B-007

システム障害発生部位判定方法と障害の分類

Discussion of how to judge a failure point in a system and categorize a type of problem

篠原 昭夫
Akio Shinohara
日本大学

泉 隆
Takashi Izumi
日本大学

Discussion of how to judge a failure in a component. It requires when we use the function chain to reach to a failing point in an open system trouble. And provide a way to categorize a type of problem using by function chain.

1. はじめに

先にオープン・アーキテクチャ製品で構成されたシステムで発生した障害で、その原因となった部位を特定する方法として機能線を提案した[1]。機能線はシステム内で発生した障害の原因調査方針を記述したグラフ構造の図である。機能線を用いた障害被疑部位特定では機能線上に存在する各コンポーネント内で問題が発生したかを判定する必要がある。本報告では各コンポーネント内での問題発生有無を判定する方法として比較法を提案する。オープン・システム向けの製品は多機能化が進んだため、同一の製品を選択していてもシステムが異なればその使用法が大きく異なる。このため他システムで障害調査事例を別システムでの障害調査に用いるのが困難なことがある。比較法はこの状況下で各システム固有の使用条件を反映しながら障害原因究明を行うための手法である。

次に障害発生被疑部位の特定が完了した機能線に対して論理的な考察を加え、障害の分類方法を提案する。更にそれぞれの障害型に対応した対策投入方法の関連付けを行い、障害発生－機能線作成－被疑部位特定－対策立案の流れを一般化することを試みる。

2．コンポーネント内の障害発生有無の判定方法

2－1．比較法

機能線上の各コンポーネント内で障害が発生したかの判定には比較法を用いるのが有効である。これは対象システムが正常に稼動している時に事前収集しておいた情報と、これと同じ対象を障害発生時に収集したものと比較、不一致部分があればここを障害発生部位と判定する方法である。一般にオープン・システムでは同一かつ同一バージョンの製品で構成された異なるシステムは、正常稼動時に必ずしも同じ挙動をしていない。このためあるシステムでの障害事例を別システムの障害調査の参考にすることが困難なことがある。比較法では当該システムで正常時に収集しておいた情報を各コンポーネント内での障害発生有無を判定するための指標として用いる。更にオープン・システム向けの製品は動作仕様の詳細が公開されていないことが多いため、このことも比較法が有用な理由となっている。

2－2．比較法を行うための準備

以下はシステム正常稼動時に採取しておくべき情報の例である。

A:システム起動中の各コンポーネントからの報告
B:各コンポーネントの独自のログ採取機能からの情報
C:対象システムの使用目的であるサービスの正常時の処理時間
D:各コンポーネントで自動記録される定期・不定期情報
E:ネットワーク、I/O パスでの帯域使用率
F:単位時間あたりで計測かつ数値化可能な情報

