ソフトウェア・エージェントによる原子力発電プラントの事故時自動操作系の概念設計に関する研究

Research on Conceptual Design of Automated Accident Recovery System in Nuclear Power Plant by Software Agent

丹羽　雄二　(Yuji Niwa)*　寺邊　正大　(Masahiro Terabe)†　鷲尾　隆　(Takashi Washio)‡

要約　本研究では，まず原子力発電プラントの運転員が安全運転を行うためには，プラントの重要なパラメータとそれらの間に存在する因果関係を考慮した上で意思決定を行う必要があることを，科学的な考察と分析結果にもとづいて指摘する．時間制約による精神的抑圧の下では，運転員がプラントの各々のプラントパラメータが本来持っている複雑な因果関係を考慮した上で最適な意思決定を行うことは不可能に近い．このような理由から，事故収拾操作の計算機による自動化に関する要請が高まっている．従って，本研究では，特に原因が不明確な原子力発電プラントの事故下で，自律的に運転員と協調して効果的な意思決定を行うことができるエージェントシステムを提案する．

キーワード　ヒューマン・マシンシステム, 原子力発電プラント, 人工知能, エージェント, 安全機能，自動化

Abstract　In this paper, investigations and analyses of the human-machine joint system have revealed the necessity of careful decision-making by Nuclear Power Plant (NPP) operators considering the critical parameters of NPP to attain safety and the causalities amongst these parameters. Under a strong time pressure, it is virtually impossible to make an optimal decision taking such causalities into account. As a result, the computerization of taking recovery actions is required. Considering a the requirement of such computerization, an autonomous system in collaboration with human (what we call the agent system), which is still effective even in such an unforeseen condition in NPP, is proposed.

Keywords　human-machine system, nuclear power plant, artificial intelligence, agent, safety function, automation

1. 緒言

近年の高度情報処理（Advanced Information Techno-logy：AIT）の技術的進歩により，原子力発電プラント（Nuclear Power Plant：NPP）の種々の事故時における支援を考えることが可能になってきた．現在は，一旦原子力発電プラントに制御系で補償不可能な外乱が印加されると，安全維持のために自動的に原子炉を停止するような機構になっている．従来の古典的な制御理論にもとづいたフィードバック制御理論の適用が，これまで原子力発電プラントに導入されてきた．しかしながら，それら制御システムは，蒸気発生器水位や加圧器圧力など，プラントの局所的プロセスを自動制御するにとどまっていた．

原子力発電プラントでは，一般的に新技術の導入については，信頼性に最重点がおかれるため，他業種の化学プロセスプラントに比べても自動化のレベルが低く押さえられてのが実状である．しかしながら，高度情報処理の進歩により，自動事故収拾システムの開発が可能な技術的環境に近づいている．そこで本稿では，高度情報処理技術を適用した事故自

* (株)原子力安全システム研究所　技術システム研究所
† (株)三菱総合研究所
‡ 大阪大学産業科学研究所

動収拾システムについての概念を確立する．

特有の強い非線形性や，プラント内の構成機器の多さから，原子力発電プラントは複雑系と考えられ，特に，事故時における自動化について保守的になってきたことは十分に理解されよう．

一方，原子力発電プラントにおける運転員の役割は，現在，非常に重要なものとなっている．従来より，事故が起こった場合には，まず運転員は事象を同定する，すわなち原子力発電プラントに何がどのような原因で起こったのかという内容について把握する．そして，同定された事象に準拠した事故時手順書（Emergency Operating Procedure：EOP）を参照しながら，原子力発電プラントの事故収拾操作を開始する．従って，これら従来の事故時手順書を参照する場合には，いかなる場合にも事象の同定が必要である．このような理由から，上にあげたような事故時手順書は，事象ベース事故時手順書（Event-Based Emergency Operating Procedure：EB-EOP）と呼ばれる．

運転員が事象の同定の段階でエラーを起こさない限り，EB-EOPを参照しながら事故収拾操作を行えば，（同定された）事故は収拾へと向かう．しかしながら，原子力発電プラントで起こりうる全ての事故を予測することは，現実的には期待できない．例えば，スリーマイル島２号機（TMI-2）の事故がその典型であろう．TMI-2の事故での経験を基に，新しい考え方にもとづくEOPの必要性が指摘されるようになった．新しい概念に基づくEOPは種々提案されたが，その１つに原子力発電プラントの「機能」に着目したものがある．

Corcoranは，原子力発電プラントの安全維持を達成するための機能について，安全機能として定義した[(1)]．Corcoranによれば，安全機能（Safety Function：SF）は，炉心損傷を回避するための人間／機械による操作の集合として定義される．複数ある全ての安全機能が満たされなければ，炉心損傷の可能性があるので，事故時に（重要）安全機能の１つでも喪失すれば，速やかに当該の安全機能回復を行うという原理に基づいたEOPである．

この事故時手順書は，各安全機能ごとにまとめられていることから，安全機能ベース事故時手順書（SF-EOP）と呼ばれている．安全機能ベース事故時手順書では，運転員は必ずしも，事故事象の同定を行う必要はない．運転員は，事象の同定に失敗した場合，プラントが予想される応答を示さなかった場合，および事故収拾操作中に状況が把握できなくなった場合には，事象ベース事故時手順書から，安全機能ベース事故時手順書へと参照の対象を移行することが新しい手順書体系で義務付けられている．

事故時において，運転員は，この安全機能について継続的に観察を続けなければならない．そして，上述のようにそれらのうちの１つでも機能が喪失した場合には，事象が同定されている場合でも運転員は直ちにその機能を復旧すべく操作を行わなければならない．

