# LDAP을 이용한 정책 정보모델링 및 공유관리

손 선 경　　신 영 석*

◈ 목 차 ◈



## 1. 서 론

인터넷 사용의 급증으로 네트워크 관련 시스템과 기술이 비약적인 발전을 해왔으나, 통신망 관리와 정보보호가 소홀한 점으로 지적되고 있다. 또한 통신망을 관리하는 측면에서 통신 사업자의 주요 정책과 동적으로 변화되는 통신망 상태에 따라 효율적으로 통신망을 관리하는 방안이 다양하게 연구되고 있다[1-7].

기존 네트워크의 노드는 패킷 헤더를 중심으로 처리하여 패킷을 포워딩(forwarding)하는 단순한 방식으로 수행한다. 그러나 액티브 네트워크(active network)의 출현으로 관리자 혹은 사용자가 원하는 프로그램을 스마트 패킷에 실장하여 전송함으로서 중간 노드에서 특별한 관리자가 미리 제공하는 프로그램을 실행하여 다양하고 유동적인 네트워크 서비스를 제공하도록 패킷을 처리한다. 따라서 이러한 중간 노드에 해당하는 액티브 라우터는 관리자에 의해 일관성 있게 네트워크 관리와 기능을 설정하고, 이를 제어하는 기능이 요구된다. 액티브 네트워크 노드는 QoS(Quality of Service)와 정보보안 등 서비스뿐 만 아니라 응용 서비스를 비롯한 다양한 기능을 제공하며, 관리자가 손쉽게 별도의 정책(policy)에 의해 계층적이며, 일관성 있게 네트워크를 제어 관리하는 기능이 요구된다.

이와 같은 정책 기반의 통신망 관리(PBNM, Policy Based Network Management) 방식은 IETF와 DMTF, The Parlay Group 등의 표준화 기관을 중심으로 표준화 규격이 활발하게 연구되고 있다[4,7,11,15,16]. PBNM 상용제품 개발은 PBNM의 대상 서비스로 QoS와 정보보호 관리 서비스를 선정하여, Cisco와 Orchestream를 비롯한 여러 상용회사에서 제품을 개발하고 있다[17,18]

인터넷은 사설망과 WAN이 통합하여 구축되는 바, QoS와 정보보호 관리기능은 구축 형태와 사설망과 공중망의 혼재로 국한된 영역에서 관련 시스템에 부분적으로 기능을 적용하여 운영하고 있다. 또한 QoS와 정보보호를 비롯한 응용 서비스는 기능적으로 접속 프로토콜에 따라 패킷 필터링, 세션 계층의 정보 암호화와 네트워크 계층의 패킷 암호화로 분리하여 운영하고 있다. 따라서 이들 통신망과 기능을 통합적으로 손쉽게 관리하는 방법이 요구되고 있으며, 관리자는 이를 위해 일정한 정책을 수립하여 관리하도록 정책에 대한 정보공유가 요구된다.

기존의 네트워크 관리는 트래픽과 서비스 집중을 이용한 해킹으로 사설망과 WAN을 대상으로 정보보호 관리 기능을 효율적으로 운영하는 데 역부족인 결과를 초래하였다. 이로서 국부적인 지역적 관리의 한계성을 탈피하며, 특정한 정책을 통신망 전체에 배포하여 통신망을 관리하는 방식으로 변화되고 있다[2]. 한 예로 통신망 구성 장치(NE, Network Element)는 인터넷에서 QoS를 응용 서비스에 따라 다양한 버퍼관리 기능을 제공하고 있다. 운영자는 사용자가 요구하는 QoS 에 따라 해당 통신망의 서비스 정책을 수립하여, 동적으로 NE에 QoS 서비스를 위해 버퍼관리 알고리즘을 적용하여 부분적 혹은 WAN과 사설망을 통합하여 전체의 통신망을 논리적 정책으로 일관성 있게 관리하고 있다[2,6,7].

* 호남대학교 정보통신공학과 부교수

본 논문에서는 정책 기반의 QoS 관리 서비스는 표준화 기관에서 QoS 정책모델이 제시되었으며(RFC 3641, 3670, 3703), 현재 상용 시스템에 적용되어 사용하고 있다. 앞으로 효율적인 정보보호 관리 서비스를 위해 보안정책 객체에 대한 정보모델링을 수행하며, 이들을 네트워크에서 보안정책 정보를 공유하는 방안을 제시한다. 먼저 인터넷 상의 라우터 및 방화벽 등의 통신망 장치를 대상으로 정책 기반의 보안정책 객체를 모델링하며, 추후 액티브 네트워크에 다양한 NE를 적용하도록 정보모델링을 하였다. 네트워크 보안정책 정보공유를 위해 정책은 LDAP(Lightweight Directory Access Protocol) 서버에 저장하며, PMT (Policy Management Tool)와 PEP(Policy Enforcement Point)는 LDAP을 이용하여 보안정책 정보를 서버에서 접속하여 공유 모델을 제안하였다.

