韓國IT서비스學會誌
第7卷 第1號
2008年 3月

학내 정보보호지침 수립에 관한 연구*

유기훈** · 최웅철** · 김신곤*** · 구천열****

A Study on Establishing Guidelines for Information Protection and Security for Educational Institutes*

KiHun Yu** · WoongChul Choi** · ShinKon Kim*** · ChunYul Goo****

■ Abstract ■

Because IT security guidelines for universities and colleges mostly focus on hardware aspects, the problems such as security incidents by a user's mistake and personal information leakage by hacking are serious in our higher educational institutes. In order to solve these information protection and security problems in the educational institutes, realizable and implementable information protection and security guidelines which will contribute to escalate information protection level should be established and at the same time, specific guidelines should be provided to make the guidelines efficient. In this paper, the information security problems and cases are categorized to develop information security guidelines for the higher educational institutes in terms of short, mid, and long term aspects and the solutions to the problems are sought. In addition, a serious of approaches to the information security are proposed such as the improvement measures for the employees of the institute to have desirable security-minded, security problem prevention and resolving methods, developing conflict coordination procedure and law and regulation system establishment for making the educational institutes be information-oriented.

Keyword : Information Protection, Security, Guideline, Educational Institute

* 이 논문은 2008년도 광운대학교 교내 학술연구비 지원 및 2005년도 한국교육전산망 연구과제 수행에 의해 연구되었음.
** 광운대학교 컴퓨터과학과
*** 광운대학교 경영정보학과
**** 교육인적자원부 전산사무관

1. 서 론

정보보호지침은 조직의 정보보호에 관한 목표와 방향을 제시하기 위한 선언으로 체계적이고 효과적인 정보보호를 시작하는 출발점이 된다. 또한 정보보호지침은 조직의 운영목표를 반영하고 지원하기 위한 것이다. 그러나 정보보호 지침이 조직의 이익이나 정보보호 목적만을 지나치게 강조하여 개인의 사생활을 침해하거나, 비윤리적인 강제를 요구하거나 또는 국내/국제법 또는 외국의 법이 적용될 경우 이를 위반해서는 안 된다. 즉, 정보보호지침은 보편타당해야 하고, 윤리적이며 사회적 법 또는 규정과 부합해야 한다[6].

조직이나 국가에서 추진하는 정보보호와 개인의 권리가 서로 충돌하는 경우가 있을 수 있다. 이러한 문제를 해결하고 정보를 적절히 보호하기 위해 고려해야 할 기본적인 요건들을 추출하기 위하여 국제적으로 다양한 노력이 이루어졌으며, OECD (Organization for Economic Co-operation and Development)의 정보보호 가이드라인, NIST(National Institute of Standard and Technology)의 컴퓨터 보안 원칙, GASSPC(Generally Accepted Systems Security Principles Committee)의 일반적으로 받아들여지는 정보보호 원칙 등이 제시되었다[7].

정보보호의 원칙은 새로운 정보시스템을 도입하거나, 운영 또는 관리계획을 수립하거나, 지침의 개발 등 정보보호를 새롭게 설계할 경우에 필요하다. 정보보호의 원칙은 이러한 경우에서의 보편타당한 지침을 제공하기 위하여 만들어 졌다. 그러나 특정한 문제에 해답을 위하여 만들어진 것은 아니다. 즉, 정보보호 원칙은 전반적인 사항에 일반적으로 적용가능하고 종합적이며 합리적인 정보보호를 위해 고려해야 할 사항을 제시한 것이다. 또한 정보보호에 대한 모든 원칙이 반드시 준수되어야 한다는 강제가 있는 것은 아니다. 하지만 이러한 원칙에서 벗어난 경우, 당면한 목적은 달성할 수 있더라도 더 거시적이고 장기적인 관점에서 문제가 발생할 수 있다[8, 9].

이에 본 논문에서는 학내 정보보호지침을 관리적, 물리적, 기술적 보안과 시스템 정보보안으로 세분화하여 정보보호 원칙에 기반한 구체적인 정보보호지침을 제안한다. 이후 본 논문의 구성은 다음과 같다. 제 2장에서는 위에서 언급한 OECD, NIST, GASSPC 에서 선정한 정보보호 기본원칙들을 소개하고, 정보보호 지침 개발 과정에서 고려해야 할 원칙들을 설명한다. 제 3장에서는 지침의 개발과정, 분류기준과 논문에서 제시하는 지침을 설명한다. 그리고 제 4장에서 결론을 맺는다.

2. 관련 원칙

2.1 OECD 정보보호 가이드라인(guideline)[2]

OECD에서 1992년에 개발한 정보보호에 대한 가

〈표 1-1〉 2004년 공공기관별 해킹 피해 현황[5]

구 분	2003년도	2004년도												총 계	비 율
		1	2	3	4	5	6	7	8	9	10	11	12		
국가기관	10	4	5	19	92	128	109	97	65	63	63	67	86	798	20%
지자체	75	7	7	4	36	58	79	70	61	80	82	120	97	701	18%
연구소	7	2	7	33	44	19	14	6	5	6	5	3	11	155	4%
교육기관	1,177	63	41	56	73	160	160	168	155	146	134	104	277	1,537	39%
산하기관	37	3	1	7	25	52	53	59	55	50	66	91	96	558	14%
기타	17	0	1	17	35	38	30	14	6	13	12	20	35	221	5%
합계	1,323	79	62	136	305	455	455	414	347	358	362	405	602	3,970	100%

이드라인(Guidelines for the Security of Information System)은 다음과 같은 사항을 목적으로 제정되었다.

- 정보시스템과 관련한 이들에게 정보보호 문화 촉진
- 정보시스템과 네트워크의 위험에 대한 인식 재고 및 신뢰성 확보
- 정보보호 운영조직 수립 및 정보시스템과 네트워크를 보호하기 위한 일관된 지침/업무/수단/절차를 개발하고 이행하는 과정에서 윤리적 가치 존중
- 정보보호 참여자간의 협력과 정보공유 촉진
- 표준 개발에 있어서 정보보호 관련 사항을 고려하도록 촉구

OECD에서 개발한 정보보호 가이드라인의 정보보호 원칙은 다음 <표 2-1>과 같이 9가지 사항의 원칙으로 정의되어 있다.

2.2 GASSPC의 일반적으로 받아들여지는 정보보호 원칙[3]

GASSP(Generally Accepted Systems Security Principles)는 1992년 미국, 영국, 독일 등을 포함한 8개국이 모여 구성한 GASSPC에서 제정한 보안 원칙으로 OECD의 '정보시스템 보안을 위한 가이드라인'에 기초를 두고 있다.

GASSP의 보안 원칙은 "보편적 원칙", "광범위한 기능적 원칙", "상세 원칙"의 3단계 계층으로 구성되어있으며 각 계층의 주요 내용은 다음과 같다.

- 보편적 원칙(Pervasive Principle)은 거의 변하지 않는 기본적인 원칙으로써 원칙의 수가 적다.
- 기능적 원칙(Broad Functional Principles)은 보편적 원칙에 종속되며 다음 단계인 상세원칙 개발의 지침을 제공 한다. 이 원칙은 기술이나 기타 영향을 미치는 요소의 중요한 변경 시에 반영되며 더 구체적이다.
- 상세 원칙(Detailed Security Principle)은 광범위한 기능적 원칙에 종속되며 기술이나 기타 영향 요소의 변경에 따라 수시로 변경될 수 있다. 상세원칙은 업무의 특수성과 특별한 보안사고 등의 문제에 따라 상황에 따라 중요성이변동할 수 있다.

3단계의 계층으로 구성된 GASSP의 정보보호

〈표 2-1〉 OECD 정보보호 가이드라인

원 칙	설 명
1. 책임성 (Accountability)	정보 시스템의 소유자, 공급자, 사용자 및 기타 관련자들의 의무와 책임이 명확해야 한다.
2. 인식 (Awareness)	소유자, 사용자 그리고 그 밖의 관련자들은 기존의 보안에 대한 적절한 지식을 습득할 수 있어야 한다.
3. 윤리성(Ethics)	정보 시스템과 정보 시스템의 보호는 모든 사람의 권리를 기본적으로 존중하여야 한다.
4. 다분야 간 협력 (Multidisciplinary)	정보시스템의 보안을 위한 대책, 실행, 절차 등에 있어서 모든 관련된 분야를 고려하여야 한다.
5. 균형 (Proportiionality)	보호 수준, 비용, 대책, 실행수간 절차 등은 정보시스템에 의존하여 가치와 잠재적인 손해의 심각성 및 발생가능성등에 적합하고 균형 있게 이루어져야 한다.
6. 통합성 (Intergation)	정보시스템 보안을 위한 대책, 실무, 절차는 보안의 일관성과 통합성을 위하여 서로 조화를 이루어야 하며 조직의 다른 대책, 실무, 절차를 포함하여 설계되어야 한다.
7. 적시성 (Timeliness)	국가적, 국제적 차원에서 공공 부문과 민간 부문은 정보시스템 침해사고를 사전에 방지하고 대응할 수 있도록 적절히 협조하여 대처하여야 한다.
8. 재평가 (Reassessment)	정보시스템 보안은 주기적으로 재평가 되어야 하고, 변화하는 보안 요구사항에 맞추어 개선되어야 한다.
9. 민주성 (Democracy)	정보시스템 보안은 정보 및 데이터의 흐름과 사용에 대한 민주적 법, 규정에 부합하여야 한다.

원칙의 내용은 <표 2-2>와 같다.

