AIR-NMSにおけるネットワーク障害切り分け機能の設計と実現

今野 将* 吉村 智志†§ 岩谷 幸雄‡ 阿部 亨* 木下 哲男*

概要 近年のネットワークは，ますます大規模・複雑になり，障害への対応など，これを管理する作業にも，より高度な知識と煩雑な処理が要求されてきている．このように増大し続けるネットワーク管理作業の負担軽減を図るために，我々は能動的情報資源(AIR)の概念を用いたネットワーク管理支援システム(AIR-NMS)を提案している．AIR-NMSは，能動的情報資源の概念を用いることで，ネットワーク内に分散する機器・アプリケーションの各種状態情報や管理者の経験的知識をエージェントとして構造化し，各々にAIRとしての能動性を与えている．これにより，AIR自身が，自律的に連携・協調を行い，ネットワーク障害に関する「障害の検知・状況の把握・原因の特定」を効果的に代行できるようになっている．本稿では，このAIR-NMSの主要機能の一つであるI-AIRに焦点をあて，ネットワークを自律的に監視し管理作業を効果的に支援するシステムを提案し，さらに，試作システムによる評価実験の結果を基に提案システムの有効性を議論する．

Design and Implementation of Classification Function of Network Faults in AIR-NMS

Susumu KONNO *, Satoshi YOSHIMURA †§, Yukio IWAYA ‡, Toru ABE * and Tetsuo KINOSHITA *

Abstract In recent years, with increasing the scale and complexity of network systems, advanced knowledge and complicated procedures are strongly required for managing network systems. To reduce the burden of network management, we proposes a novel system based on active information resource that is called AIR-NMS, for monitoring network status and supporting network management. By employing the concept of active information resource, in the AIR-NMS, the status information of each device and each application distributed and the experimental knowledge of network management in the network is structured as an agent and provided with autonomy. Consequently, through the cooperation with those agents, they monitor network failures autonomously and support network management actively. In this paper, we focus on I-AIR that is one of the prime functions of the AIR-NMS, and propose the system that supports network management.

1 まえがき

近年，ネットワーク管理者がネットワークシステムの監視・維持・管理を行うために必要な労力や専門的知識は増加・高度化の一途を辿っている．現在，この問題に対処するために，いくつかのネットワーク管理支援システムが提案・商品化されている[1, 2, 3, 4, 5, 6, 7, 8]．しかしそれらの多くは，監視・維持・管理に必要な機器の状態情報や一般的な対応策を管理者へ提示するに留まり，情報の総合的な判断や具体的対策の決定は依然として管理者の側に委ねられている．

これに対し筆者らは，能動的情報資源(Active Information Resource: AIR)[9]の概念を各機器の状

*東北大学情報シナジーセンター，Information Synergy Center, Tohoku University.
†東北大学情報科学研究科，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.
§現在，(株) 日立製作所

態情報や管理に関する諸知識へ適用することで，これらを自律的に連携・協調させ，ネットワークの管理を支援するシステム (AIR-based Network Managment Support System: AIR-NMS) の提案をしている．本稿では，このAIR-NMSの主要機能の一つであり，ネットワーク監視に重点をおいた能動化された状態情報エージェント (Status Information AIR: I-AIR) に焦点をあてる．そして，I-AIRによるネットワーク障害の切り分け機能の設計を行い，試作システムを構築し，I-AIRを用いたネットワーク管理支援システムによるネットワーク管理者の負荷軽減の効果を確認し，提案システムの有効性について議論する．

2 能動的情報資源を用いたネットワーク管理支援システム (AIR-NMS)

2.1 能動的情報資源 (AIR)

能動的情報資源 (AIR) は，情報資源の構造を強化することで，利用者の要求へ各情報資源を能動的・自律的に対応させ，情報資源のより高度な活用を図る機構である．具体的には，各情報資源（コンテンツ）に利用支援知識および利用支援機能を付加したエージェントとしてAIRを構成し，利用支援知識・機能を用いAIR相互間で連携・協調処理を行わせることにより，利用者からの処理要求（例えば，コンテンツ検索・統合・分析など）をAIR側（すなわちコンテンツ側）で自律的に実行させるものである．このとき，AIRが実際に活動する作業空間をAIRワークプレースと呼び，利用者からの処理要求はAIRインタフェースを介してワークプレース内の各AIRへ伝達される．

