ネットワーク情報を収集・加工・提供するシステム NIWH の構成とその試作

内海哲史　川端邦明　Ahmed Ashir　斎藤武夫　Glenn Mansfield 白鳥則郎
東北大学電気通信研究所　/　情報科学研究科

インターネットにおける QoS 制御やネットワーク攻撃の追跡などの高度なネットワーク運用を実現するためには、動的なネットワーク情報を収集することが必要不可欠である。本論文では、ネットワーク上の動的な情報を複数のユーザの要求に従って収集・分析・提供するシステムであるネットワーク情報ウェアハウス（Network Information WareHouse; NIWH）を提案し、その構成について検討する。ここで示す NIWH のモデルは、ユーザからネットワーク情報の収集・分析・提供要求を受ける NIWH マネージャと、NIWH マネージャから収集・分析の指示を受ける NIWH エージェントから成る。また、ネットワーク情報の収集手段としてパケット監視ツール TCPDUMP を用いた NIWH プロトタイプの設計、実装を行う。

Network Information Warehouse : Architecture and Implementation of a Prototype

Satoshi UTSUMI, Kuniaki KAWABATA, Ahmed ASHIR, Saitoh TAKEO ,
Glenn MANSFIELD, Norio SHIRATORI
Research Institute of Electrical Communication /
Graduate School of Information Sciences, Tohoku University

Information about the underlying network is essential for QoS control, intrusion detections and for effective operation of network applications. We have already proposed the basic concept of Network Information Warehouse (NIWH) which collects network information, analyzes them and provides them to the users or applications. NIWH consists of two main modules: a NIWH manager and a NIWH agent. The manager receives request from users, asks the suitable agents to provides them to the users. This paper discusses the design issues of the NIWH manager and the NIWH agents. Our prototype implementation of NIWH considers network information that can be collected by tcpdump tool.

1．はじめに

近年のインターネットの普及とその利用者の増大は著しく、インターネットの重要性は増す一方である。しかしインターネットの現状を省みると、それは必ずしも十分な機能を果たしていない。例えば、あるアプリケーション利用において、その通信がある一定以上のサービス品質を必要とするとき、現在のインターネット環境ではそれを保証することが困難である。またセキュリティの面においては、あるネットワークやホストに対して攻撃が行われたとき、その攻撃を追跡することが困難なため、攻撃者は野放しになっている。

我々は、ユーザやアプリケーションが必要とするネットワークに関する情報（以下、ネットワー

ク情報）を容易に得ることができるならば、これらの問題を解消し、より高度で信頼のあるネットワーク運用ができると考える。ネットワークトポロジーやそれぞれのパスにおける帯域容量、使用帯域量などが分かれば、より効率的にトラフィックを伝送する動的なルーティングや、ネットワーク資源を予約することによるQoS制御に役立つ。さらに、あるネットワークに対して攻撃があったとき、その攻撃の形跡をインターネット上から集めることができれば、その攻撃者を特定することの手助けにもなる。

現在、あるユーザアプリケーションがインターネット上に広く分散するネットワーク情報を必要とするとき、その情報をアプリケーション自身で収集しなければならないが、そのことは効率やセキュリティの面などから現実的でない。

そこで我々は、インターネットを含む、ネットワーク上の情報を収集・分析・管理し、ユーザにその情報を提供するシステムであるネットワーク情報ウェアハウス(NIWH: Network Information WareHouse) を提案している（図1）。