〈표 2-2〉 GASSP 정보보호 원칙

원 칙	설 명
보편성 원칙 (Pervasive Principles)	1. 책임추적성의 원칙(Accountability Principle) 2. 인식의 원칙(Awareness Principle) 3. 윤리원칙(Ethics Principle) 4. 다분야간 협력의 원칙 (Multidisciplinary Principle) 5. 균형의 원칙(Proportionality Principle) 6. 통합성의 원칙(Integrated Principle) 7. 적시성의 원칙(Timeliness Principle) 8. 재평가의 원칙(Reassessment Principle) 9. 공정성의 원칙(Equity Principle))
기능성 원칙 (Broad Functional Principles)	1. 정보보호 지침(Policy) 2. 보안 의식(Awareness) 3. 책임추적성(Accountability) 4. 정보관리(Infomation Management) 5. 환경 관리(Environment Management) 6. 인력의 자격(Qualifications) 7. 무결성(Integrity) 8. 정보시스템 생명주기(Life cycle) 9. 접근통제(Access Control) 10. 업무연속성 계획(Contingency Planning) 11. 위험관리(Risk Management) 12. 네트워크와 기반구조 보호(Infrastructure Security) 13. 정보보호의 법률, 규제 및 계약상 유구사항(Legal, Regulatory, Contractual)
상세원칙 (Detailed Security Principle)	1. 알 필요(Need to Know) 원칙 2. 갈 필요(Need to Go) 원칙 3. 할 필요(Need to Do) 원칙 4. 최소권한의 원칙(Least Privilege Principle) 5. 직무분리의 원칙(Separation of Duty) 6. 직무 순환 원칙(Rotation of Duty) 7. 2인조 근무의 원칙(Two-man Principle)

2.3 NIST의 컴퓨터 보안 원칙[4]

NIST의 컴퓨터 보안 원칙은 미국상무부 기술관리국 산하의 각종 표준과 관련된 기술을 담당하는 연구소에서 만들어졌으며 주요 내용은 다음 <표 2-3>과 같이 8가지로 구성되어 있다.

〈표 2-3〉 NIST 컴퓨터 보안 원칙

원 칙	설 명
1. 경영목표의 지원	컴퓨터 보안은 조직의 경영목표를 지원해야 한다.
2. 조직 관리를 위한 필수요소	컴퓨터 보안은 건건한 조직 관리를 위한 필수 요소이다.
3. 비용대비 효과	컴퓨터 보안은 비용대비 효과가 고려되어야 한다.
4. 명백한 책임 소재	컴퓨터 보안에 대한 책임과 책임 소재가 분명해야 한다(Computer security responsibilities and accountability should be made explicit) ※책임(Accountability) : 일반적으로 기술적인 측면에서는 책임추적성으로 번역하나 responsibility는 해야 할 사항의 측면에서 책임을 의미하고 accountability는 그 책임을 다하지 못했을 때 처벌을 받는다는 측면에서의 책임을 의미한다.
5. 보안책임의 범위	시스템 소유자들은 그들의 조직 외부에 대해서 보안 책임을 갖는다.
6. 포괄적이고 통합적인 접근	컴퓨터 보안은 포괄적이고 통합된 접근방법을 필요로 한다.
7. 정기적인 재평가	컴퓨터 보안은 정기적으로 재평가 되어야 한다.
8. 사회적 요인에 의한 제약	컴퓨터 보안은 사회적인 요인에 의해 제약된다.

정보보호 지침을 개발하는 과정에서는 지금까지 설명한 정보보호 원칙들을 고려하여 개발된 지침이 일반적인 정보보호 원칙을 반영하고 있는지, 이러한 원칙들을 위배하고 있지는 않는지 고려해야 한다. 그러나 이러한 고려는 별도의 절차를 거쳐는 것 보다는 지침 수립 과정에서 항시 염두에 두어야 할 사항이다.

각 단체가 발표한 정보보호 원칙은 일부 세부사항의 차이는 있지만 유사한 내용으로 구성되어 있다. 이들은 일반적이고 보편타당하게 받아들여질 수 있는 요소들이지만 정보보호라는 눈앞의 목표에 집중하다 보면 간과될 수도 있는 것들이므로 강조되는 것이라고 볼 수 있다.

본 논문에서는 위에서 소개한 OECD, GASSP, NIST의 원칙의 공통핵심요소를 개인적 측면, 사회적 측면, 법률적인 측면에서 구분하여 다음<표 2-4>와 같이 정리하였다.

〈표 2-4〉 정보보호 원칙의 핵심 요소 구분

구 분	설 명
개인적 측면	개인의 프라이버시(사생활)가 침해되지 말아야 하며, 정보보호의 목적을 달성하기 위하여 IT부서 또는 정보보호 담당자의 편의 중심으로 개발되지 않아야 한다.
사회적 측면	도덕적 판단기준, 사회적 측면에서 일반적으로 보편타당 하여야 한다.
법률적인 측면	다른 사람의 법적인 권리를 보장할 수 있는 바탕에서 개발되어야 하며, 정보보호의 법률 및 규제 등의 요구사항이 반영되어야 한다.

정보보호 원칙을 적절히 반영하여 개발된 정보보호 지침은 사회적으로 보편타당하며 도덕적 판단기준에 적합하고, 개인의 목적과 조직의 목표가 조화를 이루며, 정보보호 관련 법률 및 규정을 준수할 수 있는 지침이 될 수 있다.

3. 정보보호 지침서의 구성

지침서의 구성은 관리/물리/기술적 영역으로 구분하거나 정보보호 관리체계 인증심사 기준의 통제대책 영역을 기본으로 조직의 환경 및 요구사항에 따라 구성할 수 있다. 또는 관리/물리/기술의 영역적 구분을 대분류로 하고 관리체계 인증의 통제 분야를 중분류로 하여 하위에 세부 분야별 또는 대상별로 지침을 구성할 수 있다. 이와 같은 관리적, 물리적, 기술적 영역에 따른 분류 이외에도 정보보호 관리체계 인증심사 기준(정보통신부고시 제2002-22호)의 제 1장 총칙 제 2조(용어의 정의)에서는 통제사항을 “조직적 및 관리적 통제”와 “운영적 및 기술적 통제”로 정의하고 있다[1].

이러한 정보보호 지침의 구성 체계에 대해서는 특별하게 정해진 것은 없다. 직원들이 쉽게 지침의 내용을 인식하고 관련 문서를 찾아보거나 참조하기 쉬운 형태가 되면 된다. 자체적인 문서 체계를 구성하기 어려운 경우에는 유사한 환경에서 운영되고 있는 정보보호 지침 문서 체계나 기타 선진사례(Best practices)를 참조하여 사용할 수 있다. 이 연구에서는 <표 3-1>와 같은 분류체계를 따랐다.

〈표 3-1〉 정보보호 지침 문서 체계

3.1 관리적 보안	3.2 물리적 보안
(1) 최상위정보보호 지침 (2) 정보보호 조직체계 지침 (3) 정보자산 분류 및 취급 지침 (4) 정보보호 교육 및 훈련 지침 (5) 인적보안 지침 (6) 개인 정보 보호 지침	(1) 물리적 보안 지침
3.3 기술적 보안	3.4 시스템 정보보안
(1) 시스템 개발 보안 지침 (2) 암호통제 지침 (3) 접근통제 지침 (4) 전자문서 교환 지침 (5) 보안사고 관리 지침	(1) 전자우편 지침 (2) 이동 컴퓨터 보안 지침 (3) 네트워크 보안 지침 (4) 침입차단 시스템 지침

3.1 관리적 보안

3.1.1 최상위 정보보호 지침

조직의 환경과 특성을 반영하는 정보보호 지침의 목적과 본 지침에 적용을 받는 범위를 선언한다. 그리고 지침의 준수 및 관련된 법 규정의 준수의무와 정보보호에 대한 역할과 책임을 선언한다.

최상위 정보보호 지침은 학내의 정보보호를 위한 지침으로, 학내업무와 관련된 모든 정보와 정보자산을 허가되지 않은 공개, 변조, 유출, 파괴 등의 위협으로부터 안전하게 보호하기 위해 필요한 기본적인 사항을 기술하며, 이를 통하여 학내의 정보자산이 의도적이거나 비의도적인 위협으로부터 안전하게 보호하는 것을 목적으로 하며, 본 지침의 적용범위는 학내의 정보 및 정보시스템을 사용하는 모든 구성원과 학내업무와 관련한 회사의 출입자 및 근로 계약자 등 계약관계에 있는 모든 사람을 포함한다.

학내의 정보자산에 대한 정보보호의 실행은 본 정보보호 지침을 우선으로 하며, 지침에 명시되지 아니한 사항은 관련 관계규정에서 정하는 방법에 따른다. 또한 정보보호 관련 국내외의 법규나 정부의 지침은 본 정보보호 지침보다 우선하여 적용된다.

정보보호의 목표는 학내 업무의 연속성을 보장하고 보안 사고로 인한 손실 및 이미지의 훼손과 같은 피해를 최소화하는 것이다. 이를 위하여 모든 학내 구성원은 정보보호의 중요성을 인지하고 이를 준수해야 한다.

정보보호 지침의 유지 및 관리를 위해 다음이 요구된다.

- 학내의 정보보호 관련 규정은 정보보호위원회의 승인을 득한 후 인쇄물 형태나 학내의 게시판 등을 통하여 학내 구성원에게 공표해야 한다.
- 학내 구성원은 정보보호 관련 문서(지침, 지침, 절차 등)를 충분히 숙지하고 준수해야 한다.
- 정보보호 부서는 위험분석 및 평가를 실시하여 필요한 대책을 강구하고 정보보호 관련문서에 대하여 정기적으로 타당성을 검토하여 정보보호 관련 규정을 개정해야 한다.
- 정기적인 타당성 검토이외에 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발생, 정보보호 환경의 중대한 변화 등이 발생했을 경우에는 관련사항에 대하여 추가로 검토하여 개정해야 한다.
- 정보보호책임자는 학내구성원에 대해 정보보호 관련 규정에 따른 제반의무의 이행에 관한 기록을 유지해야 한다.

