http://dx.doi.org/10.14400/JDPM.2014.12.1.229

스마트워크 기반의 정보보호 감리 모형

한기준*, 김동수**, 김희완***
건국대학교 컴퓨터공학과*, 건국대학교 정보통신대학원**, 삼육대학교 컴퓨터학부***

An Audit Model for Information Protection in Smartwork

Ki-Joon Han*, Dong-Soo Kim, Hee-Wan Kim*****
Dept. of Computer Science and Engineering, Kunkuk University*
Graduate School of Information and Telecomunications, Konkuk University**
Division of Computer Engineering, Shamyook University***

요 약 스마트워크 기술은 재택근무나 스마트워크센터, 모바일 단말기 등을 활용하여 시간과 공간의 제약이 없는 유연한 근무 환경을 제공한다. 업무의 효율성을 높여주는 스마트워크 시스템에는 그 편리성만큼 여러 정보보호에 대한 위협이 존재한다. 따라서, 스마트워크 구축시에는 정보보호 대책을 적절하게 마련되도록 정보보호 감리를 수행하여야 한다. 본 논문에서는 스마트워크 환경 구축을 위해 실무·기술적 차원에서 정보보호 감리모형을 제안하였다. 정보 보호를 위해 터미널, 네트워크 및 서버 영역으로 분류하고, 전문 정보보호감리 점검항목을 도출하였다. 또한, 스마트워크 정보보호 감리시점을 수립하고 점검항목과 ISMS 통제분야를 매핑함으로써 보안성과 효율성을 동시에 향상시킬 수 있도록 감리모형을 제안하였다. 제안한 정보보호 감리영역 및 점검항목들이 스마트워크 정보보호 감리의 목적에 부합되는지를 검증하기 위해서 감리사 및 IT 업계 종사자를 대상으로 설문조사를 통하여 적합성을 검증하였으며, 13개의 점검항목에서 97% 수준으로 적합하다는 결론이 도출되었다.

주제어 : 스마트워크, 정보보호, 감리모형, 점검항목

Abstract Smartwork technology, using teleworking, smartwork centers and mobile terminal, provides a flexible work environments without constraints of time and space. Smartwork system to increase the work efficiency has the information protection threats according to their convenience. Thus, in order to build smartwork, it is proper to provide information protection audit to help ensure the information protection. In this paper, we have proposed an infortaion protection audit model at the practical and technical level for building a smartwork environment. We were classified as a terminal, network and server area for information protection, and derived a professional information protection check items. Further, by establishing a smartwork information protection audit time to map ISMS control items, we have proposed an audit model so that it is possible to improve the security and efficiency. It also verified whether the proposed model is suitable or not by doing a survey if deduced audit domain and check items correspond with the purpose of the smartwork information protection audit to auditors and IT specialists. As the result, this study was 97% satisfaction out of 13 check items.

Key Words : smartwork, information protection, audit model, check items

Received 22 November 2013, Revised 22 December 2013
Accepted 20 January 2014
Corresponding Author: Hee Wan Kim(Shamyook University)
Email: hwkim@syu.ac.kr

ISSN: 1738-1916

1. 서론

우리나라는 세계 최고 수준의 ICT(Information & Communication Technology) 인프라를 바탕으로 스마트워크가 급속히 활성화 되고 있다. 1995년부터 시작된 초고속정보통신망 구축사업을 통해 전국 기반의 광대역 네트워크 자산을 구축하여 스마트워크 이용 환경을 가장 효율적으로 구현할 수 있는 경쟁력을 가지고 있다. 또한, 스마트워크의 대표적인 단말인 스마트폰의 확산과 Wibro 등 융합형 서비스의 보급 및 클라우드 컴퓨팅 관련 기술의 발전도 스마트워크가 활성화 될 수 있는 환경을 제공하고 있다.

스마트워크 기술은 재택근무나 스마트워크센터, 모바일 단말기 등을 활용하여 원격 협업 환경을 구성하고 시간과 공간의 제약이 없는 유연한 근무 환경을 제공한다. 스마트워크 환경은 기존의 사내 IT인프라에 사외에서 스마트기기를 통해 원격으로 접속하여 업무를 수행할 수 있도록 제공하는 IT환경이다. 즉, 스마트워크 환경 구축은 기존 IT인프라에 대한 고도화 사업 특성을 갖으며 기존 데스크탑 PC환경의 보안 위협뿐 아니라 새로운 모바일 보안 위협이 발생될 수 있다. 업무의 효율성을 높여주는 스마트워크 시스템에는 그 편리성만큼 여러 보안 위협이 존재하며, 그에 대한 위험 분석 및 대책 구현이 필수적이다.

정보시스템감리는 안전하고 신뢰성 높은 정보시스템 구축 및 운영에 크게 기여해 왔다. 스마트워크 환경 구축 및 운영시에도 이에 적합한 정보시스템 감리모형을 정립하여 정보화 사업이 성공적으로 수행될 수 있도록 감리가 수행되어야 한다. 기업 및 기관이 통제할 수 없는 물리적 공간에서도 업무의 연속성을 보장하는 스마트워크 환경에서는 정보보호가 필수적으로 구현 및 관리되어야 한다. 따라서, 안전한 스마트워크 환경 구축을 위하여 활용할 수 있는 정보보호 감리 모형이 필요하다. 그러나, 기존의 정보시스템 감리에서는 정보보호 구현을 별도의 감리영역으로 구성하지 않고 있으며 스마트워크 환경에 특화된 정보보호 감리 프레임워크가 없다[7].

스마트워크 환경은 기존의 IT인프라를 사외에서 스마트기기를 활용하여 업무를 하기 위한 환경이다. 즉, 기존의 서버 및 네트워크에 대한 정보보호강화와 새로운 단말인 스마트워크 기기에 대한 점검 프로세스 및 점검항목의 도출이 필요하다.

