マルチメディア通信と分散処理　52－38
（1991．9．27）

サービス手順検証法の検討

岡本　光浩　　新津　善弘

ＮＴＴ交換システム研究所

あらまし　本報告では、ユーザ・網間のインタラクションで表現されたサービス仕様である、情報シーケンス（サービス手順）の検証法と、それにもとづいて作成した検証システムのプロトタイプによる検証結果について述べる。

サービス手順の検証は、サービス手順のマクロな流れの検証と細部のインタラクションの検証との２ステップに分けた段階的検証方式で実現する。各ステップでは、サービス設計のエキスパートが持つ知識（サービス常識）より抽出した検証ルールを保持している。サービス仕様は、このルールとのマッチングにより検証される。

プロトタイプによる検証結果からは、通常のサービス仕様の場合では、５秒以内で検証ができることが明らかになった。

A Verification Scheme for Service Procedures

Mitsuhiro OKAMOTO　　Yoshihiro NIITSU

NTT Communication Switching Laboratories

3-9-11 Midori-cho Musashino-shi, Tokyo, Japan

Abstract　This paper describes a service specification verification scheme of Information sequences (service procedures) which are expressed by message interactions between a user and network.

Service procedures are verified by the step-wise verification method which has two steps ; one is verification of general flow of service specification, the other is verification of detail flow of service specification. Each step has a rule which is based on knowledge of service design experts. Service specification is verified by matching these rules.

The results of manufacturing the prototype based on this verification scheme show that the time of specification verification for most of communication services is less than 5 seconds.

1.まえがき

通信サービスの開発において、仕様作成段階での誤りは、開発が進んだ段階での下流工程からの手戻りとなるため、効率的な開発を妨げる要因となっている。この問題を解消するため、仕様作成段階での十分な検証が要求される。また、多様なサービスを迅速に提供することを特徴とした、インテリジェントネットワーク（IN）の導入[1]により、(1)サービスについての基礎的な知識しか持たない、非エキスパートによる仕様記述、および(2)カスタマイズドサービスの仕様記述、が求められている。(1)では仕様中に誤りが含まれる可能性が大きくなることが考えられること、(2)では繰り返しの仕様変更があることや、そのスキルレベルによりさらに誤りが発生しやすくなることから、通信サービス仕様の自動検証がますます重要になってきている。

サービス仕様の検証は、従来、ＳＤＬを対象とした状態遷移の正常性の検証がほとんどであり、ＳＤＬよりさらに上位の記述である、ユーザ・網間のインタラクションで表現される情報シーケンス（サービス手順）についての検証は少なかった。特に情報シーケンスの内容まで着目したサービス仕様の検証はあまり行われていなかった。しかし、非エキスパートによる仕様記述はできるだけ簡単でなければならず、特にINではユーザ・網間の情報シーケンスによる記述が中心になると考えられるため[2]、サービス手順の検証が必須となる。

サービス手順を含む、サービス仕様の記述法と作成環境については、我々はすでに、サービス設計のエキスパートから非エキスパートまでを対象とした、階層的な記述方法を用いたサービス仕様作成システム[3],[4]を提案してきた。

本報告では、このサービス仕様作成システムでのサービス手順の記述法に基づいた、サービス手順検証法を提案する。サービス手順の検証の中心となる意味検証を自動的に行うための手法として、すでにマクロな流れの検証と細部のインタラクションについての検証の２ステップに分けておこなう段階的検証方式[5]を提案した。ここでは、各ステップでの具体的な検証項目と検証手順について述べる。また、本検証法に基づいて作成した検証システムのプロトタイプによる、サービス仕様の検証結果についても述べる。

2.仕様検証の分類

通信サービスの仕様検証は、検出する誤りの性質や採用する検証方法によっていくつかの範疇に分類できる。我々は、仕様検証を検証の手段と検証の深さの２つの観点から分類した。（表１）

表１　仕様検証の分類

		手段	
		静的検証	動的検証
深さ	構文検証	・記述の過不足 ・記述の形式、属性の誤り ・その他言語仕様との整合性	対象としない
	論理検証	・無限ループ、デッドロック ・信号順序規則との整合性 ・準正常、スクリーニング条件の正当性 ・信号方式との整合性 ・状態遷移の正常性 ・交換装置制御プロトコルとの整合性	・動作の正常性
	意味検証	・サービス常識との整合性	・サービス要求との整合性
	価値検証	対象としない	・利便性、有効性ーサービス機能 ・操作性ーマン・マシンインタフェース

