Vol.2010-DPS-142 No.6
Vol.2010-CSEC-48 No.6
2010/3/4

能動的情報資源に基づく 複数の異常検知手法の協調的連携手法

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

異常検知手法は，不正検知手法に比べ検知精度が低いため，複数の異常検知手法を組み合わせた研究が多く存在する．特定の異常検知手法を組み合わせた手法は存在するが，管理者が自由に異常検知手法を組み合わせて運用することは困難である．用いる情報資源が異なるため，相互に協調連携させて運用することが難しく管理者にかかる負担が大きい．

そこで，本研究では，複数の異常検知手法におけるネットワーク管理の自動化による管理者の負担軽減を目的として，複数の異常検知手法の協調的連携手法を提案する．本稿では，能動的情報資源に基づく本手法の設計と実装について述べ，その評価を行う．

A Cooperative Coordination Method of Plural Anomaly Detections based on Active Information Resource

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

Anomaly detection methods are low precision compared with the misuse detection methods, and therefore, there are many studies that plural anomaly detection methods are combined so as to improve precision of detecting. There are some techniques to combine specific anomaly detection methods, but freely combining plural anomaly detection methods and cooperatively operating them are difficult for managers of a network. As a result, using the plural methods is a heavy burden for the managers.

In this study, for the purpose of reducing the burden, we propose a cooperatively coordinate method of plural anomaly detection methods, which automate the network management that uses plural anomaly detection methods. In this article, we explain a design and implementation of the method based on Active Information Resource, and then evaluates it.

1. はじめに

近年，コンピュータ技術の進歩や通信技術の発達により，急速にインターネットが普及している．インターネットの普及により，WWW や E-mail などの従来から存在していたサービスに加え，電子商取引のサービス，P2P 技術を利用したインターネット電話サービス，SNS など，様々な形でインターネットが利用されている．インターネットが普及し，社会の重要なインフラとなることで，ネットワーク管理の重要性がとても高まっている．

インターネットが普及し社会基盤となる一方，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，DoS 攻撃，不正侵入の前兆を示すスキャン，情報の改竄や漏洩など，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．甚大な被害を防ぎ，安全で安定した信頼性のあるネットワークの運用のために，ネットワークの構成や状態を把握して，インシデントを早期に検知し，適切な対処を行う必要性がある．これに対し，侵入検知システム(Intrusion Detection System :IDS[1-2])というインシデントを検知するネットワーク管理機構が提案されており，情報資源 [3]として，入力，処理手順，出力などがあげられる．

また，インターネットが普及し利用者が増加することで，ネットワークシステムはますます大規模，複雑になってきている．ネットワーク管理者にとっては，より高度かつ専門的な知識や煩雑な作業が要求されるようになり，ネットワーク管理者の負担増加に繋がっている．ネットワーク管理者の負担を軽減するために，大量のネットワーク情報を処理しネットワーク管理の自動化を行う必要性がある．これに対し，ネットワーク管理システム(Network Management System :NMS)というネットワーク管理に必要な情報を自動的に収集するネットワーク管理機構が提案されており，情報資源として，ログ，ユーザ情報，機器状態などがあげられる．

図 1 にネットワーク管理の様子を示す．ネットワーク管理のために，ネットワーク管理者は，様々な種類の IDS や NMS を利用した運用を行う必要がある．IDS と NMS を相互に連携させたネットワーク管理は，異なる情報資源を扱っているため，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であり，その運用が大きな負担となっている．NMS については，ネットワーク管理者の知識や経験を付加し，IDS と相互に連携できる NMS[4]が提案されているため，本研究では IDS を対象とする．従来は，

[†]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.2010-DPS-142 No.6
Vol.2010-CSEC-48 No.6
2010/3/4

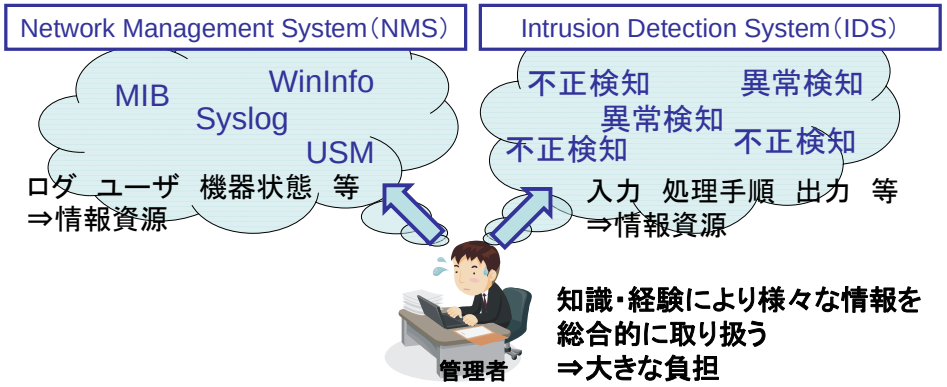

図 1　ネットワーク管理

ネットワーク管理者が行っていた知識や経験に基づいた運用を自動化し，ネットワーク管理者の負担を軽減させることを目的として，異なる情報資源によるネットワーク管理機構の相互連携の実現を目指す．