安全機能ベース事故時手順書は運転員による事象の同定を要求しないことから，事象が同定できない場合の運転員の支援に役立っているが，安全機能自体は，原子力発電プラント設計，特に確率論的安全評価の専門家の判断により決定されたものである．このため，全ての安全機能が保たれてさえいれば，炉心損傷が起こる可能性について，完全に否定できることが客観的に保証されているわけではないことに注意しよう．

筆者らは，事故時手順書システムは，想定されていない事象を含むすべての事故について適用可能なものとして準備されるべきであると考えている．この技術的目標の達成は大変困難なものであるが，安全機能をより客観的な視点から，工学的専門家の主観に基づく判断を極力介さずに定義することができるならば，解決への糸口を掴むことができる．一方で，安全機能ベース事故時手順書については，時間的な制約やプラントの挙動が明確に認識できないでいる運転員が，極めて強い心理的抑圧がかかった状況のなかで適切に参照できるのか，という疑問も残っている．このような問題点を解決するためにも，予測できない状況下における，事故時における自動収拾システムの研究の必要性が指摘される．

以上のような議論にもとづいて，本稿では主に以下のような３つのサブテーマについての問題解決について述べる．

(1) 事故状況下における機械による状況認識
(2) 自動事故収拾システムのアーキテクチュア，およびシステムと運転員の協調について

(3) 人間・機械（計算機）協調環境下におけるヒューマンマシンシステム設計

2. 原子力発電プラント事故状況下での機械による状況認識

2.1 安全機能と安全機能間の関係構造に関する客観的記述

Corcoranは，炉心損傷を防ぐための基本的な機能として,5つの安全機能を図1のように定義している．安全機能が充たされていない状況下では，原子力発電プラントの安全が脅かされているということができる．また，喪失した安全機能に対して適切な事故収拾操作がとられなければ，原子力発電プラントは深刻な状況に陥ることになる．

この安全機能の考え方は，既に商用プラントに適用されており，この概念を基にして，安全機能ベースの手順書が作成された．先にあげたような理由により，Corcoranにより定義された現在の安全機能の定義は，プラント設計者の専門的主観に依存するものである．さらには，これまで安全機能間の構造は階層的であり，それらは互いに独立な関係にあるとされてきている．この仮定は，従来の安全機能を考える上では大変便利である．並列，独立の仮定の上に安全機能ベース事故時手順書が作成されている．

しかしながら，安全機能を客観的に定義し，その因果的構造について考察することは重要である．商用の原子力発電プラントでは，安全機能は，多少乱暴な言い方をすれば，プラントパラメータ集合として解釈されている．本稿では，プラントの動的モデルを用いることにより，安全機能を客観的に再定義する．プラントモデルは, 集中系モデルで表現する．ここで安全機能を，従来の安全機能と区別する意味で安全機能規定因子（SFD：Safety Function Designator）として再定義する．

原子力発電プラントは，次のような集中定数系の状態方程式により定式化することができる．

炉心損傷回避のための安全機能（Corcoran,1981）
炉心反応度維持
炉心除熱確保
1次冷却材（からの）除熱確保
1次冷却材の圧力制御
1次冷却材のインベントリ確保

*本表では，格納容器の健全性に関する安全については含めていない．

図1　Corcoranによる安全機能

$$\frac{dX}{dt} = F(X,U) \tag{1}$$

$$Y = G(X,U) \tag{2}$$

ここで,

X ：状態変数ベクトル

Y ：出力（目的）変数ベクトル

U ：制御ベクトル

t ：時間

出力ベクトルYの各要素yは，それぞれSFDの主要パラメータであり，適当なセンサを通じて計測され評価される．状態ベクトルXの全要素は，現在の原子力発電プラントの計装系により計測可能なものである．Yの要素は全てXの要素に含まれるので，式（2）は線形方程式の形で表現することができる．すなわち，定数ベクトルと状態ベクトルの内積により表現できる．Uは制御ベクトルであり，原子力発電プラントの事故収拾に必要な操作系列により規定される．

$$U = [OP_1, OP_2 \cdots OP_n] \tag{3}$$

ここで,

OP_k：SFD維持のために実施されるタスク,

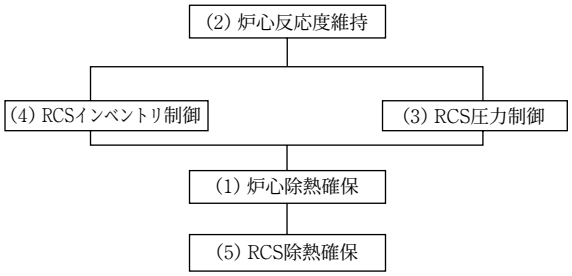
$1 \leqq k \leqq n$

原子力発電プラントのモデルが得られたならば，機械が取得したい全てのプラントパラメータを推定することができる．安全機能規定因子の定義については参考文献 [2] に詳しい．安全機能規定因子は，当該の規定因子のふるまいを表現する代表的なパラメータを持つ．原子力発電プラントの動的な振る舞

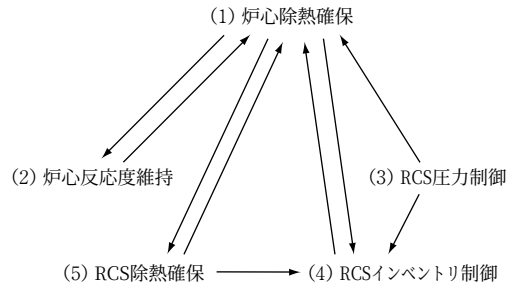
いを規定する全てのパラメータ間の因果関係について分析した．ここで，安全機能規定因子間の因果関係は，「因果推論」[3] という解析的な手法を用いて分析した結果から．各安全機能規定因子間の因果関係は，その安全機能規定因子とその他の安全機能規定因子に関連する代表パラメータの因果関係を解析することにより導出することができる．