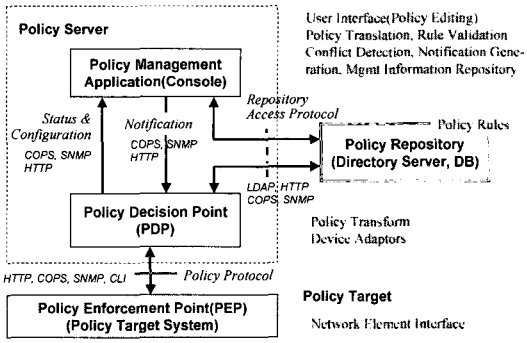
## 2. 정책 정보모델링

### 2.1 PBNM 통신 시스템

정책 기반의 통신망 관리는 통신망에서 제공하는 QoS, 정보보호 및 네트워크 자원을 공통된 형태로 공유하도록 환경을 제공하며, 이를 효율적으로 관리하는 데 있다. 정책 기반의 네트워크 관리는 NE의 MIB(Management Information Base), PIB(Policy Information Base)을 SNMP(Simple Network Management Protocol), COPS(Common Open Policy Service protocol), LDAP, HTTP 등의 프로토콜을 사용하여 네크워크 관리정보를 공유하여 정책을 관장하는 시스템에 설정된 정책규칙(policy rule)에 따라 운영된다. 정책관리 시스템은 동적으로 NE부터 수집된 정보를 분석하여 관리자가 설정하는 정책(혹은 정책규칙)에 따라 수행하도록 명령을 내리면 된다.

PBNM 시스템은 정책규칙을 제정하고, 정책에 따라 통신망을 운영하기 위해서 NE를 실시간으로 모니터링하며, 동적으로 변화되는 정보에 대해 신속하게 설정된 정책에 따라 수행하는 환경을 제공한다. 또한 설정된 정책은 일관성 있게 정보를 공유하여 실시간으로 NE에게 전달되어야 한다.

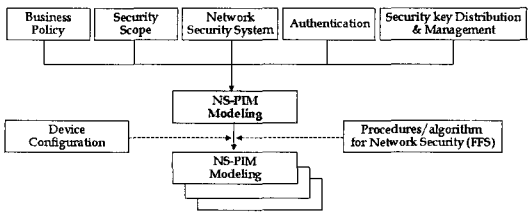
IETF 표준화 기관은 정책 기반의 네트워크 관리 기능의 표준 규격 작성을 위해 (그림 1)과 같이 PMT, PR(Policy Repository), PDP(Policy Decision Point), PEP 컴포넌트로 분류하였다. 정책 기반의 네트워크 관리를 위해 정책에 대한 기본모델 규격인 PCIM(Policy Core Information Model, RFC 3060)과 기본모델 규격을 확장한 PCIM-E (PCIM-Extension, RFC 3460)를 비롯하여 QoS와 IPsec(IP Security)에 적용을 위해 표준 규격을 작성하였으며, 이를 정보보호 네트워크에 적용을 위해 2003년부터 Opsec WG에서 표준화 연구를 수행하고 있다.




(그림 1) PBNM 시스템 컴포넌트

### 2.2 정책모델 표준화

네트워크 정책에 대한 정보모델링을 위해 우선 정책을 적용한 서비스 범위를 설정해야 하며, 이를 기반으로 다양한 NE에 운용되도록 기본적인 서비스 정책 범주와 적용 디바이스에 따른 모델이 요구된다. (그림 2)는 네트워크 보안정책에 대한 정보모델링 개념도를 보였다. 네트워크를 운영하는 통신사업자 관점에서 비즈니스 모델이 정립되며, 정보보호 서비스 범주, 이를 적용할 NE, 접속 및 확인 인증, 보안키 관리 등에 대한 범위를 설정한 후에 네트워크 정보보호 정책모델(Network Security PIM)을 정립해야 하며, 이를 PEP에 적용하기위해 다양한 NE에 따른




(그림 2) 네트워크 보안정책 정보모델링 개념도

단계적 정보모델링이 요구된다.

## 2.3 정책 정보모델

### 2.3.1 네트워크 보안정책 모델

본 연구에서는 QoS와 정보보호 서비스 중에 네트워크 정보보호에 관련된 정책에 대한 보안정책 객체를 DMTF CIM(Common Information Model ver 2.8)과 IETF PCIME를 근거하여, 라우터, 방화벽, IP 스위치, IDS(Intrusion Detection System)에 적용 가능하도록 네트워크 보안정책 객체를 모델링을 한다. 이는 결국 액티브 네트워크의 액티브 라우터에도 적용이 가능하며, 스마트 패킷을 액티브 라우터에 정책 적용과 처리를 위해 먼저 네트워크 정보보안을 위한 정책을 모델링한다. 추후 연구로 액티브 네트워크 관리를 위한 보안정책 모델로 확장하도록 한다.

