Journal of KIIT. Vol. 18, No. 4, pp. 109-119, Apr. 30, 2020. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2020.18.4.109

보안 7대 위협을 이용한 ISMS-P 인증효과에 관한 연구: 기업규모와 경력 중심으로

김동현*, 이윤호**

A Study on the ISMS-P Accreditation Effect Using the Seven Threats of Security - Focused on Enterprise Size and Career

Dong Hyun Kim*, Younho Lee**

이 연구는 서울과학기술대학교 교내 연구비의 지원으로 수행되었습니다.

요 약

정보보호 침해 사례의 증가로 인한 기업의 매출 감소, 이미지 손실은 기업에게 정보보호 관리체계 도입의 부담을 증가시키고 있다. 그럼에도 불구하고, 정보보호 관리체계 도입 시, 어떤 효과를 야기하는지에 대한 확인 사례가 없던 이유로 기업들은 정보보호 관리체계의 도입을 주저하고 있는 실정이다. 본 연구에서는 경력과 회사규모가 다른 IT 종사자 50명에게 정보보호 표준인 ISMS-P의 보안요소가 한국인터넷진흥원이 발표한 보안 7대 위협에 대해 자신의 회사를 얼마나 보호할 수 있는지에 대한 효과와 관련하여 설문을 수집하고, 이를 바탕으로 분산분석과 회귀분석을 통해 정보보호 관리체계의 효과성에 대해 분석을 진행한다. 우리는 본 연구의 결과가 기업의 ISMS-P 인증의 중요성과 체계 도입을 위한 근거자료가 되며, 또한 정보보호 가이드라인 수립이 어려운 스타트업 기업, 중소기업의 보안 체계 수립을 위해 도움이 되기를 희망한다.

Abstract

Increasing the cases of information security breaches has led to a decline in sales and an impairment of companies' reputations. To avoid this, the number of companies which start to use information security management system, is steeply increasing. However, there have been no case studies regarding the effect of the use of information security management systems. In this study, we surveyed 50 IT workers with different careers and companies. The questionnaire is about how much you can protect your company against the seven security threats announced by the Korea Internet & Security Agency when you introduce each security element of ISMS-P. Based on this, the effectiveness of the information security management system was analyzed through analysis of variance and regression. We hope that this study will be the basis for the importance of ISMS-P certification of companies and the introduction of the system, and it will be helpful for the establishment of security system for start-up companies and small and medium-sized companies that are difficult to establish information security guidelines.

Keywords
ISMS-P, information security management system, ANOVA, regression, security

* 서울과학기술대학교 IT정책전문대학원 산업정보시스템 전공 석사
- ORCID: https://orcid.org/0000-0002-3493-9839
** 서울과학기술대학교 산업공학과 ITM전공 교수 (교신저자)
- ORCID: https://orcid.org/0000-0003-1767-6165

· Received: Mar. 04, 2020, Revised: Mar. 26, 2020, Accepted: Mar. 29, 2020
· Corresponding Author: Younho Lee
Dept. of Industrial Engineering, Seoul Tech., Korea,
Tel.: +82-2-970-7283, Email: younholee@seoultech.ac.kr

Ⅰ. 서 론

한국은 과거와 달리 반도체, 2차 전지, 스마트폰 등 최첨단 기술을 바탕으로 한 기술 혁신 모델을 적용, 많은 변화를 이루어 내었다. 과거에는 해외 기술의 활용에 의존했던 이유로 기술 보호에는 소극적이었고, 중소/벤처 기업 등의 기술 유출 방지 시스템 체계는 매우 미흡하였다. 그러나 1998년, 삼성전자 반도체 기술 유출 사건[1]을 계기로 기술 보호의 필요성이 제기되면서 부정경쟁 방지 및 영업비밀 보호에 관한 법률[2], 2007년 핵심기술의 적극적인 보호를 위한 산업기술의 유출 방지 및 보호에 관한 법률[3]이 제정되었다. 이러한 법률에도 불구하고, 일반적인 기업들은 고위 경영진의 보안에 대한 지식과 경험이 부족하여 전담조직 없이 법률만으로 기술 자산에 대한 보호 효과는 어려운 실정이다[4].

이 같은 문제 인식을 바탕으로 법률적 접근보다 통합기술보안체제의 기능을 하는 국제 표준에 대해 효과적 활용방안이 대두되었고, 2013년 한국인터넷진흥원은 국제 표준 ISO27001을 기반으로 ISMS (Information Security Management System) 체계를 개발하였다. ISMS에는 80개의 보호 조치 기준이 있고, 정보통신 관련 사업자 여부, 연 매출 및 시스템 운영 조건에 따라 의무실시를 법률로 정하여 사이버 공격에 대응하는 보호 조치 기준이 마련되어 있다[5]. 또한 ISMS는 2019년에는 분리되어 있던 개인정보보호 관리체계와 통합되어 ISMS-P(Personal information & ISMS)로 진화하였고, 이와 동시에 보호 조치 기준이 22개 증가하였다.

그러나 불행히도 현재까지 이러한 증가 및 이를 바탕으로 한 인증체계의 활용은 증가하였지만, 이의 효과성에 대한 분석은 거의 전무한 실정이다. 본 연구에서는 ISMS-P의 효과성을 검증하기 위해 한국인터넷진흥원과 국내 주요 보안 회사가 공동으로 발표한 보안 7대 위협에 대해 ISMS-P의 보안 인증요소들이 각 위협을 얼마나 방어할 수 있을지에 대한 요인 분석을 진행한다. 그 결과 기술적 평균은 리커드 7척 점도[6]에서 4점 이상 획득하여 효과가 있다는 결과를 얻을 수 있었다. 또한 IT 경력과 기업의 구분에 대한 6개의 가설에 대해 ANOVA 분석[7] 결과 차이가 없다는 결론을 얻을 수 있었다.

본 논문의 구성은 다음과 같다. 2절에서는 선행 연구를 기술하고, 3절에서는 분석 대상 자료 및 분석 모형을 기술한다. 4절에서는 실증분석을 수행하고, 5절에서는 결론을 맺는다.

Ⅱ. 선행 연구

본 절에서는 선행 연구 중 보안 위협에 대응하기 위해 사용하는 ISMS-P 체계와 한국인터넷진흥원이 제시한 보안 7대 위협에 대해 상세히 기술한다.

