第XVI部

ネットワーク管理とセキュリティ

第16部
ネットワーク管理とセキュリティ

第1章 はじめに

1.1 IPv6 とネットワーク管理

IPv6 ネットワークでは、飛躍的に広がるアドレス空間を利用して、家電や自動車等これまでにない多様で大量の機器が接続されるとともに、セキュリティ、QoS 機能の追加等で、管理の必要な対象が大幅に増加する。しかし、IPv6 によるネットワーキング技術およびアプリケーションの整備状況に対して、その管理技術については大幅に立ち遅れており、早急な整備が必要になっている。さらに IPv4/IPv6 の両プロトコルの併用が予想されることから、マルチプロトコル環境での管理技術が重要である。そこで本年度は、(1) インターネット標準管理プロトコルである SNMP (Simple Network Management Protocol) の IPv4/IPv6 両対応のための設計と実装、(2)IPv4/IPv6 の両ネットワークをシームレスに管理できる標準管理技術（API および管理オブジェクト MIB のマルチプロトコル対応）の確立、(3) 新しいネットワーク機器およびサービスを効率的かつ安全に管理する技術（セキュリティ機能 SNMP v1/v2/v3 プロトコルの相互運用）の確立、の 3 点の研究開発を行った。

1.2 技術課題

IP のマルチプロトコル化、SNMP のマルチプロトコル化に対応し、シームレスでセキュアなよく管理されたネットワーク環境を構築する技術を研究開発する。技術課題は以下のとおり。

(1) IPv6 ネットワーク用インターネット標準プロトコルの研究と実装
現在のインターネット標準管理プロトコルを IPv6 ネットワークに適応するための管理プロトコルの研究と実装を行う。

(2) マルチプロトコルネットワークの管理技術の研究開発
研究開発された IPv6 ネットワーク管理プロトコルを用い、IPv6/IPv4 混在ネットワーク環境において、シームレスな管理を実現する技術の研究開発を行う。また、SNMPv1/v2/v3 のシームレスな利用環境を整備し、セキュアなネットワーク管理のための基盤技術とする。

(3) 大規模広域 IPv6 ネットワークにおける情報収集および制御技術の研究
飛躍的に増大する管理対象と管理項目を効率的に管理するための情報収集技術、および制御技術を研究開発する。

(4) ネットワーク管理におけるセキュリティ技術の研究開発
暗号通信等のセキュリティ技術に対するネットワーク管理技術の積極的な活用技術を研究開発する。

(5) 新しいネットワーク管理アプリケーションへの適応研究
新しいネットワーク管理アプリケーションからの管理情報および管理プロトコルを積極的に活用する技術を研究開発する。

1.3 実施内容

本研究における各プロトタイプ実装および運用実験は、インターネット上で広く普及している IPv4 対応 SNMP エージェントソフトウェアである net-snmp (http://www.netsnmp.org/) をベースに行った。

(1) SNMP over IPv6 プロトコルの仕様策定
インターネット標準管理プロトコルである SNMP を IPv6 ネットワーク上で実現するために、まず、(a) 変更が必要な既存 MIB の調査と IPv6 対応 MIB モデルの策定を行い、その検証のために (b)IPv6 対応のプロトタイプ実装を行った。さらに、その成果をもとに (c)SNMP over IPv6 プロトコル仕様の策定を行った。

(2) IPv4/IPv6 および SNMPv1/v2/v3 プロトコルの相互変換技術
(1) で研究開発を行った IPv6 ネットワーク管理プロトコルを、既存の IPv4 ネットワークとの共存環境において、シームレスに運用するためのプロトコル変換技術の研究開発を行った。まず、

IPv4/IPv6 マルチプロトコル対応 SNMP エージェント実現のために (a) 構造と API の検討を行い、その検証のために (b) プロトタイプ実装を行った。さらに (c) 既存プロトコル変換技術のマルチプロトコル化の検討を行い、(d)IPv4 ネットワークにおける SNMPv1/v2/v3 プロトコルを考慮した、IPv4/IPv6 マルチプロトコル相互変換エージェントの評価を行った。

(3) 情報収集の効率化および IPv6 管理技術

IPv6 ネットワークにおいて飛躍的に増大する管理対象と管理項目を効率的に管理するための情報収集技術、および制御技術の研究を行った。まず、(a) 既存管理手法の調査を行い、(b)IPv6 ネットワークへの対応の検討を行った。さらに、(b) で検討した手法の (c) 運用実験と評価を行った。

(4) セキュリティ管理技術

暗号通信等のセキュリティ技術に対する、ネットワーク管理技術の積極的な活用を行うための研究開発を行った。まず、(a)IPv6 に対応した安全な管理情報交換技術の検討を行い、(a) の技術を適応した (b) エージェントの開発を行った。次にこのエージェントを用いて (c) 運用実験と評価を行った。

(5) IPv6 を活用した管理技術

(4) までの成果をもとに、ネットワーク管理アプリケーションから IPv6 ネットワークの管理情報および管理プロトコルを積極的に活用するための技術の研究開発を行った。まず、(a) 現状の IPv6 ネットワークにおける管理情報収集技術の調査を行い、(b) 管理情報収集エージェントのマルチプロトコル化に関する検討を行った。そして、マルチプロトコル対応管理情報収集アプリケーションとして、マルチプロトコルトラフィック情報収集エージェントのための (c) プロトタイプ MIB の開発および IPv6 対応侵入検知エージェントのための (d)IPv6 SNMP メッセージ通知プロトタイプエージェントの開発を行い、(e) 運用実験と評価を行った。

1.4 開発ソフトウェアリスト

以下に、実装を行ったソフトウェアのリストを挙げる。

(1) net-snmp4.2.1 に対する IPv6 プロトコルスタックモジュール

(2) net-snmp5.0pre1 に対する IPv6 プロトコルスタックモジュール

(3) net-snmp5.0pre1 に対する IPv6 対応アクセスコントロールモジュール

(4) マルチプロトコル対応トラフィック情報収集エージェント向けプロトタイプ MIB 定義ファイルとプロトタイプ MIB エージェントモジュール

(5) IPv6 対応 IDS snort-1.6.3 に対する IPv6 SNMP 対応侵入情報通知プロトタイプエージェントモジュール

第 2 章　SNMP over IPv6 プロトコルの仕様策定

2.1 IPv6 対応 MIB モデルの検討

SNMP は標準管理情報ベース（Management Information Base、以後 MIB と表記する）で定義されている管理オブジェクトを用いてネットワーク管理情報のやりとりを行う。MIB で定義されているデータ型の中には IPv4 アドレスを表す “IpAddress” があり、これを採用している MIB は、現在標準化および提案中のものだけでも多数存在する。そこで本節ではデータ型 “IpAddress” を手がかりにし、現在 RFC で提案および標準化がなされた MIB 中で IPv4 アドレスの使用を前提としている管理オブジェクトを調査する。また IPv6 アドレスを表すデータ型 “Ipv6Address” を使用している管理オブジェクトを調査し、IPv4 ネットワーク管理から IPv6 ネットワーク管理への移行状況を調査する。