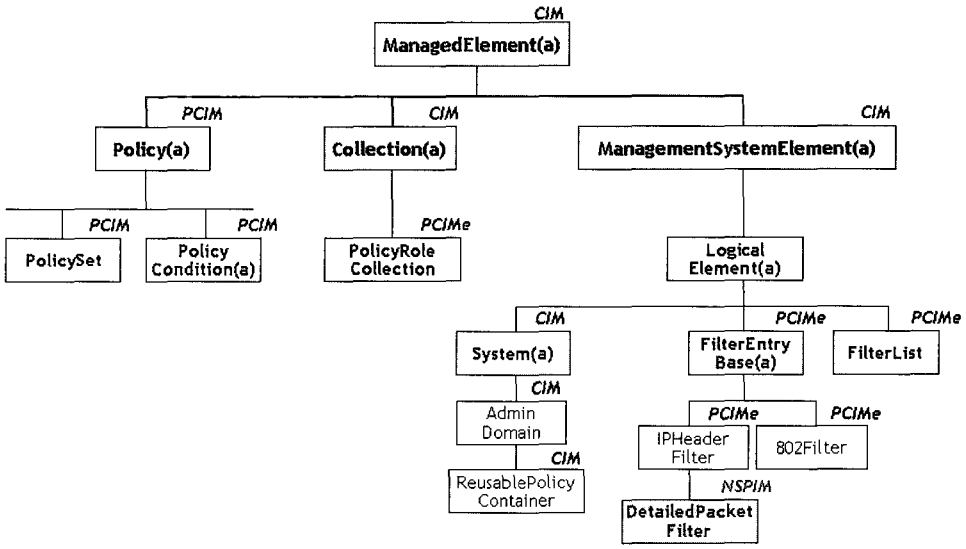
보안정책이 보안 라우터를 비롯한 NE에 적용하는 기능을 구분하기 위해 NE에서 적용 보안 기능과 이에 따른 대책을 수립하여 정책규칙과 수행 가능한 원칙을 (표 1)과 같이 기능을 그룹핑한 후에 네트워크 보안정책을 정보모델링 한다.

정책 기반의 보안정책 객체는 PolicySet을 근간으로 PolicyRule, PolicyGroup, PolicyCondition, PolicyAction로 구성된다. 그러나 NE를 단순히 관리자가 정책규칙에 의한 관리보다는 정보보호를 위해서는 통신망에서 운용되는 패킷과 정책규칙을 논리적으로 표현하는 객체로 인식해야 함에 따라 PolicyVariable, PolicyValue, Collection과 기존의 정책규칙 재사용하기 위한 PolicySet를 추가하여 Policy 객체와 의존성(dependency)을 가지도록 하였다.

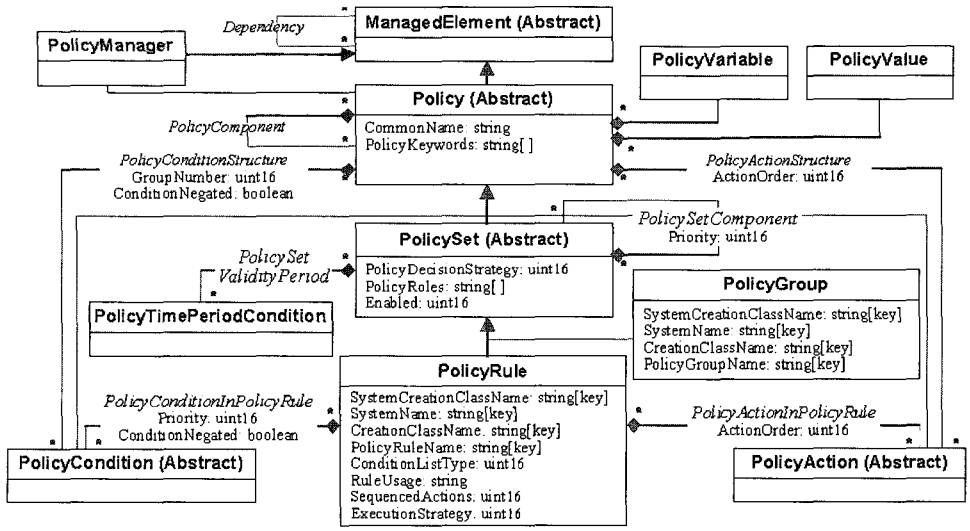
PolicyCodition은 PolicyTimePeriodCondition 등의 PCIM과 PCIME 클래스를 상속 받으며, (표 1)의 보안 시스템 기능에 따른 조건을 충족시키는 객체와 벤더에서 독자적으로 정의한 VendorPolicyCondition 객체로 의존성을 가진

