정보학연구 제6권 제4호 2003년 12월(pp.35-58)
The Journal of Information Technology, Vol.6, No.4

NEIS의 취약성에 관한 연구

우승호* · 강순덕**

요 약

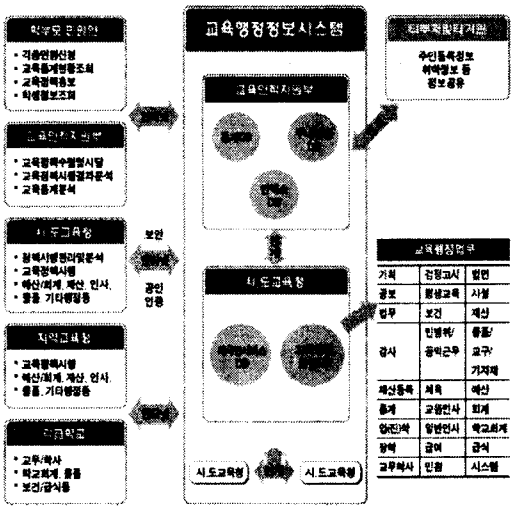
본 연구에서는 NEIS(National Education Information System)의 시스템취약성에 관한 보완 방향을 분석하여 구체적인 보완의 방향(효율성, 분리성, 편의성, 다양성, 종합성, 보안성)을 제시하므로써 보안사고를 사전에 예방하고 발생가능한 문제점을 실시간으로 점검하도록하여 보다 나은 NEIS의 구축을 위한 병렬보안 취약성 진단 시스템을 구현하므로써 보안의 효율성을 높이는데 목적을 둔다.

Ⅰ. 서론

현대는 무선과 화상회의, 다차원 인터페이스인 유비쿼터스(Ubiquitous)시대로, 유비쿼터스의 교육 즉, e-learning이 대두되어 교육계에서도 이에 순응하는 차원에서 교육행정정보시스템(이하 NEIS)를 구축하여 도입을 추진 중이다.

21세기 국가 경쟁력확보, 교육행정의 전자정부 구현, 교육행정의 정보화로 생산성 극대화, 교원 업무경감 개인정보 유출 및 교육활동의 계량화 즉 학교종합정보관리시스템에 권한 관리, 감시모니터의 미비로 데이터가 한곳에 집중되 유출에 따른 위험성이 상대적으로 큰 것으로 예상된다.[12]

NEIS(National Education Information System)는 전국 1만여 개의 초.중등학교, 16개 시·도교육청 및 산하기관, 교육인적자원부를 인터넷으로 연결하여 교육관련 정보를 공동으로 이용할 전산환경을 구축하는 전국 단위의 교육행정정보시스템이다. [11]



(그림 1) NEIS의 개념도

NEIS는 인증은 PKI기반 인증 솔루션, 권한관리는 통합인증권한관리(EAM), 접근통제는 Firewall, IDS, 서버보안솔루션, 암호화는 인증, 데이터 암호화, 감시, 모니터는 보안 로그관리 기능이다.

학교 종합정보관리 시스템(Client/Server)의

* 공주대학교 컴퓨터공학과
** 공주대학교 컴퓨터공학과

인증은 ID와 Password, 권한관리는 없고, 접근통제는 Firewall, 암호화는 간단한 인증암호화, 감시, 모니터는 없다.

NEIS시스템은 미국 캘리포니아의 초중고 교육시스템에 바탕을 두어 개발한 것으로 미국의 경우 보안 취약성의 현황은 주요기반 구조보호뿐만 아니라 공중 전화망과 인터넷에 대한 의존도가 증가, 컴퓨터, 네트워크 활용의 증가로 인하여 취약성이 발생되므로 즉 정보 및 통신분야도 취약성문제를 법적으로 규제하고 있다.[4], [5],[6]

그러나 한국의 실정은 공공기관만이 취약성과 관계된 법령 "정보통신기반보호법시행령" - 재정/시행 2001.7.16/대통령령 제 17308호 제 16조, 제 17조, 제 18조, 제 20조이며, 이에 근거하여 통제되고 있을 뿐이다.

현재 일부에서 부분 시행을 강행하기도 하였는데, 고교교사에게 해킹을 당하는 등 취약성에 대한 문제가 제기 되면서 시행여부에 난항을 겪고 있다. 올 초에 발생한 인터넷 대란으로 보안에 대한 관심이 높아지고 있는 가운데 위와 같은 사건이 발생하자, NEIS에 대한 보안상 문제점이 이슈가 되었다. NEIS는 첫째. 수기장부에 비해서 수정이 용이하다. 둘째. C/S에 있던 학교정보 담당자의 서버 관리가 도교육청으로 넘어감에 따른 업무의 경감. 셋째. 학교급간의 자료이송으로 인해 학사 업무가 신속하고 정확해진다. 넷째. 나이스의 자료를 담임이나 교과 선생님이 엑셀 파일로 저장하여 활용할 수 있다. 다섯째. 학부모들의 알 권리를 충족. 여섯째. 재 증명의 발급용이. 일곱째. 교무/학사와 연계된 교원인사나 통계 부문에서의 원활한 처리를 위해 만들었다. NEIS의 문제점으로 제기되고 있는 사항은 첫째. 학생과 학부모, 교사의 신상 정보를 본인의 동의 없이 관리함으로써 개인 정보 유출과 인권 침해의 가능성이 높은 단점이 있다. 둘째. 각 교육청에 집중된 정보를 다른 국가기관이 활용할 경우 일반 국민의 감시 및 통제 수단으로 이용될 가능이 있는 단점이 있다. 셋째. 행정적인 업무처리면에서의 교사와 학생의 창의성과 자율성 침해. 넷째. 이전 사용하던 학교종합정보시스템(CS)의 철회에 따른 활용미비. 다섯째. 국내나 국외의 해커들에 의한 해킹 및 바이러스의 위협이다.[12] 이 모든 문제의 기본적인 제반사항의 핵심은 보안에 기인한다.

해킹등 외부침입을 막는 접근통제는 방화벽과 IDS 서버보안솔루션을 갖추고 있다. 또한 데이터가 유출되더라도 이를 악용할 수 없도록 인증과 데이터 암호 모두를 구현하였다. 감시 및 모니터링은 보안 로그를 포함해 다양한 관리기능이 있다. [14],[15],[16],[17],[18]

현재 NEIS는 사회적 이슈로 떠올랐기 때문에 더욱 해커들의 표적이 되기 쉬우며, 이에 대한 보완 대책이 필요하다.

본 연구는 NEIS의 보안 기술과 보안윤리를 강화하기 위해서 특히 보안문제 중 취약성 문제인 정보보안측면에서 개인 정보 유출 가능성이 있는 시스템의 취약성 및 해킹과 바이러스에 대한 취약성을 항목별로 1. 사용자 계정, 2. 파일 접근권한, 3. 파일 변경사항, 4. 특수파일, 5. 로그인 기록, 6. 네트워크 무결성, 7. OS 패치, 8. 시스템 메일, 9. 레지스트리, 10. 예약 실행, 11. 사용자 패스워드, 12. 시스템 초기설정, 13. 사용자 파일, 14. 관리자 환경, 15. 유틸리티, 16. 네트워크 접근 가능성, 17. 웹 취약성, 18. 바이러스(only WinNT/2k)에 중점을 두었다.

<그림15>는 취약성의 구조를 3-Tier로 구현하고, <그림 16,17,18>은 취약성 도구, <그림

19>는 종합보고서, <그림20>상세보고서, <그림21>모듈별보고서, <그림22>점검결과 상세보고서, <그림23>요약보고서, <그림24>통계보고서, <그림25>상세보고서이다.

이 취약성분석 도구는 병렬적 보안취약성 진단을 함으로써 취약점검은 물론 효율성, 분리성, 편의성, 다양성, 종합성, 보안성을 높여 정기적인 감사 및 가시적인 보안 규칙의 집행으로 2003년 1월25일의 인터넷 대란, 현재 침해사고, 침해사고 사후추적 가능하므로 해커들의 침입을 예방이 가능하도록 진단한다.

II. 본론

본 연구에서는 NEIS의 제반문제 즉, 보안문제와 기존 C/S의 활용에 관하여 연구하였으며, 기존 시스템구성과 보안 대책을 보고 서버 및 네트워크 취약성에 대한 보완에 대한 대안을 제시할 것이다.

2.1. NEIS 보안정책

2.1.1. 보안시스템 구성도

교육인적자원부에서 운영되는 교육행정정보시스템을 위한 보안시스템 구성은 <그림 2>와 같다.