同じ IDS に関しても，情報資源の異なる様々な検知手法が存在するため，複数の検知手法を相互に連携させる必要があり，さらに，他のネットワーク管理機構と連携させる必要がある．そこで，能動的情報資源(Active Information Resource :AIR[3]) に基づき，異常検知手法の AIR 化と，AIR 化した複数の異常検知 AIR 間の協調的連携手法を提案する．提案手法により，環境の変化に柔軟に対応した制御を行うことでネットワーク管理者による自由な異常検知手法の追加と，検知結果を 1 つの情報資源として集約することで，他のネットワーク管理機構の連携を可能にする．この 2 点により，ネットワーク管理者の負担軽減を実現する．

以下，2 章では関連研究として異常検知手法について説明し，その問題点について述べる．3 章では 2 章で述べた問題点を解決する協調的連携手法を提案し，4 章では提案手法の実装と評価について述べる．そして最後に 5 章でまとめと今後の課題について述べる．

2.　関連研究とその問題点

ネットワークやホストを監視してインシデントを検知する IDS は，アルゴリズムの違いから不正検知手法と異常検知手法に大別することができる [5]．本研究では異常検知手法を対象とし，その詳細と運用に関する問題点について述べる．

2.1　異常検知手法

異常検知手法は，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．通常状態から逸脱した場合に，異常(通常とは異なる振舞い) として検知する手法である．不正検知手法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，異常検知手法は統計量を扱うため，不正検知手法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．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も検知できる可能性があるため，ネットワーク管理において重要な技術として注目され，多数の研究が行われている．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，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．さらに，ネットワークの構成や状態を適切に把握して，インシデントを早期に検知し，適切な対処を行うために，ネットワーク管理者はネットワークトラヒックを解析する必要があるため，ネットワークトラヒックに基づく異常検知手法を本研究の対象とする．

ネットワークトラヒックに基づく異常検知手法は，多くの場合，観測部，抽出部，算出部の 3 種類の要素にわけることができる [6]．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．ネットワークトラヒックの観測方式は，タイムスロット型，フロー型，サンプリング型に分類される．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) によるものがある．主成分分析は，複数の特徴量が相関を有し分布していることを前提としたモデルである．通常状態では，一定の相関関係が保たれているが，異常状態ではその相関関係が失われることから異常を検知する手法 [7]などが提案されている．自己相似性は，インターネットトラヒックに自己相似性が存在する [8]ことから，ネットワークトラヒックにも自己相似性が存在すると仮定し，ネットワークトラヒックを評価する．プロトコル制御に従わない DoS 攻撃トラヒックが，自己相似性を失う特性を利用し攻撃を検知する手法 [9]などが提案されている．

2.2　異常検知手法における問題点および技術的課題

異常検知手法の運用に関して，異常検知手法の自由な追加・変更による運用が困難という問題点がある．まず，その問題点について詳細を述べ，その後に問題点に対する要件と技術的な課題について述べる．

Vol.2010-DPS-142 No.6
Vol.2010-CSEC-48 No.6
2010/3/4

2.2.1 運用とその問題点

統計的手法を用いた異常検知手法は，通常状態となるモデルからの逸脱の程度を定量的に評価し異常を検知するため，不正検知手法に比べて，誤検知の割合が高く検知精度が低い．高精度なインシデント検知のためには，複数の異常検知手法を併用した運用と，統計的手法を用いる異常検知手法の特徴や実環境における動作を考慮した運用が必要である．複数の異常検知手法を併用した運用の例として，段階的に異常検知手法を組合せた研究[10]や，並列的に異常検知手法を組み合わせた研究[11]などがあげられる．

文献[10-11]の手法の概要を図 2 に示す．文献[10]では，1 段階目に使用した異常検知手法で，通常状態と同じとして正常と判断された場合と，通常状態とは異なるとして異常と判断された場合は次の段階に進まない．正常と異常の間で懐疑と判断された場合のみ次の段階に進む．そして，次の段階で懐疑と判断されたものに関してのみ再度異常検知手法によって検知を行う仕組みである．文献[11]では，複数の異常検知手法を同時に運用し，結果の論理和を最終的な検知結果とする．つまり，1 つ以上の異常検知手法で異常と判断された場合に，異常と判断する仕組みである．文献[10-11]のような複数の異常検知手法を併用した手法は,ある特定の異常検知手法を組合せた手法であり，別の異常検知手法に置き換えて運用することが困難である．異常検知手法は数多くの研究が行われているため，監視対象や監視目的によって自由に組み合わせて運用することが望まれるが，異常検知手法の入れ換えが考慮されておらず，異常検知手法の自由な追加・変更による運用が困難という問題点がある．

