



LS研総合発表会 2017

2017年6月8日(木)、東京・台場にあるグランドニッコー東京 台場にて、LS研総合発表会が開催されました。このイベントは、LS研活動の柱である「研究分科会活動」の1年の成果を、会員企業の皆様や有識者の方々と情報共有する場として毎年行われています。本年も2016年度に活動した17テーマの研究分科会について多彩な成果発表が行われました。

LS研幹事長ご挨拶

株式会社日本アクセス
占部 真純 氏



皆様こんばんは。本日は一日お疲れ様でした。私はLS研の第18代幹事長を仰せつかりました、株式会社日本アクセスの占部と申します。

2016年の研究分科会活動では、17の分科会が成立し、本日3つの会場に分かれて研究成果を発表いただきました。一年間の研究活動と論文作成、そして発表用の資料作成と大変だったと思います。私は第2会場で6編の発表を聞かせていただきましたが、いずれも3月初旬の論文提出後、今日まで入念に準備いただいたことがわかる発表内容でした。

1978年にLS研究委員会が発足されて以来、研究分科会はLS研のコアな活動として、39年間毎年実施されてまいりました。2017年度もすでに16のテーマで研究分科会活動がスタートしております。

先程の特別講演の加来先生のお話で、

私が持っていた歴史観は見事に否定されてしまいました。しかし、LS研が持つ39年間の活動の歴史は嘘つきませんし、これからもこの歴史を積み重ねていくことが、非常に大事なことと考えます。我々幹事一同も、そのお手伝いをしていくことで、会員の皆様の相互交流を拓けていくことを願っております。

あらためまして、2016年度のメンバーの方々、お疲れ様でした。また、2017年度のメンバーの方々、今日ご覧になったように、来年は皆様が一年間の研究成果をこの場で発表いただく主役でございますので、しっかり頑張ってください。

最後にFUJITSUファミリー会LS研究委員会のますますの発展を祈念いたしまして、私の挨拶とさせていただきます。

懇親パーティー



職場の違う仲間たちとの異業種交流・共同研究。一年を通じた活動成果をたたえあう姿は、みな晴れ晴れとしていた

特別講演



題目：「歴史に学び、大局観を養う」興味深い内容と快活なお話しぶりに、魅せられる会場



加来 耕三氏
『歴史研究』編集委員
内外情勢調査会講師
地方行財政調査会講師

研究成果審査 受賞分科会

LS研幹事による審査では、先見性／独創性／有用性などを評価基準に、5編が選出されました。また各会場の審査委員により、会場ごとに発表賞が選出されました。

報告書審査



優秀賞

Leading-edge Systems 研究

継続的システム開発におけるテスト効率化手法の研究



最優秀賞

Leading-edge Systems 研究

運用ログを活用した
アノマリ事象の検知と活用に関する研究



業務システム運用改善のための実態調査手法の研究



研究賞

Leading-edge Systems 研究

コンテナ技術を利用したPaaS向けプラットフォームの適用に関する研究



機械学習を中心とした人工知能および関連技術の活用法の研究



発表審査



発表賞

機械学習を中心とした人工知能
および関連技術の活用法の研究



業務システム運用改善のための
実態調査手法の研究



コンテナ技術を利用したPaaS向け
プラットフォームの適用に関する研究



最優秀賞受賞分科会 研究概要

Leading-edge Systems 研究



運用ログを活用した アノマリ事象の検知と 活用に関する研究

—障害予兆検知への活用—



1 背景

近年、AIやビッグデータ解析技術の発展に伴い、アノマリ(いつもと違う状態)による障害予兆検知が可能な環境は整いつつある。セキュリティ分野においては、不正侵入検知・防御を行うIDSやIPSの予兆検知システムの実用化が進んでいる。一方、システム運用の分野では、運用ログを用いた障害予兆検知への活用は進んでいない。システムの重要性が増すにつれ、障害予兆検知へのニーズが高まっているにも関わらず、システム運用の現場でアノマリ検知が進まない要因を、普及の観点から以下の3点が不足しているためだと考えた。

(1) 「わかりやすさ」

アノマリ検知を行う上で、統計学などの専門的な知識が必要とされている点。

(2) 「可視性」

事例が少なく、効果が不明確な点。

(3) 「試用可能性」

商用サービス利用も含めアノマリ検知を行うためには専門知識を持った人材のサポートが必要となり、試用のハードルが高い点。

2 目的

普及を妨げている要因に対して解決策を導き出し、システム運用の現場で運用ログを活用したアノマリ検知の導入ハードルを下げる必要があると考えた。具体的には、以下の3点を研究対象とした。

