경영정보학연구
제14권 제4호
2004년 12월

정보보호전문가의 직무수행을 위한 지식 및 기술 분석

최 명 길*, 김 세 헌**

Analysis of Knowledge and Skill for Security Professionals

Myeonggil Choi, Sehun Kim

Due to exponentially growing threats of cyber attacks, many organizations have begun to recognize the importance of information security. There is an explosion in demand for experienced ISMs(Information Security Managers) and ISSDs(Information Security System Developers). To educate ISMs and ISSDs, identifying the specific knowledge and skill for information security professional is critical. This paper identifies 15 items of knowledge and skill for ISMs and ISSDs using a simplified Delphi technique and categories them. The results of this paper could be used in determining what kinds of knowledge and skill should be included in the curriculum of information security programs.

Keywords : Knowledge and Skill, Information Security Manager, Information Security System Developer, Delphi Approach

* 한국전자통신연구원, 국가보안기술연구소(NSRI)
** 한국과학기술원(KAIST)

Ⅰ. 서 론

인터넷의 급격한 발달과 전자상거래의 활성화는 조직의 경쟁력을 강화하는 동력원이지만, 이러한 발전은 인증 및 보안과 같은 정보보호기능의 토대 위에서만 가능하다. 최근 급격히 증가하는 사이버 공격에 대한 보안대책은 정보통신 인프라의 중요한 근간이 되고 있다. 기업이나 공공기관 등과 같은 조직은 정보자산의 안전한 보호를 위하여 정보보호시스템을 채용하고 있으며, 정보보호를 책임지는 부서를 설립하고 있는 실정이다[Jung, 2001]. 이러한 상황에 따라 정보보호전문가에 대한 수요가 급격하게 증가하고 있지만, 경험 있고 훈련된 정보보호전문가의 공급은 부족한 실정이다[한국정보보호진흥원, 1999; 2001]. 정보보호전문가란 정보보호관리자(Information Security Managers), 정보보호시스템 개발자(Information Security System Developers), 정보시스템 운영자와 정보보호 컨설턴트 등을 의미하지만, 본 연구는 정보보호전문가를 정보보호관리자와 정보보호시스템 개발자로 한정하며, 이 두 집단은 조직의 성공적인 정보보호에 가장 핵심적인 역할을 수행한다[NIST, 1994].

정보보호는 컴퓨터공학, 통신공학, 수학, 전자상거래, 경영학, 법학 등과 같은 다양한 분야를 포함하는 학제적 성격을 가지고 있다. 따라서 정보보호전문가를 양성하는 데 있어서 다른 분야에 비하여 좀 더 복잡하며, 소요되는 시간이 상당히 길다[정보통신부, 2001]. 정보보호전문가의 양성 및 획득을 위해서는 체계적인 교육과정 및 직무분석이 필요하며, 이를 위해서는 정보보호전문가가 갖추어야 할 지식 및 기술의 식별이 선행되어야 한다.

본 연구의 목적은 정보보호전문가의 교육 및 직무분석을 위해 필요한 지식 및 기술을 식별하는 것이다. 본 논문에서 의미하는 지식이란 정보보호전문가가의 직무수행을 위해 사전에 학습을 통하여 획득 가능한 지식을 의미하고, 기술이란 직무를 실제적으로 수행할 수 있는 경험 또는 능력을 의미한다. 본 연구의 결과는 정보보호전문가 교육에 필요한 프로그램 개발 및 채용에 필요한 직무분석에 사용할 수 있다. 즉 도출된 지식 및 기술을 반영하여 정보보호전문가 양성에 필요한 교육 과정 설계, 자질을 갖춘 정보보호전문가 획득 및 조직이 필요로 하는 정보보호 기술을 식별하는 데 사용 수 있다.

정보보호관리자와 정보보호시스템개발자의 역할이 확연히 다름에도 불구하고, 이 두 집단이 필요로 하는 지식 및 기술을 동일시하여 동일한 교육과정을 통하여 정보보호관리자와 정보보호시스템 개발자를 교육하는 경향이 있다[Kim, 2002]. 정보보호관리자는 조직의 임무와 업무 지원의 우선 순위 뿐만 아니라 조직의 정보보호의 목적, 목표 및 정보보호계획을 수립한다. 정보보호관리자는 조직의 정보보호 프로그램에 대한 일상적인 관리도 감독한다. 정보보호관리자는 정보시스템과 관련된 정보보호기술을 잘 알기 때문에 정보시스템을 보호하기 위한 기술적인 정보보호대책을 구현한다[Wilson, 1998; Wood, 1995]. 정보보호관리자와 정보보호시스템 개발자의 직무간에는 차이가 존재함으로 이 연구는 정보보호관리자 그룹과 정보보호시스템 개발자 그룹의 지식 및 기술이 상이하다고 가정하고, 두 그룹에 적합한 별도의 지식 및 기술을 도출한다.

본 연구는 정보보호관리자와 정보보호시스템 개발자에게 필요한 가장 중요한 지식 및 기술을 식별하기 위하여 정보보호전문가에게 의뢰하여 약 40개의 항목으로 구성된 설문을 작성하였다. 작성된 설문을 바탕으로 델파이 방법을 사용하여 정보보호관리자와 정보보호시스템 개발자의 지식 및 기술 항목을 식별하였다. 델파이 방법은 정보시스템 분야의 전문가의 의견을 수집할 때 사용할 수 있는 유용한 기법이다[Buckely, 1995; Niederman, 1991; Palvis, 1995; Wetherbe, 1996].

다음은 본 연구에서 분석할 이슈이다.

(1) 정보보호관리자에게 있어서 가장 중요한 15개의 지식 및 기술은 무엇인가?
(2) 정보보호시스템 개발자에게 있어서 가장 중요한 15개의 지식 및 기술은 무엇인가?
(3) 정보보호관리자와 정보보호시스템 개발자의 지식 및 기술을 어떻게 분류할 것인가?
(4) 정보보호관리자와 정보보호시스템 개발자가 필요로 하는 지식 및 기술의 유사점과 차이점은 무엇인가?