2.2 AIRを用いたネットワーク管理支援

通常，ネットワークシステムを管理するための一連の作業は，ネットワークを構成する各機器の状態や履歴などネットワーク内に分散した種々の情報と，管理者が持つ経験的知識とを用いることで順次処理されていく．例えば，図1 (a) に示すネットワークシステムにおいて，サブネットA内のPCからサブネットB内のサーバへのアクセスに障害が生じた場合，現状では，管理者が自らの経験的知識を用いて以下に示す作業1〜5を行う必要があり，その労力

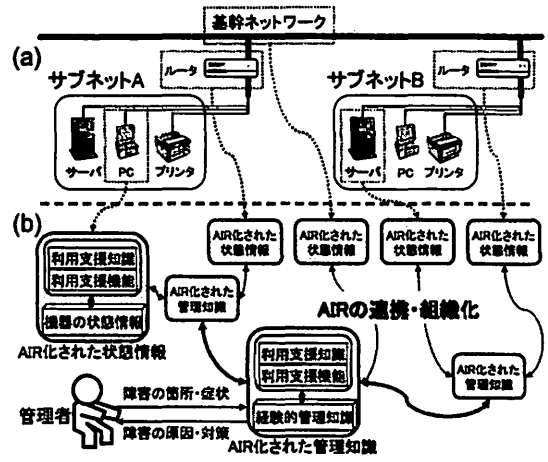

図 1: ネットワークシステムとAIR-NMS

はネットワークの規模に応じて膨大なものとなる．

作業 1 PC/ルータ/ネットワークの状態情報の収集
作業 2 収集された状態情報の統合
作業 3 障害の原因の特定
作業 4 障害への適切な対策の決定
作業 5 決定された対策を実際に適用

このようなネットワークシステム管理の場面で，各機器の状態情報や知識ベースに蓄積された管理者の経験的知識を情報資源とみなしAIR化すれば (図1 (b))，管理作業の大部分（前述の例ならば作業1〜4）をAIRの連携・協調処理により自律的に実行させることができ，管理者の労力を大幅に削減することが可能となる．また，AIRの導入により，経験的知識の継承や修正・追加，あるいは機器構成の変更への対応が容易になるため，より高度かつ柔軟なネットワーク管理が実現できる．

筆者らは，このような考えに基づくネットワーク管理支援システムとしてAIR-NMSを提案しており，AIR-NMSの構成要素として，管理者の経験的知識を持つAIRをK-AIR (Management Knowledge AIR)，ネットワーク構成機器の状態情報を持つAIRをI-AIRとし設計を行ってきた．本稿では，このうち状態情報を能動化したI-AIRに焦点を絞り，I-AIRを用いたAIR-NMSを試作し，ネットワーク管理者へのネットワーク障害の切り分け効果について実験を行った．

2.3 I-AIRによる自律的なネットワーク管理支援システム

ネットワーク上の状態情報をAIR化したI-AIRは，自身の保持している情報資源に働きかけることによって定期的にネットワークの状態の調査を行なう．

一般的に，ネットワーク管理者がネットワークを管理する場合，管理者は管理コンピュータを介して管理コマンドを使用し，情報の収集・解析を行い，必要に応じ再収集を繰り返す．一方，I-AIRによる管理方法は管理者が行なうべき作業をI-AIRの定期調査によって代行することで管理者の手をほとんど煩わすことのないネットワーク管理を実現している．またI-AIR同士の協調・連携によってネットワーク全体の情報を容易に収集し，障害に関する重要情報をI-AIRが自律的に抽出・切り分けし提供することが可能である．

このようにI-AIRによる自律的なネットワーク管理支援システムを実現することで管理における一連の作業を，特にネットワーク障害の切り分け作業を代行し管理者の負担を軽減することが可能となる．

3 I-AIRによるNMSの試作

I-AIRは，ルール型の知識に基づき自律的・能動的に活動するプログラムとして実装されるが，その実現方法としてマルチエージェントシステムを用いる方法が提案されている [10, 11, 12]．これはAIRの持つ，“知識に基づいて活動を行う”，“複数のAIRが協調・連携を行い問題を解決する”，“外部からの要求・イベントに応じて活性化される” 等の特徴を実現する上で，マルチエージェントシステムが提供する機能や動作特性が効果的に活用できることによる．