3.1.2 정보보호 조직체계 지침

정보보호 조직체계 지침은 정보보호 관리활동을 체계적이고 효과적으로 실행하기 위하여 조직의 특성에 적합한 정보보호 조직을 구성해야 하고, 조직 전반에 대한 정보보호 활동을 계획, 관리, 실행하는 정보보호 조직의 구성 체계와 정보보호 업무 담당자의 역할과 책임을 명확하게 정의해야 한다. 또한 정보보호 활동의 조정, 심의 및 승인을 담당하는 정보보호 위원회가 구성 체계에 포함되어야 한다.

정보보호 조직은 교육기관 내의 정보보호 관리업무를 체계적이고 효율적으로 수행하기 위하여 구성되어 운영 된다. 정보보호 조직은 독자적으로 업무의 수행이 가능해야 하고 정보보호 관련 업무를 총괄 하여 수행 한다. 또한 국가 정보보호 전문기관과 연계를 구축해야 한다.

이어서 정보보호과의 역할과 책임에 대하여 알아보겠다. 첫 번째로 교육인적자원부내 정보보호과의 역할과 책임은 다음과 같다.

- 개인 정보보호 및 정보통신보안 업무 총괄한다.
- 교육기관 정보보호를 위한 관리적, 기술적, 물리적 환경 구축 및 지원업무를 담당한다.
- 교육 사이버 안전센터를 구축 · 운영한다.

두 번째로 시도교육청 사이버침해사고 대응팀(CERT ; Computer Emergency Response Team)의 역할과 책임은 다음과 같다[10].

- 교육인적자원부의 보안업무 · 지침을 준수한다.
- 각 시 · 도교육청 및 산하기관(초중고 포함) 정보보호 규정 및 지침수립 하고, 시행한다.
- '종합보안상황실' 운영을 통해 관할 지역 내 침해사고에 대한 보안 업무를 지도하고 · 관리한다.
- 교육 사이버 안전센터와 연계하여 24시간 보안관제시스템 운영, 침해사고 징후, 감시, 온/오프라인 위협정보 수집 및 분석 등을 수행 한다.

세 번째로 대학 사이버침해사고 대응팀(CERT)의 역할과 책임은 다음과 같다.

- 교육인적자원부의 보안업무 · 지침을 준수한다.
- 기관별 정보보호 규정 및 지침을 수립한다.
- 교육 사이버 안전센터와 연계하여 24시간 보안

관제시스템 운영, 침해사고 징후, 감시, 온/오프라인 위협정보 수집 및 분석 등을 수행 한다.

마지막으로 단위기관(초중고, 직속기관)의 역할과 책임은 다음과 같다.

- 정보통신보안담당자 지정을 통하여 책임성 확보와 해당 CERT와 원활한 업무체계를 유지한다.
- 해당 CERT 보안지침・지침을 준수한다.

● 정보보호 위원회의 구성

정보보호 위원회를 구성하기 위해 다음을 기반으로 한다.

- 정보보호 위원회는 비 상설기구로 위원장, 심의위원, 간사 등 10명으로 구성되기도 하고, 정보보호와 관련한 전문적 지침의 수립, 조사, 계획수립 등의 중요한 활동에 도움을 받기 위하여 외부 전문가로 구성할 수도 있다.
- 정보보호 위원회는 정보보호 활동의 조정, 심의 및 승인을 담당하며, 정보보호 관련 의사결정을 지원해야 한다.
- 정보보호 조직외의 다른 모든 부서는 정보보호 관련 안건의 제의 및 보안 이슈에 대하여 정보보호부서와 상호협력 해야 한다.

3.1.3 자산분류 및 취급 지침

조직의 업무에 사용되는 정보자산의 현황을 파악하여 식별하고(목록을 유지), 정보자산별로 책임자를 지정해야 한다. 그리고 조직의 특성에 따라 정의된 보안등급과 중요도에 따라 적절한 보호수준이 유지되어야 한다.

정보자산의 조사를 위해서 학내의 모든 중요 정보자산은 그 현황이 파악되고 상위 수준의 명세를 작성해야 하며, 각 정보자산에 대한 담당자가 지정돼야 한다. 또한 해당 정보자산의 명세와 소유자의 지정은 정기적으로 재검토 되어야 하며, 정보자산의 분류와 관리는 다음과 같이 이루어진다.

- 정보자산은 해당 자산의 민감성과 중요성에 따라 분류되고 소유자가 지정되어야 한다.
- 정보자산의 분류는 해당 자산의 기밀성, 무결성, 가용성의 관점에서 침해되었을 경우 학내의 업무에 미치는 영향 및 민감도에 따라서 등급을 부여하여 관리해야 한다.
- 정보보호 관리자는 분류된 정보자산에 대하여 소유자, 관리자, 사용자를 확인하고, 적절한 통제 유지를 위해 책임 소재를 명확히 정의해야 한다.

정보자산이 조사되고 분류되고 나면 정보자산의 조사 및 분류에 따라 정보자산의 관리자, 소유자, 사용자는 다음의 역할과 책임을 준수해야 한다.

- 정보자산의 관리자(또는 소유자)는 정보의 비밀등급(보안등급)을 결정해야 하며 필요 시 정보보호를 위한 관리 요구사항을 명시하여 공지하고, 사용자의 접근권한을 승인하고 정기적으로 재검토해야 한다.
- 정보자산의 사용자는 해당 정보자산의 소유자 또는 정보보호 관리자로부터 해당 자산으로의 접근을 승인 받아야하며, 정보보호 요구사항에 따라 사용해야 한다.
- 정보보호 관리자는 정보자산의 관리자를 대신해 자산의 보안등급을 부여하고 정보보호 요구사항을 정의해야 한다.

3.1.4 정보보호 교육 및 훈련 지침

학내의 정보보호에 인식제고를 통한 모든 학내 구성원의 적극적인 참여 및 학내구성원이 준수해야 하는 관련한 정보보호 지침 및 지침, 그리고 실제 업무 중에 발생할 수 있는 실수 및 오용 등을 예방하기 위하여 종합적이고 주기적인 정보보호 교육 및 훈련을 실행하기 위해서 ‘정보보호과’의 ‘정보보호 대응팀’은 각 기관 구성원들의 정보보호에 대한 인식제고 및 실제 업무 중의 실수, 오용을 예방하기 위한 종합적인 정보보호 교육 및 훈련

계획을 수립한다. 이를 참고로 하여 각 기관의 정보보호책임자는 기관의 실정에 맞도록 교육 및 훈련 계획을 수립 시행해야 하고, 정보보호 교육의 효율성을 제고시키기 위하여 실정에 맞는 정보보호 교육관련 교재를 작성 활용해야 한다. 또한 해당 기관에서 수립된 정보보호 교육 및 훈련내용을 정보보호 위원회의 심의를 받아 교육 및 훈련 내용에 문제가 없는지 검토해야 한다.

이에 따른 교육 및 훈련은 교수, 임직원, 학생 등 대상자의 특성에 따라 구분하여 실시해야 하고, '정보보호지침'의 내용을 포함하며, 대상자가 담당하는 업무의 특성에 따른 정보보호관련 규정의 내용을 포함해야 한다. 또한 각 기관의 정보보호 책임자는 각 기관의 전체 구성원 및 외부 위탁업체 직원의 정보보호 생활화 및 인식제고를 위해 홈페이지의 전자게시판, 정기간행물 등을 이용하여 정보보호에 대한 지속적인 교육 및 홍보를 실시해야 한다.

또한 교육 및 홍보에 연계하여 각 기관의 정보보호책임자는 매년 그 해 실시한 정보보호 교육결과 보고서를 작성하여 '정보보호과'의 '정보보호대응팀'에 보고하여 지속적인 관리가 이루어지도록 해야 하고, 교육결과 및 교육결과 보고서를 보관 및 관리해야 한다.

인적 보안은 학내구성원 및 정보시스템에 접근하는 협력업체 등의 외부인으로부터 발생할 수 있는 침해사고를 예방하기 위하여 정보보호 책임의 준수, 비밀유지 및 적격심사 등의 내용을 담고 있으며, 첫 번째로 정보보호 책임의 준수는 다음과 같이 이루어진다.

- 전 임직원은 정보보호 지침 또는 관련 법규를 위반하거나 심각한 보안 사고를 일으킨 직원에 대해서는 정보보호위원회의 협의 및 승인을 받은 후 인사위원회에 상정하여 징계처리 하도록 해야 한다.

징계 대상자는 정보통신 보안사고 관련자, 고의 또는 중대한 과실로 자료를 변경, 훼손, 분실 또는 유출한 자, 개인정보의 유출, 기타 상업적 목적으로 정보를 유용한 자등에 해당될 때 이다.

- 정보보호 관리자는 학내의 전 임직원 및 외주업체 직원 등의 관련자에게 정기적인 정보보호 교육을 계획하고 실시해야 한다.
- 전 임직원 및 외주업체 직원 등의 관련자는 정보보호의 위협과 불안을 인식하고 일상 업무 중에 조직의 보안 지침을 지원 할 수 있도록 적절한 교육을 받아야 한다.

