運転プラントにおけるシステム安全の考え方

Concept of System Safety on Operating Nuclear Power Plant

法政大学	宮野　廣	Hiroshi MIYANO	Member
東京大学	山口　彰	Akira YAMAGUCHI	Non-member
東京大学	出町　和之	Kazuyuki DEMACHI	Member
大阪大学	高田　孝	Takashi TAKATA	Non-member
原子力学会	荒井　滋喜	Shigeki ARAI	Non-member
三菱総合研究所	杉山　直紀	Naoki SUGIYAMA	Non-Member

Abstract.:

The total system design on Nuclear Plant ensures “Nuclear safety” with making practically achievable efforts to prevent and mitigate nuclear and radiological accidents. The performance based system design with “Defence in depth (D-I-D)” has been laid out as the key means in “preventing accidents”, “controlling escalation to serious consequences”, and “preventing harmful consequences to the public”. D-I-D is extended to the management of severe accidents, and is an approach intended to provide protection against the development of a wide variety of events by means of redundant, diverse and independent protective barriers. It is crucial to maintain plant integrity with mass quantity of radioactive material present in reactor core, against potential consequences (risk) on people and the environment caused by external hazards, particularly, earthquake and tsunami. The fundamental approach on D-I-D is to address uncertainties by means of successive measures, so that if one measure fails, other, or subsequent measure will be available to ensure safety. Risk analysis should be conducted to validate and enhance reliability of the defence barriers against consequences on people and the environment.

Keywords: Resilience Index, Safety Assessment, Severe Accident, Accident Management, and System Safety

１．はじめに

わが国でも、様々な自然災害の脅威がある。

2007 年 7 月 16 日、新潟県中越沖地震が発生し、東京電力柏崎刈羽原子力発電所が被災した。変圧器火災の映像のセンセーショナルな印象や原発震災という見出しなどにより、地震に対する原子力発電所の安全性について国民の間に不安感が広がったが、柏崎刈羽原子力発電所は、その後の調査も含めて、全号機とも安全に停止し、原子力安全に関する特段の問題は生じなかったことが明らかとなっている。

一方、2011 年 3 月 11 日に発生したマグニチュード９の東北地方太平洋沖地震によって発生した巨大津波が太平洋沿岸の５ヶ所の原子力発電所を襲い、東京電力福島第一原子力発電所では、大量の放射性物質を放出する未曾有の大事故(過酷事故)を引き起こす事態となった。

社会は原子力が持つリスクがどのように顕在化するのかを経験することとなった。地震はその振動伝播による災害のみならず、地震の随伴事象である津波や、山崩れなども重大な災害をもたらすことがわかったのである。

連絡先:宮野 廣、〒212-0013 川崎市幸区堀川町 72-21 R1309、法政大学大学院デザイン工学研究科、
E-mail:hiroshi,Miyano.77@hosei.ac.jp

この新たな経験は、自然災害によるリスクへの取り組みを考えさせるものであった。

福島第一原子力発電所の事故は、原子力の利用はリスクを伴うものであることを明瞭に示した。自然の脅威が原子力発電所を原子力事故にまで進展させることを如何に防ぐか、また様々な自然現象による原子力事故への進展を如何に防ぐか、が重要な課題となっている。

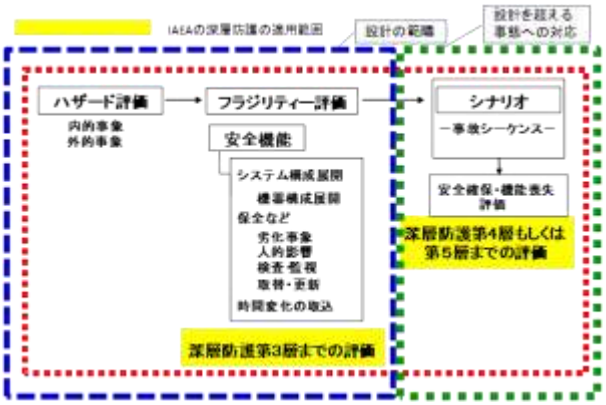
２．システム安全の考え方

「安全」の適用が複雑になってきた原子力発電所では、全体のシステムとしての原子力安全の確保を考えなければならない。系統的に安全確保を確認する仕組みについて、その考え方を **Fig.1** を参照しながら以下にその構成の概要を示す。