Ⅱ. 관련 연구

정보보호전문가에게 필요한 지식 및 기술에 대한 연구는 주로 교육과정개발과 관련하여 이루어지고 있다. 국내연구로는 "대학에서의 정보보호교육과정개발"에 대한 연구가 있다[김철, 2001]. 이 연구는 현재 대학의 정보보호교육 프로그램을 정성적으로 분석하였고, 정보보호전문가 양성 교육과정을 제시하고 있다.

한국정보보호진흥원은 정보보호 전문인력 개발과 활용에 대한 연구를 진행하였다[한국정보진흥원, 2001]. 이 연구는 정보보호전문가에게 요구되는 지식 및 기술과 관련한 정보를 제공하고 있지만, 정보보호교육시 필요한 핵심적인 지식 및 기술을 분석하고 있지 못하고 있으며, 특히 정보보호전문가를 활용할 정보보호조직의 필요를 반영하지 못하고 있다.

김기윤은 학계와 산업계의 공동 노력으로 개발한 정보보호관리 교육과정 설계에 대한 연구를 수행하였다[김기윤, 2001; Kim 2002]. 이 연구는 정보보호관리를 위한 교육과정 설계를 제시하고 있는데, 교육과정 설계는 산업계와 학계에서 도출된 결합된 노력을 바탕으로 이루어졌다.

정보보호전문가의 지식 및 기술과 관련된 국외 연구도 주로 교육과정 설계와 운영과 관련하여 이루어지고 있다. Armstrong은 대학원 과정에서 인터넷 정보보호 관리와 관련된 교육과정을 설계하였다[Armstrong, 2002]. 이 연구는 일련의 대학원 과정에서 정보보호관리 교육과정을 다루고 있다.

Logan은 학부과정에서 정보보호과정 개설에 관련한 연구를 수행하였다[Logan, 2002]. 이 연구는 보안관리에 필요한 기술 항목, 교육과정에 포함시킬 실험실 요구사항과 교육과정에 포함할 법률 등을 제시하고 있다.

Grimaila는 경영학 학부과정에서 정보보호교육과정을 제시하고 있고 교육과정의 검증을 위해 실험실 검증 연구를 수행하였다[Grimaila, 2002]. 이 연구는 학부과정에서 경영정보학과정의 정보보호과목의 설계, 수행 및 강의 수행을 서술하고 있으며, 교육과정 개발시에 고려해야 할 중요한 요소를 식별하고, 교육과정의 유효성을 검증하고 있다.

Hsu는 정보시스템보호교육의 이론과 실제에 대한 연구를 수행하였다[Hsu, 2002]. 이 연구는 두 가지 영역에 초점을 두고 있다. 첫째, 상황학습전략(situated learning strategy)에 적용할 수 있는 정보시스템 보호교육과정과 관련된 예를 제시하고 있으며, 둘째, 특정한 교수방법 설계에 대한 학생들의 피드백을 조사하고 있다. 이 연구를 통해 상황학습전략(situated learning strategy)이 이론과 실무간 조화를 추구하고, 지식 개발에 있어서 잠재력이 있음을 보여주고 있다.

정보보호전문가의 지식 및 기술 항목 분석과 관련된 국·내외의 연구는 교육과정 개발에 초점을 두고 있다. 정보보호전문가를 필요로 하는 조직이 원하는 교육과정의 개발을 위해서는 교육과정을 구성하는 정보보호전문가의 지식 및 기술을 식별하고, 지식 및 기술의 중요도를 결정하는 연구가 선행되어야 하지만, 관련된 연구가 이루어지고 있지 않은 실정이다. 이는 특정 분야의 연구자가 광범위한 정보보호 관련 지식 및 기술을 통합적으로 도출하기 어렵고, 특히 정보보호 분야가 최근 급속도로 성장하고 있기 때문이다.

Ⅲ. 연구 방법론

정보보호전문가는 정보보보호전문가에게 필요한 지식 및 기술에 대해서 다른 견해를 가질 수 있다. 정보보호전문가 그룹으로부터 일반적인 견해를 도출하여 정보보호전문가에게 필요한 지식 및 기술을 식별함으로 연구의 객관성을 확보할 수 있다. 이를 위해 본 논문은 델파이 방법을 채용하였고, 본 논문이 채용한 델파이 방법은 다음과 같이 4단계로 구성된다.

단계 1: 지식 및 기술 항목 리스트 작성
단계 2: 40개의 지식 및 기술 항목으로 구성된 설문지 작성
단계 3: 전문가 의견을 설문을 통해서 조사
단계 4: 설문 결과 분석

정보보호전문가에게 필요한 중요한 지식 및 기술을 식별하기 위해서, 먼저 정보보호전문가 그룹에게 정보보호관리자 및 정보시스템개발자에게 필요한 지식 및 기술 항목을 각 10개씩 작성해 줄 것을 요청했다. 작성된 항목을 토대로 정보보호관리자와 정보보호시스템 개발자에게 필요한 지식 및 기술 리스트를 작성하였다. 본 연구에서 적용한 구체적인 델파이 방법은 아래와 같다.

(1) 단계 1

델파이 참가자들에게 정보보호관리자 및 정보보호시스템 개발자에게 필요한 10개의 중요한 지식 및 기술 항목을 작성해 줄 것을 요청하였다. 아울러 각 지식 및 기술 항목의 중요성에 대한 이론적인 근거를 제시해 줄 것을 요청하였다. 회송된 10개의 리스트를 바탕으로 설문지를 작성했다. 설문을 분석하여 지식 및 기술 항목과 근거사항으로 구성된 리스트를 작성했다.

(2) 단계 2

델파이 방법에 참가자들이 만든 리스트를 바탕으로 40개의 지식 및 기술 항목으로 구성된 설문지를 작성하였다. <부록 A>는 40개 지식 및 기술 항목으로 구성된 설문이다. 연구자 그룹과 실무자 그룹은 지식 및 기술 항목에 대해 상당히 다른 견해를 가지고 있을 것이라고 예상하고, 설문대상을 두 개의 그룹으로 분리하였다. 첫 그룹은 연구자 그룹이며 주로 대학교수, 연구원으로 구성되어 있다. 연구자 그룹의 주된 관심사는 실무적인 측면보다 IS의 이론적인 측면에 더 많은 관심을 가지고 있으리라 예상된다. 두 번째 그룹은 실무자 그룹인데, 이 그룹은 정보보호컨설턴트, 정보보호관련 조직의 관리자, 시스템 개발자, 정부 기관의 정보보호관리자로 구성되어 있다. 이 그룹의 주된 업무는 IS 기술을 실제적으로 적용하고 사용하는 것이다. <표 1>은 설문 응답자의 직업군에 의한 분류이다. 응답자 그룹을 두 그룹으로 분류함으로 연구 결과의 유효성을 증가시킬 수 있다.

