Vol.2009-DPS-141 No.27
Vol.2009-GN-73 No.27
Vol.2009-EIP-46 No.27
2009/11/27

ネットワークトラヒック分析支援エージェントによる能動的異常検知

三杉大輔[†]　高橋優介[†]　笹井一人[††]
佐藤彰洋[†]　北形　元[††]　木下哲男[†††]

異常検知手法に基づくネットワークトラヒック分析機構は，統計量を扱うため対象とする情報が少ないが，解析時に高度かつ専門的な知識や管理者の経験が必要であり，実際にはこれらの負担が大きな問題となる．そこで本研究ではネットワークトラヒック分析機構の運用・管理を代行するエージェントと分析機構の連携による，能動的な異常検知の手法を提案する．本稿では分析支援エージェントの設計と実装について述べ，その評価を行う．

An Active Anomaly Detection based on a Support Agent of Network Traffic Analysis

Daisuke Misugi[†]　Yusuke Takahashi[†]　Kazuto Sasai[††]
Akihiro Satoh[†]　Gen Kitagata[††]　and　Tetsuo Kinoshita[†††]

The network traffic analysis mechanism based on anomaly detection method has little information because of treating a statistic. However altitude and technical knowledge and the experience of the manager are necessary and actually these burdens become a big problem at the time of analysis. Therefore we let an agent which acts for management of the network traffic analysis mechanism cooperate with analysis mechanism in this study and suggest technique of active anomaly detection. In this paper, we show a design and the implementation of the analysis support agent and perform the evaluation.

1. はじめに

近年，インターネットは www や E-mail，オンラインショッピングなど様々な形で利用されるようになり，その普及と利用者の増加に伴い人々の社会生活に欠かせない重要なインフラとなっている．しかし，インターネットにはネットワークを介して蔓延するコンピュータウィルスやワームの感染，Denial of Service 攻撃，不正侵入の前兆を示すスキャンなど，脅威となる様々なインシデントが存在し，日増しに増加している．そのため，ネットワーク管理の重要性が高まっており，ネットワークの安全で安定した運用が求められている．ネットワーク管理者はネットワーク状態を適切に把握し，インシデントを効果的に検知することが重要である．

インシデントの検知方法として，ネットワークの通常状態を統計的手法によってモデル表現し，そのモデルからの逸脱の程度を定量的に評価する異常検知手法が存在する．未知のインシデントの検知が可能である異常検知手法は，多数の研究が行われている1-2)．

異常検知手法は統計的手法によってモデル表現するため，ネットワーク構成やネットワーク環境の変化が検知精度に与える影響は大きい．しかし，実環境でのネットワーク構成やネットワーク環境の変化が考慮されていない．高精度なインシデントの検知を維持するために，ネットワーク管理者が定期的にネットワーク構成やネットワーク状態の情報を収集し，知識・経験に基づいた運用が必要で大きな負担となる．また，運用プロセスの一部しか自動化されていない．そのため，導入にあたり動作用件を策定し，ネットワーク構成やネットワーク状態にあわせた調整，そして検知結果から原因の特定・対処までの一連のプロセスの大部分をネットワーク管理者が手動で行わなければならず，その運用が大きな負担となる．特にパラメータの更新・変更といった調整や，原因の特定・評価はネットワーク管理者に大きな負担がかかるという問題が存在する．つまり運用する際に高度かつ専門的な知識やネットワーク管理者の経験が必要になる．

そこで，本研究では異常検知手法を運用する際の問題を解決するため，能動的情報資源（Active Information Resource：AIR 3)）の概念に基づくネットワーク管理者の知識や経験を予め埋め込んだエージェントを提案する．異常検知手法の運用・管理を代行するエージェントが自律的に異常検知手法と連携することで能動的な異常検知を実現し，ネットワーク管理者の知識や経験に基づいた運用の自動化を目指す．

[†]東北大学大学院情報科学研究科
Graduate School of Information Sciences，Tohoku University
[††]東北大学電気通信研究所
Research Institute of Electrical Communication，Tohoku University
[†††]東北大学サイバーサイエンスセンター
Cyberscience Center，Tohoku University

