Journal of Korea Multimedia Society Vol. 18, No. 2, February 2015(pp. 178-188)
http://dx.doi.org/10.9717/kmms.2015.18.2.178

모바일 오피스 개인정보 보호 방안에 대한 연구

박용준†, 이윤정††

A Study on countermeasure for privacy in mobile office

Yongjoon Park†, Yunjung Lee††

ABSTRACT

The proliferation of devices such as tablets and smart phones, which are now used by many people in their daily lives, has led to a number of companies allowing employees to bring their own devices to work due to perceived productivity gains and cost savings. However, despite many advantage, security breaches (e.g., information leakage) can happen for various reasons (e.g., loss or theft of devices, and malicious code) and privacy breaches can happen by using personal devices for business. We should carefully scrutinize security threats in this area. We present the security threats analysis and the technical approach in this area, and discuss privacy threats and countermeasures.

Key words: BYOD, Information Security, Mobile Office, Privacy

1. 서 론

국내 스마트폰 가입자가 4,000만 명(2014. 9월 기준)을 넘어가면서 스마트폰을 기반으로 하는 모바일 서비스의 형태와 범위가 빠르게 변화하고 있다[1]. 가장 큰 변화 중 하나는 기업의 자산으로 이용되는 장비뿐만 아니라, 개인이 직접 구매한 개인의 스마트폰, 태블릿 PC와 같은 모바일 단말기를 업무적으로 이용할 수 있도록 연결해달라는 요구, 즉 'BYOD (Bring Your Own Device)'의 확대이다[2,3]. Cisco의 시장 조사에 따르면 "BYOD는 지금 가장 성장하고 있는 트렌드로서, 근로자의 78%는 일을 하는데 자신의 기기를 소유하고, 44%는 적어도 일주일에 한 번 재택근무를 하여 매년 2500달러를 절약한다."고 한다[4]. BYOD는 모바일 단말기의 높은 이동성과 편리성으로 기존의 컴퓨터가 가지고 있던 기능들을 언제, 어디서나 이용할 수 있게 함으로써 사용자로 하여금 사회적, 경제적 효과를 얻을 수 있도록 한다.

스마트워크는 기존의 사무실을 벗어나 시간과 장소에 구애받지 않고 언제 어디서나 효율적으로 일할 수 있는 업무 개념으로, 기업들은 스마트워크를 위해 스마트폰, 태블릿 PC와 같은 모바일 단말기로 모바일 오피스를 구축하고 있다[5]. 현재는 기업이 일괄적으로 업무용 모바일 단말기를 지급하는 대신 BYOD를 접목하여 개인이 보유하고 있는 모바일 단말기를 업무에 이용할 수 있도록 모바일 오피스를 운영하는 경우가 일반적이다[3]. 하지만 가트너는 2015년 10대 전략 기술 중 1위를 차지한 '컴퓨팅 에브리웨어 (Computing Everywhere)' 부분에서 "최종 사용자의 단말기를 제어하지 못하는 환경이 만들어지고 있기 때문에 이에 대한 제어권을 잃은 IT 조직이 관리 측면에서 중대한 도전에 직면하게 될 것이다."라고 발표하며 BYOD 확대로 인한 보안위협요소가 증가할 것이라고 예측하고 있다[6].

※ Corresponding Author : Yunjung Lee, Address: (690-756) Ara-1-dong, Jeju-si, Korea, TEL : +82-64-754-3597, FAX : +82-64-725-2579, E-mail : rheeyj@jejunu.ac.kr
Receipt date : Jan. 19, 2015, Revision date : Feb. 6, 2015
Approval date : Feb. 10, 2015

† Information & Communications Technology Research Institute (E-mail : pyj.ictri@gmail.com)
†† Dept. of Computer Science and Statistics, Jeju National University
※ This research was supported by the 2014 scientific promotion program funded by Jeju National University.

모바일 오피스는 기업의 비용절감, 효율성 증대와 같은 다양한 장점에도 불구하고 단말기 분실 및 도난, 악성코드 감염과 같은 보안위협으로 개인정보 및 기업 기밀정보 유출, 불법 과금과 같은 여러 형태의 보안 사고가 발생할 수 있으며[7], BYOD 확대로 개인의 모바일 단말기를 업무에 이용하여 개인 및 기업이 개인정보 침해사고에 대한 피해를 입게 될 수 있기 때문에 개인정보를 침해할 수 있는 보안위협요소가 무엇인지 충분한 검토가 이루어져야 한다. 따라서 본 논문에서는 모바일 오피스 주요 보안위협요소들에 대하여 분석하고, 기술적 보호조치와 함께 한국정보화진흥원(NIA)의 개인정보 보호 인증(PIPL)에서 통제항목으로 주어진 개인정보보호 요구사항과 캐나다 온타리오주의 개인정보보호위원인 앤 카부키안(Ann Cavoukian) 박사가 주창한 프라이버시 바이 디자인(PbD)의 비교·분석을 통해 모바일 오피스 운영자가 개인정보보호를 위해 고려해야 하는 사항을 논의하고자 한다.

