학내전산망의 안전성 확보를 위한 보안진단 에이전트 개발

박종오† · 이철현† · 김성식††

요 약

최근 몇 년 동안 인터넷의 폭발적 증가에 따라 정보검색과 접근이 매우 용이해졌으나, 시스템 및 데이터에 대한 인증되지 않은 사용자의 부적절한 접근과 이로 인한 피해가 빈번히 발생하고 있다. 따라서 시스템 및 중요 데이터에 대한 보안 방안을 구축하는 것이 중요하게 되었다. 이는 현재 전 학교에 보급되어 있는 학내 전산망도 예외가 아니다. 그러나 현실적으로 학교 환경의 열악함으로 인해 안전한 서버와 네트워크 운영을 위한 보안 관리 운영에는 매우 미약하며, 이에 따른 많은 우려를 낳고 있다. 본 논문에서는 학교전산망의 안전성을 확보하기 위한 보안 요소를 살펴보고, 보안관리에 도움을 주는 보안진단 에이전트를 개발하였다. 이는 간단한 등록절차만 거치면 서버 뿐만 아니라 PC를 대상으로 기본적이고 중요한 보안 문제를 자동적으로 점검하여 통지함으로써 학내 전산망의 관리에 효율성을 제공할 수 있을 것으로 기대한다.

Development of Security Audit Agent for the Safety in School Network

Jong-O Park† · Chul-Hyun Lee† · Seong-Sik Kim††

ABSTRACT

Internet has being grown explosively in recent years, hence it becomes easy to search and access information. But it is happening frequently to access illegally into the systems and data, there are many damage caused by them. So, it is very important that we construct security plan for the systems and data. It is not exception on school network being diffused to all schools. But, we have weakness about security to manage server and network safely. So it is causing much anxieties. In this paper, we searched security points make sure of safety of school network, and developed security audit agent helping management of security. Through simple registration process, this agent is able to audit basic and important security problems about not only server systems but also pc systems, and notify to administrator automatically. It is expected to provide efficiency in managing school network.

1. 서 론

학교교육에 있어 전산망의 도입은 그 활용 및 교육의 미래에 대한 대비에 있어서 지극히 당연한 것으로 받아들여지고 있다. 현재 학교현장에서 인터넷의 연결과 개인용 컴퓨터 및 학사업무 관련 서버가 매우 많이 보급되어 있지만, 그에 따른 활용 및 보안 관리체계가 미흡한 것이 심각한 문제로 대두되고 있다. 본 논문에서는 이러한 문제의식에 기초하여, 학내 전산망의 효율적인 보안 관리체계를 구축함으로서 학교 현장의 현실

† 정 회 원: 한국교원대학교 컴퓨터교육과 박사과정
†† 종신회원: 한국교원대학교 컴퓨터교육과 교수
논문접수: 2001년 11월 2일, 심사완료: 2002년 1월 5일

적인 문제에 대한 실질적인 도움 제공을 목적으로 한다.

2. 관련연구

2.1. 학내 전산망의 구축 현황

정보화사업을 지속적으로 추진 중에 있는 교육인적자원부에서는 2001년 4월 20일 세계최초로 만 여 개교의 국내 모든 학교에 인터넷 연결을 완공하였다. 이것은 현 사회에 주류를 이루고 있는 정보기술(Information Technology; 이하 IT)이 단순히 학교 교육 기능의 한 분야가 아니라, 학교 교육이라는 시스템 전체를 IT속에서 함께 숨쉬게 하는 종합적이고 장기적인 발판 마련의 의의를 갖는다. 더불어 이번 정보화사업으로 컴퓨터 약 1백만대, 컴퓨터실습실 1만2897개와 함께 34만 교원에게 개별 PC가 보급됐다고 하며, 2003년까지 교육인적자원부와 16개 시·도교육청, 학교를 잇는 온라인 교육행정정보시스템을 구축할 계획[10]을 발표하였다.

이로써 전국의 모든 초·중등 학교가 최소 256Kbps 이상의 전용선과 별도의 학내전산망을 통해 인터넷에 연결된 학교 정보인프라가 구축되었고, 이를 기반으로 학교에서는 인터넷상의 다양한 교수-학습자료의 활용과 다변화된 교수방법의 적용 가능성이 한층 높아지게 되었다.