Vol.2009-DPS-141 No.27
Vol.2009-GN-73 No.27
Vol.2009-EIP-46 No.27
2009/11/27

以下，2 章では関連研究として不正検知手法と異常検知手法について説明し，異常検知手法の問題点について述べる．3 章では AIR の概念に基づいたエージェントを提案し，4 章では提案するエージェントの設計と実装について述べる．最後に 5 章でまとめと今後の予定について述べる．

2. 関連研究とその問題点

ネットワークを監視してインシデントを検知する方法は数多くの研究が行われている．それらは，アルゴリズムの違いから不正検知（ミスユース）と異常検知（アノマリ）に大別することができる4)．不正検知は実環境で適用され既に製品化された例が多いが，異常検知の場合は実環境における動作がまだ考慮されておらず，製品化された例が少ない．そこで本研究では異常検知を対象とする．本章では不正検知と異常検知について説明し，異常検知における問題点について述べる．

2.1 不正検知

不正検知とは，予めインシデントの振舞いをシグネチャとして保持し，実際のネットワークの振舞いをシグネチャとマッチングすることでインシデントを検知する方法である．代表的な例にログを入力情報とする Swatch5）と，パケットを入力情報とする Snort6）があげられる．

不正検知はファイアウォールと一緒にパケットを入力情報とした侵入検知システム（Intrusion Detection System：IDS）として実装される場合が多い．入力情報をリアルタイムでシグネチャと比較するためリアルタイム性を有するが，シグネチャ数やトラヒック量が増加するとパケットのフィルタリング処理やデータ解析，シグネチャとのマッチングを逐次処理で行わなければならないため，処理が追いつかなくなり処理能力が落ちるという問題点が存在する7-8)．また，シグネチャに存在しない未知のインシデントを検知することができず，日々出現する新種や亜種のインシデントに対応することが困難である．そのため，不正検知手法の運用にはシグネチャを常に最新の状態に保つことが重要であり，そのメンテナンスの方法として文献9）が存在する．

2.2 異常検知

異常検知とは，ネットワークの通常状態を統計的手法によりモデルとして表現し，そのモデルからの逸脱の程度を定量的に評価する．そして閾値を設け，通常状態から逸脱した場合に通常とは異なる振舞いとして検知する方法である．

不正検知はインシデントの数だけシグネチャを用意する必要が存在するが，異常検知は統計量を扱うため不正検知に比べて情報量が少なくてすむ．また，検知の際にインシデントに関するシグネチャを用意する必要がないため，シグネチャに特徴の明記が困難なインシデントや新種や亜種のインシデントを検知することが可能である．一方，統計的手法を用いた計算にはある程度の期間観測する必要があり，観測点を通過してから異常を検知するまでにタイムラグが生じるためリアルタイムな検知が困難である．

異常検知は，インシデントだけでなくネットワーク機器の不調やサーバ自体のダウンなどの障害による異常も検知できる可能性があるために，ネットワーク管理において重要な技術として注目されている．ネットワークが複雑化したりサービスが多様化しても評価する統計情報は変化しないため，異常検知手法はその有効性が期待されている．

異常検知は，多くの場合トラヒックを観測する観測部，観測したトラヒックを通常状態へと統計的手法によって定量的な形式に変換する抽出部，抽出された特徴量と通常状態として定義したモデルとの逸脱の程度から評価を行う算出部の 3 種類の要素にわけることができる10)．特に通常状態のモデルは最も重要な構成要素のため，目的に即したモデルを設計する必要がある．

観測方式により，一定の時間間隔でトラヒックの流量をカウントするタイムスロット型，複数のパケットをフローと呼ばれる処理単位で抽出するフロー型，一部のパケットのみをサンプリングして処理をするサンプリング型に分類される．また，通常状態のモデル化には，発生頻度によるものや多変量解析（主成分分析・ベイジアンネットワーク・クラスタリング・自己相似性など）によるものが存在する．さらに，異常検知を段階的に組み合わせた研究11）や，並列的に組み合わせた研究12)，不正検知と異常検知を組み合わせた研究など，複数の検知手法を用いることで精度の向上を目指す研究も数多く行われている．

