스마트워크 서비스에서 정보보호를 위한 취약성 대응 방안

김지석*, 김동수**, 김희완***

목 차

요약

스마트워크는 스마트기기를 활용하여 업무의 효율성을 높이는 것을 말한다. 스마트워크는 기업들의 업무 생산성을 향상시키고, 비용을 절감하여 업무효율성은 향상되지만, 이에 따른 다양한 정보보호에 대한 위협이 존재한다. 재택근무, 모바일 오피스, 스마트워크 센타 등을 운영하기 위해서는 다양한 네트워크 자원, 서버, 플렛폼을 지원하는 하드웨어와 소프트웨어가 필요하다. 이에 따라 정보자원을 보호하는 보안 및 정보보호에 대한 취약점이 많이 발생한다.

본 논문에서는 스마트워크 서비스를 위하여 스마트워크 환경을 분석하고 정보보호관련 기준인 IOS27001 및 KISA-ISMS의 분석을 통하여 스마트워크 정보보호를 위한 취약점을 분석하였다. 정보보호 요구사항에 대하여 사용자 및 서비스 제공자 입장에서의 요구사항을 도출하였으며, 스마트워크 보안 위협 및 취약점에 대하여 공통부분, 모바일 오피스, 재택근무, 스마트워크 센터 등으로 나누어 취약점에 대한 대응방안을 제시하였다.

표제어: 스마트워크, 정보보호, 취약점, 정보보호 요구사항, 정보보호 대응방안

접수일(2017년 10월 31일), 수정일(1차: 2017년 11월 30일), 게재확정일(2017년 12월 22일)
* 제 1저자, ㈜사이버원 컨설턴트, hulpei@hanmail.net
** 건국대학교 정보통신대학원 초빙교수, dskim@kisac.co.kr
*** 교신저자, 삼육대학교 컴퓨터메카트로닉스공학부 교수, hwkim@syu.ac.kr

1. 서론

정보통신기술의 발달과 더불어 스마트 폰의 사용이 늘어나면서 스마트워크를 활용한 업무처리 요구가 증가하고 있다. 스마트워크는 시공을 초월하여 근무자가 편리하게 업무를 수행하도록 하며, 스마트 기기를 활용하여 협업을 함으로써 업무의 효율성을 높이는 것을 말한다. 이러한 스마트워크를 활성화하기 위해서는 기존 사무실 환경을 뛰어넘는 스마트워크 서비스 환경을 제공하고, 모든 정보를 사이버 공간에서 통합적으로 안전하게 관리하고 공유하고, 사용자의 손쉬운 워크플로우 설계를 기반으로 하는 업무 환경의 변화가 필요하다. 스마트워크는 기업들의 업무 생산성을 향상시키고, 비용을 절감하는 등에 따른 업무효율성은 향상되지만, 이에 따른 다양한 정보보호에 대한 위협이 존재한다. 스마트워크 서비스를 운영하기 위해서는 다양한 네트워크 자원, 서버, 플렛폼을 지원하는 하드웨어와 소프트웨어가 필요하다. 이에 따라 정보자원을 보호하는 보안 및 정보보호에 대한 취약점이 많이 발생한다.

본 논문은 스마트워크 서비스를 위하여 스마트워크 환경을 분석하고 정보보호관련 기준인 ICS27001 및 KISA-ISMS의 분석을 통하여 스마트워크 정보보호를 위한 취약점을 분석하고자 한다. 정보보호 요구사항에 대하여 사용자 및 서비스 제공자 입장에서의 요구사항을 도출하고, 스마트워크 유형별 보안 위협 및 취약점과 정보보호 대응방안을 제시하고자 한다.

2. 관련 연구

2.1 정보보호

정보란 “ 관찰이나 측정을 통해 수집된 데이터를 실제 문제에 도움이 될 수 있도록 해석하고 정리한 지식”을 말하고, 정보화 촉진 기본법에서는 “ 자연인 또는 법인이 특정 목적을 위하여 광 또는 전자적 방식으로 처리하여 부호, 문자, 음성, 음향 및 영상 등으로 표현한 모든 종류의 자료 또는 지식”을 정보로 정의하고 있다. 따라서 우리가 정보를 보호하기 위해서는 그 정보를 사용하는 기관이나 사람에게 얼마나 의미가 있는 것인지를 파악하여야 하며, 중요도가 높은 정보는 다른 자산과 마찬가지로 중요성을 갖는다고 할 수 있다. 보호하고자 하는 정보의 가치를 정확히 평가하여 조직에 미칠 수 있는 피해 규모를 산출한 후, 이를 막기 위한 정보보호 대책을 수립해야 하며, 이러한 정보보호대책들을 실행하는데 소요될 비용을 산정하여 적절한 비용으로 가장 효과적인 방법을 수립해야 한다(Y.S Shin, 2006).

