



I E T F

第5回

Operations & Management Areaの動向
— SNMPとポリシーベースのネットワーク管理—

三宅 滋 (株)日立製作所 システム開発研究所
yake@sdl.hitachi.co.jp

はじめに

最近のIT大流行の恩恵で、一般消費者向けのTVコマーシャルの中でさえTCP/IPという言葉を目にする機会がある。一般の利用者からすれば、インターネットとは誰が面倒を見てくれているのか分からないが、いつでも自由に使える、という魔法のような世界であろう。しかし、インターネットという巨大システムの維持管理は容易なことではない。無数のオペレータの絶え間ない努力と、運用管理に関する多数の技術の標準化に対する活動がそれを支えている。今回の「連載IETF」では、そうした陰のシステムオペレーションを支える標準化の動きに注目してみたい。

OPS Areaとは?

一般的に、コンピュータネットワークなどのシステムを問題なく稼働させ続けるためには、システムの状態を絶えず監視し、障害や故障などの状況に応じたフィードバック制御

を行う必要がある。また、システム更新の際に、全体を完全に停止することなく新システムにスムーズに移行するには、綿密な計画と繊細な実行力が必要となる。無数のネットワークの集合体として稼働しているインターネットも例外ではなく、ネットワークの健全な動作を絶えず維持するには、インターネットを構成するそれぞれのネットワークに対して適切な状態監視と状況に応じた管理オペレーションを行わなければならないし、絶えず生まれてくる新しい技術を導入し続けるために、ネットワークの集合体であるインターネットを「完全に止める」などということはできない。

そうしたクリティカルなネットワークの管理とオペレーションに関する標準仕様を集中的に議論しようというコミュニティがOPS Area (Operations and Management Area)である(なお、IETFに設けられた8つのエリアに関しては、本連載の第3回に一覧が挙げられているのでそちらを参照いただきたい)。

OPS Areaの主な活動は、ネットワークの監視やフィードバック制御

といった管理とネットワークのオペレーションに利用できるフレームワーク、プロトコル、管理に使われる情報の内容などの仕様策定と、IPv4からIPv6へのスムーズな移行などのオペレーションを行うためのさまざまな方策を議論することにある。

OPS AreaのWG

2002年3月現在、OPS Areaには、22のWGが登録されている。表-1にWGの名前とChairを示した。それぞれのWGの詳しい活動内容については、各WGの趣意書¹⁾とIETF Meetingでの議事録²⁾が公開されているので参照していただきたいが、大まかに述べると次のようになる。なお、各WG名は比較的長いものが多いため、以下では略称のみを示す。

■aaa WG

ネットワークのアクセスの際に必要な機能である認証 (Authentication)、許可する活動の認定 (Authorization)、課金

WG 名 (略称)	chair
Authentication, Authorization and Accounting (aaa)	Bernard Aboba David Mitton
ADSL MIB (adslmib)	Michael Sneed
SNMP Agent Extensibility (agentx)	Bob Natale
Benchmarking Methodology (bmwg)	Kevin Dubray
Bridge MIB (bridge)	Les Bell
Distributed Management (disman)	Randy Presuhn
Domain Name Server Operations (dnsop)	Lars-Johan Liman Ray Plzak
Entity MIB (entmib)	Margaret Wasserman
Evolution of SNMP (eos)	Glenn Waters Dale Francisco
Ethernet Interfaces and Hub MIB (hubmib)	Dan Romascanu
IP Flow Information Export (ipfix)	Nevil Brownlee Dave Plonka
MBONE Deployment (mboned)	David Meyer
Site Multihoming in IPv6 (multi6)	Thomas Narten Sean Doran
Network Access Server Requirements (nasreq)	David Mitton Mark Beadles
Next Generation Transition (ngtrans)	Bob Fink Tony Hain A Durand
Policy Framework (policy)	Joel Halpern Ed Ellesson
Prefix Taxonomy Ongoing Measurement & Inter Network Experiment (ptomaine)	Mark Knopper Sean Doran
Resource Allocation Protocol (rap)	Scott Hahn Mark Stevens
Remote Network Monitoring (rmonmib)	Andy Bierman
Next Generation Structure of Management Information (sming)	David Durham
Configuration Management with SNMP (snmpconf)	Jon Saperia David Partain
SNMP Version 3 (snmpv3)	Russ Mundy David Harrington

