情報保護學會論文誌
第20卷 第6號, 2010. 12

스마트폰 이용 환경에서 국가기관 정보보호 관리방안

김 지 숙,† 임 종 인‡
고려대학교 정보경영공학전문대학원

National Institution's Information Security Management on the Smart phone use environment

Ji-sook Kim,† Jong-in Lim‡
Korea University, Graduate School for Information Management Engineering

요 약

우리사회의 급격한 스마트폰 확산은 개인생활 뿐만 아니라 조직의 업무 환경을 바꾸고 있다. 특히 스마트폰은 애플리케이션을 누구나 개발하고 사용할 수 있는 특성으로 인해 타산업과의 융합이 촉진되는 등 사회의 디지털 패러다임을 변화시키고 있다. 정부도 스마트폰 환경에 맞는 대국민서비스 향상과 국민과의 소통을 위해 '모바일 전자정부' 구축을 추진하고 있다. 하지만 스마트폰에 대한 보안위협이 급증하고 있어 이에 대한 대책을 마련하지 않으면 모바일 전자정부 활성화에 장애가 될 수 있다. 본 논문에서는 국가기관의 안전하고 효율적인 모바일 환경 구축을 위해 필요한 정보보호 방안과 이를 체계적으로 관리하기 위한 모바일 전자정부 정보보호관리체계(ISMS)를 제시하고자 한다.

ABSTRACT

The rapid spread of smart phone in recent years changes not only personal life but also work environment of organizations. Moreover, smart phone provoke service combination between industries and transit the digital paradigm in our society because of the character that anyone can develop or use the application of smart phone. Under these circumstances, the government hastens the construction of mobile-government in order to improve national services and communication with people. However, since security threats on smart phone become more critical recently, we should hurry the counter measures against mobile threats or we will face obstacles to the activation of mobile-government. On this article, we suggest the methods of information security and the Mobile-government Information Security Management System(M-ISMS) on the smart phone use environment for building up the secure and convenient mobile system in the national institution.

Keywords: smart phone, mobile office, mobile security threats, mobile-government information security management system

I. 서 론

최근 정보환경의 가장 큰 변화는 아이폰 출시를 계기로 전개되고 있는 스마트폰 확산이다. 스마트폰은 단순히 핸드폰이 아니라 '손안의 PC'로서의 기능을 하고 있으며 애플리케이션을 마음대로 이용할 수 있음에 따라 이와 관련된 새로운 서비스가 끝없이 창출되고 있다. 이러한 추세는 스마트폰이 금융, 교육, 교통, 의료 등 타산업 분야와 융합되어 사회 전반에 새로운 IT 혁명을 유도하고 있다. 이에 정부도 스마트폰을 이용한 '모바일 전자정부'를 구축하여 언제 어디서나 대국민 서비스를 제공하고 소프트웨어와 콘텐츠 산업 등 IT산업 성장을 견인하여 국가경쟁력을 제고하고자 한다. 하지만 최근 스마트폰에 영향을 미치는 악성코드가 지속 발생하고 있어 안전한 스마트폰 이용을 저해하고 있다. 특히 스마트폰을 이용하여 모바일 전자정

접수일(2010년 8월 19일), 수정일(2010년 11월 2일), 게재확정일(2010년 12월 10일)
† 주저자, scales12@korea.ac.kr
‡ 교신저자, jilim@korea.ac.kr

부를 구축할 경우, 외부에서도 내부 네트워크에 접근이 가능하게 됨에 따라 국가기관이 보유하고 있는 국가기밀이나 국민들의 개인정보, 중요 정책정보 등이 유출되어 국가안보 위협이나 국민의 재산, 생명에 위해가 발생할 수도 있으며 악성코드에 감염된 스마트폰이 PC동기화 되어 국가기관 운영 네트워크가 감염되면 국가시스템 안전성에 문제가 발생할 수도 있는 등 개인이나 사기업의 네트워크 피해와는 비교가 안 될 정도의 심각한 피해가 발생할 수 있다. 따라서 국가기관에서 스마트폰을 이용하여 모바일 전자정부를 구축할 경우에는 정보보호에 더 많은 관심과 노력을 기울여야 한다.

본 논문에서는 스마트폰 확산에 따른 변화와 이에 수반되는 정보보호 위협요인을 살펴보고 스마트폰을 활용한 모바일 전자정부에서 요구되는 정보보호 방안과 이를 체계적으로 관리하기 위한 모바일 정보보호관리체계를 제시하고자 한다.

II. 최근 정보통신 환경 변화

2.1 이동통신(Mobile telecommunication)의 발전

이동통신(mobile communications)이란 보행자, 자동차, 열차, 선박, 항공기 등과 같은 이동체를 대상으로 하는 통신으로 통신 상대방중 한쪽 또는 양쪽 모두가 움직이고 있는 경우 즉, 이동체와 고정된 지점간 또는 이동체 상호간을 연결하는 통신방식이다.

케이블이나 광케이블 등의 전송로를 사용하지 않고 전파를 통하여 정보를 교신하는 무선통신은 1897년 마르코니(G. Marconi)가 무선전신을 개발한 이래 무선전화, 방송, 팩시밀리, 데이터통신, 레이더, 텔레미터링(원격측정장치) 등으로 그 범위가 확장됐으며 전자관, 반도체소자의 발명에 힘입어 획기적인 발전을 이룩하였다.

무선통신에는 무전기, 이동통신, 주파수공용무선통신시스템, 위성전화와 같은 음성정보 전달을 주요 목적으로 하는 통신과 무선인터넷, 와이브로(Wireless Broadband Internet), HSDPA(High Speed Downlink Packet Access)와 같은 데이터정보 전달을 주요 목적으로 하는 통신이 있다. 최근에는 음성정보와 데이터정보가 통합되는 경향이다. 특히 일반인이 가장 많이 사용하는 이동통신인 휴대폰(Mobile phone)은 최근 10년간 비약적인 발전을 하여 왔으며 고기능 스마트폰의 등장으로 통신 환경이 모바일 중심으로 대체되고 있다. 이에 따라 스마트폰은 모바일통신의 한 종류지만 모바일통신을 대표하는 것으로 인식되고 있다[1].

2009년 애플의 아이폰이 폭발적인 반응을 얻으면서 이동통신 시장은 스마트폰으로 급격히 대체되고 있다. 시장조사업체 IDC(International Data Corporation) 분석에 의하면 2010년 1/4분기 세계 스마트폰 판매량은 5,470만대로 2009년 동기 3,490만대에 비해 56% 가량 성장한 것으로 나타났으며[2] 리서치 전문업체 가트너(2009)는 2012년에는 세계 휴대전화 가입자 10명 중 4명이 스마트폰을 사용할 것이라고 전망하였다[3]. 우리나라도 2009.11월 아이폰이 출시되자마자 한 달 만에 20만 명이 가입하면서 국내 스마트폰 시장에 열풍이 불더니 2010.6월 말 스마트폰 사용자는 247만 명에 육박하고 있다. 업계에서는 스마트폰 사용자가 금년 말 약 490만 명에 이르며 2012년에는 약 1,700만 명이 스마트폰을 사용할 것이라고 전망하고 있다[4].

스마트폰이란 기존 휴대폰보다 향상된 기술과 기능을 가진 새로운 타입의 휴대폰으로 컴퓨터와 성능이 비슷한 고성능 범용운영체제(OS)를 내장하고 있다. 즉 스마트폰은 이동통신 전화기에 OS가 탑재된 것으로 PDA (Personal Digital Assistants) 기능이 가능하고 휴대용 학습기, 일정관리, 주소록 관리, 내비게이션, E-북, 카메라, MP3, 동영상재생기, 전자사전 등의 기능 구현이 가능한 멀티 정보통신 기기이다. 스마트폰이 기존 휴대폰(일명 피쳐폰)과 구별되는 가장 큰 특성은 응용 프로그램의 개방성이다. 사용자가 원하는 애플리케이션과 UI(User Interface)를 자유롭게 선택하고 설치 및 삭제가 가능하다. 또 프로그램 구동 및 데이터 통신, PC연동 등의 기능 구현이 가능한 고기능 이동통신 단말기이다. 스마트폰과 일반 휴대폰(일명 피쳐폰)의 특징을 비교하면 [표 1]과 같다.

[표 1] 일반 휴대폰과 스마트폰 특징 비교

일반 휴대폰(피쳐폰)	스마트폰
· 음성중심 서비스 지원 · 고성능 카메라, MP3, 멀티미디어 지원 기능 · SMS, MMS 위주 · 개방성 프로그램 애플리케이션 설치 불가 · 휴대폰 제조사별 폐쇄된 운영체제 지원 · Wi-Fi 기반 호스트만 접속 가능	· Wi-Fi, 블루투스 지원가능 · 풀 브라우징 서비스 지원 · Multi tasking 지원 · 제 3자 개발 애플리케이션 설치 및 사용 가능 · 리눅스, 윈도우 모바일 등의 범용 OS 사용 · 터치스크린 위주 지원

2.2 스마트폰 확산에 따른 변화

스마트폰이 생활을 바꾸고 있다. PC를 켜지 않아도 전자우편을 보내고 TV를 보면서 인터넷 검색을 즐기고 전자책을 읽으며 영화 감상은 물론 온라인 쇼핑과 주식거래도 한다. PC보다 더 편하고 더 자유롭다. 이를 두고 한편에서 '웹의 시대가 끝나고 모바일 유비쿼터스 시대가 열렸다'고 말하기도 한다. 디지털 패러다임에 변화가 오고 있다는 것이다[3].