検証の手段では、サービス仕様を動作させず、机上検討やコンピュータによるアルゴリズムやルールを用いて検証をおこなう静的検証、および、コンピュータによるシミュレーションや擬似通信ノードを用いてサービス仕様を動作させて検証をおこなう動的検証の２つに分類した。また、検証の深さでは、構文検証、論理検証、意味検証、価値検証の４つに分類した。

本報告で述べる検証は、手段では静的検証に、深さでは意味検証に分類される。

3.サービス仕様記述と段階的検証方式

3.1サービス仕様作成システムの仕様記述

検証の対象となるサービス仕様は、サービス仕様作成システム（図１）で記述される。このシステムは、記述のレベルの違いにより３つの記述ステップから構成され、記述者はスキルに応じて、各記述ステップからサービス仕様を図形式で入力することができる。ま

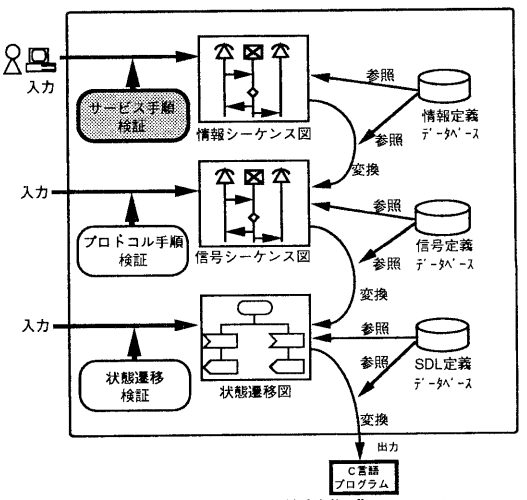


図１　サービス仕様作成システム

た検証は各記述ステップ対応に設けることとする。各記述ステップの仕様記述と検証を以下に示す。

ｽﾃｯﾌﾟ１）情報シーケンス記述→サービス手順検証

ユーザ・網間の信号方式非依存の信号（情報：発呼、着側呼出等）送受の手順。

ｽﾃｯﾌﾟ２）信号シーケンス記述→プロトコル手順検証

ユーザ・網間の信号方式依存の信号（信号：オフフック等）送受と網内部の処理概要の手順。

ｽﾃｯﾌﾟ３）状態遷移記述→状態遷移検証

網内のサービス制御処理ノードにおける内部の信号送受と処理の手順。

本報告では、ステップ１のサービス手順検証について述べる。

3.2サービス手順の検証

3.2.1サービス手順の記述

はじめにサービス手順の記述について述べる。サービス手順は、ステップ１の情報シーケンス記述（情報シーケンス図）で記述される。情報シーケンス図の例を図２に示す。シーケンスの記述要素をプリミティブと呼ぶ。情報シーケンス図のプリミティブは、表す内容により以下のように分類できる。

(1) ユーザ・網間のインタラクション（図中 ”→”）
(2) 端末に提供される通信中状態（図中 ”<=>”）

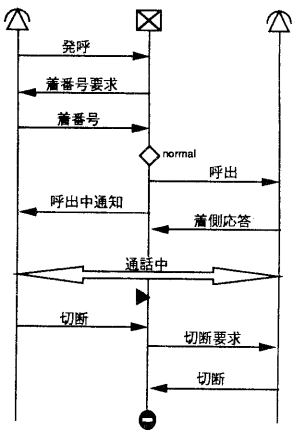


図２　情報シーケンス図の例

3.2.2サービス手順検証のアプローチ法

情報シーケンス図は、十分なサービス常識に基づいてのみ正しく記述されるが、非エキスパートは、不十分なサービス常識しか持たないため、記述した情報シーケンス図には誤りが含まれる可能性がある。このためサービス手順の検証は、サービス常識との整合性を調べる意味検証（表１）でおこなうのが望ましい。ここで述べるサービス常識とは、網がサービスを正常に動作させるための条件に関する、サービス設計のエキスパートが持つ知識である。サービス手順の意味検証は、サービス常識より抽出した検証ルールとのマッチングによる、ルールベースの検証でおこなう。