すなわち，それぞれの異常検知手法が異なる情報資源による検知手法であり，複数の異常検知手法を併用して運用する場合，相互に協調・連携させて運用することが困難である．そのため，自由な追加・変更ができない．ネットワーク管理者が，自由に異常検知手法を取り入れられる枠組みを実現させるために必要な要件として，容易に異常検知手法の追加・変更が可能であることと他のネットワーク管理機構との連携が可能であることの 2 点があげられる．追加・変更に対する技術的な課題として，システムの安定性に関する課題，連携に対する技術的な課題として，情報資源の統合に関する課題があげられる．

2.2.2 システムの安定性に関する課題

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ため，ネットワークトラヒックの変化やパラメータが，検知精度に与える影響がとても大きい．環境の変化やサービスの稼働状況などによって変化する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[12]．不適切なパラメータを設定すると検知精度が大きく低下するため，高精度なインシデント検知を維持するためには，適切なパラメータ設定が重要であるため，適切なパラメータ設定や動的なパラメータ調整に関する研究が行われている．また，実環境における動作として，異常検知手法は，継続的な動作と即時性を考慮した運用が求められる．しかし，パラメータ設定に関する研究では，リソースの適切な割り当てが考慮されていない．複数の異常検知手法を併用して運用する場合，導入する異常検知手法が増えるほど，リソースを消費することになる．実際に運用する上では，異常検知手法が導入されてい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常に変動する．そのため，リソース・計算時間と検知精度を考慮して，パラメータや組み合わせる異常検知手法の数を調整する必要があり，環境の変化に柔軟に対応して制御することが求められる．

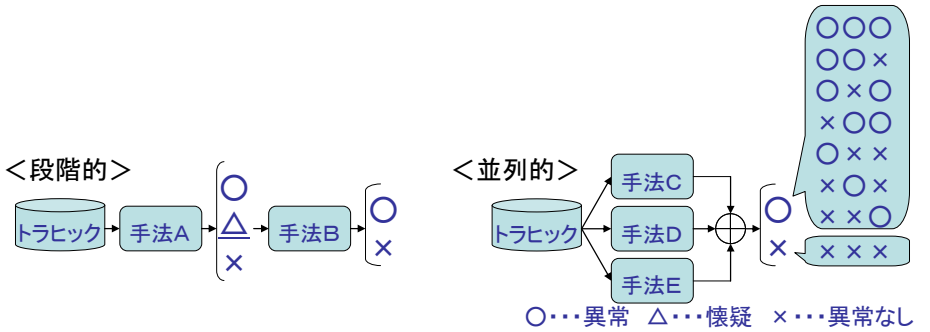

図２　検知方法の概要

2.2.3 情報資源の統合に関する課題

異常検知手法は，統計的手法に基づいた処理を行っており，観測単位毎(タイムスロット型の場合ある一定の時間間隔) で異常か否かを判断している．しかし，検知結果はそれぞれ独立しており，観測単位毎の検知結果からインシデントを特定することが困難である．そのため，実環境における動作として，異常検知手法の検知のタイミング(同期) を考慮した運用が求められる．タイムスロット型とフロー型を組み合わせた場合は，異常の検知間隔が揃わず，同じタイムスロット型でも，パラメータにより異常の検知間隔が揃わない場合が存在する．さらに，他のネットワーク管理機構と連携して，異常原因の特定やその後の対処を行う必要がある．そして，それぞれの異常検知手法や検知結果の特徴を把握し，組合せに応じた状態の総合的な把握[13]する必要がある．複数の異常検知手法を併用して運用する場合，導入する異常検知手法が増えるほど，検知結果が増え，その検知結果が全て一致する可能性が低くなる．そのため，それぞれの検知結果に意味を持たせ情報を統合する必要があり，検知結果を 1 つの情報資源として集約することが求められる．

