교육기관의 정보시스템 보안관리 방안 연구

최진명† · 김두연††

요 약

교육기관 및 대학에서 사이버침해에 의하여 정보가 유출, 위조, 변조, 삭제 등 훼손되었을 때의 피해는 매우 크다. 본 연구에서 교육 관련 행정기관과 대학을 대상으로 사이버침해의 유형, 원인 및 문제점 등을 분석한 결과 관리적, 물리적, 기술적 정보보호 활동이 취약했다. 따라서 본 연구에서는 이들 취약점을 쉽게 식별하고, 보완 또는 보안성을 강화할 수 있도록 인터넷 영역, 네트워크 중립 영역(DMZ: Demilitarized Zone), 일반 서버 영역, 내부 서버 영역(Server Farm), 사용자 영역으로 구분하여 각 영역별로 보안강화 방안을 제시하였다. 또한, 행정기관 및 대학을 위한 보안성 높은 정보시스템 아키텍처와 정보보호 기술을 올바르게 적용할 수 있는 방법을 제시하였다. 본 연구는 개념적 지침이 아닌 구체적 활동과 절차 중심의 보안관리 방안을 제시한다는 데에 의의가 있다.

주제어 : 정보시스템 구축, 보안관리, 정보보안, 인프라 보안

A Study on Security Management Methods for Information System of Educational Institutions

JinMyung Choi† · DooYeon Kim††

ABSTRACT

The damage caused by information spill, forgery, falsification, and deletion by cyber infringement in educational institutions and universities is very large. In this study, we analyzed the types, causes, and problems of cyber infringement in educational administrative institutions and universities. As a result, administrative, physical and technical information protection activities were weak. In this paper, we propose a security enhancement method for each domain by dividing them into Internet zone, network-neutral zone (DMZ: Demilitarized Zone), general server zone, internal server zone (Server Farm), and user zone so that these vulnerabilities can be easily identified, supplemented or security enhanced. In addition, we have proposed a method to apply security information system architecture and information protection technology correctly for educational administration institutions and universities. This study is meaningful not to provide conceptual guidance but to suggest specific action and procedure oriented security management plan.

Keywords : Information System Construction, Security Management, Information Security, Infrastructure Security

† 정 회 원: 건양대학교 융합IT학과 조교수
†† 정 회 원: 건양대학교 융합IT학과 부교수(교신저자)
논문접수: 2017년 11월 2일, 심사완료: 2017년 11월 15일, 게재확정: 2017년 11월 28일

1. 서론

기관 및 조직에서는 수많은 컴퓨터와 통신기기들이 유·무선 네트워크와 인터넷으로 서로 연결되어 있고, 대부분의 업무를 정보시스템을 이용하여 정보통신망에서 수행하고 있다. 그러나 네트워크로 서로 연결된 다양한 정보시스템에 대한 불특정 다수로부터의 악의적인 접근을 통한 정보의 회손, 유출, 서버 컴퓨터의 오동작 유도 등 사이버공격이 날로 빈번해지고 있다.

컴퓨터가 대중화 되는 시기였던 1990년대와 2000년대 초반에는 컴퓨터 바이러스에 의한 정보시스템 공격이 주를 이루었으나, 컴퓨터가 네트워크로 연결되고 인터넷에 쉽게 접속할 수 있게 되면서 분산 서비스 거부 공격(DDoS: Distributed Denial of Service), 지능형 지속 위협(APT: Advanced Persistent Threat)과 같은 네트워크 기반의 사이버공격으로 인해 정보시스템을 경유지로 하는 사이버공격과 정보시스템의 취약점을 이용한 개인정보유출이 주로 발생하고 있다[1].

사이버공격에 대응하기 위하여 정부는 「국가정보원법」, 「보안업무규정」(대통령령), 「정보 및 보안업무 기획·조정규정」(대통령령), 「국가사이버안전관리규정」(대통령훈령), 「국가 정보보안 기본지침」, 「전자정부법」과 동법 시행령, 「정보통신기반보호법」과 동법 시행령, 「공공기록물 관리에 관한 법률 시행령」 등의 법령을 마련하여 시행하고 있다. 교육부 역시 「교육부 사이버안전센터 운영규정」에 따라 「교육부 정보보안 기본지침」을 마련하여 행정기관 및 학교가 정보보호 활동을 강화하도록 했다. 그러나 교육기관을 대상으로 하는 사이버침해가 지속적으로 발생되고 있는데 그 원인을 살펴보면 <표 1>과 같다[2]. 이는 정보시스템 보호를 위한 관리적 보호조치와 기술적 보호조치가 원활하게 이루어지지 못한 것과 정보보호 업무를 수행하는 운영자의 사소한 부주의에 기인하고 있다.

시·도교육청과 같은 행정기관 및 대학에서는 수많은 학생정보를 관리하고 있기에 사이버 침해사고가 발생될 경우 개인정보 및 학적정보의 유출, 변조, 삭제 등의 피해가 발생될 수 있다. 이에 행정기관과 대학의 정보시스템, 정보보호시스템의 운영 현황 및 관리체계에 대한 분석결과를 토대로 정보시스템 보안관리 방안을 제시한다.

