次世代ネットワーク（JGN　IPv6）の管理に関する研究（0211009）

Management of Next Generation network (JGN IPv6)

キニ　グレン　マンスフィールド　株式会社サイバー・ソリューションズ

Glenn Mansfield Keeni　Cyber Solutions Inc.

齋藤　武夫†　阿部　勝久††

Takeo Saitoh†　Katsuhisa Abe††

株式会社サイバー・ソリューションズ†，††

Cyber Solutions Inc.†,††

研究期間　平成 14 年度～平成 15 年度

研究費総額　48,417,685 円（間接経費、消費税を含む）

概要

IPv6 による次世代インターネットの普及を促し、その潜在能力を最大限引き出すためには、ネットワーク管理技術も次世代に対応した新しい技術が必要になる。そこで本研究開発では、広域にわたる IPv6 ネットワークを安全で効率的かつ容易に管理できる管理技術の確立を目的とし、IPv6 セキュリティ管理技術の確立と監視システムのスケーラビリティの向上、IPv4 に比較して複雑性が増している IPv6 の構成管理を容易にする技術についての研究開発を行なった。具体的には、（1）パッシブ型ネットワーク情報収集プローブのセキュリティ関連機能の拡張、及び、インターネット標準プロトコルである SNMP と LDAP を基盤とした（2）分散配置されたネットワーク情報収集プローブの活用技術、さらに（3）IPv6 ネットワークマップの自動生成と活用技術に関する研究開発を実施し、JGN IPv6 ネットワーク上で実運用を行い、その評価を行った。

Abstract

New network management technology for next generation networks which operate on a new generation of protocols e.g. IPv6, is necessary. In this work, we have proposed and experimented with new network management technics, which can manage a large-scale, very high speed, wide-area IPv6 network securely, efficiently and easily.　We have focused on the following three issues, establishment of secure IPv6 network management using security features of the SNMP management framework, improvement of the management system's scalability using SNMP and LDAP, and technology to discover IPv6 network topology.

１．研究目標

パッシブ型ネットワーク情報収集プローブのセキュリティ関連機能の拡張として

（a）IPv6 セキュリティ関連情報収集機能の実現

を、分散配置されたネットワーク情報収集プローブに関して次の３点を、

(b) 分散プローブにより収集された情報の、安全で効率的な管理技術

(c) 分散プローブの、安全で効率的な管理制御技術

(d) 分散プローブによる、セキュリティ関連情報の収集利用技術

また、ネットワークマップ技術に関して次の２点の研究開発を実施することを目標とした。

(e) IPv6 ネットワークマップをベースとした情報提供ユーザインタフェース

(f) IPv6 ネットワークマップの自動生成技術

これら各課題の位置づけを図 1 に示す。

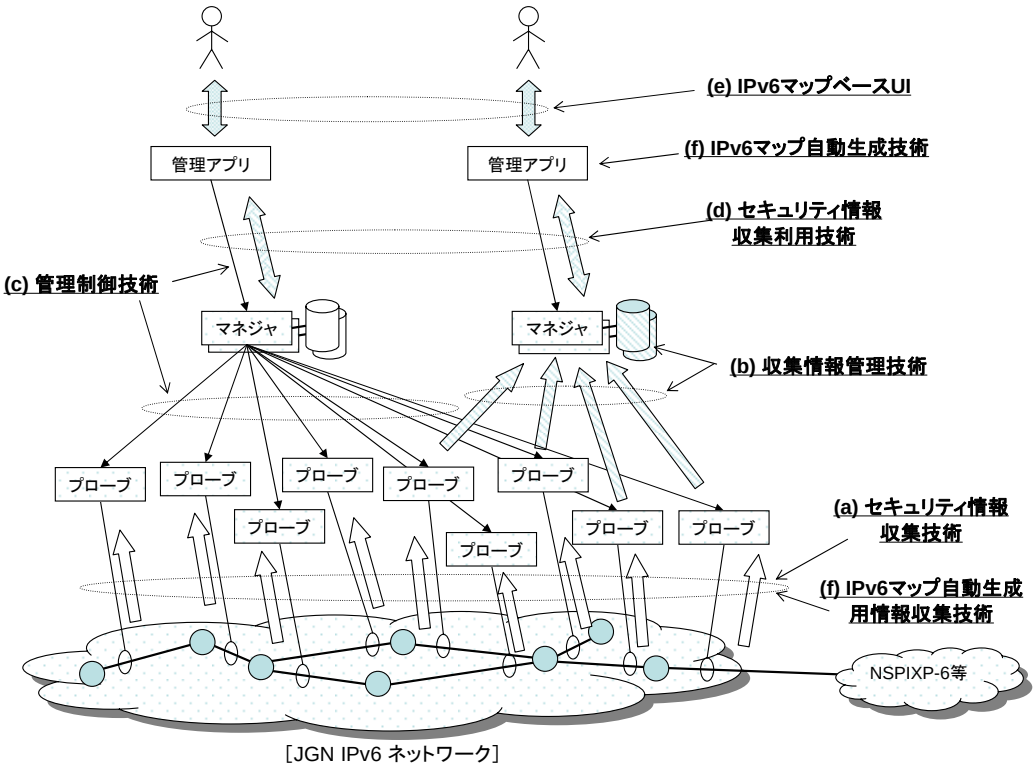

図 1　技術課題の位置づけ

２．研究内容

2.1. セキュリティ情報収集機能

パッシブ型ネットワーク情報プローブを用いたセキュリティ関連情報の収集機能についての研究開発を行った。具体的には、(1) IPv6 アドレスに対応する端末の物理アドレス（MAC アドレス等）の収集機能、および(2)シグネチャベースによる IPv6 対応侵入検知情報収集機能の開発、および(3) IPv6 ネットワークにおける攻撃手法に関する調査と考察を行なった。