Vol.2010-DPS-142 No.6
Vol.2010-CSEC-48 No.6
2010/3/4

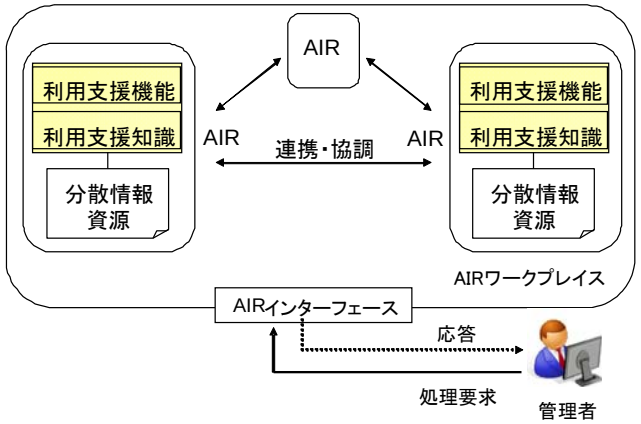

図３　AIR の概念構成図

3. 協調的連携手法の提案

2 章では，複数の異常検知手法を併用して運用する場合の問題点について述べた．本章では，その問題点を解決するため，能動的情報資源(AIR)の概念に基づき，異常検知手法の AIR 化と，AIR 化した複数の異常検知 AIR 間の協調的連携手法を提案する．提案手法により，環境の変化に柔軟に対応した制御を行うことによるネットワーク管理者の自由な異常検知手法の追加と，検知結果を 1 つの情報資源として集約することによる他のネットワーク管理機構の連携を可能にする．

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 3 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．

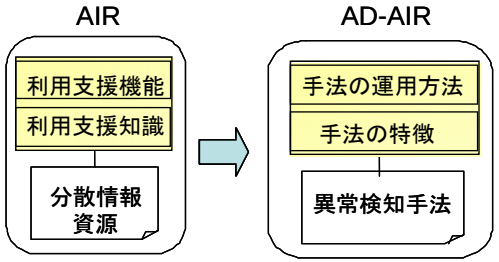

図４　異常検知手法の AIR 化

3.2 異常検知手法のAIR化

異常検知手法における情報資源(入力，処理手順，出力など) に，手法の特徴や運用に関する知識や経験を利用支援知識と利用支援機能に付加することで，AIR 化を行う．異常検知手法の AIR 化の様子を図 4 に示す．提案手法では，AIR 化した異常検知手法(Anomaly Detection AIR:AD-AIR)と，Manager の 2 種類の AIR を使用する．

AD-AIR は，統計的手法に基づく処理のプログラムを情報資源として保持する．そして，システムの安定性の保持するための，環境の変化に柔軟に対応した制御に関する知識や経験を，利用支援知識と利用支援機能として情報資源のプログラムに付加し，AIR 化する．制御に関する知識や経験を付加することで，システムの安定性を保持することができるため，容易な異常検知手法の追加・変更が可能になる．

Manager は，複数の AD-AIR からの結果を，時刻情報をもとに 1 つに集約し，情報資源として保持する．そして，AD-AIR の運用に関する知識や経験を，利用支援知識と利用支援機能として情報資源の集約した結果に付加し，AIR 化する．運用に関する知識や経験，すなわち，AD-AIR の協調・連携動作や AD-AIR の導入に関する知識や経験を付加することで，他のネットワーク管理機構との連携が可能になる．

3.3 異常検知AIR間の協調的連携

異常検知手法を AIR 化した AD-AIR と Manager の協調・連携の様子を図 5 に示す．AD-AIR は，Manager に検知結果<Incident unit> とリソース情報<Resource Information>をメッセージとして送る．Manager は，AD-AIR に運用<Control>に関するメッセージを送る．また，Manager は，他のネットワーク管理機構との協調・連携を行う．このように，AD-AIR と Manager がメッセージのやりとりを行うことで，協調・連携が可能になる．以下に環境の変化への対応と検知集約の集約に関して詳細を述べる．

Vol.2010-DPS-142 No.6
Vol.2010-CSEC-48 No.6
2010/3/4

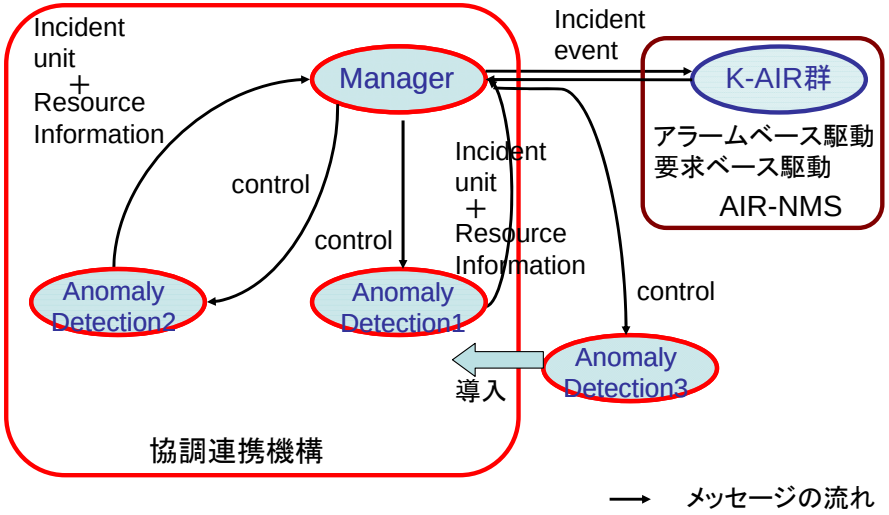

図５　協調・連携のイメージ

3.3.1　環境の変化への対応

Manager は，AD-AIR から<Resource Information>メッセージを受信する．受信したメッセージの内容と，Manager が持つ知識から状況に応じた<Control>メッセージを AD-AIR に送信する．メッセージ内容は，手法を起動・停止，動作レベル(計算時間・検知精度とパラメータの関係を順位付けしたもの) を上げる・下げるになっている．

