AHP를 활용한 스마트워크 정보보호 요소의 중요도 분석
-중소기업의 모바일 오피스를 중심으로-

강경훈[*], 임채홍[**], 임종인[***], 박태형[****]

Analysis on Importance of Information Security Factors for Smart Work using AHP
-Based on the Mobile Office for Small Businesses-

Kyung-Hoon Kang[*], Chae-Hong Lim[**], Jong-In Lim[***], Tae-Hyoung Park[****]

요 약 우리나라는 최근 온실가스 감축, 저출산·고령화 문제 해결, 생산성 향상 등을 위해 스마트워크를 서서히 도입하고 있다. 우리나라의 경우 ICT 인프라의 발달과 스마트 기기의 확산으로 스마트워크 유형 중 하나인 모바일 오피스가 가장 많이 도입되고 있으나, 중소기업의 모바일 오피스 도입률은 대기업의 절반 수준에 그치고 있으며, 중소기업의 스마트워크 도입에 있어 가장 큰 장애요인의 하나가 보안 문제인 것으로 나타났다. 따라서 본 연구에서는 중소기업이 스마트워크의 한 유형인 모바일 오피스를 도입하고자 할 때 우선적으로 고려해야 할 정보보호 요소를 분석하고자 하였다. 선행연구 분석을 통해 모바일 오피스 정보보호 요소를 단말기, 응용프로그램 및 플랫폼, 네트워크, 서버, 사용자 등 5개 영역으로 구분하여 각각 세부항목을 정리하였다. AHP를 활용한 조사 결과 상위계층에서는 '사용자'가 가장 중요한 항목으로 도출되었으며, 24개의 하위 요소 중에서는 '데이터 암호화', '무선랜 통제', '퇴사 시 단말 회수' 등이 중요한 모바일 오피스 정보보호 요소인 것으로 나타났다.

주제어 : 스마트워크, 모바일 오피스, 정보보호, 중소기업, AHP

Abstract Smart work has recently introduced as a way to solve problems such as greenhouse gas emissions, low birth rate and aging as well as to improve productivity. Because of development of ICT infrastructure and the proliferation of smart devices, the mobile office has the most commonly used within types of smart work in Korea. But the adoption of the mobile office in small businesses is only half of that of large corporations. The security issue appears to be one of the biggest obstacles to the introduction of smart work in small businesses. Therefore, the purpose of this study is to analyze the information security factors that should be considered when the mobile office is introduced to small businesses. By analyzing the previous studies, the information security factors of the mobile office are classified 5 groups composed of 24 factors. 5 groups are terminals, applications and platforms, networks, servers and users. According to the survey result using AHP, 'User' was drawn to the most important group, and 'Data Encryption', 'Wireless LAN Control' and 'Terminal Recovery When Leaving' were drawn to the important information security factors of the mobile office among 24 factors.

Key Words : Smart Work, Mobile Office, Information Security, Small Businesses, AHP(Analytic Hierarchy Process)

본 논문은 지식경제부 및 정보통신산업진흥원의 "지식정보보안인력양성 최고정보보안전문가과정" 사업의 연구결과로 수행되었음 (과제번호: NIPA-2012-H2102-12-1001)

[*]한국정보화진흥원 디지털인프라단 공공통신망지원부 책임연구원(주저자)
[**]고려대학교 정부학연구소 연구원(공동저자)
[***]고려대학교 정보보호대학원 원장/교수(공동저자)
[****]고려대학교 정보보호대학원 사이버국방연구센터 (교신저자)

논문접수: 2013년 2월 6일, 1차 수정을 거쳐, 심사완료: 2013년 3월 5일, 확정일: 2013년 3월 20일

1. 서론

우리나라는 급격한 저출산·고령화로 인해 2000년에 65세 이상 노년인구가 7.2%로 이미 고령화사회(aging society)로 진입하였고, 2018년에는 노년인구가 14%를 넘어 고령사회(aged society)로 접어들 것으로 전망된다[6]. 따라서 고령사회에 대비한 대안적인 근무제도를 준비해야 할 시기이다. 뿐만 아니라 우리나라의 2008년 1인당 노동시간은 연간 2,256시간으로 OECD 평균보다 연간 492시간 더 근무하며, 노동생산성은 57,204$로 OECD 30개국 중 21위이다[32]. 이는 장시간 노동 기반의 근로형태로는 더 이상 성과를 기대하기 어려운 상황으로 일하는 방식의 변화가 필요하다는 것을 시사한다. 최근 우리나라는 2009년 말 아이폰 출시와 함께 '스마트' 열풍이 불고 있다. 스마트폰, 태블릿PC 등이 확산되고 IT 기술이 발달함에 따라 스마트워크가 저출산·고령화, 노동생산성 등의 현안을 해결할 대안으로 떠오르고 있다.

스마트워크(Smart Wok)는 시간과 장소에 얽매이지 않고 언제 어디서나 편리하고 똑똑하게 근무함으로써 업무효율성을 향상시킬 수 있는 업무방식을 말한다. 스마트워크는 근무 장소에 따라 모바일 오피스(이동/현장근무), 홈 오피스(재택근무), 스마트워크센터(원격사무실 근무), 스마트 오피스(직장근무)로 구분할 수 있다[8]. 이미 세계 각국은 '스마트' 트렌드와 함께 저탄소 녹색성장, 비상대응체제 확립 등 사회현안 해결방안의 일환으로 스마트워크에 주목하고 있다. 우리나라도 온실가스 감축, 저출산·고령화 문제 해결, 생산성 향상 등을 위해 스마트워크를 서서히 도입하고 있다. 특히 우리나라의 경우 ICT 인프라의 발달과 스마트 기기의 확산으로 모바일 오피스가 가장 많이 도입되고 있다[30].

그러나 대기업과 중소기업의 모바일 오피스 도입률에는 큰 차이가 있다. 대기업과 중소기업 모두 모바일 오피스 도입의 중요성을 인식하고 있으나 실제 중소기업의 모바일 오피스 도입률은 대기업의 절반 수준에 그치고 있다[22].

한편 모바일 오피스는 스마트 기기로 회사 외부에서 사내 망에 접속하기 때문에 기밀사항 등 중요한 정보가 외부로 유출될 수 있는 위험성이 크다. 최근에는 스마트폰, 태블릿PC 등 모바일 단말기가 늘어나면서 보안문제가 스마트워크 도입에 걸림돌이 되고 있다. 한국정보화진흥원(2011)에 따르면 IT 인프라가 열악한 중소기업의 CEO들은 스마트워크 도입의 장애요인으로 단말/솔루션 등의 호환성 및 보안문제를 가장 많이 꼽고 있다[31].

따라서 본 연구에서는 기존연구결과를 바탕으로 중소기업이 스마트워크의 한 유형인 모바일 오피스를 도입하고자 할 때 고려해야 할 정보보호 요소의 상대적 중요도를 도출하고, 정보보호 측면에서의 스마트워크 정책 방향의 시사점에 대해 논의하고자 한다.

