공학석사 학위논문

IPS를 이용한 효율적인 학내전산망 구축에 관한 연구

2002년 8월

부경대학교 산업대학원

전 산 정 보 학 과

장 용 호

공학석사 학위논문

IPS를 이용한 효율적인 학내전산망 구축에 관한 연구

지도교수 김 창 수

이 논문을 공학석사 학위논문으로 제출함

2002년 8월

부경대학교 산업대학원

전 산 정 보 학 과

장 용 호

이 論文을 장용호의 工學碩士
學位論文으로 認准함

2002년 6월 22일

주 심 工學博士 김 영 봉 (印)

위 원 工學博士 박 승 섭 (印)

위 원 工學博士 김 창 수 (印)

목 차

표 차례

그림 차례

A Study on the Efficient Construction of School Network using IPS

Yong-Ho Jang

Dept. of Computer and Information Graduate School of Industry Pukyong National University

Abstract

As a national business of educational infomationalization aiming at transformation into an information-based society, construction of school network, its material foundation has been completed. While educational informationalization, abreast with internet, greets the turning point of high-tech educational environment, school networks have been the staple path of hacking, resulting that important inner-school data in elementary, middle school is exposed to illegal infringement. In addition, there are adverse side-effects of informationalization such as harmful, obscene, suicide, bomb sites, we suffered a great loss from them.

Therefore, it is necessary for us to devise a new security measure including the security policy-making, the enlargement of security equipment like a security server. And for the safety of school-network, the introduction of security equipments, IPS is becoming activated to prevent the information leakage and beforehand hacking accident. Especially by planning security equipment and measures for school-networks can maximize the safety of them.

We have to establish security policy-making training of security specialist and then he has to operate school networks using IPS.

We will guarantee the safety of school network and major information against hacking, infringement accident and adverse effect of informationalization and consequently maximize the use of educational information through internet.

Ⅰ. 서론

교육인적자원부에서는 90년대 후반부터 전국의 초·중·고등 학교를 대상으로 지식기반 사회를 구성하기 위한 일환으로 학교정보화 사업을 계속적으로 진행하고 있으며, 대부분의 중등학교에서는 교육자료 및 성적자료 등을 외부 해킹으로부터 보호하기 위해 방화벽을 구축하고 있다. 그러나 현재 구축된 방화벽만으로 안전한 학내 전산망 구축이 불가능하기 때문에 학교 전산망 혹은 서버 보안 시스템을 개발하고 있는 대부분의 보안 연구소 혹은 기업체들은 방화벽과 침입탐지시스템이 연계된 IPS(Intrusion Prevention System) 시스템 개발을 적극적으로 추진하고 있다.

이러한 관점에서 본 연구는 현재 구축되어 있는 중등학교의 방화벽 시스템이 기술적으로 또는 기능적으로 한계가 있기 때문에 이러한 문제점들을 분석하여 개선할 수 있는 방안을 제시한다. 이를 위해 본 논문에서는 현재의 방화벽 시스템이 가지는 장점과 확장 가능한 기능을 분석하여 향후 확장하고자 하는 IPS 시스템을 구축할 경우 경제적 혹은 기능적으로 개선할 수 있는 설계 방안을 제시하고자 한다.

현재 학교 전산망의 구축이 완료된 시점에서 초·중등학교에서 학내의 중요자료가 위조, 변조, 수정, 삭제 등의 침입사고가 일어나고 유해, 음란, 자살, 폭탄 사이트 등 정보화 역기능이 발생하고 있으며, 학교 전산망이 최근 해킹의 주요 경로가 되고 있어 학교 전산망 침해사고로 인해 유무형의 막대한 피해가 속출하고 있다. 그래서 보안정책의 수립이나 보안과 관련한 보안장비의 확충 등 보안대책이 강조되고 있다.

교육기반이 되는 학교 전산망이 방화벽만으로 구성되어진 현재 학교전산망의 취약점을 개선하고 침입방지 시스템과 같은 차세대 보안장비의 도입과 보안전문가를 양성함으로 보안대책과 보안정책을 수립함으로서 학교 전산망의 안전의 극대화가 기대될 수 있다.

본 논문에서는 이와 같은 교육기반인 학교 전산망을 보호함으로서, 초·중등학교에서의 교수·학습 분야의 정보화와 교무 업무 전산화를 실현함에 있어, 가장 기본적이고도 중요한 학교 전산망의 보안대책의 수립 및 차세대 보안장비를 이용한 학교 전산망의 보안 구축방안을 제안하고, 향후 다른 중등학교 교사들이 이와 같은 작업을 시행할 경우 좋은 연구 자료로 활용될 수 있도록 한다.

본 연구는 교육정보화의 물적 기반인 학내전산망의 안전과 보안을 위해 일선 고등학교를 대상으로 현장에서 경험한 자료와 최근 많은 연구들이 진행되고 있는 IPS

시스템과의 연동을 위한 효율적인 개선방안을 제시한다. 그리고 보안장비의 운영, 보안정책의 수립, 보안교육의 활성화, 보안인식의 제고를 확대하고 침해에 대응하기 위한 최대한의 방어정책은 인력양성이라고 볼 수 있다. 그래서 학내전산망을 효율적이고 안전하게 관리하기 위한 인력적 측면에서 보안을 전담할 수 있는 전문적인 보안전문가를 양성한다. 또한 침입기법의 다양화, 다변화, 자동화 등 해킹기술의 첨단화와 시스템 및 운영체제의 버그, 바이러스, 내부자에 의한 내부문서 불법유출과 시스템 침입, 학내 중요자료의 보안을 위해 차세대 보안장비로 각광받고 있는 IPS 시스템을 이용한 효율적인 학내전산망 구축에 관한 연구로서, 연구의 목적을 달성하기 위하여 수행하고자 하는 연구의 주요 내용 및 방법은 다음과 같다.

2장에서는 침입방지시스템의 개념과 구성 및 기능을 알아보고 국내·외의 시장분석과 기술에 관한 최근동향에 대해 살펴본다. 3장에서는 IPS의 구축모델의 제안과 학내전산망에서의 구축방법을 알아본다. 4장에서는 현재 학내전산망의 실정을 분석해보고 침입방지시스템의 도입과 활용에 대한 비교 및 분석 평가를 한다. 5장에서는 결론 및 향후 연구 방안을 제시하였다.

Ⅱ. 관련 연구

1. 침입방지시스템의 개요

1.1 정보보호시스템의 개요

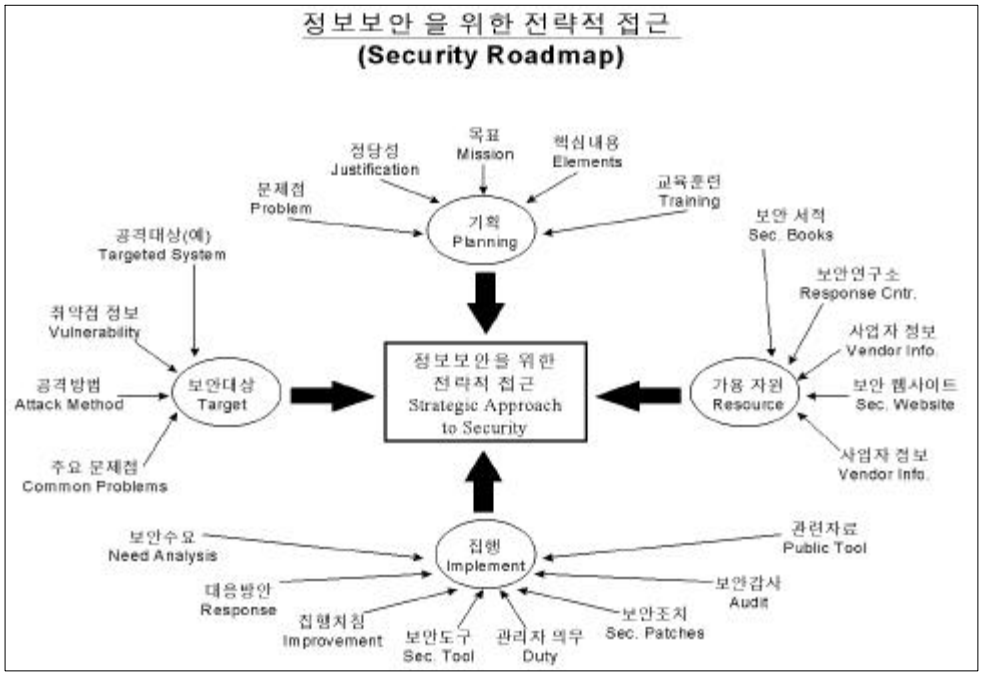
정보화와 같은 새로운 패러다임을 사회의 전반에 도입하는 과정에서는 예기치 못했던 문제점들이 나타날 수밖에 없다. 그 한 예가 정보화 역기능 현상이다. 현재 정보화 역기능 현상의 피해가 교육기관을 포함하여 우리 사회에 이미 심각한 문제를 불러일으키고 있으나, 이로 인해 야기되는 문제점들에 대한 우려만이 팽배할 뿐 실효성 있는 대응 방안이 미흡한 실정에 있다.

현재 학교에서 가장 심각한 정보화 역기능 현상은 <표1>과 같이 언어폭력(30%), 음란물의 유통(25.7%), 개인정보의 오·남용(16.6%), 컴퓨터 바이러스 유포(12.9%) 순으로 조사되었다[1].

< 표 1 > 현재 가장 심각한 역기능 현상에 관한 인식

구 분	교육정보부장	시·도교육청 전산담당자
음란물의 유통	90(25.7)	10(33.3)
컴퓨터 바이러스 유포	45(12.9)	2(6.7)
해킹	15(4.3)	2(6.7)
개인정보의 오·남용	58(16.6)	5(16.7)
지적재산권의 침해	17(4.9)	1(3.3)
통신사기 및 도박	5(1.4)	2(6.7)
사이버 매매춘	4(1.1)	
사이버 성폭력/스토킹	11(3.1)	1(3.3)
언어폭력	105(30.0)	7(23.3)

따라서 인터넷의 발전과 정보화 역기능의 방지를 위한 여러 가지 보안시스템 구축 방법이 연구되며 적용되고 있다.



[그림 1] 전략적 과정으로서의 정보보안

[그림1]과 같이 구체적인 정보보안정책 및 관리지침을 작성하기 위해서는 사전에 전략적이고 치밀한 기획(planning)이 선행되어야 하고 이를 바탕으로 효과적인 집행(implement)전략이 마련되어야 한다. 또한 보안대상(target)과 가용 자원(resource)에 대한 검토는 기획과 집행을 효율적이고 효과적이게 하기 위해 고려하여야 할 조건이다 [38].

보안의 정의를 살펴보면 재난, 실수 및 부정한 조작으로부터 정보, 시스템 및 서비스를 보호하여 보안 사고의 가능성과 영향을 최소화하는 것을 의미한다. <표2>와 같이 정보 보호는 정보의 비밀성, 무결성, 가용성 등을 보장하는 것으로 내부 또는 외부의 침입자들로 인한 정보의 파괴, 변조, 불법 유출 등 범죄 행위로부터 정보를 보호하고, 건전한 정보 유통 질서 확립과 정보의 부정적인 측면을 예방. 방지하는 것을 목표로 한다.

< 표 2 > 보안의 3가지 구조

구 분	내 용
비밀성(Secrecy)	정보의 소유자가 원하는 대로 정보의 비밀이 유지되어야 한다는 원칙
무결성(Integrity)	정당한 방법으로 권한이 주어진 사용자에게 정보서비스를 거부하여서는 안 된다는 원칙
가용성(Availability)	비 인가된 자에 의한 정보의 변경, 삭제 생성 등으로부터 보호하여 정보의 정확성, 완전성이 보장되어야 한다는 원칙

정보보호의 필요성은 정상적인 정보의 기능유지 측면에서 정보는 고유한 사용목적과 기능을 유지해야하고 필요한 장소, 사람, 시점에 정확히 전달되어야 한다.

자산의 보호 측면에서 정보는 정보와 관련된 모든 자산, H/W, S/W, 데이터 등의 손실과 왜곡으로 막대한 재정적인 손실을 가져올 수 있으므로 정상적인 통신망 운영과 재산권을 보호해야 한다. 그리고 통신망의 확대와 컴퓨터의 보급으로 정보의 집중화를 가져왔고, 정보 수집과 이용이 활성화, 다양화 되어감에 따라, 개인정보의 보호를 위해서 필요하다. 또한 기업이나 조직의 안전에 관한 측면에서 정보 통신망을 이용한 비밀정보의 유출, 파괴, 훼손으로 기업 조직의 안전 보장을 위해서 필요하다.

정보보안 시스템의 운영과 관리는 시스템을 구축하는 것보다 훨씬 어려운 문제가 많이 산재하고 있다. 현재 학교 전산망에서는 보안장비의 부재와 이를 관리하고 운영할 수 있는 보안전문가의 부재로 인한 생활기록부의 위·변조와 개인신상정보의 유출과 같은 보안에 취약성을 가지고 있으며, 날로 복잡해지고 다양화되어 가는 해킹기술과 악의적인 바이러스와 같은 침해사고가 자주 일어나고 있다. 이를 방어하기 위한 새로운 기법의 적용과 보안장비의 확충을 위한 경제적, 기술적, 관리적, 전문인력의 확보 등 산재한 문제를 가지고 있는 실정이다.

1.2 침입방지시스템의 정의 및 현황

침입방지 시스템(IPS : Intrusion Prevention System)은 공격에 대한 탐지만을 하

는 침입탐지 시스템의 한계성을 뛰어넘는 보안시스템이다. 그리고 IPS는 공격 시그니처를 찾아내 네트워크에 연결된 기기에서 수상한 활동이 이뤄지는지를 감시하며, 자동으로 모종의 조치를 취함으로써 그것을 중단시키는 보안 솔루션이다. 이것은 단순한 네트워크 단에서의 탐지가 제공하지 못하는 각종 서버를 위해 알려지지 않은 공격까지도 방어할 수 있는 실시간 침입방지 시스템으로 OS 레벨에서 실시간 방어와 탐지 기능을 제공한다. 따라서 <표3>과 같이 기존 보안장비가 가지는 수동적인 방어 개념의 방화벽이나 침입탐지 시스템과 달리 침입유도 시스템(허니팟)이 지닌 지능적인 기능과 적극적으로 자동 대처하는 능동적인 기능이 합쳐진 개념의 보안 솔루션으로 코드레드, 웜 발생시 무용지물이 된 기존 솔루션(방화벽, IDS등)의 대안으로 떠오르고 있는 차세대 보안 솔루션이다[4 9].

< 표 3 > 기존보안장비와 보안방식의 비교

보안장비	방화벽	네트워크침입탐지시스템	서버침입탐지시스템
제어방식	패킷의 헤더정보에 의한 제어	패킷의 헤더정보와 내용검색을 통한 침입탐지 및 차단	패킷검사 및 서버에서의 프로세스 검사를 통한 침입탐지 및 차단
보안방식	규칙(Rules)	패턴인식(pattern)	응용방식(API)
위험성	높다	보통	낮다
대응방식	수동적	수동적	수동적

방화벽(Firewall)이나 침입탐지시스템(IDS)같은 기존 보안제품의 문제점으로 최근에 발생한 무단 해킹 유형을 분석해 보면 기존 보안 솔루션이 더 이상 시스템이나 서버를 완벽하게 보호해 주지 못하고 있다. 그리고 님다, 코드레드 등 네트워크에서 동작하는 보안 시스템을 피해 서버로의 공격을 시도할 수 있는 기법이 개발되고 있으며 앞으로는 이러한 기반 위에서 기존 보안 제품을 우회하여 서버를 공격하는 해킹 수법이나 웜 바이러스가 계속해서 증가할 것으로 보인다. 이런 현실 속에서 새롭게 떠오르고 있는 것이 바로 서버 보안이다. 이 중에서도 실시간으로 진행되고 있는 공격을 막아내는 IPS 기술이 부각되고 있다. 이러한 이유는 기존 보안 시스템인 방화벽은 단순 차단 기능, 이미 알려진 공격 패턴을 기반으로 공격 감지시 관리자에게 알려주는 기능을 제공해 님다나 코드레드 같은 새로운 공격을 막아내는 데는 역부족이다. 그래서 실시간 공격 방어 기능을 제공하는 IPS는 IDS와 비슷한 기능을 가지고 있는 것처럼 보이지만 IDS가 공격에 대해 즉각 대응하지 못하는데 비해 IPS는 수상한 활

동을 감시하다가 서버에서 비정상적인 행동을 실행하고자 하면 그 즉시 중지시켜 버린다. 그리고 침입방지시스템의 특징과 장점을 살펴보면 <표4>와 같다[5, 6, 9].

IPS의 기존 보안제품에 대한 차별성은 사후 대응이 아닌 사전대응, 관리와 설치의 편이성, 설치와 동시에 사용 가능, customizing 기능, Exceptions, Security Levels, Policies 설정 변경, 서버 보호를 제공하는 다단계 디자인, 위험한 공격을 막아내기 위한 한가지 이상의 방법, 적용하기 쉽고 관리하기 쉬워서 보안전문가가 될 필요 없음 등을 들 수 있겠다. 방화벽이나 침입탐지시스템과 같은 수동적인 보안 시스템에 학내의 중요정보와 개인 신상정보, 성적 자료 등을 맡기고, 도저히 알 수 없는 로그만을 쌓아 둔 채 신종 해킹수법에는 무방비로 노출되어있다. 또한 향후 해킹 및 방어는 더 이상 시스템 마비나 웹서비스의 신상정보를 유출하는 행동에서 멈추지 않고 더 진화되고, 좀 더 지능적이며 무차별적인 공격을 할 것이다[4, 5, 9].

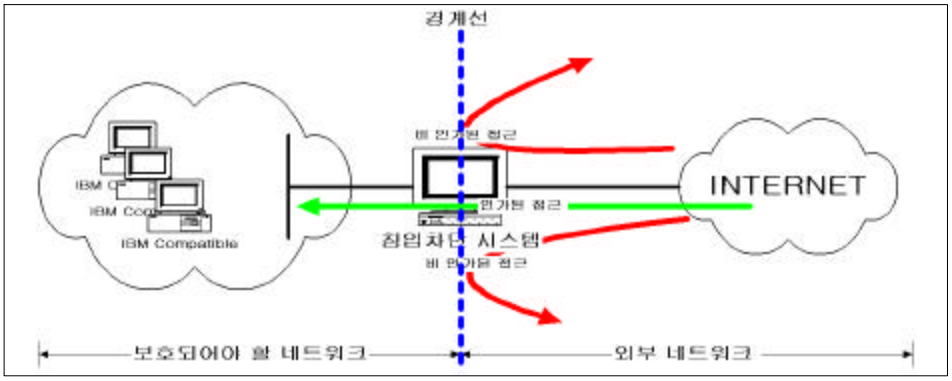
< 표 4 > 침입방지시스템의 특징과 장점

특 징	장 점
- 손실이 발생하기 전에 대응 - 독립된 에이전트 - 시스템 리소스에 접근방지 - 보안 이벤트는 E-메일, 페이저, 자식프로세스의 형태로 발생 - SNMP트랩 데이터 이용 가능 - 콘솔 당 1000개의 agent 이용 - 기존의 보안 인프라 구조 보충 - 로그정보 export기능 - 관리 보고기능을 갖춤	- 서버의 동작 가능 시간을 보장 - 시스템의 노출 방지 - 방화벽 이면의 보호 기능 제공 - 보안기술에 필요한 시간 제거 - 꾸준히 모니터링 할 필요가 없음 - 자동 업데이트 메커니즘 - 능동적인 보안 - false positive 의 감소

1.3 침입차단시스템(FireWall)의 개요와 문제점

침입차단 시스템은 내부에서 외부로 또는 외부에서 내부로 전송되는 모든 트래픽은 반드시 이를 통과해야하고 반드시 정의되고 허가된 트래픽만 통과시킨다. 또한 – 시스템 자체는 침투에 대하여 저항력을 보유해야 한다[11].

