IETF 標準化を中心としたポリシー管理技術の動向

The Trend of Policy-based Management Technology — IETF Standardization and Around —

金田 泰
Yasusi Kanada

日立製作所 研究開発本部 IP ネットワーク研究センタ
IP Network Research Center, Research & Development Group, Hitachi, Ltd.

1. はじめに

ポリシー管理 (policy-based management) はポリシーによってコンピュータ・システムやネットワークを管理する技術である．ポリシーとは条件-動作型の規則 (ポリシー規則) のならびである．ここにネットワークを制御するためのポリシー規則の例をあげる．

if (Source_IP_address == 192.168.0.1) { Priority = “high”; }

この規則は対象の機器があつかう各 IP パケットに適用され，そのパケットが IP アドレス 192.168.0.1 を始点とするパケットならばたかい優先度をあたえることを意味する．この規則をふくむポリシーをポリシーサーバが IP ネットワーク上のルータに配布することにより，上記のフローが優先配送される．

ポリシー管理は 1980 年代から Imperial College の Sloman らを中心に研究され [Slo 89, Dam 01]，とくにポリシーベースのアクセス制御は 1990 年代にはいってから活発に研究されてきた [RBAC]．ネットワークの管理モデルが従来の機器中心からサービス中心に変遷してきたことを背景として，ポリシー管理は 1998 年から DMTF (Desktop Management Task Force，分散管理技術の標準化を目的とした業界団体) と IETF (Internet Engineering Task Force) においてネットワーク標準化の対象となった．

ポリシーの形式に関しては IETF のポリシーフレームワーク・ワーキンググループ (Policy Framework WG，以下「ポリシー WG」とよぶ) を中心として標準化がすすめられてきたが，それについて 2 節でのべる．また，ポリシーの配布法や配布する各種のポリシーの具体的な表現に関しては IETF の RAP WG (Resource Allocation Protocol Working Group) を中心として各ワーキンググループにおいて標準化がすすめられてきたが，それについて 3 節でのべる．さらに，とくに最近 IETF 内外でいくつかポリシー記述言語をきめるうごきがあるので 4 節でのべる．

2. ポリシーフレームワーク

ポリシーの相互運用性を確保するには，それをデータベースに格納する際の情報モデルの標準化が重要である．アクセス制御，QoS，暗号化 (IPSec) など，ネットワークにおけるさまざまな制御・管理のためにポリシーを使用できるが，ポリシー WG においてはそれらに共通に使用されるべきポリシー・コア情報モデル (Policy Core Information Model, PCIM) [Moo 01a] を DMTF と連携しながら 2001 年に標準化し，現在はその拡張版 PCIMe の議論をつづけている [Moo 01b]．PCIM は条件-動作型の規則を基本としている．

また，PCIM を LDAP (Light-weight Directory Access Protocol) によって具体的に表現するポリシー・コアスキーマの標準化がすすめられている [Str 01]．ポリシーの格納にディレクトリを使用するのは，大規模ネットワークにおいては格納されたポリシーを多数のポリシーサーバがアクセスするため，よみだし性能が非常に重要だからである．

QoS に関する情報モデル [Sni 01] とスキーマもポリシー WG において標準化がすすめられているが，それ以外は IETF の他の WG にゆだねられている．たとえば，IPSec ポリシーについては IPSec WG や IPSec Policy WG においてあつかわれてきた[1]．

3. ポリシー配布プロトコルと配布方式

IETF においては，ポリシーにもとづいて決定をくだす対象を PDP (Policy Decision Point)，決定を適用する対象を PEP (Policy Enforcement Point) とよんでいる．ポリシーにもとづく決定の要求・配布方式としてつぎの 2 つの型がある．

- **アウトソース方式**：エンドユーザやアプリケーションが PEP 経由で PDP にオンデマンドで資源などを要求し，PDP がポリシーにもとづいて可否の決定をくだす方式．
- **プロビジョン方式**：オペレータが通信にさきだって PDP (ポリシーサーバ) 経由で PEP に決定やポリシーを配布する方式 (「はじめに」でのべた方式)．

