REAJ 誌 2001 Vol. 23, No. 2, pp. 167-175（通巻 110 号）

ヒューマンマシン共生のための知性と信頼

Trust and Intelligence for Human-Machine Symbiosis

稲垣　敏之
Toshiyuki Inagaki

要旨

人間と機械の間にはさまざまな不整合が生じている．機械の知性に対する不信や過信はそのような例である．本稿では，他者の知性への信頼や依存の観点から，ヒューマンマシンシステムにおける人間と機械の共生のあり方について考察する．

１．はじめに

われわれの身の回りには，「知性」を備えたさまざまな機械やシステムがある．設計段階で作りこまれただけの，もはや成長しない知性もあれば，人間とのインタラクションを重ねていくうちに，その人間の色に染まっていく柔軟な知性もある．人間の機能を代替あるいは拡張するために作り出されたこのような機械やシステムは，個人としての人間のみならず，組織や社会に多大な恩恵を与えてきた．

しかし，人間と機械の間にはさまざまな不整合が生じる．機械の知性に対する不信や過信はそのような例である．これらの現象は，機械やシステムの構築技術が未熟であるから生じるのではない．むしろ，高度な技術の導入が現在の不整合を促進したり，新たな問題を創出しているようにも思われる．

本稿では，異なる知性に対する信頼や依存の観点から，ヒューマンマシンシステムにおける人間と機械の共生のあり方について考察する．

２．ヒューマンマシンシステム

一般にヒューマンマシンシステムと称されるものは，図１に示すように，人間と制御対象の間にいくつかのコンピュータ（あるいは自動化システム）が介在する構造[1]を持っていることが多い．コンピュータは人間の機能の一部を代替あるいは拡張する機械であり，人間からの指示を受けたり人間に情報を提供する役割をもつ HIC（Human-Interactive Computer）と，人間に指示された目標を達成するためのフィードバック制御を担当する TIC（Task-Interactive Computer）に分けて考えると便利である．

このようなシステムにおける人間の仕事は，「何をなすべきかを決め，それをコンピュータに指示し，その指示に沿ってコンピュータが適切な制御を実行しているかどうかを監視すること」といえる．これは，部下（コンピュータ）に命じた仕事をはたして部下が的確に行っているかどうか，上司（人間）が見守っている様子に類似している．このことから，図１に示した形態を人間による監視制御（human supervisory

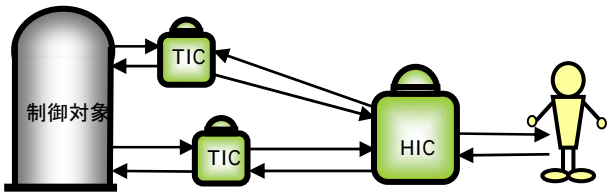

図 1.　監視制御モデル

control）と称する．

航空機や原子力プラントは，監視制御が行われるシステムの典型例であるが，一般家庭にある機器類も監視制御と無縁ではない．例えば，プログラム可能なオーディオ機器や，洗濯物の素材に応じた洗い方を指定したいとき，あらかじめ用意されたメニューにない独自の洗い方をユーザーが細かく指定できる全自動洗濯機などを使う場面は，監視制御であると考えて良い．

監視制御は，人間の肉体的負担を軽減するものではあるものの，心的負担まで軽減できるとは限らない．達成すべき目標は単純明快であっても，その実現には複雑な仕事をいくつかこなさなければならないこともある．監視制御では，それらの仕事系列を部下（コンピュータ）に任せることになるが，上司（人間）は進捗状況をつねに正確に把握していなければならない．「能力のある部下であるからおそらく間違いはないだろう」と思いつつも，気を抜くことは許されない．不適切な点が出てきたときに訂正・修正の指示が遅れると，当初目標の達成がおぼつかなくなるだけでなく，重大な損失を蒙ることにもなりかねないからである．的確な状況認識を保ち続けることが監視制御の成否の鍵を握る．しかし，状況認識を阻害する要因は多様である．

ここで，状況認識（situation awareness）の意味するところを明らかにしておこう．このことばは使いやすいため，乱用され過ぎるきらいがあるが，表１に示すような３つのレベル[2]を持つと考えることができる．