そこで，本稿では分散環境上でAIRを実現するためにADIPS/DASHフレームワーク [13, 14] を用いてI-AIRを実現する．ADIPS/DASHフレームワークを用いることで，AIRは，ルール型知識として与えられた利用支援知識に基づき，Javaプログラムとして実装された利用支援機能を起動し，情報資源の加工処理や他のAIRとの連携・協調処理を実行する．

連携・協調処理を行ったI-AIRらは，利用支援知識・機能を用いて現在ネットワークに起こっている障害の特定を行う．その後，特定した障害とその原因についての詳細を管理者にインタフェースを介して提示することで，管理者のネットワーク管理作業の支援を行う．

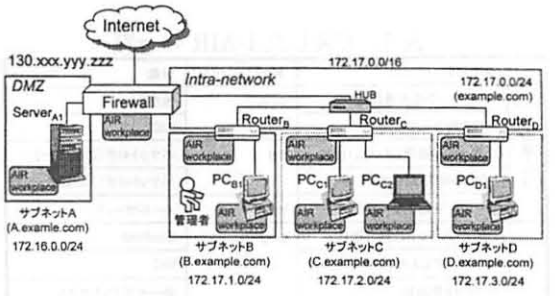

図 2: 実験ネットワーク概要図

4 実験と評価

4.1 実験環境

本稿では，図2に示すようなNAT機能を実現したファイアウォール，ルータ，各種PCから成り，4つのサブネットから構成されるネットワーク環境上に表1に示すI-AIRを実装し実験を行った．なお，今回の実験において，I-AIRは障害を観測する状態時に効果を発揮する観測用I-AIRと障害を調査する状態時に効果を発揮する調査用I-AIRの2種類に分類され，機能目的や対象に応じて20種類のI-AIRを実装し，各ノード上に平均15個の全体で約140個のI-AIRを実験ネットワーク上に配置した．

4.2 実験方法

ネットワーク上に発生する障害は，物理層からアプリケーション層にいたるまで様々な要因が考えられる．もちろん，一つの障害状況であっても，複数の原因が想定される場合があり，検証する層は一つに留まらない．また，ユーザから報告される障害の状況は，時として具体的でなく，それだけでは状況を把握できない場合も多い．障害報告を受けた管理者は，その障害がどこの層のどんな原因によるものであるかを自信がもつノウハウと経験によって切り分けていく必要がある．本実験は，このような切り分けが必要な状況を実験ネットワーク上に作り出し，被験者たる複数の管理者に対して，問題の切り分け，修復行為をさせることで，試作したNMSの効果とその範囲を検証した．

表 1: 実装した I-AIR の一覧

	機能目的	実行コマンド名	対象
観測用ツール	ネットワークの不通検知	ping	他ホスト
	NICの設定ミス検知		NIC
	大量メール送信(スパム)検知	cat	パケットログ(25番ポート)
	MSBlaster攻撃の検知		パケットログ(135番ポート)
	メール送受信エラー検知	telnet	メールサーバ
調査用ツール	TCP/IPスタックの異常検知	ping	localhost
	NICの設定ミスの検知		NIC
	ハブの障害検知		同一セグメントホスト
	ルータの障害検知		異なるセグメントホスト
	上位ホストとの通信障害検知		上位ホスト
	下位ホストとの通信障害検知		下位ホスト
	各サーバのプロセス稼動検知	ps	DNSサーバ
			SMTPサーバ
			POPサーバ
	DNSへの接続検査	nslookup	DNSサーバ
	所定ホストへの経路調査	traceroute	サーバ
	カーネル情報の調査	dmsg	localhost
	リースIPに関する調査	cat	dhcpリースログ
	メールサーバでのエラー調査		メールログ
	メール送信数によるスパム調査		