AD-AIR は，Manager から<Control>メッセージを受信する．受信したメッセージの内容から，動作レベルに応じて AD-AIR が持つ知識からパラメータを決定する．また，AD-AIR は，検知処理に必要なリソース情報を，<Resource Information>メッセージとして Manager に送信する．メッセージの内容は，CPU 使用率，メモリ使用量，計算時間になっている．このように，AD-AIR からの<Resource Information>メッセージと，Manager からの<Control>メッセージによる協調・連携により，環境の変化に柔軟に対応した制御が可能になり，ネットワーク管理者による自由な異常検知手法の追加が実現できる．

3.3.2　検知結果の集約

AD-AIR は，Manager からの<Control>メッセージと知識から決定したパラメータで異常検知を行う．そして，検知結果に属性を付けて<Incident unit>メッセージを Manager に送信する．メッセージの内容は，時刻情報，検知結果，属性となっている．属性は，それぞれの異常検知手法の特性を示したもので，TCP による異常(Protocol)，HTTP による異常(Port)，192.168.0.1 による異常(IP)などの情報になっている．

Manager は，AD-AIR から<Incident unit>メッセージを受信する．それぞれの AD-AIR から受信した<Incident unit>を時刻情報から 1 つの情報資源として集約し保持する．Manager は，他のネットワーク管理機構から要求<Request>があった場合，要求に対して情報<Incident event>を提示する．6:00-17:00 という時刻情報の要求があった場合，情報資源の中から，該当する時間帯の全ての検知結果を提示する．6:00-17:00 anomaly という時刻情報と検知結果の要求があった場合，情報資源の中から，該当する時間帯で異常と判断された検知結果を提示する．このように，AD-AIR からの<Incident unit>メッセージと，他のネットワーク管理機構との<Request>，<Incident event>メッセージによる協調・連携により，検知結果を 1 つの情報資源とした集約が可能になり，他のネットワーク管理機構との連携が実現できる．

4.　提案手法の実装と評価

本章では，3 章で提案した協調的連携手法の実装と，評価実験を行う．最初に実装の概要について述べ，予備実験として試作システムの動作確認を行う．そして，環境の変化への対応と検知結果の集約に関する評価実験を行い，提案手法の有効性を示す．

4.1　実装の概要

分散環境上で，マルチエージェントシステムを実現するためのフレームワークである ADIPS/DASH[14-15]フレームワークおよび DASH と互換性のある IDEA [16]開発環境を用いて提案手法を実装する．すなわち，AIR は，ルール型知識として与えられる利用支援知識に基づいて動作し，その過程で利用支援機能として組み込まれた Java プログラムなどを起動しながら，情報資源の加工・処理や他の AIR との協調・連携処理を実行する．　実装に用いる異常検知手法は，相関関係に基づく異常検知手法 [7]と，自己相似性に基づく異常検知手法 [9]である．

4.2　試作システム

図 6 に提案手法により AD-AIR が動作している様子を示す．図 6 では，2 種類の AD-AIR が動作している．運用する AD-AIR 名と初期パラメータを入力すると，AD-AIR が Manager によりワークプレースにインスタンシエートされ，AD-AIR の運用が開始される．　Manager は，入力された検知要請間隔で，それぞれの AD-AIR に検知要請をする．要請を受けた AD-AIR は，検知を実行する．

図 7 に検知結果を集約した様子を示す．Manager は，それぞれの AD-AIR から検知結果を集約し，1 つの情報資源として保持する．それぞれの AD-AIR の時刻，検知結果，属性に加え，リソース情報と Manager の検知要請時刻と検知結果集約時刻も合わせて保持する．