2. 이론적 논의 및 선행연구 검토

2.1 스마트워크에 대한 이론적 논의

2.1.1 스마트워크의 개념

우리나라에서는 2010년 7월 국가정보화전략위원회, 행정안전부, 방송통신위원회가 공동으로 스마트워크 활성화 전략을 발표하면서 정부와 민간에서 스마트워크에 대한 연구가 활발히 진행되고 있다. 그 가운데 대표적인 연구들을 살펴보면, 한국정보화진흥원(2010)은 스마트워크를 ICT를 이용하여 시간·장소에 제약없이 누구와도 함께 네트워크 상에서 일할 수 있는 유연한 근무방식으로 정의하였다[29]. 임광현・이동진・김진혁(2010)은 스마트워크를 인터넷을 기반으로 하여 시간과 장소에 구애받지 않고 자유롭게 업무를 처리하는 방식을 통해 근무를 하는 것으로 정의하였다[20]. 이민혜・이준기(2011)는 스마트워크란 스마트 정보통신기술과 제도적 인프라를 기반으로 근로자가 언제 어디서나 자율적으로 일하고 자유롭게 협업함으로써 성과를 극대화하도록 하는 업무 방식이라고 정의하였다[15]. 방송통신위원회(2011)는 스마트워크를 시간과 장소에 얽매이지 않고 언제 어디서나 편리하고 똑똑하게 근무함으로써 업무효율성을 향상시킬 수 있는 업무방식으로 정의하였다[8].

한편, 본 연구와 직접적으로 관련성이 높은 모바일 오피스에 관한 연구를 살펴보면, 나성욱・이윤희・지순정(2010)은 모바일 오피스를 언제 어디서나 모바일 단말기를 통해 외부에서 회사 업무를 처리할 수 있는 업무 시스템으로 설명하고 있다[7]. 방송통신위원회・한국정보화진흥원(2011)은 모바일 오피스란 스마트폰, PDA, 노트북 등을 이용하여 공간적 제약없이 업무를 수행하는 근무형태로 정의하였다[10]. 최연호(2011)는 모바일 오피스를 언제 어디서나 모바일 단말기(이동통신기기)를 통해 외부에서 회사 업무를 처리할 수 있는 업무시스템으로 정

의하였다[27].

이상의 기존연구들을 종합해 볼 때, 스마트워크는 언제, 어디서나 효율적으로 업무를 수행하는 근무방식으로, 모바일 오피스는 모바일 단말기를 통해 언제, 어디서나 업무를 수행하는 근무방식으로 정의할 수 있다.

2.1.2 스마트워크의 유형 및 특성

방송통신위원회(2011)는 스마트워크를 근무 장소에 따라 모바일 오피스(이동/현장근무), 홈 오피스(재택근무), 스마트워크센터(원격사무실 근무), 스마트 오피스(직장근무)로 구분하고 있다[8].

모바일 오피스(이동/현장근무)는 위에서 살펴본 바와 같이 모바일 단말기를 통해 언제, 어디서나 업무를 수행하는 근무방식으로 정의할 수 있으며, 업무를 수행하는 사용자, 업무를 수행할 모바일 단말, 업무를 수행할 수 있게 하는 서비스 플랫폼, 단말기가 사용하는 유무선 네트워크, 업무 정보를 가지고 있는 모바일 서버로 구성된다[7][28]. 이는 공간 제약 없이 실시간 업무처리를 가능하게 하여 현장 중심의 경영이 강화될 수 있는 특징을 가진다[10].

홈 오피스(재택근무)는 전통적으로 회사 사무실 공간에서 하던 일을 가정 내에서 수행하는 근무방식으로[10][16], 댁내에 있는 단말기와 유무선 네트워크를 통해 사내망에 접속하여 업무를 처리한다[28]. 가족과 일의 갈등을 줄일 수 있고, 주변 사람들로부터 업무 방해를 받지 않아 생산성을 향상시킬 수 있는 장점이 있으나, 고립감, 승진의 불안감 등의 단점이 있다[10].

스마트워크센터(원격사무실 근무)는 주거지 인근에 구축된 전용 시설인 '스마트워크센터'에서 IT 인프라를 활용한 사무실과 유사한 환경에서 근무하는 형태이다[10]. 스마트워크센터에 있는 단말기와 유선 네트워크를 통해 사내망에 접속하여 업무를 처리하는 방식으로[28], 근태관리 및 보안성 확보가 용이하며, 재택근무에 비해 업무집중도를 높일 수 있다[10].

스마트 오피스(직장근무)는 기존의 직장근무보다 더 업무효율성을 높일 수 있는 시설과 환경을 구축하여 근무하는 것으로 조직 간의 협업을 가능하게 하는 근무 방식인 영상회의 등이 있다[10]. 영상회의는 서비스 종류에 따라 PC형, TV set-top형, 회의실형 등이 있으며[3], 사용자, 소프트웨어 타입 또는 하드웨어 타입의 영상회의 솔루션, 유선 네트워크, 다자간 영상회의 단말을 연결해 주는 MCU(Multipoint Control Unit) 등으로 구성되며, 서로 다른 공간에 있는 조직원들 간의 동시적인 일처리를 가능하게 하고, 정보 공유를 통해 신속한 의사결정을 돕는다[10].

스마트워크는 유형별로 각각의 특성과 장점이 상이하기 때문에, 스마트워크를 도입하고자 하는 기업은 기업의 규모 및 업무 특성 등을 파악하여 최적의 스마트워크 유형을 선택하는 것이 바람직하다. 위에서 살펴본 스마트워크 유형별 특성을 간략히 정리하면 <표 1>과 같다.

2.2 모바일 오피스 보안위협 및 대응방안에 대한 논의

방송통신위원회・한국인터넷진흥원(2011)은 보안위협으로부터 스마트워크 이용자를 보호하고, 안전한 스마트워크 이용환경을 조성하기 위해 스마트워크 서비스 제공자, 관리자, 이용자로 구분하여 기술적, 관리적 보호조치를 제시하였다. 서비스 제공자는 주로 인프라 보안, 공용PC

〈표 1〉 스마트워크 유형 및 특성

구분	모바일 오피스 (이동/현장근무)	홈 오피스 (재택근무)	스마트워크센터 (원격사무실 근무)	스마트 오피스 (직장근무)
개념	모바일 단말기를 통해 언제, 어디서나 업무를 수행하는 근무방식	정보통신 기기를 통해 집에서 회사업무를 수행하는 근무방식	주거지 인근에 구축된 전용 시설인 '스마트워크센터'에서 IT 인프라를 활용한 사무실과 유사한 환경에서 근무하는 형태	기존의 직장근무보다 더 업무효율성을 높일 수 있는 시설과 환경을 구축하여 근무하는 방식
구성	사용자, 모바일 단말, 서비스 플랫폼, 유무선 네트워크, 모바일 서버(사내망) 등	사용자, 댁내 단말기, 유무선 네트워크, 사내망 서버 등	사용자, 스마트워크센터 단말기, 유선 네트워크, 사내망 서버 등	사용자, 영상회의 솔루션, 유선 네트워크, MCU 등
특성	실시간 업무처리가 가능하여 현장 중심의 경영 강화	출퇴근 시간 및 교통비 부담이 없고 생산성 향상 등의 장점이 있으나, 고립감, 승진의 불안감 등의 단점이 있음	근태 관리 및 보안성 확보가 용이하며, 재택근무에 비해 업무집중도를 높일 수 있으나, 별도의 사무공간 필요	서로 다른 공간에 있는 조직원들 간의 협업 및 정보 공유를 통해 신속한 의사결정 지원

※ [3], [7], [10], [16], [27], [28] 재구성

보안에 대한 보호조치를 마련해야 하고, 관리자는 단말기 보안, 서비스 보안, 콘텐츠 보안, 인적자산의 관리, 침해사고 대응절차 등의 보호조치를 마련해야 하며, 이용자는 정보자산 취급·관리, 정보보호에 대한 인식 제고, 침해사고 대응 등을 고려해야 한다[9].

