ヒューマンファクターを包含する記号論理体系に基づく実時間知的システムの分析

水谷哲也† 五十嵐滋‡ 塩雅之‡ 池田靖雄*

†筑波大学 ‡常磐大学 *埼玉短期大学

概要 $N\Sigma$ラベル付カルキュラスは，外部の物理的または論理的現象を制御する人間またはコンピュータプログラムの，時間に依存して変化する知識・信念およびそれに基づく決定を記述・分析・検証する形式的体系である．この体系で，信楽高原鐵道列車衝突事故およびJAL焼津沖ニアミス事故の論理的分析を行う．これらは連続系を制御するシステムであり，誤解や誤認識をもつヒューマンファクターを内包している．これらの例を分析することにより，人工知能と，プログラムが制御する外部環境およびヒューマンファクターの関係についての研究が行われる．

Abstract $N\Sigma$-labeled calculus is a formal system in order to describe time-concerned recognition, knowledge, belief and decision of humans or computer programs together with related external physical or logical phenomena.
Formal verification and analysis of the Shigaraki Kougen Railway accident and the JAL near miss accident in this formalism will be presented as examples of cooperating systems controlling continuously changing objects including human factor with misunderstanding or incorrect recognition.
Through these examples, relationship among artificial intelligence, external environment and human factors will be investigated.

1. はじめに

近年，複雑な外部系を制御する系，特に，鉄道・航空機の制御系のような，重大な事故がソフトウェアやハードウェアのバグや不具合によるもののみならず，時々刻々変わる人間の誤認識・誤判断など時間に依存するヒューマンファクターを内包する人為的なエラーから引き起こされる可能性がある系を解析・検証する形式理論の研究の重要性が明らかになってきている．

$N\Sigma$ラベル付カルキュラス(*$N\Sigma$-labeled calculus*) [Miz06], [Miz07], [Iga08]は，外部の物理的または論理的現象を制御する人間またはコンピュータプログラムの，時間に依存して変化する知識・信念およびそれに基づく決定を記述・分析・検証する形式的体系である．

自動車運行制御システムの形式化[Dam06]，人間-計算機相互システムの形式化[Cur07]等の関連研究がある．

2. $N\Sigma$ラベル付カルキュラス

Peano 数論*PA*を無限大(∞)と最小作用素(μ)を追加することにより拡張する．これを**擬数論** (*pseudo-arithmetic*) *PA*(∞)とよぶ．*PA*(∞)に，自然数または∞を値とする**特殊定数** (*special constants*) J, J_1, J_2, ... および**ラベル** (*labels*) ℓ , ℓ_1, ℓ_2, ...を加える．特殊定数はプログラム変数を表現するのに用いられ，値は自然数値または∞をとる．自然数時刻に沿って変化する値は局所モデル(*local model*)の変化を意味し，逆に局所モデルが変化すれば特殊定数の値は変化しうる．ラベルは**人格**(*personality*)を示し，マルチエージェントシステムでの**エージェント**(*agent*)または物理学における**観察者**(*observer*)等の一般化概念である．

時制(*tense*)は観測時刻からの相対的な時間を意味する．観測時刻は現在または現時点などとよび，体系内では値 0 をとる．

論理記号として@を加える．@は**同時記号**(*coincidental operator*)とよぶ．**a** を $N\Sigma$ラベル付カルキュラスの項，ℓ をラベル，**A** を命題とするとき，**A@<a**, ℓ > は **a** が示す時制で，ℓ で表される人格が，**A** が現時点で成立することを**信じる**(*believes*)，または**考える**(*thinks*)ことを示す命題である．**A@a** は **A** が **a** で成立することを示しており，**A@**ℓ は **A@<0**, ℓ >の略記である．

3. 協調連続系の表現

3.1 拍車とプログラムラベル

α，β，γ，... ，κといったメタ記号で表される**拍車** (*spurs*)はスケジューラや'X'や'○'といった時相論理(temporal logic)の'next'論理記号等の一般化概念であり，$N\Sigma$ラベル付カルキュラスの項として定義される．マルチ CPU 並行プログラム系の各プロセスおよび各外部オブジェクトに異なった拍車を割り当てる．各オブジェクトは対応する拍車が示す時刻に活性化し，変数の値を変化させる．

プログラムラベル(*program labels*)は真理値をとる特殊定数として定義され，*a*, a_1, ... といったメタ記号で表される．一つのプロセスまたはオブジェクトの中では排他的である．