따라서, 본 논문에서는 스마트워크와 정보보호 감리를 위하여 스마트워크 환경에 적합하게 정보보호 영역을 구분하고 정보보호 관리체계(ISMS : Information Security Management System, 이하 ISMS로 표기함)와 원활하게 융화가 될 수 있는 스마트워크 정보보호 감리모형을 제안하였다.

2. 관련 연구

2.1 스마트 워크

이동통신기술의 발달과 스마트기기 이용의 확산은 업무 환경에 큰 변화를 가져왔다. 고성능 연산장치와 기억장치가 내장된 스마트폰, 태블릿을 활용함으로써, 과거 사무실 안, 원격근무지 안 등으로 한정되어 있던 업무공간의 제한이 없어지고 언제 어디서가 효율적으로 업무를 처리하는 스마트워크가 가능해졌다[4].

스마트워크는 종래의 지정된 업무공간인 사무실의 개념을 탈피하여, 다양한 장소와 이동환경에서도 언제 어디서나 편리하게, 효율적으로 업무에 종사할 수 있도록 하는 미래지향적인 업무 환경을 의미한다[1]. 스마트워크를 통해 언제, 어느 장소에서나 사무실과 동일한 환경에서 업무를 지속할 수 있다[5].

스마트워크에 대한 관심과 이에 대한 활용이 커지고 있는 현 시점에서 스마트워크의 특징을 통하여 스마트워크에 대한 개념적 정의를 명확하게 할 필요가 있다.

스마트워크는 IT를 활용하여 시간과 장소에 구애받지 않고 언제 어디서나 일할 수 있는 선진화된 근무방식을 총칭한다. 이는 단순히 근무장소의 유연화만을 의미하지 않고, 일하는 방식 및 근무문화의 선진화까지 포함한다는 점에서 기존의 원격근무와 다르다[14].

스마트워크는 단순히 스마트폰과 같은 기기를 도입하여 사무환경을 바꾸어 근무함으로써 이루어지는 것이 아니다. 스마트워크는 단순히 원격근무를 의미하는 것이 아니라 원격 협업을 포함하는 개념이다. 정보통신의 발전과 함께 등장한 협업의 한 형태로서 근무자가 시간과 공간의 제약이 없이 언제, 어디에서든지 스마트워크를 수행할 수 있어 생산성을 더 높일 수 있다.

기업에서는 스마트기기를 이용하여 업무효율성을 높

이려는 시도가 증가하고 있다. PC기반에서 처리하던 주요업무가 스마트폰 등 모바일 기기로 확장되므로 기존 PC기반에서 발생 가능한 보안 위협이 스마트폰에서 재현될 수 있을 뿐 아니라, 가벼운 이동성으로 이한 분실 위험이 상대적으로 더 크다[3].

스마트워크는 이동통신 기술을 적극 활용함으로 업무처리시 공간의 제약을 받지 않는 반면에, 스마트기기의 보안 위협이 스마트워크의 보안위협으로 직결되는 문제를 안고 있다[4].

최근에는 스마트폰을 활용한 대국민 모바일 서비스의 개발·보급이 활발해지면서 국내 공공부문 모바일 웹·앱 정부 몰을 제공하는 국가대표포털(m.korea.go.kr), 다양한 민원을 스마트폰 기반으로 신청, 열람할 수 있는 모바일 민원 24, 생활법률정보, 일자리 정보, 지자체 관광, 홍보, 교통정보 등의 제공을 위한 서비스가 다양하게 제공되고 있으며 , 또한 업무보고, 직원조회, 게시판 활용 등 행정업무를 효율적으로 수행하기 위한 모바일 오피스 서비스도 시범적으로 운영되고 있다[14].

민간부분에서는 삼성그룹, 코오롱그룹, GS정유 등 주요기업에서 선도적으로 도입하여 전자결재, 이메일, 인정관리 ,게시판, 임직원 조회 등의 서비스를 제공하고 있으며 SKT, KT, 삼성SDS 등은 자사 내 도입뿐 아니라 기업 대상 모바일 오피스사업 영역을 확장 중에 있다[14].

2.2 정보보호 관리체계

정보보호라 함은 정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단을 강구하는 것을 말한다. 또한 전사적 정보보호를 정보보증(Information Assurance)으로 규정하고 기밀성·무결성·인증·부인봉쇄·가용성을 보장함으로써 정보와 정보시스템을 방어하고 보호하는 활동으로서 보호, 탐지 및 대응 능력을 통한 정보시스템의 복구를 포함하는 방어적 정보 작전으로 정의한다.

정보보호는 사용목적에 따라 다소 차이는 있으나 '정보화 역기능을 방지하기 위하여 정보 및 정보시스템을 보호하고, 정보의 비밀성·무결성·인증·부인봉쇄·가용성을 보장해 줄 수 있도록 관리적·물리적·기술적 수단을 강구하는 것'이라고 할 수 있으며 다음에 설명하는 보안에 비해 다소 포괄적인 개념을 갖고 있다고 할 수 있다[7].

ISO/IEC 27001:2005 에서는 정보보호(Information Security)를 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)과 확실성(Authenticity), 책임성(accountability), 부인방지(non-repudiation) 및 신뢰성(reliability)을 보존(Preservation)하는 것으로 정의하고 있다[11].

기업과 공공기관의 정보시스템 의존도가 커지고, 해킹, 악성코드 등 인터넷 침해가 증가하면서 고객이나 국민들에게 시스템이 안전하고 신회성이 있을을 알리는 활동이 중요한 문제로 대두되고 있다. 이와 관련하여 정보시스템과 정보자산이 안전하고 신뢰성 있게 관리체계 인증제도가 도입되어 운영되고 있다[9].

한국정보화진흥원에서는 정보보호 관리체계를 정보자산의 무결성, 비밀성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립, 문서화하고 지속적으로 관리, 운영하는 체계라고 정의하고 있다.