한국인터넷진흥원(2011)은 스마트워크 보안 취약점을 사용자, 서비스, 무선/유선 네트워크, 사내망으로 구분하여 기술적, 관리적, 물리적 정보보호 대응방안을 제시하였고, 특히 모바일 오피스의 취약점을 사용자, 단말로 구분하여 정보보호 대응방안을 제시하였다[28].

이재호・이동훈・김휘강(2012)은 스마트워크 환경에서의 보안 위협을 단말기, 응용프로그램 및 플랫폼, 네트워크 및 서버 부문으로 구분하여 각각의 보안 위협 및 대책을 제시하였다[17].

정범구(2011)는 모바일 오피스의 보안 위협을 단말기, 응용프로그램 및 플랫폼, 서버 등 세 가지로 구분하여 각각의 보안 위협에 대한 대응방안을 제시하였다[23].

이경복・박태형・임종인(2011)은 스마트워크 환경에서의 정보보호 관련 주요 이슈와 문제점을 살펴보고 스마트워크 유형에 따른 보안문제 해결방안을 제시하였다. 특히 모바일 오피스에서의 주요 단말인 스마트폰에 초점을 맞춰 모바일 악성코드, 플랫폼, 무선 통신 기술, 휴대성으로 인한 분실 및 도난 등으로 보안위협을 분석하였다[14].

이형찬・이정현・손기욱(2011)은 스마트워크 보안 요구사항을 단말, 네트워크, 모바일 센터(서버)로 구분하여 살펴보고, 그에 대한 보안 대책을 제시하였다[18].

나성욱・이윤희・지순정(2010)은 단말, 응용프로그램 및 플랫폼, 네트워크 및 서버 측면에서의 보안 이슈를 살펴보고, 이에 대한 대책을 제시하였다[7].

2.3 정보보호 분야에서의 AHP 분석의 활용

AHP(Analytic Hierarchy Process) 기법은 미국 피츠버그 대학의 T. L. Saaty 교수가 개발한 의사결정 기법이다[33][34][35][36]. 이 기법은 주어진 의사결정 문제를 계층화한 후 상위계층에 있는 요소 또는 기준의 관점에서 직계 하위계층에 있는 요소들의 상대적 중요도 또는 가중치를 쌍대비교(pairwise comparison)에 의해 측정하는 방식이며, 객관적인 평가요인은 물론 주관적 평가요인도 수용하는 매우 유연한 의사결정 기법이다[2][4][19][24][25]. AHP 기법은 일관성비율을 기준으로 설문 응답의 신뢰도를 측정할 수 있는 특성을 갖고 있기 때문에, 논리적이고 합리적인 의사결정 과정에 대한 신뢰성을 높일 수 있으며[2][11], 일반적으로 의사결정계층(Decision Hierarchy) 설정, 쌍대비교, 상대적 가중값 산정, 상대적 가중값 종합화의 4단계를 통해 진행된다[19][21][33][34][35][36]. AHP 기법은 의사결정에 관여하는 사람들의 주관적인 판단을 계량화하여 반영할 수 있어 여러 분야에서 광범위하게 사용되고 있다[1][2][4]. 정보보호 분야에서 AHP를 활용한 연구를 살펴보면 다음과 같다.

성욱준・김동욱(2011)은 정보보호 정책 부문에서 우선적으로 수행해야 할 정책대안이 무엇인가에 대해 AHP를 통해 살펴보았다. AHP 분석 결과 정보보호 정책 추진체계 변화, 기술의 발전에 상응하는 법제도적·정책적 대응, 정보보호 전문인력 육성 등이 필요한 것으로 조사되었다[12].

신영진・정형철・강원영(2012)은 공공분야에서 개인정보가 안전하게 관리되고 보호받을 수 있는 방안을 마련하기 위해 우선적으로 추진되어야 할 정책과제를 다루었다. AHP 분석 결과 개인정보보호의 정책·기술적 측면, 개인정보 침해대응적 측면, 처리단계의 관리적 측면 순으로 중요한 것으로 나타났다[13].

성기훈・공희경・김태한(2010)은 AHP를 이용한 SNS 제공환경에서 정보보호 중요위협요인 분석을 통해 정보보호 투자 결정 기준 도출에 대한 연구를 수행하였다. AHP 분석 결과 기업에서 정보보호 목적을 달성하기 위해 투자하는 경우 경제적 측면의 중요도가 기술적 측면보다 높으며, 경제적 측면에서는 서비스 이미지, 기술적 측면에서는 기밀성의 중요도가 높게 나타났다[11].

김태성・전효정(2006)은 정보보호인력의 질적인 수급 불일치를 해소하기 위해 인력의 양성이 우선적으로 필요한 분야를 AHP 방법론을 이용하여 도출하였다. AHP 분석 결과 시스템·네트워크 정보보호 기술 분야의 인력 양성이 가장 시급한 것으로 나타났다[5].

최명길, 박유진(2008)은 정보보호시스템의 각 개발 단계별로 품질 요소의 우선순위를 AHP로 도출하고, 도출된 품질 요소의 가중치를 유전자 알고리즘을 이용하여 각 단계별로 비용을 할당하는 과정을 제시하였다. AHP 분석 결과 각 개발 단계별로 이해성, 적합성, 성숙성, 상호운용성, 보안성 등의 품질요소가 중요한 것으로 나타났다[26].