(1) については、同一リンクに属する全ての端末を表すマルチキャストアドレス（FF02::1）に対する ICMPv6Echo Request を用いる手法、及び Neighbor Discovery Protocol を用いた手法についてのプロトタイプ実装を行い、その有効性について評価を行った。

(2) では、ソースが公開されている侵入検知ソフトウェアsnort[1]を用いたシグネチャベースによるIPv6 対応侵入検知情報収集機能の開発を行った。具体的には、まず(a) 検知ルール解釈機能のIPv6 対応、(b) パケット検知機能のIPv6 対応、(c) アラート出力機能のIPv6 対応についての研究と実装を行った。本実装のソー

[1] Snort, http://www.snort.org/

スコードについては、http://www.cysol.co.jp/contrib/snortv6/ にて広く一般に公開している。

(3) については、ポートスキャン及び IPv6 アドレス発信元詐称技術についての調査を行い、IPv6 アドレスの詐称を行うサンプルプログラムの実装を行った。

2.2. 収集情報管理技術

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、収集情報管理技術についての研究開発を行った。具体的には、(1) IPv6 に対応した SNMP プロトコルを基に、自律的にネットワーク管理情報を収集し蓄積するエージェントの開発、(2) (1) の JGN IPv6 ネットワーク上での運用実験と評価、(3) IPv6 に対応した LDAP プロトコルを基に、エージェントが収集管理するネットワーク情報を検索可能とする技術の研究と試作を行った。

(1) 分散プローブからの情報収集

分散配置された多数の情報収集プローブからの効率的な情報収集技術について、プロトタイプ実装を行った。このシステムの設定ファイルは図 2 に示す構造を持ち、収集されたデータは図 3 に示すディレクトリ構造下に蓄積される。ここで、cpmStatsV6IpOctets 1.0 に対応したデータは図 3 の場所(*)以下に図 4 に示すフォーマットに従って格納される。

```
CbOpt.pl udp6:v6mon.nemoto.ecei.tohoku.ac.jp nemoto v6community1 60 r0:: Version = 2
-------- ---------------------------------- ------ ------------ -- ---- -----------
|        |                                  |      |            |    |    |
|+-------+                                  |      |            |    |    |
||+-----------------------------------------+      |            |    |    |
||||+-------------------------------------------------+          |    |    |
|||||+-------------------------------------------------------------+    |    |
||||||+-------------------------------------------------------------------+    |
|||||||
||||||+- 設定ファイル文法バージョン
|||||+-- RTT 保存フラグ他
||||+--- データ取得インターバル(秒)
|||+---- SNMP コミュニティ名
||+----- 管理ドメイン(単位)
|+------ CpMonitor エージェントアドレス(udp6:前置で IPv6(UDP)アドレス)
+------- プログラム名
cpmStatsV6IpOctets 1.0
------------------ ---
|                  +- CpMonitor インタフェース番号
+------------------- 管理オブジェクト
```

図 2 情報収集・蓄積プロトタイプシステムの設定

```
/usr/local/Poller                                          ... Poller Root Dir
  conf/Poller/                                             ... Poller Conf Dir
  data/                                                    ... Poller Data Dir (*)
       2003/                                                    <year>
            3/                                                  <month>
              26/                                               <day>
                 nemoto/                                        <管理ドメイン>
                        udp6:v6mon.nemoto.ecei.tohoku.ac.jp/    <エージェントアドレス>
                                                    cpmStatsV6IpOctets.1.0
```

図 3 収集情報が蓄積されるディレクトリの構造

```
1048659820 1654457709
1048659880 1654458899
    :
1048659820 1654457709
---------- ----------
|          カウンタ値
タイムスタンプ
```

図 4 収集蓄積された情報のファイル構造

(2) JGN IPv6 ネットワークにおける分散モニタ環境の構築

本研究開発と平行し、JGN IPv6 ネットワークにおける実運用実験を行うための IPv6 分散プローブ環境の構築を行い、全国１５サイト、のべ４７箇所のギガビットおよびファーストイーサネットリンクのモニタリング環境の構築と運用を行った。（表 1）

表 1　IPv6 プローブ設置サイト

	サイト名	モニタ対象リンク		マネジャ
		100baseTX	1000base-SX	
1	東北大学シナジーセンター	1		
2	東北大学電気通信研究所	7		1
3	名古屋大学	2	1	
4	ソフトピアジャパン	3		
5	京都大学		1	1
6	広島大学	2	1	
7	広島市立大学	1		
8	九州大学	8	1	
9	佐賀大学	3		
10	TAO 北九州リサーチセンター	3		
11	TAO 大手町 IPv6 システム運用技術開発センター	2	1	1
12	TAO 岡山 IPv6 システム検証評価センター		1	1
13	堂島	2	1	
14	TAO 高知通信トラヒックリサーチセンター	3		
15	大阪大学	2	1	
16	東京大学			
	計	39	8	4