2. 모바일 오피스 보안 및 기술적 보호조치

2.1 모바일 오피스 보안

모바일 오피스는 Fig. 1과 같이 구성되며 보안 요구사항은 일반적인 정보보호의 요구사항을 포함함과 동시에 모바일 단말기에 적합한 추가적인 요구사항을 필요로 한다. 한국인터넷진흥원(KISA)의 '안전한 모바일 오피스 도입과 운영을 위한 정보보호 수칙'에 따르면 모바일 오피스 사용자와 운영자의 보안 요구사항은 Table 1과 같이 분류된다[8].

2.2 모바일 오피스 보안을 위한 기술적 보호조치

모바일 오피스를 도입하려는 기업들은 비용절감과 효율성 증대를 위해 BYOD를 고려하지만, 분실·도난의 위험, 취약한 네트워크 이용과 같은 심각한 보안위협에 노출되어 있다. 이러한 보안위협에 대한 대응 방안으로 모바일 오피스를 운영하는 기업은 Fig. 2와 같이 네트워크 접근제어(NAC: Network Access Control)와 모바일 단말 관리(MDM: Mobile Device Management) 솔루션을 도입하여 직원 개개인의 모바일 단말기와 기업 내부 시스템으로의 접근을 통제하고 있다[8].

2.2.1 네트워크 접근제어(NAC)

네트워크 접근제어(NAC)는 접속 단말이 내부 네트워크에 접근하기 전에 보안정책을 준수했는지 여부를 검사해 네트워크 접속을 통제하는 기술이다[9].

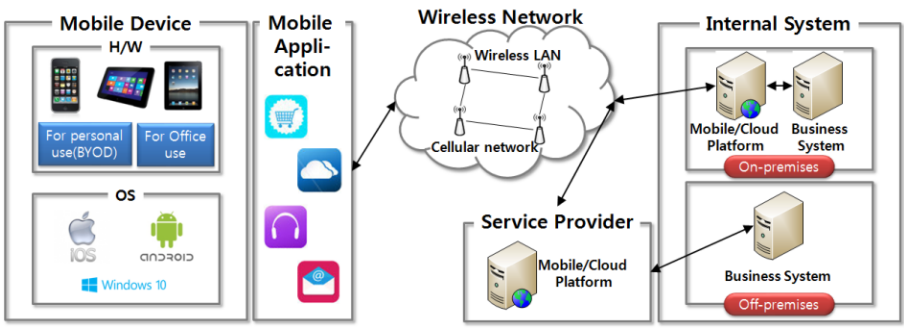

Fig. 1. Mobile Office Infrastructure.

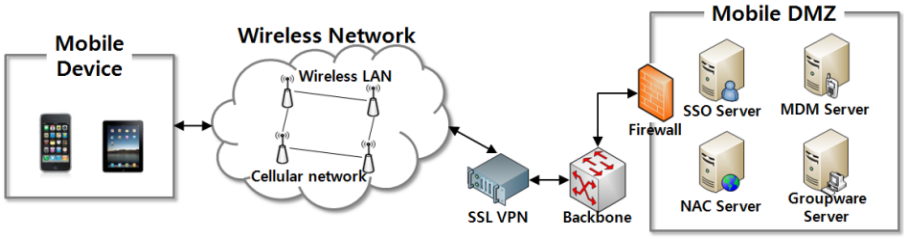

Fig. 2. Network Security equipment for Mobile Office.

Table 1. Mobile Office Security Requirement

Security Requirement Analysis				
Security Requirement for User	H/W	Authentication	Time	• User authentication at execution • Auto-lock setting at unuse over a period of time • User authentication at unlock
			Method	• A strong password policy for security • Storing user's passwords in encrypted database
			Action	• A security administrator notification about an unusual number of authentication failed
		Management	Counter measure	• Remote deletion request for loss or theft device
	S/W	Management	SW Installation	• Authorized SW installation
		OS	Patch	• Updating mobile OS with the most recent patches
			Tampering	• Verifying mobile OS integrity
		Data	Access Control	• Access control between mobile device and business PC • Using Authorized data storage medium for mobile device
	Network Security		W-LAN	• Allowing to access authorized wireless AP only
Security Requirement for Administrator	Administrative Security		Device Management	• Carrying out repair and replacement of mobile device over the control of a security administrator
			S/W Vulnerability Analysis	• Carrying out vulnerability analysis and security action before introduction of a application for work
			Security Verification	• Periodic simulation hacking and vulnerability analysis for service and infrastructure
	Business Service Security		User Authentication Security	• User authentication using OTP or accredited certificate with ID/PW
			Service Security	• (Application distribution) Prohibition of distribution for application for work via App store • (Service protection) Access restriction and integrity verification for service which is not updated
			Asset Security	• Preventing leakage, forgery, and tampering for important information
	Infrastructure Security		System Security	• Carrying out periodic patch

