韓國컴퓨터情報學會 論文誌
第16卷 第12號, 2011. 12.

2011-16-12-4-1

사이버 공격에 대비한 대학의 정보보안 현황 및 개선 방안

강 영 선*, 최 영 우**

Current Status of Information Security against Cyber Attacks in Universities and Its Improvement Methods

Youngsun Kang*, Yeongwoo Choi**

요 약

본 논문은 지식정보화사회에서 최근 화두가 되고 있는 정보보안 문제를 대학 실태조사를 통한 보안 현황을 살펴봄으로써 고등교육기관으로서 대학이 향후 모색해야 할 정보보안 개선 방안을 마련하는데 있다. 본 연구는 국내 대학 중 재학생 규모별로 임의로 선별하여 각 대학 보안담당자들을 대상으로 이메일을 통한 설문 조사를 실시하였다. 조사표본 대상 중 회신을 준 대학은 총 45개교로 27개의 4년제 대학과 18개의 2년제 대학이 설문에 응해 주었다. 본 연구의 설문 조사 결과, 정보자산에 대한 보안은 사전예방이 가장 중요하다는 것을 다시 한 번 확인할 수 있었으며, 정보보안 개선 방안으로 대학의 통합보안 관리 정책 수립과 가이드라인 제시 등의 제도적 지원 강화와 정보자산의 중요성 및 보안의 필요성을 내부 구성원과 함께 공유해야 함을 제안한다. 또한 정보보안 전문 인력의 충원 및 양성과 전담부서 설계 등 행정적·재정적 지원 방안 마련에 함께 모색되어야 함을 알 수 있었다.

▸ Keyword : 정보 보안, 사이버 공격, 침해 사고, 정보 자산

Abstract

This paper suggests several methods of improving information securities of universities through the investigations of the current status of information securities in universities, which is becoming a hot topic in knowledge and information societies. In this paper, universities were randomly selected according to their size, and surveyed through email questionnaire to the persons in charge of security in each university, and 27 universities and 18 colleges were replied. From the survey results we confirmed that the pre-prevention is the most important thing in securing information assets, also in universities, and, in this paper, systematic support must be strengthened to

• 제1저자 : 강영선 • 교신저자 : 최영우
• 투고일 : 2011. 07. 16, 심사일 : 2011. 09. 28, 게재확정일 : 2011. 10. 24..
* 숙명여자대학교 전산교육전공(Dept. of Computer Education, Sookmyung Women's University)
** 숙명여자대학교 컴퓨터과학과 교수(Dept. of Computer Science, Sookmyung Women's University)
※ 본 연구는 숙명여자대학교 2010년 교내연구비 지원에 의해 수행되었음

establish a comprehensive security management policy and guidelines for the universities, and the importance of information assets and the necessity of security needs to be shared with the members in the universities. Moreover there must be full administrative and financial support, including recruitment and training of information security professionals and the establishing a separate security division.

▸ Keyword : Information Security, Cyber Attacks, Security Incidents, Information Assets

Ⅰ. 서론

현대사회는 정보가 지배하는 세상이라 해도 지나치지 않을 만큼 빠른 속도로 첨단 정보통신 기술이 발전하고 있다. 새롭게 형성된 사이버 공간을 통해 정보 자산의 공유 기회가 커짐에 따라 부적절한 네트워크 접근 등의 부작용도 함께 발생하면서 정보자산의 관리와 보안 통제가 점차 어려워지고 있다[1]. 특히 이러한 사이버 공간에서의 의도적 또는 비의도적인 모든 위협은 현실 세계에서도 그대로 반영되면서 정보자산의 파손에 따른 피해가 점차 늘어나고 있는 추세이다. 이러한 환경 속에서 첨단 정보인프라를 구축하여 교육수요자를 중심으로 한 양질의 교육서비스를 제공하며 정보화 사업에서 괄목만한 성장을 거듭하고 있는 대학 역시 교내·외의 수많은 정보보안 위협으로부터 대응 방안을 모색하지 않을 수 없게 되었다.

과거 학사업무 전산화에서 시작된 대학 정보화는 1990년대에 들어서며 인터넷이라는 새로운 미디어의 출현과 정보기술의 비약적인 발전으로 인해서 시스템 통합 형식의 학사 및 행정업무 중심의 전산화에서 벗어나 역할기반(Role-based) 포털시스템 중심의 통합 종합정보시스템을 구축하면서 유비쿼터스 캠퍼스를 구현해 가고 있다[2]. 그러나 공개된 네트워크를 이용하는 다양한 구성원과 자율을 중시하는 대학의 특성으로 인해서 보안 사고가 빈번하게 발생하고 있으며, 정보보안 정책의 수립 및 적용에 어려움을 겪고 있는 것이 현실이다.

Ⅱ. 사이버 공격에 따른 침해사고 현황 및 대응 방안

1. 정보시스템의 이해

인터넷은 전 세계에 있는 수많은 네트워크와 컴퓨터들을 하나의 공통된 통신 표준인 TCP/IP 프로토콜로 연결하여 이들 상호간의 접속을 가능하게 하는 개방형 네트워크이다. 종전의 집중형 정보통신망의 한계를 극복하고자 개발된 인터넷은 단순히 정보통신망을 기술적으로 분산시키는 데에서 그친 것이 아니라 사이버 공간을 통해 정보자산의 흐름 자체를 사회적으로 분산시키는 결과를 만들었다.

데이터 통신을 목적으로 개발되어 온 인터넷은 다수의 사용자에 의해 컴퓨터나 네트워크가 빈번하게 사용되어질수록 제3자에 의한 정보 유출, 변경, 파괴 등과 같은 위험성과 취약성은 더욱 증가하게 되었다.

이처럼 정보를 저장하고 유통시킬 수 있는 모든 정보 매체로부터 발생할 수 있는 각종 위협으로부터 정보자산을 보유한 주체가 의도하지 않은 형태로 조직의 정보자산이 유출, 변경, 파괴되는 것을 사전에 방지하는 것이 바로 정보자산에 대한 보호이다.* 정보보안의 목표는 크게 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 유지하고 보장하는 것으로 귀결된다[1]. 이는 위기상황 발생 시 조직의 손실을 최소화하고 사업의 연속성을 유지하기 위한 모든 제반 수단과 활동을 의미하기도 한다[3].