図 5 に収集されたトラフィック情報のグラフを示す。このグラフの下２つで観測されているラフィックは、JGN IPv6 ネットワークと NSPIXP-6 間の 100baseTX リンクを流れる IPv6 トラフィックである。

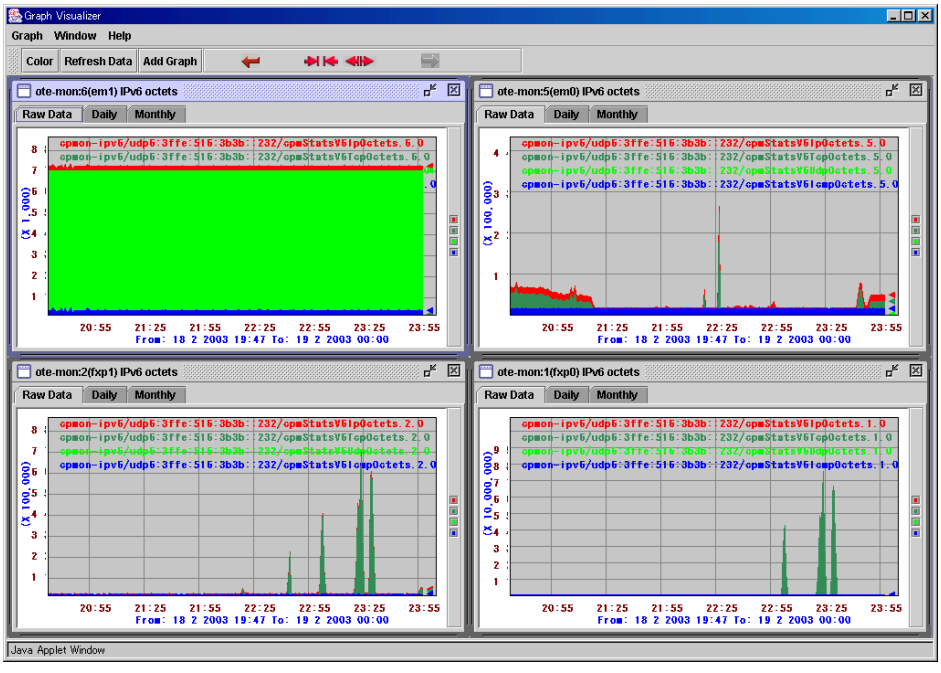

図 5　IPv6 トラフィック（TAO 大手町 ROC）

(3) LDAP を用いた分散プローブ運用支援技術の研究開発

個々の分散プローブがもつ収集情報は、そのプローブがもつ MIB の種類と、実際にトラフィックをモニタリングしているリンクの情報の組み合わせにより意味を持つ情報となる。前節で述べた SNMP を用いた分散情報収集技術を用いるためには、(a)トラフィックをモニタしたいリンクの情報と(b)そのリンクを実際にモニタリングしているプローブの情報、(c)収集したい情報の種類、が予め与えられる必要がある。

しかし、現在、これらの情報は、リンク情報についてはネットワークの運用者が、プローブの情報についてはプローブの設置者が、収集したい情報については情報の利用者がそれぞれ個別に把握している情報である。したがって、あるリンクの利用者が目的とするトラフィック情報を得るためには、ネットワークの運用者とプローブの設置者から個別に情報を得てはじめて収集可能か不可能か、また得られる情報の種類はどの様なものかを知ることになる。また、プローブの設置者は、プローブの障害や収集情報の変更、モニタ対象リンクの変更などが発生した場合、その変更情報を利用者やネットワーク運用者に効率的に知らせる手段をもたない。

そこでこれらの問題を解決する手法として、モニタ対象リンク、プローブ装置、収集情報、運用者、利用者情報等をLDAP[2]サーバに登録し、IPv6 プロトコル上でこれら情報を参照することによって分散プローブの運用と利用をより効率的に行うための技術の研究開発とプロトタイプ実装を行った。

具体的には、インターネット上で広く用いられかつ IPv6 プロトコルに対応するオープンソース LDAP サーバである OpenLDAP (http://www.openldap.org/) を用い、Passive Traffic Monitor LDAP サーバを実現するための、link およびプローブの情報と収集している情報、および管理者情報を登録するためのクラス設計と schema 設計を行った（図 6)。ここでは、RFC2280 で定義されている Routing Policy Specification Language (RPSL)を参考にした。

