사이버테러정보전 전문인력 양성 및 관리 방향에 대한 연구

권 문 택*

요 약

사이버테러정보전에 대비한 경쟁력 있는 전문인재 개발과 육성은 매우 중요한 과제인데도 불구하고 우리의 현실은 정보보호 전문 인력의 육성 필요성은 높이 인식하고 있기는 하나 실무 특기분야 위주의 인력운영과 정보보호 전문 인력 육성체계의 미비, 그리고 육성된 정보보호 전문 인력에 대한 체계적인 관리부족 등으로 육성 단계에서부터 활용에 이르기까지 매우 미흡한 실정이다. 본 연구에서는 이를 위한 해결방향으로서 정보보호 전문 인력의 육성 및 활용을 위한 발전방향을 크게 획득-양성-활용의 세 가지 차원으로 구분하여 무조건적인 양성이나 관리의 개념보다는 현행 체계를 재검토하여 필요로 하는 분야의 정보보호 전문 인력의 소요를 명확히 판단하여 체계적인 양성을 도모하고, 양성한 이후에는 조직의 목적에 합당하게 효과적으로 활용이 이루어질 수 있는 방안이 제시되었다.

A Study on Human Resource Management for Information Security in the Age of Information Warfare

Moon Taek Kwon*

ABSTRACT

This paper is about a study on human resource management for information security in the age of information warfare. this study reviewed the current status of human security resource forces for information warfare and derived problems of current practices of various organizations. Based on the analysis of the current practices the author suggested several ideas for solving the problems various. The suggestions include 1) establishment of security manpower concept, 2) set-up of manpower requirement, ideas, 3) establishment of systematic educational system, 4) standardization, etc.

Key words : Information Warfare, Human Security Resource Management

* 경희대학교 테크노경영대학원

1. 서 론

21세기 지식정보화 시대에서 국가 경쟁력은 지식과 정보가 좌우한다고 할 수 있다. 지식정보화 시대의 가장 큰 특징 중의 하나는 정보통신 기술 발전에 힘입어 정보의 공유를 통해 조직의 내부 효율성 증진과 전략적 활용을 통한 조직의 경쟁력 향상이라고 볼 수 있다. 그러나 이와 같은 순 기능이 있는 반면에 정보를 인터넷상에서 서로 공개, 공유하면서 원래의 의도와는 상관없이 정보자산에 대한 유출, 훼손, 변조 등 여러 가지 역 기능적인 문제들이 발생하게 되었고, 이제는 그 피해 정도가 사회, 국가적으로 심각한 수준에 이르는 단계에 와 있다. 이러한 문제들의 해결을 위해서는 정보보호에 대하여 각별한 관심을 가지고 체계적인 대책 수립이 필요하다.

최근 수년간 사이버 공간에서의 정보보호를 위하여 관련 기술 및 정책에 대한 연구에 많은 노력을 기울여 왔으나 가장 큰 문제점 중의 하나가 사이버테러정보전에 대비한 정보보호 분야의 기술, 정책에 대한 연구와 시스템 운영 및 교육, 그리고 실제 사이버테러정보전 공격행위가 발생했을 때 이를 무력화시킬 수 있는 전문 인력이 소요에 비하여 대단히 부족하다는 것이다. 이러한 결과가 초래 된 이유는 인터넷이라는 새로운 기술에 대하여 상업적 또는 공공적으로 활용하는 분야에는 많은 노력을 투자한 반면 역기능 요소인 사이버테러정보전에 대한 대응에는 상대적으로 관심을 덜 기울였기 때문이며 그 결과 현 시점에서 이 분야를 이끌어 갈 전문 인력이 대단히 부족하고 전문성도 매우 뒤 떨어지게 된 것이다.

정보보호 실태를 살펴 볼 때 국내의 정보보호 분야의 민간 업체는 대략 200여개가 넘고 업체에 종사하는 인력도 상당수에 달하고 있으나 실상은 소수의 몇 몇 전문 핵심 인력을 제외하고는 선진국 수준의 전문 인력이라고 하기에는 그 기술 수준이 매우 낮은 것이 사실이다. 이러한 문제점을 해소하기 위하여 국가정보원, 한국정보보호진흥원 등이 주관하여 교육과정을 개설하고 주기적인 교육을 실시하고는 있으나 체계적인 교육이 이루어지지 않고 있으며, 민간 대학에서의 전문 교육 체계도 실무에 활용하기에는 많은 문제점을 가지고 있다.

이러한 관점에서 본 소고에서는 국내에서 이루어지고 있는 사이버테러정보전에 대응하기 위한 전문 인력 양성현황을 살펴보고, 이러한 현황을 분석하여 문제점을 찾아내어 합리적인 인력 양성 방향을 제시하고자한다

2. 정보보호 조직, 인력 및 교육현황

2.1 정보보호 조직, 인력현황

사이버테러정보전에 대비하기 위해서는 전문적인 지식을 가진 정보보호 전문 인력과 이를 체계적으로 활용하기 위한 조직이 따라야한다. 현재 우리나라의 정보보호를 위한 전문 조직 운영 현황과 정보보호 전문 인력 현황을 국가 및 공공기관, 민간부문으로 나누어 살펴보면 다음과 같다(자료근거 : 2003 국가정보보호백서, 국정원).

(1) 조직 구성 현황

- 정보보호를 위한 공식적 조직을 편성하지 않은 기관 : 81%
- 전담인력은 보유하고 있으나 별도의 전담조직이 없는 기관 : 16%
- 전문 인력과 전담조직을 보유하고 있는 기관 : 3%

(2) 정보화인력 중 정보보호 전문인력 현황

- IT인력 대비 정보보호인력 20% 미만 : 70%
- IT인력 대비 정보보호인력 20% 이상 : 22%

- IT인력 대비 정보보호인력 30% 이상 : 5%
- IT인력 대비 정보보호인력 50% 이상 : 3%

상기 현황 자료를 살펴 볼 때 정보보호 전담 조직이나 인력을 보유하지 않고 있는 기관이 전체의 81%나 됨을 알 수 있고, 이는 매우 실망스런 결과가 아닐 수 없다. 또한 정보화업무를 담당하는 IT인력(정보화 인력)과 비교하여 볼 때도 정보보호 업무를 수행하는 전문 인력의 상대적 비율은 매우 부족한 실정임을 알 수 있다.

다음은 민간 부문에서의 정보보호 인력 운영 현황이다.

- 정보보호 조직 및 인력 없음 : 79%
- 정보보호 인력 별도 채용 안 함 : 19%
- 정보보호 인력 별도 채용 : 2%

상기 결과는 국내 40 여만 개의 기업에 대하여 조사한 결과로서 정보화에 대해서는 매우 많은 기업들이 참여하고 중요성을 인식하여 시스템을 도입하여 활용하고는 있으나 정보보호의 중요성을 인식하고 이에 대한 인력 확보 수준은 매우 낮다는 것을 보여주고 있다.

2.2 정보보호 교육현황

사이버테러정보전에 대비한 정보보호 전문 인력에 대한 교육은 크게 국가 및 공공기관주도로 시행되는 것과 대학을 비롯한 민간 교육기관에서 실시하는 것으로 대별해 볼 수 있다. 다음은 이 세 부문별로 진행되고 있는 교육 현황이다.