2. 침해사고 현황

한국인터넷진흥원의 '2010 정보시스템 해킹·바이러스 현황 및 대응' 보고서에[4] 의하면 2010년 한 해 동안 발생한 침해사고 유형별 전체 현황은 <표 1>과 같다. 해킹사고 피해기관별로 분류한 결과 개인(62.7%), 기업(34.7%), 대학(1.4%), 비영리(1.3%)의 순으로 나타나 2009년도 보다 개인이 차지하는 비율이 줄었지만 아직도 개인 인터넷 이용자 PC가 침해사고에 악용되는 경우가 많기 때문에 우리나라 이용자들의 보안인식 개선과 침해사고에 대비한 프로세스 마련이 시급한 것으로 나타났다[4],[5].

* 한국정보보호학회에서는 정보보호를 정보를 보호하는 포괄적인 개념으로, 정보보안은 기밀성을 중심으로 하는 기술적·관리적 보호를 강조하는 개념으로 정리하며, 정보보호 개념을 상위에 두고 있으나, 본 논문에서는 특별히 구분해서 사용하지 않지만, 인적자원 관리에서는 개념을 분리하여 사용한다.

표 1. 침해사고 유형별 현황 (건, %)
Table 1 Status of Cyber Intrusion Types

구 분	2009년	2010년
웜·바이러스	10,395	17,930
해킹신고처리	21,230	16,295
▪ 스팸 릴레이	10,148	5,216
▪ 피싱 경유지	988	891
▪ 단순 침입시도	2,743	4,126
▪ 기타 해킹	3,031	3,019
▪ 홈페이지 변조	4,320	3,043
악성 봇(Bot) 감염비율	1.0%	0.6%

국내외의 보안 침해사고는 과거의 단일시스템을 대상으로 하는 공격에서 분산 서비스 거부 공격, 웜·바이러스, 스파이웨어와 같은 네트워크 서비스 전체의 가용성을 침해하는 공격으로 계속 진화하고 있다. 이처럼 정보통신망 또는 정보시스템을 공격하는 모든 행위로 인해 정보보안 목표의 확보를 어렵게 하며, 조직의 정보자산에 영향을 주는 모든 전자적인 침해 행위와 그 결과로서 발생되는 모든 피해 영향을 일반적으로 '침해사고'로 간주한다. 정보보안의 목표 관점에서 고객정보 및 기밀정보 유출(기밀성 침해), 서비스 지연 및 중단(가용성 침해), 침입에 의한 정보 변조(무결성 침해) 등으로 그 유형을 분류할 수 있다[6],[7]. 또한 유형별 피해사고 사례로서 웹 해킹에 의한 전산망 피해(기밀성 침해)[8], 분산 서비스 거부 공격에(DDoS) 의한 침해사고(가용성 침해)[9], 제로보드 및 테크 노트 등의 취약점을 악용한 홈페이지 변조사고(무결성 침해)[10] 등이 대표적인 침해사고 예이다.

3. 국가의 대응 방안

우리나라는 2003년 1월에 발생한 1·25 인터넷 마비사고를 계기로 침해사고에 대비하기 위해서 <그림 1>과 같은 국가 사이버안전체계를 2007년에 수립하였다[11]. 대통령 직속 국가사이버안전전략회의를 구성하였으며, 국방부, 국가정보원, 정보통신부에 각각 관련 기관을 두어 대응해 왔으며, 이러한 체계를 바탕으로 2009년에는 국가정보화전략위원회를 출범시켰고, 같은 해 국가 사이버 위기 종합대책을 발표하기에 이르렀다[12].

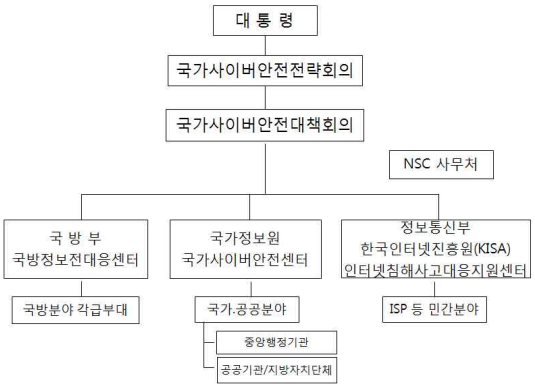

그림 1. 국가 사이버 안전체계
Fig. 1. National Cyber Security System

또한 나날이 증가하고 있는 새로운 보안 위협들로부터 조직의 정보자산을 보호하고, 침해사고에 보다 효과적으로 대처하기 위해서 2007년에 '침해사고 대응절차'를 마련하여 운영하고 있다[6],[7]. <표 2>는 침해사고 대응절차의 단계별 구성, 수행 활동, 역할 및 책임을 보여준다.

표 2. 침해사고 대응 절차
Table 2 Response Procedures to Cyber Intrusions

단계	구성	주요 활동	역할/책임
1	예 방	- 정보보호를 위한 평시 활동 - 침해사고 대응팀 구성 및 운영 - 정보보호 교육을 통한 인식 제고	전체 임직원
2	탐지/분석	- 정보자산 모니터링 - 초기 분석	운영 담당자 보안 담당자
3	대 응	- 증거 데이터 수집/보호 - 침입 유형별 긴급조치	운영 담당자 정보보호 담당자
4	복 구	- 재발방지 조치 - 시스템 통제권 회복 후 재발 방지 대책 수립	운영 담당자 정보보호 담당자 정보보호 책임자

III. 대학의 정보보안 현황

1. 실태 조사 실시

본 논문에서는 대학의 정보보안 현황을 살펴보기 위해서 비교적 교육정보화가 잘 이루어진 대학을 중심으로 현황을 파악하였다. 2010년부터 2011년 사이 전국의 대학교를 재학생 규모별로 임의로 선별하여 각 대학의 보안담당자들을 대상으로 설문 조사를 실시하였다. 4년제 대학은 수도권 15개, 비수도권 12개의 총 27개 대학과 2년제 대학은 수도권

및 비수도권을 합쳐서 총 18개 대학에서 설문에 대한 응답을 주었다.

설문은 전년도 침해사고 발생 여부와 원인, 침해사고 예방 및 대응 현황과 노력, 향후 개선되어야 할 정보보안 과제 등 세 가지 지표로 나누어 총 13개의 문항으로 구성하였으며, 설문 문항은 <표 3>에 요약하였다. 또한 조사결과를 국내 기업의 현황과 비교하기 위해서 설문 문항 중 일부는 한국인터넷진흥원(KISA)의 '2008 정보보호 실태조사-기업편'[13]과 (주)네트워크 타임즈의 '2009 Information Security Al Guide V.4'[14]를 참조하여 작성하였다.

