통합보안 관리 시스템 표준화에 관한 연구☆

김 석 훈* 손 우 용* 송 정 길**

◈ 목 차 ◈

1. 서 론

네트워크와 컴퓨터의 발달로 인하여 보안사고 발생 시 신속한 침해 사고 대응서비스를 통한 대응체계를 갖추기 위해 다양한 종류의 보안 솔루션들이 개발되고 있다. 최근 일반기업, 금융권, ISP 등의 정보보호 관리 담당자 혹은 시스템 및 네트워크 담당자들은 단품 솔루션들이 제공하는 정보보호 서비스에서 관리비용의 증가, 일관된 정보보호정책 적용이나 침해사고 공동대응의 불가 등과' 같은 효율성이나 관리 측면에 있어 여러가지 문제를 발생시켰다[1,2].

이로 인하여 인터넷이라는 개방된 환경에서 무방비 상태로 노출되어 있는 기업정보를 안전하게 보호하기 위해 복잡한 정보보호 솔루션들을 일관성 있는 정책으로 중앙에서 통합관리하고 잠재되어 있는 위험요소들을 사전에 파악하여 능동적으로 대처하고자 하는 요구에서 등장한 것이 통합보안관리(Enterprise Security Management : ESM) 시스템이다[3,5].

ESM은 침입차단시스템(Firewall), 침입탐지시스템(IDS), 가상사설망(VPN) 등 다양한 종류의 보안 솔루션을 하나로 모은 통합 보안 관리 시스템으로 보안 관리보다는 통합 시스템 관리의 형태로시스템 관리의 영역에서 먼저 출발하여 Firewall, VPN, 바이러스 검사, 컨텐츠 필터링, URL 모니터링/필터링, 침입탐지 등 별개의 보안 구성 요소를 일관적인 전체로 결합하여, 인증과 감시, 허가에서 네트워크 관리에 이르기까지 모든 것들을 망라하는 통합관리로 연구되고 있다.

따라서, 본 연구에서는 네트워크 보안 기술의 흐름을 파악하기 위하여 현재의 ESM의 국내·외 기술동향 및 시장전망과 표준화 동향을 분석하고 살펴보고자 한다. 본 연구를 통해 네트워크 보안 기술의 향후 발전 방향을 예측하고 향후 시스템 및 네트워크 관리에 적극 활용할 수 있을 것으로 기대한다.

2. 통합보안관리 시스템 연구

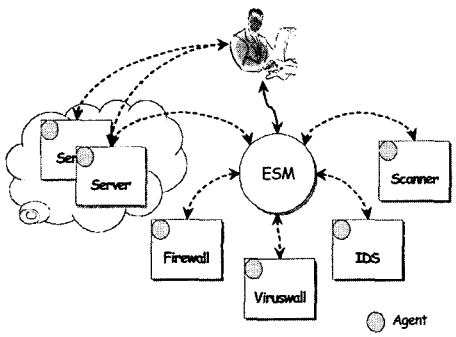
2.1 통합보안관리 시스템 개념적 정의

통합보안관리 기술은 침입탐지 시스템, 가상사설망 시스템 등 다양한 종류의 보안 시스템들을 상호 연동하여 각 기능을 통합 관리하는 중앙집중식 관리체계로서, 보안관제서비스 업체, 보안 시스템 개발 업체들 간에 컨소시움 형태나 독립적인 통합 보안관리시스템으로 개발되고 있다[8].

통합보안관리 기술 수준은 현재 자사 제품에 대한 모니터링 기능이 구현되어 있지만, 앞으로는 보안 프로토콜의 표준화를 통해 타사 제품을 포함한 이기종 보안 시스템에 대한 모니터링 기능을 가지도록 발전

☆ 본 연구는 '한국과학재단 지역협력연구센터(과제번호 : R12-2003-004-02001-0) 지원으로 수행되었음'
* 한남대학교 컴퓨터공학과 박사과정
** 한남대학교 정보통신 멀티미디어공학부 교수

하고 있으며, 수집된 자료를 분석하여 보안사건에 대한 리포팅 기능과 함께 각 보안시스템에 대한 세부 정책관리 기능이 가능한 단계로 발전할 것으로 예상되고 있다. 즉, 보안정책을 수립하고 수립된 보안정책에 따라 시스템을 구현하며, 이를 모니터링 하거나 신속하고 효과적인 조치를 위해 각종 경보 기능을 제공하는 등 일련의 워크플로우를 일관되게 지원하는 것이 그것이다.