どのレベルで状況認識が喪失されるかについては興味深いデータがある．1986 年から 1992 年の間に発生した航空インシデントからパイロットの状況認識エラーを抽出した報告があるが，それによれば，抽出されたエラー169 個のうち 80.2%がレベル１，16.9%がレベル２，2.9%がレベル３で発生しているという[3]．異常原因の同定やその後の事態の推移を正確に予測することが無理であっても，せめて「異常が発生したとき，直ちにそれに気づく」という，最低限の要求を満たすことが，なぜこれほど難しいのであろうか．

状況認識を阻害する要因の考察に際しては SHELL モデル[4]が有用である．SHELL モデルは，パイロット（ライブウェア：L）と，それを取り囲むソフトウェア（S），ハードウェア（H），環境（E），運航に関わる他の人間（L）との相互関連を表現するために考え出された．人間にとってソフトウェアやハードウェアがわかりにくいものであったなら，奇妙な現象が発生しても直ちに原因を特定することは難しい．環境に

表１　状況認識の３つのレベル[2]

レベル１：	何らかの異常が起こっていることに気づくこと
レベル２：	その異常の原因を同定できること
レベル３：	これから事態がどのように推移していくか予測できること

も不確定要素が入ることは避けられない．チームを組んでいる人間であっても，コミュニケーションが成立しなければ，相手が何を考えているか必ずしも正確には把握できない[5]．SHELL モデルに沿って実際の事故を調べてみると，事故の発端や遠因，そして次第に最終的局面へと至る過程で，何に関する状況認識がどのように失われていったかを記述することができる．

しかし，高度自動化の進んだ現在の航空機でコンピュータが果たす役割は，SHELL モデルが提案された時期に比べて格段に大きくなっており，もはや SHELL モデルでは十分な記述ができないこともわかってくる．コンピュータは，ほとんど人間と同等なエージェント的性格を持つ，いわば「第３のライブウェア」とも呼べる存在にまで成長しており，あたかも自ら意思を持っているかのように，S, H, E, L, L のいずれとも相互作用を持つことができる．時には，コンピュータの自律的行動が機体の異常を隠蔽したり，人間の知らぬ間に制御モードを変えることがあり，レベル 1 の状況認識喪失の要因となっている．1990 年にバンガロール空港[6]，また 1992 年にはストラスブール空港近辺で墜落したエアバス A320 の事故[5] [7] などはその典型である．このことから筆者は，コンピュータ（C）を明示的に意識した C－SHELL モデル（図２）[6]を提案している．

コンピュータの「知性」は，人間を支援するために設計者によって付与されたものである．その支援は，異常や危険が察知されたときにそれを人間に知らせる警報であったり，システムが危機的状況に陥るのを未然に防ぐようなプロテクション機能であったりする．これらの支援によって救われた例は少なくない．それほど，コンピュータの知性は人間にとって信頼できるものとなっている．その一方で，警報はつねに正しいとは限らず，プロテクション機能が人間の自由を束縛する厄介者のように思える場合もある．このようなことを経験すると，疑念や不信を抱くことにもなる．他者の知性に対する信頼が過大であっても過小であっても，ヒューマンマシンシステムの安全性は損われる．

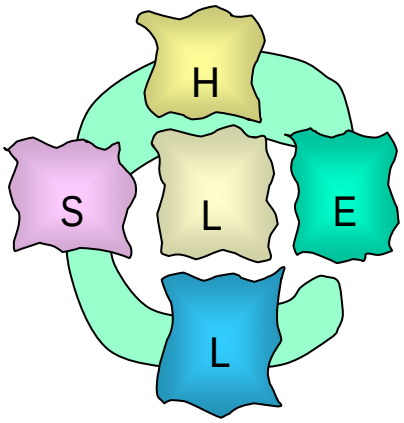

図 2.　C-SHELL モデル

３．信頼を得るには？

警報や自動化システムに対して人間が抱く信頼（trust）は，人間に対する信頼と本質的には同じであり，つぎの４つの要件がある[8] ．

（１）基礎：自然界を支配する法則や社会の秩序に合致していること

（２）能力：終始一貫して，安定的かつ望ましい行動や性能が期待できること

（３）方法：行動を実現するための方法，アルゴリズム，ルールが理解できること

（４）目的：上記の背後にある意図・動機が納得できるものであること

すなわち，「つねに一貫した動作を反復するものであっても，それを支える論理が誤っているものは信頼できず，また，たとえ論理的な誤りはなくても，正しい目的意識に支えられていると思えないものは信頼できない」ということができる．

