Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.3, Jun. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.3.769

공공분야 정보보안 역량 강화를 위한 단기 교육과정 연구*

윤 주 범†‡
세종대학교 정보보호학과

A Study on the Short Term Curriculum for Strengthening Information Security Capability in Public Sector*

Joobeom Yun†‡
Department of Computer and Information Security, Sejong University

요 약

최근 사이버공격은 국경을 초월하여 국가의 사이버 공간을 지속적으로 위협하고 있다. 이런 사이버공격은 국가 주요 기반시설을 마비시킬 수 있는 수준으로 지능화·고도화되는 양상을 보여주고 있다. 이런 사실은 원전 해킹 위협, 3·20 사이버테러 등의 사건에서 잘 볼 수 있다. 특히 국가 중요 정보가 존재하는 국가·공공기관에서는 이와 같은 사이버공격으로 대규모 피해가 예상되기 때문에 사전예방이 중요하다. 기술적인 대응도 중요하지만 국가·공공기관 근무자에게 사이버보안 교육을 통해 사이버 보안의식 고취 및 보안 전문지식 향상을 통해 보안 수준을 높이는 것이 중요하다. 이에 본 논문에서는 공공분야 근무자들에 대한 단기 교육과정을 통해 최고의 보안 효과 상승을 위한 교육과정을 제안한다.

ABSTRACT

Recently, cyber attacks are continuously threatening the cyberspace of the state across the border. Such cyber attacks show a surface which is intelligent and sophisticated level that can paralyze key infrastructure in the country. It can be seen well in cases, such as hacking threat of nuclear power plant, 3·20 cyber terrorism. Especially in public institutions of the country in which there is important information of the country, advanced prevention is important because the large-scale damage is expected to such cyber attacks. Technical support is also important, but by improving the cyber security awareness and security expert knowledge through the cyber security education to the country's public institutions workers is important to raise the security level. This paper suggest education courses for the rise of the best security effect through a short-term course for the country's public institutions workers.

Keywords: cyber security, public sector, information security, curriculum

I. 서 론

최근 국가 인프라 시설인 원전 기관을 대상으로 해킹 위협이 발생하였다[1]. 이 사건을 비롯하여 10년 동안 3·20 사이버테러, 3·4 DDoS 등 11건 이상의 주요 사이버 공격이 발생하였다. 이와 같이 사이버공격이 지능화되고 고도화됨에 따라 대규모 피해가 예상된다. 특히 국가·공공기관의 경우 국가적인

Received(02. 17. 2016), Modified(04. 19. 2016), Accepted(05. 04. 2016)
* 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2015R1C1A1A02036511)
† 주저자, jbyun@sejong.ac.kr
‡ 교신저자, jbyun@sejong.ac.kr(Corresponding author)

차원의 핵심정보를 보유하고 있으므로 국가·공공기관 근무자를 대상으로 하는 보안 교육의 중요성이 증대되고 있다.

이에 한국인터넷진흥원(KISA)에서는 '사이버보안 인재센터 연간 교육'을 통해 일반인의 정보보호 인식 제고와 재직자, 대학생, 국가·공공기관 근무자 등 분야별/수준별 교육 프로그램을 제공하고 있다[2]. 한국정보기술연구원(KITRI)는 현장형 실무인재를 양성하기 위한 목적으로 정보보호 전문가 양성과정을 구직자와 재직자로 구분하여 시행하고 있다[3].

그러나 이러한 교육과정이 주로 일반인을 대상으로 기술 중심의 교육을 하고 있으며, 국가 정보를 보호해야 하는 국가·공공기관 근무자들의 경우 정책, 관리 등에 특화된 교육이 필요하다. 이에 본 논문에서는 공공분야 사이버보안 역량 강화를 위해 공공분야 근무자에 특화된 정보보안 단기 교육과정에 대한 방향성을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 국내 정보보호 분야의 교육체계와 관련된 기존 연구를 분석하고, 3장에서 공공기관 보안담당자 업무를 분석하고 업무에 필요한 교과목을 제시한다. 4장에서는 3장에서 도출된 교과목을 바탕으로 커리큘럼을 제안하고 마지막으로 5장에서 결론을 맺는다.