그동안 이동통신 산업은 통신 사업자가 주도하는 폐쇄적인 공간에서 운영되었으나 이제는 구글의 안드로이드와 같은 범용 운영체제가 탑재된 스마트폰이 확산되고, 통신 사업자의 비싼 데이터통신망이 아닌 Wi-Fi와 같이 비용이 수반되지 않는 데이터 통신이 가능하게 되었으며, 통신 사업자의 사전승인 없이도 애플리케이션을 자유롭게 유통시킬 수 있는 개방형 앱 시장이 등장함에 따라 소비자 중심의 유통구조로 전환되고 있다[5].

이러한 IT 환경 변화는 개방을 통한 혁신을 불러일으켜 모바일시장이 활성화되는 계기를 제공할 것이다. 또한 오픈마켓 공간은 소프트웨어 및 콘텐츠 거래에 대한 새로운 수익모델을 제시하여 관련 산업을 활성화시킬 것이다. KT경제경영연구소는 [표 2]에서 보듯이 2010~2012년간 스마트폰에 의한 무선데이터 시장이 11조원으로 확대될 것이며 소프트웨어 및 콘텐츠 산업도 5조원의 시장이 열리고 2만 6천개의 일자리가 창출될 것으로 분석하고 있다[4].

스마트폰이 이처럼 IT 패러다임을 변화시키는 것은 단말기 하나로 정보를 습득하고 업무를 수행하며 사회적 관계를 형성하고 여가를 활용하는 등 단순한 핸드폰을 넘어 활용가치를 높여주는 방대한 애플리케이션에 기인한다. 나아가 이 애플리케이션이 오픈마켓을 통해 유통됨으로써 소비자에게 새로운 경험을, 개발자에게 새로운 비즈니스 창출 기회를 제공하고 있다. 애플리케이션 전문 개발업체 터치커넥트에 따르면 2010.5월 애플 앱스토어에 등록된 국내 아이폰 앱은 5,501개에 이르고[6] 특허청에 등록된 스마트폰 관련 특허 출원도 2007년 185건에 불과하던 것이 2008년 369건, 2009년 491건으로 해마다 급증세를 보이고 있는데 최근 5년간 1,637건의 특허출원 중 애플리케이션 관련 출원이 62.9%를 차지하고 있다[7].

[표 2] 스마트폰의 경제적 파급효과

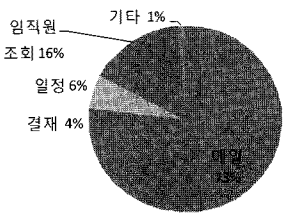
년 도	2010년	2011년	2012년	합계
무선데이터시장 (단위 : 억원)	22,673	38,556	48,833	110,062
콘텐츠·SW시장 (단위 : 억원)	8,129	16,672	24,817	49,618
일자리 창출 (단위 : 개)	6,336	8,669	11,626	26,631

스마트폰 서비스는 이미 다양하게 제공되고 있다. 은행과 증권사는 스마트폰을 통한 모바일 뱅킹과 주식매매 서비스를 시행하고 있으며 항공사는 스마트폰에서 탑승수속을 할 수 있는 모바일 서비스를 제공하고 있다. 방송사는 24시간 업데이트된 뉴스를 무료로 볼 수 있는 모바일 실시간 뉴스 서비스를 제공하고 있으며 병원에서는 스마트폰을 이용해 환자를 진료하고 있다. 한편 스마트폰을 이용한 E-learning도 활성화되고 있으며 스마트폰으로 인터넷 전화를 사용하는 모바일 인터넷전화도 인기를 끌고 있다.

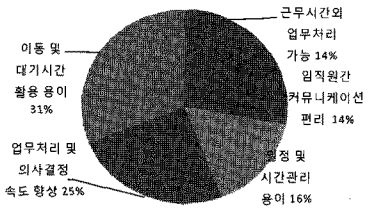
스마트폰 확산의 또 다른 변화는 모바일 비즈니스로 조직의 업무환경이 재편되고 있는 것이다. 기업과 공공부문은 운영비 절감 및 생산성 향상을 위해 스마트폰을 이용한 모바일 오피스 구축을 서두르고 있어 '이동형 사무실 시대'가 열리고 있다. 삼성경제연구소가 2010.5월 CEO 447명 대상 실시한 설문조사에서 모바일 오피스 구현을 시작한 기업이 39.2%이며 3년내 도입하겠다는 응답도 32.2%에 달하고 있다[4]. 이에 따라 모바일 오피스 시장은 2009년 2조 9천억원의 시장 규모에서 2014년 5조 9천억 원으로 증대될 것으로 예상하고 있다[8].

삼성SDS가 모바일오피스 사용자 대상 설문조사한 바에 의하면 모바일오피스 시스템을 구축한 기업에서는 [그림 1]과 같이 메일, 결재, 일정, 임직원 조회, 명함 등에 활용하고 있으며 [그림 2]에서처럼 모바일 오피스 구축으로 인해 이동 및 대기시간 절감(31%), 업무처리 및 의사결정 속도 향상(25%) 등의 효과가 있는 것으로 나타났다[9].

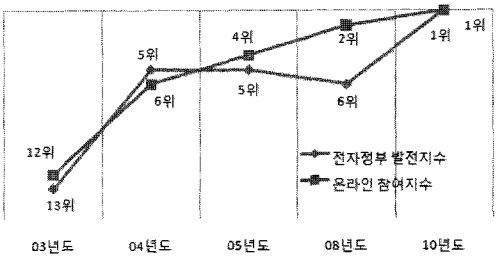
일례로 도시철도공사는 전 직원에게 모바일 단말기를 지급하여 시설물 유지관리 업무를 실시간으로 처리



[그림 1] 모바일 오피스 활용도



〔그림 2〕 모바일 오피스 효과



〔그림 3〕 우리나라 전자정부 수준 추세 변화

한 결과 시설점검 소요시간이 1시간에서 28분으로 단축되는 등 생산성과 업무효율성이 향상되어 5년간 비용의 40배가 넘는 효과가 날 것으로 예상하고 있다〔10〕. 또 포스코는 스마트폰을 이용해 공장을 관리하는 '스마트 팩토리'를 구축하였으며 코오롱, SK 등에서는 그룹 전체가 모바일 오피스를 도입 중으로〔11〕 이러한 움직임은 협력사로까지 확대되어 산업 전반의 생산성 향상이 이루어질 것으로 기대되고 있다.

2.3 국가기관 모바일 전자정부 구축 배경 및 실태

우리나라는 1987년 행정전산망사업을 시작으로 1990년대 초 정부부처 정보화사업 등 전자정부 사업을 추진하여 2002.11월 대한민국 전자정부 포털사이트(www.egov.go.kr) 서비스를 시작하였다.

전자정부는 정보통신 기술을 활용하여 행정기관의 사무를 전자화함으로써 행정기관 상호간 또는 국민에 대한 행정업무를 효율적으로 수행하는 정부〔12〕로 행정의 효율성과 투명성을 높이고 국민이 원하는 정보와 서비스를 언제 어디서나 이용할 수 있으며 국정운영 과정에 국민의 참여기회를 확대하는 역할을 수행해왔다. 전자정부 사업 중 전자민원서비스사업은 전자정부 구현을 위한 핵심사업 중 하나로 국민들은 언제 어디서나 원하는 정보를 얻을 수 있고 각종 민원을 인터넷으로 해결할 수 있게 되었다.

인터넷 민원서비스 이용실적은 2004년 연간 175만 건에서 2009년 2,571만 건으로 무려 15배 가까이 증가하였으며 행정정보 공유 이용실적은 2004년 일평균 1만 9천 건에서 2009년 17만 7천 건으로 9배 이상으로 급증하였다〔13〕. 2010.5월 현재 인터넷으로 가능한 민원은 전체 약 5,000종의 민원업무 중 35%에 해당하는 총 1,800종에 이른다. 우리나라는 지난 30년간 정보통신 인프라를 세계 최고수준으로 끌어올려 〔그림 3〕에서처럼 전자정부 수준이 꾸준히 향상되어 왔으며 2010.1월 발표된 UN의 전자정부 평가에서 전자정부 발전수준을 측정한 '전자정부 발전지수'와 온라인을 통한 시민의 공공행정 참여도를 측정한 '온라인 참여지수' 모두 192개국 중 1위로 평가되었다〔14〕.