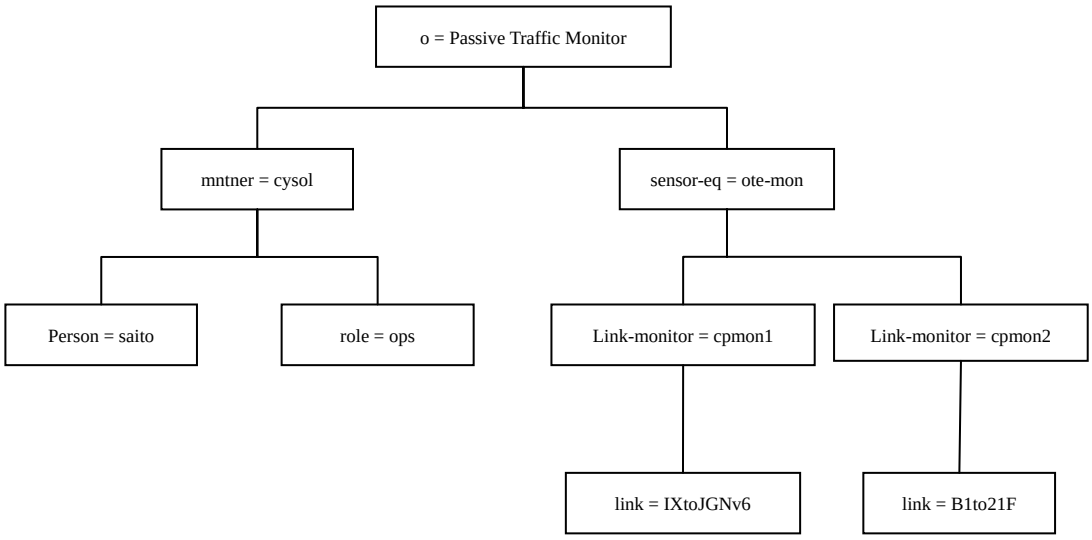

図 6　Passive Traffic Monitor の LDAP schema 図（objectclass）

これらにより、分散配置されたプローブが収集する情報を参照する際に必要な情報を LDAP サーバから検索、参照することが可能となり、さらにリンクやプローブに変更や障害が発生した際に連絡すべき担当者を容易に特定することが可能となった。

2.3. 管理制御技術

ネットワーク情報収集プローブは、それ自身の機能や構成を柔軟に変更することが可能となっている。この機能をより強力に活用するために、分散配置された多数のプローブ管理技術や、安全な制御技術の研究開発を行った。具体的には、(1) 遠隔からプローブの起動、停止、制御を行うための技術、及び(2)遠隔からプロ

[2] “Lightweight Directory Access Protocol (v3): Technical Specification”, J. Hodges, R. Morgan. September 2002, RFC 3377.

ーブの設定を変更するための技術の研究開発を行なった。

(1) SNMP を用いたプローブの起動、停止、制御

遠隔からプローブの起動、停止、制御を可能とする Sensor-Control-MIB(以下 **senConMIB**)を、SNMP の枠組みを用いて開発した。図 7 に MIB の一覧を示す.

```
> snmpwalk -v 1 -c public udp6:localhost senConMIB
SENSOR-CONTROL-MIB::senConIndex.1 = INTEGER: 1
SENSOR-CONTROL-MIB::senConID.1 = STRING: fxp0
SENSOR-CONTROL-MIB::senConStatus.1 = INTEGER: down(3)
SENSOR-CONTROL-MIB::senConLastChange.1 = STRING: xxx-3-25,14:33:31.0,-91:21
SENSOR-CONTROL-MIB::senConSecsToStart.1 = INTEGER: -1
SENSOR-CONTROL-MIB::senConSecsToStop.1 = INTEGER: -1
SENSOR-CONTROL-MIB::senConSecsToForward.1 = INTEGER: -1
SENSOR-CONTROL-MIB::senConForwardPeriod.1 = INTEGER: 110
SENSOR-CONTROL-MIB::senConForwardDestnType.1 = INTEGER: ipv4(1)
SENSOR-CONTROL-MIB::senConForwardDestn.1 = STRING: "120Forward"
SENSOR-CONTROL-MIB::senConAlivePeriod.1 = INTEGER: 130
SENSOR-CONTROL-MIB::senConAliveDestnType.1 = INTEGER: ipv4(1)
SENSOR-CONTROL-MIB::senConAliveDestn.1 = STRING: "xxx.cysol.co.jp"
SENSOR-CONTROL-MIB::senConSecsToReloadSigs.1 = INTEGER: -1
SENSOR-CONTROL-MIB::senConSigFileName.1 = STRING:
```

図 7　senConMIB

SNMP における set 命令で senConMIB の Start/Stop MO に値をセットすることにより、当該プローブを遠隔から起動、停止することが可能である。さらに、認証および暗号化をサポートする SNMPv3 を用いることでセキュアなアクセスが可能であり、またプロトコルが単純で機能のモジュール化、エージェント化が容易であるため、自動制御や一括制御も容易に可能となった。

(2) プローブの遠隔設定変更技術

プローブの起動時やマネジャからの指示により、プローブが自律的に最新の設定ファイルをダウンロードする技術として、非対称暗号鍵を用いた secure shell によるファイル転送(scp)を用いる手法について検討を行った。具体的には、RSA や DSA といったアルゴリズムによって生成できる非対称暗号鍵による認証（公開鍵暗号方式）を用い、あらかじめ公開鍵をマネジャの認証リストに入れ、プローブ側には秘密鍵を持たせることで、マネジャはプローブを認証することができ、さらに設定情報を暗号化して安全に転送することが可能となる。

図 8 に、実験を行った自動設定のプロセスを示す。この実験により、プローブは、再起動のたびにマネジャにアクセスして SNMP のユーザ情報を参照し、変更があれば更新が行えることを確認した。

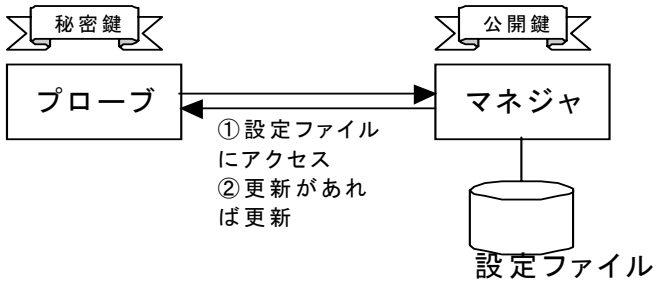

図 8 実験環境図

2.4. セキュリティ情報収集利用技術

セキュリティ関連情報に適した情報収集技術の研究開発を行った。セキュリティ関連情報は、一般的なネットワーク管理情報と比較しより即時性が求められるため、即時性をみたしかつ効率的な情報提供を行える通知技術と収集利用技術が必要となる。そこで、(1)IPv6 に対応した SNMP Inform 技術の活用に関する研究