NAC의 특징은 안티바이러스와 같은 호스트 기반의 보안기술을 기존 네트워크 보안체계와 결합해 전체 네트워크에 통합보안 체계를 구현하는 것이다. 보안 관리자는 접속단말, 사용자, 그리고 접속하는 시스템의 상태에 따라 접근 허용여부를 결정하는 보안정책을 수립한다. 네트워크에 접속하려는 접속단말은 사용자가 누구인지, 백신프로그램이 설치되었는지, 백신프로그램 업데이트가 제때 이루어지고 있는지와 같은 상태가 수립된 보안정책과 비교·검토된 후 상태에 맞는 접근권한이 부여된다.

보안정책을 따르지 않는 접속단말의 경우 네트워크 접근을 차단하거나, 악성코드에 감염되었을 경우 치료를 위한 특정 네트워크 영역의 접근만을 허용할 수 있다. 또한 접속단말이 접근제어 과정을 거쳐 네트워크에 접속한 이후에도 지속적으로 보안정책 적용 여부를 모니터링하여 이상이 있을 경우 적절한

대응을 위한 기술 및 절차를 검토하고 이를 정책에 반영한다.

NAC 구축의 표준 참조 모델로는 가트너의 NAC 구축 모델을 들 수 있다[10]. 이 모델은 접속단말 보안평가, 보안문제 대응, 네트워크 접근허용, 보안정책 준수여부의 지속적인 모니터링 및 대응에 대한 업무 순환 절차에 대하여 표현한 것으로 다음 여섯 단계로 정리할 수 있다.

① 장비·사용자에 대한 인증 정책과 시스템 상태 비교·검토 정책 수립
② 수립된 정책을 기반으로 한 접속단말 보안평가 실시
③ 평가결과에 의한 접근제어 실시
④ 격리 단말의 치료를 위한 패치 및 백신업데이트 조치
⑤ 단말 상태 변화에 따른 설정과 네트워크 접속 허용
⑥ 지속적인 모니터링 및 대응

NAC를 위한 보안정책은 위 여섯 단계를 반복하며 보완되기 때문에 보안 관리자의 지속적인 관리가 필요하다.

2.2.2 모바일 단말 관리(MDM)

모바일 단말 관리(MDM)는 휴대폰 무선전송 기술(OTA: Over The Air)을 이용하여 원격에서 언제 어디서나 모바일 단말기를 관리할 수 있는 시스템을 말한다[11]. MDM의 원래 사용 목적은 원격에서 모바일 단말기의 응용프로그램 배포, 데이터 및 환경설정 변경, 단말기 분실 및 장치 관리들을 통합적으로 관리하는 것이다. 때문에 중앙 관리 시스템을 통해 직원이 사용하는 모바일 단말기를 관리·통제할 수 있다는 장점이 있어 모바일 오피스에서는 전자우편, 그룹웨어, USB 저장매체와 같은 다양한 통신 채널에 대해 전사적 모니터링 및 통제를 위해 사용되고 있다.

먼저 기업의 보안 관리자는 모바일 단말기의 기능 모듈별 접근제어 정책을 작성하여 MDM 서버를 통하여 사용자의 모바일 단말기로 전송한다. 수립된 정책에 따라 사용자 모바일 단말기의 위성항법시스템(GPS), 마이크, 카메라 기능은 관련된 응용프로그램 실행 시 권한 확인을 통해 실행이 통제되고, 무선랜(Wi-Fi), 테더링(Tethering), USB, SD 카드, 화면 저장 기능은 기능사용이 통제된다.

응용프로그램 실행 통제는 화이트리스트(White List)와 블랙리스트(Black List) 방식이 사용되고 있다. 화이트 및 블랙리스트는 해당 응용프로그램의 이름과 패키지 명을 등록하고 응용프로그램이 실행될 때 패키지 명을 기반으로 실행통제가 이루어진다. 화이트 및 블랙리스트의 사용은 각각 하나만 적용하는 방법과 두 개를 조합하는 방법이 있다. 또한 모바일 오피스에서 사용되는 그룹웨어와 같은 업무용 응용프로그램은 기업의 보안 관리자가 MDM 서버의 스케쥴러에 등록하여 푸시 알람을 통해 사용자에게 배포를 알린다. 사용자가 응용프로그램을 설치하면 MDM 서버로 설치 유무가 전송되며 배포를 통해 설치된 응용프로그램은 화이트리스트에 등록된다.