이처럼 전자민원 서비스 이용이 활성화 되는 가운데 최근 스마트폰 보급 및 확산으로 개인이 이용하는 생활서비스와 조직의 업무환경이 모바일 기반으로 변화되고 스마트폰 환경이 이동성, 개방성, 다양성을 제공하자 국민들도 스마트폰을 활용하여 민원서비스를 받고자 하는 수요가 높아졌다. 정부도 정보통신 환경 변화에 부응하여 언제 어디서나 중단 없는 대국민서비스를 제공하는 한편 빠른 의사결정, 실시간 대응 등 공무원의 업무 효율 향상을 위해 스마트폰을 활용한 '모바일 전자정부' 구축이 필요하게 되었다.

모바일 전자정부는 공공서비스 수혜지역을 확대시키고 전자정부 접근성을 향상시키며 민원 행정 등 대국민서비스를 이동 중에도 이용할 수 있고 정보공유, 참여·소통의 수단으로도 활용 가능하기 때문에 '국민중심의 공공서비스'가 가능하다. 또한 원격근무, 이동근무 등 공무원의 업무방식을 모바일로 전환하여 업무생산성을 향상시킬 수 있으며 위치정보, 증강현실(AR: Augmented Reality)기술 등과 결합하여 새로운 형태의 융합형 공공서비스도 실현할 수 있다〔15〕. 국가차원에서도 모바일의 확산은 신규시장 창출에 따른 일자리창출과 함께 네트워크, 서비스, 콘텐츠 및 소프트웨어 등 IT산업 전반의 성장을 견인하여 국가경쟁력을 높이고 유선 IT 인프라에 비해 상대적으로 미흡한 우리나라의 차세대 무선 인프라를 선도하여 IT강국으로 재도약할 수 있는 기회가 됨에 따라 '모바일 전자정부' 활성화는 우리나라가 꼭 달성해야 할 핵심 전략이다.

행정안전부가 2010.6월 실시한 '모바일정부 추진현황 및 수요조사' 결과에 의하면 현재 법제처에서 법령·판례 등 총 23만여 건의 국가법령 정보를 제공하는 '국가법령 정보센터'를 운용중이고 행정안전부는 육교, 횡단보도, 지하도 등을 표시한 도보지도를 구축하여 취약계층 대상 맞춤형 도보안전 종합서비스인 '생활 공

감 지도'를 제공하고 있으며 경기도는 맛집, 문화·숙박시설 등 주요 문화관광 콘텐츠 1,000여건을 '경기투어'를 통해 서비스하고 있다. 또 산림청은 '실시간 산불현장 대응시스템'을 구축중이고 기상청은 기상재해 등 비상상황에 신속 대처하기 위해 '모바일 기상상황 조회시스템'을 운용할 예정으로 있는 등 7개 기관이 26개 서비스를 제공 또는 구축중이며 국토해양부의 '자동차 관리정보 서비스' 등 22개 기관 57개 서비스가 구축을 추진할 계획이다[16].

III. 스마트폰 이용 환경에서의 정보보호 위협

3.1 스마트폰 보안 위협

3.1.1 스마트폰 보안 위협

무선통신은 유선보다 보안에 취약하다. 같은 무선통신이지만 스마트폰은 일반 휴대폰에 비하여 플랫폼(H/W, S/W), 네트워크, 애플리케이션, 단말기 측면에서 보안에 더 취약한 특성을 가진다. 기존 휴대폰에서는 이동통신사업자의 통제 하에 제한된 망과 애플리케이션만이 사용 가능하여 정보보안 측면에서는 긍정적인 영향을 미쳤다. 그러나 스마트폰의 경우 소스가 공개된 범용 운영체제이거나 API(Application Programming Interface)가 제공되는 경우가 많기 때문에 정보침해자 입장에서는 바이러스나 웜을 통한 해킹이 용이하다. 또 사용자들이 스마트폰 출시 시에 탑재되어 있는 제조사 펌웨어 소프트웨어를 변조하여 아이폰의 Jailbreak(탈옥), 안드로이드폰의 경우 Rooting, 윈도우모바일은 Security Off 시킬 경우 Unlock 공격이나 키보드 해킹도 가능하다. 더욱이 미국 저작권사무국이 2010.7월 '디지털 밀레니엄 저작권법(DMCA)'을 개정하여 스마트폰 사용자들이 통신사업자 변경이나 애플의 사전승인 없이 애플리케이션을 설치할 경우 합법적으로 기기의 '락(Lock)'을 풀 수 있도록 스마트폰 '탈옥'을 합법화함에[17] 따라 스마트폰에 대한 해킹이 더욱 증가할 것으로 예상된다. 네트워크 측면에서도 기존 휴대폰은 이동통신사의 전용망만을 사용함으로써 유해한 트래픽은 사전에 차단되었다. 그러나 스마트폰은 전용망 외에도 Wi-Fi, 블루투스 등 멀티 네트워크 접속이 가능하므로 도청·변조나 DoS 공격 등이 가능하다. 스마트폰의 가장 큰 특징인 개방형 애플리케이션 역시 보안측면에서는 위험에 노출되어 있다. 기존 휴대폰은 이동통신사 전용

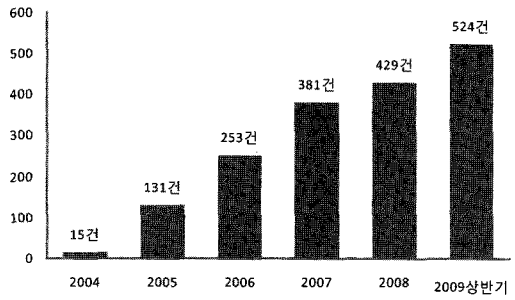
〔표 3〕 스마트폰 보안위협 유형

분류	공격유형	공격방법
플랫폼 공격	○바이러스/웜 ○시스템 Unlock ○키보드 해킹	○WiFi/블루투스/Web 이용 전파 ○PC 동기화 ○Jailbreak(iPhone), Rooting(Android), Security Off(WM) ○플랫폼 취약점 ○Rootkit(백도어, 트로이 목마 등 해킹기능 프로그램)
네트워크 공격	○WiFi 도청/변조 ○DoS 공격	○WiFi/ 블루투스 네트워크 공격
애플리케이션 공격	○Malicious App. ○Fishing App.	○Web 다운로드 ○PC 동기화
단말기 공격	○도난 및 분실 ○Malicious App.	○도난 및 분실 ○이동 저장매체 감염

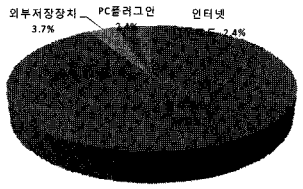
콘텐츠를 사용하기 때문에 보안 측면에서 안전성이 높았다. 그러나 스마트폰의 경우 오픈마켓 앱 스토어의 등장으로 콘텐츠의 양적·질적 성장을 이루었으나 정보침해자들이 악성코드 내장 프로그램이나 피싱 애플리케이션을 앱 스토어에 업로드하고 사용자들이 이를 다운로드할 경우 바이러스나 웜 등 악성코드가 전파되거나 PC 동기화를 통해 내부 네트워크에도 전염될 수 있다[18][19]. 스마트폰도 기존 휴대폰처럼 단말기 도난이나 분실시 단말기 내에 저장된 개인정보나 조직의 정보가 유출되고 이메일이나 SMS로 단말기에 악성 앱이 유포될 수 있다. 나아가 스마트폰은 키보드 입력이 어려움에 따라 자동 로그인 기능과 4자리 숫자 등 단순한 패스워드만을 사용할 수 있어 보안위협이 가중되고 있으며 낮은 메모리와 배터리 소모 문제로 보안 소프트웨어 사용에 한계가 있을 뿐만 아니라 이러한 특성 때문에 보안패치도 어렵고 자동업데이트도 되지 않아 보안위협에 대한 대처도 그만큼 어렵다. 더군다나 스마트폰의 종류가 다양하고 제조사별로 각기 다른 플랫폼을 사용하고 있어 단일 보안시스템을 적용할 수도 없다[20]. 스마트폰 보안 위협은 〔표 3〕과 같이 정리할 수 있다.

3.1.2 스마트폰 악성코드

스마트폰 관련 보안위협 중 가장 발생빈도가 높고 피해가 큰 위협이 악성코드에 의한 것이다. 한국인터넷진흥원 보고서에 의하면 〔그림 4〕에서 보듯이 전세



〔그림 4〕 전세계 모바일 악성코드 발생 건수



〔그림 5〕 전세계 모바일 악성코드 감염 경로

계 모바일 악성코드 발생 건수가 매년 증가하고 있다. 악성코드의 감염경로는 〔그림 5〕에서처럼 인터넷을 통한 악성코드 보다는 대부분 블루투스를 통해 유입되고 있으며 MMS에 의한 감염도 24.4%나 차지하고 있다. 이렇게 감염된 악성코드는 개인정보를 유출시키고 요금이 부당하게 청구되거나 단말기 이용이 제한되는 등의 피해를 입히고 있다〔21〕.

우리나라에서도 윈도기반 '옴니아'에 무단으로 국제전화를 걸어 요금을 발생시키는 "트레드 다이얼" 악성코드가 2010.4월 발견된 이래 약 155건의 악성코드가 발견되었으며〔22〕 개방형OS를 사용하는 안드로이드폰인 모토로라의 모토로이에 사용자 몰래 설치되어 데이터 용량을 대량으로 소비하는 악성코드가 발견〔23〕되는 등 스마트폰 보안위협이 현실화되고 있다.