(표 1) 네트워크 보안정책에 따른 condition과 action

| Function | Condition(factors) | Action |
|---|---|---|
| Alert Control Policy | source IP, destination IP, source port, destination port, protocol, attack ID, time interval | suppress aggregation ignore |
| Attack Control Policy | Snot 2.0-based signature | alert drop terminate |
| Access Control Policy | source IP, destination IP, source port, destination port, protocol, TCP 6 bits Flag, ICMP type, ICMP code, MAC address | permit deny track |
| Traffic Control Policy | source IP, destination IP, source port, destination port, protocol, average rate, normal bucket, extended bucket | export intercept rate limited control |
| Packet Monitoring Control Policy(*) | source IP, destination IP, source port, destination port, protocol, TCP 6 bits Flag, ICMP type, ICMP code, MAC address | analyze save ignore |
| Packet Filtering Control Policy(*) | source IP, destination IP, source port, destination port, protocol, TCP 6 bits Flag, ICMP type, ICMP code, MAC address, application service code, session No | grouping access control actions |
| Authenticate Control Policy | source IP, destination IP, source port, destination port, key, ID, password | pass fail & save log data |




(그림 3) 네트워크 보안정책 정보모델의 기본 클래스




(그림 4) 네트워크 보안정책 PolicySet 정보모델

다. PolicyRepository는 PolicyCondition과 PolicyAction 객체와 Policy에 연관된 객체를 정책 서버에 객체 정보로 저장한다.

보안정책 객체는 독립된 시스템에서 상호간 정보교환이 연관관계로 이루어진다. NE와 PMT, PDP/PEP에서 보안정책 객체에 대한 생성, 소멸, 접속 보안, 관리 등의 기능이 수행된다. 그러나 PMT에서 운영자에 의해 직접 통신망 구성장치의 보안정책 객체를 관리함으로서 상용제품의 회사별 의존적인 보안정책 객체 관리를 위한 PolicyManager 객체가 요구되나, 시스템 구현 측면에서 벤더에 의해 정의되도록 한다.

보안정책은 운영자에 의해서 간단한 정책규칙을 비롯하여 정책규칙 속에서 아래와 같이 다른 정책규칙을 사용과 필터 기능에 따라 PolicyVariable를 다양하게 모델

화 되어야 한다. 또한 보안정책 규칙은 PCIM과 PCIME의 PolicyRule 클래스를 근거로 설정된다. 네트워크 보안정책은 condition과 action으로 구조화된 형태로 정책규칙이 구성된다. 보안 정책규칙은 아래의 예제와 같이 복합적으로 논리화하여 규칙을 생성하는 경우에 이를 지원하도록 네트워크 보안정책 객체를 정보모델링 해야 한다.

예제 1:

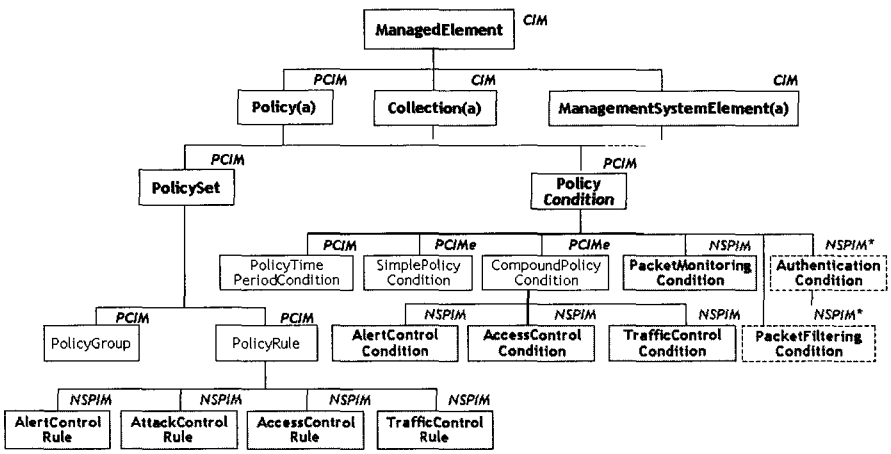
라우터에서 211.227.100.0 네트워크의 호스트는 접근 금지, 그러나 별도의 IP 주소인 211.227.100.23은 네트워크 A는 접속 가능하며, 211.227.100.2는 VPN으로 네트워크 B와 연결

"*if* <IP == 211.227.100.23> *then* <host:: access to network A>"
"*else if* <IP == 211.227.100.2> *then* <VPN connection>"
"*else if* <network == 211.227.100.0> *then* <host:: not access to network A>"