安全機能規定因子間の因果関係を分析した結果，それらの間には相互依存的な因果関係が存在し，安全機能規定因子の構造は階層型というよりは，ネットワーク型であると言える[2]．従って，これまでは安全機能間に相互関係が無いと考えられてきたが，実際には，ある安全機能を維持すべく操作がなされる場合には，その操作の影響が他の安全機能にも及ぶことになる．

安全機能規定因子の相互依存関係を，Corcoranにより提案された安全機能の構造とともに図2に示す．各安全機能規定因子は，安全機能と同じ名前になっている．これは，安全機能規定因子は安全機能を，単に客観的に再定義したものであることによる．そして，この再定義により，安全機能規定因子を現在の事故時操作手順システムに導入することを可能にした．



Corcoranによる階層的構造



ネットワーク状のSFD構造

図２　安全機能と安全機能規定因子の構造

2.2　機械システムによる状況認識

本稿において，原子力発電プラントにおける「事故」とは，炉心がプラントの安全機器と操作の失敗により，損傷するような状況を指す．安全機能規定因子が安全機能よりも優れているところは，安全機能規定因子が機械の状況認識に関する指標を提供できる点にある，機械は，プラントパラメータにより張られる状態空間の中でプラントの置かれている位置，すなわち，原子力発電プラントが危険な状態である程度と，その下で機械が行わなければならないことについて，この指標から認識が可能である．

安全機能規定因子が提供する指標のうち，最も特徴的なものは，安全余裕時間である．安全余裕時間は，機械に対して，原子力発電プラントが破滅的な状況，すなわち炉心が損傷したような状況に陥るのを避けるために，意思決定（操作の生成）と行動（操作）に与えられた時間である．もう１つの指標は，プラントパラメータにより張られる状態空間における危険領域と現在の状態が表す点との距離である．これについては，以下のように記述される．

各時刻tにおける安全機能規定因子と，代表パラメータを要素とする状態ベクトル$X(t)$は式（3）から求めることができる．操作Uを評価する指標を得るには，安全機能規定因子の維持が必要となる．この指標は，入力U，状態ベクトルX，そして現在の状態を始点として安全機能規定因子のモデルから予想される状態ベクトルXの遷移をもとに定義され，評価される．

安全機能規定因子の評価基準[2] を適用することにより，安全機能規定因子の破壊に関する判断を行うことができる．安全機能規定因子が破壊されているならば，その時点での安全余裕時間Taは評価することができる．安全余裕距離についても，同様に以下のように評価することができる．

$$D = \int |\delta X| \tag{4}$$

ここで，

$|\delta X|$：状態ベクトルの差分ノルム

は，プラントが安全機能規定因子が喪失した危険な

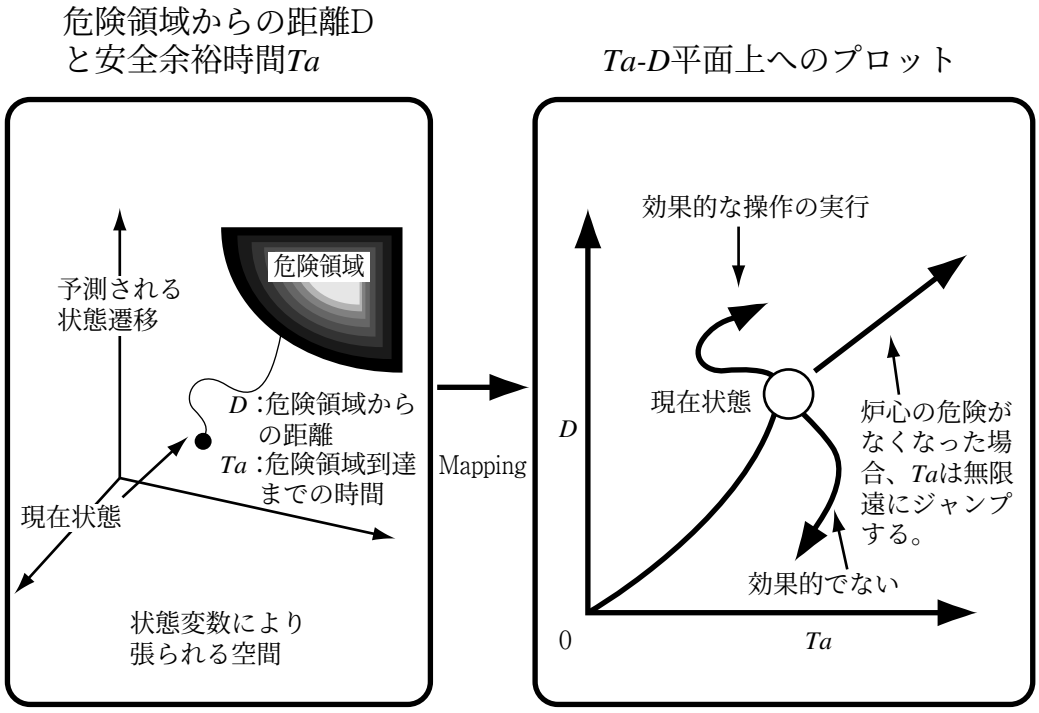


図3　*Ta-D*プロットの概念（エージェント内における状況確認）

状態（領域）と現在の状態との距離をあらわしている．現在の状態*X(0)* と制御系列*U(t)* のあらゆる組み合わせについて，その位置が*Ta-D*平面状に記される．この様子を図3に示す．より原点（左下隅）に近い点は，より重大な緊急状態にあることを示している．ただし，安全機能規定因子が維持されていたり，将来的に維持されるであろう場合には，*Ta*が無限大になる．その場合，*Ta-D*平面上の状態をあらわす点は，事故時操作が事故を終結させる程有効な場合に，平面上の原点から右上の無限遠へと不連続に遷移することになる．