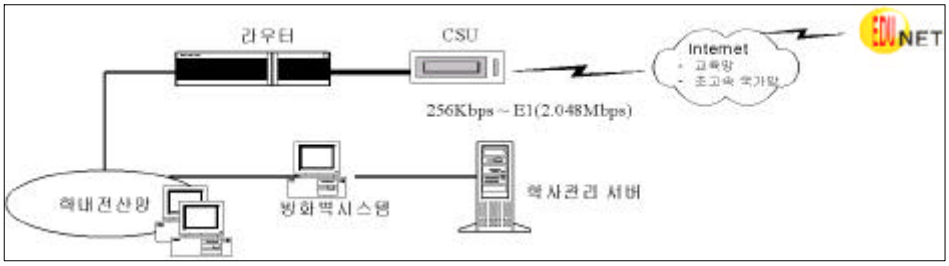
침입차단 시스템의 주목적은 [그림2]와 같이 보호된 망으로 또는 망으로부터의 접근을 제어하는 것이며, 침입차단 시스템을 통한 접근으로 망 접근 정책을 구현함으로써 평가될 수 있다[12, 17, 18, 19].



[그림 2] 방화벽의 구조

방화벽의 구축 개요는 모든 초·중등학교에 학내전산망이 구축 완료됨에 따라 교내 및 교외에서 수집한 각종 교수·학습자료를 교사와 학생이 자유롭게 공유할 수 있는 서버를 지원하고 교내의 중요자료를 외부로부터 보호 및 학생들의 유해정보접근을 차단하기 위한 보안프로그램을 지원하기 위해서이다[14, 17, 18, 19].

그래서 [그림3]과 같이 학내 전산망이 외부망과 접속 모델의 구성 요소는 백본 스위치에 접속하는 라우터, 채널 서비스 유니트 등이며, 학사관리서버가 설치될 경우 방화벽 시스템이 추가될 수 있다[14].



[그림 3] 외부망 접속시의 방화벽 구축모델

지난 몇 년간 방화벽은 보안 시스템 구축에 있어 필수적인 사항이며 이것으로 모든 보안시스템은 구축되는 것으로 생각되었다. 그러나, 방화벽을 설치하였다고 해서 모든 보안시스템이 완료되는 것은 아니다. 제대로 설정된 방화벽일지라도 시스템 자체의 문제는 가지고 있다. <표5>에서 방화벽이 필요한 이유에 대해 설명하고 방화벽이 가지는 문제점들에 대해 보여주고 있다[11,12,15,16,19].

< 표 5 > 방화벽의 필요성과 문제점

필요성	문제점
· 위협요소의 증가 및 현실화 · 네트워크에서 효율적인 보안정책의 실현필요 · 보안 노력을 한 곳에 집중 · 프라이버시 보호 · 서비스의 취약점 보호 · 보안 기능의 집중화	· 모든 보안 문제의 해결 방법은 아님 · 제공되는 서비스의 제한 · 보안 기능의 집중화에 따른 역기능 · 내부 사용자에 대한 보안 침해 등

이러한 문제점에도 불구하고 학교 전산망에서 가장 기본적인 보안의 형태는 방화벽이라 할 수 있다. <표6>과 같이 방화벽 시스템을 구현하는 것이 네트워크 보안을 충분히 보장해 준다고는 볼 수 없으나 가장 효과적이고 비용이 저렴하게드는 방법이라고 볼 수 있다[11, 17, 19].

< 표 6 > 패킷필터링의 장/단점

장점	단점
유연성, 고속, 저가격	- 승인 시 모든 내부 네트워크 접근 가능 - 사용자 인증 불가 , 미약한 로깅 - 세그먼트의 수가 많을수록 복잡 / 성능저하

침입차단 시스템은 구현된 방식에 따라 <표7>과 같이 패킷필터링 게이트웨이, 써킷 게이트웨이, 어플리케이션 프록시 게이트웨이, 하이브리드 방식 등으로 나뉘어진다. 패킷필터링은 네트워크 계층에서 패킷을 구분하여 차단하는 기본적인 방식이다. 어플리케이션 프록시 게이트웨이는 응용계층에서 프록시 설정을 통하여 침입을 차단하는 방식이다[11, 12, 15].

<표 7> 방화벽의 종류 및 특징

방화벽의종류	기 능	장 점	단 점
패킷필터	소스 및 목적지 IP주소와Port번호를 이용하여 제어한다	단순하며 처리속도가 빠르다	단순해서 사용자별로 제어 못함
서킷방식	패킷필터링과 비슷하지만 OSI의 다른 레벨에서 서킷을 만들어 동작	소스를 감출 수 있고 단순하면서 사용자에게 투명성을 보장	각 클라이언트 측의 프로그램을 수정해야 한다.
응용방식	소스를 감출 수 있으며 단순하면서 사용자에게 투명성을 보장한다.	강력한 인증 및 부가적인 서비스제공	투명성을 보장 못함
하이브리드	위의 3가지 타입들을 경우에 따라 조합적으로 사용하는 것	보안상 가장 효율적이고, 유연성 있는 보안정책을 부여가능	구축의 어려움

침입차단 시스템의 사례를 살펴보면 패킷 필터링 시스템은 작고 단순한 사이트에서 가장 일반적이고 쉽게 도입할 수 있는 것이지만, 몇 가지 단점 때문에 다른 침입차단 시스템보다 덜 선호되고 있다. 패킷 필터링 침입차단 시스템의 단점은 기록 능력이 거의 또는 전혀 없어서 관리자는 라우터가 위태로운 상태인지 공격당하고 있는지 쉽게 결정할 수 없고, 패킷 필터링 규칙을 철저히 시험하기 어렵기 때문에 사이트를 시험되지 않은 취약성에 노출시킬 수 있고, 복잡한 필터링 규칙이 필요할 경우 관리를 못하게 될 수도 있다. 이중-제어 게이트웨이 시스템은 패킷 필터링 라우터 침입차단 시스템보다 좀 나은 시스템으로, 두개의 망 인터페이스를 가진 호스트로 구성되어 있으며, 추가적인 보호를 위해 패킷 필터링 라우터를 설치할 수도 있다. 패킷 필터링 침입차단 시스템과는 달리, 이중-제어 게이트웨이는 인터넷과 보호 중인 사이트의 인터페이스를 필요로 하며 프락시 서비스는 사이트 시스템으로 프락시가 있는 TELNET, FTP 간의 IP 트래픽을 완전히 차단하고, 서비스와 접근은 게이트웨이의 프락시 서버가 제공하는 매우 보안성이 있으면서도 단순한 침입차단 시스템이다.

방어용 호스트 시스템은 이중-제어 시스템보다 융통성 있는 침입차단시스템이지만 약간의 보안을 희생해야 하므로, 이중-제어 게이트웨이 침입차단 시스템보다 더 융통

성을 필요로 하는 사이트에 적합하다. 방어용 호스트 시스템은 보호중인 서브넷 쪽에 위치한 어플리케이션 게이트웨이와 패킷 필터링 라우터를 결합하고 있는데, 어플리케이션 게이트웨이는 단지 하나의 망 인터페이스를 필요로 하며 프락시 서비스는 사이트 시스템으로 프락시가 있는 TELNET, FTP 및 기타 서비스를 통과시킨다.

방어용 서브넷 시스템은 이중-제어 게이트웨이와 방어용 호스트 시스템의 변형으로, 분리된 시스템 상에 침입차단 시스템의 각 구성 요소를 위치시켜 사용할 수 있으며, 비록 복잡하기는 해도 막대한 처리량과 융통성을 얻을 수 있다.

방어용 서브넷 침입차단 시스템은 트래픽량이 많은 사이트나 매우 빠른 트래픽을 필요로 하는 사이트에 더 적절하다. 또한 모뎀 풀과 침입차단 시스템 통합사례를 살펴보면 많은 사이트들이 사이트의 다양한 지점에 위치한 모뎀과의 다이얼인 접근을 허용하고 있는데, 이것은 잠재적인 뒷문이며 침입차단 시스템에 의해 제공되는 모든 보호를 무력화시킬 수 있다. 그래서 현재 모뎀을 다루는 가장 좋은 방법은 그것들을 모뎀 풀에 집중화시키고 그 풀로부터의 접근을 제어하는 것이다. 그리고 모뎀 풀은 단말 서버에 접근한 모뎀들로 구성되는데, 다이얼인 이용자는 단말 서버에 접근하고 거기에서부터 다른 호스트 시스템으로 접근한다.

어플리케이션 게이트웨이의 진보된 인증 도구는 모뎀뿐 아니라 인터넷으로부터 접근하는 이용자를 인증하기 위해 사용될 수 있으며, 패킷 필터링 라우터는 모뎀 풀로의 직접 접근으로부터 내부 시스템을 막는데 이용될 수 있다[11, 12, 15, 17].

1.4 침입탐지시스템(IDS)의 개요와 문제점

침입에 대한 기본 개념은 1980년에 Anderson이 비 인가된 정보로의 접근 및 정보 조작, 그리고 시스템 무기력화에 대한 고의적이면서도 불법적인 시도의 잠재 가능성이라고 규정하였다. 그 후 1987년 Denning은 침입탐지 시스템을 허가되지 않은 사용자로부터 접속, 정보의 조작, 오용, 그리고 남용 등 컴퓨터 시스템 또는 네트워크 상에서 시도됐거나 진행중인 불법적인 예방에 실패한 경우 취할 수 있는 방법으로서 의심스러운 행위를 감시하여 가능한 침입자를 조기에 발견하고 실시간 처리를 목적으로 하는 시스템으로 정의하고 있다.

침입탐지 시스템은 방화벽과 함께 활용되는 네트워크 보안 솔루션을 말한다. 그리고 침입탐지시스템은 인터넷 등 외부 망과의 접속 시 일정 요건을 갖추지 않은 사람의 침입을 사전에 방지하기 위해서 각종 해킹수법을 이미 자체적으로 내장, 침입행동

을 실시간으로 감지·제어할 수 있는 기능을 제공한다. 따라서, 침입 탐지 시스템이 방화벽에 이은 차세대 보안 솔루션으로 부각되며, 이것은 방화벽은 해킹 됐을 경우 이에 따른 피해를 최소화하고 네트워크 관리자 부재 시에도 시스템 자체적으로도 해킹 등에 대응할 수 있는 보안 솔루션에 대한 요구가 늘고 있는 상황에서, 침입탐지시스템이 이 같은 요구를 해결할 수 있는 솔루션이기 때문이다[37].

방화벽은 인터넷의 접속점에 위치하여 사내망으로 오가는 모든 트래픽을 감당해야 하는 만큼 그 성능상의 제한으로 인해 트래픽에 대한 많은 분석을 하기는 어렵다. 또한 내부의 침투자에 의한 컴퓨터/네트웍 자원에 대한 보호에 있어서는 전혀 역할을 할 수가 없다. 이러한 방화벽의 부족한 부분을 보강해줄 수 있는 것으로 침입탐지시스템이 있다[20].

침입탐지시스템의 기본개념은 침입 의도를 가지고 비 인가된 정보로의 접근 및 정보 조작 그리고 시스템의 무기력화에 대한 고의적 시도에 대한 모든 가능성을 탐지하는 행위를 의미하며 시스템에 불법적으로 접속하여 시스템을 사용, 오용, 남용하는 것을 감지하여 문제점을 처리하는 시스템을 말한다[21, 22]. 침입방지시스템(IPS) 구현에 대한 필요성과 의문은 <표8>에서 침입탐지 시스템의 필요성과 문제점에 대해 살펴보아야 한다.

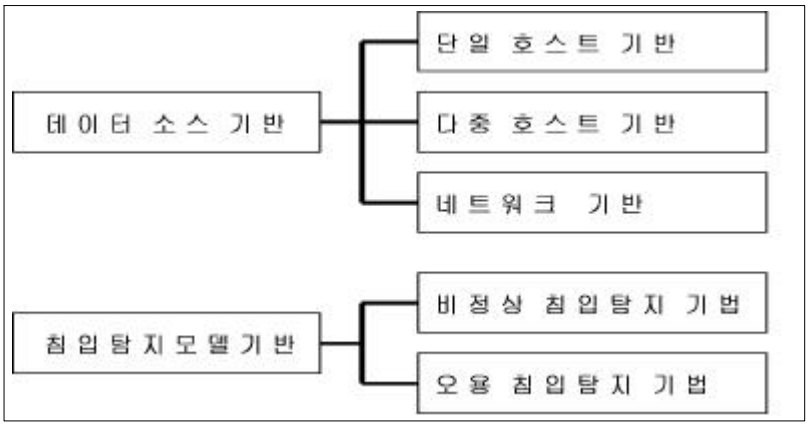
< 표 8 > 침입탐지시스템의 필요성과 문제점

필요성	문제점
- 시스템은 잠재적으로 많은 취약점을 가지고 있지만, 기술적 경제적 요인으로 공격자에 대처하지 못함 - 높은 비용과 이미 사용중인 응용 프로그램 때문에 안전한 시스템을 만들기가 현실적으로 어려움 - 완벽하게 안전한 시스템을 개발하는 것은 거의 불가능 - 보호 시스템 조차도 내부 취약점을 가질 수도 있음	- 알려지지 않은 공격에 대한 탐지 - 내부 공격자에 대한 탐지 - 분석을 위해 생성된 많은 양의 데이터에 대한 처리 문제 - 침입 행위에 대한 정확한 판정 - 침입에 대한 대응 - 성능저하(100MB 이더넷) - 침입 탐지의 오판에 따른 사람, 시간, 재정적인 낭비문제 - 식별 및 인증 기능 - 다른 보안 제품과의 확장성

침입탐지 시스템은 과거 단순히 접근 제어 기능만을 수행하는 수동적인 시스템이었으나, 점차 침입 패턴을 데이터베이스화하고 전문가 시스템을 접목시켜 네트워크나 시스템 사용을 실시간으로 모니터링 하여 의심스러운 침입을 조기에 발견하고 처리하는 것을 목적으로 하는 시스템이다.

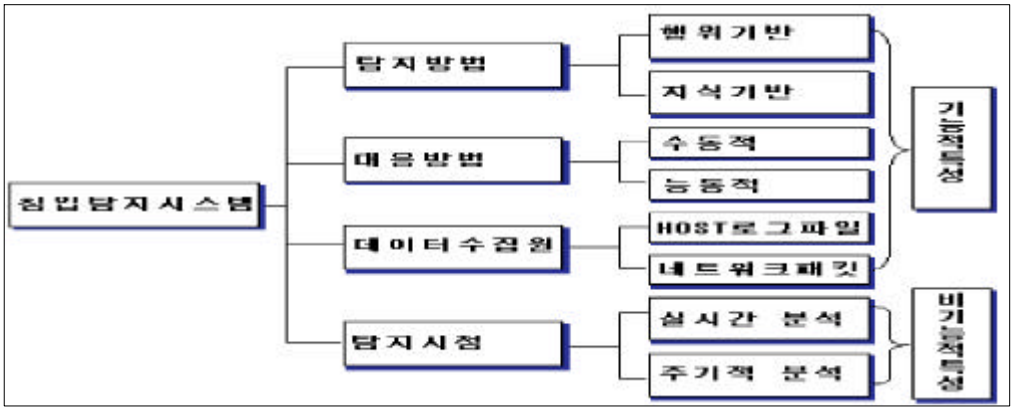
방화벽과 같은 침입차단시스템만으로는 안전하지 않다는 보안 의식 고취에 따라, 침입탐지시스템이 침입차단시스템에 이은 차세대 보안 솔루션으로 부각되고 있다. 그래서 침입탐지시스템은 네트워크 관리자를 대신하여 시스템 자체적으로 해킹에 대응하고, 침입차단 시스템이 해킹 되었을 경우 피해를 줄일 수 있는 솔루션이기 때문에 사이버 금융 및 전자상거래를 위한 서버 보호에 머물지 않고 일반화되는 추세이다 [24].

침입탐지시스템은 외부침입자뿐만 아니라 내부 사용자의 불법적인 사용, 남용, 오용행위를 탐지하는데 그 목적이 있는데, 미국 COAST의 분류에 따르면 [그림4]와 같이 데이터의 소스를 기반으로 하는 분류 방법과 침입의 모델을 기반으로 하는 분류 방법이 있다.



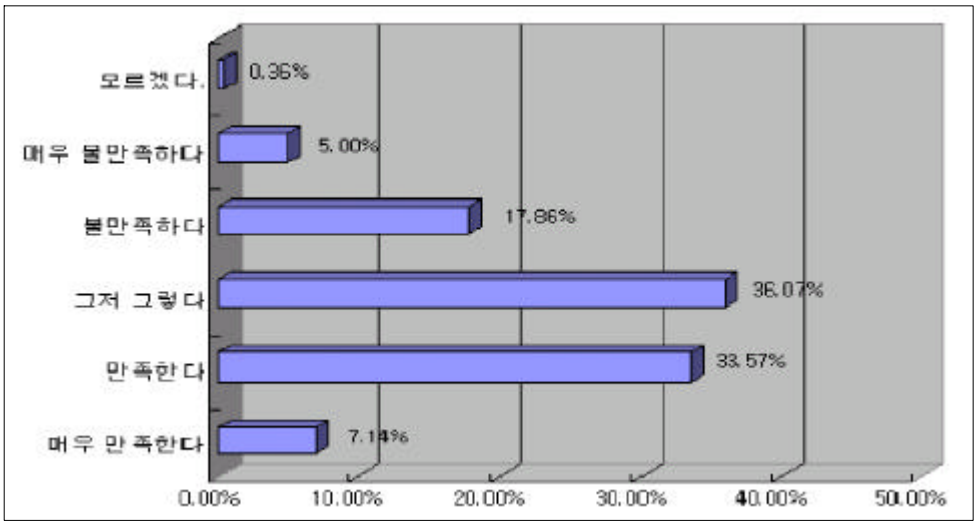
[그림 4] 침입탐지시스템의 분류

또 다른 분류방법으로는 [그림5]와 같이 IBM Zurich Research Lab의 분류가 있는데 여기서는 침입탐지시스템의 기능적 특성과 비 기능적 특성으로 분류하고 있으며, 기능적 특성으로는 침입탐지 방법, 침입탐지시 대응, 감사데이터의 수집 위치에 따라 분류하고 있고, 비기능적 특성으로는 모니터링 수행 빈도에 따라 분류하고 있다.



