스마트워크 보안 방안에 대한 연구

김태경*, 서희석**, 이동영***
*서울신학대학교 교양학부
**한국기술교육대학교 컴퓨터공학부
***명지전문대학 정보통신과
e-mail : tkkim@stu.ac.kr

A Study on the security method for Smart Work

Tae-Kyung Kim*, Hee-Suk Seo**, Dong-Young Lee***
*Dept. of Liberal Art, Seoul Theological University
**Dept. of Computer Science & Engineering, Korea University of Technology and Education
***Dept. of Information Technology and Communication, Myongji College

요 약

스마트 장비의 발달로 장소와 환경에 상관없이 자유롭게 일을 할 수 있는 스마트워크가 중요한 이슈로 부각되고 있다. 이에 본 연구에서는 스마트워크의 개념 및 해외 동향을 살펴보고, 스마트워크가 활성화되기 위해 필요한 보안 방안에 대한 주요한 요건들에 대해서 살펴보았다. 스마트워크에서 안전성이 확보된다면 저 탄소 녹색성장을 포함하여 사회의 저 출산·고령화, 낮은 노동 생산성 등 당면 현안을 해결하는 방안으로 스마트워크가 유용하게 사용될 수 있다.

1. 서론

스마트 장비의 발달로 인해 다양한 업무의 형태가 등장하고 있으며 특히 일하는 방식을 선진화하고 우리사회의 저 출산, 고령화 그리고 낮은 노동 생산성을 해결하기 위해 스마트워크에 대한 관심이 증대되고 있다. 또한 스마트기기의 보급 확산과 더불어 최근 클라우드 컴퓨팅 관련 기술이 확산되고 있으며, 최적의 스마트워크 도입을 위한 환경이 구축되어 있어 노동의 효율성을 높이고 국민의 삶의 질을 개선하기 위해서는 스마트워크 추진이 필요한 시점이다.

스마트워크는 정보통신기술을 이용하여 시간과 장소의 제약 없이 업무 수행에 있어서 관계자들과 협업하고 지속적인 업무를 수행하는 근로 형태라 할 수 있다. 스마트워크는 근로 시간과 장소의 측면에서 유연성이 심화된 개념으로, 다양한 종류의 정보·지식의 통합과 활용, 상호간의 신뢰와 협업 등을 통해 노동의 효율성 개선을 추구하는 것을 포괄적으로 함축하고 있다[1].

2. 스마트워크의 해외 현황

2.1 미국

미국에서의 스마트워크는 주로 원격근무의 형태로 진행되고 있다. 미국의 연방기관 중 원격근무를 관장하는 기관은 인사관리처 (OPM : Office of Personnel Management)와 일반행정청 (GSA : General Services Administration)이 맡고 있으며, 최근 들어 미국에서는 스마트워크 센터를 2011 년까지 100 개소를 건설하여 저 탄소 업무환경을 구축할 것이라고 발표하였다[2].

또한 미국은 원격근무 주관부처인 OPM 과 GSA 의 지원 아래 원격근무의 확대를 지속적으로 진행하였으며, 특히 2001 년도에 제정된 된 Public Law 106-346(FY 2001 Department of Transportation and Related Agencies Appropriations Act) 359 조에 따라, 각 기관은 원격근무자격을 갖춘 직원들이 성과를 저해하지 않는 범위에서 원격근무에 최대한 참여할 수 있는 정책을 수립하여 원격근무를 적극 권장하고 있다[6].

2.2 일본

일본 스마트워크의 추진정책은 스마트워크에 필요한 정보통신시스템 기반 정비, 스마트워크 보급을 위한 민간, 공무원 분야별 제도환경 정비, 공무원 스마트워크 보급 정책으로 나뉘어 추진하고 있다[3]. 일본 정부는 저 출산 고령화로 인한 노동인구 감소를 심각한 사회문제로 인식하고, 이를 해결하는 대안으로 원격근무제도를 추진하고 있다. 2003 년 e-Japan 중점계획을 기점으로 가이드라인 개발 및 환경정비 착수하였고, 2007 년에 텔레워크(스마트워크) 인구배증을 위한 액션플랜을 수립하였다[1].

