KIPS Tr. Comp. and Comm. Sys.
Vol.5, No.6 pp.143~152 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2016.5.6.143

A Study on Development of Evaluation Indicators for the Human Competency and Management In Managed Security Service (MSS)

Yang Sung Ho† · Lee Sang Jin††

ABSTRACT

Currently many central administrative agencies, municipalities and public and private institutions operate Managed security services to cope with cyber security incidents. These entities exert efforts in operating efficiencies rather than introduction of services as they used to. Accordingly, quite a few policies, directions and guidelines have been established for stable operation of Managed security services. Still, Managed security is operated by individuals, whose competencies influence the quality of Managed security services to a great extent. In this respect, the present article examines Managed security technology and methods and describes evaluation methods and examples relevant to human competencies, so as to seek for some potential courses for further development as well as more efficient approaches to human resource management in terms of institutional Managed security services.

Keywords : Managed Security Service, Human Cometency, Human Cometency Evaluation

보안관제 업무의 인적 역량 및 관리에 대한 평가지표 개발 연구

양 성 호† · 이 상 진††

요 약

현재 많은 중앙행정기관 및 지방자치단체, 공공·민간기관들이 사이버 침해사고 대응을 위해 보안관제서비스를 운영하고 있다. 과거와는 달리 서비스 도입보다는 효율적인 운영을 위해 노력하고 있다. 때문에 많은 정책과 방향, 지침들을 수립하고 안정적으로 운영되길 원한다. 하지만 보안관제는 사람이 운영하는 업무이기 때문에 개개인의 능력에 따라 많은 차이를 보이게 된다. 이에 따라 본 논문에서는 보안관제 기술과 방법에 대해 살펴본 후 인적역량에 대한 평가 방법과 예시를 통해 기관의 보안관제 업무 시 인적 관리에 효율적인 운영 방안 및 향후 발전 방향에 대해 모색해 보고자 한다.

키워드 : 보안관제서비스, 인적역량, 인적역량평가

1. 서 론

우리나라는 1970년대 산업혁명 이후 급격한 발전을 거듭하여 UN 전자정부평가 3회 연속 세계 1위를 달성하는 등 세계적으로 인정받고 있다[1]. 정부는 또한 첨단IT인프라와 이를 기반으로 한 정보 전략 및 처리/활용을 위하여 1995년도부터 전자정부 구축사업을 시작하여 현재 민원24, G4C, 국민신문고, 행정표준코드 등 많은 정부시스템들이 운영되고 있다. 이러한 시스템들은 안정적인 운영을 목표로 하드웨어, 소프트웨어, 네트워크 유지보수 외에도 공통적으로 정보보호를 포괄적으로 적용하고 있다. 이러한 시스템들은 정보통신기반보호법의 제정으로 주요정보통신기반시설로 지정되어 보안이 강화되고 있으며, 침해사고 발생 시 실시간 경보 분석 및 대응체계 운영, 취약점 및 침해요인과 대응방안에 대한 각종 정보제공을 위한 정보공유분석센터들을 설립·운영하고 있다[2]. 이러한 정보공유분석센터들의 설립에도 불구하고 공공·민간 기관들은 더욱더 지능화, 첨단화, 조직화된 사이버공격에 의해 2013년 8월까지 해킹사고는 7,589건이 발생하여 작년대비 감소하였지만 악성코드 유포 등 악의적인 행위는 13,678건으로 지속적으로 증가하고 있는 것으로 나타났다[3]. 기관 내에서 정보보안을 강화하기 위해서 보안관제 서비스를 운영을 하는 것이 바람직하며, 또한 높은 수준의 역량을 확보해야 하는데, 이를 위해 요구되는 역량의 범위는 시스템, 네트워크, 장비, 소프트웨어뿐만 아니라 IT 법률 등에 관한 지식까지 요구하는 방향으로 확대되고

† 준 회 원 : 고려대학교 정보보호대학원 정보보호학과 석사과정
†† 종신회원 : 고려대학교 정보보호대학원 교수
Manuscript Received : March 10, 2016
First Revision : April 20, 2016
Accepted : April 20, 2016
* Corresponding Author : Lee Sang Jin(sangjin@korea.ac.kr)

있는 추세이다. 보안관제 업무를 효과적으로 운영하기 위해서는 보안관제 업무에 대한 다방면의 평가와 진단이 필요하다. 보안관제 업무의 평가지표에 관한 연구는 이현도 등[4]의 논문에서 연구되었으므로, 추가적으로 수행 인력에 대한 역량분석을 통해 더욱 효과적인 보안관제가 가능할 것으로 판단된다. 따라서 본 논문은 기관 시스템 규모에 따른 정보보안 인력의 필요 역량을 분석하고 정량화할 수 있는 평가지표를 제시한다.

2. 보안관제 인적 역량 평가

2.1 연구 논문

1) 인적역량 평가 연구

인적역량 평가는 모든 환경 및 업무영역에 대해 다양하게 분석되고 있다. IT 인적자원에 대해 서우종 등[2]의 논문에서 업무프로세스에 따른 필요 역량 분석을 하였다. 하지만 보안관제라는 특수한 환경에서 보안현황, 기술 등 전문적인 역량평가가 필요하다.

2) 보안관제 연구

보안관제와 관련된 연구에는 기관운영 및 평가지표를 통한 효율적인 서비스 관리, 업무효율성을 위한 보안관제 기술 등 다양한 방면으로 연구가 활발하게 진행되었다. 보안관제를 위한 시스템운영(모니터링, 헬프데스크, 시스템장애처리 등)과 관리(장애, 구성, 변경, 성능, 용량, 가용성, 표준, 취약점, 보고서 등)에 대한 기본적인 정책을 수립하고 침해사고예방, 대응, 관리를 위한 정책도 마련하여야 한다[5]. 인력구성은 기본적으로 4명 1일 2교대가 24시간 근무의 보편적인 기준이나 경우에 따라 시간대별, 개인역량별로 구성하는 것이 바람직하다. 이러한 최적의 정책과 인력구성은 기관의 보안성 향상에 크게 기여할 것이다.

2.2 역량 평가 방법론

본 연구에서 제시하는 역량평가 방안은 관제업무에서 빈번하게 발생하는 대표적인 취약점을 Table 1과 같이 구분하여 분석시간과 난이도에 대해 현재 관제업무를 수행하고 있는 인력들을 대상으로 Table 2의 항목에 대해 설문조사를 실시하여, 역량을 평가하였다. 역량평가에는 인력 채용에 많은 영향을 주는 자격증 또는 경력사항, 학력 등을 집중적으로 분석하여 K 기관을 예로 관제인력 채용 요건이나 근무자요건이 충족하는지 알아보도록 한다. 또한, 분석된 결과를 토대로 K기관에 필요한 인적자원의 등급 및 필요 인원을 정량화 한다. 본 논문을 통하여 측정된 보안인력의 평균 업무 능력 분석을 통하여 각 기관 또는 기관 시스템 규모에 따라 통합관제시스템에서 발생하는 일일 탐지량에 대응할 수 있는 인력 구성을 판단하기 위한 평가지표로써 도움이 될 것이다[6-8].