II. 관련 연구

본 논문에서는 정보보호 분야의 교육체계에 대한 연구를 중점적으로 살펴보았다. 박태형 등[4]은 공공부문 정보보호 담당조직의 정보보호 관련 교육업무의 효율성을 평가하고 개선방향을 제시하였다. 김정덕 등[5]은 정보보호 전문인력 양성을 위한 정보보호 필수요구지식을 직무에 따라 제시하고, 융합전공 기반의 교육인증 프로그램 및 향후연구를 제안하였다. 이를 위해 미국의 정보보호 교육인증 프로그램을 분석하고, 국내 현실을 반영한 정보보호 교육인증 프로그램의 성공요인을 제시하였다. 박재용[6]은 부산광역시에 소재하고 있는 16개 대학을 중심으로 현행 경영정보학 교육과정을 분석하여 정보보안 전문인력 양성에 대한 문제점과 개선방안을 모색하였다. 김동우 등[7]은 국내 정보보호 교육체계의 문제점을 해결하고 사이버 정보보호 환경을 개선하기 위한 정보보호 교육 발전 방안을 제안하였다. 김민정 등[8]은 현재 운영 중인 국내 대학 및 대학원의 교육과정과 실제 산업체의 인력이 필요로 하는 지식 및 기술의 일치성을 분석하여 교육과정 설계의 미흡한 점을 보완할 방향성을 제시하였다. 이은주 등[9]은 국내 교육 관련기관 종사자의 기관유형, 근무지역, 담당직무별로 요구되는 정보보호 분야 지식 및 기술에 차이가 있는지 설문 결과를 분석하여 교육 관련기관의 정보보호 교육 프레임워크를 설계하여 제시하였다. 임원규 등[10]은 미국의 NICE에서 제시된 역량을 중심으로 국내 대학 정보보호관련 학과의 교육과정을 분석하였고, 이를 정보보호 학과의 교육과정 개선을 위한 기초 연구로 활용하고자 하였다. 강미화 등[11]은 대학의 정보보호 관련 전공 커리큘럼 조사 등을 통해 정보보호교육센터의 교육과정이 교육대상의 교육수요에 적합하게 운영되고 있는지 비교, 조사하였다.

국내 정보보호 분야의 교육체계 및 교육과정에 대한 연구는 기존에도 많이 진행되어 왔다. 그러나 대부분 전반적인 정보보호 교육체계나 대학 및 대학원 교육과정에 대해 분석하여 제시하는데 그쳤으며, 공공분야 근무자를 대상으로 하는 교육과정에 대한 논문은 거의 없었다. 본 논문에서는 공공분야 근무자들의 업무를 분석하고 이에 특화된 커리큘럼을 제안하였다는 점에서 관련 연구들과 차별성을 가진다.

III. 공공분야 정보보안 담당자 업무 분석 및 관련 교과목

공공분야 담당자를 위한 정보보안 커리큘럼 작성의 기준을 마련하기 위해 국가·공공기관 보안담당자 200명에게 설문을 실시하였다. 설문 문항은 주로 보안 담당자의 업무에 대한 질문과 담당자가 요구하는 정보보안 교육 내용에 대한 내용이었다.

설문 대상자를 크게 분류해 보면 국가·공공기관에서 정보보안 실무를 수행하는 그룹, 주요정보통신기반시설의 보안 담당을 수행하는 그룹, 보안관제를 수행하는 그룹으로 나눌 수 있었다. 따라서, 이와 같은 3개의 과정으로 나누어서 교육과정을 제시하려고 한다. 또한, 각각의 그룹에 대해 설문 답변 분석을 통해 주요 업무를 파악하고 수행 업무에 도움이 되는 교과목과 담당자들이 요구하는 교과목을 기반으로 교육과정의 교과목을 편성하였다.