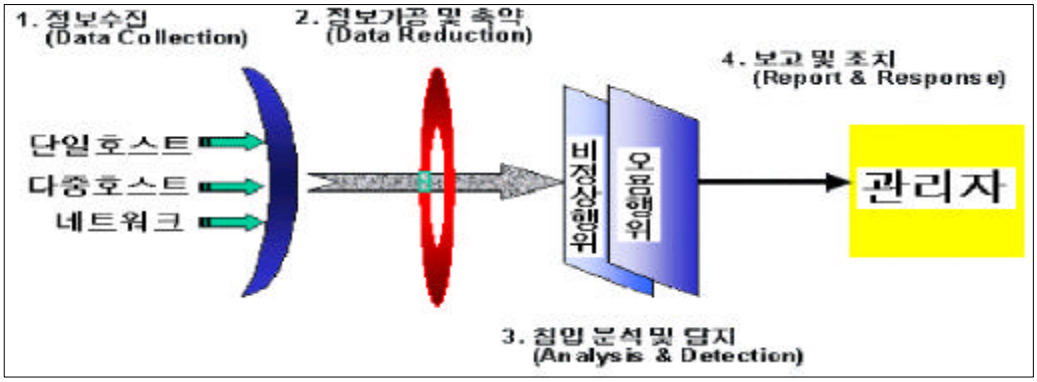
[그림 5] IBM Zurich Research Lab의 분류

침입탐지시스템에 대한 만족도는 [그림6]에서와 같이 40%가 만족하고, 36%는 그저 그렇다, 그 외 24%가 만족하지 못한다는 결론을 유추할 수 있다. 이것은 침입탐지시스템이 취약한 식별 및 인증 메카니즘과 알려지지 않은 공격에 대한 탐지 등의 문제점을 가지고 있기 때문으로 인식된다[38].



[그림 6] 침입탐지시스템의 만족도

침입탐지시스템의 기술적 구성요소는 [그림7]과 같이 정보수집, 정보가공 및 축약, 침입분석 및 탐지, 보고 및 조치단계의 4단계로 나눌 수 있다[22, 23].



[그림 7] 침입탐지시스템의 구성요소

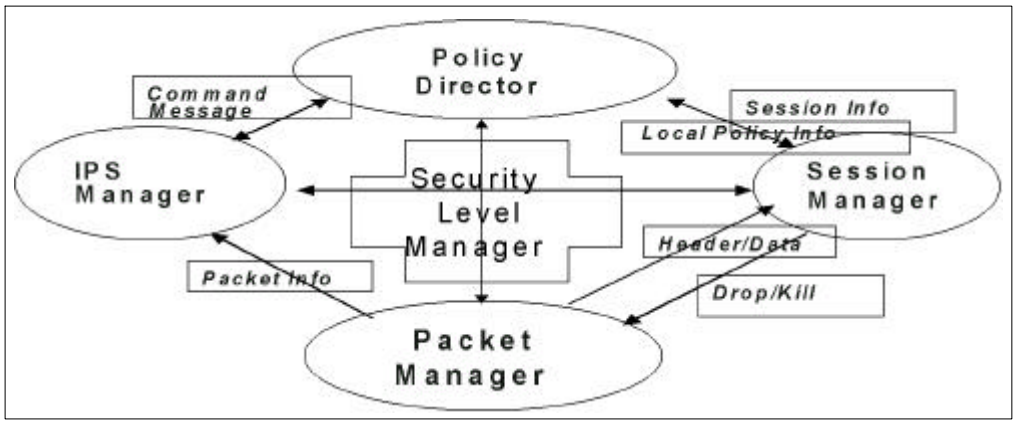
정보 수집은 호스트 로그정보와 멀티호스트간 로그정보, 그리고 네트워크 패킷정보 수집으로 나눌 수 있는데 그 중 호스트 로그정보 수집은 호스트의 운영체제에서 제공하는 각종 로깅기능을 이용하여 수집한다. 이 단계에서는 시스템의 모든 정보를 수집하여 다음 단계인 정보 가공 및 축약단계로 넘기는 기능을 수행한다. 정보가공 및 축약 기술은 원시의 데이터로부터 의미 있는 정보로 가공하는 기술을 말하는데 이 기술은 실시간 침입판정을 위한 최소한의 정보를 의미해야 하며 자체의 감사 레코드로서의 의미를 갖는다. 가공 및 축약 기술로서는 침입탐지 전문가 시스템의 기본 모델에서 사용하는 레코드 형식을 사용하는 방법과 ASAX의 NADF을 사용하는 방법이다. 분석 및 침입탐지단계는 침입여부를 판정하는 단계로 침입탐지시스템의 핵심 기술이다. 보고 및 조치단계에서 위 두 과정을 수행하고 이용하여 침입으로 판단되어지면 관리자에게 보고하고 관리자는 조치해야 한다[23].

일반적으로 네트워크 기반 침입탐지 시스템은 실시간으로 네트워크를 모니터링하고 사용자가 정의한 보안정책을 적용하여 불법적인 침입에 대응할 수 있지만, 실시간으로 패킷을 분석하기 위한 처리 능력과 저장의 한계를 극복해야 하고, 네트워크 트래픽 증가에 따른 별도의 H/W 및 S/W가 필요하다. 호스트 기반 침입탐지 시스템은 별도의 H/W없이 시스템을 감시할 수는 있지만, 서버마다 S/W를 설치해야 하고, 서버의 리소스 부하를 증가시켜 성능 저하를 가져올 수 있는 단점이 있다[20].

2. 침입방지시스템의 구성

2.1 침입방지시스템의 일반 모델과 수행과정

침입방지시스템의 기본적인 구조를 살펴봄으로써 침입방지시스템이 어떻게 수행되는지 알 수 있고 그 수행과정을 이해할 수 있다. 이러한 침입방지시스템의 보안모듈의 구성은 [그림8]과 같이 패킷관리, 세션관리, IPS관리, 정책관리의 4단계로 구성되어 있다[4].



[그림 8] 침입방지시스템의 보안모듈

Packet•Manager는 입·출력되는 서비스 패킷을 프로토콜 단위로 분리하여 각각의 FW/IDS manager에 정상여부를 판단하고 한번 분류된 패킷은 DB에서 관리하고, 각각의 Manager Process의 상태 파악 및 생성을 감독하고 갭슐 트래픽 아날라이져로부터 정상패킷 정보를 받아서 세션메니져에 전송한다. Session Manager의 역할은 단계별로 SLM정책에 유배되는 세션들에 통과 및 종료 여부에 대한 권한과 룰을 가지고 IPS 메니져와 통신하고 IPS DB에 정상세션만을 생성한다. 정책관리자에서 부여받은 로컬/루트 정책에 대한 실행 및 제어 기능을 가지고 해당 프로세스에 대한 fork/drop 메니져 기능을 제어한다.

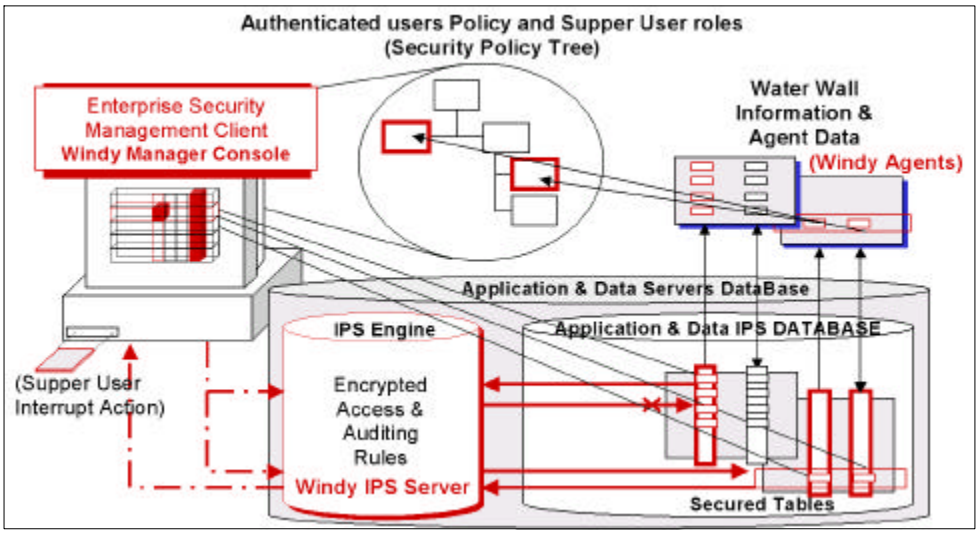
IPS Manager 슈퍼 유저가 관리하는 정상 정책 및 비정상 정책에 따라 패킷과 세션에 대한 정보와 기록을 개별 프로세스에게 전달하고 단계별 모듈 프로세스에서

수집된 침입 탐지와 제거 정보가 IPS DB에서 선택되어 커널에 전달한다. Policy Director는 SKM과 SLM에 등록할 수 있는 관리자별 정책편집기가 슈퍼유저관리 모듈에 지배를 받고 한번 위배된 정책에 대한 감사 기능을 가지고 침입에 대한 정책에 대응한 패킷이나 세션에 대한 새로운 신규 정책을 만들 리스트를 제공한다.

침입탐지시스템 데이터 레벨의 처리과정은 [그림9]와 같이 정상트래픽을 추출하여 캡슐화와 재포멧, 정형화 과정을 거쳐서 정상패킷만을 처리하고 정상패킷에서 정형화된 자료만을 DB화 한다[4].

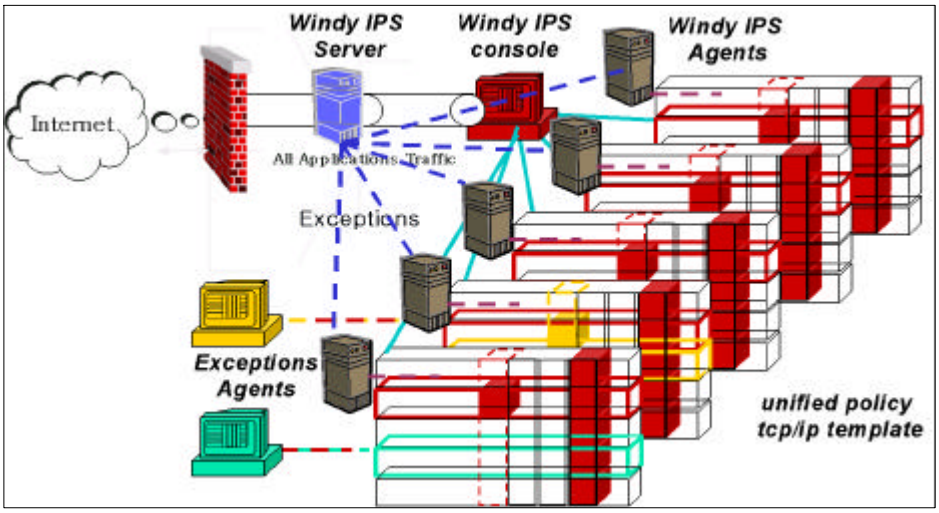
[그림 9] 데이터 레벨의 처리과정

침입방지 시스템의 일반적인 수행과정은 허용된 데이터와 허용된 어플리케이션만 통과시킨다. 이러한 침입방지시스템의 구성형태는 [그림10]과 같이 에이전트 영역의 정상 패킷만을 통과 시킨다[4].



[그림 10] 에이전트 영역의 정상 패킷만 통과

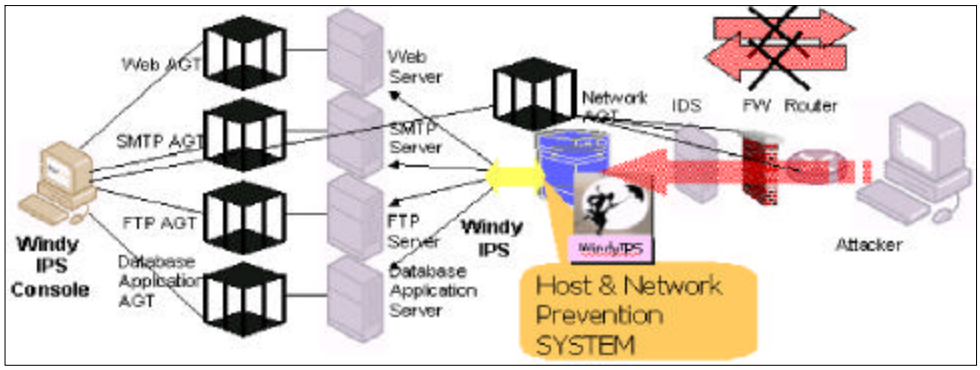
[그림11]과 같이 정상패킷에서 정형화된 패킷만을 DB 화함으로서 네트워크 전체의 신뢰성 있는 자료를 정형화시킨다.



[그림 11] 정상 패킷에서 정형화된 패킷만을 DB화

2.2 WINDY IPS의 기능과 종류

윈디시큐리티쿠퍼스의 침입방지 시스템은 [그림12]와 같이 보호받을 영역의 해당 시스템(Server & Network)에 IPS 에이전트가 초기 구축시 자동으로 탑재되어 해당 시스템의 자원 정보를 WaterWall과 통신하고 있으면서 방화벽과 침입탐지시스템을 통과하고 들어오는 모든 비정상 패킷에 대하여 IPS의 Session Kill Manager에 의해 침입 공격을 방지한다. 이때 비정상적인 공격에 대하여 해당 세션을 Drop 하는 것이 아니라 해당 Session을 완벽히 제거함으로써 네트워크 트래픽의 과부하에서 완전히 벗어날 수 있다[4].



[그림 12] 윈디 IPS 기능

보안 시스템에서 처리하지 못한 해킹 공격이나 내부자에 의한 백도어 공격을 방지할 수 있도록 IPS DataBase에 등록되어 있지 않은 모든 데이터와 어플리케이션의 내외부 출입을 완전 통제하므로 내부 중요정보의 유출을 원천적으로 봉쇄한다.

침입방지시스템의 각 보안장비와 네트웍 인터페이스의 제공형태는 <표9>와 같이 각각의 보안장비와 네트워크의 인터페이스를 제공한다.

< 표 9 > 인터페이스 제공 형태

구성		고객	인터넷	FW/IDS	IPS	응용서버	DB/Client
영역		고객망	인터넷	침입차단/탐지	침입방지	DMZ	내부망
보안요소	기술적	사용자ID 패스워드 인증키 암호화 최신패치 백신 개인방화벽	암호화 SSL SET VPN	OS보안 (ID,PASSWD, SHARE,..) 보안 규칙 침입패턴 OS기본보안 암호화	자원별접근제어 침입경보 침입감사 통합관리 로그분석 자료유출방지 SMS,NMS,NAT	응용보안 DB보안 백도어존재파악 홀스캔점검 버그패치 시스템최적화 자원별접근제어 응용서비스제어 침입로그분석	DB사용자인증 자원별접근제어 공유파일암호화 침입로그분석 중요정보목록감사 권한관리 자원관리
	관리적	개인정보 보호정책	Cert 자문	변경관리 로그분석 규칙정책 보안관리지침	최신패치적용 ID,패스워드관리 변경관리준수 운영지침준수 침입로그분석 응용서비스분석	최신패치적용 ID, 패스워드관리 변경관리준수 운영지침준수 ISMS체계준수	DATA분류체계수 립 및 준수 최신패치적용 ID,패스워드관리 변경관리 운영지침준수

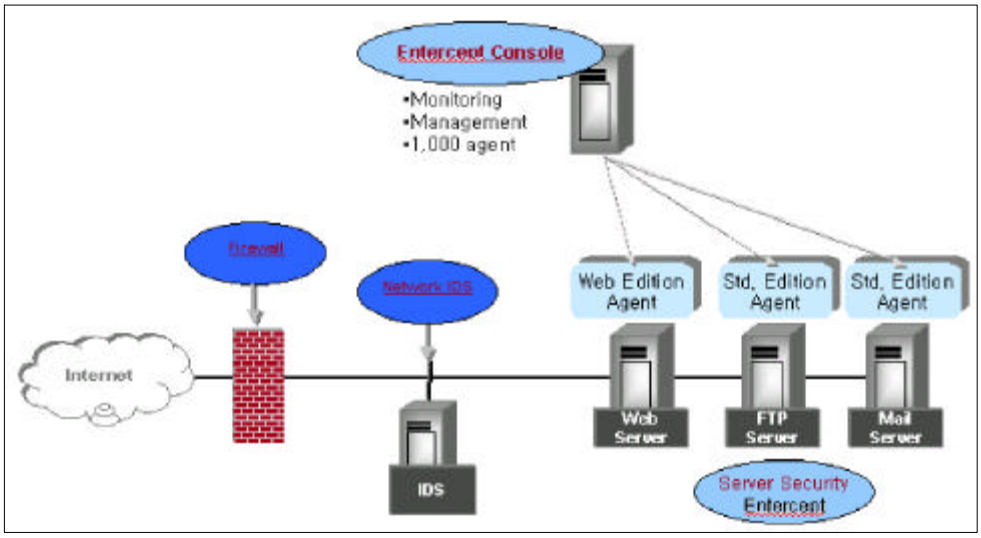
윈디시큐리티쿠퍼스의 침입방지시스템의 제품 현황을 살펴보면 <표10>과 같이 구성되어 있다.

< 표 10 > 윈디시큐리티쿠퍼스 IPS제품 현황

	Security Manager	CA Unicenter	BMC ControlSA	leapfrog opportunity
ease of use	difficult	difficult	easy	sure
ease of deployment	moderate	difficult	moderate	difficult
platforms	OS	OS(2set)	OS&Appl	Easy to add
workflow	some	no	yes	yes
web-base	no	no	yes	yes
self-case	no	no	no	yes
toolkit	script	script	yes	yes
reporting	preview	-	yes	integrated
integration	some	some	some	

2.3 ENTERCEPT IPS의 기능과 종류

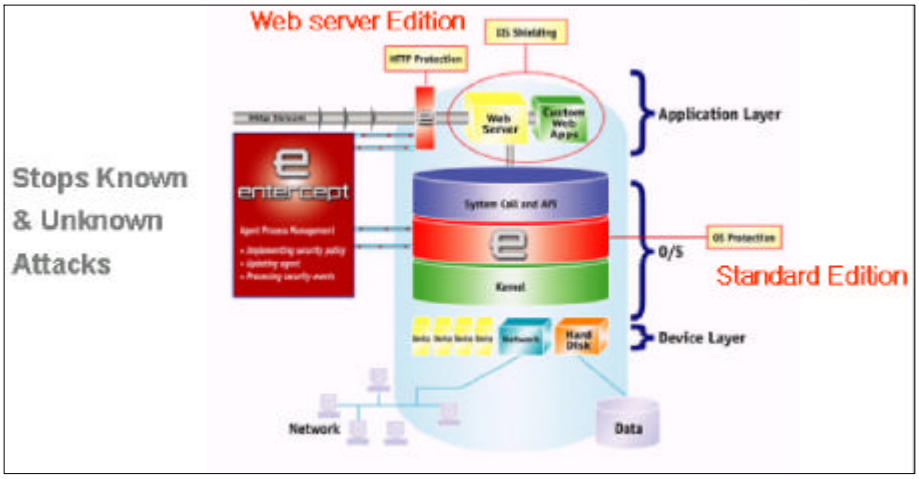
미국 엔터셉트 시큐리티 테크놀로지의 IPS 국내 독점 판매권을 갖고 있는 이카디아의 인터셉트 침입방지 시스템의 기능을 살펴보면 보안 시스템은 광범위한 서버 보호, 침입 방지, 알려지지 않은 방식의 침입에 대한 보호 등의 부가적인 능력을 필요로 한다. 인터셉은 허가받지 않은 트랜잭션이 일어나기 전에 침입을 알아내어 서버에 접근하는 것을 막는다. 기존의 감시 제품들과 달리 OS와 API가 처리하기 전에 요청을 미리 파악하여 호스트를 보호한다. 침입방지시스템의 일반구성 형태는 [그림13]과 같다. 시그니쳐와 리소스 접근 컨트롤 기술을 융합하여 알려진 침입과 알려지지 않은 침입을 막을 수 있다. 사용하기 쉽고 보안관리에 있어 시간절약을 제공하는 장점이 있다[5, 6, 7, 9].



