修士学位論文要約（平成31年３月）

ネットワーク運用支援のためのエージェント型情報提供機構に関する研究

松村　洋志
指導教員：木下 哲男，　学位論文指導教員：北形 元

Agent-based Data Provisioning Mechanism for Supporting Network and System Management

Hiroshi MATSUMURA
Supervisor: Tetsuo KINOSHITA,　Research Advisor: Gen KITAGATA

Processing network data is a useful manner for network and system administration tasks and various systems for processing data are provided in recent years. However, because the tools have a wider variety and complicated configurations, it is not easy for unprofessional administrators who manage home and office networks to appropriately utilize them. Furthermore, the growing complexity of network structures requires the administrators to introduce advanced analytics, and as a result, it increases the burden of unprofessional ones. To solve the problem, we propose a method to deliver the network data by using software agents with meta-level knowledge of the data processing tools to select the tools and to organize autonomously.

1. 序論

コンピュータ技術の発達に伴い，大量のデータを蓄積，処理して興味深い特徴やパターンを抽出する研究が様々行われてきている．ネットワークやシステム管理の分野においても，トラフィックログやシステムログ，機器の計算リソースなどのネットワークデータを分析して，ネットワークやシステムの異常を検知する手法などが提案されている [1)2)]．これに対して近年では，データの収集・蓄積・処理に特化したデータ処理ツールが提供されてきており，これらのツールを用いて，より高度なネットワーク管理の実現が期待できる．

その一方で，ツールによって扱えるデータや実行可能な処理に限りがあり，また，ツールごとに仕様が異なるという課題がある．このため管理者には，目的や場面に応じて適当なツールを選択する負担や，高度な処理のために複数のツールを組み合わせる負担などがかかる．また高度なネットワーク管理のために，管理者はデータ分析に関する専門知識を学ぶ負担もかかる．データの分析に基づく高度なネットワーク管理をより広く普及させるためには，管理者にかかる上記の負担を軽減する技術の開発が必要不可欠であると考える．

そこで本研究では，管理者が確認したい情報に対して，必要なデータ処理ツールが連携してデータを処理し，その結果を管理者に提供する，エージェント型情報提供機構を提案する．本機構により，ツールに関する知識やスキルを持たない利用者でもネットワークデータを処理し，その結果を確認することが可能となる．

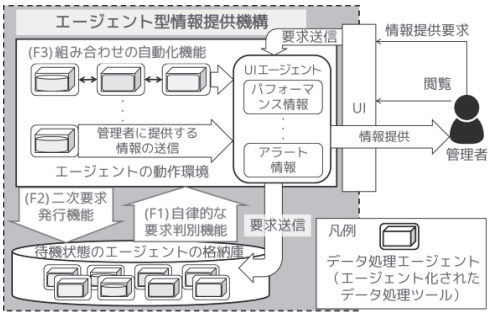

図１　エージェント型情報提供機構

2. エージェント型情報提供機構

本研究では管理者がデータ処理ツールを利用する負担を軽減するために，ツールにエージェントとしての機能を付与し（エージェント化），自身が保持するデータや実行可能な処理に関する知識と，知識を基に自律的に動作・連携する機能を与える．提案機構はツールをエージェント化したデータ処理エージェントと UI エージェントから構成され，図１にその概要を示す．

データ処理ツールをエージェント化する際には，(F1)自律的な要求判別機能，(F2)二次要求発行機能，(F3)組み合わせの自動化機能の ３ つの機能を付与する．(F1)の機能では，エージェントの格納庫内に配置されているデータ処理エージェントが，管理者や他エージェントから要求を受け取った際に，自身が保持する知識を基にその要求に対応できるかどうかの判別を行う．対応できると判別した場合には，エージェントの動作環境で動作するエージェントを生成する．(F2)の機能では，動作環境上で動作しているデータ処理エージェ