3.1 정보보안 실무 과정

기관 보안담당자의 업무를 분석한 결과, 주로 정

보보호 업무 기획, 사이버위기 발생시 기관의 대응절차 마련, 기관 및 산하기관의 정보보안 감사, 정보보안 관리 등의 업무를 수행하는 것을 알 수 있었다.

Table 1. Security officer's work and related subjects

Security officer's work	Related subjects
Security Management	- Server security management - Guideline for network construction - Network security system management
Preparation against cyber crisis	- National cyber management system - Law and system about cyber security - Preparation procedures
Deployment and operation of network security system	- Domestic IT evaluation and authentication system - Network security system management - DDoS(Distributed Denial of Service) attacks and countermeasures
Network construction and management	- Guideline for network construction
Informatization(or Information security) planning	- Recent cyber threats and responses - Law and system about cyber security
Personal information security	- Personal information security in public sector
Server security management	- Windows server security - Linux/Unix server security
PC(Personal Computer) management	- PC management tool - Business PC security management
Security audit (Vulnerability assessment)	- Penetration test practice - Risk analysis and Vulnerability assessment

3.2 정보통신기반시설 보안과정

정보통신기반시설 보안 담당자의 업무를 분석한 결과, 정보통신기반시설 유지보수 및 정비, 취약점 분석평가 실시 등의 업무와 안전한 기반시설 운영을 위한 정보보안 관리, 보안 문제 검토 등 기관 보안담당자의 업무를 수행하는 것을 알 수 있었다.

Table 2. Security officer's work and related subjects

Security officer's work	Related subjects
Maintenance of infrastructure system or SCADA(Supervisory Control and Data Acquisition)	- National infrastructure ICT system - Server security - Recent cyber threat and response
Vulnerability assessment of infrastructure system or SCADA(Supervisory Control and Data Acquisition)	- Penetration test practice - Risk analysis and vulnerability assessment
Program implement and maintenance	- Secure coding
Management of SCADA server and client	- Server security - PC management tool
Deployment and operation of network security system	- Guideline for network construction - Network security system management - Domestic IT(Information Technology) evaluation and authentication system
Preparation against cyber crisis	- National cyber management system - Law and system about cyber security - Preparation procedures

3.3 보안관제 과정

공공분야 보안관제 담당자의 경우 보안위협 탐지, 침해사고에 대한 대응 조치 업무를 수행하고 있으며 이를 위한 패킷 분석, 악성코드 분석 등의 업무를 수행하고 있음을 알 수 있었다.

Table 3. Security monitoring and control staff's work and related subjects

Staff's work	Related subjects
Security threat Detection	- Introduction to security monitoring and control - Security monitoring and control system - Recent security monitoring and control technology
Incident response	- Security monitoring and control workflow - Log gathering system
Working with ISAC(Information Sharing and Analysis Center)	- Recent security moniotring and control technology trend - Plans to work with ISAC
Detection rule management (Rule optimization)	- Network packet analysis - Writing detection rule and rule optimization
Malware analysis	- Windows incident handling - Linux/Unix incident handling - Malware analysis
Monitoring webpage fabrication	- Web based malware detection

IV. 공공분야 사이버보안 교육 커리큘럼 제안

4.1 정보보안 실무 교육과정

공공분야 보안 담당자들의 주요 업무 분석 결과를 바탕으로 다음과 같은 커리큘럼을 설계하였다.