2.2.2. 항목별 보안 대책

가. 네트워크 보안

-외부전산망으로부터 불법침입 방지와 내부망의 불법정보 유출방지

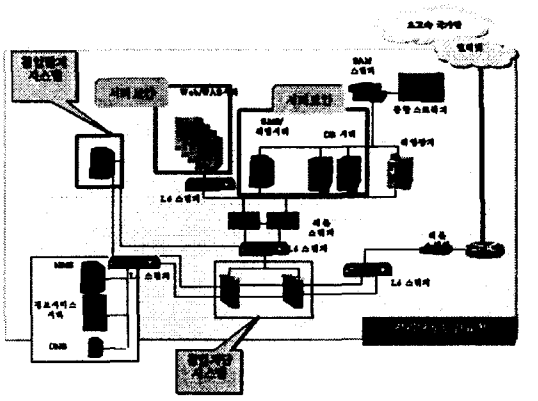
-네트워크를 통한 공격에 대비하고 보안침해 징후에 대한 정보를 분석해 실시간으로 탐지 및 통보

-네트워크에서 자료 유통의 기밀성 및 무결성 확보

해결방안:

· 네트워크 보안 대책(침입차단, 침입탐지)

· 개인정보 및 송·수신 데이터 암호화



(그림 2) 보안시스템 구성도

나. 비인가자 접근방지

-사용이 인가되고 권한이 있는 사람만이 정보에 접근할 수 있도록 관리

-서버에 대한 접근제어 및 사용자 관리

해결방안 : 전자서명을 통한 사용자 권한관리 및 접근제어, 서버보안

다. 개인정보 유출방지

-인가되지 않은 사용자에 의한 교육관련 정보, 시험관련 정보, 급여관련 정보, 주민등록 등 개인정보 조회 금지

해결방안

· 개인정보 및 송·수신 데이터 암호화

· 사용자 권한관리 및 DB 데이터 암호화

라. 정보 위·변조 방지

-송수신되는 각종 보고서, 통계자료, 시험관련

자료, 감사 및 장학 관련 자료 등의 데이터가 위·변조 되어서는 안됨
-비인가자에 의한 송·수신인 위장
해결방안 : 전자서명

마. 정보 제공자/수신자 인증 및 신원확인
-각종 증명서 발행 기관이 각급 해당 기관임을 인증
-각종 증명서 신청자가 본인임을 인증, 확인
-각종 증명 신청서 수신자가 각급 해당 기관임을 인증
-각종 응시원서 신청자가 본인임을 인증, 확인
-각종 응시원서 수신자가 각급 해당 기관임을 인증
-예산/회계/감사 자료 취합 시 제공 및 수신 기관 인증
해결방안 : 전자서명, 신원확인

바. 정보 제공자 및 수신자 부인방지
-각종 증명서 수신 또는 증명, 신청서 수신 사실부인에 대한 대응
-각종 응시원서 수신 또는 응시 신청서 수신 사실부인에 대한 대응
-예산/회계/감사 자료 수신 사실부인에 대한 대응
해결방안 : 전자서명을 통한 수·발신 부인방지, 시점 부인방지

사. 정보고속망(G4C) 연동 보안
-연동기관망에서 정부고속망 내부로의 불법침입 방지
-정보 위·변조 방지
해결방안
·네트워크 보안 대책(침입차단, 침입탐지)
·연계서버에서 XML로 변환 후 G4C보안 모듈을 통한 암호화 송신

2.2.3. 네트워크 보안
교육행정정보시스템은 교육인적자원부 및 16개 시·도교육청, 관련부처, 학부모, 학생, 기타 민원인 등 다양하고 광범위한 경로를 통해 서비스를 제공하므로 네트워크를 통해 권한 없는 자의 접근으로부터 시스템을 보호하기 위한 적절한 보안통제가 이루어진다. 네트워크는 내부망과 외부망을 분리 운영하며, 외부 트래픽은 반드시 침입차단시스템을 경유하게 함으로써 비인가자에 대한 침입을 차단해 위험범위를 좁히고, 침입차단시스템을 통과한 사용자 또는 내부 사용자에 의한 침입 시도를 사전에 탐지해 예방하도록 구성하여 교육행정정보시스템의 네트워크를 보호한다.

가. 보안시스템 접근 통제
-침입차단시스템 및 침입탐지시스템으로의 로그인 통제
-관리자 이외의 사용자 등록 제한
-시스템 조작을 콘솔에서 하거나 리모트에서 접속할 수 있는 단말을 제한

나. 외부망과의 분리
-내부망과 외부망은 물리적으로 분리
-서비스 영역(DMZ)을 내부망과 분리
-게이트웨이 보안
·모든 트래픽에 대해 침입차단시스템을 경유하게 함
·외부망으로부터의 비인가된 접근방지
·인가된 망 내부에서 외부로의 특정서비스 사용 통제
-침입차단시스템을 이용한 네트워크 접근제어
·패킷 필터링을 통한 접근제어

· 응용 계층상의 게이트웨이를 통한 접근제어
· 출발지 주소, 목적지 주소, 서비스 별 접근 제어
· 서비스별, 사용자별 접근 가능한 시간대 설정

다. 실시간 탐지 및 차단

-침입차단시스템을 통과한 트래픽에 대한 2차 방어
-내부망과 서비스 영역(DMZ)으로의 침입시도 탐지 및 차단
· 실시간 침입탐지 / 차단
· 실시간 접속감시 / 차단
· 실시간 네트워크 감시
· 실시간 네트워크 접속목록 표시
· 실시간 정보유출 탐지 / 차단
· 실시간 로그관리
· 침입탐지 시 경고
-침입차단시스템과 연동을 통한 자동 대응

▣ 네트워크 보안 정책

가. 침입차단시스템

-시스템 설치
· 외부에서 내부로 접근하기 전에 침입차단시스템으로 1차보안구간 설정
· 서비스영역의 Access는 반드시 침입차단시스템을 거치도록 구성하고 외부에 오픈되어야 할 서버는 서비스 영역에 두어 내부 네트워크와 분리
· 침입차단시스템을 우회해 통제 없이 연결되는 경로가 존재해서는 안됨
-침입차단 정책
· 접속을 허용하는 서비스 포트 이외에는 모든 서비스 포트로의 접속을 거부
· 내부 사용자가 FTP, Telnet 등 특정 서비스를 이용해 외부망에 접속하는 것을 금지함
-로깅 및 감사
· 침입차단시스템을 통과하는 모든 트래픽은 로깅 되어야 함
· 침입차단시스템의 로그 기록 데이터는 매일 점검 함
· 침입차단시스템에 설정된 보안 규칙이 관리자의 의도와 일치되는지 주기적으로 확인
-시스템 관리
· 침입차단시스템의 설정에 대한 무결성 점검은 주기적으로 실시 함
· 침입차단시스템은 최소한의 서비스 포트와 기능만을 적용하며 사용 목적 이외의 기능 및 프로그램은 제거하거나 사용을 중지함
· 침입차단시스템은 관리자를 지정하여 운영하고 관리자 이외의 접근을 통제함
· 침입차단시스템의 설정은 주기적으로 백업함

나. 침입탐지시스템

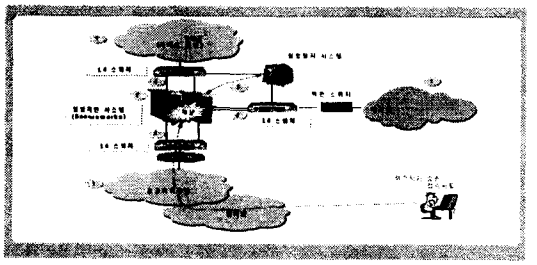
-시스템 설치
· 내부 시스템을 보호하기 위해 침입탐지시스템으로 2차보안구간 설정하여 네트워크를 감시함
- 침입탐지 정책
· 최신의 침입탐지 정책이 항상 유지되도록 관리 함
-로깅 및 감사
· 침입탐지시스템에 설정된 보안 규칙이 관리자의 의도와 일치되는지 주기적으로 확인
· 침입탐지시스템의 로그 기록 데이터는 매일 점검함
-시스템 관리
· 침입탐지시스템은 관리자를 지정하여 운영하고 관리자 이외의 접근을 통제함.
· 침입탐지시스템은 최소한의 서비스 포트와

기능만을 적용하며 사용 목적 이외의 기능 및 프로그램은 제거 하거나 사용을 중지함
- 침입탐지시스템은 관리자를 지정하여 운영하고 관리자 이외의 접근을 통제함
- 침입탐지시스템의 설정은 주기적으로 백업함

다. 침입차단시스템 구성

도교육청에 내부망과 외부망 연결지점에 침입차단시스템으로 K4E1 인증 제품인 Secureworks v3.0을 설치해 외부로부터의 접근을 차단하고 침입탐지시스템과의 연동을 통해 침입에 자동 대응한다.