MDM은 직원 개개인의 모바일 단말기를 원격으로 제어할 수 있어 효과적인 정보보호의 수단이 될 수 있지만 모바일 단말기의 통화기록, 문자메시지, 위치정보와 같은 개인정보가 침해당할 수 있어 논란이 되고 있다[12].

3. 개인정보보호 국내외 연구동향

3.1 모바일 오피스에서 개인정보보호의 개념 및 정의

한국인터넷진흥원(KISA)의 '모바일 오피스 정보보호 안내서'에서는 모바일 오피스 보안위협의 유형을 Table 2와 같이 크게 개인정보침해, 도청, 전자금융사기 및 사이트금융사기, 서비스거부(DoS/DDoS), 권한 탈취, 악성코드 및 해킹, 정보유출로 분류하고 있다[7].

Table 2와 같이 모바일 컴퓨팅 분야에서 개인정보 침해는 공격자가 위치기반서비스(LBS), 카메라, 마이크와 같이 모바일 단말기에 내장된 기능의 사용권한을 획득하여 원격에서 사생활을 감시하는 행위로 한정하고 있다[13,14].

하지만 개인정보는 사회적, 법률적으로 다양하게 정의되고 있으며, OECD 개인정보 가이드라인은 '식별되거나 식별될 수 있는 개인에 관한 모든 정보'라고 개인정보를 정의하고 있다. 또한 국내 개인정보보호법에서 개인정보란 '살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여

Table 2. Mobile Office Security Threat Types

Threat	Contents
Infringements of Privacy	Infringements of location privacy
	Illegal use of hardware resources of mobile device, such as camera and microphone
Tapping	Illegal network packet capture
	Illegal phone-tapping, such as voice and video
Phishing / Pharming	Trying to acquire sensitive information such as user names, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication
	Installing malicious applications with tainted text messages, e-mails and Web links
DoS / DDoS	Battery exhaustion by trying phone call and data transmit request
	Denial of service attack via zombie PC and zombie mobile device
System Authority Acquisition	User authority acquisition by man in the middle attack(MITM)
	SQL injection authentication bypass
	Root authority acquisition by rooting and jailbreaking
	Administrator authority acquisition by buffer overflow attacks
	Session acquisition between mobile device and internal system
Malicious code · Hacking	Cross-site scripting(XSS)
	Unnecessary ports vulnerability
	Reverse engineering
	Used as security policies bypass and attack route by tethering function
	Malicious code propagation via mo-bile device used as a USB removable media
Information Leakage	Internal information leakage by insiders
	Internal information leakage by loss and theft of mobile device
	Internal information leakage saved by mobile device function, such as recording, screen capture, and memo
	Information leakage through rogue AP
	User input information acquisition by keylogger
	Information leakage using vulnerability, such as Bluetooth and Wi-Fi
	Information leakage through install- ing and using unauthorized application
	Information leakage by business process access of unauthorized person

알아볼 수 있는 것을 포함한다)를 말한다.'라고 정의하고 있다. 따라서 모바일 오피스에서 보호해야하는 개인정보란 모바일 오피스 운영자와 사용자의 개인정보를 포함한 모바일 오피스를 운영하는 기업에서 관리하는 개인을 식별할 수 있는 모든 정보를 의미하고, 모바일 오피스 서비스를 통하여 업로드 되는 정보뿐만 아니라, 모바일 오피스를 운영하는 기업에서 수집, 저장, 처리 및 가공을 통해 새롭게 발생하는 모든 정보를 포함한다고 할 수 있다. 만약 개인의 모바일 단말기에서 기업의 정보시스템으로 이동한 개인정보가 사용목적이 달성된 후 삭제되지 않고, 미파기된 정보가 재유통 된다면 개인정보침해는 날로 심각해 질 것이다[15].

모바일 오피스는 기업의 정보자산을 보호하기 위해 네트워크 접근 제어(NAC), 모바일 단말 관리(MDM)와 같은 기술적인 보호조치와 함께 개인의 모바일 단말기를 업무용으로 사용하기 때문에 발생할 수 있는 개인정보침해사고를 막기 위해 관련 법규·정책에 의한 합리적인 통제가 필요하다.

3.2 개인정보보호 국내외 연구동향

3.2.1 개인정보 보호 인증(PIPL)

개인정보 보호 인증(PIPL: Personal Information

Protection Level)은 개인정보보호에 대한 일회성 관리가 아닌 개인정보처리자 스스로 체계적이고 지속적인 유지관리 활동을 촉진할 수 있도록 마련된 기준으로 개인정보보호법의 도입 취지에 따라 개발되었으며, 한국정보화진흥원(NIA)이 인증기관으로서 인증을 수행하고 있다[16].