- 정보보안 실무 초·중·고급 과정
- 정보통신기반시설 보안과정
- 보안관제 과정

정보보안 실무 과정은 공공분야 보안담당자들을 위한 실무 기술 습득을 위한 교육과정으로, 기관 보안담당자의 실무에 도움이 되도록 웹 취약점 점검, 모의해킹, DDoS 대응 등 주요 취약점 점검 기술과 방어 기술에 대한 실습과정을 포함하고 있다. 정보통신기반시설 보안과정은 정보통신기반시설(전력, 수자원, 교통 등) 근무자들의 보안 의식 강화를 위한 교육과정으로, 제어시스템 기관과 관련된 SCADA 보안위협 및 대응방안 과목 위주로 편성하였다. 보안관제 과정은 보안관제 지식과 탐지룰 작성 기술 및 악성코드 분석기술 등을 습득하기 위한 과정으로 실무 위주의 과목으로 편성되어있다. 초급과정은 기초 지식 및 이론 위주의 과목으로 편성하며, 중급 과정은 전문지식 및 실무 위주의 과목으로 편성한다. 고급 과정은 고급 보안기술 습득을 위한 과목으로 편성한다.

4.1.1 정보보안 실무 초급과정 커리큘럼

정보보안 실무 초급과정은 정보보안 기본 소양 교육을 목표로 하며, 기본지식 습득을 원하는 각급기관 보안 및 전산 담당자를 대상으로 한다. Table 4는 정보보안 실무 초급과정 커리큘럼이 나와 있다.

Table 4. Information security Beginner course

Time		Subjects
Day 1	09~12	○National cyber management system
	13~18	○Recent cyber threats and responses
Day 2	09~12	○Information security management assessment
	13~18	○Personal information security in public sector ○Domestic IT evaluation and authentication system
Day 3	09~12	○Tour(Security monitoring and control center)
	13~18	○Risk analysis and vulnerability assessment
Day 4	09~12	○Network security system management
	13~18	○DDoS(Distributed Denial of Service) attacks and countermeasures
Day 5	09~12	○PC management tool
	13~18	○Business PC security management

4.1.2 정보보안 실무 중급과정 커리큘럼

정보보안 실무 중급과정은 정보보안 전문기술 실습교육을 목표로 하며, 전문지식 습득을 원하는 각급 기관 보안 및 전산 담당자를 대상으로 한다. Table 5는 정보보안 실무 중급과정 커리큘럼을 나타내고 있다.

Table 5. Information security Intermediate course

Time		Subjects
Day 1	09~12	○National cyber management system
	13~18	○Recent cyber threats and responses
Day 2	09~12	○Logical network separation
	13~18	○Penetration test practice
Day 3	09~12	○Network security system management
	13~18	○Domestic IT evaluation and authentication system
Day 4	09~12	○Windows incident handling(practice)
	13~18	○Smart phone security threats and responses
Day 5	09~12	○Information security management assessment
	13~18	○PC management tool

4.1.3 정보보안 실무 고급과정 커리큘럼

정보보안 실무 고급과정은 실습 비중을 높여 고급 보안 기술 습득을 목표로 하며, 고급기술 습득을 원하는 각급기관 보안 및 전산 담당자를 대상으로 한다. Table 6은 정보보안 실무 고급과정 커리큘럼이 나와 있다.

Table 6. Cyber security Advanced course

Time		Subjects
Day 1	09~12	○Recent cyber threats and responses
	13~18	○Vulnerability analysis and assessment (theory and practice)
Day 2	09~12	○Vulnerability analysis and assessment (theory and practice)
	13~18	○Vulnerability analysis and assessment (theory and practice)
Day 3	09~12	○Malware analysis (theory and practice)
	13~18	○Malware analysis (theory and practice)
Day 4	09~12	○Malware analysis (theory and practice)
	13~18	○Malware analysis (theory and practice)
Day 5	09~12	○Malware analysis (theory and practice)
	13~18	○Summary and discussion

4.2 정보통신기반시설 보안과정 커리큘럼

정보통신기반시설(전력, 수자원, 교통 등) 근무자들의 보안 의식 강화와 보안 기술 습득을 목표로 하며, 기반시스템 및 제어시스템 정보보안 담당자를 대