2.3 異常検知における問題点

異常検知手法は実環境における動作が考慮されていないという問題点が存在する．そのため，運用時に高度かつ専門的な知識やネットワーク管理者の経験が必要であり，ネットワーク管理者にとってその運用が大きな負担となる．ネットワーク管理者の運用プロセスを図 1 に示す．まず動作用件などを策定し手法を導入するプロセス，導入した手法を実際に動かしインシデントの検知を行い，ネットワーク構成やネットワーク状態などから必要に応じて更新や変更といった調整を行う動作に関するプロセス，そして検知結果からログやパケット情報などを確認し評価・特定を行う評価に関するプロセスから構成され，原因が特定した後に対処に移る．しかし，異常検知手法はデータ処理のプログラムが逐次的で何度も動かす必要があり，この運用プロセスのうち動作に関するプロセスの一部（統計的手法に基づいて異常を検知）しか行われないため，それ以外のプロセスについてはネットワーク管理者が手動で行わなければならない．高精度なインシデントの検知を維持するためには，ネットワーク構成やネットワーク状態の情報を定期的に収集し，ネットワーク管理者の知識や経験に基づいた運用が必要となり大きな負担となる．ネットワーク構成やネットワークから計測したネットワーク状態の情報を可視化する手法が提案されている13-14）が，これらの手法は可

Vol.2009-DPS-141 No.27
Vol.2009-GN-73 No.27
Vol.2009-EIP-46 No.27
2009/11/27

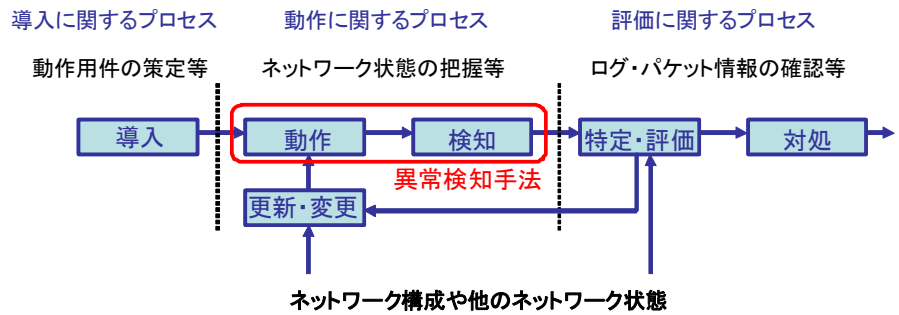

図 1　ネットワーク管理者の運用プロセス

視化する手法であり，異常検知手法におけるネットワーク管理者の負担を直接軽減する手法ではない．ネットワーク構成やネットワーク状態の情報を把握する際の負担は軽減可能であるが，ネットワーク管理者の知識や経験に基づいた運用は必要であり，ネットワーク管理者の負担は十分に軽減できていない．

このように，異常検知手法の運用にはネットワーク管理者の負担が大きいといった問題点が存在する．問題点の解決のためには，ネットワーク構成やネットワーク状態の情報の収集やネットワーク管理者の知識や経験に基づいた更新・変更といった調整などのプロセスの自動化が必要である．中でもパラメータ設定などの調整に関わる更新・変更や，異常原因を特定する特定・評価のプロセスは，ネットワーク管理者の負担が特に大きい．