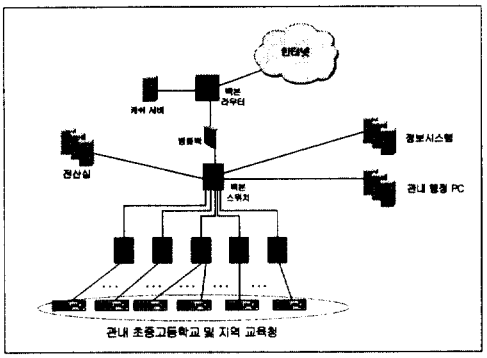
학내 전산망의 구축 현황을 몇 가지 사례를 통해 살펴보면 다음과 같은 유형으로 나눠 볼 수 있다.

(1) 학교가 직접 ISP에 연결한 경우

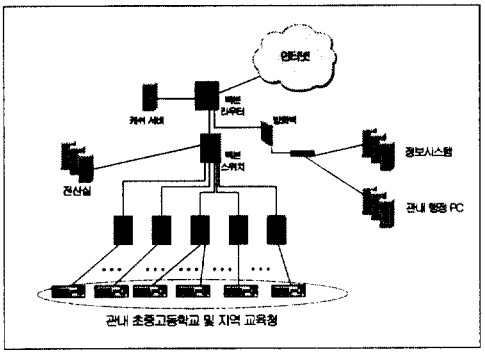
이 경우 선택 가능한 ISP는 크게 교육전산망(KREN), 연구망(KREONET), 초고속 국가망(PUBNET)과 같은 비영리 ISP와 KORNET, BORANET 등의 영리를 목적으로 하는 ISP가 있다. 비영리망에 연결된 경우는 대개 대학 등의 지역센터에 연결된다.

(2) 학교가 시도교육청에 연결한 경우

관리상의 목적으로 관내 다수의 학교가 교육청과 연결되는 경우로, 시도교육청이 충분한 통신장비, 통신회선 및 운영 인력을 확보해야 가능하다. 도교육청의 경우는 관할 구역이 지역적으로 광범위하여 광역시 교육청과 같은 경우는 중앙통제 방법이 아닌 ISP로 직접 연결을 하는 사례가 많다. 도교육청에 인접한 학교들의 경우, 광역시 교육청과 같은 형태로 인터넷에 연결되기도 하지만, 독자적으로 인터넷 연동을 취하는 학교들도 많다.



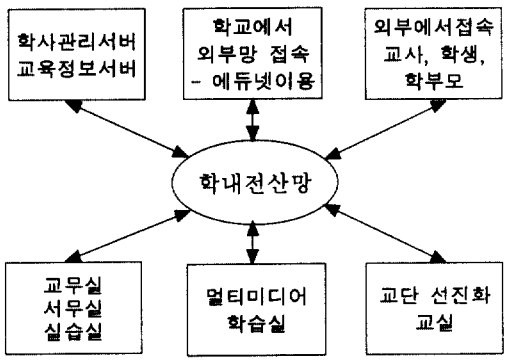
<그림 1> 네트워크 구성도 1



<그림 2> 네트워크 구성도 2

각급 학교가 직접 ISP에 연결한 경우와 시·도교육청을 통해 ISP로 연결되는 통신망 구조에는 보안 정책을 수립함에 있어 많은 차이가 있다. 시·도교육청을 통한 연결일 경우에도 '교육 기관 정보화 역기능 방지에 관한 연구'보고서[5]에 의하면, 5대 광역시를 중심으로 통신망 구조를 조사해 본 결과 <그림 1>, <그림 2>와 같이 두 가지 형태로 교육청 중심의 인터넷 연동 환경이 구성되어 있음을 볼 수 있다. <그림 3>과 같이 교육청의 보안 서버를 통하여 지역교육청 및 초·중·고등학교의 시스템 및 학내망이 연결되어 교육청 차원의 보안 정책이 각급 학교에 적용되어

지는 곳이 있으며, <그림 3>와 같이 각급 학교로 인터넷 연동만이 가능하도록 망이 연결되어지고 교육청 내에 정보시스템 및 행정 PC 등에 보안 서버를 설치하여 각급 학교로의 인터넷 속도에 주안점을 둔 망구조를 가지고 있는 곳이 있다.