〈표 2〉 모바일 오피스 보안 위협에 대한 대응방안

구분	단말기	응용 프로그램 및 플랫폼(서비스)	네트워크	서버 (사내망)	사용자 (인적 자산)
방송 통신 위원회, 한국 인터넷 진흥원 (2011)	보안 플랫폼 원격 제어 원격 백업·삭제·복원 단말기 정보관리 이용자·단말 복합인증 중요정보 암호화 DRM	애플리케이션 보안성 검증	VPN 암호화		교육·훈련 업무현황 모니터링 정보보안 관리조직 구성
한국 인터넷 진흥원 (2011)	잠금 기능 사용자 인증 원격 데이터 관리 최신 운영체제 단말 인증	취약점 제거 사용자 인증 비정상적 사용 패턴 탐지	데이터 암호화 무선랜 제한 VPN	방화벽 구축 데이터 암호화 무선랜 침입 차단 시스템 구축 사외망과 사내망을 분리할 수 있는 릴레이 서버 구축	DRM 정보 유출 추적 기술 (디지털 포렌식) 정보 유출 시 징계 방안 수립 퇴사할 경우 단말 회수 및 데이터 삭제 원격 데이터 관리 기술 (MDM) 교육
이재호, 이동훈, 김휘강 (2012)	MDM DRM	안티 바이러스 백신 단말 가상화 PMS 코드 서명	VPN	Wireless IDS 및 IPS 릴레이 서버 구축	
정범구 (2011)	원격 잠금·삭제 사용자 인증 문서 보안 접속 관리 안티바이러스 솔루션 원격 제어 플랫폼 보안	정보보호체계 확립 응용프로그램 보안 플랫폼 보안		침입차단 및 방지 고객 망 보안관제 사용자 행위 기록 업무서버 보호 서버와 사용자간 상호 인증	
이경복, 박태형, 임종인 (2011)	잠금 기능 모바일 전용 백신 보안패치 펌웨어 업데이트 원격 제어·삭제 단말기 복합인증	시스템 언락(Unlock) 탐지·차단 애플리케이션 보안성 검증 모바일 전용 백신	송·수신 데이터 암호화 VPN		
이형찬, 이정현, 손기욱 (2011)	사용자 인증 단말 인증 안티바이러스 솔루션 원격 삭제 원격 제어 접속 관리 콘텐츠 보안 하드웨어 보안	앱 보안 플랫폼 구조변경 (탈옥, 루팅 등) 탐지	무선랜 차단 암호화	침입차단 및 방지 보안관제 방화벽 로그관리	
나성욱, 이윤희, 지순정 (2010)	원격 잠금·삭제 사용자 복합인증방식 적용 단말 가상화 솔루션 데이터 전송 통제 업무자료 저장 방지 DRM 적용	정보보호체계 확립 안티바이러스 솔루션 패치관리 솔루션 사용자 인식 제고	전용회선 사용 암호화 VPN WiFi 통제	보안장비 구축·운영 침해사고대응시스템 구축 및 보안관제 FMC 인증장비 및 무선랜침입탐지시스템 구축 내·외부망 분리를 위한 릴레이 연계서버 구축	

※ [7], [9], [14], [17], [18], [23], [28] 재구성

2.4 선행연구 검토와 본 연구의 차별성

2.2(모바일 오피스 보안위협 및 대응방안에 대한 논의)에서 살펴본 선행 연구들은 모바일 오피스를 포함하여 스마트워크의 보안위협과 그에 대한 대응방안을 제시하고 있다. 본 연구에서는 2.1.2(스마트워크의 유형 및 특성)에서 정리한 모바일 오피스 구성요소를 바탕으로 모바일 오피스의 보안 위협에 대한 대응방안을 단말기, 응용프로그램 및 플랫폼, 네트워크, 서버, 사용자 등 5개 영역으로 구분하여 정리하였다(<표 2> 참조). 지금까지 살펴본 스마트워크 보안 위협 및 대응방안에 관한 연구는 주로 문헌 분석 또는 사례 분석 위주의 방식으로 진행되었으며, 실증 연구는 거의 없는 것으로 보인다.

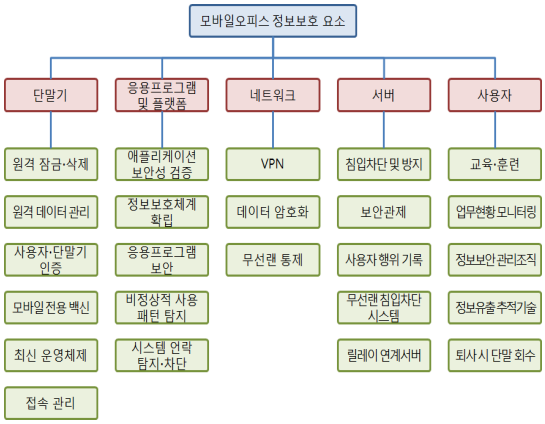
2.3(정보보호 분야에서의 AHP 분석의 활용)에서 살펴본 AHP 활용 연구는 주로 정보보호 관련 정책, SNS 환경에서의 위협 요인, 정보보호시스템 개발 단계에서의 품질 요소를 다루고 있다. 정보보호 분야에서 AHP 분석을 활용한 연구가 점차 늘어나는 추세이나, 아직까지 스마트워크 관련 내용을 다루는 연구는 없는 것으로 보인다. 따라서 본 연구는 스마트워크 정보보호 요소의 중요도 분석에 AHP를 활용하여 중소기업 종사자를 대상으로 실증 분석을 한다는 점에서 기존 연구와 차별화 된다.

3. 연구방법

3.1 스마트워크 정보보호 요소의 계층적 분류

본 연구에서는 스마트워크의 한 유형인 모바일 오피스 도입 시 우선적으로 고려해야 할 정보보호 요소를 계층적 분석방법인 AHP를 통하여 알아보고자 한다. 모바일 오피스 정보보호 요소는 2장에서 분석한 선행연구 결과를 바탕으로 [그림 1]과 같이 단말기, 응용프로그램 및 플랫폼, 네트워크, 서버, 사용자 등 5개 영역으로 구분하고 각 영역별로 정보보호 요소를 구성하였다.

각 영역별 정보보호 요소는 다음과 같다. 첫째, 단말기 영역은 방송통신위원회・한국인터넷진흥원(2011), 한국인터넷진흥원(2011), 이재호・이동훈・김휘강(2012), 정범구(2011), 이경복・박태형・임종인(2011), 이형찬・이정현・손기욱(2011), 나성욱・이윤희・지순정(2010) 등의 연구결과를 분석하여 원격 잠금·삭제, 원격 데이터 관리, 사용자·단말기인증, 모바일 전용 백신, 최신 운영체제, 접속 관리 등으로 구성하였다.



[그림 1] 모바일오피스 정보보호 요소 계층도

둘째, 응용프로그램 및 플랫폼 영역은 방송통신위원회・한국인터넷진흥원(2011), 한국인터넷진흥원(2011), 이재호・이동훈・김휘강(2012), 정범구(2011), 이경복・박태형・임종인(2011), 이형찬・이정현・손기욱(2011), 나성욱・이윤희・지순정(2010) 등의 연구결과를 분석하여 애플리케이션 보안성 검증, 정보보호체계 확립, 응용프로그램 보안, 비정상적 사용 패턴 감지, 시스템 언락(Unlock) 탐지·차단 등으로 구성하였다.

셋째, 네트워크 영역은 방송통신위원회・한국인터넷진흥원(2011), 한국인터넷진흥원(2011), 이재호・이동훈・김휘강(2012), 이경복・박태형・임종인(2011), 이형찬・이정현・손기욱(2011), 나성욱・이윤희・지순정(2010) 등의 연구결과를 분석하여 VPN(Virtual Private Network), 데이터 암호화, 무선랜(WiFi) 통제 등으로 구성하였다.

넷째, 서버 영역은 한국인터넷진흥원(2011), 이재호・이동훈・김휘강(2012), 정범구(2011), 이형찬・이정현・손기욱(2011), 나성욱・이윤희・지순정(2010) 등의 연구결과를 분석하여 침입차단 및 방지, 보안관제, 사용자 행위 기록, 무선랜 침입차단시스템, 릴레이 연계서버 등으로 구성하였다.

다섯째, 사용자 영역은 방송통신위원회・한국인터넷진흥원(2011), 한국인터넷진흥원(2011) 등의 연구결과를 분석하여 교육·훈련, 업무현황 모니터링, 정보보안 관리조직, 정보유출 추적기술(디지털 포렌식), 퇴사 시 단말 회수 등으로 구성하였다.