<표 1> 델파이 참여자의 분포

직 위	응답자	퍼센트(%)
대학교수	5	8.06
정보보호 전문연구소의 연구 관리자	9	14.5
정보보호 전문연구소의 연구원	14	25.5
정보보호 컨설턴트	6	20.9
정보보호시스템 개발 회사의 관리자	5	8.06
정보보호시스템 개발 회사의 개발자	7	12.7
정부의 정보보호 관리자	9	14.5
계	55	100.0%

(3) 단계 3

델파이 참가자들에게 정보보호관리자와 정보보호시스템 개발자에게 있어서 필요한 지식 및 기술을 각 15 항목씩 선택해 줄 것을 요청하였다. 지식 및 기술 항목을 선택한 후 각 항목의 중요도에 따라 15점(가장 중요)에서 1점(가장 덜 중요)까지 점수를 부여해 줄 것을 요청하였다. 정보보호관리자와 정보보호시스템 개발자의 지

식 및 기술의 중요도 식별과 정보보호관리자 및 정보보호시스템 개발자간의 지식 및 기술 차이점의 적절한 분석을 위해서는 <부록 A>의 40개의 지식 및 기술 항목 중에서 15개 정도의 항목을 선정하면 가능하다. 설문지는 70명의 정보보호전문가에게 발송되었고, 55명이 설문지를 회송하였다. 설문 응답율은 약 78%였다.

(4) 단계 4

회송된 설문지는 다음과 같은 절차에 따라 분석하였다. 첫째, 정보보호관리자의 지식 및 기술과 관련하여 회송된 설문지에서 가장 빈번하게 선택된 25개의 항목을 선택했다. 정보보호시스템 개발자의 경우에는 가장 빈번하게 선택된 27개의 항목을 선택했다. 이 때, 정보보호관리자와 정보보호시스템 개발자의 지식 및 기술 항목의 선택 기준은 델파이 참가자의 응답 빈도로 사용했다. 다음으로 각 항목에 대해서 델파이 참가자가 부여한 점수를 합산하였다. 빈도와 총점을 기준으로 정보보호관리자와 정보보호시스템 개발자에게 필요한 15개의 항목을 획득하였다. 델파이 참가자가 부여한 점수를 합산하여, 지식 및 기술 항목의 순위를 부여하였다. 만약 합산점이 동일할 경우 빈도가 높은 항목을 우선시 하였다.

Ⅳ. 정보보호관리자의 지식 및 기술 분석

<표 2>, <표 3>는 연구자 그룹과 실무자 그룹이 정보보호관리자의 지식 및 기술을 식별하고, 중요도를 분석한 결과이다. <표 2>는 연구자 그룹의 설문 조사 결과이고, <표 3>는 실무자 그룹의 설문 조사 결과이다.

<표 2>과 <표 3>에서, 동일한 지식 및 기술 항목이 도출되었지만, 순위에 있어서 차이가 존재한다. 연구자 그룹에서만 존재하는 항목은 "보안감사", "인터넷 기술"인 반면, 실무자 그룹에서만 존재하는 항목은 "해킹 대응"과 "정보보호표준에 대한 지식"이다. 연구자 그룹과 실무자 그룹의 견해는 거의 유사하게 나타났다는 사실은 연구 결과의 신뢰성이 매우 높다는 사실을 입증하고 있다. 연구자 그룹과 실무자 그룹간의 중요도의 차이는 이들이 직면한 업무환경과 밀접한 관련을 가지고 있다.

정보보호관리자의 지식 및 기술 항목 설문 결과를 분석하면 기존 연구 결과와 일치점을 보인다. "정보보호정책수립"과 "관리적 정보보호대책수립"은 Wilson의 연구가 제시한 컴퓨터 보안 관리자의 역할과 매우 밀접하게 관련되어 있다[Wilson, 1998]. 이 두 항목은 정보보호관리자의 역할과 책임을 나타내고 있다. 정보보호관리자는 조직의 목적을 지원하기 위해서 조직의 컴퓨터 보안 정책과 목적, 목표, 우선순위를 수립해야 한다[김기윤, 2000; Wilson, 1998; Wood, 1995, 1993]. 결국 조직의 정보보호 책임은 정보보호관리자에 달려 있다.

<표 2> 연구자 그룹의 정보보호관리자에게 필요한 지식 및 기술 항목 설문 분석 결과

순위	지식 및 기술	총점	빈도	퍼센트(%)
1	관리적 정보보호대책 수립	321	26	93
2	정보보호정책 수립	295	26	93
3	정보보호시스템 취약성 분석	229	22	79
4	기초 암호학 이해	217	24	86
5	위험 분석 및 평가	214	22	79
6	보안 환경 분석	205	26	93
7	관련 법률 및 규정 이해	192	25	89
8	정보보호시스템의 평가	164	18	64
9	보안감사	157	17	61
10	물리적 정보보호대책 설계	156	20	71
11	정보보호교육 프로그램 관리	149	24	86
12	프라이버시와 윤리	124	15	54
13	침입탐지와 차단 관리	99	18	53
14	인터넷 기술	98	17	53
15	컴퓨터 바이러스 관리	97	14	50