2.3 네덜란드

네덜란드는 스마트워크센터(SWC)를 설치하여 집과 회사의 장점을 복합한 제 3 의 공간으로 창조하여 생활 및 업무방식을 혁신적으로 변화시키고 있다. 특히 일정기준에 부합하는 비즈니스 사업장을 SWC 로 인증하고 있다[4]. 네덜란드는 전체 사업체의 49%가 원격근무 제도를 운영 중에 있으며, 고용 규모가 큰 기업일수록 원격근무자의 비율이 높고, 500 인 이상의 경우에는 91%가 원격근무를 실시하고 있다.

또한 원격근무, 영상회의, 금융 및 복지시설 등이 완비된 스마트워크센터를 공공기관과 민간기업이 공동으로 구축·운영하고 있으며, 현재까지 암스테르담 위성도시를 중심으로 90 여 개를 연계하여 구축하고 스마트 폰 기반의 애플리케이션을 제공하고 있다[4].

3. 스마트워크의 유형

3.1 재택근무

자택에서 본사 정보통신망에 접속하여 업무를 수행하고, 별도의 사무 공간이 필요하지 않으며 출퇴근 시간 및 교통비 부담이 감소한다는 장점이 있다. 단점으로는 노동자의 고립감 증가와 협동업무의 시너지 효과가 감소하고, 보안성 미흡으로 인해 일부 업무만 제한적인 수행이 가능하다[1].

3.2 이동근무

모바일 기기 등을 이용하여 현장에서 업무를 수행하는 방식이며, 대면업무 및 이동이 많은 근무환경에 유리하다. 단점으로는 스마트 폰 등을 활용한 위치추적 등 근무자에 대한 효과적인 제어가 강화되어야 한다[1].

3.3 스마트워크센터 근무

자택 인근 원격사무실에 출근하여 업무를 수행하는 방식이며, 본사와 유사한 수준의 사무환경 제공이 가능하고, 근태관리가 용이하며, 보안성의 확보 및 직접적인 가사 육아에서 벗어나 업무집중도의 향상이 가능하다는 장점을 가지고 있다. 단점으로는 별도의 사무 공간 및 관련 시설에 대한 비용부담이 발생하고, 관련 법 및 제도의 정비 및 관리조직 및 시스템의 구축이 필요하다[1].

4. 스마트워크 보안 방안

스마트워크와 같은 모바일 환경에서의 전자적인 침해행위는 실시간성과 동시성, 비대면성과 익명성, 광역성 내지 국제성, 범죄영역의 무한대성, 전파의 신속성과 피해의 대규모성, 범행의 반복성, 범죄적발 및 입증의 곤란과 손해배상의 어려움 등의 속성이 있다[5]. 그러므로 안정적인 스마트워크 서비스를 제공하기 위해서는 스마트워크 인증제도에 대한 고려가 필요하며, 스마트워크 센터 보안 인증을 위한 체크리스트 구성에 대한 세부적인 제시가 요구된다. 이외에도 스마트워크의 보안정책, 조직 · 인적 자산 보안, 침해사고 대응절차 등 주요 인증 항목에 대한 세부적인 제시가 필요하다.

4.1 스마트 장비의 인증 및 관리

스마트 장비인 모바일 단말기의 사용현황 관리 및 사용환경 제어가 가능해야 한다. 특히 단말기의 사용자와 실제 소유자가 동일인인지에 대한 확인이 이뤄져야 한다. 또 단말기 분실이나 도난이 회사 기밀의 분실 및 도난과도 같기 때문에 정보 유출 방지를 위한 암호화 기능도 제공되어야 하다. 이외에도 강력한 인증기능을 제공하기 위해 바이오 보안기술이 제공되어야 한다.