設計の範疇では、原子力発電所の安全機能が適切に維持されているか、を評価する仕組みである。すなわち、自然災害、特にわが国では地震や津波、火山活動などがあるが、これらの脅威が原子力発電所に害を及ぼすハザードとして、それに対する耐性が求められる。原子力発電所が持つ安全の基本機能をシステムとして見た時に、関連する機能と合わせて、安全確保の機能が維持される

信頼性を評価する。ここに時間の要素を入れ、材料の劣化や寿命などによるシステムとしての機能が劣化することを評価し、信頼性の低下を求めるために、システムの運用時の対応として、保全の要素を取り入れることで、現実にどのような保全ー材料の取替、検査、機器の改善などーを施せば、機能の劣化を防ぎ、信頼性が確保されるかを示すことができる。

設計を超える事態への対応の領域では、自然現象は予想もつかない事態もあることを前提に、想定を超える、すなわち設計条件を超える事態に対して、原子力発電所が事故に至ることを防ぐ様々な手立てを打つことを示している。設計を超える事態は、一律に定まらないものである。様々に想定して、考えられる様々なシナリオに対する方策を考える必要がある。それらの事態に対応して、



十分な耐性を得て安全を確保しなければならない。

Fig.1 Concept of Safety Evaluation on Design Phase and Beyond Design Phase

３．深層防護による安全確保

深層防護は，原子力安全の最も重要で基本的な考え方あるいは概念であるとの世界各国の共通認識が認められる。その考え方は，安全の確保に有効で現実的なさまざまな方策とそれらの適切な組み合わせを示唆するものである。これまでも将来も、その意義と役割は変わらないであろう。深層防護とリスク評価とがあいまって有益な安全確保に係る洞察が得られる。深層防護は、原子力安全において公衆と環境を防護するための有益な概念であり、方法である。

3.1 原子力利用における「深層防護」による安全確保とは

原子力においての安全確保の基本は、本来、危険な存在である放射性物質を大量に内在するものであり、それを放出し、環境や直接、人への影響を与え得るリスク、すなわちその可能性をいかに防ぐかということである。多くの設備、システムにおいては、その設計において、設備の損傷や破壊を防ぐことはもちろん、使う人、周囲の人に危害を及ぼさないように十分な配慮がなされ、品質管理などを含めて、設計条件を厳しく与えることで、多くの場合はそれが実現されている。原子力発電設備の設計と建設、日常の運用管理において、以下のように安全確保がなされてきた。

3.2 原子力発電所の設計、建設における安全確保

第一には、異常の発生を防止する観点から、十分な余裕と品質の確保、点検検査の充実があげられる。第二には、異常の発生に対して監視を十分にして、いち早く炉を停止することで、異常の事故への拡大を防いでいる。第三には、万が一重大な事故に至る事態となったとしても、事故を軽微なものとしてその影響を少なくし、十分な冷却と、放射性物質の閉じ込めを確実に行うことである。これにより、原子力事故と言われる、放射性物質の施設外への放出とそれに伴う人への放射性物質の影響を阻止するべく、様々な方策を施している。このように「多重に防護する」ことで、「原子力発電は安全である」としてきた。