주) 전체 응답자 수: 28, 총점: 점수 합계, 최고점: 15, 최저점: 1, 빈도: 선택한 항목

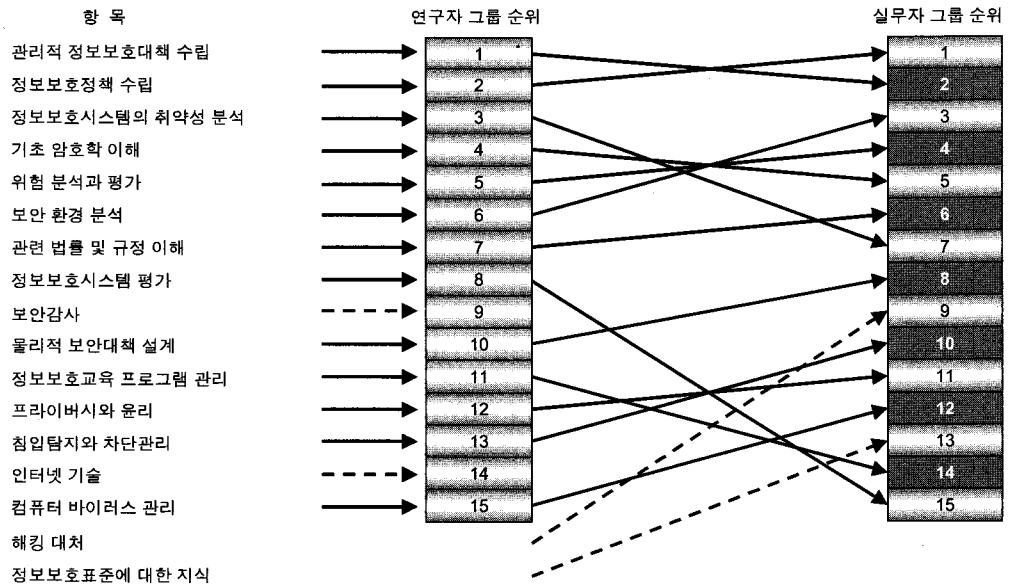
<표 3> 실무자 그룹의 정보보호관리자에게 필요한 지식 및 기술 항목 설문 분석 결과

순위	지식 및 기술	총점	빈도	퍼센트 (%)
1	정보보호정책 수립	271	26	96
2	관리적 정보보호대책 수립	246	26	96
3	보안 환경 분석	238	27	100
4	위험 분석 및 평가	193	21	78
5	기초 암호학 이해	192	19	85
6	관련 법률 및 규정 이해	192	23	70
7	정보보호시스템 취약성 분석	170	19	70
8	물리적 정보보호대책 설계	163	19	70
9	해킹대응	143	22	81
10	침입탐지와 차단 관리	138	18	67
11	프라이버시와 윤리	137	17	63
12	컴퓨터 바이러스 관리	133	18	67
13	정보보호표준에 대한 지식	115	13	48
14	정보보호교육 프로그램 관리	114	20	74
15	정보보호시스템의 평가	111	18	67

주) 전체 응답자 수: 27, 총점: 점수 합계, 최고점: 15, 최저점: 1, 빈도: 선택한 항목

시스템 보호와 관련된 항목, 특히 해킹으로부터의 시스템 보호의 중요성이 점차적으로 인식되고 있다. 인터넷침해대응지원센타(CERTCC-KR: Computer Emergency Response Team Co-ordination Center- Korea)의 공식보고서에 의하면, 해커로부터 공격을 받은 해킹피해가 26,000여건에 이른다[인터넷침해대응지원센타, 2003]. 연구자 그룹에서 제시한 해킹사고와 관련된 항목 및 순위로는 "정보보호시스템의 취약성 시험(3위)", "침입탐지와 차단 관리(13위)", "컴퓨터 바이러스 관리(15위)" 등이 있다. 실무자 그룹의 경우 위에서 언급한 항목의 중요도 순위는 각각 7위, 10위, 12위로 나타나고 있다. 실무자 그룹은 연구자 그룹에 비해 실제적인 실제적인 정보보호문제를 더 중요시 하는 경향이 있다.

정보보호대책이 점차로 수립됨에 따라 정보보호시스템의 보증개념이 강조되고 있다[DoD, 1996]. 정보보증과 관련된 정보보호관리자의 지식 및 기술 항목은 연구자그룹과 실무자 그룹에서 각각 "보안환경분석(6위, 3위)", "위험분석과 평가(5위, 4위)"와 "정보보호시스템 평가(8위, 15위)"로 나타나고 있다.



<그림 1> 정보보호관리자의 지식 및 기술 항목간의 순위 비교

위에 언급한 항목 외에도 연구자 그룹과 실무자 그룹이 순위를 부여한 항목은 "관련 법률 및 규정 이해", "보안감사"와 "물리적 정보보호 설계" 등이 있다. 이 설문 결과는 정보보호관리자도 기초 암호학을 이해해야 한다고 제시하고 있다.

<그림 1>은 두 응답 그룹의 지식 및 기술 항목의 순위를 비교하여 나타내고 있다. 비록 두 응답그룹이 매우 유사한 항목을 선택하였지만, 항목간의 순위는 약간 차이가 있게 나타나고 있다. 연구자 그룹은 "관리적 보안"에 대해 좀 더 중요성을 둔 반면에 실무자 그룹은 "침입탐지기술"에 대해서 중요성을 두고 있는 것으로 나타났다.

V. 정보보호시스템 개발자의 지식 및 기술 분석

<표 4>, <표 5>는 정보보호시스템 개발자의 지식 및 기술 항목과 관련된 연구자 그룹과 실무자 그룹의 설문 결과이다. <표 4>, <표 5>에서 보듯이, 연구자 그룹과 실무자 그룹은 "정보보호시스템 설계", "시스템 구조 분석"을 가장 중요한 항목으로 여기고 있다. 실무자 그룹과 연구자 그룹은 두 항목을 제외하고, 동일한 항목에 대해 순위를 부여하고 있다. 연구자 그룹은 "보안환경분석", "정보보호시스템의 취약성 점검" 항목에 순위를 부여하고 있는 반면, 실무자 그룹은 "보안 API (Application Interfaces)의 설계와 관리", "보안모듈의 설계와 관리" 항목에 순위를 부여하고 있다.