표 3. 설문 문항 요약
Table 3 Summary of Questionnaire

구 분	문항 구성
전년도 침해사고 발생 여부와 원인	침해사고 발생 여부, 원인 및 유형 파악
침해사고 예방 및 대응 현황과 노력	전년대비 보안강화 여부, 정보보안 부서 운영 여부, 전담인력 확보 현황, 보안 위협 요소 파악, 정보보안 교육현황 파악, 침해사고 대응방안 및 절차 규정 수립 여부, KISA 권고안 준수 여부, 보안 솔루션 파악
향후 개선되어야 할 정보보안 과제	보안수준 제고를 위해 개선되어야 할 과제 파악

2. 대학의 정보보안 현황

첫 번째 지표의 문항 중에서 전년도에 사이버 공격에 의한 침해사고 발생 여부에 대한 결과는 <표 4>와 같다. 설문 참여대학의 44.4%가 침해사고를 경험하였다고 응답하였으며, 4년제 대학의 경우 소재지와 무관하게 거의 50% 이상이 침해를 받았고, 2년제 대학은 33.3%로 상대적으로 적었다.

표 4. 전년도 침해사고 발생 여부 (%)
Table 4 Occurrences of Cyber Intrusion in Previous Year

구 분	4년제 대학	2년제 대학	전체 평균
침해 발생	51.9	33.3	44.4
침해 미발생	48.1	66.7	55.6

침해사고가 발생한 대학을 대상으로 한 원인 조사에서는 <표 5>와 같이 사용자의 보안정책 미 준수 및 의식부족을 25%로 가장 먼저 꼽았다. 다음으로 네트워크, 서버에 대한 공격 증가를 18.2%로서 대학의 규모가 큰 경우 상대적으로 침해사고에 대한 노출 가능성이 높은 것으로 나타났다. 이는 통합 관리되고 있지 않은 서버와 PC 문제로서 주로 이를 이용하는 사용자들의 보안 불감증에서 기인한 것으로 추정된다. 수도권 소재 4년제 대학의 경우 사용자의 보안정책 미준수 및 의식부족이 상대적으로 높은 비율을 차지하는 반면에 비수도권 4년제 대학과 2년제 대학의 경우 발생 원인이 골고루 지적되어 대조를 보이고 있다. 또한, 보안정책 또는 프로세스의 부재나 내부자의 정보유출 항목에 대해서는 단 3개교에서만이 침해사고의 원인으로 지목한 것은 설문조사 대상이 업무 담당자인 점을 감안하여야 할 것이다.

표 5. 침해사고 발생 원인 (중복 응답)
Table 5 Reasons of Occurrences of Cyber Intrusions (Multiple Choices)

발생 원인	비율(%)
사용자의 보안정책 미 준수 및 의식 부족	25.0
네트워크, 서버 등에 대한 공격 증가	18.2
전담인원 및 예산 부족	15.9
통합·관리되지 않는 대학 내 서버문제	11.4
공격기술보다 뒤쳐진 보안기술	11.4
무선 등 공격통로 및 보안대상 데이터 증가	6.8
공격기술의 고도화	4.5
보안정책, 프로세스 부재	4.5
내부자 정보유출	2.3

침해사고 유형은 주로 악성코드 감염(54.8%), 경유지 악용(32.3%), 홈페이지 변조(9.7%), 자료훼손 및 유출(3.2%)의 순으로 나타났으며, 네트워크 서비스 전체의 가용성이 침해되는 공격도 꾸준히 증가하고 있음을 보여주고 있다.

두 번째 지표인 각 대학의 침해사고 예방 및 대응 현황과 노력에 대한 설문에서 우선 각 대학이 전년도 대비 보안강화 여부를 묻는 문항에 대하여 <표 6>과 같이 응답 대학 대부분이 전년 대비 비슷하거나(60.0%), 전년 대비 소속 대학의 보안강화로(40.0%) 나타났다. 4년제 대학이 한층 강화됨이 48.1%로 2년제 대학 27.8%보다 보안 강화에 더욱 노력하고 있으며, 이는 침해사고 발생 여부와도 관련이 있다. '전년대비 취약해졌다' 또는 '모르겠다'로 답한 대학은 없었다.

표 6. 전년대비 보안 강화 여부 (%)
Table 6 Strengthening University Securities Comparing to the Previous Year

구 분	4년제 대학	2년제 대학	전체 평균
거의 비슷함	51.9	72.2	60.0
한층 강화됨	48.1	27.8	40.0

<표 7>은 가장 문제시 되는 보안 위협에 대한 설문 결과로서 여전히 많은 대학에서 '사용자의 보안정책 미 준수 및 정보보안 의식 부족'을 가장 위협적인 요소로 지적하였으며, 그 다음으로 '대학 경영진의 보안 의지 부족'을 지적했다.

표 7. 최근 보안 위협 요소 (중복 응답)
Table 7 Recent Factors for Threatening Information Security (Multiple Choices Allowed)

보안위협 요소	비율(%)
사용자의 보안정책 미 준수 및 정보보안 의식부족	29.5
대학 경영진의 보안 의지 부족	15.4
DoS/DDoS	12.3
웹 해킹	11.0
내부자에 의한 정보 유출	11.0
통합·관리되지 않는 대학 내 서버문제	9.6
웜 바이러스	6.8
피싱	4.1
스팸	2.7
기타	1.4

다음으로 침해사고 예방과 대응을 위한 전담부서가 대학에 배치되어 있는가를 묻는 설문 결과는 <표 8>과 같다. 4년제 대학은 66.7%가 전담부서를 운용하고 있지만, 2년제 대학은 33.3%만이 운용하여 2년제 대학이 4년제 대학보다 환경이 열악한 것을 알 수 있다.

표 8. 전담부서 존재 여부 (%)
Table 8 Existence of Exclusive Security Department

구 분	4년제 대학	2년제 대학	전체 평균
있음	66.7	33.3	53.3
없음	33.3	66.7	46.7

다음으로 보안운용 전담 인력 현황에 대한 설문에 대하여 기존의 정보부서 내에 배치된 전산담당자가 정보보안 업무를 겸해서 수행한다고 답한 대학이 31개교이며(68.8%), 별도의 전담 부서내에 배치된 정보보안 담당자가 업무를 수행하고 있다고 답한 대학이 8개교로서(16.7%) 아직 전담 정보보안 담당자를 1명 이상 배치하여 운용하는 대학이 적은 것을 알 수 있다. 특히 2년제 대학에서는 1개교만이 전담 정보보안 담당자를 운용하고 있어서 4년제 대학의 7개교에 비해서 크게 부족한 실정이다.