두 번째로 적격심사는 학내의 모든 임직원(계약직 및 임시직원 포함)의 채용 시에 신원확인 절차 등을 통하여 적격여부에 대하여 심사되어야 한다. (정보 시스템을 이용하는 모든 직원, 특히 재무정보나 고도의 기밀정보와 같이 민감한 정보를 처리하는 인원은 반드시 적성검사 이력서 및 점검 및 이수과목 및 경력 확인 등을 통한 신용 점검을 해야 한다) 심사위원에는 전문 지식을 가지고 있는 교수 혹은 전문가가 면접에 참여 하고, 현재 담당자가 있다면 면접에 참여해야 한다.

이어서 주요직무 담당자 관리는 다음과 같이 이루어진다.

- 인사이동을 포함하여 민감한 정보를 취급하거나 정보 시스템에 접근권한을 가지고 직무를 수행하는 담당자는 강화된 방법으로 적격심사가 수행되어야 한다. 적격 심사는 면접 과정을 반드시 거쳐야 하며, 다수의 전문 지식을 가지고 있는 교수 혹은 전문가들이 참여해야 한다.
- 담당자가 바뀌거나 인사이동으로 인한 업무의 변화가 있을 경우 인수인계 기간을 충분히 가지고 교육시켜야 한다. 정보 시스템 운영관리를 위한 교육 계획에는 각 직무 역할에서 필요로 하는 기술요건과 교육요건, 교육 수요 파악, 교육 시기와 빈도, 교육 실적 및 성과관리 방안 같은 사항들이 포함되어야 한다.

마지막으로 비밀유지 및 관리에 대해 기술하겠

다. 비밀유지의 방법은 학내의 중요 정보를 보호하기 위해 신규 직원의 채용 시 비밀 서약서에 서명하도록 하고, 퇴직 시에는 퇴직자 서약서에 서명을 받고 퇴직 절차에 따라 처리해야 한다. 전출자와 퇴직자의 처리는 다음과 같다.

- 전출자는 전 소속에서 재직 기간 동안 사용하였던 모든 자산, 시스템 사용권한, 산출물을 전 소속 부서장에게 반납해야 한다.
- 퇴직자는 근무 기간 동안 사용하였던 모든 자산, 시스템 사용권한, 산출물을 기관에 반납해야 한다.

또한 비밀관리를 위해서 외주업체 등의 제 3자와의 계약 시에는 비밀 누설 관련 사항을 포함한 비밀유지서약서를 징구해야 한다.

3.1.5 개인 정보 보호 지침

개인정보 보호를 위해서 첫 번째로 학내의 최고결정권자는 다음과 같은 사항을 결정하고 처리해야 한다.

- 업무의 중요도에 따라 개인정보 처리를 위한 위임 전결권자를 지정하여 개인정보의 유출 및 오남용을 예방해야 한다.
- 개인정보보호책임관을 지정 하여 운영해야 한다. 개인정보보호책임관은 다음과 같은 사항을 처리해야 한다.
  - 개인정보취급자의 개인정보 보호업무를 지도, 감독한다(개인정보취급자 및 의무 법 제11조 참조).
  - 개인정보 처리시스템의 사용자 권한설정 등 제반 보호 장치에 관한 사항을 확인, 감독한다.
  - 시스템 로그 파일 등 접속기록을 주기적으로 분석하고 오남용 사고를 예방한다.
  - 개인정보보호책임관은 위 임무수행 목적의 달성에 필요한 경우이외에는 개인정보에 접근하거나 직접 취급할 수 없도록 한다.
  - 기타 개인정보 보호를 위해 다음과 같은 사항을 조치해야 한다.
  - 변경되는 경우 개인정보에 관한 업무 인계인수를 확인하고 행한다.
  - 개인정보 보호업무의 수행과 관련하여 오류 및 부정행위가 발생하거나 예상될 경우 기관의 장에게 즉시 보고한다.

두 번째로 개인정보 처리시스템에 대한 다음의 조치사항을 따른다.

- 업무별 접근권한 설정 및 주기적인 비밀번호 변경이 이루어 져야한다.
- 입출력 및 수정 사항, 파일별, 담당자별 데이터 접근내역 등을 자동으로 기록하는 로그 파일의 생성, 이러한 로그파일은 개인정보 취급시의 책임을 명확히 할 목적이외에는 사용을 금지한다.
- 출력물에 대한 조치
  - 출력자료 등에 작업자, 면수 및 출력장비의 고유번호 등을 표시함으로써 개인정보의 유출, 오남용방지를 위해 시스템적으로 구현되도록 한다.

세 번째로 개인정보파일대장의 열람 장소를 지정 운영 한다. 운영 방법은 다음과 같다.

- 개인정보파일의 열람은 일정한 사무공간 안에서 이루어 져야 한다.
- 개인정보파일 대장 사본의 전부 또는 일부를 비치한다.
- 처리정보 열람업무에 종사하는 직원에 대한 교육을 실시한다. 교육은 열람, 정정 청구, 보호대책 및 권익구제 절차 등이 실시된다.

마지막으로 개인정보 침해신고는 신속하게 처리되어야 하며, 개인정보 침해신고의 처리절차는 민원사무처리 관계법령을 준용하고, 처리방법은 개인정보침해신고처리대장 서식에 의하여 침해신고를 접수, 처리한다.

3.2 물리적 보안

3.2.1 물리적 보안 지침

물리적 보안 지침의 핵심은 주요 정보시스템의 보호를 위한 통제구역을 설정한 후 적절한 물리적/환경적 통제를 적용하고 관리하는 것이며, 정보 유출에 대한 물리적 통제를 구현하는 것이다.

위에서 기술한 핵심사항에 따라 물리적 보안 대책을 세우려면, 물리적 정보 자산 및 관련 시설 분류는 학교에서 정보보호가 필요한 사항에 대해서는 관리를 위해 분류를 해야 하고, 보호 등급을 나누고 그 등급에 따라 관리해야 한다. 그리고 정보자산과 시설물의 분류 및 관리는 파일로 저장된 것을 출력한 문서, 라우터, 스위칭 장비, 서버 PC, 일반 PC, 방화벽 등을 물리적 정보 자산으로 분류하고, 특별한 보호가 필요한 시설, 장비, 정보시스템에 대해서는 별로도 관리자를 두어야 한다.

위와 같이 분류된 물리적 정보 자산에 대해 보호 등급에 해당하는 항목을 다음과 같이 구분한다.

- 1급 보호등급 자료
  - 직원/교수/학생 등의 개인 신상 정보를 출력한 문서가 여기에 속한다.
  - 학내 전산 시스템에 해당하는 서버 PC가 여기에 속한다. 이것은 특히 등록금 처리, 성적처리, 개인 정보를 관리하는 데이터베이스 등을 말한다.
- 2급 보호등급 자료
  - 교수가 관리하는 학생들의 성적을 출력한 문서가 여기에 속한다.
  - 학내 전산 시스템에서 네트워크 관리를 위해 사용되는 장비 중 라우터, 방화벽이 여기에 속한다.
- 3급 보호등급 자료
  - 학내 전산 시스템에서 네트워크 관리를 위해 사용되는 장비 중 스위칭 장비가 여기에 속한다.

위의 분류에 따른 관리는 다음과 같이 이루어진다.

- 1급 보호등급
  - 문서 관리에 있어서는 그것을 조회/열람할 수 있는 직책을 가진 사람만이 처리를 해야 하며, 다른 사람에게 위임해서는 안 된다.
- 2급 보호등급
  - 라우터와 방화벽은 전문 지식을 가지고 있는 네트워크 관리자가 관리를 해야 한다.
  - 다음에 설명하는 3.4.3 “네트워크 보안 지침”에 따라 관리자는 수시로 상태를 모니터링 해야 한다. 문제가 생겼을 경우 경보를 발생하는 시스템에서는 자리만을 지켜도 충분하다.
  - 라우터와 방화벽의 상태를 모니터링만 지원하는 경우 관리자는 적어도 3시간 주기마다 체크를 해주어야 한다.
  - 관리자 판단 하에 문제가 발생하면 3.3.5 “보안사고 관리 지침”에 따라 처리한다.
- 3급 보호등급
  - 스위칭 장비는 전문 지식을 가지고 있는 네트워크 관리자가 관리를 해야 한다.
  - 관리자 판단 하에 문제가 발생하면 다음에 설명하는 3.3.5 “보안사고 관리 지침”에 따라 처리한다.

이어서 사무실 보안은 문서의 관리, 컴퓨터의 관리로 나눌 수 있다. 첫 번째로 문서의 관리를 위해서는 다음이 요구된다.

- 사무실 내 정보의 무단 접근 및 손상의 위험을 줄이기 위하여 책상위에 보호등급이 정해져 있는 문서를 오랜 시간동안 방치하지 말아야 한다.
- 보호등급이 정해져 있는 문서는 이면지로도 사용하지 말아야 한다.
- 보호등급이 정해진 문서는 사용이 끝났으면 곧바로 파쇄 해야 한다.

두 번째로 컴퓨터의 관리를 위해서는 다음이 요구된다.

- 보호등급이 정해진 문서 정보가 컴퓨터에 표시된 화면을 띄워 놓고 장시간 이석하지 말아야 한다.
- 컴퓨터에 화면 보호 암호를 설정하고 시간을 5분 이하로 설정한다.

마지막으로 물리적 장비를 보호하기 위해서는 다음이 요구된다.

- 주요 시스템이 위치한 전산실 또는 서버 실 등에는 열, 연기 감지기 등의 방화시설이 설치되어야 한다.
- 고가의 장비가 있는 구역이거나 보호등급이 낮은 구역인 경우에는 사고를 방지하기 위하여 CCTV등의 보안 시설을 설치해야 한다.

3.3 기술적 보안

3.3.1 시스템 개발 보안 지침

정보시스템에 대한 원천적인 보안 강화를 위하여 정보시스템의 개발단계에서부터 보안을 고려하기 위한 요구사항의 정의, 해당 요구사항의 구현, 그리고 보안성이 가미되어 개발이 완료되어있는 어플리케이션의 보안수준 유지를 위한 변경관리에 관한 사항을 정의한다.