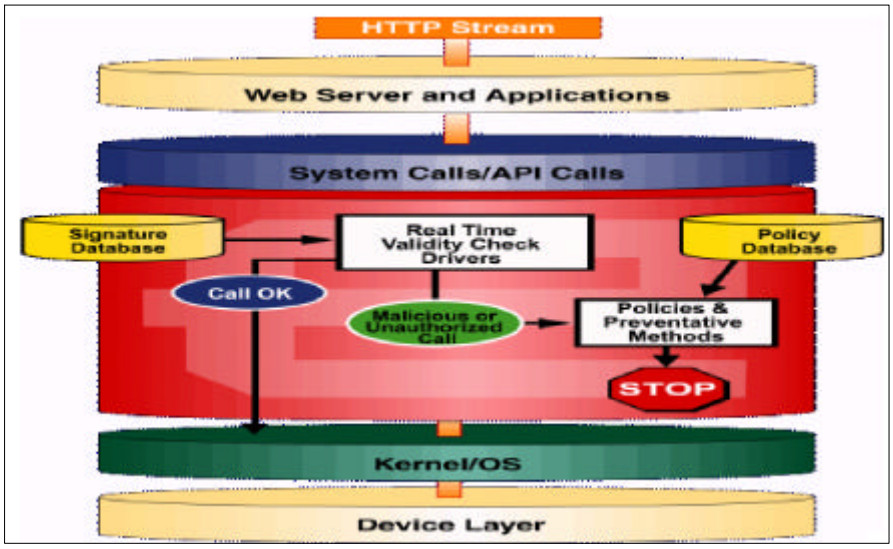
[그림 13] 인터셉 IPS의 구성 형태

인터셉의 내부구조는 [그림14]와 [그림15]의 구성형태로 구성되어 있다. 인터셉은 OS와 인접한 곳에 설치되어 OS와 커널로 들어가는 소프트웨어 호출을 가로채어 검사할 수 있다. 호출들은 알려졌거나 알려지지 않은 모든 침입방법에 대해 꾸준히 업데이트된 데이터베이스와 비교 검사된다. 침입이 발견되면 시스템을 보호하기 위해 각 환경에 맞춤화된 정책에 따라 선제공격이 취해진다. 로그 이벤트에서 터미네이터

프로세스 범위에 이르는 액션이 이루어진다.



[그림 14] 인터셉트 IPS 내부구조1



[그림 15] 인터셉트 IPS 내부구조2

인터셉의 기능에 따른 분류는 <표11>과 같이 Individual Attack, Generic Attack, Shielding and HTTP protocol protection, Resource Protection등으로 구성되어 있다.

< 표 11 > 인터셉트의 기능분류

분류	기능
Individual Attack	OS와 application에서 일어나는 활동에 대해 알려진 침입 방식과 매치(비교)시키는 과정을 이용하여 단일 해킹에 대하여 보호한다.
Generic Attack	OS와 어플리케이션에 감시를 받는 모든 종류의 해킹(알려진 침입뿐과 알려지지 않은 침입-BufferOverflow를 이용한 해킹과 같은)에 대하여 보호한다.(buffer overflow 버그를 이용한 해킹은 buffer를 임의로 overflow 시켜서 자신이 원하는 일을 수행하도록 하는 것이다)
Shielding and HTTP protocol protection	특별한 어플리케이션을 위해 부가적으로 보호. 예) IIS웹서버 부가적인 라이센스요청
Resource Protection	서비스,레지스트리 키, 사용자 인증 매커니즘 등을 포함한 시스템 리소스에 의도적으로 접근하는 것을 막는다.

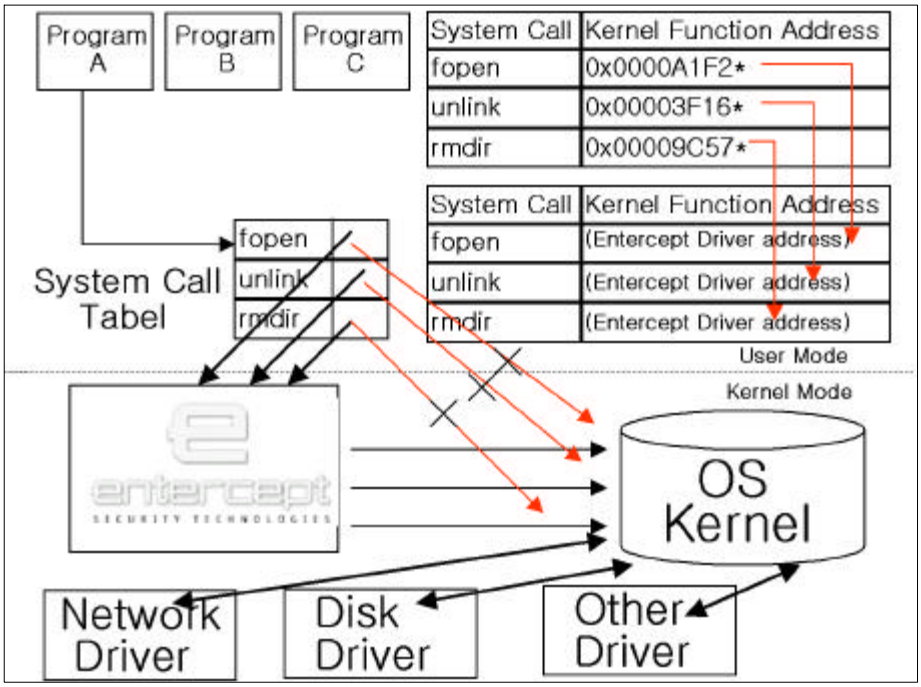
인터셉의 가장 큰 특징은 호스트에서 일어나는 모든 활동이 감시되고, 암호화, 데이터 교환, 또는 시스템 로그 정보 의존에 의한 시스템의 손상을 막을 수 있다. 침입 데이터베이스는 침입 인식 가능성에 대해 다음과 같은 타입으로 구성되어 있다.

Administrator에 대한 강력한 맞춤화 능력을 통합하면서 정책 데이터베이스는 false positive가 가상으로 제거되는 것을 허락하며 완전히 갖춘 고정 템플릿으로 이동한다. 이러한 고정 정책은 빠른 배치를 보장한다. 에이전트들은 각 서버로 배치되고 중앙 관리 콘솔로부터 컨트롤되고 업데이트되어 진다. 에이전트는 완전히 독립된 보호기능을 가진 유닛이며 동작할 콘솔에 의존하지 않는다. 이러한 접근은 어떠한 통신 포트가 열린 채로 남겨지는 것을 막고 Fail Safe 기능을 제공하는데 사용된다. 에이전트는 콘솔로부터 코드 업데이트와 새로운 침입 방법 정의에 대한 업데이트를 수행한다. 3중의 DES 암호화는 모든 통신에 대해 적용된다. 콘솔은 로그 데이터를 익스포트하는 것을 포함한 모든 관리 보고를 제공한다. 콘솔은 인터셉 인스턴트 업데이트를 통해 완전히 암호화된 통신으로 인터셉 시큐러티 홈 서버에 요청하여 업데이트한다.

인터셉트 IPS의 가장 큰 특징은 단순한 네트워크 단에서의 탐지가 제공하지 못하는 각종 서버를 위해 알려지지 않은 공격까지도 방어할 수 있는 실시간 침입방지시스템

으로 OS레벨에서 실시간 방어와 탐지기능을 제공한다.

인터셉의 일반적인 수행과정을 살펴보면 [그림16]과 같이 프로그램이 실행되기 전에 시스템 콜 테이블의 kernel-mode 함수 0x0000A1F2의 전송제어가 일어나서 예외적인 접근을 OS kernel-mode로 직접 실행이 일어나는 것을 방지하기 위해 OS와 가장 밀접하게 설치된 IPS프로그램이 명령어 체인과 연결되어 프로그램이 시스템 콜을 하기 전에 정형화되어진 적절한 명령인지의 여부를 판단하여 부적절한 명령의 경우 시스템을 Kill하고 정형화 되어진 정당한 사용자의 경우에만 사용을 허락한다[33,34].



[그림 16] 프로그램의 시스템 콜 과정

또한 웹서버의 자원과 서버를 보호하기 위한 규칙을 설정하여 서버의 자원과 서버를 보호한다. 침입방지시스템(IPS)은 시스템 커널을 수정하지 않고 시스템 콜을 가로챔으로 웹서버는 웹 파일들과 웹서버 자원만을 액세스할 수 있다. 그 밖의 모든 접근들은 허용하지 않는다는 규칙에 의해 공격과 알려지지 않은 공격에 대해 방어할 수 있다. 또한 프로그램에 의해 시스템의 자원에 접근할 경우 침입방지시스템이 시스템 콜을 가로챔으로 시스템 자원의 접근을 방지할 수 있다.

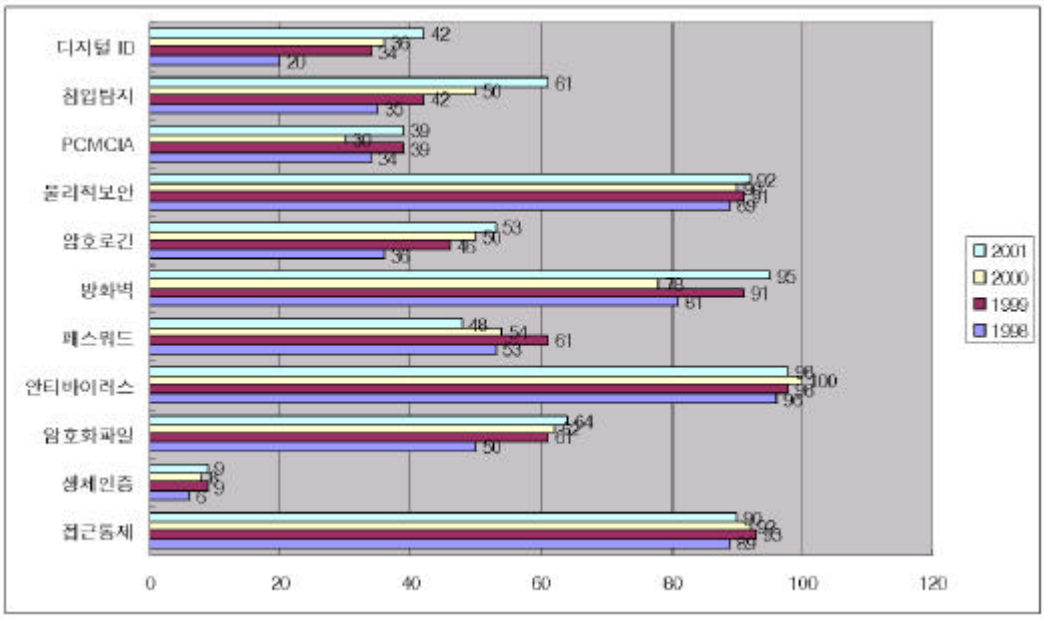
웹서버, 웹 어플리케이션 그리고 OS에 대하여 멀티 레이어 보호를 제공하는 Web Server Edition과 실시간 분석, 해킹시도에 대한 대응을 제공하는 고난도의 소프트웨어 기술을 공급하는 Standard Edition등 인터셉 침입방지제품의 종류는 <표12>와 같다.

< 표 12 > 인터셉트 IPS제품 종류

	Standard Edition	Web Server Edition
Individual Signatures	제공	제공
Generic Signature	제공	제공
Resource Protection	제공	제공
HTTP Protection	제공	제공
Web Server Shielding		제공

3. 침입방지시스템의 국외동향

국외의 경우 [그림17]과 같이 보안기술별 사용현황에서 2001년 Security Survey의 분석현황을 살펴보면 응답자의 95%가 방화벽, 61%가 IDS, 90%가 접근통제, 42%가 디지털ID 등 다양한 보안기술을 사용하고 있는 것으로 나타났으며, 2001년 조사에서 두드러지는 특징은 IDS의 사용자수가 증가하는 것은 침해상황을 탐지, 분석하도록 함으로써 각 기관들이 적극적으로 문제를 해결하려고 하기 때문인 것으로 보인다. 또한 패스워드의 사용자수가 감소하는 것을 볼 수 있는데 이것은 패스워드가 잘 작동하지 않고 잃어버린 패스워드에 대한 유지비용이 많이 들고 생산성의 저하를 가진다고 분석되었다[27].



[그림 17] 보안기술별 사용현황

침입방지시스템은 해외의 경우 미국 엔터셉트 시큐리티 테크놀로지가 지난해 처음으로 상용화했으며, 시스코 시스템즈, 컴퓨터 어쏘시에이츠 인터내셔널, 사이버 세이프, 인터넷 시큐리티 시스템, 네트워크 어쏘시에이츠, NFR 시큐리티, 시큐어 웍스, 시만텍 등이 개발에 앞장서고 있다. 특히 지난 코드레드 웜 피해 이후 IPS를 설치한 기업들이 전혀 피해를 입지 않자 앞다퉈 개발에 열을 올리고 있다. 이들 업체는 우선 자사가 공급하고 있는 IDS에 IPS를 통합함으로써 경쟁에 뒤처지지 않으려고 노력 중이다.

4. 침입방지시스템의 국내기술 및 시장동향

국내 정보보호제품 시장변화 중 큰 특징 하나는 그 동안 보안시장을 선도해왔던 안티바이러스의 비중이 감소하고 PKI, IDS 등의 3A 시장의 비중이 커졌다는 점이다. 인터넷 보안산업은 크게 방화벽, 암호, 바이러스, 3A 등 4가지 시장으로 구분할 수 있는데, 3A란 Authentication(인증), Authorization(권한부여), Administration(관리) 등 세 분야를 통칭하는 말로, 기업들이 고객이나 파트너와의 신뢰기반을 만들어 주는 핵심보안기술을

지칭하고 있다[1]. 한국IDC가 발표한 「한국보안소프트웨어 시장분석」에 따른 <표13>에서 나타난 지난해 국내 3A시장의 규모는 330억원으로 전체 보안소프트웨어 시장의 35.6%를 차지하였고, 3A 다음으로는 Firewall, Antivirus, Encryption 순의 시장점유율을 보였다. 이와 같은 3A의 확대추세는 앞으로도 계속되어 오는 2005년에는 국내 3A시장이 약 1조원 규모를 형성할 것으로 전망하고 있다. 3A가 강세를 보이는 이유에 대해 전문가들은, 3A는 외부에서도 인터넷을 통해 기업체 내부망으로의 접근을 가능하게 해주는 강력한 보안솔루션이며, 이는 곧 전자상거래의 핵심기반이 될 수밖에 없기 때문인 것으로 분석하고 있다[28].

< 표 13 > 3A의 개념과 제품군

3A	개 념	제 품
Authentication(인증)	이용자 확인과정	PKI, VPN
Authorization(권한부여)	작업가능대상 확인과정	SSO(Single Sign-On) EAM(Extranet Access Management) PMI(Privilege Management Infrastructure)
Administration(관리)	보안솔루션 통합관리	ESM(Enterprise Security Management)

정보보호 제품 및 서비스 추세는 인터넷의 확산으로 인해 정보화 환경이 가속화되면서 정보보호 기술개발도 다변화하고 있다. 내부 네트워크 환경에서 점차 외부 네트워크 환경으로 변화함에 따라 정보보호 제품 및 서비스도 개방화된 환경 속에서 보안을 담당할 수 있도록 발전하고 있다. 즉 기존 시스템이나 네트워크에 대한 외부로부터의 위험 침입을 차단시키는 기능의 수동적이고 방어적인 제품보다는 시스템이나 네트워크 자체의 안전성을 능동적으로 감지하는 기능을 가진 제품이 등장하고 있다. 특히 단일 기능을 수행하는 전용 제품에서 복합적인 보안 서비스를 수행할 수 있는 통합형태의 제품이 등장하는 추세이다. 최근 정보보호 제품 및 서비스 개발과 공급 추세를 간략히 살펴보면 다음과 같다. 먼저 인터넷의 활성화에 따라 익스트라넷 환경이 조성되면서 가상사설망(이하 VPN) 시장이 커지고 있으며, 특히 방화벽과 통합된 형태의 H/W제품이 등장하고 있다[29]. 방화벽과 통합된 형태의 IPS의 국내동향은 정보 보안업체 윈디시큐리티쿠퍼스가 최근 처음으로 IPS 제품인 윈디가드를 상용화

1) 디지털타임즈, "보안SW시장 3A 대세", 2001. 8. 17

했다. 윈디시큐리티쿠퍼스는 특히 IT 관련 국내 최고의 국책 연구소인 한국전자통신연구원에 이 제품을 납품하면서, IPS가 본격적으로 IDS의 대안으로서 관심을 끌기 시작했다. 또한 미국 엔터셉트 시큐리티 테크놀로지의 IPS 국내 독점 판매권을 갖고 있는 이카디아도 최근 해커피아·한화S&C 등과 판매 대리 계약을 체결했다. 유명 보안업체 S사도 큰 관심을 보여 모 그룹 내 독점 판매권을 요구하고 있는 것으로 알려졌다.

윈디시큐리티쿠퍼스는 한국전자통신연구소 같은 국책연구소가 국내에 잘 알려지지 않은 IPS 도입 계약을 맺은 것은 바로 이 솔루션이 기존 보안 솔루션과 달리 능동적이며 지능적으로 해킹에 대응한다는 차별성을 장점으로 인정한 것이라며, IPS가 조만간 제3세대 보안 솔루션으로 크게 각광받을 것이라 전망했다.

윈디시큐리티쿠퍼스의 IPS 개발을 시작으로 국내에서도 서버 보안 제품들이 본격적으로 출시될 전망이다. 서버 보안 솔루션은 기존의 방화벽과 IDS 등의 네트워크 보안 솔루션보다 좀 더 강력한 보안 기능을 수행한다고 평가받고 있지만, 기술 개발이 어려워 국내에서는 개발이 미진했다. 또한 서버 보안 솔루션은 방화벽이나 IDS의 아키텍처와는 달리 그 구조 자체가 일반화된 모델이 없다. 서버 보안 솔루션은 네트워크상에 오가는 패킷을 분석하는 수준의 네트워크 보안에 비해 주공격 대상인 서버 상에서 직접 보안 기능을 수행한다는 점에서 차별성을 갖는다. 대표적인 서버 보안 솔루션으로 보안 기능이 강력하다는 평가를 받고 있는 시큐어 OS의 경우 윈도NT나 유닉스 등의 상용 OS 커널을 변경해야 하므로 각 OS의 소스를 보유해야 한다는 단점이 있다. 최근 시큐브가 기존 OS의 커널을 변경하지 않는 시큐어OS 제품을 출시했지만, 기술 개발을 위한 노력과 효율성 측면에서 IPS가 더 효과적이라는 분석이 대두되고 있다. 그러나 어느 한 보안 제품만으로는 나날이 지능적으로 발전하고 있는 해킹·바이러스에 대응하기에는 불가항력이라는 의견이 지배적이다. 방화벽과 IDS·시큐어OS·IPS 등이 상호 보완적으로 시스템을 방어해야 한다는 것이다. 보안 전문가들은 이제 정보보안은 원인 분석과 사후 대책, 치료의 차원을 넘어 사전 예방과 어떠한 불법 침입도 허용 불가라는 개념에서 출발해야 그 동안의 일방적인 패배를 극복하고 그나마 창과 방패의 균형이 이뤄질 것이라고 분석되었다.