例 1：システム正常稼動中サーバーの 1 日当たりのログ情報量(MB/day)
例 2：ディスク装置に格納されるユーザー・データ量の 1 ヶ月あたりの増加量

比較法で使用可能な情報の種類は多岐にわたるが、次の方針で収集すべき情報を決定することが望ましいと考えられる。

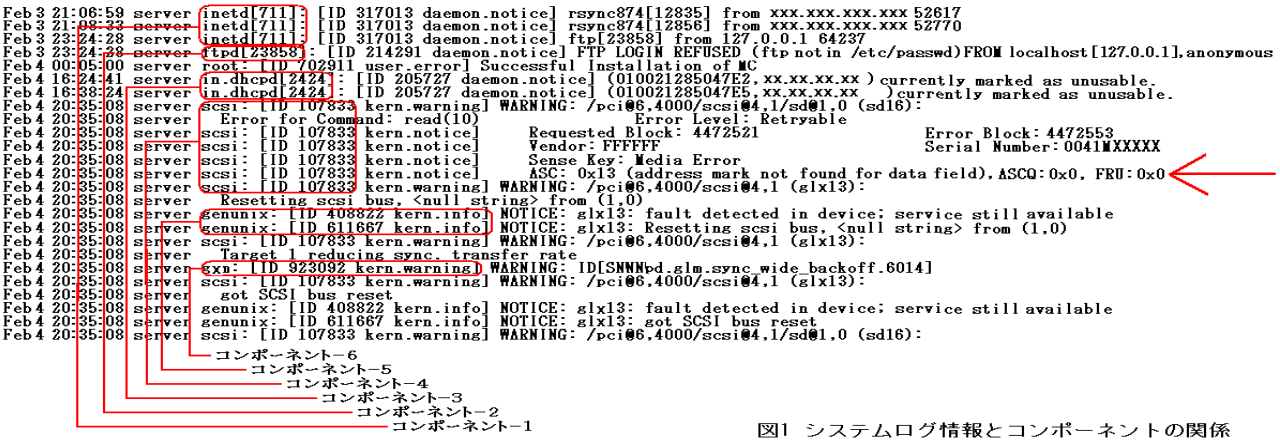

図1 システムログ情報とコンポーネントの関係

[1] 対象システムの使用目的に注目する（前出: C, E, F)
[2] 対象システムで使用されているコンポーネントの特徴に注目する(前出: A, B, D)

これらの情報は個別に収集されるため、機能線上のコンポーネント構成とは一致していない。ＯＳのログ・メッセージを例とすれば、これは複数コンポーネントから個別に報告された情報が報告された順序に記録されているだけであり、各コンポーネント間の相関情報、因果関係の情報等は含まれていない。このため収集された情報を比較法で使用するには、個々の情報がどのコンポーネントに対応するかを分別し、コンポーネント毎に時系列に再配置する作業が必要となる。図１はあるＯＳのシステムログに記録された情報が、どのコンポーネントに対応しているかを示した例である。

２－３．比較法での留意点

比較法では次の２点に留意をする必要がある。

[1] 時差修正の必要性

各コンポーネントから個別に収集した情報には記載時刻に相対的な時差を含んでいることが殆どである。例えばサーバー本体に外部接続されたディスク装置などはそれ自体にサーバー本体とは独立した時計を内蔵している。このためこの外部接続機器の情報はサーバー側にインストールされたソフトウェアを用いて採取されるが、そこに記録されている時刻は外部機器内蔵のものであり、サーバー本体の時計を基準に採取された他の情報とは時差が生じる。このような理由から機能線全体での基準時刻を定め時差を修正する作業が必要である。更に事象が発生した実時刻とそれが記録されるまでに要した時間にも注意を要する。また事象が何秒かに渡って継続するものである場合には、ログに記録される時刻はその開始時刻か、終了時刻のどちらかが考えられる。このような挙動は正常稼動時に採取した情報を事前に分析しておくことで把握可能である。

[2] 調査対象の障害に関連しないエラー記録

あるコンポーネント内で検出された障害発生記録が調査対象の障害と関連していないことがある。これは収集された情報が調査対象の障害が発生した時刻の前後まで網羅しているためである。経験的には前出[1]の時差修正が完了しているならば、長時間に渡り同じ障害での事象が繰り返し記録されている場合の除き、対象障害の発生時刻の前後数分より離れた時刻のエラー記録は調査対象外と判断できることが多い。

付記：事前情報収集の有用性

比較法で使用することを目的に事前収集された情報は、発生した障害への対策に利用できることがある。例えば障害の影響で設定・構成情報などが消失した場合に、これを修復するために事前収集情報を利用することがある。このことは比較法の本質とは無関係であるが、オープン・システムでの障害調査・対策実施の過程では有益である。

２－４．比較法の実例

システムが正常に稼働している記録に障害に関連したメッセージが記録されている実例を図２に示す。図中で①,②はシステム正常稼働に伴い定期的に記録される情報、③は障害を記録している部分である。