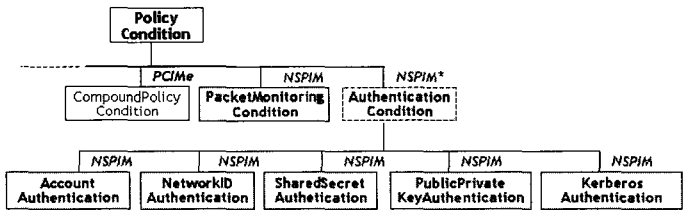
예제 2:

211.227.100.0 네트워크에 VPN을 제외한 연결을 금지하며, 라우터의 트래픽이 70% 수준을 유지하며, 특정 IP 주소로 접속을 요구하는 경우에 경보 및 접속 log 정보를 모니터링

"*if* <access packet == 211.227.100.0> *then* <Traffic BW =< 70%>"
"*and* {*if* <connection service == VPN> *then* <host:: access to network>
*or if* <IP address == assigned IP address> *then* <monitoring its packets>}"




(a) PolicySet 정보모델




(b) PolicyCondition정보모델

(그림 5) 네트워크 보안정책의 PolicySet과 PolicyCondition 정보모델

PolicyRule은 (표 1)에서 정의된 보안 시스템에 적용된 기능을 기반으로 AlertControlRule, AttackControlRule, AccessControlRule, TrafficControlRule을 구성하며, PolicyCondition에 CompoundPolicyCodition에 AlertControlCodition, AttackControlCodition, AccessControlCodition, TrafficControlCodition을 구성하여 보안 시스템의 주요 기능을 담당한다. 또한 PacketMonitoringCondition, PacketFilteringCondition을 두어 각각의 패킷에 따른 조건을 부여하였으며, Authentication 클래스를 정의하여 보안 시스템의 접속 및 정책규칙 액세스에 따른 인증을 하도록 하였다. Authentication은 DMTF CIM의 AccountAuthentication, NetworkIDAuthentication, SharedSecretAuthentication, PublicPrivateKeyAuthentication, KerberosAuthentication을 클래스를 수용하였다.

PolicyAction에 보안 시스템의 주요 기능인 AlertControlAction, AttackControlAction, AccessControlAction, TrafficControlAction을 정립하고, NetworkPacketAction와 RejectConnectionAction을 정의 하였다. (표 1)의 주용 기능에서 본 바와 같이 조건에 따른 동작(action)을 AlertControlAction은 AlertSurpressAction, AlertIgnoreAction, AlertAggregationAction 등으로 (그림 6)과 같이 정의하였다.

본 논문에서는 보안정책 정보모델은 IETF PCIM/E를 근거로 작성하였으며, 객체 접속에 따른 인증을 위해 Authentication을 5개 객체로 정립하였으며, PolicyAction에 PCIME 객체외 NetworkPacketAction, RejectConnectionAction을 추가하여 연결 및 접속에 따른 제어를 하였다.

최근 DMTF CIM 정책관리 표준안(버전 2.9)에서는 정책객체 접속에 따른 인증과 등급, 질의(query) 조건, method condition 등의 개체를 정의하고 있으나, 본 연구에서는 제외하였다.

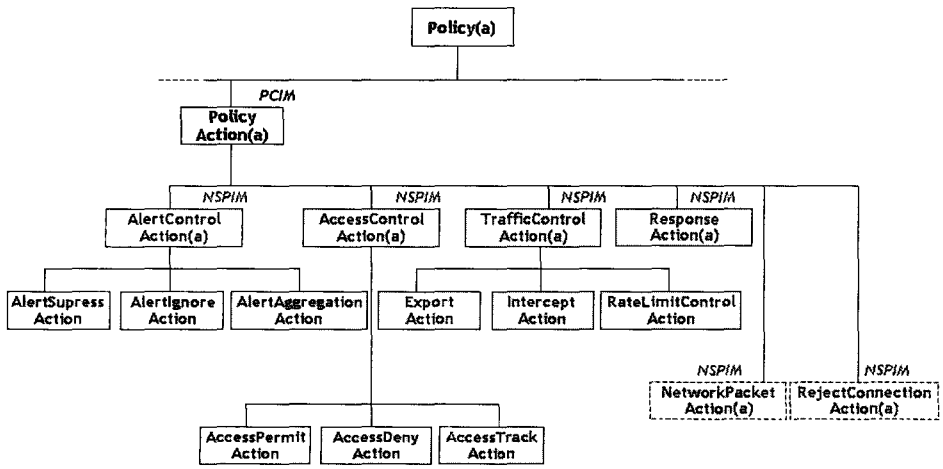
### 2.3.2 정보모델링 예제

네트워크 보안정책 클래스의 PolcyCondition 중에 트래픽 제어를 담당하는 TrafficControlCondition 객체를 정보모델링하는 간단한 예제를 다음과 같이 보였다.