これらは、いずれも設計における多重防護の仕組みであり、原子力発電プラントの設計で、事態を想定した範囲においての、事故を回避する仕組みである。

3.3 設計条件を超える事態への対応

深層防護の本質は、想定を超えた場合の対応を含めて考えることにある。東日本大震災での想定を大幅に超える津波の到来への対応がまさに、この想定外への対応の不十分さが事故をもたらすということを示したものであった。すなわち、深層防護は、設計で考えてきたこと、設計の想定範囲、設計条件の範囲を超える事態への対応という観点で、最終的に守らなければならない安全確保の目的、原子力事故を未然に防ぐという視点での安全を確実する、最も重要な考え方であることを示した。これは特別に原子力設備に限ったものではなく、他にも通用できる安全確保の考え方である。

これまでの設計で考えてきた想定、設計条件での安全確保を確実に行うことに加え、万一、設計条件を超える事態に対しての、安全確保策を施すことで、原子力事故に至る可能性を小さくしようとするものである。

このように、人や環境に放射線の影響を与えるという事態（「原子力事故」という）に至ると考えられるような原子力施設の事態を、設計での確実な対応により排除すること、さらに設計を超えて起きるような場合において

も、適切な対応によって原子力事故となる可能性を徹底的に小さくすること、また、それでも原子力事故に至った場合には、影響を受ける地域の人、それぞれが様々な対応により身を守る「防災」の対応を加えて、これらの様々な視点での対応策で成り立つのが「深層防護」という原子力における安全確保の仕組みである。

3.4 実効性の確保

自然現象に対する防護レベル設定とこれに基づく安全対策の実施には，いくつかの困難さが伴っている。設計基準を超えて，アクシデントマネジメントの領域に至ったとして起りうるシナリオを全て網羅しておくことは困難であると言わざるを得ない。例えば，可搬式設備などで柔軟性，融通性をもった対応も効果があると考えられるが，一方で多様なアクシデントマネジメント（AM）策を進めるために，組織と人間に対応する能力と責任感、適切な判断力、統率力などが必要となる。

シビアアクシデントが実際に起こっている状態でのAM 策の実施には，多くの実施上の困難さが伴うことも明らかである。例えば，高い放射線環境での様々な作業には時間的空間的制限があり，運転員には制御室での居住性にも大きな制約がもたらされる。さらに AM 策として用意されていたものの中には，ある事故条件下で必ずしも容易に実施できないものがある。

深層防護が原子力安全の原則であるためには，オンサイト，オフサイトを含めた多重，多様の安全確保がなされることに加え，AM策や防災対応の実効性を確保するための訓練や演習，およびそれらの不断の見直し等の多くの因子を有機的に結び付けることが必要である。

４．プラント設計における原子力安全

4.1 設計による安全確保

原子力発電システムは、一般の製品と同様に仕様書の要求に基づき設計され、建設、運用に供せられる。その信頼性、安全性は、理論や法令、規制基準に基づき確保される。その基盤となる考え方は、「原子力安全」を確保する思想であり、「深層防護」によるその確保の方法である。このような仕組みであることを認識して、各組織はそれぞれの役割を果たさなければならない。ここで改めて「設計」の範囲を確認する。設計とは、その時点で想定される運用に適切に適用するためのものであり、使用中の原子慮る施設の安全を担保するものであり、要求仕様に基づき要求性能を満足し、「原子力安全」が確保されるように、設備の健全性を確認するための解析評価などを行い確認することである。それにより設備を製造、建設し、また運転、保守を行うための計画を立案し、全体を整合させて図面や手順書などとして設計図書に集約する。

4.2 設計基準と設計の基本的考え方

設備としての原子力発電プラントの設計において、安全設計はシステム設計の一環として炉心設計と合わせて行われる。「深層防護」の考え方を適用し、防護レベル全体を通して原子力安全確保を図る設計への取り組み全体を整合させて考えるのが「安全設計」であり、それを受けてプラントの設備を論理的に構築するのが設備設計である。これまでの設計は、安全設計は深層防護の主に第3層までを中心に安全確保の仕組みを検討してきており、「設計基準」を定める設計基準事象が重要な位置づけをもっていた。設備設計は、深層防護の第 1 層から第 3 層を対象とし、この中で適切な仕様の設備を備えることで安全設計の要求を満たすプラントシステムを構築し、構造を作りあげることである。これにより原子力安全を確実に維持することを目指してきた。**Table1** には原子力安全を確保する重要な機能、すなわちフロント系の機能、バウンダリ機能(閉じ込める)、冷却機能(冷やす)、制御機能(止める)、その他のサポート系の機能とそれを構成するシステム・機器の例を示す。