3.2 連続系の近似表現

連続系を含む協調系を表現し，解析・検証するためには微分概念を取り扱う必要 がある．本論文では 2 階の導関数をプログラム変数と同一視し，1 階の導関数および原始関数を高階の導関数の積分により定義する．その積分はオイラー積分による近似式として定義する．

4. 実時間知的協調システムの形式的表現・分析

4.1 信楽高原鐵道列車事故

事故の概要 1991 年(平成 3 年)5 月 14 日，10 時 35 分ごろ滋賀県の信楽高原鐵道信楽線の小野谷信号場～紫香楽宮跡駅間で，信楽発貴生川行きの上り普通列車と，京都発信楽行きの JR 直通下り快速列車とが正面衝突した．信楽駅を貴生川駅行きの普通列車が発車しようとした際，通常青に変わるはずの出発信号機が発車時刻になっても赤のままであったが，信楽高原鐵道では誤出発検

Analysis of Time-Concerned Intellectual Systems based on a Symbolic-Logical System involving Human Factor
†Tetsuya Mizutani: University of Tsukuba
‡Shigeru Igarashi, Masayuki Shio: Tokiwa University
*Yasuwo Ikeda: Saitama Junior College

index	condition	action	tense	personality
1	*Clock=r*, global		*r*	* *S, J*
2	*A=l, B≦0 ¬13R, ¬lock, global*		*Clock=0*	* *S, J*
3	*r+≡r≦Clock, def*			* *S, J*
4		α=10:25+1	*A=l*	* *S*
5		$\gamma=\alpha$	〃	*S*
5'	—	—	—	—
6		$\gamma=\alpha$	*A=d+u*	*S*
7		$\kappa=\alpha$	*A=d*	*S*
8	*¬13R*	*γ=lock*		* *S*
9	*lock*	*γ=¬lock*		* *S*
10	0<*i*<imax	$\alpha^{i+1}=\alpha^{i}+1$		* *S, J*
11	0<*i*≦imax	*A=l-i・u*	α^{i}	* *S, J*
12		$\beta=13R+1$	*B=d*	* *S, J*
13	0<*j*<jmax, j≠jmid	$\beta^{j+1}=\beta^{j}+1$		* *S, J*
14	0<*j*≦jmid	*B=j・v*	β^{j}	* *S, J*
15	jmid<*j*≦jmax	*B=d+j・w*	β^{j}	* *S, J*
16		$\beta=\kappa$	B=c	* *S, J*
17		$\kappa=12R$		* *S, J*
18	*¬lock*	$\kappa=13R$		* *S, J*
19	10:16≦[*B*=0], global			* *S, J*
20	v≦c/(9・60), global			* *S, J*
21	*d<A<l⇒B≦ d*		x+10:25+1	*S*
22	*¬Crash*		x+10:25+1	*S*
23	*d<A<l∧d≦B<d*		∃x.x+10:25+1	*
24	*Crash*		∃x.x+10:25+1	*

表 1　信楽高原鐵道運行システムの公理タブローによる表現

知装置を頼りにして普通列車を 11 分遅れで見切り発車させた．しかし，対向の小野谷信号場の下り出発信号機は信楽駅上り列車が出発したら赤に変わるはずなのに青のままで，下り快速列車は青信号に従ってそのまま進行し，正面衝突に至った．

形式化　列車運行システムを公理タブロー(axiom tableux)[Iga03][Miz06]で表したものを表 1 に示す．人格の対象は信楽鉄道と JR であり，各々のラベルを *S, J* とする．1-20 がこのシステムの公理系である．このうち 5 は小野谷信号場の下り出発信号機を適切に赤信号にするための信号を信楽駅から信号場まで送る公理である．これらより 21 および 22，すなわち衝突事故が起こらないことが導かれる．5'は実際に起った行為で，5 が成立しないことを示している．5 を除いた 1-4, 6-20 から 23 および 24 すなわち衝突事故が起こることが導かれる．

4.2 JAL焼津沖ニアミス事故

事故の概要　2001 年(平成 13 年)1 月 31 日，15:51 ごろ静岡県焼津沖で羽田から那覇に向かっていた日本航空 907 便と韓国の釜山から成田に向かっていた日本航空 958 便の 2 機の旅客機がニアミスを起こし，907 便は衝突回避のため急降下した．原因は少なくとも以下の 3 点があげられる．(1)訓練中であった管制官が，958 便に下降指示を出すはずが便名を取り違えて上昇指示を出さねばならない 907 便に降下を指示した．(2)直後に 907 便の TCAS(空中衝突防止装置)は上昇の指示を出していたが，管制の指示は航空管制では「国土交通大臣の命令である」とみなされていたため機長はこれに従った．(3)事故当時は TCAS の指示は機械の誤作動が多いとして，TCAS と航空管制官の指示が矛盾している場合には、航空管制官の指示を優先することとなっていた．