다음은 전체교직원 또는 보안 운용담당자를 대상으로 정보보안 교육의 실시 여부에 대한 설문결과로서 <표 9>와 같으며, 년 1회 이상의 정보보안 교육을 정기적으로 실시하는 대학이 33개교로(73.3%) 나타났으며, 2년제 대학은 61.1% 실시로 이에 대한 개선이 필요하다. 그러나 정보보안에 대한 위기의식이 전반적으로 고조되었음을 확인할 수 있다.

표 9. 정보보안 교육 실시 여부 (%)
Table 9 Having Information Security Education

구 분	4년제 대학	2년제 대학	전체 평균
실시(1회 이상)	81.5	61.1	73.3
미실시	18.5	38.9	26.7

침해사고에 대비한 대응방안 및 절차 등의 규정 또는 프로세스가 있느냐는 문항에 대하여는 <표 10>과 같이 34개(75.6%) 대학이 있다고 응답하였으며, 특히 4년제 대학인 경우에는 24개(88.9%) 대학이 규정 또는 프로세스가 있다고 응답하였다. 2년제 대학의 경우 대응방안 및 규정을 상대적으로 적게 보유한 것으로(55.6%) 나타났다. 또한 이러한 절차들이 KISA가 권고하는 안을 따르는 대학이 74%로 나타나서 대부분의 대학이 KISA의 권고안을 준수하고 있는 것으로 나타났다.

표 10. 대응방안 및 절차 보유 여부 (%)
Table 10 Having Response Procedures

구 분	4년제 대학	2년제 대학	전체 평균
보유	88.9	55.6	75.6
미보유	11.1	44.4	24.4

침해사고에 대비한 대응방안 및 절차 등의 규정 또는 프로세스가 있다고 응답한 34개 대학을 대상으로 KISA에서 권고하는 <표 2>의 침해사고 대응 절차인 예방, 탐지·분석, 대응, 복구 절차에 대한 각 단계별 활동에 대한 책임을 묻는 설문 결과는 <표 11>과 같다. 각 절차에 대해서 정보보안·보호 담당자 및 전산 운영 담당자가 주로 역할을 담당하고 있으며, 여기서 전체 65.3%를 차지하는 정보보안·보호 담당자는 전산담당자가 보안 업무를 겸해서 수행하는 것도 포함하고 있다. 따라서 대학의 정보부서 내 인력들이 정보보안을 위한 제반활동 전반을 책임짐에 따라 장기적으로 이들의 업무 부담이 증가하고 이로 인해 보안정책 적용에 있어서도 갈등이 발생할 소지가 있을 것으로 예상된다. 따라서 보안전문 인력을 충원하는 문제는 대학의 정보보안 수준 제고를 위한 중요한 과제이다.

현재 사용 중인 보안 솔루션을 묻는 설문에 대해서는 응

답한 대학 모두가 PC용 백신 및 웹 방화벽을 사용하고 있었으며, 방화벽, IDS(Intrusion Detection System)·IPS(Intrusion Prevention System) 등의 기본적인 보안 솔루션들을 모두 도입하여 사용하는 것으로 파악되었다. 또한, 안티바이러스·스팸게이트웨이형, 안티 DoS(Denial of Service)·DDoS(Distributed DoS), VPN(Virtual Private Network), DB 보안솔루션, PMS(Patch Management System), 서버보안 및 재해복구 백업솔루션 등 다양한 보안솔루션들이 사용되고 있어서 대학의 보안 상태가 예상보다 높은 것으로 파악되었다.

표 11. 침해사고 대응 절차에 따른 책임 수행 (중복응답)
Table 11 Responsibilities of Each Response Procedure (Multiple Choices Allowed) (%)

책임 담당	예방	탐지·분석	대응	복구	전체 평균
전체 교·직원	3.9	0.0	0.0	5.1	2.3
전산운영 담당자	29.4	28.6	29.6	32.2	30.0
정보 보안·보호 담당자	66.7	67.3	66.7	61.0	65.3
기타	0.0	4.1	3.7	1.7	2.3

마지막 지표인 향후 대학의 보안수준 강화를 위해 개선되어야 할 과제를 묻는 설문에 대한 결과는 <표 12>와 같이 '보안전문가 등의 전담인력 확보 및 확충'과(27%) '사용자 및 경영자의 보안인식'을(23%) 가장 시급한 과제로 꼽았으며, 그 뒤를 이어 '충분한 보안예산 할당'(20.3%), '보안전담 부서 신설 등의 조직개편'(17.6%), '보안규정 및 프로세스 마련'(10.8%) 등의 구조적인 문제를 지적하였다. 보안담당자들의 이러한 지적은 향후 대학 조직 내 정보보안 전담부서의 구성과 인력 배치에 있어서 관심을 가져야 할 사항이다.

표 12. 향후 개선 과제 (중복응답)
Table 12 Future Assignments for the Improvements (Multiple Choices Allowed)

개선 과제	비율(%)
보안전문가 등의 전담인력 확보 및 확충	27.0
사용자 및 경영자의 보안 인식	23.0
충분한 보안예산 할당	20.3
보안전담 부서 신설 등의 조직 개편	17.6
법·제도·대응절차 등 보안 관련 규정 및 프로세스 마련	10.8

3. 기업 정보보안 현황과의 비교

대학의 정보보안 현황 및 수준을 기업과 비교하기 위해서 한국인터넷진흥원(KISA)에서 실시한 '2008 정보보호 실태조사-기업 편'에서 국내 기업의 정보보안 실태조사 결과를 참조하였다.* 여기서 기업 실태조사 지표인 "정보보호 기반 및 환경", "정보보호 대책", "개인정보보호 및 스팸 대응", "침해사고 대응" 및 "침해사고 피해" 중 대학 실태조사에서 사용한 세 가지 지표를 중심으로 살펴보았다[13].

기업의 "정보보호 기반 및 환경"을 살펴보면 조사 기업 전체의 33.4%가 정보보안을 위해 문서화된 정책을 수립하여 실시하고 있으며, 정보보안을 위한 인력, 조직 및 교육 운영에 있어서는 조사 대상 기업의 12.7%만이 전담 정보보안 조직을 설치하여 운영하고 있었다. 정보보안 교육의 필요성을 지적한 기업은 전체 49.1%로 나타났으며, 특히 개인정보를 다루는 기업의 93.7%가 개인정보 관리자를 대상으로 한 교육이 절실하다고 응답하였다. 그러나 실제 정보보안 교육을 실시하는 기업은 전체 13.7%에 그쳐서 현실의 요구와는 큰 차이가 있었다. 또한, 정보보안 관련 인력의 배치에 있어서는 기업 역시 정보보안책임자의 임명비율이 12.2%로 매우 저조한 것으로 나타났다. <표 13>에 기업과 대학의 정보보호 기반 및 환경에 대한 비교를 정리하였다.

