分散協調型の故障診断と秩序再構成

溝口　博三*　・下川　俊彦**
吉田　紀彦***

Decentralized Cooperative Fault Diagnosis and System Reorganization

by

Hiromi Mizoguchi *, Toshihiko Shimokawa **, Norihiko Yoshida ***

Fault diagnosis and recovery in decentralized cooperative systems such as multi-agent systems are different from the ones in centralized systems. The self diagnosis of a system is actually integration of mutual diagnoses of the system components, and the recovery is actually self reorganization of the system. This paper presents an approach toward this sort of diagnosis and recovery applying a theory of distributed network diagnosis, and its implementation and some empirical evaluation.

1．はじめに

自律分散協調系は，卑近な比喩で言えば蟻の集団のように，冗長性を内在することから耐故障性に優れることが，集中系に比較しての重要な優位性の一つと言われている．しかしながら，系全体が構成要素の協調と秩序によって構成されているからには，障害の性質によっては単一構成要素の故障でも系全体に影響を及ぼす可能性がやはり残っている．すなわち，構成要素の停止障害に対しては他の構成要素が自律的に処理を代行して系全体の秩序が再構成されるので頑健であるが，一方，コミッション障害など誤った要素間通信を誘発する障害に対しては，他の構成要素もそれに影響を受けるため，系全体の故障に繋がりえる．そのような系を復旧させるためには，故障要素の同定とその隔離ないし修復が必要となる．そこで我々は，自律分散協調系における耐故障性の向上に向けた考察を進めている．

一般に集中系における耐故障性の向上には，監視機を付加して自己診断を行う，系を多重化してバックアップする，などの方策がとられる．これに対して上記のような自律分散協調系では，その冗長性を有効に活用すべく，構成要素の相互診断と相互バックアップによって耐故障性を向上させることが必要となる．分散ネットワーク診断の分野では，すでにそのような相互診断の理論モデルについて研究が進んでいるが，それを実際の自律分散協調系に応用しようとするに際しては，故障の検出・同定・隔離・復旧に関する具体的な方式を考案し，それを中央集権制御なしに行う機構を構築しなければならない．さらに，自律分散協調系は動的であるのが普通であり，系内の構成要素の集合も動的に変化しえる．そこで，系のそのような動的変化にも追従しえる機構である必要がある．

本論文では以下，第2章で分散ネットワーク診断の理論モデルについて概要をごく簡単にまとめる．次いで第3章で，それを自律分散協調系に適用する際に必要となる故障の検出・同定・隔離・復旧の方式について述べる．第4章ではプロトタイプの設計，そして第5章でごく簡単な例題による実験を示す．第6章は検討とまとめである．

2．ネットワーク診断理論

構成要素間の相互診断に基づく分散ネットワーク診

平成13年4月20日受理

* 三菱電機（Mitsubishi Electric Corp）
** 九州大学大学院システム情報科学研究院（Graduate School of Information Science and Electrical Engineering, Kyushu University）
*** 情報システム工学科（Department of Computer and Information Sciences）

断理論として，Preparata, Metze and Chien の PMC モデルがある [1]．これは，ある要素による別の要素の検査について，正常な要素による検査は信頼できるが異常な要素による検査は信頼できないという前提の下で，最高 t 個までの多重永久故障を許す内から少なくとも 1 つの故障要素を検出可能な t 重故障逐次診断可能系，および全ての故障要素を同時に検出可能な t 重故障同時診断可能系を定式化したものである．このモデルは故障状態が時間的に変化しない永久故障を対象としているが，診断可能な系の必要十分条件，検査結果集合（症候群）からの故障要素の同定などについて，多くの研究がなされている．