まず，異常検知手法は統計的手法に基づいた処理を行っている．そのためパラメータ設定が検知精度に与える影響が大きい．その上，ネットワークトラヒックは時間的にも空間的にも大きく変動するため，適切なパラメータを前もって設定することが困難である15)．不適切なパラメータを設定すると精度が大きく低下するため，実世界で異常検知を適用するためには，適切なパラメータ設定が重要である．パラメータの決定には学習が必要であるが，学習期間が短いと十分なデータが得られず，長いとネットワークトラヒックの大局的変化に追従できないというトレード・オフが存在する．動的なパラメータ設定など適切なパラメータ設定に関する研究が行われているが，それらの研究では CPU やメモリといったリソース制約のない理想的な環境の場合が多く，実環境で処理速度がどのように変化するか考慮されていない場合が多い．実際に運用する上ではマシンのスペックや他のサービスの稼働状況などにより動作環境は常に変動するため利用可能なリソース量も変動する．リソースに制約が存在するため，理想的な環境を想定したパラメータでは，処理負荷が大きく検知システムとして継続的に動作できない可能性が存在する．そのため，検知システムが止まらないよう使用

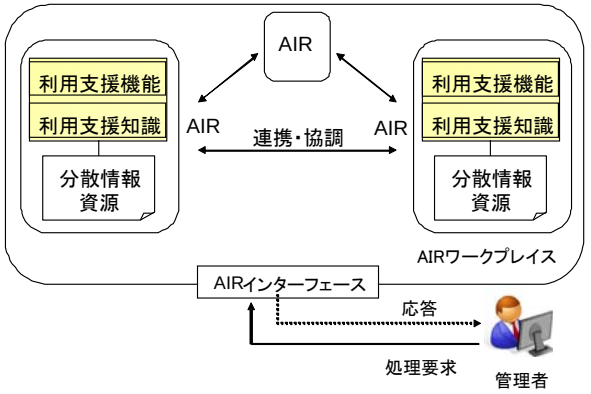

図 2　AIR の概念構成図

可能なリソース量を把握しその範囲の中で最適なパラメータに設定する必要があるため，ネットワーク管理者に大きな負担がかかる．

次に，異常検知手法は通常と異なる振舞いを異常と定義するため，異常原因の特定が困難である．異常と判断された場合，それがインシデントによるものか判断が検知結果からだけでは推測が困難である．未知のインシデントが検知できるが，異常原因の特定に時間を要してしまう．手法により扱う統計量が違うため手法毎に検知されやすい異常，検知されにくい異常が存在する．そこで，複数の手法を組み合わせれば精度の向上と異常原因の絞込みが可能になると考えられる．しかし，文献 12）では 1 段階目で異常か通常と判断されると次の段階に進まず懐疑と定義された場合のみ次の段階に進む．文献 13）では複数の手法のうち 1 つの手法で異常と判断された場合も，全ての手法で異常と判断された場合でも同じ異常と定義されてしまう．本来は違う種類の異常が同じ異常と定義されてしまう可能性が存在する．そのため，異なる特徴量に基づく複数の手法を組み合わせて検知結果の組み合わせに応じて状態を把握する必要があり16)，それぞれの手法に意味を持たせることが重要である．実際に運用する上では，ネットワーク管理者が統計的手法や検知結果の特徴を把握し，さらにパケットやログ情報などから経験に基づいて異常原因を判断しなければならない．頻繁に異常が検知されると，その都度原因の調査が必要であるためネットワーク管理者に大きな負担がかかる．

そこで本研究では，異常検知手法における運用面の問題を解決するため，AIR の概念に基づきネットワーク管理者の知識や経験を予め埋め込んだエージェントを提案する．異常検知手法の運用・管理を代行するエージェントを異常検知手法と連携することで能動的な異常検知を目指す．

Vol.2009-DPS-141 No.27
Vol.2009-GN-73 No.27
Vol.2009-EIP-46 No.27
2009/11/27

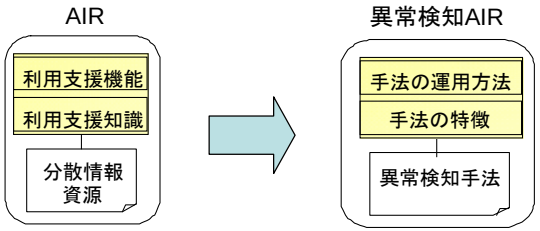

図 3　異常検知手法の AIR 化

3. 異常検知手法の AIR 化

本研究では，管理者の負担が大きいという異常検知手法の運用上の問題を解決するため，AIR の概念に基づきネットワーク管理者の知識や経験を予め埋め込む異常検知手法の AIR 化を提案する．