2.2 정보보호 관리체계(ISMS)

조직의 주요 정보자산을 보호하기 위해 정보보호 관리 절차와 과정을 체계적으로 수립하여 지속적으로 관리 운영하기 위한 종합적인 체계이며, 법적 정의로서 정보통신망의 안전성 및 정보의 신뢰성을 확보하기 위해 수립, 운영하고 있는 관리적, 기술적, 물리적 보호조치를 모두 포함하는 종합적인 관리체계를 의미한다. 즉 비즈니스 위험 접근방법에 근거하여 정보보안을 수립, 구현, 운영, 모니터, 검토, 유지 및 개선하기 위한 전체 경영관리체계 혹은 경영시스템의 일부로서, 문서화된 정보, 말해지는 정보 및 컴퓨터 정보 등 모든 정보가 보안의 대상이 되며, 정보자산의 기밀성, 무결성, 가용성 및 준거성을 달성하기 위하여 이러한 위험의 정보를 평가하고 그 위험을 막기 위한 대책을 수립·운영하기 위한 것이다(J.S Kim, 2014).

- 기밀성(Confidentiality) : 접근이 인가된 당사자에 의해서만 접근하는 것을 보장하는 것
- 무결성(Integrity) : 인가된 당사자에 의해서, 인가된 방법으로만 변경 가능한 것
- 가용성(Availability): 적절한 시간에 인가된 당사

자에게 접근 가능해야 하는 것

2.3 ISO/IEC 27001

정보보안관리는 보안위험을 식별하고 이러한 위험을 효과적으로 관리할 수 있는 대책을 다룬다. ISO/IEC 27001은 기업이 고객 정보의 기밀성, 무결성 및 가용성을 보장한다는 것을 공개적으로 확인하는 데 초점을 둔다. 기업들이 부딪치는 대부분의 상황에 필요한 통제를 식별하기 위한 단일한 참조점을 제공하고 중소기업은 물론 대기업까지 광범위한 범위에 적용될 수 있도록 하여 공통적인 정보보안관리 문서를 참조함으로써 기업들 간의 네트워킹에 있어서 상호 신뢰가 가능하도록 한다. 따라서 이 표준은 지침과 권고안의 성격을 가진다(J.Y Lee, D.S Kim and H.W Kim, 2010).

ISO/IEC 27001은 11개의 주요 통제 분야(Domain), 39개의 세부 분야, 그리고 133개의 통제항목으로 구성되어 있다. ISO/IEC 27001은 위험의 평가 결과에 따라 위험을 감소시키기 위한 통제사항을 통제항목에서 선정한다는 특징을 갖는다. 본문이 아닌 표준 성격의 부록으로 정의한 배경은 조직의 보안위험평가 결과에 따라 선택/제외 및 추가되는 보안통제항목이 존재할 수 있기 때문이다(H.I Jang, H.H Han, N.Y Lee and C.H Cho, 2010).

ISO/IEC 27001의 통제사항 선정은 정보보호 관리체계를 수립하는 과정에서 이뤄진다. 먼저 정보자산, 위협, 취약점 등을 식별하여 위험을 분석하고 평가한다. 이를 바탕으로 위험을 처리하기 위한 방안을 찾는다. 위험 처리 방안으로는 통제사항 적용, 위험 유지, 위험 회피, 위험 전가 등이 있다. 통제사항 선정은 위험 평가 및 위험 처리 절차에 따라 식별된 요구 사항에 따라 이뤄진다. ISO/IEC 27001의 통제사항 선정을 위한 위험관리 절차로 위험평가 부분은 위험의 크기를 산정하여 분석하고, 그 위험 가치를 평가한다(ISO, 2005).

2.4 KISA-ISMS

2002년 한국정보보호진흥원에서 정립하여 발표된 KISA ISMS는 “ 정보통신망 이용 촉진 및 정보보호 등에 관한 법률”의 제47조에 의거하여 “ 조직의 주요 자산을 보호하기 위해 정보보호관리 절차와 과정을 체계적으로 수립하여 지속적으로 관리운영하기 위한 종합적인체계” 를 말하며, 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위하여 수립·운영하고 있는 기술적, 물리적, 관리적, 조직적 보호조치와 통제사항을 포함한다. 이는 방송통신위원회 고시뿐만 아니라 한국 통신기술협회(TTA) 표준으로 등록되어 있다(Y.C Choo and J.Y Choi, 2010).

KISA-ISMS에는 13개 통제분야와 92개 통제사항이 있다. KISA-ISMS에서 통제사항 선정은 정보보호관리체계 과정 중 위험 관리 과정에서 이루어진다. 위험관리는 먼저 전략과 계획을 수립하고, 다음으로 위험을 구성하는 요소들로 분석한다. 그리고 이러한 분석 결과를 기초하여 위험을 평가한 다음 필요한 정보보호 대책을 선정한다(H.I Jang, H.H Han, N.Y Lee and C.H Cho, 2010),

Tab. 2-1. KISA-ISMS Information Protection Measures Control Items

Field	Detailed Control Contents	Num. item
information protection policy	approval and publication of policy, maintenance of policies	6
information security organization	organizational structure, responsibilities and roles	4
outsider security	contract and service level agreement security management, outsider security execution management	3
Classification of information assets	investigation and assignment of information assets, classification and handling of information assets	4
information security education	establishing, implementing and evaluating education and training programs	4

