F-060

能動化されたトラヒック情報によるネットワーク異常検知

Anomaly Detection based on the Activated Information of Network Traffic

三杉 大輔† 笹井 一人†† 高橋 優介† 佐藤 彰洋† 北形 元†† 木下 哲男†††
Daisuke Misugi Kazuto Sasai Yusuke Takahashi Akihiro Satoh Gen Kitagata Tetsuo Kinoshita

1．はじめに

インターネットの発展に伴い，ネットワーク管理の重要性が高まっている．ネットワークの安全で安定した運用のため，ネットワークの管理者は，ネットワーク状態を適切に把握し，不正侵入や Denial of Service 攻撃，ウィルス感染といったインシデントを効果的に検知する必要がある．

高度なインシデントの検知の方法として，近年，異常検知手法が注目され，高い成果をあげている．しかし，異常検知手法の運用には，ネットワーク状態，すなわち規模や構成，運用しているサービスなどに応じた調整が不可欠である．高精度なインシデントの検知を維持するため，管理者が定期的にネットワーク状態の情報を収集し，管理者の知識・経験に基づいた調整を行う必要がある．そのため，管理者にとってその運用が大きな負担となる．

そこで本稿では，管理者にかかる負担を軽減するために，運用プロセスの中で経験的に獲得される知識をあらかじめ異常検手法に埋め込む，異常検知手法の能動的情報資源（Active Information Resource：AIR[1]）化を提案する．AIR 化により，ネットワーク状態の情報と，管理者の知識・経験に基づいた調整の自動化が可能になる．

2．関連研究とその問題点

2.1 インシデントの検知

本研究では，トラヒック解析に基づくインシデントの検知を対象とする．インシデントの検知の方法については数多くの研究が行われており，不正検知手法と異常検知手法に大別される．

不正検知手法は，既知のインシデントの特徴を明確にしてシグネチャを作成する．検知条件をシグネチャに事前に記述することで，シグネチャと一致した場合インシデントとして検知する．つまり，不正検知手法におけるインシデントの検知精度はシグネチャに依存する．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る．その方法として文献[2]が存在する．

異常検知手法は，何らかの指標からネットワークの通常状態を定義する．そして通常状態からの逸脱を統計的に正常・異常の判定を行い，異常と判断された場合にインシデントとして検知する．不正検知手法に比べ，シグネチャを作成する必要がないため，特徴の明記が困難なインシデントや未知のインシデントの検知が可能である．そのため，ネットワークの複雑化やサービスの多様化に伴い，異常検知手法は，その有効性が期待されている．

† 東北大学大学院情報科学研究科
†† 東北大学電気通信研究所
††† 東北大学サイバーサイエンスセンター

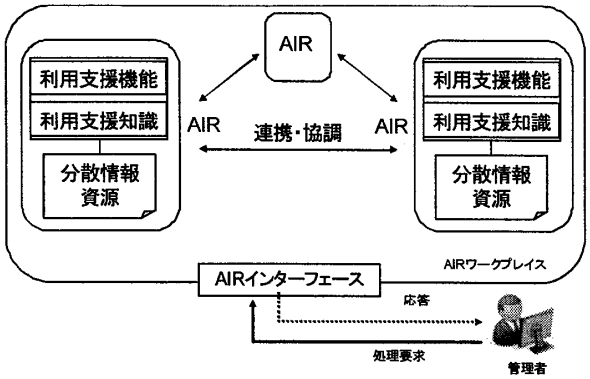

図1 AIR の概念構成図

2.2 異常検知手法の問題

異常検知手法の運用には，定期的なネットワーク状態の情報の収集と，調整が必要である．従来は，管理者が手動で収集と調整を行っており大きな負担となっていた．そこで，管理者の調整の負担を軽減するため，ネットワークの構成やネットワークから計測した情報を可視化する手法が提案されている[3,4]．しかし，それらの手法においても，管理者の知識・経験に基づいた調整が必要で，手動で調整する必要があり，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，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，ネットワーク状態の情報の収集や，管理者の知識・経験に基づいた調整の自動化を行う必要がある．