AIR 化によりネットワーク管理者の行う知的な部分を AIR が代行するため，異常検知手法自体の可用性を向上する．異常検知手法の運用・管理を代行するエージェントを異常検知手法と連携することで能動的な異常検知を実現し，ネットワーク管理者の知識や経験に基づいた運用の自動化が可能になると考えられる．

3.1 AIR

AIR とは，情報資源に利用支援知識と利用支援機能を持たせることで，情報資源を利用する際に必要な煩雑な作業を情報資源自身に行わせる手法である．利用支援知識とは情報資源の内容を有効的に活用するための用法に関する知識であり，利用支援機能とは情報資源を加工し利用の手助けをする機能である．利用支援知識や利用支援機能は情報資源に付加するエージェントやマルチエージェントとして構成･実装される．こうした機能的な強化・拡張に基づく分散情報資源の構造化を AIR 化と呼ぶ．AIR の概念構成図を図 2 に示す．

情報資源を AIR 化することにより，それらの情報資源を利用する際の手間を削減し，利用者の支援を行うことが可能となる．これにより，情報資源自体が能動性・自律性を持つことになり，AIR 同士がお互いに協調・連携することで，複雑・柔軟な処理を能動的・自律的に代行したりすることが可能になる．

3.2 異常検知手法の AIR 化

異常検知手法の AIR 化は，異常検知手法を情報資源としてベースプロセスで実行し，手法の特徴や運用方法，運用に必要なネットワーク管理者の知識や経験，即ち，

（1）異常検知手法を導入する場合に必要な知識
（2）異常検知手法が動作している場合の調整に必要な知識
（3）異常検知手法を評価する場合に必要な知識

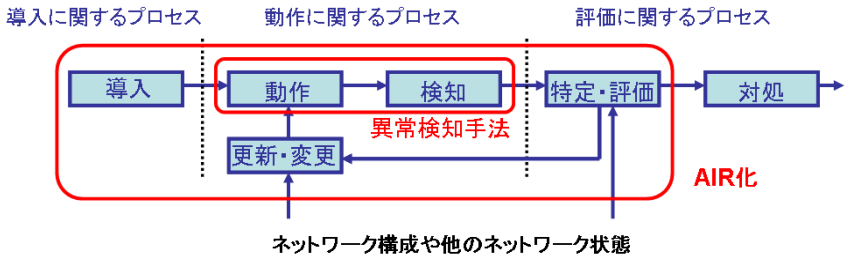

図 4　ネットワーク管理者の運用プロセス（AIR 化）

をルール型の利用支援知識とそれによって作動する利用支援機能に埋め込むことを意味する．図 3 に異常検知手法を AIR 化した様子を示す．従来の異常検知手法では統計的手法に基づいて検知を行う動作と検知の部分しか自動的に行えなかったが，AIR 化することで，その前後の導入に関するプロセスや動作に関するプロセスの調整，さらに評価に関するプロセスにおいても AIR が代行してくれる．つまり，ネットワーク管理者の知識や経験に基づいた運用の自動化が可能になり，それによってネットワーク管理者の負担軽減が可能になると考えられる．図 4 に AIR 化された異常検知手法のネットワーク管理者の運用プロセスを示す．（1）に関して，ネットワーク管理者がその異常検知手法に関する詳細な分析や結果予測を行わなくても，対象とするネットワークへ容易に適応することが可能になると考えられる．（2）に関して，ネットワーク構成やネットワーク状態の情報から，環境の変化に対応した調整が可能になると考えられる．（3）に関して，検知結果とネットワーク構成とネットワーク状態から，異常原因の絞込みも可能になると考えられる．異常検知手法の AIR 化の実現に関して，本稿では，まずルール型の利用支援知識を作成するため，（1）から（3）のそれぞれの運用プロセスに関するモデルを構築する．