설문 결과를 분석하면 정보보호시스템 개발자에게 필요한 기술을 분류하면 "보안기술", "정보기술", "해킹대처기술" 등이다. "정보보호시스템 설계"와 "시스템 구조 분석" 항목은 연구자 그룹과 실무자 그룹에서 각각 1위와 2위의 중요도를 보여주고 있다. 전체적으로 볼 때, 이 두 항목이 중요한 것으로 나타나고 있다. 보안기술과 관련된 다른 항목은 "기초 암호학 이해", "키 프로토콜의 설계 및 관리" 및 "암호 프로토콜의 설계"가 중요한 지식 및 기술 항목으로 식별되었고, 실무자 그룹과 연구자 그룹에서 중요한 순위를 차지하고 있다.

설문결과에서는 "암호적용 능력"의 중요성이 덜 강조되었지만, 델파이 참가자들은 설문지의 근거사유에서 "암호적용 능력"의 중요성을 지적하고 있다. "암호적용 능력"은 응용시스템과 암호를 통합하는 핵심기술이다[Buckley, 1995; Schneier, 1993]. 암호시스템의 성공적인 개발을 위해서는 정보보호시스템 개발자는 각 응용시스템과 암호의 특성을 알아야하고, 응용시스템에 따라 암호를 선택할 수 있어야 한다.

<표 4> 연구자 그룹의 정보보호시스템 개발자에게 필요한 지식 및 기술 설문 결과 분석

순위	지식 및 기술	총점	빈도	퍼센트 (%)
1	정보보호시스템 설계	309	27	96
2	시스템 구조 분석	254	25	89
3	기초 암호학 이해	244	21	75
4	네트워크 보안 프로토콜 이해	214	26	93
5	키 관리 및 설계	187	21	75
6	네트워크 프로토콜 이해	182	22	79
7	정보보호시스템 시험	179	22	79
8	시스템 프로그래밍	178	21	75
9	암호 프로토콜 설계	170	19	68
10	운영체제구조의 이해	170	19	68
11	암호적용 능력	154	17	61
12	보안환경 분석	151	19	54
13	인터넷 기술	117	17	57
14	정보보호시스템 취약성 분석	97	15	43
15	침입탐지 및 차단 관리	89	16	46

주) 전체 응답자 수: 28, 총점: 점수 합계, 최고점: 15, 최저점: 1, 빈도: 선택한 항목

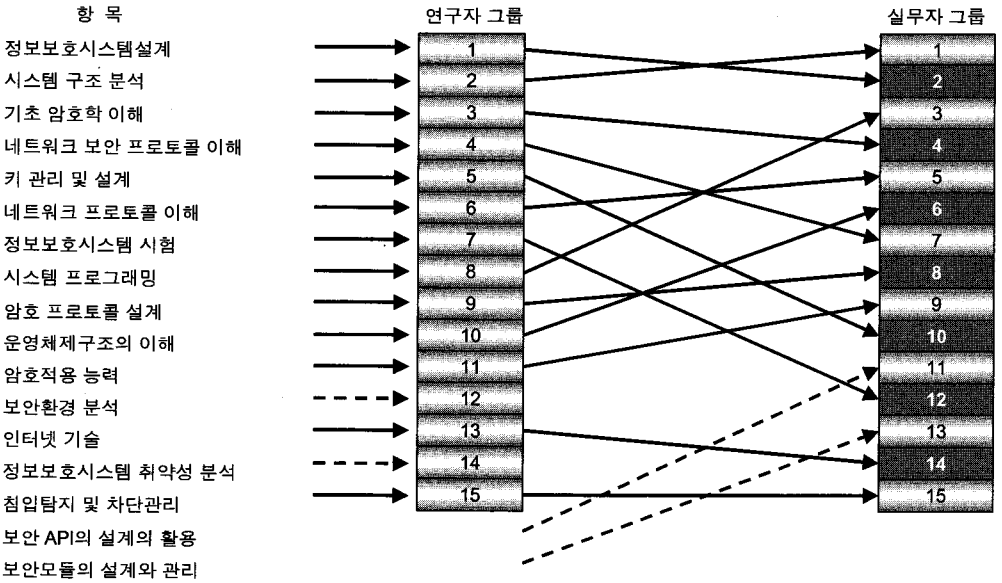
<표 5> 실무자 그룹의 정보보호관리자에게 필요한 지식 및 기술 설문 결과 분석

순위	지식 및 기술	총점	빈도	퍼센트 (%)
1	시스템 구조 분석	264	26	96
2	정보보호시스템 설계	258	26	96
3	시스템 프로그래밍	251	24	88
4	기초 암호학 이해	236	22	81
5	네트워크 프로토콜 이해	228	25	92
6	운영체제구조의 이해	198	23	85
7	네트워크 보안 프로토콜	186	22	81
8	암호 프로토콜	179	20	74
9	암호적용 능력	178	21	77
10	키 관리 및 설계	173	23	85
11	보안 API의 설계와 활용	154	21	77
12	정보보호시스템 시험	143	21	77
13	보안모듈의 설계와 관리	117	16	59
14	인터넷 기술	112	14	51
15	침입탐지 및 차단 관리	107	18	61

주) 전체 응답자 수: 27, 총점: 점수 합계, 최고점: 15, 최저점: 1, 빈도: 선택한 항목

실무자 그룹은 보안 API(Application Interfaces)와 보안모듈의 중요성을 지적하였다. 보안 API와 보안모듈은 실무자 그룹의 조사에서 각각 11위와 13위를 차지하였다. 이 항목은 정보보호시스템의 개발경향을 반영하고 있다. 정보보호시스템은 일반적으로 하드웨어 근간의 보안서비스를 제공하는 보안모듈과 응용시스템과 보안모듈을 연결해 주는 보안 API로 구성되어 있다 [Baskerville, 1993; NIST, 1994; Tryfonas, 2001]. 정보보호시스템 개발과정에서 정보보호시스템 개발자는 외부에서 만들어진 보안모듈을 주로 사용한다. 따라서 보안시스템의 효과적인 개발을 위해서는 시스템 개발자는 보안모듈과 응용시스템을 연결하는 보안 API를 적절하게 사용할 수 있어야 한다.