<표 1> 사이버공격 피해 원인

- 관리자 PC 보안 미흡
- 관리자 PC에 사내 서버 접속정보 보관
- 서버 접근이 관리자 IP 이외도 가능
- 웹 서버 보안 미흡(웹셸 업로드)
- 보안 패치 미흡
- 업데이트 파일의 무결성 검증 미흡
- 업데이트 서버의 취약한 인증
- 서버 내 방화벽 설정에서 타 서버 접근 허용
- 개발 서버가 동일 망에 존재
- 디폴트 비밀번호 사용
- 불필요한 명령어 사용제한 없음

2. 정보시스템 보안성 강화 연구

정보시스템을 구축하기 위한 정보전략계획 수립단계에서는 정보보호 관련 법규 및 조직 분석, 전략 수립, 아키텍처 정의 등의 활동을 수행한다. 정보시스템 개발의 분석단계에서는 정보보호 요구사항 분석, 위험 평가, 정보보호 계획을 수립한다. 설계단계에서는 정보보호 아키텍처의 개발과 시험 계획을 수립하고, 구현단계에서는 정보보호 솔루션을 도입하며, 정보보호 교육 및 훈련 계획의 수립과 시스템 운영지침을 마련한다. 시험단계에서는 정보보호 취약성과 침투시험을 하고, 정보보호 평가 및 승인 활동을 수행한다[3].

정보보안을 위하여 시·도교육청 등 행정기관, 각 급 학교는 정보통신망 또는 정보시스템에 대한 접근이나 사용 허가를 받은 사용자의 관리, 정보통신 시설보안, 침해 예방을 위한 모의 훈련 실시, 정보보안 교육 실시 등을 포함하여 정보통신기반시설에 대한 보안대책, 안정성 확인 및 보안적합성 검증 등을 수행해야 한다[4]. 그리고 침해사고 발생 시 이를 신고, 전파, 조사복구 및 대응 등을 위한 관리적 활동을 수행해야 하며[5], 민원인을 위한 인터넷 검색실의 운영, 용역업체 개발실 운용, 무선랜 운용, 웹 서버 운용, 물리적 네트워트 분리, 세션 보더 컨트롤러(SBC: Session Border Controller)를 이용한 논리적 네트워크 분리, 통합 보안관리시스템(ESM: Enterprise Security Management) 운용, 정보유출방지 시스

템 및 보조기억매체 통제시스템 운용 등 기술적 관점에서의 정보보호 조치를 수행해야 한다[6][7].

개인정보보호를 위해서는 윈도우 운영체제의 보안 프로토콜인 IPSec(Internet Protocol Security), 가상사설망(VPN: Virtual Private Network) 방식의 암호화 방법과 국가정보원에서 검증대상으로 지정한 암호알고리즘을 이용하여 데이터베이스 서버 및 데이터베이스관리시스템 자체를 암호화해야 한다. 또한, 홈페이지에서 개인정보가 노출되는 유형과 이에 따른 조치방법을 마련해야 한다[8][9].

학교와 같은 교육기관에 적합한 인터넷 방화벽의 배치, L2 스위치, L3 라우터 배치, 웹 보안을 위한 네트워크 아키텍처를 제시하여 정보보호 관점에서 기본적인 정보시스템의 아키텍처를 설계하여야 한다[10][11][12].

보안인식 교육이 정보보안 침해의 가능성을 줄이는데 직접적으로 기여하지 않는 경우도 있지만 대체로 개인의 정보보안 활동에 영향을 끼치고 있으며, 보안인식 교육을 통해 사이버공격에 대한 심각성을 일깨워 줌으로써 사이버침해의 가능성을 줄이려는 노력을 하게 된다. 또한, 조직은 개인의 정보보안에 대한 인식개선 교육만이 아니라 상황별로 실제 취해야 할 행동에 대해서도 교육을 병행해야 한다[13][14].

기존 연구는 정보시스템을 올바르게 구축하는 방법, 정보보안을 위한 고려사항, 네트워크 구축 가이드라인, 개인정보보호를 위한 기술적 보호조치 및 정보보안 인식 교육 등 정보보호와 관련된 개별적 방법 및 활동 등에 한정하고 있어, 보안성을 고려한 정보시스템의 구축 및 운영 측면에서 관련 기술의 선후 적용 및 배치, 관계성 등을 고려한 보안강화 제시가 미흡하다. 이에 [15]에서 제시하고 있는 관리적 보안, 물리적 보안, 기술적 보안 관점으로 교육관련 행정기관과 대학의 정보시스템 보안 현황을 분석하고, 보안성 높은 정보시스템을 구축할 수 있는 아키텍처와 운영 방안을 제시한다.

3. 행정기관 및 대학의 정보보호 현황

교육부의 도움을 받아 시·도교육청 12개 기관, 소속기관 3개 기관, 산하단체 9개 기관, 대학 157개 기관 및 대학병원 2개 기관 등 총 183개 기관의 정보화 업무 담당자를 대상으로 전자문서로 설문조사를 실시했다.

3.1 관리적 보안 현황

서버, 네트워크 장비 및 정보시스템 등의 정보보호를 위하여 보안 취약점 점검 실시 여부를 조사한 결과 응답 기관의 82.3%가 연 1회 이상 보안 취약점 점검을 실시하고 있으나, 일부 대학과 대학병원에서는 보안 취약점 점검을 실시하지 않고 있는 것으로 파악되었다.