表 2.2 から、IP–MIB、TCP–MIB、UDP–MIB に代表されるノードに関する統計情報を扱う MIB に対しては IPv6 対応がなされていると推定できる。一方、BGP4–MIB や OSPF–MIB に代表されるルーティング情報を扱う MIB は IPv6 対応が進んでいない。

2.2 IPv6 対応 SNMP エージェントの開発と評価

前節ではネットワーク管理情報を扱うためのフレームワーク MIB の IPv6 対応について調査したが、IPv6 ネットワーク上で動作する SNMP 対応アプリケーションが存在しなかった。つまり、IPv6 ネットワーク情報をやりとりするためには IPv4 ネットワーク

表 2.1. “IpAddress” を利用している MIB

MIB 名	オブジェクト数
MIB–II[99]	8
AppleTalk MIB[143]	2
BGPv3 MIB[153]	8
SNA APPN MIB[100]	2
DNS Server MIB[8]	3
DNS Resolver MIB[7]	4
BGP4–MIB[152]	11
SMDS–if MIB[23]	1
RIPv2–MIB[93]	4
OSPF–MIB[14]	13
MIP–MIB[30]	18
IP–MIB[96]	3
TCP–MIB[97]	2
UDP–MIB[98]	1
RMON2–MIB[144]	5
IP–FORWARD–MIB[13]	6
IOPA–MIB[54]	3
IPATM–IPMC–MIB[29]	10
ATM–MIB[133]	1
TN3270E–MIB[148]	1
RADIUS–AUTH–CLIENT–MIB[3]	1
RADIUS–AUTH–SERVER–MIB[159]	1
RADIUS–ACC–CLIENT–MIB[2]	1
RADIUS–ACC–SERVER–MIB[158]	1
IP Tunnel MIB[134]	4
DOCS–CABLE–DEVICE–MIB[78]	12
DOCS–IF–MIB[79]	1
VRRP–MIB[75]	4
DISMAN–EXPRESSION–MIB[80]	1
NOTIFICATION–LOG–MIB[81]	1
DOCS–BPI–MIB[155]	1

表 2.2. “Ipv6Address” を利用している MIB

MIB 名	管理オブジェクト
IPV6–TCP–MIB[37]	ipv6TcpConnLocalAddress
	ipv6TcpConnRemAddress
IPV6–UDP–MIB[38]	ipv6UdpLocalAddress
IPV6–MIB[62]	ipv6AddrAddress
	ipv6RouteDest
	ipv6RouteNextHop
	ipv6NetToMediaNetAddress

表 2.3.　SNMP over IPv6 パケットの送受信の評価

	IPv6 パケット送信	IPv6 パケット受信
マネージャ	○	○
エージェント	○	○

が必要であった。IPv6 ネットワーク管理を IPv4 から独立させるためにも IPv6 対応 SNMP アプリケーションの開発が必須である。本節では [163]、[161]、[52] を参考に、ucd–snmp–4.2.1 を IPv6 に対応させ、評価を行った。表 2.3 に評価の結果を示す。

2.3 SNMP over IPv6 プロトコル仕様の策定

RFC1906 において SNMPv2 プロトコルの UDP へのマッピングが定義されている。そこでの定義は以下の通りである。

```
-- SNMPv2 over UDP over IPv4
snmpUDPDomain OBJECT-IDENTITY
        STATUS  current
        DESCRIPTION
                "The SNMPv2 over UDP transport domain. The corresponding
                 transport address is of the type SNMPUDPAddress."
        ::= { snmpDomains 1}

SnmpUDPAddress ::= TEXTUAL-CONVENTION
        DISPLAY-HINT "1d.1d.1d.1d/2d"
        STATUS  current
        DESCRIPTION
                "Represents a UDP address:
                    octets  contents              encoding
                      1-4    IP-address      network-byte order
                      5-6    UDP-port        network-byte order
                "
        SYNTAX  OCTET STRING (SIZE(6))
```

SnmpUDPAddress の定義から UDP over IPv4 へのマッピングを想定している。UDP over IPv6 へのマッピングのために現在 Internet-drafts、“Textual Conventions for Transport Address”[39] が提案され、標準化へのプロセスが進められている。我々は、本研究の成果から、管理アプリケーションから見た場合に IP 層非依存な Transport Domain が必要であるとの立場から、その提案を反映させるために、現在 IETF のメーリングリスト等で積極的に議論を進めている。

第 3 章　IPv4/IPv6 および SNMPv1/v2/v3 プロトコルの相互変換技術

3.1 マルチプロトコル対応 SNMP エージェントの検討

IPv4 ネットワークから IPv6 ネットワークへの移行過渡期では、運用ネットワークの機器の中には SNMP/IPv4 のみ対応する機器が存在する可能性がある。また、SNMP は version1 対応のアプリケーションが広く普及しているが、version1 が抱えるセキュリティ的問題点から SNMPv3 対応が急がれている。しかし、現状では SNMPv3 対応のアプリケーションは数多くない。故に、SNMP プロトコルの IPv4/IPv6 変換また SNMP のバージョンの相互変換が必要である。

本研究開発では、NET-SNMP Project[118] が開発している net-snmp-5.0.pre1 を用いた。この SNMP アプリケーションはオープンなコミュニティで開発が続けられ、安定度が高いため、本研究開発の実験に使用しても支障がないと判断した。また執筆者からも逆に NET-SNMP Project に対する貢献を積極的に行っている。

3.2 マルチプロトコル対応 SNMP エージェントの開発

net-snmp-5.0.pre1 を元に、本研究開発では以下の機能を追加実装した。

- IPv4/IPv6 シームレス snmpAPI

この追加実装は FreeBSD 4.4-Release 上で行った。この追加実装と NET-SNMP Project が開発したプロキシモジュールを用いることにより IPv4/IPv6 および SNMPv1/v2/v3 マルチプロトコル対応 SNMP エージェントを実現することができた。

ここでは、net-snmp-5.0.pre1 を元にしたマルチプロトコル対応 SNMP エージェントの利用法について述べる。基本的には通常の使い方と同様である。ただし、IPv6 アドレスでエージェント等を指定する場合は “[ ]” で囲まなければいけない。エージェントの使い方も通常の使い方と同様である。snmpd.conf には IPv6 アドレスも記入することができる。図 3.1 の例は prefix-length が 64、prefix-address が 3ffe:200:1a0:ff00::からなるアドレスからアクセスする際のコミュニティ名を COMMUNITY に設定している。

```
#       sec.name  source          community
com2sec mynetwork 3ffe:200::/64 COMMUNITY
```