航空機に搭載されている対地接近警報装置 GPWS（Ground Proximity Warning System）を例にとると，これは航空機が地表面や水面に衝突するのを防止しようとする意図を持っている（図３参照）から，（４）は満たされる．しかし，（２）は完全に満足されるわけではない．GPWS は切り立った崖の検知は不得意であり，地形によっては不要な警報を発するからである．

また，オートパイロットやオートスラストなどを駆使してみごとに操縦するコンピュータの能力は，誰もが認めるところであるが，パイロットたちに，「いったいこいつは何をしているのだ？」，「つぎは何をやるつもりだ？」と言わせるようなこともある[9]．コンピュータの「意図」が人間に理解できていないからである．

相手が信用できないときは，頻繁に相手の行動をチェックしなければならない．このことによって，本来の自分の任務が疎かになり，事故が発生することも起こる．実際，1992 年ストラスブールでのエアバス A320 墜落事故では，なかなか所定のコースに乗れない機長の技量に不信を抱いた副操縦士が機長の操縦に気を取られ，飛行状況を把握するための手順である高度，降下率，速度のコールアウトを怠った様子が見られる[10]．

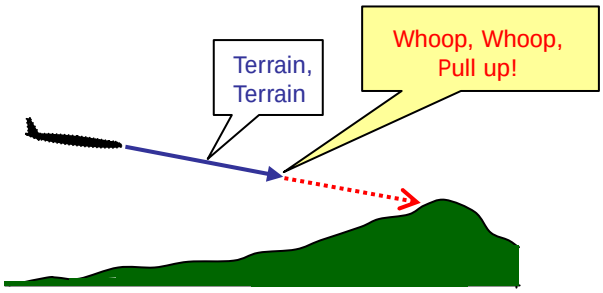

図 3.　地表接近率が大きい場合の GPWS 警報音声

相手に対する信頼が確立すると，相手の行動をモニターする頻度が減るのがふつうである．完全に相手に任せきりという状況も起こりうる．相手が信頼に値するものであれば，相手に任せきりにすることは正しい判断である．しかし，complacency とよばれる状況に陥ると，安全上，重大な問題が生じる．

complacency は，警戒心が欠如し，本来払うべき注意を払っていない状況をいう[11]．すなわち，信頼に値しないものを信頼してしまう誤り，すなわち過信である．制御対象がどのような状態にあるかを常時監視する単調さに飽き，「いままでの実績が示すように，このプラントの信頼性は高い．おそらく今日も何も問題は起こらないだろう．万一，不具合が生じたとしても，そのときは警報が鳴るはずだ」というケースは，complacency の典型である．警報システムに全権を委ねているうちに，その警報システムが欠報モード故障に陥り，完全に状況認識を喪失したまま事故に至った事例[12]は，さまざまな分野で見ることができる．

４．警報への信頼と依存

警報は状況認識支援の重要な道具であるが，つねに正しいとは限らない．対地接近

警報装置（GPWS）が 1970 年代半ばに導入された頃は，誤報の多いシステムであった．「狼が来た！」と騒ぎ立てた少年がそのうちに信用されなくなったように，GPWS が警報を発しても，「いつもの誤報だろう」と放置する現象が見られるようになった．「高価だが，信用できない GPWS など搭載する必要はない」との経営判断を下すエアラインも出現した．GPWS を搭載しない航空機を運航しているエアラインは世界で数パーセントに過ぎないが，正常な機体がパイロットも気づかないまま地表や水面に激突する CFIT（Controlled Flight Into Terrain）事故の約 3 割は，それらのエアラインが起こしている（図４）[13].

