IETF 標準化を中心とした ポリシー管理技術の動向

金田　泰　(日立製作所)

ポリシー管理とは?

- ポリシー (ベース) 管理 (Policy-based management)
  - ポリシーにもとづいてネットワークやコンピュータや人間をふくむシステムや管理すること.
- さまざまなベンダのさまざまな機器を統一的な方法・インタフェースで管理 (制御) できる.

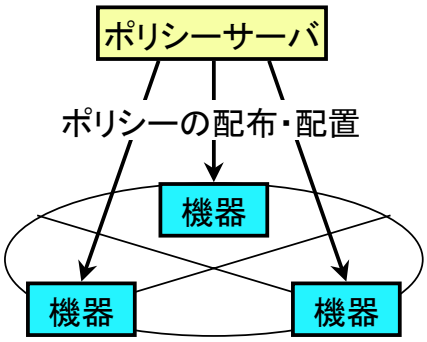
ポリシー管理に関する用語

■ **ポリシーとは?**
- ◆ ポリシー規則のならび: P = {r1, r2, …, r*n*}.

■ **ポリシー規則とは?**
- ◆ 条件-動作型の規則: if 条件 then 動作
- ◆ 例: ネットワークにおける優先配送ポリシー規則

```
if Source_IP_address == 192.168.0.1 then
    Priority = “high”;
```

■ **ポリシーの配備** (deployment)
- ◆ ポリシーはポリシーサーバから機器に配備されることによって機能する.
- ◆ Deployment はもとは軍隊用語であり, IETF の用語ではない.



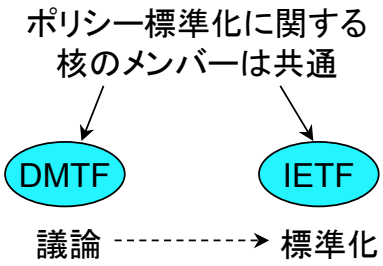
ポリシー管理に関する歴史

■ **研究**
- ◆ 1980 年代～
  - ▮ Imperial College の Morris Sloman らがポリシーにもとづくシステム管理を研究.
  - ▮ 現在もこのグループがポリシー研究の中核のひとつ.
- ◆ 1990 年代以降
  - ▮ ポリシーベース・アクセス制御が活発に研究された.
  - ▮ 学会の例: 1st-5th ACM Workshop on Role Based Access Control, 1996-2000.

ポリシー管理に関する歴史 (つづき)

■ 標準化

- ◆ 1998 年～
  - ▮ DMTF と IETF において標準化がすすめられた.
    - – DMTF (Desktop Management Task Force) は分散管理技術の標準化を目的とした業界組織.
    - – IETF (Internet Engineering Task Force) はインターネットのプロトコルの標準化を目的とした組織.



IETF における標準化の概要

■ ポリシーフレームワーク

- ◆ ポリシーの情報モデル (抽象的な形式) とディレクトリのための表現形式がポリシー WG において標準化されている.
  - ▮ ポリシー WG: 正確には Policy Framework Working Group

■ ポリシーの配布法・配布形式

- ◆ RAP WG を中心として標準化されている.
  - ▮ RAP WG = Resource Allocation Protocol Working Group

■ ポリシー記述言語

- ◆ ポリシー WG でもとりあげられたことがある.
- ◆ 現在は OPES WG などで議論されている.
  - ▮ OPES WG = Open Pluggable Edge Service Working Group

ポリシーフレームワーク

情報モデル標準化の必要性

■ 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形式を標準化する必要がある．

ポリシー WG におけるおもな標準化

■ ポリシー・コア情報モデル (Policy Core Information Model, PCIM)

- ◆ さまざまな分野の制御・管理に共通に使用されるべき部分.
- ◆ DMTF と連携しながら 2001 年に標準化された (RFC 3060).
- ◆ 現在はこのモデルの拡張版 PCIMe の議論をつづけている.
  - ▮ PCIMe = Policy Core Information Model Extension.
  - ▮ PCIMe の最新版は 2002 年 2 月のインターネット・ドラフト.

■ ポリシー・コアスキーマ (Policy Core LDAP Schema, PCLS)

- ◆ PCIM の LDAP (Light-weight Directory Access Protocol) による具体的な表現形式.
- ◆ まだ RFC になっていない.
  - ▮ 最新のものはインターネット・ドラフト draft-ietf-policy-core-schema-14 (2002 年 1 月).
- ◆ ポリシーの格納にディレクトリを使用する理由
  - ▮ 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.

ポリシー WG におけるおもな標準化 (つづき)

■ QoS に関するポリシー情報モデルとスキーマ (QoS Policy Information Model (QPIM), QoS Policy LDAP Schema (QPLS))

- ◆ これらもポリシー WG において標準化がすすめられてきた.