Table 1. Vulnerability group and based on analysis

구 분	기준1	기준2
웹 취약점 이벤트	분석시간	난이도
악성코드 이벤트		
정보수집 이벤트		
비인가접근 이벤트		
서비스거부 이벤트		

Table 2. Competency evaluation Items

조사항목		내용
인적사항		성별, 학력, 전공, 나이
경력	경력유형	이전 업무의 경력유형
	근무개월	이전 업무의 총 근무 개월
현재 업무	근무개월	현 보안관제 업무의 총 근무 개월
	기술자 등급	소프트웨어기술자등급
	전문지식 및 기술	보안관제 업무 관련 전문지식
	업무처리 능력	보안관제 업무 숙련도

2.3 표본 특성

1) 응답자의 일반적 특성

설문의 응답결과 중 분석에 사용된 표본 수는 총 93부이며, 응답자의 일반적 특성을 살펴보면 Table 3과 같다. 응답자의 성별은 남성이 압도적으로 많았으며(98.9%), 여성은 1명(1.1%)에 불과했다. 이는 관제 근무가 24시간 운영됨에 따라 여러 가지 복합적인 상황에 의해 남성이 많은 것으로 확인되었다. 연령별로는 30대가 가장 많았고(68.8%), 그 다음으로는 20대(25.8%), 40대 이상(5.4%) 순으로 나타났다. 그리고 정보보호 전공자가 대부분이었고(92.5%), 비전공자는 7명에 지나지 않았다(7.5%). 학력은 4년제 대졸자가 가장 많았고(77.4%), 2~3년제 대졸(11.8%), 대학원졸(9.7%), 고졸(1.1%) 순으로 나타났다.

Table 3. Characteristics of respondents

구분		빈도	퍼센트
성별	남자	92	98.9
	여자	1	1.1
연령	20대	24	25.8
	30대	64	68.8
	40대 이상	5	5.4
전공	정보보호전공자	86	92.5
	비 정보보호전공자	7	7.5
학력	고졸	1	1.1
	2, 3년제 대졸	11	11.8
	4년제 대졸	72	77.4
	대학원 졸업 이상	9	9.7
합계		93	100.0

2) 응답자의 직능

응답자의 업무능력 실태를 살펴보면, Table 4에서 보는

바와 같이, 소프트웨어 기술자등급은 초급기술자가 가장 많았으며(28.0%), 그 다음으로는 중급기술자(25.8%) 고급기술자(12.9%) 등의 순으로 나타났다. 정보보호 관련 업무의 경력은 1~2년차가 가장 많았고(34.4%), 그 다음으로는 4년 이상(25.8%), 3~4년(16.1%), 2~3년(14.0%), 1년 미만(9.7%) 순으로 나타났다. 관제 업무 경력으로는 4년 이상(37.6%)이 가장 많았으며, 1~2년(21.5%), 2~3년(17.2%), 3~4년(15.1%), 1년 미만(8.6%) 순으로 나타났다. 이러한 집단 구성비율은 본 연구의 응답자들에게 한한 것이며, 전체 미응답자의 성별, 연령, 전공, 경력, 자격증 등 차이가 있을 수 있으나 통계학적 분석에 유의미한 변경요소는 연구결과 내로 포함될 확률이 높다.

Table 4. Respondents ratings and career

구분		빈도	퍼센트
소프트웨어 등급	초급기능사	6	6.5
	중급기능사	9	9.7
	고급기능사	1	1.1
	초급기술자	26	28.0
	중급기술자	24	25.8
	고급기술자	12	12.9
	특급기술자	7	7.5
	해당 없음	8	8.6
정보보호 관련 업무 경력	1년 미만	9	9.7
	1-2년	32	34.4
	2-3년	13	14.0
	3-4년	15	16.1
	4년 이상	24	25.8
정보보호 관제 업무 경력	1년 미만	8	8.6
	1-2년	20	21.5
	2-3년	16	17.2
	3-4년	14	15.1
	4년 이상	35	37.6
합계		93	100.0

2.4 실태조사

다음은 중복응답문항에 대한 분석 결과이다. 정보보호 관련 자격증 보유현황은 Table 5와 같다. 먼저 어떠한 자격증도 가지고 있지 않다고 한 응답자는 93명 중 34명(36.6%)이었다. 나머지 59명의 자격증 소지자 가운데 응답자들이 가장 많이 보유하고 있는 자격증은 CISSP로 나타났으며(66.7%), 그 다음으로는 CISA, 기타, SIS순으로 나타났다. 정보보호관련 지식습득 경로에 대한 분석 결과는 Table 6과 같다. 많은 응답자가 직장에서 지식을 습득한다고 하였으며(35.3%), 학원과 독학의 비율은 동일하게 나타났다(23.9%). 그 다음으로 학교수업과 동아리/스터디의 경우도 동일한 비율로 나타났다(8.2%). 정보보호장비 운영경험에 대한 분석결과는 Table 7과 같다. Firewall이 가장 많이 운용하는 것으로 나타났으며(23.2%), 그 다음으로는 ESM, IPS/ IDS, 웹방화벽, DDos 대응장비 순으로 나타났고, 기타는 3.1%에 불과했다. 사용가능한 프로그램언어에 대한 분석 결과는 Table 8과 같다. 응답자들은 C++를 가장 많이 다룰 줄 아는 것으로 나타났으며(32.5%), 그 다음으로는 C(26.6%), Java(22.7%) 순으로 나타났다. 그 외 언어로는 C#(6.4%), Python(4.9%), Peral(3.4%), 기타(3.4%) 순으로 나타났다[9-11].