○ 구현형태



(그림 3) 침입차단 시스템 구현형태

○ 구현내용

① 네트워크 분리
- 외부망으로부터 전라남도교육청 시스템 내부의 사설망을 보호하기 위한 네트워크 보안 장치로 침입차단시스템을 설치
- 외부망과 전라남도교육청의 내부망 사이에 위치해 내부 정보에 대한 외부 사용자의 접근을 제어함으로써 네트워크를 통한 침입 및 불법 정보유출을 방지
- DNS 서버와 NMS 서버, 정보서비스 서버 등 공개용 서버를 별도의 네트워크(DMZ)로 구분해 내부망과 분리하고, 이 서비스 영역의 접근은 반드시 침입차단시스템을 거치도록 구성하여 인터넷상에서의 불특정 다수로부터 접근제어
- 서비스 영역(DMZ)의 공개용 서버와 내부 주요 서버에 대한 차등화된 보안정책 운영

② 이중화
- 침입차단시스템의 효율적인 사용 및 사용자에게 빠른 서비스를 제공하기 위해 L4 스위치를 사용한 로드 밸런싱을 구현하고 이중화함으로서 트래픽의 분산과 무정지시스템 구현
- 인터넷 트래픽의 분산화로 인하여 속도를 향상시키고 Single of Failure의 문제점을 해결

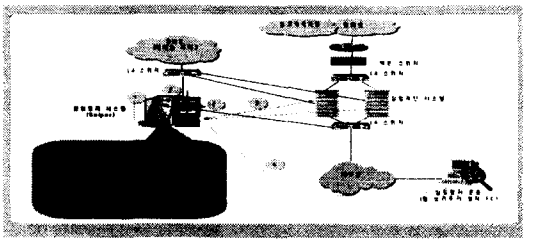
③ 자동대응 및 차단
- 침입차단시스템과 침입탐지시스템을 상호 연동하여 침입탐지시스템에서 탐지된 침입자에 대한 정보를 바탕으로 침입차단시스템이 실시간으로 해당 공격을 최전방에서 원천 봉쇄
- 침입탐지시스템은 해킹이라고 판단되는 Session 정보를 침입차단시스템으로 송부하고, 침입차단시스템은 일시적인 Rule을 생성하여 해당 세션을 Blocking시키고 관련 정보를 로그에 남기게 됨으로써 보안 솔루션간의 미흡한 점을 보완하여 효율적인 운영

④ 확장성
- 외부 연계가 계속 증가되므로 확장성이 유연한 시스템으로 구성
- 인터넷 사용량 증가 및 백업을 위해 필요시 침입차단시스템 증설
- 침입차단시스템과 L4 스위치간에 초고속 네트워크 환경인 Gigabit Ethernet 환경을 지원함으로써 네트워크 병목현상을 최소화하고 향후 확장을 대비

라. 침입탐지시스템 구성

전라남도교육청에 침입탐지시스템으로 K4 인증 제품인 윈스테크넷의 Sniper v2.0을 설치 스위치 장비의 미러링 기능과 멀티포트 기능을 이용하여 내부망과 서비스 영역(DMZ)을 실시간으로 모니터링 하도록 구성하며, 침입차단시스템과의 연동을 통해 침입에 자동 대응

○ 구현형태



(그림 4) 침입탐지 시스템 구현형태

○ 구현내용

① 감시기능

· 해킹의 피해로부터 시스템을 보호하기 위하여 시스템 내부로 침투하는 여러 가지 방식의 해킹시도를 무력화 시킴

· 해킹 수법을 자체적으로 내장하고 침입행동을 실시간으로 감지하고 제어

· 24시간 네트워크 감시기능을 이용하여 보안의 허점이나 내부 네트워크의 오용으로부터 시스템에 피해가 발생하기 전에 관리자가 상황을 인식할 수 있도록 자동으로 탐지하여 통보하고 대응

② Stealth 모드 설정

· 침입차단시스템을 통과해 내부망 침입을 시도하는 트래픽을 탐지, 멀티포트지원 기능을 이용해 서비스 영역(DMZ)을 동시에 모니터링

· 침입탐지시스템의 모니터링 포트는 IP 주소를 숨기는 Stealth 모드로 설정

· 대용량 트래픽 처리를 위해 Gigabit 인터페이스 지원

③ 침입차단시스템 연동

· 침입탐지시스템에서 공격이 탐지되면 관련 차단 정책을 침입차단시스템에 자동 생성해 침입시도를 차단

④ 모니터링

· 침입탐지 상황 및 시스템 운영 상황은 로컬 또는 리모트의 콘솔을 통해 모니터링

■ 서버보안

교육행정정보시스템을 구성하는 서버들은 역할에 따라 다양한 계정 그룹을 가지게 되며 서버 및 계정 그룹에 따라 별도의 권한을 부여해야 한다. 계정 관리 및 권한에 따른 접근제어는 서버 보안의 대부분을 차지하며 특히 분산된 서버운영 환경에서 적절한 수준의 관리를 유지하기가 어려우므로 이에 대한 대책을 마련한다.

서버보안 시스템은 UNIX 사용자의 계정 관리 기능과 접근제어 기능, 권한관리 기능, 로깅 및 모니터링 기능을 통해 전국단위 교육행정정보시스템을 위한 서버보안을 강화시킨다.

① 서버보안 방안

가. 계정관리

-계정의 환경점검(유효기간, 사용 쉘 등)

-계정의 특성에 의한 그룹화

-새로운 계정에 대한 보안 정책 자동 적용

-단기간 서버 사용을 위한 계정의 Lifetime 설정

-주요 계정 보호를 위한 동시 사용 세션 제한

-주요 계정 보호를 위한 Login 시도 제한

-계정 패스워드 정보의 별도 관리

-계정 패스워드 설정에 관한 강제 제한(길이, 복잡성 등)

나. 접근제어
-허용된 단말기 또는 콘솔에서의 접근제어
-로그인 시도 실패 시 접근제어
-계정별 서버에 접근할 수 있는 시간대를 여러 유형으로 제어
-미사용 시 화면보호기를 통한 접근제어
-주요 파일, 프로세스, 서비스에 대한 접근제어
-root 권한을 얻을 수 있는 사용자 제한
-root 계정에 대해 자원에 대한 접근제어

다. 로깅/모니터링
-서버별 보안 현황 관리
-계정 그룹별 로그 관리
-암호만료, 사용자프로필 감시
-배치작업 감시
-시스템 로그 이벤트 감시 및 시스템 이벤트 기록 보호
-보안 프로그램 자체에 대한 보호 기능
-주요 파일에 대한 무결성 점검, 변경된 파일의 실행 차단

② 서버보안 정책
가. 계정 및 패스워드 관리
-패스워드 재사용 금지
-패스워드에는 사용자 ID가 포함될 수 없음
-패스워드는 영숫자를 혼합해 설정
-패스워드 사용주기 및 최소길이 지정
-접근 거부된 계정은 관리자에 의해서만 리셋
-로그인 시도횟수를 제한
-슈퍼유저 계정은 콘솔에서만 로그인하거나 특정 단말에서만 로그인할 수 있도록 제한

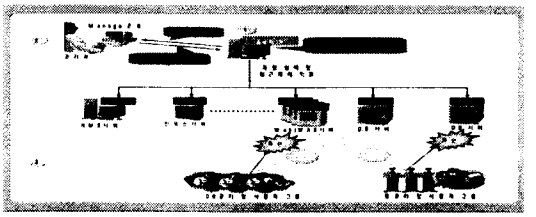
나. 권한관리
-슈퍼유저에게만 서버의 모든 자원 접근 허용
-시스템 어플리케이션 관리자는 슈퍼유저 권한을 일부 통제하고 시스템 자원 일부만 접근 허용
-어플리케이션 개발자 및 일반 사용자는 슈퍼유저 권한을 통제하고 시스템 자원 접근을 통제
-슈퍼유저 권한으로 실행되는 프로그램의 사용을 제한
-파일과 디렉토리에 대한 접근을 제한

다. 서버관리
-신규서버는 디폴트 계정 및 패스워드를 삭제하거나 변경하고 알려진 취약점을 조치한 후 네트워크에 연결
-사용중인 소프트웨어에 대해서는 최신의 보안 패치를 적용
-필요치 않거나 사용되지 않는 OS, 네트워크 서비스는 제거하거나 중지
-모든 계정의 로그인 및 사용내역은 로그 파일에 기록되어 일정기간 이상 보관
-중요한 파일에 대한 접근, 수정, 삭제 내역은 기록되어 일정기간 이상 보관

③ 서버보안 구성

시스템 계정관리와 패스워드 관리를 통해 로그인 시 인증을 보다 강화하고 서버에 대한 계정별 접근제어를 설정해 불법접근에 의한 사고에 대비한다. 이러한 서버 보안 정책은, 모든 대상 서버에 시큐브의 TOS를 설치하고 Admin 역할을 하는 보안관리 서버를 선정한 후, 이 서버를 통해 각 보안대상 서버에 일관되게 적용된다.

가. 구성내용
① Admin 서버에서 각각의 관리대상 서버에 등록된 사용자들의 정의 및 관리하는 Admin 작업 수행



(그림 5) 서버보안

② Manager 콘솔의 Report기능을 이용하여 서버 보안과 관련된 여러 가지 자료를 얻을 수 있으며, 여러서버에 대한 접근제어 기능을 강화

③ 적용된 서버 보안 정책에 따라 계정 및 그룹별 접근제어

④ 서버보안 정책 적용

가. 구현형태

(그림 6) 서버보안 구현형태

나. 구현내용

① 관리단위별로 일관된 서버 보안정책 수립 및 위반사항 점검, 수정, 감사, 보고 체계 구축

② 서버보안 관리자가 서버보안 정책을 정의하고 이를 관리서버에서 적용해 운영하며, 다양한 보고서를 통하여 보안성의 문제점을 파악하는 등 전체 서버보안 정책을 일관서 있게 적용

· root 계정 기능분산 및 접근권한 제어
· 계정 및 패스워드 관리
· 터미널 및 콘솔에서의 서버 접근제어 설정
· 로그인한 사용자에 대하여 시스템 내부의 파일 또는 특정 프로세스에 대한 접근제어
· 시스템 접근내역 로깅
· Manager Console은 X-터미널 또는 Window NT, Window2000(Professional or Server)에 설치

■ 데이터 보안(인증 및 암호화)

PKI(Public Key Infrastructure, 공개키 기반구조)는 정보시스템에 안전성을 부여하고 통신시스템의 신뢰성을 높이기 위한 기반구조로, 네트워크상에 연결된 각 사용자 및 메시지에 대한 인증기능을 부여하기 위해서 공개키 방식을 이용한 인증용 기반구조로 암호학적 키와 인증서(Certificate)의 배달 시스템이라고도 한다.

