分散オブジェクト技術を用いた ネットワーク監視システムの設計

知念 眞也† 長田 智和† 谷口 祐治‡ 玉城 史朗†
†琉球大学 理工学研究科 ‡琉球大学 情報処理センター

概要

近年のインターネット技術の発達により，企業や大学などのネットワークは大規模化・複雑化してきている．そのような大規模ネットワークでは，運用管理ポリシーの異なる複数のサブネットワークが混在しているため，ネットワーク監視システムは分散監視型で構築すべきである．またそのシステムは，ネットワーク構成の変化や機能追加・削除に柔軟に対応できるシステムである必要がある．ゆえに本稿では，分散オブジェクト技術であるモバイルエージェント (Aglet) を用いて，大規模分散ネットワークにおいて十分な柔軟性，発展性を持った分散監視システムを提案する．

Design of a network monitoring system with distributed object technology

Shinya CHINEN † Tomokazu NAGATA †
Yuji TANIGUCHI ‡ Shiro TAMAKI †

†Graduate School of Science and Engineering, University of the Ryukyus
‡Center for Integrated processings, University of the Ryukyus

Abstract

In recent years, the networks such as a company or a university become large scale and complication by the development of internet technology. Such large networks, a network management systems must construct a distributed system, Because the plural subnetworks which have different management policy exist. Also, the system has to cope with a change of network flexibly and an addition the function.

In this note, we propose a flexible and possible distributed network managemen system constructed by mobile agent (Aglet).

1 はじめに

近年のインターネット技術の発展により，企業や大学などのネットワークは大規模化しており，組織の構内ネットワークには FDDI，ATM，GigabitEthernet 等の様々な回線網が混在する複雑な形態が増えてきた．そのような大規模ネットワークにおいては，各サブ

ネットワークごとに異なる運用管理ポリシー(AUP:Acceptable User's Policy)が存在することが多く，従来の集中監視型ネットワーク管理システムでは対応が困難である．故に，AUP毎のネットワークを管理する分散監視型管理システムを構築する必要がある．また，ネットワーク構成変更や新しいネットワーク攻撃などの理由により，ネットワーク監視内容は多種多様になり，市販のネットワーク管理システムでは柔軟に対応することは困難である．つまり，ネットワーク管理は非定型的で変化するものであるため，スケーラブルな監視システムでなければならない．

そこで本研究では，分散オブジェクト技術であるモバイルエージェントを利用し，大規模な分散ネットワーク環境下においても柔軟に対応できる分散監視型システムを提案する．

本稿では，第2節で従来型の監視システムの問題点とその改善策を挙げる．第3節では，提案するネットワーク分散監視システムの構成を述べ，第4節では実際のネットワークへの実装例を説明する．そして第5節で課題を挙げ，第6節でまとめを述べる．

2 従来のネットワーク管理システム

2.1 問題点

一般に SNMP(Simple Network Management Protocol) を用いた集中監視型のネットワーク管理システムは，マネージャ(管理装置)とエージェント (管理対象機器) により構成され，マネージャがエージェントに一対一でポーリング (問い合わせ) を行って情報を収集し，それらの情報をもとにネットワーク状態を判断し管理を行う．また、トラップ機能により障害の通知を行う．小規模の LAN の場合，基本的には1台のマネージャが複数台のエージェントを全て監視するという構成となり (図1)，大規模な，LAN や WAN を介したネットワークとなると，それぞれの拠点ごとにマネージャを配置し，さらにそのマネージャを統括するマネージャを配置して全体の監視を行う．そのように監視対象ネットワークが大規模になると，ネットワーク構成変更に伴う監視システムの構成変更が困難となり，大規模であるゆえマネージャ間の通信におけるコストやセキュリティ等が問題となってくる．

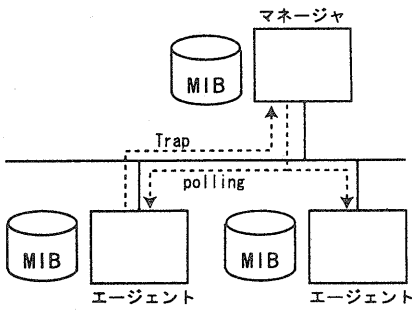

図 1: SNMP の構成

また，市販のネットワーク管理ソフトやシステムでは，限られた項目でしか監視，及び障害検出を行えないことが多く，様々なネットワーク攻撃が発生している今日では，従来通りの障害検出法では検出できない攻撃も増えている．そして大規模ネットワークにおいては，サブネット特有のトラフィックパターンによる障害検出の必要性も考えられる．このような新しい機能の追加や不必要になった機能の削除が柔軟に行えないと，大規模ネットワークで使用するに当たって問題が生じてくる．

