정보통신 인프라 정보보호 제어 프레임워크 연구

한국전자통신연구원 정보보호연구단 나중찬, 김진오, 손선경, 장종수

차 례

Ⅰ. 서 론

정보통신 인프라는 사람 및 기계간의 거리에 관계없이 데이터를 전달 및 처리하는 기계적, 전기적 및 전자적 활동이다. 종종, 정보통신 인프라를 단지 모뎀, 컴퓨터 및 단말기와 같은 통신을 제공하는 요소들의 종합으로 간주한다. 그러나 정보통신 인프라는 다수의 시스템들과 장치들이 연결된 데이터 통신 시스템으로 구성 요소들 사이에 상호 접속을 통하여 데이터 등을 전송할 수 있는 정보통신망을 말한다.

네트워크에 연결되어 있다는 것은 그렇지 않은 것에 비해 훨씬 더 보안이란 위협요소에 노출되어 있다는 것을 의미한다. 또한 이러한 네트워크는 컴퓨터 시스템간의 상호접속 및 정보 교환의 편리한 역할을 하지만, 시스템에 대한 불특정 다수의 접근이 가능하기 때문에 시스템 침입자에 의한 보안 사고의 위협을 내포하고 있다. 네트워크의 물리적인 광범위함, 네트워크 경로 및 사용자의 다양성 등은 네트워크 상에서 특유의 보안 문제를 일으키며, 네트워크 구성요소 중 일부에 문제가 발생하더라도 전체 네트워크에 영향을 끼친다. 또한 최근 심각한 피해를 입히고 있는 웜 바이러스 형태의 해킹 기법은 수분 내지 수십 분 내에 해당되는 지역이나 공공기관 기간망을 마비시킬 수 있는 피해를 줄 수 있다.

따라서 정보통신 인프라 환경에서는 네트워크 자체의 목적을 침해하는 것을 최소화하기 위해 네트워크에 연결됨으로써 발생 가능한 위협요소를 고려해야만 한다. 이에 따라 최근에는 네트워크의 중요한 기능이 제대로 수행되는지, 유해한 요소가 존재하는지, 정보가 정확한 지에 대해 보증하는 방법이 요구되어 정보통신 인프라 정보보호 제어 프레임워크(이하, 보안제어 프레임워크

라 함)에 관한 연구가 중요하게 되었다. 또한 사이버테러 대응을 위한 움직임에는 정보보호 차원의 법령 제정과 일반 인터넷 사용자들에 대한 교육, 침입의 조기 탐지 및 대응으로 연결되는 조기 경보체계의 개발, 각종 주요 시스템의 취약성 분석을 통한 보안성 강화 방안의 연구에 집중되고 있다고 할 수 있다.

본 논문에서는 정보통신 인프라의 정보보호를 효과적으로 보장하기 위해서 관리적 및 물리적인 측면 보다는 기술적인 측면의 보안제어 기술과 관련하여 외국의 연구동향과 국내의 연구개발 현황을 알아보고, 정보통신 인프라에서의 정보보호를 위한 보안제어 프레임워크를 기술한다.

Ⅱ. 관련 연구

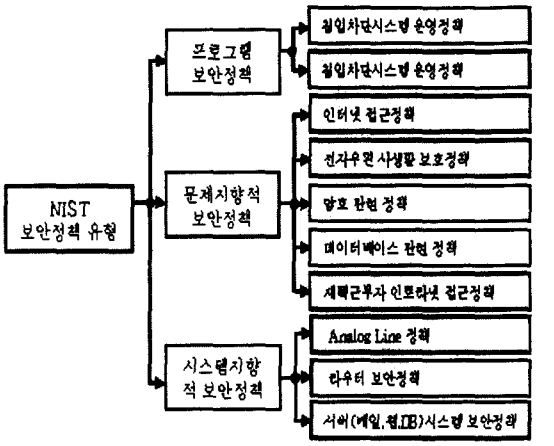
보안제어 프레임워크는 네트워크 관리자를 위해 보안정책의 구현을 단순화하고, 이를 기반으로 조직의 네트워크 전체를 일관된 정책에 따라 효율적인 네트워크 뷰를 제공해야 한다. 본 장에서는 정책 기반 관리와 관련된 연구를 살펴본다.

2.1 보안정책 분류

보안정책은 조직의 기술과 정보 자산에 접근하기 위해 사용자들이 지켜야 하는 규칙의 형식문이다. 이러한 보안정책의 주된 목적은 조직의 기술과 정보 자산을 보호하기 위한 필수적인 요구사항을 사용자와 운영자, 관리자에게 알려주는 것이고, 정책에 따라 컴퓨터 시스템과 네트워크를 취득하고 구성하고 감사하기 위한 기본 지침을 제공하는 것이다.

보안정책은 조직체 내에서 정보보호 임무를 관리하기 위한 수단이다. 그러나 모든 조직체에 적용할 수 있는 하나의 정형화된 정책이 존재하는 것은 아니다. 이러한 모든 보안정책의 유형을 분류하기 위해 많은 연구가 진행되어 왔다[1,2,3,4,5].

NIST(National Institute of Standards and Technology)는 보안 관련 프로그램을 효율적으로 관리 및 구성하기 위하여 설정하는 프로그램 정책, 각 기관별로 필요성이 제기되는 분야 혹은 사안에 대하여 적절한 행위를 규정하는 문제 지향적 보안정책, 개별적인 시스템 단위로 요구되는 보안항목을 정의하는 시스템 지향적 보안정책으로 분류하였다[1]. [그림 2-1]은 NIST에서 분류한 보안정책 유형을 보여준다.



〔그림 2-1〕 NIST 보안정책 분류

Smith & Newton은 ISO 15408 1999 정보기술 보안평가를 위한 공통 기준(CC, Common Criteria)에 기반을 두어 CC 보호 프로파일 개발자를 위해 <표 2-1>과 같이 보안정책을 분류하였다[2].

〈표 2-1〉 Smith/Newton의 보안정책 분류

기능 보안정책	보안 서비스 제공 분야
보증 보안정책	제품 및 개발 분야
관리 보안정책	절차, 계획, 교육 분야

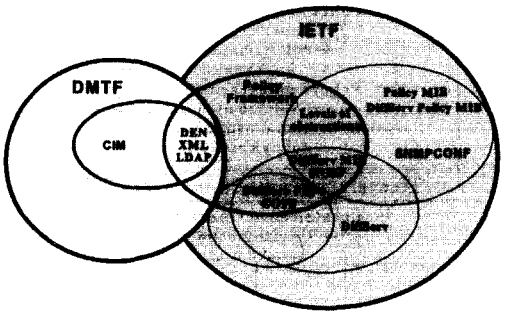
기능 차원의 보안정책은 제품의 기능성과 대조되는 것으로서 기밀성, 무결성, 이용성, 신뢰성, 책임성, 부인봉쇄, 공통의 시스템 접근성 등을 포함하는 보안의 기능적 측면을 고려한다. 보증 차원의 보안정책은 제품 행위의 완성도, 개발환경의 안전성, 제품을 생산하는데 있어 활용된 소프트웨어 개발 규율 등을 고려한다. 즉, 이러한 정책은 시스템 및 제품의 보증과 개발상의 보증을 포함한다. 관리 차원의 보안정책은 제품의 성공적인 활용 및 배치에 중심을 두고 있다. 훈련, 절차, 시스템 사용, 시스템 관리, 부수적인 사건에 대한 계획 등이 포함된다.