より一般には，故障状態が時間的に変化する間欠故障も考えなければならない．そこでは正常要素から永久故障要素への検査のみが信頼でき，間欠故障要素に対する複数回の診断はその度に結果が異なる恐れがあり，間欠故障要素に対する複数の正常要素からの診断は結果が一致しない恐れがある．系内の故障要素を正常と判定することを「不完全な」診断，正常要素を故障を判定することを「不正確な」診断と呼ぶが，間欠故障の存在は不完全な診断を引き起こす．これは原理的に避けられない．そこで，間欠故障を含む系において少なくとも正確な診断を保証する故障診断が，t/r-自己診断可能系 [2]，t/r/r-自己診断可能系 [3]，t/r/τ-自己診断可能系 [4] などとして定式化されている．なお，ここで t は故障要素数の最大値，r は間欠故障要素数の最大値を表す．

これらを踏まえて，香田らは間欠故障も含む自己診断可能系の効率的な構成方法を「高度構造化系 (highly structured system)」として定式化した [5,6,7,8]．これをごく簡潔に説明する．

分散ネットワーク診断の理論では，構成要素を節点 v，要素 v から別の要素 u への診断を弧 e = (v, u) で表し，系を節点と弧の集合からなるグラフ G = [V, E] (V = {v}, E = {e})で表す．Fig.1 に図示するように（円が要素，矢印が検査），ある要素を核の被検査要素 (kernel unit) として長さ 1 の検査列を ν 本，長さ 2 の検査列を μ 本持つようなグラフを，副系 (subsystem) H(v; μ, ν) と呼ぶ．ここで，系内の全ての要素 v が副系 H を持つ時，その系を高度構造化系と呼ぶ．

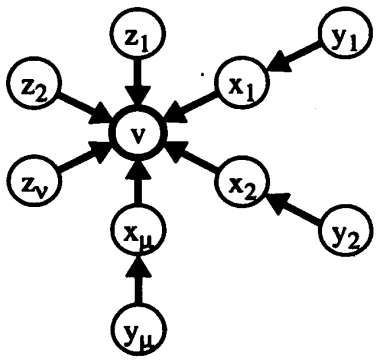


Fig. 1. Subsystem H(v; μ, ν) in Highly Structured System.

高度構造化系においては，次の定理が証明されている．

(1) 系 G の全ての副系 H について下式が成り立つならば，G は t 重故障同時診断可能系である（⌊ x ⌋は x を越えない最大の整数）．

$$\mu + \lfloor \nu/2 \rfloor \geq t$$

(2) 系 G の全ての副系 H について下式が成り立つならば，G は t/r/τ- 自己診断可能系である．

$$\mu + \lfloor (\nu-1)/2 \rfloor \geq t + \min(r, \tau + 1)$$

さらに，上記それぞれの定理を満たす系について，検査数を最小にする症候群解析法も構築されている．例えば前者については，O(|E|) の検査数で解析可能な系が構成できる．

3．自律分散協調系への適用

前章で概要を簡単に説明した診断理論は，系内の故障要素の同定を可能にする条件，および同定手順の構成法を論じている．分散協調的な故障診断の中核となるべきものではあるが，これを実際の自律分散協調系の故障診断および修復に応用するには，様々な処理を補う必要がある．それらの処理は系の動的構成に対応し，かつ中央集権制御を排したものでなければならない．それらを，要素間の監視・検査，故障の検出・同定・隔離・復旧のそれぞれについて，順に述べる．

(1) 要素間の相互監視・検査

構成要素は（広い意味での）通信によって互いに監視・検査を行う．要素間の故障検出は，通常の故障検出と同様に，停止障害とオミッション障害については通信のタイムアウト検査によって，コミッション障害については通信応答の正当性検査によって行う．要素間の通信路の故障検出も，これに準ずる（ただし，監視側要素が故障している可能性もある）．

一般に，系がその構成要素について全対全の直接の通信路を有するとは限らない．一方，他と通信路を有しない孤立した構成要素（群）の存在を考慮する必要はない．ここでは，全ての要素から他の全ての要素に直接・間接の通信路を経由して到達可能であるとする．ただし，通信路の故障にも対応するためには，通信路も冗長でなければならない．