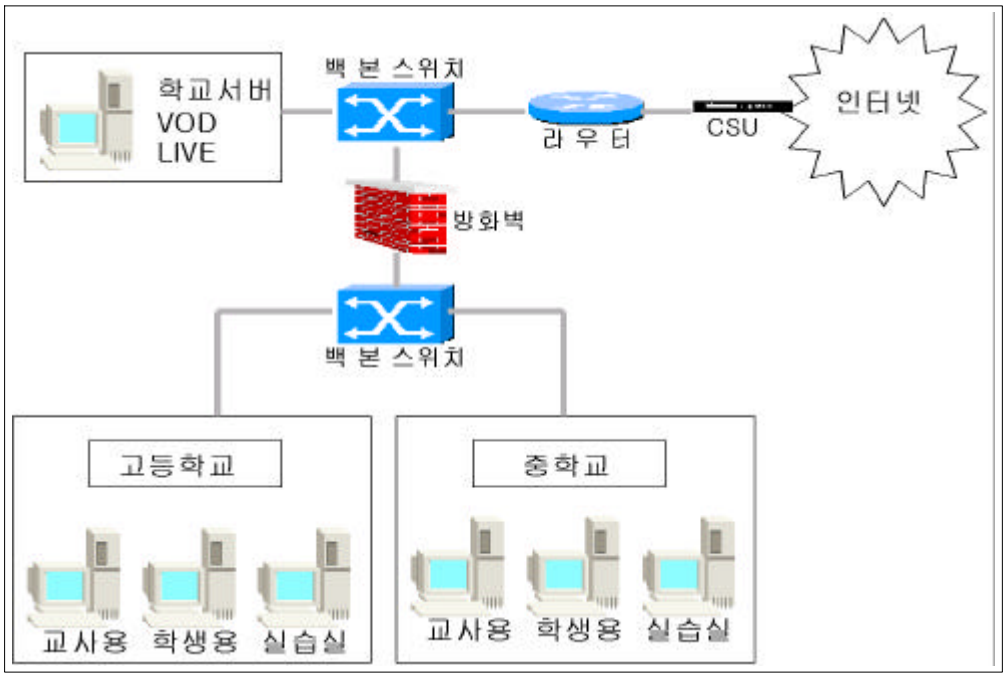
Ⅲ. 침입방지시스템의 구축모델과 방법론

1. 학내전산망과 침입방지시스템을 이용한 제안 모델

일선의 실제 방화벽이 설치된 학교전산망을 분석해 봄으로서 침입방지시스템 설계시 학교전산망의 문제점을 찾아 볼 수 있을 것이다. 현재 보안상 가장 취약한 구조를 가지고 있는 중·고등 통합학교의 실제 사례를 분석해보면 이 학교는 중학교와 일반계 고등학교가 붙어 있는 학교로서 1, 2, 3층은 고등학교, 4층은 중학교로 사용하고 있으며 중학교 Web 서버와 고등학교 Web서버가 따로 분리되어 있고, [그림 18]의 망 구성도를 보면 VOD서버와 기타 서버들은 고등학교에서 활용을 많이 하고 있다.

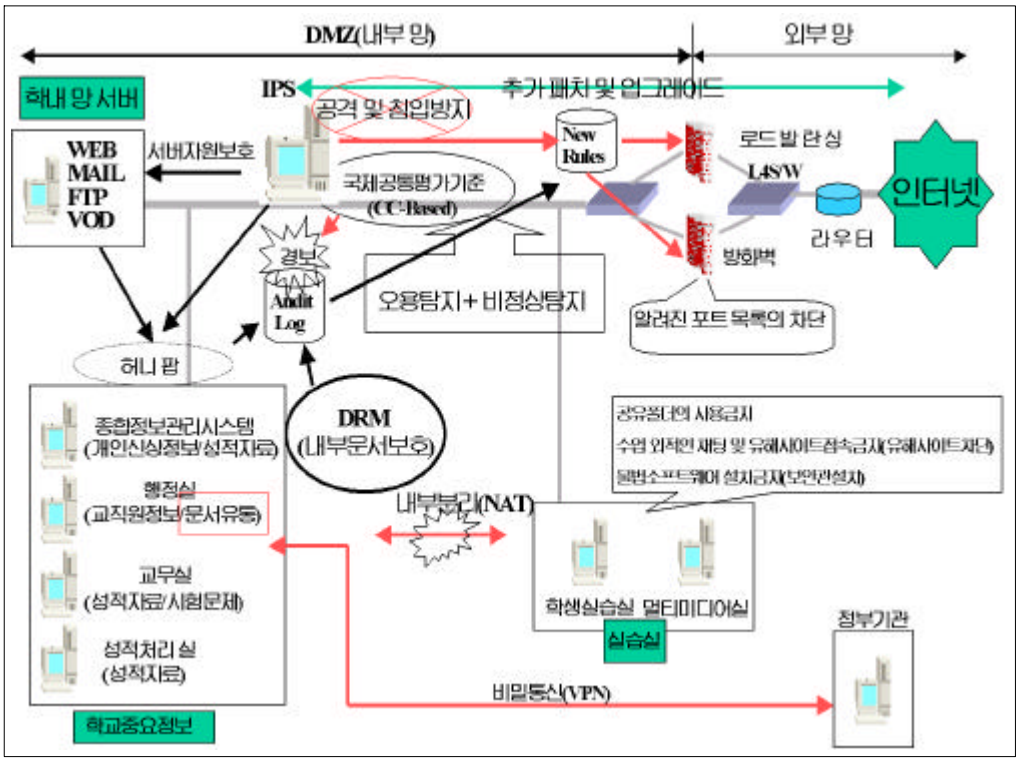
다른 학교에 비해서 서버 컴퓨터를 많이 보유하고 있으며, 학습에도 상당히 활용을 많이 하고 있다. 이번에 중학교를 따로 분류해서 서버를 운영하고 있지만, 학교의 IP가 많이 부족하며, 고등학교경우는 IP를 가상IP로 활용하고 있다. 네트워크 상의 장애가 가끔씩 발생을 하고 있는데 중학교와 고등학교의 네트워크를 완전히 분리하지 못해서 발생하는 요인으로 고등학교 백본 스위치의 2 Port 만이 사용을 하고 2Port는 중학교에서 사용을 하고 있다. 차후에 문제가 발생을 했을 때 중학교 망에도 문제 발생할 요지가 있으므로 중학교도 별도의 백본 스위치를 연결해야되는 필요성이 있다[30].

이학교의 경우에 중학교와 고등학교의 경우 교사용과 학생용, 실습실용 컴퓨터의 네트워크 구성형태가 불안전한 보안구조를 가짐으로 교사용 컴퓨터가 학생용이나, 실습실용 컴퓨터에서 침해 및 내부자에 의한 불법접근을 방어할 수 없는 구조를 가지고 있다. 그리고 기본적인 보안 정책이 방화벽만을 사용하고 있지만 해킹으로 인한 학내망이 침해될 경우 중학교와 고등학교 전체의 네트웍이 영향을 미치고 연쇄적인 피해를 가져올 수 있는 형태의 보안이 취약한 모델이라 볼 수 있다. 이 학교의 경우 추가적인 보안장비와 보안정책을 갖지 않는다면 해킹 및 침해사고가 일어날 경우 전체 네트워크와 학교 성적 및 중요정보의 피해가 일어날 수 있다.



[그림 18] 중·고등통합학교

방화벽만으로는 해킹 및 바이러스, 내부자의 침입 등으로 인한 개인신상정보, 성적자료의 위·변조, 시험문제의 유출, 유해정보로 부터의 보호, 제3의 해킹경유지라는 현실적 문제를 방화벽이 설치된 환경에서 IPS를 도입함으로 가장 효과적인 보안정책을 실현하고자 [그림19]와 같은 IPS를 도입한 구성모델을 제안하였다.



[그림 19] 침입방지시스템 제안모델

최초의 보안장비는 라우터를 통한 필터링을 시행한다. 일반적으로 라우터는 트래픽의 속도와 연관됨으로 Layer 4 스위칭에서 병목을 제거하는 로드 밸런싱 구조를 고려하였다. 방화벽은 프록시 기능을 통한 캐싱기능과 보안정책을 시행하고 알려진 취약한 포트를 기본적으로 차단한다. 또한 NAT기능을 통해 사설IP를 사용하여 IP 부족 현상을 해소하고 내부의 IP를 숨김으로 IP공격에 대비하였다. 학교의 중요 정보와 성적, 신상자료, 시험문제의 유출을 방지하기 위해 학생용과 교사 및 성적과 중요정보를 다루는 네트워크를 서브넷 마스크로 그룹을 분리하고 DRM기법을 적용하였다.

학생 실습실과 멀티미디어실은 외부 해킹을 방지하기 위해 공유폴더의 사용을 제한하고 수업외적인 인터넷의 사용과 유해사이트의 접속, 채팅을 금지시킨다. 이때 필요시 소프트웨어적으로 인터넷 및 컴퓨터의 사용을 제한하는 넷 헬프 등의 상용프로그램 설치도 고려된다. 또한 불법 소프트웨어나 오락 등 인스톨을 방지하기 위한 하드디스크 보안관을 설치하는 것이 바람직하다. 교사용 및 업무용 컴퓨터는 백오리피

스 등 해킹용 프로그램이 설치될 가능성을 배제하기 위해 학생용 디스켓과 학생들이 업무용 컴퓨터를 불법적으로 사용하는 것을 금지시킨다. 그리고 정부기관과 전자문서 교환시 문서암호화 및 비밀통신(VPN)이 필요하다. 또한 교사용 및 업무용 컴퓨터의 사용시 부팅암호와 비사용시 권한 제한을 위한 화면보호기 암호설정 및 비활성 자료의 접근을 차단한다. 학교의 중요정보를 보호하기 위해서는 문서와 데이터베이스의 암호화가 필요하다. 내부문서 유출을 막기 위한 제도적인 방지장치나 데이터베이스 연관 마이닝 기법의 적용도 고려된다. 그리고 방화벽을 통과하는 공격, 내부자의 침해 및 바이러스, 유해정보, 서비스 거부, 해킹 등 방화벽의 문제점을 보완하고 서버의 보호와 학내전산망의 취약한 부분을 IPS를 통해 보안정책을 사용하였다. 또한 해킹 패러다임의 변화에 따른 새로운 공격기법에 대비해 취약점에 대한 보안정책을 실현할 수 있는 가장 효율적인 모델이라 볼 수 있다. 현재 방화벽의 문제점으로 거론되고 있는 바이러스 및 내부자 침입에 대한 한계성으로 추가적인 보안정책을 구축하기 위해 침입탐지시스템(IDS)이 거론되고 있지만 가격대비 성능의 문제와 경제적인 부분을 고려한다면 침입방지시스템 (IPS)을 사용하는 것이 보다 효과적인 보안정책을 구축할 수 있으리라 기대된다.

현재 학교에 설치된 방화벽만으로 학교전산망의 모든 보안 문제의 해결방법은 아니다. 방화벽이 안고 있는 취약점으로 인한 바이러스, 서비스거부공격, 백도어의 위협, 내부사용자에 의한 학교의 중요자료 침해, 더욱 고도화 지능화되어 가는 해킹 패러다임의 변화에 적절한 대응조치의 미흡 등으로 인해 학내 전산망이 새로운 침해 및 보안 사고를 야기하고 있어 학교 정보화 교육 본래의 기능을 수행하지 못하고 있다. 이러한 방화벽의 문제점을 보완하기 위해 새로운 기법과 기술을 적용한 보안장비의 확충이 절실히 필요한 실정이다. 방화벽의 기능은 외부침입에 대한 차단의 역할만을 담당하고 있어 내부자에 의한 학교중요자료의 위·변조 등에 취약하고 해결방안이 전혀 없는 상태이다. 또한 패킷만을 필터링 함으로 IP주소에 대한 차단은 할 수 있지만 문서형태의 E-MAIL에 첨부된 서크립트형의 바이러스에 대한 방어 및 차단의 역할을 하지 못한다. 그리고 TCP/IP의 인증 기반 미약으로 서비스거부 공격이나 인터넷 웜, 코드레드, 써캠 등의 공격에 취약성을 가지고 있어 서비스 거부 공격을 당하면 인터넷 통로 구실을 하는 방화벽의 부하로 인해 전체 시스템이 다운되는 문제가 발생한다. 또한 네트워크 및 보안전문 기술의 부재로 인해 보안정책이 부실하여 최근 언론에 보도된 해커에 의해 제3의 해킹경유지로 학교 서버가 이용된 것을 외국 침해대응팀 역추적에 의해 발견되었다. 그러나 학교의 관계자는 무엇이 침해되었는지

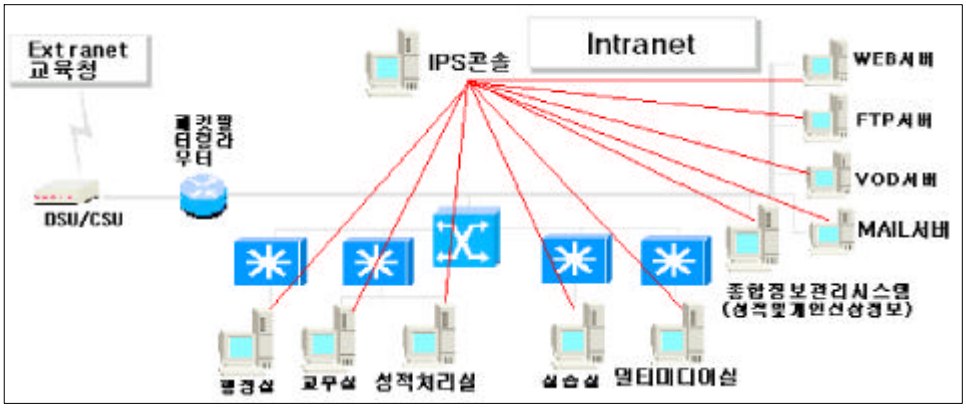
전혀 모르는 실정이었다. 그리고 시험문제가 유출되어 학교의 홈페이지에 게재된 사건과 내부자에 의해 학생 신상정보가 외부로 유출된 사례 등을 들 수 있다. 침입탐지 시스템은 방화벽에 부가적으로 기본적인 차단의 다음 단계로서 탐지하는 기능을 수행한다. 이 시스템은 단지 탐지만 할 뿐 실시간 공격의 방지를 제공하지는 않는다. 늘어나고 있는 여러 상황들은 네트워크 IDS가 제한된 탐지 능력과 공격시도들에 대한 적절한 구분이 원천적으로 어려움이 있다는 것을 보여 주고 있다. 결과적으로 많은 공격들은 탐지되지 못한 채 남겨지고, 게다가 False positive들이 생성된다. IDS와 같은 어떠한 서명 기반 시스템이라도 제품의 데이터 베이스 안에 알려진 공격의 시그니쳐가 존재할 때에만 동작하게 된다. 침입방지시스템은 침입이 일어나기 전에 실시간으로 침입을 막으면서, 다양한 침입 기술에 대하여 보호할 수 있는 다양한 방법의 보안 기술로서 웹서버와 웹 어플리케이션을 보호하고 알려졌거나 알려지지 않은 방식의 침입으로부터 OS에 대한 보호를 한다. 또한 엄청난 false positive가 발생하는 것을 피할 수 있도록 정확하게 침입을 구별하며 SMTP/FTP/DNS, HTTP 통신을 감시한다. 최소한의 환경을 필요로 하면서 쉴새 없이 업데이트 받는 기능과 솔루션을 쉽게 배치할 수 있고, 다양한 서버들에 걸쳐 쉽게 업데이트 할 수 있는 기능을 제공하는 새로운 개념의 보안솔루션이다. 점점 더 지능화되고 다양해지는 해커들의 침입기술과 웹에서 가능한 보통 툴들의 사용으로 기존 방식의 보안 제품들이 무력화되고 있다고 해도 과언이 아니다. 그 대안으로 침입방지시스템은 효과적인 보안 제품이라고 할 수 있겠다. 현실적인 학교전산망의 보안전문 기술 부재로 인한 관리와 운용의 편이성등을 고려하고 경제성과 가격대비 성능부분을 고려한다면 IPS의 도입이 가장 적합하고 볼 수 있다. IPS 설치환경 및 제품사양을 살펴보면 기존의 방화벽이나 IDS 처럼 네트워크 기반의 보안 소프트웨어가 아닌 서버기반의 보안 솔루션으로 각 서버에 직접 소프트웨어 형태로 탑재 되어 침입방지 기능을 제공한다. 소프트웨어 형태가 각 서버에 탑재되는 서버 기반이기 때문에 기존에 사용하고 있는 보안 솔루션들과 시스템 구성상의 충돌은 전혀 고려하지 않아도 된다. 즉 기존에 또는 새롭게 도입하려는 방화벽이나 IDS등 보안장비의 유무나 구성형태와는 전혀 상관없이 서버에 직접 탑재된다. 서버의 운영체제가 다른 경우에도 통합은 가능하다. 단, 현재 지원하고 있는 운영체제는 윈도우 계열과 솔라리스 계열의 제품환경을 가지고 있다. 학내 전산망에서 침입방지시스템의 구축목표는 <표14>와 같이 방화벽만으로 구축된 현재 학교전산망에서 방화벽의 문제점을 해결하고 한층 강화된 보안정책의 설정과 로그기능의 강화 및 패치와 업데이트의 자동화로 관리·운영상의 편리성과 내·외부의 침

입을 관리함을 목적으로 한다.