또한 "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제 47조 1항에서는 정보보호 관리체계를 "정보통신서비스 제공자가 정보통신망의 안전성 및 정보의 신뢰성을 확보하기 위하여 수립, 운영하고 있는 기술적, 물리적 보호조치를 포함한 종합적인 관리체계"로 정의를 내리고 있다.

ISO/IEC 27001에서는 정보보호 관리체계를 "전반적인 관리시스템의 일부로 비즈니스 위험 접근법을 기반으로 정보보호를 수립, 구현, 운영, 모니터, 검토, 유지 및 개선하기 위한 시스템"이라고 정의하고 있으며, 관리시스템에는 조직구조, 정책, 계획 활동, 책임, 실무 절차, 프로세스 및 자원이 포함된다고 명시하고 있다[9].

정보보호 관리체계(ISMS)는 비즈니스 위험 접근방법에 근거하여 정보보안을 수립, 구현, 운영, 모니터 검토, 유지 및 개선하기 위한 전체 경영관리체계 혹은 경영시스템의 일부로서, 문서화된 정보, 말해지는 및 컴퓨터 정보 등 모든 정보가 보안의 대상이 된다[7].

보보호 관리체계 인증제도를 통하여 일회적이던 조직의 정보보호활동을 체계적이고 지속적인 관리가 가능하게 함으로써 전사적으로 균형 잡힌 정보보호활동을 할 수 있게 된다. 특히 기업의 정보보호관리에 대한 표준적 모델 및 기준을 제시하여 기업의 정보보호 관리체계 구축·운영을 촉진하고 정보보호활동에 대한 프로세스 개선을 통하여 동시에 기업의 주요 정보자산 유출 및 피해를 사전에 예방하고 대처할 수 있도록 하는 데 목적이 있다

고 할 수 있다[8].

대표적인 정보보호 관리체계 인증제도로는 ISO가 운영하는 ISO/IEC27000[17] 이 있다. 또한 국내에서는 2001년 도입된 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 제 47조에 의한 정보보호 관리체계 인증제도(방송통신위원회 KCC ISMS[10])가 운영되고 있다. 본 논문에서는 KCC ISMS를 보다 범용적인 명칭인 KISA ISMS를 사용하였다. 미국은 FISMA(Fedral Information Security Management Act)법에 의한 FIPS(Fedral Information Processing Standards) 199, FIPS 200제도[15][16]를 운영하고 있다[9].

2.3 스마트워크 정보보호 감리의 필요성

스마트워크를 통해 근무 위치와 무관하게 원격 협업 환경을 구성하고 보다 유연한 근무 환경 기반 형성이 가능하여 업무 효율성 향상 등 많은 이점을 기대할 수 있다. 이에 행정안전부에서는 2010년 11월 스마트워크 센터 1호를 개설하고 정부의 각 부처나 자치단체는 물론 공공기관 및 민간기업의 직원도 이용 가능한 공간을 국내 최초로 구축하였다. 또한 2015년까지 스마트워크 센터를 50개까지 증설하고 스마트워크 센터 시설기준 및 운영방법과 스마트워크 확산을 위한 법·제도적 기반을 제정하는 등 공공 및 민간 기업의 스마트워크 센터의 구축 및 운영을 지원하는 국내 스마트워크 환경 구축에 앞장서고 있다[13].

스마트워크를 도입하는 기업 및 기관은 이를 통해 신속한 의사결정 및 생산성 향상 효과를 기대하며 사업을 추진한다. 그러나, 스마트워크 단말 및 물리적 공간 위협에 따른 단말기 도난, 분실, 해킹 등으로 인한 기밀 정보 유출에 대한 우려로 인하여 스마트워크 확산에 걸림돌이 되고 있다.

스마트워크 환경에는 기존의 보안 위협과 모바일 요인 등에 의한 보안 위협이 추가적으로 존재한다. 따라서, 안전한 스마트워크 환경을 구축하기 위해서 신뢰성이 높고 체계적인 위험관리를 통해 위험을 분석 및 평가하여 적절한 정보보호 대책을 마련하였는지 점검할 수 있는 정보보호 감리 제도가 필요하다.

2.3.1 정보보호관리체계(ISMS)와 정보보호 감리

정보보호 감리는 일회성을 갖는 프로젝트로서 위험관리 프로세스에 따라 위험을 적절히 분석 및 평가하고 이를 수용 가능한 수준으로 감소시킬 수 있는 비용대비 효과적인 정보보호 대책을 구현하도록 점검한다.

반면, 정보보호관리체계는 기업 및 기관의 정보보호 수준을 일정하게 유지하기 위한 지속적인 정보보호 활동으로 프로젝트가 아닌 순환주기를 갖고 있는 프로그램이다. 정보보호관리체계는 전사적으로 균형잡힌 정보보호 활동을 할 수 있게 해주며 기업의 정보보호관리에 대한 표준적 모델 및 기준을 제시하고 있다[8]. 국내외 표준 정보보호관리체계는 위험관리를 기반으로 수립 및 관리되며 신뢰성이 높다. 정보보호관체계는 위험을 평가하고 그 결과에 따라 통제항목을 선정하여 관리한다.

스마트워크 환경은 기존에 사내에서 사용하던 조직의 IT인프라를 사외에서 스마트폰 등의 단말기를 통해 원격으로 접속하여 사용할 수 있도록 지원하는 업무 환경이다. 정보보호관리체계를 관리하고 있는 조직에서 스마트워크 정보시스템을 신규로 구축할 경우, 운영 단계에서 정보보호관리체계의 다음 순환주기에 신규 정보시스템에 대한 위험을 평가하고 통제사항을 선정하여 기존 시스템과 함께 관리된다.

안전한 스마트워크 환경 구축을 구축하고 지속적으로 스마트워크 환경의 정보보호 수준을 유지하기 위해서는 위험관리를 기반으로 정보보호 감리를 수행하고 정보보호 관리체계를 수립 및 관리하여야 한다. 이 두 제도에서 수행하는 위험관리 프로세스는 상호보완적인 관계이다. 정보보호감리와 정보보호체계에서 수행한 위험관리 산출물은 각각의 투입물로 활용될 수 있으므로 동일한 위험관리 표준을 적용하는 것이 훨씬 효율적이다.