보안 요구사항의 정의는 다음과 같다.

- 새로운 어플리케이션을 개발하거나 기존의 어플리케이션을 업그레이드 할 경우 정보보호 관리자는 해당 어플리케이션이 처리하는 데이터의 중요도에 따른 보안 요구사항을 파악하여 적용되어야 할 보안기능을 결정해야 한다.
- 어플리케이션의 설계 시에는 반드시 사용자 인증에 대한 보안 요구사항을 정의해야 한다.
- 통신에 사용되는 중요한 메시지에 대해서는 무결성과 비밀성 보장을 위한 암호화의 여부를 결정해야 한다.
- 사용자 인증이나 메시지에 사용된 암호화 방식은 언제든지 모듈의 교체만으로 교환을 가능하게 하여 위험상황에 대비 한다.
- 정의된 요구사항은 개발 단계에 들어가기 전에 정보보호 관리자에 의해 검토 되어 적절한 수준의 보안요구 사항이 포함되어 있는지 체크한다.

보안 요구사항의 구현을 위해서는 다음이 요구된다.

- 정보보호 관리자는 어플리케이션의 개발 단계별로 정의된 보안 요구사항에 대한 개발요건이 정보보호 요구사항이 만족되어 개발되었는지 확인해야 한다.
- 어플리케이션의 개발자는 완료된 어플리케이션의 보안 요구사항이 사용목적에 맞게 적절히 포함 되었는지, 사용된 보안 모듈은 무엇인지, 취약점은 무엇인지를 파악하여 정보보호 담당자에게 보고해야 한다.

어플리케이션의 변경관리는 다음을 만족해야 한다.

- 운영중인 어플리케이션에 대한 수정은 지정된 담당자에 의해서만 수행되어야 한다.
- 운영중인 어플리케이션 및 소스 전산자료 관리자에 대한 모든 수정 및 변경은 기록되어 관리되어야 한다.
- 테스트 중이거나 개발 중인 프로그램의 관리는 운영 중인 프로그램과 분리된 영역에서 관리되어야 한다.

3.3.2 암호통제 지침

학내에서 사용되는 중요정보에 대한 기밀성을 유지하기 위해 암호통제를 적용해야 한다. 암호통제는 학내에서 사용하는 암호에 대한 지침과 암호의 사용 및 암/복호화에 사용되는 키 관리에 대하여 준수해야 할 사항을 기술한다.

암호지침에서 학내의 중요자료는 제 3자에게 노

출되거나 비인가된 자에 의해 변경되지 않도록 하기위해 암호설정을 해야 한다.

암호 설정을 하기 위해서는 다음을 점검해야한다.

- 사용자 ID와 연속으로 3자 이상 같지 않아야 한다.
- 사용자를 통해 알 수 있는 이름, 생일, 전화번호, 주소 등을 이용하여 암호를 설정하지 않아야 한다.
- 일반 사전에 등록된 단어는 사용을 피해야 한다.
- 동일한 비밀 번호를 여러 사람이 공유해서는 안 된다.
- 암호의 길이는 최소 문자와 숫자의 조합으로 8자 이상이어야 한다.
- 보호등급이 1급인 경우에는 반드시 특수문자(!, @, #, $, %, ^ 등)를 한 자 이상 사용하여 설정하도록 한다.
- 이전 암호는 재사용을 금지해야 한다.
- 암호는 문서로 남기지 않도록 해야 하며, 남겨야 할 필요성이 있는 경우 물리적으로 보안성이 있는 곳에 둘 수 있어야 한다.
- 암호 내용을 파일로 저장될 경우에는 암호화된 형태로 저장해야 한다.

● 암호 프로그램 사용

암호 프로그램의 사용을 위해서는 암호 프로그램의 선정과 키 관리가 필요하며, 사용법을 알아야한다.

첫 번째로 암호 프로그램의 선정은 공개로 제공하는 프로그램을 사용하지 말고, 책임 소지 문제와 프로그램의 업데이트를 위해 신뢰성 있는 프로그램을 선정해야 한다.

암호 프로그램의 선정 방법은 다음을 따른다.

- 사용하고자 하는 암호 프로그램을 만든 회사가 공신력이 있는 회사인지 확인해야 한다.
- 마스터키의 존재 여부 및 백도어의 존재 가능성 등을 검토해야 한다.
- 암호 프로그램에 국가 인증이 되어 있는지 확인해야 한다.

두 번째로 키 관리 방법은 다음을 따른다.

- 암호 키의 생성은 담당 사용자가 하는 것을 원칙으로 하되, 사전에 생성되어 배포되는 경우, 키의 안정성 및 중복성 등을 정보보호책임자로부터 검증 받아야 한다.
- 암호 키의 사용, 보관, 배포, 복구 시에는 정보보호책임자의 사전 승인을 득한 권한이 있는 사용자만 사용가능 하도록 관리되어야 한다.
- 정보보호책임자는 암호프로그램 또는 암호화 알고리즘의 사용에 대하여 담당자 지정, 이용통제, 원시프로그램(Source)의 별도보관 등 프로그램의 유포 및 부당 이용이 방지될 수 있도록 엄격히 통제 및 관리해야 한다.

마지막으로 암호 프로그램의 사용은 보호 등급이 높은 자료인 경우에는 사용하는 프로그램에서 암호를 설정할 수도 있지만, 철저하게 보안을 하기 위해 보안 프로그램도 추가로 사용할 수 있다.

3.3.3 접근 통제 지침

조직의 중요 정보자산 및 정보시스템에 대한 접근을 업무적 필요와 정보보호의 요구사항을 적절하게 반영하여 통제하기 위한 접근통제의 규칙과 내부 및 외부 사용자에 대한 접근 관리, 그리고 시스템/네트워크/어플리케이션의 각 부문별로 필요한 접근통제 사항을 정의한다.

접근통제 지침에서 접근통제의 범위는 다음과 같다.

- 정보시스템의 사용자별 접근권한은 시스템, 어플리케이션, 네트워크 등의 시스템 별로 명시 및 관리되어야한다.
- 정보시스템에 대한 접근통제는 “자산 분류 및

통제 지침"에서 분류된 정보의 보안등급에 맞추어 일관성 있게 통제되어야 한다.

- 정보시스템별(네트워크, 시스템, 어플리케이션)로 명시적으로 허용되지 않은 전산자원에 대한 접근은 허용하지 않는 것을 원칙으로 한다.
- 정보시스템별(네트워크, 시스템, 어플리케이션) 관련 특별권한은 유형별로 분류되어져야 하고, 일반사용자에게 허용되어서는 안 되며 권한이 있는 시스템 관리자에게만 접근이 허용되어야 한다.
- 모든 정보시스템에 대한 사용자의 권한은 주기적으로 확인해 비인가 되거나, 불필요한 권한을 제거해야 한다.

사용자의 접근 관리에서 사용자 ID관리를 위해서는 다음이 요구된다.

- 사용자 ID 등록 및 삭제는 정형화된 절차에 따라 등록 및 삭제가 이루어져야 한다. (보안 등급이 설정된 곳에 접속이 가능한 ID에 대해서는 관리자 혹은 팀장의 승인이 있어야 한다.)
- 사용자 ID는 사용자를 식별할 수 있도록 유일한 사용자 ID를 가져야 한다(사용자를 식별할 수 있어야 함으로, 임의의 정할 수 없도록 학내에서 발급해야 한다).
- 주기적으로 사용되지 않는 사용자 ID를 확인하여 삭제해야 한다(아웃소싱 직원이나 임시직 같은 경우 사용되지 않을 때 바로 삭제해야 한다).
- ID의 생성이 초기에 부여된 패스워드 또는 재부여된 사용자의 패스워드는 최초 시스템 접속 시 변경되어야 한다(일정한 기간 안에 변경이 되지 않을 시에는 통보를 하도록 하고, 그래도 변경이 되지 않을 시에는 로그인 접속을 중단을 하는 강한 조치가 필요하다).
- 모든 정보시스템의 패스워드는 앞에서 설명한 3.3.2 "암호통제 지침"의 암호통제 지침을 적용해야 한다.

시스템의 접근통제를 위해서는 다음이 요구된다.

- 사용자 로그인 시 잘못된 접근시도는 기록되어야 하며, 정해진 회수 이상 잘못된 접속시도를 할 경우 해당 ID 또는 터미널에서의 접속을 통제해야 한다.
- 중요 시스템 유틸리티 및 운영체제 명령어에 대한 접근은 업무상 필요한 사용자에게만 허용해야 하고 사용한 내용은 기록 검토되어야 한다.
- 장비 및 운영체제 유지관리를 위한 외주업체의 작업용 ID 등은 필요시 생성하여 작업 기간 동안만 사용하도록 하고 사용이 끝나면 삭제해야 한다.

네트워크의 접근통제를 위해서는 다음이 요구된다.

- 인터넷 등의 외부 네트워크로부터 학내 내부 네트워크로의 접근은 침입차단시스템의 접근통제 등과 같은 적절한 정보보호 대책이 적용된 후 접속을 허용해야 한다.
- 장비 및 운영체제 유지관리를 위한 외부업체에서 학내의 내부 네트워크로의 온라인 접속은 허용하지 않아야 한다. 예를 들어 Window의 경우 원격 데스크톱 연결이나 원격 제어 프로그램을 실행하여 외부에서 원격으로 제어를 할 수 있도록 하면 안 된다.
- 보안 등급이 높은 정보를 취급 및 제공하는 정보시스템은 상대적으로 보안 등급이 낮은 정보시스템과 물리적으로 분리된 네트워크 구간에 위치시켜야 한다.
- 네트워크 장비의 ID및 패스워드 관리는 '3.3.3의 사용자 접근관리'를 원칙으로 한다.