2.2.1 국가기관에서의 교육

(1) 국가정보원

국가정보원은 부설 교육기관인 국가정보대학원 내에 '사이버테러 대응 교육과정'을 개설하여 정규적인 교육을 실시하고 있으며 또한 각급기관의 요청에 의한 정보보안 특강 및 지방기관에 대한 정보보안설명회 등을 지속적으로 실시하고 있다. 국가정보대학원에서 실시하는 사이버테러 대응교육은 국가공공기관 보안담당자와 주요 정보통신 기반시설 관리기관의 보호책임자 등이 주요 대상이며, 필요에 따라 민간기관과 보호업체의 정보보호관계자도 참여하고 있다. 이 교육과정은 설치된 이후 2004년까지 총 33회에 걸쳐 행자부 등 정보기관의 정보보호 담당 관련자들에게 교육을 실시하여 많은 호응을 얻었으며 비교적 내용이나 커리큘럼이 충실하게 진행되고 있다는 평을 받고 있다. 이 과정의 주요 교육내용은 국가정보보호정책, 해킹사고조사 및 복구방법, 취약성 분석 및 평가, 공격대응기법, 정보보호시스템 운영관리 등 12개 분야로 구성되어 있다 <표 1>은 국정원 사이버테러 대응교육 과정이다

〈표 1〉 국정원 사이버테러 대응교육 과정

과 목	교육 내용
사이버전과 국가/공공기관의 역할	사이버전 관련 선진국 동향
	우리나라 실태 분석 및 역할
국가정보보안정책 및 관련법령	보안업무규정, 전자정부법, 기반보호법 등 보안관련 법령소개
	국가정보보안업무 중점 추진사항
최신정보보호기술 동향	암호 및 정보보호 학술대회 논문 해설
정보시스템 취약점 분석평가	정보시스템 취약성 분석 툴 소개 및 운영방법
해킹사고 분석 및 복구	해킹사고 사례소개
	운영체제별 로그분석 및 피해시스템 복구
사이버공격 대응기법	주요기반시설 공격기법 분석 및 응용
정보보호제품 도입 및 운영절차	정보보호제품 도입 및 운영
	정보보호제품 보안설정 기법

국정원은 상기 정규 교육과정에 추가하여 각급 국가 및 공공 기관의 교육 수요에 맞추어 상호 협의 하에 인터넷 시대에서의 정보보호에 대

한 보안교육을 실시하고 있으며 전국을 순회하며 정보보안설명회를 실시함으로써 교육기회를 제대로 가질 수 없는 지방 소재 국가 및 공공기관에 대한 교육을 수행하고 있다.

(2) 정보통신부

정보통신부도 매년 한국정보통신교육원에서 각급 정부 부처 정보화를 담당하고 있는 공무원들을 대상으로 정보보호 교육을 실시하고 있다. 이 교육과정은 관리자를 위한 일반과정과 실무자를 위한 심화과정 및 전문과정으로 구분하여 실시하고 있는데 2003년도부터는 일반대학생들과 민간 기업체에 종사하는 민간인들에게도 교육을 확대 실시하고 있다. 또한 정보보호에 대한 인식을 확산하고 경각심을 제고하기 위하여 대학생들에게는 보안업체를 방문하여 기술동향을 직접 확인 할 수 있는 기회를 제공하고 있으며, 전 국민에게 정보보호를 생활한다는 차원에서 정보보호, 정보윤리, 정보화 역기능에 대한 홍보활동도 강화하고 있다.

한국정보통신교육원은 지난 4년간의 총 201회의 교육을 실시하였으며, 년도별 인원은 2001년에 1,123명, 2002년에 1,212명, 2003년에 1,091명, 2004년에 876명으로서 총 4,302명이며, 이중에서 정부 기관 종사자에 대한 교육실적은 경찰청 267명, 검찰청 149명, 국방부 259명, 정통부 37명, 일반부처 164명이다.

(3) 국가보안기술연구소

국가보안기술연구소는 국정원의 산하 연구 기관의 역할을 하면서 다양한 교육을 실시하고 있다. 교육은 암호학, 정보전, 보안시스템(전산/통신보안) 등 정보보호 전문분야 별로 나누어 정부기관 종사자, 사용자, 제작업체 종사자 등에 대해 기초 정보보호 교육 실시 및 정보보호 마인드를 확산시키고 있는데 해마다 대략 700여명을 대상으로 교육을 실시하고 있으며, 정기적으로 세미나 또는 학술 대회를 개최하여 많은 관련 종사자들에게 포괄적인 기술 동향과 흐름을 전파하고 있다. 또한 국가공무원, 정보보안 담당 지방공무원들을 대상으로 사이버테러 시연회를 개최하는 등 정보보호의 실태와 대응방안에 대한 교육을 지속적으로 실시하고 있으며 전문적인 기술 연구도 겸하여 실시하고 있다.

(4) 한국정보보호진흥원

한국정보보호진흥원은 그 조직의 기본 임무에 맞추어 민간분야를 중점 대상으로 다양한 교육과정을 운용하고 있다. 교육과정은 최근의 전자상거래 활성화에 부응하기 위하여 주로 전자서명, 인증관리체계에 비중을 두고 진행되고 있으며, 교육과정은 실무 운영자과정, 개인정보보호 전문교육과정, 침해사고대응팀 구축 및 운영과정 그리고 대학원생 정보보호기술 교육과정으로 총 4개의 과정이 개설되어 있다. 최근 전문 교육실적 현황은 363명의 중소기업 서버관리자를 대상으로 한 해킹 및 바이러스 교육이었으며, 전자서명인증관리체계 운영자과정, CERT 추진단 교육과정 등 비 전문과정에 2,500여명을 단기간 교육으로 배출한 바 있다.

2.2.2 대학에서의 교육

인터넷의 빠른 정착에 따라 전자상거래 등 기업에서의 정보기술 활용이 활성화 되면서 정보보호 교육의 중요성이 인식한 대학에서도 관련 학과를 개설하기 시작하였다. 국내 대학 중에서 정보보호관련 학과를 최초로 개설한 대학은 지방에 소재한 중부대학교이다. 중부대학교는 1997년에 컴퓨터안전관리학과를 최초로 개설하였는데, 이후 2001년에 순천향대학교에서 정보보호학과를 개설하면서 지금 현재는 15개의 대학에 정보보호관련 학과가 개설되고 있다.

대학원의 경우에는 1998년 동국대학교 국제 대학원의 정보보호학과가 처음 개설되었으며, 2000

년에는 고려대학교 조치원 캠퍼스에 석/박사과정, 2001년에는 경기대학교의 정보보호기술공학과가 일반대학원에 개설이 되었고, 고려대학교 정보보호전문대학원이 개설되었다. 동시에 여러 대학의 특수대학원에서도 정보보호석사과정이 개설되었으며 기타 2년제 대학에서도 관련학과가 개설되기 시작하였다. <표 2>, <표 3>은 현재 정보보호 관련 학과를 개설하여 인력을 양성하고 있는 대학 및 대학원 현황이다(자료출처 : 2005 국가정보보호백서).