被験者は，ネットワークの管理経験（1 年から 7 年）を持つ 5 人の学生である．被験者は，試作した NMS 端末の前に着座し，実験者から障害報告を受ける．用いた障害状況は，後述するように障害報告のみでは分からない複数の原因が想定されるものを用いた．被験者は，障害報告を受けた後，NMS から報告されるネットワークの状態情報を利用して，検証すべき障害原因を切り分け，必要な回復行為を行うよう教示した．このとき，被験者が障害を解消するまでに要した時間と，回復に費やした手順（コマンド単位）を計測した．また，基準として試作 NMS を使わない場合の回復行為についても計測を行った．

実験に用いた障害状況を表 2 に示す．物理層，TCP/IP 層，アプリケーション層の 3 つの層において複数の障害原因が考えられる 4 つの状況について各被験者ごと計測した．なお，試作 NMS を用いた場合に設定した障害原因は表中の網掛け部分である．各障害状況の詳細は，以下の通りである．

障害 1：ホスト PC_{B1} に接続できない ある特定ホストに接続できない場合．考えられる主な障害原因としては，NIC(Network Interface Card) の設定ミス，ケーブルの断線などの物理層に近い原因，当該ネットワークポートが閉じている場合，あるいは閉じていなくてもそのサービスが提供されていない場合などが考えられる．今回は，PC_{D1} から PC_{B1} へファイル転送・接続ができない障害が報告された場合を想定し，物理層の障害として NIC の設定ミスを特定することとした．

障害 2：偽装型スパムメールが送信されてくる 障害報告としてスパムメールが送信されてくるのみが与えられる．管理者は，スパム送信ホストを特定し，それが自身の管理するネットワーク内から発信されていれば，それを切り離す必要がある．今回は，内部ホスト PC_{D1} から送信元を外部のホスト偽装し送信される偽装型のスパムメールが大量に送信されている場合を想定し，送信ホストが自ネットワークの内部か外部かの切り分けとケーブルの切り離しまでに要する測定をした．

障害 3：ネットワークが遅い 単に「ネットワークが遅い」といった漠然とした状況を報告された管理者は，多様な原因を想定しさまざまな検証を行う必要がある．単にケーブル劣化による接触不良である場合や，異常なホストがネットワーク上に存在し，不正なパケットの発生のためにネットワーク帯域を圧迫している可能性も考えられる．後者の場合，その不正ホストは何か，さらに不正なパケット発生の理由は何かを切り分けていく必要がある．今回は，頻繁にネットワークに接続・切り離しが行われるノート PC(PC_{C2}) が外出時に MS Blaster に観戦し，そのまま自ネットワークに接続したために，MS Blaster の攻撃が発生し，ネットワーク帯域を浪費した結果，ユーザの通信速度に影響が出たという状況を把握し，PC_{C2} を切り離すまでに要する時間を測定した．

障害 4：メールの送受信ができない アプリケーション層に現れる障害は，それ以下の層での原因からアプリケーション自体の設定ミス，サーバにおける設定などその多様性が一番顕著となる．また，この障害報告のように障害が「送信」，「受信」どちらに生じているのかすら不明の場合もあり得るため，管理者の検証範囲は相当広くなる．今回は，SMTP サーバのプロセスがダウンしていたために，ネットワーク上のクライアントからの送信ができないという障害を特定することとした．

表 2: ネットワーク階層毎にみた障害状況と原因

ネットワーク階層	障害状況	考えられる障害原因
物理層	1．ある特定のホストに接続できない	NICの設定ミス
		ケーブルの断線
		接続ポートが閉じている
		サービスが提供されていない
TCP/IP層	2．偽装型スパムメールが送信されてくる	内部のホストから送信
		外部のホストから送信
	3．ネットワークが遅い	ケーブルの劣化
		ネットワークに大量のパケットが流出している
アプリケーション層	4．メール送受信が出来ない	ケーブルの断線
		接続ポートが閉じている
		サービス設定ファイルミス
		SMTP、POPサーバプロセスダウン