2.1 ISMS-P

ISMS-P는 개인정보보호를 포함하는 정보보호의 절차와 과정을 체계적으로 문서화하여, 이에 대한 지속적 관리 및 효율적인 운영을 위한 일련의 과정 및 활동을 말한다. 이러한 과정 및 활동을 통해 ISMS-P는 정보자산의 기밀성, 무결성, 가용성을 실현하는 것을 목표로 하며, 이를 통해 비즈니스의 안정성을 재고할 수 있고, 윤리 및 투명 경영을 위한 정보보호 관련 법적 준거성을 확보할 수 있다. 또한 침해 사고나 집단 소송에도 ISMS-P 인증기관은 경제적 피해를 최소화할 수 있다. 또한 ISMS-P 인증은 정보보호와 관련하여 대외 이미지 및 신뢰도 향상에 기여할 수 있다. 뿐만 아니라 정보기술 관련 정부 수행과제 입찰시 인센티브를 부여받을 수 있다[8].

표 1은 ISMS-P의 구성을 나타낸다. 구성은 관리체계 수립 및 운영 16개 항목, 보호 대책과 요구사항 64개 항목, 그리고 개인정보처리 별 요구사항의 22개 단계로 구성되어 있다[5].

표 2에는 ISMS-P을 의무적으로 인증 받아야 하는 기관을 명시하고 있다. 전기통신사업 및 정보통신서비스에 해당 하는 기업들이 속하고 있음을 확인할 수 있다. 해당 기관들은 미 인증 시 최대 3000만원 이하의 과태료가 부과된다[5]. 또한 해당 의무기관이 아니더라도 정보보호 관리체계를 구축, 운영을 하거나 필요로 하는 기업들은 인증 취득이 가능하다. 인증을 받은 기업들은 윤리 및 투명 경영을 위한 법적 준거성 및 대외 이미지 및 신뢰도 향상이 가능하다.

표 1. ISMS-P의 구성
Table 1. Organization of ISMS-P

통합인증	분야(인증기준 개수)	
1. 관리체계 수립 및 운영 (16)	1.1 관리체계 기반 마련(6) 1.3 관리체계 운영(3)	1.2 위험관리(4) 1.4 관리체계 점검 및 개선(3)
2. 보호대책 요구사항 (64)	2.1 정책, 조직, 자산 관리(3) 2.3 외부자 보안(4) 2.5 인증 및 권한 관리(6) 2.7 암호화 적용(2) 2.9 시스템 및 서비스 운영관리(7) 2.11 사고 예방 및 대응(5)	2.2 인적보안(6) 2.4 물리보안(7) 2.6 접근통제(7) 2.8 정보시스템 도입 및 개발 보안(6) 2.10 시스템 및 서비스 보안관리(9) 2.12 재해복구(2)
3. 개인정보처리 단계별 요구사항 (22)	3.1 개인정보 수집 시 보호조치(7) 3.3 개인정보 제공 시 보호조치(3) 3.5 정보주체 권리보호(3)	3.2 개인정보 보유 및 이용 시 보호조치(5) 3.4 개인정보 파기 시 보호조치(4)

표 2. ISMS-P 의무대상자
Table 2. Organizations mandatory to obtain ISMS-P certification

대상자 기준	세부분류 (정보통신 서비스 제공자)	비고
(ISP)전기통신사업법의 전기통신사업자로 전국적으로 정보통신망 서비스를 제공하는 사업자	인터넷접속 서비스, 인터넷전화 서비스 등	서울 및 모든 광역시에서 정보통신망 서비스제공
(IDC)타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자	서버호스팅, 코로케이션 서비스 등	정보통신 서비스부문 전년도 매출액 100억 이하인 영세 VIDC 제외
(매출액 및 이용자기준)연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 매출액 100억 또는 이용자수 100만 명 이상인 사업자	인터넷 쇼핑몰, 포털, 게임, 예약, Cable-SO 등	정보통신서비스 부문 전년도 매출액 100억 이상 또는 전년도말 기준 직전 3개월간 일일평균 이용자수 100만 명 이상
	상급종합병원 대학교	직전연도 12월31일 기준으로 재학생 수가 1만명 이상인「고등교육법」제2조에 따른 학교

2.2 보안 7대 위협

한국인터넷진흥원은 2014년 12월부터 구성 운영 중인 사이버 위협 인텔리전스 네트워크에 참여하는 국내 주요 보안업체 6개사 (안랩, 이스트 시큐리티, NSHC, 하우리, 잉카인터넷, 빛 스캔)와 함께 2019년 주목해야 할 7대 사이버 공격 전망을 발표했다[9].

2019년 사이버 보안을 화두로 ① 다양한 경로를 통한 크립토 재킹 확산, ② 소셜 네트워크를 이용한 악성코드 유포, ③ 엔드 포인트 보안취약점을 겨냥한 공격, ④ 지능화된 스피어피싱과 APT 공격, ⑤ 사물인터넷을 겨냥한 신종 사이버 위협, ⑥ 소프트웨어공급망 관련 사이버 공격 증가, ⑦ 악성 행위 탐지를 우회하는 공격 기법의 진화에 대한 위협이 있으며, 상세내용은 표 3과 같다[9].

III. 분석 자료 및 분석 모형

본 절에서는 분석 자료에 대해 소개하고, 분석 모형 및 가설을 설정한다.

3.1 분석 자료

본 연구에서 수행할 분석을 위해 수집한 자료는 [ISMS-P와 보안7대 위협 요소 간 관계연구 설문]이라는 제목으로 IT 실무자 50명을 대상으로 설문을 실시하여 획득하였다. 분석의 정확도를 높이기 위해 30명 이상의 설문을 받아 표본의 정규성을 보장 받으려고 노력하였으며, 가용한 시간 자원 내에서 최대한의 설문을 받기 위해 노력하였다.