図 3.1.　snmpd.conf の設定例

```
# proxy to SNMP over IPv4 agent
proxy -v1 -c COMMUNITY 192.168.0.254 .enterprise.73.14.1 .1
proxy -v2c -c COMMUNITY 192.168.0.254 .enterprise.73.14.2 .1
proxy -v3 -u user -l authNoPriv -a MD5 -A AUTHPASS \   （実際は 1 行）
192.168.0.254 .enterprise.73.14.3 .1
proxy -v3 -u user -l authPriv -a MD5 -A AUTHPASS -x DES -X PRIVPASS \  （実際は 1 行）
192.168.0.254 .enterprise.73.14.4 .1

# proxy to SNMP over IPv6 agent
proxy -v1 -c COMMUNITY 2001:200:1a0:ff00::ffff .enterprise.73.15.1 .1
proxy -v2c -c COMMUNITY 2001:200:1a0:ff00::ffff .enterprise.73.15.2 .1
proxy -v3 -u user -l authNoPriv -a MD5 -A AUTHPASS \  （実際は 1 行）
2001:200:1a0:ff00::ffff .enterprise.73.15.3 .1
proxy -v3 -u user -l authPriv -a MD5 -A AUTHPASS -x DES -X PRIVPASS \  （実際は 1 行）
2001:200:1a0:ff00::ffff .enterprise.73.15.4 .1
```

図 3.2.　プロキシモジュールの設定

表 3.1.　GET-Request に対するプロトコル変換技術評価

			プロキシ先							
プロキシ元			IPv4				IPv6			
			v1	v2c	authNoPriv	authPriv	v1	v2c	authNoPriv	authPriv
	IPv4	v1	○	○	○	○	○	○	○	○
		v2c	○	○	○	○	○	○	○	○
		authNoPriv	○	○	○	○	○	○	○	○
		authPriv	○	○	○	○	○	○	○	○
	IPv6	v1	○	○	○	○	○	○	○	○
		v2c	○	○	○	○	○	○	○	○
		authNoPriv	○	○	○	○	○	○	○	○
		authPriv	○	○	○	○	○	○	○	○

3.3 プロトコル変換技術の検討とマルチプロトコル対応 SNMP エージェントの評価

前節で用いたマルチプロトコル対応評価には net-snmp-5.0.pre1 のプロキシエージェントと本研究開発で開発したそれに対する IPv6 プロトコルスタックモジュールを用いた。以下にプロキシモジュールの設定を図 3.2 に挙げる。

実験環境を図 3.3 に示す。

評価対象は、SNMP を SNMPv1、SNMPv2c、SNMPv3 (securitylevel authNoPriv)、SNMPv3 (securitylevel authPriv) の 4 つ、IP のバージョンは v4、v6 の 2 つとした。SNMPv3 を試す際に用いた認証アルゴリズムは HMAC-MD5-96、暗号化アルゴリズムは CBC-DES を用いた。表 3.1 に GET-Request に対する結果を示す。

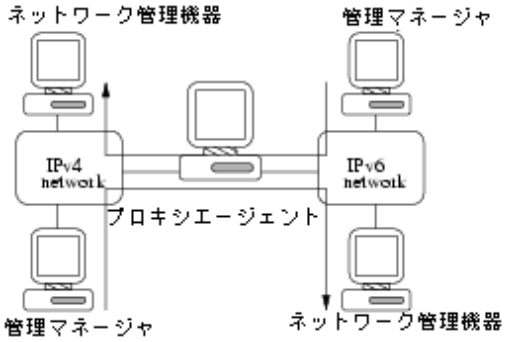

図 3.3.　プロトコル変換技術評価環境

以上により、IPv4/IPv6 および SNMPv1/v2/v3 プロトコルの相互変換技術は可能であることを示した。

第 4 章　情報収集の効率化および IPv6 管理技術

4.1 情報収集効率化のためのアーキテクチャ

近年、ネットワークシステムの規模がますます増大するにつれ、単一の管理ステーション方式、すなわち集中的な管理手法が現実的でない状況が出現してきている。発生する問題を具体的に挙げると、(1) 管理ステーションの負荷の増大、(2) 複数の管理ステーションからの情報収集によるネットワーク負荷

の増大、さらに、管理対象ネットワーク機器の一元管理が不可欠なため、(3) ネットワーク管理者の作業量が増大する。また、(4) 耐障害性にも劣り、たとえば管理ステーションに障害が発生すると、管理自体が不可能になり、普及までの間、全ての管理情報の利用が不可能になる。

これらの問題を解決するために、我々は、分散・自律型マネジャにより構成されるネットワーク管理情報収集システムの研究を行っている 。このシステムでは、従来 1 箇所のみで行われていた管理情報の収集と蓄積の機能を複数箇所に分散させて配置するアーキテクチャを持つ。これらの機能は自律的に動作し、ネットワーク管理アプリケーションが動作する管理ステーションを “シニアレベルマネジャ” と呼ぶのに対して、“ミドルレベルマネジャ” という名称を持つ（図 4.1）。

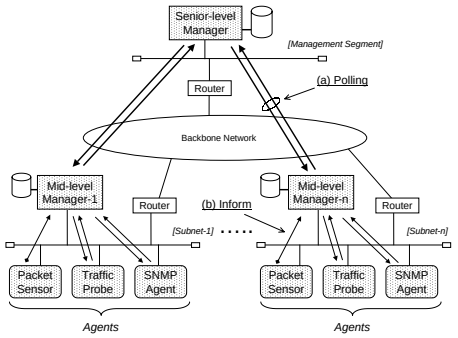

図 4.1.　分散情報収集システムのアーキテクチャ

このアーキテクチャにより、情報収集を分担して行うことによるスケーラビリティの確保と管理者の負担の分散が図れる。さらに、情報の取捨選択や集約化による管理トラフィックの低減や、シニアレベルマネジャと各ミドルレベルマネジャが独立して自律的に作動することにより、システム全体としての耐障害性の向上も実現することができる。

4.2 分散情報収集システムを構成する技術要素

集中管理方式では、管理対象ネットワークは全て管理者が把握しており、情報収集の設定も管理者自身が直接行うため、収集される情報の属性が不明確となることはない。しかし、分散型管理システムの場合は、各ミドルレベルマネジャは自律的に管理情報収集対象の設定と情報収集を行い、さらに収集された情報に対してある程度の処理も行うことも想定される。したがって、シニアレベルマネジャから見て、ミドルレベルマネジャが収集蓄積する情報を、一意に把握することを可能にしなければならない。シニアレベルマネジャから見た収集対象情報の一意性を確保するためには、(1) 共通の管理情報対象名と属性、および (2) 収集対象情を報蓄するミドルレベルマネジャの位置情報の管理が必要となる。我々は、これらを解決するためのメカニズムとして、情報項目テーブルの定義と、それを管理するインデックスサーバシステムの構築を行っている 。