정보보호가 제대로 되지 않았을 경우에 직접적이며 그리고 금전적으로 가장 피해를 당하기 쉬운 부문은 바로 민간 부문이다. 특히 인터넷을 활용한 전자 상거래나 e-비즈니스 거래행위에 있어서 민간부문은 정보의 해킹, 바이러스 등에 취약하게 노출되기 쉽다. 그러나 이러한 역기능은 결과적으로 국가와 사회적으로 크나큰 피해로 확산 될 우려가 있으므로 국가기관에서도 정보보호교육과 보안홍보를 위해 노력하고 있으며, 민간기업체들도 스스로 교육시설을 개설하고 있

〈표 2〉 국내정보보호 학과 개설 4년제 대학

분류	대학명	학 과
대학	서울여대	정보보호학전공
	대전대학교	전산정보보호학
	서울여자대학교	정보보호공학
	순천향대학교	정보보호학과
	목포대	정보보호전공
	중부대학교	정보보호관리학
	세명대학교	정보보호학과
	호서 대학교	정보보호전공
	목원대학교	정보보호소학부
	대불대학교	정보보안공학부
	건양대	정보보호학과
	한국기술교대	정보보호학 전공
	대구한의대	전산정보보호학과
	영동대	인터넷 보안학과
	천안대	정보보호전공

〈표 3〉 국내정보보호 학과 개설 대학원

분류	대학명	학 과
대학원	동국대국제정보대학원	정보보호학과
	순천향대 산업정보대학원	정보보호 기술협동
	경기대 산업정보대학원	컴퓨터보안전공
	경기대 대학원	정보보호기술 협동
	고대 정보보호대학원	정보보호학과
	단국대 정보통신대학원	정보보호학과
	성균대 정보통신대학원	정보보호학과
	전남대 대학원	정보보호협동
	호서대 첨단정보기술대학원	정보보호 및 전자상거래
	목포대 대학원	정보보호기술협동
	부경대 대학원	정보보호협동
	순천향대 일반대학원	정보보호학과
	한경대 정보통신대학원	정보보안학과
	항공대 항공산업정보대학원	정보보호학과
	한서대 대학원	정보보호학과
	한세대 대학원	정보보호학과
	세종대 정보통신대학원	정보보호기술공학
	경북대 대학원	정보보호학과
	국민대 법무대학원	정보보안전공
	성균관대 일반대학원	KISA산학협동과정
	광운대 정보통신대학원	정보보호전공
	상명대 뉴미디어 정보통신대학원	컴퓨터 정보보호전공
	전북대 대학원	정보보호공학과
	한남대 정보산업대학원	정보보호학과

다. 이 중에서 몇몇 업체의 교육과정과 민간교육시설의 교육과정을 살펴본다면, 첫째 한국정보보호교육센터(KISEC)에서의 교육이다.

이 교육기관은 크게 장기전문가과정과 단기전문가과정 그리고 자격증과정을 개설하고 있는데, 장기전문가과정은 전반적인 정보보호기술과 해킹방어 그리고 컨설팅 과정 등 다양하게 구성되어 있고, 단기 전문가과정을 정보보호기술의 핵심부

분만 단기로 교육을 시키고 있다. 또한 자격증과정은 한국정보보호진흥원이 주관하는 국제공인자격증인 정보보호 전문가 자격증(Specialist Information Security : SIS)과 국제적인 자격증인 CISSP, CISA 등으로 나누어 자격증 획득을 위한 교육을 실시하고 있다.

두 번째 교육기관은 주식회사 해커스랩을 들 수 있는데 온라인 교육을 실시하고 있다. 이 교육기관은 일반인들도 쉽고 재미있게 접근할 수 있도록 시스템을 구성하고 있으며 시스템을 통해 해킹을 직접 해볼 수 있게 만들어 놓아 실무적인 체험을 할 기회를 제공하고 있다. 기타 삼성멀티캠퍼스, (주) 웨이브 코리아 아이엔씨, 현대정보기술, 사이버텍 홀딩스 등에서 정보보호 개론, 시스템, 해킹/보안, 네트워크 보안 등에 관한 교육을 실시하고 있다.

2.3 정보보호 전문가 자격

정보보호를 보장할 수 있는 전문가에 대한 자격 기준은 공인된 시험을 통해 획득한 자격증이 될 것이다. 따라서 정보보호에 대한 관심도가 높아지고, 정보통신기반보호법 제정 이후 주요정보기반시설에 대한 보안컨설팅업무가 활기를 띠면서 정보보호 분야에 자격증이 관심을 끌게 되고 자연히 이 분야에 대한 자격증 취득자가 증가하고 있는 실정이다. 현재 우리나라에 존재하는 정보보호 관련 자격증은 국가공인자격증, 민간자격증, 국제공인 자격증으로 크게 나누어 볼 수 있는데 이 자격증을 획득함으로써 전문가로서의 지위를 인정받기 위해 준비를 하는 지망생들도 증가하고 있다.

정보보호 자격증은 크게 국제공인 자격증, 우리나라 국가공인자격증 및 민간 자격증으로 구분 된다 국제공인 자격증은 국제적으로 인정받는 자격증으로서 국제 정보보호 컨소시엄인ISC (ISC : International Information Systems Security Certification Consortium)가 주관하는 CISSP (Certificated Information Systems Security Professional), SANS(System Administration, Networking, and Security) 연구소에서 시행하는 GIAC (Global Information Assurance Certification) 등 다양한 자격증이 있다. 이를 크게 세 가지로 나누면 ① 정보보호 전반에 대한 이론과 개념, ② 전문분야의 지식과 실무능력, ③ 특정제품의 관리 및 운용으로 구분 지어 볼 수 있다. 대표적으로 첫 번째에는 CISA(감사 및 통제), CCP(시스템 개발 및 운용보안), SNSCP(데이터 및 시스템 보호) 등이 해당되며, 두 번째에는 CCP(인명 및 재산보호), CBCP(재난 대비 및 복구), CCCI (컴퓨터 범죄 수사)등이, 세 번째에는 MCSE(마이크로소프트), CCIE(시스코) 등이 여기에 속한다. 이러한 다양한 자격증은 정보보호만을 목적으로 하는 자격증도 있지만 시스템 엔지니어링 등 IT전반에 걸친 다양한 부분을 포괄한다고 볼 수 있다.

국가공인자격증은 한국전산원에서 시행하는 정보시스템감리사가 있다. 이는 정보시스템 감리를 수행할 전문 인력의 확보와 정보시스템 감리 체계의 확립을 지원하며, 민간부문 정보시스템 감리의 활성화를 유도하기 위한 자격증으로서 시험과목으로는 필기전형에 프로젝트관리, 데이터베이스, 소프트웨어공학, 시스템구조(아키텍처 및 보안)가 있고 이론교육 및 현장실무교육 후 면접을 통해 자격증을 수여하는 제도로 구성 된다.