3.2.3段階的検証方式[5]

サービス仕様の検証において、効率的で容易な誤り修正の方法として、以下の２つが考えられる。

(1) 修正によってサービス仕様に影響を及ぼす範囲が広い誤りを先に、狭い誤りをその後に修正する。
(2) 誤りの性質ごとに対応して修正する。

(1) の影響範囲の広い誤りとは、サービス手順のマクロな流れに関するものと考えられる。また(2) の誤りの性質は、３.２.１で述べたプリミティブの表す内容に対応すると考えられる。以上より、ここでは端末に提供される通信中状態に着目した。情報シーケンス図の通信中状態を表すプリミティブを状態、通信中状態間のユーザ・網間のインタラクションをまとめて通信中状態の遷移手順とすると、情報シーケンス図は図３(b)のように書くことができる。この図をマクロ化情報シーケンス図と呼ぶ。各記述要素は次の性質を持つ。

状態：(a)通話中(b)保留中(c)初期状態の３状態で構成。
（例、話者a-b間 通話中、話者a-c 間 保留中）

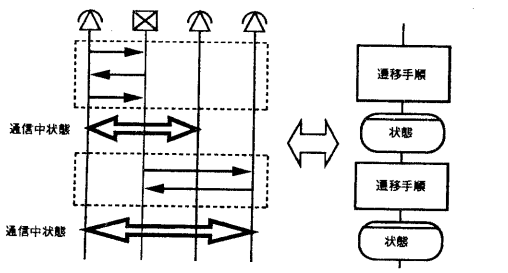
遷移手順：状態の遷移を起こすプリミティブを遷移トリガ（例えば、発呼、コールウェイティング時の話者切り替え等）として定義し、この遷移トリガを検出することによって遷移手順と見なす。

検証は、マクロ化情報シーケンス図から検証を以下の２ステップに分けた、段階的検証方式でおこなう。

（ステップ１）マクロ化シーケンス検証
通信中状態とその遷移の正常性の検証

（ステップ２）遷移手順検証
ユーザ・網間のインタラクションの正常性の検証

検証の手順は、先にステップ１でサービス手順のマクロな流れを検証し、その後ステップ２でサービス手順の細部のインタラクションについて検証する。



(a) 情報シーケンス図　(b) マクロ化情報シーケンス図

図３　情報シーケンス図とマクロ化情報シーケンス図の対応

4.マクロ化シーケンス検証

マクロ化シーケンス検証では、端末に提供される通信中状態とその遷移について検証する。

4.1 検証項目

検証項目は、通信中状態遷移の正常性を表す以下のサービス常識にもとづいて抽出した。

サービス常識（1－1）通信中状態と遷移トリガは一対一に対応する：マクロ化情報シーケンス図上では、状態（通信中状態）と遷移手順（遷移トリガ）が交互に現われることによって通信中状態の遷移が進む。

サービス常識（1－2）通信中状態と遷移トリガにより次通信中状態が決まる：ある通信中状態に対して、次に来ることが許された、遷移トリガによって通信中状態の遷移を生じた場合、遷移する次の通信中状態が存在し、一つに決まる。

これらのサービス常識より抽出した、検証項目を表2に示す。

表2　マクロ化シーケンス検証の検証項目

サービス常識	検証項目
(1-1) 通信中状態と遷移トリガは一対一に対応する	(1-I)通信中状態と遷移トリガは交互に現われるか
(1-2) 通信中状態と遷移トリガにより次通信中状態が決まる	(1-II)遷移する先の次通信中状態が存在するか
	(1-III)次通信中状態の記述が前通信中状態からの遷移の結果と一致するか

表3　通信中状態と遷移トリガの数値表現

通信中状態

$(s_1, h_1 \mid s_2, h_2 \mid \cdots \mid s_n, h_n)$

$s_i \rightarrow 1$：通話回線iが通話中
0：〃　非通話中
$h_i \rightarrow 1$：通話回線iが保留中
0：〃　非保留中
$(i = 1, 2, \ldots, n)$

