場と有限状態機械の概念に基づいたモバイル並行システムの仕様化手法とその適用

板橋吾一[†1] 高橋薫[†2] 加藤靖[†2]
加藤貴司[†3] ベッド B. ビスタ[†4]

一般にシステムを高信頼に設計するには，その要件や内容を曖昧なく厳密に仕様化することが望ましい．本論文では，セルラーシステムなど，並行性や移動性を特徴として有するシステムを対象に，その形式的なモデル化と仕様化の手法を提案する．本手法ではまず，システムの構成単位であるエンティティ間の通信の局所性を取り扱うために場の概念を導入する．ここで，エンティティを通信型有限状態機械でモデル化し，エンティティの移動やそれらの間の結合関係とその動的変化を明示的に扱えるようにしている．これらエンティティの組織体としてシステム全体を定義することで，モバイル並行性を有するシステムの仕様の形式的な取扱いと動作の形式的な検証が可能となっている．また，本提案手法を具体的に PHS システムの仕様化とエージェント指向コンピューティングの分野の仕様化に適用を行い，本手法の適用可能性と有効性について確認する．

A Specification Method for Mobile and Concurrent Systems Based on the Concept of Field and Finite State Machine, and Its Application

Goichi Itabashi,[†1] Kaoru Takahashi,[†2] Yasushi Kato,[†2]
Takashi Katoh[†3] and Bhed B. Bista[†4]

This paper proposes a modeling and formal specification method for mobile and concurrent systems such as a cellular system. In this method, the concept of a field is first introduced to deal with the locality of communication between entities (e.g. terminals) within the system. An entity is modeled as a communicating finite state machine, and the migration of an entity and the dynamic change of associations among entities can be explicitly specified. Thereby, it becomes possible to formally treat and validate the behavior of such systems. In order to demonstrate the applicability and effectiveness of our method, we apply it to the specification of the Personal Handyphone System and an agent oriented computing.

1. はじめに

移動性と並行性を有するモバイル並行システムにおいて，システム構成要素（エンティティ）間にはなんらかの結び付きが存在し，エンティティ間の結び付きはシステム全体の構造を決定する．このようなシステムとして移動通信が考えられる[1)]．移動通信では，セルラー方式や PHS に見られるように，移動局と基地局との交信可能な領域を狭くし，その分だけ基地局を多く配置して無線周波数の再利用を行っている．移動通信では，移動局，つまりエンティティがシステム内を自由に移動し，エンティティ間の結び付きを静的なだけではなく動的にも確立・切断することによって全体の処理が実行される．その結果システム全体の構造は動的に変化し，システムの設計は難しくなる．

上記のようなモバイル並行システムを設計するためには，システムを曖昧なく厳密に仕様化することが望ましい．これにより仕様段階でのシステムの解析が可能となり，システム設計の高信頼化が達成できる．

ネットワークの動的変化およびエンティティの移動性を曖昧なく仕様化するために π 計算[2)]が提案され，さらには通信の局所性を表現するために文献 3)~5) などの手法が提案されている．これらは CCS[6)]や CSP[7)]

†1 株式会社サイエンティア
Scientia Corporation
†2 仙台電波工業高等専門学校
Sendai National College of Technology
†3 東北大学
Tohoku University
†4 岩手県立大学
Iwate Prefectural University

などのプロセス計算モデルに基づいており，より抽象的で簡潔な仕様を記述することができるが，結び付きの確立・切断の表現が明示的ではなく，システムをブラックボックス化し，外部イベントの観点から仕様化するため，システムの実装には距離がある．これに対して，筆者らはこれまで通信型有限状態機械（CFSM: Communicating Finite State Machine）[8)~10)]の概念を用いて，エンティティ間の結び付きの確立・切断およびエンティティの挙動をより明示的に表現する方法について検討を行ってきた[11)]．有限状態機械は，内部状態を持ち，外部環境との入出力相互作用を介して状態遷移を起こしながら動作を繰り返していく抽象的実体である．これは記述内容の理解の容易性に加え，システムの実装にもより近いという特徴を有する．

本論文では，上記の有限状態機械の概念および通信の局所性を有効に表現する手段としての場の概念に基づいて，モバイル並行システムの設計を高信頼・効率的にすることを目的に，システム構成要素間での通信路の動的な設定，局所的な通信，構成要素のシステム内での自由な移動などの特性を反映したシステムのモデル化と仕様化の手法を提案する．これにより，システムの実装の前に，システムの挙動をシミュレートしたり検証したりすることが可能になる．なお，本論文は文献 11) の手法を，通信の局所性，構成要素の移動性，通信路の設定の多様性に関して拡張・強化したものであり，仕様化の適用範囲を大幅に向上させている．

以下本論文では，まず 2 章で場と有限状態機械の概念に基づいたモバイル並行システムのモデル化と形式化，そしてシステムの挙動の特性化について述べる．次に 3 章で，本手法の適用性と有効性を示すために，PHS システム[13)]の仕様化，およびエージェント指向コンピューティング分野[14)]の仕様化を行い評価する．最後にまとめと課題を 4 章で示す．

2. 仕様化手法

本章ではまず，有限状態機械（CFSM）の相互作用の局所性と移動性を取り扱うために場の概念を導入する．次に，システムエンティティを有限状態機械の概念を用いてモデル化・形式化し，最後に，システム全体の挙動を有限状態機械全体の状態遷移の観点から特性化する．

2.1 場

有限状態機械が存在しうるロケーション（位置，場所）の有限集合を L とする．L の要素を l とし，各ロケーションを自然数で表す．有限状態機械はロケーションの上を自由に移動可能であると仮定する．チャネルは有限状態機械間および環境と有限状態機械との結び付きを表す抽象概念である．ここで環境はモデル化しないシステムの外界を表し，システム仕様に記述しない有限状態機械群を表すと考える．たとえば，システムのエンティティを一部だけ記述する場合は記述しない部分を環境として考える．環境と有限状態機械の間には暗黙のチャネルがあると考える．これを環境チャネルと呼び，$\mathbf{c}_{\mathrm{e}}$ で表す．有限状態機械間のチャネルの集合は $\mathcal{C}_f$ で表す．便宜上，ある固定正整数 m について，$|\mathcal{C}_f| = m$ とし，$\mathcal{C}_f$ の各要素を c_i $(1 \leq i \leq m)$ で表す．

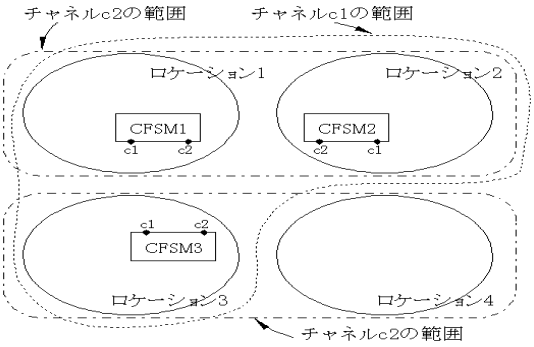


図 1 場の例
Fig. 1 An example of a field.