인증서 기반의 인증 및 전자서명, 암호화 기술을 적용하여 개방된 웹 프로그램에서 발생할 수 있는 데이터의 노출, 위·변조, 신원확인 문제, 법적효력 문제 등을 해결하여 교육행정정보시스템의 안전성과 신뢰성이 확보되도록 한다.

교육행정정보시스템의 보안서비스 구현형태는 다음과 같다.

○ 사용자 인증
-X.509 기반 강한 인증 구현
-송신자 : 전자서명 생성 및 전송
· 인증서의 대칭키 암호화용 개인키와 Time Stamp를 이용하여 전자서명 생성 후 서버로 전송
-서버 : 전자서명 검사

○ 기밀성
-사용자와 교육행정서버간 End-to-End 암호화 적용
· 교육행정시스템 Client : 암호화 및 복호화
· DB서버에는 암호화된 상태로 저장
-사용자와 교육행정서버간 검정고시 정답, 임용고시 정답의 End-to -End 암호화는 정보보호센터의 SEED 알고리즘 적용

○ 무결성
-사용자 : Client와 WAS서버간 전자서명 적용
-WAS서버 : 전자서명된 주요 Data의 무결성 검사
-DB서버 : 전자서명된 Data의 보관

① 사용자 인증

교육행정정보시스템은 교육인적자원부 및 16개 시·도교육청, G4C 등 관련 부처간 연계가 필요한 부분과 민원인과의 연계 두 가지 부분이 존재함으로 공인 인증기관 기반(NPKI)의 인증 인프라를 사용한다.

인증 인프라 확산을 위하여, 기 구축된 공인인증기관의 인증 인프라를 수용하고, 교육인적자원부에는 등록관리 시스템인 RA 서버를, 16개 시·도교육청에는 등록관리 시스템과 연계되는 BRA 서버를 설치하여 사용자에게 편리한 인증서 등록환경을 제공한다.

가. 인증서비스 기관 및 대상

인증서비스를 제공하는 기관과 그 대상은 다음과 같다.

-한국전산원
· 교육인적자원부 및 16개 시·도교육청, 각급 국·공립 학교 교직원, 사립 학교 교직원

나. 인증서비스 적용방안

인증서비스 적용 방안은 다음과 같다.

-인증서 상호연동
· 지정 공인인증기관이외의 공인인증기관은 등록대행은 하지 않으나 모든 공인인증기관에서 발급한 인증서를 수용할 수 있도록 상호연동
-사용자 등록
· 교육인적자원부에 RA서버와, 전라남도교육청에서 BRA를 이용하여 등록대행서비스를 실시
· 전라남도교육청에서 학적, 인사 DB를 이용하여 사용자 정보를 공인 인증기관으로 일괄/수시 등록 처리

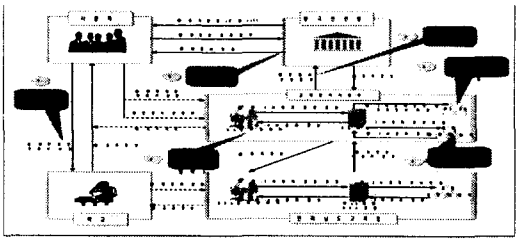
다. 인증기반 구축

전자문서를 거래하는 사용자 상호간의 신뢰성 있는 거래를 보장하기 위하여 공인인증기관(한국전산원)의 인증서비스를 지원 받아 인증기반을 구축

-공인인증기관 서비스 사용
· 한국전산원에 구축된 인증서비스를 이용
-등록관리 서버
· 사용자의 신분을 확인하고 사용자 정보를 인증기관에 제공함으로써 인증기관 인증서 발행의 신뢰성을 확보
· 인증서비스의 중계 및 관리기능을 지원
-암호화 및 전자서명 모듈
· 인증과 관련된 서비스를 제공
· 중요 Data(근무성적평정, 학생성적 등)의 암호화 및 전자서명 기능을 제공

라. 인증서비스 처리 흐름

인증서를 발급받기 위한 흐름도는 다음과 같다.



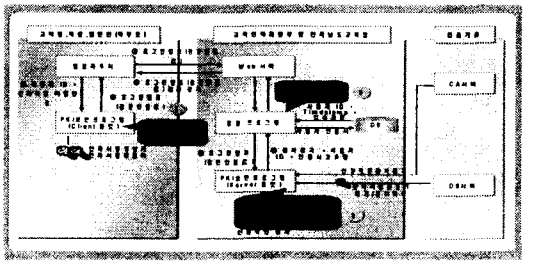
(그림 7) 인증서비스 흐름도

① 대면확인을 통한 신원확인
② RA/BRA 관리자가 인증서 신청서를 통한 신원정보 입력
③ 교원, 일반직, 기타직 테이블을 이용한 사용자 신원확인
④ RA를 이용한 인증기관(CA)로의 신원정보 전송
⑤ 등록정보(참조번호,인가코드) 사용자에게 통보 및 인증서 정보 저장
⑥ 사용자는 등록정보를 인증기관에 등록 후 인증서 발급

마. 접속인증 형태

전자서명을 사용한 강한 인증(Strong Authentication)을 적용한다. 강한 인증값 생성시 Time Stamp를 적용하여 이전의 접속인증값 재사용을 방지한다.

인증서 발급 후 접속인증은 다음과 같다.



(그림 8) 접속인증 형태

① 사용자의 전자서명 인증서를 이용하여 로그인정보(강한 인증값)를 생성하여 웹 서버로 전송. 로그인정보는 사용자의 ID, 사용자의 인증서, 사용자의 전자서명, Timestamp를 포함

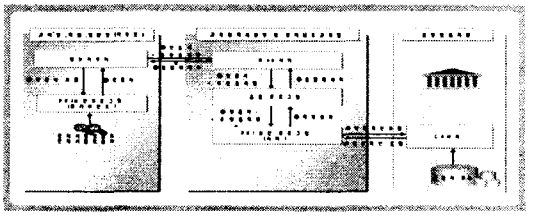
② 사용자로부터 전송받은 로그인 정보는 보안 프로그램에서 사용자 전자서명 검사, 인증서의 유효성 및 신원확인을 검사하고 검사결과를 응용 프로그램으로 전달

③ 응용 프로그램은 사용자 등록 DB에 사용자등록 여부를 확인한 후 Timestamp, 접속권한을 검사한 후 접속권한을 응용프로그램에 설정, 사용자 DB에 사용자의 인증서가 등록되어 있지 않으면 인증서를 사용자 DB에 등록

바. 신원확인

ON-LINE상의 인증서가 필요한 실제 사용자에 대한 공인인증기관의 신원확인 서비스를 이용하여 비인가자에 의한 인증서 불법도용 및 개인정보 유출을 방지하여 시스템의 신뢰성을 증가 시킨다.

사용자 신원확인은 다음과 같다.



(그림 9) 신원확인

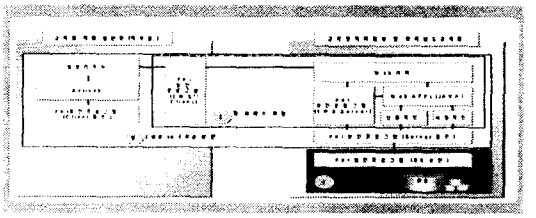
② 전자서명 및 암호화 적용

개방된 인터넷 환경에서 정보보호를 위한 웹 서비스 보안, 지정된 송·수신자 사이의 END to END 보안, 접근권한이 있는 그룹만이 정보의 변경 및 조회할 수 있는 DB 보안을 적용 통합적인 관점에서 응용 프로그램 보안을 구성한다.

-RSA With SHA1 전자서명 알고리즘 적용.

-SEED 전자신고서 알고리즘 적용
-전자서명과 암호화를 위한 개인키와 공개키를 각각 생성, 운영
-개인키는 SEED 알고리즘을 적용한 PBE (Password Based Encryption) 방식으로 암호화하여 PC에 저장 활용

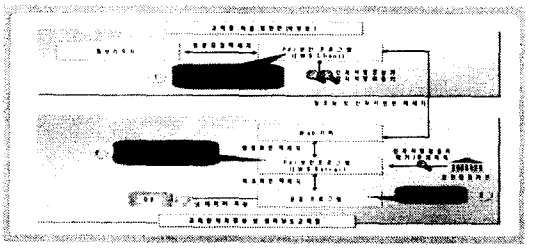
보안적용 영역은 다음과 같다.



(그림 10) 전자서명/암호화

가. 웹서비스 보안

인터넷상에서 정보 보호를 위한 네트워크 보안, ID/패스워드 방식의 응용 프로그램의 보안 취약점 개선을 위한 접속인증, 전자적 정보유통 사실에 대해 유통 당사자가 부인하는 것을 방지하기 위한 부인방지, 시점확인, 신원확인을 적용한다. 웹서비스 보안은 다음과 같다.



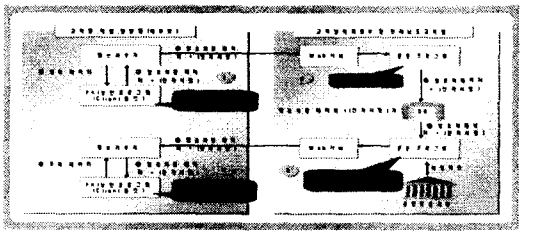
(그림 11) 웹서비스 보안

① 수신자가 웹브라우저에서 정보를 Web 서버로 전송하거나 수신할 시 보안 적용기준에 따라 암호화 및 전자서명을 하여 전송
② 수신 시 복호화 및 전자서명 검사 실시
③ 접근권한이 통제되는 페이지의 경우 로그인 시 사용자 접근권한을 설정하고, 응용 프로그램에서 이를 확인하여 접근제어 처리

나. END to END 보안

END to END보안은 데이터의 송신자와 수신자 사이에 긴밀한 데이터의 보안이 필요한 시스템 구성에 적용한다.