민간 정보보호전문가 자격으로서는 정보보안관리사, 정보보호전문가, 인터넷보안전문가 자격이 있다. 정보보안관리사는 정보통신(컴퓨터)자격관리협회에서 시행하는 것으로서 정보보안관리사(ISM) 1급과 2급이 있다. 이는 통신망에서 발생하는 각종 정보누출, 도청, 그리고 정보변조 등의 공격과 시스템에 가해지는 해킹 및 바이러스 기술 등의 다양한 전자적 침해에 대비하며, 인터넷과 전자상거래 상에서 개인 및 거래정보

의 안전하고 신뢰성 있는 전달을 보장하는 보안 전문가 자격이다. 이 자격증은 암호학에 바탕을 두고 운영체제, 시스템, 네트워크 상의 해킹 및 바이러스 기술 등의 다양한 전자적 침해에 대비하며, 인터넷과 전자상거래 상에서 개인 및 거래 정보의 안전을 보장하기 위해 개설하였으며 실기 시험을 통해 합격하면 소정의 자격증을 수여한다.

정보보호전문가 자격증은 한국정보보호진흥원과 한국정보통신대학원 대학교가 공동으로 시행하는 자격제도로서 1급과 2급이 있다. 이 제도는 체계적인 보안 전문 인력 양성을 목적으로 2002년에 처음 시행되었으며, 정보공유, 분석 센터의 기준 및 기준심사를 통해 정보통신부의 인정을 받는 자격증이다. 이 자격증의 시험과목은 시스템보안, 네트워크보안, 애플리케이션 보안, 정보보호론 4개 분야의 필기시험과 필기를 통과한 자에 대한 실기시험으로 구분된다.

인터넷보안전문가 자격증은 한국정보통신자격협회에서 주관하는 자격제도로서 서버를 보호하고 보안설정, 보안 분석, 해킹방지, 서버 복구 등 서버에 대한 해킹에 효과적으로 대처하고 정보를 보호할 수 있는 인터넷 보안 관련 기술력을 보장하기 위해 생긴 자격증이다. 시험과목은 정보보호개론, 운영체제, 네트워크, 보안, 시스템언어 5과목에 대한 필기전형 후에 시스템 보안관리, 시스템침해분석, 침입차단시스템구축 등의 실기시험을 통과하면 자격증을 수여 한다.

3. 정보보호 인력 현황 및 소요 전망

3.1 정보보호 인력 현황

3.1.1 정보보호 산업 인력 현황

국가정보원이 발간한 2005년도 정보화 백서에 의하면(<표 4> 참조) 2004년 11월 말 현재 정보보호 산업의 인력(정보보호 비관련직 제외)은 총 4,006명 정도인 것으로 추정되고 있으며, 이 중에서 정보보호 관련 연구 개발 인력은 2,164명으로 54%의 비중을 차지하고 있으며. 정보보호 관리직 인력은 924명으로 23%의 비중을 차지하고 있는 것으로 분석되고 있다. 또한 정보보호 영업직 인력은 386명으로 9.6%, 기타 정보보호 관련직 인력은 532명으로 13.2 % 비중을 차지하고 있다.

〈표 4〉 정보보호 산업 인력 현황

구 분	세부분류	인원수
정보보호 연구 및 개발직	암호 및 인증기술	696
	시스템 및 네트워크 기술	1,176
	응용기술 및 서비스	292
	소 계	2,164
정보보호 관리직	정보시스템 관리	688
	정보보호컨설팅	256
	소 계	924
정보보호 영업직	정보보호 마케팅	386
	소 계	386
기타정보보호 관리직	정보시스템 감리 및 인증	44
	정보보호 교육	28
	기 타	460
	소 계	532
전체 합계		4,006

정보보호 관련 연구 개발 인력의 경우, 시스템 및 네트워크 관련 인력이 1,176명으로 전체 인력의 29.3% 정도를 차지하고 있으며, 암호 및 인증기술 분야는 696명으로 전체 정보보호산업 인력의 17.3%를 차지하고 있는 것으로 분석되었다. 그러나 응용기술 및 서비스는 292명(7.2%)으로 상대적으로 낮은 것으로 분석되고 있다.

정보보호 관리직에는 시스템 관리 인력이 668명(전체 정보보호산업 인력의 16.6%)이고, 정보보호 컨설팅 인력은 256명으로 전체 정보보호 산업 인력의 6.3%를 차지하고 있는 것으로 분석되어 상대적으로 취약한 구조를 보여주고 있다.

기타 정보보호 관련직에서는 정보시스템 감리 및 인증 인력이 44명으로 파악되었고, 정보보호 교육 인력이 28명으로 전체 정보보보산업 인력 중 가장 적은 비중을 차지하고 있는 것으로 나타나고 있다.

3.1.2 전공별 정보보호산업 인력 현황

2004년 11월 말 현재 정보보호 산업 인력의 전공별 특성을 살펴보면 정보통신학과 및 관련 학과 전공자가 전체의 63.5%를 차지하고 있으며, 비 관련학과 전공자는 16.1%로 나타나고 있다. 또한 수학과와 통계학과 등 관련학과 전공자는 11.5%에 해당되며 순수 정보보호학 전공자는 8.9%로 분석되고 있다(<표 5> 참조).

〈표 5〉 정보보호산업 전공별 인력현황

구 분	전공별 인원
정보보호학과 전공자	356(8.9%)
수학과, 통계학과 등 관련학과 전공자	461(11.5%)
정보통신학과 및 관련학과 전공자	2,544(63.5%)
비 관련학과 전공자	645(16.1%)
합 계	4,006(100%)

3.1.3 수준별 정보보호산업 인력 현황

정보보호 산업 수준별 인력을 특급, 고급, 중급, 초급의 4단계로 나누어 살펴보면 <표 6>과 같다. <표 6>을 분석해 보면 초급인력이 1,769명으로 전체의 43.9%, 중급인력이 1,188명으로 29.6%을 차지하는 것으로 분석되고 있다. 고급인력은 745명으로 정보보호 산업 인력의 18.5%를 차지하고 있으며, 특급인력은 313명으로 7.8%를 차지하고 있다.

특급, 고급, 중급 인력 중 시스템 및 네트워크 기술 분야가 각각 109명, 229명, 376명 등 총 1,176명으로 상대적으로 높은 비율을 차지하고 있으며, 정보시스템 감리 및 인증분야와 정보보호 교육 인력은 각각 44명, 28명으로 상대적으로 매우 취약 한 것으로 분석되고 있다. 또한 컨설팅이나 정보시스템 감리 및 인증, 정보보호 교육 인력은 초급이나 중급의 인력보다 고급의 인력이 보다 많이 분포하고 있다.

〈표 6〉 수준별 정보보호산업 인력현황

세부분류	특급	고급	중급	초급	합계
암호 및 인증기술	52	116	171	357	696
시스템 및 네트워크기술	109	229	376	462	1,176
응용기술 및 서비스	17	75	99	101	292
정보보호시스템 관리	27	84	189	368	668
정보보호 컨설팅	21	81	68	86	256
정보보호 마케팅	45	89	125	127	386
정보시스템감리 및 인증	9	23	4	8	44
정보보호 교육	6	9	7	6	28
기 타	27	39	149	245	460
합 계	313	745	1,188	1,760	4,006

3.2 향후 정보보호 산업 인력 전망

<표 7>은 2003년도에 발간된 국가정보보호백서에 게재된 2007년도까지의 정보보호산업 기술인력 총 수요 전망이다. 이 자료에 의하면 정보보호연구 및 개발직 등 모든 분야에서 정보보호 관련 인력수요는 꾸준히 늘어 날 것으로 전망돼고 있다. 전체적으로 전망되는 총 수요 현황은 2006년에 4,455명, 2007년에는 4,779명으로 예상되는데 매년 12.3%의 증가를 예상하고 있다.