■ その他

- ◆ デバイス・レベルの QoS 情報モデル
  - ▮ 条件-動作 型のモデルではない (ポリシーのモデルではない) が, ポリシー WG において議論されてきた.
  - ▮ 最新のドラフトは draft-ietf-policy-qos-device-info-model-07 (2002 年 2 月)

他の WG におけるポリシー情報モデルの標準化

- **Core, QoS 以外のポリシー情報モデルの標準化は他の WG にゆだねられている.**
  - 例: IPSec ポリシー
    - 最初は IPSec WG, その後 IPSec Policy WG においてあつかわれてきた.
- **MPLS TE ポリシーに関するエピソード**
  - NEC 磯山氏他が MPLS トラフィックエンジニアリング・ポリシーのインターネット・ドラフトを提出.
  - こ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.

ポリシーの配布法と配布形式

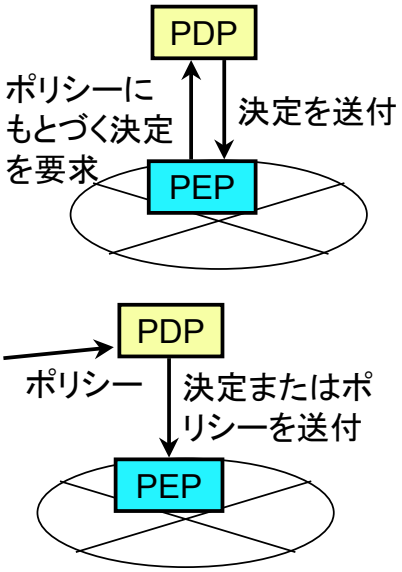
ポリシー配布の基礎

■ PDP と PEP

- ◆ PDP (Policy Decision Point) とはポリシーにもとづいて決定をくだす対象のこと.
- ◆ PEP (Policy Enforcement Point) とは決定を適用する対象のこと.

■ ポリシーにもとづく決定の要求・配布方式

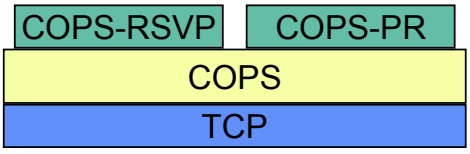
- ◆ アウトソース方式 ・・・・・・・・・・・・・・・・・・・・・・・・
  - ▮ エンドユーザやアプリケーションが PEP 経由で PDP にオンデマンドで資源などを要求し, PDP がポリシーにもとづいて可否の決定をくだす方式.
- ◆ プロビジョン方式 ・・・・・・・・・・・・・・・・ オペレータ
  - ▮ オペレータが通信にさきだって PDP (ポリシーサーバ) 経由で PEP に決定やポリシーを配布する方式.

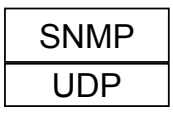


ポリシー配布プロトコル

■ COPS プロトコル

- ◆ 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プロトコル.
  - ▮ COPS = Common Open Policy Service.
- ◆ RAP WG によって 2000 年に標準化された (RFC 2748).
- ◆ COPS は下位のプロトコルとして TCP を使用する.
  - ▮ SNMP は (通常) UDP を使用するので, それより信頼性がたかく, 大量のポリシーをおくるのに適している.

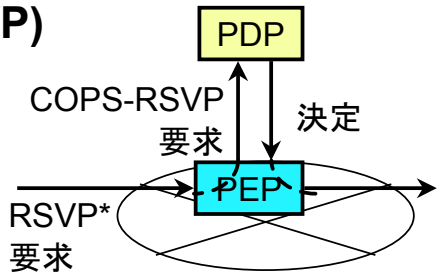




ポリシー配布プロトコル (つづき)

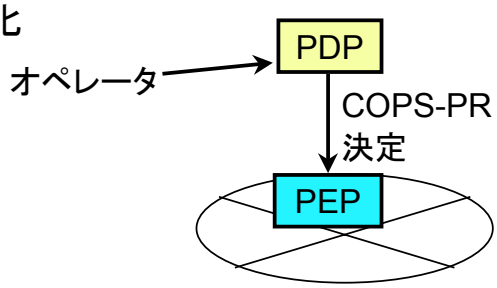
■ COPS-RSVP (COPS usage for RSVP)

- ◆ アウトソース方式のための COPS 用法.
- ◆ RAP WG によって 2000 年に標準化された (RFC 2749).



■ COPS-PR (COPS usage for PRovisioning)

- ◆ プロビジョン方式のための COPS 用法.
- ◆ RAP WG によって 2001 年に標準化された (RFC 3084).



