한국위기관리논집 제7권 제4호 2011. 8 135~150쪽

스마트 시대의 보안 위협

- EU5*의 대응과 시사점 -

임상규**, 이창길***, 김종업****

지난 20여 년간 정보통신기술(ICT)은 많은 발전을 거듭하였고, 다양한 디지털 기기와 서비스를 가져다 주었다. 컴퓨터, 인터넷, 그리고 휴대폰은 현대인의 필수품이 되었고, 생활 & 업무 방식의 새로운 패러다임을 만들었다고 할 수 있다. 특히, 2007년 스마트 폰의 등장으로 기존의 무선인터넷, PDA 등과 결합된 스마트 시대의 도래는 이전과는 확연히 구분되는 디지털 세상이 되었다. 하지만, 스마트 시대가 가져온 다양한 편익에 비례해 해킹을 통한 개인정보의 유출, 시스템 파괴 등과 같은 보안 위협을 함께 수반하였다. 본 논문은 스마트 시대의 보안 위협과 관련해 유럽연합(EU) 내에서 가장 큰 영향력을 가지고 있고, 정보화 부문에서 앞서있는 EU5 국가들의 스마트 시대 보안 위협에 대한 공동 대응 방안을 살펴보았다. 이를 통해, 서비스 제공 부문에 비해 보안 부문에서 소홀한 한국에의 시사점을 찾는데 목적이 있다고 하겠다. DDos 공격, 농협의 전산망 파괴 같은 문제가 되풀이 되고, 급속하게 증가한 스마트 폰의 보급에 따라 분실 & 도난을 통한 개인정보의 유출, 스마트 폰을 통한 해킹이나 잘못된 애플리케이션 제공으로 많은 피해가 발생하기 때문이다. EU5 국가들이 제시한 위험 요인과 대응이 모든 문제를 해결할 수는 없지만 한국에 시사하는 바는 크다고 하겠다.

주제어: 스마트 시대, 스마트 폰, 보안 위협, 유럽연합, EU5

Ⅰ. 서론

1. 연구의 필요성

1990년대 이후 정보통신기술의 발전은 공상과학 영화에서 보았던 것과 같은 새로운 기기와 서비스를 제공하기에 이르렀다. 컴퓨터, 인터넷, 그리고 휴대폰은 현대인의 필수품이 되었고, 삶의 방식을 바꾸었다. 즉, 인터넷과 모바일 폰(mobile phone) 등으로 대변되는 디지털 기기들(Digital devices)들은

* 'EU 5'는 유럽연합(European Union, EU)을 주도하며, 유럽 대륙에서 가장 큰 영향력을 가진 영국, 독일, 프랑스, 스페인, 그리고 이탈리아를 지칭한다.

** 제 1저자, *** 제 2저자, **** 교신저자.

아침에 눈을 떠서 저녁에 잠자리에 들기까지 물, 공기, 음식 다음으로 일상생활에서 가장 필요하고 중요한 것이 되었다.

2000년대 접어들어 더욱 빠른 성장과 발전을 거듭한 모바일 기술은 스마트폰을 비롯한 이전에 생각하지 못했던 디지털 기기들을 현실화 시켰다. 이러한 스마트폰, PDA 같은 첨단 디지털 정보기기들의 활용은 인터넷과 접목되어 이전에 경험하지 못한 새로운 형태의 정보화 시대를 만들어 내었는데 이를 '스마트 시대'(smart age)라고 부른다. 스마트 폰과 테플릿 PC 등 스마트 기기가 일반 휴대폰(Feature phone)과 데스크 탑의 판매율을 훌쩍 앞지르면서 스마트 혁명이 불고 있다. 스마트 기기(smart devices)와 무선 인터넷을 기반으로 언제 어디에서든지 모든 사람들에게 똑똑한 서비스를 제공할 수 있는 정보통신기술 환경이 도래하였음을 의미하는 것이다. 이러한 스마트 시대를 주도하는 것이 컴퓨터, 인터넷, 그리고 모바일의 기능까지 포함하는 '스마트 폰'(smart phone)으로 현재 정보통신기술의 총아이며 스마트 시대의 아이콘이라고 할 수 있다. 이러한 새로운 디지털 기기들에 의한 스마트 시대의 도래는 세계적인 흐름이며 국가간, 대륙간의 공간적 한계와 제약을 극복한 장벽 없는 가상의 사회와 국가를 만들어 내고 있고 지속적인 발전을 거듭하고 있다.