2010.4월 현재 스마트폰과 관련된 악성코드는 600여 종이 보고되었으며 그 숫자는 계속 증가하고 있다. 스마트폰에서 발견된 악성코드 유형으로는 기기사용을 불가능하게 만들거나 장애를 유발하는 '단말기 장애 유발형 악성코드', 단말기 전력을 지속적으로 소모시켜 배터리를 고갈시키는 '배터리 소모형 악성코드', 단말기의 메시지 서비스나 전화 통화를 지속적으로 시도해 요금을 발생시키는 '통신요금 발생형 악성코드', 감염된 단말의 정보나 사용자 정보를 외부로 유출시키는 '정보유출형 악성코드', 모바일 단말을 통해 PC를 감염시키는 '크로스 플랫폼형 악성코드'가 있다. 스마트폰

〔표 4〕 스마트폰 주요 악성코드 현황

구분	발견 시기	운영 체제	주요 특성
Cabir.A	04.6	심비안	· 최초의 웜 바이러스로 심비안에서 발견됨 · 단말 배터리 수명 단축, 블루투스를 통해 전파
InCE.Duts	04.7	윈도우 모바일	· 단말기 루트 폴더의 모든 파일을 감염시킴
Skulls	04.11	심비안	· 단말 아이콘을 해골모양으로 변경·동작 정지 및 해당 프로그램 삭제
WinCE. Brador	05.8	윈도우 모바일	· 사용자 모르게 설치되어 단말을 원격 제어
Red browser	06.3	공통 (자바)	· 스마트폰 단말에서 사용자 모르게 불특정 다수에게 SMS 발송
FlexiSpy	06.3	심비안	· 사용자 모르게 통화 기록, SMS, 콘텐츠, 개인정보를 빼내 판매
InfoJack	08.3	윈도우 모바일	· 인터넷 연결시 단말의 시리얼번호, OS정보를 빼가고 파일설치 유도
Ikee	09.11	아이폰	· 아이폰 단말기간에 감염되어 사용자 바탕화면을 교체
iPhone/ Privacy	09.11	아이폰	· 감염된 단말에서 무선랜 접속시 개인정보를 원격지로 전달
Duh Worm	09.11	아이폰	· 감염된 단말로 은행사이트 이용시 비밀번호 유출 및 원격 제어

* 전성민의 "스마트폰 사용환경 변화가 정보보안에 미치는 영향연구"(p28)와 심재홍,이석래의 "모바일 인터넷 정보보호를 위한 모바일 악성코드 동향 분석"(p46) 재구성

최초의 웜 바이러스는 2004.6월 심비안 플랫폼이 탑재된 스마트폰에서 발견된 'Cabir.A'이었으며 단말 배터리의 수명을 단축시키고 블루투스를 통해 전파되었다. 지금까지 발견된 대표적 스마트폰 악성코드는 〔표 4〕와 같다.

한편, 심비안에서 발견된 악성코드는 주로 구버전(7.x, 8.x)에서 약 97%가 발견되었으며 인증체계를 도입한 신버전(9.x) 플랫폼에서는 3%에 그치는 등 발생비율이 현저히 감소하고 있어 모바일 보안정책에서 주목해야 할 부분이다〔24〕. 스마트폰 사용자들 사이에 큰 인기를 끌고 있는 아이폰의 경우 2009년 세 종류의

악성코드가 발생하였는데 이들 악성코드의 공통적인 특징은 '탈옥'된 아이폰의 SSH를 통하여 접근하고 설정된 기본 패스워드를 이용해 루트권한을 획득하여 정보 유출, 원격 제어, 악성코드 삽입 등이 가능하게 된다.

보안 전문가들은 현재까지 스마트폰 웜이 PC에 퍼지는 자기증식 위협은 나타나지 않고 있으나 2010년에는 아이폰과 안드로이드 시스템에서 바이러스가 자기 전파력을 갖게 될 것으로 예상하고 있다[25].

3.2 스마트폰 보안 실태

스마트폰 사용이 증가할수록 스마트폰에 대한 보안 위협도 높아지고 있다. 스마트폰 보안 위협에 효과적으로 대응하기 위해서는 스마트폰 사용자들의 보안관리 실태를 정확히 파악하여 대응방안을 마련하는 것이 요구된다.

방송통신위원회가 2010.5월 한국인터넷진흥원과 공동으로 실시한 국내 스마트폰 이용실태 조사에서 스마트폰 이용자의 47.2%가 보안문제(바이러스 및 악성코드 감염, 개인정보 유출 등)에 대해 걱정하는 것으로 나타났으며 주로 '이메일 및 문자메시지 첨부파일 다운로드(67.7%)와 'Wi-Fi, 블루투스 등 무선 네트워크 접속(64.8%)을 통해 보안문제가 발생한다고 인식하고 있었다. 한편 스마트폰 이용자의 69.9%가 '의심스러운 메시지 및 메일을 삭제'하는 것으로 보안문제에 대응하고 있으며 바이러스 검사(51.9%)나 비밀번호 설정·변경(49.1%) 등 적극적인 방법으로 대처하는 경우는 상대적으로 낮은 것으로 조사되었다[6].

또 스마트폰 악성코드 "트레드 다이얼"의 국내 등장을 계기로 전자신문이 스마트폰사용자카페와 공동으로 2010.4.30-5.2간 스마트폰 사용자회원 6만 1,775 명을 대상으로 스마트폰 백신사용에 대해 설문조사한 결과 응답자(989명)의 52.38%가 백신을 사용하지 않고 있으며 스마트폰 백신을 사용 중인 사용자도 백신의 효과를 못 느낀다(61.8%)고 답변하여 백신사용에 대한 불신이 높은 것으로 조사되었다[26].

IV. 스마트폰 이용 환경하의 국가기관 정보보호 방안

4.1 스마트폰 보안위협 대응방안

스마트폰에 대한 정보보호는 스마트폰 보안 위협에 대해 대응방안을 마련하는 것이 효율적이다. 우선 스마트폰 플랫폼에 대한 보안위협인 바이러스·웜과 시스템 Unlock 공격 및 키보드 해킹에 대해서는 운영체제의 보안취약점과 보안 업데이트를 공지하고 사용자에게 스마트폰 백신 사용 및 정기적 업데이트를 실시하고 시스템 Unlock을 탐지하는 체계를 갖추어야 한다.

스마트폰 애플리케이션에 대한 보안위협인 악성코드 내장 애플리케이션과 피싱 애플리케이션에 의한 피해를 막기 위해서는 앱 스토어에 업로드하는 애플리케이션에 대한 검증을 강화하는 것이 필요하다. 이를 위해 애플리케이션 개발자 대상 안전개발 가이드를 제시하고 악성코드에 대한 정보를 공유하는 체계를 마련하여 안전한 소프트웨어 유통환경을 조성하는 것이 요구된다. 또 애플리케이션 자원에 대한 모니터링을 실시하여 자원관리를 강화해야 한다[27].

시스템 네트워크 공격에 대응하기 위해서는 Wi-Fi 통신에 대한 암호화와 인증체계를 구축하여 Wi-Fi 도청·변조를 막고 모니터링을 통해 DoS 공격에 대응해야 한다.

스마트폰 단말기에 대한 보안위협은 단말기 분실·도난에 대비하여 패스워드 설정과 개인정보 원격 삭제 및 데이터 암호화, 위치 추적 등의 기술을 적용하고 저장 정보에 대한 백업도 정기적으로 실시해야 한다. 또 단말기에서 애플리케이션이나 이메일, 기타 자료를 다운로드할 경우 악성코드에 감염되는 것을 예방하기 위해 스마트폰용 백신을 설치하고 주기적인 바이러스 검사를 시행하도록 해야 한다[28]. 이를 정리한 것이 [표 5]이다.

[표 5] 스마트폰 보안위협 대응방안

분류	공격유형	대응방안
플랫폼 공격	○바이러스·웜 ○시스템 Unlock ○키보드 해킹	○취약점의 빠른 업데이트 ○스마트폰용 백신 사용 ○시스템 Unlock 탐지
애플리케이션 공격	○Malicious App. ○Fishing App.	○앱스토어기반 설치 권장 ○애플리케이션 검증 강화 ○자원 제어 모니터링
네트워크 공격	○WiFi 도청 및 변조 ○DoS 공격	○WiFi 통신 암호화/인증 ○자원제어 모니터링
단말기 공격	○도난 및 분실 ○Malicious App.	○패스워드 설정 ○데이터 암호화 ○개인정보 원격 삭제 ○위치 추적 ○저장정보 백업 ○스마트폰용 백신 사용 ○바이러스 검사

4.2 스마트폰 이용 환경하의 국가기관 정보보호 관리 체계 구축 방안

4.2.1 모바일 전자정부 보안관리 고려사항

국가기관은 이윤을 추구하는 민간 기업과는 많은 차이점을 가지고 있다. 국가기관은 행정을 수행하는 기관으로 그 업무는 크게 관리와 정책 업무로 나눌 수 있다. 관리적 측면은 재화와 인적 자원에 관한 것으로 조직, 인사, 재무 관리 및 최근 중요성이 강조되고 있는 정보관리가 해당되며 정책업무는 일련의 사회문제를 해결하는 정부의 적극적인 활동방침으로 공공분야의 고유 영역이라 할 수 있다. 이런 측면에서 국가기관이 취급하는 행정정보는 행정활동을 목적으로 사용자나 공공조직에 가치 있는 형태로 처리, 가공된 자료나 정보원으로 공공정보의 성격을 가지며 일반 사기업의 정보와는 다른 특징을 가지고 있다.