Field	Detailed Control Contents	Num. item
human security	assigning and regulating responsibilities, confidentiality, qualification assessment and management of key personnel	5
physical security	physical information protection measures, data center information protection, equipment protection, office protection	9
system development security	analysis and design security management, implementation and implementation security management, change management	10
password control	Establishing password policies, using passwords, managing keys	2
access control	Access control policy, user access management, access control domain	14
operational security	operating procedures and responsibilities, system operations, network operations, media and document management, malicious SW controls, and remote operations	22
infringement management	infringement incident response plan and structure, response and recovery, follow-up management	7
IT disaster recovery	infringement incident response plan and structure, response and recovery, follow-up management	3

3. 스마트워크 정보보호

3.1 스마트워크 정보보호 도입 유형

스마트워크는 각 유형별로 서로 다른 특성을 가지고 있기 때문에 서로 다른 정보보호 방안이 필요하다. 예를 들어 모바일 오피스는 주로 모바일 단말을 사용한다. 이런 모바일 단말은 분실 가능성이 높고, 무선 네트워크를 사용한다. 그러므로 단말 분실 시 외부에서 데이터를 파기 시킬 수 있는 방안이나, 무선 네트워크에 대한 정보보호 방안이 필요하다. 이에 반해 스마트워크 센터 근무는 사무환경을 제공해주고, 같은 PC에서 여러 명의 직원이 사용할 수 있다. 그러므로 직원의 인증을 통해 개별적인 접근권한을 부여해주어야 한다. 스마트워크 정보보호 유형은 크게 모바일오피스, 재택근무, 스마트워크 센터로 구분할 수 있는데, 국내의 도입기관으로는 모바일오피의 경우 기상청, 삼성증권, 삼성전자에서 도입했다. 재택근무의 경우 ETRI와 일본총무성이 대표적이며, 스마트워크 센터는 KT와 행정안전부에서 설치하여 운영 중이다. 삼성전자의 경우 갤럭시S Ⅱ에 ‘ 시스템 웹엑스 미팅센터’, ‘ 시스코 모바일’, ‘ 시스콘 애니커넥트 시큐어 모빌리티 클라이언트’ 탑재하고, 갤럭시 탭에 ‘ 시스코 세이프티 앤 시큐리티 솔루션’을 탑재하여 모바일오피스를 운영한다. ETRI의 경우 데스크톱 가상화를 통한 데이터 유출을 방지하고, 스마트워크 관제 시스템을 도입하여 재택 업무 환경을 관제하고 스마트워크 서비스를 관리한다. 일본총무성에서는 SSL-VPN에 의한 안전한 회선과 정보의 암호화를 통하여 이용자 및 PC 인증을 하고, 바이러스 대책 및 PC 방화벽 소프트웨어 탑재하였으며, PC 하드 디스크 전체의 암호화와 PC에 데이터를 두지 않는 원격 조정환경 등을 포함한 시스템을 구축하였다. 행정안전부에서는 출입통제를 위한 혈관 인식 시스템 및 CCTV 등을 장착하고, SBC(Server Based Computing) 기반의 가상화 시스템을 구축하여 운영하고 있다(Korea Internet Promotion Agency, 2011),

3.2. 스마트워크 유형별 기반요소 기술

3.2.1 모바일오피스

모바일 O/S 및 단말기의 경우에는 출시되고 있는 스마트폰의 경우, 다양한 O/S와 그에 따른 각각의 장단점을 보유하고 있으나 업그레이드와 Version-Up 작업이 지속적으로 이루어지고 있으므로, 이를 검토하여 기업에 적합한 O/S와 단말기를 선정하는 작업이 필요하다(Korea Broadcasting Commission, 2011).

모바일 서버 플랫폼은 다양한 단말 환경을 지원하여 적은 비용으로 다양한 스마트폰 환경에 적용될 수 있는 기능을 제공해야 한다. 물론, 기존 산업용

PDA의 환경과의 동시 지원여부도 가능해야 한다. 또한, 통합개발환경(Integrated Develop Environment, IDE)을 통해서 프로젝트의 구성, 코딩, 테스팅, 디버깅 같은 작업을 지원할 수 있어야 하며, 모바일 프레임워크를 제공하고 충분한 추상화 계층을 제공함으로써 다양한 단말환경에 적용이 가능해야 한다. 또한, 단말들의 효율적인 관리 및 제어기능을 제공하고, 단말분실 또는 해킹 등의 취약점을 해결할 수 있는 보안기능도 제공할 수 있어야 한다. 그리고 백엔드 통합 기능을 제공함으로써, 기존의 비즈니스 로직과의 연동, SNS와의 연동등과 같이 모바일 환경을 충분히 활용할 수 있는 기능을 제공하여야 한다. 마지막으로 플랫폼 확장성 및 유연성을 제공함으로써 비즈니스의 확장시 충분히 수평적 확장이 가능하여야 하며, 비즈니스 로직 등이 코드의 변경 없이 다양한 환경에 쉽게 적용되고, 공유될 수 있도록 하여야 한다(Korea Broadcasting Commission, 2011).

Tab. 3-1. Mobile client platform features[8]

Classification	Characteristics
independantative application	- Separate development of individual applications for each O / S - Performance is excellent, but the cost is increased by developing each OS separately.
single application through integrated middleware	generalized regardless of OS, but needs to reflect version up and change of each OS in middleware, so be delayed in support period or increase in operating cost, and the performance due to the middleware is lowered.
hybrid client platform	- high performance, medium cost

3.2.2 재택근무

재택근무를 위해서는 사무실의 사무 환경이 집에 구축되어야 하며 다음 제시되는 4가지 방식인 인프라, 보안관리, 운영관리, 시스템관리 군으로 구분할 수 있다(Venture Business Association, 2009).