3.3.4 전자문서 교환 지침

전자 정보의 교환 또는 기타 소프트웨어 및 데이터가 포함된 정보자산에 대한 전자거래를 수행하는 경우 전자거래의 사기, 계약 분장, 정보의 노

출 및 수정 등을 예방하고 통제하기 위한 내용을 기술한다.

교환합의서의 작성은 정보자산(소프트웨어, 데이터 포함)의 거래가 있을 경우에 전자거래에 대한 교환자산의 관리 및 배포, 위반 책임이 명시되게 작성해야 한다. 또한 정보보호책임자는 전자거래와 관련한 방송, 수령 등에 대한 관리 책임 및 절차 등에 대하여 보안성을 검토해야 한다.

전자거래의 보안 관리를 위해서는 다음이 요구된다.

- 정보보호책임자는 업무의 목적으로 수행되는 전자거래의 안전성과 신뢰성을 확보하기 위하여 전자거래에 따른 신분확인 절차, 무결성 확보방법, 부인방지대책, 전자교환 정보의 안정성 확보 대책을 마련해야 한다.
- 전자거래 시에 고객 등에 대한 개인정보 또는 금전적인 내용을 포함하는 경우, 별도의 대책을 수립해야 한다.

이용자 공지사항은 정보보호책임자가 안전한 전자거래를 위해 전자거래의 이용자가 준수해야할 사항과 이용자의 책임이 명시된 문서를 전자거래 시에 참고할 수 있도록 공지해야 한다. 공지사항에는 전자거래와 관련한 보안 서비스의 목적과 절차를 설명하며, 안전한 전자거래를 위해 이용자가 준수해야하는 사항을 선정하여 공지해야 한다.

3.3.5 보안사고 관리 지침

해킹, 바이러스, 악성 프로그램 등에 의한 보안 침해사고를 사전에 예방하고, 침해사고가 발행한 경우에 신속하고 대응하며, 유사한 침해사고의 재발을 방지하기 위하여 보안 침해사고의 징후 탐지, 조사, 보고, 대응, 기록 및 재발 방지를 위한 사례의 공지 및 징계 처리 등을 주요 내용으로 구성한다.

보안침해사고에 대한 보고와 대응을 위해 학내 구성원은 정보보호사고 대응절차를 숙지하고 있어야하며 정보보호사고를 탐지하면 적절한 절차에 따라 조치를 취해야 한다.

침입발견 시 학내 구성원은 업무 수행 시 보안침해사고, 취약점, 소프트웨어 오류를 탐지하였을 경우, 정보보호 담당자에게 보고하고, 정보 보호 관리자는 침입자가 발견되었을 경우 다음 사항에 중점을 두고 대응 조치를 취한다.

- 불법 침입이 있을 경우 침입자의 접속을 추적한다.
- 내부 네트워크에서 칩입한 경우는 침입한 단말기의 위치를 확인한다.
- 외부에서 침입한 경우에는 로그를 유지하며 담당자와 공동으로 대응 한다.
- 침입자를 추적할 자신이 없거나 침입으로부터 시스템의 보호가 우선시 되는 경우에는 접속을 차단한다.

침입 시 사후 조치는 정보보호 관리자가 침입되었던 시스템에 대해 보안 진단도구나 점검표를 이용하여 다음 사항을 확인한다.

- 새로운 계정이 만들어져 있는지를 확인한다.
- 외부에서 허가 없이 접속 가능한 파일들의 변경 유무를 확인한다.
- 관리자 권한의 프로그램이 새로 만들어져 있는지를 확인한다.
- 특정파일의 접근 모드가 변경되었는지를 확인한다.
- 시스템 유틸리티의 변경 및 수정여부를 확인한다.

이상 징후 및 침입 탐지를 위해서는 시스템, 네트워크, 어플리케이션 담당자가 로그를 주기적으로 분석하여 비정상적인 행위나 징후가 파악되면 학내의 정보시스템에 불법 접근이 발생했을 가능성이 있으므로, 시스템을 점검하고 즉시 정보보호 담당자에게 결과를 보고해야 한다.

정보보호 관리자는 침입자의 침입을 방지하기 위해 다음 사항을 조치한다.

- 침입 탐지된 시스템에 대한 접근 가능한 부분을 수시로 점검하여 불법침입을 사전에 예방
- 불필요한 사용자계정 또는 비밀번호가 없는 사용자 계정 삭제
- 자동화된 시스템 보안진단도구를 이용하여 침두 가능한 비밀번호 사요여부 색출 제거
- 시스템의 로그를 매일 또는 주기적으로 분석하여 시스템 침입 흔적이 있는 지 확인
- 최근의 불법 침입 방법 및 대책에 대한 자료를 입수하여 보안 대책에 반영

또한 정보통신시스템에 대한 각종 위협으로부터 보안 취약성을 진단하기 위하여 정보 통신보안 측정을 실시한다.

정보통신보안의 측정은 다음과 같은 경우 실시한다.

- 정보통신보안사고가 발생하여 정보통신망의 취약성 진단이 요구될 때
- 주요 정보통신시스템에 대한 불법침입이나 도청 등으로부터 보호대책이 필요한 경우
- 정보 통신수단에 의하여 학내의 기밀 유출 등 누설 우려가 있는 경우
- 정보통신시스템에 대한 보안성 검토와 보안 시스템 설치 등에 대한 보안대책 확인이 요구 되는 경우
- 정보 통신보안 책임자가 학내의 보안상 필요하다고 생각하는 경우
- 위의 경우 이외에 보안측정은 정기적으로 실시되어야 한다.

보안 침해사고의 조사 및 보고는 다음을 따른다.

- 정보보호 담당자는 보안 침해사고 원인 및 사고 경위에 대해 조사 및 분석하고 재발 방지를 위한 대책을 마련한다.
- 보안 사고의 내용은 정보보호 위원회에 보고한 후, 보안 사고의 원인 및 경위에 대한 조사가 종결될 때까지 공개하지 않는다.
- 각 부서의 최고 담당자는 학내의 보안 및 이익에 중대한 영향을 미칠 수 있다고 판단되는 보안위규에 대해서는 가장 신속한 방법으로 정보보호담당자에게 보고해야 한다. 보고서에는 일시 및 장소, 사고 개요, 조치내용, 사고자 및 관계자의 인적사항 같은 내용이 포함된다.

보안 침해사고의 기록 및 보관은 다음을 따른다.

- 정보보호 담당자는 정보보호 사고 발생 시 사고 일자 및 사고 내용과 사고 처리 등의 내용을 상세히 작성하여 사고일지를 문서화 한다.
- 문서화된 사고 일지는 잠금 장치가 있는 캐비닛에 적절히 보관 및 관리 한다.
- 정보보호담당자는 정보보호 사고 일지를 최소 3년간 보관하고, 정보보호 사고 관련 자료를 년 단위로 분석하여 정보보호위원회에 보고한다.
- 보고된 자료는 분석하여 해당 년도의 보안사고 대처 계획에 활용한다.

보안 침해사고 사례의 공지 및 징계는 다음을 따른다.

- 정보보호 담당자는 동일한 사건의 발생을 방지하기 위해 시스템 장애 및 보안사고 등을 모든 학내 구성원에게 공지한다.
- 정보보호 지침이나 절차를 위반한 직원에 대해서는 정보보호 위원회의 협의 후 인사위원회에 상정하여 징계처리 하도록 한다. 특히, 심각한 보안 사고를 일으켰다고 사료되는 직원에 대해서는 정보보호 위원회의 협의 후 경찰, 검찰 등 관련기관에 고발조치를 할 수 있다. 징계처리 대상에는 정보통신 보안사고 관련자, 고의 또는 중대한 과실로 자료를 변경, 훼손, 분실 또는 유출한 자, 개인 정보의 유출, 기타 다른 목적으로 정보를 유용한 자 등이 있다.

3.4 시스템 정보보안

3.4.1 전자우편 지침

전자우편이 업무 처리의 주요 수단 중에 하나로 사용되면서 중요도가 높아졌으며, 역기능으로 바이러스의 감염경로, 내부 정보의 유출, 스팸 메일 등으로 악용될 수 있는 위험이 높아졌다. 이와 같은 오용 및 피해를 예방하기 위하여 전자우편의 불법적인 사용 통제, 악의적인 목적으로의 사용제한, 안전한 전자우편의 관리에 대하여 정의한다.

전자우편의 사용에 있어서 학교의 전자우편은 정상적인 용도로 사용되어져야 하며, 불법적인 용도나 불순한 목적으로 사용되지 말아야 한다.

전자우편의 정상적인 용도로의 사용을 위해 다음이 요구된다.

- 해킹 프로그램으로 자신의 메일 계정을 이용하여 메일 서버에 접근을 시도 하지 않는다.
- 할당 받은 메일 계정을 사용하여 불법 광고를 전송하지 말아야 한다.
- 의도적으로 웜이나 바이러스를 메일에 첨부파일로 전송하지 말아야 한다.
- 상대를 비방하거나 프라이버시를 침해하는 메일을 전송하지 말아야 한다.
- 자신의 메일계정 정보를 실명으로 작성해야 한다.

잘못된 전자우편의 사용으로 인해 문제가 발생하는 경우에는 전자우편 관리자가 당사자에게 통보하고 이것을 검사 및 조사 할 수 있다.

전자우편의 사용제한을 위해서는 전자 우편의 사용 시 메일 정보 시스템 자원의 낭비를 초래하거나, 불법적인 행위에 대한 내용을 포함해서는 안되고, 대외적으로 알려지지 않아야 할 정보를 외부로 송신할 때는 보안 절차를 거쳐야 한다.