정보보호시스템 개발자의 지식 및 기술 항목 선정에 있어서 실무자 그룹과 연구자 그룹은 동일한 항목을 선정하였지만, 순위에 있어서 차이가 존재한다. <그림 2>는 순위의 차이를 나타내고 있다. 연구자 그룹은 보안기술을 정보보호시스템 개발자에게 있어서 중요하다고 판단하고



<그림 2> 정보보호시스템 개발자의 지식 및 기술 항목간의 순위 비교

있는 반면, 실무자 그룹은 정보기술을 더 중요하다고 판단하고 있다.

Ⅵ. 정보보호전문가의 지식 및 기술 분류

정보보호전문가 양성을 위한 교과과정 개발, 숙련도 측정, 체계적인 직무분석을 위해서는 도출된 지식과 기술을 체계적으로 분류할 필요가 있다. 체계적인 분류를 위해서는 특정한 분류기준이 필요하다. 정보보호전문가의 업무수행에 있어서 필요한 지식 및 기술 분류는 정보보호기술 분류 연구 결과를 활용하면 가능하다.

Armstrong은 정보보호기술을 일반적인 기술(generic skill), 정보보호기술(special skills)와 실제적인 기술(practical skills)로 구분하고 있다[Armstrong 2002]. 일반적인 기술은 문제해결능력(problem solving), 프로젝트 및 위험 관리기술(project and risk management), 변화관리(change management) 등으로 구성된다. 정보보호기술은 네트워크 및 통신보안기술(network & communication security), 데이터베이스 보안(database security), 인터넷 보안(internet security), 웹사이트관리(web site management) 등으로 구성된다. 실제적인 기술은 실제적인 프로젝트 관리 및 연구 관리를 실제적으로 수행할 수 있는 능력과 경험이며, 능력과 경험은 실제 프로젝트와 연구를 수행하거나 사례연구를 통해서 익힐 수 있다. 이 연구에서 제시하는 관리적인 지식 및 기술이 위주인 정보보호관리자의 지식 및 기술 분류에는 적합하지만, 정보보호기술을 대부분 필요로 하는 정보보호시스템 개발자의 지식 및 기술 분류에는 적합하지 않다.

Venter는 정보보호기술을 2가지 기준을 사용하여 분류하고 있다[Venter, 2003]. 첫째 기준은 정보보호의 시점, 즉 기술이 데이터와 정보자원과 상호작용을 하는 시점에 따라 능동적인 기술(proactive)과 반응적인(reactive) 기술로 분류하고 있다. 능동적이라는 의미는 침해가 발생하기 전에 데이터나 정보자원을 보호하기 위해서 특정한 정보보호기술을 이용하여 예방적인 조치를 취한다는 의미이다. 반응적이라는 의미는 정보침해가 발견되는 즉시 데이터나 정보자원을 보호하기 위해서 특정한 정보보호기술을 이용하여 대책을 취한다는 의미이다. 두 번째 기준은 능동적인 기술과 반응적인 기술이 적용이 되는 대상인 네트워크, 호스트, 어플리케이션 등이다. 네트워크 수준의 정보보호기술은 전화선이나 다른 수단을 이용하여 정보를 공유하기 위해서 연결된 컴퓨터 시스템상에 전송되는 데이터나 자원을 안전하게 전송하게 한다. 호스트 수준의 정보보호기술은 컴퓨터에 있는 데이터나 자원을 안전하게 유지하게 하는 기술이다. 어플리케이션 수준의 기술은 호스트에 있는 컴퓨터 프로그램과 관련된 데이터나 자원을 안전하게 유지하게 하는 기술이다. 이 분류체계는 정보보호기술 분류에 있어서 요소기술을 분류하는 데 유용하게 사용할 수 있지만, 관리적인 정보보호기술을 분류할 수 있는 기준으로는 협소한 단점이 있다.

국내에서는 김기현[김기현, 1998]은 A.J.Menezes 연구[Menezes, 1997], ISO/IEC 7498-2[ISO/IEC, 1989] 등의 연구를 토대로 정보보호기술을 정보보호기반기술, 시스템 및 네트워크 보안, 응용서비스 보안, 보안관리기술로 분류하고 있다. 정보보호기반기술은 암호 관련 기반기술, 시스템 관련 기반기술 등으로 구성된다. 암호관련 기반기술은 암호알고리즘 분석, 암호 프로토콜로 구성되고, 시스템 관련 기반기술은 인증 및 식별, 접근통제 등으로 구성된다. 시스템 및 네트워크 보호기술은 컴퓨터보호기술, 통신보호 및 TEMPEST, 네트워크보안기술 등으로 구성된다. 응용서비스 보안기술은 전자상거래, 정부서비스 보호, 교육서비스 등으로 구성된다. 보안관리기술은 키 관리, 네트워크 보안관리, 시스템 안전 감시 및 운영 관리 등으로 구성된다. 이 분류의 특징은 많은 정보보안기술을 포함시킬 수 있는 장점이 있

는 반면, 분류된 기술 요소들간의 중복성이 존재한다는 점이다.

정보보호관리자의 지식 및 기술 분류를 위해서는 Armstrong과 김기현이 제시한 분류체계가 Venter가 제시한 분류체계를 사용하는 것 보다 유용하다. 본 연구는 Armstrong과 김기현의 연구 결과를 채용하여 정보보호관리자의 지식 및 기술 분류 기준을 실제적인 기술, 정보보호기술, 정보보호관리기술로 분류한다.

정보보호시스템 개발자의 지식 및 기술 분류는 Venter가 제시한 분류체계를 사용하는 것이 유용하다. 그러나 Venter가 제시한 분류체계는 정보통신기술 등을 포함하지 않고 있어 정보통신기술을 포함시켜야 한다. 이 기준을 사용할 때는 다소 중복되는 기술이 존재할 수 있다. 정보통신기술을 분류기준으로 고려할 때, 정보시스템 개발자의 지식 및 기술을 분류하면 다음과 같다.