Tab. 3-2 Information communication infrastructure technology required for telecommuting[4]

Classification		Contents
Infra	computers & accessories	notebook, PC, monitor, keyboard, mouse
	multifunction machine	combined scanner and copier
	communication equipment	accessory equipment and routers for laptops
	video equipment	web camera
	communications network	high-speed communication network
Security	antivirus	antivirus for viruses and malware
	intrusion prevention	web firewall and PC firewall
	integrated PC security	internal data leak prevention and security USB
	DB / content Security	DB security and encryption, DRM
	access management	network access control and biometrics (fingerprint)
	virtual private network	virtual private network (VPN)
Operation	electronic payment	electronic payment program
	electronic messenger	programs for communication
	file sharing	file sharing program for smooth work
	e-mail	e-mail management program
	project management	project management program
	remote collaboration management	tools to collaborate remotely
System Management	DMS	client PC HW / SW asset management
	PMS	OS patch /vaccine/application update
	data backup	data redundancy security backup and management
	system recovery	immediate restoration management in case of system problems
	personal video conference	web image communicate programs

3.2.3 스마트워크 센터

스마트워크 센터에서 IT 인프라는 네트워크와 어플리케이션으로 구분할 수 있다. 네트워크는 원격근무가 가능하도록 하는 유무선 네트워크를 제공하는

것으로 LAN케이블, LAN단자, 허브(Hub), AP(Access Point) 등이 있다. 어플리케이션은 원격사용자가 외부에서도 회사와 같은 환경에서 근무할 수 있도록 협업 또는 커뮤니케이션 등을 제공하는 것으로, 가상기업의 인트라넷, 웹 디스크, 일정관리, 실시간 협업(영상회의, UC 등), 웹 메일, 오피스프로그램 등이 있다(Korea Broadcasting Commission, 2011).

Tab. 3-3. Component of smartwork center application infrastructure[8]

Classification	Contents
business	knowledge management, personnel management, payment, electronic documents, etc.
communication	UC, clubs, blogs, etc.
information sharing	web disk, archive, bulletin board, etc.
security	anti-spyware, DRM, server based computing(SBC)
office	spreadsheets, words, presentations, etc.

스마트워크 센터 운영 인프라는 스마트워크 센터의 효과적인 활용을 위해서 운영관리 시스템을 활용하여야 한다. 일반적으로, 근로자가 스마트워크 센터의 각종 시설을 편리하게 예약하고 사용할 수 있도록 시설관리, 안내데스크, 출입 체크 등의 운용 관리 인프라를 구축한다.

스마트워크 센터의 문서, 출입통제 등에 사용되는 물리적인 성격의 보안시설을 의미한다. 스마트워크 센터의 성격상 다양한 소속의 근로자들이 공용으로 사용하기 때문에 출입보안, 서버보안, 문서 출력보안, 공용 PC환경 보안, 방음시설 등이 있다.

Tab. 3-4. Component of smartwork center security infrastructure[8]

Classification	Contents
access control	access history management using RFID
user management	manage user location information using RFID and WiFi
network security	firewall, DB security, intrusion detection, web security, etc.
server security	servers with security-related solutions

3.3 스마트워크 보안가이드 분석

스마트워크 활성화를 위한 정보보호 권고는 안전한 스마트워크 이용 환경을 조성하기 위하여 기업들이 자율적으로 이행할 수 있는 기술적·관리적 보호조치를 제시한다. 또한, 현장이동근무(모바일 오피스), 재택근무(홈오피스), 스마트워크 센터근무 등 다양한 스마트워크 유형을 고려하여 이용자가 실질적인 근무 환경에 맞게 적용할 수 있도록 기능별, 구성요소별 정보보호 대책을 스마트워크 서비스 제공자/관리자/이용자 준수사항으로 제시하였다(Korea Broadcasting Commission, 2011).

Tab. 3-5. Information protection recommendations for smartwork activation

Type	Classification	Instances
service provider	infra security	technological protection measures such as hacking correspondence, wired / wireless network security, physical security
	public PC security	technological protection measures for public PC memory storage devices and removable storage media in the center
manager	terminal, service, contents	administrative protection measures for terminal, service and content protection from malicious code, lost or stolen
	human asset	administrative protection measures such as training and monitoring for user's safe use of smart work service

Type	Classification	Instances
	infringement incident response	procedures to cope with various security breaches that can occur in smart work
user	information asset	providing the user with the inspection and carrying out the procedure for the proper protection of information assets
	raise awareness	conduct educational and learning activities such as information protection precautions and response procedures to raise awareness of users' continuous information protection
	infringement incident response	guidance for users to promptly respond to security breaches in smart work environments

4. 스마트워크 정보보호 요구사항 및 취약점

4.1 스마트워크 정보보호 요구사항

본 절에서는 다양한 스마트워크 도입 사례 및 스마트워크 보안 위협 사례를 바탕으로 스마트워크 유형별로 정보보호 요구사항을 도출하였다.