2007년 스마트 폰이 보급된 이후 최근 몇 년간 급속하게 확산된 스마트 폰을 위시한 스마트 기기들은 인간 생활의 패턴을 바꾸었고, 삶의 패러다임 변화를 야기했다고 볼 수 있다. 하지만, 이들 첨단 디지털 기기들을 활용한 스마트 시대는 보다 다양하고 빠른 서비스의 제공이라는 밝은 측면과 함께 해커, 개인정보의 유출, 시스템 파괴, 사이버 테러공격 등과 같은 이라는 어두운 면을 동시에 만들어 내었다. 다시 말해, 새로운 기기들의 발전으로 인한 스마트 시대의 도래는 이전에 즐기기 못한 새로운 경험을 가져다주었지만, 개인의 사생활 침해, 불건전한 정보유통, 시스템 파괴, 데이터 해킹 및 훼손 등의 정보사회의 부작용과 문제점을 동반하고 있다(정익재, 2007: 211). 즉, 스마트 시대가 되면서 이전보다 정보화로 인한 많은 편익을 가질 수 있게 되었지만, 그에 비례해서 개인과 조직이 보유한 정보의 유출과 해커의 공격에 의한 시스템과 기기의 파괴 같은 다양한 보안의 문제들이 발생한 것이다. 지진, 태풍, 홍수 등의 자연재해와 전쟁과 테러와 같은 위협 요인들이 전통적인 재해·재난이라면 스마트 시대의 정보보안의 위협은 새로운 형태의 재난이라고 볼 수 있다. 올해 초에 해외로부터의 DDos 공격, 농협 전산망 파괴 같은 새로운 재난은 전통적인 재해·재난처럼 인간 생명에는 큰 위협이 없지만, 안보·경제·사회적인 측면에서 보면 오히려 그 범위와 피해 규모가 크다고 볼 수 있다. 국가 기간 전산망과 금융 시스템의 불통, 안보시스템의 파괴는 국가의 존망을 위태롭게 할 수 있다. 스마트폰을 위시한 디지털 기기의 보급으로 스마트 시대가 도래 하였지만, 보안 위험에 대한 선행연구가 많지 않고, 이들 선행연구들은 정보보안의 취약성을 다룬 정익재(2007)와 스마트 서비스 도입·확산과 관련해 법제도의 개선을 연구한 정필운(2011)을 제외하고는 대부분의 연구들이 정책적인 부문이 아니라 기술적인 부분에 초점을 맞추고 있다. 또한, 국내의 보안 위협 침해 사례를 중심으로 기술하고 있어, 해외의 보안 위협 동향과 대응 방안에 대한 사례 연구가 필요하다고 볼 수 있다.