4.2 인프라 보안

안전한 스마트워크 인프라 환경을 위한 해킹대응, 유 · 무선 네트워크 보안, 물리적 보안 등 기술적 보호대책이 수립되어야 한다. 특히 가상사설망(VPN)과 같은 보안 접속을 통해 무선망에서의 데이터의 안전한 전송이 이루어져야 하며, 무선랜 보안, 모바일 악성코드에 대한 대처가 요구된다. 이외에도 네트워크 접근제어, 스마트워크 센터 내의 다양한 모바일 기기, 애플리케이션 등을 통제할 수 관제 서비스를 구축하여야 한다.

4.3 공용 PC 보안

스마트워크 센터 내에 있는 공용 PC 들의 저장장치, 이동식 저장매체 등에 대한 기술적 보호대책을 마련해서 안전하게 사용할 수 있어야 한다.

4.4 디지털저작권관리(DRM)

모바일 환경에서 문서보안 기능을 제공할 수 있는 디지털저작권관리 기능이 제공되어야 한다. 이러한 기능을 통해서 지리적으로 떨어진 다양한 스마트워크 센터에서도 안정적인 문서작업 및 업무 수행이 가능해야 한다. 또한 콘텐트 보호를 위한 관리적 보호대책이 제공되어야 한다.

4.5 사용자의 보안의식 제고

스마트워크의 사용자는 언제 어디서나 항상 보안에 노출되어 있다는 것을 인식하고, 모바일 기기의 비밀번호 설정, 주기적인 패치 및 안정성이 확인되지 않은 앱 프로그램의 미 설치 등의 기본적인 보안관리를 수행하여, 일반적인 해킹이나 공격에 안전하게 대처할 수 있어야 한다. 또한 정보자산의 적절한 보호를 위해 이용자가 점검 및 수행할 수 있는 수칙을 제공해서 이용자가 주도적으로 보안점검을 수행할 수 있도록 해야 한다.

4.6 스마트워크 임대사업자 인증체계 구축

스마트워크의 활성화를 위해서는 스마트워크 작업을 수행할 수 있는 다양한 스마트워크 센터가 구축되어야 하며, 스마트워크 센터의 신뢰성을 확보하기 위해서는 스마트워크 센터를 제공하는 임대사업자들을 인증할 수 있는 세부적인 절차와 점검 항목들이 제시되어야 한다.

4.7 침해사고 대응절차 수립

스마트워크 환경에서 발생 가능한 다양한 보안 침해사고에 대한 대응절차를 수립하여 보안 침해사고 발생 시 이용자가 신속하게 대처해야 할 사항을 안내할 수 있어야 한다.

5. 결론

스마트워크는 대용량의 무선 네트워크 인프라가 안정적으로 구축되고, 다양한 이동성이 확보된 스마트

장비들이 등장하면서 사회의 당면 문제인 저 출산·고령화, 낮은 노동 생산성 등의 현안을 해결하는 방안으로 급속하게 그 필요성이 대두되고 있다.

그러나 이동 환경에서 발생할 수 있는 다양한 보안 문제들이 발생할 수 있으며, 이에 대한 효율적인 대처 방안들이 마련되지 않으며 여러 가지 심각한 위험을 초래할 수 있다. 그러므로 본 논문에서는 스마트워크 환경에서 고려해야 할 보안 방안에 대해서 살펴보았으며, 제기된 보안 방안들을 효과적으로 대처함으로 안정적이고 효율성 있게 스마트워크를 사용할 수 있게 할 수 있다.

참고문헌

[1] 이재성, 김홍식, "스마트워크 현황과 활성화 방안 연구", 한국지역정보학회지 제 13 권 제 4 호 2010 년 12 월

[2] 김승호, “미국 연방정부 원격근무 실태와 확대 조치”, 주미한국대사관 보고서 2009 년.

[3] 일본 国道交通省, “기업을 위한 텔레워크 도입, 운용 가이드북”, 2009년.

[4] 한국정보화진흥원, “IT 기반 원격근무 재조명과 정책이슈”, 제 7 호, 2009 년.

[5] 이준호, “스마트 모바일의 발전과 정보보안”, 정보통신정책연구원 22(13), 2010 년

[6] 김승호, “미국 연방정부 원격근무 실태와 확대 조치”, 주미한국대사관 보고서, 2009 년.