표 3. 2018/2019년 사이버 공격 상세
Table 3. Details of the 2018/2019 cyber attack outlook

2018년 보안위협 현황	2019년 보안위협 전망
① 다양한 경로를 통한 크립토 재킹 확산 : 안랩	
1) 다양한 경로와 유포기법 사용 2) 기업 서버를 대상으로 마이너 악성코드 감염 3) 백신의 업데이트 방해 및 감염인지 어렵도록 교묘하게 동작	1) 모바일 기기 보편화로 인한 채굴 악성 2) 취약한 IoT 기기를 대상으로 대량 감염 및 채굴 3) 웹브라우저에서 동작하는 채굴 스크립트
② 소셜 네트워크를 이용한 악성코드 유포 : 이스트 시큐리티	
1) SNS 해킹 2) SNS을 이용한 연예인 계정 해킹과 송금유도 3) 피싱사이트 활보	1) SNS를 이용한 대규모 악성코드 유포 2) SNP (Social Network Phishing) 지능화 3) SNS을 이용한 Spear Phishing
③ 엔드포인트 보안취약점을 겨냥한 공격 : NSHC	
1) 정상 S/W 기능을 이용한 악성코드 감염기법 증가 2) 인증서 도용 및 S/W 업데이트 기능 이용한 악성코드 유포 증가 3) CPU 취약점을 이용한 악성코드 활용	1) 스크립트 악성코드와 윈도우 OS 시스템의 관리 기능을 이용한 공격 심화 2) 공개용 코드와 모의해킹 S/W를 활용한 공격심화 3) 보안 S/W 정상기능을 악성코드 감염 및 제어 수단으로 활용
④ 지능화된 스피어피싱과 APT 공격 : 하우리	
1) 암호화폐, 부동산, 증시 등 민감한 사회 이슈를 이용한 공격 지속 2) 공개 소프트웨어 활용 3) 워터링 홀을 통해 Active X를 이용한 APT 공격	1) 인공지능 기술로 강화된 개인 맞춤형 스피어피싱 메시지 및 공격 등장 2) 가짜뉴스 등 자극적 이슈 소재를 이용한 악성코드 유포 가능성 증대 3) 보안이 취약한 중소기업을 대상으로 한 APT 공격 증대
⑤ 사물인터넷을 겨냥한 신종 사이버 위협 : 잉카인터넷	
1) IP카메라, 음성인식스피커 등 스마트홈 기기 사용에 증가에 따른 사이버 위협 증가 2) 스마트카, 교통 시스템, 전력망 등 도시 인프라 대상 사이버 공격 발생 3) 스마트 냉장고, 차량 블루투스 해킹 시연	1) IoT 봇넷의 변종 및 다양한 봇넷 출현으로 IoT 기기의 좀비 기기화 증가 2) IoT 봇넷을 이용한 DDos 공격으로 블록체인 및 암호화폐 네트워크 공격 3) 좀비화된 IoT 기기를 통한 개인정보 탈취 및 악성코드 유포의 숙주로 악용
⑥ 소프트웨어공급망 관련 사이버 공격 증가 : 빛스캔	
1) 개발업체 대상 사이버 공격으로 홈페이지 서비스 중단 사고 발생 2) 쇼핑몰 웹 솔루션 업체의 S/W 취약점을 악용한 웹해킹 3) 소프트웨어 코드서명 인증서가 해킹으로 외부에 유출	1) 소프트웨어, 웹사이트 대상 공격증가 2) 소프트웨어 취약점을 악용한 해킹 및 정보유출 증가 3) 소프트웨어 코드서명 인증서를 해킹하는 공격증가
⑦ 악성 행위 탐지를 우회하는 공격 기법의 진화에 대한 위협 : 한국인터넷 진흥원	
1) 공격의 흔적을 지우고 악성기능을 모듈화한 IoT 봇넷 VPN 필터 등장 2) 백신탐지를 우회하는 초소형 POS (PinkKite, TinyPOS) 악성코드 등장 3) 안티 머신러닝 기능을 갖추고 있는 파이록키 랜섬웨어 발견	1) DGA를 이용하여 C&C 차단을 회피하는 악성코드 증가 2) 머신러닝기반 백신 및 탐지 시스템을 우회하는 사이버 위협의 진화 3) 패치관리, 보안관리 등 중앙관리 S/W의 취약점을 악용한 공격 지속

설문내용은 모집단의 정확성을 높이기 위해 ⓐ IT 전공자, IT분야 종사자인지 확인하였고(O, X), ⓑ 회사경력 및 연구경력(0~5년, 5~10년, 10~15년, 15년 이상)을 통해 다양성을 확보했다. 또한 ⓒ 종사하고 있는 회사의 종업원 수를 (0~50명, 50~100명, 100~300명, 300~500명, 500명~1000명, 1,000명 이상)의 범주 중 하나로 파악하여 기업의 규모를 확인하였다.

설문 항목은 ISMS-P의 보안 인지 요소인 [(1) 관리체계 기반 마련, (2) 위험관리, (3) 관리체계 운영, (4) 관리체계 점검 및 개선, (5) 정책, 조직, 자산 관리, (6) 인적보안, (7) 외부자 보안, (8) 물리보안, (9) 인증 및 권한 관리, (10) 접근 통제, (11) 암호화 적용, (12) 정보시스템 도입 및 개발 보안, (13) 시스템 및 서비스 운영관리, (14) 시스템 및 서비스 보안관리, (15) 사고 예방 및 대응, (16) 재해복구, (17) 개인정보 수집 시 보호조치, (18) 개인정보 제공 시 보호조치, (19) 개인정보 파기 시 보호조치, (20) 정보주체 권리 보호]의 적용이 보안 7대 위협 [① 다양한 경로를 통한 크립토 재킹 확산, ② 소셜 네트워크를 이용한 악성코드 유포, ③ 엔드포인트 보안 취약점을 겨냥한 공격, ④ 지능화된 스피어피싱과 APT 공격, ⑤ 사물인터넷을 겨냥한 신종 사이버 위협, ⑥ 소프트웨어 공급망 관련 사이버 공격 증가, ⑦ 악성 행위 탐지를 우회하는 공격 기법의 진화에 대한 위협]에 대하여 설문 참여자 본인의 회사의 정보자산을 잘 보호할 수 있는지 7점의 리커드 척도(Likert scale)를 사용하여 평가하였다.

0점에 가까울수록 전혀 효과가 없다는 것을 의미하고, 7점에 가까울수록 매우 효과가 있는 것으로 답하도록 하였다. 표 4는 설문조사 응답자의 현황이다.