Table 5. Certification Related to Information Security

구분	빈도	퍼센트
CISSP	54	66.7
CISA	17	21.0
SIS	3	3.7
기타	7	8.6
합계	81	100.0

※ 자격증 소지자 59명의 다중응답결과임

Table 6. Knowledge Acquisition Related to Information Security

구분	빈도	퍼센트
학교수업	15	8.2
학원	44	23.9
독학	44	23.9
직장	65	35.3
동아리/스터디	15	8.2
기타	1	.5
합계	184	100.0

※ 전체 응답자 93명의 다중응답결과임

Table 7. Operating Experience of Information Security Equipment

구분	빈도	퍼센트
ESM	77	21.6
IPS/IDS	71	19.9
Firewall	83	23.2
웹 방화벽	59	16.5
DDoS 대응장비	56	15.7
기타	11	3.1
합계	357	100.0

※ 전체 응답자 93명의 다중응답결과임

Table 8. Experience for Programming Language

구분	빈도	유효 퍼센트
C	54	26.6
C++	66	32.5
C#	13	6.4
Java	46	22.7
Python	10	4.9
Perl	7	3.4
기타	7	3.4
합계	203	100.0

※ 전체 응답자 93명의 다중응답결과임

Table 9. Technology of Managed Security Service (MSS)

구 분	가능	불가능
① 모니터링 및 패킷분석을 통한 오탐/진탐 판단할 수 있는가?	94.6	5.4
② 간단한 스크립트 언어(Perl, Python, Ruby) 등을 통한 긴급대응 가능한가?	34.4	65.6
③ IPS/IDS 자체 탐지 Rule 제작 가능한가?	74.2	25.8
④ 각종 정보보호 및 서버 로그를 통한 상관분석이 가능한가?	87.1	12.9
⑤ 방화벽 및 서버보안 장비를 통한 접근통제정책(ACL)을 직접 수립가능한가?	89.2	10.8
⑥ 악성 파일에 대한 동적 분석 후 긴급백신(악성 파일, 레지스트리 삭제) 제작이 가능한가?	23.7	76.3
⑦ OWASP Top10에서 제공되는 알려진 웹 취약점에 대해 이해하고 있는가?	94.6	5.4
⑧ 정보보호 장비 장애 시 트러블슈팅이 가능한가?	58.1	41.9
⑨ 정보보호 장비 및 서버 Database 및 Log에서 원하는 데이터 추출이 가능한가?	66.7	33.3

Table 9는 응답자들의 실제 정보보호관제 기술의 정도를 정리한 것이다. 응답자들은 오탐/진탐의 판단과 웹 취약점의 이해에서는 90% 이상의 높은 수치를 나타냈으나, 스크립트를 통한 긴급 대응과 긴급백신 제작에 대해서는 가능한 응답자보다 할 줄 모르는 응답자가 더 많은 것으로 나타났다. 또한 장비 장애 시 트러블슈팅과 장비 및 서버에서의 데이터 추출 영역도 다소 취약한 것으로 나타났다.

2.5 표본특성에 따른 역량 분석

1) 이벤트별 통계

Table 10은 정보보호관제사들의 역량분석을 위한 변수들인 이벤트별 처리 시간과 주관적 난이도에 대한 기술통계 결과를 나타낸 것이다. 점수가 적을수록 처리 시간이 적고 주관적인 난이도 또한 쉬운 것을 의미하므로 관제 역량이 높다고 볼 수 있다. 각 이벤트에 대한 분석시간의 점수는 모두 2점 내외이므로 응답자들은 각 이벤트를 탐지하는 데 10분 내외가 소요되는 것을 알 수 있으며, 주관적 난이도 역시 대체적으로 쉽다고 여기는 것으로 나타났다.

Table 10. Events analysis time and detection difficulty

구 분		Min	Max	Mean	SD
웹 취약점 이벤트	분석시간	1.00	5.00	2.31	1.193
	난이도	1.00	5.00	2.53	0.826
악성코드 이벤트	분석시간	1.00	5.00	2.37	1.006
	난이도	1.50	5.00	2.54	0.718
정보수집 이벤트	분석시간	1.00	5.00	1.77	1.029
	난이도	1.00	4.00	1.78	0.825
비인가접근 이벤트	분석시간	1.00	5.00	1.97	1.047
	난이도	1.00	4.00	1.95	0.839
서비스거부 이벤트	분석시간	1.00	5.00	2.13	1.048
	난이도	1.00	4.67	2.19	0.817

n=93
분석시간: 1="5분 이하", 2="5~10분 이하", 3="10~15분 이하", 4="15~20분 이하", 5="20분 이상"
난이도: 1="매우 쉬움", 2="쉬움", 3="보통", 4="어려움", 5="매우 어려움"

2) 직능에 따른 차이

성별, 연령, 전공, 학력의 인구통계학적 특성은 Table 3에서 보는 바와 같이 집단 간 분포가 고르지 못하고 비교집단의 표본 수가 너무 적어 분석을 하는 데 어려움이 있다. 따라서 응답자의 직능에 따라 이벤트별 분석시간 및 주관적 난이도에 차이가 있는지 알아보고자 한다. 구체적으로는 응답자의 직능 가운데 소프트웨어 등급과 관제업무 경력에 따른 차이를 살펴보았으며, 소프트웨어 등급은 집단별 표본수를 고르게 하기 위해 하위집단을 재구성하였다. 즉, 소프트웨어 등급은 '기능사 이하', '초급기술자', '중급기술자', '고급기술자', '특급기술자'로 분류하였고, 관제업무경력은 최초의 분류를 그대로 사용하였다. 분석 방법은 집단을 재분류하여도 하위집단의 표본수가 적어 비모수 통계기법을 적용하였으며, 3개 이상의 집단 간 분포의 동질성을 살펴보는 Kruskal-Wallis 검증법을 사용하였다.

a) 소프트웨어 등급에 따른 차이

먼저, 소프트웨어 등급에 따른 이벤트별 분석시간은 Table 11과 같다. 소프트웨어 등급에 따라서는 악성코드 이벤트에 대해서만 분석시간에 차이가 있는 것으로 나타났다. 즉 악성코드 이벤트에 대하여 중급기술자의 처리시간이 가장 짧은 것으로 나타났으며, 그 다음으로는 고급기술자, 특급기술자, 기능사 이하, 초급기술자 순으로 나타났다. 소프트웨어 등급에 따른 이벤트별 난이도는 Table 12와 같으며, 웹 취약점 이벤트를 제외한 악성코드 이벤트, 정보수집 이벤트, 비인가접근 이벤트, 서비스거부 이벤트에서 유의한 차이가 있는 것으로 나타났다. 주관적 난이도가 적은 순으로 악성코드 이벤트는 특급기술자, 중급기술자, 고급기술자, 기능사 이하, 초급기술자 순이었으며, 정보수집 이벤트는 특급기술자, 중급기술자, 초급기술자, 고급기술자, 기능사 이하, 비인가 접근 이벤트는 특급기술자, 중급기술자, 고급기술자, 초급기술자, 기능사 이하 순으로 나타났고, 서비스 거부 이벤트는 특급기술자, 중급기술자, 초급기술자, 고급기술자, 기능사 이하 순으로 나타났다.