有限状態機械間の相互作用はある範囲内に制限され，この相互作用可能な範囲はチャネルによって異なると考える．これを次のように表現する．

定義 1. 有限状態機械が存在しうる場 $\mathcal{F}$ を次のように定義する☆．

$$\mathcal{F} = \{(c_i,\ COM(c_i)) \mid c_i \in \mathcal{C}_f,\ COM(c_i) \subseteq \mathcal{P}(L),\ 1 \leq i \leq m\}$$

□

ある c $(c \in \mathcal{C}_f)$ と P $(P \subseteq L)$ について，$P \in COM(c)$ であることは P に属するロケーションに存在する有限状態機械はチャネル c を経由して互いに相互作用可能であることを意味する．逆に，P に属していないロケーションに存在する有限状態機械はチャネル c を経由して互いに相互作用することはできない．$COM(c_i)$ のそれぞれの要素を c_i の範囲と呼ぶ．

例 1. $L = \{1,\ 2,\ 3,\ 4\}$ および $\mathcal{C}_f = \{c_1,\ c_2\}$ に対して，場 $\mathcal{F}$ の例を示す．

$$\mathcal{F} = \{(c_1,\ COM(c_1)),\ (c_2,\ COM(c_2))\}$$
$$COM(c_1) = \{\{1,\ 2,\ 3\}\},$$
$$COM(c_2) = \{\{1,\ 2\},\ \{3,\ 4\}\}.$$

図 1 は，ロケーション 1 に $CFSM1$，ロケーション 2

☆ $\mathcal{P}(S)$ は集合 S のべき集合を表す．

に $CFSM2$，ロケーション 3 に $CFSM3$ を配置した例である．すべての有限状態機械はチャネル c_1 と c_2 を持ち，場 $\mathcal{F}$ の上を移動可能である．この状況において，すべての有限状態機械はチャネル c_1 を経由して互いに相互作用可能である．$CFSM1$ と $CFSM2$ はチャネル c_2 を経由して相互作用可能である．しかしながら，$CFSM3$ はチャネル c_2 を経由しては $CFSM1$，$CFSM2$ と相互作用することができない．これは $\{1,\ 2,\ 3\} \subseteq P \in COM(c_2)$ であるような P が存在しないからである． □

このように，有限状態機械間の相互作用は場によって制約を受け，その設定に変化を持たせることで種々の局所性と相互作用形態を表現できるようになる．

ここで提案する場の概念には次の 2 つの性質（制約）を持たせる．

(1) $COM(c)$ が $P \subseteq L$ かつ $l \in P$ であるような P を含まないとき，同じロケーション l の上にある有限状態機械はチャネル c を経由して互いに相互作用することはできない．

(2) $P,\ P' \in COM(c)$ $(P \neq P')$ のとき，P と P' は互いに素でなければならない．さもないと $l \in P \cap P'$ であるような l についてチャネル c の範囲がオーバラップし，どの範囲が選ばれるかを一意に識別することができなくなる．

2.2 システムのモデル化

モバイル並行システムを，チャネルを経由して相互作用を行ういくつかの有限状態機械の集まりとしてモデル化する．

定義 2. モバイル並行システム Sys を次のように定義する．

$$Sys = \langle (CFSM_1,\ \cdots,\ CFSM_k,\ \cdots,\ CFSM_n),\ (l_1,\ \cdots,\ l_k,\ \cdots,\ l_n),\ \mathcal{C} \rangle$$

ここで，$\mathcal{C}$ $(\mathcal{C} = \mathcal{C}_f \cup \{\mathbf{c}_e\})$ は Sys のチャネルの有限集合を表す．$CFSM_k$ $(1 \leq k \leq n)$ は通信型有限状態機械であり次のように定義する．

$$CFSM_k = \langle Q_k,\ C_k,\ E_k,\ \delta_k,\ q_{k0} \rangle$$

ただし，Q_k は状態の有限集合，C_k は $CFSM_k$ の持ちうるチャネルの有限集合 $(C_k \subseteq \mathcal{C})$，$E_k$ はイベントの有限集合（下に列記），δ_k は状態遷移関数 $(\delta_k : Q_k \times E_k \to Q_k)$，$q_{k0}$ は $CFSM_k$ の初期状態 $(q_{k0} \in Q_k)$ である．l_k $(1 \leq k \leq n)$ は $CFSM_k$ の初期ロケーションを表す． □

上記定義中のイベントとして以下のものを考える．(i) $(c,\ (\alpha_1,\ \cdots,\ \alpha_h))$：チャネル c $(c \in C_k)$ を経由した $CFSM_k$ の入力または出力の列 $\alpha_1 \cdots \alpha_h$ の生起；(ii) $(c,\ a)$：チャネル c $(c \in C_k)$ を経由した $CFSM_k$ の制御イベント a の生起；(iii) p：$CFSM_k$ の内部処理 p の生起．本モデルでは，状態遷移中になんらかの処理 p を定義できることを仮定している☆；(iv) $(d,\ u)$：判断結果が自然数 u で表されるような処理判断 d の生起．上と同様，状態遷移中になんらかの判断 d を定義できることを仮定している．任意の判断 d を評価可能で，その値域が $\mathcal{P}(\mathcal{N})$ ($\mathcal{N}$は自然数の全体) であるような関数 $\mathcal{I}$ を仮定する．もし，$u \in \mathcal{I}(d)$ ならば，u は判断 d を評価した結果の 1 つであると考える；(v) (“$move$”, l)：$CFSM_k$ のロケーション l $(l \in L)$ への移動；(vi)“ε”：内部イベントの生起．他の有限状態機械とは同期をとらずに有限状態機械内で勝手に生起できる性質を持つ．これは故障など例外事象の記述に役立つ．

$CFSM_k$ における状態遷移はこれらのイベントの生起により可能となる．以上からここで与えている通信型有限状態機械は，他の有限状態機械（環境）との相互作用やロケーション移動を行いながら，内部処理・内部遷移分岐をともなって状態遷移動作を繰り返す抽象的実体ととらえることができる．

制御イベントとしてチャネルの確立（connect），チャネルの切断（disconnect），チャネルの強制放棄（abandon）を考える．種々のモバイル並行システムの仕様記述を可能とするため，チャネルについて以下のような取扱いを考慮している．チャネルは不特定多数の有限状態機械の間で確立することができ，また，指定した有限状態機械との間のチャネル確立を拒否することができる．入力または出力は環境も含めて n $(n \geq 2)$ 個の有限状態機械間および環境と有限状態機械との間にチャネルが確立して初めて可能となる．すなわち，チャネルが確立しているときのみ互いの入出力が可能となる．ただし，環境チャネルは各有限状態機械との間に暗黙に確立されていると仮定する．また，仕様記述者は有限状態機械間に，あらかじめ暗黙に確立されているチャネルを指定することができる．これを暗黙確立チャネルと呼ぶ．有限状態機械間および環境で入出力されるオブジェクトにはメッセージとチャネル名の 2 つの型を想定する．メッセージはチャネル名以外の意味を持つ情報を表し，例としてはデータパケットや音声情報がある．チャネル名の入出力を可能とすることで，たとえば，他から受け取ったチャネル名が表すチャネルを用いた有限状態機械間の新たな相互作用などが表現できるようになる．この概念は π 計算[2]から借りたものであり適用性は高い．

☆ 定義形式には立ち入らない．

記法 1. 個々の有限状態機械に対する記法・記号を以下のように定める．(1) $\#c$：チャネル c の確立．拒否したい有限状態機械があれば $\#c[[\mathbf{x}]]$ のように書く．ここで $\mathbf{x}$ は拒否指定する有限状態機械のリストである；(2) $/c$：チャネル c の切断；(3) $//c$：チャネル c の強制放棄；(4) $?x$：メッセージ x の入力；(5) $??y$：チャネル名 y の入力；(6) $!m$：メッセージ m の出力；(7) $!!c$：チャネル名 c の出力；(8) $c\alpha_1 \cdots \alpha_i \cdots \alpha_h$：チャネル c での入出力系列 $\alpha_1 \cdots \alpha_h$；(9) $\hookrightarrow l$：ロケーション l への移動；(10) $q \xrightarrow{e} q'$：状態 q から q' へのイベント e による遷移；(11) $q \xrightarrow{e}$：$q \xrightarrow{e} q'$ なる q' が存在；(12) $q \not\xrightarrow{e}$：$q \xrightarrow{e}$ でない；(13) $q \rightarrow$：$q \xrightarrow{e}$ なる e が存在；(14) $q \not\rightarrow$：$q \rightarrow$ でない． □

本仕様化法では，有限状態機械の移動先のロケーション l があらかじめ分かっているものとして $\hookrightarrow l$ のように記述することを前提にしており，移動先があらかじめ分かっていないような場合の記述は対象外としている．

有限状態機械は通常の状態遷移図のように図式的に表現可能である．状態は円記号で示す．遷移は状態間の矢印で示す．矢印には遷移の原因となるイベント（名）がともなう．イベントの中でも処理と判断は特別な記号で表す．処理イベントは矩形で示し，内部に処理のステートメントを示す．判断イベントはひし形または三角形で示し，内部に判断のステートメントを示す．本仕様化法では，処理と判断のステートメントの形式的な表現は与えず，仕様記述者にまかせる．図を簡単に読みやすくするために，処理記号と判断記号の元の状態と行き先の状態は，省略してもよいことにする．