4.1.1 사용자 입장에서 정보보호 요구사항

가) 공통 요구사항

① (사용자인증) 서비스를 등록한 본인 이외에는 인증을 통과할 수 없어야 함

② (단말인증) 서비스를 등록한 단말 이외에는 서비스를 사용할 수 없어야 함

③ (가용성) 사용자는 언제, 어디서나 서비스를 사용할 수 있어야 함

④ (무결성) 애플리케이션 및 콘텐츠의 무결성을 보장해야 함

⑤ (접근제어) 전송되거나 서버에 저장되는 데이터는 데이터와 특성에 따라 보호되어야 함

⑥ (자료백업) 클라우드 스토리지에 저장된 자료의 손실을 막기 위해 백업 기능을 제공해야 함

⑦ (내용 프라이버시) 제3자는 사용자가 사용하는 서비스 및 콘텐츠의 내용을 알 수 없어야 함

나) 모바일 오피스에서의 요구사항

① (AP 인증) AP에 대한 안전성 분석 기능을 제공해야 함

② (자료저장 제어) 자료의 유출을 막기 위해 허가된 스토리지 외에는 저장되지 않아야 함

③ (자료공유 제어) 서비스를 사용할 수 있는 사용자들 간의 자료 공유가 제한되어야 함

④ (사용 제어) 서비스를 사용하는 본인 이외에 다른 사람들이 서비스 내용을 볼 수 없어야 함

⑤ (위치 프라이버시) 사용자가 휴대 단말을 이용하여 서비스를 받을 경우 제3자는 사용자의 위치를 추적할 수 없어야 함

다) 재택근무에서의 요구사항

① (기밀성) 전송되거나 서버에 저장되는 데이터는 데이터의 특성에 따라 보호되어야 함

② (자료저장 제어) 자료의 유출을 막기 위해 허가된 스토리지 외에는 저장되지 않아야 함

③ (사용 제어) 서비스를 사용하는 본인 이외에 다른 사람들이 서비스 내용을 볼 수 없어야 함

④ (위치 프라이버시) 사용자가 휴대 단말을 이용하여 서비스를 받을 경우 제3자는 사용자의 위치를 추적할 수 없어야 함

⑤ (출력물 제어) 자료의 유출을 막기 위해 정보가 저장된 출력물을 관리할 수 있어야 함

라) 스마트워크센터에서의 요구사항

① (기밀성) 전송되거나 서버에 저장되는 데이터는 데이터의 특성에 따라 보호되어야 함

② (자료저장 제어) 자료의 유출을 막기 위해 공용 단말에 저장된 정보를 다른 사용자가 확인할 수 없어야 함

③ (출력물 제어) 자료의 유출을 막기 위해 정보가 저장된 출력물을 관리할 수 있어야 함

4.1.2 서비스 제공자 입장에서의 정보보호 요구사항

① (서비스보안) 사용자가 사용하는 서비스가 다양한 공격으로부터 원치 않은 피해를 방지할 수 있어야 함

② (단말보안) 사용자가 사용하는 단말기가 다양한 공격으로부터 원치 않은 피해를 방지할 수 있어야 함

③ (서버보안) 서버가 다양한 공격으로부터 원치 않은 피해를 방지할 수 있어야 함

④ (부정사용방지) 인가되지 않은 사용자가 서비스를 이용할 수 없어야 함

⑤ (출입통제) 서비스 허가자 외에는 센터 출입을 제한해야 함

4.2 스마트워크 유형별 보안 위협

스마트워크 정보보호 요구사항을 바탕으로 스마트워크 도입 및 운영 관점에서의 보안 위협 및 취약점을 도출하였다. 스마트워크 세 가지 분류는 업무를 수행하는 위치, 사용하는 단말과 서비스의 차이로 구분된다. 하지만 실제 사내망에 있는 정보를 사용한다는 점이나 유무선 네트워크를 사용한다는 점은 동일하다. 그렇기 때문에 구조적 관점에서 보면 스마트워크를 공통부분과 모바일오피스, 재택근무, 스마트워크 센터의 특화된 부분으로 구분할 수 있다.

Tab. 4-1. Security Threats and Vulnerabilities by Smart Work Structure[7]

Category	Contents
Common Threats and Vulnerabilities	
User	Malicious employees who want to leak information
	Withdrawal of employees with company information
Service	Security vulnerability in business services
	Use non-licensed business services for account hijacking
Wireless	Wireless LAN connection with non-secured AP
	Direct exchange of information between employees
Network	Packet sniffing in network section
	Hacking network equipment such as switches, routers
Internal Network	Internal server hacking via mobile terminal
	Security Vulnerability in Cloud Computing
Security Threats and Vulnerabilities of Mobile Office	
User	Careless work by employees
Terminal	Lost or stolen business terminal
	Use terminal of family members, relatives etc.
	Information backup, synchronization of employee terminal
	Sale and transfer of employee terminals
	Security vulnerability of terminal operating system
	Use business applications on unlicensed terminals
Telecommuting Security Threats and Vulnerabilities	
Home	Lost or stolen business terminal
	Use terminal of family members, relatives etc.
	Malicious software such as viruses and worms
	Lost or damaged printouts
Security Threats and Vulnerabilities of Smart Work Center	
Center	Lost or damaged printouts
	Access to non-licensed centers
	Use non-licensor's public terminal
	Malicious software such as viruses and worms
	Business information stored in public terminal

스마트워크 환경에서는 다양한 보안위협이 존재하고 있으며 이러한, 보안위협은 전혀 막을 수 없는 위협들이 아니라 사용자나 기업의 측면에서 관리하면, 보다 안전한 스마트워크 환경을 구축할 수 있다. 국내외 기업에게 스마트워크 도입을 촉진하고, 스마트워크 환경 구축을 활발하게 하기 위해서는 스마트워크에 대한 보안 대책을 마련하여 보안 사고를 최소화하고 미연에 방지할 수 있도록 하여야 한다.