각 영역에 포함되는 정보보호 요소의 내용에 대한 설명과 더불어, 참조한 기존연구는 <표 3>에 좀 더 자세히 제시하였다.

3.2 조사 방법

본 연구에서는 중소기업 종사자를 대상으로 2012년 11월 12일부터 11월 23일까지 약 2주간 온라인 설문조사를 실시하여 136명의 표본을 추출하였다.

AHP 조사와 관련해서, 각 문항간의 이원쌍대비교는 Saaty(1980), Saaty(1982), Saaty & Vargas(1991a), Saaty & Vargas(1991b), 조근태・조용곤・강현수(2003), 조근태 역(2005) 등의 핵심적인 연구를 참조하여 1-5점 척도 방식으로 진행하였다[24][25][33][34][35][36]. 총 응답자 136명에 대해서 AHP 분석에서는 일관성 비율이 기준값(CR=0.1)을 벗어 나거나† 설문지 응답이 불성실한 지를 꼼꼼히 검토한 후[2][4][24][25], 최종적으로 136명 모두

〈표 3〉 모바일 오피스 정보보호 요소

영역	하위 요소	주요 내용	선행 연구
단말기	원격 잠금·삭제	단말기 분실·도난 시 단말기를 사용하지 못하도록 원격에서 잠금 또는 데이터 삭제 조치	[7] [9] [14] [17] [18] [23] [28]
	원격 데이터 관리	단말기 내 중요정보의 원격 백업, 삭제, 복원 등	
	사용자·단말기 인증	사용자 및 단말기 인증을 통해 타인이 모바일 오피스 시스템에 접근하는 것을 차단	
	모바일 전용 백신	모바일 전용 바이러스백신의 설치와 보안패치 적용	
	최신 운영체제	정기적인 보안패치 적용으로 최신 악성코드 유입 차단	
	접속 관리	PC와 스마트폰 사이의 데이터 전송 통제 및 P2P/웹하드 접속 금지 등	
응용프로그램 및 플랫폼	애플리케이션 보안성 검증	애플리케이션 아키텍처에 대한 보안을 검토하고 검증하기 위해 국내외 보안성 평가 및 인증제도에 따라 검증	[7] [9] [14] [17] [18] [23] [28]
	정보보호체계 확립	개발(인증·가이드·코드서명), 판매(SW검증), 사용(SW정보 공유) 전 단계에서 안전한 SW 유통체계 환경 조성	
	응용프로그램 보안	응용프로그램 공급사이트를 통한 정기적인 패치 관리	
	비정상적 사용 패턴 탐지	응용프로그램 접속 내역 분석을 통해 비정상적인 사용 패턴 탐지	
	시스템 언락(Unlock) 탐지·차단	기본적으로 탑재되어 있는 펌웨어를 고의적으로 조작한 펌웨어로 교체하는 언락(Unlock) 탐지 및 차단	
네트워크	VPN	인터넷망과 같은 공중망을 사설망처럼 이용할 수 있는 VPN(Virtual Private Network) 적용	[7] [9] [14] [17] [18] [28]
	데이터 암호화	데이터 및 음성의 도·감청 방지를 위해 송·수신 데이터 암호화	
	무선랜(WiFi) 통제	보안이 취약한 무선랜(WiFi)을 통한 시스템 접속 통제	
서버	침입차단 및 방지	방화벽, 침입탐지시스템 등 보안장비 구축·운영	[7] [17] [18] [23] [28]
	보안관제	침해사고 대응을 위해 24시간 보안 관제	
	사용자 행위 기록	사용자가 수행한 작업 로그 저장	
	무선랜 침입탐지 시스템	무선랜을 통한 침입 탐지 및 차단 시스템 구축	
	릴레이 연계서버	스마트폰에서 내부 업무서버로 직접 연결을 차단하고, 외부망과 내부망을 분리할 수 있는 릴레이 연계서버 구축	
사용자	교육·훈련	장비 및 소프트웨어의 사용법뿐만 아니라 스마트워크 정책, 보안사고 발생 시 대응 방법 등에 대한 교육·훈련	[9] [28]
	업무현황 모니터링	기업정보 보호를 위해 내부규정 준수 여부 및 단말기 사용현황 등 업무현황 모니터링	
	정보유출 추적기술 (디지털 포렌식)	악의적인 정보 유출을 탐지·추적할 수 있는 기술(디지털 포렌식) 도입	
	정보보안 관리조직	스마트워크를 위한 정보보안 관리조직 구성	
	퇴사 시 단말 회수	모바일 오피스 사용자가 퇴사할 경우 사용하던 단말 회수 및 데이터 삭제	

† 일반적으로 일관성비율(Consistency Ratio)이 10%(0.1)를 넘게 되면 의사결정자가 논리적 일관성을 잃고 있는 것으로 판단하여 의사결정과정을 점검하는 기준으로 삼고 있으나(조근태・조용곤・강현수(2003), 조근태 역(2005), 김윤주・심준섭(2007)), 여러 가지 상황을 고려할 때 20%(0.2)까지는 의미를 가진다는 견해(고길곤・하혜영(2008))도 존재한다. 그러나 본고에서는 이 가운데 좀 더 엄격한 조건의 일관성비율을 기준으로(CR=0.1) 판단하였다.

를 대상으로 그룹쌍대비교를 실시하여 분석 결과를 도출하였다. 실증분석에서 사용한 분석프로그램은 Expert Choice의 그룹쌍대비교(Group Pairwise)와 엑셀(EXCEL)을 활용하여 의사결정과정을 구조화하고 여러 표본의 견해를 종합하여 그룹의사결정의 질을 높이고자 하였으며, 분석결과의 정확성을 검증하는 과정을 거쳤다.

4. 조사결과 분석

4.1 표본의 현황

분석에 활용된 표본은 136개로, 표본의 주요 현황을 살펴보면 <표 4>와 같다. 이상의 내용을 각각의 주요 특성별로 살펴보면 다음과 같다.

〈표 4〉 표본의 현황

구분		빈도	퍼센트
소속기관 직원규모	10명 미만	24	17.6
	10-50명 미만	45	33.1
	50-100명 미만	11	8.1
	100-300명 미만	11	8.1
	300명 이상	45	33.1
성별	남자	91	66.9
	여자	45	33.1
직급	임원급	17	12.5
	부장급	25	18.4
	과장급	43	31.6
	사원급	47	34.6
	기타	4	2.9
직무분야	사무직	70	51.5
	전산직	24	17.6
	기술직	32	23.5
	영업직	4	2.9
	기타	6	4.4
실무능력	5년 미만	41	30.1
	5-10년 미만	26	19.1
	10-15년 미만	39	28.7
	15-20년 미만	22	16.2
	20년 이상	8	5.9
모바일 오피스 정보보호에 대한 전문지식 수준	매우 낮음	14	10.3
	낮음	30	22.1
	보통	59	43.4
	높음	26	19.1
	매우 높음	7	5.1
합계		136	100.0

첫째, 표본들의 소속기관은 300명 이상과 10-50명 미만이 33.1%로 가장 많은 비중을 차지하고 있으며, 그 다음으로는 10명 미만(17.6%), 100-300명 미만과 50-100명 미만(8.1%)의 순임을 알 수 있다. 따라서 상대적으로 직원 규모가 많은 조직과 더불어, 다소 직원 규모가 적은 조직이 유사한 비중으로 분포하고 있음을 유추할 수 있다.