이외에도 SANS는 정보통신 인프라 환경에서 보안 위협이 발생할 수 있는 부류를 28가지로 분류하여 보안 요구사항을 기술하고 있다[3].

2.2 보안정책 모델

보안정책 모델은 보안정책을 표현하고 관리 및 공유가 가능한 스키마와 그 스키마를 구성하는 클래스 계층구조로 제공되기 위한 것이다.

IETF(the Internet Engineering Task Force)와 DMTF(Distributed Management Task Force)에서는 [그림 2-2]와 같이 공동 표준화 영역으로 상호협조 하에서 네트워크 관리를 위한 정보모델링을 수행하고 있다.



〔그림 2-2〕 IETF와 DMTF 표준화 그룹간의 관계

그러나 IETF와 DMTF 간의 표준화는 DMTF가 앞서가고 있으며, DMTF는 벤더 간의 컨소시엄으로 상용제품 개발을 목적으로 구현 가능 규격을 제시함에 따라 IETF보다는 능동적이며 신속하게 표준화 규격을 제시하고 있다.

2.2.1 DMTF 표준화

정보 모델은 그동안 일반적으로 많이 이용되었던 SNMP(Simple Network Management Protocol) MIB(Managed Information Base)을 이용하여 ASN.1(Abstract Syntax Notation One), GDMO(Guideline for the Definition of Managed Objects), GRM(General Relationship Model) 방식을 사용하였다. 그러나 객체지향 설계기술과 분산시스템 기술의 발전으로 객체기반의 정보모델이 OMG(Object Management Group), TINA (Telecommunication Information Network Architecture), ITU-T((International Telecommunications Union - Telecommunication Standardization Sector), IETF, DMTF 등의 표준화 연구기관에서 정착되었다.

최근 DMTF는 통신망 장치와 호스트의 하드웨어 자원, 시스템 자원, 응용서비스 자원 관리를 위해 계층별 기능과 시스템 차원의 관리객체 모델링에 관한 표준을 정립하고 있으며, 정책 기반의 네트워크 관리에 관련된 표준은 <표 2-2>와 같이 CIM(Common Information Model) Policy Ver.2.9를 제시하였다[6].

〈표 2-2〉 CIM Policy Specification V2.9

Core	CIM_Core29
Application	CIM_Application29
	CIM_Application29_AppServer UML/PDF
	CIM_Database29
Device	CIM_Device29
Network	CIM_Event29
	CIM_Interop29

	CIM_IPSecPolicy29
	CIM_Metrics29
	CIM_Network29
	CIM_Physical29
	CIM_Policy29
	CIM_Support29
System	CIM_System29
User	CIM_User29

DMTF CIM은 데스크톱 개인용 컴퓨터를 관리하기 위한 표준을 제안한 DMI(Desktop Management Interface)[7], 디렉토리 안에 네트워크 요소 및 서비스를 표시하기 위한 표준 정보모델을 제안한 DEN(Directory Enable Network)[8], 인터넷상에서 웹을 기반으로 하는 네트워크 관리를 위한 정보모델과 이를 전달하는 메시지 전달 방식을 제안한 WBEM(Web Based Enterprise Management)[9] 등을 기반으로 표준을 정립하고 있다. 특히 CIM은 XML(eXtensible Markup Language) 기반의 정보모델로 손쉽게 접속이 가능하도록 연구를 진행하고 있다[10].

CIM_Policy29는 정책객체를 사용하는 사용자 또는 운영자의 접속에 대한 인증과 접속범위 설정을 위한 클래스, 정책 저장소로의 질의 조건 클래스, 외부 저장소에서 접속하는 방법을 설정하는 클래스가 정의되어 보다 충실한 보안정책 모델을 제공하였다.

2.2.2 IETF 표준화

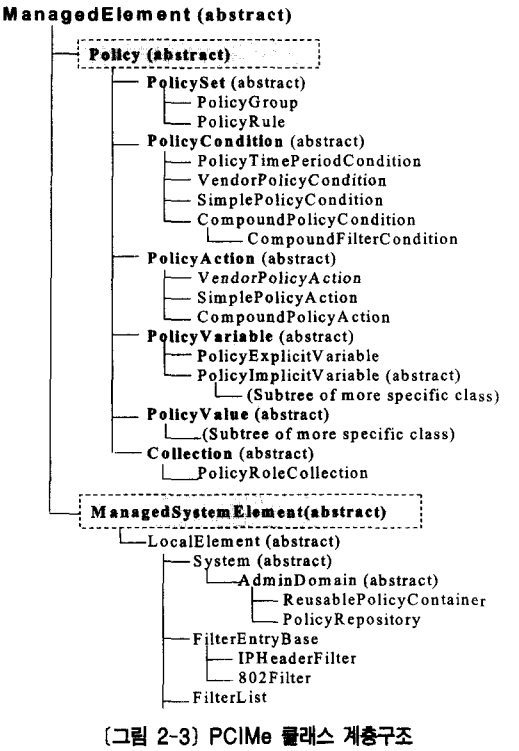
IETF에서는 <표 2-3>와 같이 시스템 제조자에 독립적이고 상호운영이 가능한 정책모델인 PCIM(Policy Core Information Model)[11]에 대해 RFC3060으로 기본 규격을 완성하였다. PCIM은 DMTF의 CIM Ver.2.5를 기반으로 작성되었으며, 최근 PCIM에서 정의한 정책모델이 미흡하여, PCIM에서 부족한 부분을 추가한 PCIMe(PCIM Extensions)[12]로 재작성하여 RFC3460으로 규격을 제시하였다.

〈표 2-3〉 IETF 정책 핵심 모델 관련 규격

3060	Policy Core Information Model	2001.2
3460	Policy Core Information Model (PCIM) Extensions	2003.1

IETF PCIM은 DMTF의 CIM의 확장으로써 IETF의 정책 프레임워크 워킹 그룹과 DMTF에서 함께 개발하였고, 정책 정보를 표현하기 위한 객체 지향 정보 모델을 기술하고 있다. 이 모델은 정책의 제어와 정책 정보를 표현하는 구조 클래스(Structural Class)와 구조 클래스의 상호 연관성을 나타내는 연관 클래스(Association Class)를 정의하고 있다.

다음 [그림 2-3]은 정책 핵심 정보 모델을 구성하고 있는 구조 클래스들의 상속 계층 구조이다.