動的系において，新たな要素が加入する場合には，通常処理に必要な通信路を既存の要素との間に確立す

ることになるが，これに併せて相互監視・検査の通信路も確立する．新たな要素の存在は，通信路を経由して系内の全ての要素に伝えられる．

(2) 故障要素の同定

相互監視によって故障（の可能性）の検出された要素について，それを核要素として副系 H を構成し，故障診断の手順を遂行する．ここで満たされているべき条件は，詳細は割愛するが，系内の全要素数を n，最大多重故障要素数を t として，下式で表される．

$$n > 2t + 1$$

しかしながら，一般に動的系では要素の増減がありえるため，n が既知とは限らない．その場合には n の下限を仮定して，検査可能な最大多重故障要素数を決定する．ただし個々の副系については，実際の μ と ν の値から検査可能な最大多重故障数が決まる．

ここでの最大の問題は，「誰が」副系を設計して「誰が」結果を解析するかであり，理論モデルでは全く考慮されていない．仮にこれらの処理の中央集権制御を許容するしても，その中枢要素の故障には対応できない．これらの処理を自律分散協調的に行うには，原理的には，全ての要素に全ての要素の存在と通信関係，すなわち系全体のトポロジーを把握させておいて，同一の処理を行わせることになる．故障要素には正しい処理を期待することができないが，n と t の間の上記の関係から，多数決的に正しい処理の結果を得ることができる．以上の方策は要件として非常に厳しいものであって，厳密に任意の時点で保証することはできず，通信量も多大になるが，現時点ではこの方策をとる．

(3) 故障要素の隔離と系の復旧

一般に，自律分散協調系では，一部の構成要素が機能を停止しても，他の要素が自律的に処理を代行して系全体の秩序が再構成されるように構築されている．裏返すと，そのように構築されているのが自律分散協調系である．そこで，故障要素については，それを他の要素から隔離することによって，系を復旧することができる．これは，従来の静的冗長系や動的冗長系とは，類似する例も考えられるが，種類を異にする冗長系である．具体的には，故障要素の存在を系内の全ての（正常）要素が互いに通知し，この通知を受け取った要素は故障要素との通信を遮断する．

このような秩序再構成における問題として，第1に，系内の要素を幾つまで隔離しても正常に再構成しえるかは，自律分散協調系の構成に依存する．第2に，系が均質，すなわち全て同種の要素から構成されている場合には議論はまだ容易であるが，非均質，すなわち異種の要素が混在している場合には，これもその自律分散協調系の性質に依存する．

一方で，その要素の故障が修復可能なものであるならば，その要素に異常であることを知らしめて修復を試みさせるべきである．すなわち，要素は自分が異常である旨の通知を他から受け取ったならば（それは自分だけでは判断できないので），自己を修復する可能性を探るべきである．しかしながら，修復可能か否かは故障の性質に依存するので，ここでは当該要素に異常であることを知らしめるところまでしか考えない．

4．故障診断と修復の具体的機構

前章で考察と検討を行った基本方式に基づいて，故障診断・修復機構を，具体的に次の手順を実行するものとして構築する．

(1) 系に新たに加入した要素は，既存の要素との間に通常処理に必要な通信路を確立するとともに，監視・被監視の相互関係を確立し，同時に系のトポロジーを取得する．一方，新たな要素の加入は，系内の全ての要素に通知される．なお，全ての要素は他のいずれかから監視されなければならない．監視する側の要素は，通信の正当性とタイムアウトを適宜監視する．

(2) 自らが検査する要素集合の内に異常なものを発見した要素は，その存在を系内の他の要素に通知する．各要素は，その通知された要素を核とす副系を設計する．（それらの要素そのものが異常でなければ）設計される副系は同一のものになるので，それに従って各要素は必要に応じて副系に参加し，系全体として副系を構築する．必要なだけの μ と ν が確保できない場合には，診断は失敗となる（最低の $t = 1$ を満たすには，$\mu = 1$ または $\nu = 2$ が必要）．