形式化　双方の航空機のパイロット，管制(ACC)および TCAS の動作を公理タブローで記述したものが表 2 である．このうち，[Actual]は実際のニアミス事故の動作のタブローであり，5.2 で表される ACC の行為(JL907 に降下指示を出す)が誤っていることは明らかである．

[Actual (incorrect, insecure)]

idx	condition	action	tense	personality
1	*¬ACCCl*(JAL907)	D_1= *PitchDown* = α	*t*; ↑(*ACCDes*(JL907) ∨ *TCASDes*(JL907))	* JL907
2	*¬ACCDes*(JAL907)	D_2= *PitchUp* = α	*t*; ↑(*ACCCl*(JL907) ∨ *TCASCl*(JL907))	* JL907
3		D_3=(A=-a)= α	t; ↑ *PtchDwn*(JL907)	* JL907
4		D_4=(A=-b)= α	*t*; ↑ *PtchUp*(JL907)	* JL907
5.1	$A_t<B_t$	*ACCDes*(JL907)	*t*;*Dang*(A, B)	* ACC
5.2	**otherwise**	*ACCDes*(**JL907**)	*t*;*Dang*(A, B)	ACC
6.1	$A_t<B_t$	*TCASDes*(JL907)	*t*;*Dang*(A, B)	* TCAS
6.2	**otherwise**	*TCASDes*(JL958)	*t*;*Dang*(A, B)	* TCAS

[Correct, Secure]

1	*¬TCASCl*(JAL907)	D_1= *PtchDwn* = α	*t*; ↑(*ACCDes*(JL907) ∨ *TCASDes*(JL907))	* JL907
2	*¬TCASDes*(JAL907)	D_2= *PtchUp* = α	*t*; ↑(*ACCCl*(JL907) ∨ *TCASCl*(JL907))	* JL907
5.2	**otherwise**	*ACCDes*(**JL958**)	*t*;*Dang*(A, B)	ACC

表 2　JAL 運行システムの公理タブローによる表現

これに対し，[Correct, Secure]は誤りを修正した(5.2)上に，「パイロットは ACC より TCAS の命令を優先する (1, 2)」とより安全なシステムに修正したもので，万一管制官が誤認識により誤指示を出しても事故は起こらないということが導かれる．

5. 結論

時間に依存して変化するヒューマンファクター，すなわち知識・信念およびそれに基づく決定によって外部の物理的または論理的現象を制御システムの解析・検証のための形式的体系 $N\Sigma$ ラベル付カルキュラスを，解析の具体例とともに紹介した．今後の目標は，人間の誤認識に対してもシステムが安全であることを示す形式的体系を構築することである．

参考文献

[Cur07] Curzon, P., Ruksenas, R. and Blandford, A. : An Approach to Formal Verification of Human-Computer Interaction, *Formal Aspect of Computing*, **19** (2007), pp. 513–550.

[Dam06] Damm, W., Hungar, H. and Olderog, E.-R. : Verification of Cooperating Traffic Agents, *International Journal of Control*, **79** (2006), pp. 395–421.

[Iga03] Igarashi, S., Mizutani, T., Ikeda, Y. and Shio, M. : Tense Arithmetic II: @-calculus as an Adaptation for Formal Number Theory, *Tensor, N. S.*, **6** (2003), pp. 12–33.

[Iga08] Igarashi, S., Shio, M., Mizutani, T. and Ikeda, Y. : Specification and Verification of Cooperative Real-Timing Processes in @-Calculus, submitted.

[Miz06] Mizutani, T., Igarashi, S., Ikeda, Y. and Shio, M. : Labeled @-Calculus: Formalism for Time-Concerned Human Factors, *AISC 2006, 8th International Conference on Artificial Intelligence and Symbolic Computation, Lecture Notes on Artificial Intel ligence*, **4120** (2006), pp. 25–39.

[Miz07] Mizutani, T., Igarashi, S., Shio, M. and Ikeda, Y. : Human Factors in Continuous Time-Concerned Cooperative Systems Represented by $N\Sigma$-labeled Calculus, *Fifth Asian Workshop on Foundation of Software* (2007), pp. 42–51.