

≪「報告書詳細版」は巻末の付録USBメモリに収録しています≫

第9部

クラウドコンピューティング基盤の構築と運用(概要版)

浅井 大史、小林 諭、島 慶一、関谷 勇司

第1章 はじめに

WIDEクラウドワーキンググループは、今後のクラウド技術の研究開発を推進するために2010年1月に設立された。複数のWIDE組織間に渡って運用される広域連邦型クラウドシステムであるWIDEクラウドシステムの運用と、それをういた研究開発を行っている。

2015年度は、仮想計算機監視の策定及びシステムログ解析技術の研究開発を実施した。

第2章 仮想計算機監視MIB策定

大規模な基盤システムを運用するには、整備された監視の仕組みが必要となる。仮想計算機の数が増加していく環境において、多数の仮想計算機の状態を外部の管理ドメインから把握することは重要であるが、現状において、統一した監視手法が確立されているとは言い難い。

WIDEクラウドワーキンググループでは、自身で仮想計算機基盤を運用した経験からこの問題に注目し、仮想計算機の監視に必要な要素の洗い出しと、それらの情報をやりとりするための標準化された手段が必要であると考えた。本活動は2012年のIETFでの提案を発端とし、同時期に提案されていた他のグループからの類似提案を統合しつつ、WIDEプロジェクト主導により2015年10月にRFC7666[52]として発行に漕ぎ着けたことにより完了した。

第3章 システムログ解析技術

WIDEクラウドワーキンググループでは小林の手法[53]を元にしたシステムログ解析技術の研究を実施している。本研究で言及するシステムログとは、UNIX系システムで利用されているsyslog(3)ライブラリを用いて出力されるテキスト文字列を指す。ただし、解析手法はログ出力ライブラリの実装方法とは独立しているため、記録された文字列がsyslog(3)ライブラリから出力されるものと類似していれば、任意のシステムで出力されたログを汎用的に取り扱うことが可能である。

システムログは自由形式で記述されたテキストデータであり、その処理にはある種の言語解析的な手法が必要となる。その代わりに、もともとログに含められていた意味、ログを出力するタイミングが、あらかじめプログラマによって意図的に調整されているといった点から、異常事態の意味を取り出すことが可能ではないかと考えている。今後は、より正確なログメッセージの分類手法を確立していく。また、ログメッセージの分類には大きな計算負荷がかかることも分かっており、リアルタイムでの運用を目指した分散処理システムなどへの適用も検討していく。

異常検知には様々な手法が考えられ、今回はログメッセージの出現間隔やログメッセージ間の因果関係を利用した。より正確な異常判定のため、今後も様々な手法を検討していく。

第4章 まとめ

今年度は仮想計算機監視MIBの標準化と、システムログを用いた異常検知手法の研究開発を実施した。MIBに関しては、今後は実装の拡充及び将来に向けた改定を検討していく。システムログ解析については、基礎技術の確立を継続するとともに、データセットの拡充、高速・リアルタイム処理のための技術開発などを進め、他の異常検知手法との比較などによる提案技術の有用性の検証を続けていく。