3.3 運用プロセスのモデル化

異常検知手法の導入には，最初に（a）に関して分析を行い把握する必要があり，更に監視目的に適した（b）に関する調整を行わなければならない．動作中の異常検知手法においては，常に（c）と（d）の評価を行う．そして，現在の環境に適した（b）を再調整する．評価に関しては，まず（c）と（e）を把握し，そこから（f）を判断する．（f）の結果より（g）が判断可能である．適用する環境により手法が適切かどうか大きく分かれるために，常に（h）を評価する必要がある．この（h）といった（i）を把握することで，現在の環境に適した（b）を再調整する．

提案した AIR を実装するための設計として，下記のモデルから得られた（a）から（i）を，AIR の構成要素であるルール型の利用支援知識と，それによって作動する利用支援機能に分配して，知識を異常検知手法に埋め込む．

Vol.2009-DPS-141 No.27
Vol.2009-GN-73 No.27
Vol.2009-EIP-46 No.27
2009/11/27

(a)　動作用件，入力・出力の情報，検知結果の特徴
(b)　監視場所・監視対象，データの保持期間，パラメータ，通常状態，異常を判定する閾値
(c)　ネットワーク構成，ネットワーク状態
(d)　計算時間，CPU 使用率，メモリ使用量
(e)　ログやパケットの情報
(f)　異常の発生箇所，異常の原因
(g)　インシデントか否か
(h)　false positive，false negative
(i)　評価情報

4. 提案した AIR の設計と実装

3 章の（1）から（3）についてそれぞれ AIR 化による動作例を示した．中でも更新・変更や特定・評価については 2 章で述べたようにネットワーク管理者の負担が大きいといった問題点が存在する．そこで 4 章では更新・変更について AIR 化の設計について述べる．なお，AIR 化する異常検知手法については，文献 1）の手法を用いる．

4.1 相関関係に基づく異常検知手法

文献 1）の手法は，トラヒックの任意の 2 種の特徴量間の相関係数の算出し，その発生確率をヒストグラム化した相関係数ヒストグラムを通常状態として用いる．相関係数の算出は，複数の連続したスロットからなるウインドウ毎に全特徴量の組合せで行う．検知の際も全組合せの相関係数を同様に求め，通常状態の相関係数ヒストグラムと比較し，求めた相関係数の発生確率が閾値以下となる組合せが一定数以上ある場合に異常と判断する．図 5 に概要を示す．この手法では，特徴量の生成，相関係数の算出，ヒストグラム生成，そして異常検知と 4 つの処理のプログラムが逐次的で何度も起動する必要がある．そのため，処理が毎回止まらずに常時検知し続けるように変更する必要が存在する．

4.2 パラメータの調整

異常検知手法は実環境における動作が考慮されていないという問題点が存在する．リソースの制約を受けない理想的な環境を想定した動作例が多いが，実際に運用する上では CPU やメモリといったリソース制約を受ける．マシンのスペックや他のサービスの稼働状況などにより動作環境は常に変動するため利用可能なリソース量も変動する．理想的な環境を想定したパラメータでは，処理負荷が大きく検知システムとして継続的に動作できない可能性が存在する．そのため，検知システムが止まらないよう使用可能なリソース量を把握しその範囲の中で最適なパラメータに設定する必要が存在する．本稿ではリソース量として（Ⅰ）から（Ⅲ）の 3 種類を常時計測する．