또한, 사이버침해의 주된 창구로 활용되는 홈페이지에 대해서는 모든 홈페이지에 대하여 연 1회 이상 보안 취약점 점검을 실시하고 있는 기관은 48.1%, 일부 홈페이지에 대해서만 실시하는 기관 44.3%, 홈페이지 보안 취약점 점검을 연 1회도 실시하지 않는 기관이 7.7%로 파악되어 여러 기관이 홈페이지를 이용한 사이버공격 위험에 노출되어 있다고 볼 수 있다.

행정기관에서는 민원서비스용 PC, 대학에서는 교육용 PC에 어떤 IP 정책을 사용하느냐에 따라 보안성이 달라질 수 있다. 시·도교육청은 업무용 PC와 민원서비스용 PC가 서로 다른 대역의 사설 IP를 사용하고 있어, 안전한 IP 관리 정책을 적용하고 있다. 그러나 대학의 경우 업무용 PC와 교육용 PC 모두 공인 IP를 사용하고 있거나, 업무용 PC와 교육용 PC가 공인 IP와 사설 IP를 혼용하여 사용하기도 한다. 두 유형의 PC 모두 사설 IP를 사용하더라도 업무용 PC와 교육용 PC가 서로 같은 대역을 사용하여 교육용 PC가 외부로 부터 공격을 받은 경우 업무용 PC까지 공격받을 수 있는 위험성이 있다.

IP에 대한 체계적 관리를 통해 비인가자의 정보시스템 접근을 차단하기 위하여 33.3%의 기관이 관리자를 통해 관리하고, 32.2%는 IP 관리시스템을 사용하고 있으며, 30.1%는 접근제어시스템을 이용하고 있다. IP가 체계적으로 관리되지 않는다고 응답한 기관은 대학으로 이들 대학에 대하여는 관리적 관점에서의 정보보호 지원이 실행될 필요가 있다.

3.2 물리적 보안 현황

여러 정보시스템이 외부 용역업체에 의하여 관리되기도 하여 용역업체 PC가 인터넷 서비스를 이용한다면 이 PC가 사이버공격의 도구로 활용될 수 있기 때문에 용역업체 PC 역시 최대한 인터넷 서비스 이용을 차단하여야 한다. 그러나 실제 행정기관과 대학 모두 관리자 PC만 인터넷 서비스 이용이 차단되는 비율이 5.0%, 관리자 PC와 외부 용역업체 PC 모두 인터넷 서비스 이용이 차단되는 비율은 18.2%에 불과해 정보보호 취약요인이 존재하는 것으로 파악되었다.

기관의 보안정책에 따라 기관 밖에서 또는 인터넷 망 구간에서 내부 정보서비스(업무 포털, 전자결제시스템 등)를 차단하거나 허용할 수 있으나 본 설문조사에 응답한 기관 중에서 64.8%에 해당하는 기관들은 외부 인터넷 망 구간에서 내부 정보서비스의 사용을 허용하고 있고, 18.7%의 기관이 가상사설망을 통하여 외부에서 내부 정보서비스를 직접 사용할 수 있으며, 16.5%에 해당하는 일부 대학과 산하단체에서만 외부 인터넷 망 구간에서 내부 정보서비스 사용을 차단하고 있다.

3.3 기술적 보안 현황

설문에 응답한 12개 시·도교육청 중에서도 1개 기관을 제외한 11개 기관이 업무망과 인터넷 망을 분리하여 운영하지 않고 있었으나, 5개 산하단체는 모두 분리하여 운영하는 것으로 파악되었다.

네트워크 중립 역역인 DMZ의 웹서버 보안을 위하여 운영하고 있는 보안장비는 웹 방화벽(51.1%), 웹 방화벽과 DDoS 방어장비 운영(41.8%), 보안장비 미운영 (7.1%)의 순으로 파악되었다.

내부 업무용 서버 중에서 매우 중요한 서버인 데이터베이스 서버, 웹 서버, 웹 어플리케이션 서버가 DMZ 영역에 위치하고 있는 지를 분석한 결과 응답기관의 65.4%는 데이터베이스 서버를 DMZ 영역과 분리된 네트워크 영역에서 운영하고 있으나, 12.1%는 여전히 데이터베이스 서버의 일부를 DMZ 영역에 설치하여 운영하고 있고, 22.5%는 모든 데이터베이스 서버를 DMZ 영역에 설치하여 운영하고 있다.

기관에서 DMZ 영역에 위치하고 있는 웹 서버와 웹 어플리케이션 서버에 할당된 IP 유형을 살펴본 결과 웹 서버, 웹 어플리케이션 서버들은 모두 공인 IP로 운영한다는 응답이 79.1%로 가장 많았고, 다음으로 일부 서버만 공인 IP 부여(13.2%), 모두 사설 IP 부여(5.5%) 및 일부 서버만 사설 IP 부여(2.2%) 순으로 나타났다. 이들 응답결과를 기관별로 구분하면 <표 2>와 같다.