표 4. 설문 응답 현황
Table 4. Details of the survey response

ⓐ IT 전공자, IT분야 종사자		ⓑ 회사경력 및 연구경력		ⓒ 종사하고 있는 회사의 종업원 수	
O	50	0 ~ 5년	10	0~50명	3
		5 ~ 10년	6	50~100명	3
X	5	10 ~ 15년	15	100~300명	9
		15년 ~	19	300~500명	5
				500~1,000명	8
				1,000명~	22

설문 항목 중 ISMS-P 보안인지 요소는 표 1의 대분류 항목인 관리체계 수립 및 운영, 보호 대책 요구사항, 개인정보처리 단계별 요구사항의 3가지 항목에 대한 평균으로 합 처리하였다. 그 후 ANOVA 일원 배치 분석 및 사후 분석을 진행하였다.

3.2 가설 설정

정보보호를 위한 대부분의 선행연구는 우리나라의 산업기술보호를 위한 제도가 정착된 기간이 짧아 주로 산업기술보호, 정보보호를 위한 법적, 제도적 문제점이나 지원 등을 주로 다루었다. 반면 전술한 바와 같이 정보보호 제도나 그 영향요인을 분석한 선행연구는 거의 없었다.

본 연구는 ISMS-P를 이용하여 보안 7대 위협의 방어 효과성을 평가하였을 때, ⓑ 회사경력 및 연구경력과 ⓒ 종사하고 있는 회사의 종업원 수 상관없이 차이 없이 응답자들이 위협에 대한 방어에 효과가 있을 것으로 예상했다. 가설 설정은 표 5와 같다.

표 5. 가설 설정
Table 5. Hypothesis setup

가설 설정
1. 경력과 상관없이 관리체계 수립 및 운영에 대한 중요성은 유의한 차이가 있다.
2. 회사규모와 상관없이 관리체계 수립 및 운영에 대한 중요성은 유의한 차이가 있다.
3. 경력과 상관없이 보호대책 요구사항에 대한 중요성은 유의한 차이가 있다.
4. 회사규모와 상관없이 보호대책 요구사항에 대한 중요성은 유의한 차이가 있다.
5. 경력과 상관없이 개인정보처리 단계별 요구사항에 대한 유의한 차이가 있다.
6. 회사규모와 상관없이 개인정보처리 단계별 요구사항에 대한 유의한 차이가 있다.

Ⅳ. 실증분석 결과

수집한 설문이 분석 자료로 사용가능 유무를 분산 동질성 검사를 통해 타당성을 검토한다. 이를 위해 구체적으로, 본 연구에서 수집한 설문의 기술적 평균을 확인하고, 표 5에 설정한 가설에 관해 확인한다.

4.1 모집단의 분산 동질성 확인

모집단의 분산 동질성 확인을 통해 해당 데이터가 사용 가능한지의 여부를 확인하였다. 그 결과는 표 6과 같다.

표 6. 회사경력 및 연구경력에 따른 ISMS-P 동질성 검증
Table 6. Verification of ISMS-P homogeneity according to the length of the company experience and research experience

구분	Levene 통계량	df1	df2	유의 확률
관리체계 수립 및 운영	.707	3	46	.552
보호대책 요구사항	1.889	3	46	.145
개인정보처리 단계별 요구사항	2.253	3	46	.095

표 7. 종사하고 있는 회사의 종업원 수에 따른 ISMS-P 검증
Table 7. Verification of ISMS-P homogeneity according to the number of the employees in the companies for which the responders work

구분	Levene 통계량	df1	df2	유의 확률
관리체계 수립 및 운영	1.481	5	44	.215
보호대책 요구사항	.944	5	44	.462
개인정보처리 단계별 요구사항	.753	5	44	.588

표 8. 회사경력 및 연구경력에 따른 보안 7대 위협 응답 동질성 검증
Table 8. Verification of homogeneity of the reponses regarding the seven major security threats according to the length of the company and research experiences

구분	Levene 통계량	df1	df2	유의 확률
다양한 경로를 통한 크립토재킹 확산	1.333	3	46	.275
소셜 네트워크를 이용한 악성코드 유포	2.300	3	46	.090
엔드포인트 보안취약점 겨냥한 공격	2.421	3	46	.078
지능화된 스피어피싱과 APT공격	2.179	3	46	.103
사물인터넷을 겨냥한 신종 사이버 위협	1.277	3	46	.293
소프트웨어 공급망 관련 사이버 공격 증가	1.538	3	46	.217
악성행위를 탐지를 위회하는 공격기법 증가	1.718	3	46	.176

표 6의 내용과 같이 회사경력 및 연구경력에 따른 ISMS-P의 동질성 검증 결과 유의 확률이 “관리체계 수립 및 운영”은 .552, “보호대책 요구사항”에서는 .145, 마지막으로 “개인정보처리 단계별 요구사항”은 .095로 모두 유의 확률 0.05 이상임을 확인할 수 있다. 따라서 모든 경우에 동질성이 있음을 확인할 수 있었다.

또한 표 7은 종사하고 있는 회사의 종업원 수에 따른 각 가설의 ISMS-P 동질성 검증결과를 보여 주고 있다. 그 결과, “관리체계 수립 및 운영”은 .215, “보호대책 요구사항”은 .462, “개인정보처리 단계별 요구사항”은 .588로 유의 확률 0.05이상이므로 동질성이 있음을 결론내릴 수 있다.

표 8과 같이 회사경력 및 연구경력에 따른 보안 7대 위협 동질성 검증 결과, 다양한 경로를 통한 크립토 재킹 확산 .275, 소셜 네트워크를 이용한 악성코드 유포 .090, 엔드 포인트 보안취약점을 겨냥한 공격 .078, 지능화된 스피어피싱과 APT 공격 .103, 사물인터넷을 겨냥한 신종 사이버 위협 .293, 소프트웨어 공급망 관련 사이버 공격 증가 .217, 악성행위 탐지를 우회하는 공격 기법의 진화에 대한 위협 .176로 모두 유의 확률이 0.05 이상이며 따라서 동질성이 있다 결론 내렸다.