2.3 システムの挙動

システムの挙動を次の 6 つのイベントによって特性化する．(i) チャネル確立（グループ形成）；(ii) オブジェクトの入出力（グループ内入出力）；(iii) チャネル切断（グループ解消）；(iv) チャネルの強制放棄；(v) ロケーションの移動；(vi) 内部処理（内部イベント，判断，処理）．システム状態を導入することにより，システムの挙動をシステム状態の遷移系列（システム状態グラフ）として表現する．

始めに，システムの挙動を次に述べる考えをもとにして特性化する．

(1) システムの挙動開始時には，後述の暗黙確立チャネルを除き，有限状態機械間にチャネルは確立されていない．各有限状態機械と環境との間には，環境チャネルが暗黙に確立され，すべての有限状態機械は初期状態にあり，あるロケーション上に存在している．

(2) チャネル確立

(a) 環境チャネルを除いて，複数の有限状態機械が connect を同時に発することで，それらの間にチャネルが確立する．connect の発生時，有限状態機械は対応するチャネルの範囲に属するロケーションに存在しなければならない．connect の発生による状態遷移は対応する 1 つ以上の有限状態機械の connect の発生による状態遷移と同期して起こる．チャネルが確立した後，関連する有限状態機械は，そのチャネルによって互いに接続される．そして，有限状態機械間で入出力イベントの実行が可能となる．チャネルによって接続された有限状態機械の集団をグループと呼ぶ☆．なお，有限状態機械の間でチャネル確立を拒否することができる．チャネル確立の拒否というのは，拒否指定した有限状態機械間ではチャネル確立を拒否し，他の有限状態機械との間ではチャネル確立を行ってもよいことを意味する．これは電話システムなどで着信拒否をモデル化するのに使用できる．拒否相手の設定はチャネル確立の時点で行う必要があり，確立後の拒否相手変更は行えないことに注意されたい．また，暗黙確立チャネルは，connect を発することなしに該当する有限状態機械との間で暗黙に確立されている☆☆．これは制御用の通信路や周波数など常時設定されているチャネルを表すのに使用できる．

(b) 環境チャネルは，connect を発することなしに，任意の有限状態機械と環境の間で暗黙に確立されている☆☆☆．

(3) オブジェクトの入出力

(a) 環境チャネルを除いて，1 つの有限状態機械のオブジェクトの出力による状態遷移は，グループの他の入力と同期して起こる．つまり，グループの形成形態に応じて，ポイントツーポイント型を含むマルチキャスト型の同期通信を想定しており，入出力は 1 つの有限状態機械とグループに属する他のすべての有限状態機械との間で行われる．なお，各有限状態機械はチャネルの範囲に属するロケーションに存在しなければならない．

(b) 環境チャネルに関しては，有限状態機械はオブジェクトを入出力可能な状態にいるときに，入出力を実行して状態遷移することができる．

(4) チャネルの切断

(a) 環境チャネルを除いて，グループを形成したチャネルはそのグループのすべての有限状態機械が同

☆ 各グループを有限状態機械の集合で表す．
☆☆ 該当する有限状態機械間から成るグループが暗黙に形成される．
☆☆☆ 有限状態機械と環境から成るグループが暗黙に形成される．

期して disconnect を発することで切断される．disconnect の発生時，各有限状態機械はチャネルの範囲に属するロケーションに存在しなければならない．グループはチャネルが切断された後に解消される．disconnect の発生による状態遷移は，グループの他の disconnect の発生と同期して起こる．なお，暗黙確立チャネルに関しては，同様に切断を行ってもよく行わなくてもよい．

(b) 環境チャネルの切断はできない．

(5) チャネルの強制放棄

(a) 環境チャネルを除いて，グループを形成したチャネルはそのグループの中にある有限状態機械が abandon を発することで強制的に切断される．これは復旧回復などの記述に使用できる．abandon の発生時，各有限状態機械はチャネルの範囲に属するロケーションに存在しなければならない．グループはチャネルが切断された後に解消される．なお，暗黙確立チャネルに関しては，同様に放棄を行ってもよく行わなくてもよい．

(b) 環境チャネルの放棄はできない．

(6) 有限状態機械は移動イベントの実行により，どのロケーションにも移動することができる．

(7) 有限状態機械は内部イベント，判断イベント，処理イベントの実行によって状態が変化する．

(8) システム全体はそれぞれの有限状態機械の状態遷移によって挙動が進行していく．

チャネル確立の例として，$CFSM1$，$CFSM2$，$CFSM3$，$CFSM4$ の 4 つの有限状態機械がチャネル c で確立を試みる場合について示す．$CFSM1$ と $CFSM2$ はどちらも $CFSM3$，$CFSM4$ を拒否指定し，$CFSM3$ は $CFSM1$ とのチャネル確立を拒否，そして，$CFSM4$ は相手を指定していないものとする．この場合，$CFSM1$ と $CFSM2$ でチャネル c が確立可能であり，$CFSM3$ と $CFSM4$ でチャネル c が確立可能である．よって，$CFSM1$ と $CFSM2$，$CFSM3$ と $CFSM4$ の 2 つのグループができる．以下では，$CFSM_r$ がチャネル c で確立を拒否指定している有限状態機械群を $R_c(r)$ で表す．

以上の特性化から，各有限状態機械の状態，各有限状態機械が存在しているロケーション，そして各チャネルの状態で表現するシステム状態を考えることができる．システムの挙動をそのようなシステム状態の遷移の系列として定義することができ，それをシステム状態グラフと呼ぶ．

定義 3. モバイル並行システム

$$Sys = \langle (CFSM_1, \cdots, CFSM_k, \cdots, CFSM_n),\ (l_1,\ \cdots,\ l_k,\ \cdots,\ l_n),\ \mathcal{C} \rangle$$

に対して，Sys のシステム状態を以下のように定義する．

$$s = \langle (q_1, \cdots, q_k, \cdots, q_n), (l'_1, \cdots, l'_k, \cdots, l'_n), (sc_1, \cdots, sc_i, \cdots, sc_m, sc_e) \rangle$$

ここで，q_k $(1 \leq k \leq n)$ は $CFSM_k$ の状態である．$l'_k \in L$ $(1 \leq k \leq n)$ は $CFSM_k$ の存在しているロケーションを示している．そして，sc_i $(1 \leq i \leq m)$ と sc_e はチャネル c_i と $\mathbf{c}_e$ $(c_i,\ \mathbf{c}_e \in \mathcal{C})$ の状態である．sc_i はチャネル c_i で形成されたグループの集合を意味する．sc_e は $\{\{CFSM_1, env\}, \cdots, \{CFSM_n, env\}\}$ であり，env は環境を表す． □

定義 4. システム状態グラフ G は次の 4 項組である．

$$G = \langle S, E, \delta, s_0 \rangle$$

ここで，S はシステム状態の集合，E はイベントの集合，δ $(\delta : S \times E \to S)$ はシステム状態の遷移関数，s_0 は初期システム状態である．E はチャネルの確立（グループの形成），オブジェクトの入出力（グループ内での入出力），チャネルの切断（グループの解消），チャネルの強制放棄（グループの解消），内部イベント，判断，処理から成る． □

記法 2. システム状態に対する記法・記号を以下のように定める．(1) $\#c\{a, b, \cdots\}$：$CFSM_a$，$CFSM_b$，$\cdots$ によるチャネル c の確立（グループの形成）；(2) $/c\{a, b, \cdots\}$：$CFSM_a$，$CFSM_b$，$\cdots$ によるチャネル c の切断（グループの解消）；(3) $//c\{a\}$：$CFSM_a$ によるチャネル c の強制放棄（グループの解消）；(4) $c\{a, b, \cdots\}(u_1, u_2, \cdots)$：$CFSM_a$，$CFSM_b$，$\cdots$ によるチャネル c でのオブジェクト u_1，u_2，$\cdots$ の入出力（グループ内の入出力）；(5) $\varepsilon\{k\}$：$CFSM_k$ の内部イベント；(6) $\diamondsuit\, d(u)$：結果が u であるような判断 d；(7) $\square\, p$：処理イベント p；(8) $s \xrightarrow{e} s'$：システム状態 s から s' へのイベント e による遷移；(9) $s \xrightarrow{e}$：$s \xrightarrow{e} s'$ なる s' が存在；(10) $s \not\xrightarrow{e}$：$s \xrightarrow{e}$ でない；(11) $s \to$：$s \xrightarrow{e}$ なる e が存在；(12) $s \not\to$：$s \to$ でない． □