手法の詳細は，ここではページ数の制約から省略するが，ここであげた情報が優先して維持すべき安全機能規定因子に関する判断の基礎となる情報を提供することは明らかである．

3. 原子力発電プラント事故時の事故収拾システム

3.1 計算機化事故時操作手順書と提案システム

原子力発電プラント事故時の事故収拾システムについて議論する前に，事故時手順書の機械化に関する定義を明確化する．

これまでに述べたとおり，原子力発電プラントの運転員は，事故時には，事故時手順書を参照しながら収拾操作にあたる．事故時手順書は，これまで一般的な操作手順書と同様にドキュメントの形で準備されてきた．このため，完全に自動化事故収拾システムに至るまでには，以下に述べるように，多くの前段階を経ることが必要である．

実際には，事故収拾操作が計算機化されるべきか否かという問いについては，これまであまり議論されていない．しかしながら，事故収拾操作について「どの程度まで計算機化すべきであるのか」，いいかえると，「計算機化する」あるいは「自動化する」ことの真の意義はどこにあるのか，という内容についてはよく議論されている．事故時手順書のGUI上の表示については，事故時操作手順書の自動化における重要な段階である[(4)]．一方，本稿でとりあげるような自動事故収拾システムのレベルや残された課題について把握することも必要である．

最も初期のレベルをレベル0とする．これは，従

来からのものであり，最も一般的な形式である．

(1) レベル－0　事故時手順書はドキュメントである．このレベルでは，操作手順は，印刷された手順，あるいはチェックリストとして表現されており，これは，従来からの形式で，これまで用いられてきたものである．

(2) レベル－1　事故時手順書は，極めて原始的な形で計算機化されている．このレベルでは，操作手順は電子化されており，手動スクロールが可能なVDU上に表示される．ただし，ここでは，フォーマットの変換は含まれていない．このレベルの特徴は，ディスプレイ上でスクロールすることにより，操作手順全体を認識しやすくしていることである．

(3) レベル－2　操作手順書は，ディスプレイ上に表示される．このレベルでは，操作手順の表現が変更される．この機能は，計算機に制御されたディスプレイやコンピュータグラフィクスにより実現される．フォーマット，プロセスとのリンクづけに関する詳細については，後で述べる．この段階から，計算機化手順書と呼ぶことにする．

(4) レベル－3　操作の追跡，監視機能をもつ計算機化された操作手順書である．これより下位のレベルとの違いは，操作を通じて，必要な部分だけを表示できる点にある．これらの機能は，自動スクロールに代表されるように，運転員のタスクを軽減するのに重要である．

(5) レベル－4　自動化された手順書(1)：操作を機械に委任する．このレベルでは，運転員の指示により，整理された操作手順の一部が自動的に実行される．ここでの計算機化の範囲は，操作手順の表示から，操作手順の実行まで拡張されている．

(6) レベル－5　自動化された手順書(2)：機械が操作を提案し，運転員が最終的に承諾することにより，事故時操作の管理を行う．機械はプロセスを監視し，適切な操作を選択し，実行する主体が運転員よりも操作システムになっているような状況である．しかしながら，実行レベルについては，運転員による承諾が必要なである．

(7) レベル－6　自動化された手順書(3)：問題駆動型の自動化

さらに自動化が進むと，操作システムがプロセスに生じている問題を同定し，運転員による実行や確認の必要なく自動的に操作を実行する．

(8) レベル－7　自律化されており，必要に応じて操作が実行される．(完全自動化)

このレベルは，以下の２つの条件により，さらに分割することができる．そのうちの１つは，操作の実行結果が運転員に通知されるものと，一般の制御器のように．実行結果が運転員に通知されないものに分けることができる．後者については，基本的に全自動化に対応しており，操作を運転員にとって実施し易くするという検討は全く必要がない．操作の実行は完全に計算機化されている．

3.2　原子力発電プラントの自動事故収拾システム

原子力発電プラントにおける完全自動化を実現するためには，全ての事故が予想され，事前に解析されていなければならない．現状での完全自動化は困難な状況にある．このため，原子力発電プラントにおける運転員の役割を無視することは，不可能である．従って，人間中心の自動化（Human Centered Automation）が現在，ヒューマン－マシン研究でしばしば行われている．このような技術困難にも関わらず，安全機能の構造が非常に複雑なネットワーク構造をもつ因果関係にあり,制御が難しいことから,事故時手順書の機械高度化，すなわち高度なレベルでの計算機化についての強い要請が生まれる．完全に計算機による自動化を行った事故時手順生成システムについて考えた場合，計算機（機械）システムの信頼性は完全ではない．原子力発電プラントのようなプロセス系は，サーボ機構よりも，大きな時定数で状態が遷移する．このため，原子力発電プラントの運転員（人間）には，深い洞察を行うことによる事故時操作への寄与が期待できる．加えて，本稿で提案する自動事故収拾システムは，プラントモデルにもとづいて適切な事故収拾操作を生成する．実際のプラントプロセスは，モデルでは完全に表現できないことは明らかである．その結果として，機械システムは不適切な操作を生成してしまう可能性がある．このため，人間は機械システムによる操作生成結果を評価しなくてはならない．