〔그림 2-3〕 PCIMe 클래스 계층구조

PCIMe의 주요 클래스 역할은 다음과 같다.

- o *PolicyGroup* : 연관된 *PolicyRule*들의 집합이나, 연관된 *PolicyGroup*들의 집합을 위한 컨테이너 클래스
- o *PolicyRule* : 정책 규칙과 연관된 것으로 조건을 만족하면 동작을 취한다와 같은 의미를 표현하기 위한 클래스
- o *PolicyCondition* : 정책 규칙에서 정책 조건을 나타내는 클래스
- o *PolicyAction* : 정책 규칙에서 조건을 만족하면 수행되는 동작을 표현하는 클래스
- o *PolicyTimePeriodCondition* : 미리 정해진 스케줄에 따라 정책규칙을 활성화 또는 비활성화시킬 수 있는 기능을 제공하는 클래스
- o *PolicyRepository* : 정책과 관련된 정보를 위해 관리적인 측면에서 정의된 컨테이너 클래스
- o *VendorPolicyCondition*, *VendorPolicyAction* : 특정 제조사를 위한 클래스

PCIMe에서는 *ipHeadersFilering* 클래스가 신규로 추가되었으며, *policyRulePriorities*와 같이 기존에 있던 클래스가 삭제되었다.

정책은 정책 규칙(*PolicyRule*)들의 집합을 사용하여 적용되고, 각 정책 규칙(*PolicyRule*)은 조건(*PolicyCondition*)의 집합과 동작(*PolicyAction*)의 집합으로 구성된다. 여러 정책 규칙은 정책 그룹(*PolicyGroup*)과 결합되고, 이러한 그룹은 정책들의 계층을 표현하기 위해 또 다른 그룹을 구성하게 된다.

이전에 살펴본바와 같이, IETF에서의 정책 모델은 정책모델의 핵심을 정의하였고, 특정 시스템에 적용할 때는 정책모델의 핵심을 기반으로 확장하여 사용하도록 하고 있다. 최근 IETF는 PCIMe 기반의 정책모델 핵심을 특정 시스템에 적용을 위해 세부정책모델로 확대하고 있다. <표 2-4>는 특정 시스템에 적용을 위해 IPSec 구성관리 서비스와 QoS(Quality of Service)를 선정하여, IPSec 구성관리 정책모델(IPSec CPIM, RFC 3585)[13]과 QoS 구성관리 정책모델(QPIM, RFC 3644)[14] 표준 규격을 제정하였다.

〈표 2-4〉 IETF 세부정책 모델 관련 규격

3585	IPsec Configuration Policy Information Model	2003.8
3644	Policy Quality of Service (QoS) Information Model	2003.11
3670	Information Model for Describing Network Device QoS Datapath Mechanisms	2004.1

IETF IPSec CPIM은 트래픽을 주고받는 주체, 각 주체들이 주고받는 데이터 유형, 트래픽이 보호되는 시점 등의 구성관리 측면에서 PCIMe를 기반의 정책모델 표준규격을 제정하였다.

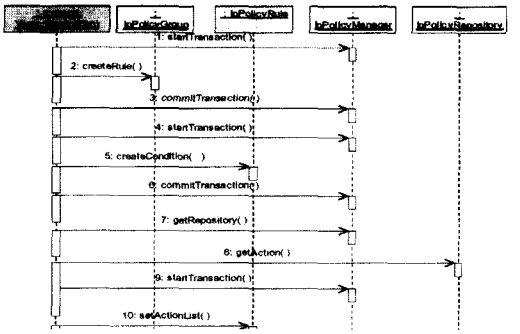
IETF QPIM은 PCIMe를 기반으로 정책기반의 QoS를 지원하게 하며, 비즈니스 차원의 정책을 정책 적용 디바이스로 정책을 제공하는 절차로 이루어진다. 네트워크 토폴로지와 운영방식, 서비스 제공범위, 제어절차 및 방법론에 따라 매우 다양하여 일관된 QoS 정책모델을 제시하기가 어렵다. 특히 디바이스 수준의 QoS 정책모델은 해당 디바이스에 따라 다르므로 RFC 3670과 같이 네트워크 토폴로지, QoS 범위, 제어방법을 설정하여 단계적으로 표준 규격을 제정하고 있다[15].

향후 PCIMe를 기반으로 정책기반의 특정 네트워크 보안 서비스를 위해서는 IPSec CPIM과 QPIM 정책모델의 활동에 제기되었던 이슈 및 활동을 파악해야 할 것이다.

2.2.3 Palay 표준화

Parlay 그룹은 향후 개방형 정보통신 환경에서 시스템 및 서비스 관리 기술을 위한 API(Application Programming Interface)와 정책 기반의 응용 서

비스 제공을 위한 정책 모델을 제시하고 있다[16]. 특히 통신사업자 중심으로 결성된 표준화 기관인 Parlay 그룹은 유럽 공동체의 표준화 기관인 ETSI(European Telecommunications Standards Institute)와 공동으로 정책정보 모델을 구현 가능한 UML(Unified Modeling Language) 기반으로 표준규격으로 선정하여 연구를 진행하고 있다. 또한 응용 서비스 운영 시스템과 통신사업자 간의 통신망 장비를 제어함에 따라 신호절차 및 정책 객체 간의 오퍼레이션에 세부적인 규격을 제시하고 있다.



〔그림 2-3〕 Parlay Group의 UML 기반의 정책모델 사례

DMTF와 IETF에서의 정책모델과는 달리, Parlay 그룹의 정책 모델은 응용 서비스를 제공하는 차원에서 QoS, 보안, 통신망 관리 서비스를 비롯한 응용 서비스를 직접 제공하는 차원으로 보다 손쉽게 접근하는데 의미가 있다고 할 수 있다.

2.3 정책기반 네트워크관리

현재의 네트워크는 기존 네트워크에서 새로운 고객과 이들이 선택한 서비스에 있어서의 변화를 수용하기 위해 과거 어느 때보다 더욱 규모와 복잡성 측면에서 급속도로 변모하고 있다. 이러한 네트워크의 환경 변화는 신뢰성, 보안성, 성능에 대한 요구사항을 추가시킨다. 또한 문제가 발생할 경우에는 장애관리는 더욱 어려워짐에 따라 관리의 복잡성을 추가시킨다. 특히 변화가 빈번한 환경에서의 네트워크 설치, 구성 및 관리할 능력이 되는 고도의 숙련된 기술자를 더욱더 많이 필요로 할 것이다. 따라서 시스템 구축 및 운영을 위해서는 관리되는 장비와 관리 응용으로 지능이 담긴 정책을 배포함으로써 변화가 빈번한 복잡한 네트워크를 보다 쉽게 효율적으로 관리될 수 있게 해야 한다. 자동화된 정책기반 네트워크 관리(PBNM, Policy-based Network Management)는 적은 수의 숙련된 기술자로 하여금 보다 폭넓은 장비에서 훨씬 복잡한 서비스를 배치할 수 있게 한다.