< 표 14 > 침입방지시스템 구축 목표

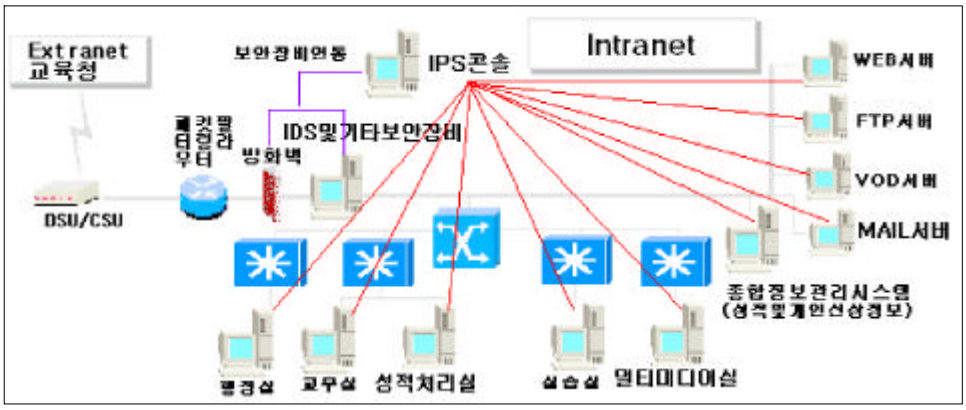
목적	현재의 학내전산망이 방화벽만으로 구축되어 보안기능의 허점을 가지고 있음으로 침입탐지기능과 서버자원을 보호하고 침입탐지시스템(NIDS)이 가지고 있는 비정상탐지문제, 허니팝 개념, 내부정보 유출 차단 등의 문제점을 해결하여 학내전산망 고유의 기능인 교육정보화를 실현하고 보다 안전하게 내·외부 침입을 관리할 수 있는 시스템 구축
규격	① 기존 방화벽의 기능에 침입탐지 기능을 추가 및 상호연동에 의한 효율적인 보안정책의 구현 : 패킷필터링 규칙, 오용탐지 방식, 국가보안등급 K4 등급의 관리 기능, 방화벽과 연동한 차단기능 자동업데이트 기능 ② 추가기능 - 비정상 탐지기능 : 연관 마이닝 기법 적용 - 내부문서 유출관리 기능 : DRM 기법 등을 응용 - CC 표준안 로그관리 기능 : 기존 국가보안등급 K4 등급을 국제공통표준규격 적용 - 적용시스템 : 솔라리스 및 NT 기반의 방화벽이 설치된 학교 전산망 - 보안패치 및 업데이트 기능 : 보안적용을 위해 관리자의 수작업을 통한 보안정책을 인터넷을 통한 자동업데이트와 상호 연동에 의한 효과적인 보안정책의 구현 ③ 네트워크 적용시스템 성능 : 트래픽 처리를 위해 Giga Bit 처리
성능·기능	- 방화벽의 보완 기능 : 방화벽만으로 처리할 수 없는 내부자의 침해와 잦은 보안정책의 변경을 자동처리 - 보안정책 : 자동 업데이트 및 패치 - 탐지방식 : 비정상탐지+오용탐지 - 대응방식 : 능동적 실시간 처리 - 비정상 탐지 기술 : 연관마이닝 기법 적용 - 감시기능 : 허니 팝 기능 추가 - 내부 파일 유출 관리 : DRM 기능을 이용한 관리 기법 적용 - 로그관리 : 국제공통표준규격(CC) 표준안 적용
용도	- 방화벽을 우회하는 공격과 문제점을 보완하고 보안정책을 강화 - 전산망을 운영하는 모든 학내전산망의 불법 침입을 탐지할 수 있는 내·외부의 침입탐지 - DRM 기법을 응용한 내부 문서 유출관리 기능 지원
적용	- 학교 전산망을 운영하는 모든 교육기관

학교의 특성상 방화벽과 같은 보안 장비가 없을 때의 IPS시스템 구성 형태는 [그림 20]과 같다. IPS시스템은 방화벽과 같은 보안 장비가 없을 때도 설치가 가능하다. IPS 에이전트들이 각각의 호스트에 탑재되어 보안기능을 수행한다. 이 구성방식의 특징은 호스트로의 공격은 막을 수 있지만 네트워크 상의 트래픽에 관련된 보안은 막지 못하는 보안 기능이 다소 미약한 형태라 볼 수 있다. 그래서 IPS를 설치하기 위한 최소한의 보안 장비로는 방화벽을 갖춘 형태의 보안정책이라 할 수 있다.



[그림 20] 보안장비가 없을 때의 IPS구축 모델

방화벽, IDS와 기타의 보안장비(바이러스 월등)를 갖추었을 때 보안모델의 구성은 [그림21]과 같이 구성할 수 있다. 이 모델은 가장 강력한 보안정책을 가지고 있는 모델이라 할 수 있다. 현재 학교의 실정이 방화벽만 구축된 상태라면 침입탐지장비와 기타보안장비의 구입에 따른 경제적인 문제가 대두될 수 있고 또한 새로운 보안장비의 도입에 따른 관리자 및 운영자의 보안교육과 보안정책, 관리 및 운영 등 많은 예산과 인력에 따른 추가적인 문제가 발생할 수 있다.



[그림 21] 방화벽, IDS등의 보안장비와 IPS설치 모델

또한 보안전문지식을 필요로 하고 학내전산망 침해시 대응과 복구가 사후처리를 해야하는 문제를 안고있는 IDS보다 침해차단과 보안정책의 변경, 자동 업데이트라는 점에서 인력적 측면과 관리운영 부분에서 더 효과적이라 볼 수 있겠다. 다음 <표15>는 위에서 제안 된 IPS의 구성형태를 요약 정리해 보았다.

< 표 15 > IPS와 기존 보안장비와 연동한 설치 환경

(1) IPS 설치하기 위한 최소한의 보안 장비	
방화벽	
(2) 보안장비(방화벽, 침입탐지등)가 없을 경우의 IPS 설치 환경	
설치가능여부	설치가능 에이전트들이 각각의 호스트에 탑재된다.
보안정책	네트워크 상의 트래픽에 관련된 보안은 막지 못하나 호스트로의 공격은 막을 수 있다.
(3) 방화벽만 있을 경우의 IPS 설치 환경	
설치가능여부	설치가능 방화벽이 설치된 후 IPS설치
보안정책	가장 적합하게 외부로부터의 공격을 막는 확실한 방안
(4) 방화벽과 IDS를 모두 설치된 경우의 IPS 설치 환경	
설치가능여부	설치가능
보안정책	가장 높은 강도의 보안정책을 사용할 수 있다. 추가로 침입탐지(IDS)를 설치할 필요는 없다.

2. 침입방지시스템을 이용한 학내전산망 구축방법

학내 전산망의 문제점인 유해정보(음란물, 자살, 폭탄, 엽기 등), 바이러스, 해킹 제3의 경유지, 내부자에 의한 학교 중요정보(성적, 개인정보) 위·변조와 수정 등의 문제를 해결하기 위해 먼저 방화벽은 베스쳔 호스트를 구축하여 시스템 자체의 보안수준을 높인다. 알려진 모든 시스템 관련 버그들을 수정하여 간결하고 무결한 시스템 상태로 만든다. 그리고 시스템 로그 기록을 활용한다. 필요 없는 모든 서비스를 중지시킨다. 시스템이 동작하는데 반드시 필요한 서비스만 남기고 나머지는 중지시킨다. 불필요한 사용자 계정을 모두 삭제한다. 꼭 필요한 경우가 아니면 베스쳔 호스트 내의 사용자 계정은 모두 삭제시켜야 한다. 사용자 계정이 존재하지 않는 베스쳔 호스트가 높은 수준의 보안 수준을 제공할 수 있기 때문이다. IP 포워딩기능, 소스라우팅 기능을 없앤다. 커널이 제공하는 기능 중 다음과 같은 몇 가지의 기능은 보안의 위험성을 가지고 있는데, 이들 기능이 우선적으로 제거되어야 할 것이다. (IP forwarding OFF, IP Masquerading OFF, NFS, RPC 관련 기능) 만약, 베스쳔 호스트가 듀얼-홈드 호스트로 구축되었으면 IP 포워딩 기능을 삭제해야한다.

학교전산망의 취약성은 보안정책, 보안교육, 보안장비 등의 부재로 인한 보안의 총체적 허술 이라 볼 수 있으며 이를 전담할 수 있는 보안전문인력의 양성이 무엇보다 시급한 실정임으로 각 단위 학교당 보안전문인력을 1인 이상 보안전문교사를 선정하여 보안전문교육을 이수하여 학교전산망의 안전과 보안정책의 수립, 보안교육의 내실화와 보안장비 도입의 효율과 운용을 전담할 수 있는 보안전문가 교육이 필요하다고 사려된다.

보안전문교육은 보안장비의 효율적인 운용, 보안정책 수립과 보안교육을 전담하도록 보안전문가 과정을 정보보호센터나 특수연수기관을 통하여 이수하도록 한다. 그리고 보안전문교육과정의 편성은 산학협동으로 이루어지고 있는 교과목을 이수하도록 하는 것이 바람직하다.

교과목의 편성은 정보보호에 대한 전문적인 이론교과와 실제 보안장비와 해킹에 관련한 실습으로 교과과정을 <표16>과 같이 편성한다.

< 표 16 > 정보보호 전문과정 교과목

교과목의 편성	
이론교과	정보보안관리, 네트워크보안, 운영체제보안, 암호알고리즘, 프로그램 보안, 데이터베이스보안, 시스템관리, 보안프로토콜, 전자상거래보안, 저작권보호기술, 정보윤리
실습교과	각종보안장비의 운용 , 해킹 및 크래킹과 보안관련 실습

보안전문강좌 및 시간일정의 구성은 <표17>과 같이 구성하여 이론과 실습을 겸비하여 전문적인 보안전문 교육을 이수하도록 한다.

< 표 17 > 정보보호 전문가 교육과정의 강좌 일정

	09:30 12:00	13:00 15:30	15:30 18:00
10일	개회식/보안요소	암호 알고리즘-1	정보보호관리기법
	암호 알고리즘-2	암호 알고리즘-3	암호알고리즘-연습
	네트워크 보안-1	네트워크 보안-2	보안제품평가-1
	보안제품평가-2	Braid Group	Braid Group
	보안 프로토콜-1	보안 프로토콜-2	프로그램 보안-1
	데이터베이스보안1	데이터베이스보안2	OS 보안-1
	OS 보안-2	OS 보안-3	저작권 보호기술
	정보보안 관리	PKI 및 응용-1	PKI 및 응용-2
	PKI 및 응용-3	정보윤리-1	정보윤리-2
	UNIX 시스템보안	실습개요-1	실습개요-2
3일	해커스랩과 A3 Security Consulting에서 진행		

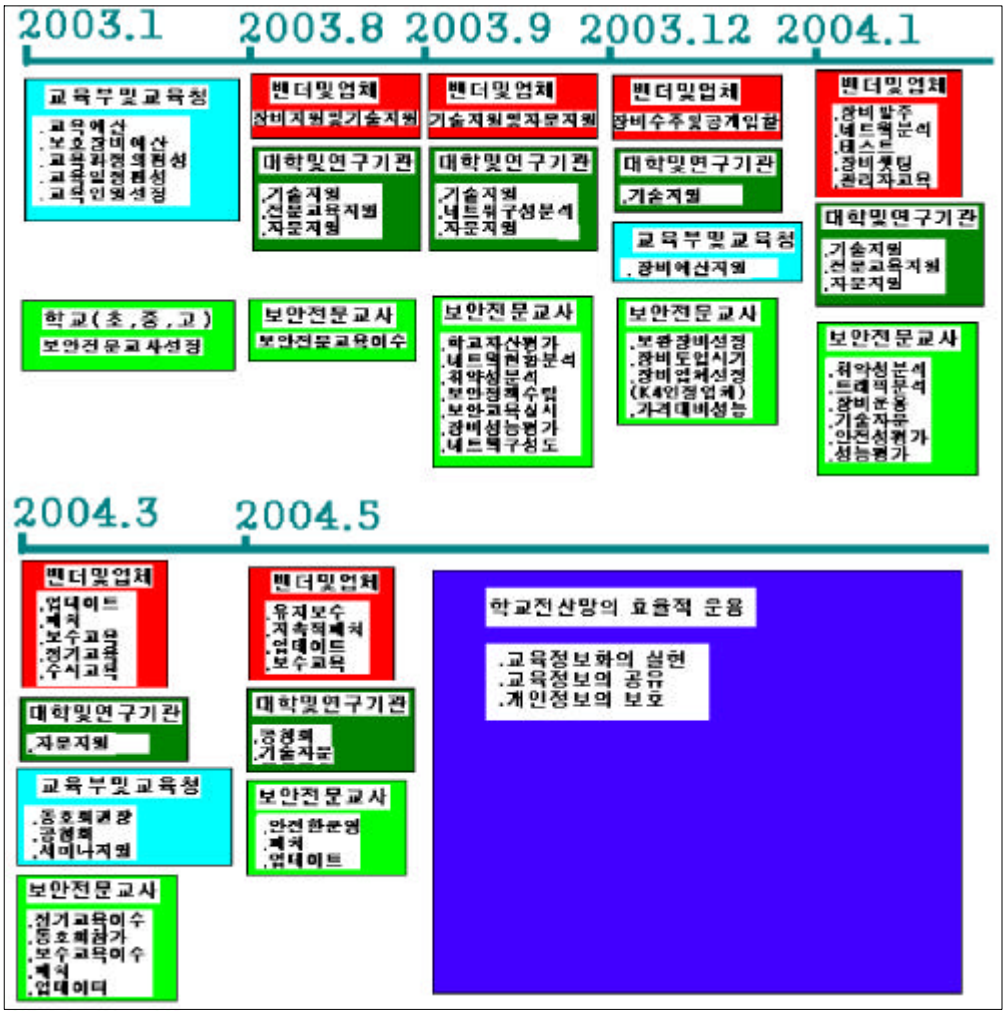
정보보호전문교사 양성을 위한 교육예산의 편성은 <표18>과 같이 구성하고, 교육시기는 학교전산망의 부실과 안전을 위해서는 정보보호 전문가의 교육이 빠른 시간에 이루어지는 것이 바람직하지만 학교의 현실과 보안전문교사의 선정, 수업 등을 감안하여 2003년 하계방학동안이 가장 적절하다고 본다.

< 표 18 > 정보보호 전문교사 양성을 위한 예산

교육예산의 편성		
부산시교육청 교사1인당 교육비 61시간 기준: 280,000원 (교재비, 강사료, 출장비, 시설사용료, 각종소모품비 포함)		
총교육시간 : 97.5시간 교사1인당 교육비:447,541원	학교수(부산) 554개교(초,중,고)	정보보호전문총소요예산 2억4천7백9십3만7천원

보안전문가의 교육효과는 전체 학교의 보안정책 내실화와 보안전문교사가 학교내 전교직원을 대상으로 보안교육을 자체 연수함으로서 보안인식의 파급효과가 증대될 것이고 또한 보안장비의 운영 측면에서 보안정책 수립과 효율적인 운영이 기대되고 학교전산망의 취약성을 최대한 방어할 수 있는 전문가를 둠으로서 내·외부의 해킹과 바이러스에 대한 적극적인 방어대책이 될 것이다.

침입방지시스템 도입을 위한 연도별 세부적인 계획은 [그림22]와 같이 구성 한다. 침입방지시스템 기술의 보급과 연구가 전세계적으로 활성화되고 있어 현재 침입방지시스템을 설치 운영하고 있는 정부기관과 업체의 추이를 살펴보면서 침입방지시스템의 개발이 완료되고, 침입방지시스템의 안전이 확보되고, 시스템 가격이 하락하는 2003년 말이나 2004년 초가 침입방지시스템의 도입시기로 적절하다고 본다.



[그림 22] 침입방지 시스템 도입을 위한 연도별 일정

침입방지 시스템을 도입하기 위한 준비작업으로 보안전문가의 양성이 우선되어야 한다. 이는 보안장비에만 의존하여 기존 밴더나 업체의 셋팅에 따른 안일함으로 현재 학교전산망의 부실과 취약성을 초래하였고 이를 관리 운영하는 전문기술과 인력이 절대적으로 부족하기 때문으로 분석된다.

보안전문가 양성을 통해 학교전산망에서 네트워크의 취약성과 장비성능분석을 통하여 현재 허술한 학교전산망의 전체적인 안전성과 신뢰성 점검을 한다. 그리고 네트워

크 구성도를 대학이나 연구기관을 통해 보다 적합하고 효율적인 네트워크 구성을 연구하고, 분석하여 가장 안전한 네트워크 망 구축과 이에 필요한 장비의 도입을 추진한다.

침입방지 시스템 도입을 위한 예산은 <표19>와 같이 침입방지업체의 실제 견적을 기준으로 W사의 견적 2200만원과 E사의 견적 1800만원을 기준하여 보안장비 도입을 위한 예산 편성을 하였다.

< 표 19 > 침입방지 시스템 도입을 위한 예산편성 [단위 : 만원]

구분	소 요 예 산 및 내 용
전국단위의 장비도입 (부산: 초, 중 ,고)	국회 예결위에 교육부 예산을 확보하여 지역교육청을 통하여 예산을 집행
	장비가격(1EA) : 1800×554(초,중,고) =99억7천200
각 단위학교의 경우 (1개교)	학교 기자재 선정 위원회의 의결을 거쳐 예산을 확보하여 장비를 도입
	장비가격(1EA) : 1800

각 단위 학교(1 개교)에서 침입방지 시스템과 같은 고가(高價) 장비의 도입은 아직 침해에 대해 민감하지 못한 단위 학교의 현실과 재정적인 문제로 인해 시행 및 도입이 적합하지 않음으로 전국단위의 장비도입이 전국의 단위학교에 학교전산망의 보안과 안전을 보장할 수 있다.

침해 및 바이러스에 의해 피해를 보면서 원인을 모르는 경우가 대부분이고 원인을 안다해도 재정적 예산과 장비 부족으로 대응하기 힘든 것이 현재 단위학교의 문제로 인식할 수 있다.

침입방지 시스템 관리와 운영요소를 <표20>에서와 같이 보안장비의 운영적 측면에서 침입방지시스템을 운영하기 위해서는 네트워크에 대한 기초지식과 운영체제에 대한 지식이 필요함으로 정보보호 전문가 교육과정을 이수하면 보안전문 교사가 충분히 침입방지시스템을 운영하고 관리 할 수 있으리라 기대된다. 또한 시스템 업체 및 밴더의 추가적인 수시교육, 정기교육 등과 업데이트 및 네트워크 환경의 변화에 대해서는 보수교육 등을 통해 시스템 운영의 효율화를 기대할 수 있다.

운영체제의 환경은 윈도우 NT, 2000 계열과 종합정보관리 시스템의 운영체제인 유닉스의 솔라리스를 지원함으로 생활기록부 및 성적자료의 관리가 용이하고 하드웨어적인 환경이 100MB 정도의 공간을 필요로 함으로 설치가 쉽고 인터넷으로 자동 업데이트 됨으로 시스템 관리와 운영을 하기 위한 전문적인 지식을 요구하지 않아도 최대의 방어 정책을 사용할 수 있다.

< 표 20 > 침입방지시스템 관리와 운영요소

구 분	내 용
기술적요소	네트워크 기초지식, 운영체제기초지식
운영체제환경	WINDOW NT, 2000, Solaris
메모리 환경	128MB이상
HDD 환경	100MB이상
구성형태	H/W+S/W 일체형, S/W형
업데이트	인터넷을 통한 프로그램 업데이트
네트웍환경변화	소프트웨어적 환경을 가짐으로 빠르게 대처

Ⅳ. 분석 및 평가

1. 학교 전산망의 현재 실정분석 및 평가

학교전산망의 취약성은 <표21>에서 나타난 바와 같이 전국 학교 정보화 현황은 100%로 구축이 완료된 상태에서 정보보호센터가 집계한 국내 해킹 피해 건수는 2001년 4월까지 1620건으로 지난해 연간 피해 건수(1943건)에 육박하고 있다.

< 표 21 > 전국 학교 정보화 현황 2001. 5

항목	현황
학교전산망 구축	1만 64개교(100%)
학생실습용PC보급대수	43만 1981대
교원용PC보급대수	34만 854대
인터넷가능학교(정보통신부)	1만5개교(5393개교는전송속도512K이하)

전문가들은 해킹 확산의 주무대로 초중고 및 대학 전산망을 꼽고 있다. 기업이나 관공서와 달리 보안 인력이나 보안 의식이 거의 없기 때문이다. 침해사고 대응 팀 협의회 위원장은 학교망에 대한 해킹이 성적이나 입시 관리, 회계 관련 데이터에 대한 도용이나 훼손으로 번질 경우 문제는 더욱 심각해진다고 보고되었다. 학교 전산망의 취약점은 관리측면의 보안문제점으로는 교육정보화를 위한 총체적인 보안 정책 부재, 교육정보시스템 보안운영에 필요한 보안 지침 부재, 보안문제 발생 시 대응 조치 지침 부재를 들 수 있다. 기술적 측면의 보안 문제점으로는 네트워크 및 시스템의 각 요소별 보안 대책 미비, 침입차단시스템 등 보안시스템의 운영 미숙, 별도 인터넷 망사용에 대한 보안 대책 미비를 들 수 있다. 또한 인적 측면의 보안 문제점으로는 해킹 대응 등 보안 전문인력 부족 등을 들 수 있겠다.