メッセージやチャネル名の入力は，各有限状態機械において定義した対応する変数への入力値の代入によって表す．たとえば，!“Tom” が 1 つの出力であり，?$name$ が対応する入力であるとき，“Tom” が変数 $name$ に代入される．すべての変数名は有限状態機械中でつねにグローバルであると仮定する．有限状態機械 $CFSM_k$ における変数 u に値 v を代入することを $[u := v]CFSM_k$ で表す．

これまでの準備の下，モバイル並行システム仕様の動的意味としてのシステム状態グラフを次のように定義する．

定義 5. モバイル並行システム

$Sys = \langle (CFSM_1, \cdots, CFSM_k, \cdots, CFSM_n),\ (l_1,\ \cdots,\ l_k,\ \cdots,\ l_n),\ \mathcal{C} \rangle$

に対し，$\mathcal{F} = \{(c_i, COM(c_i)) \mid 1 \leq i \leq m,\ COM(c_i) \subseteq \mathcal{P}(L),\ c_i \in \mathcal{C}_f\}$ をその場とする．また，$IEC = \{(c_i,\ IG(c_i)) \mid 1 \leq i \leq m,\ IG(c_i) \subseteq \mathcal{P}(\{CFSM_1, \cdots, CFSM_n\}),\ c_i \in \mathcal{C}_f\}$ を暗黙確立チャネルとする．このとき，対応するシステム状態グラフ $G = \langle S, E, \delta, s_0 \rangle$ を以下の規則の適用により推論される最小のものとして定義する．

(1) 初期システム状態

$s_0 = \langle (q_{10}, \cdots, q_{k0}, \cdots, q_{n0}),\ (l_1, \cdots, l_k, \cdots, l_n),\ (sc_1, \cdots, sc_i, \cdots, sc_m, sc_e) \rangle \in S$

ここで，

各 i $(1 \leq i \leq m)$ について，$(c_i, IG(c_i)) \in IEC$ のとき $sc_i = IG(c_i)$，そうでないとき $sc_i = \phi$，

$sc_e = \{\{CFSM_1, env\}, \cdots, \{CFSM_n, env\}\}$.

(2) チャネル確立（グループの形成）☆

$s = \langle (\cdots, q_a, \cdots, q_z, \cdots),\ (\cdots, l_a, \cdots, l_z, \cdots),\ (\cdots, sc_i, \cdots) \rangle \in S$,

$q_a \xrightarrow{\#c_i[[\mathbf{x_a}]]} q'_a,\ \cdots,\ q_z \xrightarrow{\#c_i[[\mathbf{x_z}]]} q'_z$,

$\{l_a, \cdots, l_z, \cdots\} \in COM(c_i)$,

$(c_i, COM(c_i)) \in \mathcal{F}$,

$\{CFSM_a, \cdots, CFSM_z\} \notin sc_i$

ならば

$E_{c_i} = \{CFSM_a, \cdots, CFSM_z\}$ とおき，後述の「グループ決定アルゴリズム」を適用し EG_{c_i} を得る．

各 $g \in EG_{c_i}$ について：

$s' = \langle (\cdots, q''_a, \cdots, q''_t, \cdots, q''_z, \cdots),\ (\cdots, l_a, \cdots, l_z, \cdots),\ (\cdots, sc'_i, \cdots) \rangle \in S$,

ただし，$t \in g$ で $t \in \{a, \cdots, z\}$ のとき $q''_t = q'_t$，$t \notin g$ で $t \in \{a, \cdots, z\}$ のとき $q''_t = q_t$，

$sc'_i = sc_i \cup \{g\}$,

$s \xrightarrow{\#c_i g} s'$.

(3) オブジェクト入出力（グループ内の入出力）

(a) sc_i におけるオブジェクトの入出力☆☆

$s = \langle (\cdots, q_a, \cdots, q_z, \cdots),\ (\cdots, l_a, \cdots, l_z, \cdots),\ (\cdots, sc_i, \cdots) \rangle \in S$,

$q_a \xrightarrow{c_i \alpha_{a1} \cdots \alpha_{aj} \cdots \alpha_{ah}} q'_a,\ \cdots$,

$q_z \xrightarrow{c_i \alpha_{z1} \cdots \alpha_{zj} \cdots \alpha_{zh}} q'_z$,

$\{l_a, \cdots, l_z, \cdots\} \in COM(c_i)$,

$(c_i, COM(c_i)) \in \mathcal{F}$,

$\{CFSM_a, \cdots, CFSM_z\} \in sc_i$,

ただし，入出力イベント $\alpha_{aj}, \cdots, \alpha_{zj}$ $(1 \leq j \leq h)$ は次の2つの条件のいずれかを満たす．

(1) ある r $(r \in \{a, \cdots, z\})$ について $\alpha_{rj} = !m$ のとき，すべての t $(t \in \{a, \cdots, z\} - \{r\})$ について $\alpha_{tj} = ?x_t$.

(2) ある r $(r \in \{a, \cdots, z\})$ について $\alpha_{rj} = !!c$ のとき，すべての t $(t \in \{a, \cdots, z\} - \{r\})$ について $\alpha_{tj} = ??y_t$.

ならば

$s' = \langle (\cdots, q'_a, \cdots, q'_z, \cdots),\ (\cdots, l_a, \cdots, l_z, \cdots),\ (\cdots, sc_i, \cdots) \rangle \in S$,

入出力イベント $\alpha_{aj}, \cdots, \alpha_{zj}$ が上の条件のどちらを満たすかにより次のいずれかを行う．

(1) のとき，すべての t $(t \in \{a, \cdots, z\} - \{r\})$ について $[x_t := m]CFSM_t$.

(2) のとき，すべての t $(t \in \{a, \cdots, z\} - \{r\})$ について $[y_t := c]CFSM_t$.

$s \xrightarrow{c_i\{a, \cdots, z\}(\theta)} s'$.

$\theta = val_c(\alpha_{a1}, \cdots, \alpha_{z1}), \cdots, val_c(\alpha_{ah}, \cdots, \alpha_{zh})$

ここで，$val_c(\alpha, \beta, \cdots)$ は出力イベントの値（メッセージまたはチャネル名）を入出力イベント $\alpha, \beta, \cdots$ から取り出すことを表す．

(b) $\mathbf{c}_e$ におけるオブジェクトの入出力（割愛）

(4) チャネル切断（グループの解消）☆☆☆

$s = \langle (\cdots, q_a, \cdots, q_z, \cdots), (\cdots, l_a, \cdots, l_z, \cdots),\ (\cdots, sc_i, \cdots) \rangle \in S$,

$q_a \xrightarrow{/c_i} q'_a,\ \cdots,\ q_z \xrightarrow{/c_i} q'_z$,

$\{l_a, \cdots, l_z, \cdots\} \in COM(c_i)$,

$(c_i, COM(c_i)) \in \mathcal{F}$,

$\{CFSM_a, \cdots, CFSM_z\} \in sc_i$

ならば

☆ ここで，チャネル c_i でグループを形成しようとしている有限状態機械を $CFSM_a, \cdots, CFSM_z$ とする．またそれぞれが存在するロケーションを $l_a, \cdots, l_z$ とする．

☆☆ ここで，チャネル c_i でグループを形成している有限状態機械を $CFSM_a, \cdots, CFSM_z$ とする．またそれぞれが存在するロケーションを $l_a, \cdots, l_z$ とする．