(1) 統計学などの専門知識を必要としない手順の確立。

(2) アノマリ検知による障害予兆検知を実証することで効果を明確化。

(3) 低コストで試用可能な条件の整備。

上記を解決し、「明日から使える(始められる)障害予兆検知」の成果を得ることを目的とした。

3 アプローチ

障害予兆検知の成功事例として生産設備の故障予兆検知を、データマイニングの標準プロセスであるCRISP-DMにあてはめ分析を行い、主に以下の2点を課題として設定し対策を行った。

(1) データの理解

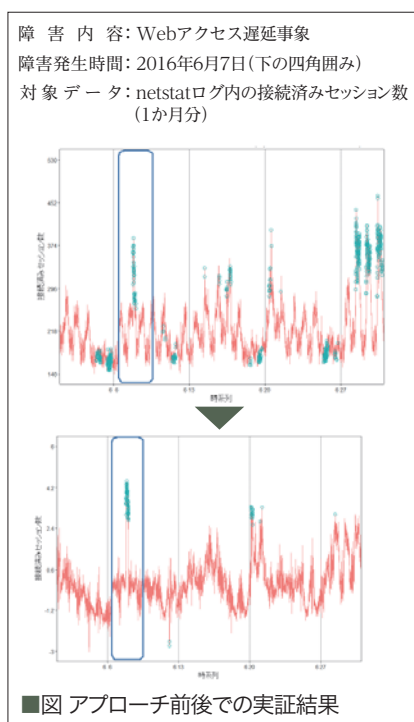
運用ログは、分析対象のログを選択することが重要なのは勿論のこと、そのデータの特徴を把握することが重要かつ難しい課題である。対象のシステムを熟知した管理者しか把握出来ない状態では、普及するはずがない。本分科会では、データの特徴の中で特に周期性に着目し、運用ログから機械的に検出する方法を独自に考案した。

(2) データの加工・準備

単純にデータを表形式や数値化するだけでは、満足な結果は得られない。同じ数値であっても、時間帯によって異常とみなされる場合や、みなされない場合があるからである。これを解決するために、本分科会では、周期性を考慮しつつデータを正規化する方法を考案した。

4 実証結果

実際に発生した以下の障害に対して、本分科会で考案したアプローチを施す前後で検証した。



アノマリ事象検知には、無償で公開されているTwitter, Inc製Anomaly Detection(統計用言語Rで動作)を利用し、評価基準は検知時刻と偽陽性率(過剰検知の少なさ)とした。検知は図の丸印で表記。

(1) 検知時刻:

実際の検知時刻よりも加工前で36分前、加工後で31分前に検知(5分遅延)。

(2) 偽陽性率:

加工前6.9%から加工後0.7%(6.2ポイント改善)。

わずかながら検知時刻は遅れたものの、大幅に誤った検知が削減され、加工による有用性を立証した。

5 成果

本分科会の成果として、アノマリ検知技術による障害予兆検知の導入ハードルを下げるために、下記の解決案を示した。

(1) 既存ツールの問題点を改善する手法を考案し、利用方法と合わせて整理・体系化した。

(2) 体系化した方法論を活用ツール(プログラム及びマニュアル)として整理した。

上記活用ツールは、既存ツールにおいて普及の妨げとなっていた以下の点で優れている。

(ア)「わかりやすさ」

具体的な考え方と手順を含む内容となっているため、障害予兆を検知するにあたり、専門的な知識を必要としない。

(イ)「可視性」

実際の運用ログを用いた実証を行い、実運用に耐えうる精度の確保、及び従来の検知時刻よりも早期の障害検知に成功した。

(ウ)「試用可能性」

全て無償のソフトウェアにて構成しており、誰でも試用することが可能である。

以上より、システム運用の現場で「明日から使える(始められる)障害予兆検知」を実現するための環境を整備出来たと考える。

今後は、この成果を各社で活用して頂き、更なる事例・手法を公開することで、アノマリ検知による障害予兆検知の精度向上と普及を期待したい。

代表者コメント

1回目の分科会では、メンバーそろって、アノマリ検知は難しい、普及していないという思いからのスタートでした。そこで生まれたキーワードが、「明日から始めるアノマリ検知」。このキーワードを念頭にメンバー一丸となって、調査・検証を進め、障害予兆検知を始めるための成果と素晴らしい経験を得ることができました。



内田 洋平 氏
 ヤマトシステム開発株式会社