表-1 OPS AreaのWGとChair

(Accounting) について、包括的な要件を議論している。

■ adslmib WG

ADSL (Asymmetric Digital Subscriber Line) をはじめとした xDSL による高速通信を管理するた

めの管理オブジェクトと MIB (Management Information Base) のパラメータの定義を議論している。

■ agentx WG

SNMP (Simple Network Man-

agement Protocol) Agent の拡張性を保証するために Agent 内部で利用する通信方式や Agent の実装方法を議論している。

■ bmwg WG

ネットワーク性能に関連した各種のベンチマークについて、用語や方式をまとめ、推奨方式を検討している。

■ bridge WG

さまざまなプロトコルのブリッジ機能を管理するための管理オブジェクトと MIB のパラメータの定義を議論している。

■ disman WG

SNMP を使ったネットワークの分散管理アプリケーションが利用するアラーム、イベントなど各種の管理オブジェクトと MIB の定義を議論している。

■ dnsop WG

Domain Name System (DNS) と Zone ファイルの管理オペレーションのガイドラインを作成している。

■ entmib WG

ひとつの SNMP Agent によって複数の MIB のインスタンスを管理しやすくするための相互関連を管理する MIB と、RMON MIB (Remote MONitoring MIB) 等で必要なセンサに関する MIB の議論を行っている。

■ eos WG

SNMP を利用した新しいネットワーク管理のパラダイムを検討している。

■ hubmib WG

Ethernet (IEEE 802.3) で定義されたインタフェースとハブの管理オブジェクトと MIB の定義を議論している。

■ ipfix WG

IP Flowの厳密な定義を行い、その情報を外部のシステムで利用するためのインタフェースとデータモデルの要件を検討している。

■ mboned WG

マルチキャストのネットワーク (MBONE) を広く展開するための種々のオペレーションについて議論している。

■ multi6 WG

複数の接続点でインターネットに接続したネットワーク環境 (Multi-homing) の問題点と解決策について、IPv6を対象として議論している。

■ nasreq WG

ダイヤルアップやVPN (Virtual Private Network) 等の遠隔からのアクセスを処理するNetwork Access Serverについての要件を検討している。

■ ngtrans WG

IPv6への移行について、シナリオ、使用するツール、他のWGとの連携など広範囲にわたって議論している。

■ policy WG

ポリシーベースネットワーク管理を行うための、ポリシーのメタモデルとネットワークのQoS保証を例とした実装方法の検討を行っている。

■ ptomaine WG

急激に増加しているインターネットの経路管理テーブルの問題点を整理し、解決策を議論している。

■ rap WG

以前は、RSVP (Resource Reservation Protocol) のアドミッション制御を議論していたが、現

在はポリシーベースネットワーク管理用プロトコルCOPS (Common Policy Service Protocol) 関連の実装を中心に活動を行っている。

■ rmonmib WG

ネットワークの稼働状況を遠隔から概観するためのRMONおよびRMON2で用いられるMIBの仕様検討を行う。

■ sming WG

MIBの定義に用いられるSMIの拡張について、ポリシーベース管理に用いるPIB (Policy Information Base) の観点から議論している。

■ snmpconf WG

SNMPを利用してネットワークノードの設定管理・変更を行うための仕様を議論している。

■ snmpv3 WG

SNMPv2に続くSNMPの次バージョンを検討している。

ネットワーク管理のフレームワーク—SNMPとMIB—

OPS Areaの活動を概観すると、合計22のWGのうち、9のWGで名称の中にSNMPまたはMIBという単語が含まれており、さらにほとんどのWGでSNMPやMIBに関連した議論が行われていることが分かる。SNMPとは、RFC1157で規定されているネットワーク管理を行うための基本プロトコルであり、これを利用するとRFC115で規定されたSMI (Structure of Management Information) に基づいた書式で記述された各種のMIBによって、ネットワーク上のノードやサービスの設定状況や稼働状態を管理することができる。

これら一連の仕様は1988年8月にRFC (RFC1065, RFC1066,

RFC1067) となり、それ以降ネットワーク管理用プロトコルの標準として広く使われている。この頃に開催されていたIETF Meetingは第10回であることから、OPS Areaで議論されているSNMPの仕様の基本は、IETFのかなり初期の段階から議論されてきたものであることが分かるだろう。それだけIETFに参加している技術者のあいだに、ネットワークの管理に対する問題意識が高かったことがよく分かる。

