6F－4

ペトリネット理論に基づいたシステムの信頼性解析について*

勝間田 仁† 栗原 正仁† 大内 東† 菅澤 喜男‡

†北海道大学工学部　‡日本大学生産工学部

1 はじめに

コンピュータシステムが大規模化し複雑になり，その設計段階において，システムの性能や信用性 (dependability) を向上させる設計案について，その有効性を評価することは重要である．

システムの信頼性評価において，ペトリネット理論を拡張した確率ペトリネットがシステムの挙動を定性的に理解するための理論的解析モデル [1] として，システムの動作解析および性能評価に広く用いられ様々なツールとして開発されてきている．

従来，システムの故障関係をモデル化する方法として，信頼性ブロック図あるいはフォールトツリーが用いられてきた．しかし，これらの方法は，対象とするシステムが大規模・複雑になると解析が困難になる．

本稿では，基本的な分散処理形態を有するシステム [3] を取り上げ，各要素ごとにおいて故障を考慮した動作手順をチャート図として表現し，ペトリネットに変換する．変換されたペトリネットのシステム信頼性解析について検討する．

2 ペトリネット

ペトリネット (Petri Net, 以後 PN と記す)[2] は，非同期・並列的な動作をする分散処理システムなどをモデル化するのに優れたモデル化技法として知られている．

ここでは，PN の概説を行う．

PN は，次の四つの組で定義される二部有向グラフである．

$$N =< P, T, A, M_0 > \tag{1}$$

ただし，

$$P = \{p_i \mid 1 \leq i \leq |P|\} \tag{2}$$

$$T = \{t_j \mid 1 \leq j \leq |T|\} \tag{3}$$

システムにおける条件と対応づけられる場所 P は，有限個の場所 (place) p_i の集合で○印で表す．システム中の事象に対応づけられる遷移 T は，有限個の遷移 (transition) t_j の集合で｜印で表される．A は有限個の有向線分の集合で，場所 p_i から遷移 t_j への有向線分の部分集合と遷移 t_j から場所 p_i への有向線分で構成される．M_0は初期刻印でシステムの初期状態の設定により決定される．

3 分散処理システムの PN モデル

3.1 分散処理システム

本稿で取り上げる，オンライン処理とローカル処理を中心とするメインシステムとサブシステムの代替が可能な基本的な分散処理形態を有するシステムの故障発生を考慮したシステム動作の概説を行う．

メインシステムは主にオンライン処理をし、サブシステムは主にローカル処理をする．ある一定の条件を満たすとメインシステムとサブシステムが交替しシステム全体としての機能を果たす．しかし，メインシステムとサブシステムが交替中に通信障害等が起こると双方の機能とも停止し，システム故障状態となる．

*System Reliability Analysis By Petri Net Theory

Masashi KATSUMATA, Masahito KURIHARA and Azuma OHUCHI
Faculty of Engineering, Hokkaido University
Yoshio SUGASAWA
Faculty of Industrial Technology, Nihon University

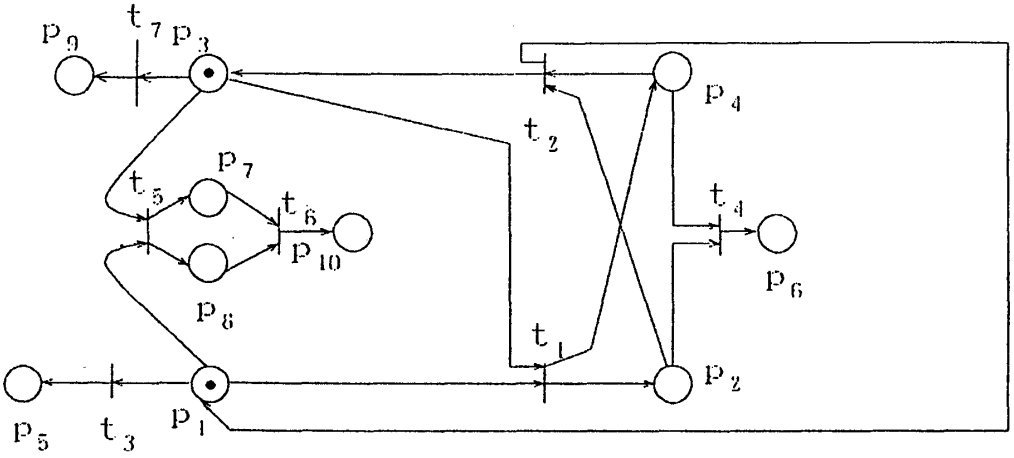

図 1: 故障を考慮した分散処理システムの PN モデル

3.2 動作手順の PN モデル

分散処理システムを構成しているメインシステムとサブシステムの故障を考慮した動作手順をフローチャート図で表す．本稿では図を省略する．

システムの動作手順を PN によってモデル化したものを図 1 に示す．

図 1 における各場所 (p_i = 1,2,...,10) と各遷移 (t_j = 1,2,...,7) の意味は次の通りである．

p_1: サブシステムがローカル処理中
p_2: サブシステムがメインシステムと交替中
p_3: メインシステムがオンライン処理中
p_4: メインシステムがサブシステムと交替中
p_5: サブシステムが故障しシステム故障状態
p_6: メインシステムとサブシステムがトラップ状態
p_7: サブシステム修理中
p_8: メインシステムがローカル処理中
p_9: メインシステムが故障しシステム故障状態
p_{10}: メインシステムとサブシステムが故障状態

t_1: メインシステムがオンライン処理からローカル処理へ，サブシステムがローカル処理からオンライン処理へそれぞれ切り替えられ，メインシステムとサブシステムの交替が始まる

t_2: メインシステムとサブシステムの交替が終了 し，メインシステムがオンライン処理，サブシステムがローカル処理にそれぞれ復帰する

t_3: 通信障害などでサブシステムがシステム故障となる

t_4: サブシステムとメインシステムとが交替中に通信障害などが発生し，システムがトラップ状態となる

t_5: サブシステムが故障となり，メインシステムがローカル処理を代行する

t_6: サブシステムの故障がメインシステムの機能でフォローしきれないためシステムが故障 となる

t_7: メインシステムが故障しシステムがシステム故障となる

4 システムの信頼性解析への検討

PN の解析手法である到達可能グラフを用いることでマルコフモデルの生成が可能になり，システムまたは諸状態の信頼性評価値に関する計算も可能となる．

5 おわりに

本稿では，基本的な分散処理形態を有するシステムを取り上げ，各要素ごとにおいて故障を考慮した動作手順をチャート図として表現し，PN に変換し，PN の信頼性解析について検討した．今後の課題としては，より現実的な解析を行う場合にはモデルの大規模・複雑化を招くのでモデル化の階層化について検討する必要がある．

参考文献

[1] A. M. Johnson, Jr. and M. Malek : Survey of Software Tools for Evaluating Reliability, Availability, and Serviceability, ACM Computing Surveys, 20, 4, 227-269 (April 1988).

[2] W. Reisig : Petri Nets, Springer-Verlag, Berlin (1982).

[3] 勝間田 仁, 菅澤 喜男 : 分散処理システムを例とした不変集合解析によるシステムの系列な故障診断, 情報処理学会論文誌, Vol. 35, No.10, pp. 2214-2219 (1994).