이처럼 기업의 정보보안 기반 및 환경을 대학과 비교해 볼 때, 비록 두 실태 조사의 기간과 조사대상 표본 집단의 차이가 있지만 대학이 전반적으로 정보보안 기반 및 환경이 앞서 있음을 알 수 있었다. 이는 2,800개의 광범위한 기업에 대한 조사와의 비교로서 미처 정보보안에 대한 관심을 가질 수 없는 기업도 많이 포함되어 있음을 추측할 수가 있다. 또한, 과거 다른 기관에 비해 상대적으로 앞서 있던 기업의 정보보안 환경이 시간이 지난 현재에도 여전히 획기적인 개선으로까지는 이어지지 않음을 확인할 수 있었다. 그러나 정보보안을 위한 인력과 조직, 교육 운용에 있어서는 대학과 비교할 때 정보보안 역할과 책임 배분이 비교적 분명하였으며, 그에 따른 역할 수행과 운영에 있어서도 체계화되어 있었다.

* 한국인터넷진흥원(KISA)에서 실시한 '2008 정보보호 실태조사-기업 편'의 실태 조사기간은 2007년 11월부터 12월까지였으며, 조사 표본 사업체는 총 2,800개로 종사자 수 5명 이상의 네트워크로 연결된 컴퓨터를 1대 이상 보유하고 있는 전국의 사업체를 대상으로 함

표 13. 정보보호 기반 및 환경 비교 (%)
Table 13 Comparisons of Information Security Bases and Environments

항 목	기 업	대 학
정보보안 문서화된 정책 수립	33.4	75.6
정보보안 전담 조직 보유	12.7	53.3
정보보안 교육 실시	13.7	73.3

기업의 “침해사고 대응 및 피해 현황”을 살펴 본 결과 전반적인 재해 및 침해사고에 대비하여 대응활동과 비상복구 계획을 수립하여 운영하고 있는 기업은 전체 조사 기업의 31.2%였다. 그러나 전체 50.3%에 이르는 기업들이 사이버 상에서 정보보안 사고가 발생할 때 신고 조차하지 않은 것으로 응답하여, 기업 역시 ‘사용자와 경영자의 보안인식 개선’이 시급한 것임을 확인할 수 있었다.

침해사고 발생에 대해서 기업은 주로 다운받은 프로그램이나 이메일을 통한 웜·바이러스(41.4%)와 애드웨어·스파이웨어(40.1%) 등 악성코드 감염 순으로 나타났으며, 대학에서도 마찬가지로 주로 악성코드 감염(54.8%)이 가장 많은 것으로 파악되었으며, 이에 대한 결과를 <표 14>에 비교, 정리하였다. 대학과 기업 두 집단의 정보보안 수준 정도를 비교하는 것 자체가 표본의 차이 등으로 다소 무리한 점은 있지만, 두 집단의 인프라 격차 등을 실태 조사를 통해서 비교해 보는 것도 의미가 있다고 생각한다.

표 14. 침해사고 발생 유형 비교 (중복응답)
Table 14 Comparisons of Cyber Intrusion Types

구 분	유 형	%
기 업	악성코드 감염: 바이러스, 웜, 트로잔 공격	41.4
	악성코드 감염: 애드웨어, 스파이웨어 감염	40.1
	외부 비인가 접근	11.4
	DoS 공격	9.2
대 학	악성코드 감염	54.8
	경유지 악용	32.3
	홈페이지 변조	9.7
	자료 훼손 및 유출	3.2

Ⅳ. 대학의 정보보안 대응 방안

1. 정보자산 분류 및 보안정책 수립

2010년도 교육과학기술부가 수행한 교육기관에 대한 정보보호 수준을 진단한 결과에 따르면 시·도 교육청, 국·공립대학, 사립대학 순으로 보안 수준이 낮아지는 것으로 조사되었으며, 대학의 경우 통합보안 관리체계가 취약한 것으로 파악되어 대학차원의 제도적 보완이 시급한 것으로 나타났다[15]. 또한, 대학의 정보보안 현황을 살펴 본 결과 대학의 발달된 정보 인프라에도 불구하고, 이를 활용한 정보보안 정책의 구현에 있어서 대학 구성원의 보안 인식 부족과 전담조직 및 전문 인력 등의 부족은 여전히 대학 정보화의 걸림돌로 작용하고 있다. 대학이 보안 정책을 보다 효과적으로 실현하기 위해서는 무엇보다도 사용자와 경영진 모두 대학의 정보자산에 대한 가치와 중요성을 정확하게 인식하고 이를 위한 공동의 목표를 공유하는 것이 필요하다. 이에 대한 출발점으로서 정보자산을 체계적으로 분류와 그에 따른 정보보안 정책을 수립하는 것이 우선되어야 한다.

대학 본부와 경영진이 중심이 되어 대학 전체의 정보자산에 대한 보안 목적과 목표를 설정한 후, 그에 따라 정보자산을 적절하게 분류함으로써 대학의 광범위한 정보자산을 한정된 인력과 예산으로 효율적인 운용을 기대할 수 있다. 분류된 정보자산은 그 중요도와 절취 및 불법변경 시의 손실가치, 파괴 시 복구비용, 그리고 정보자산의 사용권자 등 다양한 기준에 따라 보안등급을 체계적으로 결정해야 한다. 또한 적절한 가이드라인과 통제 방안을 마련하여 전체 구성원과 공유하는 것이 필요하다.

최근에 많은 대학들이 자산분류체계 기준을 순자산 가치 관점에서 정보자산 가치 관점으로 바꾸고 있다. <표 7>은 실제 대학에서 정보자산을 유형별로 분류한 사례를 보여주며[16] 최근 많은 대학들이 정보보호 규정에 따라 대학 소유의 자산 중 보안이 필요한 정보자산에 대하여 구체적인 분류와 관리를 강화하고 있다. 이는 정보자산에 대한 가치를 학교 당국도 함께 공유하고 정보보안 정책수립에 필요한 지침을 제공하는 데 도움이 되고 있다.