표 9. 종사하고 있는 회사의 종업원 수에 따른 보안 7대 위협 응답 동질성 검증
Table 9. Verification of homogeneity of the reponses regarding the seven major security threats according to the number of the employees in the companies to which the responders belong

구분	Levene 통계량	df1	df2	유의 확률
다양한 경로를 통한 크립토재킹 확산	.833	5	44	.533
소셜 네트워크를 이용한 악성코드 유포	1.237	5	44	.308
엔드포인트 보안취약점 겨냥한 공격	1.067	5	44	.392
지능화된 스피어피싱과 APT공격	1.818	5	44	.129
사물인터넷을 겨냥한 신종 사이버 위협	1.145	5	44	.351
소프트웨어 공급망 관련 사이버 공격 증가	1.368	5	44	.255
악성행위를 탐지를 위회하는 공격기법 증가	.565	5	44	.726

표 9와 같이 종사하고 있는 회사의 종업원 수에 따른 보안 7대 위협 동질성 검증 결과, 다양한 경로를 통한 크립토 재킹 확산 .533, 소셜 네트워크를 이용한 악성코드 유포 .308, 엔드 포인트 보안취약점을 겨냥한 공격 .392, 지능화된 스피어피싱과 APT 공격 .129, 사물인터넷을 겨냥한 신종 사이버 위협 .351, 소프트웨어 공급망 관련 사이버 공격 증가 .255, 악성 행위 탐지를 우회하는 공격 기법의 진화에 대한 위협 .726로 유의 확률이 0.05 이상이므로 동질성이 있었다. 수집한 데이터 모두 데이터의 분산 동질성을 만족하여 분석 데이터의 타당성을 증명했다.

4.2 ISMS-P를 이용한 보안 7대 위협 방어 효과성 확인

표 10과 같이 ISMS-P을 이용한 보안 7대 위협에 대한 7점 리커드 척도의 기술적 평균을 확인하였다.

표 10. ISMS-P의 보안 7대 위협에 대한 효과에 7점 리커트 척도 분석
Table 10. Evaluation result of 7-point Likert scale for untility of ISMS-P for each of 7 security threats

7대 위협	7점 척도
다양한 경로를 통한 크립토 재킹확산	4.26
소셜 네트워크를 이용한 악성코드 유포	4.32
엔드 포인트 보안 취약점 겨냥한공격	4.35
지능화된 스피어피싱과 APT공격	4.43
사물인터넷을 겨냥한 신종사이버위협	4.23
소프트웨어 공급망 관련 사이버 공격 증가	4.52
악성 행위탐지를 우회하는공격기법의진화	4.39

다양한 경로를 통한 크립토 재킹 확산 4.26, 소셜 네트워크를 이용한 악성코드 유포 4.32, 엔드 포인트 보안취약점을 겨냥한 공격 4.35, 지능화된 스피어피싱과 APT 공격 4.43, 사물인터넷을 겨냥한 신종 사이버 위협 4.23, 소프트웨어 공급망 관련 사이버 공격 증가 4.52, 악성 행위 탐지를 우회하는 공격 기법의 진화에 대한 위협 4.39로 모두 4.0 이상을 넘어 보안 효과가 있다는 것을 확인할 수 있었다.

4.3 가설 확인 및 검증

앞서 설정한 6가지 가설인 (1) “경력과 상관없이 관리체계 수립 및 운영에 대한 중요성의 인식은 유의한 차이가 있다.”, (2) “회사규모와 상관없이 관리체계 수립 및 운영에 대한 중요성의 인식은 유의한 차이가 있다.”, (3) “경력과 상관없이 보호대책 요구사항에 대한 중요성의 인식은 유의한 차이가 있다.”, (4) “회사규모와 상관없이 보호대책 요구사항에 대한 중요성의 인식은 유의한 차이가 있다.”, (5) “경력과 상관없이 개인정보처리 단계별 요구사항에 대한 중요성의 인식은 유의한 차이가 있다.”, 그리고 (6) “회사규모와 상관없이 개인정보처리 단계별 요구사항에 대한 중요성에 대한 인식은 유의한 차이가 있다.”에 대해 ANOVA 일원 배치의 분산분석, 동일집단군 분석 사후분석 결과를 통해 차이가 있는지 유의 확률을 확인하였다.

표 11은 모든 가설에 대한 분산분석 결과, 그림 1은 모든 가설에 대한 집단 동질성 분석결과, 마지막으로 표 12, 13은 각 가설들에 대한 후처리 분석 결과를 나타낸다.

표 11. 모든 가설에 대한 분산분석 결과.
Table 11. Result of variance analysis for all hypotheses

가설		제곱합			df			평균제곱		F	유의확률
		집단-간	집단-내	합계	집단-간	집단-내	합계	집단-간	집단-내		
경력 차이	관리체계 수립 및 운영	0.995	52.65	53.645	3	46	49	0.332	1.145	0.29	0.833
	보호대책 요구사항	3.216	66.935	70.151	3	46	49	1.072	1.455	0.737	0.536
	개인정보처리 단계별 요구사항	5.896	102.177	108.073	3	46	49	1.965	2.221	0.885	0.456
회사 규모 차이	관리체계 수립 및 운영	0.433	52.212	52.645	5	44	49	0.087	1.209	0.072	0.996
	보호대책 요구사항	2.601	67.55	70.151	5	44	49	0.52	1.535	0.339	0.887
	개인정보처리 단계별 요구사항	7.192	100.882	108.074	5	44	49	1.438	2.293	0.627	0.68