情報項目テーブルは、ミドルレベルマネジャが収集する管理対象情報の属性一覧であり、属性一覧と対の形で、収集蓄積された情報へのアクセス手段情報も格納される。ミドルレベルマネジャはこのテーブルを保守し、インデックスサーバに登録を行う（図 4.2）。

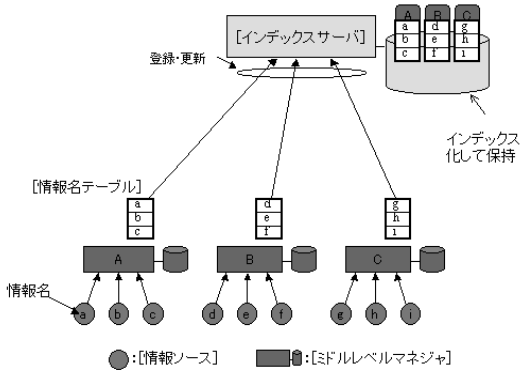

図 4.2.　インデックスサーバ

インデックスサーバは、全ての中間マネジャの情報項目テーブルを、中間マネジャへのポインタとあわせて保持している。シニアレベルマネジャは、管理対象名をキーとしてインデックスサーバに問い合わせ行い、必要な管理情報を入手するための情報を取得する（図 4.3）。

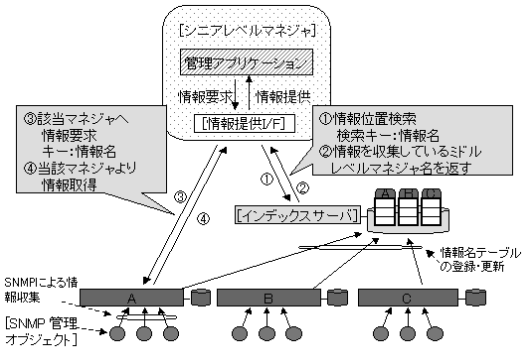

図 4.3.　インデックスサーバを利用した管理情報へのアクセス手順

```
CbOpt.pl 192.168.0.10 JGNv6 public 60
                IF:v1:P161 Version = 2
cpmStatsV4IpDgrams 4
cpmStatsV4IpOctets 4
cpmStatsV4UdpDgrams 4
cpmStatsV4UdpOctets 4
cpmStatsV4TcpSegs 4
cpmStatsV4TcpOctets 4
cpmStatsV4IcmpMsgs 4
cpmStatsV4IcmpOctets 4
```

図 4.4. NetPoller 設定ファイルの例

ミドルレベルマネジャは、管理対象ネットワーク上の複数の機器から、設定された複数の管理情報を、SNMP プロトコルを用いて自律的に収集と蓄積を行う。この管理情報の収集と蓄積機能を実現するために、“NetPoller” という情報収集エンジンを利用している。NetPoller は、大量の管理情報の長期間におけるアーカイブを想定し、正確な時間間隔で管理情報の収集と時刻情報を付加した蓄積を行う。以下に、管理情報収集のための設定例を示す。この例では、192.168.0.10 のホストから、60 秒毎に、2 行目以降に記述された MIB オブジェクト情報を収集蓄積することとなる。

4.3 分散情報収集システムの動作

前節で述べた分散情報収集システムを用いた運用評価とデモンストレーションを、CEATEC JAPAN 2001 において行った。分散情報収集システムは、JGN トラフィック情報収集提供システム JaNI のサブシステムの 1 つであるリアルタイム情報収集蓄積機能を実現するために利用されている。情報収集の対象としたものは、同会場で併設にデモンストレーションが行われた “デジタルシネマ転送制御実験” により JGN 上を流れる ATM トラフィックである。デジタルシネマ転送実験は、IP トラフィックエンジニアリング技術を用い、動的にトラフィック転送経路が変更されるもので、その様子をリアルタイムにモニタリングするために JaNI システムが用いられた。

図 4.5 に、監視対象トラフィックの経路パスと、実際にトラフィック情報を収集する位置を示す。この図において、東大（東京都）に設置されている ATM スイッチと幕張 RC（千葉県幕張市）に設置されている ATM スイッチは、相互接続性のない、まったく異なった運用ポリシーをもつ管理ネットワークに

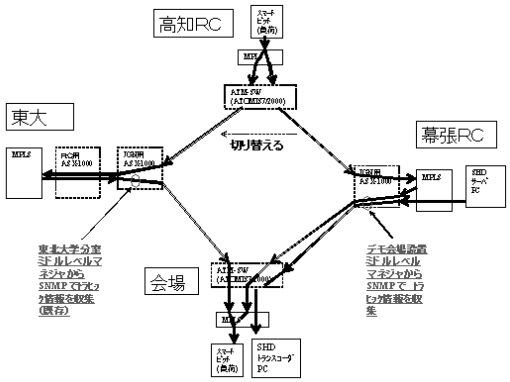

図 4.5. デジタルシネマ転送実験におけるトラフィック情報収集位置

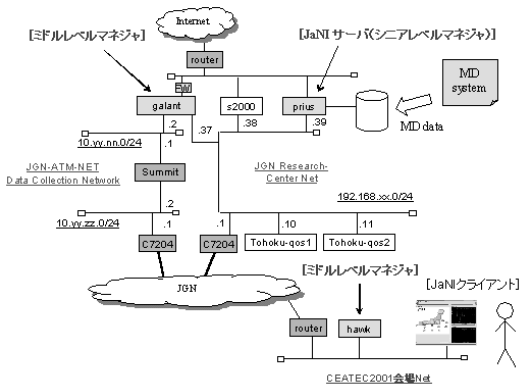

図 4.6. 分散情報収集システムの配置

接続されている。そのため、それぞれのスイッチまで接続性があるネットワークセグメントに複数のミドルレベルマネジャを配置することにより、情報収集の実現とシニアレベルマネジャへの情報提供を実現した。

図 4.6 に、このときの分散情報収集システムの配置構成を示す。東大および幕張 RC の ATM スイッチのトラフィック情報は、それぞれ東北大学（宮城県仙台市）およびデモ会場（幕張メッセ）に設置されたシニアレベルマネジャにより収集蓄積され、東北大学に設置された JaNI システム（シニアレベルマネジャ）へ情報提供が行われた。

デモ会場に設置された JaNI クライアントは、東北大学に設置された JaNI サーバから情報を得ることにより、IP エンジニアリングによる遠隔地のにおけるトラフィックの変化の様子を、リアルタイムかつ統合された形でユーザに提供することが可能となった。図 4.7 に、統合されたトラフィック情報提供の画面を示す。