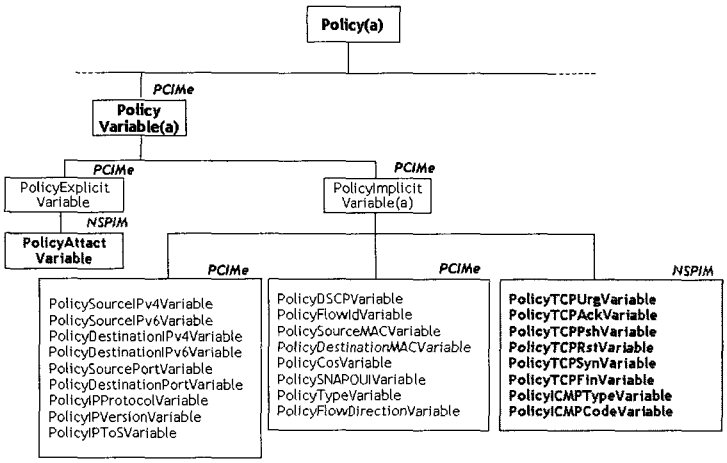
TrafficControlCondition은 트래픽 폭주를 판단하는 조건으로써, 발신지(source) IP, 목적지 IP, 발신지 포트, 목적지 포트, 프로토콜에 대한 비교를 각각 SimplePolicyCondition의 인스턴스(instance)로 생성하고, 이들을 묶어서 TrafficControlCondition으로 구성한다. 일정 시간 동안의 트래픽 용량에 대한 평균 비율, 정규 용량, 초과 용량과 특정 서비스의 요구 및 반복을 조건 수립에 가능한 속성을 갖는다.

1) TrafficControlCondition 클래스

| | |
|---|---|
| NAME | TrafficControlCondition |
| DERIVED FROM | CompoundPolicyCondition |
| ABSTRACT | False |
| PROPERTIES | AverageRate, NormalBucket, ExtendedBucket |




(그림 6) 네트워크 보안정책의 PolicyAction 정보모델




(그림 7) 네트워크 보안정책의 PolicyVariable 정보모델

(ServiceTurn), (IterationNumber)

2) Property AverageRate

| | |
|---|---|
| NAME | AverageRate |
| SYNTAX | uint16 |
| DEFAULT VALUE | 0 |

3) Property NormalBucket

| | |
|---|---|
| NAME | NormalBucket |
| SYNTAX | uint16 |
| DEFAULT VALUE | 0 |

4) Property ExtendedBucket

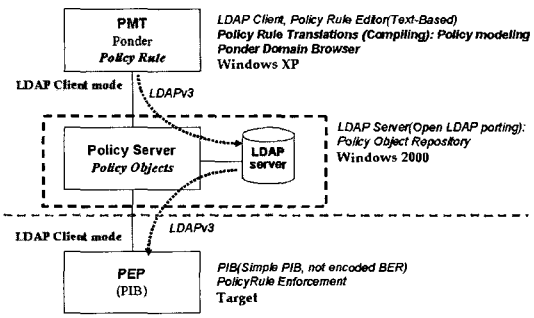
| | |
|---|---|
| NAME | ExtendedBucket |
| SYNTAX | uint16 |
| DEFAULT VALUE | 0 |