<그림 3> 교육정보화 통합 모델 개념도

2.2. 학내 전산망의 활용

교육정보화는 국민적 인식 기반에 기초하여 교육정보화에 대한 법과 제도 등을 정비하고, 이에 기초하여 교육정보화를 추진하는 핵심적인 인적 자원인 교원들의 정보화 연수를 실시함과 동시에 휴먼웨어를 개발하며, 교육환경의 첨단화를 통해 초·중등학교 정보화, 대학 정보화, 교육행정 정보화 세 분야를 추진하고, 이와 같은 일련의 과정을 통해 열린교육과 평생학습사회 실현을 위한 사이버학습체제를 구축함으로써 지식정보화를 대비한 창조적 인재를 육성하는 것을 목표로 하고 있다[1]. 학내전산망은 이러한 교육 정보화 사업의 일환인 '학교 정보인프라 구축'에 따라 우선적으로 추진되었다.

활용측면에서 보면, 학내 전산망은 학습과정에서 교사와 학생간에 이루어지는 의사소통 수단이며, 한정된 컴퓨터와 교육예산의 범위에서 장비 활용도를 크게 신장시킬 수 있다. 교육용 소프트웨어를 호출하거나 분배하는 수단으로 활용되고 다수의 학생이 프린터를 공유하는 수단으로도 활용될 수 있다. 컴퓨터 조작 지도나 학생의 학습 진행 상황을 원격지에서 확인하는 수단으로도 활용되고 자료를 효과적으로 입력하거나 검색하는 수단으로도 활용될 수 있다[3][9].

학내 전산망은 현재 추진되고 있는 교육정보화 사업의 기반을 조성해 주는 역할을 하게 된다. 따라서 학내 전산망을 기반으로 다양한 형태의 교육 정보화 관련 시설들을 연계함으로써 많은 효과를 기대할 수 있다[2]. 구체적인 활용 분야는 (1) 종합정보관리시스템, (2) 교무업무지원시스템, (3) 학사관리시스템, (4) 교육정보시스템, (5) 재무회계시스템, (6) 도서관리시스템, (7) 입시업무시스템, (8) 원격교육, (9) 멀티미디어메일, (10) 전자결재시스템, (11) 교육행정시스템, (12) 문서유통시스템 등이 있다.

3. 학내전산망 보안

3.1. 보안 관리에 대한 요구

컴퓨터 시스템은 한 명의 사용자만이 사용하는 것이 아니라, 여러 명의 사용자가 동시에 사용하는 환경으로 발전해 가면서 다른 사용자로부터 자원을 보호할 필요성이 높아지고 있다. 컴퓨터를 네트워크라는 통신 수단으로 연결하여 사용하게 되면서, 단순히 한 시스템의 사용자뿐만이 아니라 네트워크로 연결된 다른 시스템의 사용자와도 관련을 맺게 되었으며, 인터넷이라는 거대한 네트워크로의 연결은 누가 언제 어디서 시스템에 영향을 미칠지 알 수 없는 단계에까지 이르렀다. 다른 사용자의 영향은 단순한 문제만을 일으킬 수도 있으나 시스템 전체에 심각한 영향을 미칠 수도 있다. 따라서, 컴퓨터 시스템의 보안이라는 문제가 심각하게 대두되었다.

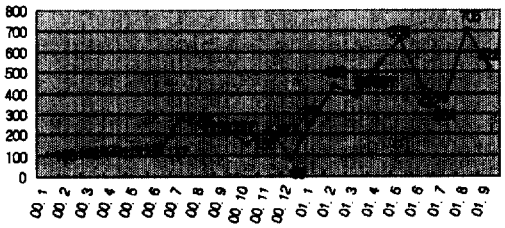
학내 전산망도 인터넷 기술을 이용함에 따라 인터넷이 갖는 장점과 함께 문제점들도 공유한다. 즉, 인터넷은 정보의 보고이기도 하면서 정보를 훼손하고 파손할 수 있는 능력을 제공해 주기도 한다[6]. 인터넷을 통한 불법 침입으로 인해 내부 정보 자산이 파괴되거나 유출되는 사례가 발생하고 있고, 인터넷의 개방성으로 인해 온라인 성적 처리 혹은 보관된 성적의 데이터 침해가 발생될 수 있다. 교사들의 성적, 시험문제 등 각종 학사 자료와 행정실의 학교 운영에 관한 자료

들에 대해서는 외부 사용자는 물론이고 내부 사용자로부터도 보호되어야 한다.