최근 공공정보에 대한 공개요구가 늘고 있는데 "공공기관의 정보공개에 관한 법률" 등 법에 근거하여 공공기관은 관련 정보를 국민에게 공개하고 있고 국민들은 공공기관에 정보공개를 청구할 수도 있다. 반면 공공기관은 국가안보, 공공질서 유지 등을 위해 비밀로 유지함이 필요한 기밀정보와 중요 정책 정보, 공공기관 보유 개인정보 등이 무단 유출되지 않도록 관리해야 할 의무를 가지고 있다.

전자정부 구축으로 공공기관의 많은 업무들이 네트워크로 연결되어 있으며 이는 공무원들의 업무 효율성과 생산성을 높이고 대국민 서비스를 크게 개선시키는 효과를 가져왔다. 정부는 정보환경 변화에 능동적으로 대처하기 위해 언제 어디서나 어느 기기로도 전자정부에 접근할 수 있는 유비쿼터스 전자정부를 궁극적 목표로 설정하고 있다. 유비쿼터스 전자정부가 구축되면 국민은 물론 공무원도 어디서나 본인이 원하는 네트워크에 접근할 수 있게 된다. 최근 스마트폰을 이용한 모바일 전자정부는 유비쿼터스 전자정부로 가는 과정에 있다고 볼 수 있다.

모바일 전자정부에서는 스마트폰을 통해 메일, 결제 등 업무를 수행할 수 있도록 시스템을 구축하게 되어 국가기관 내부 네트워크에 연동이 가능해짐에 따라 내부 네트워크가 노출될 위험이 있으며 이메일이나 문서 전송시 트래픽이 도청될 수 있다. 또한 권한 없는 외부자가 스마트폰을 통해 내부 네트워크에 무단 접근하거나 내부 직원이 권한을 넘는 정보에 접근할 위험성도 내재되어 있다. 특히 악성코드에 감염된 스마트폰으로 내부 네트워크에 연결될 경우 악성코드가 유포되거나 시스템에 장애가 발생할 수도 있어 전자정부의 신뢰성이 떨어짐은 물론 심할 경우 국가안보와 국민의 재산, 생명에도 악영향이 미칠 수 있을 정도로 그 파급영향은 막대하다.

이처럼 국가기관의 정보보호의 중요성이 막대함에 따라 우리나라는 중요 국가기관의 시스템에 대해서는 내부 네트워크와 인터넷을 분리하여 그 피해를 예방하고자 하고 있다. 그런데 최근 정보통신 기술은 서로 융합되고 다른 분야와 통합되어 새로운 서비스와 기술이 개발되는 추세임에 따라 이에 부응할 필요성도 커지고 있다. 특히 모바일 전자정부에서는 공무원이 외부에서도 인터넷을 통해 내부 네트워크에 접근하여 필요한 업무를 처리할 수 있어야 모바일 시스템 구축에 따른 긍정적 효과가 나타나고 모바일 전자정부도 활성화된다.

하지만 정부는 별도 보완책이 마련될 때까지 모든 공무원은 스마트폰으로 전자결재나 내부 전자우편을 열람하지 못하도록 하고 있는 것으로 알려졌다[29]. 이렇게 되면 내부 네트워크와 인터넷을 분리한 기관에서는 스마트폰을 이용하여 내부 네트워크에 대한 접근은 차단되고 인터넷으로 연결이 가능한 대민업무에 대해서만 접근할 수 있어 극히 제한적인 형태의 모바일 정부 시스템이 될 수밖에 없는 상황이다. 즉 완전한 형태의 모바일 전자정부 구축이 어렵게 되어 공무원의 일하는 방식 개선이라는 목표는 물론이거니와 대국민서비스 측면에서도 빠른 의사결정에 의한 실시간 처리가 원활하지 않게 될 수도 있다. 따라서 모바일 전자정부 구축 시에는 대국민 서비스 개선과 업무 효율성 제고라는 목표와 더불어 국가기관 보유 정보보호라는 목표를 동시에 이룰 수 있는 방안을 고려해야 한다. 정보보호라는 목표달성을 위해서는 보안위협에 대응하여 시스템의 안전성을 확보할 수 있어야 하므로 인가자가 인가 받은 서비스에만 접근할 수 있는 접근 통제 대책을 수립, 운영하고 악성코드가 유포되지 않도록 애플리케이션에 대한 검증 및 악성코드 감염 경로에 대한 통제와 관리를 철저히 하는 것이 중요하다.

4.2.2 모바일 전자정부 정보보호관리체계 구축 방안

4.2.2.1 전자정부 정보보호관리체계 구조

스마트폰을 이용한 모바일 전자정부가 활성화되기 위해서는 필요한 시스템이 제대로 구축되고 구축된 시스템은 각종 보안위협으로부터 안전하여야 한다. 이를

위해서는 모바일 전자정부에 대한 정보보호 절차와 과정을 체계적으로 수립하고 지속적으로 관리 운영하는 정보보호관리체계(Information Security Management System)를 구축하는 것이 필요하다. 정보보호 관리체계는 정보자산의 비밀성, 무결성, 가용성을 확보하기 위하여 필요한 절차와 과정을 체계적으로 수립·문서화 하고 지속적으로 관리·운영하는 시스템으로 조직이 달성하고자 하는 통제 목적을 제시하고 그러한 목적을 달성하기 위하여 조직 스스로 자신의 상황을 평가하고 대책을 수립하고 이를 지속적으로 관리 운영할 수 있어 모바일 전자정부의 정보보호 수준을 제고할 수 있기 때문이다.

정부는 2009.12월 행안부 훈령으로 "전자정부 정보보호 관리체계 인증 등에 관한 지침"을 제정하고 2010.6월 이를 개정, 시행하고 있다. 이는 국가기관이 정보보호를 위해 필요한 관리적·기술적·물리적 기준에 적합한 정보보호관리체계를 갖추었는지 심사하여 인증기준에 따라 적절히 운영되고 있는 경우 인증서를 부여하고 지속적으로 사후관리를 수행하기 위한 것으로 국가기관이 정보보호관리체계를 제대로 구축하였는지 검증하기 위한 것이다.

전자정부 정보보호관리체계 인증제도는 정보보호 관리체계 인증을 위한 국제표준인 ISO/IEC 27001과 국내 민간기업의 정보보호관리체계 인증제도인 한국인터넷진흥원(KISA)의 정보보호관리체계(ISMS)를 반영한 구조에 대국민서비스를 위해 중요한 개인정보보호 항목을 추가하여 인증심사기준이 마련되었다[30]. 따라서 동 제도는 PDCA(Plan-Do-Check-Act)사이클을 따라 정보보호 위험을 평가하여 필요한 통제를 선정, 구축하고 이를 문서화하여 운영하며 정기적으로 평가 개선할 것을 요구하는 과정을 통해 정보보호관리체계를 구현하도록 하고 있다.

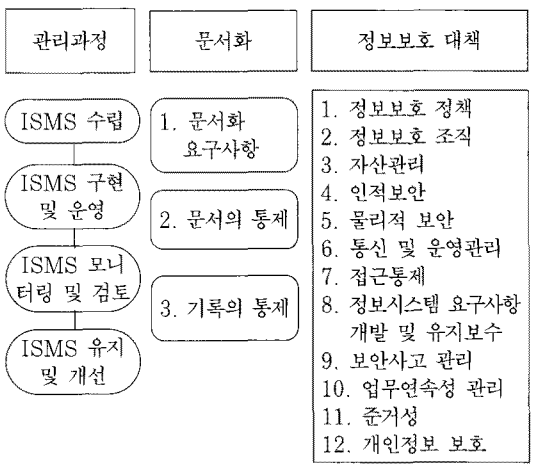
정보보호 관리체계를 수립하여 운영하고 있는 중앙행정기관이나 중앙행정기관과 동일한 법·제도의 적용을 받거나 또는 조직문화를 공유하는 지방자치단체와 소속기관이 자신의 정보보호 관리체계가 인증 심사기준에 적합한지를 확인받기 원할 경우 인증기관인 KISA에 심사를 신청하면 KISA는 자격을 갖춘 인증심사원으로 하여금 인증심사기준에 의한 심사(서류심사, 업무수행능력 심사, 현장실사)를 실시하고 이를 인증위원회에서 심의·승인하면 인증서를 발급하게 된다. 인증의 범위는 단위 조직은 물론 특정 IT시스템이나 서비스 시스템에 한정하여 받을 수도 있다.