プラントのユーザサイドでは，原子力発電プラントにおいて，事故時に対する完全自動化システムの導入に対する躊躇がある．その理由として，完全自動化システムを導入した場合，運転員が自動化システムに過度に依存することにより技術レベルが低下し，結果として，計算機の機能喪失が原子力発電プラントの制御を不能にしてしまうことが考えられる．以上のような理由により，現在の商用原子力発電プラントにおける事故時手順書の計算機化レベルは，低いままになっている．このような背景から，人間と機械による協調に関する研究が現実的で好ましい．その意味では，提案する自動事故収拾システムの自動化レベルは先に挙げた分類にしたがうとレベル5に相当する．全自動化に向けての段階と人間の役割および責任分担の変化に関する分類については，Sheridan[5] にまとめられており，本研究の人間と機械の協調に関する考え方は，これにもとづいている．

4. エージェント型操作支援システム

4.1 エージェント

本章では，我々がエージェントという概念を事故時操作支援システムに導入した理由，エージェントの定義，提案するエージェントシステムについて述べる．

第２章で述べたとおり，安全機能規定因子間には複雑な因果関係が存在する．運転員は，時間的な抑圧がかかる事故時の状況下でこれら複雑な安全機能規定因子について把握しておくことが必要になる．さらには，運転員は，事故収拾に残された時間だけではなく，実行可能な操作の状況についても把握しておく必要がある．事故時における運転員は，事故により混乱しがちであり，とくに進行している事故状況について把握することが困難な状況に置かれているために，操作の決定から実行という一連の作業を適切に行うことが困難な状況に置かれている．そこで，本研究では運転員の作業を代行することが可能なマシンシステムについて検討することにした．筆者らは，このマシンシステムをエージェントという概念を用いて設計した．

エージェント，あるいはエージェントシステムの定義は，簡単には「自律的に行動するもの」である．また，Russellら[6] はエージェントについて，「自律的に状況を認識し，行動しながら知的に行動するもの」であると定義している．さらに，Russellらは，人工知能の研究を合理的なエージェントに関する研究である，と主張している．

原子力発電プラントの支援システムに必要な機能は，まさに合理的なエージェントを設計することに同義である．本稿では，「合理的」 という用語の概念を，「限られた資源を管理しながら，操作を実行し，目標を達成する（事故を収拾する）システム」であると定義する．筆者等は，運転員支援システムとして，運転員と協調して事故の収拾にあたることができる，合理的な，言い換えると知的なエージェントシステムを提案する．

エージェントは，自らの支援形態について，以下のような3つの運転員支援モードを持ち，事故の状況に応じて支援モードを切り替える．

(1) SFDモデル：プラントに事故が起こった兆候をエージェントが発見した場合，先ずエージェントはSFDモードで動作を開始する．このモードでは，エージェントは詳細な定量的プラントモデルを用いてプラント状況の分析を行う．さらに，第２章で説明したとおり，生成した事故収拾のための操作系列の評価に用いる，安全余裕時間（*Ta*）と安全余裕距離（*D*）の計算にも，この定量的プラントモデルを用いる．エージェントが生成した最も効果的な操作系列は，インタフェースを通じてエージェントから運転員に提示される．

(2) メタモデル：SFDモードにおいて，エージェントが定量的モデルが事故の進行によりプラントの現状にそぐわないことを発見した場合，この定量的モデルの利用を中止し，メタモデルモードへと移行する．メタモデルは基本的な物理則を反映した定性的な記述がされている．エージェントは，メタモデルを用いた結果を用いて，事故収拾に効果があると見込まれるものについて，リストアップして運転員に提示する．

(3) マクロモデル：さらに事故が進行し，プラントの基本的なコンフィグレーションが破壊され，操作の目的が格納容器の保護に絞られているような

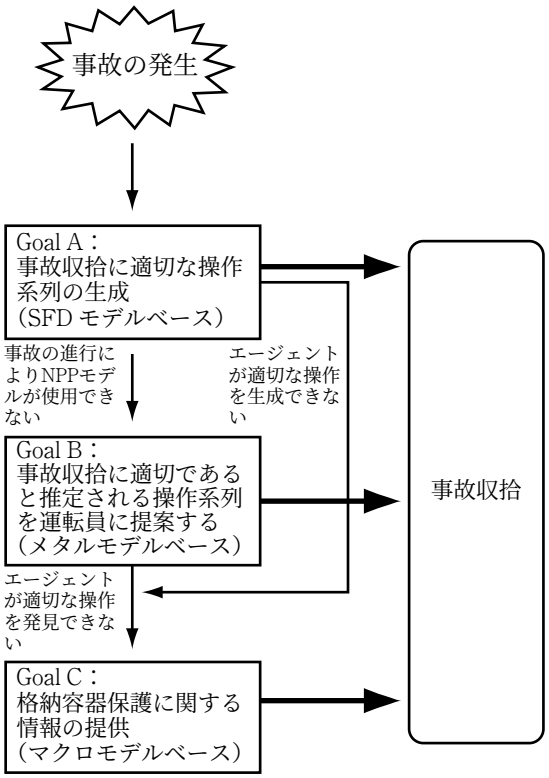


図４　エージェントにおけるモードの切り替え

状況では，エージェントは，マクロモデルに移行する．この状況下では，事前に予測および準備された推論規則はほとんど利用できない．よって，マクロモードでのエージェントの運転員支援の形態は，プラントと実行可能操作に関する情報の集約である．

モードを切り替える機構について，図4にまとめる．上に述べたように，各モードは異なる目標を持つ．また，運転員とエージェントとの協調形態は，各モードにおいて異なる．

4.2　SFDモデルモード

ここでは，SFDモデルベース支援時のエージェント操作支援システムを提案する．エージェントの内部機構を図5に示す．エージェントシステムは，自身の環境である原子力発電プラントと運転員の情報を入手し，働きかけるために２つのインタフェースをもつ．マシン（エージェント）－プロセス（原子力発電プラント）は，複数のセンサー，伝送器，表示灯等から構成される自動操作/制御に用いられる