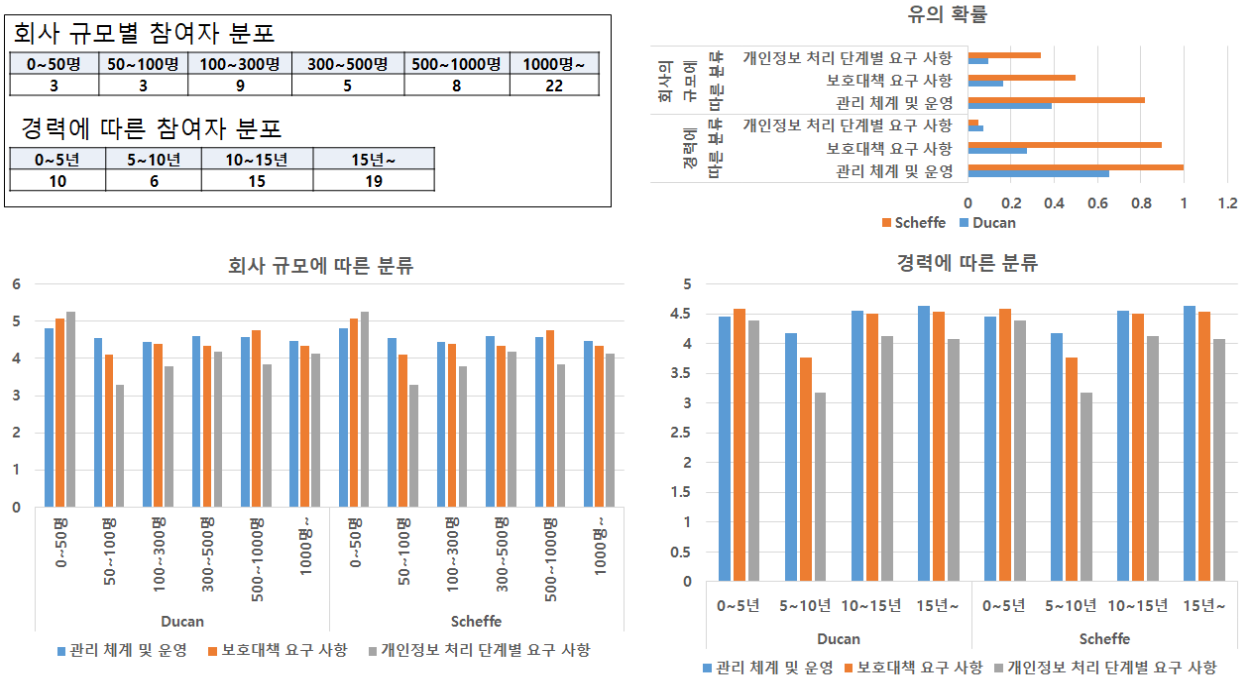

그림 1. 각 가설에 대한 상이한 집단 간 집단 동질성 실험 결과

Fig. 1. Analysis to check if the same group among the groups of various company sizes and various career lengths based on the responses for all hypotheses

표 12. 경력에 따른 각 가설들에 대한 후처리 분석 결과: (A) 관리체계 및 운영, (B) 보호대책 요구사항, (C) 개인정보 처리 단계 별 요구사항 (scheffe 분석)

Table 12. Post analysis results on the hypotheses regarding the length of careerer: (A) Management system and operation, (B) Protection measures requirement, and (C) Requirements in the step of processing personal information (scheffe analysis)

A= ⓑ-1	B= ⓑ-2(년)	평균차 (A-B)			표준 오차			유의 확률			95% 신뢰구간					
											하한값			상한값		
		(A)	(B)	(C)	(A)	(B)	(C)	(A)	(B)	(C)	(A)	(B)	(C)	(A)	(B)	(C)
0~5년	5~10	0.277	0.824	1.219	0.552	0.623	0.77	0.968	0.629	0.481	-1.33	-0.98	-1.01	1.88	2.63	3.45
	10~15	-0.098	0.087	0.26	0.437	0.492	0.608	0.997	0.999	0.98	-1.37	-1.34	-1.51	1.17	1.52	2.03
	15~	-0.176	0.045	0.318	0.418	0.471	0.582	0.981	1	0.96	-1.39	-1.32	-1.37	1.04	1.41	2.01
5~10년	0~5	-0.277	-0.824	-1.219	0.552	0.623	0.77	0.968	0.629	0.481	-1.88	-2.63	-3.45	1.33	0.98	1.01
	10~15	-0.375	-0.737	-0.959	0.517	0.583	0.72	0.912	0.662	0.624	-1.87	-2.43	-3.05	1.12	0.95	1.13
	15~	-0.453	-0.779	-0.901	0.501	0.565	0.698	0.845	0.597	0.647	-1.91	-2.42	-2.93	1	0.86	1.12
10~15년	0~5	0.098	-0.087	-0.26	0.437	0.492	0.608	0.997	0.999	0.98	-1.17	-1.52	-2.03	1.37	1.34	1.51
	5~10	0.375	0.737	0.959	0.517	0.583	0.72	0.912	0.662	0.624	-1.12	-0.95	-1.13	1.87	2.43	3.05
	15~	-0.78	-0.042	0.058	0.37	0.417	0.515	0.997	1	1	-1.15	-1.25	-1.44	0.99	1.17	1.55
15~ 년	0~5	0.176	-0.045	-0.318	0.418	0.471	0.582	0.981	1	0.96	-1.04	-1.41	-2.01	1.39	1.32	1.37
	5~10	0.453	0.779	0.901	0.501	0.565	0.698	0.845	0.597	0.647	-1	-0.86	-1.12	1.91	2.42	2.93
	10~15	0.078	0.042	-0.058	0.37	0.417	0.515	0.997	1	1	-0.99	-1.17	-1.55	1.15	1.25	1.44

가설 (1)에 대해서는 분산분석 시 유의 확률이 .833, 동일집단군 분석 Ducan .387, Scheffe .818, 사후분석 결과 모두 유의 확률 0.05 이상이므로 가설을 기각할 수 있다. 즉, 경력과 상관없이 관리 체계 수립 및 운영의 중요성에 대해서는 유의미한 차이가 없이 인식하고 있다고 알 수 있다.

또한 가설 (2)에 대해서는 분산분석 시 유의 확률이 .996, 동일집단군 분석 Ducan .652, Scheffe .998, 사후분석 결과 모두 유의 확률 0.05 이상이므로 가설을 기각할 수 있다. 결국, 회사규모와 상관없이 관리체계 수립 및 운영의 중요성은 동일하게 인식함을 확인할 수 있다.

표 13. 회사규모에 따른 모든 가설들에 대한 후처리 분석 결과: (A) 관리체계 및 운영, (B) 보호대책 요구 사항, (C) 개인정보처리 단계 별 요구사항 (scheffe 분석)

Table 13. Results of post-processing analysis on all hypotheses according to company size: (A) Management system and operation, (B) Protection measures requirements, (C) Personal information processing stage requirements (scheffe analysis)