또한, 정보보호관리체계의 통제분야 및 항목과 정보보호 감리 점검항목을 매핑하여 정보보호 구현 적합여부를 점검한다면 시스템 구축 후 운영단계에서 전사적 정보보호 관리체계(ISMS) 다음 순환주기에 용이하게 신규 시스템이 융화 될 수 있어 정보보호관리체계 관리시 시간과 노력을 절약 할 수 있어 효율적이다.

따라서, 신규 보안위협이 계속 발생되고 정보보호가 프로젝트의 성패를 좌우하는 스마트워크 환경 구축 프로젝트의 경우에는 ISO27001 및 KISA ISMS와 같은 신뢰성 높은 정보보호관리체계 표준의 관리과정 프로세스에 따라 일회적으로 위험관리를 수행하여 정보보호를 구현하고, 운영단계에서부터 정보보호관리체계 순환주기에

따라 정보보호 수준을 지속적으로 유지함으로써 보안성과 효율성을 모두 향상시킬 수 있다.

2.3.2 스마트워크 정보보호 감리 프레임워크

현재의 정보시스템 감리 프레임워크로는 스마트워크 구축시 정보보호 적합성 여부를 판단하기에 미흡하며, 이지용이 제시한 “정보보호아키텍처에 근거한 정보보호 감리모형”은 전사적 정보보호 계획 및 체계를 중심으로 정보보호 활동의 전체 과정을 수용하는 프레임워크로서 전사적 정보보호 정책 및 체계를 수립 및 관리하지 못하고 있는 기업 및 기관이 급변하는 IT환경에 맞춰 스마트워크 구축을 할 경우 적용하기에 어려움이 따른다.

정보보호 관리체계는 조직의 정보보호 수준을 지속적으로 유지시킬 수 있는 이상적인 프로그램이나 최초 수립시 시간과 예산이 많이 소요되어 아직 국내에서 ISMS 인증을 받은 기관이나 기업이 많지 않다. 국내에서는 신뢰도가 높고 널리 알려진 ISO/IEC 27001과 KISA ISMS 인증을 획득한 기관이나 기업의 수는 현재 225개로 매우 적다. 따라서, 전사적 정보보호 관리체계가 부재한 조직에서도 안전한 스마트워크 환경을 구축할 수 있도록 별도의 정보보호감리 프레임워크가 필요하다.

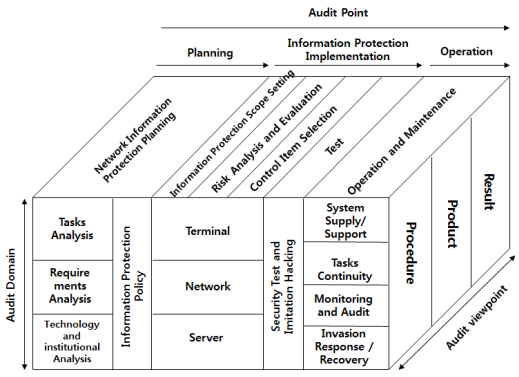
스마트워크 환경은 기존의 IT인프라를 사외에서 스마트기기를 활용하여 업무를 하기 위한 환경이다. 즉, 기존의 서버 및 네트워크에 대한 정보보호강화와 새로운 단말인 스마트워크 기기에 대한 점검 프로세스 및 점검항목의 도출이 필요하다.

따라서, 전사적 관점에서 위험을 분석하는 것도 중요하지만 직관적으로 정보보호감리 영역을 단말, 서버, 네트워크 영역으로 구분하여 각각에 대한 위험을 분석 및 평가하고 적절하게 대책을 마련했는지 점검할 수 있는 스마트워크 정보보호 감리 프레임워크를 정립해야 한다.

3. 스마트워크 정보보호 감리 모형

3.1 정보보호 감리 프레임워크

정보시스템 감리지침에서의 감리점검 프레임워크는 감리영역과 사업유형 및 감리시점 그리고 감리관점/점검기준의 세 축으로 구성되어 있으며, 스마트워크 정보보호 감리 프레임워크는 [Fig. 1]과 같다[6].



[Fig. 1] Information Protection Audit Model for Smartwork[7]

사업유형은 크게 스마트워크 계획수립, 스마트워크 시스템 정보보호 구현 및 운영/유지보수로 구분하였다. 스마트워크 시스템 정보보호 구현은 단말, 네트워크 서버 감리영역별로 정보보호 범위 설정, 위험 분석 및 평가, 통제사항을 선택 및 구현, 시험 시점으로 세분화하여 위험관리에 기반하여 정보보호를 구현할 수 있도록 감리모형을 설계하였다.

감리영역은 감리기준 제8조 제1항 제4호에서 제시하고 있는 평가를 작성하는 표준화된 단위(영역)를 사업유형별, 감리시점별로 구분하여 감리영역으로 규정함으로써 감리의 일관성을 확보할 수 있도록 하였다.

감리관점/점검기준은 감리가 대상사업을 바라보는 관점이다. 즉, 감리는 사업을 기반으로, 대상 사업에 대한 방법론, 사업추진계획, 절차 등 사업에 대한 절차와 그 결과로 생성되는 산출물을 점검/평가하고, 결론적으로 대상 사업이 당초에 목적했던 성과 또는 기대효과를 달성할 수 있도록 하는 역할을 한다.

감리관점별 점검기준은 감리를 시행할 때 감리관점별 점검하는 기준으로, 각 관점의 특성, 또는 품질기준으로 볼 수 있다[5].