2. 연구의 목적과 방법

편리하고 다양한 유용성과 편익을 제공하는 스마트 시대의 어두운 면에 대한 보안 대책은 정보통신 기술의 발전과 함께 시급히 해결해야 하는 가장 중요한 이슈가 되었다. 유럽지역에서 스마트한 정보화를 주도하는 영국, 독일, 프랑스, 이태리, 그리고 스페인은 이러한 시대적 흐름에 부응하기 위해 전통적인 재해·재난에 대한 대비와 함께 새로운 디지털 시대의 위협 요인을 제거하기 위한 노력하고 있다. 이들 5개국은 유럽에서 정치·경제·군사 부문에서 가장 큰 영향력을 가졌고, 동시에 유럽연합(EU)을 주도하는 주요 회원국이다. 또한, 유럽연합(EU)내에서뿐만 아니라 유럽 대륙에서 가장 앞선 정보통신강국들인 이들의 보안 대책은 스마트 폰의 이용 증가와 함께 보안문제는 더욱 중요해졌다. 하지만, 행정안전부 외(2011: 264-267)에 따르면 2010년 이후 정보보호와 보안 관련이 예산과 인력이 감소하였다. 따라서 한국은 정보통신기술을 선도하는 위치에 있지만 상대적으로 보안에 소홀한 모습을 보이고 있어 보안 위협에 대한 EU5의 대응 방안은 한국에게 가장 절실하고 필요한 정책이라고 할 수 있다. 스마트 폰 사용자가 전체의 30%인 1,500만 명을 넘어섰고, 세계 최고 수준의 초고속 인터넷 망과 다양한 디지털 기기의 보급으로 스마트 시대의 구현이 빠르게 진행되고 있는 한국은 정보보안 부문에 대한 정책적 측면의 대비가 상대적으로 부족하다. 스마트 기기의 보급과 서비스 확대에는 빠르게 대응하고 있지만, 개인정보보호, 해커의 공격, 정보유출, 그리고 시스템 파괴 같은 보안 문제에 대해서는 스마트 하지 못하다고 볼 수 있다.

본 연구는 스마트 시대가 도래 했지만, 보안 위협에 대한 인식이 부족하고 스마트한 콘텐츠와 서비스의 제공에만 초점을 맞추고 있어 닥쳐온 보안 위협에 대한 적절한 대응이 없다는 문제를 인식하였다. 따라서 스마트 시대를 대표하는 스마트 폰을 중심으로 하여 보안 위협과 대응 방안에 대해 다루었다. 먼저, 본 연구는 제2장에서 스마트 시대의 도래와 정보보안 위협의 증가에 대한 고찰을 하였다. 제3장에서는 사례분석으로서 유럽연합의 스마트시대 현황과 문제점을, 제4장에서는 스마트 시대에 대응한 EU5 국가들의 정보 보안 위협 대책을 분석하였다. 제5장은 연구의 결론 및 시사점을 다루었다. 본 연구는 문헌연구를 중심으로 하였고, 유럽연합과 한국의 정부 보고서와 관련 저널의 논문, 그리고 정보보안 관련 기관과 기업의 홈페이지의 조사를 통해 이루어졌다.

Ⅱ. 스마트 시대의 도래와 정보보안 위협

1. 스마트 시대의 도래

1990년대 중·후반 이후 눈부시게 발전을 거듭한 휴대폰은 단순통화 기능으로 출발하여 PDA 기능, 모바일 결제(M-commerce), MP3, 카메라, DMB, 그리고 인터넷 및 이메일(e-mail) 접속기능에 이르기

까지 매우 빠른 속도로 진화하고 있다(이형찬 외, 2010: 61-61). 이런 최신 디지털 기기들 중에서도 기존 휴대폰의 통화기능에 PC 환경에서 제공되던 다양한 인터넷 서비스 기능까지 하나의 단말기로 융·복합화된 것이 스마트 폰이다. 스마트 폰은 미국 Apple사의 iPhone이 출시되면서, 전 세계적으로 일반 휴대폰에서 스마트폰으로 시장이 급변하고 있다(장상근, 2010: 64). 스마트폰의 보급이 급격하게 증가하는 요인은 더 이상 기본적인 이동통신 서비스(음성 및 문자 데이터 송·수신)만을 통해서는 사용자의 다양한 욕구를 만족 시키지 못하기 때문에, 장소에 구애 없이 기본 이동통신 서비스와 더불어 자유롭게 인터넷 접속이 가능하고 다양한 어플리케이션들[1] 이 제공되기 때문이다. 즉, 스마트 폰을 통해 본격적인 유비쿼터스(Ubiquitous) 세상을 열어가는 기반이 되었고, 이전과는 확연하게 구분된 서비스를 이용할 수 있게 되었다. 스마트 폰은 휴대 단말 기능의 융·복합화 및 인터넷 연동의 가속화 추세는 제2세대(2G)에서 제3세대(3G)를 거쳐 현재 제4세대(4G)까지 발전을 거듭하고 있다. 스마트 폰은 일상생활뿐만 아니라 업무(Office)에 활용하는 모바일 워크(Mobile work) 시대가 된 것이다. 스마트 폰이 중심이 된 PDA 같은 모바일과 초고속 인터넷 망을 활용해 일을 하거나 일상생활에 활용하는 정보화 시대를 '스마트 시대'(smart age)라고 한다. 스마트 폰은 통화 기능은 물론 이메일(e-mail), 인터넷, 전자도서(e-book) 등으로 활용 가능한 소형 컴퓨터 기능을 갖춘 멀티 휴대전화로, 전 세계 스마트 폰 시장은 점차 확대되고 있다.