一方，危険が迫っているときに GPWS が警報を発しないことがある．従来の GPWS は鉛直方向の地表面を検知することで「降下率が過大であるか」などを計算する方式をとっているため，機体針路前方に切り立った山や崖が突如として現れる場合にはほとんど無力である．また，フラップを出し，車輪を下ろした状態で緩やかに降下している場合は「この機体は着陸しようとしている」と判断し，針路が滑走路へ向かっていなくても警報は出ない．これらは，いわば GPWS の知性の限界を示すものといえよう．

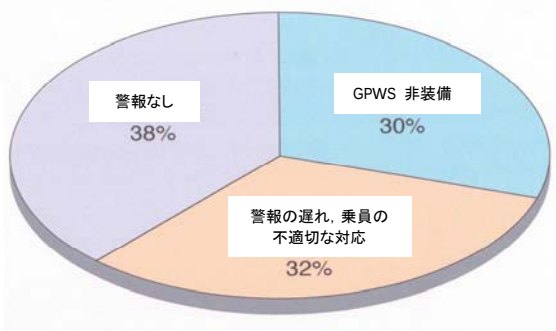

図 4.　CFIT 事故と GPWS

現在では，地形データベースを備え，前方の障害物の認識能力を高めた機能強化型（Enhanced）GPWS の配備が進められている．

ひとくちにヒューマンマシンシステムのオペレータと言っても，パイロットのように，厳しいトレーニングを積んでいることを仮定できるオペレータもいれば，一般の車のドライバーのように，必ずしも専門的な知識や高度な技量を持つことが保証されていないオペレータもいる．後者のオペレータの場合，誤報と欠報の２つの故障モードをもつ警報システムに対して，どのような信頼を感じるだろうか．筆者らは，先行車が急減速したことを検知すると，警報を発してドライバーにブレーキをかけるよう注意を促す仮想的な車間警報システムを構築し，警報の故障モードが人間に及ぼす影響を調べてみた[14].

実験で用意した環境はつぎの２種類である．（１）誤報環境：もし正しくない警報が発生するとすれば，それが誤報である可能性は，欠報である可能性より高い．しかし，欠報モード故障が決して起こらないという保証はない．（２）欠報環境：もし正しくない警報が発生するとすれば，それが欠報である可能性は，誤報である可能性より高い．しかし，誤報モード故障が決して起こらないという保証はない．なお，誤報環境，欠報環境のいずれにおいても，実験中に発せられる警報の９割は正報である．

正報が発せられてからブレーキをかけるまでに要した時間（反応時間とよぶ）を上述の２つの環境下で測定して解析したところ，被験者は２つのグループに分かれた．すなわち，「欠報環境における正報への反

応時間が，誤報環境における正報への反応時間より短く，しかもその差が統計的に有意である被験者」からなるグループ１と，「欠報環境における正報への反応時間と，誤報環境における正報への反応時間の間に統計的に有意な差が認められなかった被験者」からなるグループ２である．さらに，グループ１の反応時間はグループ２の反応時間に比べて短く，しかもその差は統計的に有意であることが確かめられた．

また，この実験では，「車間警報システムをあてにしていたか」どうかを被験者にたずね，システムへの依存性の観点から被験者をグループ分けした．「信頼できるものとして，警報システムをあてにしていた」という被験者をグループＡ，「警報システムに依存せず，自分で状況を把握しようとした」という被験者をグループＢとした．

正報への反応時間と，警報システムへの依存性という，２つの異なる観点からのグループ分けであるが，興味深いことに，グループ１とグループＢが被験者集合として一致し，グループ２とグループＡが一致した．このことは，つぎのように解釈できる．

警報システムに依存していたグループＡ（あるいは２）は，警報を受けてから先行車が減速しているかどうかを確認し，必要ならブレーキをかける．したがって，誤報環境，欠報環境のいずれでも正報への対応のしかたは同じである．

一方，警報システムに頼らないグループＢ（あるいは１）は，先行車が減速しているかどうかをつねに自らモニターしているため，警報が発せられてから状況を判断しようとするグループＡ（あるいは２）の被験者より素早い対応が可能となる．さらに，グループＢの被験者は警報システムに依存していなかったが，警報に必ずしも不信を抱いていたとはいえない．「欠報環境で発せられる警報は正報である可能性が高い」性質を利用しているからである．このことが，「欠報環境における正報への反応時間が，誤報環境における正報への反応時間より短い」という結果をもたらしたものと考えられる．

上記の実験結果は，「高信頼性をもつ警報システムの実現は，メーカーの願いであり誇りでもあるが，仮にユーザーがその警報システムを信頼するあまり依頼心を抱くと，かえって緊急を要する場面での状況認識ならびに対応が遅れることも起こりうる」ことを示唆している．「信頼しつつも適度な警戒を怠らない」ことの重要性を意味するが，はたして現実には容易なことといえるだろうか．警報システムと人間の間で主客転倒が起こらないこと，これが監視制御形態を持つヒューマンマシンシステムの基本的要請である．