서비스 사업자는 안정적인 네트워크 제공과 효율적인 유지 관리하는 것은 하나의 필수적인 전제조건이다. 그러나 표준 없이는 효율적인 네트워크 운영 목표를 위한 자동화된 정책기반 네트워크 관리는 제공할 수 없다. 따라서 오래전부터 IETF에서는 장비 제조사에 의존되지 않고, 체계적이고 통일된 관리가 가능한 정책 기반의 네트워크 관리 프레임워크를 제공하기 위해서 <표 2-5>과 같은 표준 워킹그룹을 통해 표준화 작업을 진행하고 있다.

〈표 2-5〉 IETF 정책기반 네트워크 관리 프레임워크 관련 워킹 그룹

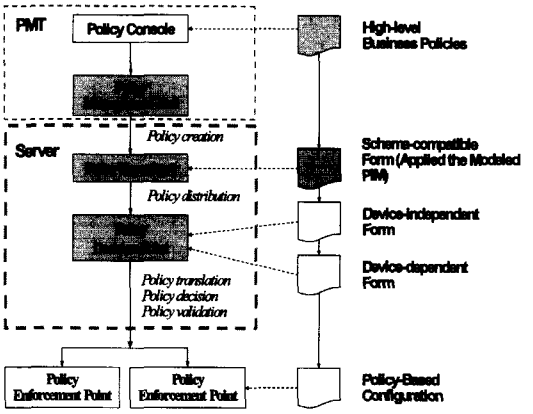
policy	- 정책서버 구조 - 정보모델 - PFDL 정의	정책기반 프레임워크 표준화
rap	- COPS - COPS-PR	정책전달프로토콜 표준화
diffserv	- 서비스 품질 차등 서비스 PIB	서비스 품질 차등 서비스 표준화
ipsp	- IP 보안정책 시스템 - IP 보안정책 모델 - IP 보안명세 언어	IP 보안 서비스 프레임워크 표준화
snmpconf	- Policy MIB 정의	기존 SNMP에의 적용 방안

Policy(Policy Framework) 워킹그룹과 RAP(Resource Allocation Protocol) 워킹그룹에서는 주로 정책 기

반의 프레임워크에 대한 표준화를 추진하고 있으며, 나머지 워킹그룹에서는 특정 시스템 적용을 위한 세부프레임워크로 확장하는 작업을 추진하고 있다.

2.3.1 Policy 워킹그룹

Policy 워킹그룹에서는 PBNM 프레임워크의 표준화에 중점을 두고 표준화 작업을 진행하고 있으며, 특히 네트워크의 QoS 제어를 위한 정책을 강하게 의식하고 있다. [그림 2-4]는 Policy 워킹그룹에서 제시한 정책기반 네트워크 관리 프레임워크를 나타낸 것이다.



〔그림 2-4〕 정책기반 네트워크 관리 프레임워크

정책 도메인 내의 각 정책수행기(이하 PEP, Policy Enforcement Point))는 자신의 *Role*과 *Capability* 정보를 정책결정기(이하 PDP, Policy Decision Point)에 전달한다. PDP는 이 정보를 이용하여 해당 PEP에 적용해야 하는 정책들을 결정한 후, 정책전달 프로토콜을 이용하여 PEP에 전송한다. PDP와 PEP간의 통신은 COPS(Common Open Policy Service) 프로토콜을, PDP와 정책 저장소 간의 통신은 LDAP(Lightweight Directory Access Protocol)을 이용하도록 권고하고 있다.

정책을 운영하는 시스템에서의 디바이스 차원의 정책인 SPPI(Structure of Policy Provisioning Information)는 PIB(Policy Information Base)를 작성하는데 이용되는 SMI(Structure and Identification of Management Information for TCP/IP-based Internet)를 RFC3159로 확정되었다[17]. 또한 효율적인 정책정보의 공유 및 저장을 위해 LDAP 스키마를 적용한 정책모델을 RFC3703으로 규격을 제정하였다[18].

최근 우선순위에 의한 정책 선택, 정책 유효시간 관리 등에 대해 이슈로 제안되고 있으며, 또한 DMTF와 함께 웹을 기반 방식을 위해 정책을 XML 형태로 저장하는 표준을 추진 중에 있다.

2.3.2 RAP 워킹그룹

RAP 워킹그룹은 정책전달 프로토콜 표준화에 초점을 맞추어 진행하고 있다. 정책전달 프로토콜은 PDP와 PEP 간의 정책 교환 및 설정 방식에 따라 구분되는 COPS[19]와 COPS-PR(COPS for Provisioning)[20] 모델을 표준 규격으로 제정하였다. COPS는 특정 이벤트에 대한 PEP 행위를 결정할 때, PDP에 통보하고 정책결정을 PDP에게 위임하는 수동적인 방식이다. 반면에 COPS-PR은 정책의 전략적 변경에 대해 결정된 정책을 사전에 PEP에 반영하는 능동적인 방식이다.

RAP 워킹그룹은 주로 QoS 정책에 대해 초점을 맞추어 표준화 작업을 진행하고 있으며, 지속적으로 RSVP(Resource Reservation Setup Protocol)에 적용을 위한 확장하는데 필요한 COPS 객체를 변경할 예정이다.

2.3.3 기타 워킹그룹

diffserv(Differentiated Services)와 IPSec 워킹그룹에서 분리된 IPSP(IP Security Policy) 워킹그룹에서는 서비스 품질 차등 서비스와 IPSec 서비스에 정책 기반 시스템을 적용하기 위한 시스템 고유의 정책과 정책 스키마를 정의하는 작업을 진행하고 있다. 또한

snmpconf(Configuration Management with SNMP) 워킹그룹에서는 기존의 SNMP에서 이용되고 있는 MIB 형태의 Policy MIB 정의가 활발히 진행하고 있다.

Ⅲ. 보안제어 프레임워크

최근 보안제어 프레임워크는 필요한 중앙 집중식 정책 관리와 자동 제어 시스템을 제공함으로써 보안관리를 용이하게 하는 필요성이 대두되고 있다. 이에 따라 본 장에서는 보안제어 프레임워크 개념을 본 후, 보안제어 프레임워크를 구축 시 고려사항을 분석한다.

3.1 보안제어 프레임워크 개념

넓은 의미에서의 보안제어 프레임워크는 정보보호 목표 달성 측면에서만 보지 않고, 조직 전체의 경영전략 및 정책과 연계하여 이의 달성을 위해 관리적, 기술적, 물리적 정보보호 통제수단을 통합한다는 의미로 사용한다. 즉, 보안제어 프레임워크는 시스템 또는 네트워크 등 특정 정보기술을 보호하는 것뿐만이 아니라 응용시스템, 데이터, 인적자원 등 정보통신 인프라 자원 전반에 걸쳐 반영되어야 하며 또한 조직의 업무와 밀접한 관련이 있기 때문에 조직의 임무, 전략, 정책과의 연계성을 고려해야 한다.