보안이란 생산활동을 위해 보호할 가치가 있는 인원, 문서, 시설, 기술 등 제반 산업기밀의 침해 방지 및 관계없는 자에게 누설되지 않도록 보호하는 활동을 말한다[8]. 이에 따라, 학교망에서도 보안에 대한 요구가 증가하고 있고 학교망에 적합한 보안정책과 운영이 필요하다. 보안 체계를 구성하기 위해서는 비밀성, 무결성, 신분인증, 접근통제, 바이러스 등의 기본 요소들을 학내망 환경에 기초하여 신중히 검토하여야 한다.

3.2. 보안사고 유형 및 통계

<그림 4>는 2001년 9월까지 한국정보보호센터의 월별 국내 해킹피해 접수 통계를 보여주고 있다. 2000년 이후로 점점 더 증가하는 불법 침입을 보여주듯이, 인터넷의 이용이 급증할수록 점점 더 많은 피해가 발



<그림 4> 월별 국내 해킹피해 접수현황

생되고 있다. 이러한 양상은 과거 단순히 인위적인 동작에 의해 특정 시스템에만 영향을 미치는 것과는 달리, 점차로 여러 가지 취약점을 동시에 이용하여 자동화된 코드에 의한 웜 바이러스성의 양상을 띄며 전염의 특성을 갖고 있어 그 전파력이 커지고 있기 때문이다.

<표 1>은 불법적인 전산망의 대표적인 침투형식의 유형과 2001년 월별 침해사고 건수를 나타낸 것이다. 일반적으로 이러한 피해 통계는 보고

<표 1> 전산망 침투의 유형별 기법 및 침해 사고 건수 (2001년 1월~9월)

구 분	기 법	건 수 (월별)									비 고
		1	2	3	4	5	6	7	8	9	
사용자 도용 (Impersonation)	가장 일반적인 해킹방법으로 알려져 있는데 다른 일반 사용자의 ID 및 패스워드를 도용하는 방법으로 sniffer 등을 이용하여 정보를 알아낸 후 시도하는 공격기법	4	26	22	42	31	29	23	21	10	개인사용자계정 도용 등
SW 보안 오류 (SW Vulnerability)	컴퓨터 내의 시스템 SW나 응용 소프트웨어의 버그 등을 이용한 공격기법	0	0	5	5	111	7	5	6	4	IIS Unicode 관련 오류
버퍼 오버플로우 취약점 (Buffer Overflow)	최근 많이 이용되고 있는 방법으로서 소프트웨어 변수관리 상의 문제인 오버플로우 버그를 이용하여 불법으로 명령어를 실행하거나 권한을 가지는 공격 기법	11	29	78	46	29	14	29	19	20	named/bind 등의 취약점 이용
구성 설정 오류 (Configuration Vulnerability)	시스템 SW의 설치나 운영 상에 오류를 이용한 공격기법	0	0	3	3	1	0	2	1	1	사용자 권한 설정 오류
악성 프로그램 (Malicious Codes)	바이러스, 웜 등의 악성코드를 이용한 공격이나 불법침입후 설치하는 뒷문프로그램, 트로이목마 등 해킹 프로그램	85	125	70	89	85	64	65	495	268	백오리피스, Code Red 웜, Code Blue 웜, Nimda 웜 등
프로토콜 취약점 (Protocol Infrastructure Error)	인터넷의 통신 프로토콜인 TCP/IP의 구조취약점을 이용한 구조적인 공격기법	0	0	0	0	0	1	0	0	0	
서비스 거부 공격 (Denial of Service Attack)	시스템이나 네트워크의 정상적인 동작과 서비스를 방해하거나 정지시키는 공격 기법	6	8	4	12	9	1	5	0	4	smurf, TFN2K 공격, Code Red 웜의 부작용 등
E-Mail 관련 공격 (Email Vulnerability)	전자우편 폭탄, 스팸메일 공격 기법	4	5	2	7	9	6	8	11	6	스팸메일 관련 공격
취약점 정보수집 (Vulnerabilties Probing)	어떤 시스템을 공격하기 전에 시스템의 취약점을 알아내고자 하는 보안헛점 정보수집 공격기법	157	245	200	332	383	309	226	151	201	포트,named/bind, ftpd, rpc.statd 취약점 스캔
사회공학 (Social Engineering)	관리자를 속여 패스워드를 알아내거나 권한을 얻어내는 공격 기법	0	0	0	1	0	1	1	1	0	사회적 친분 등을 이용