Table 11. Events analysis time according to the Software engineer rating

구분		N	Mean (SD)	평균 순위	X2	유의 확률
웹 취약점 이벤트	기능사 이하	24	2.57(1.388)	51.52	4.152	.386
	초급기술자	26	2.48(1.112)	52.21		
	중급기술자	24	2.18(1.247)	42.88		
	고급기술자	12	1.90(1.022)	36.54		
	특급기술자	7	2.03(0.716)	44.21		
악성코드 이벤트	기능사 이하	24	2.69(1.138)	54.58	10.135	.038*
	초급기술자	26	2.69(1.121)	54.88		
	중급기술자	24	1.90(0.575)	35.17		
	고급기술자	12	2.08(1.052)	38.04		
	특급기술자	7	2.18(0.238)	47.64		
정보수집 이벤트	기능사 이하	24	2.11(1.254)	53.56	9.310	.054
	초급기술자	26	1.95(0.878)	54.71		
	중급기술자	24	1.31(0.471)	36.54		
	고급기술자	12	1.81(1.527)	41.46		
	특급기술자	7	1.43(0.535)	41.21		
비인가 접근 이벤트	기능사 이하	24	2.38(1.345)	54.21	3.377	.497
	초급기술자	26	1.73(0.533)	44.98		
	중급기술자	24	1.83(0.816)	45.75		
	고급기술자	12	1.75(1.138)	39.08		
	특급기술자	7	2.29(1.604)	47.64		
서비스 거부 이벤트	기능사 이하	24	2.44(1.203)	53.63	4.452	.348
	초급기술자	26	2.10(0.723)	50.56		
	중급기술자	24	1.94(1.075)	40.71		
	고급기술자	12	2.14(1.425)	43.67		
	특급기술자	7	1.71(0.488)	38.36		

* p<.05

Table 12. Events difficulty according to the Software engineer rating

구분		N	Mean (SD)	평균 순위	X2	유의 확률
웹 취약점 이벤트	기능사 이하	24	2.57(0.972)	51.48	4.243	.374
	초급기술자	26	2.64(0.755)	50.92		
	중급기술자	24	2.58(0.891)	46.67		
	고급기술자	12	2.33(0.710)	37.17		
	특급기술자	7	2.20(0.476)	35.07		
악성코드 이벤트	기능사 이하	24	2.76(0.829)	55.06	20.354	.000***
	초급기술자	26	2.77(0.790)	55.42		
	중급기술자	24	2.20(0.423)	34.44		
	고급기술자	12	2.67(0.515)	55.50		
	특급기술자	7	1.86(0.197)	16.57		
정보수집 이벤트	기능사 이하	24	2.42(0.897)	65.54	31.890	.000***
	초급기술자	26	1.86(0.619)	50.94		
	중급기술자	24	1.25(0.442)	30.00		
	고급기술자	12	1.89(0.903)	50.54		
	특급기술자	7	1.00(0.000)	21.00		
비인가 접근 이벤트	기능사 이하	24	2.50(0.978)	62.23	15.977	.003**
	초급기술자	26	1.96(0.445)	49.25		
	중급기술자	24	1.63(0.824)	36.92		
	고급기술자	12	1.75(0.866)	41.00		
	특급기술자	7	1.43(0.535)	31.29		
서비스 거부 이벤트	기능사 이하	24	2.56(0.707)	59.81	23.636	.000***
	초급기술자	26	2.26(0.584)	53.98		
	중급기술자	24	2.01(0.960)	36.81		
	고급기술자	12	2.28(0.863)	46.21		
	특급기술자	7	1.19(0.378)	13.43		

** p<.01, *** p<.001

b) 경력에 따른 차이

관제 경력에 따라서는 모든 이벤트에 대하여 분석시간에 유의한 차이가 있는 것으로 나타났다. Table 13에서 보는 바와 같이 웹 취약점 이벤트와 악성코드 이벤트는 경력이 오래되었을수록 분석시간도 짧았으며, 정보수집 이벤트는 4년 이상, 2~3년, 3~4년, 1년 미만, 1~2년, 비인가 접근 이벤트는 2~3년, 4년 이상, 3~4년, 1~2년, 1년 미만, 서비스 거부 이벤트는 3~4년, 4년 이상, 2~3년, 1~2년, 1년 미만 순으로 분석시간이 짧은 것으로 나타났다. 관제경력에 따른 이벤트별 난이도 역시 Table 14와 같이 모든 이벤트에 대하여 유의한 차이가 나타났다. 모든 이벤트에 대하여 3~4년 경력자가 4년 이상 경력자보다 주관적으로 인지하는 난이도가 낮게 나타났다. 주관적 난이도가 낮은 순으로 웹 취약점 이벤트, 비인가 접근 이벤트, 서비스 거부 이벤트의 경우는 3-4년, 4년 이상, 2~3년, 1~2년, 1년 미만 순이었고, 악성코드 이벤트는 3~4년, 4년 이상, 1~2년, 2~3년, 1년 미만, 정보수집 이벤트는 3~4년, 2~3년, 4년 이상, 1~2년, 1년 미만 순으로 나타났다.

2.6 정보보호관제 인적 역량에 대한 영향요인

위 2.5단원에서 살펴본 집단 간의 동질성 분석만으로는 하위 집단 간의 2표본 차이 검증에 어려움이 있으며, 정보보호관제사들의 역량에 영향을 미칠 수 있는 다른 변수들의 교란효과를 완전히 통제할 수 없기 때문에 다변량분석(multi-variate analysis)을 실시하였다. 이를 위해 먼저 이변량 상관관계분석(bivariate correlation analysis)을 실시하였고, 이에 따라 종속변수인 이벤트별 분석시간과 주관적 난이도에 유의한 상관관계를 지닌 변수들만 사용해 다중회귀분석(multiple regression analysis)을 실시하였다.

Table 13. Events analysis time according to the career

구분		N	Mean (SD)	평균 순위	X2	유의 확률
웹취약점이벤트	1년 미만	8	3.35(1.145)	70.44	18.513	.001***
	1-2년	20	2.87(1.126)	59.75		
	2-3년	16	2.35(1.249)	48.00		
	3-4년	14	2.14(0.916)	45.79		
	4년 이상	35	1.81(1.074)	34.39		
악성코드이벤트	1년 미만	8	3.41(1.535)	66.06	19.447	.001***
	1-2년	20	2.88(0.741)	63.65		
	2-3년	16	2.41(1.221)	45.50		
	3-4년	14	2.18(0.558)	45.46		
	4년 이상	35	1.90(0.723)	34.43		
정보수집이벤트	1년 미만	8	2.38(1.302)	59.50	29.519	.000***
	1-2년	20	2.63(1.081)	69.68		
	2-3년	16	1.54(0.851)	41.88		
	3-4년	14	1.74(1.056)	47.29		
	4년 이상	35	1.25(0.538)	33.41		
비인가접근이벤트	1년 미만	8	3.00(1.195)	70.69	17.682	.001**
	1-2년	20	2.45(1.099)	59.83		
	2-3년	16	1.56(0.512)	39.31		
	3-4년	14	2.07(1.385)	44.82		
	4년 이상	35	1.60(0.736)	38.64		
서비스거부이벤트	1년 미만	8	2.75(1.123)	58.81	14.200	.007**
	1-2년	20	2.57(1.077)	59.88		
	2-3년	16	2.33(1.211)	51.59		
	3-4년	14	1.64(1.151)	30.93		
	4년 이상	35	1.83(0.707)	41.27		

