6J－4

通信ソフトウェア設計支援環境：ITECS (3)
－仕様検証支援－

山野 敬一郎† Dusan Jokanovic† 太田 正孝† 高橋 薫††
†(株)高度通信システム研究所 ††東北大学

1. はじめに

現在我々は，通信ソフトウェアの設計を高信頼に支援するための環境としてITECS[4]を提案している．本報告では，このITECSにおける仕様検証支援について述べる．本支援環境で用いられている手法は，まず各種の記述技法によって記述された通信ソフトウェアの仕様を，形式的仕様記述言語の一つであるLOTOS (ISO8807) に統合し，LOTOSによる仕様の正当性の確認･検証を行う．次に，通信ソフトウェアの開発における詳細化過程の各段階において，下位レベルの仕様が上位レベルの要求仕様を正しく実現しているかどうかの検証を行うことによって，通信ソフトウェアの仕様設計支援を行うものである．さらに本報告では，ITECSの仕様検証環境を用いた，通信サービス仕様の検証の実行例を示す．

2. 仕様の詳細化過程と検証

我々は，通信ソフトウェア等の大規模システムの仕様の開発過程を，図1に示すような仕様の段階的な詳細化過程として位置づけている．つまり，ある要求仕様をもとに，それを段階的に詳細化していくことによって詳細設計仕様が得られ，最終的に実際のソフトウェアを開発するという過程である．この過程を高信頼に支援するためには，以下のような3段階の検証による開発支援が必要であると考えられる．

(1) 記述された仕様のチェック
各詳細化の段階において，記述された仕様がシンタクスおよびセマンティクス上，正しく記述されているかどうかの検証．これは，主に仕様記述支援の段階に含まれる検証機能である．

(2) 記述された仕様の正当性の確認
仕様が設計者の意図を正しく反映しているかどうかの検証．シミュレーション等を行うことによる，動作の確認という面での検証である．

(3) 仕様の詳細化過程における仕様間の検証
詳細化された下位レベルの仕様が上位レベルの要求仕様を正しく実現しているかどうかの検証である．

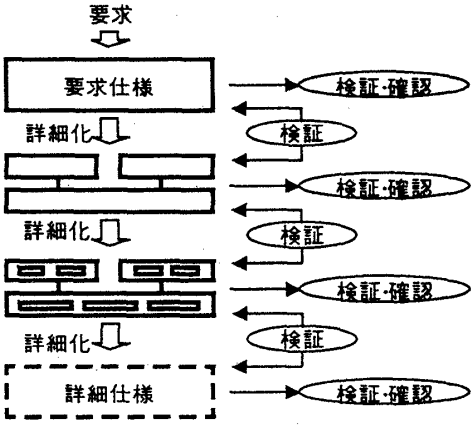

図1 仕様の詳細化過程と検証

3. ITECSにおける仕様検証支援環境

ITECSでは，前節の仕様検証支援の考え方を実現するために，図2に示すような仕様検証支援環境を構成する．

ここでは，前節の各検証項目に対応して，次の3段階の検証を行う．

① LOTOS仕様チェック
② 仕様動作確認
③ 仕様間検証

以下，各検証項目について詳細を述べる．

① LOTOS仕様チェック
ITECSの仕様作成支援環境では，LOTOS，SDL，MSC等の仕様記述法によって記述された仕様をLOTOSに統合する．このとき，統合されたLOTOS仕様のシンタクスチェック，および静的なセマンティクスチェックを行う．さらに，SDLやMSCとLOTOSとの，相互変換の正当性の検証も行う．

② 仕様確認
①で確認したLOTOS仕様を意味解釈し，LOTOS

A Support Environment for Communication Software Design : ITECS (3)
— Specification Verification —
Keiichirou YAMANO†, Dusan JOKANOVIC†, Masataka OHTA†, Kaoru TAKAHASHI††
† Advanced Intelligent Communication System Laboratories　†† Tohoku University

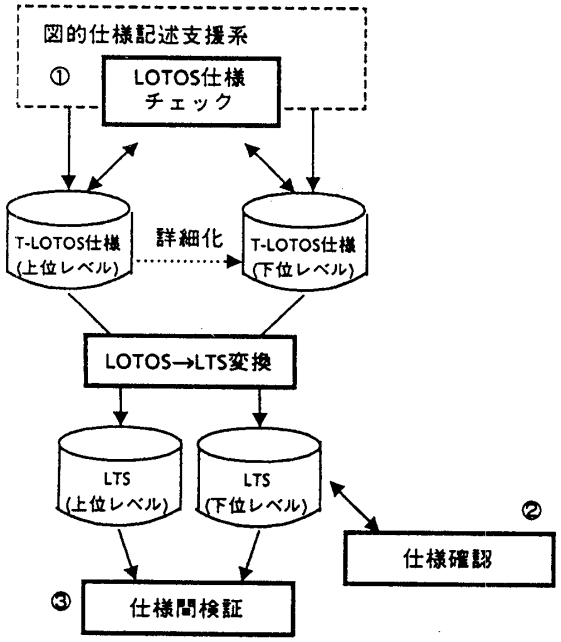

図2 仕様検証支援環境

の意味モデルであるLTS (Labelled Transition System : ラベル付き遷移システム)を生成する．これによって，到達可能性，デッドロック，無限ループ等の検出や，仕様のシミュレーションによる動作確認を含む仕様検証を行う．