된 사례만을 근거로 하기 때문에 실제로는 훨씬 많은 침해가 있다고 볼 수 있다. 또, 한 사고에 여러 가지 해킹수법이 사용되는 경우나 또는 공격자가 관련 로그 등을 모두 삭제하여 정확한 해킹수법을 파악할 수 없는 경우도 있다.

이러한 해킹의 결과로 해당 시스템의 파괴, 자료유출 및 변조 등 뿐만 아니라 소속 네트워크 전체까지 영향을 미치고 있다.

3.3. 정보보안 상의 문제점

네트워크에 의존한 정보 처리가 점차 늘어나고 그 침해유형과 빈도가 늘어나고 있는 현 시점에서, 학내 전산망도 예외일 수 없다. 그러나 실질적으로 학내 전산망에서 안전한 서버와 네트워크 운영을 위한 보안 관리 운영 체계에는 미약하거나 다양한 문제점이 존재한다.

현재 초·중등학교의 정보보안 상의 총괄적인 문제점을 구분하면 <표 2>와 같이 3가지로 구분할 수 있다[5]. 일반적으로 초·중등학교는 대학기관에 비해 기술 및 인적자원 측면에서 전산망의 정보보안 환경이 취약하며, 그 인식에 있어서도 많이 뒤쳐짐을 보이고 있다. 이에 공공기관의 일부인 학교에서 발생되는 중요 데이터 및 장비 유지에 있어 보다 절실한 보안 대책이 요구되고 있다.

<표 2> 학교 정보보안의 문제점

관리측면의 보안문제점	· 교육정보화를 위한 총체적인 보안 정책 부재 · 교육정보시스템 보안운영에 필요한 보안 지침 부재 · 보안문제 발생시 대응조치 지침 부재
기술적 측면의 보안 문제점	· 네트워크 및 시스템의 각 요소별 보안 대책 미비 · 침입차단시스템 등 보안시스템의 운영 미숙 · 별도 인터넷 망 사용에 대한 보안 대책 미비
인적 측면의 보안 문제점	· 해킹 대응 등 보안 전문인력 부족

종합적으로 볼 때 학교현장에서 발생되는 정보보안상의 문제점은 교육정보화에 따른 디지털 데이터의 급증과 전산망의 확대로 인해 증가되는 정보침해의 위협에 대해 전산망 및 정보보호에 관한 전문적 기술을 가진 전문인력의 양성 및 그 보조수단이 필요한 것이다. 이에 보안상의 문제점을 진단하고 이를 적절히 처방해 줄 수 있는 시스템의 개발이 절실히 요구된다.

4. 보안진단 에이전트

4.1. 개발환경

보안진단 에이전트의 특성상 TCP/IP 패킷을 원활하게 제어할 수 있고, 고효율을 도모하고 자동화된 개발을 할 수 있는 환경이 필요하다. 본 연구에서는 이러한 환경에 적합한 운영체제로 Linux를 정하였고, Apache와 mySQL, PHP 등을 통해서 보안진단 에이전트를 개발하였다. 구체적인 개발환경은 <표 3>과 같다.