☆☆☆ $CFSM_a, \cdots, CFSM_z$ そして $l_a, \cdots, l_z$ はオブジェクトの入出力の場合と同様．

$s' = \langle(\cdots, q'_a, \cdots, q'_z, \cdots), (\cdots, l_a, \cdots, l_z, \cdots), (\cdots, sc'_i, \cdots)\rangle \in S,$
$sc'_i = sc_i - \{\{CFSM_a, \cdots, CFSM_z\}\},$
$s \xrightarrow{/c_i\{a,\cdots,z\}} s'.$

(5) チャネル強制放棄（グループの解消）☆

$s = \langle(\cdots, q_a, \cdots, q_t, \cdots, q_z, \cdots), (\cdots, l_a, \cdots, l_z, \cdots), (\cdots, sc_i, \cdots)\rangle \in S,$
$q_t \xrightarrow{//c_i} q'_t \quad (t \in \{a, \cdots, z\}),$
$\{l_a, \cdots, l_z, \cdots\} \in COM(c_i),$
$(c_i, COM(c_i)) \in \mathcal{F},$
$\{CFSM_a, \cdots, CFSM_z\} \in sc_i$

ならば

$s' = \langle(\cdots, q_a, \cdots, q'_t, \cdots, q_z, \cdots), (\cdots, l_a, \cdots, l_z, \cdots), (\cdots, sc'_i, \cdots)\rangle \in S,$
$sc'_i = sc_i - \{\{CFSM_a, \cdots, CFSM_z\}\},$
$s \xrightarrow{\varepsilon\{t\}} s'.$

(6) ロケーション移動☆☆

(a) $COM(c_i)$ 内の移動（チャネルの範囲内の移動）

$s = \langle(\cdots, q_k, \cdots), (\cdots, l_k, \cdots), (\cdots, sc_i, \cdots)\rangle \in S,$
$q_k \xrightarrow{\hookrightarrow l'_k} q'_k$

ならば

$s' = \langle(\cdots, q'_k, \cdots), (\cdots, l'_k, \cdots), (\cdots, sc_i, \cdots)\rangle \in S,$
$s \xrightarrow{\varepsilon\{k\}} s'.$

(b) $COM(c_i)$ 外への移動（チャネルの範囲外への移動）

$s = \langle(\cdots, q_k, \cdots), (\cdots, l_k, \cdots), (\cdots, sc_i, \cdots)\rangle \in S,$
$q_k \xrightarrow{\hookrightarrow l'_k} q'_k$

ならば

$s' = \langle(\cdots, q'_k, \cdots), (\cdots, l'_k, \cdots), (\cdots, sc'_i, \cdots)\rangle \in S,$
$sc'_i = sc_i - \{\{CFSM_a, \cdots, CFSM_z\}\},$
$s \xrightarrow{\varepsilon\{k\}} s'.$

(7) 内部イベント

$s = \langle(\cdots, q_k, \cdots), (\cdots), (\cdots)\rangle \in S,$
$q_k \xrightarrow{\varepsilon} q'_k$

ならば

$s' = \langle(\cdots, q'_k, \cdots), (\cdots), (\cdots)\rangle \in S,$
$s \xrightarrow{\varepsilon\{k\}} s'.$

(8) 判断イベント

$s = \langle(\cdots, q_k, \cdots), (\cdots), (\cdots)\rangle \in S,$
$u \in \mathcal{I}(d),$
$q_k \xrightarrow{\diamond d(u)} q'_k$

ならば

$s' = \langle(\cdots, q'_k, \cdots), (\cdots), (\cdots)\rangle \in S,$
$s \xrightarrow{\varepsilon\{k\}} s'.$

(9) 処理イベント

$s = \langle(\cdots, q_k, \cdots), (\cdots), (\cdots)\rangle \in S,$
$q_k \xrightarrow{\Box p} q'_k$

ならば

$s' = \langle(\cdots, q'_k, \cdots), (\cdots), (\cdots)\rangle \in S,$
$s \xrightarrow{\varepsilon\{k\}} s'.$

□

チャネル確立拒否を考慮したグループの決定アルゴリズムを示す．

アルゴリズム 1. 「グループ決定アルゴリズム」
確立しようとしているチャネルを c_i，チャネル c_i で確立を試みようとしている有限状態機械の集合を E_{c_i} とする．

(1) $EG_{c_i} := E_{c_i}$.
(2) $E_{c_i} \neq \emptyset$ ならば E_{c_i} 中の勝手な有限状態機械を選択し，それを $CFSM_r$ とし次のステップに進む．そうでなければステップ 5 へ進む．
(3) $CFSM_r$ と $R_c(r)$ 中の有限状態機械が同じ集合に属さないよう EG_{c_i} 中の各要素を分解し，EG_{c_i} の要素を再構成する．再構成された要素間に部分集合の関係があれば小さな方を除去し，部分集合の関係がいっさいないようにする．また，単独の有限状態機械だけから成る要素もないようにする．
(4) $E_{c_i} := E_{c_i} - \{CFSM_r\}$．ステップ 2 へ戻る．
(5) 終了し，EG_{c_i} 中の各要素をチャネル c_i で確立可能な有限状態機械のグループとする． □

ステップ 3 において $R_c(r) = \emptyset$ の場合は何も行われない．また，ステップ 3 中の制限はチャネル c_i が確立されうるグループをできるだけ大きくとることと，単独の有限状態機械だけではグループができえないことからきている．

グループがいかに決定されるかの例を示す．

例 2. システムの挙動のある時点で，E_c={*CFSM1*, *CFSM2*, *CFSM3*, *CFSM4*} で，$CFSM1$ が $\#c[[\mathbf{3}, \mathbf{4}]]$，$CFSM2$ が $\#c[[\mathbf{3}, \mathbf{4}]]$，$CFSM3$ が $\#c[[\mathbf{1}]]$，

☆ $CFSM_a, \cdots, CFSM_z$ そして，$l_a, \cdots, l_z$ はオブジェクトの入出力の場合と同様．
☆☆ $CFSM_a, \cdots, CFSM_z$ そして，$l_a, \cdots, l_z$ はオブジェクトの入出力の場合と同様．

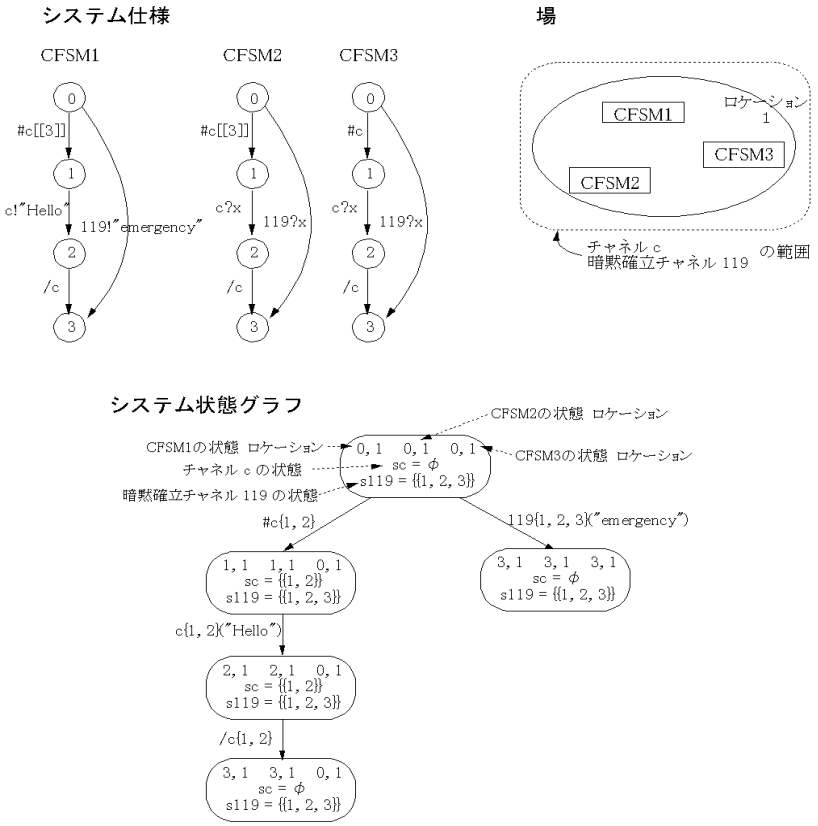


図 2 システム仕様，場，挙動の例
Fig. 2 An example of a system specification, field and behavior.