- o 관리적 보안제어 측면 :
  관리적 보안제어 측면에서는 정보보호 정책, 표준, 지침 등 관련 문서의 존재 유무와 내용의 충실성 수준, 정보보호 관련 전담 인력/조직(정보보호 전담조직, 정보보호 운영 및 감사 등)의 규모, 역할 및 책임, 정보보호 교육 및 훈련 프로그램의 존재 유무 및 수준 등을 구축한다.
- o 기술적 보안제어 측면 :
  기술적 보안제어 측면에서는 정보통신 인프라 정보보호 구성요소 측면에서 현재 구축되었거나 향후 구축 예정인 정보보호 기능 또는 시스템을 식별하고, 기 구축된 정보보호 시스템간의 연동 및 상관관계를 정립한다.
- o 물리적 보안제어 측면 :
  물리적 보안제어 측면에서는 정보통신 인프라 시설물의 위치와 주요 설비의 출입통제 등 물리적 보호를 위한 장비를 식별하고 외부로부터의 물리적 침투에 대한 통제들을 파악한다. 또한 화재, 수재 등 자연재해 대응, 항온항습, 먼지 등 환경 대응을 위한 통제를 식별한다.

보안제어 프레임워크는 경제적인 범위에서 위험 또는 위협을 최소화할 수 있도록 정보통신 인프라 환경의 무결성, 가용성, 비밀성 등을 고려한 적절한 수준의 보안제어 정책을 수립하는데 목적이 있다. 따라서 효과적인 보안제어 정책 수립을 위해서는 정보통신 인프라 자산의 가치와 손실을 측정하여 적절한 수준의 보안제어 정책을 마련해야 한다. 또한 조직의 정보보호를 효과적으로 보장하기 위해서는 다양한 기술적인 보안제어 정책뿐만 아니라 이들을 계획하고, 설계하고, 관리하기 위한 정책 및 절차 등이 확립되어야 한다.

강력한 보안제어 체계를 구축하는 데는 많은 비용을 요구하며, 따라서 비용과 자원의 현명한 관리가 중요하다는 점이다. 가장 최적의 보안제어 프레임워크를 정립해야 한다는 확실한 기준을 제시해야 하지만, 각 조직마다 갖고 있는 도전과 힘은 같을 수가 없다. 또한 새롭게 재정 또는 개정되는 보안제어 정책은 기존의 상위 정책이나 규칙, 법령 등과 부합되어야 한다.

3.2 보안제어 프레임워크 고려사항

정보통신 인프라에 대한 사이버테러로부터 인프라를 효율적으로 보호하기 위해 보안제어 프레임워크는 시급히 연구 개발하여야 할 매우 중요한 문제이다.

3.2.1 보안제어 정책

보안제어 정책은 정보통신 인프라 상에서 자원에 접근하고자 하는 요구에 대하여 어떤 것을 허가해 주고 어떤 것을 거부할 것인지를 정의한 것으로, 그 성격상 보안제어 기술의 개발보다 선행되어야 할 핵심 과제이다.

보안제어 정책을 운영하는 시스템은 스위치, 라우터, 방화벽, 침입탐지시스템 등의 다양한 시스템으로 구성된다. 이들 시스템은 정보통신 인프라 상의 통신 및 시스템들을 안전하게 보호하기 위하여 보안 위협 요인들을 분석하고 제공되어야 하는 보안제어 서비스들을 정의하여 이를 위한 메커니즘을 개발하는 것이 대부분이었다. 또한 보안제어 정책을 분류함에 있어 시스템 중심의 보안제어 정책(system-centric security control policy)을 분류하여 보안제어 서비스를 제공하였다. 그러나 이러한 연구는 단편적인 기술적 측면의 연구에 불과하고 포괄적인 보안제어 프레임워크를 제공하지 못하고 있는 실정이다. 즉, 수많은 개별적인 시스템을 설치 및 제어할 경우, 제조사와 사용자는 모두 관리 부담의 증가와 보고 통합의 필요성 및 이들 시스템을 한 개의 응집력 있는 단일체로 결합하기 위한 요구사항을 깨닫게 된다.

따라서 최근 정보통신 인프라 침해에 대한 보안제어 정책을 수립함에 있어 기본적으로 아래의 사항을 고려해야 한다.

- o 공통된 보안제어 정책 정의 :
  보안제어 정책을 정의함에 있어서의 특징 중의 하나는 제어대상인 시스템에 부합되는 정책을 사용하기보다는 다른 도메인 간 또는 서브 도메인 내에서 공통된 정책 설정 및 관리, 공유, 재사용성을 제공해야 한다. 결국 전체 보안제어 도메인을 하나의 보안제어 도메인으로 본다면 이 하나의 보안제어 도메인에서 구현된 보안제어 정책은 서로 호환이 가능하며, 체계적인 정보통신 인프라의 보호가 가능하게 된다.
- o 우선순위에 기반을 둔 보안제어 정책 수립 :
  보안제어 정책의 내용에는 주기적인 위험 분석 결과에 따라 제시된 정보보호 우선순위에 대한 결정을 반영하여야 한다. 우선순위가 높은 보안제어 정책을 우선적으로 수립함으로써 네트워크 침해에 대해 경제적인 범위에서 피해를 최소화할 수 있게 된다.
- o 차별적용에 기반을 둔 보안제어 정책 분류 :
  보안관리자에 의해 수립되어 영구히 적용되는 정적 보안제어 정책과 동적인 보안상황을 반영하기 위하여 순간적으로 자동으로 적용되고 보안상황이 종료되면 함께 종료되는 임시방편적으로 수립되는 동적 보안제어 정책을 분류하여 적용함으로서 인프라 침해 피해에 대한 국지화가 가능하다.

3.2.2 보안제어 정책 모델

보안제어 정책 모델은 응용개발자, 통신망 보안관리자, 보안제어 정책 관리자에 의해 확장 가능한 방식으로 보안제어 정책을 표현하고 관리 및 공유할 필요성이 생김에 따라 이를 만족시킬 스키마를 제공하기 위한 것이다. 이를 위해서는 다음과 같은 사항을 고려해야 한다.

- o 정책 적용이 가능한 시스템의 기능 정립 :
  보안제어 기능을 세부적으로 분류하여 그룹화함으로서 정책 조건과 그에 따른 동작으로 구분하여 적용 대상 시스템에 적합한 보안제어 정책을 설정하고, 적용 대상 시스템에서 보안제어 정책이 올바르게 수행하도록 정책 모델링이 이루어진다.
- o 표준화된 보안제어 정책 모델 정립 :
  표준화된 정책 모델링은 정보통신 인프라 상에서 다양한 보안제어 대상 시스템들 간에 정책 정보를 공유하기가 손쉬워지며, 보안제어 정책에 의해 정보통신 인프라를 구성하는 다양한 시스템들을 일관성 있게 관리함으로서 통신망

운영자에 효율적인 보안제어 기술을 제공한다.