한국도 예외가 아닌데, 2007년부터 스마트폰 도입이 활성화됐던 미국, 유럽 등 해외에 비해 국내는 스마트폰 보급이 매우 미미한 수준에 불과했다. 그러나 2008년 12월 무선인터넷 표준 플랫폼인 위피 탑재 의무 폐지 등 규제 완화 이후 2009년 11월 아이폰의 국내 출시를 계기로 스마트폰이 본격 확산되기 시작했다. 2009년 말 80만 명에 불과했던 스마트폰 가입자 수가 2011년 7월을 기점으로 1천 5백만 명을 돌파할 정도로 단기간에 빠른 성장세를 보이고 있다.

이러한 증가세가 지속되어 올 연말에는 스마트폰 가입자가 2천만 명을 돌파할 것으로 전망되는 등 본격적인 스마트폰 대중화 시대에 진입하였다(방송통신위원회 보도자료. 2011. 3. 24). 국내 스마트폰 가입자의 현황을 살펴보면 아이폰(iPhone)의 OS와 구글(Google)의 안드로이드 시스템이 전체 가입자 중 약 87%를 차지하고 있다(<표 1> 참조).

<표 1> 국내 스마트폰 가입자 현황

(단위: 만대)

구 분	'10.3월	'10.6월	'10.9월	'10.12월	'11.1월
안드로이드 (%)	5(3.3)	45(18.2)	204(46.3)	415(57.5)	494(59.8)
아이폰 OS (%)	50(33.1)	81(32.8)	115(26.1)	184(25.5)	219(26.5)
MS 윈도우 (%)	85(56.3)	102(41.3)	101(22.9)	102(14.1)	93(11.3)
기 타 (%)	11(7.3)	19(7.7)	21(4.7)	21(2.9)	20(2.4)

※ 자료: 방송통신위원회(2011).

1) 카카오톡(Kakaotalk) 같은 실시간 대화(SNS), 금융결제, 도로정보 검색 등이 대표적이다.

2. 스마트 시대의 보안 위협의 증가

스마트 폰은 모바일 워크(mobile work)와 클라우딩 컴퓨팅(Clouding computing) 같은 유비쿼터스(Ubiquitous) 환경이 만들어 지면서 새로운 형태의 업무 방식과 이전과 다른 라이프 스타일(Life style)의 스마트 시대를 가져다주었다. 이형찬 외(2010: 61)에 따르면 스마트 시대의 대표 브랜드인 스마트 폰의 사용이 증가하면서 데이터 서비스, 실행 파일의 공유, 업무용 이용이 증가하게 되었고 새로운 보안 취약점으로 이어지게 되었다. 또한, 스마트 폰의 지능화 및 네트워크 기능 탑재 추세에 발맞추어 이들 스마트 폰을 공격하는 모바일 악성코드가 급증하고 있다. 즉, 스마트 폰이 과거에는 사용자도 적고, 플랫폼(Platform)[2]의 기능적 제약으로 인해 주목을 받지 못했지만, 현재 스마트 폰은 고성능의 다양한 기능을 갖추고 있으며, Wi-Fi, Blue tooth 등 다양한 접속 경로를 통해 다른 매체들 간의 연결도 편리해졌다.