A=ⓑ-1(명)	B=ⓑ-2(명)	평균차 (A-B)			표준 오차			유의 확률			95% 신뢰구간					
											하한값			상한값		
		(A)	(B)	(C)	(A)	(B)	(C)	(A)	(B)	(C)	(A)	(B)	(C)	(A)	(B)	(C)
0~50	50~100	0.25	0.976	1.952	0.898	1.012	1.236	1	0.966	0.775	-2.88	-2.55	-2.35	3.38	4.5	6.26
	100~300	0.357	0.669	1.476	0.733	0.826	1.009	0.999	0.984	0.827	-2.2	-2.21	-2.04	2.91	3.55	4.99
	300~500	0.212	0.741	1.08	0.803	0.905	1.106	1	0.984	0.965	-2.59	-2.41	-2.77	3.01	3.89	4.93
	500~1000	0.213	0.316	1.407	0.745	0.839	1.025	1	1	0.862	-2.38	-2.61	-2.16	2.81	3.24	4.98
	1000~	0.341	0.723	1.138	0.677	0.763	0.932	0.998	0.969	0.911	-2.02	-1.93	-2.11	2.7	3.38	4.38
50~100	0~50	-0.25	-0.976	-1.952	0.898	1.012	1.236	1	0.966	0.775	-3.38	-4.5	-6.26	2.88	2.55	2.35
	100~300	1.07	-0.307	-0.476	0.733	0.826	1.009	1	1	0.999	-2.45	-3.18	-3.99	2.66	2.57	3.04
	300~500	-0.038	-0.235	-0.872	0.803	0.905	1.106	1	1	0.986	-2.84	-3.39	-4.72	2.76	2.92	2.98
	500~1000	-0.37	-0.66	-0.545	0.745	0.839	1.025	1	0.986	0.998	-2.63	-3.58	-4.12	2.56	2.26	3.03
	1000~	0.91	-0.253	-0.815	0.677	0.763	0.932	1	1	0.978	-2.27	-2.91	-4.06	2.45	2.4	2.43
100~300	0~50	-3.57	-0.669	-1.476	0.733	0.926	1.009	0.999	0.984	0.827	-2.91	-3.55	-4.99	2.2	2.21	2.04
	50~100	-1.07	0.307	0.476	0.733	0.826	1.009	1	1	0.999	-2.66	-2.57	-3.04	2.45	3.18	3.99
	300~500	-1.45	0.072	-0.396	0.613	0.691	0.845	1	1	0.999	-2.28	-2.34	-3.34	1.99	2.48	2.55
	500~1000	-1.44	-0.353	-0.068	0.534	0.602	0.736	1	0.996	1	-2.01	-2.45	-2.63	1.72	1.74	2.49
	1000~	-0.16	0.053	-0.339	0.435	0.49	0.599	1	1	0.997	-1.53	-1.65	-2.43	1.5	1.76	1.75
300~500	0~50	-0.212	-0.741	-1.08	0.803	0.905	1.106	1	0.984	0.965	-3.01	-3.89	-4.93	2.59	2.41	2.77
	50~100	0.38	0.235	0.872	0.803	0.905	1.106	1	1	0.986	-2.76	-2.92	-2.98	2.84	3.39	4.72
	100~300	0.145	-0.072	0.396	0.613	0.691	0.845	1	1	0.999	-1.99	-2.48	-2.55	2.28	2.34	3.34
	500~1000	0.001	-0.425	0.327	0.627	0.706	0.863	1	0.996	1	-2.18	-2.89	-2.68	2.18	2.04	3.33
	1000~	0.13	-0.019	0.058	0.545	0.614	0.75	1	1	1	-1.77	-2.16	-2.56	2.03	2.12	2.67
500~1000	0~50	-0.213	-0.316	-1.407	0.745	0.839	0.862	1	1	0.862	-2.81	-3.24	-4.98	2.38	2.61	2.16
	50~100	0.037	0.66	0.545	0.745	0.836	0.998	1	0.986	0.998	-2.56	-2.26	-3.03	2.63	3.58	4.12
	100~300	0.144	0.353	0.069	0.534	0.602	1	1	0.996	1	-1.72	-1.74	-2.49	2.01	2.45	2.63
	300~500	-0.01	0.425	-0.327	0.627	0.706	1	1	0.995	1	-2.18	-2.04	-3.33	2.18	2.89	2.68
	1000~	0.129	0.407	-0.269	0.454	0.512	0.999	1	0.986	0.999	-1.45	-1.38	-2.45	1.71	2.19	1.91
1000	0~50	-3.41	-0.723	-1.138	0.677	0.763	0.911	0.998	0.969	0.811	-2.7	-3.38	-4.38	2.02	1.93	2.11
	50~100	-0.91	0.253	0.815	0.677	0.763	0.975	1	1	0.978	-2.45	-2.4	-2.43	2.27	2.91	4.06
	100~300	0.016	-0.053	0.339	0.435	0.49	0.997	1	1	0.997	-1.5	-1.76	-1.75	1.53	1.65	2.43
	300~500	-0.13	0.019	-0.058	0.545	0.614	1	1	1	1	-2.03	-2.12	-2.67	1.77	2.16	2.56
	500~1000	-0.129	-0.407	0.269	0.454	0.512	0.999	1	0.986	0.999	-1.71	-2.19	-1.91	1.45	1.38	2.45

가설 (3)에 대해서는 분산분석 시 유의 확률이 .536, 동일집단군 분석 Ducan .163, Scheffe .497, 사후분석 결과 모두 유의 확률 0.05 이상이므로 가설을 기각하였다. 즉, 경력과 관계없이 보호대책 요구사항의 중요성은 동일하게 인식하고 있음을 확인할 수 있다.

가설 (4)에 대해서는 분산분석 결과 유의 확률이 .887 임을 알 수 있다. 또한 동일집단군 분석 결과 Ducan 확률은 .273, Scheffe 확률은 .896을 보여주고 있다. 마지막으로 사후분석 결과를 보여주고 있으며 모두 유의 확률이 0.05 이상임을 알 수 있다. 이러한 분석 결과를 바탕으로 우리는 가설을 기각할 수 있다.

이러한 분석을 바탕으로, 우리는 회사규모와 관계없이 보호대책 요구사항에 대해서는 동일한 수준으로 중요하게 생각하고 있음을 확인할 수 있다.

가설 (5)에 대해서는, 분산분석 시 유의 확률이 .456이고, 동일집단군 분석 결과 Ducan .095, Scheffe .337 임이 밝혀졌다. 또한 사후분석 결과 모두 유의 확률 0.05 이상이므로 가설을 기각할 수 있다. 즉,

경력과 상관없이 개인정보처리 단계별 요구사항에 대한 중요성은 유의한 차이가 없다는 것을 알 수 있다.

마지막으로 가설 (6)에서는 분산분석 시 유의 확률이 .680, 동일집단군 분석인 Ducan .073, Scheffe .510, 그리고 사후분석 결과 모두 유의 확률 0.05 이상이므로 가설을 기각할 수 있다. 결론적으로 회사규모와 관계없이 보안 담당자는 개인정보처리 단계별 요구사항에 대해 유사한 관점을 갖고 있다는 것을 알 수 있다.