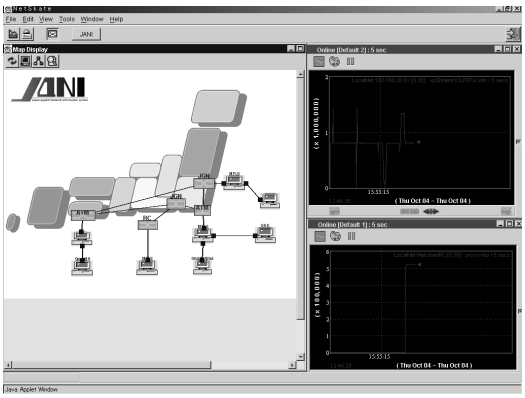

図 4.7.　観測されたトラフィック情報

```
CbOpt.pl 192.168.0.10 JGNv6 public 60
                IF:v1:P161 Version = 2
cpmStatsV6IpDgrams 3
cpmStatsV6IpOctets 3
cpmStatsV6UdpDgrams 3
cpmStatsV6UdpOctets 3
cpmStatsV6TcpSegs 3
cpmStatsV6TcpOctets 3
cpmStatsV6IcmpMsgs 3
cpmStatsV6IcmpOctets 3
```

図 4.8.　IPv4 プロトコルによる管理情報収集設定例

```
CbOpt.pl 3ffe:516:3005::10 JGNv6 public 60
                    IF:v1:P161 Version = 2
cpmStatsV6IpDgrams 3
cpmStatsV6IpOctets 3
cpmStatsV6UdpDgrams 3
cpmStatsV6UdpOctets 3
cpmStatsV6TcpSegs 3
cpmStatsV6TcpOctets 3
cpmStatsV6IcmpMsgs 3
cpmStatsV6IcmpOctets 3
```

図 4.9.　IPv6 プロトコルによる管理情報収集設定例

4.4 IPv6 ネットワークへの対応技術の検討

前節までに述べた、分散情報収集システムは IPv4 ネットワークを対象に研究開発され、実験システムの構築と運用も IPv4 ネットワーク上で行われている。これらの技術を IPv6 ネットワークに適応するためには、以下の要素技術のそれぞれについての検討が必要となる。

(1) インデックスサーバの IPv6 対応技術

(2) ミドルレベルマネジャにおける自立的情報収集蓄積機能の IPv6 対応技術

(1) については、(a) インデックスサーバに格納される情報項目テーブルにおいて、情報ソースおよび情報蓄積サーバを示す IPv4 アドレス格納部を、それぞれ IPv4/IPv6 両アドレスを格納可能なデータ構造とすること、および、(b) 検索のキーである情報名の情報ソース部に IPv6 アドレスを指定可能にすること、さらに (c) 検索通信プロトコルの IPv6 対応化により可能となる。本研究は、ネットワーク管理における基盤技術の研究開発に焦点を絞るため、シニアレベルマネジャ関連にあたる本技術の実装と評価は行っていない。

(2) については、以下に挙げる複数の対応方法がある。

(i) IPv4/IPv6 プロトコル変換技術の利用
IPv6 ネットワーク上に存在する収集対象管理情報の属性（管理情報の位置および属性情報）を、前章において研究開発を行った IPv4/IPv6 プロトコル変換エージェントに登録し、IPv4 ネットワーク上のミドルレベルマネジャが、このエージェントに対して SNMP アクセスを行うことで、IPv6 ネットワーク上の情報収集を行う。

(ii) ミドルレベルマネジャの IPv4/IPv6 マルチプロトコル対応化
ミドルレベルマネジャの、自立的情報収集機能部に、IPv6 に対応した SNMP 情報収集機能を実装する。

(i) の方法は、(ii) の実装を行ったミドルレベルマネジャを用いる場合でも、運用上 (ii) のマネジャから到達できないネットワークの管理情報を収集する場合にも利用でき、たとえば、プロトコルやポリシーが異なる複数のネットワークからなる環境などで、とても有用な技術となる。

4.5 IPv6 対応情報収集エージェントの評価

我々は、前節で述べた (i) の技術について、前章までにその実装と評価を終えている。そこで、以下では (ii) の技術のプロトタイプ実装について評価を行う。このプロトタイプ実装は、既に述べている IPv4 対応の “NetPoller” のソースコードをベースとしており、前章で開発を行った IPv4/IPv6 マルチプロトコル対応 SNMP エージェントの SNMP ライブラリを

```
manager% pwd
/mnt0/local/NetPoller/data/2002/4/12/
                    JGNv6/192.168.0.10
manager%  more cpmStatsV6IpOctets.3
1018537211 35521390
1018537265 35524336
1018537324 35527450
1018537386 35530560
1018537445 35533618
1018537506 35537984
1018537565 35541042
1018537626 35544080
        :
```

図 4.10. SNMP over IPv4 プロトコルにより収集された情報

```
manager% pwd
/mnt0/local/NetPoller/data/2002/4/12/
                JGNv6/3ffe:516:3005::10
manager% more cpmStatsV6IpOctets.3
1018537212 35521390
1018537266 35524336
1018537325 35527450
1018537386 35530560
1018537445 35533618
1018537506 35537984
1018537565 35541042
1018537627 35544080
        :
```

図 4.11. SNMP over IPv6 プロトコルにより収集された情報

利用している。このプロトタイプ実装による、IPv4 および IPv6 プロトコルを用いた SNMP 情報収集設定例を、それぞれ図 4.8、図 4.9 に示す。

動作の検証のために、情報収集対象エージェントとして、前章で実装を行った IPv4/IPv6 マルチプロトコル対応 SNMP エージェントを用いた。エージェントが動作する 1 つのホストマシンに、IPv4 アドレス（192.168.0.30）と IPv6 アドレス（3ffe:516:3005::30）の両方を設定し、同じ MIB オブジェクト情報を同時に収集し、その同一性の確認を行った。図 4.10 に IPv4 プロトコルにより収集蓄積された情報を、図 4.11 に IPv6 プロトコルにより収集蓄積された情報を示す。

以上の結果より、IPv4/IPv6 マルチプロトコル対応のミドルレベルマネジャが正常に動作していることがわかった。

第 5 章　ネットワーク管理におけるセキュリティ技術

5.1 IPv6 に対応した安全な情報交換技術の検討

SNMP を用いたネットワーク管理におけるセキュリティを考える上で以下に挙げた事項は検討すべき問題点である。

- エージェント、マネージャの認証
- 通信データの完全性
- 通信データの秘匿性
- 通信データストリームの第 3 者による変更 (リプレイ攻撃など)
- エージェントの特定管理オブジェクトへのアクセス権利