(3) 副系に参加した要素は，各々の検査結果を系内の他の要素に通知する．各要素は，その症候群を解析して故障要素を同定する．ここでも（それらの要素そのものが異常でなければ）解析結果は同一のものになるので，それに従って系全体として故障要素を同定する．

(4) 正常な要素は故障と同定された要素にその旨を通知し，自己修復を期待する．通知を受けた要素は自己修復を試み，可能であればその旨を返答する．自己修復が不可能だった場合には，正常な要素は故障要素との通信路を遮断し，故障要素を隔離して系全体の秩序を再構成する．

5．実験と評価

前章までで述べた故障診断・復旧機構の動作を検証

する実験例として，非常に単純な次の問題を取り上げて結果を示す [9,10].

自律的円環構成系

この系では，構成要素どうしが互いに情報を交換しつつ，中央集権制御なしに自律的に，無秩序な初期状態から円周という秩序的な形を形成する．ミルウォーキー大の鈴木によって考案された分散アルゴリズムであり，その概要は次の通りである．

各要素は次の情報および機能を持つ．

・最終的に構成される円の直径を知っている．

・自分と他の要素との距離を算出する機能を持つ．

そして，次の処理を行う．

(1) 自分と他の要素との距離から，最も近い要素と最も遠い要素を知る．

(2) 最遠要素との距離が円直径よりも長い場合には，最遠要素に少し近づく．

(3) 最遠要素との距離が円直径よりある割合だけ短い場合には，最遠要素から少し遠ざかる．

(4) 最遠要素との距離が円の直径にほぼ等しい場合には，最近要素から少し遠ざかる．

(5) 各要素は上記の (1)〜(4) を繰り返し，全ての要素が (4) の状態に至ったら終了する．

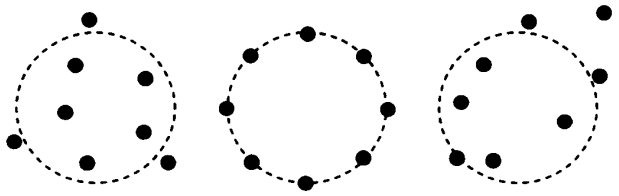
ここで，次の故障を入れ込む．

・距離測定機能の故障

・円直径情報の異常

いずれも距離判断の異常を引き起こし，円環の形状を歪ませるが，後者は他の正常要素から正しい直径情報を受け取ることによって自己修復可能としている．

このアルゴリズムの実行例を Fig. 2 に簡単に示す．



(a) Initial State. (b) Ideal Final State. (c) Faulty Final State.
Fig. 2. Circle Forming Example.

(a)の初期状態から，全要素が正常であれば(b)の最終状態に移行するが，例えば1要素の持つ直径値が誤って大きくなっていると，(c)が右上にずれていくような結果となって，正しい最終状態が得られない．

すなわち，このアルゴリズムは中央集権制御なしに秩序を形成する自律分散協調系ではあるが，一部の要素の故障が系全体に波及する可能性を内在し，一般に自律分散協調系について言われるような高い対故障性を持たない．

実験では，前章で述べた故障診断・復旧機構のプロトタイプを各構成要素に埋め込んで動作させ，故障診断・復旧機構が正しく起動されること，故障要素が正しく同定されること（これは理論モデルの動作の再確認に過ぎない），およびその結果が正常要素（群）に正しく通知され，故障要素（群）が隔離されて系が再構成されること，修復可能な故障については当該要素への通知によって修復がなされること，要素の増減に故障診断・復旧機構が正しく追従することを検証した [11,12].