〈표 7〉 정보보호 산업 기술 인력 총 수요 전망

구 분	2006년	2007년
정보보호연구 및 개발직	2,546	2,684
정보보호관리직	1,814	1,992
기타 정보보호 관련직	95	103
소 계	4,455	4,779

이를 좀더 분석해 보면 정보보호연구 및 개발직위 인력수요는 2006년에 2,546명, 2007년에는 2,684명 정도 될 것으로 예상되며, 정보보호관리직의 수요는 2007년에 1,992명에 이를 전망이다.

4. 정보보호 전문인력 양성체계 문제점

미래의 국가, 공공기관 및 민간 부문에서의 경쟁력은 이미 주지하는 바와 같이 인터넷을 포함한 첨단정보전쟁으로 판가름 날 것이라는 것이 일반적인 예측이다. 이러한 미래 경쟁 환경을 전제로 할 때 현재의 우리나라의 정보보호 대응력은 매우 낮은 수준으로 평가되고 있다. 이는 여러 가지 요인 즉, 투자의 빈약, 조직구조의 취약 등에도 원인이 있겠으나 가장 중요한 요인 중의 하나는 정보보호 전문 인력의 획득, 육성, 활용이 체계적으로 이루어지지 않고 있다는 데 있는 것이다. 본 항에서는 전항에서 제시한 여러 가지 현황과 자료를 바탕으로 도출된 문제점을 종합하여 몇 가지 사항으로 나누어 정리하고자 한다. 특히 구체적인 사실관계에 의한 예를 들 때는 정부 및 민간부문 모두를 대상으로 할 수 없기 때문에 필자가 다년간 종사하였든 A사의 사례를 중심으로 예로 들었음을 밝혀둔다.

4.1 정보보호 전문 인력 개념, 분류의 모호성

일반적으로 정보보호 전문 인력은 "정보체계를 통해 정보를 생산하고 유통하여 이를 활용함으로서 국가 및 사회, 민간부문의 각 분야의 활동을 지원하는데 있어서 해킹, 바이러스 및 사이버 테러를 예방하고, 문제 발생시 이를 퇴치하기 위한 일련의 활동에 관련된 인력"으로 정의할 수 있다. 그러나 현재 이러한 포괄적인 용어에 의한 전문 인력 정의에 대해서 구체적인 기술 수준을 바탕으로 한 전문 인력 자격 기준이 각 기관마다 다르게 설정되어 있고, 더욱이 구체성이 결여되어 있어서 실제 통계상 또는 인사 운용상에서는 전문 인력과 그렇지 못한 인력이 구분되지 않고 집계되고 있는 실정이다. 따라서 그때 그 때 일반적인 정보화 인력 중에서 가용인력을 전문 인력이라고 분류하면서 보직 하는 경우가 많아 고도의 기술과 전문지식이 필요한 분야에 일반 정보화 인력이 보직되고 통계에 잡히는 경우가 비일 비재한 실정이다.

4.2 인력 적정 수준 소요 부족

이미 전항에서 언급한 바대로 정보보호 산업분야 기술 인력 중에서 가장 핵심이라 할 수 있는 분야는 정보보호 연구 및 개발직이다. 2003년도 국가정보보호백서 자료에 의하면 이 분야 소요 인력 증가율은 매년 평균 11.7%이다. 그러고 정보보호 관리직 및 기타 정보보호 관련직 소요 증가율도 대략 13% 내외로 분석되고 있다. 그러나 이 수치는 설문조사에 응한 기업이나 국가 및 공공기관의 수치이고 실제로는 이보다 숫자상으로는 대략 15% 정도는 더 잡아야 할 것 이라는 것이 학계의 일반적인 추정이다. 따라서 이러한 소요를 충족시킬 수 있는 정도의 전문 인력이 꾸준히 양성하여야 할 것이다. 특히 정보보호연구 및 개발직 인력이 2007년도에는 최소 약 2,700여 명이 필요할 것으로 예측 되는 바 2004년 말 현재 현재의 2,100여 명의 인력으로는 턱없이 부족한 실정이다.

더욱이 이는 2004년 말 현재 직위 소요로 책정된 인원이므로 5년 후 소요 예측치가 어떻게 증가 할지는 정확히 가늠하기가 어려운 실정으로서 전문 인력 부족은 더욱 심화 될 것으로 판단된다. 따라서 현 시점에서는 정보보호 전문 인력에 큰 문제가 없는 듯 보이나 이는 직위 소요가 과소 책정된데 기인하므로 직위 소요 재검토와 이에 따른 획득 방안이 마련되어야 할 것이다.

그리고 이러한 부족현상은 정보보호 관리직이나 기타 정보보호 관련직 보다는 정보보호연구 및 개발직에서 더욱 심화 될 것으로 판단되는데 이를 위한 시급한 대책이 필요하다. 그 이유는 전문화 된 분야일수록 단 기간 내에 양성이 불가능하고 최소 5년 이상의 교육과 실무부서 근무경력이 필요하기 때문에 부족한 인력을 단기간 내에 보충할 수가 없기 때문이다.

4.3 정보보호 전문인력 양성과정 문제점

4.3.1 양성 인력에 대한 부정확한 소요제기

모든 인력관리의 시발점은 소요제기부터 시작된다. 국방부의 예를 들어 현행 정보보호 인력 소요체계를 보면 각 군 별로 매년 다음해에 교육시킬 국내외의 위탁교육수요를 해당특기분야 참모부 및 부대별로 종합하여 인사참모부에서 종합하여 결정하고 있다. 그러나 교육 소요 제기 과정을 보면 현재 해당분야에서 필요로 하는 정보보호 인력이 어느 정도이며 대상자를 선발하여 어떠한 분야에 교육을 받도록 하고, 교육 이수 후 활용은 어떻게 할 것 인지와 몇 년 활용 후 진출은 어떻게 할 것인지, 후임자의 획득을 어떻게 할 것인지 등 활용기준계획이 모호한 상태에서 교육계획을 수립하고 있는 실정이다. 또한 정보보호 전문 인력직위 자체가 각 부서별로 판단기준이 상이하여 명확히 설정되어 있지 않음으로 인하여 장기적인 안목의 종합적인 계획 수립이 곤란한 실정이다.

4.3.2 신기술에 대한 보수 교육체계 미흡

정보보호 분야의 기술 진보는 다른 분야보다도 더욱 빠른 추세로 변하고 있다. 따라서 정보보호에 대한 신기술 보수교육이 어느 분야보다도 더욱 시급하다. 보수교육이란 의미는 정규교육에서 미진한 부분을 보완하고 변화하는 기술추세를 그때그때 따라잡기 위해 실시하는 것이다.