RAP WG はポリシーに関する要求・配布のためにポリシーサーバ-機器間等で使用する COPS プロトコル [Dur 00] を 2000 年に標準化した．COPS は下位のプロトコルとして TCP を使用する．このプロトコルの用法として上記の要求・配布方式に対応してアウトソース方式のための用法である COPS-RSVP (COPS usage for RSVP) [Her 00] とプロビジョン方式のための用法である COPS-PR (COPS usage for PRovisioning) [Cha 01] とが標準化された．

COPS-PR によってはこばれるポリシーの形式をポリシー情報ベース (Policy Information Base, PIB) とよぶ．COPS-PR と PIB との関係は SNMP (Simple Network Management Protocol，インターネットにおけるネットワーク管理プロトコル) と MIB (Management Information Base) との関係にちかく，MIB を記述するための構文である SMIv2 (Structure of Management Information Version 2) に対応するものとして SPPI (Structure of Policy Provisioning Information) [McC 01] が標準化されている．SPPI が規定している PIB の形式は条件-動作型の規則にしばられず，汎用性がある．各種の PIB のうち共通につかわれる Framework PIB は RAP WG があつかっているが，分野ごとの PIB は各分野

[1] Chadha らの MPLS トラフィックエンジニアリング・ポリシーのように，その分野のポリシーをあつかう WG が存在しないため，どの WG でもあつかわれないままになってしまったインターネット・ドラフトもある．

の WG において標準化がすすめられている．おもなものとして Diffserv PIB，IPSec PIB などがある．

IETF の SNMP Conf (Configuration Management with SNMP) WG はポリシーをはこぶプロトコルとして SNMP をつかおうとしている．この目的のために Policy Based Management MIB [Wal 01] や DiffServ Policy MIB [Haz 01] を開発している．SNMP は UDP を使用しているので信頼性がひくく大量のポリシー通信には向かないが，COPS とはちがってあらたなプロトコルスタック開発が不要だという利点がある．

現在はポリシー管理のために CLI がもっともひろくつかわれているが，今後も上記のプロトコルのいずれかが CLI や他のプロトコルを駆逐することはないとかんがえられる．

4．ポリシー記述言語に関する動向

ポリシーを記述するにはその構文と意味とをきめる必要がある．つまり，ポリシー記述言語が必要である．Kosiur [Kos 01] はその標準化の重要性を指摘している．ポリシーは通常は「データ」だとかんがえられているが，それが実行可能であるためにはプログラミング言語としてのポリシーの意味が記述される必要がある [Kan 01].

ポリシー記述言語の標準化に関しては 1998 年に Strassner らが PFDL (Policy Framework Definition Language) をポリシー WG に提案したが，時期尚早として当面は言語を議論しないことをきめた経緯がある．また，PCIM にはポリシーの形式だけが記述されたのに対して PCIMe のドラフトにはいったんプログラミング言語的意味が部分的に記述されたが，51 回 IETF ポリシー WG 会合 (2001-8) において今後は記述しないことがきめられた．しかし，最近はポリシー WG 以外でポリシー記述言語に関するいくつかのうごきがみられる．

ポリシー配布には COPS と PIB を使用するのが従来の IETF のながれだったが，最近の Open Pluggable Edge Service (OPES) BOF (BOF とは WG の前段階の会合) には，ポリシーフレームワークには準拠しようとしているものの，ここにおさまらない内容がある．OPES BOF は最近の 4 回の IETF 会議 (2000 年 12 月 ～ 2001 年 12 月) においてひらかれたが，ここでは web コンテンツなどを加工するサービス (たとえば広告の挿入・削除) などを制御するポリシー記述言語 IRML (Intermediary Rule Markup Language) を議論している．

IETF 以外では，Sloman らのグループが高水準のポリシー記述言語 Ponder [Dam 01] を設計している．Ponder はおもにセキュリティポリシーの記述を目的としているが，アクセス制御だけでなく (管理者の) 義務 (obligation) がポリシーとして記述できるという特徴がある．Ponder のポリシーは人手の介在なしにはネットワークに配布できない (したがって Ponder はプログラミング言語ではない) とかんがえられるが，ネットワークへの配布法も検討されている [Lup 01].