END to END 보안은 다음과 같다.



(그림 12) END to END

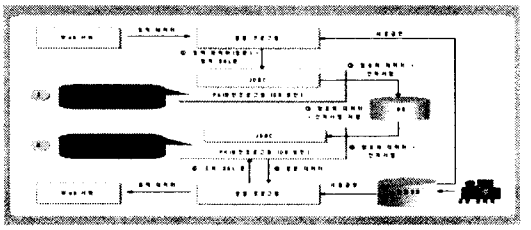
① 사용자의 웹브라우저에서 사용자 혹은 조회 가능자(수신자)의 인증서로 암호화 및 전자서명하여 Web 서버로 전송
② 응용 프로그램에서 전송받은 암호화된 데이터를 DB에 저장
③ 정보 조회 시 응용 프로그램에서 조회 가능시간을 확인한 후 DB의 데이터를 읽음
④ Web 서버를 거쳐 웹브라우저로 암호화된 데이터를 전송하면 웹브라우저에서 보안 프로그램을 호출하여 암호화된 데이터를 복호화 및 전자서명 검사하여 정보를 확인

다. DB보안

DB에 데이터 보관 도중 접근권한이 있는 사용 그룹이외의 사용자가 정보의 변경 및 조회하는 것을 방지할 필요가 있는 업무에 적용한다.

DB보안은 다음과 같다.

① DB에 데이터를 입력 시 응용 프로그램에서 입력구문과 데이터를 입력하면 PKI 보안 프로그램에서 보안 적용규칙에 따라 암호화 및 전자서명을 수행하여 이 값을 DB에 저장

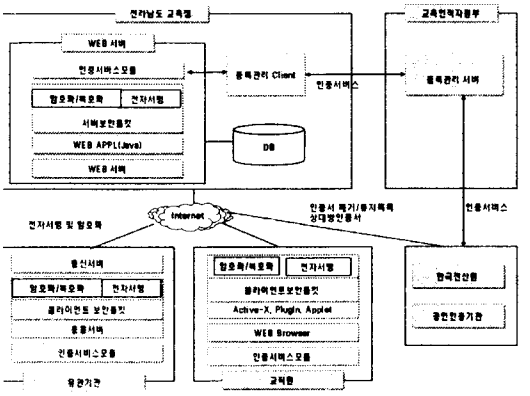


(그림 13) DB보안

② 데이터를 조회 시 응용 프로그램에서 조회 문장을 입력하면 보안툴킷에서 DB에 저장된 암호화 및 전자서명을 읽어 복호화 및 전자서명 검사를 수행한 후 복호화된 데이터를 반환

③ 소프트웨어 구성도

응용프로그램 보안 대상이 되는 모든 서버와 클라이언트에는 각각 인증서버의 모듈과 보안툴킷이 설치가 되어 보안 서비스가 제공된다. 따라서, 서버 응용프로그램 및 웹브라우저상의 클라이언트에서는 이 두가지 모듈을 이용한다. 인증서 발급 및 설치를 위해서는 인증서비스 모듈을 이용하게 되고, 암호화 키 생성 및 암/복호화 기능을 위해서는 보안툴킷이 사용되어 진다.



(그림 14) 소프트웨어 구성도

■ 정보시스템실 보안 대책

① 통제구역 및 제한구역의 설정

정보보호를 위해 시스템실을 통제구역으로 설정하고, 외래인의 출입통제가 요구되는 모든 구역을 제한구역으로 설정한다.

※ 시스템실: 시스템 운영을 위한 서버 및 통신장비 설치장소→ 본청 교육정보화과 별실

② 통제구역의 통제 방안

통제구역에 대한 불필요한 접근을 통제하기 위해 다음과 같이 통제 방안을 강구한다.

가. 인가된 자의 출입만 허용될 수 있도록 별도의 물리적 보안장치, 출입관리 기능을 구현하고, 안전성이 우수한 개폐장치를 설치·운영

나. 지문인식 출입 관리시스템 구축 및 24시간 감시카메라 설치

다. 통제구역의 출입자는 업무상 관련자로서 비밀취급인가자로 제한

라. 퇴직, 전출, 전보 등에 의해 업무상 출입의 필요성이 상실된 경우 즉시 접근권한을 해제

마. 비인가된 장비의 반입 제한

바. 유지보수업체에 의한 장애처리, 성능개선 등이 필요한 경우에는 시스템 관리자, 네트워크 운영자의 입회 하에 작업 실시

사. 전산장비의 유지·보수를 위한 외부 업체 직원의 지속적인 출입을 요하는 자는 신원확인 등의 보안 조치강구

아. 월 1회(매월 첫주 금요일) 보안 진단의 날을 이용 출입자 확인 및 전산, 통신장비 등 전반적인 보안관리 실태 점검

③ 방제 및 위해 방지

가. 안정적인 전원공급을 위한 UPS 2중화 설

치 운영

나. 기계실내 항온·항습을 위한 항온항습기 설치 운영

다. 기계실내 스프링 쿨러 등 방화 시설설치

라. 외부로부터의 침입 방지를 위한 출입문 통제장치(지문인식 출입 관리시스템 구축) 및 방범창 설치

마. 유사시 전산자료 및 전산장비 비상반출 우선 순위 지정

① 해당 기관의 중요 정보 자료 및 문서(백업자료 포함)

② 중요 응용소프트웨어 전산자료 및 문서

③ 주전산기급 장비

④ 자료(기타 미디어에 수록되어 있는 자료)

⑤ 전산기급 장비(서버급, 워크스테이션급, PC급)

⑥ 기타 주변장치

④ 보안 교육

『교육행정정보시스템』운영에 따른 정보통신수단에 의한 개인정보 및 기관 이익에 관련된 사항의 누설을 방지하고 중요자료의 보호와 유출을 막기 위해 정보통신보안 기본지침에 의거하여 정보통신보안에 대한 교육계획을 수립하고 지속적인 교육을 실시한다.

2.1.2. 백업정책

① 목적

교육행정정보시스템의 가장 중요한 자원인 교육행정정보데이터를 시스템 오류, 사용자의 실수, 바이러스, 해커의 침입, 자연재해 등의 장애로 인한 데이터 훼손 또는 손실로부터 보호하기 위하여 별도의 저장장치에 백업하여 둠으로써, 신속한 데이터의 복구를 통한 교육행정정보시스템의 안정적인 운영을 기하고자 함.

② 정의

가. 백업 : 운용중인 백업대상 데이터를 백업매체에 온라인 또는 오프라인으로 저장하는 일련의 활동

나. 백업방법

○ 온라인(Online) 백업 : 백업대상 시스템이 정상운영중에 이루어지는 백업

○ 오프라인(Offline) 백업 : 백업대상 시스템 프로세스의 일부 또는 전체를 운영중지한 후 이루어지는 백업

다. 백업대상 : 전라남도교육청 교육행정정보시스템에서 운영중인 서버 및 기타 장비에 한함

라. 백업매체 : 보조Disk, 백업테입(LTO, DAT), CD-ROM, 플로피디스켓 또는 기타 백업매체

마. 백업시스템 : LTO 테입에 백업을 수행하는 H/W(STK L80) 및 S/W(NetWorker)

③ 백업대상 분류

〈표 1〉 백업 대상 분류

구분	백업 대상	대상 시스템
오라클 데이터베이스	데이터 베이스	통합스토리지(Hitachi 9910)
DB 서버	OS, Application, Log	DB(1~2), SMS 서버
HP 서버	OS, Application, Log	Web/Was(1~4) 서버
보안서버	OS, 보안설정툴, Log	IDS, F/W(1~2),
기타 SUN 서버	OS, Application, Log	NMS, DNS, Info서버
네트워크 장비	Configuration data	Router, L4 switch, L3 switch

④ 백업자료 보관장소 : 교육정보화과 「전산데이타금고」에 보관

⑤ 서버별 백업 정책

☐ Oracle Database

가. 시스템 개요

(1) 용도 : 교육행정정보시스템 27개 단위업무별 데이터베이스 자료

(2) 백업 대상

○ 운영시스템: DB서버(SunFire 4800), 통합스토리지(Hitachi 9910), 백업시스템(StorageTek L80)

○ 어플리케이션: RawDevice data (Veritas Volume Manager로 구성)

나. 백업 정책

(1) 내장 디스크에 의한 백업

○ 백업 방법 : 통합스토리지의 하드디스크에 Raid 1 방식으로 이중화되어 실시간(Realtime) 백업

○ 서비스 상태 : 온라인

(2) 백업시스템에 의한 백업 정책

〈표 2〉 백업 정책

백업 정책 / 구 분	Online Full 백업	Online Incremental 백업	Offline Full 백업
백업방법	Online	Online	Offline(NetWorker백업)
백업주기	주1회(일요일)	매일(월-토)	2개월(홀수월)
보관주기	1개월	1개월	2개월
보관장소	백업시스템(L80)	백업시스템(L80)	별도