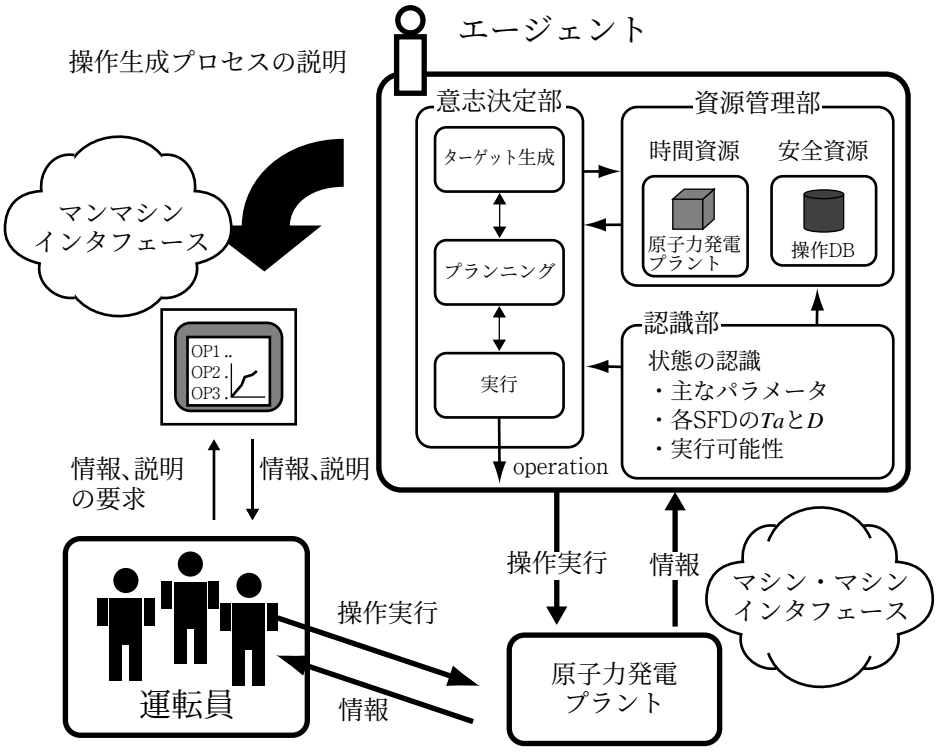


図５　エージェントの内部構造

機器群である．一方，エージェントシステム自身は，6つのウィンドウにより構成されるGUIからなるヒューマン・マシンインタフェースを持つ．これについては，次章にて詳述する．エージェントシステムは，自身の情報処理結果，運転員への提案内容，実行した操作内容について，このインタフェースを通じて提示する．

SFDモデルベース中のエージェントは，主に以下のような３つのパートからなる．

(1) 認識部
(2) 資源管理部
(3) 意思決定部

認識部は，マシン（プラント）-マシン（エージェント）インタフェースを通じて得た情報から事故の状況を把握する．認識された状況は，原子力発電プラントのパラメータのみにより表現されるわけではなく，各安全機能規定因子ごとに前述のように定義される安全余裕時間（Ta）や安全余裕距離（D）を用いて表現される．安全余裕時間や安全余裕距離は，認識部を通じて送られてくるプロセス信号（プラントパラメータ）の情報と定量的モデルを用いて計算される．

資源管理部では，合理的に目標を達成するのに必要な２種類の資源を管理している．その１つは，「時間資源」とよばれるものであり，もう一つは，各時点における実行可能な操作の集合である．この資源は，ある状況下において事故収拾を行うために利用可能な機器群に対応する．この資源を本研究では，「安全資源」と呼ぶことにする．

エージェントシステムは，安全機能規定因子，「炉心からの除熱確保」（SFD_1と記す．）の安全余裕時間を時間資源の指標として用いる．資源管理部は，原子力発電プラントの集中定数化（単純化）された動的定量モデルを保有する．このモデルでは，各パラメータがステップ状及びランプ状に入力されるものと仮定している．資源管理部では，第２章で説明したように，このモデルを用いて入力された状態パラメータから安全余裕時間を計算する．この時間資源は，各単位時間が経過するごとに断続的に変化する．もし，何の収拾操作も行われなかった場合には，安全余裕時間は短くなる．これとは逆に，有効な操作の実行に成功した場合には，安全余裕時間は増加する．

エージェントシステムは，この時間資源を事故収拾操作の決定と実行，すなわち，状況を評価し，事故を収拾する操作系列の案を生成し，序で適切な操作系列を選択し，さらに，これを実行することに用いることができる．

エージェントは，全行動（基本単位となる操作）に関する安全資源データベースを持ち，計装から得られている情報や過去に行った操作の情報をもとに，各操作の実行可能性が反映されるようになっている．これら操作は，その操作が最も効果を与える安全機能規定因子ごとに整理されてデータベース化されている．

意思決定部は以下のような３レイヤ（層）からなる．

(1) ターゲットレイヤ
(2) 操作生成レイヤ
(3) 操作実行レイヤ

ターゲットレイヤでは，ヒューマン・マシンシステムが目標とすべき内容について決定する．ターゲットとしては，「炉心損傷を回避する」と「安全余裕時間（炉心損傷が始まるまでの時間）を長くする」という２つが準備されている．

エージェントシステムが事故を検知して最初に始動した場合には，ターゲットを「炉心損傷回避」に設定する．そして，ターゲットの達成に適当な操作探索に失敗した場合には，「安全余裕時間を延長」に切り替える．