<표 2> DMZ 영역의 웹 서버 및 웹 어플리케이션 서버의 IP 구성 형태

기관	모두 공인 IP	일부 공인 IP	모두 사설 IP	일부 사설 IP	총계
소속기관	2	0	1	0	3
시·도 교육청	6	3	3	0	12
대학	131	17	4	4	156
산하단체	5	3	1	0	9
대학병원	0	1	1	0	2
총계	144	24	10	4	182

* 미응답 1개 기관 제외

사이버침해에 따른 피해는 대부분 기관에서 사용하는 PC가 인터넷에 접속할 때 빈번하게 발생한다. 따라서 기관 내 중요 서버 및 업무망은 외부에 공개되어 있는 인터넷 망과 분리되어 있어야 하고, 중요 서버 등의 접근은 접근이 허용된 관리자 PC만 접근하여야 하며, 관리자 PC는 인터넷 접속을 차단하는 것이 바람직하다. 그러나 일부 대학 및 대학병원에서는 모든 PC에서 서버나 네트워크에 접근할 수 있는 것으로 파악되었다.

무선인터넷에 대한 정보보호 현황을 분석한 <표 3>을 보면 75.3%의 기관에서 인터넷 공유기, 스마트 기기의 핫스팟 등을 이용하여 업무용 PC에서 무선인터넷에 접속할 수 있는 상태이다.

<표 3> 업무용 PC에서 인터넷 공유기로 무선인터넷 접근 가능 여부

기관 구분	접근 가능	접근 차단	기타	%
소속기관	0	2	1	1.6
시·도교육청	6	5	1	6.6
대학	128	20	8	85.2
산하단체	2	6	1	4.9
대학병원	1	0	1	1.1
총계	137	33	12	99.4

* 미응답 1개 기관 제외

무선 인터넷 접속이 가능한 기관에서는 행정업무구간과 학생구간을 분리하여 차단정책을 실시하고 있었고, 인터넷 접속을 차단하는 기관에서는 무선 랜이 없거나 무선 랜카드를 매체제어솔루션으로 통제하고 있다.

4. 정보시스템 보안성 강화

설문조사를 통해 파악된 행정기관 및 대학의 정보시스템 보안구축 및 운영 현황은 정부의 법제도 및 가이드라인을 준수하지 않은 것이 아니라 올바르게 적용하지 못함에 따른 위험성을 내포하고 있음을 알 수 있다. 이에 따라 정보시스템 구축 및 운영을 크게 다섯 가지 영역 - 인터넷, DMZ, 일반 서버, 내부 서버, 사용자 - 으로 구분하여 보안성 강화 방안을 제시한다.

4.1 정보시스템 구축·운영 영역별 보안강화

4.1.1 인터넷 영역

정보시스템을 이용한 서비스 구성 시 통신에 필요한 포트를 명확히 하여 해당 포트만 허용하고 나머지는 모두 차단 - 화이트 리스트(White list) 유지방식 - 한다. 포트차단을 위한 정책 반영 시 정책에 대한 적용일자, 적용내용, 서비스 종료일자 등을 명시하여 왜 반영 하였는지 알 수 있게 하고, 사용목적이 종료된 정책은 즉각적으로 해제하는 정책관리가 필요하다.

웹 어플리케이션 서버인 톰캣의 관리자 포트인 8005 등과 같이 누구에게나 알려져 있는 시스템 관리자 접근 포트는 반드시 포트 번호를 변경 하고, 컴퓨터 운영체제에서 "netstat -an"을 통해 보이는 서비스 포트들에 대해서는 사용 목적을 확인 후 불필요한 통신 포트나 서비스를 차단 또는 제거 한다. 스위치의 물리적 포트인 경우 셀프루프(Self-Loop) 차단 기능 등이 있는지 확인하여 루프 시 포트 자동 차단 기능을 활용한다.

보안장비의 배치는 순서가 중요하므로 OSI Layer중 몇 Layer까지 체크하는 장비인가를 고려한다. 일반적으로 Layer가 높을수록 내부망 단에 가깝게 설치되는 경향이 높으며, 이는 상위 Layer를 보는 장비일수록 부하에 영향을 크게 받기 때문이다. Layer 4에 해당하는 방화벽이 Layer 7에 해당하는 침입방지시스템(IPS: Intrusion Prevention System)보다 외부망쪽에 가깝게 설치된다. 외부 특정 공격이 설치된 보안장비에 영향을 끼치지 않도록 우선순위를 고려해야 한다. DDoS 장비는 Layer 4~7 및 흐름을 체크하는 장비이지만 항상 외부망에 가깝게 설치된다. 이는 DDoS 장비가 없을 경우 DDoS 공격 시 방화벽이나 침입방지시스템 등의 장비가 정지될 수 있기 때문이다.

침입차단시스템의 경우 인바운드 패킷에 대한 차단과 내부에서 발생되는 아웃바운드 패킷도 고려하며 비용의 투자가 가능하다면 백본을 두고 상하로 위치하거나, 이중화를 하여 서비스의 분산, 지속성을 유지하되 정책은 동기화 기능을 통해 차단 정책에 대한 누락을 없앤다.

개인정보필터링의 경우에는 DMZ 영역과 사용자 PC 영역에 적용하여 개인정보 노출 위험을 줄이고, 유해사이트 차단시스템의 경우 내부 구성원에 대한 관리 포인트이기에 내부 백본에서 외부망으로 향하는 구간을 미러링하여 설치하며, 장비의 특징상 네트워크에 영향을 끼치지 않고 데이터 흐름을 모니터링 할 수 있는 TAP(Test Access Port)을 사용하거나, 백본 옆에 연결하는 구성을 하여야 한다.

