氏　　名	菊池　慎司		
学位の種類	博士(情報科学)		
学位記番号	博情第 288 号		
学位授与年月日	平成 25 年 12 月 20 日		
論文題目	Improving Reliability in Management of Cloud Computing Infrastructure by Formal Methods (クラウドインフラ運用管理における信頼性向上のための、形式的検証手法の適用)		
論文審査委員	主査　平石　邦彦	北陸先端科学技術大学院大学	教授
	小川　瑞史	同	教授
	緒方　和博	同	准教授
	青木　利晃	同	准教授
	石川　冬樹	国立情報学研究所	准教授

論文の内容の要旨

本研究の目的は、クラウドコンピューティングシステムのような情報システムの運用管理に対して、形式的検証技術を適用することにより、サービスの信頼性の評価や信頼性の向上を実現する手法を開発することである。

情報システムにおける障害の多くはシステム運用上の設定誤りや操作誤り等の人為ミスが原因となっているため、それらを防ぐことがシステム信頼性向上の急務である。そのような人為ミスのうち、本研究においては、運用管理において遵守すべき制約の見落としに属するものを対象とし、それらを防ぐことでシステム運用管理の信頼性向上を実現する技術を開発する。制約の種類としては、(1)「ある物理サーバ上で稼働している仮想マシンのリソース量は、物理サーバのキャパシティを超えない」等のシステム構成変更時の制約や、(2)「システムに single point of failure となる構成要素がない」等のシステムの構成上の脆弱性に関する制約の 2 種類を検討対象とする。システムの挙動を網羅的かつ効率的に分析可能な形式的検証技術を活用することにより、これらの制約の充足可能性の機械的な分析が可能になれば、その分析結果をシステム管理者にフィードバックし、システム管理における重要な制約の見落としを抑止することで、システム運用管理の信頼性向上に貢献できると考えられる。

本論文においては、システム運用管理の信頼性向上のために、形式手法を用いた以下の 2 つのアプローチを提案し、それぞれについて評価を行った結果について述べる。

(1) システム変更プロセスの自動合成

モデル合成手法を用いた、システム構成変更における変更プロセス合成手法を提案する。宣言的に記述された制約(要件) を満たしたプロセスを自動的に構築することにより、システム変更における制約見落としに起因する障害発生を抑止する。

(2) システム構成に潜む脆弱性の特定

モデル検査手法を用いて、システムの構成や、システムに与える変更操作がシステムの構成上の脆弱性(single point of failure 等) に与える影響 (ある操作が single point of failure を発生させうるか等) を評価する手法を提案する。構成や変更操作に潜むリスクを認識することで、サービス障害の発生を未然に抑止するのに貢献する。

論文審査の結果の要旨

本論文はクラウドシステムの運用管理における信頼性向上を目的として、形式手法に基づいた手法を提案したものである。近年、多くの情報システムやサービスがクラウドコンピューティングにより実装されるようになってきた。クラウドシステムにおける障害発生の多くはシステム運用上の設定誤りや操作ミスなど人為的要因がほとんどであり、実際、人為ミスがシステムの停止やデータ損失につながった事例が報告されている。本論文は、クラウドシステムの運用管理において遵守すべき制約の見落としに関する人為ミスを対象とし、それらを防ぐことでシステム運用管理の信頼性を向上させることを目的としている。そのための方法として形式手法を用いた以下の２つのアプローチを提案し、それぞれについて実システムを想定した例題に適用して解析および評価を行っている。

(1) システム変更プロセスの自動合成：クラウドシステムの構成（コンフィグレーション）変更時における変更プロセスを自動的に合成する手法を提案した。宣言的に記述されたシステム構成に関する制約を満たすような操作プロセスを自動的に合成することにより、システム変更における制約見落としに起因する障害発生を抑止することが可能になる。具体的には、変更前後のシステム構成および変更ルールを形式手法のツールである Alloy Analyzer 上で記述し、変更手順を自動的に求める方法を提案した。さらに、変更後のシステム構成に関する要件を分割し，それらをサブゴールに設定することで、メモリ使用量を低減することのできる新しい探索手法を開発した。

(2) システム構成に潜む脆弱性の特定：モデル検査手法を用いて、システムの構成や、システムに与える変更操作がシステムの構成上の脆弱性（single point of failure 等）に与える影響を評価する手法を提案した。この手法は、システムの構成や変更操作に伴う潜在的リスクを顕在化させることで、サービス障害の発生を未然に抑止することに貢献する。具体的にはシステム構成、変更規則、障害の発生等をモデル検査ツールの NuSMV 上で記述し、時相論理式の形で与えられたシステムの脆弱性を検証する方法を提案した。

上記の手法は, プライベートクラウドなど比較的小規模のクラウドシステムには十分適用可能であると判断できる．しかしながら，パブリッククラウドなど大規模なクラウドシステムへの提案手法の適用については未検討であり，今後の課題として残されている．クラウドシステムの運用管理, 特にシステム構成に関する様々な要件の網羅的な分析を形式手法により行う手法を提案したことは本論文の重要な貢献であり，今後の研究の発展が期待される。

以上、本論文はクラウドシステムの運用管理に形式手法を導入し、実際のシステムを想定した例題に提案手法を適用することでその有効性を確認したもので、学術的ならびに実システムの信頼性向上にも貢献するところが大きい。よって、博士（情報科学）の学位論文として十分価値あるものと認めた。