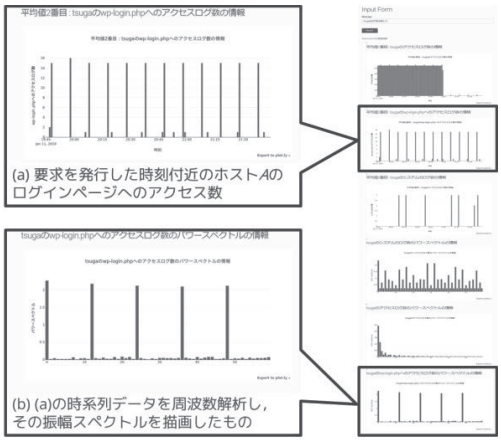

図 2　事例 4 における試作システムの出力例

ントが，データの分析や可視化処理などの追加の処理を実行したり，管理者に追加の情報を提供したりするために，格納庫内の他エージェントを動作環境へ呼び出すことを行う．(F3)の機能では，(F1)，(F2)の機能によって動作環境に生成された複数のデータ処理エージェント間で連携するためのメッセージ交換を行い，データの送受信の設定や，処理を実行するタイミングなどを制御している．この機能によって，一つのデータに対して複数の分析や可視化処理を並列に実行することが可能となる．

3. 試作システムの実装と実験

本機構の有用性を検証するために，本機構に基づく試作システムを実装し，システムを用いた動作実験を行った．本研究では試作システムとして 5 種類のデータ処理ツールを用意し，8 種類のデータ処理エージェントと 1 種類の UI エージェント，ブラウザ上で試作システムの処理結果を表示する UI 提供サーバを実装した．

動作実験では，ネットワーク管理における状況の確認作業の事例を 5 つ取り上げ，それらの事例において管理者の要求に対して試作システムが提供する情報を確認した．事例の 1 つである，周期性を持つブルートフォース攻撃が発生しているときに，試作システムに「ホスト A のログを分析して」という要求を発行したときのシステムの出力結果を図 2 に示す．図 2 の出力結果では，ログインページへのアクセス数を棒グラフに描画した情報(a)と，(a)の情報を周波数変換し，その振幅スペクトルを描画した情報(b)などが提供され，試作システムが管理者の要求に関連するデータを分析，可視化して提供できることが確認できた．また，(a)の情報からログインページへ度々多くのアクセスがあることが確認でき，(b)の情報からログインページのアクセス数に周期性があることが確認できる．(a)，(b)の情報を併せて提供することによって，「ログインページへ定期的に多くのアクセスがある」ことが確認でき，これらから周期性を持つブルートフォース攻撃が行われていたと推察できると考えられる．

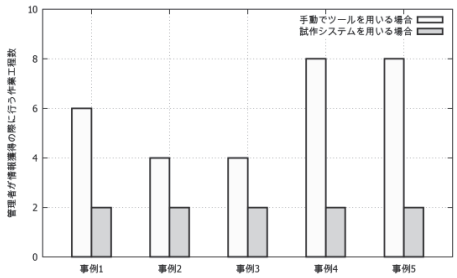

図 3　試作システムを用いる場合と用いない場合の作業工程数

また，管理者が情報を獲得する際に必要な作業工程を，試作システムを用いる場合と用いない場合で列挙した．各事例においての作業工程の数をまとめたものを図 3 に示す．図 3 から，試作システムを用いることによって，用いない場合と比べて平均して約 63.3%の作業工程数を削減することが確認できた．これらから，試作システムを用いることで，より少ない作業負担で，ネットワーク状況の理解につながる分析・可視化されたデータを確認することが可能となり，本機構の有用性が示された．

4. 結論

本研究では，データ分析に基づく高度なネットワーク管理支援の実現を目指して，エージェント型情報提供機構を提案した．また，提案を基に複数のデータ処理ツールをエージェント化し，ネットワーク管理における 5 つの事例を取り上げて動作実験を行った．実験結果から，各事例において試作システムがデータを取得，分析，可視化することでネットワークの状況理解に役立つ様々な情報を提供可能であることを確認した．また試作システムを利用する場合と手動でツールを利用する場合とを比較して，より少ない作業工程での情報収集が可能となることを確認した．

文献

1) I. Cohen, M. Goldszmidt, T. Kelly, J. Symons, J.S. Chase, “Correlating instrumentation data to system state: A building block for automated diagnosis and control,” USENIX AssociationOSDI’04:6th Symposium on Operating Systems Design and Implementation, pp. 231-244, 2004.
2) T. Kimura, K. Takeshita, T. Toyono, M. Yokota, K. Nishimatsu, and T. Mori, “Network Failure Detection and Diagnosis by Analyzing Syslog and SNS Data: Applying Big Data Analysis to Network Operations,” NTT Technical Review, Vol. 11, No. 11, 2013.