전자우편의 관리는, 문제점을 인지하는 것이 중요하다. 그럼으로, 다음과 같은 사항들에 대해서는 충분히 숙지하는 것이 필요하다.

- 전자우편의 사용은 서로를 모르고 전송하는 경우가 많으므로, 최소한의 예의는 가지고 사용해야 한다.
- 스팸 메일이 오는 경우에는 그냥 삭제하지 말고, 다음과 같은 적극적인 자세를 취하도록 한다.
  - 전자우편의 주소가 자신이 사용하는 학교 계정과 같은 주소라면, 바이러스나 웜에 의한 경우일 수도 있으므로, 보안 관리자나 전자우편 관리자에게 통보하도록 한다.
  - 전자우편의 주소가 외부 계정인 경우. 메일 프로그램사용 시 주의사항'을 참고하여 외부 계정을 스팸 메일 주소로 등록하도록 한다.
- 전자우편의 제목을 선정적으로 작성하거나, 웜이나 바이러스를 첨부하여 전송하지 않도록 한다. 관리자는 이것이 무지에 따른 원인으로 일어날 수 있는 문제이므로 이것을 인지 할 수 있도록 교육하고 공지하도록 한다.

또한 특정한 목적을 가진 웹 페이지에 가입을 하는 경우, 메일 정보를 기입하는 경우가 있는데, 이처럼 전자우편을 가지고 적용되는 사례에 대해 주의 사항이 있다.

주의 사항은 다음과 같다.

- 무책임 하게 메일링 리스트에 가입하여, 메일 서버의 계정 용량을 불필요하게 사용하지 않도록 주의 한다.
- 신규로 메일링 리스트에 가입할 때에는 반드시 자신에게 필요한 주제인가를 먼저 파악하여 가입하고, 향후 불필요한 경우를 대비해 탈퇴 신청의 절차도 조사 해 둔다.
- 전자우편 프로그램의 기능 중에 자신의 주소록에 해당하는 사람들 전체에게 전송하는 기능이 있는데, 실수로 특정인에게 보내야 할 전자우편이 전체에게 전송하지 않도록 한다.

3.4.2 이동 컴퓨터 보안 지침

노트북 등의 이동 컴퓨터의 사용이 증가하고,

외부로의 빈번한 이동으로 인하여 발생할 수 있는 위험을 예방하기 위하여 바이러스의 관리, 주요 정보의 유출 방지, 내외부로의 반출/입 통제 등에 대한 사항을 정의한다.

이동 컴퓨터의 사용 및 보안을 위해 이동 컴퓨터의 사용에 있어서 휴대폰 PC, 노트북 등의 이동 컴퓨터를 사용하여 내부 네트워크에 연결하고자 할 때에는 내부 네트워크의 보호를 위해여 보안 담당자의 승인을 받은 후 연결해야 하고, 학내의 이동 컴퓨터를 사용하는 사용자 중에 보안 등급이 높은 자료를 가지고 있는 이동 컴퓨터를 분실 시 정보의 유출을 방지하기 위하여 부팅 암호를 설정하고, 중요 정보에 대해서 암호를 설정해야 한다. 또한 내부 네트워크에 연결하고자 할 때에는 정보의 유출 가능성이 높으므로 보안에 대해 철저해야 한다.

보안 방법은 다음과 같다.

- 보안 등급이 높은 시스템에 연결하여 외부인이 작업을 해야 할 필요성이 있는 경우에는 작업에 들어가기 전에 USB메모리나 하드 디스크의 용량을 체크하고, 작업 후에 변동 사항이 있는지를 점검한다.
- 보안 등급이 높은 시스템에 접근이 가능한 이동 컴퓨터에 대해서 학내 외로 빈번한 반출/입이 이루어지는 경우 보안 담당자의 승인을 받은 후 반출입증을 부착해야 하며, 팀별 보안담당 직원에게 반출/입 확인을 받아야 한다.

3.4.3 네트워크 보안 지침

조직의 모든 정보자산은 외부로부터의 불법적인 접근으로 발생할 수 있는 사고를 예방하기 위해 네트워크의 보안 통제 및 네트워크 통신장비 자체에 대한 보안통제, 그리고 체계적인 IP 주소 관리에 대한 사항을 정의한다.

네트워크 구성 및 접근통제는 상용망 연동, 유관 기관망 연동, 내부망 통제로 나누어진다.

첫 번째로 상용망 연동은 다음과 같이 이루어진다.

- 외부 네트워크와 연결되는 모든 경로에는 내부 네트워크의 보호를 위해서 비인가자의 불법접근을 차단할 수 있는 침입차단시스템 등을 설치하여 내부 네트워크를 보호해야 한다.
- 인터넷 등 상용망과의 접속은 불법침해를 방지하고 효율적인 보안 관리를 위하여 외부로의 접속점을 지정 운용함으로써 임의 접속을 차단해야 한다.
- 외부에서 내부 시스템에 접속할 경우 인가된 사용자라 할지라도 강화된 인증통제와 가상사설망(VPN ; Virtual Private Network) 등의 추가적인 보안 시스템을 거치도록 한다.
- 정보통신망에 상용되는 IP주소는 체계적으로 관리 되어야 하며, 내부 네트워크의 보호를 위해서 가능한 내부 네트워크에 대해서는 사설주소 체계를 이용한다.
- 웹서버, 메일서버 등 외부에 정보를 제공하기 위한 목적으로 운영되는 정보시스템은 내부 네트워크와 분리된 별도의 네트워크 영역을 구성해야 한다.
- 외부에서 내부 네트워크로의 접속은 웹서버, 메일서버 등의 공개 시스템을 위한 별도의 네트워크 영역으로의 접근을 제한적으로만 허용하며, 내부 네트워크로의 직접 접근은 허용하지 않는 것을 원칙으로 한다.

두 번째로 유관 기관망 연동은 다음과 같이 이루어진다.

- 다른 기관의 정보통신망과 연결하여 사용하고자 할 경우에는 보안 관리 책임의 한계를 설정하여 운용해야 한다.
- 유관 기관과의 접속은 전용회선 사용을 원칙으로 한다. 다만 부득이한 경우 심의를 거친 후 적절한 보안대책을 수립, 운용해야 한다.
- 외부망과 접속하는 경우에는 전산자료 제공 범위 및 이용자의 접근제한 등에 대해 심의를 거친 후 적절한 보안대책을 수립, 운용해야 한다.

- 외부망 연결에 따른 보안 취약성 해소를 위하여 접속자료를 주기적으로 분석하고 보안 도구를 이용하여 정보통신망의 취약성을 수시 점검해야 한다.
- 정보보호 담당자가 필요하다고 인정하는 경우 정보통신망 접속의 효율적 구성과 운영을 지원하기 위하여 외부망 접속 중계기관을 지정 운영할 수 있다.

마지막으로 내부망 통제는 다음과 같이 이루어진다.

- 전산자료 제공 범위 및 이용자의 접근제한에 따라 적절한 보안대책을 수립, 운용해야 한다.
- 비밀자료를 취급하는 정보통신시스템의 경우 일반 시스템과 논리적으로 분리시켜 운영한다. 다만, 부득이한 경우 심의 후 가장 높은 전산자료의 보호등급에 따른 보안 대책을 강구해야 한다.

네트워크 보안관리를 위해서는 네트워크의 운용 및 관리를 해야 한다. 그것은 다음과 같이 이루어진다.

- 대학교 내에 설치한 전산망의 모든 관리와 운영은 전산소에에서 담당한다.
- 전산망 관리자는 장애발생 및 복구 시에는 장애발생의 원인과 복구에 대한 보고서를 작성하여 상급자에게 서면으로 이를 보고하고 유지해야 한다.
- 네트워크 신규 접속, 변경, 해지
  - 신규, 변경, 해지라 함은 네트워크에 접속되어 정보보호 자산에 엑세스를 할수 있는 모든 서버, 클라이언트, 네트워크 및 네트워크 장비 등을 뜻한다. 네트워크 신규 접속, 변경, 해지는 통제되어야 하며, 주관부서장의 승인을 득해야 한다.
- LAN포트 사용에 대한 허가
  - 내 · 외부 네트워크에 사용 되어지는 모든 LAN 포트는 침입차단 및 침입탐지 시스템에서 등록 관리 하며, 기본적인 포트 외에는 상용을 금함을 원칙으로 한다. 부득이 포트의 추가 발생시는 주관부서장의 승인을 득해야 한다.
- LAN주소 사용에 대한 허가
  - 사설/공인 IP의 관리는 업무담당자가 관리하며, 주관부서장의 승인을 득한 후 신규 부여 및 회수/변경 등의 업무를 진행 한다.
  - 신청자는 IP등록 신청서를 작성하여 업무담당자에게 제출하여 부여 받은 IP를 사용해야 하고, 감사 결과 해당 IP에서 발생된 문제점에 대해서는 IP등록 대장상에 있는 사용자로 간주하여 책임을 추궁 할 수 있다.
- 내부 네트워크 정보의 외부 유출 금지
  - 공식적인 허가 없이 네트워크의 내부 주소, 구성환경, 그리고 관련 시스템 설계정보는 외부 네트워크에 있는 시스템이나 사용자가 접근할 수 없어야 한다.
- 네트워크는 물리적으로 광범위하고 경로가 다양하며, 많은 사람에게 이용되고 있기 때문에 여러 가지 보안문제를 야기하고 있다. 따라서 중요한 정보자산에 영향을 미치는 불법시도를 사전에 감지하고 자산을 보호하기 두 가지 보안관리 활동이 요구된다. 첫 번째로 전산망관리에는 일관성과 기밀성을 위해 통합관리 원칙에 따른 네트워크관리, 네트워크 주소(IP 주소)에 대한 변경 통제, 방화벽을 통한 내부 시스템 접근을 통제하고, 관련정보 로깅(Logging)관리, 특수계정(슈퍼유저 및 root) 로그인 통제, 다이얼 업 모뎀에 의한 접속을 제한 등이 있다.