開発と、Inform 技術により収集した情報を活用するためのアプリケーションの技術として、(2) Java 関連技術の IPv6 対応についての調査を行った。

(1) については、我々はネットワーク侵入検知システムsnortのアラート出力プラグインの一つ、SNMP アウトプットプラグインを実装した実績があり[3]、この実装のIPv6 対応化のための検討と実装、評価実験を行った。図 9 に、リンクローカルアドレスfe80::207:e9ff:fe23:b34aで稼動しているsnortからマネジャマシンに送ったアラートの出力を示す。

```
2004-03-19 18:34:44 fe80::207:e9ff:fe23:b34a%em0 [fe80::207:e9ff:fe23:b34a%em0]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (13928239) 1 day, 14:41:22.39
SNMPv2-MIB::snmpTrapOID.0 = OID: SNORT-ID-ALERT-MIB::sidaAlertGeneric-2
SNORT-ID-ALERT-MIB::sidaAlertTimeStamp.7.128 = STRING: 1079688884.241791
SNORT-ID-ALERT-MIB::sidaAlertMsg.7.128 = STRING: BAD-TRAFFIC same SRC/DST
SNORT-ID-ALERT-MIB::sidaAlertImpact.7.128 = INTEGER: badUnknown(2)
SNORT-ID-ALERT-MIB::sidaAlertMoreInfo.7.128 = STRING:
http://www.cert.org/advisories/CA-1997-28.html,
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016,
SNORT-ID-ALERT-MIB::sidaSensorAddressType.7.128 = INTEGER: ipv4(1)
SNORT-ID-ALERT-MIB::sidaSensorAddress.7.128 = STRING: "192.168.0.11"
SNORT-ID-ALERT-MIB::sidaAlertSrcAddressType.7.128 = INTEGER: ipv4(1)
SNORT-ID-ALERT-MIB::sidaAlertSrcAddress.7.128 = STRING: "192.168.0.49"
SNORT-ID-ALERT-MIB::sidaAlertDstAddressType.7.128 = INTEGER: ipv4(1)
SNORT-ID-ALERT-MIB::sidaAlertDstAddress.7.128 = STRING: "192.168.0.49"
SNORT-ID-ALERT-MIB::sidaAlertSrcPort.7.128 = INTEGER: 1101
SNORT-ID-ALERT-MIB::sidaAlertDstPort.7.128 = INTEGER: 1102
SNORT-ID-ALERT-MIB::sidaAlertEventPriority.7.128 = INTEGER: 2
SNORT-ID-ALERT-MIB::sidaAlertSrcMacAddress.7.128 = STRING: 0:e0:18:a8:16:93
SNORT-ID-ALERT-MIB::sidaAlertDstMacAddress.7.128 = STRING: ff:ff:ff:ff:ff:ff
SNORT-ID-ALERT-MIB::sidaAlertProto.7.128 = STRING: Protocol: UDP
SNORT-ID-ALERT-MIB::sidaAlertRuleID.7.128 = INTEGER: 527
SNORT-ID-ALERT-MIB::sidaAlertRuleRevision.7.128 = INTEGER: 4
SNORT-ID-ALERT-MIB::sidaAlertPacketPrint.7.128 = STRING:
bcabc0cda40d5c182e0b0ed84af0a006:028:032
```

図 9　snort 用 IPv6 対応 SNMP Inform 出力プラグインの実行例

(2)については、基盤技術となる IPv6 上の http および Java RMI 通信の調査と検証を進めており、IPv6 のみのネットワーク上におけるトラフィック情報の収集とアーカイブ、管理アプリケーションからの情報利用（Java アプリケーション）が可能であることを確認した。

2.5. IPv6 ネットワークマップをベースとした情報提供ユーザインタフェース

図 10 に開発を行ったネットワークマップを基にしたネットワーク情報表示アプリケーションの表示例を示す。本例では、JGN IPv6 の東北・北海道地域を構成するネットワークが表示されており、ネットワークマップ上で情報を表示したい機器を選択すると、その機器が持っている現在のトラフィック情報を可視化することが可能である。また、収集蓄積された過去のトラフィック情報も参照可能となっている。