Vol.2010-DPS-142 No.6
Vol.2010-CSEC-48 No.6
2010/3/4

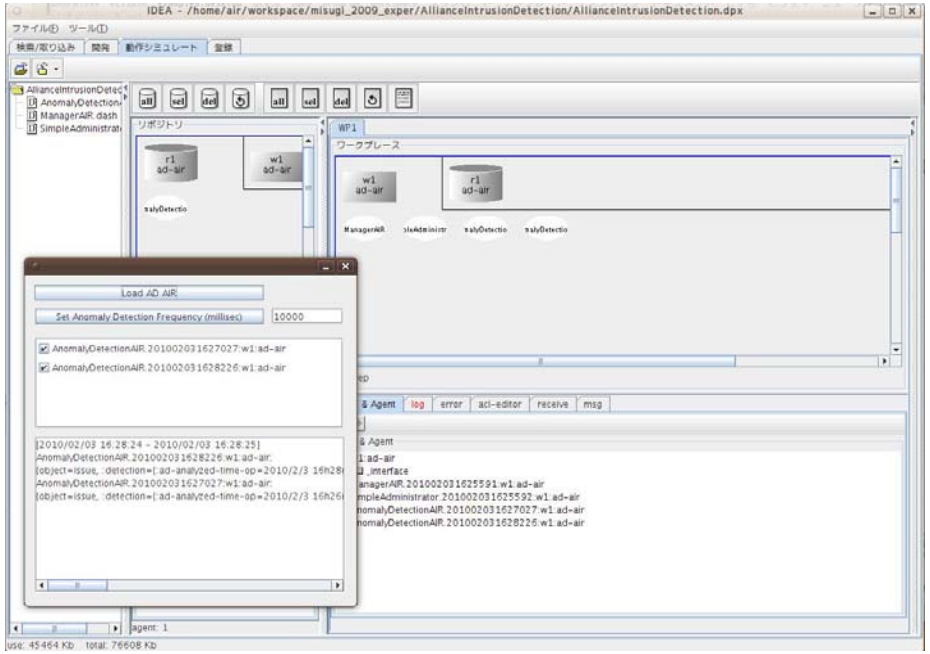

図 6　提案手法による AD-AIR の動作

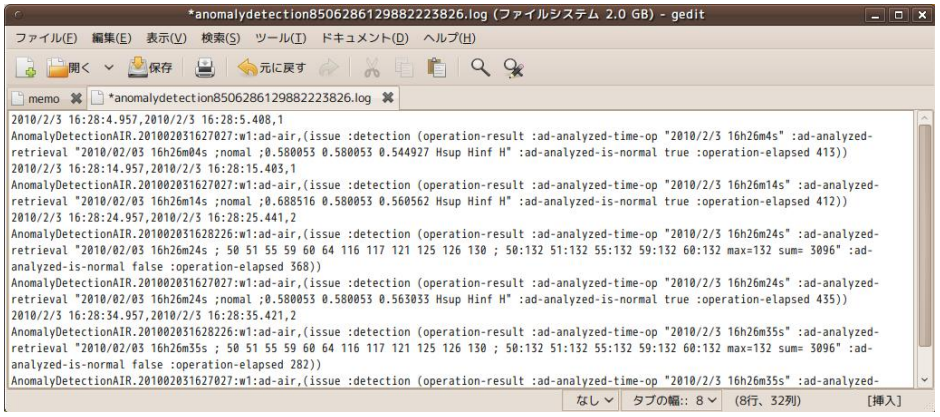

図 7　提案手法による集約

4.3　評価実験

自由に異常検知手法を追加し環境の変化に柔軟に対応した制御か可能かどうかと，検知結果を 1 つの情報資源として集約し他のネットワーク管理機構との連携が可能かどうかの評価実験を行う．両方とも実験環境は以下の通りである．

- CPU：　Intel(R)Core(TM) i5 CPU 750　2.67[GHz]
- OS：　Ubuntu 9.10
- 実装：　ADIPS/DASH フレームワーク
- 動作環境：　IDEA

4.3.1　環境の変化への対応に関する評価実験

提案手法が自由に異常検知手法を追加し，環境の変化に柔軟に対応した制御か可能か評価する．動作シナリオは，AD-AIR を複数起動し環境を変化させ即時性(Manager の検知要請間隔＞1 回の計算時間)が確保できない場合に，即時性が確保できない AD-AIR を停止させる．Manager の検知要請間隔の変更と，負荷をかけることにより即時性を確保できない状況を作り，Manager とそれぞれの AD-AIR の 1 回あたりの処理時間を評価する．

図 8 と図 9 に結果のグラフを示す．図 8 では，パラメータを変え 3 種類の AD-AIR で検知を行っている．そして，ある時刻で検知要請間隔を 10000[ms]から 1000[ms]に変更した場合の 1 回あたりの処理時間をグラフにしたものである．手法 A は，1 回の計算に約 2000[ms]かかるため，検知要請間隔を変更すると即時性を失ってしまう．そのため，検知要請間隔を変更した際に手法 A は運用を停止している．手法 B と手法 C は，両方とも検知要請間隔を 1000[ms]に変更しても即時性を保持できるため，何も制御されずそのまま検知を行っている．手法 A が制御されないと，手法 A は即時性を保持できないため，手法 A と手法 B の検知結果を集約することが困難になると考えられる．図 9 では，2 種類の AD-AIR で検知を行っている．そして，ある時刻で実験用のマシンに負荷をかけた場合の 1 回あたりの処理時間をグラフにしたものである．手法 A は，負荷をかけると計算時間が増え検知要請間隔の 1000[ms]を超え即時性を失ってしまう．そのため，負荷をかけた際に手法 A は運用を停止している．手法 B も，負荷をかけると計算時間が増えているが，検知要請間隔の 1000[ms]を超えていないため，何も制御されずそのまま検知を行っている．手法 A が制御されないと，手法 A，手法 B ともに検知要請間隔の 1000[ms]を超えるようになり，過負荷状態で手法が両方とも停止してしまう可能性がある．