$CFSM4$ が $\#c$ であったとする．このとき「グループ決定アルゴリズム」の (1) により，まず EG_c={{*CFSM1*, *CFSM2*, *CFSM3*, *CFSM4*}} となる．(2) で $r = 1$ とすると，$R_c(r)$={*CFSM3*, *CFSM4*}であり，(3)で EG_c={{*CFSM1*, *CFSM2*}, {*CFSM3*, *CFSM4*}} と構成される．(4) では，E_c={*CFSM2*, *CFSM3*, *CFSM4*} となる．このことをたとえば $r = 2$, 3, 4 の順で繰り返していくと，EG_c={{*CFSM1*, *CFSM2*}, {*CFSM3*, *CFSM4*}} と変わらず，また，(4) により最後に $E_c = \emptyset$ となる．よって (2) の条件によりアルゴリズムは終了し，EG_c の要素である {*CFSM1*, *CFSM2*} と {*CFSM3*, *CFSM4*} の 2 つのグループがチャネル c の確立とともに形成されることになる． □

本論文で提案したシステムのモデル化と形式化のもと，システム仕様がどのように表現されるかを以下の簡単な例で示す．場の設定とともに，仕様化されたシステムの挙動は，上で定義したシステム状態グラフの生成規則の適用により系統的に導出できる．なおここでは，1 つの場の例だけを与えるが，場の設定に変化を持たせることによって，種々の局面でのシステム挙動を導出し観察することが可能になる．これは，本仕様化手法の大きな特徴といえる．

例 3. 図 2 左上は，システムが 3 つの有限状態機械から成ると仮定し，各々の仕様を状態遷移図表現で示している．同図右上は設定した場と有限状態機械の初期ロケーションを示している．同図の場 $\mathcal{F}$，ロケーション集合 L，チャネル集合 $\mathcal{C}_f$，暗黙確立チャネル定義 IEC は形式的には，次のように与えられる．

$$\mathcal{F} = \{(c, \{\{1\}\}),\ (119, \{\{1\}\})\}$$
$$L = \{1\}$$
$$\mathcal{C}_f = \{c, 119\}$$
$$IEC = \{(119, \{\{CFSM1, CFSM2, CFSM3\}\})\}$$

これらシステム全体の仕様から，上記定義により生成されたシステム状態グラフを同図下に示す☆．初期システム状態では，$CFSM1$，$CFSM2$，$CFSM3$ の間にチャネル 119 が暗黙に確立されている．一方，チャ

☆ システム状態中，環境チャネルの状態は省略している．

ネル c は明示的に確立されなければならない．この場合，$CFSM1$ と $CFSM2$ は $CFSM3$ との確立を拒否しているため，$CFSM3$ を除外した $CFSM1$ と $CFSM2$ から成るグループが形成される．そして，有限状態機械間相互の通信は確立されているチャネルを経由してグループ内で行われる．この例ではそれぞれのチャネルに関して，1 回の相互作用を行っている．その後，チャネル c に関しては明示的に切断が行われている． □

3. 適　　用

本章では，提案した仕様化手法を PHS システムとエージェント指向コンピューティングの一応用である分散センシングシステムの記述に適用する．

3.1 PHS システム

3.1.1 概要と準備

PHS システム[13]は固定網のインテリジェントネットワークとマイクロセルゾーン方式に基づく無線アクセス系を組み合わせた簡易型の通信システムである．PHS サービスエリア中をコードレス電話機 PS（Personal Station）が自由に移動し，その周囲には基地局 CS（Cell Station）が設置される．基地局の上位には PHS 接続装置（PHSCU: PHS Control Unit）が存在し，そこから加入者系交換機へ接続が行われる．加入者系交換機から上部は既存の一般電話の交換網が用いられる．PS の位置コード，認証情報，課金情報を記録しているデータベース（DB）は交換機とは別のノードで扱われる．このデータベースノードから得られる情報に基づいて移動する PS への着信接続が制御される．**図 3** はサービスエリアの内容である．ここで 1 つの CS でカバーできる通話可能エリアをセルという．DB に記憶されている位置コードは，PHSCU ごとに割り当てられており，通話相手の呼び出しは，1 つの PHSCU に接続されているすべての CS で行われる（一斉呼び出し）．

本仕様化手法は，システム構造の動的変化を効果的に記述できることを設計の主眼点としているため，動的な変化がある PS と CS の相互関係を中心に仕様化する．既存の固定電話回線網の部分は省略し環境と考える．仕様化対象のエンティティは動的な変化がある PS と CS，そして PS のハンドオーバ時にインタフェースの切替えを行う PHSCU とする．実際の PHS サービスエリアはセルの集まりで構成されているため，仕様化では一部のセルを取り出して行うことで実際のネットワークへの適用可能性を見る．仕様化の前に，各エンティティの動作と役割について概観する．

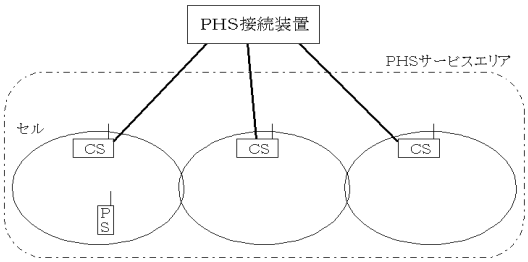


図 3 サービスエリア
Fig. 3 Service area.

- PS：PS はサービスエリア中を自由に移動しながらつねに CS と交信をしており，CS を介して他の PS と通話することができる．本仕様化では簡単化のため，サービスエリア中に存在する PS は 2 つとする．PS の動作は次のとおりである．
  - 通話：CS が存在するロケーションでの他の PS との通話要求や，CS が存在しないセルでの他の PS との通話要求．
  - 通話中の移動：PS が通話をしている際の通話が可能なセルへの移動や，通話が不可能なセルへの移動．
- CS：CS は制御チャネルを用いてつねに PS と交信をしており，PS の移動や通話時に PHSCU へ制御信号を発信する．CS は固定回線で PHSCU と接続される．仕様化では，制御用にあらかじめ PS-CS 間と CS-PHSCU 間に暗黙確立チャネルがあるとする．
- PHSCU：PHSCU は複数の CS を統括しており，一斉呼び出しエリアを形成している．また，ハンドオーバ時に CS のインタフェースの切替えを行う．ここでは PHSCU あたり 2 つの CS を配置する．

3.1.2 仕　様　化

仕様化する PHS システムの場を**図 4** のように設定する．$\mathbf{c}_e$ は環境とのオブジェクト入出力に用いるチャネルであり，PHSCU がこのチャネルを用いて環境となっている既存電話回線網と情報を入出力する．チャネル C は PHSCU と CS が保持している暗黙確立チャネルであり，PHSCU-CS 間の通信に使われる．なお，物理的には C は CS ごとに分離したチャネルであると考えられるが，ここでは簡単化のためそれらをまとめて C としている．チャネル Ccは CS と PS が保持しており，CS–PS 間で扱われる制御信号の送受信に使われる．これも暗黙確立チャネルと考える．チャネル Cvは CS が保持しており，PS の通話時に CS との間に動的に割り当てられる通話チャネルを総称する．PS の通話要求時に CS から隣接の CS で使われていない通話チャネルが PS に渡される．同図はエンティティ

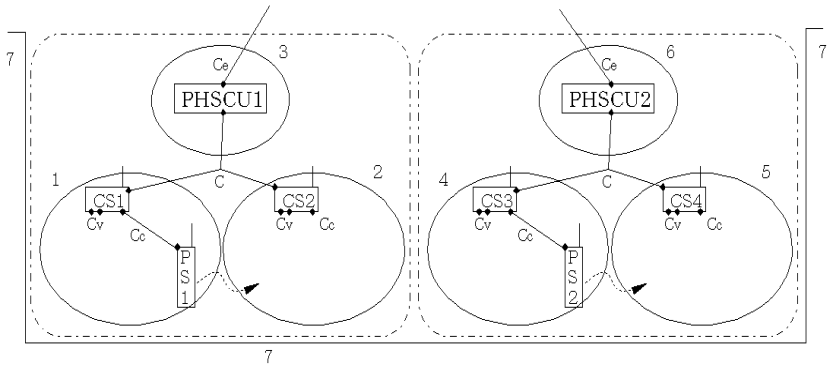


図 4 PHS システムの場
Fig. 4 Field of PHS system.

