア面を記載すべきと考える。	

３．特重施設のバックアップ等(他の設備との関係等)を踏まえた保全の在り方

3.1 考え方

特重施設はセキュリティとしての機能を要求されているので、セキュリティ機能を代替可能な手段を講じることで運転中保全を適用可能とする考え方もある。規制要求の系統数ｎを満足するために、待機除外にした時のセキュリティレベルを維持すること、例えばセキュリティ機能に対応可能なSA可搬設備や監視人員体制強化等でセキュリティレベルを保障することで運転中保全を許容するような、補修の自由度を上げることが望ましい。

3.2 懸案

設備設計の要求として、特重施設は設計基準地震・津波に対し一定程度の裕度を要求されている。SA 可搬設備はセーフティ、セキュリティのどちらも対応可能であり、要求ｎを満足する条件で特重施設のバックアップとなりうるが、それらにより特重施設を運転中保全する時、SA 設備の設計基準を超える一定程度の裕度内の地震・津波が発生した場合の対応について考え方を整理しておく必要があると思われる。

また、特重施設の運転中保全を実施するための作業要領や手順を整備すると共に、作業員の訓練等ソフトウェア面から見た保全の在り方も今後検討する必要があると考える。

４．特重施設の運用時の位置づけ

4.1 保全での活用の考え方

- 特重施設で SA 設備の機能をバックアップする場合（例えば、特重施設をバックアップとして SA 設備を運転中保全する等）、規制要求上では炉心損傷防止機能を除いたセーフティ機能を特重施設でバックアップすることは可能である。この時、セキュリティ機能は常に“待機状態”であるため、セーフティ／セキュリティ機能への規制要求を個別に満足すると考えることができる。
- SA 設備のセーフティ機能のバックアップ中にテロが発生した場合、セーフティ機能をバックアップしていた特重施設はそのままテロ対応へと自動的に移行（規制要求であるセキュリティ機能を発揮）することとなる。

以上のことから、深層防護としての独立性を確保した上で、SA 設備のバックアップとしての活用が可能であると考えられる。

4.2 課題

- 特重施設を実際に運用する時、特重施設を規制基準で示しているタイミング（航空機衝突その他テロ発生時）のみで使用するのか、それとも SA 時にも最優先で使用するのか、様々な事象を想定した訓練等により対応力を強化していく必要がある。
- 特重施設を SA 設備の機能のバックアップとして活用するとき、それぞれの情報管理レベルを考慮した管理運用を検討する必要がある。

５．Beznau 発電所（スイス）のバンカーシステムの調査を踏まえた考察

5.1 バンカーシステムの位置付け

バンカーシステムは、地震、洪水、強風、火災、内部溢水、航空機衝突に起因した事故に対して炉心損傷の防止を目的とした施設であり、2 トレインある既設安全系に対する更なる安全性向上及びセキュリティ対応の位置付けとして追加で設置された安全系トレインと考えられる。したがって、日本の特重施設（セキュリティ対応及び一部 SA 設備のバックアップ）とは役割が異なるものと解釈できる。実際、Beznau 発電所ではバンカーシステムの導入により、CDF が顕著に向上している。

5.2 特重施設とバンカーシステムのメンテナンス、LCO、AOT の考え方

Beznau 発電所では、全燃料取出中の方が低リスクという考え方に基づき、バンカーシステムのオンラインメンテナンスを実施していない。また、バンカーシステムの LCO および AOT は Tech. Spec.にて規定されている。これは 5.1 節に示すように、バンカーシステムが追加の安全系トレインの位置づけでありプラントのリスク低減に大きく寄与するためと考えられる。日本においては、DBA 設備および SA 設備により十分なリスク低減効果が期待できることから、バンカーシステムと同様の LCO や AOT、メンテナンス方法を特重施設に

設定する必要はないと考える。ただし、日本の特重施設が Beznau 発電所のバンカーシステムのように、リスク低減に大きく寄与する場合はその限りではないと考える。なお、セキュリティ機能としての特重施設待機逸脱（LCS）、LCS 逸脱許容時間、特重施設の復旧完了時間は、2 章に示す通り考慮する必要がある。

5.3 まとめ

日本の特重施設は航空機衝突およびテロによる格納容器の破損を防止することを目的としたセキュリティの機能及び一部 SA 設備のバックアップを担う施設であり、セーフティとしての機能要求は基本的に常設および可搬の SA 設備で満足するものである。したがって、本研究会で議論した結果と本調査結果を比較、考察した結果、上述の 1～4 章で示した検討結果は妥当であると考える。ただし、特重施設がリスク低減にどの程度寄与するかは今後議論していく必要があると考える。

以上

＜SA設備を特重施設でバックアップする時の考え方（例）＞

４章の特重施設の運用時の位置づけの内容を以下に図式化

A.　通常運転時の規制の機能要求

規制要求		セーフティ	セキュリティ
SA設備	常設	○	－
	可搬	○	○
特重施設		－	○

○ 機能要求を満足
△ 待機除外中
－ 機能要求なし

B.

SA設備を特重施設でバックアップすると設定した時（SA設備の運転中保全を実施等）

規制要求		セーフティ	セキュリティ
SA設備	常設	△	－
	可搬	○	○
特重施設		○※1	○

・セキュリティとしては、SA設備の可搬と特重施設で要求ｎを満足する

・セーフティとしては、SA設備の常設/可搬と特重施設で要求ｎを満足する

・特重施設をセーフティ機能のバックアップとしても、セキュリティの機能は待機状態であるため同時にセキュリティの機能要求を満足する。

C.

SA設備を特重施設でバックアップ時にテロ発生（SA設備の運転中保全時にテロ発生等）

規制要求		セーフティ	セキュリティ
SA設備	常設	－※2	－
	可搬	－※2	○
特重施設		－	○

・特重施設でSA設備をバックアップ時にテロが発生しても、特重施設のセキュリティ機能は上記Bより待機状態であるため、そのままテロ対応機能へと自動的に移行

※1 セーフティ上の機能要求はないものの、炉心損傷防止機能を除きSA設備と同等の機能を一部有する。

※2 設計上、セーフティとして機能要求を満足することは期待しない。

許認可上のセーフティ／セキュリティに対する各設備への機能要求マトリクス

＜PWR/BWR合本版＞

		セーフティ										セキュリティ		
		事故事象					内的・外的事象							
事故事象及び内的・外的事象		設計基準事故	炉心損傷防止	PCV破損防止	SFPにおける燃料損傷防止	停止時の燃料損傷防止	地震	津波	その他自然現象	内部火災	内部溢水	APC	その他テロ	大規模損壊
DBA設備		○	－	－	－	－	○	○	○	○	○	－	－	－
SA設備	常設	－	○	○	○	○	△*1	△*1	△*1	△*1	△*1	－	－	－
	可搬	－	○	○	○	○	△*1	△*1	△*1	△*1	△*1	○	○	○
特重施設		－	－	－	－	－	△*2	△*3	△*1	△*1	△*1	○	○	－

○ 機能要求あり
△ 内的・外的事象発生中での機能要求なし（事象静定後は機能要求あり）
－ 機能要求なし

*1 設備設計の要求として、設計基準と同じものを適用
*2 設備設計の要求として、設計基準地震に対し一定程度の裕度を要求
*3 設備設計の要求として、設計基準津波に対し一定程度の裕度を要求

特重施設の要求について

上記の整理より、特重施設はセキュリティーの観点での要求であると整理できる。 なお、特重施設への設備設計の要求として、地震津波に対しては、設計基準に対して一定程度の裕度を有することが要求されている。