표 15. 정보자산 분류 1
Table 15 Classification 1 of Information Assets

분야	유형	
정보자산	H/W	서버
		네트워크
		보안시스템
		PC & 주변기기
	S/W	
	Data	
	인적 자원	
	문서	
물리·환경적 자산		
활동자산		

또 다른 관점에서의 정보자산 분류는 <그림 2>와 같이 정보자산의 발생단계에서부터 그 가치가 소멸할 때까지 통제와 감독을 일관성 있게 유지하고자 분류하는 방법이다[17]. 이처럼 정보자산에 대한 분류체계 수립은 그동안 자율적이지만 비효율적으로 운영되면서 대학자원의 남용을 초래해 온 기존의 정보보안 정책에서 탈피할 수 있는 중요한 출발점이 된다.

그림 2. 정보자산 분류 2
Fig. 2. Classification 2 of Information Assets

정보보안에 필요한 구체적인 정책으로는 교육기관의 보안관제 체계를 위협관리시스템 및 보안정보관리시스템(SIMS: Security Information Management System)으로 확대해서 연동해야 하며, 침해공격에 대비한 종합관제 모듈을 개발하여 관제범위 및 관제대상 기관을 확대하여 침해사고를 미연에 완화시켜야 한다. 이를 바탕으로 정기적으로 정보보안 취약점에 대한 점검을 수행하여 재난복구시스템 및 통합인증 게이트웨이를 구축하여 전자서명에 대한 인증체계를 고도화 하여야 한다. 또한 대학 행정에 전자서명 인증서 도입을 의무화하는 한편 지속적인 보급과 정보보안 실무자를 위한 정기적인 교육과 정보보안지침 및 가이드북 제정을 통하여 교육기관의 정보보안 수준을 향상시키는 것이 필요하다[15].

2. 조직 설계 방안

일반적으로 한 조직에서 조직의 정보자산을 효과적으로 운용하면서 보안 정책을 조직 전체에 현실적으로 적용하기 위해서는 이를 위한 기본적인 경영관리의 틀과 경영진의 확고한 지원이 전제되어야 한다. 이러한 경영관리의 틀은 보통 전체 조직 구조를 설계하고, 설계된 각 조직부문에 알맞은 업무를 분장하여 책임과 권한 및 인력을 적절하게 분장함으로써 구현될 수 있는데, 이는 정보보안을 위한 통제는 이와 같이 구현된 경영관리의 틀 안에서 보다 효과적으로 운영될 수 있기 때문이다[17].

앞 장의 설문 결과에서 응답한 대학의 약 53%가 침해사고 예방과 대응을 위한 전담부서를 설치하여 운영하고 있는데, 이러한 전담부서는 <그림 3> (1)과 같이 대학의 정보화 부서에서 정보보안담당자를 지정하여 보안업무를 병행하여 수행하거나, <그림 3> (2)와 같이 정보부서 내에 정보보안팀을 별도로 구성하여 보안업무를 수행하는 경우도 있다. 후자가 개선된 형태의 조직으로서 대학의 정보부서 내에 정보보안 기능을 추가하여 운영하는 것이다. 그러나 그동안 단기적 성과평가 측면을 강조해 온 정보부서와 정보보호담당자 또는 책임자로 하여금 정보보안 정책을 수립하고 업무 수행을 추가하면 정보보안 정책의 궁극적인 목표를 달성하는데 어려움과 갈등 발생이 예상된다.

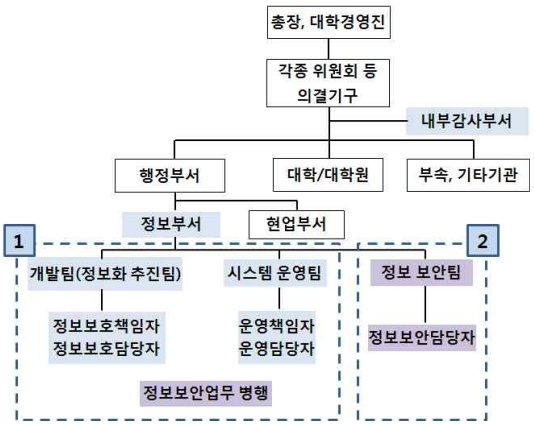

그림 3. 현행 조직: (1) 기존 정보부서에서 보안업무 병행, (2) 기존 정보부서 내 신규부서로 설치 운영
Fig. 3. Current Organization: (1) Parallel Jobs of Information Security Duties in Current Information Dept. and (2) New Information Security Team in Current Information Dept.

따라서 대학의 정보보안 목표를 달성하고 보안 정책을 원활히 수행하기 위해서는 <그림 4>와 같이 정보보안 조직을 독립적으로 설계하여 운영하는 것이 필요하다. 이 방식에서는 독립적인 정보보안 부서 운영뿐 만아니라 정보보안 심의위원회 구성 및 내부감사 부서에서의 정보보안 정책에 대한 감사를 수행하도록 한다. 이는 정보보안부서와 현업부서 또는 정보보안부서와 정보부서 간의 책임과 권한이 균형 있게 분할되어 상호 견제가 가능하도록 한 것이며, 적절한 통제가 이루어질 때 비로소 조직 전체의 정보보안 정책이 효과적으로 구현되게 될 수 있다고 판단되기 때문이다.

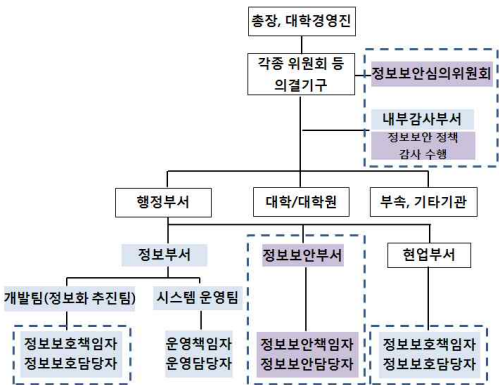

그림 4. 정보보안을 위한 조직 설계 제안
Fig. 4. Suggestion of Information Security Organization

<표 16>은 현재의 조직과 제안하는 조직에서 서로의 장단점을 간단히 비교하였다.

표 16. 조직 설계의 장단점 비교
Table 16 Strength and Weakness of Each Organization

항 목	현행 조직	제안 조직
장 점	기존 조직 및 인력 활용에 따른 비용 감소	정보보안 목표 달성 가능성 높음
단 점	정보보안 목표 달성 가능성 낮음	전문 인력 확보에 따른 비용 증가

3. 역할 및 책임 배분

대학 조직과 인적 부문으로 나누어 정보보안 역할 및 책임을 살펴보고자 한다.