SNMP はネットワーク管理情報を扱うプロトコルの標準として広く認知されているが、現在最も普及している SNMP version 1 はセキュリティに対する配慮が充分ではなく、認証が弱く、情報の暗号化にも対応していない。また管理オブジェクト毎に対するアクセスコントロール機能が備わっていなかった。その問題点を踏まえて SNMP version2/3 では、上記のセキュリティの問題に対して考察を行い、その結果 User-based Security Model[20]、View-based Access Control Model[150] が提唱された。また、一部の SNMP アプリケーションでは、SNMP アーキテクチャで定義されていないが IP アドレスによるアクセスコントロール機能を実装しているものがある。

本章では、NET-SNMP Project[118] が開発している net-snmp-5.0.pre1 を元にして、以下のネットワーク管理におけるセキュリティ技術を IPv6 に対応させるために必要な技術の考察、開発および評価を行う。

- IP アドレスによるアクセスコントロール
- User-based Security Model と View-based Access Control Model

5.2 IPv6 に対応した安全な情報交換技術の開発

一部の SNMP エージェントではコミュニティネームベースによる認証機構に加えて SNMP マネージャ

```
#          sec.name  source          community
com2sec mynetwork 3ffe:200::/64 COMMUNITY
```

図 5.1. IPv6 アドレスによるアクセスコントロールの設定例

の IPv4 アドレスによる認証機構を実装している。IP アドレスによるアクセスコントロールは、IP アドレスのなりすましを防ぐことができるならば、許可する組織の IP アドレスを指定することによって、効果的に制限をかけることができる。IPv6 では、経路情報の集約が効果的になされていることから IPv6 アドレスによる認証機構、アクセスコントロールの実現は有意義である。そこで本実装では net-snmp-5.0.pre1 を元にして、IPv6 アドレスとコミュニティネームを組み合わせたアクセスコントロールを実装した。以下に、今回実装した IPv6 アドレスによるアクセスコントロールの設定例を記す。

図 5.1 では prefix-length が 64 である prefix-address 3ffe:200:0:0 からのコミュニティネーム COMMUNITY からのアクセスを許可する設定になっている。

User-based Security Model が提供する SNMP アーキテクチャのセキュリティ技術を以下に挙げる。

- エンティティ認証機能
- データ認証、完全性検証機能
- プライバシー機能
- 時間

これらの機能は基本的にはトランスポートプロトコル層、つまり IPv6 に依存していない。ゆえに User-based Security Model の IPv6 対応化に関する特別な設計は必要でない。

View-based Access Control Model が提供する SNMP アーキテクチャのセキュリティ技術を以下に挙げる。

- エージェントの特定管理オブジェクトへのアクセス権利コントロール

これらの機能は基本的にはトランスポートプロトコル層、つまり IPv6 に依存していない。ゆえに View-based Access Control Model の IPv6 対応化に関する特別な設計は必要でない。

5.3 IPv6 に対応した安全な情報交換技術の評価

ここでは前節に説明した IPv6 に対応したネットワーク管理におけるセキュリティ技術の実装の評価を行う。評価対象は net-snmp-5.0.pre1 とそれをもとに本研究開発で実装した net-snmp-5.0.pre1 に対する IPv6 セキュリティ技術改良版である。

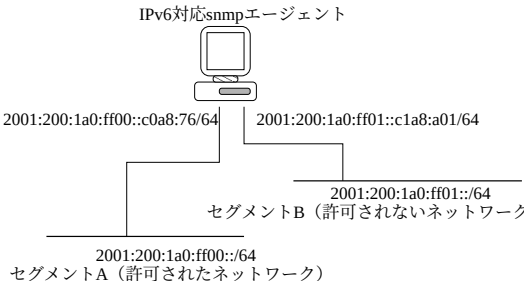

図 5.2. IPv6 アドレスによるアクセスコントロール技術評価用ネットワーク

表 5.1. アクセスコントロール技術評価テスト結果

セグメント	コミュニティネーム	結果
A	RIGHT	○
A	WRONG	Access deny
B	RIGHT	Access deny
B	WRONG	Access deny

net-snmp-5.0.pre1 では IPv6 アドレスによるアクセスコントロール技術は実装されていないので、我々の改良版を評価対象にした。図 5.2 に評価に用いたネットワークを説明する。

IPv6 対応 snmp エージェントはセグメント A (2001:200:1a0:ff00/64) から、コミュニティネーム RIGHT によるアクセスを許可し、セグメント B からのアクセスは一切許可しない設定とした。テスト内容と結果を表 5.1 に記す。

表 5.1 の結果は IPv6 アドレスによるアクセスコントロール技術が正しく実装されたこと示している。

次に net-snmp-5.0.pre1 と我々の実装との間の IPv6 ネットワーク管理におけるセキュリティ技術の対応について比較調査を行った。net-snmp-5.0.pre1 では VACM とアドレスによるアクセスコントロール機能を切り離すことはできないが、我々の実装では、IPv6 アドレスによるアクセスコントロールを実装することによって IPv6 対応 VACM を実現した。USM に関してはフレームワークの設計がトランスポートプロトコル層とは独立しているためオリジナルの net-snmp-5.0-pre1 でも IPv6 に対応していた。表 5.2 に結果をまとめた。

表 5.2. IPv6 ネットワーク管理におけるセキュリティ技術の対応についての比較調査

	net-snmp-5.0.pre1	本研究開発の実装
IPv6 アドレスによるアクセスコントロール	×	○
IPv6 対応 USM 認証サポート	○	○
IPv6 対応 USM 認証・暗号化サポート	○	○
IPv6 対応 VACM	×	○

第 6 章　IPv6 ネットワークの管理技術

6.1 IPv6 ネットワークにおける管理情報収集技術の現状

IPV6 に関係した管理情報ベース（IPV6-TCP-MIB、IPV6-UDP-MIB、IPV6-MIB、IPV6-ICMP-MIB）について、代表的なプラットフォーム上での実装状況の調査を行った。

調査を行った時点（2001 年末）では、IPv6 トランスポートをサポートしているベンダー製のルーターにおいて、上記 MIB をサポートしているルーターは存在しなかった。他のプラットホーム（Workstation、PC 等）でも、kame および usagi が実装されている FreeBSD 4.x、NETBSD 1.5.x、Linux 以外では、その実装を確認することは出来なかった。

さらに、実装が確認されたプラットホームについて、MIB の詳細な実装状況の調査を行った。

(1) IPV6-TCP-MIB
NetBSD 上でのみ MIB にアクセス可能であったが、正常な値が取得できず、実装が十分でないことがわかった。

(2) IPV6-UDP-MIB
NetBSD、FreeBSD において MIB にアクセス可能であったが、(1) と同様に正常な値が取得できず、実装が十分でないことがわかった。

(3) IPV6-MIB
全定義 MIB 72 種類のうち、NetBSD と FreeBSD は 29 種類、Linux では 9 種類の実装が確認された。

(4) IPV6-ICMP-MIB
全定義 MIB 36 種類のうち、NetBSD と FreeBSD でのみ、34 種類の実装が確認された。

以上の調査により、IPv6 関連の管理情報ベースの実装は全般に遅れており、現状では通信部分の IPv6 化だけを推し進めても IPv6 ネットワークに関して管理を満足に行い得る情報を収集できない状況にあることが明らかになった。