[3] Snort SNMP Output Plug-in, http://www.cysol.co.jp/contrib/snortsnmp/

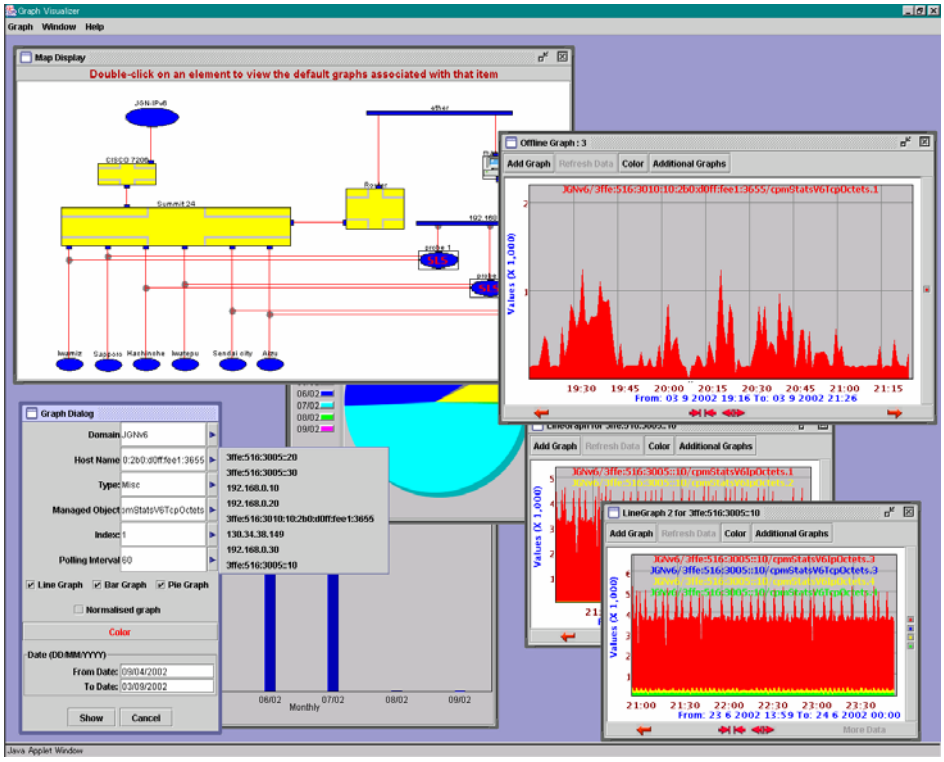

図 10　ネットワークマップを基にしたネットワーク情報表示アプリケーション

2.6. IPv6 ネットワークマップ自動生成技術

IPv6 ネットワーク上からオンラインで収集可能なネットワーク情報を基に、IPv6 ネットワークマップを自動生成する技術の研究開発を行った。具体的には、(1) IPv6 ルーティングに関する SNMP MIB 情報の利用の調査、及びパッシブトラフィックプローブによる情報収集技術により得られる (2) リンクレイヤ情報、(3) BGP-4 情報、(4) OSPFv3 情報を基にしたネットワークマップ自動生成技術の検討とプロトタイプ実装を行った。

(1) については、IETF のIPv6 分科会が提案を行っているIP Forwarding Table MIB[4]の利用について考察を行った。しかし、現在のところ、IPv6 に対応したIP Forwarding Table MIB情報を収集可能な機器は存在しないため、現状では、パッシブトラフィックプローブを用いたネットワークマップの自動生成技術の方が有望であろう。

パッシブトラフィックプローブを用いたネットワークマップ自動的生成技術は、ネットワーク構成機器から直接情報を収集する必要がないため、ルータ等がネットワーク構成情報を提供できない場合でもネットワークマップを作成することが可能である。

(2) のリンクレイヤ情報を収集する手法では、イーサネットフレームヘッダにおける物理アドレスと、そのパケット内の IPv6 ヘッダ情報を分析し、同一サブネット内のルータおよびホストを識別してネットワークマップを生成する技術を確立した。図 11 に、生成されたネットワークマップの例を示す。

[4] “IP Forwarding Table MIB”, B. Haberman, Febrary 2004, Internet-Draft, draft-ietf-ipv6-rfc2096-update-07.txt.

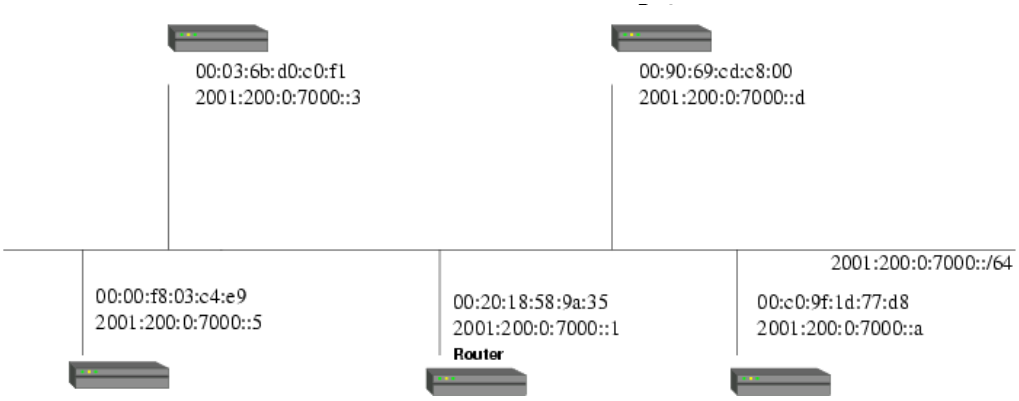

図 11　2001:200:0:7000::/64 ネットワークマップ

(3) の BGP-4 情報の利用では、(a) Open メッセージ、(b) Update メッセージ、(c) Notification メッセージ、(d) Keep Alive メッセージのそれぞれについて分析することにより、ネットワークマップの基となるグラフが生成できることが確認できた。例として、メッセージタイプが Keep Alive である BGP-4 パケットの発信元と到達先を結んだグラフを図 12 に示す。