2.2 提案システムでの改善法

提案するシステムでは，ネットワーク管理システム自体をモバイルエージェントの集合として構築することで問題点の改善を行う．本システムでは，モバイルエージェントにデータ処理・収集機能を持たせることで通信トラフィックの削減及び処理の分散化を図ることができ，また，モバイルエージェント自身のセキュリティ機能を利用することで，移動中のセキュリティもより安全に確保することができる．そして，システムが様々な機能を持ったエージェントの集合であり，エージェントの移動・消滅により機能追加・削除が行われるため，柔軟性・発展性を持ったシステムを構築できる．

3 モバイルエージェントを用いたネットワーク監視システム

本システムでは，モバイルエージェント技術としてIBMが提供するAgletsを用いる [5]．Agletsとは，移動エージェントプラットフォームの一つであり，Agletsによって実装された移動エージェントはAgletと呼ばれる．Agletは Javaで記述されたクラスとして実現され，エージェントの移動能力とエージェント間対話能力を持つ [5]．Agletには，生成 (Creation)，消滅 (Disposal)，移動 (Dispatch)，到着 (Arrival)，非活性化 (Deactivation)，活性化 (Activation) のイベントがあり，エージェントサーバがその状態遷移を行う．

本監視システムは様々な機能を持ったAgletsによって構成されるため，両ホストにはJava実行環境及びAglets実行環境が整っているものとする．両ホストでは，基本的なエージェントサーバアプリケーションが常時動作しており，そのサーバを通してAgletの送受信などを行う．

以下，提案するネットワーク監視システムの構成を述べていく．

3.1 システム構成

本システムはAgletの集合によって構成され，そのAgletグループの機能によって大きく二つのホストに分けられる．一つは主に監視機能をもつ監視Agletグループで構成される監視ホストで，もう一つは主に監視ホストとのやり取りを行う統括Agletグループで構成される統括ホストである．(図2)．

(1) 統括ホスト (統括Agletグループ)
統括ホストは監視対象ネットワークに最低1台設置され，ベースとして以下の機能を持つAgletグループによって構成される．

a. 監視ホストの巡回によるデータ収集・生存確認
ネットワーク内の監視ホストを巡回し監視データを収集する．Agletは巡回する監視ホストのリストを持っており，そのリストを参照して巡回を行う．監視ホストへ移動できない場合は，何度か移動を試みた後，現在まで収集したデータと残りの監視ホストのリストを持って統括ホストへ帰還する．そして現在まで収集したデータを統括ホスト内に保存し，残りの監視ホストのリストを持ち再度巡回を行う．また，この巡回により監視ホストの生存確認も同時に行う (図3)．

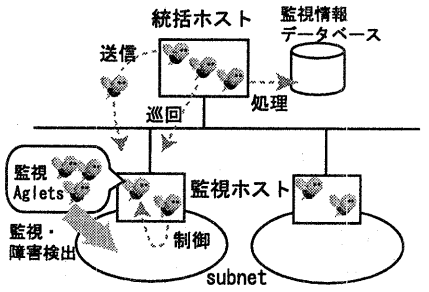

図2: 基本システム構成

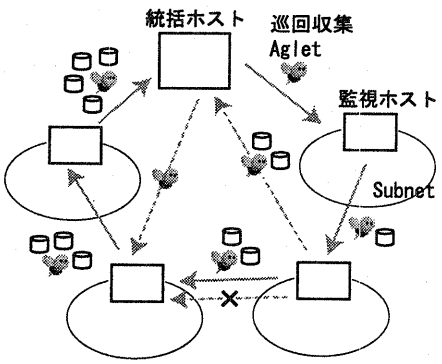

図3: 管理情報収集

b. 監視機能を持ったAgletの送信
管理者によって選択された，新たに監視ホストに追加する監視機能を持ったAgletを監視対象ネットワーク上の監視ホストへ送信する．又は，監視ホストからの要求 (監視機能を持つAgletが消滅

した場合など)によって，該当するAgletを送信する．

c. データ処理
収集したデータに対して，データの統合や解析等の処理を行う．

d. 他統括ホストとの通信
他ネットワーク上に配置された統括ホストに対して，そのネットワーク上に配置された監視ホストへ監視機能を持ったAgletの追加要求の送信や，収集されたデータの送受信等を行う．他ネットワークに対する通信は全て統括ホスト間でのみ行う．