最近の動向ではないが，ルーティング・ポリシーに関しては 1998 年に RPSL (Routing Policy Specification Language) が IETF 標準になり (RFC 2280, RFC 2622)，トラフィック計測用規則の記述言語 SRL (Simple Ruleset Language) が 1999 年に IETF に提案された (RFC 2723)．これらのネットワークポリシー言語を Stone ら [Sto 01] がサーベイしている．

5．むすび

ポリシー管理に関する標準化は IETF においてルータへの Diffserv の設定などネットワーク下層を中心にすすみ，それにもとづいてポリシーサーバ等の製品が開発されてきた．しかし，標準化はこれまでかならずしも成功していない．PCIM はこれらの製品において重要な位置にはないし，ポリシー管理の有力な適用先とかんがえられてきた QoS においては Diffserv PIB が複雑であつかいにくいものになっている．また，これらの標準にはポリシー管理に関する研究成果があまりいかされていない．今後は web など，より上位のサービスの制御において研究成果がいかされ，普及していくであろう．それとともに，ポリシーに関する標準化の舞台も IETF からネットワーク上位層をあつかう他の標準化団体にうつっていくとかんがえられる．

謝辞

草稿に関して詳細な意見をいただいた日立アメリカの三宅滋氏に感謝する．

参考文献

[Bec 01] Beck, A., and Hofmann, M.: “IRML: A Rule Specification Language for Intermediary Services”, *Internet Draft*, IETF.

[Cha 01] Chan, K. H., et al.: “COPS Usage for Policy Provisioning (COPS-PR)”, RFC 3084, Proposed Standard, IETF, 2001-3.

[Dam 01] Damianou, N., et al.: “The Ponder Specification Language”, *Policy 2001*, Lecture Notes in Computer Science, No. 1995, pp. 18–38, Springer, 2001-1.

[Dur 00] Durham, D., ed.: “The COPS (Common Open Policy Service) Protocol”, RFC 2748, Proposed Standard, IETF, 2000-1.

[Haz 01] Hazewinkel, H.: “The DiffServ Policy MIB”, *Internet Draft*, IETF.

[Her 00] Herzog, S., ed.: “COPS usage for RSVP”, RFC 2749, Proposed Standard, IETF, 2000-1.

[Kan 01] Kanada, Y.: “Taxonomy and Description of Policy Combination Methods”, *Policy 2001*, Lecture Notes in Computer Science, No. 1995, pp. 171–184, Springer, 2001-1.

[Kos 01] Kosiur, D.: Understanding Policy-Based Networking, Wiley, 2001.

[Lup 01] Dulay, N., et al.: “A Policy Deployment Model for the Ponder Language”, *IM 2001*, IEEE, 2001-5.

[McC 01] McCloghrie, K., et al.: “Structure of Policy Provisioning Information (SPPI)”, RFC 3159, Proposed Standard, IETF, 2001-8.

[Moo 01a] Moore, B., et al.: “Policy Core Information Model – Version 1 Specification”, RFC 3060, Proposed Standard, IETF, 2001-2.

[Moo 01b] Moore, B., et al.: “Policy Core Information Model Extensions”, *Internet Draft*, IETF.

[RBAC] 1st-5th ACM Workshop on Role Based Access Control, 1996-2000.

[Slo 89] Sloman, M. S., and Moffett, J. D.: “Domain Management for Distributed Systems”, *IFIP Symp. on Integrated Network Management*, North Holland, pp 505–516, 1989-5.

[Sni 01] Snir, Y., et al.: “Policy Framework QoS Information Model”, *Internet Draft*, IETF.

[Sto 01] Stone, G. N., et al.: “Network Policy Languages: A Survey and a New Approach”, *IEEE Network*, 2001-1/2.

[Str 01] Strassner, J., et al.: “Policy Core LDAP Schema”, *Internet Draft*, IETF.

[Wal 01] Waldbusser, S., et al.: “Policy Based Management MIB”, *Internet Draft*, IETF.