3.2 위험분석 및 평가 단계의 감리점검항목

정보보호를 구현하기 위해서는 위험분석 및 평가가 선행 되어야 한다. 감리영역별로 정보보호의 범위를 설정한 후 각 영역별 취약성 및 위협을 분석하여 위험을 평가하는 단계이다.

위험분석단계에서는 식별된 정보자산에 영향을 줄 수

있는 모든 위협과 취약성, 위협을 식별하고 분류해야하며, 이 정보자산의 가치와 위험을 고려하여 잠재적 손실에 대한 영향을 식별·분석해야 한다. 위험평가단계에서는 이미 파악되었거나 잠재적인 위협과 취약성으로 인해 입을 수 있는 피해와 현재 구현된 정보보호 대책의 실패 가능성 및 영향을 평가한다.

스마트워크 환경은 기존 업무환경의 위험요소를 모두 다 갖고 있는 상태에서 모바일 단말 사용 및 근무위치 등에 따른 추가적인 보안 위협에 노출되어 있다. 따라서, 스마트워크 환경 구축 프로젝트에 있어서 위험을 분석하고 평가하는 단계는 매우 중요하다.

위험분석 및 평가 단계에서는 감리영역별로 위험을 분석 및 평가하였다. 보안위협의 종류는 스마트워크의 유형, 업무의 특성, 위치 등에 따라 상이하다. 위협의 종류는 무수히 많지만 스마트워크 정보보호 감리 수행시 참고가 될 수 있도록 대표적인 몇 가지 위험에 대한 분석을 점검항목으로 반영하였다.

3.2.1 단말

단말에서의 감리점검항목들은 스마트워크 유형에 따라 물리적 공간에 의한 단말의 위험에 대한 분석 및 평가 여부, 원격 접근에 따른 위험 분석, 단말기 도난 및 분실에 따른 위험 분석, 단말기 소유주가 악의적으로 업무자료를 외부로 유출할 경우의 위험 분석 및 평가를 점검항목으로 도출하였다. 또한, 위치추적(GPS)의 취약점에 따른 위험 분석, 스마트워크 단말의 이동저장 매체화에 따른 자료유출로 안한 위험, 화면 캡처에 대한 보안 위협 등을 위험분석 및 평가단계의 감리점검 항목으로 도출하였다.

3.2.2 네트워크

네트워크에서의 감리점검 항목들은 스마트워크 유형에 따른 네트워크 위험에 대한 분석 및 평가, 비인가 네트워크 송수신에 대한 위험 분석, 도청에 의한 위험 분석, 무선구간에서의 해킹에 대한 위험과 DDoS 등 유해 트래픽에 따른 위험분석 및 평가 등을 위험분석 및 평가단계의 감리점검 항목으로 도출하였다.

〈Table 1〉 Terminal Audit Check Items in Risk Analysis and Evaluation Phase

Check Items	References
Did you analysis and evaluate the risk of terminal by the physical space according to the type of smartwork ?	[1]
Did you analysis and evaluate the risk by remote access ?	[3][12]
Did you analysis and evaluate the risk by the terminal theft ?	[1][2][3] [12]
Did you analysis and evaluate the risk by Malware infections ?	[1][2] [3][12]
Did you analysis and evaluate the risk when terminal owner maliciously leaked out the data ?	[1][2]
Did you analysis the firmware vulnerability ?	[1][2][3]
Did you analysis and evaluate the vulnerability of Internet browser ?	[3]
Did you analysis and evaluate the vulnerability of GPS ?	[3][4]
Did you analysis and evaluate the vulnerability of authentication bypass ?	[3]
Did you analysis and evaluate the rsik of data leakage by the smartwork terminal ?	[1][2][4]
Did you analysis and evaluate the security vulnerability of screen capture ?	[1][2][4]

〈Table 2〉 Network Audit Check Items in Risk Analysis and Evaluation Phase

Check Items	References
Did you analysis and evaluate the network risk by the type of smartwork ?	[1]
Did you analysis and evaluate the network risk by receiving unauthorized network ?	[3][4]
Did you analysis the risk of the wiretapping ?	[1][2][3]
Did you analysis and evaluate the risk of electric wave ?	[3]
Did you analysis and evaluate the network risk by the hacking of the wireless link ?	[1][4][10]
Did you analysis and evaluate the risk of Rogue AP ?	[3][4]
Did you analysis and evaluate the risk of DDoS ?	[1][2][3]

3.2.3 서버

서버에서의 감리점검 항목들은 스마트워크 유형에 따른 서버 위험 분석, 원격 접근에 따른 위험 분석 및 평가, 악성코드 감염에 따른 보안 위험 분석, 서버 운영체제의 취약점 분석, 서버 어플리케이션의 취약점 분석과 악성 어플리케이션 업로드 및 배포에 대한 위험분석 등을 위험분석 및 평가단계의 감리점검 항목으로 도출하였다.

〈Table 3〉 Server Audit Check Items in Risk Analysis and Evaluation Phase

Check Items	References
Did you analysis and evaluate the server risk by the type of smartwork ?	[1]
Did you analysis and evaluate the risk by remote access ?	[12]
Did you analysis and evaluate the risk by Malware infections ?	[3][12]
Did you analysis and evaluate the risk of server OS ?	[3]
Did you analysis and evaluate the vulnerability of server application ?	[3]
Did you analysis the risk of malignant application upload and deployment ?	[3]

3.3 통제사항 선택 및 구현 단계의 감리점검 항목

위험분석 및 평가단계에서 도출된 감리점검 항목들을 바탕으로 통제사항을 선택하여 구현하는 단계이다. 위험을 수용 가능한 수준으로 통제하기 위한 항목들을 선택하여 구현한다. 통제사항 선택 및 구현은 기업 및 기관에서 수립하여 관리하고 있거나 향후 수립할 정보보호 관리체계(ISMS)에 용이하게 반영 및 적용하여 될 수 있도록 검점항목과 통제항목을 매핑하여 도출하였다.