さまざまな事象、特に外的事象としての自然現象への対応について、これまでは一般論として定まった考え方はない。地震動に対しての設備設計を見てみると、学術における様々な考え方を基準に、包括的な対応として、地震動の大きさを定め設備の健全性を評価する方法を定めている。設計に用いる基準は以下のように考えられてきた。自然現象の脅威を過去のデータを基に科学的に想定される範囲で保守的に扱い、不確実性を考慮して基準を超える事態にも構造健全性が確保されるように、設計基準を定量的に定めてきた。十分に余裕をもった設計が行われ、この設計に基づき、製造、建設が行われてきた。同様に、他の自然現象、例えば竜巻、火山の爆発、隕石の落下などの脅威についても、このようなデータに基づく評価および物理理論に基づく評価を元にした設計を行わなければならない。

4.3 原子力安全を確保する設計へのとりくみ

1) 安全設計の課題と分析、対応策

従来の原子力発電所の設計においては、「深層防護」の第 3 層までにおいて、まず“止める”、“冷やす”、“閉じ込める”のフロント系を確実にすることが主要な考え方

であった。しかし、一方重要なことは、「電源」の喪失という事態への対応であり、このような事態を左右する機能、サポート系の機能に対してもフロント系と同様に十分な対応が必要である。

原子力発電所の安全設計は、システム設計に活かされ、安全設計で要求したシステムの機能を満足する設計が行われなければならない。システム設計には、機器設計や配管設計、計装制御・電気設計などが含まれ、すべての機器類が統括される。システム設計において、異常時、事故時の安全確保に電源や電気系統まで、さらに総合した評価に取り組むことが重要である。

このような安全に対する取り組みは常に見直し、確実に対応しなければならない。

安全設計は、深層防護の第 1 層から第 3 層までの設備設計はもちろん、第 4 層、第 5 層などを含めた取り組みでなければならない。その上で、必要な機能を評価する“システム安全”の考え方を安全評価に導入することにも取り組まなければならない。深層防護の思想を徹底させ、安全設計が深層防護全体を整合させるものであり、そのための仕組みを構築し、確実に実行される取り組みとすることが求められる。

4.4　設備設計の分析、対応策

設計基準事象としてはLOCA などの内部事象を中心に、設備を厚くすることで確実に安全を確保することを目指した設計が進められてきた。

自然現象は必ずリスクを伴うものであり、正確な評価は難しいが、自然現象をよく把握し原子力災害のリスク評価に十分に対応しなければならない。地震動に対しては残余のリスク評価に取り組み始めたが、他の事象に対しても同様に、リスク評価に取り組まなければならない。

設計基準は超えるものとして安全確保に取り組まなければならない。

すなわち、基準を超えてしまった場合への対応として、深層防護の考え方が適用される。それがアクシデントマネジメント（AM）策である。AM領域においても、設計基準を超える事態を想定し、多様性、独立性を考慮した設計により設備を備えることで、AM策として有効に使える設備が準備される。特に、事故時のアクシデントマネジメントでは、異常時には日ごろ使わない設備を用いる場合が多く、さまざまな事態を想定して、演習や訓練を徹底しなければならない。