遷移トリガ

$< Ts_1, Th_1 \mid Ts_2, Th_2 \mid \cdots \mid Ts_n, Th_n >$

$Ts_i \rightarrow +1$：通話回線iを通話中に遷移
-1：〃　非通話中に遷移
0：遷移をおこなわない
$Th_i \rightarrow +1$：通話回線iを保留中に遷移
-1：〃　非保留中に遷移
0：遷移をおこなわない
$(i = 1, 2, \ldots, n)$

表4　検証項目（II）の検証ルールの例

検証ルール：すでに通話中の回線に、通話中への遷移をさせる遷移トリガを入力していないか
誤りの条件：通信中に関する表示値 s_i が　$s_i > 1$

4.2 検証手順と検証ルール表現法

各検証項目に対する検証手順と検証ルール表現法は以下のとおり。

検証項目（1－I）：本検証では、読み込むプリミティブに応じて、以下の値を取るフラグを設ける。

通信中状態を読み込む：フラグ＝1
遷移トリガを読み込む：フラグ＝0

正しい仕様の場合は、通信中状態を読み込んだときフラグが0、遷移トリガを読み込んだときフラグが1となる。この条件を検証ルールとして保持する。

検証手順は以下のとおり。

step(i)：シーケンスからプリミティブを読み込む。
step(ii)：プリミティブを読み込んだときのフラグの値とフラグの条件とを比較する。一致しなければ誤りとする。

検証項目（1－II）：通信中状態と遷移トリガを表3に示すような数値で表現する。遷移トリガは、遷移前後の通信中状態の差分値で表現されている。検証では、遷移前の通信中状態の値に遷移トリガの値を加算することで遷移後の通信中状態を求める。検証ルールは通信中状態として存在するための数値の条件で表されている。検証ルールの例を表4に示す。

検証手順を以下に示す。

step(i)：シーケンスからプリミティブを読み込む。
step(ii)：読み込んだプリミティブが遷移トリガならば、対応する数値表現に変換する。
step(iii)：前通信中状態を表す数値に、step(ii)で変換した数値を加算して、次の通信中状態を求める。

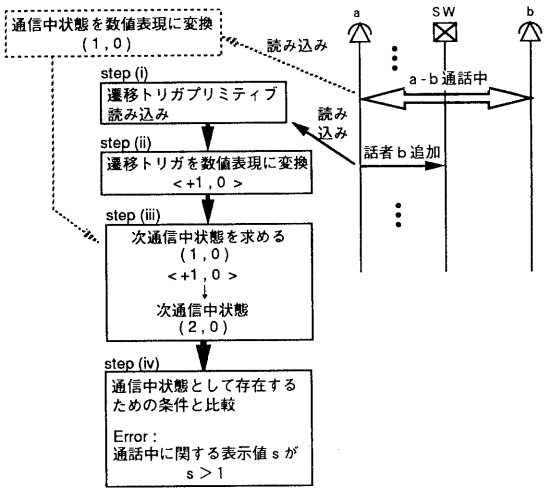


図4　マクロ化シーケンス検証の例（検証項目（1-II））

step(iv)：step(iii)で求めた次の通信中状態が、通信中状態として存在するための条件と比較する。条件と一致しなければ誤りとする。

検証例を図4に示す。

検証項目（1－III）：検証項目（1－II）で求めた通信中状態とサービス仕様から読み込んだ通信中状態とを比較する。検証手順は以下のとおり。

step(i)：シーケンスからプリミティブを読み込む。
step(ii)：読み込んだプリミティブが通信中状態ならば、検証項目（1－II）で求めた通信中状態と比較し、一致しなければ誤りとする。