(그림 1) 통합 보안 관리 시스템

2.2 통합보안관리 시스템 분류

ESM은 워크플로우에 따라 사용자 및 정책 관리와 취약성 및 위협 평가로 분류할 수 있다[9].

(표 1) 시용자 및 정책관리 제품군

개발사	제품명	주요특징
BMC Software	CONTROL-SA	많은 Platform과 Application 지원
CA	eTrust	사용자관리, 인증, 암호화 등 제공
Bull Soft	AccessMaster Security Policy	Single Sign-On을 위한 각종 기능 제공
	AccessMaster Single Sign-On	바이오메트릭, 스마트카드 등 지원
Schumann Security Software	Security Administration Manager(SAM)	대형 사업장에 적합하도록 설계
Unisys	SP User Manager	사용자 관리
	SP Sign-On	Single Sign-On 제공
	SP I-Net	네트워크 관리

● 사용자 및 정책관리

보안 또는 관리정책에 따른 사용자 및 Access 관리에 무게 중심을 둔 범주이다. 이 범주에는 인증이나 Single Sign-On의 기능을 포함하는 경우가 많고, 초기 ESM 모습이 많이 반영되어 보안적 측면보다는 시스템 관리적 측면의 성격이 강하다.

● 취약성 및 위협 평가

네트워크 및 시스템의 취약점, 위협 요소들을 분석하고 모니터링하는 관리도구의 형태를 취하며 제품에 따라 분석 또는 정책관리, 모니터링 및 경보(Alert) 등 어느 쪽에 초점을 두느냐에 따라 특성이 약간씩 다르다. 최근 ESM 기술의 주류를 이루고 있으며 기존 보안 제품들과의 통합(Integration)이 활발히 진행되는 범주이다.

(표 2) 취약성 및 위협 평가 제품군

개발사	제품명	주요특징
CheckPoint	Provider-1	OPSEC 기반의 자사 침입차단, 침입탐지 등 통합관리
Intellitactics	Network Security Manager	보안정책에 설정 및 이에 따른 Audit
Axent	Enterprise Security Manager	사용자/password 관리, File Access/Attribute, Login등 호스트 기반의 취약점 점검 및 Reporting
e-Security	Open e-Security Platform	각종 침입차단, 침입탐지 등 통합관리
Internet Security Systems(ISS)	Internet Scanner	Network 취약점 분석
	System Scanner	System 취약점 분석
PentaSafe	VigilEnt Security Management	사용자 관리, File/Directory 관리, Network 관리, Audit 및 Reporting

2.3 통합보안관리 시스템 동향

국내에서도 최근 ESM 개발 열기가 뜨겁게 달아오르고 있고, 공공 시장에 집중되던 통합보안관리(ESM)

솔루션 수요가 금융권과 일반기업으로 확대되고 있다. 디지털이지스, 이글루시큐리티가 상반기 제품 출시 이후 인젠과 어울림정보기술이 그 뒤를 이어 제품을 발표하며 본격적인 ESM 춘추전국 시대를 예고하고 있다[10].

하지만 국내의 ESM은 이제 제품이 출시되고 있는 단계이고 시장에서 검증을 거치지 않았다는 점에서 우려할 부분은 있으나 점차 보편적으로 사용할 수 있는 잠재적 시장이 조성되고 있다는 판단이다. ESM의 전체 시장규모는 전체 보안시장의 5~10%정도로 추산되며 이의 선점을 위하여 초기시장에서의 각축이 예상된다. 현재까지 출시된 주요 국내 제품의 종류와 특징은 (표 3)과 같다.