그러나 현재 운영되고 있는 정보보호 보수교육체계는 정보보호 전문 인력 보수교육체계로서는 전문성 있는 내용 면에서나 커리큘럼의 일관성면에서 미흡한 실정이고 더욱이 각 교육기관별로 독자적인 의사결정체계로 운영되고 있기 때문에 교육과정이 상이하고, 이로 인해 체계적이고 균형 있는 정보보호 교육이 미흡한 실정이다.

4.4 보직 및 승진관리 소홀

보직 및 승진은 모든 조직에서 인력을 지탱하는 요체며 기둥역할을 하고 있다. 인사가 만사라는 말이 있듯이 이 부분은 다른 어떤 분야보다 중요하게 다루어야 할 것이다. 특히 대규모 정부조직에 있어서는 전문 인력을 효과적으로 활용할 수 있는 인사관리제도가 대단히 중요하다. 즉, 경력보직관리 및 승진제도 등이 미흡하면 아무리 좋은 교육을 받은 우수한 인재라도 제대로 활용되지 못하고 도태되고 말기 때문이다.

예를 들면 국방 분야의 경우 교육 및 보직 관리면에 있어서 선 교육, 후 활용이 인사관리의 원칙이지만 정보보호 분야 위탁교육 후 해당 활용 부서에 보직이 되지 않거나 승진 등 인사상 불이익을 받거나 이에 대한 적절한 보상이 이루어지지 않아 교육의 실효를 거두지 못하고 있는 실정이다.

5. 정보보호 전문인력 양성 및 활용체계 발전 방향

5.1 발전방향에 대한 전제

전항에서 기술한 여러 가지 문제점을 해소하기 위한 발전방안은 단순히 기술적, 관리적 측면에서만 접근하면 아니 될 것이다. 개념정립, 인력획득, 양성 및 배치와 활용 등 관리체계는 시스템적 접근법에 의하여 관련 요소들을 두루 살

펴보면서 동시에 앞으로 전개될 사이버테러정보전 양상과 기술변화 등등을 면밀히 검토하여 수립하여야 한다. 그리고 정보보호선진국의 동향을 파악하여 벤치마킹을 하고, 또한 대기업 등 민간기업의 정보기술 활용 현황 등도 함께 고려하여 실현가능성 있는 방안이 되어야 할 것이다

그리고 각 방안은 국가 정보화 발전방향과 전문 인력 양성 및 관리체계, 그리고 교육을 맡은 각 급 기관 및 민간부문이 상호 유기적인 관계를 맺어 통합적인 커리큘럼 하에 추진이 되어야 할 것이다.

5.2 정보보호 인력 양성체계 발전방향

5.2.1 정보보호 인력 개념 재정립

21세기 지식 정보화 시대에서 '정보우위'를 확보할 수 있는 '정보보호 인력' 양성을 위해서는 우선 정보보호 인력에 대한 개념 정립이 필요하다. 정보보호 인력 개념이 현재는 정보화 종사자 또는 정보통신 전문가로만 인식하고 있어 대부분의 조직이나 기관 또는 민간부문에서 마치 정보보호 인력은 곧 하드웨어, 소프트웨어 등 일반적인 정보화 전문 인력으로 인식하고 있는 실정이다.

이는 다양한 정보기술 영역에 대한 인식과 개념이 부족한데 기인하며 또한 정보보호 정책. 정보보호 사업계획 수립의 중요성을 간과한 결과이다. 이로 인하여 정보보호정책, 사업계획 수립을 위한 전문 인력의 양성 계획이 없어 대부분의 조직에서 정보보호에 대한 구체적인 정책과 계획수립이 미흡하고 이로 인하여 정보보호 기술 발전 및 활용에 걸림돌이 되고 있는 실정이다.

5.2.2 전문 인력 소요획득체계 정립

아날로그 시대에서 디지털 시대로 패러다임으로 바뀌면서 인재가 조직의 성장과 경쟁력을 결정하는 핵심요소로 부각되고 있으며, 나아가 향후에는 "5%의 우수인재가 95%의 종업원을 선도하고 먹여 살린다"라고 한다. 인터넷 디지털 사회에서 정보기술 활용이 원활하게 이루어지려면 소수의 정예인력, 바로 정보보호 전문 인력이 그러한 역할을 수행하게 될 것으로 예측되고 있기 때문에 우수자원을 확보 하여야 한다.

정보보호 분야 전문 인력은 일반 정보화 분야 인력에 비해서 심도 깊은 전문지식을 요구하고 업무수행 결과가 즉각적이고 광범위하게 파급되기 때문에 각급 정부 기관이나 공공기관, 그리고 민간부문에서 인력을 선발할 때 대학전공 및 성적, 경력과 함께 논리력, 판단력 등 기본 자질 등을 고려하여 선발해야 한다.

따라서 정보보호 분야에서 가장 전문성이 높은 정보보호 연구 및 개발직은 대학 때부터 체계적인 선발 및 교육이 이루어져야 하며 기타 정보화 관련직은 가급적 어느 정도 하드웨어, 소프트웨어 등 정보화 분야에서 실무 경력을 이수한 경력자를 선발하도록 하는 것이 적절할 것으로 판단된다. 특히 대규모 정부 조직은 특기별 인사관리를 실시함으로써, 해당분야의 전문성을 유지하고 있는 실정인데 이를 정보보호 분야에도 적용하여 정보보호 분야 특기를 부여하고 임용 이후부터 특기 전문성 분야에 반복 보직하여 정보보호 전문기술을 지속적으로 함양해 가도록 관리가 되어야 할 것이다.

한 가지 국방부의 사례를 들어 예를 든다면 다음과 같다. 현재 국방부 내 정보보호 전문 인력의 획득 소요 산출은 국방부의 지침 아래 각 부, 감실 또는 단위부대장이 소요를 제기하여 종합하는 누적적 인력계획 과정을 채택함으로써 군 전체 차원에서 거시적이고 장기적인 전문 인력 수급 계획을 수립하지 못하고 있다. 왜냐하면 정보보호 소요 인력에 대한 파악이 될 시점에서 각급부대의 책임자에 따라 일정한 기준이 없이 그 때 그 때 소요를 제기하기 때문이다.

이러한 문제점을 해소하기 위해서는 정보보호 인력이 장차 사이버테러정보전하에서 국방 경쟁

력을 좌우 한다는 인식하에 국방부 본부의 조정 통제 아래 보다 체계적으로 각 군 본부의 정보보호 인력 수급계획이 이루어져야 할 것이다. 또한 계획 수립시 현재의 직위수요만이 아니라 보직, 진급, 전역시기 등을 고려하여 장기적인 인력수급계획 이루어져야 할 것이다.

5.2.3 전문 인력 양성 체계 정립

정부 조직과 같은 대규모 조직에 근무하는 정보보호 분야의 종사자들에 대한 전문성 계발을 지속적으로 지원하기 위해서는 단계별로 경력계획을 수립하여 경력을 관리하여야 한다. 경력계획은 인력수급계획, 직무분석, 교육훈련, 보직관리, 그리고 근무평정 등 일련의 인사관리 과정과 밀접한 관련을 맺고 있다. 이 분야 발전 방향을 제시함에 있어서 국방부 정보보호 전문 인력에 대한 예를 활용하여 설명하겠다.