5.遷移手順検証

遷移手順検証では、ユーザ・網間のインタラクションについて検証する。

5.1 検証項目

検証項目は、ユーザ・網間のインタラクションの正常性を表す以下のサービス常識にもとづいて抽出した。

サービス常識（2－1）冗長な記述がない：同じプリミティブの連続した記述や、サービスの手順として無意味な繰り返しの記述がない。

サービス常識（2－2）必要な入出力の漏れがない：網からの要求に対するユーザの応答や、サービスとして必要な入出力は、漏れなく記述されている。

サービス常識（2－3）禁止的な位置でのプリミティブの記述がない：プリミティブが、その意味からみて不適当な位置に記述されていない。

これらのサービス常識より抽出した、検証項目を表5に示す。

表5　遷移手順検証の検証項目

サービス常識	検証項目
(2-1) 冗長な記述がない	(2-I)同一プリミティブが連続して記述されていないか
	(2-II)同一プリミティブが二重に出力されていないか
(2-2) 必要な入出力の漏れがない	(2-III)網の動作に必要なプリミティブの入力があるか
	(2-IV)端末への情報通知プリミティブの出力があるか
	(2-V)入力要求に対する入力があるか
	(2-VI)開始／終了時に必要な入出力があるか
(2-3) 禁止的な位置でのプリミティブの記述がない	(2-VII)プリミティブの意味に反する位置に入出力がないか

5.2 検証手順と検証ルール表現法

各検証項目に対する検証手順と検証ルール表現法は以下のとおり。

検証項目（2－I）：以下の手順で検証する。

step(i)：シーケンスからプリミティブを読み込む。

step(ii)：読み込んだプリミティブと直前のプリミティブとを比較し、一致すれば誤りとする。

検証項目（2－II）～（2－VII）：ユーザ・網間のインタラクションは、プリミティブの順序関係で定義されるので、そこに含まれる誤りも、主として順序関係に関するものと考えられる。このため、遷移手順検証の検証ルールはプリミティブの順序関係に着目して表現する。検証ルールは以下に示す項目により構成する。

(1) 検証の対象となるプリミティブ名
(2) 検証条件として検索対象となるプリミティブ名
(3) (2)の(1)に対するシーケンス上での位置
(4) (2)が(1)に対して存在が必要か禁止か
(5) 誤りの度合い（ErrorかWarningか）

これらの項目を用いて、検証ルールを表現する。検証ルールの例を表6に示す。

表6　検証項目(2-II)～(2-VII)の検証ルール表現の例

検証ルール	「着番号要求の直後に着番号が入力されているか」
項目	(1)検証の対象となるプリミティブ名：着番号要求 (2)検索対象のプリミティブ名　：着番号 (3)検索位置　：直後 (4)存在の必要／禁止　：必要 (5)誤りの度合い　：Error

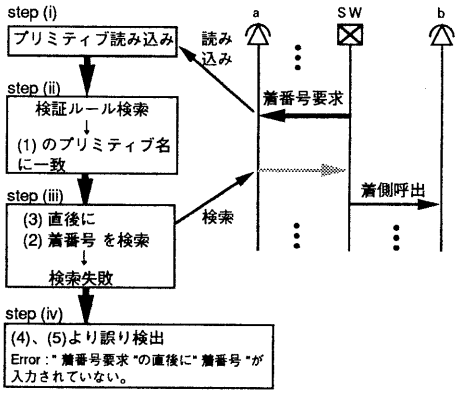


図5　遷移手順検証の例（表6の検証ルールによる場合）

検証手順を以下に示す。

step(i)：シーケンスからプリミティブを読み込む。

step(ii)：読み込んだプリミティブに関する検証ルールが存在するか検索する。

step(iii)：読み込んだプリミティブと検証ルールの項目(1)のプリミティブ名とが一致すると(3)の位置に(2)のプリミティブを検索する。

step(iv)：検索結果と(4)、(5)にもとづいて、検証結果を得る。

上記手順による検証例を図5に示す。

5.3 誤りの度合いの表現方法

遷移手順検証で検出される誤りは、その内容によって誤りの度合いが異なる。誤りの度合いを以下の2つに分類する。

(1) サービスによらず、誤りとなるもの
(2) 一般的なサービス常識には外れるが、サービスによっては、必ずしも誤りと断定できないもの

誤り度合いの表現は、以下の2つを用いる。

Error：誤り
Warning：誤りかどうか決められないもの

上記(1)に属する誤りに対しては、" Error "を表示し、(2)に属する誤りに対しては、" Warning " を表示する。

6.プロトタイプによる検証システムの試作評価

これまで述べてきた検証方式を評価するため、検証システムのプロトタイプを試作した。このプロトタイ

プによるサービス仕様の検証結果について述べる。

6.1 検証システムプロトタイプの試作

サービス手順は3.2.1で述べたように図形式（情報シーケンス図）で記述される。情報シーケンス図は、その記述要素が一対一に対応する言語形式記述を持つ。言語形式記述のサービス仕様の例を図6に示す。検証は、この言語形式の仕様からプリミティブ（図中、下線部が1つのプリミティブで、図形式の矢印の1本に相当）を読み込むことによって実現する。