3.2.3 정책기반 네트워크 보안제어

정책기반 네트워크 보안제어는, 지금까지는 네트워크 운용관리와 별도로 취급되어 왔던 네트워크보안관리 영역을 PBNM 프레임워크 안에 통합시킴으로써 네트워크 자원에 대한 운용 및 보안 관리를 공통된 정책에 따라 일관적으로 제어할 수 있는 기능을 제공한다. 따라서 정책기반 네트워크보안관리는 네트워크 보안관리자가 원하는 보안정책에 따라 망의 보안기능이 자동적으로 운용되는 네트워크, 즉 보안정책에 의해 보안동작이 규정되는 네트워크 보안장비로 구성되고 관리되는 네트워크로 정의할 수 있다.

정책기반 네트워크 보안제어를 실현하기 위해 다음과 사항을 고려해야 한다.

- o 계층적 정책기반 네트워크 보안제어
  계층적 정책기반 네트워크 보안제어는 전체 보안제어 정책 공간을 효율적인 사용이 가능하고, 같은 도메인 내 보안제어 정책 협상을 하지 않아도 된다. 따라서 계층적 구조는 엔터프라이즈 네트워크, 더 나아가 글로벌 네트워크 환경에서 적합성과 확장성 있는 제어 프레임워크를 제공할 것이다.
- o 표준화된 정책 교환 프로토콜 활용
  보안제어 정책은 각 정보보호 시스템 단위로 필요한 보안제어 서비스에 부합되는 정책 기술을 채택하여 사용할 수 있으나, 보안제어 정책을 운영하는 시스템들의 상호호환성을 위해 보안제어 시스템의 구현과 객체들 사이의 정책 교환 및 설정을 위한 통신은 표준화된 프로토콜을 사용하도록 한다.
- o 정책적용 대행서버를 통한 기존 장비 연동
  네트워크를 구성하는 장비가 정책 적용 기능을 제공하지 못하고 있기 때문에 실제 망으로의 적용은 앞으로의 과제로 남아있다고 할 수 있다. 현재로서는 SNMP, CLI(Comnand Line Interface) 등과 같은 기존의 프로토콜을 이용하고 정책적용 대행 서버를 활용하는 단계적 접근 방안이 가장 유효하다.

Ⅳ. 사례연구 : X-Guard

X-Guard(eXtensible-Guard)는 기본적으로 IETF Policy 워킹그룹에서 제시하는 정책기반 네트워크 관리 프레임워크를 따르며, 네트워크 안전성을 위한 정책기반 보안제어 서비스를 제공한다.

4.1 보안제어 정책 분류

정보통신 인프라 환경에서 보안제어 정책을 운영하는 시스템의 주요 보안제어 서비스를 그룹화하면 <표 4-1>과 같이 보안제어 정책을 운영하는 시스템 관리, 트래픽 제어, 접근제어, 라우팅 제어, 경보 제어 등 5개의 영역의 서비스 그룹으로 분류한다.

〈표 4-1〉 보안제어 정책 분류

시스템 관리 정책	보안제어 대상 시스템 구성관리 등을 규정하는 정책
패킷필터링 정책	방화벽 또는 라우터에서 유입패킷의 차단여부를 규정하는 정책
트래픽제어 정책	라우터 또는 트래픽제어 장비에서 과다 트래픽의 제어를 규정하는 정책
경로제어 정책	유해 트래픽을 특정 포트로 라우팅을 위한 규칙을 규정하는 정책
경보제어 정책	보안 장비에서 전송하는 경보 전달을 제어하는 정책

4.2 보안제어 정책 모델

<표 4-2>은 보안 시스템의 주요 기능에 따라 정책조건과 그에 따른 action을 제공하기 위한 condition factor와 처리 형태(action)를 제시하였다.

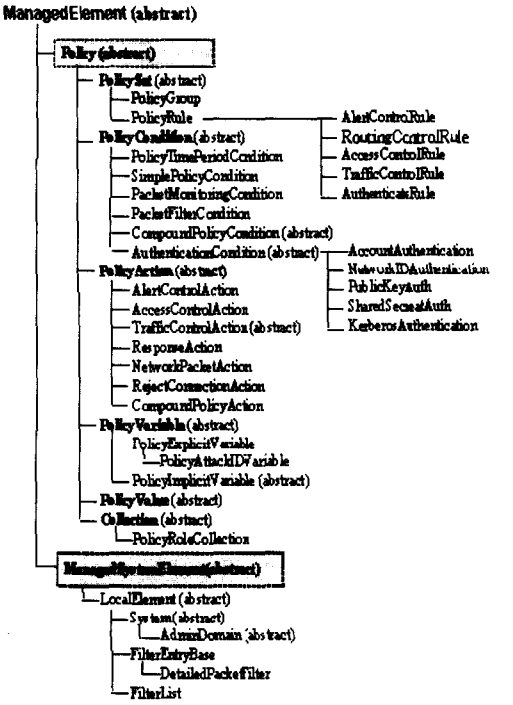
〈표 4-2〉 보안제어 정책 적용 매개변수

트래픽 제어정책	Source/Destination IP, Source/Destination Port, Protocol, Average Rate,	Export RateLimit
경로제어 정책	Destination IP	Drop
패킷 필터링 정책	Source/Destination IP, Source/Destination Port Protocol, TCP 6 Flags, ICMP Type, ICMP Code, MAC Address	Permit Deny Track
경보제어 정책	Source/Destination IP Source/Destination Port Protocol, Attack ID, Time Interval	Suppress Aggregate Ignore

예를 들어, 트래픽 제어 정책의 경우, 각각의 파라미터(Source IP, Destination IP, Source Port, Destination Port, Protocol, Average Rate 등)로 구성된 조건에 따라 트래픽을 export 하거나 제한된 대역폭으로 제어(rate limited control)하도록 하며, 다른 기능들도 해당 조건에 따라 처리하도록 보안기능을 정립하였다.

X-Guard 정책 클래스 계층 구조는 [그림 4-1]과 같다.