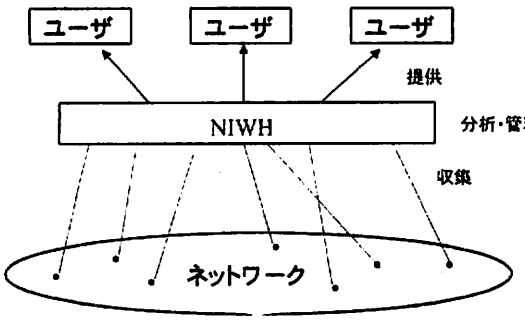

図1 NIWHの提案

本論文では、NIWHの基本的な構成を示し、そのプロトタイプシステムとしてパケット情報を収集するNIWHを設計、実装する。

2．NIWHの構成

2．1 NIWHモデル

NIWHは、ネットワーク情報を収集・分析し、その情報をユーザに提供するシステムである。ネットワークから直接収集するネットワーク情報（一次的ネットワーク情報）として、ネットワークを流れるパケット、SNMPネットワーク管理情報、ネットワークアプリケーションの持つデータなど、様々な情報が想定される。ここではシステムの設計に先立ち、ネットワーク情報やその分析手法に依存しない、システムのモデル化を行う。NIWHの扱うネットワーク情報は幅広く分散するため、その収集や管理などの機能をそれぞれ分散して実現することを考える。図2にNIWHシステムのモデル（NIWHモデル）を示す。

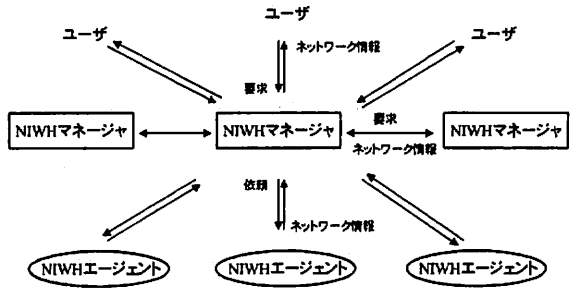

図2 NIWHモデル

NIWHモデルは、その構成要素としてNIWHマネージャ、NIWHエージェントを持つ。ユーザは必要なネットワーク情報について、任意のNIWHマネージャに対して収集・分析・提供の要求を行うことができる。NIWHマネージャは、ユーザからのネットワーク情報収集・分析・提供の要求を受け取り、NIWHエージェントに収集・分析の指示をする。1つのNIWHマネージャは、1つ以上のNIWHエージェントを指示の対象とする。NIWHエージェントは、NIWHマネージャの指示に従って、一次的ネットワーク情報を収集し、その情報を処理する。対象外のNIWHエージェントが収集するネットワーク情報が必要なとき、NIWHマネージャは他のNIWHマネージャに収集・分析・提供の要求をすることによって、必要な情報を得る。このようなモデルに従うことによ

って、NIWH システムは限られた範囲を形成しながら、幅広いネットワーク情報を対象とすることができる。

2．2 NIWH エージェント

NIWH エージェントは、NIWH マネージャの指示に従って動作する。NIWH エージェントの持つ基本的な機能を次に挙げる。

(1) ネットワーク情報収集
(2) ネットワーク情報の一次的分析
(3) ネットワーク情報のマネージャへの受け渡し

(1)について、一般的に一次的ネットワーク情報は広く分散しているので、その収集は多数の NIWH エージェントによって行われる。

(2)について、NIWH エージェントは一次的ネットワーク情報をそのまま NIWH マネージャに受け渡さずに、その情報をある程度分析してから受け渡すことができる必要がある。収集したネットワーク情報のデータ量が大きいとき、NIWH エージェントで分析することによって NIWH マネージャへ受け渡すトラフィック量を押さえることができる。例えば、一次的ネットワーク情報のフィルタリングや、値の時間変化についての解析などを行う。

(3)について、(1)で得た一次的ネットワーク情報や、(2)で得た分析情報をマネージャへ渡す。

2．3 NIWH マネージャ

NIWH マネージャの持つ基本的な機能を次に挙げる。

(1) ユーザまたは他の NIWH マネージャからの要求の処理
(2) NIWH エージェントへの指示
(3) 他の NIWH マネージャへのネットワーク情報収集・分析・提供の要求
(4) ネットワーク情報の二次的分析
(5) ネットワーク情報の管理
(6) ネットワーク情報の提供