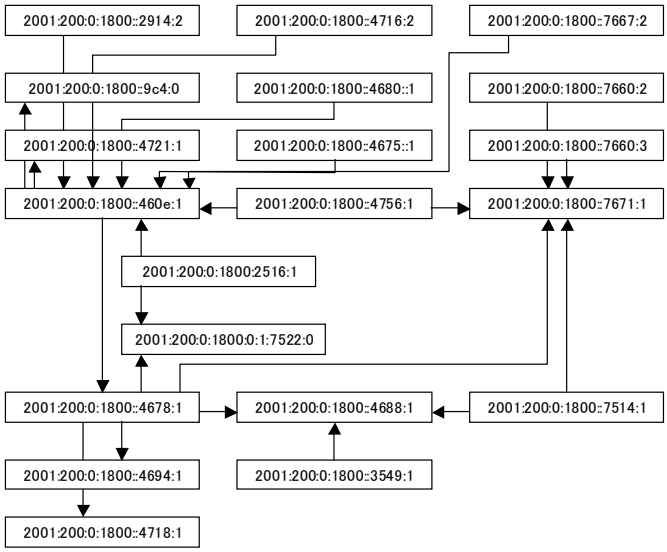

図 12　Keep Alive メッセージである BGP-4 パケットの発信元と到達先を結んだグラフ

(4) の OSPFv3 情報の利用では、Router LSA 情報における（Advertisement Router ID、Interface ID）から（Neighbor Router ID、Neighbor Interface ID）への写像を抽出することによりネットワークマップを生成する。本手法により、ネットワーク上に流れる OSPFv3 情報をパッシブモニタでモニタリングして構築したネットワークマップを図 13 に示す。ルータ（図中の箱）の中にある数字とピリオドの組は Router ID を示している。線はルータのつながりを意味している。線につけられている数字とピリオドの組は Interface ID を示している。OSPFv3 では Router ID、Interface ID には IPv4 アドレスの意味付けはされていないが、慣習上 IPv4 アドレスの形で記述される。

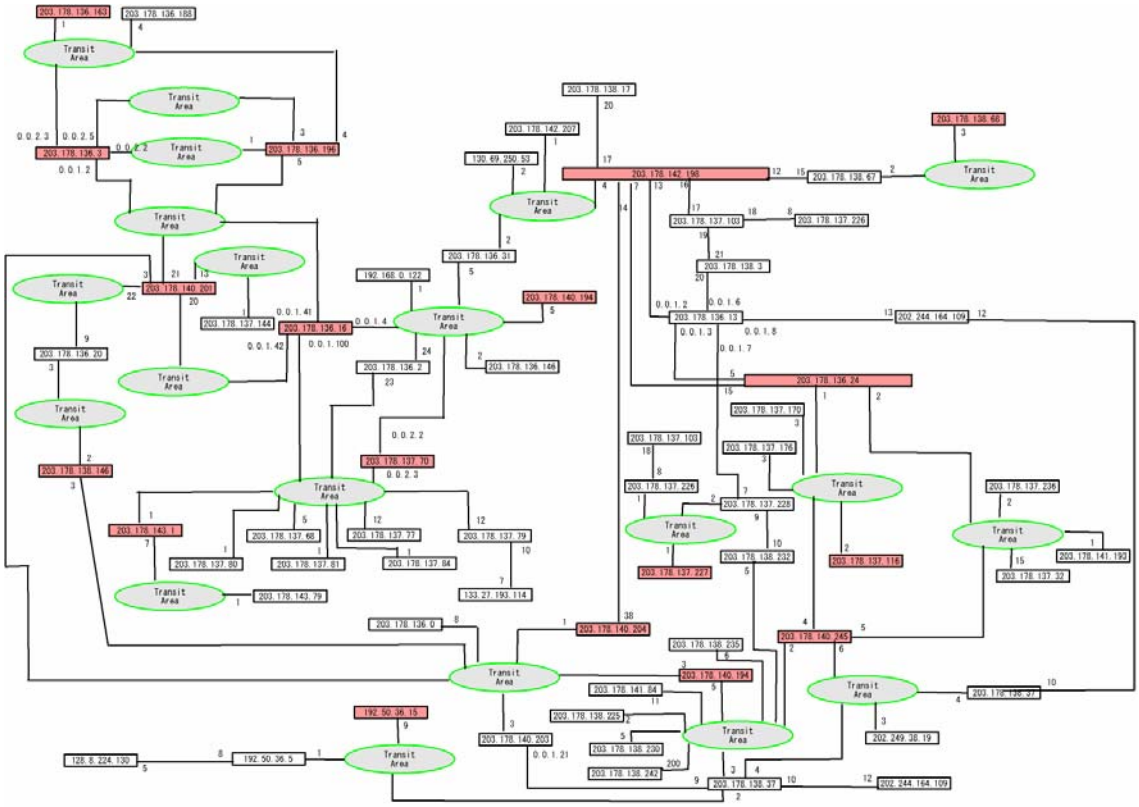

図 13　OSPFv3 ネットワークマップ

３．研究結果

IPv6 ネットワークの管理運用するための分散化された情報収集管理技術、ネットワークマップを基にした統合情報提供技術の実現を目的とした本研究では、（１）パッシブ型ネットワーク情報収集プローブのセキュリティ関連機能の拡張、および、インターネット標準プロトコルである SNMP と LDAP（ディレクトリアクセスプロトコル）を基盤とした（２）分散配置されたネットワーク情報収集プローブの活用技術、さらに（３）IPv6 ネットワークマップの自動生成と活用技術に関する研究開発を実施し、JGN IPv6 ネットワーク上で実運用を行い、その評価を行った。