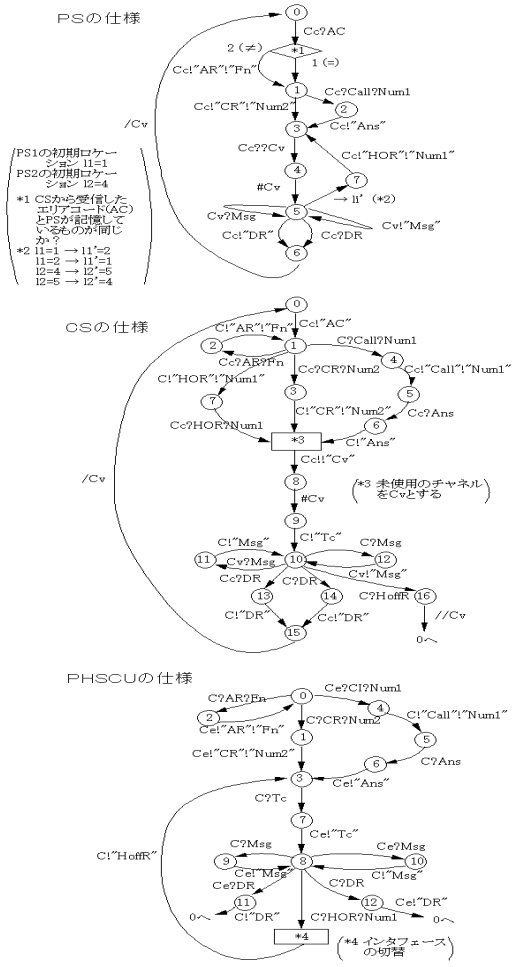


図 5 PHS システムの仕様
Fig. 5 Specification of PHS system.

の配置も示しており，PS はロケーション 1，2，4，5 にいる場合，CS と制御チャネルを確立し，通話要求などを CS に向け送信することができる．ロケーション 7 は CS が存在していない PHS サービスエリアの範囲外を示している．

表 1 入出力オブジェクト一覧
Table 1 List of input/output objects.

記号	内容
AR	位置登録要求
AC	エリアコード
Fn	自 PS の機体番号
CR	通話要求
Num1	自 PS の番号
Num2	相手先 PS の番号
Call	呼び出し
CI	呼び出し要求
Ans	応答信号
Tc	通話開始信号
Msg	通話内容
HOR	ハンドオーバ要求
HoffR	ハンドオフ要求
DR	切断要求

PHS システム全体の仕様を**図 5** に示す．図 4 に示すとおり，PS，CS，PHSCU はそれぞれ複数存在するが，それらは同じ仕様となっているため，まとめて 1 つにしてある．いずれも初期状態は 0 である．CS と PHSCU はともに複数の呼を同時に扱うが，ここではその中の 1 つの呼に代表して仕様化を行っている．**表 1** はエンティティ間で入出力されるオブジェクトの一覧である．紙面の都合上，エンティティ個々の仕様の詳細は省略し，システム全体の流れを中心に説明する．

PS の電源が投入されると CS のエリアコード *AC* を受信する．そこで PS は記憶しているエリアコードとの相違が認められた場合，チャネル *Cc* を用いて位置登録コード *AR* と PS の機体番号 *Fn* を CS へ送信する（以上，PS の状態 0 から 1 への遷移）．CS は受信した *AR* と *Fn* を固定回線 *C* を用いて PHSCU へ送信し（CS の状態 2 から 1 への遷移），PHSCU が環境（既

存電話回線網）へ PS の位置登録を行う（PHSCU の状態 2 から 0 への遷移）．PS が通話をする場合，CS，PHSCU を介して環境へ通話要求 *CR*と相手先 PS の番号 *Num2*を送信する（PS の状態 1 から 3 への遷移）．この際，CS は隣接の CS で用いられていない通話チャネルを選択し，*Cc*を用いて PS へ渡す（CS の*3 から状態 8 への遷移）．相手先の PS が存在している PHSCU では環境から呼び出し要求 *CI*とその PS の番号 *Num1*を受信する（PHSCU の状態 0 から 4 への遷移）．これにより PHSCU が統括しているすべての CS に対して呼び出し *Call*を行う（PHSCU の状態 4 から 5 への遷移）．CS を介して呼び出しを受けた PS は応答信号 *Ans*を CS，PHSCU を介して環境に返す（PS の状態 2 から 3 への遷移）．そして CS から通話チャネルを受け取る（PS の状態 3 から 4 への遷移）．発信元と発信先の PS はそれぞれ最寄りの CS と通話チャネルを確立する（PS の状態 4 から 5 への遷移）．ここで通話チャネル確立を行った CS は PHSCU を通して環境へ通話開始信号 *Tc*を送信し，通話の開始を知らせる（CS の状態 9 から 10 への遷移）．PS どうしが通話中やりとりする通話内容 *Msg*は CS，PHSCU，環境を通して通話相手の PS へ送信される（各有限状態機械の *Msg*による遷移）．そして通話が終了する際には PS が切断要求 *DR*を CS，PHSCU を通して環境へ送信し，通話相手の PS もその DR を受信し通話チャネルを切断する（PS の状態 5 から 6，6 から 0 への遷移）．PS が他のロケーションに移動する場合はチャネル *Cc*を用いて移動先のロケーションに存在する CS へハンドオーバ要求 *HOR*とその PS の番号 *Num1*を送信する（PS の状態 5 から 7，7 から 3 への遷移）．ロケーション先の CS はこれらを PHSCU へ渡し，PHSCU はインタフェースの切替えを行う（PHSCU の*4）．そして，元のロケーションに存在する CS に対し，ハンドオフ要求 *HoffR*を送信し（PHSCU の*4 から状態 3 への遷移），それを受け取った CS は今まで使用していた通話チャネルを強制放棄する（CS の状態 16 から 0 への遷移）．PS は移動先のロケーションに存在する CS から新しい通話チャネルを受信し，通話を継続する（PS の状態 3 から 4 への遷移）．

以上の仕様例をもとにして，本仕様化手法について以下評価する．

まず仕様の概観に関し，図 5 から分かるように，本手法は状態遷移の観点から内容を記述するため，理解性の点で優れていることが分かる．これは，プロセス代数モデルなどの式を通した仕様化手法と比べ対照的である．

処理や判断など一部，非形式的な表現を扱っているが，対象としての各エンティティの仕様記述，場を通したそれらの間の関係，通信の局所性などが必要な範囲内でうまく表現されており，適用性は満足していると思われる．

エンティティ間の固定的な接続関係と動的な接続関係が暗黙確立チャネルと通常のチャネルを使い分けることで表現できている．

モバイル系の特徴であるエンティティの移動性が明示的に表現できている（PS の仕様中の状態 5 から状態 7 への遷移参照）．

チャネル名の受渡し機能により，通常時およびハンドオーバ時の通話チャネルの動的な割当てが明確に仕様化可能となっている（PS の仕様中の状態 3 から状態 4 への遷移，および，CS の仕様中の処理*3 から状態 8 への遷移参照）．これは本適用に限らず，構成要素間の（論理的/物理的）接続関係の動的変化をともなうような並行システムの仕様化に貢献する．

3.2 分散センシングシステム

エージェント指向コンピューティングの一例として，契約ネットプロトコル（契約ネット）を応用した分散センシングシステムがある[14),15)]．仕様およびその説明については文献 16) に譲るが，PHS システムの仕様化の場合と同様，本手法の適用性を確認することができた．