** p<.01, *** p<.001

Table 14. Events difficulty according to the career

구분		N	Mean (SD)	평균 순위	X2	유의 확률
웹취약점이벤트	1년 미만	8	3.25(0.563)	74.88	18.152	.001**
	1-2년	20	2.77(0.803)	58.78		
	2-3년	16	2.54(0.819)	46.03		
	3-4년	14	2.19(0.659)	37.96		
	4년 이상	35	2.37(0.852)	37.96		
악성코드이벤트	1년 미만	8	3.50(0.886)	76.81	25.369	.000***
	1-2년	20	2.73(0.555)	56.50		
	2-3년	16	2.77(0.844)	55.84		
	3-4년	14	2.09(0.601)	27.14		
	4년 이상	35	2.29(0.446)	38.66		
정보수집이벤트	1년 미만	8	2.75(0.345)	79.44	28.972	.000***
	1-2년	20	2.28(0.782)	62.28		
	2-3년	16	1.50(0.730)	37.75		
	3-4년	14	1.38(0.804)	32.96		
	4년 이상	35	1.57(0.689)	40.70		
비인가접근이벤트	1년 미만	8	3.00(0.535)	77.88	21.373	.000***
	1-2년	20	2.30(0.801)	57.45		
	2-3년	16	1.88(0.619)	46.00		
	3-4년	14	1.64(0.745)	37.89		
	4년 이상	35	1.66(0.802)	38.07		
서비스거부이벤트	1년 미만	8	2.79(0.248)	75.50	32.684	.000***
	1-2년	20	2.62(0.744)	63.58		
	2-3년	16	2.35(1.057)	47.22		
	3-4년	14	1.52(0.844)	22.93		
	4년 이상	35	2.01(0.545)	40.54		

** p<.01, *** p<.001

a) 상관관계분석

먼저 변수들의 상관관계를 분석한 결과는 Table 15와 같다. 인구통계학적 특성 중 성별은 여성이 1명에 불과하였으므로 투입하지 않았다. 종속변수인 이벤트 분석시간과 이벤트 난이도는 매우 높은 상관도(r=.820, p<.01)를 나타내 정보보호관제사의 인적 역량을 나타내는 변인들로 매우 적합하다는 것을 알 수 있다. 인구통계학적 특성들은 이러한 종속변수에 대하여 유의한 상관관계를 보이지 않았으며, 직능요인인 소프트웨어 등급과 관제경력은 유의한 부(-)의 상관관계를 나타내었다. 즉, 소프트웨어 등급이 높을수록 그리고 관제경력이 오래되었을수록 이벤트 분석시간이 적게 소요되고 주관적으로 느끼는 난이도는 낮은 것으로 나타나 인적 역량이 높음을 알 수 있다.

Table 15. Bivariate correlation analysis

구분	연령	전공	학력	SW 등급	관제 경력	분석 시간	난이도
연령	1						
전공	-.191	1					
학력	.171	.056	1				
SW 등급	.573**	.063	.272**	1			
관제경력	.442**	-.040	.305**	.411**	1		
분석시간	-.039	-.058	-.187	-.227*	-.509**	1	
난이도	-.188	-.108	-.189	-.384**	-.509**	.820**	1

* p<.05, ** p<.01

b) 다중회귀분석

먼저 이벤트 분석시간에 대한 소프트웨어 등급과 관제경력의 영향관계를 분석한 결과는 Table 16과 같다. 분석 모형의 설명력은 25.9%이며, 분산은 통계적으로 유의한 것으로 나타났다. 공차한계도 최대값인 1에 가깝고, VIF도 10보다 현저히 적어 다중공선성도 낮은 것으로 나타났다. 분석결과, 소프트웨어 등급과 관제경력을 함께 고려하였을 경우 관제경력만 이벤트 분석시간에 통계적으로 유의미한 부(-)의 영향력을 갖는 것으로 나타났다. 즉, 관제경력이 오래되었을수록 이벤트 분석시간이 짧아지는 것으로 나타났다. 이벤트 난이도에 대한 소프트웨어 등급과 관제경력의 영향관계는 Table 17과 같으며, 모형의 설명력은 29.6%이고, 분산도 통계적으로 유의하였다. 다중공선성의 문제도 없는 것으로 나타났다. 분석 결과, 소프트웨어 등급과 관제경력이 모두 이벤트 난이도에 통계적으로 유의한 부(-)의 영향을 미치는 것으로 나타났다. 즉, 소프트웨어 등급이 높을수록 그리고 관제경력이 오래되었을수록 이벤트에 대한 난이도가 쉽다고 여기는 것을 알 수 있다. 그러나 소프트웨어 등급보다는 관제경력의 영향력이 더 큰 것으로 나타났다.

Table 16. Factors of event analysis time

종속변수 : 이벤트 분석 시간	비표준화 계수		표준화 계수	t	p	공선성 통계량	
	B	표준 오차	베타			공차	VIF
(상수)	3.246	.232		13.999	.000		
SW 등급	-.010	.044	-.022	-.223	.824	.831	1.203
관제 경력	-.312	.062	-.500	-5.022	.000***	.831	1.203
R2=.259, F=15.750(p=.000***)							

*** p<.001

Table 17. Factors of event difficulty

종속변수 : 이벤트 분석 시간	비표준화 계수		표준화 계수	t	p	공선성 통계량	
	B	표준 오차	베타			공차	VIF
(상수)	3.152	.165		19.113	.000		
SW 등급	-.069	.032	-.211	-2.172	.033*	.831	1.203
관제 경력	-.193	.044	-.423	-4.362	.000***	.831	1.203
R2=.296, F=18.958(p=.000***)							