③ 仕様間検証

本支援環境では，仕様の詳細化の過程における仕様間の検証を行うため，Simulation関係による検証と部分検証の考え方を適用する．

一般的に，二つのLOTOS仕様間の検証を行う場合には，弱bisimulation等による等価性の概念がよく知られている．しかし，仕様の詳細化過程では，下位レベルの仕様に，上位レベルの仕様にない付加的な情報，例えば例外処理を加える場合がある．あるいは，複数の上位レベルの仕様を組み合せて下位レベルの仕様を構成する場合がある．これらの場合には一般的な等価性の概念を適用することができない．本検証系では，ここに文献[1][2]に示されているSimulation関係の概念を適用することによって，上記のような関係の検証を行っている．また，検証のための判定アルゴリズムについては，文献[3]の方法を用いている．

次に，ITECSの対象となる通信ソフトウェアの詳細化したレベルの仕様は，一般的に非常に大規模で，仕様全体に対して検証を行うことは，効率的ではない．そこで我々は，部分検証の手法によって，大規模なシステムの仕様検証を行う．つまり，詳細化の過程において上位レベルの仕様を構造化分割し，分割された各部分に関して，それを詳細化した下位レベルの仕様とそれぞれ検証を行う．最終的に，それらの下位レベルの仕様を組み合わせた仕様全体が，正しく詳細化されていることを確認する．これは，前述のSimulation関係の考え方を部分的な検証対象に適用することによって検証可能であると考えられる．

これら2つの検証方法によって，大規模なシステムの開発に対応した検証が可能となる．

4. システム実行例

ここでは，簡単な電話交換サービスの仕様を，ITECSの仕様検証支援系を用いて検証した例を示す．現在は，LOTOS仕様をLTSに解釈することによる仕様確認と，2つの仕様間のSimulation関係による検証システムが実行可能である．

LOTOS仕様をLTSに意味解釈し，それをグラフ表示したものを図3の右側に，上位レベルと下位レベルの2つの仕様間の検証を行った例を図3の左側に示す．

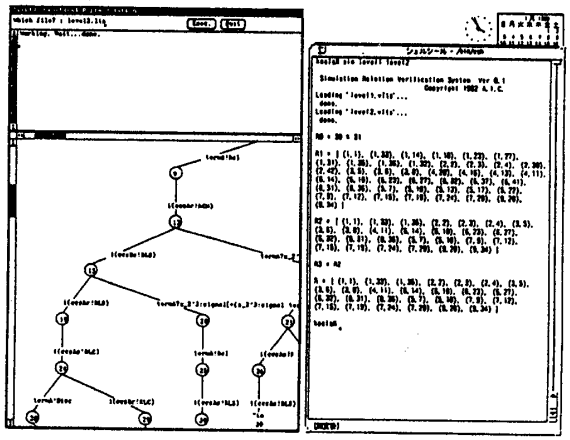

図3 システム実行例

5. おわりに

本報告では，通信ソフトウェア設計支援環境ITECSの仕様検証支援について述べた．具体的には，LOTOS仕様に統合された仕様を検証･確認し，さらに仕様の詳細化過程における仕様間の検証を行うことによって，高信頼な通信ソフトウェア仕様の開発支援が行えることを示した．そして，ITECSによる仕様検証の実行例を示した．

今後の課題としては，各支援ツールの統合，ユーザインタフェースの向上を含むITECSの検証支援環境の完成と，それを用いた実際の通信システムの仕様記述への適用が考えられる．

参考文献

[1] R.Milner : "Communication and Concurrency," Prentice Hall (1989).

[2] K.Yamano, D.Jokanovic, T.Ando, M.Ohta and K.Takahashi : "Formal specification and verification of ISDN services in LOTOS," IEICE Transactions on Communications, E75-B, No.8 (1992).

[3] 高橋薫, 山野敬一郎, 太田正孝 : "プロセス仕様の検証のための模倣性判定法," 電子通信学会論文誌 Vol.J76-D-I, No.1 (1993).

[4] 太田他: "通信ソフトウェア設計支援環境 : ITECS (1) -全体構成-," 情報処理学会第46回全国大会, 6J-2 (1993).