둘째, 표본들의 성별은 남자가 66.9%로 여자 33.1% 보다 다소 많은 비중을 차지하고 있음을 알 수 있다.

셋째, 표본들의 직급은 주로 사원급이 34.6%로 가장 많은 비중을 차지하고 있으며, 그 다음으로는 과장급(31.6%), 부장급(18.4%), 임원급(12.5%) 등의 순임을 알 수 있다. 따라서 대체로 직급이 낮음 표본이 상대적으로 많은 비중을 차지하고 있음을 유추할 수 있다.

넷째, 표본들의 직무분야는 과반수가 사무직(51.5%)에 해당되며, 그 다음으로는 기술직(23.5%), 전산직(17.6%), 기타(4.4%), 영업직(2.9%) 등의 순임을 알 수 있다.

다섯째, 표본들의 실무경력은 주로 5년 미만이 30.1%로 가장 많은 비중을 차지하고 있으며, 그 다음으로는 10-15년 미만이 28.7%, 5-10년 미만 19.1%, 15-20년 미만이 16.2%, 20년 이상이 5.9%의 순임을 알 수 있다. 따라서 대체로 실무경력이 균형적으로 표본이 추출된 것으로 보인다.

여섯째, 표본들은 주로 보통수준에 해당된다는 비중이 43.4%로 가장 많았으며, 그 외에는 낮은 수준이 22.1%, 높은 수준이 19.1%, 매우 낮음이 10.3%, 매우 높음이 5.1%의 순으로 거의 유사한 비중을 보이고 있음을 알 수 있다.

4.2 AHP를 활용한 스마트워크 정보보호 요소의 중요도 분석 결과

<표 5>는 AHP를 통해서 모바일 오피스 각 영역 및 세부 하위요소에 대한 상대적 우선순위를 분석한 결과를 종합적으로 제시한 것이다. 이를 통해서 제1수준에 해당되는 각 영역별 가중치와 순위, 그리고 제2수준에 해당되는 세부 하위요소별 가중치와 순위와 더불어, 제1수준과 제2수준을 종합하여 세부 하위요소별 전체 가중치의 순위를 파악할 수 있다. 이상의 내용을 각 영역(제1수준)과 세부 하위요소(제2수준)로 세분화하여 상대적으로 중요한 우선순위를 살펴보자.

4.2.1 영역별 우선순위 비교

영역(Level1)에 대한 우선순위의 분석 결과, '사용자'가 24.810%로 상대적으로 가장 높은 비중을 차지하고 있으며, 그 다음으로는 '서버(21.682%)', '응용 프로그램 및 플

〈표 5〉 AHP를 활용한 스마트워크(중소기업 모바일 오피스) 정보보호 요소의 중요도 분석

영역(Level 1)			하위 요소(Level 2)			전체	
영역 구분	가중치 (%)	가중치 (순위)	하위 요소	가중치 (%)	가중치 (순위)	가중치 (%)	가중치 (순위)
단말기	11.457 %	5	원격 잠금·삭제	9.237%	6	1.058%	24
			원격 데이터 관리	12.522%	5	1.435%	23
			사용자·단말기 인증	19.911%	2	2.281%	20
			모바일 전용 백신	18.412%	3	2.110%	21
			최신 운영체제	17.781%	4	2.037%	22
			접속 관리	22.137%	1	2.536%	19
응용 프로그램 및 플랫폼	21.517 %	3	애플리케이션 보안성 검증	16.041%	5	3.451%	18
			정보보호체계 확립	16.651%	4	3.583%	16
			응용프로그램 보안	20.431%	3	4.396%	10
			비정상적 사용패턴 탐지	22.170%	2	4.770%	8
			시스템 언락(Unlock) 탐지·차단	24.708%	1	5.316%	6
네트워크	20.535 %	4	VPN	27.090%	3	5.563%	5
			데이터 암호화	41.261%	1	8.473%	1
			무선랜(WiFi) 통제	31.649%	2	6.499%	2
서버	21.682 %	2	침입차단 및 방지	19.788%	3	4.291%	12
			보안관제	18.873%	5	4.092%	14
			사용자 행위 기록	19.558%	4	4.241%	13
			무선랜 침입탐지시스템	21.788%	1	4.724%	9
			릴레이 연계서버	19.993%	2	4.335%	11
사용자	24.810 %	1	교육·훈련	15.828%	4	3.927%	15
			업무현황 모니터링	14.371%	5	3.565%	17
			정보유출 추적기술 (디지털 포렌식)	21.151%	3	5.247%	7
			정보보안 관리조직	23.720%	2	5.885%	4
			퇴사 시 단말 회수	24.931%	1	6.185%	3
소계	100%	–	–	500%	–	100%	–

랫폼(21.517%)', '네트워크(20.535%)', '단말기(11.457%)'의 순으로 상대적 가중치가 높은 것으로 나타났다. 따라서 중소기업의 모바일 오피스의 영역 가운데 '사용자'와 관련된 다양한 세부 요소(교육훈련, 업무현황 모니터링, 정보유출 추적기술, 정보보안 관리 조직, 퇴사 시 단말 회수)에 대한 우선적인 고려가 필요하다고 인식하고 있음을 알 수 있다.

4.2.2 영역내 세부 하위요소별 우선순위 비교

각 영역내 세부 하위요소(Level2)에 대한 우선순위 분석결과를 살펴보자. 첫째, '단말기' 영역의 세부 하위요소에 대한 우선순위 분석결과, '접속관리'가 22.137%로 가장 높은 가중치를 보이고 있으며, 그 다음으로는 '사용자·단말기 인증(19.911%)', '모바일 전용 백신(18.412%)', '최신 운영체제(17.781%)', '원격 데이터 관리(12.522%)', '원격 잠금·삭제(9.23%)'의 순으로 우선순위를 보이는 것으로 나타났다. 즉 '접속관리'는 PC와 스마트폰 사이의 데이터 전송 통제 및 P2P/웹하드 접속 금지 등을 의미하는 것으로, 이에 대한 우선적인 고려가 필요함을 시사하는 것으로 판단된다.

둘째, '응용 프로그램 및 플랫폼' 영역의 세부 하위요소에 대한 우선순위 분석결과, '시스템 언락(Unlock) 탐지·차단'이 24.708%로 가장 높은 가중치를 보이고 있으며, 그 다음으로는 '비정상적 사용패턴 탐지(22.170%)', '응용 프로그램 보안(20.431%)', '정보보호체계 확립(16.651%)', '애플리케이션 보안성 검증(16.041%)'의 순으로 우선순위를 보이는 것으로 나타났다. 즉 '시스템 언락(Unlock) 탐지·차단'은 기본적으로 탑재되어 있는 펌웨어를 고의적으로 조작한 펌웨어로 교체하는 언락(Unlock) 탐지 및 차단을 의미하는 것으로, 이에 대한 우선적인 고려가 중요할 수 있음을 잘 보여준다.