4.3 実験結果と考察

実験結果を表 3〜6 に示す．実験結果から，各障害において手順・時間ともに I-AIR 未使用時の作業量の約 15%近くに軽減されるという結果が得られた．

各実験結果より，被験者の管理経験年数の面から見ると管理に対する経験量の差を埋めることが可能となり，概ね管理者の負担軽減が行えたといえる．ただし，“障害 3：ネットワークが遅い” における管理者 C のように I-AIR を用いた場合のほうが時間・手順ともに数字が大きくなってしまうケースも確認できた．この原因を探るために，実験後に管理者 C に確認したところ，I-AIR の提示する情報の一部に，無加工のログ情報が含まれており，そこから障害状況を読み解くのに時間がかかったためであることが分かった．これより本システムをより良いシステムとしてゆくには，I-AIR が提示する情報に対して管理者に理解しやすい形式に加工する機能が必要であると考えられる．

発生させる障害に関して考察すると，試作システムを使わない場合，対応するネットワーク階層がアプリケーション層のように高い階層に原因があると相対的に時間がかかることがわかった．これは管理者がネットワーク調査時に ping のように比較的低い階層から調べてゆく傾向があるために高い階層に原因のある障害には検知・復旧に時間がかかることが原因だと考えられる．しかし I-AIR を用いた場合，階層にとらわれることなく，全ての階層で同時に調査を行うため，どの階層の障害でも短時間で検知・情報提供することが可能である．実験からは管理者の負荷軽減率はアプリケーション層において特に大きくなり（負担がより軽減され），アプリケーション層に原因がある障害には I-AIR がより有効であることが示された．

表 3: 障害 1：ホスト PC_{B1} に接続できない

	A(管理経験7年)		B(管理経験2年)		C(管理経験1年)	
	時間(秒)	手順数	時間(秒)	手順数	時間(秒)	手順数
I-AIR未使用	282	40	756	20	1056	20
I-AIR使用	52	2	51	2	99	5
I-AIR使用/未使用(%)	18.4	5.0	6.7	10.0	9.4	25.0
	D(管理経験3年)		E(管理経験2年)		平均	
	時間(秒)	手順数	時間(秒)	手順数	時間(秒)	手順数
I-AIR未使用	771	20	680	22	709	24.4
I-AIR使用	226	5	125	4	110.6	3.6
I-AIR使用/未使用(%)	29.3	25.0	18.4	18.2	15.6	14.8

表 4: 障害 2：偽装型スパムメールが送信されてくる

	A(管理経験7年)		B(管理経験2年)		C(管理経験1年)	
	時間(秒)	手順数	時間(秒)	手順数	時間(秒)	手順数
I-AIR未使用	92	5	221	4	1096	24
I-AIR使用	40	2	93	3	49	3
I-AIR使用/未使用(%)	43.5	40.0	42.1	75.0	4.5	12.5
	D(管理経験3年)		E(管理経験2年)		平均	
	時間(秒)	手順数	時間(秒)	手順数	時間(秒)	手順数
I-AIR未使用	1170	26	901	23	696	16.4
I-AIR使用	129	2	83	4	78.8	2.8
I-AIR使用/未使用(%)	11.0	7.7	9.2	17.4	11.3	17.1

表 5: 障害 3：ネットワークが遅い

	A(管理経験7年)		B(管理経験2年)		C(管理経験1年)	
	時間(秒)	手順数	時間(秒)	手順数	時間(秒)	手順数
I-AIR未使用	682	35	205	3	208	3
I-AIR使用	94	1	53	1	528	4
I-AIR使用/未使用(%)	13.8	2.9	25.9	33.3	253.8	133.3
	D(管理経験3年)		E(管理経験2年)		平均	
	時間(秒)	手順数	時間(秒)	手順数	時間(秒)	手順数
I-AIR未使用	323	3	330	9	349.6	10.6
I-AIR使用	63	1	61	1	159.8	1.6
I-AIR使用/未使用(%)	19.5	33.3	18.5	11.1	45.7	15.1

表 6: 障害 4：メールの送受信ができない

	A(管理経験7年)		B(管理経験2年)		C(管理経験1年)	
	時間(秒)	手順数	時間(秒)	手順数	時間(秒)	手順数
I-AIR未使用	1499	49	369	16	996	31
I-AIR使用	73	2	59	2	98	4
I-AIR使用/未使用(%)	4.9	4.1	16.0	12.5	9.8	12.9
	D(管理経験3年)		E(管理経験2年)		平均	
	時間(秒)	手順数	時間(秒)	手順数	時間(秒)	手順数
I-AIR未使用	565	7	680	22	821.8	25
I-AIR使用	81	2	125	4	87.2	2.8
I-AIR使用/未使用(%)	14.3	28.6	18.4	18.2	10.6	11.2