4.3.2　検知結果の集約に関する評価実験

提案手法が検知結果を 1 つの情報資源として集約し，他のネットワーク管理機構との連携が可能か評価する．動作シナリオは，AD-AIR を複数起動し検知を行う．そして，時刻情報と検知結果を Manager に要求し，Manager が要求に対して結果を提示する．要求してから結果を提示するまでの所要時間と情報量を評価する．

Vol.2010-DPS-142 No.6
Vol.2010-CSEC-48 No.6
2010/3/4

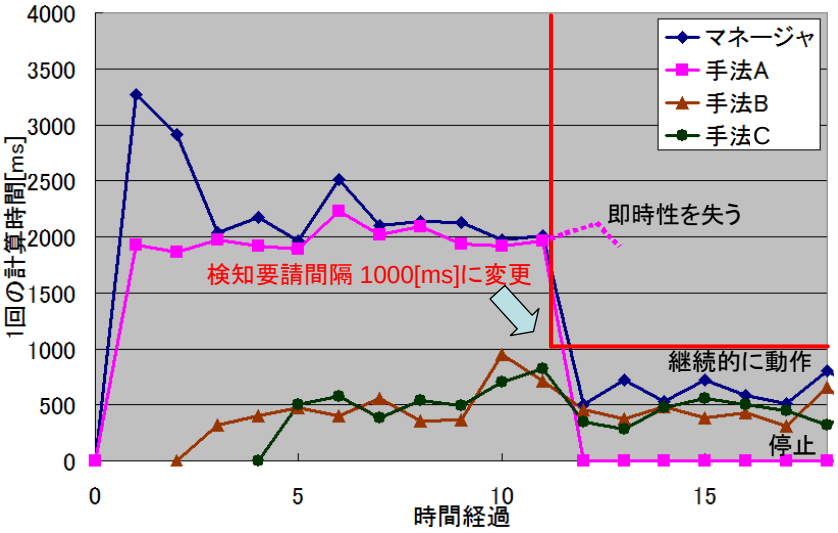

図８　検知要請間隔を変更した場合

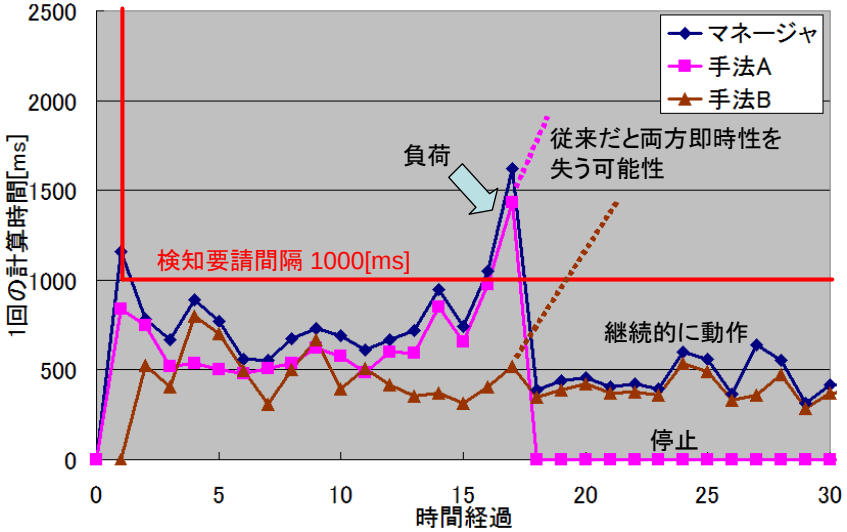

図９　負荷をかけた場合

表１　AD-AIR が 3 種類の場合にかかる時間　[ms]

条件	3 時間分	6 時間分	9 時間分
全て	708	884	1367
異常のみ	636	752	1256

表２　AD-AIR が 2 種類の場合にかかる時間　[ms]