셋째, '네트워크' 영역의 세부 하위요소에 대한 우선순위 분석결과, '데이터 암호화'가 41.261%로 가장 높은 가중치를 보이고 있으며, 그 다음으로는 '무선랜 통제(31.649%)', 'VPN(27.090%)'의 순으로 우선순위를 보이는 것으로 나타났다. 즉 '데이터 암호화'는 데이터 및 음

성의 도·감청 방지를 위해 송·수신 데이터의 암호화를 의미하는 것으로, 이에 대한 우선적인 고려가 요구되는 것으로 판단된다.

넷째, '서버' 영역의 세부 하위요소에 대한 우선순위 분석결과, '무선랜 침입탐지시스템'이 21.788%로 가장 높은 가중치를 보이고 있으며, 그 다음으로는 '릴레이 연계 서버(19.993%)', '침입차단 및 방지(19.788%)', '사용자 행위 기록(19.558%)', '보안관제(18.873%)'의 순으로 우선순위를 보이는 것으로 나타났다. 즉 '무선랜 침입탐지시스템'은 무선랜을 통한 침입 탐지 및 차단 시스템 구축을 의미하는 것으로, 이에 대한 우선적인 고려가 필요함을 잘 보여준다.

다섯째, '사용자' 영역의 세부 하위요소에 대한 우선순위 분석결과, '퇴사 시 단말 회수'가 24.931%로 가장 높은 가중치를 보이고 있으며, 그 다음으로는 '정보보안 관리 조직(23.720%)', '정보유출 추적기술(디지털 포렌식)(21.151%)', '교육훈련(15.828%)', '업무현황 모니터링(14.371%)'의 순으로 우선순위를 보이는 것으로 나타났다. 즉 '퇴사 시 단말 회수'는 모바일 오피스 사용자가 퇴사할 경우 사용하던 단말 회수 및 데이터 삭제를 의미하는 것으로, 이에 대한 우선적인 고려가 필요함을 잘 보여준다.

4.2.3 영역과 세부 하위요소 종합 우선순위 비교

전술한 영역(Level1)과 세부 하위요소(Level2)의 상대적인 가중치를 종합적으로 고려할 때, 상대적 우선순위를 살펴보자. 이는 영역(Level1)과 세부 하위요소(Level2)의 도출된 상대적 가중치를 서로 곱하여 산출되는 종합적인 우선순위를 의미한다.

그 결과, 전체 세부 하위요소 간에는 아주 큰 가중치의 차이를 보이는 것은 아니지만, 상대적으로 '네트워크' 영역의 '데이터 암호화'가 8.473%로 1순위, '네트워크' 영역의 '무선랜 통제'가 6.499%로 2순위, '사용자' 영역의 '퇴사 시 단말 회수'가 6.185%로 3순위 등으로 상대적으로 높은 가중치를 보이는 것으로 나타났다. 따라서 '데이터 및 음성의 도·감청 방지를 위해 송·수신 데이터 암호화', '보안이 취약한 무선랜(WiFi)을 통한 시스템 접속 통제', '모바일 오피스 사용자가 퇴사할 경우 사용하던 단말 회수 및 데이터 삭제' 등을 우선적으로 고려하여 모바일 오피스를 구현할 필요가 있음을 알 수 있다.

5. 결론

5.1 요약 및 시사점 논의

스마트워크는 시간과 장소에 얽매이지 않고 언제 어디서나 편리하고 똑똑하게 근무함으로써 업무효율성을 향상시킬 수 있는 업무방식을 말하며, 과학기술 및 정보통신기술의 발달로 많이 이슈화되고 있다. 이에 본 연구에서는 중소기업이 스마트워크의 한 유형인 모바일 오피스를 도입할 때 고려해야할 정보보호 요소를 도출하고, 이들 간에 상대적 우선순위를 실증적으로 분석해봄으로써, 정보보호 측면에서의 스마트워크 정책 방향을 제시하고자 하였다.

본 연구의 주요 연구결과를 요약하면 다음과 같다. 첫째, 영역(Level1)에 대한 우선순위의 분석 결과, '사용자'가 24.810%로 상대적으로 가장 높은 비중을 차지하고 있어, 이와 관련된 세부 요소들에 대한 우선적인 고려가 필요한 것으로 나타났다.

둘째, 각 영역별 세부 하위요소에 대해서 분석해보면, ① '단말기' 영역은 '접속관리'가 22.137%로 가장 높은 가중치를 보이고 있으며, ② '응용 프로그램 및 플랫폼' 영역의 경우, '시스템 언락(Unlock) 탐지·차단'이 24.708%로 가장 높은 가중치를 보이고 있다. ③ '네트워크' 영역에서는 '데이터 암호화'가 41.261%로 가장 높은 가중치를 보이고 있으며, ④ '서버' 영역은 '무선랜 침입탐지시스템'이 21.788%로 가장 높은 가중치를, ⑤ '사용자' 영역의 경우, '퇴사 시 단말기 회수'가 24.931%로 가장 높은 가중치를 보이고 있어, 이러한 요소들을 우선적으로 고려해야 함을 알 수 있었다.

셋째, 전술한 영역(Level1)과 세부 하위요소(Level2)의 상대적인 가중치를 종합적으로 고려하였을 경우에는 상대적으로 '네트워크' 영역의 '데이터 암호화(8.473%)'와 '무선랜 통제(6.499%)'가 각각 1, 2순위, '사용자' 영역의 '퇴사 시 단말 회수'가 6.185%로 3순위 등으로 상대적으로 높은 가중치를 보이는 것으로 나타났다. 따라서 이러한 요소들을 우선적으로 고려하여 모바일 오피스를 구현할 필요가 있음을 알 수 있다.

5.2 연구의 한계와 후속연구의 방향

본 연구는 방법론상에서 다음과 같은 한계를 가질 수 있어 향후 해석상의 주의와 추가적인 보완 연구 등이 이루어져야 한다.

본 연구의 AHP 체계가 모바일 오피스에서 고려해야 하는 정보보호 요소를 모두 포함한 것인지, 그리고 각 계층별 하위항목간의 정렬이 타당하게 이루어진 것인지 등에 대한 방법론적 비판이 존재할 수 있다. 왜냐하면 의사결정 체계에 대한 자의성에 대한 비판은 AHP 방법론이 가지는 근원적인 한계이기 때문이다. 따라서 본 연구의 AHP 조사체계가 모바일 오피스와 관련된 세부 내용을 충분히 반영하고 있다고 주장하기 보다는 향후 다양한 외생적, 내생적 환경과 수요를 반영하여 추가적으로 고려해야 할 요소가 무엇인지를 지속적으로 고민해보아야 할 것이다. 따라서 본 연구의 측정도구를 현실에 맞게 보다 정교화 하여 다양한 분석단위를 대상으로 한 추가적인 실증분석이 이루어질 필요가 있다.

그리고 본 연구에서 활용한 양적인 방법론이 가지는 근본적인 한계를 보완하기 위해서 각 기관(중소기업)의 상황에 맞는 심층적인 사례분석이나 인터뷰, 면접 등의 질적인 방법론을 활용한 보완적인 연구가 이루어질 필요가 있다.

참 고 문 헌

[1] 강진규・민병찬 (2008). AHP의 이론과 실제. 도서출판 인터비젼.