개인정보 보호 인증은 Table 3과 같이 '개인정보 보호 관리체계'와 '개인정보 보호대책 구현' 2개의 분야로 구성되어 있으며, '개인정보 보호 관리체계' 분야는 PDCA(Plan-Do-Check-Act)의 관점에서 '보호 관리체계의 수립(Plan)', '실행 및 운영(Do)', '검토 및 모니터링(Check)', 그리고 '교정 및 개선(Act)'에 해당하는 총 4개의 통제영역으로 구성되어 있다.

'개인정보 보호대책 구현'은 '개인정보 보호 관리체계'의 수립에 따른 구현을 정의한 것으로 개인정보의 처리단계(수집, 이용 및 제공, 저장, 파기)에 따른 법적 요구사항, 정보주체의 권리보장을 위한 보호대책 구현, 관리적·기술적·물리적 보호대책 구현 총 5개의 통제영역으로 구성되어 있다.

3.2.2 프라이버시 바이 디자인(PbD)

'프라이버시 바이 디자인(PbD: Privacy by Design)'은 캐나다 온타리오주의 개인정보보호위원인 앤 카부키언(Ann Cavoukian) 박사가 처음 주창해 큰 호응을 얻고 있다. 그 개념은 ① 처음부터 '개인정보보호'를 필수 요소로 삼을 것, ② RFID나 생체인식, 데이터 암호화 기술 같은 신기술이나 신상품을 디자인하는 초기 단계에 개인정보보호 기능을 내장할 것, ③ 개인정보의 수집, 저장, 공유, 공개가 연관되는 신기술이나 서비스는 개인정보 생명주기 전체에 걸쳐 관리대책을 세울 것, ④ 개인정보 관리 전반을 투명하게 운영할 것, ⑤ 사용자의 개인정보를 존중할 것 등이며, 이를 바탕으로 개인정보보호를 위한 7대 기본 원칙을 수립하였다[17].

앤 카부키안 박사는 PbD 7대 기본 원칙을 기반으로 하여 2013년 12월 'BYOD: Is Your Organization Ready?'라는 문서를 발표하였고, Table 4와 같이 7가지 점검항목을 제시하고 조직과 개인의 개인정보에 대한 인식을 제고하여 모바일 오피스를 구축할

Table 3. PIPL Control Items

Part	Domain	Contents
Personal Information Protection Management System	1. Establishment of a security management system	• Privacy management plan, Privacy organization, and Assignment of management responsibility
	2. Execution and Operation	• Documentation of protection system, Personal information asset identification, Establishment of risk management plan, Implementation of protection measures
	3. Review and Monitoring	• A review on matching between personal information protection management and implementation of protection system
	4. Correction and Improvement	• A review on periodic improvement status and sharing status of personal information protection management plan
Personal Information Protection measures	5. Personal information processing	• Protection measures for personal information in each processing phase
	6. Guarantee of right for personal information subject	• Processing of request of access, correction, deletion, and stopping processing of personal information subject
	7. Administrative stability measures	• Appointment as CPO, Education and training for personal information protection, Outsourcing management status, Response procedure for personal information leakage
	8. Technical stability measures	• Access control, Logging, and Password policy etc.
	9. Physical stability measures	• CCTV installation and operation, Access control systems etc.

Table 4. PbD BYOD program Readiness/Capability Checklist (Code B = BYOD)

Code	Control	Description
B1	Acceptable Use Policy	Clear and concise definitions and statements of what is allowable on the device, once access to organizational data is permitted. Additionally, this can guide the behaviour of employees, such as incident response personnel and IT teams when dealing with personal devices.
B2	Privacy Policy	Inclusive of mobile device use and behaviour expected from both employees and third parties acting on behalf of the organization
B3	Statement of location of use	Where the devices are expected to be used
B4	Decision on operation model for Mobile Device Management (MDM) - Internal versus outsourced	This will impact who has access to corporate data and personal data
B5	Decision on mobile device camera use	Statement of where and when the camera capabilities of the device are permitted. This can be enforced technically via MDM technologies.
B6	Data classification and extending it to mobile device use	Statement of where and when the camera capabilities of the device are permitted. This can be enforced technically via MDM technologies.
B7	Consideration of Android solutions such as SE Linux, Samsung KNOX, Cisco AnyConnect, Aruba Workspaces, etc.	Recent announcements of elevated security solutions for Android need to be proven in pilot deployments. Where they are successful, they provide strong separation of personal and corporate data.

수 있는 출발점으로 삼고자 하였다. 이 점검항목들은 ① 사용제한정책, ② 개인정보보호정책, ③ 사용 장소의 예상, ④ MDM 운영 모델 결정, ⑤ 모바일 단말기 카메라 사용 여부 결정, ⑥ 모바일 단말기에서 사용 가능하도록 데이터 분류 및 확장, ⑦안드로이드 보안 솔루션 사용고려이며, 최종적으로 모바일 오피스의 개인정보보호를 위한 5단계 프레임워크를 제안, 그 내용은 다음과 같다[18].