서비스 분산 시스템의 경우 DMZ 영역에도 적용하여 불특정 다수의 접속에 대한 트래픽에도 대비하도록 하며, Layer 7의 스위치를 통해 변경되지 않는 콘텐츠들은 캐싱을 통해 빠른 서비스를 제공하도록 한다.

4.1.2 DMZ 영역

서버의 경우 1차적으로 불필요하게 오픈된 포트와 서비스를 차단하도록 설정하며, 2차적으로는 상단 침입차단장비에서 화이트 리스트 기반으로 허용하여야 하는 IP와 Port에 대한 정책을 설정한다. 이때 교육부 위협탐지정책 등으로 통보된 불량 IP의 경우 침입차단장비에 반드시 등록한다.

데이터베이스 서버 및 내부 시스템은 DMZ 영역에 두지 않고 내부 서버 영역으로 위치를 변경하며, DMZ 영역에서 내부 서버 영역으로 들어오

는 트래픽 역시 침입차단장비를 거쳐 들어올 수 있도록 구성한다.

홈페이지 서버의 경우 웹 취약점에 대한 공격이 가장 많으므로 웹 방화벽을 두어 모니터링하고, 웹 및 DMZ 영역에서 서비스하는 것 중 중요정보를 담고 있는 콘텐츠는 전송 계층 보안(TLS: Transport Layer Security)의 암호화 트래픽을 통해 전달될 수 있도록 설정한다.

4.1.3 일반 서버 영역

사설 IP 영역을 구성하려면 최초 환경 구성이 어렵고, 현재 운영 중인 IP 영역의 변경이 어려울 수 있으므로 기관의 의지가 중요하다. 공인 IP가 많을수록 외부 접근시도의 주요 공격대상이 되므로 내부적인 서비스만 담당하는 경우 공인 IP 사용에 주의한다. 사설로 운영되지만 인터넷을 사용할 경우 네트워크 주소 변환(NAT: Network Address Translation), 포트 주소 변환(PAT: Port Address Translation)을 통해 외부에 쉽게 노출되지 않도록 한다. 내부 서버 영역에서 대내 서비스를 담당하는 서버들의 경우 사설 IP를 사용하도록 한다.

4.1.4 내부 서버 영역

내부 서버에 업로드 시킨 Data는 DRM 등을 통해 암호화된 파일로 관리하되, 암호화는 256 비트 이상으로 국가정보원장이 승인한 암호논리를 사용한다. 암호화 적용 후 패킷 스캔을 통해 정상적으로 암호화 전송이 되는지 점검한다.

접근제어시스템을 통해 권한이 허가된 관리자 단말 및 사용자만 접근을 승인한다. 접근제어시스템을 통해 정당한 관리자가 접속 후에도 작업 및 명령어에 대한 작업 기록 및 접근 기록을 관리하며, 인가되지 않은 별도의 저장장치 및 외부로의 통신을 허용하지 않는다. 또한, 별도의 실행파일이 서버 내에 실행될 때는 관리자의 승인을 받도록 하여야 하며, 가능한 범주에서 작업자별 계정을 분리하고, 각 작업별 접근 권한 및 실행권한을 차등하여 할당한다.

원격데스크톱, Telnet 등의 원격 접속 포트는 공개되어 있으므로 해당 포트를 차단한다. 부득이하게 포트와 서비스 사용을 허용한 경우 목적이 달성되면 해당 서비스 및 포트를 차단하거나 SSH 22번에서 다른 포트로 변경한다. 또한, 공인 IP 할당을 최소화 하고, 허용된 서비스 이외의 불필요한 응용프로그램의 설치를 통제한다.

4.1.5 사용자 영역

내부 사용자에게 IP를 할당할 경우 네트워크 접근제어(NAC: Network Access Control) 및 IP 관리도구를 이용하여 사용하는 IP와 MAC간의 충돌을 보호하고, 변경금지를 설정하며, 임의 단말의 유입을 자동적으로 차단한다. 인터넷 PC의 경우 네트워크 접근제어를 이용하여 백신 소프트웨어 등 필수 프로그램의 기본적인 보안체계를 갖추어야 하며, 이외에 인증을 통해 신원을 확인하고 사용할 수 있는 프로세스를 갖춘다. 개인 단말의 보안 외에도 유해사이트 차단시스템을 통해 접근 가능한 사이트만을 허용하고, 그 외 사이트는 모두 차단한다.

비인가 무선인터넷 사용을 차단하기 위해서는 외부의 미승인 AP에 내부 단말이 연결되는 것을 방지하기 위하여 내부 단말에 Agent 혹은 내부망에 별도의 무선침입탐지시스템(WIPS), 무선네트워크접근제어(WNAC) 장비를 설치하여 선별적으로 AP에 접속할 수 있도록 강제적인 보안 정책을 적용한다. 네트워크 이름(SSID)의 브로드캐스팅을 중지하고, 추측이 어려운 복잡한 SSID를 사용한다. WPA2 이상(256비트 이상)의 암호체계를 사용하여 소통자료를 암호화하고, MAC 주소 및 IP 주소 필터링을 설정하며 동적 호스트 구성 프로토콜(DHCP: Dynamic Host Configuration Protocol) 사용을 금지한다. 또한, 원격 인증 전화 사용자 서비스(RADIUS: Remote Authentication Dial-In User Service)를 사용하고, 무선망을 통한 업무망 정보시스템 접근을 정보보호시스템 등으로 차단한다. 그리고 무선단말기, 중계기(AP) 등 무선랜 구성요소별 분실, 탈취, 훼손, 오용 등에 대비한 관리적, 물리적 보안대책을 수립한다.