[2] 고길곤・하혜영 (2008). 정책학 연구에서 AHP 분석기법의 적용과 활용. 한국정책학회보, 17(2), 287-312.

[3] 김상현・송재필・손진수 (2008). 네트워크를 통한 실질적이고 효과적인 다자간 영상회의 서비스. 한국정보통신설비학회 학술대회, 478-481.

[4] 김윤주・심준섭 (2007). 가중치 추출기법의 비교 : AHP, JA, Swing 기법을 중심으로. 국가정책연구, 21(1), 5-33. 국가정책연구소.

[5] 김태성・전효정 (2008). AHP를 이용한 정보보호인력 양성 정책 분석. 한국통신학회논문지, 31(5B), 486-493.

[6] 김필주・장원환・이춘근・정연옥・이영래・김은혜 (2008). 초고령 사회에 대비한 효율적 인력 활용.

[7] 나성욱・이윤희・지순정 (2010). 스마트폰과 모바일 오피스의 보안 이슈 및 대응 전략. CIO REPORT Vol.26, 1-28. 한국정보화진흥원.

[8] 방송통신위원회 (2011). 스마트워크 활성화 추진계획.

[9] 방송통신위원회・한국인터넷진흥원 (2011). 스마트워크 활성화를 위한 정보보호 권고 해설서.

[10] 방송통신위원회・한국정보화진흥원 (2011). 기업을 위한 스마트워크 도입·운영 가이드북.

[11] 성기훈・공희경・김태한 (2010). AHP를 이용한 SNS 정보보호 위협요인 분석. 정보보호학회논문지, 20(6), 261-270.

[12] 성욱준・김동욱 (2011). AHP(Analytic Hierarchy Process)를 이용한 정보보호정책 우선순위에 관한 연구. 한국행정학회 하계학술발표논문집, Vol.2011, 1-21.

[13] 신영진・정형철・강원영 (2012). 공공분야 개인정보보호 정책 집행과제의 우선순위 분석 : 개인정보보호 수준진단 지표의 선정 및 중요도를 중심으로. 정보보호학회논문지, 22(2), 379-390.

[14] 이경복・박태형・임종인 (2011). 스마트워크 환경 변화에 따른 보안위협과 대응방안. 디지털정책연구, 9(5), 29-40.

[15] 이민혜・이준기 (2011). 스마트워크 연구에 대한 고찰과 향후 연구 주제. 정보화정책, 18(2), 2011년 여름호, 72-84.

[16] 이애련 (2009). 저출산시대에 재택근무 활성화 방안에 관한 연구. 한국여성교양학회지, 제18집, 21-47.

[17] 이재호・이동훈・김휘강 (2012). 스마트워크 환경에서 이상접속탐지를 위한 의사결정 시스템 연구. 정보보호학회논문지, 22(4), 797-808.

[18] 이형찬・이정현・손기욱 (2011). 스마트워크 보안 위협과 대책. 정보보호학회지, 21(3), 12-21.

[19] 이호경 (2009). 고객중심의 IPTV 서비스품질모형 개발에 대한 연구. 석사학위 논문, 성균관대학교.

[20] 임광현・이동진・김진혁 (2010). 스마트워크 연구 경향분석. 정보화정책, 17(4), 2010년 겨울호, 3-22.

[21] 임정아 (2011). AHP를 이용한 건설-IT 융합 사업의 성공요인과 평가체계에 관한 연구. 석사학위 논문, 성균관대학교.

[22] 전자신문・중소기업기술정보진흥원 (2010). 신정보화 수준 조사.

[23] 정범구 (2011). 스마트오피스 환경에서 보안대책 연구. 석사학위 논문, 건국대학교.

[24] 조근태 역 (2005). 네트워크 분석적 의사결정. 서울: 동현출판사. Saaty, T. L. (1980). The Analytic Network Process(2nd).

[25] 조근태・조용곤・강현수 (2003). 앞서가는 리더들의 계층분석적 의사결정. 서울 : 동현출판사.

[26] 최명길・박유진 (2008). 유전자 알고리즘을 이용한

통합정보보호시스템의 최적 품질 수준 탐색에 관한 연구. 대한경영학회지, 21(6), 2751-2769.
[27] 최연호 (2011). 모바일 오피스 유형분석을 통한 정보보호관리체계(ISMS) 정보보호모형의 개선에 대한 연구. 석사학위 논문, 고려대학교.
[28] 한국인터넷진흥원 (2011). 스마트워크 도입을 위한 정보보호 수립 기준 연구.
[29] 한국정보화진흥원 (2010). 일하는 방식의 대혁명적 변화 '스마트 워크'. Smartwork Insight 제1호.
[30] 한국정보화진흥원 (2011). 스마트워크 도입현황 진단을 통한 활성화 방안에 관한 연구.
[31] 한국정보화진흥원 (2011). 스마트워크 활성화를 위한 수요조사 결과.
[32] 행정안전부 (2010). 스마트워크 추진 계획.
[33] Saaty, T. L. & Vargas, L. G. (1991a). Prediction, Projection and Forecasting. Boston: Kluwer Academic Publishers.
[34] Saaty, T. L. & Vargas, L. G. (1991b). The Logic of Priorities. RWS Publications.
[35] Saaty, T. L. (1980). The Analytic Hierarchy Process. Mcgraw-Hill.
[36] Saaty, T. L. (1982). Decision Making for Leaders: The Analytical Hierarchy Process for Decisions in a Complex World. Belmont. Calif: Lifetime Learning Publication

강 경 훈

- 2001년 2월 : 성균관대학교 문헌정보학(학사)
- 2013년 2월 : 고려대학교 공공보안정책학(석사)
- 2003년 4월~현재 : 한국정보화진흥원 책임연구원
- 관심분야 : 네트워크정책, 정보보호정책, 스마트워크
- E-Mail : emptyee@nia.or.kr

임 채 홍

- 2003년 2월 : 광운대학교 행정학(경영학 부전공)(학사)
- 2005년 2월 : 고려대학교 행정학(계량행정)(석사)
- 2008년 2월 : 고려대학교 행정학(정책분석평가)(박사수료)
- 2008년 3월~현재 : 고려대학교 정부학연구소 연구원
- 관심분야 : 정책분석평가(과학기술정책, 사회문화정책), 계량분석 및 방법론
- E-Mail : dlacoghd@hanmail.net

임 종 인

- 1980년 2월 : 고려대학교 수학(학사)
- 1982년 2월 : 고려대학교 수학(석사)
- 1986년 2월 : 고려대학교 수학(박사)
- 1986년 3월~현재 : 고려대학교 교수/정보보호대학원장
- 관심분야 : 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등
- E-Mail : jilim@korea.ac.kr

박 태 형

- 2002년 2월 : 고려대학교 서양사학(행정학부전공)(학사)
- 2004년 2월 : 고려대학교 행정학(석사)
- 2011년 2월 : 고려대학교 정보보호대학원 정보보호공학(정보보호정책 전공)(박사)
- 2011년 3월~2013년 2월 : 고려대학교 정보보호대학원 연구교수
- 2013년 3월~현재 : 고려대학교 사이버국방연구센터
- 관심분야 : 정보보호정책, 성과평가, 사이버국방, 방위사업
- E-Mail : mosto2004@korea.ac.kr