L-015

監視経路の冗長性に基づく障害原因箇所推定手法の提案

A Method to Estimate the Failure based on Redundancy of Monitoring Networks

川岸 諒子†　　魚住 光成†
Ryoko Kawagishi　　Mitsunari Uozumi

1．はじめに

情報システムの安定稼働を実現するためには、情報システムを構成するネットワークやサーバ等の稼働状況を常に監視し、障害発生時における障害原因の調査・復旧を迅速に実施する必要がある。

情報システムの監視では、監視対象機器の異常検知を知らせるアラームが監視者へ通知され、監視者により、ネットワーク構成図等を元にした障害原因箇所の調査、障害原因の特定、障害の復旧作業が実施される。情報システムを構成するネットワークの複雑化に伴い、障害原因箇所の調査にかかる時間は増加している[1]。

本稿では、Ping による死活監視でアラームが通知された場合に、優先的に調査すべき箇所を推定する手法について述べる。本手法を用いることにより、これまで監視者が実施していた調査の優先度が低い箇所に対する調査時間が削減され、調査を効率的に実施出来るようになる。調査時間が短縮されることにより、現状よりも更に短時間で障害復旧までを行うことが可能となる。

2．監視業務の現状

監視装置よりアラームが通知されると、監視者は、ネットワーク構成図等を元に、障害原因箇所の調査、障害原因の特定、障害の復旧作業を実施する。

アラーム発生時には迅速な対応が求められるため、ネットワークやサーバ等の情報システムの構成情報を管理しておく必要がある。IT サービスマネジメントのベストプラクティスをまとめた書籍である ITIL（Information Technology Infrastructure Library）においても、構成管理データベース（CMDB：Configuration Management Database）による構成管理を推奨している[2]。現状では、構成情報は、CMDB、一覧表、ネットワーク構成図等の様々な方法や形式によって保存されており、これらの情報を元に、障害原因箇所の調査等が行われている。

監視には、システムやサービスが適切に稼働しているかどうかを監視する死活監視と、OS やハードウェアのリソース利用状況を監視するリソース監視の大きく 2 種類がある。監視の目的や監視対象機器に応じた監視が行われるわけだが、Ping を用いた死活監視は導入が容易であり、多くの企業、システムにおいて利用されている。

Ping 監視は手軽である半面、異常が発生した場合に提供される情報が少なく、障害原因が監視対象機器であるか、監視装置から監視対象機器までの監視経路であるか、調査を行わないと分からない。ここで言う監視経路とは、監視装置から監視対象機器までの間に存在するルータやスイッチ等の通信を中継する装置を指す。

† 三菱電機株式会社 情報技術総合研究所, Mitsubishi Electric Corporation, Information Technology R&D Center

3．Ping 監視における課題

監視経路の信頼性は、監視対象機器と比べ、必ずしも高いわけではない。そのため、Ping 監視でアラームが発生した場合、監視対象機器だけでなく監視経路に対しても調査を行う必要がある。

監視が単純なネットワーク構成で行われている場合、監視者は、ネットワーク構成図や経験等から、監視対象機器と監視経路のどちらから調査すべきかを判断することが出来るかもしれない。しかし、複雑なネットワーク構成の場合や監視者の経験が浅い場合、どのような順序で調査したら良いかを判断することは難しい。監視者が調査の順序を間違えた場合、障害原因である可能性が低い箇所に対する調査も実施することとなり、障害原因箇所の調査に時間がかかってしまう。

迅速な障害復旧を行う上で、監視者が実施してしまう不要な調査時間を削減することが課題となっている。

4．解決策

監視装置から監視対象機器までの監視経路の冗長化有無を元に、障害原因が監視対象機器である尤もらしさを表わす尤度を算出し、アラームと共に監視者へ通知することによって課題の解決を図る。これにより、監視者は、優先的に調査すべき箇所を把握でき、優先度の低い箇所に対する不要な調査時間の削減が可能となる。

監視経路の冗長化有無について、図 1 の例で説明する。（1）が冗長化無、（2）が冗長化有の監視経路である。（1）では監視装置から監視対象機器までの監視経路が 1 種類であるのに対し、（2）ではルータ 1 を通る経路とルータ 2 を通る経路の 2 種類の監視経路が存在する。ここでは、監視経路の中継装置が全て冗長化している場合を、監視経路が冗長化されていると言うこととする。

（2）のように監視経路が冗長化されている場合、監視経路の信頼性は（1）に比べて向上している。（2）において監視経路が障害原因であるためには、冗長化された監視経路で共に障害が発生している必要がある。

監視経路の冗長化有無は、監視経路に関する構成情報を管理し、それを元に判定を行う。

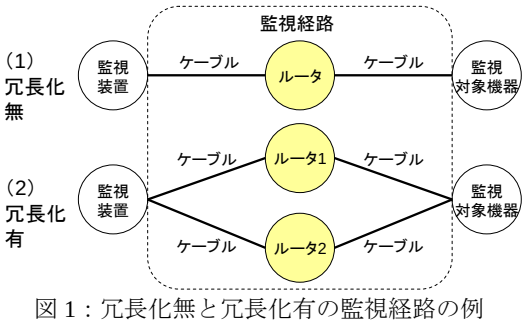

図 1：冗長化無と冗長化有の監視経路の例

4. 1. 監視経路の構成情報

監視経路の構成情報を利用することにより、監視経路の冗長化有無の判定を実現する。判定に利用する情報は、次の 2 種類である。

- 監視経路情報
- 監視経路の中継装置の状態情報

監視経路情報は、監視装置から監視対象機器までの監視経路の種類を表わす情報であり、監視経路の中継装置の状態情報は、ルータ等の中継装置が工事等により稼働停止しているかどうかを表わす情報である。