정보 보안 관리 실태를 파악하기 위한 기초 자료로서 일선 학교에 보급되어 있는 서버의 기종과 운영체제를 조사하였다. <표22>에 나타난 바와 같이 조사 결과 하드웨어는 PC 서버가 가장 많았으며, 그 다음으로 SUN 서버가 많았다. 많이 보급된 운영체제 순서로는 윈도우 NT, 리눅스, Solaris의 순이었다. 일선 학교에 보급된 운영체

제가 윈도우 NT, 리눅스 운영체제가 상당 수 운영되고 있어 이에 대한 보안 대책 수립이 필요함을 시사하고 있다.

< 표 22> 학내망 서버의 하드웨어 및 운영체제 현황(시·도 교육청)

구 분	하드웨어	운영체제	보급수량 (학교수)	비 고
서울	SUN, PC(서버)	Solaris 2.51 Windows NT	1,001	구축 중
부산	PC(서버)	NT	555	
인천	HP(서버) Sun Compaq(Digital) PC PC 기타 기타	NT Solaris 2.x NT NT Linux NT Linux	1 1 1 1 2 19 1	
대구	PC	NT	263	
광주	PC(서버)	Window NT	227	
대전	Sun, 기타	Linux, Solaris 2.x	187	
울산	PC(서버)	NT	19	
경기	PC(서버)	Linux, NT, Windows	1,478	
강원	PC(서버)	Linux		학교별로 추진되어 파악이 어려움
충북	PC(서버)	NT, Linux	232	192개교 추진중
충남	PC(서버)	Linux	269	
전북	PC(서버)	NT	253	
전남	PC(서버)	NT, Linux	228	
경북	HP	NT Linux	112 133	
경남	Sun, PC(서버), 기타	Solaris NT 기타	108 644	
제주	PC(서버)	NT	39	

프락시 서버의 경우 <표23>과 같이 16개 시·도교육청 중 2곳을 제외한 14개 교육청이 프락시 서버를 사용하고 있었다. 프락시 서버는 대부분 속도 개선을 위해 사용되고 있었다.

< 표 23 > 프락시 서버 사용 유무 (시·도교육청)

구 분	빈도(%)
있음	14(87.5)
없음	2(12.5)

정보 시스템 보안에서 패스워드의 관리는 가장 기본적인 사항이다. 가장 기본적이지만 중요한 사항이기 때문에 패스워드 관리 실태를 조사해 보았다. <표24>와 같이 조사 결과 99%의 학교에서 패스워드를 관리하고 있는 것으로 조사되었다.

< 표 24 > 패스워드 관리 실태

구 분	빈도(%)
실시하고 있다	200(99.0)
실시하고 있지 않다	2(1.0)

한편 전산시스템이 외부로부터의 해킹이나 기타 다른 이유로 장애를 일으키거나 데이터가 사고로 삭제될 경우에 대비한 백업 관리 또한 넓은 의미에서 정보 보안에 매우 중요한 사항이다. <표25>와 같이 응답자의 96.4%가 현재 백업 관리를 하고 있는 것으로 조사되었다.

< 표 25 > 백업 관리 실태

구 분	빈도(%)
실시하고 있다	188(96.4)
실시하고 있지 않다	7(3.6)

서버 및 개인 컴퓨터 운영관리 실태를 살펴보면 서버 운영시 가장 중요한 요소 중

한 가지는 서버에 대한 접근이다. 즉 서버에 대한 접근 권한이 설정이 되어있는 지와 누가 서버에 접근을 할 수 있는 지 여부이다. 조사결과 <표26>과 같이 서버의 중요 자료에 대한 접근 권한 설정에 대하여 96.9%가 설정하고 있다고 응답하였다.

<표 26> 서버의 중요 자료에 대한 접근 권한 설정

구 분	빈도(%)
설정하고 있다	185(96.9)
설정하고 있지 않다	6(3.1)

<표27>에서 나타난 서버에 접근 가능한 자에 관한 응답에는 78.4%가 전용 컴퓨터실 관리자로 응답하였으나 교사들 모두라고 응답한 학교도 19.1% 였고, 소수이기는 하지만 학생들도 접근할 수 있다고 응답한 학교가 1%로 나타나, 일부 학교에서는 서버 접근 관리에 문제가 있음이 조사되었다. 서버 접근 가능한 자는 시스템 관리자의 통제하에서 이루어져야 하며, 기본적으로 관리자 권한은 특히 제한해야 한다.

<표 27> 서버에 접근 가능한 자

구 분	빈도(%)
전용 컴퓨터실 관리자	160(78.4)
교사들 모두	39(19.1)
학교내 모든 학생	2(1.0)
기타	3(1.5)

<표28>과 같이 서버의 계정 관리 현황을 묻는 질문에는 복수 응답이 가능하도록 하였는데 전담 운영자에 의하여 시스템 관리자 계정 운영(35.8%), 전담 운영자에 의하여 이용자 계정 발급(27.7%), 관리자 계정은 절대로 공유되지 않음(22.2%)순으로 나타났다. 서버의 이용자 접속 현황(로그)을 조사 대상의 5%만 관리되고 있어 이에 대한 대책 수립이 필요함을 시사하고 있다.

< 표 28 > 서버 계정 관리 현황

구 분	빈도(%)
전담 운영자만이 시스템 관리자 계정 운영	137(35.8)
관리자 계정은 절대로 공유되지 않음	85(22.2)
전담 운영자에 의하여 이용자 계정이 발급	106(27.7)
이용자 계정 발급 대장을 통해 계정 발급	36(9.4)
서버의 이용자 접속 현황(로그)을 관리	19(5.0)

서버에 새로운 프로그램을 설치하거나 A/S 등의 이유로 외부 인력의 서버에 대한 접근이 불가피한 경우가 있다. 이 때 어떤 일을 어떻게 처리하였는지를 기록하고 관리하는 것은 보안에 대단히 중요하다. 이러한 맥락에서 <표29>와 같이 프로그램 포팅, A/S 등의 이력 관리를 조사해 보았다. 응답한 학교의 91.0%가 실시하고 있다고 답하였고, 9%가 실시하고 있지 않다고 답하였다.

< 표 29 > 서버 운영 관리(프로그램 포팅, A/S 등의 이력 관리) 실태

구 분	빈도(%)
실시하고 있다	172(91.0)
실시하고 있지 않다	17(9.0)

학교 전체 차원에서 관리하는 서버와는 달리 교사들이 개인 업무용으로 사용하는 컴퓨터에 대한 보안 관리 실태에 대해서도 <표30>과 같이 질문을 해 보았다. 역시 복수 응답이 가능하도록 하였는데 32.6%가 여러 사람에 의해 공유되며 개인별 관련 파일들에 대하여 별도 백업을 하고 있음으로 반응하였고, 담당 교사만 사용하나, 백업은 거의 하지 않음에 32.2%가 응답하였다. 또한 26.9%가 여러 사람에 의해 공유되며, 백업은 거의 하지 않음으로 조사되었다. 교사의 업무용 PC도 중요한 보안 대상이므로 이에 대한 대책을 마련해야 함을 시사하고 있다.

< 표 30 > 학교의 개인 업무용(교사용) 컴퓨터 운영

구 분	빈도(%)
담당 교사 이 외에는 누구도 접근할 수 없으며, 수시로 중요한 문서를 백업하고 있음	19(8.4)
담당 교사만 사용하나, 백업은 거의 하지 않음	73(32.2)
여러 사람에 의해 공유되며 개인별 관련 파일들에 대하여 별도 백업을 하고 있음	74(32.6)
여러 사람에 의해 공유되며, 백업은 거의 하지 않음	61(26.9)

정보 시스템에 대한 불법 침입 실태를 알아보기 위하여 통신망 침해 사고 및 컴퓨터 바이러스 사고 경험을 조사해 보았다. 조사 결과 <표31>에서와 같이 8.7%의 학교가 통신망 침해 사고를 경험하였다고 응답하였다.

< 표 31 > 통신망 침해 사고 경험

구 분	빈도(%)
사고 난 적 있음	18(8.7)
사고 난 적 없음	190(91.3)

통신망 침해 사고를 당한 학교에 대해 사고 유형을 조사해 본 결과 <표32>와 같이 인터넷을 통한 시스템 해킹 사고가 53.8%로 가장 많았고, 그 외 항목인 ID 및 패스워드 도용에 의한 사고, 학교 내 사용자에 의한 침해 사고, 자체 관리 및 운영 미숙에 의한 사고가 동일한 비율로 조사되었다. 따라서 인터넷을 통한 해킹 방지를 위해서 불법 칩입 차단 시스템이 설치되어야 하고 통신망 침해 방지를 위한 대책이 수립되어야 함을 시사하고 있다.

< 표 32 > 통신망 침해 사고 유형

구 분	빈도(%)
ID 및 패스워드 도용에 의한 사고	2(15.4)
인터넷을 통한 시스템 해킹 사고	7(53.8)
학교 내 사용자에 의한 침해 사고	2(15.4)
자체 관리 및 운영 미숙에 의한 사고	2(15.4)

정보 시스템 및 통신망이 불법침입으로부터 얼마나 취약한 가를 평가해 보는 취약성 분석에 대한 조사도 실시하였는데 <표33>과 같이 60.9%의 학교가 취약성 분석 테스트 경험이 없었으며, 전문가에 의한 분석은 5.8%에 불과 하였고, 26.1%는 취약성 분석 자체에 대해 알지 못하는 것으로 조사되었다. 조사 결과 취약성 분석에 대해 인지도가 극히 낮은 것으로 조사되었다.

< 표 33 > 정보시스템 및 통신망에 대한 취약성 분석 경험

구 분	빈도(%)
전문가	12(5.8)
자체 분석	15(7.2)
경험 없음	126(60.9)
모름	54(26.1)

컴퓨터 바이러스 침해 사고의 경우는 <표34>와 같이 34.5%의 학교와 1개의 교육청만이 사고 경험을 가지고 있었다. <표35>와 같이 사고 회수도 학교의 경우 78.7%가 1 2회에 그쳐 학교에서 컴퓨터 바이러스에 의한 사고는 그다지 많지 않은 것으로 조사되었다.

< 표 34 > 컴퓨터 바이러스 침해 사고 경험 단위 : 빈도(%)

구 분	학교	교육청
있음	70(34.5)	1(6.3)
없음	133(65.5)	15(93.8)

< 표 35 > 컴퓨터 바이러스 침해 사고 회수 단위 : 빈도(%)

구 분	학교	교육청
사고회수 1.00	33(54.1)	
2.00	15(24.6)	
3.00	3(4.9)	1(100)
4.00	2(3.3)	
5.00	2(3.3)	
6.00	2(3.3)	
20.00	4(6.6)	

* 빈칸은 응답하지 않은 것임

정보 시스템에 대한 불법침입을 막기 위하여 통상 침입 차단 시스템이 사용된다. 침입 차단 목적으로 사용되는 방화벽(firewall)의 설치 여부를 조사해 본 결과 <표36>과 같이 40.9%의 학교만이 현재 방화벽을 설치하고 있는 것으로 나타났다. 한편 <표37>의 침입 탐지 시스템의 경우에는 학교의 10.4%, 교육청의 18.8%만이 갖추고 있어 외부로부터의 침입에 대처 및 추적에 매우 취약한 것으로 나타났다.

< 표 36 > 방화벽 설치 여부

구 분	빈도(%)
있다	85(40.9)
없다	114(54.8)
모르겠다	9(4.3)

< 표 37 > 침입 탐지 시스템 설치 여부 단위 : 빈도(%)

구 분	학교	교육청
있음	21(10.4)	3(18.8)
없음	152(75.2)	13(81.2)
모르겠음	29(14.4)	

교육청의 방화벽 설치 여부와 위치를 조사한 결과 <표38>에서와 같이 7개 시·도 교육청에서 방화벽이 설치되지 않은 것으로 나타났다. <표39>와 같이 방화벽이 설치

된 경우 통신망 구조에서 대부분 라우터 안 단에 설치하였으나 1개 교육청의 경우는 라우터 밖에 설치하여 운영하고 있는 것으로 조사되었다.

< 표 38 > 방화벽 설치 현황 (시·도교육청별)

구 분	교육청을 통한 ISP 연결시 설치된 방화벽의 위치	각 학교에서 ISP로 직접 연결시 방화벽 설치 학교수
서울		1,001
부산	라우터 안	323
인천	미정	29
대구	없음	
광주	라우터 안	
대전	라우터 안	
울산	없음	없음
경기	라우터 안	
강원		일부 학교 자체 추진 중
경북	라우터 안	570개교 설치 예정
경남		2000년말까지 모든 관내 학교 설치 예정
충북		
충남	라우터 밖	없음
전북		2000년말까지 모든 관내 학교 설치 예정
전남	라우터 안	30
제주	라우터 안	없음

* 빈칸은 응답하지 않은 것임

< 표 39 > 학교에서 사용 중인 방화벽 제품명 (시·도교육청)

구 분	빈도(%)
수호신	3(11.1)
시큐어웍스	4(14.8)
화랑	4(14.8)
인터가드	7(25.9)
기타	1(3.7)

많은 학교에서 교육정보부장이 정보 보안을 담당하고 있는데, 이 들의 정보 보안 연수를 받았는 지의 여부를 조사해 보았다. <표40>과 같이 39.9%만이 정보 보안 교육을 받았고, 60.1%가 받은 적이 없다고 응답하였다.

< 표 40 > 교육정보부장의 정보 보안 교육(연수) 경험

구 분	빈도(백분율)
받은 적이 있다	79(39.9)
받은 적이 없다	119(60.1)

정보 시스템 불법 침입 방지에 관한 교육 지침이 일선 학교에 필요하다. <표41>에서 조사 학교 중 80.8%가 없음, 7.9%가 모르겠음으로 응답하였고, 11.3%만이 교육지침을 가지고 있다고 답하여 학교에서 정보 시스템 불법 침입에 대한 교육이 매우 취약한 것으로 나타났다. <표42>에서 나타난 것과 같이 교육지침을 가지고 있는 학교에서도 그 내용이 미흡하다는 반응이 40.9%, 이해하기 힘들다는 반응이 22.7%에 달해, 교육지침서를 가지고 있는 소수의 학교에서조차도 그 내용이 유용하지 못하여 불법 침입 방지의 실효성을 거두기가 어려운 것으로 나타났다.

< 표 41 > 불법 침입 방지에 관한 교육지침서 구비 여부

구 분	빈도(백분율)
있음	23(11.3)
없음	164(80.8)
모르겠음	16(7.9)

< 표 42 > 불법 침입 방지에 관한 교육지침의 내용

구 분	빈도(백분율)
충분하다	2(4.5)
그저 그렇다	14(31.8)
미흡하다	18(40.9)
이해하기 힘들다	10(22.7)

일선 학교의 보안상 취약점을 좀더 실질적으로 파악하기 위하여 4개 학교를 대상으로 해킹 허점 파악용 프로그램을 이용하여 공격을 시도하여 보안 현황을 파악해 보았다. 극히 제한된 숫자의 학교만을 대상으로 한 결과이기 때문에 본 점검결과를 일반화하여 보기는 힘들지만 학교의 보안 현황에 대한 참고가 될 수 있을 것이다.

<표43>은 보안 시스템에 대한 점검 결과이다. 네 학교 모두 학교 밖에서 원격으로 내부 시스템의 정보를 얻을 수 있는 등 보안이 매우 취약한 것으로 나타났다.

이상에서 보건데 일선 학교의 서버시스템의 샘플 점검에서 보안에 취약한 운영체제 버전을 사용하고 있다. 보안 문제가 있는 운영체제는 신속히 보안패치를 하고, 불필요한 서비스는 제거해야 한다. 일선 학교는 보안에 대한 전문지식이 부족함으로 시도교육청에서 필요한 보안정보를 신속히 제공할 수 있는 조직이나 체계를 갖추거나 관련 전문기관과 업무협조체계를 구축 운영해야 한다.

IP운영에서는 외부에 공개되는 웹서버, 메일서버 등은 공인 IP로 할당하고, 내부사용자들의 PC 등은 사설 IP로 할당한다. 침입탐지시스템의 설치는 침입차단시스템의 부족한 기능을 할 수 있는 부분으로 가급적 설치·운영하는 것이 좋다.

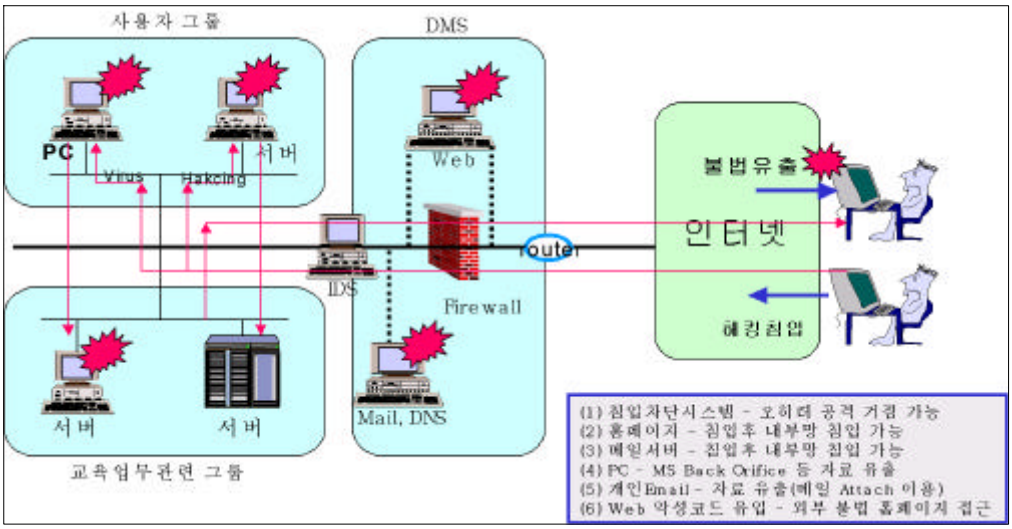
< 표 43 > 학교 보안 시스템에 대한 점검 결과

구 분	보안 문제점
학교 A	- 원격에서 내부시스템의 정보를 얻을 수 있음 - rpc, imap의 프로그램 오류에 의한 버퍼 오버플로우 공격을 당할 수 있음
학교 B	- 원격에서 내부시스템의 정보를 얻을 수 있음 - rpc, imap의 프로그램 오류에 의한 버퍼 오버플로우 공격을 당할 수 있음
학교 C	- 원격에서 내부시스템의 정보를 얻을 수 있음 - rpc, imap의 프로그램 오류에 의한 버퍼 오버플로우 공격을 당할 수 있음 - linux의 관리 시스템인 linuxconf에 의한 버퍼 오버플로우 공격을 당할 수 있음 - login과 shell 같은 명령어를 사용하여 인증없이 호스트에 접속할 수 있으므로 상당히 위험함 - pop3 같은 경우 안전하지 않은 버전을 사용했을 경우 버퍼오버플로우 공격을 당할 수 있음
학교 D	원격에서 내부시스템의 정보를 얻을 수 있음 - rpc, imap의 프로그램 오류에 의한 버퍼 오버플로우 공격을 당할 수 있음 - linux의 관리 시스템인 linuxconf에 의한 버퍼 오버플로우 공격을 당할 수 있음 - login과 shell 같은 명령어를 사용하여 인증없이 호스트에 접속할 수 있으므로 상당히 위험함 - pop3 같은 경우 안전하지 않은 버전을 사용했을 경우 버퍼 오버플로우 공격을 당할 수 있음

학내 전산망 보안에 관련된 자료를 요약해 보면 학교 전산망의 보안장비가 미흡하고 보안지침 및 교육현황에서는 보안의 전문교육과 보안지침의 이해가 대체로 낮다는 것을 알 수 있다. 그리고 프락시 서버가 없는 경우도 있음으로 캐싱 기능과 보안기능이 침해될 가능성도 있다. 패스워드 및 백업관리를 살펴보면 대체로 학교전산망에서는 관리를 잘하고 있음을 알수 있고 서버운영 및 관리현황을 살펴보면 잘 운영

되고는 있지만 서버접근과 권한설정에 조금 허술한 경향도 살펴 볼 수 있다.