操作生成レイヤでは，エージェントシステムは安全資源と時間資源を参照しながら，いくつかの操作系列を生成し，効果について評価を行う．この評価は，操作系列OPiを実行した場合に，安全余裕時間Ta（SFD_1,OPi）がどれ程長くなるかにより評価する．もし，安全余裕時間が何も操作を行わなかった場合の安全余裕時間Ta（SFD_1,φ）よりも長くなった場合には，その操作は事故収拾に効果があるものとして評価される．さらに，操作が安全余裕時間を無限大にする場合には，この操作を実行すれば事故が収拾できると予測されることを意味している．このような操作が見つかった場合には，エージェントは操作を運転員に提示し，操作に対する承認を求める．

系列として生成が可能な操作系列は多くあるが，

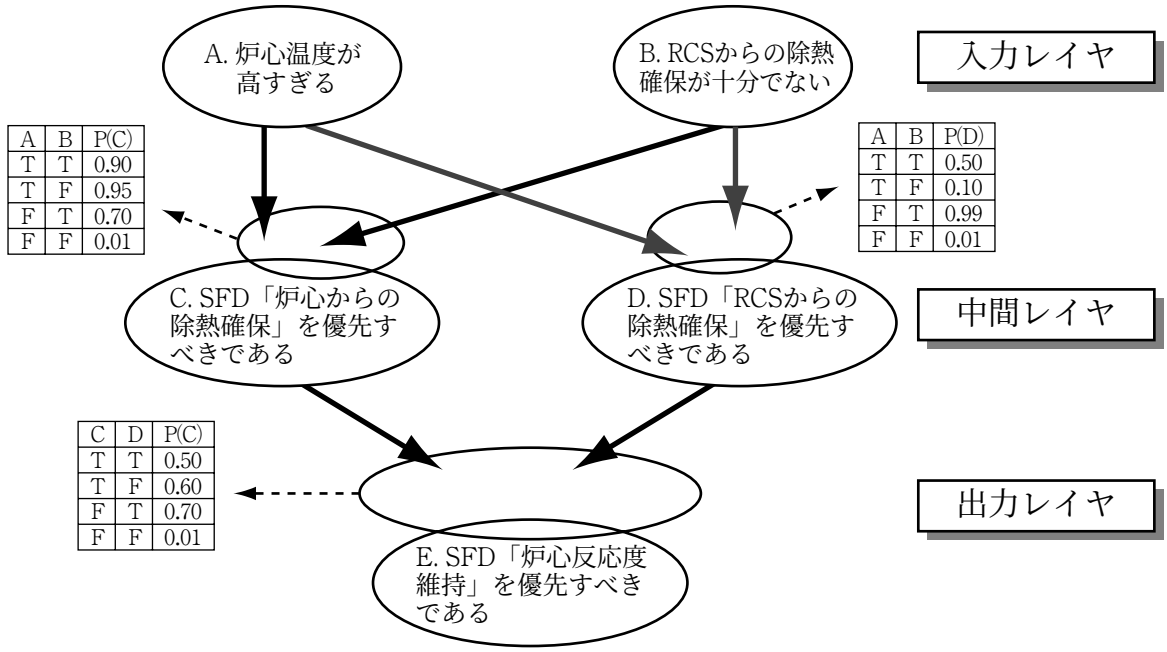


図6　ベイジアンネットワークによる熟練者の知識表現

エージェントは，まず（SFD_1），すなわち，炉心除熱確保に関するものとして準備されている操作系列から評価を開始する．もし，（SFD_1）について準備されている操作系列の全てが事故の収拾に効果がないという評価になった場合には，エージェントは，第２章で述べた安全機能規定因子間の因果構造を参照しながら次に検討する安全機能規定因子を決定する．

この次に検討する安全機能規定因子の決定には，熟練者の知識を表現したベイジアンネットワークを用いて行う．ここでは，各安全機能規定因子に対応する5つのベイジアンネットワークが準備されている．ベイジアンネットワークの入力は，各安全機能規定因子を構成する主なパラメータである．そして，出力は，その安全機能規定因子を次に検討する対象とする選択確率である．このベイジアンネットワークの例を図6に示す．

操作実行レイヤでは，操作の実行についての管理を行う．すなわち，生成された操作系列の実行確認と実行操作の完了確認について，このレイヤで行うことになる．本章で述べたように，提案するエージェントシステムは，インタフェースを通して自律的にプラントや運転員等の環境を自律的に認知し，行動するものである．そしてエージェントは，資源を適切に管理しながら事故収拾に適切な操作を導出した結果をインタフェースに提示することにより知的に運転員を支援している．

4.3　メタモデルモード

エージェントが，SFDモードで用いられる定量的モデルが事故の進行により状況にそぐわないと判断した場合には，モードをメタモデルモードに変更する．このモードでは，エージェントは定性的モデルを用いた推論により，事故収拾に有効な操作をリストアップすることによる支援を行う．メタモデルは，「もし，RCSの冷却材の体積（V_{RCS}）が増加したら，炉心温度（T）は低下する」というような定性的な表現がされたルールによりモデル記述がなされている．また，各操作のプラントパラメータへの効果についても，同様に「もし，操作が実行されたら，1次冷却材ループの冷却材体積（V_{RCS}）は増加する」，というように定性的な記述がされている．

これらメタモデルと操作による効果の記述を用いて推論を行うことにより，エージェントは炉心損傷を防ぐことが可能であろうと思われる操作を抽出する．そして，その操作をリストアップした結果を運転員に参考として表示する．