(표 3) 국내 ESM 제품 현황

개발사	제품명	주요특징
디지털 이지스	이지스 엔터프라이즈	자사 침입차단, 침입탐지 등 통합관리, 모니터링
이글루 시큐리티	스파이더-1	각종 침입차단, 침입탐지 등 통합관리, File/Directory 관리, Real-Time Alert 제공
어울림 정보기술	SecureWorks ESM	자사 침입차단 통합관리, 모니터링, 타 제품 지원예정
인젠	NewWatcher ESM	자사 침입 차단, 침입 탐지등 통합관리, ESM 컨소시엄 추진
시큐아이 닷컴	시큐아이 엠에스에스	웹 기반의 보안통합관리 툴 자사의 보안관제서비스에 사용

3. 통합보안관리 시스템 표준화 동향

3.1 ISTF(Internet Security Technology Forum)

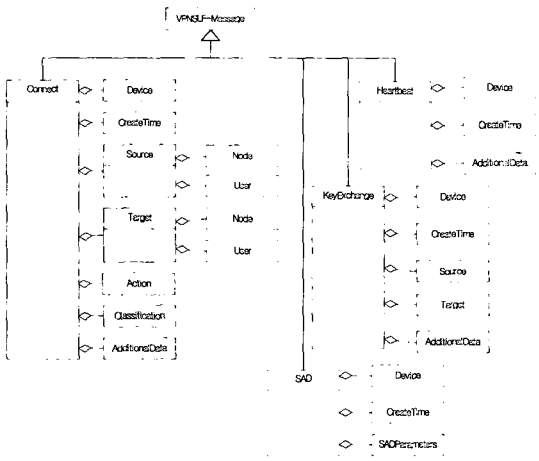
인터넷보안기술포럼(Internet Security Technology Forum: ISTF)은 인터넷 보안기술 분야의 민간 업체들이 중심이 되어 구성된 민간 포럼으로 인터넷 보안기술 관련 국제 표준화 활동에 공동 대응하고 시장수요를 반영한 표준 개발을 위해 2001년 창립되었다[4].

ISTF의 주요 역할은 인터넷 보안기술 관련 최신 기술정보의 수집, 분석, 보급 및 활용을 촉진하고, 인터넷 보안기술 관련 국내 표준을 개발하며, 인터넷 보안 관련 제품 상호운용성 항목 발굴 및 상호운용성 시험을 수행한다. ISTF에서는 Firewall, VPN, IDS 등 여러 보안 업체의 보안 솔루션을 중앙에서 통합 관리할 수 있도록 로그형식 표준안을 2003년 4월에 제정하였다.

3.2 가상 사설망 시스템 로그 데이터 모델

가상 사설망 시스템의 로그 형식을 객체 지향 방법론 설계 언어인 UML의 클래스 다이어그램으로 로그의 데이터 모델을 정의하여 개념적인 표현이 가능하게 하였으며, VPN 로그 형식에서 가장 상위 클래스는 VPNSLF-Message(Virtual Private Network System Log Format-Message)로 모든 종류의 메시지를 총칭한다[4].

여기에는 크게 두 종류의 메시지가 있는데, 시스템에서 접속시의 메시지를 의미하는 Connect 클래스와 시스템의 동작 상태를 의미하는 Heartbeats 클래스이다. VPN 로그 데이터 모델의 세부적인 내용을 UML의 클래스 다이어그램으로 설계한 결과는 (그림 3)과 같다.