条件	3 時間分	6 時間分	9 時間分
全て	204	381	475
異常のみ	178	334	414

表 1 と表 2 に結果の表を示す．両方とも，検知要請間隔は 30000[ms]とし，9 時間検知を行ってから実験を行った．評価は全て 3 回ずつ行っている．表 1 はパラメータを変え 3 種類の AD-AIR で検知を行った場合，表 2 は 2 種類の AD-AIR で検知を行った場合に，要求してから提示するまでの所要時間の平均を示している．これらから，指定する時間が増えるほど，保持する検知結果が増えることから，要求から結果を提示するまでに時間がかかることがわかる．しかし，今回の評価実験からは，ネットワーク管理者は，数秒以内に必要な情報を手に入れることができた．従来の異常検知手法は，オフラインの評価であり実環境での動作が考慮されておらず，ネットワーク管理者は，必要な情報がある場合その都度異常検知手法を動作させネットワークトラヒックから検知する必要がある．そのため，必要な情報を手に入れるまでに多くの時間を要すると考えられる．つまり，提案手法の場合，従来に比べて必要な情報を手に入れるまでの所要時間が短くてすむと考えられる．

4.3.3　評価実験に関する考察

環境の変化への対応に関する評価実験より，即時性が保持できない AD-AIR があった場合に，その AD-AIR の運用を停止することで，全体の即時性を保持したまま継続的に運用させることができた．提案手法により，環境の変化に柔軟に対応して制御することが可能になり，容易に異常検知手法の追加・変更が可能になったと言える．

検知結果の集約に関する評価実験より，ネットワーク管理者は，必要な情報を短時間で正確に手に入れることができた．提案手法により，検知結果を 1 つの情報資源として保持することが可能になり，他のネットワーク管理機構との連携が可能になったと言える．

5.　まとめと今後の課題

近年，ネットワーク管理の重要性がとても高まっている．ネットワーク管理として，侵入検知システム(IDS)や，ネットワーク管理システム(NMS)が提案されている．しか

し，IDS と NMS を相互に連携させたネットワーク管理は，異なる情報資源を扱っているため，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であり，その運用が大きな負担となっている．そこで，本研究では，ネットワーク管理機構の中で，異常検知手法という IDS を対象とし，ネットワーク管理者の負担を軽減させることを目的として，異なる情報資源によるネットワーク管理機構の相互連携を目標とした．

複数の異常検知手法を併用して運用する場合，相互に協調・連携させて運用することが困難であり，自由な追加・変更ができないという問題点が存在する．ネットワーク管理者が，自由に異常検知手法を取り入れられる枠組みを実現させるためには，容易に異常検知手法の追加・変更が可能であり，他のネットワーク管理機構との連携が可能でなければならない．

そこで，本研究では，能動的情報資源(AIR)の概念に基づき，異常検知手法の AIR 化と，AIR 化した複数の異常検知 AIR 間の協調的連携手法を提案した．提案手法により，環境の変化に柔軟に対応した制御を行うことによるネットワーク管理者の自由な異常検知手法の追加と，検知結果を 1 つの情報資源として集約することによる他のネットワーク管理機構の連携が可能になる．

そして，ADIPS/DASH フレームワークおよび DASH と互換性のある IDEA 開発環境を用いて提案手法の実装を行った．環境の変化への対応に関する評価実験から，環境の変化に柔軟に対応して制御することが可能になり，容易に異常検知手法の追加・変更が可能になった．検知結果の集約に関する評価実験から，検知結果を 1 つの情報資源として保持することが可能になり，他のネットワーク管理機構との連携が可能になった．以上のことからネットワーク管理者の負担が軽減できたと言える．

今後は，環境の変化への対応に関して，手法の停止以外の制御機能の追加を行う．また，検知結果の集約に関して，他のネットワーク管理機構からの要求に対して提示する(要求ベース)だけではなく，提案手法が異常を検知した時，インシデントを特定し，他のネットワーク管理機構にアラームを出す機能(アラームベース)について検討を行う．

参考文献

1) Cisco Intrusion Detection System. http://www.cisco.com/en/US/products/sw/secursw/ps2113/.
2) Dragon Intrusion Detection System. http://www.enterasys.com/ids/.
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) S.Konnno，A.Sameera，Y.Iwaya，T.Abe，T.Kinoshita.“Knowledge-Based Support of Network Management Tasks Using Active Information Resource”．International Conference on Intelligent Agent Technology，pp.195–199，December 2006.
5) 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.
6) 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.
7) 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.
8) W.E.Leland, M.S.Taqqu, W.Willinger, D.V.Wilson.“On the Self-Similar Nature of Ethernet Traffic”. Computer Communications，Vol.23，No. 4，pp. 183–193，April 1993.
9) 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.
10) 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.
11) 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.
12) 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.
13) 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.
14) 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.
15) DASH-Distributed Agent System based on Hybrid architecture. http://www.agent-town.com/dash/.
16) 打矢隆弘，前村貴秀，菅原研次，木下哲男．“エージェントシステムのインタラクティブ開発環境”．電子情報通信学会論文誌，Vol. J88-D-I，No. 9，pp. 1344–1355，2005.