비인가 단말의 경우 관리자의 허가를 받아 사용하도록 하며, 내부망에 접근하고자 할 때 IP 실

명제를 구현하며, 할당 받은 IP, MAC 주소 외 임의의 단말을 연결할 수 없도록 IP 관리방안을 수립한다. 인가된 단말이라 하더라도 단말 내에 백신 소프트웨어, 정보보안을 위한 필수 프로그램, 운영체제나 백신 소프트웨어의 최신 패치 등이 적용이 되지 않은 단말기에 대해서는 네트워크 서비스를 제한하도록 한다.

휴대용 저장매체의 통제를 강화하기 위하여 데이터 유실방지(DLP: Data Loss Prevention), 매체제어 등의 솔루션을 통해 인가받지 않은 저장매체를 사용하지 못하도록 한다. 보안 USB를 외부에 반출할 경우 반출 시스템을 통하여 인가 및 이력 관리를 하고, 내부에서 활용할 경우 사용자별 권한에 따라 읽기와 쓰기 기능 제어 및 사용이력에 대한 감사로그를 관리한다. 사용자 PC의 경우 USB 자동실행 등을 제한하는 정책을 적용하고, 외부 매체 연결 시에 자동 백신 검사의 기능을 활성화한다. 서버실 등 출입통제 구역을 진입할 경우 단말, USB, 휴대폰 등 저장 매체의 반입을 제한하며, CCTV 등을 이용하여 작업자에 대한 관리감독을 수행한다.

4.2 정보시스템 구성 방법

방화벽, 네트워크 시스템(백본, L7 및 L4 스위치 등)은 장애에 대비하여 이중화로 구성하여 Active-Active, Active-Standby의 형태로 운영한다. 이중화는 Active-Active로 운영하는 것보다 Active- Standby로 운영하면 장비의 안정성을 높일 수 있다. Active-Active로 운영하더라도 장애에 대비하여 이중화 시스템의 총 사용 용량의 절반 이내에서 시스템을 운영하면 장비의 안정성을 높일 수 있다.

행정기관의 네트워크 장비(L3이상 스위치라우터 등) 및 보안기능이 있는 L2 스위치는 국가정보원의 공통평가기준(CC: Common Criteria) 인증을 받은 제품을 도입하거나 교육부를 거쳐 국가정보원의 보안성 검증을 거친 제품을 도입하여야 한다.

정보시스템에 대한 DDoS 공격에 대비하기 위하여 DDoS 방지시스템을 게이트웨이(라우터, L3 이상 네트워크 스위치 등) 뒤쪽에 설치한다.

시·도교육청 등 행정기관은 나이스(NEIS), 에듀파인(Edufine) 등 교육기관의 중요 정보시스템의 보안을 강화하기 위하여 이중으로 침입차단시스템 등 보안장비를 설치하여 운영한다.

대학의 경우 대학 본부와 분교 또는 캠퍼스 연결은 전용회선을 통해 침입차단시스템을 연결하면 별도의 보안장비 없이 대학 본부의 보안 정책이 대학 캠퍼스에 적용될 수 있다.

네트워크 상단의 네트워크 보안시스템의 경우 성능이 낮은 장비가 성능이 높은 장비보다 상단에 설치되는 경우 보안시스템에 부하가 과도하게 발생하여 트래픽 병목 및 서비스 장애가 발생할 수 있다. 이를 해결하기 위해서는 네트워크 보안시스템을 설계할 때 장비의 배치순서를 고려해야 한다.

L4 스위치나 L7 스위치는 DSR(Direct Server Return) 방식으로 구성한다. 이를 통해 부하분산(Load Balancing)을 구성해 나가는 패킷이 L4 스위치나 L7 스위치를 거치지 않고 사용자에게 데이터가 전달되는 방식으로 구성함으로써 네트워크 대역대마다 여러 대의 L4 스위치나 L7 스위치를 두지 않아도 된다. L4 스위치 대신 L7 스위치를 도입하고 웹 가속기와 함께 홈페이지를 운영하는 기관은 L7 스위치를 통해 홈페이지 프로그램 파일(HTML, JSP 등)을 직접 웹 서버로 전달하도록 하고, 이미지 파일(gif, jpg 등), 플래쉬 파일(flv, swf), 동영상 파일(wmv)은 웹 가속기로 전달되도록 L7 스위치를 설정한다. 이로써 사용자에게 빠른 홈페이지 서비스를 제공할 수 있고, 홈페이지 프로그램이 전달되면서 발생하는 속도 저하 문제를 해결할 수 있다.

