4A-06

社会インフラシステムにおける稼働情報を用いた障害原因調査ツールの提案

山形　知行† 但馬　慶行‡ 益子　英昭† 武澤　隆之† 入江　直彦†

株式会社　日立製作所　インフラシステム社†

株式会社　日立製作所　横浜研究所‡

１．概要

社会インフラ向け制御システム(以下、インフラ制御システム)は様々なセンサー・コントローラや制御用計算機を組み合わせて構成されるシステムであり、十年単位の長期運用が行われる。この間に、他システムとの連携、システム適用範囲の拡大等、様々な使用環境の変化を伴い、初期に想定していない使用方法による障害が運用開始後に起こることが多い。また、リアルタイム性が求められる分野のため、非同期・割込処理があり、障害の調査手法も独特である。

本研究は、複数のサブシステムからなるインフラ制御システムにおいて、障害原因の特定を容易にすることを目指している。発生している事象を時系列で俯瞰するツールにより障害原因特定の時間短縮を実現した。また、障害解析時に専門家の分析方法を蓄積することで、特定分野の専門家に依存しがちな障害分析ノウハウを共有できる見込みを得た。

２．目的

インフラ制御システムは鉄道運行管理、電力系統制御、上下水管理といった分野に適用され、図１のような構成となっている。本研究では、個々の制御用計算機で記録される既存のログを活用し、システム障害の原因箇所特定を容易にすることを目的とする。近年、センサー等のハードウェアからの統計情報を使用した障害原因の予防保全サービス[1]や、fluentd[2]のようにシステムのログを収集管理するツール、ログを統計的に可視化するツール[3]等が情報通信系の分野を中心に開発されている。一方、インフラ制御システムでは、例えば進路制御・ダイヤ管理・保守運用管理といった複数のサブシステムを組み合わせた構成をとるため、各サブシステムの専門家がログを分析し、結果を持ち寄って合同で原因調査することも少なくなかった。しかし、事象の全体像をとらえて根本原因にフォーカスすることは容易ではなく、また、原因調査は専門家の知識に頼ることが多いという問題があった。本稿では、まず障害の全体像を俯瞰するためにログを可視化する方法を説明する。次に、可視化したログの専門家による分析方法(ノウハウ)を他の調査者に共有するための仕組みを説明する。

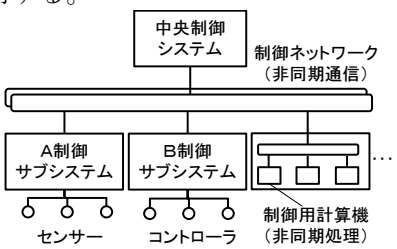

図１．社会インフラ向け制御システムの構成

３．稼働情報集約・連携の手法

インフラ制御システムでは、それぞれの機器が受けた要求内容・処理過程・応答結果等の稼働情報を時系列のログとして記録している。一方、これらのログはサブシステムや機能の特性に応じて独自の形式で記録されてきた。本稿では、異なるログを共通で俯瞰できるようにするための稼働情報の収集・整理方法と可視化方法を述べる。

３．１．稼働情報の収集・整理

異なるログを収集するためには、ログやそのレコード項目が分類され、値の意味が時系列で整理されている必要がある。本ツールでは、図２のようにツリーによる項目分類を行った。また、ログデータは共通の時間軸とログ分類軸を持ち、その値はログに特定のキーワードが含まれるかどうかといったインデックス値を用いた。

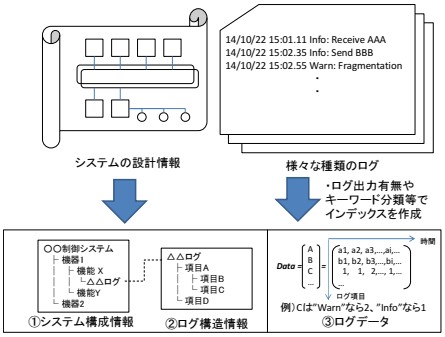

図２．異なるログの統合手法

３．２．稼働情報の可視化

障害は、エラー表示のような表面的な障害事象と根本原因が異なることが多々ある。このた

The Proposal of a Failure Analysis Tool for Social Infrastructure System based on Middleware Journals

† Infrastructure Systems Company, Hitachi, Ltd.

‡Yokohama Research Laboratory, Hitachi, Ltd.

