5H－3

通信ソフトウェア設計支援環境: ITECS(4) *
－ 仕様検証支援系 (Verifier, Vega) －

山野 敬一郎　高橋 薫　土岐田 義明 †
(株) 高度通信システム研究所 ‡

1　はじめに

近年の通信システムの大規模化・複雑化・高度化に伴い、その設計段階において仕様を誤りなく厳密に記述することが重要視されている。このため、種々の形式記述技法(FDT)が提案され、あわせてその記述のための支援環境が開発されている。

現在我々は、通信ソフトウェアの設計を高信頼かつ効率的に支援するための環境として、FDTの一つであるLOTOS (ISO8807)を中心とした支援環境ITECS (InTegrated Environment for high reliability Communication Software design and development)を提案し、開発を行っている。本報告では、特に仕様の検証に注目し、ITECSにおける仕様検証支援環境に関する紹介を行う。

2　仕様設計支援環境：ITECS

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、次の二種類の検証が必要であると考えられる。(1)仕様の詳細化過程における仕様間の検証、つまり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と、(2)各詳細化段階における仕様の正当性の検証、つまり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である。

以上の開発過程に基づき、通信ソフトウェアの設計支援環境ITECSは、図2に示すような構成となっている。まず仕様記述支援系を用いて、GLOTOS, MSC等の仕様記述技法による要求仕様を与え、これらの要求仕様をLOTOSに統合する。LOTOSによって記述された仕様はAnalyzerによってLOTOSの意味表現である遷移システムの形式に変換され、仕様検証支援系によって検証を行う。検証結果が正しければ、仕様記述支援系を用いて仕様の詳細化を行う。以上の過程を繰り返し段階的な詳細化を行うことによって、最終的にLOTOSによる詳細化仕様を生成する。この仕様をもとに、実際のソフトウェアを開発し、あるいは試験仕様生成支援ツールTESGENにより、TTCNによる試験仕様を生成することができる。

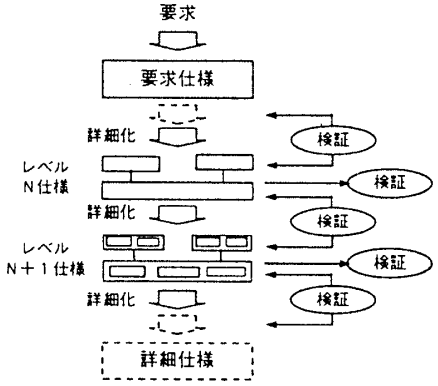

図 1: 仕様の詳細化過程

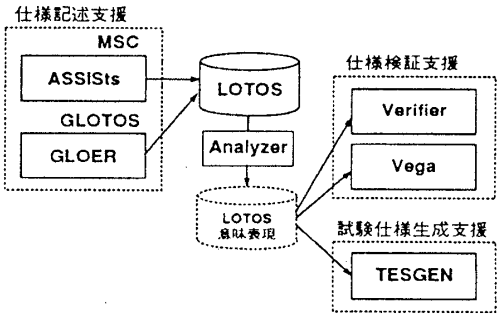

図 2: ITECS システム構成

3　ITECSにおける検証支援

ITECSでは、VerifierとVegaの二種類の検証支援ツールにより、前述の仕様検証手法を実現している。以下、それぞれのツールに関する説明を行う。

3.1　Verifier

Verifierは、図1に示すような仕様の詳細化過程における仕様間の検証を行うツールである。具体的には、詳細化の各段階において以下のような仕様検証手法を適用する。まず、与えられたレベルN仕様を

*A Support Environment for Communication Software Design: ITECS(4) - Specification Verification (Verifier,Vega) -
†Keiichirou YAMANO, Kaoru TAKAHASHI, Yoshiaki TOKITA
‡Advanced Intelligent Communication System Labs.