５．警報の真偽が即座に判定できないときは？

警報が発せられたとき，正報か誤報か，即座に判断できない場合がある．ある程度の時間をかけての情報収集や，事態の進展を見守ることが許されるなら，結局は警報の正誤が判断できるようになる．しかし，十分な時間的余裕がないときはどうすればよいのだろうか．答えはそれほど単純ではない．「自分で確信が持てないときは，警報を信用する」という，いわば倫理的に正しいことがつねに良いとはいえないからである．

このことを明らかにするため，筆者は，「自分では確証が持てなくても，ともかく警報が鳴っているのだから，警報が正しいものとして対応する」Trustful Policy（TP 方策）と，「警報が鳴っていても，自分で正しいと確認できないのだから警報が誤りであると見なす」Distrustful Policy（DP 方策）の比較を試みた[15]．対象としたのは，航空機における代表的な 3 種の警報，（１）対地接近警報装置 GPWS の「プルアップ」警報，（２）航空機衝突防止装置 TCAS（Traffic Alert and Collision Avoidance System）の回避アドバイザリ（Resolution Advisory）（図５），（３）離陸滑走時の「エンジン故障」警告（caution）メッセージ であり，警報が発せられたとき正報あるいは誤報の条件つき確率，人間が警報を正しく識別する確率，識別を誤る確率，警報の正誤判断に躊躇

（１）採るべきである．TP 方策によって不必要なゴーアラウンドをしたとしても経済的損失を蒙るだけだが，DP 方策を採用してそのまま降下を続けると地表に激突する可能性が増大し，危険回避操作の時間的余裕がなくなる場合がある．

（２）TCAS の回避アドバイザリの正否が判断できない場合は，必ずしも TP 方策が良いとは限らない．誤った回避操作のために指定航路を外れると，管制が当該機を直ちに元の航路に戻すことは難しくなる．特に混雑する空域では，管制の制御を受けられない状況で，周辺のすべての機とのコンフリクトを避けつつ飛行を続けることは，決してたやすいことではない．

（３）離陸滑走時の「エンジン故障」警告メッセージ の正否が判断できない場合は，DP 方策を採るべきである．たとえエンジン故障が離陸決心速度Ｖ１より手前で発生したとしても，判断に躊躇しているうちに時間が経過する．この状況で TP 方策を用いると，離陸中止操作の開始がＶ１を越える可能性が生じる．

なお，（１）と（３）は現在のエアライン各社が採用している方策と一致する．特に（３）はいわゆる Go-Mindedness とよばれる概念を支持する結果となっている．しかし，（２）については種々議論のあるところであり，今後さらに詳細な検討を行う必要であろう．

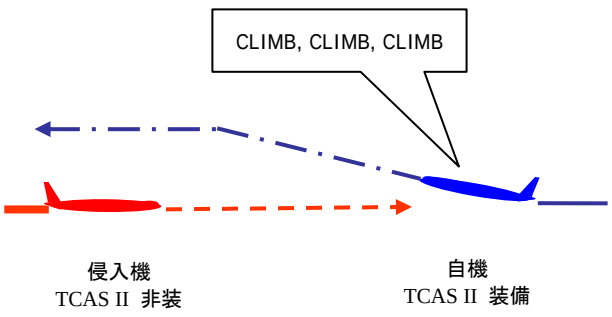

図 5.　TCAS による回避アドバイザリ（上昇）

６．人間と機械の分権協調

警報システムにいかなる知性を付与するかは，今後も挑戦的な課題であり続ける．しかし，警報は，あくまで人間自身に状況を正しく認識させるための情報の提供である．重要な情報を提示しても，人間がその価値を理解しなかったり，情報を見落としたりするようなことがあれば，元も子もな

い.

このようなとき，システム信頼性・安全性に関心のある読者諸賢なら，警報に対応する素振りを見せない人間にかわって，自動化システムに安全を確保させれば良いではないかとお考えになるのではなかろうか.しかし，昨今の流行りでもある「人間中心の自動化」は，人間からの指示なしに自動化システムが勝手に行動するしくみを是としない.「最終決定権を持つのは人間でなければならない」という思想[16] [17]だからである.