(2) 監視ホスト (監視Agletグループ)
監視ホストは監視対象ネットワーク上の適切なセグメントごとに設置され，ベースとして以下の機能を持つAgletグループによって構成される．

a. 監視対象ネットワークの監視・障害検出
統括ホストから送信された様々な監視機能を持つAgletによって，対象ネットワークの監視・障害検出を行う．この対象ネットワーク監視に必要な機能を持ったAgletは，全て統括ホストから送信される．

b. 監視機能を持つAgletの制御
監視ホスト上で動作している監視機能を持つAgletの起動・停止・再読み込みなどの制御を行う．

統括ホストが何らかの理由で停止した場合は，他の統括ホストや監視ホストでその代理を行う．代理を行うホストでは，統括ホストを動作させるのに必要なAgletが非活性化状態で待機しており，定期的な統括ホストの生存確認において，もし統括ホストが停止している場合には待機させておいたAgletを活性化させ統括ホストの代理を行う．その後統括ホストが復旧すると，一時的に保存しておいた収集データを統括ホストへ送信する．その状況において監視ホストは，統括ホスト検索順の格納されたファイルを保持しており，その順序に従って統括ホストを決定する．

監視ホスト停止の場合も，統括ホストとほぼ同様にして代理を行う．しかし代理を行うホストの設置場所によっては行えない監視機能が存在するため，代理ホストでは可能な範囲での監視機能代理を行う．

このようにして両ホストにおいて代理機能をもたせたホストを置くことで，システムを連続稼動させることが可能となる．

3.2 大規模分散ネットワークへの適用

本システムを大規模分散ネットワークに適応させる場合，その構成は図4に示す形となる．

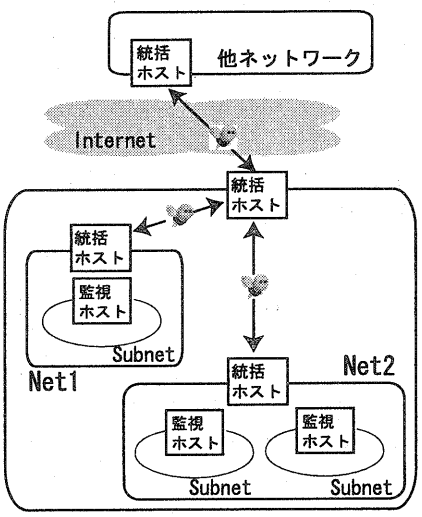

図4: 大規模分散ネットワークへの適用

基本的には，それぞれの組織のネットワークの形態に応じて監視ホストを分散配置し，それらをまとめる統括ホストを一つ配置するという構成となる．各組織間の通信は統括ホスト間でのみ行う．組織内にAUP(又はsub-network)が複数存在する場合は，そのAUP毎に統括ホストを設置し，各AUP間のデータのやり取りは統括ホスト間でのみ行う．つまり，監視ホスト

は統括ホストを通してのみ他AUP及び他組織とのデータのやり取りが行える．

本システムでは，統括・監視ホストにおける一つ一つの機能はそれぞれ独立したAgletが担っているため，統括ホストに監視機能を持たせること，またその逆も可能である．したがって，監視対象ネットワークの形態に応じて柔軟な構成を取ることができる．

4 運用システムへの実装

本監視システムの実装・検証は，琉球大学の実験ネットワーク及び，沖縄県地域IXのネットワークであるOIX(Okinawa Internet eXchange) [6] 参加組織のネットワーク上にホストを設置し，動作確認等を行っている．このOIX参加組織には大小さまざまな組織が存在するため，本監視システムの分散ネットワークにおける実験環境としては非常に有効である．設置ホスト構成としては，琉球大学情報工学科には統括ホストとしてWindows2000ホストを1台，監視ホストとしてUNIXホストを1台，琉球大学総合情報処理センターには統括ホストとしてUNIXホストを1台，監視ホストとしてUNIXホストを2台，OIX参加組織のISP一社に統括・監視ホストとしてUNIXホストを1台となっている (図5)．これらホストにおいて，Aglet環境を構築後Agletサーバを起動し，OIXの共同研究の一つとして行っているトラフィック統計と連携させた，Tcpdumpによるトラフィック統計を行う機能を持つAgletによるトラフィック統計 (図6) と，そのデータの巡回収集を行っている．

このように本システムをWANを経由するようなネットワークにおいて構築する場合，考慮しなければならないのがセキュリティである．ネットワーク攻撃に対するセキュリティ要件としては機密性・完全性があり，第3者にエージェントの中身を盗聴されないよう保護しなければならない．その他に，エージェントに関しての認証・アクセス権限による制限を行うことも重要である．そこで実装したAgletでは，前者に関してはAgletサーバ間の通信を行うATP(Agent Transfer Protocol)の下位層にSSLを利用して通信路を暗号化することでAgletの保護を行い，また，後者に関しては，Java2で示された細粒度アクセス制限モデルを参考にしたAglets Security Policyファイルによる制限と，Agletサーバにおけるセキュリティドメイン認証 [5] を用いて問題点の解決を行う．