국가기관 정보보호관리체계 인증기준은 관리과정, 문서화, 통제항목(정보보호 대책)의 3개 분야로 구성되어 있다. 관리과정이란 정보보호관리체계를 수립·운영하기 위하여 유지·관리하여야 할 과정으로 정보보호관리체계 수립, 구현 및 운영, 모니터 및 검토, 유지 및 개선의 4단계 15개 심사기준으로 구성되어 있으며 문서화는 문서화 요구사항, 문서의 통제, 기록의 통제 3개 기준으로 되어 있다. 통제항목 즉, 정보보호 대책의 수립여부를 점검하기 위한 통제사항은 12개 분야 156개 세부항목이 들어가 있다. 전자정부 정보보호관리체계 인증기준의 구조는 [그림 6]과 같다.

4.2.2.2 전자정부 정보보호관리체계 분석

정보보호관리체계의 관리과정과 문서화 분야는 절차와 과정에 관한 사항으로 환경이 바뀌어도 큰 변화가 없으나 통제항목 즉, 정보보호 대책 분야는 정보통신 환경이 바뀌면 그에 맞춰 관리와 운영이 변화되어야 한다. 특히 새로운 정보통신기기나 IT기술이 도입되면 정보보호 대책에는 변화가 생기게 된다. 모바일 전자정부는 기존의 전자정부에서 진화하여 스마트폰을 이용할 수 있게 됨에 따라 정보보호 측면에서 기존보다 다양하고 첨단화 및 지능화 된 보안위협에 노출되어 있어 이에 대한 적절한 정보보호 대책을 강구하여야 한다.

하지만 현행 "전자정부 정보보호관리체계 인증 등에 관한 지침"에는 스마트폰 보급 확산과 이를 전자정



[그림 6] 전자정부 정보보호관리체계 인증기준 구조

부에 적용하여 구축한 모바일 전자정부라는 환경변화가 제대로 반영되어 있지 않다. 동 지침에서 제시되고 있는 모바일 환경은 스마트폰 확산 이전의 정보환경 즉, 사무실 등 고정된 장소에서 PC를 통해서 네트워크에 접근하고 PDA나 노트북과 같은 이동형 정보통신기기와 USB와 같은 휴대형 저장매체도 필요시에만 사용하도록 통제할 수 있는 환경에 맞추어 정보보호 대책이 마련되어 있는 실정이다. 이에 따라 최근 스마트폰 이용 환경에 의한 변화 즉, 범용 운영체제(OS)가 적용되고 Wi-Fi나 블루투스로 접속이 가능하며 애플리케이션을 임의로 업로드·다운로드 할 수 있고 스마트폰을 통해 언제 어디서나 내부 네트워크에 접근할 수 있는 확장된 정보통신 환경에서의 보안위협에 대응할 수 있는 정보보호 대책은 미흡한 실정이다.

이를 구체적으로 살펴보면 다음과 같다. 우선 물리적 보안 분야에서 정보처리 시설 및 장비보호라는 통제목표를 위해 장비 및 저장매체를 반입, 반출하기 위한 안전한 승인절차를 마련하도록 하고 있지만 스마트폰 이용 환경에서는 스마트폰에 대한 승인절차 만으로는 통제목표를 달성하기가 어려우며 스마트폰 단말기에 대한 보호대책이 포함되어야 할 것이다. 통신 및 운영관리 분야에서 유해소프트웨어 통제를 위해 모바일 코드(자바스크립트, 액티브엑스 등)의 안전한 실행을 위한 통제방안을 수립하도록 하고 있으나 스마트폰 이용 환경에서는 유해소프트웨어가 플랫폼의 취약점에 의하거나 스마트폰 시스템을 unlock시키거나 Wi-Fi·블루투스를 통해 전파되기도 하고 악성코드가 내장된 애플리케이션을 다운받아 유포될 수도 있는 등 유해소프트웨어 유포 경로가 다양함에 따라 특정 경로만의 통제로는 대응하기 곤란하므로 악성코드 유포 경로별로 특화된 통제방안을 마련할 것이 요구된다. 또 정보교환에 대한 정보보호 대책으로 통신설비를 사용한 정보 교환 시 안전한 절차와 통제를 수립하고 전자메일, 메신저 및 P2P 통신과 같은 전자적인 교환에 대한 보호방안을 수립토록 하고 있는데 스마트폰 환경에서는 정보교환에 대한 통제가 내부 네트워크 내에서만 이루어지지 않기 때문에 기술적 통제가 용이하지 않으며 전자메일, 메신저도 Wi-Fi·블루투스 등 멀티 네트워크를 통해 접속할 수 있어 통제 목표를 이루기 위해서는 내부 네트워크 접근 시 모니터링 방안을 수립하고 스마트폰 사용자의 보안의식을 높이기 위한 교육을 강화하여야 한다. 접근통제 분야에서는 네트워크 접근 통제를 위해 사용자가 인가 받은 서비스에만 접속할 수 있도록 통제하는 방안을 수립하며 원격 사용자의 접속을 통제하기 위해 적절한 인증방법을 사용하도록 하고 서비스 그룹 및 사용자, 정보시스템 별로 네트워크를 분리하여 운영하도록 하고 있는데 스마트폰 이용 환경에서는 외부에서도 내부 네트워크에 접근할 수 있기 때문에 이러한 통제의 목적을 달성하기 위해서는 스마트폰에 인증기능을 적용하며 네트워크 접속을 모니터링하고 통제할 수 있는 기술적 조치가 필요하다. 또 이동 컴퓨팅 도구와 통신설비를 사용하는 위험을 감소시키기 위해 적절한 보호방안을 적용하고 원격지 근무 활동에 관한 정책, 운영 계획과 절차를 개발·적용하도록 하고 있는데 스마트폰 이용 환경에서는 이러한 통제를 더욱 세분화하고 구체화하여야 한다. 마지막으로 정보시스템 요구사항 개발 및 유지보수 분야에서 시스템 파일의 보안을 위해 운영시스템에서 소프트웨어를 설치할 시 이에 대한 통제 절차를 수립 및 수행하고 소프트웨어 패키지 수정은 엄격하게 통제하여 꼭 필요한 변경일 경우로 제한하도록 하고 있는데 스마트폰 이용 환경에서는 개인이 애플리케이션을 임의로 업로드 할 수 있고 스마트폰을 통해 내부 네트워크에 접근할 수 있어 PC동기화 되므로 기관에서 사용하는 소프트웨어 현황을 관리하고 개인이 임의로 애플리케이션을 다운로드 못하게 통제하는 등 애플리케이션에 대한 정책과 사용 절차를 마련하고 시행하도록 개선해야 한다.

4.2.2.3 모바일 전자정부 정보보호관리체계 개선방안

스마트폰은 PC 이상의 기능을 하고 있다. 특히 최근 소셜 네트워크의 활성화와 다양한 애플리케이션 개발로 스마트폰은 개인이 항상 휴대하면서 네트워크에 임의 접근할 수 있는 전천후 모바일 기기가 되고 있다. 나아가 각 기관에서는 이러한 특성을 활용하여 모바일 오피스 구축을 추진하고 있다. 스마트폰은 이제 더 이상 개인이 휴대하는 전화기에 머물지 않고 휴대용 멀티미디어 정보통신기기 수준에 이르고 있는 실정이다. 국가기관에서 스마트폰을 업무에 활용할 경우 정보시스템과 정보보호에 더 많은 주의를 기울여야 하는 이유가 여기에 있다.

모바일 전자정부에서 대국민서비스와 공무원의 업

무에 스마트폰을 활용할 경우에는 스마트폰의 이동성·다양성·개방성을 고려할 때 정보보호 정책부터 바꿔야 할 것이다. 지금까지의 논의를 토대로 모바일 전자정부 정보보호관리체계의 통제항목(정보보호 대책)에는 다음의 사항을 고려하여 심사기준을 수정·추가하여 스마트폰 이용 환경에 적합한 정보보호관리체계로 개선하는 것이 요구된다.

정보보호 정책 분야에 스마트폰 사용에 관한 보안정책을 정의하여 기관의 정보보안 규정에 문서화하여야 한다. 자산관리 분야에서는 스마트폰을 정보자산에 포함하여 분류기준을 마련하고 스마트폰을 이용한 정보처리 규정을 마련하여야 한다. 인적보안 분야에는 직원들이 조직의 스마트폰 보안정책을 인지하도록 교육시키며 스마트폰의 보안 취약성, 공격 유형, 보안설정 방법 등을 스마트폰 사용자들에게 정기적으로 교육시켜야 한다. 물리적 보안 분야에서는 정보처리 시설 및 장비 보호를 위해 AP 접근 방지를 위한 보호케이스 설치, 데이터 라인·파워라인에 보호케이스 설치 등의 보안대책을 강구하여야 한다[31]. 또 외부 반출 장비의 보호를 위해 스마트폰 단말기에 패스워드를 설정하고 개인정보 원격 삭제 및 위치 추적기능을 적용하며 백신을 사용하는 등 단말기 도난 및 분실 대책을 마련하여야 한다. 스마트폰 반출·입에 대한 승인절차를 마련하기 위해 스마트폰 사용자 현황을 파악하고 매뉴얼을 확보하여야 한다.