3.1 부서별 역할과 책임

먼저 대학 조직 부문별 정보보안 역할과 책임을 나누기 위해서는 무엇보다도 대학 조직과 구성원 전체를 하나로 통합하여 관리할 수 있는 총괄 기구가 마련되어야 하며, 이를 바탕으로 <그림 4>에서 제안한 것과 같이 정보보안심의위원회(가칭), 정보보안부서, 현업부서, 정보부서로 구분하여 각각의 역할과 책임을 <표 17>과 같이 부여한다.

3.2 인적자원 간 역할과 책임

본 논문에서는 대학 경영진, 행정부서의 일반직원, 정보보안 담당자 및 책임자, 운영자·정보보호 담당자 및 책임자로* 나누어 정보보안을 위한 역할과 책임을 <표 18>과 같이 부여한다.

* 대학 실태조사 표본 대학 중 2개 대학의 업무분장 사례를 참조함

표 17. 각 조직의 역할 및 책임
Table 17 Roles and Responsibilities of Each Organization

조 직	역할 및 책임
정보보안심의 위원회	- 대학의 정보보안 관련 제반업무 총괄 - 침해사고 처리에 대한 책임 및 심의·결정 - 대학 정보자산에 대한 불법적 침해 행위에 대한 처벌 등의 심의·결정 - 정보보안 교육 및 정보보안 사항 등의 이행 여부 점검 및 감사
정보보안부서	- 정보보안의 구체적인 목표 및 정책 수립 - 정보보안 기준 및 가이드라인 제시 - 주기적인 점검을 통한 정보보안 목표 및 정책 타당성 점토 - 구성원 교육, 정보보안 관련 타부서 지원 - 내부 감사부서와 연계한 대학 정보자산에 대한 보안통제 실시 - 침해사고 사전예방 및 처리 절차 수립/수행 - 보안점검 수시 실시
현업 부서	- 정보 분류체계에 따른 부서 내 정보자산 식별, 분류 - 정보보안 기준 및 가이드라인에 따른 각 부서 업무 기획·추진, 통제 및 보안 수행
정보 부서	- 대학 정보시스템 개발, 운영 및 관리 - 현업부서에 다양한 정보서비스 제공 - 정보보안부서와 협조하여 정보시스템, 네트워크, 서버, PC, 응용프로그램, DB 등의 보안점검 수행 - 정보시스템 또는 정보통신망 이용자 관리

대학의 정보자산에 대한 보안 목표와 원칙을 수립하기 위해서는 대학 경영진의 의지 표명이 가장 중요한데, 이는 대학의 정보보안 정책 추진에 있어서 실제적인 원동력이 되기 때문이다. 또한 현업에서 업무를 수행하는 일반직원은 조직 내에서 정보자산의 발생자이며 관련된 정보자산의 보안을 위해 정보자산에 대한 통제 기능을 일부 수행하는 역할자이기도 하다[18]. 최근 많은 대학에서는 정보보호 담당자가 대학의 보안 기능까지 담당하고 있지만, 본 논문에서는 이전의 정보보호 담당자의 이와 같은 역할 중 보안 기능은 정보보안 담당자에게로 이관하고, 현업부서의 일반직원 중 일부를 정보보호 담당자로 임명하여 정보부서의 업무 중 현업부서와 공유 가능한 업무의 일부를 분담하도록 하는 것을 제안한다.

4. 인적자원 관리

앞에서 언급한 것과 같이 정보보안의 궁극적인 목표는 정보자산에 대한 파괴, 절취, 변조, 유출 등과 같은 다양한 위협으로 부터 정보자산을 보호하여 조직의 손실을 최소화하고 이익을 최대화하는데 있다. 따라서 한 조직에서 인적자원

의 부적절한 관리는 조직 전체에 막대한 손실을 초래하는 원인이 될 수 있기 때문에 정보보안의 궁극적인 목표를 달성하기 위해서는 직원의 채용에서 배치 및 고용 종료에 이르기까지 정보보안을 위한 책임과 역할을 지속적으로 관리해야 한다.

직원의 신규채용 단계에서는 수습기간 동안 대상 직원이 해당직무에 적합한지에 대한 검증이 필수적으로 선행되어야 하며, 신규배치 또는 재배치 후에는 분장된 업무 수행에 있어서 대학의 정보보안 정책과 지침을 철저하게 준수하도록 유도해야만 한다. 또한 필요한 경우에 대학 경영진은 업무를 분리해서 특정 정보자산에 대한 직원의 접근권한과 사용권한을 서로 배타적으로 관리할 수 있게 하며[17], 이는 의도적이든 비의도적이든 내부자에 의해 발생할 수 있는 모든 위협으로부터 정보자산을 보호하기 위한 것이다.

표 18. 인적 자원간 역할 및 책임
Table 18 Roles and Responsibilities of Each Personal Groups

구 분	역할 및 책임
대학경영진	- 대학 정보자산의 보안 목표, 원칙 수립을 위한 강한 의지 표명 - 정보보안 현안에 대한 이해 및 보안 정책 수립과정에의 적극적인 참여
일반 직원	- 자신이 보유한 정보자산에 대한 일부 통제 기능 수행, 정보자산의 중요도에 따른 식별 - 정보자산 분류, 정보보안 가이드라인/지침에 따른 업무 수행 - 현업에서의 침해사고 발생 관찰 및 보고 - 정보보안 교육 참여, 내부 보안감사 협조
정보보안담당자 및 책임자	- 종합적인 보안계획 및 가이드라인 수립 - 주기적인 보안점검 실시, 침해사고 사전예방 및 침해사고 발생 시 대응 - 보안점검에 필요한 자료 및 제반 사항을 현업부서에 요구, 그에 따른 시정여부 확인 - 현행 보안정책의 타당성 및 효율성 평가 - 구성원 보안교육 실시
운영자, 정보보호담당자 및 책임자	- 정보부서 정보통신망에 대한 사용자 접근 통제, 시스템/서버 등 대학 전체 인프라 시설의 도입, 운영, 평가 - 침해사고 발생 시 정보보안담당자와 협조하여 복구 수행 - 각종 소프트웨어 관리, 시스템프로그램이나 응용프로그램 등에 접근하여 인가된 수정과 백업 작업 수행, 대학 홈페이지 구축 운영, 현업부서의 지원요구에 대한 서비스 제공

정보보안정책이나 절차를 의도적으로 위반하여 정보자산에 대한 불법적인 행위를 한 내부자에 대해서는 정보보안 관련 규정이나 학칙에서 그에 상응한 처벌을 가할 수 있도록 명시함으로써 정보보안을 위한 대학 구성원들이 경각심을 갖도록 해야 한다.