<표 4> 네트워크 구간 설정 예

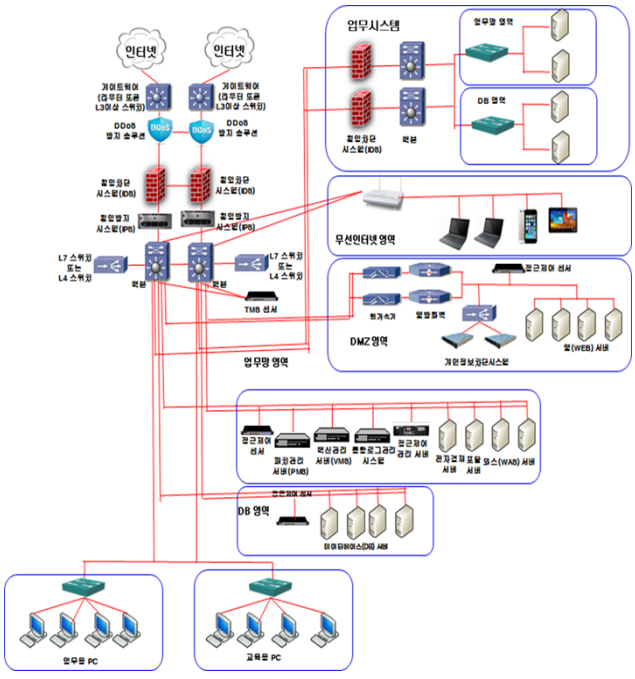
대상	IP 주소
DMZ 영역	192.X.X.1~192.X.X.255
업무망 영역	172.X.X.1~172.X.X.255
DB 영역	168.X.X.1~168.X.X.255
업무용 PC	10.1.X.1~10.1.X.255
교육용 PC	10.1.X.1~10.1.X.255

DMZ 영역, 업무망 영역, DB 영역, PC 등 기관 내 정보시스템은 <표 4>와 같이 사설 IP로 운영하며, 네트워크 영역은 서로 다르게 설정하고, 서

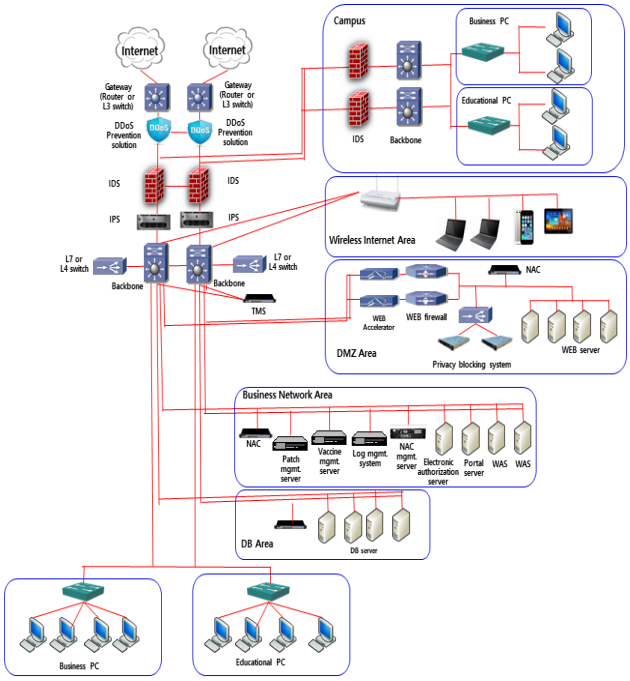
로 다른 네트워크 영역을 연결할 경우 침입차단 시스템을 이용하여 필요한 통신포트만 오픈하여 지원한다. DMZ 영역 내 정보시스템에 공인 IP가 부여되면 시스템 관리자가 유지보수, 관리 등을 위해 정보시스템 접근 시 외부 인터넷 영역을 통해 접근하게 되며, 이 때 시스템 관리자가 정보시스템 관리를 위해 전송하는 중요 데이터가 외부 해킹에 의해 유출될 수 있다.

위협관리시스템(TMS: Threat Management System) 센서를 백본 뒤에 설치해 소관 기관의 정보시스템을 대상으로 하는 해킹 행위를 탐지하고 대응한다. 핫스팟을 이용한 업무용 PC의 인터넷 접속 차단과 비인가자 접근을 차단하기 위하여 PC 접근제어시스템을 설치한다. 무선인터넷은 기관장이 지정한 장소에만 설치하고 침입차단시스템 등을 별도의 영역으로 분리하여 무선인터넷을 통해 내부의 중요 정보시스템(서버, 네트워크, PC 등)에 접근이 불가능하도록 차단하고, 인터넷 서비스만 지원한다.

이상의 정보시스템 구성 방안을 적용한 행정기관과 대학의 정보시스템 아키텍처는 [그림 1], [그림 2]와 같다.



[그림 1] 행정기관의 정보시스템 아키텍처



[그림 2] 대학의 정보시스템 아키텍처

5. 결론

국내외에서 빈번하게 발생되고 있는 사이버침해 사례를 분석해 보면 인터넷을 통한 기관 외부의 불특정 다수로부터의 악의적인 사이버공격에 의하여 여러 기관 및 기업의 중요 정보가 유출되거나 훼손, 삭제 및 인터넷 접속 불가 등의 피해를 입는 사례가 발생되고 있고, 침해 사례의 발생 빈도가 증가하고 있다.

다수의 개인정보와 중요 업무 자료를 생산, 보유, 활용 및 공유하고 있는 일선 행정기관 및 각급 학교도 사이버공격에 대하여 안전지대가 아니다. 실제로 여러 교육청과 대학에서 발생된 사이버침해 사례를 분석한 결과 그 원인이 주로 정보시스템 및 정보보호시스템에 대한 기술적인 이유와 관리적인 이유에 기인하고 있다.