Table 7. Infrastructure security officer course

Time		Subjects
Day 1	09~12	○National infrastructure ICT (Information & Communication Technology) system
	13~18	○SCADA(Supervisory Control and Data Acquisition) security threats and responses
Day 2	09~12	○Network separation and data transmission between networks
	13~18	○Malware distribution using update server
Day 3	09~12	○Infrastructure ICT system security guineline
	13~18	○Infrastructure ICT vulnerability analysis and assessment
Day 4	09~12	○Secure SCADA system design
	13~18	○Penetration test practice
Day 5	09~12	○Network security system management
	13~18	○Discussion about strengthening infrastructure ICT security

상으로 한다. Table 7은 정보통신기반시설 보안을 나타낸다.

4.3 보안관제 과정 커리큘럼

보안관제 과정은 보안 관제 기초 지식 및 탐지룰 작성 기술 습득을 목표로 하며, 부문보안관제센터 근무자를 대상으로 한다. Table 8은 보안관제 과정의 커리큘럼이다.

Table 8. Security monitoring and control staff course

Time		Subjects
Day 1	09~12	○Introduction to security monitoring and control
	13~18	○Understanding of TMS(Threat Management System), ESM (Enterprise Security Management)
Day 2	09~12	○Network packet analysis (pratice)
	13~18	○Log gathering system
Day 3	09~12	○Windows incident handling
	13~18	○Linux/Unix incident handling
Day 4	09~12	○Writing detection rule and rule optimization (practice)
	13~18	○Tour (Security monitoring and control center)
Day 5	09~12	○Strengthening human security
	13~18	○Discussion about strengthening security monitoring and control

4.4 제안한 커리큘럼 분석

국가·공공기관 근무자를 대상으로 하는 정보보안 의식 제고를 위한 방문 특강은 연중 수시로 이루어지고 있고, 보안 담당자들의 실무 능력 제고를 위한 집합 교육은 연간 1천명 이상을 대상으로 이루어지고 있다. 집합 교육은 규모와 목표에 따라 1일에서 5일까지 실시되고 있다.[12]

국내 대학교의 정보보호학과 커리큘럼은 주로 보안방어기술에 중점을 두고 설계되어 있다. 또한, 산학협력을 위한 프로젝트 및 인턴쉽 등 산업기술에 활용이 가능한 내용 위주로 교과목이 구성되어 있다. KISA 아카데미의 행정기관 정보보호 교육은 정보보호 관리체계 수립에 중점을 두고 주로 기술적인 부분에 초점을 맞추고 있다. 이에 반해 본 논문에서 제시하는 커리큘럼은 공공분야 근무자들이 국가의 보안 정책 및 지침에 대한 업무 처리, 사이버위협에 대한 관제 및 대응에 초점을 맞추고 있다.

V. 결 론

최근 국가·공공기관을 대상으로 한 해킹 위협, 방송사 사이버테러 사건 등 지능화·고도화된 사이버 위협이 지속적으로 발생하고 있다.

이에 대하여 한국인터넷진흥원(KISA) 및 한국정보기술연구원(KITRI) 등에서 정보보호 인력 양성을 위한 다양한 교육을 시행하고 있다. 그러나 각 기관에서 정보보호 교육을 진행함에 있어 공공분야 보안 담당자들을 대상으로 한 교육이 미흡하다는 한계를 보여주고 있다. 본 논문에서는 공공분야 근무자들에 특화된 정보보호 교육과정을 제안하기 위해 각급 기관 보안 담당자의 업무를 분석하고 이에 도움이 되는 교과목을 편성하였다.

이러한 요구사항을 토대로 본 논문에서는 정보보안 교육 커리큘럼을 제안하였다. 본 논문에서는 국내 정보보호 교육 현황을 살펴보고 기존에 미흡하였던 국가·공공기관 근무자에 특화된 커리큘럼을 처음으로 제안했다는 점에서 의의가 있다.