* p<.05, *** p<.001

2.7 정보보호관제 인적 역량분석 결과

위의 분석을 통해 소프트웨어 기술자 등급과 관제경력, 이벤트분석시간, 이벤트난이도가 유의한 결과를 나타내는 것으로 분석되었다. 그중 정보보호관제 인력의 채용에 큰 영향을 미치는 소프트웨어 기술자 등급과 정보보호 관제 근무경력을 대상으로 분포도 및 영향력에 대해 알아본다. 먼저 다양한 정보통신분야에서 사용되어졌던 소프트웨어 기술자 등급이 정보보호관제사에게 미치는 영향을 살펴보고자 한다. 소프트웨어 기술자등급은 모든 정보통신분야를 아우르는 등급이었다. 2013년 1월 1일자로 폐지되었으나 노임단가는 기존 방식을 도입하고 있다. 정보보호관제요원들은 정부, 공공 등의 주요 기관에 용역업체를 통해 투입되는 경우가 많으며 소프트웨어 기술자 등급으로 투입인력 대비 비용이 산정되고 있다. 또한 전문 인력의 채용시에도 정보처리기사 자격증 취득 여부와 관련 경력에 따라 평가되므로 소프트웨어 기술자 등급이 많은 영향을 주고 있다. 따라서 정보보안관제사의 개인역량 평가 및 노임 기준 선정 등에 많은 어려움이 따른다[8]. 앞서 분석한 결과에 따르면 Table 18과 같이 전체의 80%가 기능사 이하, 초급, 중급기술자의 분포를 보여주고 있으며, 고급기술자 및 특급기술자가 다소 작은 분포를 보여주고 있다. 24시간 근무형태를 가지는 보안관제의 경우 업무시간의 패턴과 피로도 등으로 인해 업무선호도가 낮아 고급 이상의 기술자는 많지 않은 것으로 조사 되었다. Fig. 1에서 중급기술자부터 기능사 이하 또는 초급기술사까지는 등급난이도에 따라 많은 분석을 할 수 있다는 것을 알 수 있다. 하지만 고급기술자, 특급기술자의 경우 중급기술사보다 월등히 빠른 처리시간을 보여야 하지만 점차 분석처리속도가 느려지는 등 불규칙적인 분포를 보이고 있다. 다음으로 정보보안관제 경력이 정보보안관제사에게 미치는 영향을 Fig. 2에서 살펴본다. 관제경력 대비 처리속도의 분석결

Table 18. Software engineer rating or career distribution of the respondents

구분	분포	구분	분포
기능사 이하	25.9%	1년 미만	8.6%
초급기술자	27.9%	1~2년	21.5%
중급기술자	25.8%	2~3년	17.2%
고급기술자	12.9%	3~4년	15.1%
특급기술자	7.5%	4년 이상	37.6%

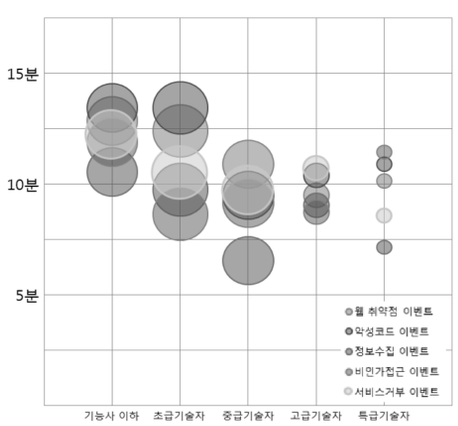

Fig. 1. Software engineer rating distribution of the event handling

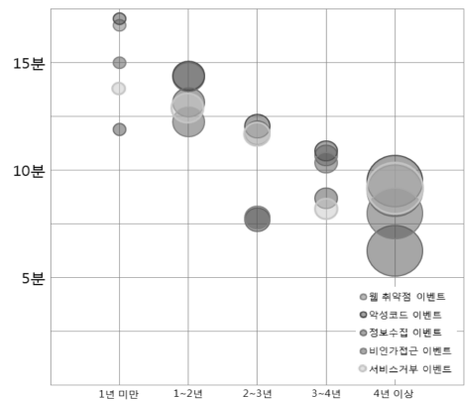

Fig. 2. Career distribution of the event handling

과 경력이 많을수록 빨라지는 것을 분포도를 통해 확인할 수 있다. Fig. 1과 Fig. 2를 통해 경력에 따른 역량기준이 영향력이 높은 것으로 나타났다. 이 같은 결과는 정보처리 분야의 자격증에 의한 소프트웨어 기술자는 IT업종의 모든 분야에 적용되고 있기 때문에 정보보호와 같은 특정 분야에서 해당 등급으로 인적 역량을 판단하기에는 다소 어려움이 있는 것으로 나타났다. 따라서 Table 1과 함께 유의미한 부(-)의 영향력을 가지는 관제경력의 평가지표를 활용하여 보안관제 인적 역량평가를 하는 것이 적합한 것으로 판단된다.

3. 보안관제 인적자원 관리 방안

본 연구에서 기관 보안관제의 인적자원 관리방안은 5단계로 구성된다. 우선 정보보안관제 업무의 정책을 기반으로 보안관제 대상 시스템의 중요도에 맞춰 일일 보안관제 목표치를 수립하고, 한편으로는 현재 업무 담당자들이 보유하고 있는 역량의 수준을 분석한다. 그 다음, 앞의 단계에서 산출된 기관 보안관제 목표치에 대해서 정보보안관제 인적 보유역량을 본 연구에서 실시한 결과를 참조하여 업무 처리 시간에 따라 적합한 인력을 산정하고, 추가적으로 인력 충원 또는 전문교육을 지원하도록 한다. Table 19에서 제시된 각각의 단계를 K기관 정보보안관제팀을 통해 실제분석으로 설명하고자 한다. K기관은 대규모의 보안관제영역을 가지고 있으며 현재 4조 2교대의 근무형태로써, 1개조에 2명씩 편성되어 총 8명이 근무를 하고 있다[12].

Table 19. 5 step quantify of Managed Security Service

기관 보안관제 목표 수립
↓
정보보안관제 인적 역량 분석
↓
일일 분석 대상 이벤트량 점검
↓
목표 대비 분석량
↓
인력 충원 또는 전문교육 지원

3.1 K 기관의 보안관제 목표 수립

정보보안관제 업무의 정확한 목표를 수립하기 위해서는 자산에 대한 위험 분석이 필요하다. 자산분석과 위협, 취약성을 통해 위험을 도출할 수 있으며 도출된 위험으로 보호되어야 할 대상 정보시스템과 조직의 위험을 측정하고, 측정된 위험이 허용 가능한 수준인지 판단 또는 평가하여 비용대비 효과적인 대응책을 제시하여 시스템 보안 정책과 대응책 구현 계획 수립 등을 진행할 수 있다. 자산의 분류기준은 기관마다 상이할 수 있으며 대체적으로 서버, 네트워크 장비, 정보보호시스템, 데이터베이스, 어플리케이션, 물리적·인적 자산, 개인PC 등이 있다. K기관은 주요정보통신기반시설을 대상으로 관제를 수행하므로 취약점 분석·평가기준에 따라 Table 20과 같이 자산 유형분류 예시를 통해 식별된 대상목록의 각 자산에 대하여 중요도를 산정한다. K기관의 관제대상은 대부분 업무PC가 차지하고 있으며, 중요도가 높지 않은 웹 서비스 등을 가지고 있다. 따라서 K기관의 서비스수준관리지표에 따라 Table 21에 중요시스템의 하(75%)의 자산가치를 설정하고, 일일 평균 관제분석 목표치에 대해 평균 경보 이벤트량의 75% 이상 분석 수행을 지표로 설정하였다.