これらの調査結果から、我々は、IPv6 ネットワーク管理情報生成エージェントのマルチプロトコル対応化の必要性を認識し、新たに以下の 2 つの管理エージェントを開発することにした。

(a) マルチプロトコルトラフィック情報収集エージェント

(b) IPv6 対応ネットワーク侵入検知情報メッセージ通知エージェント

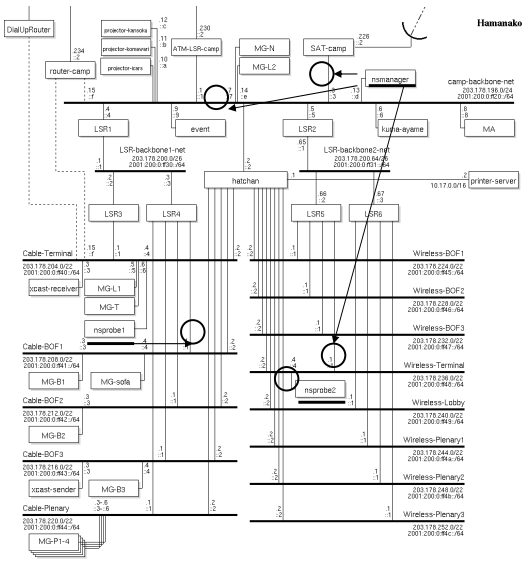

図 6.1. WIDE-camp Spring 2002 でのマルチプロトコルトラフィック観測実験

6.2 マルチプロトコルトラフィック情報収集エージェントの実装

このエージェントは、ネットワーク上のトラフィックを受動的に観測し、IPv4/IPv6 トラフィックの計測を行い、その情報を管理アプリケーションに提供する。我々は、計測された統計情報を SNMP によって外部に提供するためのに、CpMonitor MIB を開発

し、マルチプロトコル対応 SNMP-API 上に実装した。トラフィック情報の計測部は Snort の Out-put plugin として実装した。

6.3 IPv6 対応ネットワーク侵入検知情報メッセージ通知エージェントの実装

我々は、以前、Snort によって検知された侵入情報を、IPv4 ベースの SNMP-Inform プロトコルを用いてマネジャに通知するためのプラグインモジュールを開発した。このモジュールでサポートしている侵入検知情報通知のための MIB 定義（Snort-Common-MIB、Snort-Intrusion-Detection-Alert-MIB）は、現在 snort のリリースパッケージとともに配布されている。

本研究開発では、このプラグインモジュールを基に、マルチプロトコルに対応した侵入検知と侵入検知情報の通知が行えるシステムの研究開発を行った。本システムは、以下の 2 つの部分より構成される。

(1) マルチプロトコル対応侵入検知機能部
(2) マルチプロトコル対応侵入検知情報通知機能部

前者の機能を実現するために、TAHI の TANAKA Takashi 氏が制作した、IPv6 対応侵入検知モジュールパッチをそのまま利用した。我々がプロトタイプ実装を行ったモジュールは、後者の機能を実現するためのものである。本プロトタイプ実装には、本研究開発で実装を行った IPv4/IPv6 対応 SNMP エージェントのライブラリを基盤として用いている。

6.4 マルチプロトコルトラフィック情報収集エージェントの運用実験

開発したプロトタイプシステムの機能、性能を検証するため、まず、WIDE project が開催した WIDE-camp Spring 2002 の会場ネットワークにプロトタイプシステムを実装し試験運用実験を行った。実験環境を図 6.1 に示す。

実験においては、マルチプロトコルパケット監視機能（snort++-backEnd）を実装した nsprobe 3 台（1 台は nsmanager と兼任）、また、分散監視制御機能（snort++-frontEnd-MIB）および分散情報アクセスサポート機能を実装した nsmanager を実験ネットワークに設置し、分散して情報収集を行えることが確認された。そして、収集情報を統合的に可視化する機能（DemoGrapher）は JavaApplet の形で実装され、実験ネットワークのどこからでも Web ブラウザを利用して情報を取得することができた。図 6.2 に、取得した情報の表示画面を示す。IPv4/IPv6 のマルチプロトコルモニタリングが統合的に実現されていることがわかる。

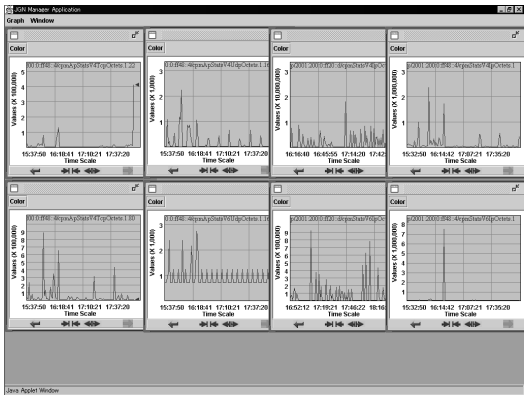

図 6.2.　マルチプロトコルトラフィック観測実験における表示画面

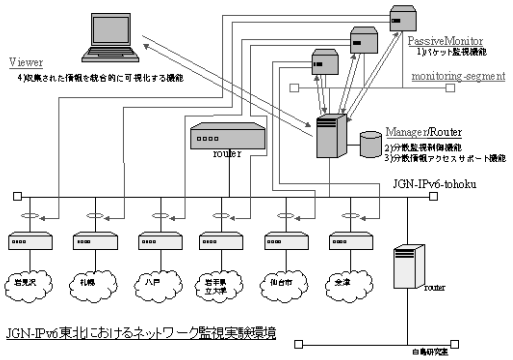

図 6.3.　東北大学分室内評価実験環境構成図

さらに我々は、WIDE-camp での試験運用実験を受けて、本格的な評価実験を行うための実験システムを、通信・放送機構ギガビットネットワーク研究プロジェクト東北大学分室に構築されている JGN-IPv6 ネットワークをテストベッドとして構築中である。図 6.3 に、その構成図を示す。

現在は 3 台のプローブ（p1、p2、p3）が分担して、東北各地区のトラフィックをそれぞれ個別にモニターしている。各プローブがモニターしているトラフィックはそれぞれ以下のとおりである。

p1）[.0] Summit →岩見沢市自治体ネットセンター
　　[.1] Summit ←岩見沢市自治体ネットセンター
　　[.2] Summit →札幌情報総合センター
　　[.3] Summit ←札幌情報総合センター
p2）[.0] Summit →八戸工業大学
　　[.1] Summit ←八戸工業大学