교육전산망의 취약현황으로는 [그림23]과 같이 침입차단시스템을 통해 교육정보시스템을 접근하는 경우의 취약점은 침입차단시스템의 구성오류 등 운영상의 오류나, 메일을 통한 우회적인 공격을 당할 수 있다. 그리고 일부만 침입차단시스템을 통해 교육정보시스템을 접근하는 경우의 취약점은 관내 초·중·고 및 지역교육청은 자체 보안관리가 제대로 되어 있지 않은 경우 해킹공격에 무방비 상태로 될 수 있다[1].



[그림 23] 학교 전산망 취약 위험요소

2. 침입방지 시스템 도입과 활용에 대한 분석 및 평가

현재 학교전산망에서 현재 보유하고 있는 보안 장비를 요약하여 살펴보면 학교전산망에서의 보안정책이 미약하고 취약성을 많이 가지고 있다.
그리고 학교전산망에서는 방화벽만으로 모든 보안정책을 사용하고 있음으로 날로 새로운 기법과 기술이 향상되어 가는 해킹 및 침해사고 등에 취약한 일면을 가지고 있다. 또한 학교전산망의 운영과 보안에 관한 보안전문 인력의 부재로 인한 보안정책이 부실한 것이 현재의 실정이다. 그래서 학교 전산망에서 차후의 보안정책을 사용하기 위해 제안된 침입방지시스템을 방화벽, IDS 등의 보안시스템을 비교 분석해 분석을 해보면 <표44>와 같다[4, 18, 20].

< 표 44 > 보안장비의 비교 분석

평가부분	FireWall	IDS	IPS
보안정책	수동적	수동적	능동적
운영기반	네트워크	네트워크	네트워크, 호스트
패치방식	수작업	수작업	자동업데이트
내부자보안정책	낮다	보통	높다
바이러스대응	낮다	보통	높다
설치방법 및 운용	어렵다	어렵다	쉽다
보안정책의변경	어렵다	보통	쉽다
네트웍환경변화	고정적	고정적	유연성
알려진침해대응	낮다	보통	높다
꾸준한 모니터링	필요	필요	불필요
보안침해시대응	낮다	보통	높다
침해시보안대응시간	느리다	보통	빠르다
서버의 리소스 부하	높다	높다	낮다

<표44>에서 알 수 있듯이 현재 학교전산망에서 보안정책이 대부분 방화벽만으로 구성되어 있기 때문에 내부자의 보안침해와 바이러스에 의한 보안침해 사고에 대응하기에는 부적절하다. 그래서 차후의 보안 정책으로 거론되고 있는 침입탐지시스템의 도입과 침입방지시스템을 가격대비 성능을 <표45>를 통하여 비교, 분석해 보면 침입차단시스템의 경우 학교전산망에 납품한 S사의 가격은 소비자가격은 고가인데 실제납품가격은 교육기관을 고려하여 괄호안의 가격으로 견적되었다. 침입탐지시스

템은 국가보안등급 K4를 인정받은 S사의 장비가격을 1로 보면 E사의 침입방지시스템의 가격은 약 1.09배가 된다. 가격적인 부분은 침입탐지시스템의 가격이 유리하지만 별차이가 없다고 본다. 현재 침입방지시스템의 경우 잘 알려지지 않은 신기술로 개발업체가 소수이지만 대부분의 기업이 침입방지시스템의 중요성을 인식하여 개발중임으로 향후의 가격경쟁은 침입탐지장비보다 유리할 것으로 기대된다.

침입탐지시스템과 침입방지시스템의 기능은 침입차단시스템을 통과한 해킹에 대한 방어와 바이러스 등에 대한 방어기능 부분은 유사하고 내부자의 침입 시에는 침입방지시스템의 기능이 더 효율적이라 본다.

< 표 45 > 보안장비간의 가격비교 [단위 : 백만원]

	침입차단시스템	침입탐지시스템	침입방지시스템
가격	36(2.5)	16.5	18

편리성 측면에서는 침입탐지시스템은 방화벽을 통과한 침해와 내부자의 불법적인 행위에 대하여 로그의 기록과 보고 조치만을 취하기 때문에 침해되어진 바이러스 및 보안사고에 대한 조치기능이 미흡하다. 또한 침해 복구에 대한 새로운 보안정책 및 기술을 적용해야하고 그에 따른 복구시간을 필요로 하고 침해사고에 대한 대처방안이 수동적이다. 그래서 침입방지시스템을 사용하면 보안정책의 변경을 자동으로 업데이트 함으로서 침해에 대한 사전 차단과 복구에 대한 시간을 줄 일수 있으며 침해사고에 대해 능동적인 대처와 자동적인 처리를 함으로 편리성 측면에서 침입탐지시스템의 경우보다 더 편리하다고 분석되어 진다. 또한 설치시 네트워크의 환경과 장비간의 호환성 부분이나 트래픽 분석 등의 기간이 길지만 침입방지시스템의 경우 설치가 간편하다는 장점을 가지고 있다.

안전성의 측면에서는 침입탐지시스템은 표준화와 국가공인 등급인 K4등급과 신뢰성 등을 확보하고 있지만 침입방지시스템의 경우에는 최첨단의 신기술임으로 아직 표준화와 국가공인 등급을 부여받지 못하고 있지만 국가연구기관인 한국전자통신연구원 등에서 현재 사용하고 있으며 서울도시가스등의 공인업체에서 사용하고 있음으로 차후에 표준화와 국가공인 등급과 보안안전성을 확보하리라 본다.

확장성 측면의 분석은 침입탐지시스템은 H/W 일체형이라 네트워크의 환경이 변화에 기계적인 환경을 가지고 있음으로 확장이나 변경에 대한 적절한 대처에 한계성을 가지고 있지만 침입방지시스템의 경우에는 S/W적인 부분의 업그레이드로 설

치와 제거 확장성 부분에서는 IDS보다 더 효율적이라 볼 수 있겠다. 그래서 침입탐지시스템과 침입방지시스템의 비교 분석해 보면 침입방지시스템이 더 경제적이고 효율적이며 강력한 보안정책을 사용할 수 있을 것이라 본다.

이상과 같이 침입방지시스템의 도입에 따른 장비도입에 따른 가격대비 성능의 분석, 운영적인 측면, 관리적인 측면, 확장성, 안전성의 측면을 분석해 보았다. 위의 분석과정 중에서 가격적인 부분이 침입방지 부분이 조금 우세하지만 실시간 방어와 능동적인 방어체계의 부분이 뛰어나고 방화벽이 가지는 잦은 패치와 업그레이드 등의 전문적인 보안정책을 요구하는 보안장비의 문제를 침입방지시스템이 자동으로 업데이트 함으로 보안전문인력이 없는 학교의 현실을 고려한다면 운영적인 측면에서 훨씬 효과적이고 실용성을 가지는 보안정책이라 할 수 있겠다.

침입방지시스템을 도입함으로서 현재 방화벽이 가지는 침입차단의 기능을 더욱 활성화시킬 수 있고 방화벽의 단점으로 거론되고 있는 관리·운영의 어려움을 극복할 수 있고 새로운 보안정책의 적용을 위해 전문적인 보안기술의 적용하기 어려운 학교의 현실에 가장 적절하다고 기대된다. 따라서 본 논문에서는 방화벽만으로 구성되어진 학교전산망에서 차후의 보안정책으로 보안장비 도입시 침입방지시스템의 도입이 적절하고 효과적이라고 평가한다.

Ⅴ. 결론 및 향후과제

본 연구는 교육정보화의 국가적인 시책아래 물적 기반인 학교 전산망의 구축 완료된 시점에서 초·중등학교 학교 전산망이 인터넷과의 연동으로 해킹 및 침해사고로 인한 보안의 중요성이 강조되고 있어 날로 복잡해지고 다양화되어 가는 학교전산망의 종합적인 보안관리를 위하여 방화벽과 침입방지시스템의 연동을 통한 효율적인 학교전산망의 보안모델 구축을 제안하였다. 그러나 침입방지시스템과 방화벽과의 연동에 관한 부분이 국외 제품인 인터셉트의 경우에만 시스코사의 방화벽과 체크포인트사의 방화벽만이 연동 가능하고 현재 학내망에서 사용중인 시큐어웍스 방화벽과는 연동기능이 없다. 또한 국산 제품인 윈디사의 침입방지시스템의 경우 현재 방화벽 장비와의 연동 기능이 없어서 차후에 연동기능을 고려하고 있어서 침입방지시스템과 방화벽간의 연동기능 미흡으로 보안장비간에 서로 연동하여 관리할 수 있는 통합관제(ESM)와 종합적인 방어체계의 확립이 필요하다. 그리고 국가공인 K4인정과 같은 보안의 안전성 문제가 대두되고 있지만 차후 고려될 것이라 기대된다.

현재 학교전산망에서 방화벽의 보안기능이 설치업체의 최초의 셋팅에 의존하고 있으며 로그파일의 분석과 해킹기술의 패러다임의 변화에 따른 다양화와 첨단화되어 가는 침입기술에 대한 방어와 운영체제가 가지고 있는 버그 그리고 방화벽 자체의 결함 등으로 인한 꾸준한 패치와 업데이트 등 산재한 문제를 방치하고 있는 실정이다. 이와 같이 보안 정책과 보안장비를 운영하기 위한 보안전문가의 부재로 인해 보안의 부실을 초래하고 있어 보안전문가의 선정 및 보안을 전담할 수 있는 보안전문가의 양성이 무엇보다 우선해야 한다고 본다. 현재의 방화벽은 누가 네트워크에 있는 다른 기계에 연결할 능력이 있는지를 아는 것이 불가능하다. 필수적으로 요구되는 것은 네트워크의 외부에서 내부로, 접근을 시도하는 호스트에 더 가깝게 보안 기능을 옮기는 능력이다. 궁극적으로 이런 수준의 보안이 지원되기 위해서는 IPSEC 같은 보안 메커니즘이 요구된다[36].

향후 연구로는 현재 인터넷을 지원하는 TCP/IP V4의 보안 및 인증기능의 취약점을 해결하기 위한 차세대 인터넷인 TCP/IP V6의 도입과 OSI환경이 아닌 커널기반의 SECURE OS, 사이버 테러대응을 위한 컴퓨터 퍼런딕스와 같은 정보보안에 대한 개념이 현재의 수동적 대응에서 능동적 대응으로 바뀌고 있다. 이에 따라 외부침입에 대해 수동적으로 대응해온 기존 정보보안 솔루션의 개념이 네트워크와 시스템 구성

의 기본 인프라로서 침입을 원천 봉쇄하고 침입 자체를 역추적 하는 수준의 능동적 개념으로 진화될 전망이다. 최근 정보통신부가 오는 2009년까지 총 900억원을 투입하여 한국전자통신연구원과 한국정보보호진흥원을 통해 보안엔진 및 보안노드 시스템, 침입감내시스템(ITS), 보안등급(GOS)서비스 기술등 차세대 보안 솔루션 프로젝트를 수행하고 있다. 이와 같은 정보보안에 대한 새로운 기법이 제시되고 있는바 학교전산망에서도 점진적인 보안체제의 전환과 연구가 더 필요하다고 볼 수 있겠다.

참고문헌

[1] **유재택 외**, **교육기관 정보화 역기능 방지에 관한연구**, **한국교육학술정보원**, 2000

[2] **김학범**. **접근통제기술**, **한국정보보호센터**, 2001

[3] **정해귀**, Digital CS journal, 2002**년 1월호**. **통권 제**20**호**.

[4] **윈디시큐리티쿠퍼스**, Windy IPS**소개서**, 2002, http://www.nextwar.com

[5] **이카디아**, Entercept **소개서**, 2002, http://www.ekardia.com

[6] **이카디아**, Entercept 2.0 white paper, 2002, http://www.ekardia.com

[7] **이카디아**, Entercept 2.01 white paper, 2002, http://www.ekardia.com

[8] An entercept™ technologies white Paper, Entercepter e-SERVERS PROTECTION, 2002, HTTP://www.entercept.com

[9] An entercept™ technologies white Paper, Entercepter 2.0 white paper, 2002, HTTP://www.entercept.com

[10] An entercept™ technologies white Paper, Server Protection for today & Tomorrow, 2002, HTTP://www.entercept.com

[11] **안성수**, **침입차단시스템**, **한국정보보호센터**, 2001

[12] ETRI IT**정보센터**, **침입차단시스템** 30**대품목기술**/**시장통합요약보고서**, 2001

[13] **서울시교육청**, **전산보안 연수자료**, 2001

[14] **신성균외**, **교육정보화기반구축통합모델에 관한연구**, **멀티미디어교육지원센터**, 1998

[15] **김우곤**, **침입차단시스템**, **한국정보보호센터**, 2001

[16] Intrusion.com, Why Firewalls are Not Enough, 2001

[17] **기우서**, **학교 전산망 보호를 위한 방화벽에 관한 연구**, **석사학위논문**, 1999

[18] **이명일**, **종합보안관리시스템의 침입탐지시스템 구축에 관한 연구**, **석사학위논문**, 2000

[19] **박노동**, **학내전산망 구성과 활용 실태에 관한 연구**, **석사학위논문**, 2001

[20] **임채훈 외**, **인터넷보안**: VPN, FireWall/IDS **기술**, **한국통신학회 학술지기고문**, 2001

[21] **김상철**, **정보보호** 2001 **보안도구의 활용**, **해킹바이러스지원센터**, 2001 http://www.kisa.or.kr/

[22] **배병철**, **정보보호** 2001 **침입탐지 및 대응기술동향**, **국가보안기술연구소**, 2001 http://www.kisa.or.kr/

[23] **이은직**, **네트워크를 통한 침입방지 시스템에 관한 연구**, **석사학위논문**, 2000

[24] **문형돈외**, **침입탐지시스템 기술 및 시장 동향**, ETRI IT**정보센터**, 2000

[25] **한국전자통신연구원**, **정보보호 기술 개론서**, 1999

[26] **펜타시큐리티**, **침입탐지시스템**, 2001 http://www.pantasecurity.com

[27] **황성원**, 2001 CSI/FBI Computer Crime & Security Survey **분석**, 2001

[28] **황성원**, **정보보호산업최근동향**, **정보보호센터 동향분석**, 2001

[29] **길민정**, 2001**년 상반기 국내 정보보호 시장현황**, **정보보호센터 동향분석**, 2001

[30] **신상범**, **교육정보화에 따른 학교 전산망의 설계에 관한 연구**, **석사학위논문**, 2001

[31] **이상호**, **방화벽구축실무지침**, 1999.11 http://www.linuxlab.co.kr/

[32] **오영희**, Secuiry for UNIX+, **포항공대 유닉스 보안연구회**,1997

[33] An entercept™ technologies white Paper, System Call Interception, 2002, HTTP://www.entercept.com

[34] An entercept™ technologies white Paper, Attackers And Their Tool, 2002, HTTP://www.entercept.com

[35] Megan Restuccia, Firewall Load Bancers, November 21, 2000 http://www.sans.org/infosecFAQ/firewall/load_balancers.htm

[36] **박창윤외**, **컴퓨터네트워크**, **사이텍미디어**, 2001

[37] **서울여대**, **침입탐지시스템**, **대학동아리 최종 발표회 발표자료**, 2001 http://www.kucis.org

[38] **김기현**, **침입탐지시스템 제품동향**, **한국정보보호진흥원**, 1999

[39] **한국정보보호진흥원**, **각국 정보화정책과 그에 따른 예측가능한 위험요소연구**, 2000

감사의 글

학위논문 겉 표지의 검은색은 수많은 밤을 지새우고, 황금 글씨는 학문에 대한 열정과 땀으로 어둠을 밝히는 찬란한 지식의 금빛을 발하기까지 수많은 시행착오와 시련의 완성임을 몰랐기에 그 동안 짧은 지식으로 안달하고 자만하던 지난날들에 짙은 부끄러움을 느낍니다. 먼저 오늘이 있기까지 저의 든든한 믿음이며 학문적으로 정신적으로 저를 이끌어주신 존경하는 김창수 지도 교수님께 진심으로 깊은 감사를 드립니다. 부족한 저의 논문이 완성되기까지 많은 가르침을 주셨던 김영봉 교수님, 박승섭 교수님 부족한 저에게 소중한 가르침을 주신 여정모 교수님, 박흥복 교수님, 윤성대 교수님, 이경현 교수님, 박지환 교수님, 박만곤 교수님, 정순호 교수님께 감사를 드립니다.

불혹(不惑)의 나이에 논문을 쓰면서 새삼 제 주위의 많은 사람들의 고마움 속에 살고 있었음에 소중함과 감사를 드립니다. 혼돈 속에서 방황할 때 힘이 되어준 친구들, 조언을 해 주시는 많은 선배님들, 자신감을 잃지 않게 도와준 동기들, 어려움을 함께 해준 사랑하는 가족, 너무 어렵고 힘이 들었을 때 뒷받침을 해주신 지도 교수님, 연구실 가족들의 성원으로 제가 논문을 완성할 수 있었기에 다시 한번 머리 숙여 모든 분께 감사를 드립니다.

병환에 시달리면서도 자식의 걱정을 해 주신 저의 자랑스런 아버지 장승, 어머니 김춘자님 두 분 모두의 건강과 쾌유를 바라며 감사 드립니다.

존경하는 장인 김명조님과 오늘이 있기까지 저의 자식들을 돌봐주시고 뒷바라지를 해주신 장모 김정순 여사님 두 분 모두의 건강을 빌며 감사 드립니다. 또한 언제나 한결같은 믿음과 사랑으로 묵묵히 인내해준 저의 사랑스럽고 예쁜 아내 미경과 밝은 미소와 재롱으로 시름을 잊게 해준 사랑하는 두 아들 형록, 형래에게 고마움과 아버지의 사랑을 전합니다. 그리고 많은 날을 같이 해주셨던 고인이 되신 저의 작은 아버지 장월태님의 임종 앞에 본 논문을 전하고 싶습니다.

항상 자신의 일처럼 걱정하며 도와주신 연구실의 모든 가족들에게 깊은 감사를 드립니다. 그리고 저의 논문이 완성되기까지 많은 도움을 주신 부산정보고등학교의 이승헌 이사장님과 김원일 교장선생님 이하 전 교직원 선생님께 감사를 드립니다.

마지막으로 저의 동기(정동호 님, 박철동 님, 변옥남 님, 현영숙 님)께 감사와 졸업을 축하드립니다.

부족하고 서투른 저를 이렇게 이끌어 주신 모든 분들께 이 논문을 바칩니다.

2002년 8월

장 용 호