이에 본 연구에서는 시·도교육청 등의 행정기관과 여러 대학의 정보보호 실태를 조사·분석하였다. 분석결과 대부분의 행정기관은 정부의 정보보호 관련 법제도의 권고사항을 최대한 반영하여 관리적, 물리적, 기술적 정보보호 활동을 수행하고 있으나, 대학의 경우 행정기관에 비하여 법제

도니 지침의 적용이 엄격하게 준수되지 못하고 있고, 정보보호 인프라가 충분히 갖추어져 있지 않거나 정보보호 전문 인력이 부족하여 정보보호 활동이 취약하다. 이의 결과로 대학은 행정기관에 비하여 여러 정보시스템이 사이버공격에 노출되어 빈번하게 사이버침해가 발생되고 있다. 따라서 교육기관에서 정보시스템을 구축하거나 운영할 때 인터넷 영역, DMZ 영역, 일반 서버 영역, 내부 서버 영역 및 사용자 영역 별로 수행하거나 지켜야 할 보안성 강화 방안을 제시했다.

또한, 행정기관 및 대학의 정보보호 업무담당자들이 보다 정확하게 체계적으로 정보보호 활동을 수행하여 사이버공격을 예방하고, 피해 발생 시 즉각적으로 대응활동을 수행할 수 있도록 보안관리 방안과 보안성 높은 정보시스템 아키텍처를 제시했다.

본 연구는 행정기관과 대학에서 현재의 정보시스템을 관리적 관점, 물리적 관점, 그리고 기술적 관점에서 보안성을 높이는데 활용될 수 있다. 그리고 기관 내에 정보보호 전문가가 부족하더라도 본 연구에서 제안하는 보안관리 방안과 정보시스템 아키텍처를 참고하여 정보시스템을 구축하고, 정보보호 활동을 수행함으로써 자발적이고 적극적인 사이버침해에 대한 예방 및 대응활동을 수행할 수 있다.

참 고 문 헌

[1] 신경아, 이상진 (2012), 클라우드 컴퓨팅 서비스에 관한 정보보호관리체계, **정보보호학회논문지**, 22(1), 155-167.

[2] 한국인터넷진흥원 (2013), **2013년 주요 침해사고 사례와 대응, 17th 해킹방지워크숍**, 한국인터넷진흥원.

[3] 한국인터넷진흥원 (2005), **정보시스템 구축 단계별 정보보호 가이드라인**, 한국인터넷진흥원.

[4] 교육부 (2014), **정보보안 기본지침 (교육부 예규 제19호)**, 교육부.

[5] 국가사이버안전센터 (2005), **국가사이버안전 매뉴얼**, 국가사이버안전센터.

[6] 국가보안기술연구소 (2013), **안전한 정보통신 환경 구현을 위한 네트워크 구축 가이드라인**, 국가보안기술연구소.

[7] Michael Goodrich, Roberto Tamassia (2014), **Introduction to Computer Security 1st Edition,** Edinburgh: Pearson Education.

[8] 행정자치부 (2012), **공공기관 개인정보처리 단계별 기술적 보호조치 가이드라인**, 행정자치부.

[9] 행정자치부 (2006), **전자정부 보안관리 실무 매뉴얼 - 정보시스템 구축개발 및 운영관리 담당자용 -**, 행정자치부.

[10] Karen S., Paul H. (2008), *Guidelines on Firewalls and Firewall Policy*, U.S. Department of Commerce.

[11] Martin P., Brian C., Srinvas T., Steve G., John S., Bruce M., Rahul K. (2013), Cisco Service Ready Architecture for Schools Design Guide, https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Education/SchoolsSRA_DG/SchoolsSRA-DG.html.

[12] 한국정보화진흥원 (2008), **학교 통신망 구축 운영 가이드**, 한국정보화진흥원.

[13] 백민정, 손승희 (2011), 일반 논문 : 중소규모 조직구성원의 정보보안인식과 행동이 정보보안성과에 미치는 영향에 관한 연구, **중소기업학회논문지**, 33(2), 113-132.

[14] 임명성 (2014), 정보보안 인식 교육의 효과에 대한 연구, **디지털정책학회논문지**, 12(2), 27-37.

[15] 유기훈, 최웅철, 김신곤, 구천열 (2008), 학내 정보보호지침 수립에 관한 연구, **IT서비스학회논문지**, 7(1), 23-43.

최 진 명

2000 숭실대학교
컴퓨터학과(공학석사)
2007 숭실대학교
컴퓨터학과(공학박사)
2007~2012 한국지역정보개발원 정책연구단
책임연구원
2013~현재 건양대학교 융합IT학과 조교수
관심분야: 정보시스템 아키텍처, 소프트웨어 아키텍처, 정보기술 아키텍처, 정보보안, 소프트웨어 개발 프로세스
E-Mail: jameschoi@konyang.ac.kr

김 두 연

1988 숭실대학교
전자계산학과(공학석사)
2007 숭실대학교
컴퓨터학과(공학박사)
2003~2012 교육과학기술부 부이사관
2012~현재 건양대학교 융합IT학과 부교수
관심분야: 소프트웨어공학, 데이터베이스, 스마트교육
E-Mail: kimdoo@konyang.ac.kr