통신 및 운영관리 분야의 유해소프트웨어 통제를 위해 조직에서 필요한 애플리케이션 현황을 파악하고 공무원 개인이 임의로 스마트폰에 애플리케이션을 다운받지 않도록 통제하여야 한다. 또 스마트폰을 이용한 정보의 교환에 대한 절차와 통제를 수립하고 스마트폰에는 중요정보를 저장하지 않도록 하여야 한다. 스마트폰을 이용하여 교환하는 문서는 암호화하고 스마트폰에 저장된 정보에 대해서도 백업을 주기적으로 하여야 한다. 전자메일, 메신저 및 P2P 통신과 같은 전자적인 교환과 관련 악성코드가 유포되지 않도록 스마트폰에 안티바이러스 제품을 설치하여야 한다. 스마트폰으로 기관의 네트워크에 원격 연결을 허용할 경우에는 모니터링 통제항목의 정보시스템 사용 모니터링 방안을 수립하고 모니터링 결과를 주기적으로 검토하여야 한다.

접근통제 분야에는 스마트폰의 내부 네트워크 접근을 허용할지 여부에 대한 정책을 수립·문서화하고 이를 주기적으로 검토하여야 한다. 또 스마트폰이 USB나 블루투스를 사용하여 내부 네트워크에 동기화 할 수 있는지에 대한 사항도 보안관리 정책에 포함하여야 한다. 스마트폰을 이용해 정보시스템과 서비스에 접근을 허용하거나 취소하기 위한 공식적인 사용자 등록 및 해지 절차를 마련하여야 한다. 모바일 전자정부에서는 유무선을 통합한 멀티 네트워크가 가능하므로 네트워크 접근통제가 특히 중요하다. 따라서 스마트폰 사용자가 인가 받은 서비스에만 접속할 수 있도록 통제하는 방안을 수립하고 원격 사용자의 접속을 통제하기 위해 스마트폰에 인증기능을 적용하며 스마트폰으로부터의 접속을 인증하기 위한 자동 장비인식 방식을 사용하여야 한다. 또 스마트폰 서비스 그룹 및 사용자, 정보시스템 별로 네트워크를 분리하여 운영하며 스마트폰으로부터의 네트워크 접속은 접근통제 정책과 업무 요구사항에 따라 제한하여야 한다. 정보통신 기기로서의 스마트폰은 탁월한 이동성으로 언제 어디서나 서비스가 가능하다는 장점이 있지만 이동 컴퓨팅에 따르는 위험을 감소시키기 위해서는 단말기와 네트워크에 대한 보호방안이 적용되어야 한다. 최근 스마트폰을 이용한 모바일오피스의 한 형태로 사무실 대신 집 가까운 곳에 마련된 별도의 사무실에서 업무를 보는 '스마트워크 센터'가 활발히 구축되고 있는데 이러한 원격지 근무 활동에 관한 정책, 운영 계획과 절차가 개발되고 적용되어야 한다.

정보시스템 요구사항 개발 및 유지보수 분야에서는 운영소프트웨어 통제를 위해 전자정부용 애플리케이션은 개발기준을 마련하여 공시하고 전자정부에 적용되는 소프트웨어를 검증하여야 하며 소프트웨어 패키지 변경 제한을 위해 스마트폰 사용자가 임의로 소프트웨어를 변경하지 못하도록 통제하여야 한다. 한편 '전자정부 모바일 앱 등록 센터'를 설치하여 프로그래밍 오류나 보안 취약성을 검증할 수 있는 체계를 구축하면 안전성을 높일 수 있을 것이다[32].

현행 전자정부 정보보호관리체계 통제항목을 스마트폰 이용환경을 고려한 모바일 전자정부 정보보호관리체계 통제항목으로 수정·추가하여 제안한 것을 정리하면 [표 6]과 같다.

〔표 6〕 스마트폰 이용 환경하의 전자정부 정보보호관리체계 통제대책

분야	통제	세부통제	인증심사기준 추가 개선사항
정보보호 정책	정보보호 정책	정보보호 정책의 문서화	스마트폰 사용에 관한 보안 정책을 정의하여 정보보안 규정에 문서화한다.
자산 관리	정보 자산 분류	분류기준/ 정보처리 규정	스마트폰을 정보자산에 포함하여 분류기준을 작성하고 스마트폰을 이용한 정보처리 규정을 문서화한다.
인적 보안	재직시 인적 보안	정보보호 교육 및 훈련	직원들에게 기관의 스마트폰 보안정책을 인지시키며 스마트폰의 보안 취약성, 공격 유형, 보안설정 방법 등을 정기적으로 교육시킨다.
물리적 보안	정보처리 시설 및 장비 보호	케이블 보호	AP 접근방지를 위한 보호케이스 설치, 데이터 라인·파워 라인에 보호케이스 설치 등의 보안대책을 시행하여야 한다.
		외부반출 장비의 보안	스마트폰 단말기에 패스워드를 설정하고 개인정보 원격삭제 및 위치추적기능을 적용하고 백신 사용 등 단말기 도난 및 분실대책을 마련하여야 한다.
		장비의 반출·입	스마트폰 반출·입에 대한 승인절차를 마련하기 위해 스마트폰 사용자 현황을 파악하고 매뉴얼을 확보하여야 한다.
통신 및 운영관리	유해 소프트웨어 통제	악성코드 통제	애플리케이션 현황을 파악하고 개인이 임의로 스마트폰에 애플리케이션을 다운받지 않도록 통제하여야 한다.
	백업	정보백업	스마트폰에 저장된 정보보호를 위해 주기적으로 백업을 수행하여야 한다.
	정보의 교환	정보 교환의 통제	스마트폰을 이용한 정보 교환에 대한 절차와 통제를 수립하며 스마트폰에 중요 정보를 저장하지 않도록 하고 문서는 암호화 하여야 한다.
		전자적 교환 보안	전자메일, 메신저 및 P2P 통신과 같은 전자적인 교환 시 스마트폰에 안티바이러스 제품을 설치하여야 한다.
	모니터링	정보시스템 사용 모니터링	스마트폰으로 내부 네트워크 연결을 허용할 경우 정보시스템 사용 모니터링 방안을 수립하고 주기적으로 검토하여야 한다.
접근 통제	접근 통제 업무 요구 사항	접근통제 방안 수립	스마트폰의 내부 네트워크 접근 허용 여부에 대한 정책을 수립하여야 한다.
	사용자 접근 관리	사용자 등록	스마트폰을 이용해 정보시스템과 서비스에 접근을 허용하거나 취소하기 위한 공식적인 사용자 등록 및 해지 절차를 수립하여야 한다.
	네트워크 접근 통제	네트워크 서비스 사용정책	스마트폰 사용자가 인가 받은 서비스에만 접속할 수 있도록 통제방안을 수립하여야 한다.
		원격접속 사용자 인증	원격 사용자의 접속을 통제하기 위해 스마트폰에 인증기능을 적용하여야 한다.
		네트워크 에서의 장비 인식	스마트폰으로부터의 접속을 인증하기 위한 자동 장비인식 방식을 사용하여야 한다.
		네트워크 분리	스마트폰 서비스 그룹 및 사용자, 정보시스템 별로 네트워크를 분리하여 운영하여야 한다.
		네트워크 연결 제어	스마트폰으로부터의 네트워크 접속은 접근통제 정책과 업무 요구사항에 따라 제한하여야 한다.
	이동 컴퓨팅 및 원격지 근무	이동 컴퓨팅 및 통신	스마트폰 단말기와 네트워크에 대한 적절한 보호방안이 적용되어야 한다.
		원격지 근무	스마트워크 센터 등 원격지 근무 활동에 관한 정책, 운영 계획과 절차가 개발되고 적용되어야 한다.
정보시스템 요구사항 개발 및 유지보수	시스템 파일의 보안	운영 소프트웨어 통제	전자정부용 애플리케이션은 개발기준을 마련하여 공시하고 전자정부에 적용되는 소프트웨어를 검증하도록 한다.
	개발·지원 과정에서의 보안	소프트웨어 패키지 변경 제한	스마트폰 사용자가 임의로 소프트웨어를 변경하지 못하도록 통제하여야 한다.