Table 20. ex) Classification of assets

유 형	종 류
네트워크장비	네트워크와 관련된 라우터, 스위치 등
보안장비	웹 방화벽, 침입차단시스템 등
시스템장비	서비스 및 업무를 위한 서버, 제어PC (HMI) 등의 시스템을 말하며 O/S 등 소프트웨어 포함

Table 21. ex) Asset values according to importance of information systems

시스템 중요도	자산가치	시스템의 중요도 산정 기준
핵심 시스템	상(99%) 중(95%) 하(90%)	항상 일정한 성능 및 기능으로 제공 되어야 하는 시스템으로써 가용성측면이 높아 기관의 업무에 심각한 영향을 미치는 정도로써 복구에 비용 및 시간이 높은 시스템
중요 시스템	상(85%) 중(80%) 하(75%)	시스템 장애 시 다른 시스템의 기능으로 대체될 수 있으나, 반드시 복구되어야 하는 시스템
일반 시스템	상(70%) 중(65%) 하(60%)	시스템 장애 시 장기간 동안 다른 시스템의 기능으로 대체될 수 있으나, 서비스 운영에 추가적인 자원이 소모되는 시스템

3.2 K 기관의 보안관제 인적 역량 평가

이 단계에서는 앞서 본 연구에서 시행된 보안관제 인적 역량 분석을 통해 도출된 Table 22의 경력에 따른 관제 이벤트별 처리 시간을 기준으로 산정하였다.

이벤트 처리시간에 미치는 영향력이 큰 정보보안관제 경력으로 각각의 처리시간을 분석한 결과 Fig. 3의 분석결과가 나타났으며, 이는 보안관제 경보이벤트에 대해서 탐지오류 여부 및 분석, 사고 등록까지의 업무처리 시간을 나타낸 것이다. 분석 및 사고등록을 하기 위해 탐지오류 여부를 가려내야 하는데 탐지오류를 판단하는데 소요되는 시간이 처리시간의 10% 정도를 차지하고 있다. 따라서 3년 이상의 경력 기준으로 탐지오류 판단 소요시간은 약 1분 정도가 소요되는 것으로 판단된다.

Table 22. Event handling time according to career

구분	웹취약점	악성코드	정보수집	비인가접근	서비스거부	평균
1년 미만	3.35	3.41	2.38	3.00	2.75	2.9
1-2년	2.87	2.88	2.63	2.45	2.57	2.6
2-3년	2.35	2.41	1.54	1.56	2.33	2
3-4년	2.14	2.18	1.74	2.07	1.64	1.9
4년 이상	1.81	1.90	1.25	1.60	1.83	1.6

※ 1 = 5분, 2 = 10분 이하, 3 = 15분 이하, 4 = 20분 이하, 5 = 20분 이상

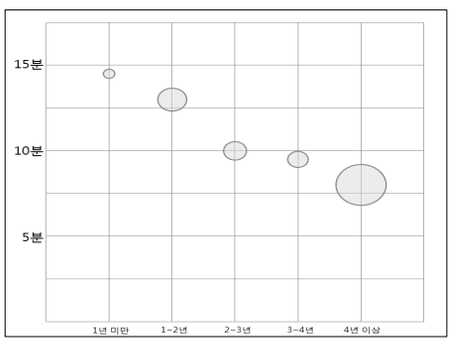

Fig. 3. Average processing time distribution according to career

3.3 K 기관의 보안관제 인적 역량 평가

일일 보안관제 이벤트의 발생량에 따른 인적 정량화를 위해 K기관의 일일 평균 관제 경보이벤트에 대해서 분석을 실시하였다. K기관은 하루 평균 3만건 정도의 경보이벤트가 발생하였고, 정확한 분석대상을 도출하기위해 정책에 의해 확정된 탐지차단 건에 대해서만 수행하였다. Table 23은 중복탐지건을 제외한 관제요원의 확인 대상인 이벤트이다.

Table 23. Daily analysis target events of K Institutions

구분	경보이벤트
차단	1769
[비인가접근]	127
[서비스거부공격]	606
[악성코드]	272
[웹해킹]	759
[정보수집]	5
탐지	6555
[비인가접근]	397
[서비스거부공격]	2074
[악성코드]	1036
[웹해킹]	3010
[정보수집]	38
총합계	8324

3.4 K 기관의 보안관제 목표 대비 분석량

앞서 3.1에서 기관 보안관제 목표를 위해 대상 시스템의 규모와 중요도 등을 산정하여 75% 수준의 관제가 필요하다고 판단하였다. 2절에서 확인된 2년~3년 이상의 경력자 기준 탐지 판단 소요시간이 1분, 2년 이하는 1.3분이 소요되므로 현재 근무하고 있는 인력의 경력을 기준으로한 일일 이벤트판단 건수는 Table 24와 같다. 3.3절에서의 중복된 탐지건을 제외한 일일 최소 분석 대상 신규 이벤트량인 약 8천3백건에 대하여 기관에서 기관 관제 목표치를 적용하여 이벤트량에 대해서 알맞은 인력으로 운영하고 있는지 확인한 결과, Table 25에서 도출된 일일 최소 이벤트가 Table 24의 일일 분석량 보다 약 1,148건 정도 미흡한 것으로 나타났다.

Table 24. Daily analysis events of K Institutions

구 분 (경력)	일일이벤트 판단 건수 (1명 기준)	근무인원 (1일기준)	일일이벤트 판단 건수 합계
2년 이하	1,107건	2명	2,215건
2년 이상	1,440건	2명	2,880건
총합계	2,547건	4명	5,095건

Table 25. Daily analysis aims of K Institutions

구분	경보 이벤트	관제 목표치	일일최소목표량
차단	1,769		1,326
[비인가접근]	127		95
[서비스거부공격]	606		454
[악성코드]	272		204
[웹해킹]	759		569
[정보수집]	5		3
탐지	6,555	75%	4,916
[비인가접근]	397		297
[서비스거부공격]	2,074		1,555
[악성코드]	1,036		777
[웹해킹]	3,010		2,257
[정보수집]	38		28
총합계	8,324		6,243

3.5 K 기관의 보안관제 대책

3.4절에서의 결과를 토대로 인력 충원 또는 전문교육 지원 등의 역량강화가 이루어져야 기관의 일일 관제 분석량이 관제 목표치를 상회할 수 있다. 전문교육에는 취약점 분석 등의 교육 보다는 시스템보안, 네트워크보안, 응용소프트웨어보안 등의 세분화되고 집중적인 교육이 관제요원의 역량을 강화하는데 많은 직·간접적인 효과를 얻을 수 있다. 앞서 3.4절에서 도출된 K기관의 관제 목표 미달수치인 1,148건을 충족하기 위해서는 관제근무사의 전문교육 또는 시스템 자동화 등으로 향상시키거나, 3년 이상 경력의 직원이 4개조에 1명씩, 총 4명 정도 더 요구되는 것으로 확인되었다.