(1)ついて、NIWH マネージャは、ユーザまたは他の NIWH マネージャからの要求を解析し、その要求を実現するための準備を行う。

(2)について、ユーザまたは他の NIWH マネージャからの要求を満足するため、NIWHエージェントに一次的ネットワーク情報の収集や一次的分析を指示する。

(3)について、対象の NIWH エージェントが扱うネットワーク情報だけではユーザからの要求を満足できないとき、他の NIWH マネージャにネットワーク情報の収集・分析・提供を要求する。

(4)について、(2)の指示や(3)の要求によって、対象の NIWH エージェントや他の NIWH マネージャから受け取ったネットワーク情報を分析する。例えば、複数の NIWH エージェントが収集・分析したネットワーク情報を利用するような分析は NIWH マネージャが行う必要がある。

(5)について、NIWH エージェントや他の NIWH マネージャから受け取ったネットワーク情報、(4)で分析したネットワーク情報をデータベース等で管理し、提供の要求に備える。

(7) ついて、(5)で管理するネットワーク情報をユーザや他の NIWH マネージャに提供する。

3. NIWH プロトタイプ

3． 1 NIWH プロトタイプの概要

ここで試作する NIWH は、一次的ネットワーク情報として NIWH エージェントを通過するパケットを収集する。収集手段として TCPDUMP というパケット監視ツールを用いる。構成は、2章の NIWH モデルに従う。

この NIWH プロトタイプがユーザに提供可能なネットワーク情報は、NIWH エージェントを備えた各ノードにおける特定のパケットについての(1)トラフィック量、(2)パケット数、(3)パケットヘッダ情報とする。

この NIWH プロトタイプは、NIWH マネージャ間通信機能を削除した NIWH のサブセットである。この NIWH プロトタイプは一つの NIWH

マネージャとその指示の対象となる複数のNIWHエージェントから構成される。

このNIWHプロトタイプの物理的なネットワーク構成は、例えば図3のようになる。図3のネットワーク構成では、1つのNIWHマネージャが3つのNIWHエージェントを指示の対象とする。ルーティング機能を持った、イーサネットを結ぶホストにNIWHエージェントを置いて、そのホストのインタフェースを通過するパケットを収集する。

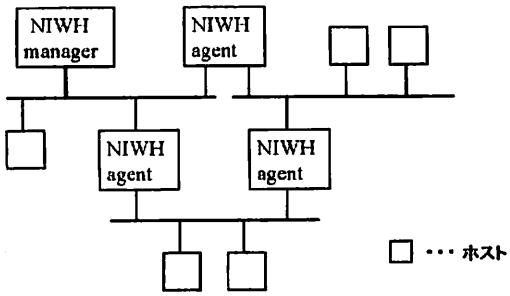

図3 NIWHプロトタイプを用いたネットワーク構成例

このNIWHプロトタイプは、ユーザからのネットワーク情報確保要求に従ってパケット情報を収集・分析し、データベースにその情報を蓄える。ネットワーク情報確保要求は、(1)ネットワーク情報確保場所、(2)ネットワーク情報確保開始時刻、(3)ネットワーク情報確保時間、(4)ネットワーク情報タイプIDからなる。ネットワーク情報確保要求は、例えば

ネットワーク情報確保要求1
ネットワーク情報確保場所・・・エージェントA
ネットワーク情報確保開始時刻
・・・2000/10/1/10:00:00
ネットワーク情報確保時間・・・10秒
ネットワーク情報タイプID
・・・icmp-echo-request_packet

となる。このネットワーク情報確保要求は、エージェントAを10時00分00秒から10時00分10秒まで通るパケットについて、ICMPエコー要求（icmp-echo-request）パケットの数を調べ、その情報を確保することを要求する。NIWHプロトタイプのモジュール構成を図4に示す。