4. むすび

本論文では，モバイル並行システムのモデル化と形式的仕様化のための手法を提案した．本手法では，理解性や実装への移行性に優れた有限状態機械の導入および通信の局所性を有効に表現する手段としての場の導入に加えて，種々のバリエーションに対応できる通信路の設定，構成要素の移動性などの表現・記述能力の導入を行った．また，本手法に基づいて PHS システムと分散センシングシステムを仕様化し，適用性の評価を行った．

なお，グループ形成中にその構成要素が移動すると，グループを解消するような意味論を与えており，形成中の頻繁な移動の性質を有するシステムの記述への適合性は高くないといえる．しかしながら，電子会議，（主に 1 対 1 的な）チャット風アプリケーション，適用例にもあったようなエージェントアプリケーションなどでは，いったんグループが構成されると，セッションの終了までは構成要素の出入り（移動）がそれほどあるものではないと思われる．よって，本方式のグループ通信は万能ではないにせよ，適度な範囲の適用性を

満足していると考える．また，移動はむしろグループ形成中ではないときに頻度が高いと想定され，その場合の移動による制約は何もない．

以上により，仕様の動作シミュレーションツールや検証の方法論をこの手法と組み合わせて用いることによって，システム設計の効率化・信頼化が期待できるようになる．このため，本手法を基本としたシミュレータなどの設計支援ツールの開発が課題の１つとして考えられる．

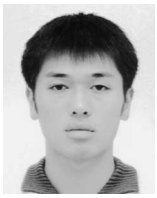
一方，仕様中の処理や判断の記述の形式化を行っていないため，その部分の機械的な解釈ができないなどの難点は残している．これをこのままにするか，抽象データ型記述のような方法で形式化するかは，記述内容の理解性の観点からなお検討の余地がある．また，本論文での適用では，仕様化の際に対象のエンティティ数を固定して扱ったが，実際領域では数は個数不定が自然であり，今後その記述法を考察し導入することが望ましいと考えられる．

謝辞 本研究の遂行に多大なご協力をいただいた佐藤俊之氏，小野悟氏，四釜健志氏，加納稔久氏に感謝の意を表します．

参 考 文 献

1) Akyildiz, J.F., Mcnair, J., Ho, J.S.M., Uzunalioglu, H. and Wang, W.: Mobility Management in Next-Generation Wireless Systems, *Proc. IEEE*, Vol.87, No.8, pp.1347–1384 (1999).
2) Milner, R., Parrow, J. and Walker, D.: A Calculus of Mobile Procceses, Part I and Part II, *Journal of Information and Computation*, Vol.100, pp.1–77 (1992).
3) Ando, T., Takahashi, K., Kato, Y. and Shiratori, N.: Maintenance of Mobile System Ambients using a Process Calculus, *Computer Networks*, Vol.32, No.2, pp.229–256 (2000).
4) Sangiorgi, D.: Locality and Non-interleaving Semantics in Calculi for Mobile Processes, Technical Report ECS-LFCS-94-282, Laboratory for Foundations of Computer Science, Department of Computer Science, University of Edinburgh (1994).
5) Amadio, R.M.: An Asynchronous Model of Locality, Failure, and Process Mobility, *INRIA Research Report 3109* (1997).
6) Milner, R.: *Communication and Concurrency*, Prentice-Hall (1989).
7) Hoare, C.A.R.: *Communicating Sequential Processes*, Prentice-Hall (1985).
8) Battiston, E., Cindio, F.D. and Mauli, G.: Modular Algebraic Nets to Specify Concurrent Systems, *IEEE Trans. Softw. Eng.*, Vol.22, No.10, pp.689–705 (1996).
9) Shaw, A.C.: Communicating Real-Time State Machines, *IEEE Trans. Softw. Eng.*, Vol.18, No.9, pp.805–816 (1992).
10) Harel, D., Lachover, H., Naamad, A., Pnueli, A., Politi, M., Sherman, R., Trauring, A.S. and Trakhtenbrot, M.: Statemate: a Working Environment for the Development of Complex Reactive System, *IEEE Trans. Softw. Eng.*, Vol.16, No.4, pp.403–414 (1990).
11) Takahashi, K., Ando, T., Kano, T., Itabashi, G. and Kato, Y.: Specification and Validation of a Dynamically Reconfigurable System, *IEICE Trans. Fundamentals*, Vol.E81-A, No.4, pp.536–565 (1998).
12) Takahashi, K., Itabashi, G. and Kato, Y.: Specification of a Mobile System based on Finite State Model, *Proc. 1st International Conference on Parallel and Distributed Computing, Applications and Technologies*, pp.209–214 (2000).
13) NTT DoCoMo, 別冊技術情報 alles (1999).
14) 木下哲夫，菅原研次：エージェント指向コンピューティング，ソフト・リサーチ・センター (1995).
15) Smith, R.: The Contract Net Protocol: High-Level Communication and Control in a Distributed Problem Solver, *IEEE Trans. Computers*, Vol.29, No.12, pp.1104–1113 (1980).
16) 佐藤俊之：有限状態モデルに基づいたモバイルシステムの仕様化手法とその適用，仙台電波工業高等専門学校平成 12 年度卒業研究論文 (2001).
17) 金指文明，富樫　敦：M-π 計算：モジュール記述を持つ計算体系，情報処理学会マルチメディア・分散・協調とモバイル（DICOMO99）シンポジウム，1-B-8 (1999).
18) 金指文明，塚崎，富樫　敦：Field Walker：プロセス計算に基づく分散プログラミングシステム，ソフトウェア工学の基礎 VI（日本ソフトウェア科学会 FOSE'99），pp.28–35, 近代科学社 (1999).
19) Sato, I.: A Hierarchical Model of Mobile Agents and Its Multimedia Applications, *Proc. IEEE 7th ICPADS Workshops*, pp.103–108 (2000).

(平成 13 年 5 月 10 日受付)
(平成 13 年 10 月 16 日採録)



板橋 吾一

1998 年仙台電波工業高等専門学校情報通信工学科卒業．2000 年同専攻科情報システム工学専攻修了．2000 年株式会社サイエンティア入社．分散並行システムの仕様記述と検証，エージェント指向コンピューティングの応用に関する研究に従事．1999 年電子情報通信学会東北支部学生賞奨励賞受賞．2000 年テレコムシステム技術学生賞受賞．電子情報通信学会会員．

高橋 薫（正会員）

1974 年から 1993 年東北大学電気通信研究所勤務．1993 年から 1995 年（株）高度通信システム研究所客員研究員．現在，仙台電波工業高等専門学校情報通信工学科教授．博士（工学）．分散並行システムの仕様記述と検証，エージェント指向コンピューティングに関する研究開発，地理情報システムの研究開発等に従事．著書「コンピュータネットワーク入門」（共著），「ソフトウェア工学の基礎知識」（共著）等．情報処理学会 25 周年記念論文賞，1991 年テレコムシステム技術賞，1997 年電子情報通信学会情報ネットワーク研究賞各受賞．電子情報通信学会会員．

加藤 靖（正会員）

1978 年東北大学大学院博士課程修了．現在，仙台電波工業高等専門学校情報工学科教授．情報システム工学専攻主任．工学博士．1995 年から 1996 年 Twente 大学研究員．分散システムの設計と検証，形式記述技法，時制論理，セルオートマトン，iTRON 等に関する研究に従事．著書「情報数学」，「マイクロコンピュータ・周辺技術」「レジスタと演算回路」（共著）等．福島，宮城，岩手県技術アドバイザ，花巻市企業化支援センター技術情報交流研究会会長．電子情報通信学会，JSEE 各会員．

加藤 貴司

2001 年東北大学大学院情報科学研究科博士後期課程修了．現在，東北大学電気通信研究所助手．博士（情報科学）．マルチエージェントシステムにおけるエージェントの協調に関する研究に従事．人工知能学会，電子情報通信学会各会員．

ベッド B. ビスタ（正会員）

1991 年 York 大学電子工学科卒業．1997 年東北大学大学院情報科学研究科博士課程修了．1997 年から 1998 年宮城大学勤務．現在，岩手県立大学ソフトウェア情報学部講師．博士（工学）．プロトコルの仕様記述と合成，形式記述技法に関する研究に従事．IEEE 会員．