3.3.1 단말

통제사항 선택 및 구현 단계의 단말에서의 감리점검 항목으로는 단말 분실·도난 대책, 악성코드 대책, 단말 인증 대책, 사용자 인증 대책, 원격제어 대책, 플랫폼 보안 대책, 앱 보안 대책과 콘텐츠 보안 대책 등이 적정하게 선택 및 구현되었는지를 점검항목으로 도출하였다.

〈Table 4〉 Terminal Audit Check Items in Control Items Selection and Implementation Phase[4]

Check Items	ISMS Control Items
Did you select and implement the counterproposal of the lost terminal properly ?	A.9 Physical / Environmental Security
Did you select and implement the counterproposal of the malware properly ?	A.10 Communication /Operations Management
Did you select and implement the counterproposal of the terminal certification properly ?	A.11 Access Control
Did you select and implement the counterproposal of the user certification properly ?	
Did you select and implement the counterproposal of the remote control properly ?	
Did you select and implement the counterproposal of the flatform security properly ?	A.12 Information Systems Development/ Maintenance
Did you select and implement the counterproposal of the app security properly ?	
Did you select and implement the counterproposal of the contents security properly ?	

3.3.2 네트워크

통제사항 선택 및 구현 단계의 네트워크에서의 감리점검 항목으로는 무선랜 연결 대책, 통신망 암호화 대책과 침입차단 및 방지 대책이 적정하게 선택 및 구현되었는지를 점검항목으로 도출하였다.

〈Table 5〉 Network Audit Check Items in Control Items Selection and Implementation Phase[4]

Check Items	ISMS Control Items
Did you select and implement the counterproposal of the wireless LAN connection properly ?	A.10 Communication /Operations Management A.11 Access Control
Did you select and implement the counterproposal of the network encryption properly ?	
Did you select and implement the counterproposal of the intrusion prevention properly ?	

3.3.3 서버

통제사항 선택 및 구현 단계의 서버에서의 감리점검 항목으로는 보안 관제 대책과 서버보안이 적정하게 선택 및 구현되었는지를 점검항목으로 도출하였다.

〈Table 6〉 Server Audit Check Items in Control Items Selection and Implementation Phase[4]

Check Items	ISMS Control Items
Did you select and implement the counterproposal of the security management properly ?	A.10 Communication /Operations Management
Did you select and implement the counterproposal of the server security properly ?	A.12 Information Systems Development/ Maintenance

Ⅳ. 제안의 검증

본 논문에서 안전한 스마트워크 환경 구축을 위한 정보보호 감리영역, 감리시점, 감리점검항목 등에 대하여 그 필요성 및 실효성을 검증하기 위하여 감리사 및 IT 업계 종사자를 대상으로 설문하는 방법을 사용하였다.

본 연구에서 50 여명의 감리사 및 IT 종사자들에게 설문을 요청하였으며, 최종 30명에게 응답을 받아 분석하였다.

4.1 감리점검사항에 관한 설문 대상

설문조사의 대상은 <표 5-1> 과 같이 선정하였으며, 감리사(43.3%), 개발자(10%), 네트워크관리자(10%), 서버관리자(23.3%), 보안관리자(13.3%)로 구성되어 있다.

〈Table 7〉 Results of a Survey on Understanding Characteristics of the Surveyers

Category	Auditors	Developers	Network managers	Server managers	Security managers	Total
Numbers	13	3	3	7	4	30
Percent	43.3	10	10	23.3	13.3	100

4.2 스마트워크 정보보호 감리점검항목에 관한 설문 결과

스마트워크 정보보호 감리점검항목에 대한 설문은 4장에서 제안한 안전한 스마트워크 환경 구축을 위한 정보보호 통제사항 선택 및 구현 단계의 점검항목을 나열하여 각 항목마다 매우필요(5점), 필요(4점), 보통(3점), 필요없다(2점), 전혀 필요없다(1점)의 값으로 표기하도록 하였다. 설문 결과에 따른 항목 적합성 검증은 보통(3)을 기준으로 “매우필요・필요”는 적합으로, “필요없다・전혀 필요없다”는 부적합 의견으로 검증하였다. 이는 적합의 정도를 표로 나타낼 때, 보통을 기준으로 3단계로 간결하게 표현하지만, 실제적으로 평균과 표준편차는 설문에 응답한 값으로 표시하였다.

4.2.1 단말영역 정보보호 통제사항 선택 및 구현 점검항목

단말영역 정보보호 점검항목에서 단말 분실·도난 대책의 적정성에서 27명, 원격제어 대책이 적정하게 선택 및 구현성에서 26명, 콘텐츠 보안 대책의 적정성에서 29명이 적합하다고 응답하였다. 나머지 모든 점검항목에서는 30명 모두 적합하다고 응답하여 전체 평균 적합하다고 응답한 응답율은 97%로 나타났다.

〈Table 8〉 Results of Terminal Audit Check Items

Check Items	Appropriate	middle-ground	Inappropriate	Average	Standard Deviation
Did you select and implement the counterproposal of the lost terminal properly ?	27	3	0	4.20	0.51
Did you select and implement the counterproposal of the malware properly ?	30	0	0	4.40	0.38
Did you select and implement the counterproposal of the terminal certification properly ?	30	0	0	4.63	0.29
Did you select and implement the counterproposal of the user certification properly ?	30	0	0	4.50	0.35
Did you select and implement the counterproposal of the flatform security properly ?	26	4	0	4.10	0.54
Did you select and implement the counterproposal of the flatform security properly ?	30	0	0	4.43	0.37
Did you select and implement the counterproposal of the app security properly ?	30	0	0	4.47	0.36
Did you select and implement the counterproposal of the contents security properly ?	29	1	0	4.50	0.38
Average response rates of the check items	29 97%	1 3%	0 0%	4.40	0.41

<Sampling Error ±0.41%P(95%Confidence Level)>

4.2.2 네트워크 영역 정보보호 통제사항 선택 및 구현 점검항목

네트워크 영역 정보보호 점검항목에서 무선랜 연결 대책이 적정하게 선택 및 구현성에서 29명, 통신망 암호화 대책의 적정성에서 29명, 침입차단 및 방지 대책의 적정성에서 30명이 적합하다고 응답하였다. 점검항목 3가지 전체 평균 적합하다고 응답한 응답율도 단말영역과 같이 97%로 나타났다.