X-Guard에서 정의하는 정책 모델링은 PICMe를 기본으로 하며, policyRule 클래스는 alertControlRule, attackSignatureRule, accessControlRule, trafficControlRule, authenticateRule 클래스로 구성되며, policyCondition은 PCIMe에 부가적으로 packetMonitoringCondition, packetFilterCondition, authenticationCondition 클래스를 추가하였다. authenticationCondition 클래스는 5개의 authentication 관련 클래스를 세분화하여 모델링하였다. policyAction 클래스는 alertControlAction, trafficControlAction, responseAction, networkPacketAction, rejectConnectionAction 클래스로 구성하였다. policyVariable과 policyValue 클래스는 PCIMe에서 IPv4와 IPv6용 variable을 정의한 바,



〔그림 4-1〕 X-Guard 정책 클래스 구조

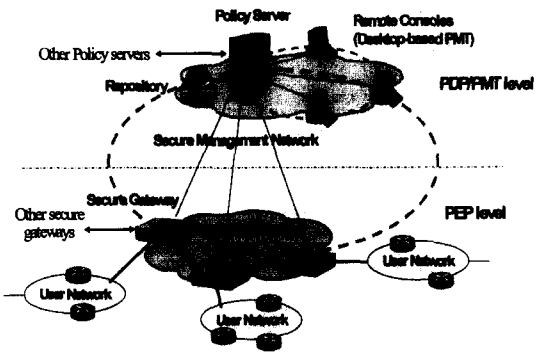
IPv4에 적용하는 현재의 보안 시스템에 따른 variable과 value로 모델링 하였다. policyExplicitVariable에서는 policyAttackIDVariable 클래스를 정의하였다.

4.3 정책기반 네트워크 보안제어

보안정책을 적용하는 시스템은 [그림 4-2]에 나타나 있듯이 PEP 기능의 보안장비와 정책서버(PMT와 PDP)를 대상으로 한다.

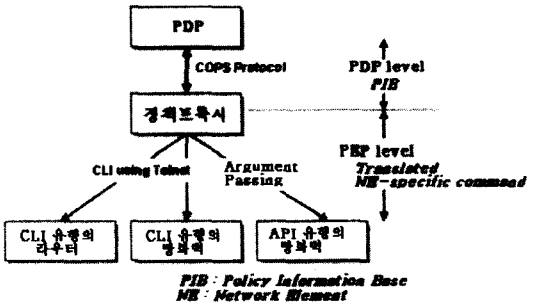
정책서버는 PMT와 PDP, 정책 저장소를 네트워크 운영 형태에 따라 구성될 수 있다. IETF COPS 표준을 준수하는 프로토콜은 보안장비와 정책서버 간의 정책 교환 및 설정을 수행하는 활용된다.

현재 네트워크 상에서 동작하는 대부분의 보안 장비 및 네트워크 장비는 X-Guard에서 기술하고 있는 보안제어 정책을 이해하지 못한다. 즉,



〔그림 4-2〕 X-Guard 보안제어 구조

기존의 사용 장비는 각각의 관리 콘솔에서 전달한 장비 고유의 명령에 기반을 두어 동작하며, 각 설정 방법도 장비마다 다양하다. 따라서 하나의 통일된 정책에 기반을 두어 이들 장비를 일원적으로 관리하기 위해서는 [그림 4-3]과 같이 중앙의 공통된 포맷의 보안제어 정책을 각 장비에 맞게 번역하고 적용해주는 정책적용 대행 서버(정책프록시)가 필요하다.



〔그림 4-3〕 X-Guard 정책프록시

X-Guard 정책프록시와 PDP 간의 인터페이스는 COPS 프로토콜을 이용하여 PIB 기반의 정책을 전달한다. 또한 X-Guard 정책프록시와 보안제어 대상 시스템(방화벽, 라우터) 간의 인터페이스는 CLI와 API를 통해 보안제어 정책을 적용하는 방화벽 보안장비와 CLI를 통해 구성관리를 수행하는 기존 라우터를 대상으로 하였다. 즉, X-Guard 정책프록시는 X-Guard 보안제어 정책을 각 장비에 해당되는 CLI로 번역한 후, Telnet 프로토콜을 이용하여 라우터 또는 CLI 유형의 방화벽에게 전달한다. 그리고 API 유형의 방화벽은 X-Guard 정책프록시에 의해 API를 이용한 X-Guard 보안제어 정책을 전달받는다.

V. 결 론

보다 크고 복잡한 네트워크를 관리하는 데 따른 문제를 해결하기 위한 노력을 시작한 것은 불과 최근에 들어와서다. 효율적인 운용관리를 위한 대안으로 PBNM 기술에 대한 연구와 표준화가 진행되어 왔다.

하지만 PBNM이 현실화되지 않는 몇 가지 문제점들이 있다. 첫째, IETF에서의 관련 정책도 IPSec 구성관리 및 QoS와 관련된 분야에만 치중되어 있다. 정책기반 네트워크 보안제어를 위해서는 폭넓은 범주의 보안서비스를 지원해야 한다. 둘째, 보안제어에 있어 표준의 결핍은 진정한 정책기반 관리 기법을 지연시키며, 장기적으로 볼 때 이것은 우리가 네트워크 안전성이라는 목표에 다가가는 것을 막는다. 셋째, 많은 사람들에게는 장비 관리를 위해 CLI가 기본 표준이 되고 있는데, 그것은 방대한 설치로 인한 결과이다. 그러나 CLI는 대부분 전용 인터페이스로서 제조사마다 다르고, 어떤 경우는 제품마다 버전마다 달라지기도 한다. 그렇다고 해서 CLI가 나쁘다는 것은 아니다. 왜냐하면 아스키(ASCII, American Standard Code for Information Interchange)이기 때문에 SNMP ASN.1 표시보다도 이해하기가 훨씬 쉬우며, 보안제어를 정책 목표에 맞게 변경하는 작업이 간단하다. 그러나 잦은 변경으로 인한 전반적으로 무거운 수정 절차과정을 겪게 되는 결점을 갖는다. 넷째, XML 인터페이스는 보안제어 절차를 변경하는데 CLI보다

는 용이한 측면에서 하나의 접근 방안이 될 수 있지만, 보안제어 정책을 정의 및 저장하는 데는 아무런 도움이 되지 못한다. 다섯째, PDP와 PEP 간에 지능을 갖는 정책 교환을 위한 표준 프로토콜인 COPS는 많은 업체들의 관심을 끌 것으로 생각되었지만, 실제 COPS를 지원하는 업체들은 많지 않다. 현재 보안제어 정책 전달은 독자적인 전달 프로토콜을 이용하고 있다. 보안제어를 위해 다양한 방식으로 네트워크 인프라에 접근하는 것은 진정한 정책관리를 제지할 뿐만 아니라 완전히 잘못된 접근 방식이다. 보안제어를 위해서는 다양한 범주의 인프라 장비 형태, 모델 및 버전을 지원해야 한다. 체크포인트사 중심의 OPSEC(Open Platform for Security)[21]은 종합적인 보안제어를 목표로 하고 있는 측면에서 하나의 접근 방안이 될 수 있지만, 보안제어 정책을 전달하는데 있어 단순한 정책만을 전달하는 SNMP를 이용하고 있어서 실시간 정책 적용여부에 그 한계점이 있다. 그러나 위에서 언급한 문제점들은 시간이 지나면 해결될 것으로 기대된다.