두 번째로 방화벽관리에는 방화벽 시스템에 대한 계정통제, 외부로부터 접근 시도는 반드시 로그관리 등이 있다.

- 네트워크 관리자는 네트워크 장비들에 대한 보안

지침을 작성하여 운영해야 하며, 네트워크 장비 및 IP 할당에 대한 구성 내역을 관리해야 한다.

- 네트워크 사용자는 부서장의 사전승인 없이 개인 소유의 컴퓨터, 주변장치 또는 소프트웨어를 학내로 내로 가져와서 네트워크에 연결해서는 안 된다.
- 네트워크 관리자는 네트워크의 구성변경 또는 새로운 네트워크와 접속 시 정보보호 관리자와 함께 보안성 검토를 실시하여 대책을 마련한 후 변경작업을 수행해야 한다.

정기적인 통신장비 보안점검은 네트워크 관리자가 허가되지 않은 장비의 접속을 탐지하거나 네트워크에 연결되어 있는지를 검사하기 위해 매달 통신관련 장비 및 네트워크를 점검해야 한다.

3.4.4 침입차단시스템 지침

조직의 중요한 정보시스템과 모든 사용하는 컴퓨터에 대하여 외부로부터의 비인가된 불법 접근을 차단하기 위한목적으로 도입된 침입차단시스템의 안전한 관리를 위해 침입차단시스템의 지침에 대한 문서화와 침입차단시스템의 구성 및 관리, 접근통제 규칙의 관리에 대해 정의한다.

침입차단시스템 지침의 문서화를 위해서 학내 내부와 연결되는 모든 침입차단시스템은 기존에 설치되었거나 혹은 도입예정된 것이든 간에 반드시 문서화 되어야 하고, 문서화는 반드시 학내의 정보보호 조직의 검토를 받아야 한다.

침입차단시스템의 구성은 다음과 같다.

- 침입차단시스템의 연결은 정보보호 조직에 의해 검토되고 승인되어야 하며, 내부 네트워크와 연결되는 모든 침입차단시스템은 다음과 같이 정보보호 조직에 의해 승인된 제품이어야 한다. 승인된 제품으로는 각급기관에 적용 가능한 평가등급을 획득하고 인증서를 받은 제품, 각급기관의 소관업무 및 정보통신망 특성을 지원할 수 있는 제품, 지속적인 유지보수 및 침입차단 시스템 운용기술 지원능력을 구비한 업체의 제품 등이 있다.
- 침입차단시스템 하드웨어의 물리적 연결은 설치, 설계, 운영 및 관리를 담당하는 인가된 사람으로 제한돼야 한다.
- 침입차단시스템은 외부에 공개된 지역에 위치해서는 안되며, 무정전 전원공급 장치(UPS ; Uninterruptible Power Supply), 과전압 보호 장치, 에어컨, 화재경보기 등의 장치에 의해 적절한 운영환경이 보장된 곳이어야 한다.
- 침입차단시스템에 모뎀을 직접적으로 연결해서 접속해서는 안된다. 또한, 침입차단시스템은 안전한 모뎀 Pool로 외부로 접근할 수 있으나 이는 비상 호출용으로만 제한되어야 한다.
- 외부에서의 내부로의 접속은 학내 정보보호 조직에 의해 승인된 가상 사설망(VPN ; Virtual Private Network)으로만 제한되어야 한다.
- 침입차단시스템은 비인가자 출입통제 등 보안관리가 용이한 곳에 설치해야 한다.

구성된 침입차단시스템 접근통제 규칙의 관리는 다음과 같이 이루어진다.

- 침입차단시스템의 접근통제규칙은 명확하게 사용이 정의된 IP주소와 서비스Port 단위로 규칙을 적용해야 한다.
- 침입차단시스템을 통한 접근통제는 인터넷을 포함한 외부에서 공개된 서비스를 제공하는 영역인 보안구역(DMZ ; DeMilitarized Zone) 영역으로의 제한된 접근만을 허용하는 것을 원칙으로 한다.
- 각급기관의 장은 운용요원에 대하여 운용관리 직무지식, 시스템 취약성 분석 및 보안진단 방법, 보안사고 발생 시 긴급조치 능력 등에 대한 교육·훈련계획을 체계적으로 수립 시행해야 한다.
- 정보보호책임자는 침입차단시스템에 대해 재사용 공격이 불가능한 신분확인 기능, 사용자 및 호

스트 컴퓨터 주소 등급에 기반 한 강제적 접근 통제 기능, 침입차단시스템 운용에 요구되는 저장파일 및 전송데이터의 무결성, 기타 각급기관의 특성에 맞는 보안기능, 감사기록 및 추적기능 등의 보안기능을 포함하여 관리되도록 한다.

- 정보보호책임자는 주기적으로 침입차단시스템에 일반사용자 계정이 있는지 여부, 침입차단시스템 환경설정에 관련된 파일의 접근허용모드가 알맞게 설정되었는지 여부, 침입차단시스템 관리자 권한을 도용할 수 있는 프로그램 변경 및 은닉 여부, 비인가자의 침입여부를 확인하기 위한 시스템 접근기록 등의 사항을 점검해야 한다.

4. 결 론

지금까지 정보보호원칙을 반영하여 정보보호지침이 포함해야하는 여러 고려사항을 구체적으로 설명하였다. 그동안 정보보호지침을 수립할 때에는 고려해야 할 항목이 많고, 당장에 큰 변화를 볼 수 없었기 때문에 하드웨어적인 발전과 발을 맞출 수 없었다. 하지만 정보보호원칙이 적용된 정보보호지침과 개략적이고 형식적인 정보보호지침은 보안성과 정보화 수준의 차이를 극명하게 가르게 된다. 보안성을 전제할 수 없다면 결국에는 하드웨어적인 발전에도 장애가 생길 수밖에 없으며, 정보화 수준의 차이는 국가경쟁력을 좌우할 것이다.

본 논문에서는 우리나라 대학이 가지고 있는 보편적인 정보화 환경을 대상으로 하여 세부적으로 정보보호원칙을 제안하였으며, 구체적으로 관리지침을 정의하였다.

향후 본 논문에서 설명한 원칙을 기반으로 하여 지침을 수립 및 적용할 경우, 대학 구성원들의 정보화 마인드 고취와 함께 보안사고 및 해킹감소 등 대학 정보화의 활성화와 질적인 발전 그리고, 건전한 IT문화가 구축될 수 있을 것으로 기대한다.

참 고 문 헌

[1] 최우혁, “정보보호 관리체계 인증심사 기준”, 정보통신부고시, 제 2002-22호, 2002.

[2] WPISP, “OECD Guidelines for the Security of Information Systems and Networks : TOWARDS A CULTURE OF SECURITY”, (2002), p.116.

[3] Ralph Spencer Poore, “Generally Accepted System Security Principles”, 1999.

[4] NIST, Table of Contents for Special Publication 800-12 Chapter 2, 2004.

[5] 인터넷침해사고 대응지원센터(KrCERT/CC), http://www.krcert.or.kr.

[6] 국가사이버안전센터(National Cyber Security Center), http://www.ncsc.go.kr.

[7] 국가보안기술연구소(National Security Research Institute), http://www.nsri.re.kr.

[8] 한국정보보호진흥원(Korea Information Security Agency), http://www.kisa.or.kr.

[9] 경찰청 사이버테러 대응 센터(Cyber Terror Response Center), http://www.ctrc.go.kr.

[10] CERT(Computer Emergency Response Team), http://www.cert.org.

◈ 저 자 소 개 ◈

유 기 훈 (playboyyu@kw.ac.kr)

광운대학교 컴퓨터소프트웨어학과를 졸업하고, 현재 동 대학원에서 컴퓨터과학과 석사과정에 재학 중이다. 주요 관심분야는 무선 네트워크, 무선 센서 네트워크, 라우팅 알고리즘 등이다.

최 웅 철 (wchoi@kw.ac.kr)

서울대학교 컴퓨터공학과를 졸업하고 동 대학원에서 컴퓨터공학 석사학위를 받았다. 미국의 University of Illinois, Urbana-Champaign, IL에서 컴퓨터과학 박사학위를 받았다. 그리고 Bellcore(Bell Communications Research) Lab., Morristown, NJ.에서 Research Scientist로 근무하였다. 2001년부터 광운대학교 컴퓨터과학과 조교수로 재직하고 있다. 관심분야는 정보시스템 감리및 감사, 정보시스템 보안, 망 설계및 관리, QoS 등이다.

김 신 곤 (shinkon@kw.ac.kr)

연세대학교 경영학과를 졸업하고 서울대에서 경영학 석사학위를 받았다. Georgia State University에서 컴퓨터 정보시스템 (CIS) 석사를 취득 후 동 대학원에서 경영정보학 박사학위를 받았다. (주) 코리아로터리서비스의 기술연구소장으로 있으면서 즉석복권 시스템을 개발하였고 1992년부터 광운대학교 경영정보학과 교수로 재직하고 있다. 관심분야는 경영정보시스템, 시스템 분석 및 설계, 비즈니스 인텔리젼스, 고객관계관리 및 데이터마이닝, 비즈니스 모델링 등이다.

구 천 열 (cykoo@moe.go.kr)

교육인적자원부 전산사무관