# 3. 보안정책 공유모델

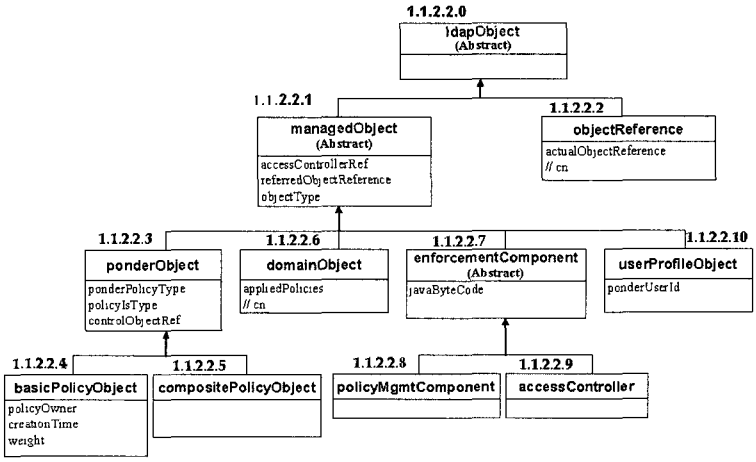
## 3.1 공유모델

DMTF CIM 모델링은 MOF(Microsoft Object Formatter)를 사용하여 보안정책을 모델링 하였다[15]. 그러나 MOF 방식은 클래스 정의를 일관적으로 정의함으로서 표준화 규격 작성이 유리하나 실제 개발자에게 클래스 간의 오퍼레이션 표현에 다소 불편한 점이 있는 바, 본 연구에서 보안정책 객체는 UML 도구(ROSE tool)를 사용하였으며, 클래스 다이어그램과 협력/시퀀스 다이어그램을 기반으로 설계하였다. CIM 정보모델링에 사용한 MOF 방식을 일부 보안정책 클래스 정의에 적용한 바, ManagedElement 객체 컴포넌트 수용과 객체 간의 상속성 유지와 정의된 클래스에 따른 syntax, 클래스 계위 및 instantiate 등의 편리성을 확인하였다. 그러나 네트워크 보안정책 객체를 텍스트 형식으로 표현을 IETF의 표준규격의 기술 방식에 의존하였다. 객체 속성과 오퍼레이션, 상호연관 등의 클래스 정의는 UML 도구로 설계하여 확인 하였다.

정의된 보안정책 객체를 실제 시스템에 적용 환경으로 Ponder toolkit을 활용하였다[12]. 본 연구에서는 정보공유 구조 모델을 (그림 8)와 같이 LDAP 서버와 LDAP 클라이언트 모델로 제시하여, 보안정책 모델에 따른 정책규칙




(그림 8) 보안정책 정보모델 검증을 위한 적용 환경




(그림 9) LDAP Schema 객체 모델

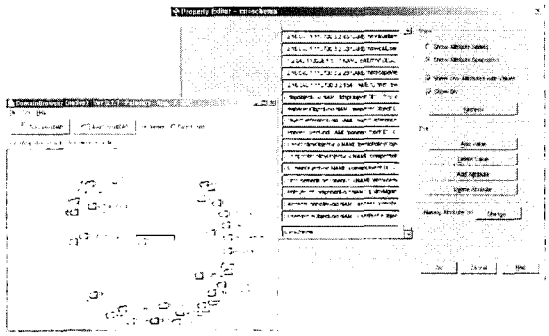
객체의 생성 및 LDAP 서버를 이용하여 정보의 공유 기능을 확인하였다. LDAP 서버는 iPlanet를 Windows 2000 서버에 포팅 하였다[11]. PMT 기능을 가지는 Ponder toolkit의 도메인 브라우져에서 LDAP 클라이언트 접속 기능을 적용하였으며, (그림 10)은 수행화면을 보였다.

## 3.2 LDAP 서버

LDAP 서버에 보안정책 객체를 저장하기 위해서는 LDAP schema를 설정해야한다. LDAP schema는 (그림 9)과 같이 ldapObject(1.1.2.2.0)를 top으로 managedObject와 objectReference로 구분하여 iPlanet 서버에 ldapObject 객체를 텍스트 형태로 일괄 작업으로 추가하였다.

## 3.3 정보공유 검증

Imperial 대학에서 개발한 Ponder toolkit은 정책 기반의 정책규칙을 JAVA와 XML로 생성하며, 생성된 객체를 관리하는 도구이다. 본 연구에서는 제안된 보안정책 모델에 따라 보안 정책규칙을 설정하여 Ponder 정책규칙 descriptor를 통해 JAVA 소스 코드을 생성한 후, 이를 컴파일하여 생성된 객체를 정책서버인 LDAP 서버에 저장한다. 저정된 객체는 Ponder의 도메인 브라우저에 접속하여 LDAP 서버에 저장된 객체 속성을 확인할 수 있으며, 객체 속성에 대한 수정이 가능하였다. 따라서 PMT와 PEP



(그림 10) Ponder 도메인 브라우저와 IPlannet 수행화면

에서는 LDAP 서버와 LDAP 프로토콜을 이용하여 보안에 관련된 정책규칙 객체를 접속하여 정보를 공유할 수 있다. 정책규칙은 Ponder toolkit에서 제공하는 정책기술 규격 언어(버전 2.3)를 사용하여 기술하였다[5].

본 연구에서는 iPlanet LDAP 서버에 보안정책 객체를 효과적으로 모니터링을 하기위해서 ponder toolkit의 도메인 브라우저와 별도로 Softerra의 LDAP 브라우저를 이용하여, 객체 간의 상황과 인터페이스를 확인하였다.

# 4. 결 론

본 논문은 인터넷 상에서 네트워크 관리정보를 보다 효율적인 관리를 위해 정책 기반의 정보보호 관리 시스템에 적용되는 보안정보 객체에 대한 기능 정립으로 DMTF

와 IETF에서 제안하는 객체 모델링 방식을 도입하여, 보안정책 객체를 모델링 하였다. 보안정책 객체는 PolicySet를 비롯하여 (표 1)에서 정의된 기능을 기반으로 (그림 5)와 같이 5개의 PolicyCondition, PolicyAction, PolicyVariable, PolicyValue 객체로 구분하였으며, 타켓 시스템의 ManageElement는 DMTF CIM 컴포넌트를 수용하였다.