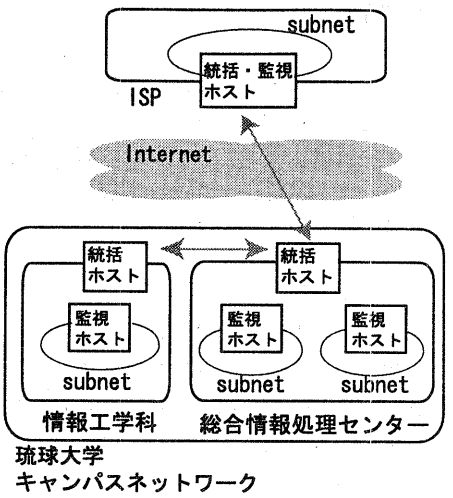

図 5: 実装環境

>>> total	393593(100.000) :	71347132(100.000)
>>> tcp protocol	343089(87.168) :	65675192(92.050)
< irc >	162748(41.349) :	12472601(17.482)
< nntp >	60532(15.379) :	6593201(9.241)
< pop3 >	11293(2.869) :	5412759(7.587)
< tcp >	19392(4.927) :	3381775(4.740)
< www >	89124(22.644) :	37814856(53.001)
>>> udp protocol	27320(6.941) :	2588192(3.628)
< ntp >	175(0.044) :	15750(0.022)
< snmp >	5703(1.449) :	638584(0.895)
< udp >	21442(5.448) :	1933858(2.710)
>>> misc protocol	23184(5.890) :	3083748(4.322)
< dns >	3411(0.867) :	506782(0.710)
< icmp >	8882(2.257) :	772840(1.083)
< rip >	10891(2.767) :	1804126(2.529)

図 6: トラフィック統計例

5 今後の課題

現在は，提案するシステムの基盤となる部分の実装と検証を行っている．今後は以下の点に重点を置き，実装・検証を行う．

(1) 統括・監視ホスト移動
ネットワーク構成変更によるホスト移動を，セキュリティを考慮に入れ，スムーズで柔軟に行えるシステムの実装を行う．

(2) 経路制御
モバイルエージェントでは，エージェント自身がマルチホップの通信経路を動的に決定することが可能である．それを利用し，データ巡回収集 Aglet において通信路の状態やバンド幅に応じた経路制御を行い，より効率的な巡回方法を実装する．

(3) 障害予測
単純な閾値を用いた障害検出ではなく，各監視ホストから収集されたデータをに基づき，過去の履歴の比較，データ解析等による障害予測を行う．

(4) 監視機能 aglet の追加
現在は tcpdump を用いたトラフィック統計 Aglet を用いて，ネットワークの監視を行っているが，今後は SNMP 等も利用して様々な監視を行う Aglet の追加を行っていく．

6 まとめ

本稿で提案してきたネットワーク監視システムでは，分散オブジェクト技術であるモバイルエージェント (Aglet) を導入したシステムを構築した．大規模分散ネットワークという環境においては，モバイルエージェントの利点 (スケーラブルなシステム，断続的な通信への対応，遠隔評価，自律行動等) が十分に発揮できることが言えるであろう．また，Java ベースである Aglet を使用することでプラットフォーム非依存のシステム構築が可能である．

既存の管理手法と比較すると，本管理システムでは以下の点で有効であると考えられる．

(1) プラットフォーム非依存
(2) 大規模分散ネットワークへの適用
(3) システムのスケーラビリティ
(4) 管理トラフィックの削減
(5) システムの連続稼動
(6) セキュリティ

今後は，第 5 章で挙げた項目に関する実装を行い，引き続きネットワーク監視システムの設計及び実装と検証を行っていく．

参考文献

[1] 長田智和，谷口祐治，玉城史朗，“ネットワーク管理におけるモバイルエージェントを用いた自立分散システムの適応”，計測自動制御学会第 12 回自立分散システム研究会，pp.59-62，2000

[2] 一井信吾，“分散オブジェクト方式分散ネットワーク監視・障害検出システムの設計”，情報処理学会 DSM 研究報告，99-DSM-16,pp.31-36,1999

[3] 三好優，釜洞健太郎，朴容震，浦野義頼，富永英義，“モバイルエージェントによる大規模・分散型ネットワーク管理法の一提案”，情報処理学会 DSM 研究報告，????????

[4] DANNY B.LANGE, MITSURU OSHIMA, “PROGRAMMING AND DEPLOYING JAVA MOBILE AGENTS WITH AGLETS”, ADDISON-WESLEY, 1998

[5] 小野康一，“移動エージェント Aglets のセキュリティ・モデル”，コンピュータソフトウェア，Vol.17 No.4(2000), pp.2-14, 1999

[6] http://www.oix.u-ryukyu.ac.jp/

[7] http://www.trl.ibm.co.jp/aglets/