4.3 스마트워크 정보보호 취약성 대응

스마트워크 환경에서 정보보호 취약성 대응 방안은 스마트워크 정보보호 요구사항 및 스마트워크 보안 위협·취약점과 선행 연구 자료의 일부 내용을 추가 ·수정하여 대응방안을 제시하고자 한다. 하나의 취약점 및 위협에 대해서는 다양한 대응방안이 존재할 수 있으며 공통부분, 모바일오피스, 재택근무, 스마트워크 센터 등 스마트워크 환경 유형별 정보보호 대응방안을 제안한다.

공통부분에서는 정보를 유출하고자 하는 악의적인 직원이 있을 경우를 대비하여 정기적인 정보보호 교육 실시하고, 디지털 콘텐츠 저작권 관리하며, 정보 유출에 대한 추적과 정보 유출시 직원 징계방안 수립하여야 한다. 기업 정보를 가진 직원이 퇴사하는 경우에는 정기적인 정보보호 교육 실시하고 직원에게 지급된 장비 회수 및 업무 데이터를 삭제하며, 원격 데이터 관리 및 정보 유출에 대한 추적을 할 수 있도록 한다. 업무 서비스의 보안 취약점에 대하여는 자동화 도구를 활용한 취약점 분석하여 제거하고, 보안 취약점 발견 시 보고 할 수 있는 프로세스 수립하고 정기적인 정보보호 교육 실시하여야 한다. 계정도용으로 인한 비허가자의 업무 서비스 사용에 대하여는 사용자 인증은 ID/Password 방식, 기기인증서, 공인인증서 방식 및 단말고유정보, OTP, 생체인식 등 복합인증방식 적용하고, 비정상적인 사용 패턴 모니터링 및 수행 업무 로그 분석하여 정보유출을 방지하여야 한다. 보안이 설정되지 않은 AP와의 무선랜 연결시에는 업무용 무선 AP외 타 무선 AP 접근 차단하고 전용 인터넷망 또는 이동통신 전용회선을 이용하고, 네트워크 종단 간 데이터 및 음성 도· 감청 방지를 위해 암호화 및 VPN 적용하여야 한다. 또한, 비인가된 무선랜을 통한 접근시 업무 서비스 사용 제한하고 정기적인 정보보호 교육 실시하여야 한다. 블루투스, 와이파이, 다이렉트와 같은 직원간의 직접적인 정보교환 시에는 직원간 미 승인된 정보 공유 제한하고, 시스템을 통한 주요정보 접근 통제 및 허가되지 않은 유무선망 제한한다. 네트워크 구간에서의 패킷 스니핑시에는 전용 인터넷망 또는 이동통신 전용회선 이용하고 네트워크 종단 간 데이터 및 음성 도· 감청 방지를 위해 암호화 및 VPN 적용하여 전송되는 데이터를 암호화한다. 스위치, 라우터 등 네트워크 장비 해킹시에는 내· 외부망 접점지점에 침입차단 및 탐지 시스템 등의 보안장비를 구축하여 운영하고, 네트워크 종단 간 데이터 및 음성 도· 감청방지를 위해 암호화 및 VPN 적용한다. 휴대단말을 경유한 내부 서버 해킹시에는 인가된 단말기에 대한 접속 허용 및 단말기별 보안 취약점 점검하여야 한다. 클라우드 컴퓨팅의 보안 취약점에 대하여는 사용자 식별 및 인증 통합 관리, 개인별 업무환경 제공하고 서비스 내의 분산된 중요정보는 안전한 암호화 및 키 관리 등의 보호대책을 마련하고 방화벽, 침입차단, 접근제어, 보안관제 등 보안 시스템 구축하여 모니터링하여야 한다.

모바일 오피스 운영시에는 직원의 부주의한 업무 수행시 모바일 장비 및 소프트웨어의 사용법에 대한 교육 실시하고, 정기적인 모바일오피스 관련 정보보호 교육실시하며, 모바일 화면 정보보호 스크린 장치를 설치하여야 한다. 업무 단말의 분실·도난 취약점에 대하여는 모바일 단말 잠금(원격 잠금) 및 원격 파일 삭제 기능 등 물리적 보안책 마련하고, 모바일 단말기 암호, 세션 유지시간, 입력 오류 횟수 제한을 설정하고, 사용자 인증은 ID/Password 방식, 기기인증서, 공인인증서 방식 및 단말고유정보, OTP, 생체인식 등 복합인증방식 적용한다. 모바일 단말기에 업무 자료는 저장하지 않으며, 필요시 암호화하여 저장한다. 업무 단말의 정보 백업시에는 업무 단말 주요 정보에 대한 백업 실시하여야 한다. 업무 단말의 판매·양도 취약점에 대하여는 업무 단말 교체 시 기존 장비 정보 삭제 여부 점검하고, 업무 단말의 판매·양도 시 보안 관리자에게 승인 및 점검하고 정보가 저장된 단말을 판매·양도 하지 않도록