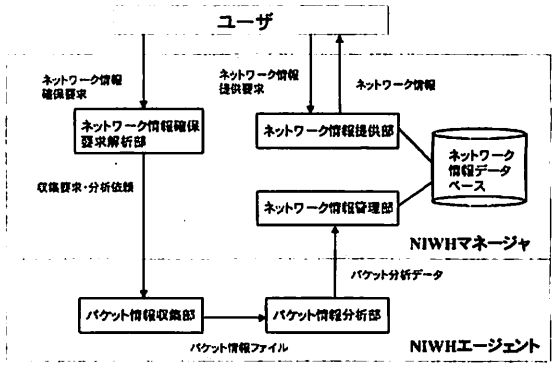

図4 NIWHプロトタイプのモジュール構成

ネットワーク情報収集・分析処理の流れは、以下のようになる。

（1）ネットワーク情報確保要求解析部は、ユーザからのネットワーク情報確保要求を解析する。

（2）パケット情報収集部は、ネットワーク情報確保要求の解析結果に従いパケット情報を収集する。

（3）パケット情報分析部は、ネットワーク情報確保要求の解析結果に従い、収集したパケット情報を分析する。

（4）ネットワーク情報管理部は、データベースに分析したネットワーク情報を格納する。

またネットワーク情報提供処理では、

（5）ネットワーク情報提供部は、ユーザからのネットワーク情報提供要求に従ってユーザにネットワーク情報を提供する。

以下では、特に（1）、（2）、（3）について、すなわちパケット情報収集手順及び分析手順について述べる。

3．2 NIWHマネージャの設計

このNIWHプロトタイプにおけるNIWHマネージャは主な構成要素として、ネットワーク情報確保要求解析部、ネットワーク情報管理部、ネットワーク情報提供部を持つ。このNIWHプロトタ

イプは、ネットワーク情報の二次的分析を必要としない（すなわち、すべての分析はNIWHエージェントで行われる）。ここでは、パケット情報収集及び分析に関わるネットワーク情報確保要求解析部について詳しく述べる。

- ネットワーク情報確保要求解析部

ここではユーザからのネットワーク情報確保要求を解析して、NIWHエージェントに対するパケット情報収集指示とパケット情報分析指示を生成する。

パケット情報収集処理のために必要な情報は、パケット収集場所、パケット収集開始時刻及び、パケット収集時間である。またパケット情報分析処理のために必要な情報は、分析対象のパケットの収集場所（パケット分析場所）、分析対象のパケットが収集された時間帯（パケット分析開始時刻からパケット分析時間）及び対象のパケットの分析方法である。ユーザから与えられた複数のネットワーク情報確保要求から、これらの情報を整理しそれぞれパケット情報収集支持、パケット情報分析指示を生成する。なお、パケットの分析方法はネットワーク情報確保要求の要素であるネットワーク情報タイプIDによって決定される。

例えば、3．1節のネットワーク情報確保要求1及び次のネットワーク情報確保要求2がユーザからNIWHマネージャに与えられるとする。

ネットワーク情報確保要求2
ネットワーク情報確保場所・・・エージェントA
ネットワーク情報確保開始時刻
・・・2000/ 10/ 01/ 10:00:05
ネットワーク情報確保時間・・・10秒
ネットワーク情報タイプID・・・all_traffic

これらのネットワーク情報確保要求から生成される、NIWHエージェントに対するパケット情報の収集指示及びパケット情報分析指示は次のようになる。

パケット情報収集指示1
パケット情報収集場所・・・エージェントA
パケット情報収集開始時刻
・・・2000/ 10/ 1/ 10:00:00
パケット情報収集時間・・・10秒

パケット情報分析指示1
パケット情報分析場所・・・エージェントA
パケット情報分析開始時刻
・・・2000/ 10/ 01/ 10:00:00
パケット情報分析時間・・・10秒
ネットワーク情報タイプID
・・・icmp-echo-request_packet