[.2] Summit →岩手県立メディアセンター
[.3] Summit ←岩手県立メディアセンター
p3) [.0] Summit →仙台市情報・産業プラザ ネ！ットU
[.1] Summit ←仙台市情報・産業プラザ ネ！ットU
[.2] Summit →会津大学情報処理センター
[.3] Summit ←会津大学情報処理センター

マネージャでは IPv4 はもちろん IPv6 を用いて各プローブの収集情報を逐次取得・蓄積している。なお、収集中のトラフィックデータは 2002 年 4 月 1 日現在以下の URL で公開中であり、Java 対応のブラウザを用いてデータを取得・閲覧することができる。

URL:http://130.34.38.187/~koide/DemoGrapher/

図 6.4 に、公開中の様子を示す。

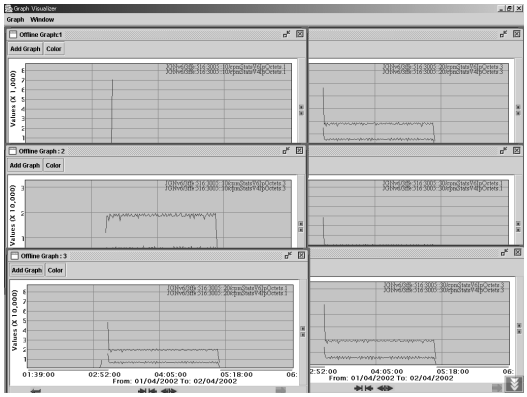

図 6.4. 東北各地区のトラフィック表示

6.5 ネットワーク侵入検知情報メッセージ通知エージェントに対するローカルテスト

ネットワーク侵入検知情報メッセージ通知エージェントと IPv6 対応 SNMP trap エージェントを用い、侵入検知情報の IPv6 による通知試験を行った。ネットワーク侵入検知情報メッセージ通知エージェントの設定ファイルを図 6.5 に示す。IPv6 通信を行うための “-6” オプションが指定されている。

この設定で動作させた際の IPv6 対応 SNMP trap エージェント側のログを図 6.6 に示す。

以上より、IPv6 により侵入検知情報が通知されていることが確認された。

第 7 章　まとめ

本研究では、(1) インターネット標準管理プロトコルである SNMP（Simple Network Management Protocol）の IPv4/IPv6 両対応のための設計と実装、(2) IPv4/IPv6 の両ネットワークをシームレスに管理できる標準管理技術（API および管理オブジェク

```
output trap_snmp: alert, 1, inform -v 2c -6 siga.priv.cysol.co.jp:5555 public
alert icmp any any -> any any (msg:"ICMP test";)
```

図 6.5. 進入検知情報通知エージェントの設定例

```
2002-03-01 18:31:25 2001:200:1a0:ff00::c0a8:3a [2001:200:1a0:ff00::c0a8:3a]:
system.sysUpTime.0 = Timeticks: (432006560) 50 days, 0:01:05.60
.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapOID.0 =
                                                    OID: enterprises.10234.2.1.3.1
enterprises.10234.2.1.1.1.3.1 = "Snort! <*-.Version 1.8.3 (Build 88)"
enterprises.10234.2.1.1.1.5.1.5 = 1
enterprises.10234.2.1.1.1.6.1.5 = "192.168.0.58"
enterprises.10234.2.1.2.1.2.1.5 = "1014975085.395145"
enterprises.10234.2.1.2.1.4.1.5 = "ICMP"
enterprises.10234.2.1.2.1.6.1.5 = 1
enterprises.10234.2.1.2.1.7.1.5 = "192.168.0.191"
enterprises.10234.2.1.2.1.8.1.5 = 1
```

図 6.6. 通知情報のログ

トMIBのマルチプロトコル対応）の確立、(3) 新しいネットワーク機器およびサービスを効率的かつ安全に管理する技術（セキュリティ機能SNMP v1/v2/v3プロトコルの相互運用）の確立、の3点の研究開発を実施した。

取り組んだ技術課題は、(a) IPv6ネットワーク用インターネット標準管理プロトコルの研究と実装、(b) マルチプロトコルネットワークの管理技術の研究開発、(c) 大規模広域IPv6ネットワークにおける情報収集および制御技術の研究、(d) セキュリティ管理技術の研究開発、(e) 新しいネットワークアプリケーションへの適用研究の5つである。

(a) では、IPv6 MIBモデルの策定を行い、SNMP over IPv6プロトコル仕様の策定を行った。(b) では、(a) の成果をもとに、IPv4/IPv6マルチプロトコル対応SNMPエージェントの研究開発を行い、シームレスな管理を実現するための標準管理技術となる、IPv4/IPv6トランスポートプロトコルおよびSNMPv1、v2、v3プロトコルに対応したマルチプロトコル相互変換エージェントの実装を行った。(c) では、大規模ネットワークにおける管理技術の調査とIPv6ネットワークへの適応に関する調査研究を行い、IPv4/IPv6併用大規模ネットワーク管理の基盤となるマルチプロトコル対応自立型情報収集エージェントの実装を行った。(d) では、ネットワーク管理におけるセキュリティ技術の調査を行い、IPv6アドレスによるアクセスコントロール機能の設計と実装、およびSNMPv2、v3プロトコルのIPv6プロトコル上での動作検証を行った。(e) では、IPv6ネットワークにおける管理情報収集技術の現状調査を行い、“マルチプロトコル対応トラフィック情報収集エージェント” および “ネットワーク侵入検知情報メッセージ通知エージェント” の開発と運用実験を行った。

IPv6プロトコルに関する研究および開発は日本が世界をリードしており、本研究はそのコミュニティの中で進められた。本研究は、世界的に見ても、IPv6に関する最先端のネットワーク管理とネットワークセキュリティ技術の研究開発である。

本研究の成果は、IPv6ネットワークを管理するにあたって必要不可欠である基盤技術を世界に先駆けて与え、さらに、大規模マルチプロトコルネットワーク管理のために不可欠な要素技術の確立と、IPv6ネットワークに適合した管理情報収集エージェント技術の実現を可能とした。IPv6ネットワークの管理基盤のみならず、IPv4/IPv6混在ネットワークにおける管理技術の確立は、今後のIPv6ネットワーク普及の規模とシナリオに鑑みても、その波及効果は非常に大きいといえる。

現在、本研究の成果をもとに、SNMPプロトコルのIPv6化にかかわる国際標準化の議論（draft-ietf-ops-taddress-mib-02.txt）を、IETF総会やIETFのメーリングリスト等で積極的に展開している。また、本研究の成果を、net-snmpプロジェクトに対して、積極的にコントリビュートしている。

今後、本研究の成果をもとに、よりよく管理されたネットワークの実現をめざし、セキュリティ管理技術の普及をはかるためのマルチプロトコル対応セキュリティ管理サポートシステムの研究開発や、マルチベンダー機器におけるマルチプロトコル対応SNMP実装の相互接続性検証システムの研究開発等をすすめる予定である。