향후 연구에서는 제안한 커리큘럼 이외에도 커리큘럼을 다양화하는 연구가 필요하다. 또한, 본 논문에서 제시된 커리큘럼에 대한 만족도를 측정하여 정보보안 교육을 더욱 고도화할 필요가 있다.

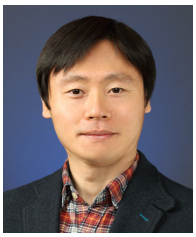
References

[1] Edaily, "Only one accident was arrested for 10 years, 10 have fallen into the labyrinth," http://www.edaily.co.kr/news/NewsRead.edy?SCD=JE41&newsid=01131606609438784&DCD=A00504&OutLnkChk=Y, Jan. 17, 2016.

[2] KISA Cyber Security Human Resources Center, "Our Works," http://www.kisa.or.kr/business/promotion/promotion_sub1.jsp, Jan. 17, 2016.

[3] KITRI, "Information Security professiona l development," http://www.kitri.re.kr/ kitri/information/security_v2.web, Jan. 20, 2016.
[4] Tea-hyoung Park, Jong-in Lim, and Sin-yong Mun, "Evaluating the Education business Efficiency of Information Security Organizations in Public Sector Using DEA Models," The Korean Association For Regional Information Society, 13(4), pp. 1-24, Dec. 2010.
[5] Jung-duk Kim and Tae-suk Baek, "A Study on Essential Body of Knowledge and Education Sertification Program for Information Security Professional Development," Digital Policy & Management, 9(5), pp. 113-121, Oct. 2011.
[6] Jae-yong Park, "An Analysis on Training Curriculum for Educating Information Security Experts," Korea Management and Information, 31(1), pp. 149-165, Mar. 2012.
[7] Dong-woo Kim, Seung-woan Chai, and Jae-cheol Ryu, "A Study of Domestic Information security Education System," Journal of The Korea Institute of Information Security & Cryptology, 23(3), pp. 545-559, June 2013.
[8] Min-jeong Kim, Hae-ni Lee, Shin-jeong Song, and Jin-ho Yoo, "A Study on the Curriculum of Department of Information Security in Domestic Universities and Graduate Schools and Comparison with the Needs of Industry Knowledge," Journal of The Korea Institute of Information Security & Cryptology, 24(1), pp. 195-205, Feb. 2014.
[9] Eun-ju Lee, Hyo-jung Jun, Tae-sung Kim, and Yeon-bok Kim, "Development of Information Security Education Framework for Information Security Employees: A Case of Educational Institutions," The Journal of the Korea Contents Association, 14(1), pp. 386-399, 2014.
[10] Wongyu Lim and Seong-jin Ahn, "A Study on Improvements of the Information Security Department via the Curriculum Analysis," The Journal of Korean Association of Computer Education, 17(6), pp. 71-80, Nov. 2014.
[11] Mi-Hwa Kang, Hyo-jung Jun, and Tae-sung Kim, "Difference between Information Security Education Demand of Information Security Employees and Curriculum of Information Security Education Center," Information Systems Review, 16(3), pp. 179-190, Dec. 2014.
[12] NIS, Ministry of Science, ICT and Future Planning, Korea Communication Commission, and Ministry of Security and Public Administration, 2013 National Information Security White Paper, pp. 211-213, Apr. 2013.

〈저자소개〉



윤 주 범 (Joobeom Yun) 종신회원
1999년 2월: 고려대학교 컴퓨터학과 학사
2001년 2월: 서울대학교 컴퓨터공학과 석사
2012년 2월: KAIST 전산학과 박사
2001년 3월~2015년 2월: ETRI 부설연구소 선임연구원
2015년 3월~현재: 세종대학교 정보보호학과 조교수
〈관심분야〉 네트워크 보안, 시스템 보안, 클라우드 컴퓨팅 보안