또한 정보자산에 대한 보안인식을 높이고 보안 정책을 효과적으로 수행하기 위해서는 정보보안 교육과 훈련이 정기적으로 실시되어야 한다. 이러한 정보보안 교육 및 훈련에는 반드시 대학 경영진들도 함께 참여해야 하며, 이는 정보자산에 대한 경영진들의 보안 책임감을 한층 강화시킴으로써 향후 정책 시행에 보다 적극적으로 대처하도록 하기 위함이다. 따라서 향후 대학에서의 정보보안 교육은 보안에 대한 인식을 제고하고, 각종 침해사고로부터 정보자산의 손실을 최소화할 수 있도록 대상별, 주제별로 차별화된 보안 교육을 주기적으로, 필요에 따라 수시로 실시할 수 있어야 한다.

V. 결론 및 제언

본 논문은 사이버공격에 의한 대학의 침해사고 발생 현황 및 침해사고에 대비한 각 대학의 대응 노력과 실태를 조사하였으며 그 결과를 기업과 비교하였다. 이를 바탕으로 사이버공격에 의한 침해사고에 대비하여 향후 대학이 모색해야 할 정보보안 대응 방안을 제시하고자 하였다.

대학의 정보보안 실태를 조사한 결과 보안 수준이 비교적 높았으며, 자교의 보안시스템에 대한 보안담당자들의 강한 자신감도 볼 수 있었다. 그러나 잘 구축된 보안 인프라에도 불구하고, 보안정책을 준수하지 않는 사용자와 경영진의 인식부족, 보안운용 전담조직의 미비 및 전문 인력 부족 등은 여전히 대학이 개선해야 할 점으로 파악되었다.

본 논문에서 제안한 정보보안 원칙들은 가장 일반적이면서도 본질적인 것들로서 침해사고로부터 대학의 정보자산을 보호하는 최우선 방법은 사전예방이며, 대학 경영진은 대학의 궁극적인 정보보안 목표를 중심으로 통합보안 관리 정책을 수립하고, 표준 지침이 될 수 있는 가이드라인을 구성원에게 제시하는 등 제도적 지원을 강화해야 한다. 또한, 내부 구성원에 대한 정기적인 교육과 훈련을 실시하고, 처벌규정 등의 제도적 장치를 마련하여 적극 홍보함으로써 사이버 공간에서의 침해사고에 대한 위험성을 구성원에게 인지시키고, 정보자산의 중요성과 보안의 필요성을 공유하도록 하는 것이 필요하다. 이와 함께 정보보안 전문 인력의 충원과 양성, 보안 전담부서의 설치 등에 과감한 투자가 필요한데, 이는 향후 글로벌화된 교육시장에서 경쟁력을 높이기 위한 중요한 요소가 될 것이다.

끝으로 대학이 침해사고 등으로부터 정보자산을 보호하고 차세대 정보화 시대에 부응하는 새로운 개념의 정보화된 캠퍼스로 거듭나기 위해서는 대학 간의 긴밀한 네트워크 형성과 공동의 협력방안도 함께 모색되어야 한다.

참고 문헌

[1] S. J. Shin, D. H. Ryu, J. H. Na, S. W. Kim, "Information Risk Management", Intervision, 2004.

[2] S. O. Kang, "Informatization Status of 58 Universities in Korea", Datanet, October, 2005.

[3] K. K. Kim, H. K. Shin, S. S. Park, B. S. Kim, "Study on Influences of Information Asset Protection Outcomes to Organization Outcomes: Focusing on Management Activities and Statistical Activities", Information Management Studies, Vol. 40, No. 3, pp. 61-77, 2009.

[4] Korea Information Security Agency, "2010 Status and Actions of Information System Hacking and Virus", KISA-RP-2010-0051, 2010.

[5] Computer Emergency Response Team, "Monthly Magazine: Trends and Analysis of Security Incidents", 2009.

[6] H. Y. Kim, C. S. Park, "Security Issues & Issues: Response Procedures of Security Incidents", AhnLab, 2007.

[7] Korea Information Security Agency, "Guidelines to Responses and Recovery of Security Incidents", 2007.

[8] K. H. Sung, "Numerous Damages Happen to Enterprise Information Systems By Hacking Attacks From China", Money Today, June, 2008. (http://news.mt.co.kr)

[9] H. S. Oh, "Numerous Stops in Businesses by Cyber Attacks even in Blue House, National Defense Ministry and Government Agencies", Data Net, July, 2009.

[10] Y. J. Lee, "Rapid Increase of Site Security Accidents: Preparing Government and Non-Government Emergency Actions", Digital Daily (http://www.ddaily.co.kr), August, 2007.

[11] J. T. Seo, M. H. Lee, J. S. Choi, K. H. Han, H. S. Hwang, et al, "Cases of Various Cyber Intrusion Incidents", National Cyber Security Center, April, 2007.

[12] Ministry of Public Administration and Security, "2011 National Information White Paper", 2011.

[13] Korea Information Security Agency, "2008 Investigation of Information Security - Enterprise", 2008.

[14] Network Times, "2009 Information Security AI Guide V.4", pp. 34-42, 2009.

[15] Ministry of Education, Science and Technology, "2010 Directions of Information Security", 2010.

[16] Pohang University of Science and Technology, "Regulations of Information Security", 2008.

[17] Korea Institute of Information Security & Cryptology, "Information Security Managements and Policies", Korea Information Security Agency, 2002.

[18] S. Y. Lee, "Responsibilities of Enterprise Information Security Managers", Information Security 21c, Vol. 85, September, 2007.

저 자 소 개

강 영 선

1994 : 강릉대학교 전자계산학과(학사)
2010: 숙명여자대학교 교육대학원 전산교육전공 졸업(석사)
1996~현재 : 고려대학교 교직원
관심분야 : 정보보호, 사이버 보안 등
E-mail : kys1005@korea.ac.kr

최 영 우

1985 : 연세대학교 전자공학과(학사)
1994 : University of Southern California 컴퓨터공학(공학박사)
1997 ~현재 : 숙명여자대학교 컴퓨터과학과 교수
관심분야 : 영상처리, 패턴인식, 정보시스템 구축 등
E-mail : ywchoi@sookmyung.ac.kr