SNMPのフレームワークによれば、ネットワーク管理のモデルは、ネットワークを構成するルータなどの装置上で稼働するエージェントと、ネットワーク全体を統括的に管理するマネージャから構成される。ネットワーク管理者が、オペレーションの必要に応じてマネージャからエージェントに対する指示を出すことにより、エージェントが各装置の管理情報の取得や更新を行うというのがSNMPの基本的な動作である。オペレーションは、管理情報の読み出し (Get)、書き込み (Set)、状態変更の通知 (Trap) の3つの動作があり、メッセージは要求 (Request) と回答 (Response) の組合せで実現される。たとえば、ネットワークの管理者が、ネットワーク上にあるルータの設定状態を知りたい場合には、ネットワーク管理システム (NMS: Network Management System) から、知りたい管理情報の種類を指定してGetRequestをルータに対するコマンドとして投げると、相当する管理情報がGetResponseとして回答される。あるいは、ネットワーク上のあるルータ機器の通信ポートのうち1つが故障してしまったような場合、故障が起こったルータ機器がSNMPのTrapによりNMSに故障を通知すれば、ネットワーク管理者はNMSの故障表示を介して、ルータ機器の故障をいち早く察知し、部

品の交換などの対応ができる。このように、SNMPは単純であるが、非常に効果的なネットワークエレメントの管理手法を提供する。実際に、SNMPは、ネットワーク関連装置のかなりの製品に実装されており、大規模ネットワークの稼働状況を、SNMPにより監視を行っている例が多い。

SNMPによるネットワーク管理の質は、それによって管理可能な対象が何であるかに依存する。この部分の役割を担うのがMIBである。SNMPが開発された当初のMIBは、システムの識別、インタフェースカード、基本的なプロトコルについての管理情報を提供するものであった。その後、さまざまな装置、プロトコル、サービスエンティティなど、管理対象となるものについてMIBが次々と定義された。2001年11月時点での標準規格となるRFCをリストアップしたRFC3000によれば、StandardおよびProposed Standardの状態にあるMIBだけでも70種以上ある。他にも議論が進行中のMIBや、ベンダが独自に定義できるPrivate MIBも多数あるため、実際にSNMPとMIBによって管理可能なシステムは実に多岐にわたる。最近の傾向としては、新しいプロトコルやサービスが提案されてある程度仕様が定まってくると、その管理に必要となるMIBの定義も併せて行われるという流れになっているようである。現在では、IPプロトコルそのものとは直接の関連のないFibre ChannelスイッチやSCSIなどのストレージ関連の装置やプロトコル用のMIBを定義しようとする動きもある。

||| ポリシーフレームワークとSMIng

これまでSNMPとMIBによるネットワーク管理が対象としてきたものは、ネットワーク上にあるルータ

のように、個別の装置やサービスが中心であり、そのオペレーションも主な稼働管理や設定管理のような遠隔からの監視を目的としたものであった。近年になってRSVPやDiff-Serv (Differentiated Services) のような、インターネット上でのQoS保証のプロトコルやメカニズムが注目され、複数の装置を含んだドメイン全体に対して、QoS保証の設定を同時に行う必要が出てきたこともあり、ポリシーベースネットワーク管理 (Policy-based Network Management; PBNM) の概念がrap WGを中心として取り上げられるようになった³⁾。

PBNMは、If...Then...形式の基本的な動作ルールを組み合わせることで、管理オペレーションの簡略化と、ドメイン全般で一貫した動作を保証しようという試みである。この基本ルールの集合をポリシーとして定義し、DMTF (Distributed Management Task Force) が定義したCIM (Common Information Model) に準拠した情報モデルを構築していくこととなった。この作業にあたったのがpolicy WGで、1998年の第42回IETF MeetingでGeneral AreaのBOFとして開催され、1999年末の第46回IETF Meeting以降はOPS Areaに入っている。policy WGでは、これまでにPolicyの基本的な情報モデルPCIM (Policy Core Information Model) とその拡張モデルPCIMe (PCIM Extension) およびQoS保証関連ポリシーの情報モデルQPIM (QoS Policy Information Model) , QDDIM (QoS Datapath Device Information Model) の策定をほぼ終了して、活動は収束方向に向かっている。なお、IPSecなどのQoS保証以外のポリシーに関しては、それぞれのWGで個別に検討が進められている。

SNMPのMIBに相当するものとして、rap WGとpolicy WGの議

論の中で登場したポリシーに関するもう1つの仕様が、PIBの議論である。PCIMがポリシーの定義自体を管理するために用いられるのに対して、PIBは管理ドメイン内の各装置にポリシーを伝えるために用いられるものである。PIBの定義を行うために、従来のMIBの定義に用いられていたSMIを拡張したSPPI (Structure of Policy Provisioning Information) が提案された。クラス定義とインスタンスの扱いという概念が取り入れられ、よりオブジェクト指向的なアプローチをとったものである。このSPPIについて集中的に議論するのがsming WGである。