〈Table 9〉 Results of Network Audit Check Items

Check Items	Appropriate	middle-ground	Inappropriate	Average	Standard Deviation
Did you select and implement the counterproposal of the wireless LAN connection properly ?	28	2	0	4.37	0.45
Did you select and implement the counterproposal of the network encryption properly ?	29	1	0	4.47	0.39
Did you select and implement the counterproposal of the intrusion prevention properly ?	30	0	0	4.57	0.33
Average response rates of the check items	29	1	0	4.47	0.39
	97%	3%	0%		

<Sampling Error ±0.39%P(95%Confidence Level)>

4.2.3 서버영역 정보보호 통제사항 선택 및 구현 점검항목

서버 영역 정보보호 점검항목에서 보안 관제 대책의 선택 및 구현의 적정성에는 28명, 서버보안의 선택 및 구현의 적정성에서는 30명이 적합하다고 응답하였다. 전체 평균 적합하다고 응답한 응답율은 97%로 나타났다.

〈Table 10〉 Results of Server Audit Check Items

Check Items	Appropriate	middle-ground	Inappropriate	Average	Standard Deviation
Did you select and implement the counterproposal of the security management properly ?	28	2	0	4.40	0.44
Did you select and implement the counterproposal of the server security properly ?	30	0	0	4.63	0.29
Average response rates of the check items	29	1	0	4.52	0.37
	97%	3%	0%		

<Sampling Error ±0.37%P(95%Confidence Level)>

4.3 스마트워크 정보보호 감리의 필요성 및 실효성에 대한 검증

스마트워크 환경 구축을 위한 정보보호 감리의 필요성과 실효성에 대한 설문 결과, 스마트워크 정보보호 감리영역 분류의 적정성에서는 93%의 필요성을 보였으며, 보안성 향상에서도 93%의 효과있음으로 응답하였다. 나머지 스마트워크 정보보호 감리의 필요성, 감리시점의 적정성과 이를 통한 ISMS 관리에 기여 정도의 설문에는 100%의 필요함으로 응답하였다. 모든 항목에서 93% ~ 100% 수준으로 “필요함” 및 “있음”으로 응답하였다.

〈Table 11〉 Results of a Survey on Necessity in Smartwork Information Protection Audit

Category	Necessary	Unnecessary
Necessary of smartwork information protection audit	100%	0%
Appropriateness of smartwork information protection audit domain	93	7%
Appropriateness of smartwork audit time/point	100%	0%
Improvement of Security	93%	7%
Contribution of ISMS managements	100%	0%

4.4 스마트워크 정보보호 감리 점검항목의 적합성에 대한 검증

통제사항 선택 및 구현 단계의 13개 감리항목에 대한 설문 결과, 97% 수준으로 모든 항목에 대하여 “적합”하다고 응답을 하였다. 따라서, 13개 점검항목을 통제사항 선택 및 구현의 적합/부적합 여부를 판단하는데 활용 가능할 것으로 사료된다.

〈Table 12〉 Total Results of Appropriateness in Check Items for Smartwork

Audit Fields	Check Items	Appropriate	Middle-Ground	Inappropriate	remarks
Terminal	8	97%	3%	0%	Appropriate
Network	3	97%	3%	0%	Appropriate
Server	2	97%	3%	0%	Appropriate

V. 결론 및 향후 연구 과제

최근 무선인터넷의 활용증가와 스마트폰, 태블릿PC등

모바일 기기의 폭발적인 확산 등으로 정보화 환경이 급변하고 있으며, 정부는 업무 생산성의 향상, 저출산·고령화 대비, 저탄소 녹색성장 등 국가 사회현안의 해결을 위한 방안의 일환으로 스마트워크 활성화를 추진하고 있다.

스마트워크 환경은 기존 PC환경의 보안 위협 뿐 만 아니라, 급변하는 모바일 네트워크 등 IT기술을 기반으로 발전하고 있어 그에 따른 신규 보안 위협이 계속적으로 발생되고 있다. 따라서, 안전한 스마트워크 환경을 구축하기 위해서는 위험을 분석 및 평가하여 적절한 정보보호 대책을 마련하는 위험관리를 필수적으로 수행해야 되며, 운영단계에서도 지속적인 위험관리를 통해 새로운 위험에 대해 적절한 통제를 마련하여 안전한 스마트워크 정보보호 수준을 유지시킬 수 있어야 한다.

따라서, 스마트워크 환경 구축시에는 신뢰성 있고 국내외 위험관리 표준 절차에 따라 위험을 분석 및 평가하여 정보보호 대책을 적절하게 마련하도록 점검 및 문제점을 개선토록 정보보호 감리를 수행하여야 하며 스마트워크 환경 운영시에도 지속적인 위험관리를 통해 정보보호 수준을 유지할 수 있도록 정보보호관리체계(ISMS)를 수립 및 관리해야 한다.

따라서, 본 논문에서는 전사적 정보보호 계획 및 체계가 구축되어 있지 않은 조직에서도 신뢰성 있는 표준 위험관리 절차에 따라 안전한 스마트워크를 구축하고, 기존 관리 중이거나 향후 수립할 ISMS와도 유기적으로 연동되어 안전하고 효율적으로 정보보호 수준을 유지할 수 있도록 하는 스마트워크 정보보호 감리 모형을 정립하였다.