(그림 3) VPN 시스템 로그 클래스

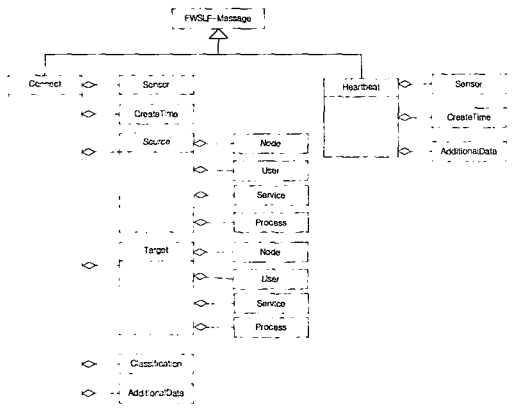
(그림 3)에서 정의한 각각의 클래스 모델을 XML 문서의 규칙과 형식을 만족하기 위하여 DTD로 정의한 결과는 (그림 4)와 같다.

```
// VPNSLF-Message 클래스 DTD
<!ENTITY % attlist.vpnslf "version CDATA #FIXED '1.1' ">
<!ELEMENT VPNSLF-Message (
 (Connect | Heartbeat | KeyExchange | SAD )*)>
<!ATTLIST VPNSLF-Message%attlist.vpnslf; >

// Connect 클래스 DTD
<!ENTITY % attvals.criticaltype
"(unknown|normal|suspicious|warning|critical)">
<!ELEMENT Connect (
Device, CreateTime, Source, Target, Action
Classification, AdditionalData* )>
<!ATTLIST Connect ident CDATA '0'
criticality %attvals.criticaltype 'unknown'
tunnelname CDATA '0' >

// Heartbeats 클래스 DTD
<!ELEMENT Heartbeat (Device, CreateTime, AdditionalData* )>
<!ATTLIST Heartbeat ident CDATA '0'>
```

(그림 4) VPN 시스템 로그 표준 DTD

3.3 침입차단 시스템 로그 데이터 모델

Firewall 로그 형식에서 가장 상위 클래스는 FWSLF-Message로 모든 종류의 메시지를 총칭한다. 시스템에서 접속시의 메시지를 의미하는 Connect 클래스와 시스템의 동작 상태를 의미하는 Heartbeats 클래스가 크게 적용된다. Firewall 로그 데이터 모델의 세부적인 내용을 UML의 클래스 다이어그램으로 설계한 결과는 (그림 5)와 같다.



(그림 5) 침입차단 시스템 로그 클래스

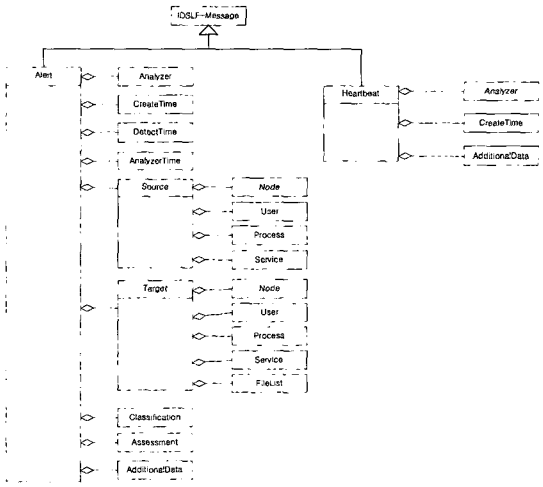
(그림 5)에서 정의한 각각의 클래스 모델을 XML 문서의 규칙과 형식을 만족하기 위하여 표준 DTD로 정의한 결과는 (그림 6)과 같다.

```
// FWSLF-Message 클래스 DTD
<!ENTITY % attlist.fwslf "version CDATA #FIXED '1.1'">
<!ELEMENT FWSLF-Message ((Connect | Heartbeat)*)>
<!ATTLIST FWSLF-Message %attlist.fwslf;>

// Connect 클래스 DTD
<!ENTITY % attvals.criticaltype "(unknown|normal|
 suspicious | warning | critical )">
<!ENTITY % attvals.actiontype "(unknown |
pass | block | protect) ">
<!ELEMENT Connect (Sensor, CreateTime,
Source, Target, Classification, AdditionalData*)>
<!ATTLIST Connect ident CDATA '0'
criticality %attvals.criticaltype 'unknown'
action %attvals.actiontype 'unknown'>

// Heartbeats 클래스 DTD
<!ELEMENT Heartbeat (Sensor, CreateTime, AdditionalData*)>
<!ATTLIST Heartbeat ident CDATA '0'>
```