본 논문에서는 정보통신 인프라에서 시스템 관리 측면에 유리한 정책기반 네트워크 관리 기술에 기반을 두어 효율적인 운영관리가 가능한 IETF Policy 워킹그룹의 정책 프레임워크에 따라 정보보호 제어 프레임워크를 연구하였다. IETF의 PCIM/PCIMe를 근거로 보안제어 정책 모델을 정의하였으며, 정책기반 네트워크 보안제어 프레임워크를 실현하기 위해 현실적으로 가장 유효한 접근 방안인 정책프록시를 활용하여 단계적으로 적용하는 방법을 수행하였다.

앞으로의 연구사항으로는 단계적인 보안시스템 적용에 따른 X-Guard의 세부 클래스 정의와 확장 및 보완이 요구된다. 또한 정보통신 인프라의 침해에 대하여 추가적인 보안제어 정책을 정의해야 한다.

끝으로 제한된 네트워크 보안제어 숙련자 환경에서 망의 진화에 따른 보안관리의 복잡성과 인프라 공격에 따른 피해 전파 신속성에 따른 보안제어의 실시간성이 문제로 대두되고 있으며, 더 나아가 사회 전반적인 문제로 확대될 때 정책기반 네트워크 보안제어는 비로소 자리매김을 할 것이다.

참고문헌

[1] NIST, NIST Computer Security Special Publications http://csrc.nist.gov/publications/nistpubs/index.html

[2] G. Smith and R. Newton, "*A Taxonomy of Organizational Security Policies*," Proceedings of the 23rd National Information Systems Security Conference, Baltimore, Maryland, Oct. 2000, http://csrc.nist.gov/nissc/2000/proceedings/toc.html (current 24 November 2001).

[3] SANS, The SANS *Security Policy Project*, www.sans.org/newlook/resources/policies/policies.htm

[4] Georgia Institute of Technology, "*Computer and Network Usage Policy*," http://adminguide. stanford.edu/62.pdf, June 2004.

[5] B. Fraser, "Site Security Handbook," RFC 2196, IETF, Sep. 1997.

[6] DMTF, "*Policy Version 2.9 CIM Specification*," http://www.dmtf.org, 2004.

[7] DMTF, "*Desktop Management Interface (DMI) Specification version 2.0*," http://www.dmtf.org/standards/documents/DMI/DSP0001.pdf, June 24, 1998.

[8] Christopher M. King, et al, "*Directory Enabled Network (DEN)*," Macmillan Technical Publishing, 2001.

[9] DMTF, "*Web-Based Enterprise*

Management," http://www.dmtf.orgstandards/wbem.

[10] DMTF, "*Specification for the Representation of CIM in XML Version 2.0*," http://www.dmtf.org/standards/documents/WBEM/CIM_XML_Mapping20.html, June 2nd, 1999.

[11] B. More, E. Ellesson, J. Strassner, and A. Westerinen, "Policy Core *Information Model - Version 1 Specification*," RFC 3060, IETF, Feb. 2001.

[12] B. More, "*Policy Core Information Model (PCIM) Extensions*," RFC 3460, IETF, Jan. 2003.

[13] J. Jason, L. Rafalow, and E. Vyncke, "*IPsec Configuration Policy Information Model*," RFC 3585, IETF, Aug 2003.

[14] Y. Snir, Y. Ramberg, J. Strassner, R. Cohen, and B. Moore, "*Policy Quality of Service (QoS) Information Model*," RFC 3644, IETF, Nov. 2003,

[15] B. Moore, D. Durham, J. Strassner, A. Westerinen, and W. Weiss, "*Information Model for Describing Network Device QoS Datapath Mechanisms*," RFC 3670, IETF, Jan. 2004.

[16] ETSI, "*Open Service Access; Application Programming Interface; Part 13: Policy management SCF*," ETSI ES 202 915-13 V1.1.1, http://www.parlay.org/specs/index.asp, Jan. 2003.

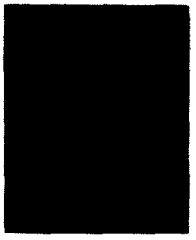
[17] K. McCloghrie, M. Fine, J. Seligson, K. Chan, S. Hahn, R. Sahita, A. Smith, and F. Reichmeyer, "*Structure of Policy Provisioning Information(SPPI)*," RFC 3159, IETF, Aug. 2001.

[18] J. Strassner, B. Moore, R. Moats, and E. Ellesson, "*Policy Core Lightweight Directory Access Protocol (LDAP) Schema*," RFC 3703, IETF, Feb. 2004.

[19] D. Durham, J. Boyle, R. Cohel, S. Herzog, R. Rajan, and A. Sastry, "*The COPS(Common Open Policy Service) Protocol*", RFC2748, IETF, January, 2001.

[20] K. Chan, J. Seligson, D. Durham, S. Gai, K. McCloghrie, S. Herzog, F. Reichmeyer, R. Vavatkar, and A. Smith, "*COPS Usage for Policy Provisioning (COPS-PR)*," RFC3084, IETF, March, 2001.

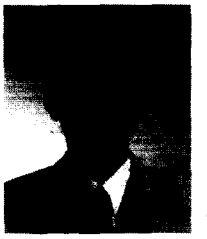
[21] OPSEC, Build Your Security Infrastructure With Best-of-Breed Products From OPSEC," OPSEC White Paper, 2004.



나 중 찬

1986년 2월 : 충남대학교 계산통계학과 이학사
1989년 2월 : 숭실대학교 전자계산학과 공학석사
2004년 2월 : 충남대학교 컴퓨터과학과 이학박사
1989년 2월 ~ 현재 : ETRI 능동보안기술연구팀 팀장

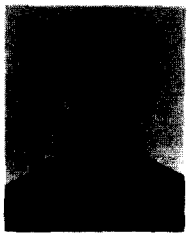
<관심분야> 비정상트래픽 분석, 네트워크 공격상황 분석, 네트워크 방어 시스템



장 종 수

1984년 2월 : 경북대학교 전자공학과 공학사
1986년 2월 : 경북대학교 전자공학과 공학석사
2000년 2월 : 충북대학교 컴퓨터공학과 공학박사
1989년 7월 ~ 현재 : ETRI 네트워크보안그룹 그룹장

<관심분야> 네트워크보안, 정책기반보안관리, 비정상트래픽탐지, 유해정보차단



김 진 오

1994년 : 인하대학교 전자계산공학과 공학석사
1991년 ~ 1998년 : ETRI 네트워크기술연구소
1998년 ~ 2001년 : (주)팍스콤
2001년 ~ 현재 : ETRI 능동보안기술연구팀 선임연구원

<관심분야> 네트워크 공격상황 분석, 프로그래밍언어

손 선 경

1999년 2월 : 전남대학교 전산학과 이학사
2001년 2월 : 전남대학교 전산통계학과 이학석사
2001년 ~ 현재 : ETRI 능동보안기술연구팀 연구원

<관심분야> 정책 모델링, 컴퓨터통신 미들웨어, 정책기반보안관리