図2 通常稼働記録と障害記録

３．機能線による障害の分類

障害発生コンポーネントの特定が完了した機能線を分類することを考える。分類の結果、各障害の型はそれぞれに固有の障害対策に関連付けられる。提案する分類はそれぞれが異なった対策方法に繋がる。障害は以下の３種の型に分類できると考えられる：

- 3-1 通常型
- 3-2 両端決定不可型
- 3-3 タイムアウト階層違反型

3-1. 通常型

通常型では障害発生コンポーネントが機能線上に唯一存在している。最も一般的な障害の形態であると考えられる。

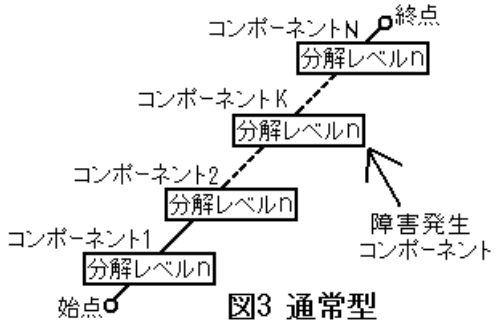

図3 通常型

3-2. 両端決定不可型

両端決定不可型では図４のように被疑部位が隣接する２つのコンポーネントにまで絞り込まれているが、そのどちらで障害が発生したかを決定できない。

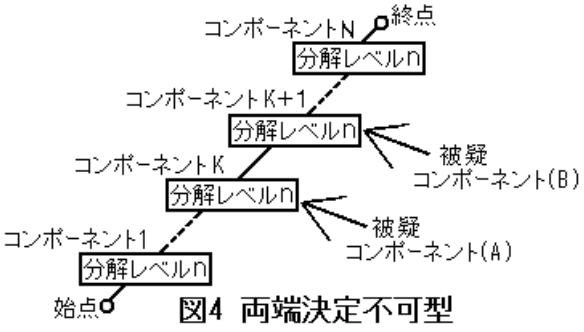

図4 両端決定不可型

図 4 で被疑コンポーネント(A)と(B)はともに障害発生原因の可能性があるが、実際にどちらで障害が発生したかを判定することができない。
また機能線の性質から、この型は分解レベルが低い際には 3-1 の通常型であるが、被疑コンポーネントの分解レベルをあげると両端決定不可型となる場合があることに注意を要する。分解レベルの高低差による通常型と両端決定不可型の関係の実例を挙げる。

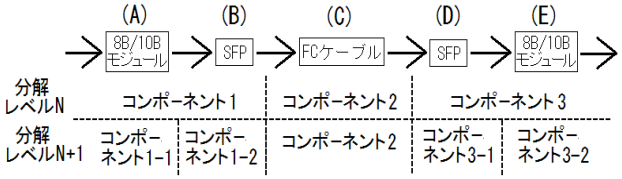

図5 両端決定不可型と分解レベルの関係

図 5 は Fibre Channel の Node 間通信部分の機能線である。ここでコンポーネント 3 がビット受信エラーを検出したと仮定する。このエラーが記録される可能性は分解レベルが N の場合には以下の 3 通りが考えられる：
（Ⅰ）コンポーネント 1 の送信に問題がある
（Ⅱ）コンポーネント 2 を通過中にビットが反転した
（Ⅲ）コンポーネント 3 の受信に問題がある
ここで調査の結果(Ⅲ)が発生したと仮定する。するとこの障害は 3-1 通常型に分類される。しかしながら、分解レベルを N+1 に上げると、コンポーネント 3 は隣接する 2 つの被疑コンポーネント 3-1 と 3-2 になる。しかしながら一般的に使用されている Fibre Channel 製品の仕様では 3-1 と 3-2 のどちらで障害が発生したかを確定する情報を得ることができない。すなわち両端決定不可型は製品仕様の制約のため被疑コンポーネントを唯一に絞り込めない状態であるといえる。