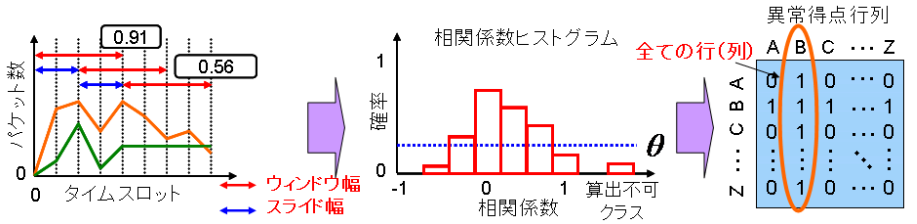

図 5　相関関係に基づく異常検知手法

計測するそれぞれのリソース量について閾値を定義し，閾値を超えたら処理負荷が大きいと判断し処理負荷が減るようにパラメータを調整する．（Ⅲ）については，閾値をスライド幅に設定する．これら 3 種類の指標から，ネットワークの構成やネットワーク状態の変化を検知し，環境の変化に合わせたパラメータ調整を行うことで，外的な要因で環境が変化しても処理負荷を調整し継続して検知し続けるシステムが実現可能になると考えられる．AIR がこれらの動作制御を自律的に行うため，ネットワーク管理者が煩わしい操作を行う必要がなく負担が軽減可能になると考えられる．閾値を超えた場合の調整に関する知識には（ア）から（エ）の 4 種類の知識を考える．

（Ⅰ）CPU 使用率（Ⅱ）メモリ使用量（Ⅲ）計算時間
（ア）タイムスロット幅を大きくする
（イ）ウインドウ幅を小さくする
（ウ）スライド幅を大きくする
（エ）観測量を減らす

4.3 設計・実装

文献 1）の手法を ADIPS/DASH フレームワーク 17-18）を用いてエージェントにより AIR を実現する．（Ⅰ）から（Ⅲ）をプロダクションルール型知識として与えられた利用支援知識として，（ア）から（エ）を利用支援知識に基づいて作動する利用支援機能として実装する．AIR 化によるエージェント間のやり取りの概要を図 6 に示す．

それぞれがエージェントとして実装され，トラヒックは特徴量の生成プログラム，特徴量は相関係数の算出プログラム，通常状態はヒストグラム生成プログラム，検知は異常検知プログラムを情報資源としてベースプロセスで実行される．これらの間の時系列データ，相関係数行列，ヒストグラムについてはベースプロセス間通信となっている．これら 4 種類のエージェントを制御するエージェントがマネージャである．