もとに、1段階抽象度を低くしたレベルN+1仕様を定義する。次に、このレベルN+1仕様が、レベルN仕様を正しく詳細化しているかどうかの検証を行う。一般的に、二つのLOTOS仕様間の検証には、弱bisimulation[1]など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、付加的な情報を加える場合や、複数の上位レベルの仕様を組み合わせて下位レベルの仕様を構成する場合がある。このような場合には、一般的な等価性の概念を適用することができない。従って、VerifierではSimulation関係[1][2]の概念を用い、文献[3]の判定アルゴリズムによる検証を行っている。

また、Simulation関係による検証は、大規模・複雑な仕様についても、仕様の構造化分割と部分検証の概念を適用することによって、対応可能である。

このようにVerifierを用いることによって、最終的に得られる詳細化仕様が与えられた要求仕様を正しく実現していることが保証され、大規模なシステムの仕様記述においても、効率的で高信頼な通信ソフトウェアの設計支援が可能になると考えられる。

図3は、Verifierの実行画面例である。

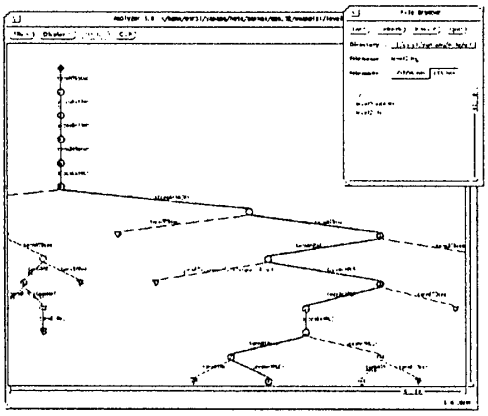

図 3: Verifier実行画面

3.2 Vega

Vegaは、通信ソフトウェアの仕様が時間的性質において設計者の意図を正しく反映しているかどうかを、容易に検証するためのツールである。具体的には、LOTOSで表現された通信ソフトウェアの仕様に対応する遷移システム表現を解析することにより、設計者が時制論理に基づく論理式で表現した性質、つまりイベント間の時間的な依存関係などを満たしているかどうかの検証を行うことができる[4]。

例えば、ISDNサービスを記述した仕様において、電話の発呼がいつか相手側に着呼するというような時間的性質を、その仕様が正しく記述しているかを自動的に調べることができる。このような時間的性質は、有用表現と呼ばれる、設計者にとって簡易で便利な論理式を用いて表現可能である。

Vegaの機能を一覧すると、次のようになる：

- 与えた時間的性質を仕様が満足しているかどうかのチェック
- 時間的性質の簡易で便利な表現のための有用表現の提供
- ライブラリ提供による有用表現の自由なカスタマイズ
- チェックする仕様の範囲を特定化することによる効率的な検証の提供

図4は、Vegaの実行画面例である。

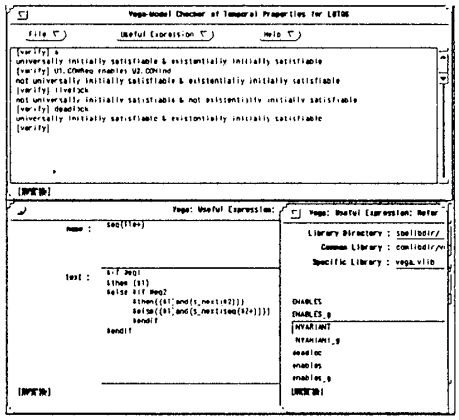

図 4: Vega実行画面

4 おわりに

本報告では、ITECSの仕様検証支援について述べた。ITECSでは、仕様の詳細化過程における仕様間の検証を行うVerifierと、記述された仕様の時間的性質を検証するVegaを用いることによって、大規模な通信ソフトウェアの設計においても、効率的な仕様の記述および検証が行え、高信頼な通信ソフトウェアの仕様記述が行えると考えられる。

今後の課題として、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の完成と、実際の通信ソフトウェア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, et.al. : "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," 電子情報通信学会論文誌, Vol.J76-D-I, No.1 (1993).

[4] 高橋 薫, 加藤 靖, 安藤 敏彦, 野口 正一 : "LOTOSと時制論理に基づくプロトコル検証," 情報処理学会 マルチメディア通信と分散処理研究会, DPS 58-11, pp.83-90 (1992).