<표 6> 정보보호관리자의 지식 및 기술 분류

실제적인 기술	정보보호기술	정보보호관리 기술
관리적 정보보호대책 기술	정보시스템 평가	정보보호시스템의 취약성 분석
정보보호정책 수립	침입탐지와 차단기술	위험분석과 평가
관련 법률 및 규정	위험분석과 평가	보안환경 분석
보안감사	인터넷 기술	물리적인 보안대책 설계
정보보호교육 프로그램 관리	컴퓨터 바이러스 관리	정보보호표준
프라이버시와 윤리	해킹 대처	
	기초 암호학	

<표 7> 정보보호시스템 개발자의 지식 및 기술 분류

<table>
<tr><th colspan="3">능동적인 기술</th><th colspan="3">반응적인 기술</th><th rowspan="2">정보통신기술</th></tr>
<tr><th>네트워크 수준</th><th>호스트 수준</th><th>애플리케이션 수준</th><th>네트워크 수준</th><th>호스트 수준</th><th>애플리케이션 수준</th></tr>
<tr><td colspan="3">기초 암호학 이해</td><td colspan="2">침입탐지 및 차단</td><td></td><td>정보시스템 설계</td></tr>
<tr><td colspan="3">키 관리 및 설계</td><td colspan="2">해킹 대처</td><td></td><td>시스템 프로그래밍</td></tr>
<tr><td colspan="3">암호프로토콜 설계</td><td colspan="3">정보시스템 취약성 분석</td><td>운영체제구조</td></tr>
<tr><td colspan="3">암호적용 능력</td><td rowspan="7" colspan="3">네트워크 보안 프로토콜 이해</td><td>인터넷 기술</td></tr>
<tr><td colspan="3">보안환경 분석</td><td>정보보호시스템 시험</td></tr>
<tr><td colspan="3">보안 API 설계와 활용</td><td>시스템 구조 분석</td></tr>
<tr><td colspan="3">정보시스템 취약성 분석</td><td>네트워크 프로토콜</td></tr>
<tr><td colspan="2">보안모듈 설계, 관리</td><td></td><td rowspan="2"></td></tr>
<tr><td>네트워크 보안 프로토콜 이해</td><td></td><td></td></tr>
</table>

Ⅶ. 정보보호관리자와 정보보호시스템 개발자의 지식 및 기술의 유사점과 차이점

<표 2>, <표 3>과 <표 4>, <표 5>를 비교하면, 정보보호관리자와 정보보호시스템 개발자의 지식 및 기술이 확연히 다름을 발견할 수 있다. <표 2>와 <표 4>에서 공통적인 지식 및 기술 항목이 4개 존재하고, <표 3>와 <표 5>에서는 공통적인 지식 및 기술 항목이 2개 존재한다. 이 사실은 정보보호관리자와 정보보호시스템 개발자간의 교육과정의 구별이 필요함을 나타낸다. 정보보호관리자에게 필요한 교육과정은 정보보호기술에 대한 전반적인 이해와 관리적 이슈들을 포함할 수 있도록 개발되어야 한다. 정보보호시스템 개발자에게 필요한 교육과정은 기본적이며, 기술지향적인 능력을 향상시킬 수 있도록 개발되어야 한다.

Ⅷ. 결 론

이 연구는 정보보호전문가에게 필요한 지식 및 기술 항목을 식별 및 각 항목의 중요도 결정을 위해 정보보호산업 및 연구에 종사하는 전문가의 의견을 반영하는 델파이 방법을 사용하였다. 델파이 방법 적용의 신뢰성을 향상시키기 위해 응답자 집단을 연구자 그룹과 실무자 그룹으로 구분하여, 연구 결과를 상호 비교하여 신뢰성을 향상시킬 수 있었다.

본 연구는 델파이 방법을 사용하여 정보보호관리자와 정보보호시스템 개발자의 직무수행을 위해 필요한 가장 핵심적인 지식 및 기술 항목을 각각 15개씩 도출하고, 중요도 순위를 획득할 수 있었다. 연구결과 도출된 지식 및 기술의 체계적으로 사용할 수 있도록 국내외의 정보보호 기술분류 기준을 적용하여 정보보호관리자 및 정보보호시스템 개발자의 지식 및 기술을 분류하였다.

정보보호전문가가 참여한 델파이 방법에 의해 개발된 연구의 결과인 지식 및 기술 항목은 정보보호 교육과정 개발의 지침으로 사용할 수 있고, 조직의 정보보호전문가 양성과 획득 및 조직의 정보보호기술 개발을 위해 사용할 수 있다.

향후에는 본 연구의 결과인 도출된 지식 및 기술을 바탕으로 정보보호전문가의 양성시 지식 및 기술을 적용하는 과정을 보여주는 교육과정 적용 모형을 개발하는 연구를 수행할 필요가 있다.

〈참 고 문 헌〉

[1] 김기윤, 나현미, "정보보호관리자의 직무분석," *정보보호학회지*, 제10권 제4호, 2000, pp. 69-74.

[2] 김 철, "대학의 정보보호 교육과정 개발 연구," *정보보호학회지*, 제11권 제3호, 2001, pp.75-89.

[3] 인터넷침해대응지원센타, http://www.krcert.or.kr/upload/statistics/2003_12.pdf.

[4] 정보통신부, *정보보호 기술개발 5개년 계획*, 정보통신부 보고서, 2001.

[5] 한국정보보호진흥원, *정보보호 인력 수급 및 활용 방안 연구*, 한국정보보호진흥원 연구보고서, 1999.

[6] 한국정보보호진흥원, *주요 민간부분 정보보호실태 조사*, 보고서, 2001.

[7] 김기현 외, 3인, "정보보호기술분류," *정보보호학회지*, 제8권 제1호, 1998.

[8] Helen Armstrong, "Internet Security Management: A Joint Postgraduate Curriculum Design," *Journal of Information Systems Education*, Vol. 13, No. 3, 2002, pp. 249-258.

[9] Baskerville, R., "Information System Security Design Methods: Implication for Information Systems Development," *ACM Computing Surveys*, Vol. 5, No. 4, 1993, pp. 375-414.

[10] Buckley, C., "Delphi: Methodology for Preferences More than Predictions," *Library Management*, Vol.16, No.7, 1995, pp.16-19.

[11] Cooper, J.A., *Computer and Communication Security*, McGraw-Hill, New York, 1989

[12] DoD, *Department of Defense Directive S-3600.1 Information Operations(IO)*, US. Department of Defense, 1996.