もし，人間中心の自動化が「いついかなる場合でも最終決定権は人間に与えられるべきである」とする主張であるなら，この考え方はあまりにも頑なものであるといわざるを得ない．システムに異常が生じた状況では，危険を回避するためになすべきことは多い．しかも，状況の把握，意思決定，操作・行動に許される時間は必ずしも十分ではない．高い信頼性を誇っていたシステムの異常であれば，オペレータは平穏な状況から突如として戦場に放り出されたようなものである．パニックに陥ったとしても不
思議ではない場面で，それでもなお，すべての決断，操作は人間が行うべきなのだろうか.

人間の組織で考えてみよう．何人かの部下を持つ上司がいたとする．突然，この組織の存亡に関わる事態が生じた．迅速かつ的確な対応が求められている．しかし，有能な部下たちは，事態を分析してさまざまな案を進言してくるものの，上司から指示を受けるまで全く行動を起こそうとしない.上司も有能であるから，つぎつぎに決裁し，指示を与えていくが，切迫する時間のなかで，とても一人でさばききれない.「何をすれば良いのかわかっているなら，いちいち人に命令されるまでじっとしていないで，自分でさっさとやってくれよ！」と怒鳴りたくなる.

人間と自動化システムから成るシステムでも，基本的には同じである．コンピュータのように高い知性をもつ機械なら，なおさらそうであろう．どちらか一方に権限を固定するのではなく，眼前に迫った状況に応じて，両者で権限や責任を分担する分権協調形態を考えておく必要があるのではないだろうか．表２に示す「自動化レベル」は，権限や責任の分担にさまざまな形態がありうることを示している[1]．もちろん，表２に示されたもの以外にも，意味のある形態がありうることには注意しておく必要がある.

表２　自動化レベル

---

(1) コンピュータの支援なしに，すべてを人間が決定し，実行.

(2) コンピュータはすべての選択肢を提示し，人間はそのうちのひとつを選択して実行.

(3) コンピュータは可能な選択肢をすべて人間に提示するとともに，そのひとつを選んで提案.
それを実行するか否かは人間が決定.

(4) コンピュータは可能な選択肢の中からひとつを選び，それを人間に提案.
それを実行するか否かは人間が決定.

(5) コンピュータはひとつの案を人間に提示．人間が了承すれば，コンピュータがそれを実行.

(6) コンピュータはひとつの案を人間に提示する.
人間が一定時間以内に実行中止を指令しない

限り，コンピュータはその案を実行.

(7) コンピュータがすべてを行い，何を実行したか人間に報告.

(8) コンピュータがすべてを決定・実行する．人間に問われれば，何を実行したか人間に報告.

(9) コンピュータがすべてを決定・実行する．何を実行したか人間に報告するのは，その必要性をコンピュータが認めたときのみ.

(10) コンピュータがすべてを決定し，実行.

「人間中心の自動化」が主張するように人間に最終決定権を与えておこうとするなら，自動化レベルは最高でも５に留めておかなければならない．しかし，筆者の研究グループが，航空機の離陸継続・中断の意思決定や仮想プラントの制御を例に，数理モデルならびに認知工学的実験によって解析したところによれば，レベル６以上の自動化がシステムの安全性を確保するうえで不可欠であることが判明している[18,19].

また，図１に示したような制御対象，２種類のコンピュータ（TIC, HIC），中央制御室オペレータ，フィールドオペレータから成る監視制御系として原子力プラントをモデル化し，プラント異常が発生したときの対応手順の自動化を検討してみた[20]．機器故障や診断の誤りなどを考慮して，異常への対応に必要な時間の期待値や人間のワークロードなどを最小にするためには，自動化レベル６が最適であるという結果が得られた．ここでも，いわゆる「人間中心の自動化」の理念から外れる結果が得られたことになる.

これらのことは，「人間と機械のどちらに最終決定権を与えるか」については，定性的に議論しても意味がないことを示している．すなわち，制御対象，起こりうる異常などを具体的に設定し，危険を回避するためのタスク系列を明確にした上で，システムの安全確保の観点から人間と自動化システムの分権協調形態を定量的に解析することで，はじめて議論の精密化が可能である．事故が発生したときに現れるような，「自動化するか，しないか」などの単純な議論からは，もはや卒業しても良い時期である[9].