５．プラント設計でのシステム安全

5.1 原子力安全に必要な機能と構成する系統

Table1 には、原子力発電所に必要な重要な機能とそれを構成する構築物、系統、機器を示した。設計に求められる基本的な要素は、バウンダリ機能、冷却機能、制御機能であり、その他に挙げた電源供給機能と合わせて原子力発電所に基本として必要な重要な要素である。原子力発電所の設計は、これらの機能が適正に結びつき維持されることで成り立っている。それがシステム設計である。それにより設計基準内のどのような事象に対しても、設備の健全性、安全性が確保されることが担保される。

一方、設計基準事象を超える場合の対応は、事象、事態により対応が異なることから、このレベルではシナリオが重要となる。多くのシナリオを想定し、それぞれに対応できる方策を準備することが必要となる。その上で、設備や手順を標準化して規格化して行くことで、より系統的な対応が取れる仕組みが構築される。

5.2 事故に備える論点

1) 設計基準を超えることへの対応

地震動での構造健全性が論点となっている。すなわち、地震動の大きさがわずかに基準値を超えることの意味である。例えば地震動の周波数帯域のある部分で基準を超える場合や、振動波形そのものが一瞬越える場合などがあるが、それらがプラントの安全性や構造健全性を脅かすものと認識されていることである。中越沖地震での柏崎刈羽原子力発電所の地震動が基準地震動に対して 3 倍を超すプラントもあったが、設備の健全性は十分に保たれていることが確認された。地震動に対する構造設計には大きな余裕があることが認識された。その後、全国の原子力発電所においては、基準地震動の見直しがなされ、厳しく設定されたもののまだ余裕があることが確認されている。これは単純に構造上の健全性の余裕が評価されたものであるが、機能上の余裕はさらに大きなものがあると推察される。

“設計基準を超える”意味を考え直さなければならない。すなわち、今回の東北地方太平洋沖地震でも、東日本太平洋岸にある多くの原子力発電所では基準地震動をわずかだが超える地震動加速度が観測された。プラントの状態を表す観測データに表れるような影響はなく、これまでの解析評価や他のプラントの実績からも地震時の健全性は確保されたと考えられた。したがって、基準地震動を超える事態に対しては、これまでのように単に加速度応答の基準値を見直すことではなく、今後の免震装置の導入をも視野に入れた幅広い評価法を検討すべきで

あろう。

また、津波に対しても基準津波を設定するが、この場合は津波の計測点から発電所に到達するまで少ないものの時間があることから、基準を超えた津波の大きさにより、対応策の準備、始動を変えることができる。従って、「いつ設計基準を超えた」、また「どの程度、超えているのか」の判断基準を定めなければならない。それがアクシデントマネジメント（AM）策を実行する上では重要な判断となる。

2)想定を超える自然災害に設計はどう答えるか

これほど大きな津波が来襲するとは、「想定外」であったと言われる。それに対して、原子力安全では「想定外」は許されないと言われる。1000 年に一度程度の大きな津波の予測は容易ではない。耐津波設計は、耐震設計と同様に地殻の動きから、波の発生、伝搬、遡上、浸水等と様々な現象を評価した後の、建屋、設備の構造設計や電気計装設計の複合である。津波の大きさのシミュレーションは様々に行われ、様々な推定がなされている。基準津波を設定したとしても、基準値を超える津波は来ないだろうが、超えないとは保証はできない。程度は異なるが、地震動と同様、超えることを想定した対応が求められる。様々な自然災害に対して、想像力を豊かな対応が求められる。

しかし、深層防護としての想定外への対応、設計基準を超えることへの対応は、実施できるが、例えば不確実性の大きな新たな自然災害への脅威に対して、対策が必要と言えるか、またそれを受け入れられるのか、難しい課題である。常に、新たなハザードがないか、また対応策が適切かの、問いかけ、見直しを継続させることが重要である。

６．新たな設計への取り組み

－レジリエンスの基本概念－

これまでの設計は、安全設計により設備に求められる仕様を決めて、設計基準を担保することを確実に行うことで、原子力安全を確保すればよいとの考えであった。このような設計には重大な限界がある。