첫 번째 단계, 각 사용자의 업무영역, 업무시간, 접근이 허용된 데이터와 정보시스템을 고려하여 요구사항을 정립하고 최종 사용자를 분류

두 번째 단계, 사용자 단말기의 운영체제의 종류에 따라 MDM과 같은 기술의 적용여부가 달라질 수 있고, 업무환경을 무선인터넷으로 구축한다면 사용자의 연결지점과 관리지점이 달라질 수 있으므로 사용할 기술을 선택하고 사용을 허용할 모바일 단말기를 선택

세 번째 단계, 정보시스템뿐만 아니라 조직원을 포함한 조직의 모든 자원에 대해 보안, 개인정보보호 정책을 개발하고, 정책에 대한 배포, 교육, 검토, 모니터링, 시행, 위험 요소 최소화 및 정책 불이행에 대한 조치사항을 수립

네 번째 단계, MDM과 같은 모바일 오피스에 특화된 보안기술 뿐만 아니라 자산관리, 저장소 통제, 네트워크 접근 제어, 권한 설정, 암호 설정과 같은 기존 보안 기술도 함께 적용하고 관리

다섯 번째 단계, 모바일 오피스 최종 사용자들의 분류 및 보안 기술, 보안 정책의 강화로 사용자들의 지원 요청이 증가할 것이므로 초기에 안정적인 업무 수행을 보장하기 위한 절차를 수립하고 지속적으로 관리

4. 모바일 오피스 개인정보 보호 방안

4.1 연구 및 분석 개요

모바일 오피스 보안을 위한 네트워크 접근 제어(NAC)와 모바일 단말 관리(MDM) 솔루션은 기업의 보안 관리자가 수립한 보안정책에 따라 운영되지만, 모바일 오피스를 위한 표준화된 보안정책 및 개인정보보호를 위한 규제방안은 없는 실정이다. 따라서 모

바일 오피스에서 정보보안과 더불어 개인정보를 보호하기 위해 관련 법규·정책에 의한 합리적인 통제, 즉 개인정보를 보호할 수 있는 정책의 가이드라인을 제시하고 이를 인증하는 제도가 필요하다.

또한 국내에서 개발하여 수행하고 있는 인증제도들은 기관 및 기업과 같은 조직의 정보시스템이나 개인정보처리시스템을 대상으로 하고 있어, 사용자 조직 즉, 각 사용자의 모바일 단말기에 초점이 맞춰진 모바일 오피스 개인정보보호 요구사항을 완벽히 만족하지 못하고 있다. 이에 따라 본 논문에서는 국외에서 연구가 진행 중인 모바일 오피스 개인정보보호 이슈 및 요구사항과 NIA-PIPL과의 비교·분석을 통하여 모바일 오피스에 특화된 프레임워크를 제안하고자 한다.

4.2 모바일 오피스 개인정보 보호 인증(M-PIPL) 프레임워크

Fig. 3은 본 논문에서 제안하는 모바일 오피스 개인정보 보호 인증(M-PIPL) 프레임워크이다. M-PIPL 프레임워크는 '개인정보 보호 관리체계'에 PbD 모바일 오피스의 개인정보보호를 위한 5단계 프레임워크를 적용하여 '요구사항 정립-적용 기술 선택-정책 개발-보안-지원'의 단계를 거치며, '개인정보 보호대책'은 NIA-PIPL의 '개인정보 보호대책'을 적용하여 개인정보 처리, 정보주체 권리보장, 관리적·기술적·물리적 확보조치로 이루어져 있다.

M-PIPL은 PIPL의 2개 분야를 유지하되 '개인정보 보호 관리체계'를 모바일 오피스에 맞춰 변경함으로써 기관 및 기업과 같은 조직의 모바일 오피스 개인정보보호 요구사항을 충족시킬 수 있으며 '개인정보 보호대책'은 '개인정보 보호 관리체계'의 수립에 따른 구현을 정의한 것이기 때문에 관리체계 5단계를 반복수행하며 보호대책을 강화할 수 있다. M-PIPL의 통제 영역은 Table 5와 같다.

4.3 제안 프레임워크의 특징

본 논문에서 제안한 M-PIPL 프레임워크는 다음과 같은 특징을 가지고 있다.

첫째, 다수의 사용자를 제어하고 개인정보 침해 경로를 식별하기 위해 각 사용자가 접근 가능한 데이터, 정보시스템 및 요구사항을 정립한 후 최종 사용자를 분류·관리하므로 모바일 오피스를 구축한 조직이 소유하고 있는 개인정보 유출 예방대책을 수립할 수 있다.