교육을 진행하여야 한다. 업무 단말 운영체제의 보안 취약점에 대하여는 플랫폼의 보안 취약점 및 정기적인 업데이트를 공지하고 사용자 안전 사용 방법 등에 대한 인식을 제고하고 최신 운영체제 설치 및 보안 패치 여부 점검하여 취약점이 존재하는 운영체제에 대한 업무애플리케이션 실행을 제한하고 정기적인 보안패치를 업데이트하여야 한다.

재택근무 부문에서는 바이러스·웜 등의 악성 소프트웨어 취약점은 바이러스, 스파이웨어, 웜 등 악성코드에 대비한 안티바이러스 솔루션을 도입하고 단말 및 서버에 백신 프로그램 설치 및 주기적인 검사, 자동업데이트 설정하여 두고 악성코드 대응 및 유해 트래픽 차단 등 악의적인 공격을 사전에 탐지하는 차단 시스템을 도입한다. 장애 발생 시 신속한 대응 및 복구체계를 구축하고 주기적인 운영체제 업그레이드 및 패치를 하여야 한다.

스마트워크 센터 부문에서는 출력물의 분실 또는 부실 관리에 대하여 허가되지 않은 업무 정보 및 단말화면은 프린터 등 출력장치를 통한 출력을 금지하며, 승인된 출력물은 콘텐츠 보호를 위한 DRM 적용하여야 한다. 비 인허가자의 센터 출입이나 공용 단말 사용에 대하여는 비 인가자의 스마트워크 센터 및 서비스 제공을 위한 주요 네트워크, DB, 서버 등 인프라 시설에 대한 접근을 통제할 수 있도록 CCTV, 바이오 인증, 스마트카드 등 물리적 보안대책 마련하고, 출입통제시설에 대한 출입 기록대장 작성하여 관리하여야 한다. 스마트워크용 PC를 사용하여 가상 데스크톱에 접속할 경우, 특정업무와 관련한 중요정보 접근 제한하고 공용 단말기에 대한 사용자 인증(ID/Password, 공인인증서, OTP, 생체인식 등)을 강화하고, 예약자 확인 시스템을 통해 허가된 사용자만 단말을 사용하도록 하여야 한다. 바이러스·웜 등의 악성 소프트웨어 사용에 대하여는 바이러스, 스파이웨어, 웜 등 악성코드에 대비한 안티바이러스 솔루션을 도입하고, 단말 및 서버에 백신 프로그램 설치 및 주기적인 검사, 자동업데이트 설정하여 악성코드 대응 및 유해 트래픽 차단 등 악의적인 공격을 사전에 탐지하고 차단하는 시스템을 도입하여야 한다. 장애 발생 시 신속한 대응 및 복구 체계 구축을 통하여 주기적인 운영체제 업그레이드 및 패치를 하여야 한다. 공용 단말에 저장된 업무 정보에 대하여는 단말기에 업무 자료는 저장하지 않으며, 필요시 암호화하여 저장하고, 스마트워크 센터 공용 단말기 기억저장장치에 업무관련 정보는 단말기 사용 후 자동 삭제하도록 하고, 스마트워크 센터 이용자를 위한 정기적인 정보보호 교육을 실시하여야 한다.

5. 결론

스마트워크는 기업들의 업무 생산성을 향상시키고, 비용을 절감하는 등 에 따른 업무효율성은 향상되지만, 이에 따른 정보보호 및 보안 위협과 정보보호 취약점 역시 빠른 속도로 증가하고 있다. 따라서 기업은 중요 자산에 대한 접근통제 등 관리적·물리적·기술적 관련 정보보호 조치를 준수함으로서 기업이 보안을 고려한 안전한 스마트워크 환경을 구축할 수 있다.

본 논문에서는 스마트워크 서비스를 위하여 스마트워크 환경을 분석하고 정보보호관련 기준인 ISO27001 및 KISA-ISMS의 분석을 통하여 스마트워크 정보보호를 위한 취약점을 분석하였다. 정보보호 요구사항에 대하여 사용자 및 서비스 제공자 입장에서의 요구사항을 도출하였으며, 스마트워크 유형별 보안 위협 및 취약점에 대하여 공통부분, 모바일오피스, 재택근무, 스마트워크 센터 등 스마트워크 환경 유형별 정보보호 대응방안을 제시하였다.

본 연구의 대응방안에 대하여 보다 논리적이고 체계적인 방법 설계와 사례가 제시되길 바라며, 실제 적용하여 유용성을 검증하여 지속적인 유지 및 보완작업을 해 나감으로써 보다 실용적이고 정보보호 체계로 개선되기를 기대한다.