보안 정책규칙의 다양한 표현을 위해서는 PCIM/E을 기반으로 PolicyVariable과 PolicyValue 객체는 개별 패킷의 모니터링을 위해 시간 및 로그 정보를 수용하여 IETF와 다르게 정의하였다. 또한 보안 시스템에서 요구하는 패킷을 객체화 하기위한 FilterEntryBase, Authentication, RejectConnectionAction, NetworkPacketAction 객체를 정의 하였다.

정보공유 모델을 LDAP을 활용하여 서버와 클라이언트 모델로 구성하였으며, 본 연구에서는 Ponder toolkit 환경에서 정책규칙을 컴파일하여 생성된 객체를 LDAP 서버에 저장하였으며, 이를 LDAP 브라우져로 객체를 확인하였다. 앞으로 PEP에서 LDAP를 통해 보안정책을 다운로딩하여 해당 디바이스에 따른 정책규칙 수행에 대한 연구와 구현이 필요하다. 또한 네트워크 정보보호 뿐 만 아니라 시스템, 운영체제, 보안정책 접속, 운영관리에 대한 구체적인 정보모델도 요구된다.

앞으로 연구사항은 다양한 NE에 보안정책 정보모델에 대한 적용과 정보보호를 위한 적극적인 보안정책 객체의 발굴이 요구되며, 액티브 네트워크에 적용을 위한 기본 모델을 정립하고 이를 수용하는 방향을 제시하고, 이를 위한 국내외 표준화 규격 연구가 요구된다.

## 참 고 문 헌


[1] Morris Sloman, et al. *"Using CIM to Realize Policy validation within the Ponder Framework"*, GMC-2003, July 2003.

[2] Emil Lupu, et al. *"Security and Management Policy Specification"*, IEEE Network, Vol 16, No 2, March 2002.

[3] B. Moore, et al., *"Policy Core Information Model-Version 1 Specification"*, RFC 3060, IETF, Feb 2001.

[4] B. Moore, et al., "PCIM-Extension", IETF, RFC 3460, Jan 2003.

[5] Nicodemos Damianou, et al., *"Ponder: A Language for Specifying Security and Management Policies for Distributed Systems"*, Version 2.3, Imperial College Report Document, Oct 2000.

[6] Andrea Westerinen and Winston Bumpus, *"The Continuing Evolution of Distributed Systems Management"*, IEICE Trans. INF & SYST, Vol. E86-D, No. 11, Nov 2003.

[7] DMTF Document, *"CIM Core Policy Model"*, Version 2.9, DMTF, Aug 2004.

[8] 김도수, 신영석, 김진오, "정책 기반의 보안 게이트를 위한 보안정책 정보모델링", 한국정보처리학회 추계학술대회, 2003.11.

[9] 손승원, "Active Security 기술 발전 방향", Sigcomm Review, 한국정보처리학회, Vol. 1, No. 1, 2000.12.

[10] 김현주, 장범환, 정태명, "Active 네트워크의 관리기술 현황과 전망", Sigcomm Review, 한국정보처리학회, Vol. 1, No. 1, 2000.12.

[11] The Parlay group, *"Policy Management SCF"*, ETSI ES 202 915-13 Ver 1.1.1, Jan 2004.

[12] Open LDAP Foundation, *"open LDAP 2.1 Administrator's Guide"*, Jan 2003.

[13] SUNTONE, *"IPlanet Directory Server Administration's Guide"*, Dec 2001.

[14] Ponder, *http://www-dse.doc.ic.ac.uk/Research/policies/ponder.shtml*, 2003.

[15] DMTF, *http://www.dmtf.org*, 2004.

[16] IETF, *http://www.ietf.org*, 2004.

[17] Cisco, *http://www.cisco.com/en/US/products/sw/secursw/ps2133/*, 2004.

[18] Orchestream, *http://www.orchestream.com*, 2003.

## ◐ 저 자 소 개 ◑


**손 선 경**

1999년 : 전남대학교 전산학과 이학사
2001년 : 전남대학교 전산통계학과 이학석사
2001년~현재 : 한국전자통신연구원(ETRI) 정보보호연구단
네트워크보안그룹 능동보안기술연구팀 연구원
관심분야 : 정보보안, 네트워크 정보모델링

**신 영 석**

1982년 : 전북대학교 전자공학과(공학사)
1984년 : 전북대학교 대학원 전자공학과(공학석사)
1993년 : 전북대학교 대학원 전자공학과(공학박사)
1984년~1998년 2월 : 한국전자통신연구원 선임연구원
1993년 3월~1994년 8월 : 일본 NTT 통신망연구소 객원연구원
1998년 3월~현재 : 호남대학교 정보통신공학과 부교수
관심분야 : 멀티미디어통신 프로토콜, 객체지향 모델링, 통신망관리