[13] Michael R.G. and Kim, I.K., "An Undergraduate Business Information Security Course and Laboratory," *Journal of Information Systems Education*, Vol. 13, No. 3, 2002, pp. 189-196.

[14] Carol, H. and Backhouse, J., "Information Systems Security Education:Redressing the Balance of Theory and Practice," *Journal of Information Systems Education*, Vol. 13, No. 3, 2002, pp. 249-258.

[15] ISO/IEC 74982-2, *Information Processing Systems- OSI Basic Reference Model- Part2, Security Architecture*, 1989.

[16] Jung, B., et al., "Security Threat to Internet: a Korean Multi-Industry Investigation," *Information & Management*, Vol. 37, Issue 8, 2001, pp. 487-498.

[17] Kim, K.Y. and Surendran, K., "Information Security Management Curriculum Design: A Joint Industry and Academic Effort," *Journal of Information Systems Education*, Vol. 13, No. 3, 2002, pp. 227-236.

[18] Kim, S.H. and Choi, M.G., "Educational Requirement Analysis for Security Professionals in Korea," *Journal of Information Systems Education*, Vol. 13, No. 3, 2002, pp. 237-248.

[19] Patricia Y. Logan, "Crafting an Undergraduate Information Security Emphasis within Information Technology," *Journal of Information Systems Education*, Vol. 13, No. 3, 2002, pp. 177-182.

[20] Menezes, A.J., et al., *Handbook of Applied Cryptograpy*, CRC Press, 1997.

[21] Niederman, F., et al., "Information System Management Issues for the 1990s," *MIS Quarterly*, Vol. 17, No. 4, 1991, pp. 475-500.

[22] NIST, *Security Requirement for Cryptography Module*, NIST Standard, FIPS PUB 140-1, 1994.

[23] Palvis, P., et al., "An Expanded global Information Technology Issue Model: an Addition of Newly Industrialized Countries," *The Journal of Information Technology Management*, Vol. 6, No. 2, 1995, pp. 29-39.

[24] Schneier, B., *Applied Cryptography*, John Wiley & Sons INC., New York, 1993.

[25] Tryfonas, T., "Embedding Security Practices in Contemporary Information Systems Development Approaches," *Information Management & Computer Security*, Vol. 9, No. 4, 2001, pp. 183-197.

[26] Venter H.S. and Eloff, J.H.P., "A Taxonomy for Information Security Technologies," *Computer & Security*, Vol. 22, Issue 4, 2003, pp. 99-307.

[27] Wetherbe, J.C., et al., "Key Issues in Information System Management: 1994~1995 SIM Delphi Results," *MIS Quarterly*, Vol. 20, No. 2, 1996, pp. 225-242.

[28] Wilson, M., *An Introduction to Computer Security: The NIST Handbook*, NIST Special

Publication 800-16, 1998.

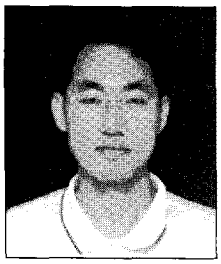
[29] Wood, C.C., "Shifting IS Security Responsibility from User Organizations to Vendor/Publisher Organizations," *Computers & Security*, Vol. 14, Issue 4, 1995, pp. 283-284.

[30] Wood, C.C., *How to Achieve a Clear Definition of Responsibilities for Information Security*, DATAPRO, Information Security Service, 1993.

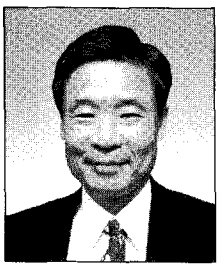
<부록 A>

지식 및 기술	
1. DB 보안기술 이해	21. 운영체제구조의 이해
2. E-Business 보안 기술 이해	22. 위험분석과 평가
3. 관련 법률 및 규정 이해	23. 의사소통기술
4. 관리적 정보보호대책 수립	24. 이동통신보안기술
5. 기초 암호학 이해	25. 인증서 관리
6. 네트워크 보안 프로토콜 이해	26. 인터넷 기술
7. 네트워크 프로토콜 이해	27. 정보보호교육 프로그램 관리
8. 물리적 보안대책 설계	28. 정보보호시스템 평가
9. 백업기술	29. 정보보호시스템의 취약성 분석
10. 보안감사	30. 정보보호정책 수립
11. 보안모듈의 설계와 관리	31. 정보보호컨설팅
12. 보안환경 분석	32. 정보보호표준에 대한 지식
13. 보안환경분석	33. 정보시스템 시험
14. 보안API의 설계와 활용	34. 정보시스템 설계
15. 스마트카드 보안 이해	35. 정보전 이해
16. 시스템 프로그래밍	36. 침입탐지와 차단관리
17. 시스템구조분석	37. 키 관리 및 설계
18. 암호 프로토콜 설계	38. 통신보안기술 이해
19. 암호 수학 이해	39. 프라이버시와 윤리
20. 암호적용 능력	40. 해킹대처

◆ 저자소개 ◆



최명길 (Choi, Myeonggil)
부산대학교 경영학과 및 동대학원을 졸업하고, KAIST 산업공학과에서 경영정보시스템 전공으로 박사학위를 취득하였다. 국방과학연구소(ADD) 연구원(1995~2000)을 거쳐 한국전자통신연구원(ETRI) 국가보안기술연구소(NSRI)에서 선임연구원으로 재직 중이다. 주요 관심분야는 워크플로우시스템, 전자상거래보안, 보안정책, 정보시스템 보안 평가, 보안관리 등이다.



김세헌 (Kim, Sehun)
서울대학교 물리학과를 졸업하고, Stanford University에서 경영과학전공으로 석사학위와 박사학위를 취득하였다. KAIST 산업공학과 교수로 재직 중이다. *IEEE Tans. on Vehicular Technology, Computer Networks, Telecommunication Systems, IEICE Transaction on Communication* 등 유명 저널에 다수의 논문을 게재하였고, 한국경영과학회, 한국정보보호학회 논문지 편집위원장 및 한국정보보호학회 학회장 등을 역임하였다.

◈ 이 논문은 2004년 7월 30일 접수하여 1차 수정을 거쳐 2004년 9월 24일 게재확정되었습니다.