これからの設計は、通常運転、異常の検知、異常への対応、設計基準を超える事態への対応、緊急時の対応（防災）の深層防護の第 1 層から第 5 層までの各層を通して整合した安全設計が求められ、共通する評価指標を定めて最適化を目指した設計を提案する。さらに、事故後の対応、レジリアンスと言われる復帰、復興までも視野に入れた安全確保の体系が必要となろう。

設備設計はマネジメントの領域まで踏み込んだ対応が求められ、またマネジメントは設備設計、防災の領域まで踏み込んで検討することが求められる。プラントの安全確保は設備設計だけでは十分に対応はできない。尺度の異なる領域に渡る、機能を中心とした新たな原子力安全確保の概念を構築する必要がある。

設計は重要な役割を担っている。原子力安全を確実に維持するには、基本的には「深層防護」の概念に従った安全設計に基づくものとしなければならない。設計は、IAEA の深層防護の第1層－第5層の異なる次元への対応を整合させて最適化するものであり、第 1 層－第 3 層の設備設計主体の領域と第 4 層、第 5 層のマネジメント主体の領域の相互連携が重要である。プラント全体を求められる機能で結合させたシステムとして、安全確保の仕組みとしなければならない。

原子力発電システムの設計においては、地盤・建屋・機器・配管・電気・計装などのシステム全体を考えた整合化を図るトータルシステムとすること、通常運転から事故・緊急時の対応まで考慮した仕組みとしてのトータルプロセスの視点、深層防護の全領域を考えたマネジメント、ハードとソフトの最適化を図るトータルマネジメントとする、これらを統合した総合的、俯瞰的な取り組みであるトータルデザインとしなければならない。

レジリエンスについて、深層防護との関係を Fig.2 に概念で示す。様々な事態を想定した対応策、機能の回復策、確保策を事前に考え、準備しておく。実際には、影響の大きさは安全機能のレベルで表されるが、概念として深層防護との関係で示した。

レジリエンスの基本概念は、この図の通常時の「備え」から「予防措置」、「状態把握」、「AM・回復」、「新たな平衡状態の維持」まで広く対応することを指すもので、ここでのレジリエンス指標の評価は、このような状態を想定しながら、様々な対応策が、どのような能力を持つのかを表すものである。従って異常の発生から始まる評価の状態は、仮想の状態を示し、仮想の状態から準備されている手段がどのレベルまで回復するのかを評価して、様々な手段の持つ能力を総合して、プラントの持つレジリエンス指標として示そうとする試みである。

保全指標と、レジリエンス指標を用いることで、プラントのシステムとしての安全能力が施される保全により、またAM策により安全性がどの程度改善されるのか、ど

の手段を選択するのが良いのか、などの評価にもちいることができる。

謝辞

本研究は、株式会社三菱総合研究所が原子力規制庁から受託した高経年化技術評価高度化事業「経年プラントの総合的な安全評価手法に係る調査研究」による成果の一部である。

参考文献

[1] 原子力安全のための耐津波工学の体系化に関する調査委員会：「原子力安全のための耐津波工学ー地震・津波防御の総合技術体系を目指してー」日本地震工学会、原子力学会（2015 年 4 月）.

[2] 日本原子力学会(2014)：福島第一原子力発電所事故　その全貌と明日に向けた提言、
学会事故調　報告書、丸善出版（2014 年 3 月）.

[3] N.Sekimura、H.Miyano、T.Itoi,Resilience : Engineering:New Discipline for Enhancement of Nuclear Safety: Short Paper of ICMST-Kobe 2014（2014-11）pp.85-90.