3. 異常検知手法の AIR 化

3.1 概要

本稿では，管理者の知識・経験によっていた異常検知手法に，その運用に関する情報をあらかじめ埋め込むことで，異常検知手法自体の可用性を向上し，運用時の管理者の負担を軽減する，異常検知手法の AIR 化を提案する．そしてそのフレームワークを提示する．

3.2 異常検知手法における AIR の役割

AIR は，ある情報資源にその利用に関する知識を埋め込んだ（AIR 化）ものである．これまで利用者側に要求されてきた個別の資源に関する詳細な知識獲得のプロ

セスを，情報資源自体が能動的に提示，もしくは実行できるようにする，概念的フレームワークである．図 1 に AIR の概念構成図を示す．

ここでは，個別の異常検知手法にそれを利用するための知識，すなわち，

(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

を埋め込むことを意味する．(1) から (3) の知識が埋め込まれた異常検知手法は，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，容易に適用するネットワークにおいて実装可能である．また，埋め込まれた知識は外部からアクセスが可能であるため，異なる理論的な背景に基づく異常検知手法を効果的に組み合わせたり，比較して無駄な異常検知手法を排除することで，リソース配分の最適化が可能になる．異常検知手法の AIR 化の実現に関して，本稿では，まず (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 異常検知手法運用プロセスのモデル化

3.3.1 異常検知手法を導入する場合のプロセス

異常検知手法の導入には，(a) から (c) に関して分析が必要である．更に，監視対象に適した (d) を行い，正常な動作が行われているか (e) を行うことが必要である．

(a) 入力する情報の種類
(b) 動作用件
(c) 検知される異常の種類
(d) パラメータ設定
(e) 検証

3.3.2 異常検知手法が動作している場合のプロセス

動作中の異常検知手法においては，常に (f) から (h) の評価を行う．そして，現在の環境に適した (i) や (j) を選択する．そしてそれに適した (k) や (l) を調整する．また，管理者の要求に応じて (i) や (j) を選択し，それに適した (k) や (l) を調整する．さらに，管理者の要求や 3.3.3 の評価の判断結果から (m) を調整する．

(f) ネットワーク状態の情報
(g) 計算時間（リアルタイム性）
(h) リソース消費
(i) 監視場所
(j) 監視対象
(k) パラメータ設定
(l) 通常状態の定義
(m) 正常・異常を判断する閾値

3.3.3 異常検知手法を評価する場合のプロセス

異常検知手法は，適用するネットワーク環境により適切か否かが大きく分かれるために，常に (n) や (o) を評価する必要がある．これらは，異常判定が下された場合に，実際のネットワークで何らかのインシデントが確認されたか否かという (p) をもとに (q) を行う必要がある．

(n) false positive
(o) false negative
(p) トラッキング結果
(q) 適切・不適切の判断

3.4 知識の埋め込み

異常検知 AIR 群を実装するための設計として，上記の 3.3 のモデルから得られた (a) から (q) 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プロセスであ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．そして，能動的な異常検知手法の運用を行うことができるフレームワークを提示する．

4. おわりに

本稿では，ネットワークのインシデント検知における異常検知手法を，実際に運用する際の管理者にかかる負担を軽減するために，運用プロセスの中で経験的に獲得される知識を，あらかじめ異常検知手法に埋め込む，異常検知手法の AIR 化を提案した．AIR 化された異常検知手法は，他の異常検知手法と連携・競合することで，最適なリソース配分と高度なインシデント検知を可能とする．ここでは，まず異常検知手法の運用プロセスをモデル化し，運用時に要される知識を示した．

今後の設計方針としては，示された知識を AIR の構造上に分配し，その仕様を策定する．その上で，目的の機能に関する動作実験，システム側への負荷に関する評価について検討を行っていく．

参考文献

[1]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).
[2]oinkmaster，http://oinkmaster.sourceforge.net/
[3]向坂真一 他，“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).
[4]高田哲司 他，“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).