4. 결 론

오늘날 급격한 정보통신의 발달로 그 의존도가 가파르게 상승하고 있다. 이에 따라 사이버공격 또한 무자비한 파괴에서 금전적 이득 또는 범국가적인 형태로 발생되고 있다. 최근 우리나라에서는 개인정보 탈취, 금융정보 탈취 등 피해가 속출하고 있다. 최근 발생한 개인정보 누출 규모는 약 1억 3천만 건으로 국민 모두의 개인정보가 유출됐다는 이야

기다[17]. 또한 시스템 파괴 목적의 해킹 공격도 그 사례가 더욱 지능적이고 고도화되어 더욱더 정보보안관제의 중요성이 강조되고 있다. 하지만 정보보호관제 인력의 처우는 소프트웨어등급단가 기준으로 처리하고 있어 비용 및 업무강도로 인해 기피하는 직종으로 분류되고 있다. 이를 개선하기 위해서는 많은 지식을 습득해야 하는 정보보호인력에 대한 처우개선이 필요한데, 정보보안관제근무는 24시간 정해진 순번에 따른 근무 특성 때문에 휴가나 다른 업무를 할 수가 없다. 설문조사결과에서도 대부분 사회초년생이나 2~3년차에 응답자들이 분포하고 있는 것을 알 수 있다. 기관에 알맞은 인력을 운용하기 위해서는 본 논문에서의 역량분석 및 정량화에 따른 실제 적용결과에 따라 관제 경력과 보안관제이벤트별로 개인의 역량을 파악하여 일반직원에 비해 조금 더 보상을 하는 것이 적합하다. 분석 예로 든 K기관에서는 적합한 보안관제를 위해 외주용역 계약으로 8명이 충원되어 1개조에 4명이 근무를 하고 있지만 소프트웨어기술단가를 기준으로 용역비가 산출되었다. 본 논문에서는 일반적인 보안관제에서의 공통적인 업무(기술)을 도출하여 분석을 하였지만 개개인의 정확한 실력을 검증하기 위해서는 추가적인 연구를 통해 향후 전문자격증제도 뿐만 아니라 처우개선을 위한 정책연구가 필요할 것이다.

References

[1] Ministry of the Interior [Internet], http://www.moi.go.kr/, Oct., 2014.

[2] Young-jin Kim, Su-yeon Lee, Hun-young Kwon, and Jong-in Lim, “A Study on the Improvement of Effectiveness in National Cyber Security Monitoring and Control Services,” *Jonornal of The Korea Institute of Information Security & Cryptology*, Vol.19, No.1, pp.103-111, Feb., 2009.

[3] Korea Internet & Security Agency, “INTERNET & SECURITY FOCUS,” Aug., 2013.

[4] Hyun-do Lee and Sang-jin Lee, “A Study on development of evaluation indicators on the Managed Security,” *Jonornal of The Korea Institute of Information Security & Cryptology*, Vol.22, No.5, pp.1133-1143, Oct., 2012.

[5] Ja-young Oh, “What's Managed Security Service,” boannews, Dec., 2006.

[6] Woo-jong Suh, Dae-seok Kang, Yong-won Kang, and Jin-won Hong, “A Competency Analysis Methodology for Improving the Productivity of IT Human Resources,” *The Journal of Productivity*, Vol.22, No.1, pp.69-91, Feb., 2008.

[7] Wan-suk Yi, Woong Go, Dong-ho Won, and Jin Kwak, “Development of S-SLA's Grading Indicator based on the Analyses of IPS's Security Functions,” *Jonornal of The Korea Institute of Information Security & Cryptology*, Vol.20, No.6, pp.221-235, Dec., 2010.

[8] Korea Software Industry Association [Internet], http://www.sw.or.kr/.

[9] Hyun-jeong Cho, “IPS, the future network security product,” *Journal of Computing Science and Engineering*, Vol.23, No.1, pp.21-26, Jan., 2005.

[10] Young-su Jang, “Sofeware security vulnerability improvement using open static analysis tool,” Korea Unviersity, Feb., 2011.

[11] Alberto Dainotti, Antonio Pescape, and Giorgio Ventre, “A Packet-level Characterization Of Network Traffic,” *CAMAD*, pp.38-45, June, 2006.

[12] Joong-gil Park, “Methodology of Analyze the Risk Using Method of Determinated Quantity,” *The Journal of Information Processing System*, Vol.13, No.7, pp.851-858, Dec., 2006.

[13] The Open Web Application Security Project(OWASP) Project Handbook 2013 [Internet], http://owasp.org/, Oct., 2012.

[14] Jin-kook Kim, Jung-heum Park, and Sang-jin Lee, “A Framework for Data Recovery and Analysis from Digital Forensics Point of View,” *Journal of Information Processing Systems*, Vol.17, No.5, pp.391-398, Oct., 2010.

[15] Jae-Chan Moon and Seong-je Cho, “Vulnerability Analysis and Threat Mitigation for Secure Web Application Development,” *Jonornal of Korea Society of Computer*, Vol.17, No.2, pp.127-137, Feb., 2012.

[16] Chae-tae Im, Joo-hyung Oh, and Hyun-cheol Jeong, “Study of Technical Trends and Analysis Method of Recent Malware,” *Journal of Computing Science and Engineering*, Vol.28, No.11, pp.117-126, Nov., 2010.

[17] Noh Ung-rae congressman [Internet], http://blog.naver.com/with_wraenoh/220480698919, Sep., 2015.

양 성 호

e-mail : sevencores@klid.or.kr

2008년 동명대학교 컴퓨터공학부(학사)

2010년~현 재 고려대학교 정보보호대학원 정보보호학과 석사과정

2010년~현 재 한국지역정보개발원 책임연구원

관심분야 : 디지털 포렌식, 보안관제, 모의해킹 등

이 상 진

e-mail : sangjin@korea.ac.kr

1987년 고려대학교 수학과(학사)

1989년 고려대학교 수학과(석사)

1994년 고려대학교 수학과(박사)

1989년~1999년 ETRI 선임연구원

1999년~2001년 고려대학교 자연과학대학 조교수

2001년~현 재 고려대학교 정보보호대학원 교수

2006년~현 재 한국디지털포렌식학회장

2008년~현 재 고려대학교 정보보호연구원 디지털포렌식센터장

관심분야 : 디지털 포렌식, 모바일 포렌식, 심층 암호, 해쉬 함수