<표 3> 에이전트 개발환경

구 분		내 용
운영체제		Linux (Kernel/2.4.2)
데이터베이스		mySQL/3.23.38
에이전트	Front-End	-Apache/1.3.20 -PHP/4.0.4pl1
	Back-End	-gcc/2.96 -perl/5.6 -bash/2.04 -samba/2.2.1

4.2. 설계

학내 전산망마다 방화벽은 개별적인 설치 및 설정에 의해 동작되며, 전산망 내부의 서버들은 자체적인 보안 설정과 방화벽에 의해 보안에 대한 안정성을 확보하게 된다. 보안진단 에이전트는 이처럼 구축된 학내 전산망 외부에서 점검 동작을 수행한다. 이때 이미 알려진 버그 등의 정보를 이용하여 원격지에서 침입가능 여부를 검사하고 문제점을 조사하기 위해 의도적인 침입을 시도한다.

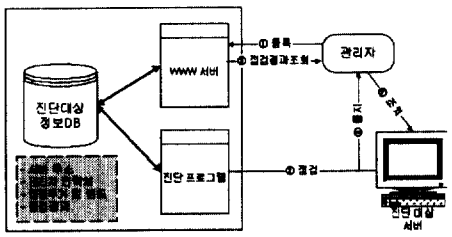
작업의 특성상 임의적으로 스캔하여 진단하지 않고, 신청자의 신청절차에 의거 원하는 서버만을 대상으로 일정 주기로 점검을 수행한다. 에이전트의 수행절차는 다음과 같다.

(1) 점검을 필요로는 하는 서버를 서버 관리자가 에이전트에 등록한다.

(2) 등록된 서버 정보와 점검 희망 주기에 의해 점검 영역별로 진단을 수행한다.

(3) 수행된 결과를 서버 관리자에게 통지한다.

(4) 서버 관리자는 점검 결과에 의한 권고 및 조치사항에 의거 조치를 수행한다.



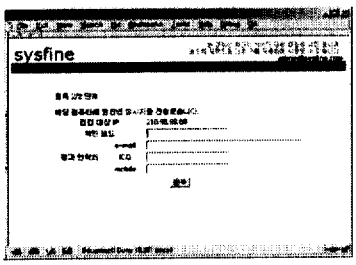
<그림 5> 시스템 구조 및 수행 절차

점검은 해당 운영체제를 먼저 판단하고, 그에 따른 취약점과 문제사항을 확인하는 과정으로 진행되며, 점검 결과를 정리하여 통지하게 된다.

4.3. 구현

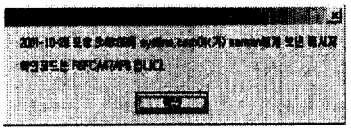
4.3.1. 점검대상 서버 등록

먼저 점검을 원하는 서버의 관리를 담당하는 관리자가 점검 대상 서버를 에이전트에 등록한다. 본 에이전트에서는 자신의 서버가 아닌 대상을 점검하는 등의 오용을 방지하기 위해, 등록시에는 관리자 확인과정을 거치게 된다. 등록을 요청한 관리자에게 임의로 생성된 확인코드를 보내고, 그 코드를 같이 입력해야만 등록이 완료되므로 해당 시스템 관리자이외의 타인이 해킹과 같은 다른 목적으로 서버를 점검할 수 없도록 되어 있다.



<그림 6> 점검 요청 등록 화면

확인코드는 Unix 혹은 Linux 시스템일 경우는 root 계정으로 e-mail을 통해서 보내고 되고, Windows 시스템일 경우에는 윈팝업 메시지를 통해 전달된다.



<그림 7> 확인코드 수신 화면

4.3.2. 점검

점검 요청된 서버는 일단 운영체제에 따른 시스템 유형을 판단하고, 해당 시스템에 필수적인 일련의 점검 요소를 판단하여 보안 점검을 수행한다. 운영체제별 오류, WWW, DNS 등 서버스 오류, 파일 공유 보안 및 웜 바이러스 감염 여부 등으로 여기서는 이미 알려진 보안 문제를 비롯하여, 잠재적인 보안 문제, 그리고 관리자 판단에 의해 조치 결정이 내려질 필요가 있는 권고사항 등으로 구분하여 처리하게 된다. 이 과정에서는 공개된 보안 점검 도구 등을 포함하여 자체 개발된 프로그램과 스크립트 등을 이용한다.