둘째, 사용자의 요구사항을 수렴하여 사용자의 모바일 단말기와 무선네트워크 접속을 제어할 기술을 선택할 수 있어 기술 적용 시 사용자의 반발을 최소화 할 수 있고, 개인정보에 접근하는 경로와 모바일 단말기가 한정되므로 모바일 오피스 운영자가 효율적인 개인정보 보호 활동을 할 수 있다.

셋째, 모바일 오피스 운영 현황에 따라 개인정보 보호 정책을 개발하여 운영자와 사용자가 개인정보에 접근, 활용 시 지켜야 할 가이드라인을 제시할 수 있고, 주기적인 교육과 검토를 통하여 개인정보보호 인식이 제고되어 개인정보 침해사고 예방효과를 높일 수 있다.

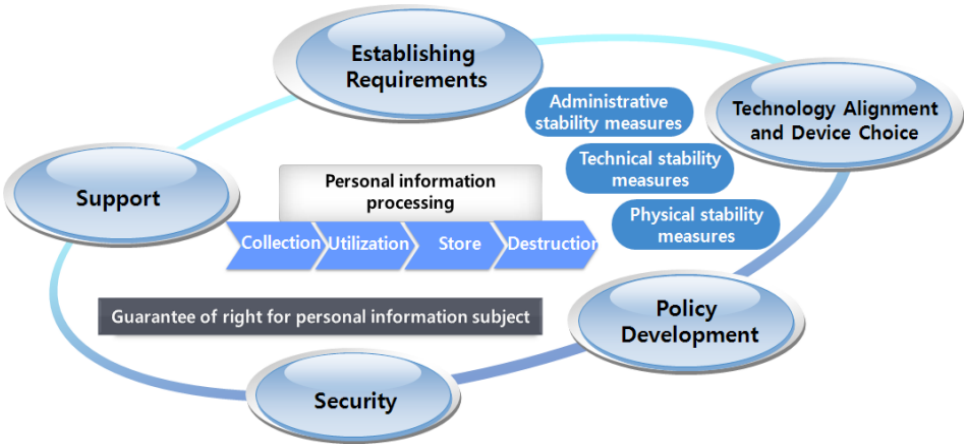

Fig. 3. M-PIPL Framework.

Table 5. M-PIPL Control Items

Part	Domain	Contents
Personal Information Protection Management System	1. Establishing Requirements	• Job criticality, time sensitivity, value derived from mobility, data access, and systems access
	2. Technology Alignment and Device Choice	• MDM option(asset management, ncryption, password policy, remote lock/wipe, and email/Wi-Fi/VPN configuration), virtual desktop computing infrastructure (VDI), WLAN device connectivity
	3. Policy Development	• Information security concerns, data protection concerns, confidentiality issues, ownership issues, information regarding any tracking/monitoring, guidance regarding how to assess the security of Wi-Fi networks, and acceptable and unacceptable behaviour
	4. Security	• Asset and identity management, local storage controls, removable media controls, network access levels, network application controls, corporate vs. personal app controls, permissions, authentication, password settings, move, add and change management, device health management, unauthorized usage alerts, data loss prevention, and web and messaging security
	5. Support	• Potential on-site support and same day or 24-hour device replacement, based on their location
Personal Information Protection measures	6. Personal information processing	• Protection measures for personal information in each processing phase
	7. Guarantee of right for personal information subject	• Processing of request of access, correction, deletion, and stopping processing of personal information subject
	8. Administrative stability measures	• Appointment as CPO, Education and training for personal information protection, Outsourcing management status, Response procedure for personal information leakage
	9. Technical stability measures	• Access control, Logging, and Password policy etc.
	10. Physical stability measures	• CCTV installation and operation, Access control systems etc.

넷째, 제안 프레임워크는 PIPL의 기본 형식을 따르고 있어 모바일 오피스를 운영하는 조직이 PIPL을 도입할 때 관련된 통제 영역을 연계할 수 있다.

5. 결 론

스마트시대로 빠르게 접어들며 일상적인 개인의 생활환경뿐만 아니라 업무환경도 모바일 환경으로 변화하고 있다. 모바일 오피스로 변화하는 업무환경을 안전하게 정착시키기 위해 먼저 개인의 모바일 단말기를 업무에 활용할 때 발생하는 보안문제를 해결해야 하며, 그 중 개인정보보호는 기업의 사활을 좌우할 수 있는 핵심 보안문제로 우선적으로 고려해야할 요소이다. 하지만 국내 모바일 오피스에 대한 인식 및 보안 관련 연구 활동은 현재 가시화 되고 있는 일부 서비스 및 기술을 제외하고는 대부분이 여전히 초기단계이며 모바일 오피스 보안과 관련한 표준 및 전문 인력이 부족한 실정이다.