（１）パッシブ型ネットワーク情報収集プローブのセキュリティ関連機能の拡張として

　　(a) IPv6 セキュリティ関連情報収集機能の実現

を、（２）分散配置されたネットワーク情報収集プローブに関して次の３点を、

　　(b) 分散プローブにより収集された情報の、安全で効率的な管理技術

　　(c) 分散プローブの、安全で効率的な管理制御技術

　　(d) 分散プローブによる、セキュリティ関連情報の収集利用技術

また、（３）ネットワークマップ技術に関して次の２点の研究開発を行った。

　　(e) IPv6 ネットワークマップをベースとした情報提供ユーザインタフェース（ＵＩ）

　　(f) IPv6 ネットワークマップの自動生成技術

(a)では、パッシブ型ネットワーク情報プローブに対して、IPv6 アドレスに対応する端末の物理アドレス（MAC アドレス等）の収集機能の研究開発を行った。シグネチャベースによる侵入検知情報ソフトウェア snort-2.0.2 の IPv6 対応のための研究開発を行った。

(b)では、管理対象と管理項目を効率的に管理するための収集情報管理技術を研究開発した。そしてそれらエ

ージェントが収集管理するネットワーク管理情報を、ディレクトリ技術を用いて検索可能とすることにより、情報収集の負荷を分散し、ネットワーク管理システムの負荷の軽減や、ユーザアプリケーションからの積極的な管理情報の利用が可能になった。

(c)では、分散配置された多数のプローブ管理技術や、安全な制御技術の研究開発を行った。具体的には、遠隔から、もしくは自律的に、複数プローブの一括設定変更や起動，停止、プローブの機能試験等を行うための技術の研究開発を行った。

(d)では、セキュリティ関連情報に適した即時性が求められる情報通知技術として、IPv6 に対応した SNMP Inform 技術の活用を行った。具体的には、侵入検知システム snort のアラート出力機能の一つである SNMP Output Plug-in を IPv6 に対応し、SNMP Output Plug-in が出力する SNMP Inform を IPv6 ネットワーク上で受信した。

(e)では、IPv6 ネットワークマップをもとにした、過去情報の参照が可能なネットワーク情報可視化ツールの研究開発と、一般ユーザが利用しやすい、ネットワークマップを基にした、ネットワーク情報閲覧ＧＵＩの研究開発を行った。

(f)では、IPv6 ルーティングに関する SNMP MIB 情報や、パッシブプローブを用いてオンラインで収集した IPv6 ネットワーク経路情報を基に、ネットワークマップの基本情報である IPv6 サブネットの情報やサブネット間の接続情報、AS レベルでの IPv6 ネットワーク接続情報や AS パス情報を生成するアルゴリズムの研究開発を行った。

４．今後の展開と波及効果

本研究の成果で確立される技術により、IPv6 ネットワークの安全性を高め、また、IPv6 ネットワーク上で稼動するアプリケーションが管理情報を積極的に利用するための基盤技術となる。また、より積極的に管理情報を活用する、ネットワークへの親和性を高めた高度なアプリケーションを実現できるようになる。また、それらを用いた応用技術の、本研究開発で利用する JGN IPv6 ネットワークを通じて運用，評価、開発し、大規模な検証を行った。以上により、本研究開発は、立ち遅れている IPv6 ネットワークの管理の側面を積極的に推進するとともに、ネットワークの安全性を高め、さらに、ネットワーク管理の新たな可能性を提示し、来るべき高度情報通信社会への移行を促進させる効果があると主張できる。

５．誌上発表リスト

[1] Glenn Mansfield Keeni, Kazuhide Koide, Debasish Chakraborty, and Norio Shiratori.、“SNMP in the IPv6 Context.”、2003 Symposium on Applications and the Internet Workshops (SAINT 2003 Workshops), pp254-257、(2003)

６．口頭発表リスト

[1]Glenn Mansfield Keeni、“SNMP in the IPv6 Context.”、SAINT 2003 Workshops (Orlando) (2003)
[2]土井一夫、“パッシブモニタ(CpMonitor)によるトラフィック情報可視化実験”、WIDE Project 2003 年春合宿（滋賀県長浜市） (2003)
[3]齋藤武夫、“JGN IPv6 ネットワークモニタリング環境について”、第 13 回インターネット技術第 163 委員会研究会（京都府亀岡市） (2003)
[4]土井一夫、“Pluggable CpMonitor”、WIDE Project 2003 年秋合宿（静岡県浜名郡） (2003)
[5]小出和秀、“JGN IPv6 ネットワークモニタリング:現状の問題点と今後の課題”、第 14 回インターネット技術第 163 委員会研究会（高知県須崎市） (2003)

７．申請特許リスト

なし

８．登録特許リスト

なし

９.受賞リスト

なし

10.報道発表リスト

なし

11.ホームページによる情報提供

[1]http://ote-man.otemachi.jgnv6.jp/、“次世代ネットワークの管理に関する研究”、ヒット数（未調査）
[2]http://ote-man.otemachi.jgnv6.jp/PmonSetup/ 、“IPv6 Passive Monitor Setup Manual”、ヒット数（未調査）
[3]http://www.cysol.co.jp/contrib/snortv6/、“Snort-IPv6 extended snort featuring IPv6 function.”、ヒット数（未調査）