Reference

[1] Y.S Shin(2006), " A model for improving the level of information protection for SMEs using ISMS," Graduate School of Information Communication, Konkuk University, Master Thesis (신영수(2006), " 정보보호관리체계(ISMS)를 활용한 중소 기업 정보보호 수준 향상 모델," 건국대학교 정보통신대학원 석사학위 논문)

[2] J.S Kim(2014), " Smartwork environment using Information Security Management System Study on Security Audit," Graduate School of Information Communication, Konkuk University, Master Thesis (김지석(2014), " 스마트워크 환경에서 정보보호관리체계를 이용한 보안감리에 대한 연구," 건국대학교 정보통신대학원 석사학위 논문)

[3] J.Y Lee, D.S Kim and H.W Kim(2010), " A Design of the Information Security Auditing Framework of the Information System Audit," The Journal of Korea Society of Digital Industry and Information Management, 6(2), 233-245 (이지용, 김동수, 김희완(2010), " 정보시스템 감리에서의 정보보호 감리모형 설계," 디지털산업정보학회논문지, 제6권 제2호, 233-245)

[4] H.I Jang, H.H Han, N.Y Lee and C.H Cho(2010), " A Model of Control Selection in Information Security Management System," The Journal of Korean Institute of Communications and Information Sciences, 35(8), 195-204. (장호익, 한호현, 이남용, 조창희(2010), " 정보보호관리체계 통제사항 선정 모델 연구," 한국통신학회논문지 제35권 제8호(통신산업응용), 195-204)

[5] ISO/IEC 27001, 「Information technology -Security techniques - Information security management systems - Requirements」, ISO, 2005.

[6] Y.C Choo and J.Y Choi(2010), " A Study on Information Protection Model Extending Information Security Management System in Smart Mobile Office Environment," Proceedings of the Korean Information Science Society. (추연철, 최진영(2010), " 스마트 모바일오피스 환경에서의 정보보호관리체계(ISMS)를 확장한 정보보호 모형 연구," 한국정보과학회 학술발표논문집)

[7] Korea Internet Promotion Agency(2011), Study on Establishment of Information Protection for Smart Work Introduction
(한국인터넷진흥원(2011), 스마트워크 도입을 위한 정보보호 수립 기준 연구)

[8] Korea Broadcasting Commission(2011), Smart work introduction guidebook for companies
(방송통신위원회(2011), 기업을 위한 스마트워크 도입 운영 가이드북)

[9] Venture Business Association(2009), Green SW Technology and Market Trends - Virtual Office (벤처기업협회(2009), 그린 SW기술 및 시장동향 -Virtual Office분야)

[10] Korea Broadcasting Commission(2011), Information Protection Recommendations for Smart Work Activation (방송통신위원회(2011), 스마트워크 활성화를 위한 정보보호 권고)

Ji Seog, Kim(hulpei@hanmail.net)

Ji Seog Kim received the MS degree in the Graduate School of Information Communication from Konkuk University in 2014. His major is information system audit. He has been a senior consultant in the Department of Consulting Headquarters at Cyberone Corporation since 2011. His current research interests include information system audit, cyber security, security management, and security consulting.

Dong Soo, Kim(dskim@kisac.co.kr)

Dong Soo Kim received the bachelor's degree in the Department of Computer Science from Kwanwoon University in 1981. He received the Ph.D. degree in the Management Information System from Kookmin University in 2005. He has three Certificate as a Professional Engineer(P.E.) in Information Systems Management, Computer Application System, and Computer Communications from Korean Ministry of Science and Technology. He is a chief consultant in the department of Information System Auidt at KISAC company and an invited professor in the Graduate School of Information Communication at Konkuk University. His current research interests include u-city audit, e-business, and information system audit.

Hee Wan, Kim(hwkim@syu.ac.kr)

Hee Wan Kim has been a professor in the Department of Computer Engineering at Shamyook since 1996. Hereceived the Ph.D. degree in the Department of Computer Engineering from Sungkyunkwan University in 2002. He has two Certificate as a Professional Engineer(P.E.) in Information Systems Management and Chief Information System from Korean Ministry of Science and Technology. His current research interests include database, information system audit, database security, and software engineering.

Vulnerability Countermeasures for Information Security in Smart Work Services

Ji Seog, Kim*, Dong Soo, Kim**, Hee Wan, Kim***

ABSTRACT

Smart work refers to enhancing the efficiency of work by utilizing smart devices. Smart work improves business productivity by improving business productivity of companies, reducing costs, but there is a threat to various information protection. To operate telecommuting, mobile office, and smart work center, hardware and software are needed to support various network resources, servers, and platforms. As a result, there are many vulnerabilities to security and information protection that protect information resources.

In this paper, we analyze the smart work environment for smart work service and analyze vulnerability for smart work information protection through analysis of ICS27001 and KISA-ISMS. We have developed requirements for information protection requirements for users and service providers. We have developed a solution for information security protection for smart work environments such as common parts, mobile office, telecommuting, and smart work center for security threats and weaknesses per smart work type.

Keywords: smart work, information protection, vulnerability, information protection requirements, information protection countermeasures

* Senior consultant, Cyberone Coporation, Dept. of consulting headquarters, hulpei@hanmail.net
** Invited professor, Konkuk University, Graduate school of information communication, dskim@kisac.co.kr
*** Professor, Sahmyook University, Division of Computer-Mechatronics, hwkim@syu.ac.kr