Table1 Basic Safety Function and System applied to D-I-D

	バウンダリ機能	冷却機能	制御機能	その他(共通機能)
第1層	・原子炉冷却材圧力バウンダリ(PS-1) ・原子炉冷却材を内蔵する(PS-2) ・原子炉冷却材圧力バウンダリに直接接続されていないものであって、放射性物質を貯蔵する(PS-2) ・放射性物質放出の防止(MS-2) ・原子炉冷却材保持(PS-4/2以外)(PS-3) ・放射性物質の貯蔵(PS-3) ・核分裂生成物の原子炉冷却材中への拡散防止(PS-3)	・炉心形状の維持(PS-1) ・通常時炉心冷却(PS-3)	・過剰反応度の印加防止(PS-1) ・原子炉冷却材の量確(PS-3)	・燃料を安全に取り扱う(PS-2) ・電源供給(非常用を除く)(PS-3) ・プラント計測・制御(1)(2)(3)(安全保護系除く)(PS-3) ・プラント運転補助(1)(2)(PS-3) ・原子炉冷却材の浄化(PS-3)
第2層	・原子炉冷却材圧力バウンダリの過圧防止(MS-1) ・安全弁及び逃がし弁の吹き止まり(PS-2)	・原子炉停止後の除熱(MS-1) ・制御室外からの安全停止(MS-2) ・原子炉圧力の上昇の緩和(MS-3) ・原子炉冷却材の補給(MS-3)	・原子炉の緊急停止(MS-1) ・未臨界維持(制御棒による系)(MS-1) ・未臨界維持(ほう酸水注入系)(MS-1) ・出力上昇の抑制(MS-3)	
第3層	・放射性物質の閉じ込め機能、放射線の遮へい及び放出低減(PCV)(MS-1) ・放射性物質の閉じ込め機能、放射線の遮へい及び放出低減(R/B)(MS-1)	・炉心冷却(MS-1) ・燃料プール水の補給(MS-2)		・事故時のプラント状態の把握(MS-2)
第4，5層 （＊）	・過酷事故対応(PCVベント)(MS-3)	・過酷事故対応(補給水系)(MS-3) ・過酷事故対応(消火系)(MS-3)	・過酷事故対応(ほう酸水注入系)(MS-3)	・緊急時対応上重要なもの及び異常状態の把握(1)(2)(3)(MS-3)

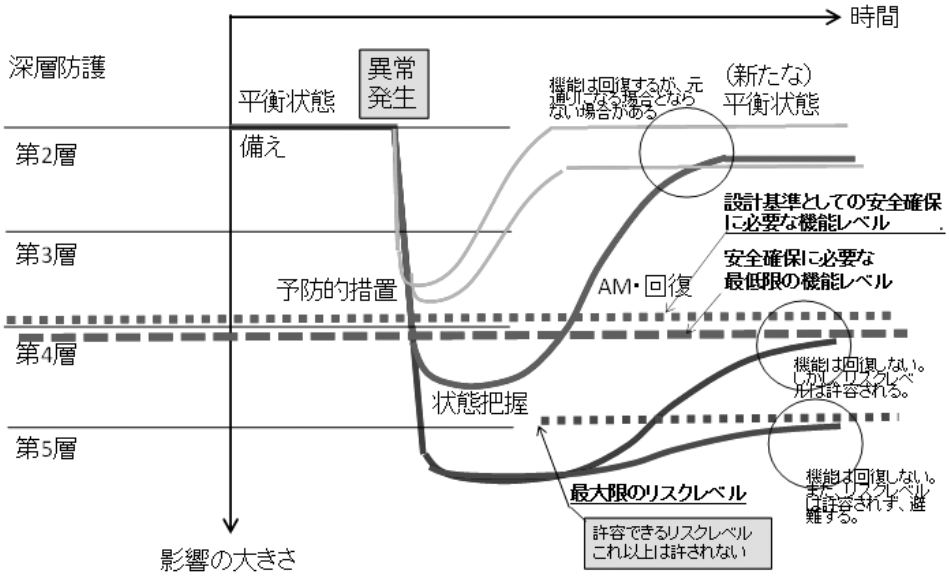


Fig.2 Concept of Resilience and D-I-D