5 まとめ

本稿では，AIR の概念をネットワーク管理支援システム AIR-NMS の構成要素の 1 つである I-AIR に焦点をあて，I-AIR を用いた自律的なネットワーク管理支援システムを試作した．そして，実際のネットワークを模して構築した実験ネットワークにおいて，試作した I-AIR を用いて実験を行い，I-AIR がネットワーク管理に必要な一連の作業の多くを，特にネットワーク障害の切り分け作業を代行することにより，ネットワーク管理者の負担を大幅に軽減し，管理者に依存しない柔軟で幅広い管理支援を行なえることを確認した．特に，アプリケーション層に原因がある障害には I-AIR がより有効であることが確認できた．

今後，提案手法に基づく実用的な知的管理支援ツールの実現を目指して，実環境での実験を含めた検討を継続して行ってゆく予定である．

謝辞

本研究の一部は，日本学術振興会 科学研究費補助金 若手研究 (B)(16700048) 及び，総務省戦略的情報通信研究開発推進制度 (SCOPE) 特定領域重点型研究開発 次世代ネットワーク技術 (031102005) の支援により行われた．

参考文献

[1] Stephan, R., Ray, P. and Paramesh, N.: Network Management Platform based on Mobile Agent, *International Journal of Network Management*, Vol. 14, pp. 59–73 (2003).

[2] Baker, S. M. and Moon, B.: Scalable Web Server Design for Distributed Data Management, *15th International Conference on Data Engineering*, p. 98 (1999).

[3] Consens, M. and Hasan, M.: Supporting network management through declaratively specified data visualizations, *IEEE/IFIP 3rd International Symposium on Integrated Network Management*, pp. 725–738 (1993).

[4] Cabri, G., Leonardi, L. and Zambonelli, F.: Network Management based on Mobile Agents using Programmable Tuple Spaces, *4th International Conference and Exhibition on The Practical Application of Intelligent Agents and Multi-Agents* (1999).

[5] Hasan, M., Sugla, B. and Viswanathan, R.: A conceptual framework for network management event correlation and filtering systems, *IEEE/IFIP 6th International Symposium on Integrated Network Management*, pp. 233–246 (1999).

[6] Virmani, A., Lobo, J. and Kohli, M.: Netmon: Network management for the SARAS softswitch, *IEEE/IFIP Network Operations and Management Symposium*, pp. 803–816 (2000).

[7] Damianou, N., Dulay, N., Lupu, E., Sloman, M. and Tonouchi, T.: Tools for domain-based policy management of distributed systems, *IEEE/IFIP Network Operations and Management Symposium*, pp. 203–218 (2002).

[8] Satoh, I.: Building Reusable Mobile Agents for Network Management, *IEEE Transactions on Systems, Man and Cybernetics*, Vol. 33, No. 3, pp. 350–357 (2003).

[9] 木下哲男: 分散情報資源活用の一手法 — 能動的情報資源の設計 —, 信学技報 AI99-54, pp. 13–19 (1999).

[10] Li, B., Abe, T. and Kinoshita, T.: Design of agent-based active information resource, *The 1st International Conference on Agent-Based Technologies and Systems*, pp. 233–244 (2003).

[11] Konno, S., Iwaya, Y., Abe, T. and Kinoshita, T.: Design of Network Management Support System based on Active Information Resource, *The 18th International Conference on Advanced Information Networking and Applications*, pp. 102–106 (2004).

[12] 今野将, 吉村智志, 羽鳥秀明, 岩谷幸雄, 阿部亨, 木下哲男: 能動化された状態情報に基づくネットワーク管理支援方式, 情報処理学会論文誌, Vol. 46, No. 2, pp. 493–505 (2005).

[13] 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指向アーキテクチャ, 情報処理学会論文誌, Vol. 37, No. 5, pp. 840–852 (1996).

[14] DASH GROUP: *DASH - Distributed Agent System based on Hybrid architecture.* [Online].Available: http://www.agent-town.com/dash/.