본 논문에서 제시한 안전한 스마트워크 환경 구축을 위한 정보보호감리 모형은 실무·기술적 차원에서 정보보호를 전문적으로 구현할 수 있도록 스마트워크 정보보호를 단말, 네트워크, 서버 보안 영역으로 분류하고 각각에 대한 전문적이고 세부적으로 정보보호 항목을 도출하였다. 또한, ISMS를 통해 지속적으로 정보보호 수준이 유지될 수 있도록 점검항목과 ISMS 통제분야를 매핑함으로써 보안성과 효율성을 동시에 향상시킬 수 있도록 설계하였다.

스마트워크 정보보호 감리 모형을 통해 모바일 등 급변하는 IT기술의 보안위협으로부터 스마트워크 IT인프라 및 정보자산을 안전하고 효율적으로 보호할 수 있는 스마트워크 환경을 구축할 수 있기를 기대한다.

본 연구에서는 실제 스마트워크 환경 구축 사업에 적용하여 효과성을 검증하지 못한 한계는 지니고 있다. 따라서 실제적인 스마트워크 정보보호 감리에 적용해 나가면서 수정·보완하여 안전한 스마트워크 환경 구축을 위한 정보보호 감리모형으로 자리 잡을 수 있도록 추가적인 연구가 필요하며, 적합성 검증을 위한 데이터의 신뢰성과 타당성에 대한 실증이 요구되는 한계를 가지고 있다.

REFERENCES

[1] Korea Communications Commission, introduction, operation guidebook of smartwork for enterprise, Korea Communications Commission, 2011

[2] National Information Society Agency, CIO Report 26 Smart phones and mobile office security issues and response strategies, National Information Society Agency, 2010

[3] Hae Soo Hwang, Ki Hyuk Lee, A study on the mobile security model for secure smartwork, Review of KIISC 21(3), pp.22-34, 2011

[4] Hyung Chan Lee, Jung Hyun Lee, Ki Wook Son, Smartwork security threats and countermeasures, Review of KIISC 21(3), pp.12-21, 2011

[5] Ho Sun Yun, Sung Back Hong, Hyung Yul Yum, In Jae Kim, Mobile VPN structure suitable for smartwork environments, Journal of Advanced Information Technology and Convergence(JAITC) 9(5), pp.159-166, 2011

[6] National Information Society Agency, u-Work Service Activation Support Project, National Information Society Agency, 2007

[7] Ji Yong Lee, Dong Soo Kim, Hee Wan Kim, A design of the information security auditing framework of the information system audit, Korea society of digital industry and information management 6(2), pp.233-245, 2010.

[8] Dong Soo Kim, Nam Jae Jun, Hee Wan Kim, Design of financial information security model based on enterprise information security architecture, Korea society of digital industry and information management 6(4), pp.307-317, 2010.

[9] Ho Ik Jang, Ho Hyun Han, Nam Yong Lee, Jang Hee Jo, A study on the selection model of information protection management system control items, The journal of korea information and communications society 35(8), pp. 195-204, 2010

[10] Korea Communications Commission Notice 2010-3, Notice regarding information security management system certification, Korea Communications Commission, 2010

[11] Hee Myung Lee, Jong In Lim, A study on the development of corporate information security level assessment models, Review of KIISC 18(5), pp.161-170, 2008

[12] Myeong Soo Jeong, Dong Bum Lee, Jin Kwak, An analysis of smartwork security threats and security requirements, Korea institute of information security and cryptology 21(3), pp.55-63, 2011

[13] Ministry of Security and Public Administration, Smartwork promotion plan, Ministry of Security and Public Administration, 2010

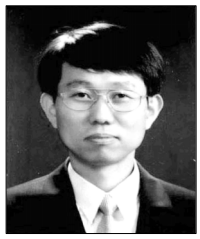
[14] National Information Society Agency, National Information white papers, National Information Society Agency, 2011

[15] FIPS PUB 199, 「Standards for Security Categorization of Federal Information and Information Systems」, NIST, 2006.

[16] FIPS PUB 200, 「Minimum Security Requirements for Federal Information Systems and Organizations」, NIST, 2006.

[17] ISO/IEC 27000, 「Information technology -Security techniques - Information security management systems - Overview and Vocabulary」, ISO, 2009.

김 희 완(Kim, Hee Wan)



- 1995년 8월 : 성균관대학교 정보공학과(공학석사)
- 2002년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
- 1996년 5월 : 정보관리기술사 취득
- 2007년 1월 : 정보시스템 수석감리원 자격 취득
- 2001년 3월 ~ 현재 : 삼육대학교 컴퓨터학부 교수
- 관심분야 : 정보시스템 감리, 프로젝트 관리, 데이터베이스, 소프트웨어 공학
- E-Mail : hwkim@syu.ac.kr

김 동 수(Kim, Dong Soo)

- 1981년 2월 : 광운대학교 전자계산학과(이학사)
- 2001년 2월 : 서울산업대학교 전자계산학과(공학석사)
- 2005년 2월 : 국민대학교 경영정보학과(경영학박사)
- 1991년 12월 전자계산조직응용기술사 취득
- 1995년 8월 정보통신기술사 취득
- 1998년 2월 ~ 현재 : (주)키삭 대표컨설턴트
- 2008년 3월 ~ 현재 : 건국대학교 정보통신대학원 겸임교수
- 관심분야 : u_city 감리, 프로젝트 관리, 정보시스템 감리, 소프트웨어 공학
- E-Mail : dskim@kisac.co.kr

한 기 준(Han, Ki Joon)

- 1979년 2월 : 서울대학교 수학교육학과(이학사)
- 1981년 2월 : KAIST 전산학과(공학석사)
- 1985년 2월 : KAIST 전산학과(공학박사)
- 1990년 1월 ~ 1991년 1월 : Stanford 대학 전산학과 Visiting Scholor
- 1985년 3월 ~ 현재 : 건국대학교 컴퓨터공학부 교수
- 관심분야 : 데이터베이스, GIS, LBS, 텔레매틱스, 정보시스템 감리 등
- E-Mail : kjhan@db.konkuk.ac.kr