図 2 に示した監視経路に関する監視経路情報と状態情報の例を図 3、図 4 に示す。これは、監視経路が全 8 種類、中継装置 4 が稼働停止している状態の例である。

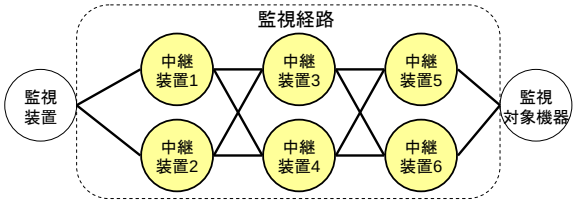

図 2：監視経路の例

1	監視装置→中継装置1→中継装置3→中継装置5→監視対象機器
2	監視装置→中継装置1→中継装置3→中継装置6→監視対象機器
3	監視装置→中継装置2→中継装置3→中継装置5→監視対象機器
4	監視装置→中継装置2→中継装置3→中継装置6→監視対象機器
5	監視装置→中継装置1→中継装置4→中継装置5→監視対象機器
6	監視装置→中継装置1→中継装置4→中継装置6→監視対象機器
7	監視装置→中継装置2→中継装置4→中継装置5→監視対象機器
8	監視装置→中継装置2→中継装置4→中継装置6→監視対象機器

図 3：監視経路情報

監視経路の中継装置	状態
中継装置1	稼働中
中継装置2	稼働中
中継装置3	稼働中
中継装置4	稼働停止
中継装置5	稼働中
中継装置6	稼働中

図 4：監視経路の中継装置の状態情報

4. 2. 監視経路に対する冗長化有無の判定

監視装置よりアラーム通知された場合に、4.1.節で説明した構成情報を利用して、監視経路の冗長化有無の判定を実行する。判定の流れを以下に示す。

- アラームを通知した監視装置からアラームが発生したとされる監視対象装置までの監視経路の構成情報（監視経路情報、監視経路の中継装置の状態情報）を参照
- 状態情報より、現在稼働停止している中継装置の有無を確認
- 稼働停止している中継装置がある場合、監視経路情報より、稼働停止している中継装置を含まない監視経路（利用可能な監視経路）を抽出
- 抽出した監視経路に含まれる各中継装置の出現回数を数え、抽出した監視経路数と比較、冗長化有無を判定

図 2～4 の例の場合、図 4 より中継装置 4 が稼働停止であるため、図 3 の監視経路のうち利用可能な経路は 1～4 の 4 種類となる。この中で、各中継装置の出現回数を数えると、中継装置 3 が 4 回、それ以外は 2 回である。中継装置 3 の出現回数 4 回は、利用可能な監視経路数と同じであり、つまり、冗長化されていないことが分かる。この例では、障害原因箇所は、冗長化されていない中継装置 3、または、監視対象機器である可能性が高い。

4. 3. 監視対象機器に対する尤度の算出

前節の判定より、冗長化されていない中継装置の個数が判明する。図 2～4 の例では、中継装置 3 の 1 個である。この数を利用して監視対象機器が障害原因である場合の尤度の算出を行う。尤度算出の流れを以下に示す。

- 冗長化されていない中継装置の数を算出
- 以下の式により、監視対象機器が障害原因である可能性を示す尤度を算出
  - ➢ 1／（N＋1） N：冗長化無の中継装置数

例えば、冗長化されていない中継装置数 N＝0 の場合、監視対象機器が障害原因である場合の尤度は 1.0、N＝1 の場合の尤度は 0.5 となる。図 2～4 の例では 0.5 である。

以上より、構成情報を用いた監視経路の冗長化有無の判定と監視対象機器に対する尤度の算出により、障害原因とその可能性を推定することが可能である。

4. 4. システム構成例

システム構成例を以下に示す。本提案は、アラームと共に障害原因である場合の尤度を合わせて通知する機能であるため、既存の統合監視システム等に追加または連携する形で実装することが可能である。

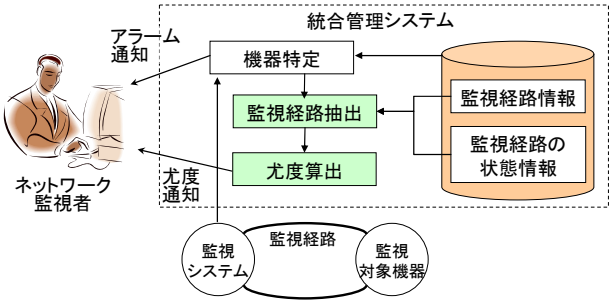

図 5：システム構成例

5. おわりに

本提案により、監視経路の冗長化有無を元に推定された調査すべき箇所とその尤度が監視者へ通知される。これにより、監視者は、通知された尤度を元に調査箇所と優先度を把握することができ、効率的な調査を実施することが可能となる。特に、ネットワーク構成が複雑な場合や経験の浅い監視者の場合において、調査時間の短縮効果が期待出来る。

本提案は Ping 監視を前提とした手法であった。今後は、Ping 以外の監視についても取り組んでいく予定である。

6. 参考文献

[1]紅林輝他, 知識ベースに基づくネットワークトラブルシューティングの自動化, IC2010

[2] ITIL サービストランジション,
Office of Government Commerce, The Stationery Office, 2008