(3) 업무담당자 : [별첨] 장비별 및 관리자 책임자

□ DB, SMS 서버

가. 시스템 개요

(1) 용도

○ DB서버: 교육행정정보시스템 데이터베이스 운영용 Oracle DBMS

○ SMS서버: 각종 서버시스템 관리 및 백업시스템 응용 S/W 구축

(2) 백업 대상

○ 운영시스템

- DB: DB서버(SunFire 4800), 통합스토리지(Hitachi 9910), 백업시스템(StorageTek L80)
- SMS: SMS서버(SunFire v480), 백업시스템(StorageTek L80)

○ 어플리케이션

- DB: Oracle 9i, NetWorker Agent
- SMS: Oracle 8i, NetWorker 3.x, HP OpenView(OPC)

나. 백업 정책

(1) 내장 디스크에 의한 백업

○ 백업 방법 : 이중화된 내장 하드디스크에 대한 HardCopy

○ 서비스 상태 : 온라인

(2) O/S 및 Application 백업

○ 백업 방법 : DAT Tape에 의한 백업

○ 서비스 상태 : 오프라인

○ 백업 주기 : 2개월(홀수월 첫주 금요일 18:00)

○ 보관 주기 : 2개월

○ 보관 장소 : 별도장소

(3) 백업시스템에 의한 백업

○ 백업 방법 : 백업 S/W에 의해 백업시스템에 백업

○ 서비스 상태 : 온라인

-Full backup : 온라인

-Daily Incremental backup : 온라인

○ 백업 주기 : 2주

○ 보관 주기 : 2주

○ 보관 장소 : 백업시스템(L80)

(4) 업무담당자 : [별첨] 장비별 및 관리자 책임자

□ HP서버

가. 시스템 개요

(1) 용도

웹브라우져를 이용 교육행정정보스시템에 접속하여 27개 단위업무를 수행할 수 있도록 Web/Was 서비스를 제공하며, 시·도간 연계, S/W 분배, 인증 및 인증서 재발급 등이 이루어 짐.

(2) 백업 대상

○ 운영시스템: HP-Unix 11.11i

○ 어플리케이션: WebToB, JEUS, TIBCO, ReportDesigner, Cardio

나. 백업 정책

(1) 내장 디스크에 의한 백업

○ 백업 방법: 내장된 하드디스크(36GB) 두 개가 Mirroring하도록 구성되어 있어, 같은 내용이 두 개의 디스크에 복제되므로 실시간 백업이 이루어짐.

○ 서비스 상태 : 온라인

(2) O/S 백업

○ 백업 방법 : DAT Tape에 의한 백업

○ 서비스 상태 : 오프라인

○ 백업 주기 : 2개월 (홀수월 첫주 금요일 18:00)

○ 보관 주기 : 2개월

○ 보관 장소 : 별도장소

(3) 백업시스템에 의한 백업

○ 백업 방법 : 백업 시스템 운영관리 지침에 의한 백업

○ 서비스 상태 : 온라인

-Full backup : 온라인

-Incremental Backup : 온라인

○ 백업 주기 : 2주

○ 보관 주기 : 2주

○ 보관 장소 : 백업시스템(L80)

□ 보안서버

가. 시스템 개요

(1) 서버별 용도

○ IDS서버 : DMZ와 내부 Network 간 침입탐지서버

○ F/W서버 : 허가된 네트웍 접근에 대한 허용 및 해킹 등 불법 접근 통제

(2) 백업 대상

○ 운영시스템 : SunFire v480, SunFire 280R (DNS)

○ 어플리케이션 : 각 시스템별 Application

나 백업 정책

(1) 내장 디스크에 의한 백업

○ 백업 방법 : 이중화된 내장 하드디스크에 대한 HardCopy

○ 서비스 상태 : 온라인

(2) O/S 및 Application 백업

○ 백업 방법 : DAT Tape에 의한 백업

○ 서비스 상태 : 오프라인

○ 백업 주기 : 2개월(첫주 금요일 18:00)

○ 보관 주기 : 2개월

○ 보관 장소 : 별도장소

(3) 백업시스템에 의한 백업 : 없음

(4) 업무담당자 : [별첨] 장비별 및 관리자 책임자

□ 기타 서버

가. 시스템 개요

(1) 서버별 용도

○ NMS서버 : 각종 Network node 및 node간의 Network 운영현황 관리

○ DNS서버 : 교육행정정보시스템 각종 도메인 네임 서비스

○ Info서버 : 교육행정정보시스템 지원서

비스

(2) 백업 대상

○ 운영시스템 : SunFire v480, SunFire 280R(DNS)

○ 어플리케이션 : 각 시스템별 Application

나. 백업 정책

(1) 내장 디스크에 의한 백업

○ 백업 방법 : 이중화된 내장 하드디스크에 대한 HardCopy

○ 서비스 상태 : 온라인

(2) O/S 및 Application 백업

○ 백업 방법 : DAT Tape에 의한 백업

○ 서비스 상태 : 오프라인

○ 백업 주기 : 2개월(첫주 금요일 18:00)

○ 보관 주기 : 2개월

○ 보관 장소 : 별도장소

(3) 백업시스템에 의한 백업 : 없음

(4) 업무담당자 : [별첨] 장비별 및 관리자 책임자

□ 네트워크 장비

가. 시스템 개요

(1) 네트워크 장비별 용도

○ Router : 교육행정정보시스템 네트웍 구성 및 네트웍 필터링(Filtering)

○ L4 Switch : Network Traffic 제어 및 Load Balancing

○ L3 Switch : Network Traffic 제어

(2) 백업 대상 : Router, L4 Switch(Alteon 180e), L3 Switch(nortell)

나. 백업 정책 : Configuration 백업

○ 백업 방법 : 해당 장비별 Configuration 내역을 Text로 출력 보관

○ 서비스 상태 : 오프라인

○ 백업 주기 : Configuration 변동시

○ 보관 주기 : 영구 보관

○ 보관 장소 : text file을 보관하며, 1부 출력하여 해당 장비별 담당자가 보관

다. 업무담당자 : [별첨] 장비별 및 관리책임자 [2],[3]

2.2. NEIS의 취약성에 대한 보완

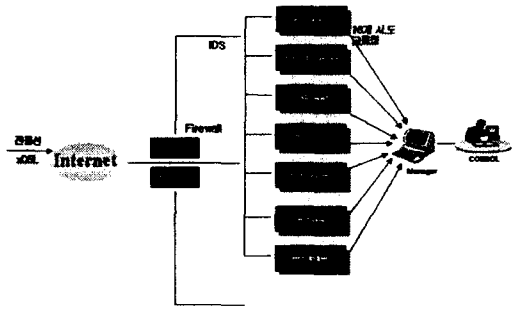
NEIS를 현재 제기되고 있는 문제점 중 문제점으로 대두되고 있는 것이 보안문제이다. NEIS는 데이터가 한곳에 집중되어 이의 유출시 발생하는 파급효과가 상당히 크다. 해킹 및 바이러스에 대한 대책이 미흡하다는 점이다. 이러한 문제로 인하여 개인정보가 유출될 수도 있고, 이는 NEIS에 기록된 정보의 성격에 따라 인권침해문제로 연결되기도 한다.

본 연구는 위와 같은 문제를 해결하기 위한 것이다.

먼저 NEIS에 대한 취약성을 보완하기 위해서는 취약성 분석 도구가 필요하다. 앞서 살펴본 NEIS의 시스템 구축방법은 취약성에 대한 고려가 되어있지 않다.

아무리 뛰어난 설계와 구성을 갖춘 시스템이라 해도 항상 취약성이 존재한다. 그런 취약성은 바이러스나 해킹에 시스템을 노출시킨다. 이를 미리 예방하고 문제의 사전제거를 위해 필요한 것이 취약성 분석 도구이다. 실시간 취약성 분석도구는 시스템의 변경사항에 따라서 아래와 같은 사항들을 체크하여 관리자에게 보고하도록 구축되어야 한다.

NEIS 취약성의 구조



(그림 15) NEIS의 취약성 구조

■ 취약성 분석 항목

1. 사용자 계정
2. 파일 접근 권한
3. 파일 변경 사항
4. 특수파일
5. 로그인 기록
6. 네트워크 무결성
7. OS 패치
8. 시스템 메일
9. 레지스트리(only WinNT/2k)
10. 예약 실행
11. 사용자 패스워드
12. 시스템 초기설정
13. 사용자 파일
14. 관리자 환경
15. 유틸리티
16. 네트워크 접근 가능성
17. 웹 취약성
18. 바이러스(only WinNT/2k)

이러한 시스템 도입을 위해서는 현재의 2-Tier 방식으로는 불가능하다. 그렇기 때문에 3-Tire방식을 도입하여 취약성 분석 도구를 설치한다면 거의 완벽한 보안 시스템을 구축할 수 있다.

현재 해킹 기술은 나날이 발전하고 있고, 바이러스 또한 변종들이 속속들이 등장하여 이미 패치되어 취약성이 보완 되었다 해도 안심할 수 없다. 실시간 취약성 분석을 통하여 보안장비(Firewall,IDS)를 업그레이드해야하며, 취약성 분석도구 또한 최신 정보에 맞는 분석항목을 추가하여 이에 대비하여야 한다.