3-3. タイムアウト階層違反型

タイムアウト階層違反型は通常型で障害発生部位を特定後、そのコンポーネントの分解レベルを上げ被疑部位を更に絞り込む調査を行うと障害発生の痕跡を持つコンポーネントが発見できない状態である(図 6)。このような状態となる原因は 2 つ考えられるが、ここでは B のみを対象とする。
A：分解レベルが高い状態のコンポーネントから情報が誤っている
B：分解レベルの低い状態での障害発生コンポーネントと判定された部位が自発的にタイムアウト障害を作り出している

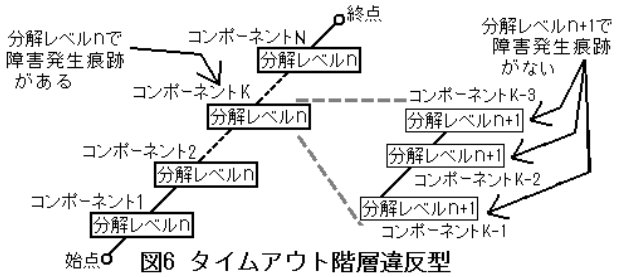

図6 タイムアウト階層違反型

この型の障害は発動点と階層違反をしているコンポーネントとが一致していることが多い。

4．各障害型への対策投入方法

各障害型はそれぞれに対応した対策投入方法に関連付けができる。つまり機能線による障害発生コンポーネントの特定後は各型に対応した対策投入法が一意に決定される。

4-1. 通常型への対策投入

通常型の場合には障害が発生したコンポーネントにのみ対策を投入する。

4-2. 両端決定不可型への対策投入

両端決定不可型の場合は、対策投入を一回で完了させるには隣接コンポーネント双方を対象にする必要がある(同時投入)。どちらのコンポーネントで障害が発生したかを特定する必要がある場合には、一方のコンポーネントのみに対策を投入しその後の効果を見極める過程を経る必要がある(順次投入)。このときの対策投入は一回で 1 箇所のみの変更を実施するよう注意する(1 手順-1 変更の原則)。図 5 を例にすれば左側の(A)から(E)の方向へ順次対策を投入する。この原則は DOA(交換後の部品での障害発生)検知を容易にする効果がある。また DOA は交換前の部品で発生していた障害と異なる障害をあらたに発生させることがあり、両端決定不可型の障害対策実施をより困難にする要因の一つとなっている。一方で両端決定不可型ではないと誤認識した状況で部品交換を実施すると DOA を誤検出することがある。両端決定不可型と DOA の関係はオープン・システムの障害対策投入時の問題点の特徴の一つといえる。

4-3. タイムアウト階層違反型への対策投入

タイムアウト階層違反型への対策投入法は 3 通りが考えられる。
[1] 階層違反をしているコンポーネント自体に対策を投入する。一般的には階層違反の論理部分を修正することとなる。
[2] 階層違反をしているコンポーネントがエラー発生元と報告しているコンポーネントに対策を投入する
[3] [1],[2]双方のコンポーネントに対策を投入する
この型への対策投入時にも 1 手順-1 変更の原則を考慮することが望ましい。

5．まとめ

オープン・システム内で発生した障害が機能線で記述されているときに、この機能線上の各コンポーネント内で障害が発生したかを判断する方法として比較法を提案した。これはシステム正常稼動時に事前収集された情報を障害発生後の情報と比較し、通常時には記録されない情報を障害発生の痕跡であるとして注目する。また比較法に用いる目的で事前収集されていた情報は、設定・構成情報が破壊、消失された障害への対策にも利用できる。
更に機能線を用いることにより障害を 3 種類の型に分類することを提案した。またそれぞれの障害型には固有の対策投入法が関連付けられることを示した。障害原因調査は機能線を用いることにより決まった手順で一意に対策投入方法まで辿り着くことができる。

[参考文献]
[1] 篠原昭夫、泉隆：「オープン・システム上での障害発生部位特定方法の提案」 情報処理学会第 75 回全国大会，5A-2(2013-03)