V. 결 론

최근 우리 사회에 스마트폰이 빠른 속도로 확산되고 있다. 스마트폰은 이동통신 전화기에 고성능 범용 운영체제가 탑재되어 멀티 정보통신기기로 기능하고

있으며 Wi-Fi·블루투스를 활용하여 어디서나 접속이 가능하고 애플리케이션을 오픈마켓에서 임의로 업로드·다운로드 할 수 있는 특성으로 인해 개인생활을 바꾸고 있으며 조직에서는 모바일오피스에 활용되어 업무 효율성과 생산성을 높이고 있다. 정부도 스마트폰 이용 환경에 부응하여 모바일 전자정부를 구축하고 스마트폰으로 대국민서비스를 제공하는 한편 실시간 대응, 원격 근무 등을 통해 공무원의 일하는 방식을 개선시키고 있다. 하지만 스마트폰은 플랫폼, 네트워크, 애플리케이션, 단말기 등에 다양한 보안 위협요인이 존재하며 악성코드에 의한 피해도 매년 증가하고 있는 실정이다. 이러한 상황에서 국가기관이 스마트폰을 활용한 모바일 전자정부를 구축하면서 보안대책을 제대로 마련하지 않고 스마트폰을 이용한 서비스를 확대할 경우 중요정보 유출 및 시스템 장애 등이 발생하여 정부 신뢰도가 떨어짐은 물론 심할 경우 국가안보와 국민의 재산, 생명에도 영향을 미칠 수 있을 정도로 그 파급영향이 막대하다. 따라서 국가기관은 스마트폰을 활용한 모바일 전자정부 구축 시에는 대국민 서비스 개선과 업무 효율성 제고라는 목표와 더불어 국가기관 보유 정보보호라는 목표를 동시에 이룰 수 있는 방안을 고려해야 한다. 이를 위해서는 보안위협을 지속적으로 통제 관리할 수 있도록 스마트폰 이용 환경에 적합한 정보보호관리체계를 구축하는 것이 필요하다.

이에 본 논문에서는 "전자정부 정보보호관리체계 인증 등에 관한 지침"(행안부 훈령, 201.6월 개정)을 통해 전자정부 정보보호관리체계의 구조를 살펴보고 통제항목(정보보호 대책)에 대한 분석결과 스마트폰 이용 환경 변화가 제대로 반영되어 있지 않은 것을 확인할 수 있었다. 이에 스마트폰 사용에 관한 보안정책 정의와 문서화 등 정보보호 정책 분야를 비롯하여 자산관리, 인적·물리적 보안, 통신 및 운영관리, 접근 통제 분야 등에 대해 스마트폰 이용 환경에서 모바일 전자정부 정보보호관리체계 개선방안을 제시하였다.

모바일 전자정부는 정부가 궁극적 목표로 설정하고 있는 유비쿼터스 전자정부로 가는 과정에 있다고 볼 수 있다. 이러한 시점에서 모바일 전자정부 정보보호 관리체계 구축은 모바일 환경에서의 정보보호가 중요하다는 것을 공무원 개개인이 인식할 수 있도록 정보보호 마인드를 변화시키고 다양화·지능화·첨단화되는 보안위협에 단편적, 일회적으로 대응하는 것보다 체계적, 지속적으로 관리하는 것이 정보보호에 더 효율적임을 일깨워주며 보안사고가 발생한 후나 보안점검, 감사 등 타율적 규제가 아닌 자율적으로 정보보호를 수행하여 각 기관이 정보보호에 대한 자생력을 키울 수 있다는 점을 시사한다고 볼 수 있다.

국가기관이 모바일 전자정부 환경에서 정보보호관리체계를 구축하는 것은 정보보호에 대한 기관의 체질을 개선하는 작업으로 초기에는 어려움이 있을 수 있으나 지속적인 정보보호관리체계 운영을 통하여 국가기관의 정보보호 수준이 지속적으로 개선될 수 있는 기반이 마련될 것이며 장기적으로는 정보보호 수준이 획기적으로 개선될 것으로 기대된다.

참고문헌

[1] 김영춘, 민경일, 신용달, 조용석, 현대사회의 정보통신 개론, pp. 211-254, 홍릉과학출판사, 2010년 2월

[2] 김성용, "스마트폰 시장 1년새 56% 급성장," 연합뉴스, 2010년 5월

[3] 이윤찬, "진정한 유비쿼터스 혁명 진행: IT 부품·SW 기회 잡을 때," 이코노미스트(1040), pp. 16-18, 2010년 6월

[4] 백준봉,홍범석,최명호, "아이폰 시장 전망과 경제적 파급효과 분석," KT경제경영연구소, pp. 1-13, 2010년 6월

[5] 임두순, "2010 이동통신서비스 중심 스마트폰," 통신연합(51), pp. 58-63, 2010년 3월

[6] 손재권, "스마트폰 쓰나미 : 국내 개발 앱 5,501개 등록, 이중에서 몇 개나 돈 될까," 이코노미스트(1040), p 26, 2010년 6월

[7] 윤석이, "스마트폰 열풍, 특허출원 봇물," 연합뉴스, 2010년 5월

[8] 최명호, "모바일 오피스로 달라질 미래의 모습," KT경제경영연구소, pp. 1-6, 2010년 4월

[9] 윤두식, "모바일 오피스 위험 대응을 위한 관제 서비스," 한국정보보호학회 Smart Mobile Security 2010 세미나발표집, pp. 199-214, 2010년 6월

[10] 배한철, 오윤수, 최명호, 백홍진, "모바일오피스 구축의 경제적 효과 : 도시철도공사 사례 분석," KT경제경영연구소, pp. 1-40, 2010년 2월

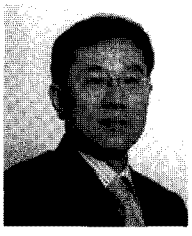
[11] 손재권, "SK그룹의 모바일 오피스 실험 : 기업 특성에 맞춘 맞춤형으로 승부," 이코노미스트(1033), pp. 36-37, 2010년 4월

[12] 행정안전부, "전자정부법 제2조 제1호," 법률 제10303호, 일부개정, 2010년 5월

[13] 행정안전부, "모바일 확산에 따른 전자정부 정책방향," 스마트폰 기반 전자정부 추진전략 세미나 발표집, pp. 1-36, 2010년 6월
[14] http://www.mopas.go.kr/goms/un2010
[15] 김정미, 백인수, "공공서비스 선진화를 위한 IT 신기술 활용방향," 한국정보화진흥원, IT정책연구시리즈(6), pp. 1-13, 2010년 4월
[16] 행정안전부, "전자정부 지원사업을 통한 모바일 전자정부 추진방안," 스마트폰 기반 전자정부추진전략세미나발표집, pp. 1-28, 2010년 6월
[17] 샌프란시스코AFP=연합뉴스, "美 저작권사무국, 스마트폰 '탈옥' 합법화," 연합뉴스, 2010년 7월
[18] 전성민, "스마트폰 사용 환경의 변화가 정보보안에 미치는 영향 연구," 석사학위논문, 연세대학교 정보대학원, pp. 1-59, 2009년 12월
[19] 이동훈, "스마트폰의 보안위협 및 대응," 한국정보보호학회 Smart Mobile Security 2010 세미나 발표집, pp. 19-35, 2010년 6월
[20] 김수용, "안드로이드 보안모델 및 보안위협," 한국정보보호학회 Smart Mobile Security 2010세미나발표집, pp. 121-130, 2010년 6월
[21] 김승열, "알 수 없는 불안감, 모바일 보안," p 15, 2010년 4월
[22] 임석훈, 송영규, "스마트폰 악성코드 포착-보안비상," 서울경제신문, 2010년 4월
[23] 서동규, "안드로이드폰 악성코드 주의보 발령," 전자신문, 2010년 5월
[24] 심재홍, 이석래, "모바일 인터넷 정보보호를 위한 모바일 악성코드 동향 분석," 정보보호학회지 19(6), pp. 41-48, 2009년 12월
[25] Andreas Antonopoulos, "Hot security prediction for 2010," Network World, vol. 26, no. 35, p 16, Dec. 2009
[26] 장윤정, "스마트폰 사용자 50% 이상 백신사용 안한다," 전자신문, 2010년 5월
[27] 강성주, "스마트폰시대 사이버안전 정책 방향," 한국정보보호학회 Smart Mobile Security 2010 세미나발표집, pp. 39-62, 2010년 6월
[28] Sangho Kim, ChoonSeong Leem, "Security threats and their counter measures of Mobile portable computing devices in ubiquitous computing environments," ICCSA 2005, LNCS 3483, pp. 79-85, 2005
[29] 박성민, "공무원 스마트폰 통한 전자결재 제한," 연합뉴스, 2010년 8월
[30] 오경희, 김정덕, 박태완, 권헌영, 김지연, 박미화, "정보보호관리체계 인증제도 연구," pp. 58-74, 행정안전부, 2008년 12월
[31] 한국인터넷진흥원, "무선랜 보안 가이드," 한국인터넷진흥원, pp. 1-119, 2008년 11월
[32] 한근희, "모바일 전자정부 보안기술 적용방안," 한국정보보호학회 Smart Mobile Security 2010 세미나발표집, pp. 67-90, 2010년 6월

〈著者紹介〉

김 지 숙 (Ji-sook Kim) 학생회원
2008년 3월~현재: 고려대학교 정보경영공학과 박사과정
〈관심분야〉 정보보호, 정보보호 정책, 정보보호 관리체계



임 종 인 (Jongin Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 이학석사
1986년 2월: 고려대학교 수학과 이학박사
1986년 3월~2001년 1월: 고려대학교 자연과학대학 정교수
2001년 2월~현재: 고려대학교 정보경영공학전문대학원((구)정보보호대학원) 원장, 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원, 방송통신위원회 인터넷협의회 운영위원 등
〈관심분야〉 정보법학, 디지털포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등