* RSVP = resource ReSerVation Protocol

ポリシーの配布形式

■ ポリシー情報ベース (Policy Information Base, PIB)

- ◆ COPS-PR によってはこばれるポリシーの形式が PIB
- ◆ PIB を記述するための構文記法が SPPI (Structure of Policy Provisioning Information)
  - ▮ SPPI は 2001 年に標準化されている (RFC 3159).
  - ▮ SPPI は, MIB を記述するための構文記法である SMIv2 (Structure of Management Information Version 2) にもとづいている.
- ◆ PIB の形式は条件-動作型の規則にしばられず, 汎用的.

■ COPS-PR/PIB と SNMP/MIB

- ◆ ネットワーク管理のプロトコルとデータ表現のために, SNMP と MIB とがつかわれてきた.
  - ▮ SNMP = Simple Network Management Protocol.
  - ▮ MIB = Management Information Base.
- ◆ COPS-PR と PIB の関係は SNMP と MIB の関係に対応している.
  - ▮ SPPI と SMIv2 とが対応する.

PIB の標準化

- **標準化の中核は RAP WG**
  - 各分野で共通につかわれる Framework PIB や他のいくつかの PIB は RAP WG があつかっている.
    - どの PIB もまだドラフトの状態.
    - 標準化されずにおわる可能性もでてきた.
- **各分野の PIB はその分野の WG において標準化されている.**
  - Diffserv PIB は Diffserv WG.
  - IPSec PIB は IPSec WG.
  - …

COPS/PIB 以外のポリシー配布法

- **SNMP**
  - SNMP Conf WG はポリシー配布に SNMP をつかおうとしている.
    - SNMP Conf WG = Configuration-Management-with-SNMP Working Group.
  - ポリシー制御のための MIB の開発
    - Policy Based Management MIB や DiffServ Policy MIB を開発している.
  - SNMP と COPS との比較
    - 利点: 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.
    - 欠点: 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.
- **CLI**
  - 現在はポリシー制御のために CLI がもっとも多用されている.
    - CLI = Command-Line Interface
  - 設定インタフェースとしてはテキスト・ベースのほうがこのまれる (?)

COPS か SNMP か，それとも…

- **現在，COPS は主要なポリシーサーバ製品がサポートしているが，相互運用性はとぼしい．**
  - ◆ COPS をサポートしているネットワーク機器はすくない．
    - ▮ サポートしている機器の例:
      Cisco Catalyst 6000 シリーズ (LAN スイッチ)，日立 GR2000 (ルータ)．
  - ◆ COPS の用法は統一されていない．
    - ▮ PIB が標準化されていない．
    - ▮ COPS-PR はゆるい標準なので相互運用性が保証されない．
- **テキスト・ベースでありファッショナブル (?) な点で XML が魅力的．**
- **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 (?)**

ポリシー記述言語

ポリシー記述言語はなぜ重要か?

- 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 — ポリシー記述言語が必要である.
- 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.

ポリシー記述言語の標準化

- ポリシー WG における議論
  - PFDL (Policy Framework Definition Language)
    - 1998 年に Strassner らが PFDL を提案.
    - 時期尚早として当面は言語を議論しないことをきめた.
  - PCIMe に関する議論
    - 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.
    - 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.

ポリシー記述言語の標準化 (つづき)

■ 他の WG における議論

- ◆ OPES WG の IRML (Intermediary Rule Markup Language)
  - ▮ 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 を議論している.
    - – IRML は XML ベース！
  - ▮ OPES = Open Pluggable Edge Service
    - – OPES は 49～52 回の IETF では BOF (BOF とは WG の前段階の会合) としてひらかれ，53 回 (先週) に WG になった.
- ◆ 過去に標準化されたポリシー記述言語
  - ▮ ルーティング・ポリシーの記述言語 RPSL (Routing Policy Specification Language)
    - – 1998 年に標準になった (RFC 2280, RFC 2622).
  - ▮ トラフィック計測用規則の記述言語 SRL (Simple Ruleset Language)
    - – 1999 年に標準になった (RFC 2723).

ポリシー記述言語に関する研究動向

■ Ponder

- ◆ Sloman らのグループが高水準のポリシー記述言語 Ponder 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.
- ◆ 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.

むすび

- **ポリシーに関する標準化は 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んできた.**
- **IETF 標準にもとづくポリシーサーバ等の製品が開発された.**
- **ポリシーに関する標準化はかならずしも成功していない.**
  - PCIM などのモデルは上記の製品において重要な位置にはない.
  - QoS はポリシー管理の有力な適用先とかんがえられてきたが, Diffserv PIB は複雑であつかいにくいものになっている.
  - 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.
- **今後の方向**
  - 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.
  - 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組織にうつっていくであろう.