(1) 교육과정의 체계화

국방부에서는 정보보호 전문 인력을 양성하기 위해서 국내외 민간대학 학위과정, 군내 보수교육과정, 그리고 민간 교육기관 연수를 통한 전문교육을 실시하고 있으며, 군내 전문교육기관으로 국방대학교 석사과정이 있다. 그러나 교육과정의 다양성에 비하여 교육과정간의 커리큘럼 등 세부적인 내용물에 있어서는 체계화가 되어 있지 않고 단절된 것이 현실이다. 더욱이 전공분야에 대한 선택이 자유로 와서 비교적 인기가 없는 정보보호 분야 전공자가 소요에 비하여 턱 없이 모자란 형편이다. 이러한 점을 감안하여 볼 때 전문 인력의 교육 후 활용도를 높이기 위해서는 군내 및 군외 교육기관에서 전문교육을 실시하되, 전공 및 보수교육과정에 대한 활용분야와 연계성을 높이기 위해서는 교육과정의 일관성 있는 체계가 정립되어야 하고 개인별 특기분야와 부합된 전공분야를 선택하여 학위교육을 이수할 수 있도록 규정화하여 하여야 한다.

또한 사전 교육 입교시 활용부서장에게 교육주제와 연구방향을 보고 후에 승인이 이루어질 수 있도록 하여야 하고, 해당 활용부서장은 당면해 있는 분야에서 요구되는 발전사항을 사전에 제시하여 충분히 연구 검토가 이루어지도록 조치하여야 한다. 이때 각 군의 인사참모부는 상기 취지대로 위탁교육의 이행이 제대로 이루어지고 있는지 반복적으로 확인감독 할 책임을 질 수 있도록 하여야한다.

이와 더불어 현재 군과 학계의 제휴 일환으로 국방대학교와 민간대학 간 학점교류가 실시되고 있는바 상호간의 실질적인 교류를 추진한다면 군사부문 또는 민간부문에 있어 교육간 미흡한 부분을 보완할 수 있을 것이며, 이를 통하여 국방의 정보보호 전문 인력의 개발목적에 부합될 수 있는 방향이 정립될 수 있을 것이다.

(2) 표준화된 양성 및 보수교육체계 확립

정보보호 인력의 양성에 있어서 표준화된 교육체계 확립이 시급히 요망된다. 현재 각 교육기관별 정보보호에 관한 교육과정 및 교육내용이 상이하여, 국가차원에서 볼 때 정보보호균형 발전을 위한 양성 교육 과정의 표준화가 시급히 요구되고 있다. 현재는 단계(과정)별 정보보호 교육내용의 방향성 설정 미흡으로 임무 수행에 맞는 정보보호 능력 배양이 곤란하다. 특히 국방부문의 예를 든다면, 각 군의 초군반 및 고군반 교육내용이 상이하여 장차 상위 계급에 진출하여 보다 차원 높은 직무를 수행시에 여러 가지 부작용이 우려된다. 이에 대한 발전방향은 국방부의 경우 각 군 군내 양성 교육 과정의 표준화를 달성하고 단계별, 과정별 목표에 부합하는 교육내용 설정을 하여야 할 것이다.

또한 현재 정부 각 부처에서 자체적으로 실시하고 있는 정보보호 전문 인력을 위한 보수교육과정의 수준은 매우 미약하여 새로운 정보보호 기술 습득에 심각한 제한을 받고 있는 실정이다.

이로 인해 새로운 사이버테러정보전에 대한 대응책이 적기에 수립되거나 대응하기가 곤란하고, 또한 정보보호 전문 인력 전부를 대상으로 신기술 습득을 위한 실무위탁교육을 실시할 경우 비용 과다 지출이 예상되고 있다.

따라서 이의 개선방향으로서 현재 국내에 운영되고 있는 정보보호 양성 및 보수교육 기관간에 커리큘럼과 과정에 대한 체계를 정립하여 교육업무를 분장하여 특화시키고, 정부 부처 및 민간 부문의 정예요원을 선발하여 전문 교육기관에 신기술 습득을 위한 실무위탁교육과 연수교육 기회를 확대하여야 할 것이다. 그리고 각 부문별로 정예 요원이 교육을 받은 후 여기에서 습득한 신기술을 전파하기 위해 필요시 각 기관 및 부처별로 자체 정보보호 전문 인력 보수교육 과정을 신설할 필요가 있다.

5.3 정보보호 전문인력 활용체계

아무리 우수한 인재라도 적재적소에 활용하지 않으면 그 효과는 반감 될 것이다. 이런 맥락에서 볼 때 정보보호 전문 인력의 효과적인 활용은 장차 우수자원을 전문 인력으로 확보하는데 결정적인 영향을 미치게 된다. 이와 같이 중요한 의미를 갖는 정보보호 전문 인력활용의 성패는 전문교육을 이수시켜 관련 전문직위에 보직하는 것으로 끝나는 것이 아니라 잠재역량을 최대로 발휘할 수 있는 여건을 조성해주고, 인센티브를 부여함으로써 정보보호전문가로서의 맡은 바 역할에 최선을 다하도록 동기 부여시키는데 달려 있다고 하겠다.

5.3.1 전문 인력 장기보직 활용체계 확립

정보보호 전문 인력의 경우에는 이론과 실무를 겸비한 핵심 정보보호 인력으로 육성, 관리하여야 하기 때문에 유사분야에서 장기 보직되어야 할 것이다. 정부 각 부처 및 공공기관은 전문인력을 정보보호 전문분야에 장기 활용하도록 하기 위하여 기본적으로는 해당 특기 실무분야의 실무부서 직위를 편제화하고, 주기적으로 전문성 계발 및 학문적 성과 접목 등을 위해서 각 종 교육기관에서 교육을 받을 수 있도록 배려를 하여야 한다. 이렇게 함으로써 전문교육과정에서 습득한 지식을 자신의 것으로 소화할 수 있는 기회를 제공하게 됨은 물론 전문성 계발을 촉진하고 실무 보직 경험을 통하여 정보보호 전문 인력이 되었을 때 사이버테러정보전에 대응할 수 있는 능력이 획기적으로 향상 될 수 있을 것이다.

그러나 어느 정도 경력이 진행 된 이후에는 정보보호관리직 또는 관련직으로 보임하여 정책직위도 경험하도록 순환부임 하도록 함으로써 정책 수립시 관계 특기분야에 대한 폭넓은 지식과 경험을 바탕으로 체계적이고 합리적인 의사결정을 할 수 있도록 하여야 한다.

5.3.2 직무분석을 통한 적재적소 배치

정보보호 전문 인력의 잠재 능력 활용을 극대화하기 위해서는 장기 보직에 더하여 적절한 부서와 직위에 보직되어야 한다. 정보보호 전문 인력을 어떠한 곳에 보직해도 업무는 수행하겠지만 업무의 내용이나 수준이 적절하지 않거나 전문성을 발휘할 수 있는 여건이 조성되어 있지 않는 직위 또는 부서에 배치한다면 국가 차원에서는 고급인력의 낭비를 초래하게 되고 개인적 차원에서는 잠재능력을 최대로 발휘하지 못함으로써 사기저하는 물론이고 조기퇴직의 동기를 제공하게 될 것이다.