6．おわりに

本論文では，自律分散協調系における耐故障性の実現に向けて，自律分散協調という特徴を活かすべく，分散ネットワーク診断の理論モデルの適用を試み，それを実際の系に応用するに際しての故障の検出・同定・隔離・復旧に関する具体的な方式について，試案を述べた．

自律分散協調系やマルチエージェントシステムにおける故障診断や障害復旧に関しては，吉田らの研究 [13] や Leckie らの研究 [14] があるが，それらに対して本論文は，分散ネットワーク診断理論の適用というところに特徴を持つ．

なお，ここでの議論は，故障要素によって引き起こされた他の要素や系全体の障害について，それを復旧するために，タイムワープ機構を用いて分散ロールバックを行うことなどまでは考えていない．

分散ネットワーク診断は理論としては一定の成果を産んでいるが，実際への応用に際しては様々な問題を解決しなければならない．本論文ではまずそれらの問題を列挙したが，全てに最適な解法を与え得たとは考えていない．例えば，より通信回数の少ない，すなわちより効率のより方式を探求するなどの努力を今後も引き続き進める．

また，本論文で取り上げた例題は，例題のための例題とも言うべきごく些細な問題であって，より本格的な規模の問題に適用しての評価も行っていく．

謝　辞

本研究の端緒を開いて頂き，貴重な助言を頂いた香田教授（九州大学）に感謝する．

参考文献

[1] P. Preparata, G. Metze and R. T. Chien, "On the Connection Assignment Problem of Diagnosable Systems", IEEE Trans. Electromag. and Comput., EC-16:6, 848-854

(1967)

[2] S. Mallela and G. M. Masson, "Diagnosis without Repair for Hybrid Fault Situations", IEEE Trans. Comput., C-29:6, 461-470 (1980)

[3] C. L. Yang and G. M. Masson, "A Generalization of Hybrid Fault Diagnosability", Proc.15th Ann.Int'l Symp. on Fault-Tolerant Computing, 36-41 (1985)

[4] C. L. Yang and G. M. Masson, "A new Measure for Hybrid Fault Diagnosability", IEEE Trans. Comput., C-36:3, 378-383 (1987)

[5] 香田，" t 重故障同時診断可能システム"，電子通信学会論文誌，J61-D:9，680-687 (1978)

[6] 香田，" t 重故障逐次診断可能システム"，電子通信学会論文誌，J61-D:9，688-694 (1978)

[7] T. Kohda and K. Abiru, "A Recursive Procedure for Optimally Designing a Hybrid Fault Diagnosable System", Proc.18th Ann. Intㅋl Symp. on Fault-Tolerant Computing, 272-277 (1988)

[8] T. Kohda, "A Simple Discriminator for Identifying Faults in Highly Structured Diagnosable Systems", J. Circuits, Systems and Computers, 4:3, 255-277 (1994)

[9] 香田，吉田，朱雀，吉田，"自己診断可能な自律分散系"，第20回情報理論とその応用シンポジウム論文集，Vol. I，193-196 (1997)

[10] 香田，吉田，朱雀，吉田，"マルチエージェントシステムにおける故障の分散的自己診断"，第 6 回マルチ・エージェントと協調計算ワークショップ論文集，6 pages.，http://www.kecl.ntt.co.jp/msrg/macc97/ (1998)

[11] 溝口，下川，吉田，牧之内，"故障耐性のある自律分散系"，第14回情報処理学会九州支部研究会，322-329 (2000)

[12] 溝口，"分散エージェント系における耐故障性アルゴリズムの実現"，九州大学修士論文 (2000)

[13] 吉田，増澤，藤原，"自律ロボット群のための停止故障耐性のある分散型問題解法"，電子情報通信学会論文誌，J79-D-I:6 (1996)

[14] C. Leckie, R. Senjen, B. Ward and M. Zhao, "A Multi-Agent System for Distributed Fault Diagnosis", Proc. 2nd Int'l Conf. on Practical Application of Intelligent Agents and Multi-Agent Technology, 71-85 (1997)