모바일 오피스를 도입하지 않은 기업에서도 개인이 소유한 모바일 단말기로 업무를 수행할 수 있기 때문에 모바일 오피스를 운영하는 기업뿐만 아니라 모든 조직은 정보자산과 개인정보를 보호하기 위한 끊임없는 노력이 필요하다. 국내 모바일 단말기 제조기술 및 공급 속도를 고려했을 때 대부분의 기업들이 모바일 오피스를 도입하여 운영할 것으로 전망되지만 모바일 오피스 운영에 앞서, 보안문제들을 인지하

고 예방할 수 있도록 합리적인 정책을 마련하고 보안 체계를 구축하고 전담할 수 있는 전문 인력 또한 양성해야 한다.

더불어 국외 선진 사례 및 연구 등을 통해 제시된 모바일 보안위협과 개인정보보호 요구사항을 국내 환경에 맞게 적절히 구현하여 모바일 오피스의 안전한 운영을 도모해야 한다. 국내외 개인정보보호 정책과 연구를 비교, 분석하여 정책의 가이드라인을 제시하고 모바일 오피스 개인정보보호와 관련한 연구 및 투자가 이루어져야 한다. 향후에는 모바일 클라우드 컴퓨팅을 고려하여 모바일 컴퓨팅 보안과 클라우드 컴퓨팅 보안의 위협요소를 분석하고 클라우드 서비스 사업자에게 요구되는 개인정보보호 방안과 연계하는 연구가 필요하다.

REFERENCE

[1] MSIP, *Wireless Communication Services Statistics*, 2014.

[2] R. Ballagas, M. Rohs, J. Sheridan, and J. Borchers, "Byod: Bring Your Own Device," *Proceeding of the Workshop on Ubiquitous Display Environments at International Conference on Ubiquitous Computing*, pp. 6-13, 2004.

[3] J. Shim, D. Mittleman, R. Welke, A. French, and J. Guo, "Bring Your Own Device (BYOD): Current Status, Issues, and Future Directions," *Proceeding of the Nineteenth Americas Conference on Information Systems*, pp. 1-20, 2013.

[4] A. Scarfo, "New Security Perspectives around BYOD," *Proceeding of the 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications*, pp. 446-451, 2012.

[5] S. Park and J. Lee, "Propulsion Systems and Practices for Smart Work," *Information & Communications Magazine, The Korean Institute of Communications and Information Sciences*, Vol. 29, No. 12, pp. 3-9, 2012.

[6] Gartner, Gartner Identifies the Top 10 Strategic Technology Trends for 2015, http://www.gartner.com/newsroom/id/2867917 (accessed Dec., 10, 2014)

[7] KISA, *Information Security Guide for Mobile Office*, 2013.

[8] KISA, *Information Manual for Introduction and Operation of Secure Mobile Office*, 2012.

[9] Wikipedia, Network Access Control, http://en.wikipedia.org/wiki/Network_Acce ss_Control (accessed Dec., 13, 2014)

[10] L. Orans and M. Nicolett, "Gartner's Network Access Control Model," *Gartner IT Security Summit,* 2005.

[11] K. Rhee, W. Jeon, and D. Won, "Security Requirements of a Mobile Device Management System", *International Journal of Security and Its Applications*, Vol. 6, No. 2, pp. 353-358, 2012.

[12] The Kyunghyang Shinmun, *POSCO, Outsourcing Employees 'Cyber Inspectors' Controversy*, 2013.

[13] N. Fernando, S. Loke, and W. Rahayu, "Mobile Cloud Computing: A Survey," *Future Generation Computer Systems*, Vol. 29, No. 1, pp. 84-106, 2013.

[14] H. Dinh, C. Lee, D. Niyato, and P. Wang, "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches," *Wireless Communications and Mobile Computing*, Vol. 13, No. 18, pp. 1587-1611, 2013.

[15] N. Moon, S. Yong, J. Oh, and T. Cho, "A Study on Privacy for the Services in Digital Convergence," *Journal of Korea Multimedia Society*, Vol. 10, No. 4, pp. 24-32, 2006.

[16] NIA, *Personal Information Protection Level Guide*, 2013.

[17] 7 Foundational Principles, http://www.privacybydesign.ca (accessed Jan., 30, 2015.)

[18] PbD, *BYOD: (Bring Your Own Device) Is Your Organization Ready?*, 2013.

박 용 준

2006년 전남대학교 컴퓨터정보학부 이학사
2010년 전남대학교 정보보호협동과정 이학석사
2014년~현재 제주대학교 전산통계학과 박사과정
2014년~현재 정보통신기술연구원 선임연구원
관심분야 : 개인정보보호, 정보보호관리체계, 침입탐지

이 윤 정

2002년 고려대학교 컴퓨터학과 이학박사
2004년 9월~현재 제주대학교 전산통계학과 부교수
관심분야 : 네트워크 보안, 유무선 통신 보안, 정보보안