(그림 6) 침입차단 시스템 로그 표준 DTD

3.4 침입탐지 시스템 로그 데이터 모델

IDS 로그 형식에서 가장 상위 클래스는 IDSLF-



(그림 7) 침입탐지 시스템 로그 클래스

```
// IDSLF-Message 클래스 DTD
<!ENTITY % attlist.idslf "version CDATA #FIXED '1.1'">
<!ELEMENT IDSLF-Message ((Alert | Heartbeat)*)>
<!ATTLIST IDSLF-Message %attlist.idslf;>

// Alter 클래스 DTD
<!ELEMENT Alert(Analyzer, CreateTime, DetectTime?,
AnalyzerTime?, Source*, Target*, Classification+,
Assessment?, (ToolAlert | OverflowAlert | CorrelationAlert)?,
AdditionalData* )>
<!ATTLIST Alert ident CDATA '0' >

// Analyzer 클래스 DTD
<!ELEMENT Analyzer (Node?, Process? )>
<!ATTLIST Analyzer analyzerid CDATA '0'
 manufacturer CDATA  #IMPLIED
 model        CDATA  #IMPLIED
 version      CDATA  #IMPLIED
 class        CDATA  #IMPLIED
 ostype       CDATA  #IMPLIED
 osversion    CDATA  #IMPLIED>
```

(그림 8) 침입탐지 시스템 로그 로그 표준 DTD

Message로 모든 종류의 메시지를 총칭한다. 시스템에서 검출하는 메시지를 의미하는 Alerts 클래스와 시스템의 동작 상태를 의미하는 Heartbeats 클래스가 크게 적용된다. IDS 로그 데이터 모델의 세부적인 내용을 UML의 클래스 다이어그램으로 설계한 결과는 (그림 7)과 같다.

4. 통합보안관리 시스템 전망

공공 시장에 집중되던 통합보안관리(ESM) 솔루션 수요가 금융권과 일반기업으로 확대되고 있다. 2003년 초부터 한미은행, LG 투자증권, 증권전산 등 은행과 증권사의 ESM 도입이 이어졌으며 지난 8월 KTF가 올해 최대 규모의 ESM 프로젝트를 시작한 것을 비롯해 SK텔레콤 등 일반 기업에서도 ESM 도입의 물꼬가 터지기 시작했다. 이에 따라 ESM 업체들의 전체적인 매출이 늘어나는 가운데 금융권 및 일반기업 매출 비중 또한 갈수록 높아지고 있다.

2004년 들어 ESM 사업을 크게 강화한 인젠은 주로 대형 통신업체의 프로젝트를 수주하면서 공공 시장에 비해 금융권 및 일반기업 비중이 크게 증가했다. 인젠은 ESM 관련 매출이 2001년 48억원에서 작년 67억원으로 증가했으며 올해도 91억원의 실적이 예상되는 등 가파른 상승세를 타고 있다. ESM 전문업체인 이글루시큐리티도 작년 전체 매출 가운데 금융권과 일반기업의 비중이 34.6%였는데 올해는 51.6%로 17% 포인트 높아졌고, 전체 매출은 아직 집계되지 않았지만 작년에 비해 50% 정도 증가할 것으로 예상하고 있다. 보안 업계에서는 내년에는 ESM 시장이 큰 폭으로 확대되면서 금융권과 일반기업의 수요가 늘어나는 추세가 이어질 것으로 전망했다.

2003년에는 2002년에 1차로 지정된 23개 주요정보통신기반시설에서 많은 ESM 수요가 나왔지만 2004년에는 2차 주요정보통신기반시설이 66개로 늘어났기 때문에 내년 ESM 수요 전망을 밝게 만들고 있다. 특히 통신 이외에 불모지였던 일반기업 시장에서 제조 등 보안솔루션을 많이 사용하고 있는 대형 업체도 ESM을 도입하려는 움직임을 보이고 있어 시장 확대를 부추길 것으로 예상된다.