4.4 분석 종합

표 14는 가설 확인 및 검증 결과의 요약이다. 데이터 분석 결과 모든 가설을 기각하였다. 경력과 회사규모 상관없이 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보처리 단계별 사항에 차이가 없다는 것을 보인다. 이를 해석하면 초보자 부터 전문가 소기업에서 대기업까지 모든 요소가 효과가 있으며 종합적으로 고려해야 한다는 것을 뜻한다.

표 14. 가설에 대한 분석 결과
Table 14. Analysis results on hypotheses

가설 설정	확인
1. 경력과 상관없이 관리체계 수립 및 운영에 대한 중요성은 유의한 차이가 있다.	기각
2. 회사규모와 상관없이 관리체계 수립 및 운영에 대한 중요성은 유의한 차이가 있다.	기각
3. 경력과 상관없이 보호대책 요구사항에 대한 중요성은 유의한 차이가 있다.	기각
4. 회사규모와 상관없이 보호대책 요구사항에 대한 중요성은 유의한 차이가 있다.	기각
5. 경력과 상관없이 개인정보처리 단계별 요구사항에 대한 유의한 차이가 있다.	기각
6. 회사규모와 상관없이 개인정보처리 단계별 요구사항에 대한 유의한 차이가 있다.	기각

V. 결 론

본 연구에서는 국내 기업군의 산업기술 보호 및 정보유출 방지와 관련된 ISMS-P 적용의 효과성을 분석하였다. ISMS-P의 보안요소가 적용될 경우 한국인터넷진흥원 사이버 위협 인텔리전스 네트워크에서 지정한 2019년도 보안 위협에 대해 본인 회사의 정보 자원이 얼마나 잘 보호될 수 있는지를 설문을 통해 정보를 수집하고, 통계적 분석 방법을 통해 결과를 도출하였다. 그 결과 데이터 동질성 분석에서는 차이가 없었고, 기술 통계적 결과 모두 리커트 척도 7점 중 4점 이상 획득하여 기술적으로 보호가 된다고 평가됨을 알 수 있었다.

또한 6가지 가설인 (1) “경력과 상관없이 관리체계 수립 및 운영에 대한 중요성은 유의한 차이가 있다.” (2) “회사규모와 상관없이 관리체계 수립 및 운영에 대한 중요성에 대한 인식은 유의한 차이가 있다.” (3) “경력과 상관없이 보호대책 요구사항에 대한 중요성에 대한 인식은 유의한 차이가 있다.” (4) “회사규모와 상관없이 보호대책 요구사항에 대한 중요성에 대한 인식은 유의한 차이가 있다.” (5) “경력과 상관없이 개인정보처리 단계별 요구사항에 대한 중요성의 인식은 유의한 차이가 있다.” (6) “회사규모와 상관없이 개인정보처리 단계별 요구사항에 대한 중요성의 인식은 유의한 차이가 있다.”를 모두 기각하여 경력과 회사규모에 상관없이 응답자들이 동일한 결과를 내었다는 것을 파악하였다. 이를 바탕으로 실무자의 경력과 회사규모와 상관없이 ISMS-P의 모든 요소는 기업의 보안 실무자 또는 IT 분야 종사자들이 중요하게 생각하고 있다는 것을 알 수 있었다.

본 연구는 ISMS-P 실시 이후 효과에 관해 확인한 연구이지만, 데이터 수가 50명에 한정되어 있고, IT 실무자 입장에서만 확인한 결과인 한계가 있다. 향후 연구로써 더 많은 샘플과 다양한 입장에서 동일한 연구가 이루어져 ISMS-P의 우수성이 널리 알려지는 추가 연구가 진행되기를 희망한다.

References

[1] Samsung Electronics, "LG Electronics Semiconductor Technology Leak Case", https://imnews.imbc.com/replay/1998/nwdesk/article/1981013_30723.html. [Accessed: Mar. 02, 2020] (Written in Korean)

[2] Unfair Competition Prevention and Trade Secret Protection ACT, Apr. 17, 2018. https://elaw.klri.re.

kr/kor_service/lawView.do?hseq=48681&lang=ENG [Accessed: Mar. 03, 2020]

[3] Act on Prevention pf Divulgence and Protection of Industrial Technology, Mar. 14, 2017. https://elaw.klri.re.kr/kor_service/lawView.do?hseq=42638&lang=ENG [Accessed: Mar. 03, 2020]

[4] J. S. Nam, "Actual Condition of Damage of Industrial Secrets Leakage Crime and its Measures at Small or Medium Sized Business-Focusing on Legal, Systematic Methods", Korean Association of Public Safety and Criminal Justice Review, Vol. 21, No. 1, 46, pp. 43-75, Mar. 2012.

[5] Ministry of Science, "Technology, Information and Communication, Ministry of Public Administration and Security", Korea Communications Commission, Korea Internet Corporation, pp. 1-256, 2019.

[6] G. Albaum, "The Likert Scale Revisited", International Journal of Market Research, Vol. 39, No. 2, pp. 1-21, Mar. 1997.

[7] St, Lars and Svante Wold, "Analysis of variance (ANOVA)", Chemometrics and intelligent laboratory systems, Vol. 6, No. 4, pp. 259-272, Nov. 1989.

[8] Sung-Wook Hong and Jae-Pyo Park, "Effective Management of Information Security and Personal Information Management System", Journal of the Korean Academic Industrial Society, Vol. 21, No. 1, pp. 634-640, Jan. 2020.

[9] Korea Internet & Security Agency, "Seven major cyber attack trends in 2019", Dec. 2018. https://www.kisa.or.kr/notice/press_View.jsp?mode=view&p_No=8&b_No=8&d_No=1739&ST=total&SV= [Accessed: Mar. 03, 2020]

저자소개

김 동 현 (Dong Hyun Kim)

2018년 8월 : 성균관대학교 정보보호학과 석사
2019년 8월 : 서울과학기술대학교 IT정책전문대학원 산업정보시스템 전공 석사
2013년 ~ 현재 : 캐논코리아 IT담당
관심분야 : 데이터보안, 정보보안

이 윤 호 (Younho Lee)

2006년 8월 : KAIST 전산학과 박사
2007년 10월 ~ 2009년 2월 : GeorgiaTech GTISC 박사후과정
2013년 9월 ~ 현재 : 서울과학기술대학교 ITM전공 부교수
관심분야 : 응용암호, 데이터보안