このように、OPS Areaでのネットワーク管理に関する動向は、従来のSNMP/MIBのフレームワークの適用範囲を拡大する方向と、PBNMのような新しいネットワーク管理パラダイムに沿った拡張を行う方向という、大きな2つの流れから構成されている。

||| 最近開催されたBOF

前述のWGのほかにも、年3回のIETF Meetingには、BOF (Birds Of a Feather) が何セッションか開催される。正式なWGへと発展していくBOFは必ずしも多くはないが、BOFが開催されるということは、かなりの数のエンジニアが何らかの理由でその分野に着目しているということで、活発な議論が期待できる。果たしてBOF開催の理由が何であるのか、新たな問題提起がきちんと行われるのかは、実際にBOFに参加して開催提案者の趣意を聞いてみないと分からないので、BOFにはできる限り参加するのが望ましいだろう。

以下は、最近2回のIETF Meetingで開催されたOPS AreaのBOFとその検討内容である。

■ IP Path Tracing (ippt) BOF

52nd IETF Meetingで開催。ハッシュを利用したIPパケット送信元の逆探知の手法とプロトコルの要件と問題点を議論した⁴⁾。

■ Configuration Management requirements (ops-nm) BOF

52nd IETF Meetingで開催。ネットワーク管理を行っているオペレータのコミュニティから、ネットワークの構成管理オペレーションに関する要望事項をまとめることを目的としたBOF。合計2回の開催が予定されている。

■ DNS Research Measurements (dnsmeas) BOF

52nd IETF Meetingで開催。各研究機関が実施したDNSの計測データを集約して検討することを目的とする。学術的研究の要素が強く、IETFよりもむしろInternet Research Task Force (IRTF)の活動である。

■ Packet Sampling (psamp) BOF

53rd IETF Meetingで開催。IPパケットをサンプリングして解析するための要件を、主にネットワークエレメントに要求される機能の面から議論することを目的としている。IPフローの状態を捉えようという活動としてipfix, rmonmibなどがあるが、IPパケットのマイクロ視的な情報を提供するという観点で異なっている。

■ Secure Internet Key Distribution (siked) BOF

52nd IETF Meetingで開催。さまざまなサービスに用いられるプロトコルで利用可能なPublic Keyの配布を行う方法を議論することを目的としている。

これらのBOFの中で、筆者が最

も注目したのはops-nm BOFである。このBOFは、これまでSNMP/MIBの仕様決定では、現場のオペレータからのフィードバックがあまり取り入れられなかったのではないかと、という反省に基づいて開催された。そして、実際に現場のインタビューをまとめてみると、設定変更は主としてコマンドラインによって行っているという意見が大勢であった。この背景には、SNMP/MIBはネットワーク監視には便利だが設定には使いづらい、という意図が汲み取れると筆者は感じている。逆に言えば、新しい管理パラダイムであるPBNMに対しては、きちんと設定系もサポートしなければ使われない、という厳しい要求が突きつけられたことにもなる。今後のOPS Areaの動向では、こうした設定変更を行うためのネットワーク管理プロトコルをどのように標準化するかという点に注目したいと考えている。

おわりに

— IETF Meeting 参加の誘い

OPS Areaが対象としているネットワーク管理とオペレーションという分野は、一般のユーザから注目されることが少ない領域である。しかし、この分野は、システムを構築し、定常的なサービスの提供を維持するためには欠かせない技術を数多く含んでいる。これはネットワークシステムに限らず、すべてのシステムの維持・管理に通じるものである。システムの運用に携わる技術者ばかりでなく、普段はネットワークを利用するだけのユーザも含めて、できるだけ多くの技術者がこの分野に興味を持ち、新たな技術を開発したり、新たなシステムを構築したりする際には、管理やオペレーションについて一考していただきたいと考えている。

そのための予備知識として、

OPS Areaの各WGで繰り広げられる熱い議論を、ぜひ一度実際に皆さんの目で確かめていただければ幸いです。

参考文献

- 1) IETF Working Groups, <http://www.ietf.org/html.charters/wg-dir.html>
- 2) IETF Online Proceedings, <http://www.ietf.org/proceedings/directory.html>
- 3) 小泉 稔, 三宅 滋, 平島陽子: ポリシーベースによるQoS制御, オーム社 (2001).
- 4) Mansfield, G.: IPPT (IP Path Tracing) Bof, 第52回IETF報告会, INTAP, (2002) <http://www.net.intap.or.jp/INTAP/ietf/52nd/3.htm>

(平成14年4月8日受付)