물론 이러한 장비에 접근 가능한자는 최소한으로 줄여야 한다. 보안실무자(Admin), 보안책임자(Total Admin), 보안 감사자(Viewer)의 3인에게만 관리권한을 부여하고 이 3인이외에는 철저한 접근 통제를 실시하여야한다. [10]

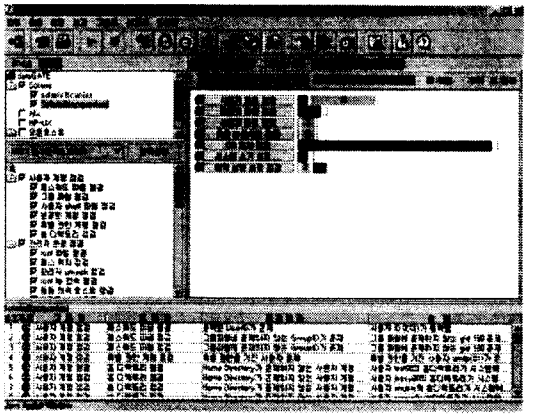
2.3. 취약성 보완을 위한 분석 도구에 기능

-3Tier Architecture(Manager/Agent/Console)
-S-security support(ubiquitous)
-Web based Graphical User Interface
-Authorization management (administrator , user)
-Scheduling
-Concurrent Check on multi system
-Support Security Grades(total grade 100)
-Provides statistical reports of the detected result
-Check modules are extended automatically
-Laser Point(Office up down)

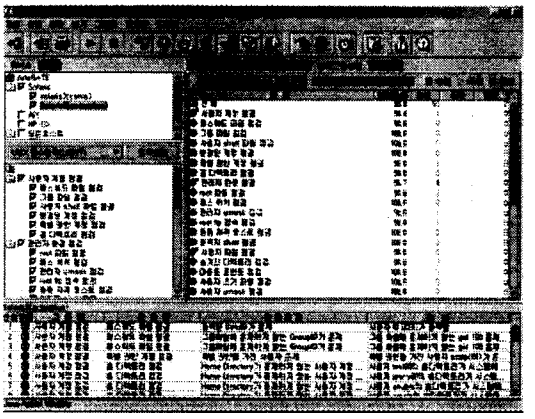
<그림16>, <그림17>, <그림18>은 취약성도구를 실행하였을 때 그림이다.

<그림19> 취약성 분석도구의 종합보고서를 보여준다.

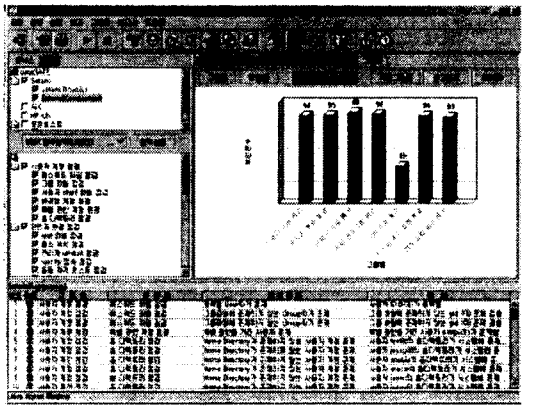
<그림20> 취약성 분석도구의 그룹별보고서를 보여준다.



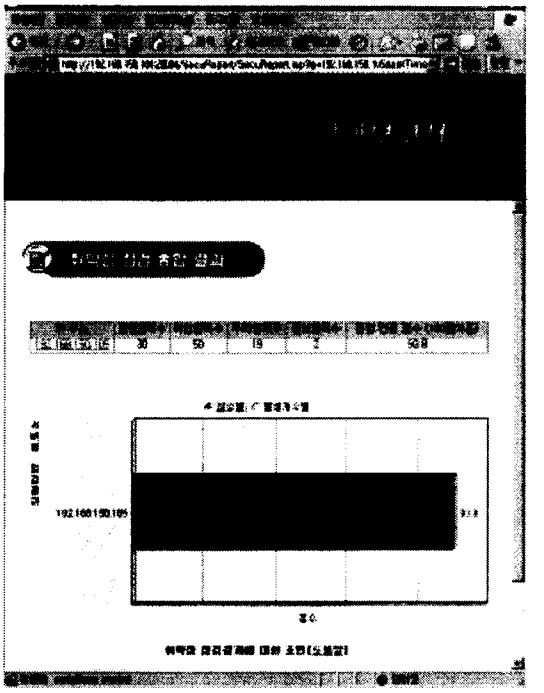
(그림 16) 취약성 도구 실행1



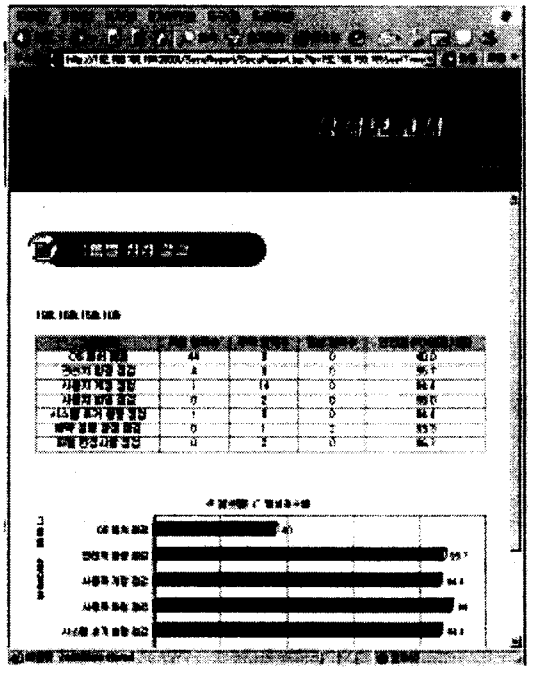
(그림 17) 취약성 도구 실행2



(그림 18) 취약성 도구 실행3

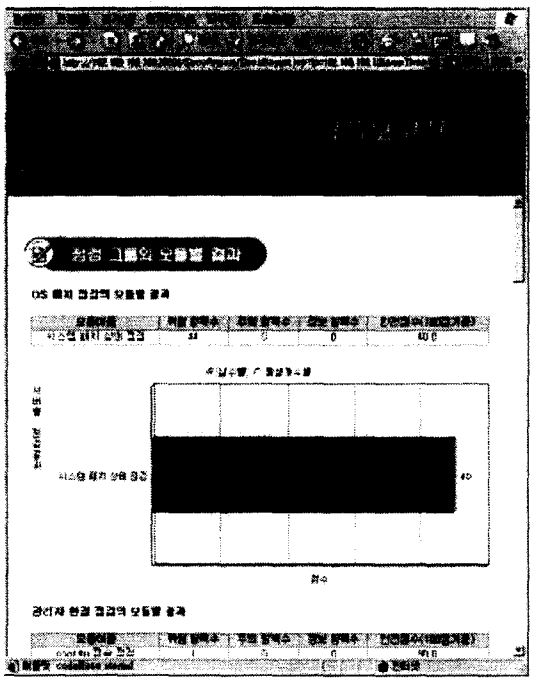


(그림 19) 종합 보고서



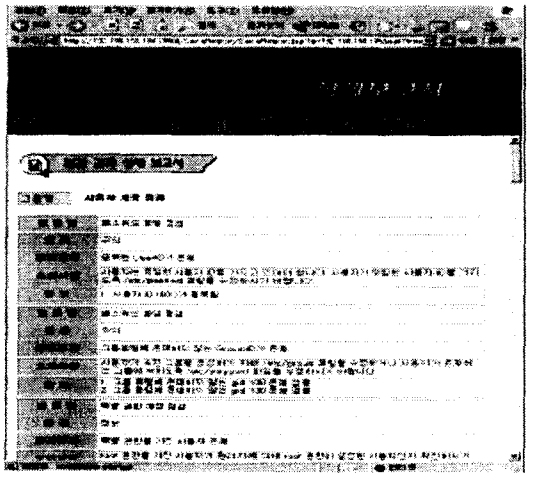
(그림 20) 그룹별보고서

<그림21> 취약성 분석도구의 모듈별보고서를 보여준다.



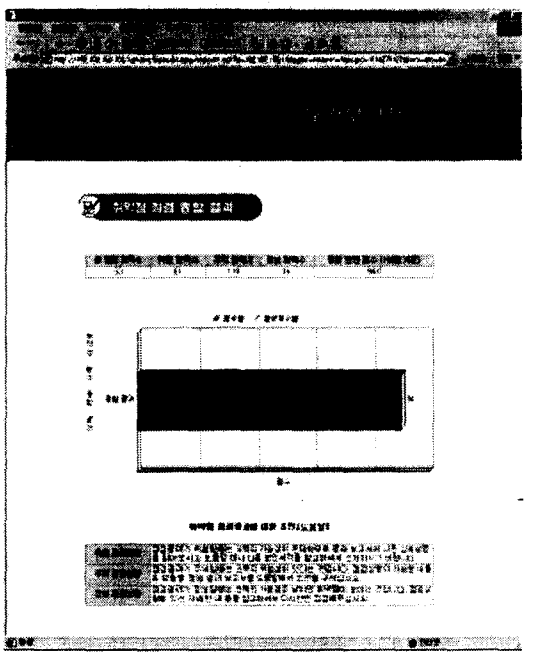
(그림 21) 모듈별 보고서

<그림22>취약성 도구의 점검결과 상세보고서를 보여준다.