Vol.2009-DPS-141 No.27
Vol.2009-GN-73 No.27
Vol.2009-EIP-46 No.27
2009/11/27

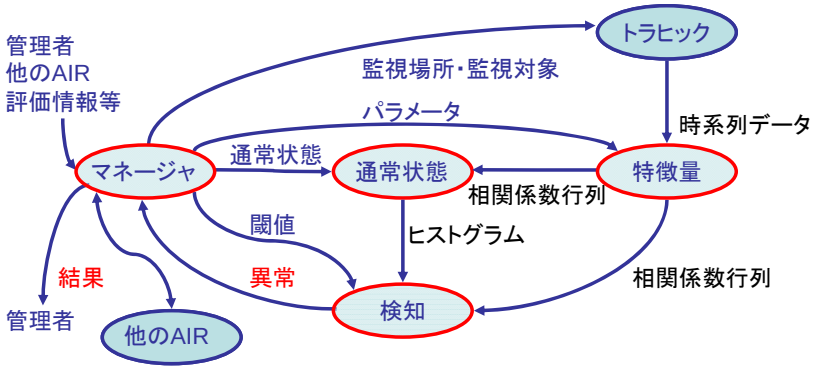

図 6　AIR 化によるエージェント間のやり取り

マネージャからの監視場所・監視対象，パラメータ，通常状態，閾値，異常，結果についてはメッセージとなっている．

5.　まとめと今後の予定

ネットワーク管理において重要なインシデントを検知する方法として，ネットワークの通常状態を統計的手法によってモデル表現し，そのモデルからの逸脱の程度を定量的に評価する異常検知手法が高い成果をあげ注目されている．しかし，異常検知手法は実環境における動作が考慮されていないという問題点が存在する．ネットワーク管理のプロセスの一部しか自動化されていないため，導入から原因の特定・対処までの一連のプロセスの大部分をネットワーク管理者が手動で行わなければならない．特にパラメータの更新・変更といった調整や，原因の特定・評価は高度かつ専門的知識やネットワーク管理者の経験が必要になるため，ネットワーク管理者に大きな負担がかかる．そこで，本研究では異常検知手法を運用する際の問題を解決するため，AIR の概念に基づきネットワーク管理者の知識や経験を予め埋め込んだエージェントを提案した．異常検知手法の運用・管理を代行するエージェントを異常検知手法と連携することで能動的な異常検知を実現し，ネットワーク管理者の知識や経験に基づいた運用の自動化を目指して，本稿ではパラメータの更新・変更について文献 1）の AIR 化について述べた．

今後は動作確認・評価を行い，文献 2）といった他の手法についても AIR 化を行う．またもう 1 つの問題であった原因の特定・評価に関しても検討を行う．

参考文献

1)　和泉勇治，廣瀬淳一，角田裕，根元義章，“相関係数発生確率行列を利用したネットワーク状態評価方式”，電子情報通信学会論文誌 B，Vol.J90-B，No.7，pp.660-669，2007.
2)　高橋秋典，五十嵐隆治，上田浩，岩谷幸雄，木下哲男，“R/S Pox Diagram に基づくトラフィック異常検知に関する研究”，電子情報通信学会技術研究報告 NS2008-50，pp.45-50，2008.
3)　木下哲男，“分散情報資源活用の一手法”，電子情報通信学会技術研究報告，AI99-54，pp.13-19，1999.
4)　武田圭史，磯崎宏，“ネットワーク侵入検知”，ソフトバンクパブリッシング株式会社，2000.
5)　Snort，http://www.snort.org/.
6)　Swatch，http://swatch.sourceforge.net/.
7)　M.Stillerman，C.Marceau，and M.Stillman，“Intrusion Detection for Distributed Applications”，Communications of the ACM，42(7)，pp.62-69，July 1999.
8)　林經正，横山幹，高原厚，岩橋政宏，“Snort を用いた侵入防止システムの構築と侵入検知処理速度高速化の検討”，情報処理学会研究報告，2003-CSEC-21，pp.59-64，2003.
9)　oinkmaster，http://oinkmaster.sourceforge.net/.
10)　和泉勇治，根元義章，“ネットワークトラヒックの異常検知技術”，電子情報通信学会 2008 年総合大会講演論文集，BS-5-1，2008.
11)　辻雅史，和泉勇治，角田裕，根元義章，“段階的トラヒック解析によるネットワーク異常検出方式”電子情報通信学会技術研究報告，IN2005-72，pp.67-72，2005.
12)　佐藤陽平，和泉勇治，根元義章，“複数の検出モジュールによるネットワーク異常検出の高精度化”電子情報通信学会技術研究報告，NS2004-144，pp.45-48，2004.
13)　肥村洋輔，福田健介，長健二朗，江崎浩，“統計的異常トラフィック検出手法の動的パラメータ最適化に関する研究”電子情報通信学会技術研究報告，IN2008-106，pp.121-126，2008.
14)　石黒正揮，鈴木裕信，村瀬一郎，篠田陽一，“インターネット上の脅威分析を支援する空間および時間的な特徴量に基づく分析手法”，情報処理学会論文誌，Vol.48，No.9，pp.3148-3162，2007.
15)　向坂真一，小池英樹，“内部ネットワーク監視を目的とした時間・論理・地理情報の統合的視覚化システム”情報処理学会論文誌，Vol.49，No.1，pp.503-512，2008.
16)　高田哲司，小池英樹，“見えログ：情報視覚化とテキストマイニングを用いたログ情報ブラウザ”，情報処理学会論文誌，Vol.41，No.12，pp.3265-3275，2000.
17)　藤田茂，菅原研次，木下哲男，白鳥則郎，“分散処理システムのエージェント試行アーキテクチャ”，情報処理学会論文誌，Vol. 37，No.5，pp.840-852，1996.
18)　DASH-Distributed Agent System based on Hybrid architecture，http://www.agent-town.com/dash/.