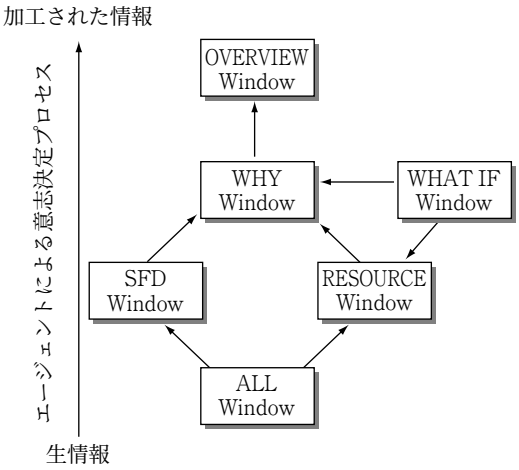


図7　インターフェースの画面構成

4.4　マクロモデルモード

このモードでは，エージェントは事故収拾に対して有効な操作を抽出するという他モードのような支援形態をあきらめ，このモードにおけるエージェントの役割は，プラント，とくに格納容器の状態に関する情報を集約し，エージェントに提示する．例えば，エージェントは格納容器中の水素ガス分布に関連する情報を提示する．

5.　ヒューマン・マシンインタフェース

ヒューマン・マシン協調型システムにおいては，適切なヒューマン・マシンインタフェースの開発が重要な意味を持つ．インタフェースを規定する要因のなかで，エージェントが自己の信号処理プロセスを如何に明確な形で運転員に対して情報として提示するか，すなわち透明性（transparency）の問題は，これまでも注目を集めてきた．ヒューマン・マシンシステムの協調において，互いの信頼感は大変重要な要素である．このような考え方をもとにして，6つのウィンドウにより構成されるインタフェースを設計した．この画面構成を図7に示す．

ウィンドウの機能構成と階層構成は，エージェントの情報処理流れに沿ったものになっている．運転員は，プラントプロセスの状況や安全機器の状況などの情報をはじめとするエージェントが保有する情報について，インタフェースを通じて受けることができる．

(1) Overview ウィンドウ：Overviewウィンドウは，全ウィンドウのなかでも基本的な位置を占めるものである．エージェントは，生成した操作に関する情報をこのウィンドウを通じて運転員に提示する．生成した操作系列の情報は，図3に示したような*D-Ta*平面グラフ形式でウィンドウに表示されるので，運転員は，その操作系列による効果などについて容易に把握することができる．また運転員は，提案された操作系列の実行の許可および拒否について，このウィンドウを通じてエージェントに伝達することができる．

(2) Why ウィンドウ，What If ウィンドウ：運転員は，Whyウィンドウと What Ifウィンドウを通じて，エージェントが行った操作生成に関する意思決定プロセスへの疑問を質問という形で問うことができる．例えば，「なぜ，その操作を提案したのか？」，「この操作系列の効果については，どのような評価になったのか？」というような内容に関する回答をエージェントから得ることができる．このような質問を通じたコミュニケーションは，運転員とエージェントの相互理解に大変役立つものである．

(3) SFD ウィンドウ：SFDウィンドウは，SFDとその相互関係に関するCAIの役割を果たすウィンドウである．このウィンドウでは，各SFDに関する情報と相互関係に関する情報を運転員の要求に応じて提示することができる．

(4) Resource ウィンドウ：Resourceウィンドウでは，操作の実行可能性と安全機器の利用可能性に関する情報が提供される．例えば，各時点における実行可能な操作のリストや，その時点において実行可能な操作が再び実行可能になるまでの推定時間等の情報が提供される．これらの情報の全てはエージェントの内部で生成，あるいは管理されている情報である．

(5) All ウィンドウ：Allウィンドウは，エージェントが持つ各SFDに関する基本的な情報である，主要パラメータ値，安全余裕時間，安全余裕距離などの情報が運転員に提供される．このウィンドウ

から提供される情報により，エージェントが意思決定の下にしている内容を運転員も把握することができる．

運転員は，自分の見たいウィンドウのアイコンをクリックすることにより，そのウィンドウへと移ることができる．

6. 結言

前稿[2]では，安全機能について従来よりも明確かつ客観的な記述を行うことを目的として定義した安全機能規定因子，SFDという概念を用いて，SFD間に存在する因果構造を因果推論を用いて導出した．その結果，このSFD間に存在する因果構造は大変複雑なことが判明した．従って本稿では，事故時において運転員がこれを理解した上で操作を行うことは大変困難であることを指摘し．この様な状況で運転員を支援するものとして，炉心損傷を回避可能な操作を自動的に生成するエージェント型事故自動収拾システムの提案を行った．このエージェントシステムは，エージェント自らが管理する資源（即ち，時間余裕，その状況に使用可能な安全機器）を鑑みながら意思決定を行うものであり，知的で自律的なシステムとして振る舞うことができる．

人間－機械の協調において，ヒューマン・マシンインタフェースは重要である．従って，ヒューマン・マシンコラボレーションの協調形態やこれを活性化するヒューマン・マシンインタフェースの設計論についても議論した．意思決定プロセスをいかに判りやすく運転員に提示するかという問題は，ヒューマン・マシンインタフェースの設計において，非常に重要な要素であり，具体的なスクリーンイメージの設計は，将来ここに提案した様な運転員の教育訓練を含めて今後の研究課題である．

文献

(1) W.R.Corcoran et al., Critical Safety Functions. Nuclear Technology, 55pp.690-712（1981）

(2) 丹羽雄二，鷲尾隆, 原子力プラントにおける安全機能の構造と定義， INSS Journal, No.3, pp.230-241（1996）

(3) 鷲尾隆,物理法則による外性駆動変数の導出,日本人工知能学会誌, vol.5, No.4pp.482-491（1990）

(4) Y.Niwa, E. Hollnagel and M. Green, Guidelines for computerized presentation of emergency operating procedures. Nuclear Engineering and Design, Vol. 167, pp.114-127（1996）

(5) T.B.Sheridan, Supervisory control：Problem, theory and experiment for application to human-computer interaction in undersea remote systems., Dept. of Mechanical Engineering, MIT（1982）

(6) S.Russell and P. Norvig, Artificial Intelligence：A Modern Approach, Prentice Hall, New Jersey（1995）