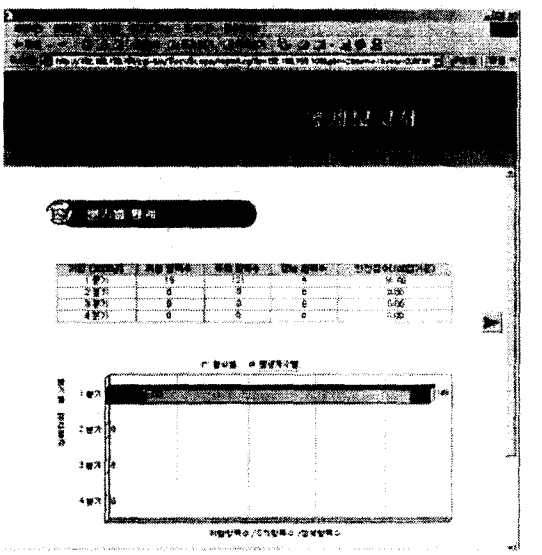
(그림 22) 점검결과 상세보고서

<그림23>취약성 도구의 요약보고서를 보여준다.



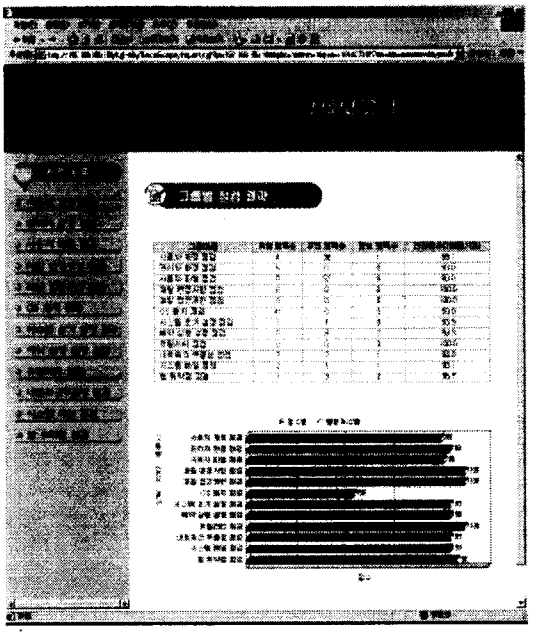
(그림 23) 요약보고서

<그림24>취약성 도구의 통계보고서를 보여준다.



(그림 24) 통계보고서

<그림25>취약성 도구의 상세보고서를 보여준다.



(그림 25) 상세보고서

Ⅲ. 결론

정보통신 INFRA의 고도화, 네트워크형 S/W 발전, Internet이용의 확산, 네트워크 연결 경로의 다양화, 위협요소 증가, 바이러스 Smap, Juck Mail, DOS, DDOS etc 자원의 성능 및 가용자원에 대한 이용율을 저하 할뿐 아니라 새로운 보안 취약성증가 인터넷 웜, 해킹 etc 사이버 공격에 의한 피해 사고 증가 한다. 그래서 현재 네트워크 보안 현황은 보안 방화벽 접근통제-(네트워크 안팎의 접근통제, 인증, VPN기능을 위한 설계, 접근이 허용된 트래픽인가? 접근이 허용된 보안으로 인식 되던, 공격을 찾기 위해 네트워크 트래픽의 내용을 모니터링, 허용된 트래픽이 정상적인 트래픽인가 악의적인가? 트래픽 인가를 구분 HTTP기반의 공격들을 관찰해야한다.[1]

실시간 탐지 및 유해 트래픽 차단시스템의 필요성으로 사이버 공격, 활동적인 위협에 대한 실시간 및 타이밍 상에 공격을 못 막을 가능성에 대비 및 IP address로 부터의 트래픽을 차단하도록 지시한다. 현재의 문제점인 시스템이 공격을 받은 후에 탐지, 향후 공격해온 IP address, 새로운 Worm, 해킹에 대비 취약성에 관한 것이 보안연구의 대상이다.

현재 NEIS의 제일 주된 문제는 보안이다.

본 연구에서 인터넷 연결점검의 방화벽 앞/뒤에 Load Balancer를 설치하여 성능향상을 도모하고, 방화벽 장애시에도 네트웍이 끊어지지 않도록 통합관리 콘솔을 설치, 내부망에서도 중요 세그먼트 망(Server)은 별도의 방화벽 설치 운영 내부 사용자의 인터넷 이용시 실수, 부주의 또는 고의로 인한 불법적인 정보유출 및 오용을 예방 및 탐지하고 통제할 수 있는 에이전트 모듈과 관리 모듈이 구분되어 통합관리가 네트워크 영향이 없이 실시간 모니터링, 다양한 보고서/ 관리 기능, 침입 탐지 및 웹 등을 3차원 실시간으로 application으로 완성했다.

따라서 시스템이 공격을 받은 후에 탐지, 향후 공격허용 IP address 차단 DOS공격에 대비할 수 있도록 사전준비를 했다. 즉, 새로운 공격에 대한 Live Up Data기능, Worm차단기능 수행했다.

한국정보보호진흥원에서는 취약점 정보 수집(named/bind, ftpd, rpc취약점), 악성프로그램(Code Red Worm, Nimda Worm), 버퍼오버플로우, 사용자도용, S/W보안오류, 서비스 거부 공격, E-Mail관련공격들을 근간으로 한 3-Tire (Manager , Agent, Console)로 구성했다. <그림 15>

취약성의 구조는 Agent에서 감사결과를 Mana

ger에게 보내고 Manager는 보안감사를 Agent에 보낸다. 취약성 분석 도구의 실행은 <그림16>, <그림17>,<그림18>이다. Manager는 최종 감사보고서를 Console(보안관리자)에게 보낸다.

종합보고서는 <그림19>, 그룹별 보고서는 <그림20>, 모듈별보고서는 <그림21>, 점검결과 상세보고서는 <그림22>, 요약보고서는 <그림23>, 통계보고서 <그림24>, 상세보고서는 <그림25>와 같다.[20]

매니저/에이전트 구조의 분산화 및 예약실행에 의한 과부하 방지 및 부하 균형 보장(효율성), 선택된 정책에 의한 선별적인 취약성 진단이 가능(분리성), 웹 기반의 사용자 인터페이스에 의한 관리적 편의성 제공(편의성), 다양한 보고서 제공(다양성), 여러 대의 시스템을 동시에 관리할 수 있는 콘솔 제공(종합성), 콘솔/매니저/에이전트의 통신 암호화(보안성)기능을 구현하였다.

이로써 취약성에 대한 실시간 점검보고서와 통계보고서로써 병렬보안 취약성을 진단할 수 있다.

앞으로 방화벽에 의해 허용되는 외부 트래픽 내부 트래픽 무선 Internet과 Cellphone, PCS까지 지원되는 것이 연구 대상이다.[20]

참고문헌

[1] 교육행정정보시스템에 대한 왜곡. 오해와 그 실상 4. 2003. http://bugok.ms.kr/ex/neis-001.htm

[2] NEIS사용을 위한 개인별 PC 및 학내망 점검 요령. www.gwhsed.go.kr

[3] 교육행정정보시스템(NEIS) 운영계획 4. 2003. www.jne.go.kr

[4] Commission on Class Size and Composition (2001). *A public discussion paper.* Toronto, Canada.

[5] Department for Education and Employment (2000). *Statistics of education: Class size and pupil teacher ratios in England.* London, UK.

[6] Department for Education and Employment (2001). *Class size in maintained schools in England.* January 2001 (provisional). London, Uk.

[7] Bryan Burrough, "Der Hacker des FBI," Spiegelreporter 12월호 2001년.

[8] NEIS, 보안성 강화로 풀자 http://news.hankooki.com/lpage/opinion/200 305/h200305191718012

[9] 대한교원신문 "끝 모를 'NEIS 싸움' http://www.teachworld.com/news-paper/ data_room/edu_artical/2003/...

[10] 정보교사 "네이스 해킹했다" http://www.secuve.co.kr/pressroom/pr-essroom/pressroom3_view.htm?table=bbs...

[11] NEIS 정부홈페이지 http://www.neis.go.kr

[12] 전교조 홈페이지 http://www.eduhope.net

[13] 종합뉴스 데이터 베이스 http://www.kinds.or.kr

[14] 국민일보 4. 3. 2003 00면 1563자 http://www.kukminilbo.co.kr

[15] 경향신문 3. 20. 2003 06면 2106자 http://www.khan.co.kr

[16] 동아일보 http://www.donga.com

[17] 대한매일 4. 1. 2003 11면 8
htttp://www.kdailyh.com/news/
[18] 세계일보 4. 4. 2003 27면 1330자
http://www.segye.com/service1/shell General.asp?TreeID=2
[19] 정혜련, 정태명, "침입 시나리오 분석에 기반한 다중 공격의 분류 및 탐지 방법에 관 한 연구", 「1999SEC 추계 학술발표 논문집」, 제6권 제2호, pp.182-189.
[20] http://security-focus.com

A Study on NEIS Vulnerabilities Analyze Tool Supplement

Seung-Ho Woo*· Soon-Duk Kang**

Abstract

We analyze specific supplementation direction(Efficiency, Isolation, convenience, synthesis, variety, secutiry) about system vulnerabilities of the NEIS(National Eduation Information System) in this research.

The efficiency constructs parallel security vulnerabilities diagnosis system NEIS which the security problem prevents and checks.

* Division of Information & Communication Engneering, Kongju National University
** Division of Information & Communication Engneering, Kongju National University