**利用者名：コンピュータサイエンス学部　教授　串田 高幸**

Scopus

**Title:** Reduction of Redundant Alerts by Relationship Discovery Based on Port Usage
（ポートの使用状況に基づいて接続関係の検出による冗長アラートの削減）
**Authors:** Manato Hirao, Tomoyuki Koyama, Takayuki Kushida
（平尾　真斗(東京工科大　大学院生)、小山　智之(東京工科大学　大学院生)、串田　高幸(東京工科大学　教授)）
**Journal:** Lecture Notes in Networks and Systems Volume 1493 (2026) pp. 501-511
**掲載年月：**2026 年 1 月

**研究概要：**
一般にクライアントサーバモデルでおこった障害は，サーバ障害がクライアントまで波及する．例えば，NFS のサーバとクライアントが使用されているシステムにおいて，NFS サーバのファイルシステムの使用率が 80%を超えたら，同じように NF クライアントの使用率も 80%を超える．例えば，NFS サーバとクライアントを用いたシステムにおいて，サーバ上のファイルシステムの使用率が 80%を超えると，クライアント上のファイルシステムの使用率も 80%に達する．NFS サーバとクライアントの両方のファイルシステムの使用率が監視されているとき，これらの両方からアラートが同時に送られる．この例では，アラート送信時に障害箇所と影響を受けていない箇所の両方が含まれることになる．そのため，アラートに対処するエンジニアは，複数のアラートからシステム障害の根本原因に関連するアラートを特定することに時間がかかる．この論文では，サーバとクライアントのソフトウェアの接続関係を解析することによって，システム障害の根本原因に関連するアラートだけにして，アラートの数を削減するアルゴリズムを提案している．
提案アルゴリズムは，各ソフトウェアで確立済みになった接続に関する重みを計算する．これらの各ソフトウェアの重みのなかで最も高い重みをもっている接続関係にだけをアラートとする．それ以外の接続関係は，アラートにしないことによってアラートの数を削減する．実験では，NFS サーバとクライアントと RKE2 を使用した Kubernetes クラスタを使って，実際に起こった障害を再現して提案を評価した．評価として，Alertmanager を使用した場合と Alertmanager と提案手法を組み合わせた場合のアラート数をそれぞれ比較した．結果は，NFS サーバおよびクライアントの障害では，Alertmanager を用いて 4 件のアラートが送信されて，また組み合わせ方式を用いて 1 件のアラートが送信された．また，RKE2 クラスタの障害では，Alertmanager を用いて 3 件のアラートが送信されて，組み合わせ方式を用いて 1 件のアラートが送信された．この実験結果から，提案手法は冗長なアラートを削減して障害箇所のみのアラートを送信された．これらの評価結果から提案手法では，原因箇所のアラートだけを生成することができ，またアラートの数を削減することができることを示した．

**研究背景：**
IT システムにおいて，システム管理の研究開発は，他の分野に比べて新技術の採用が遅い．そのため，多くの場合はエンジニアの経験とスキルに頼って行われているのが現状である．IT システムで起こっている障害では，迅速に原因個所を発見して，障害を復旧させる必要がある．障害が起こった時に IT システムでは，複数のアラートが同時が発生する．このとき，複数のアラートのアラートのうち，どのアラートが，障害の原因究明に最も関係があるかの調査が必要となる．この調査には，IT システムの障害に関する経験とスキルがあるエンジニアが対応する必要があり，時間と労力がかかっている．

**研究成果：**
この研究の成果は，提案方法の IT システムの接続関係を使うことによって，障害でおこった複数のアラートのうち，原因箇所のみのアラートだけを通知する方法が有効であることを評価実験から検証できたことである．

**社会への影響：**
一般的に使われている IT システムのアラート機能に，この提案方法のソフトウェアを組み込むことによって，今まで経験とスキルがあるエンジニアが対応しなければならなかった原因箇所の特定を，自動的に行うことができるようになる．この結果，IT システムのシステム管理の自動化と省力化への貢献することができる．

**専門用語：**

**アラート**：IT システムに異常があるとき，監視システムによって自動的に生成されてエンジニアにチケットとして送られる．

**NFS**：ネットワークファイルシステムのこと．ローカルエリアネットワークを介して，複数のクライアントがサーバのファイルシステム共有するための技術のことである．

**Kurbernetes**： コンテナのデプロイを管理するための方式の一般的な名前である．

**RKE**: Kubernetes を実現しているオープンソースソフトウェアの名前である．

**Alertmanager**: アラートを管理するオープンソースソフトウェアの名前である．