め、調査の際は一旦システム全体で起こっている事象を俯瞰したうえで、フォルトツリー解析のように想定原因に至る複数の経路を掘り下げる。本ツールでは、時間の粒度・表示する項目の取捨選択・ログデータの値に対する表示色(以下、分析フィルタ)をインタラクティブに設定できるインターフェースとし(図３)、システム全体の俯瞰から個別原因の掘り下げまでを効率良く行えるようにした。

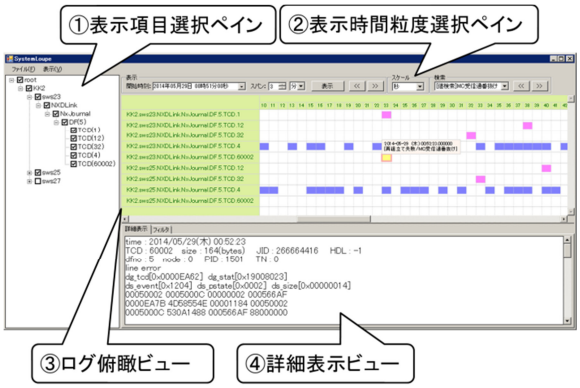

図３．障害原因調査ツールのインターフェース

４．障害分析ノウハウ共有の手法

障害の原因調査に専門家の設計知識や経験は欠かせないが、長期運用での属人性を下げるためにも、非専門家が調査できるようにしたいというニーズがある。本稿では、専門家の調査手法をツールに蓄積し、非専門家をガイドする手法について述べる。

４．１．分析ノウハウの蓄積・整理

専門家による障害原因調査では、根本原因を探す際に使う分析フィルタを定型化できることが分かった。このため、まずこの定型的な分析フィルタを記録しておける仕組みを用意した。次に、専門家がどのような分析フィルタを使いながら調査を行ったか自動で記録する仕組み(以下、操作履歴)により、専門家の調査過程を再現できるようにした。

しかし、操作履歴による画面の再現は非専門家が見ても理解が難しい。これは、専門家の操作目的(どのような事象の発生有無を確かめようとしたか)が分からないためである。このため、本ツールでは、操作履歴に対して後から調査事象や見分け方を記載してノウハウＤＢとして保存できるようにした(図４)。

４．２．分析ノウハウによるガイド

保存されたノウハウＤＢを非専門家があらかじめ全て学習するのは現実的ではない。本ツールでは、調査事象のキーワードで調査項目を検索できるようにした。また、事象の見分け方はチェックリスト形式で表示し、非専門家が事象を見落とさないよう工夫した。これにより、非専門家であってもチェックリストと再現画面を参考にしながら、解析対象の実ログを調べることが可能となった(図４)。

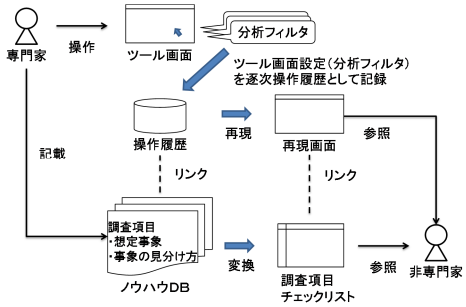

図４．分析ノウハウ蓄積とガイドの流れ

５．実験・結果

制御ネットワーク輻輳障害の過去事例を題材に解析の被験者実験を行った。対象の制御システムは、制御用計算機・表示装置等が 10 台以上で構成されるシステムであり、各々の装置で毎分数百件の通信ログが出力される。可視化の効果は専門家 1 人で、ノウハウ共有の効果は当該システムの開発に携わっていないソフト開発者 5 人で評価した。

表１　稼働情報可視化による専門家の解析時間

	専門家手作業	専門家分析ﾂｰﾙ使用
解析時間	2 時間	10 分

表２　分析ノウハウ共有による障害原因正答率

	１回目の回答	２回目の回答
非専門家正答率	40%	80%

６．考察

ネットワークトラブルは関連する機器が多く、事象の全体像を把握するのに時間を要していた。本ツールで全体像を俯瞰することにより、最初に問題が起こった箇所を容易に特定でき、調査時間の短縮に繋がった。

また、障害分析ノウハウの共有では、分野が異なる開発者であっても数回の試行で原因にたどり着くことが分かった。

７．まとめ

本稿では、複数のログを横断的に調査することによる障害原因調査の効率化と、分析ノウハウの共有方法について述べた。今後は、類似障害事象の自動検索等についても検討していく。

参考文献など

[1] 森津 他，社会インフラの持続的な提供を支える O&M サービス，日立評論 2013/04 pp. 34-37
[2]fluentd: An open source data collector http://www.fluentd.org/
[3]Kibana:visualize logs and time-stamped data http://www.elasticsearch.org/overview/kibana/