운영체제별 점검 요소는 <표 4>와 같으며, 보안 진단 에이전트의 처리 동작의 구현 코드는 <그림 8>과 같다.

<표 4> 점검 요소

운영체제	대상	요 소
Windows	일반	- 컴퓨터명 - 운영체제 버전 - 활성 포트 및 서비스
	SMB	- 암호설정된 공유폴더의 억세스 가능 취약성 - CodeRed/Nimda 웜 바이러스 등의 감염에 의한 시스템 공유 현황
	IIS	- Index Service .htw 처리 버그 - unicode 처리 버그 - Translate:f 헤더 처리 버그 - directory traversal 버그
	Troyan/ worm	- Back Orifice 등의 감염으로 인한 backdoor 점검
Unix / Linux	일반	- 컴퓨터명 - 운영체제 버전 - 활성 포트 및 서비스 - RPC 정보
	CGI	- phf 등의 각종 CGI 처리 버그
	DNS	- named Buffer overflow 취약성
	SMTP	- sendmail Buffer overflow 취약성
	Troyan/ worm	- rootkit 등의 감염으로 인한 backdoor 점검

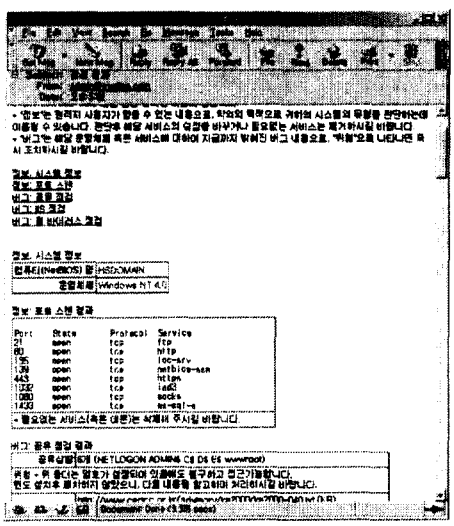
```
struct AUDIT_REPORT *agent_report;

/* 실행 초기화 */
output_report_header();
agent_report = check_system(ip);
if (agent_report->sys_os == SYS_WINDOWS) {
     audit_win_sysinfo(agent_report);
     audit_portscan(agent_report);
     audit_share(agent_report);
     audit_win_iis(agent_report);
     audit_win_worm(agent_report);
     audit_win_backdoor(agent_report);
} else {
     audit_nix_sysinfo(agent_report);
     audit_portscan(agent_report);
     audit_rpcinfo(agent_report);
     audit_nix_cgi(agent_report);
     audit_nix_named(agent_report);
     audit_nix_sendmail(agent_report);
     audit_nix_backdoor(agent_report);
}
output_report_tailer();
send_report(agent_report);  /* email 전송 */
```

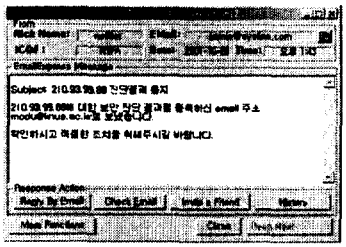
<그림 8> 에이전트(Back-End) 메인코드

4.3.3. 점검 결과 통지

점검이 완료되면 그 결과를 점검 요청시 등록한 통지대상에게 곧바로 전달한다. 점검 결과의 주 내용은 <그림 9>와 같이 HTML 형태의 e-mail을 통해서 전달되며, 그와 동시에 <그림 10>과 같이 ICQ와 같은 인스턴트 메신저와 이동통신의 SMS의 문자서비스를 통해 점검이 완료되었음을 알리게 된다.



<그림 9> 점검 결과 내용 수신 화면



<그림 10> 점검 결과 통지 화면

5. 결 론

정보화가 가져다주는 각종 편리함의 이면에는 인간의 책임을 요구하는 많은 부작용이 공존한다. 인간으로 인해 발생하는 부작용의 처치에 대한 책임은 결국 인간에게 부여되며, 그 일환으로 부작용에 대한 적극적인 대처가 필수적이다. 전산망의 이용에 따른 부작용 현상은 비단 교육에 대한 적용에 있어서만 발생되는 것은 아니지만, 상대적으로 교육현장의 인력 및 관심 부족으로 인해 보안 문제에 대한 대처가 미흡하다.