７．さらなる発展を目指して

現在の技術で実現されている多くのシステムは，基本的に極めて高い信頼性を有している．故障が起こるとしても稀であり，いつどこで起こるか予測するほうが難しい.このような状況で，ほとんど起こりもしない異常に備え，いつでも直ちに対応できるように監視を続けなければならない．監視制御で人間に課せられた重要な任務とはいえ，監視業務は単調であり，退屈を伴う．しかも，いざというときになると，一挙に緊張は高まり，抽象的かつ論理的思考も要求される．監視制御は，実は人間に不向きな形態であるといってよいのではないだろうか.

このような中で，人間と知能機械が単に「共存」するだけでなく，たがいに他者の弱点を補い，他者の長所を進展させていく「共生」形態を実現しようとするとき，両者がたがいの意図を正しく認識できるしくみを考案することが重要である．過去の航空事故では，自動化システムの自律行動が，パイロットの状況認識を混乱させるオートメーション・サプライズ（automation

surprises）現象[21]が見られる．いかに高い知性を持っていても，たがいの意図が了解できていないところに信頼は生まれない．さらに，信頼を醸成しつつも過信を招かないようにすることは，決して易しいことではない．しかし，高い信頼が警戒心を損い，安全を脅かす事態に至ることだけは，なんとしても避けなければならない．信頼と警戒心の絶妙なバランス，ヒューマンマシンシステムの安全確保の課題である．

参考文献

[1] Sheridan: Supervisory Control, Handbook of Human Factors, Wiley, 1295-1327 (1997).

[2] Endsley: Towards a Theory of Situation Awareness in Dynamic Systems; Human Factors, 37(1), 32-64 (1995).

[3] Jones & Endsley: Investigation of Situation Awareness Errors; Proc. 8th International Symposium on Aviation Psychology, 746-751 (1995).

[4] Hawkins: Human Factors in Flight, 2nd Ed., Avebury Technica (1993).

[5] 稲垣:ヒューマンマシンシステムにおけるチームの功罪，日本原子力学会第１１回ヒューマンマシンシステム研究夏期セミナー, 15-25 (2000).

[6] 稲垣 : 状況認識喪失の多様性，ヒューマンインタフェース学会誌，2(1),33-35(2000).

[7] 稲垣:誰のための自動化？, 計測と制御, 32(3), 181-186 (1993).

[8] Lee & Moray: Trust, control strategies and allocation of function in human machine systems; Ergonomics, 35(10), 1243-1270 (1992).

[9] 稲垣 :「人間中心の自動化」は何をめざす？，計測と制御，37(8), 572-577 (1998).

[10] 前根：事故のモンタージュ VII, 全日空(1998).

[11] Moray & Inagaki: Laboratory studies of trust between humans and machines in automated systems, Trans. Inst MC, 21(4/5), 203-211 (1999).

[12] 稲垣：ヒューマン・マシン・システム――高信頼性が損う安全性：システム／制御／情報，41(10), 403-409 (1997).

[13] Bresley & Egilsrud: Enhanced Ground Proximity Warning System, Safety Bird, 33, 12-22 (1997).

[14] Inagaki & Yokoba: Trust in and reliance on an automated warning with two failure modes: Observations from a viewpoint of situation awareness, Proc. HPSAA, 82-87 (2000).

[15] Inagaki & Parasuraman: Probabilistic analysis of human interaction with automated alerts, Proc. 5th PSAM, 2405-2410 (2000).

[16] Woods: The effects of automation on human's role; NASA CP-10036, 61/85 (1989).

[17] Billings: Aviation Automation, LEA (1997).

[18] Inagaki: Situation-adaptive autonomy for time-critical takeoff decisions, International Journal of Modelling and Simulation, 20(2), 175-180 (2000).

[19] Moray, Inagaki, & Itoh: Adaptive automation, trust, and self-confidence in fault management of time-critical tasks, Journal of Experimental Psychology: Applied, 6(1), 44-58 (2000).

[20] Furukawa, Niwa, & Inagaki: Levels of automation in emergency operating procedures for a large-complex system: Probabilistic

analysis on human-automation collaboration, Proc. HCI 2001 (to appear).
[21] Sarter, Woods, & Billings: Automation Surprises, Handbook of Human Factors, Wiley, 1926-1943 (1997).