検証システム（図7）は検証処理部、ルール部ともにC言語により記述し、ワークステーション上に実現した。

```
service {
  Set_Up ( Caller, Node );  ◀── 下線部が図形式の
  Dial_Urgency ( Node, Caller );   矢印1本に相当
  Dial ( Caller, Node : r ) ;
  .if ( r = NORMAL)     {
      Calling ( Node, Callee ) ;
      Calling Info. ( Node, Caller ) ;
      {
          Answer ( Callee, Node ) ;
          Speaking ( Caller, Callee ) ;
          {
          Disconnect ( Caller, Node ) ;
                  :
          |
          Disconnect ( Callee, Node ) ;
                  :
```

図6　サービス仕様の言語形式記述の例

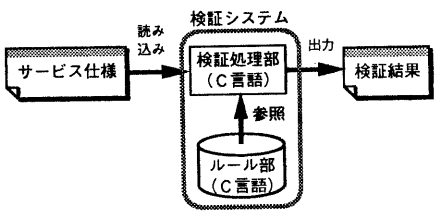


図7　検証システム

6.2 試作結果と考察

検証は、サービス仕様の中に、あらかじめ設定しておいた誤りを検出させる方法を用いた。仕様中に記述されたプリミティブの種類と、検証プログラムで保持する検証ルールの数は以下のとおり。

プリミティブの種類：26

ルール数：47

検証結果として以下のことが得られた。

検証動作の正常性：あらかじめ仕様中に設定された誤りを、検証によってもれなく検出できるかどうかを確認した。その結果、設定した誤りに関してはすべて検出することができ、動作の正常性が確認された。

誤り検出に要する時間：検証を起動させてから終了するまでの時間を測定した。記述量と時間の関係を図8に示す。測定では、従来作成した通信サービスで、最も複雑な仕様である電話会議サービスに相当する基本通話の40倍の記述量の場合で4.4秒であり、通常のサービスでは、これ以下で検証できることがわかった。

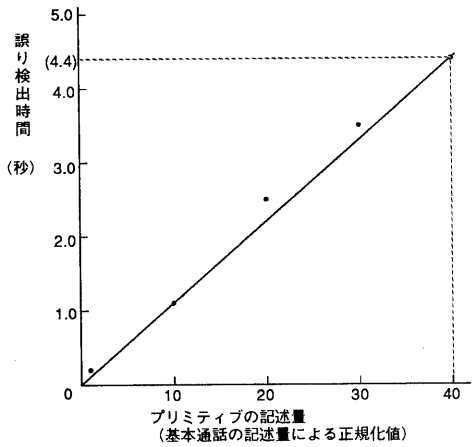


図8　プリミティブの記述量と誤り検出に要する時間の関係

7.むすび

ユーザ・網間のインタラクションで表現される、サービス手順の検証法について述べた。また本検証法にもとづいてプロトタイプを試作し、それによってサービス仕様を検証した結果についても述べた。プロトタイプによる検証結果より、通常のサービス仕様では、5秒以内で検証できることがわかった。

今後の課題を以下に示す。

(1)本検証法を、INサービスシナリオ作成環境へ適用する。

(2)サービス仕様の作成工程に本検証法を適用し、有効性および検証能力の評価をおこなう。

文　献

[1] 岡田、重松、佐藤：”インテリジェントネットワークにおけるサービス定義・制御の階層的構造”、信学技法、SSE 90-17 (1990.5).

[2] 新津、水野、岡本：”INにおけるサービス自動作成環境構成法”、信学技法、SSE 90-116 (1991.1).

[3] Y.Niitsu and O.Mizuno : " Interactive Specification Environment for Communication Service ", IEEE J-SAC, Vol. 8, No. 2, pp. 181-188 (1990.2).

[4] 水野、新津：”サービス記述手順に基づく階層形サービスソフトウェア生成法の検討”、信学技法、SSE 89-63 (1989.7).

[5] 岡本、新津：”サービス手順段階的検証法の検討”、'90秋季信学全大、B-417.