따라서 정부 기관 등 대규모 조직은 정보보호 전문 인력직위에 대하여 직무분석을 실시하여 적절한 배치가 이루어지도록 하여야 할 것이다. 예컨대 정부 등 대규모 조직에서는 과거에 인력수급계획의 잘못으로 고급 정보보호 기술 교육을 이수하고도 적절한 직위에 대한 소요가 없어 일반 직위 또는 교육과 일치되지 않는 직위에

보임된 사례가 자주 발생한 사례가 있는데 이는 잠재역량을 최대로 발휘할 수 있는 보직 체계가 제대로 정립되어 있지 않았기 때문이다.

5.3.3 보상체계의 개선

자본주의 사회에서는 인간을 움직이는 힘의 원천 중에 하나가 승진과 금전적 보상이다. 따라서 아무리 정보보호 전문 인력의 활용을 위해서 제도적 장치가 잘 마련되어 있다 하더라도 적절한 보상이 주어지지 않는다면 자신의 잠재능력을 최대로 발휘하지 않음으로써 높은 성과를 기대할 수 없게 된다. 이러한 맥락에서 적절한 승진 및 보수체계는 정보보호 전문 인력의 능력과 노력에 상응한 사회적 형평성을 유지하게 하고 우수인재의 조기 퇴직을 방지할 뿐만 아니라, 정보보호 연구 활동에 대한 인센티브를 적용함으로써 연구활동을 활성화시키는데 기여할 수 있을 것이다.

대부분의 민간 조직에서는 우수 인재를 획득하여 유지하고, 동기부여를 통해 효과적으로 활용하기 위하여 다양한 인센티브를 개발하고 있지만 가장 대표적인 인센티브 제공방법은 승진이나 보수 일 것이다. 여기에서는 국방부문의 예를 들어 한 가지 방안을 제시하고자 한다. 군에서는 승진이 가장 큰 업무 성과에 대한 보상이다. 그러나 직위 소요의 제한 때문에 승진이 어려운 분야, 예를 들면 군 교수에게는 교수 수당을 별도로 지급하고 있다. 예컨대, 사관학교 교수요원의 경우 연구 활동 지원을 위하여 교수수당과 연구조성비를 지급하여 진급지연과 미 진급에 대한 보상을 하고 있다. 따라서 국방부의 경우 정보보호 전문 인력에 대하여 해당직위에 부합하는 인센티브를 차등 지급하여야 하겠으며, 또한 매년 각종 연구결과물을 토대로 일정수준의 연구수당을 별도로 책정하고 지급하는 방안을 강구하여야 하겠다. 이러한 수당을 신설함에 있어서 단순히 수당개념의 고정액을 산정하는 것이 아니라 경력과 연구물을 명확히 판단하여 보다 현실적이고 직접적인 수당 지급의 현실화를 이루어야하겠다.

5.3.4 CEO의 인식전환과 지속적인 관심

정보보호 인력을 실무적인 차원에서 아무리 체계적으로 양성하고 활용하려고 해도 조직에서의 최고경영자가 관심을 가지고 있지 않으면 결국은 큰 성과를 보지 못할 것이다. 왜냐하면 인간이 어떠한 조직에서 경력을 쌓아가면서 업무를 수행 할 때 가장 관심을 갖는 것 중에 하나가 그 조직에서 중요한 인재로서 인정을 받고 싶어하는 것이다. 따라서 업무 특성상 별로 외부에 나타나지 않는 정보보호 업무를 수행함에 있어서 조직의 경영진들이 관심을 갖지 않고 등한시한다면 전문 인력으로서 계속적인 실력 배양과 경력을 쌓아가려 하지 않을 것이다. 이러한 관점에서 조직의 최고경영자가 정보보호 업무를 중요하게 인식하는 자세가 필요하며 지속적인 관심을 가지고 양성, 보직 및 승진 등에 배려를 하여야 할 것이다

6. 결 론

본 연구보고서는 정보보호 전문 인력에 대한 획득-양성-활용이라는 전체 과정 속에서 전문 인력을 어떻게 양성 및 관리 할 것인가에 대한 방향에 초점을 맞추어 연구하였다.

선진 각국들은 나름대로 정보기술을 효과적으로 활용하고 사이버테러정보전에 대비하여 정보보호 전문 인력을 확보하고 유용하게 활용하기 위해 많은 노력을 기울이고 있다. 즉, '경쟁력 있는 정보보호 전문인재 개발과 육성'을 그들 전략 중심의 한 축에 두고 있는 추세이다. 따라서 우리나라도 우선 정보보호 전문 인재 획득 및 양성의 원칙을 나름대로 분명히 설정하여 조직적이며, 체계적으로 양성하고 확보할 필요가 있다

하겠다.

그러나 우리의 현실은 정보보호 전문 인력의 육성 필요성은 높이 인식하고 있기는 하나 실무 특기분야 위주의 인력운영과 정보보호 전문 인력 육성체계의 미비, 그리고 육성된 정보보호 전문 인력에 대한 체계적인 관리부족 등으로 육성 단계에서부터 활용에 이르기까지 매우 미흡한 실정이다.

이를 위한 해결방향으로서 본 연구에서는 정보보호 전문 인력의 육성 및 활용을 위한 발전 방향을 크게 획득-양성-활용의 세 가지 차원으로 구분하여 제시하였다. 여기서 제시한 일부 발전 방향들은 학문적 연구 차원이 가미된 이상적인 방안이 될 수도 있겠으나 정보보호 경쟁력을 발전시키기 위해서는 무조건적인 양성이나 관리의 거념보다는 현행 체계를 재검토하여 필요로 하는 분야의 정보보호 전문 인력의 소요를 명확히 판단하여 체계적인 양성을 도모하고, 양성한 이후에는 조직의 목적에 합당하게 효과적으로 활용이 이루어질 수 있도록 최대한 노력하여야 할 것이다.

참 고 문 헌

[1] Dessler, G., Human Resource Management(8th), Prentice Hall International Inc., 2000.

[2] Russ, C. F. Jr., "Manpower Planning System : Part I", Personnel Journal, Vol. 61, pp 35-45, Jan. 1982.

[3] 국정원, 2003 국가정보보호 백서, 2003.

[4] 국정원, 2005 국가정보보호 백서, 2005.

[5] 권문택, "국방정보화 전문인력 양성 및 확보 방안 연구", 국방연구과제 보고서, 2001.

[6] 김종훈 외, "국가 주요기반 구조 보호를 위한 정보전 대응체계 연구", WISE 99호, 1999.

[7] 남길현, "한국의 정보보호 현황", 제3회 해킹 방지 워크샵, 2000.

[8] 안성일, "보통신기반보호를 위한 법, 제도 정비방안", SIS, 2000.

[9] 최광표 외, "국방전문인력 육성 및 관리방안 연구", 한국국방연구원, 2000.

[10] 한재민, '경영정보시스템', 학현사, 2001.

권 문 택

1970년 육군사관학교(이학사)
1981년 미국 University of Iowa(공학석사)
1987년 University of Wisconsin (경영정보학박사)
경희대학교 테크노경영대학원 종신교수
경희대학교 정보처리처장
경희사이버대학교 학장