학내 전산망에서 각종 교육자료 및 학생성적 등의 데이터와 서비스를 제공하는 서버를 안전하게 운영하기 위해서는 무엇보다 관리자의 책임의식과 적극적인 행동이 필요하지만, 최소한의 노력으로 대처할 수 있는 환경이 필요하다. 본 연구를 통해 개발된 에이전트는 간단한 점검의뢰 절차로 보안 측면에서 학교 서버의 안전을 확인하고, 문제 발견시 필요한 조치 방법과 관련 정보를 제시하는 기능을 제공한다.

그러나 보안의 특성상 현재로서는 대상 서버들을 임의적으로 점검할 수 없기 때문에, 서버 관리자의 요청시에만 수동적으로 운영되는 제한점이 있다. 한 학교 전산망의 취약점은 네트워크의 특성상 주변 전산망에 순식간에 영향을 미치며 확산될 수 있다. 따라서 보안에 대한 책임을 각급 학교에 개별적으로 위임하는 것보다는, 교육청 단위로 관내 모든 학교에 대해 통일적이고 일괄적인 보안 점검을 수행할 수 있도록 하는 방안을 고려할 필요가 있다.

참 고 문 헌

[1] 교육부, 한국교육학술정보원(2000). 2000 교육정보화백서. 한국교육학술정보원.

[2] 박명숙 외(1999). 학교정보화 실태 분석 및 활성화 방안 연구. 한국교육학술정보원.

[3] 박찬정(2000). 학교망을 위한 혼합방화벽 구축 및 접근제어 규칙을 위한 그래픽 인터페이스 구현. 한국컴퓨터교육학회지. 3(2).

[4] 신성균 외(1998). 교육정보화 기반 구축 통합 모델에 관한 연구. 멀티미디어교육지원센터.

[5] 유재택 외(2000). 교육 기관 정보화 역기능 방지에 관한 연구. 한국교육학술정보원.

[6] 이미향 외(1999). 초등학교 인트라넷 구축을 위한 보안 시스템 설계. 한국정보교육학회 동계 학술대회 발표지.

[7] 장훈 역(1998), 시스템 관리의 핵심, 한빛미디어. [원전: AEleen Frish (1996). Essential System Administration. O'Reilly.]

[8] 한국네트워크연구조합(1999), 학내 전산망 구축 지침서, 진한도서.

[9] 한병래 외(1999). 교수-학습을 위한 학내전산망 구축의 문제점 및 개선 방안. 한국컴퓨터교육학회지. 2(2).

[10] 교육인적자원부(2001) http://www.moe.go.kr/

[11] 한국정보보호진흥원 침해사고대응팀(2001). http://www.certcc.or.kr/

[12] Security Focus(2001). http://www.securityfocus.com/

박 종 오

1992 한국교원대학교 수학교육과(교육학학사)
1995 한국교원대학교 컴퓨터교육과(교육학석사)
1999~현재 한국교원대학교 컴퓨터교육과 박사과정
관심분야: 원격교육
E-Mail: modu@knue.ac.kr

이 철 현

1993 한국교원대학교 수학교육과(교육학학사)
1995 한국교원대학교 컴퓨터교육과(교육학석사)
1999~현재 한국교원대학교 컴퓨터교육과 박사과정
관심분야: 컴퓨터 교육, ICT 활용 교육
E-Mail: leesleek@cc.knue.ac.kr

김 성 식

1977 고려대학교 경영학과 졸업
1977~1991 교육부 및 대통령교육정책 자문위원회 근무 (행정고시 19회)
1986 미국 카톨릭대학교 전산학과 졸업
1988 미국 오리곤 주립대학교 전산학 석사
1992 고려대학교 전산과학과 이학박사
1992~현재 한국교원대학교 컴퓨터교육과 부교수
관심분야: 인공지능, 알고리즘, 원격교육, DB
E-Mail: seongkim@knue.ac.kr