5. 결 론

현재 여러 종류의 침입탐지 시스템이 개발되고 있으나 각각의 보안 시스템간의 정보표현과 결과보고 방법이 그에 대한 의견 통일이 어려우며, 많은 과탐지(false positive)가 존재하여 관리자를 피곤하게 하는 요소가 되고 있다. 이러한 환경에서도 중요한 서비스를 지속적으로 제공하여 사용자의 신뢰도를 떨어트리지 않아야 하고, 침입이 발생하더라도 침입자를 즉각적으로 색출하여 대응할수 있는 기반이 마련되어야 한다.

본 논문에서는 다양한 보안 시스템들 간의 상호 호환성과 확장성을 제공하기 위하여 통합보안관리 시스템을 위한 침입탐지 시스템, 침입차단 시스템, 가상사설망 간의 로그 표준 메시지 교환 형식인 XML과 DTD의 확장을 통해 메시지 형식을 정의하고, 유연성을 보장하는 표준을 살펴보았다.

향후 연구 방향으로는 DTD로 이루어진 메시지 표준을 XML Schema로 재정의 하고, 보안 관리자의 부재중에 생기는 침입에 대한 차선책으로 웹기반 인터페이스를 XSLT를 통해 구현하도록 하여 실시간 모니

터링 및 침입자의 악의적인 공격에 손쉽게 대처할 수 있는 연구가 필요하다. 또한, 통합보안관리 시스템이 국내 뿐만 아니라 세계 시장에서도 경쟁력을 가지고 성장하기 위해서는 정책기반의 이기종간 통합보안관리 시스템의 추론엔진 개발이 필요할 것이다.

참고문헌

[1] 전자신문, http://www.etnews.co.kr

[2] 한국정보보호진흥원, http://www.kisa.or.kr

[3] 한국전자통신연구원, 인터넷 보안 시스템 기술시장 보고서, 2002. 12

[4] 인터넷보안기술포럼(ISTF), http://www.istf.or.kr

[5] 이영석, "ESM 자료조사" ETRI 기술문서, 2002.12.

[6] Judy Novak, Stephen Northcutt, "Network Intrusion Detection," New Riders Publishing, 2003

[7] Earl Carter, "Cisco Secure Intrusion Detection System," Sicso Press, 2001

[8] 오승희 외, "최신 네트워크 보안 기술 동향 분석", 한국정보과학회 추계학술 발표 논문지, 제 30권 2호, 2003.10

[9] 정영서 외, "네트워크 정보보호 시스템 발전 방향", SK Telecommunications Review, 제 13권 제 2호, 2003. 2

[10] 이영석 외, "통합 보안 관리를 위한 이기종 보안 시스템 연동", 한국정보보호학회 학회지, 제 13권 제 1호, 2003.2

◐ 저 자 소 개 ◑

김 석 훈

2001년 배재대학교 정보통신공학과 졸업(공학사)
2003년 한남대학교 대학원 컴퓨터공학과 졸업(공학석사)
2003년~현재 한남대학교 대학원 컴퓨터공학과 박사과정 재학중
관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 모바일 컴퓨팅, ESM etc.

손 우 용

1998년 한남대학교 컴퓨터공학과 졸업(공학사)
2000년 한남대학교 대학원 컴퓨터공학과 졸업(공학석사)
2001년~현재 한남대학교 대학원 컴퓨터공학과 박사과정 재학중
관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 분산처리 시스템, ESM etc.

송 정 길

1966년 한남대학교 수학과(이학사)
1982년 홍익대학교 대학원 전자계산학과(이학석사)
1988년 중앙대학교 대학원 전자계산학과(이학박사)
1990년~1991년 University of illinois 객원교수
1979년~현재 한남대학교 정보통신·멀티미디어 공학부 교수
관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 분산시스템, ESM, etc.