パケット情報分析指示2
パケット情報分析場所・・・エージェントA
パケット情報分析開始時刻
・・・2000/ 10/ 01/ 10:00:05
パケット情報分析時間・・・10秒
ネットワーク情報タイプID・・・all_traffic

ネットワーク情報確保要求1とネットワーク情報確保要求2の確保場所が同一（エージェントA）のため、パケット情報収集指示の収集時間帯は、それぞれの確保時間帯の和集合となっている。NIWHマネージャはそれぞれの指示を、それぞれ対象の場所にあるNIWHエージェントに対して与える。

3．3 NIWHエージェントの設計

ここではインタフェースに流れ込むパケットの情報を収集するNIWHエージェントの設計について述べる。このNIWHエージェントは主な構成要素として、パケット情報収集部とパケット情報分析部から成る。ネットワーク情報収集部では、パケット監視ツールであるTCPDUMPを用いる。

- パケット情報収集部

パケット情報収集部では、NIWH マネージャから与えられたパケット情報収集指示に従って、パケット情報を収集する。すなわち、パケット情報収集開始時刻からパケット情報収集時間、パケット情報を収集する。

パケットの収集手段として、TCPDUMP を用いる。TCPDUMP は、そのインタフェースに流れ込むパケットのパケット生データを出力する。パケット情報収集部は、TCPDUMP から得られるパケット生データをストリームに出力する。そして、このパケット生データのストリームをパケット情報分析部に渡す。

- パケット情報分析部

パケット情報分析部では、NIWH マネージャが生成したパケット情報分析指示に従ってパケット生データを分析する。すなわち、パケット情報分析開始時刻からパケット情報分析時間の間に収集したパケットに対して、ネットワーク情報タイプ ID によって決定される分析を施す。3．2節のパケット情報分析要求に現れるネットワーク情報タイプ ID、icmp-echo-request_packet 及び all_traffic はそれぞれ、ICMP エコー要求のパケット数及び全トラフィック量（オクテット）を意味する。それぞれのパケット情報分析の結果は図5のようになる。

icmp-echo-request_packet
エージェントA

10:00:00	1
10:00:01	1
10:00:02	0
10:00:03	1
10:00:04	2
10:00:05	2
10:00:06	0
10:00:07	0
10:00:08	1
10:00:09	2

all_traffic
エージェントA

10:00:05	8232
10:00:06	7221
10:00:07	2113
10:00:08	8771
10:00:09	8922
10:00:10	3091
10:00:11	1232
10:00:12	1211
10:00:13	6712
10:00:14	2311

図5 NIWHプロトタイプによるパケット情報分析結果

4．まとめ

本論文では、高度なネットワーク運用に必要なネットワークに関する情報を収集・分析・提供するシステム NIWH を提案し、その構成を示した。また、TCPDUMP を用いたパケット情報を収集するプロトタイプシステムの設計、実装を行った。このプロトタイプシステムは、限られた範囲（NIWH マネージャが管理する範囲）における分散するネットワーク情報を提供する。

5．現在の状況

NIWH の目的は、幅広く分散するネットワーク情報を必要とするユーザやアプリケーションに対して、その情報を提供することである。現段階で想定している、NIWH が情報を提供するアプリケーションは、インターネットにおける QoS を制御するシステム、帯域容量と使用帯域から最適な経路を得るルーティングシステム、ネットワークやホストに対する攻撃の発信元を追跡するシステムなどである。これらのシステムが必要とするネットワーク情報を洗い出し、それらのネットワーク情報を得る方法を検討している。

参考文献

[1] J. E. van der Merwe et al.," Measurement and Analysis of IP Network Usage and Behavior," IEEE Communications Magazine, May. 2000

[2] Ahmed Ashir, Glenn Mansfield, Takeo Saitoh, Masakazu Kaneko, Norio Shiratori, "An Open and Configurable Network Information Warehouse Service," Passive and Active Measurements - PAM-2000 New Zealand April 2000