하지만, 보안을 고려해 본다면 접근성이 좋아졌다는 것은 보안 위협에 노출될 수 있는 영역이 더 많아 진 것이며, 악성코드 전파 경로 또한 다양해 졌다는 문제가 발생되었다. 또한 스마트 폰 사용자가 증가하고 어플리케이션이 다양해질수록 취약한 영역이 많아지고, 이러한 취약성을 이용한 공격들과 더불어 SNS(Social Network Service, 소셜 네트워크)[3]를 통한 사회 공학적 공격 기법들이 나타날 수 있으며, 이외에 다양한 보안 위협이 발생할 수 있다(장상근, 2010: 66). 최근 스마트 폰의 사용자가 증가하면서 다양한 해킹 사례가 발생하고 있는데, 스마트 폰 플랫폼 시장은 아이폰, 안드로이드, 그리고 윈도우 모바일이 주도적으로 이끌어 나가고 있다고 해도 과언이 아니다. 이들 대표적인 스마트 폰 플랫폼이 스마트 시대의 대표적인 기기라고 해도 충분히 보안 문제가 발생할 수 있다는 것을 단적으로 보여준 것이라고 할 수 있다(<표 2> 참조).

---

2) 플랫폼(Platform)은 소프트웨어 응용 프로그램들을 돌리는데 쓰이는 하드웨어와 소프트웨어의 결합이다. 플랫폼은 하나의 운영체제 또는 컴퓨터 아키텍처라고 단순히 말할 수 있으며 그 두 가지를 통칭해서 말할 수 있다. 컴퓨터 플랫폼(Computing platform)은 소프트웨어가 구동 가능한 하드웨어 아키텍처나 소프트웨어 프레임워크(응용 프로그램 프레임워크를 포함하는)의 종류를 설명하는 단어이다. 일반적으로 플랫폼은 컴퓨터의 아키텍처, 운영체제(OS), 프로그램 언어, 그리고 관련 런타임 라이브러리 또는 GUI(Graphical User Interface, 그림 위주의 컴퓨터 운영방식)을 포함한다(ko.wikipedia.org).

3) 온라인상에서 불특정 타인과 관계를 맺을 수 있는 서비스로, 이용자들은 SNS를 통해 인맥을 새롭게 쌓거나 기존 인맥과의 관계를 강화시킨다. 국내의 대표적인 SNS로는 '싸이월드'(Cyworld), 미투데이(me2day), 카카오톡(Kakaotalk) 등이 있고, 국외에는 트위터(Twitter), 페이스북(Facebook) 등이 있다.

<표 2> 최신 스마트 폰 해킹 대표 사례

플랫폼 (Platform)	악성행위 유형	버전
아이폰(iPhone)	전화번호부, 파일시스템 목록 등 개인정보 탈취	OS 3.1.3
	좀비 프로세스 활용한 DDos 공격 가능성	OS 3.1.3
	SMS, 전화번호부, 사진 등 탈취	Safari
안드로이드(Android)	ID, 패스워드 탈취	OS 2.1
윈도우 모바일 (Windows Mobile)	프로세스 메모리 해킹을 통한 SMS 메시지 탈취	CE 5.2
	리턴 오리엔티드 프로그래밍 기법 및 쉘코드 (shellcode)[4] 작성을 통한 공격 가능성	CE 5.2

※ 자료: 이형찬 외(2010: 64) 연구를 중심으로 재구성.

손경호(2010: 72-73)와 나성욱(2011: 12-20)의 연구를 종합하면, 일반적으로 스마트 폰의 확산에 따른 보안 위협은 세 가지로 구분할 수 있다. 먼저, 단말기 보안 이슈이다. 스마트 폰 단말기의 도난·분실로 인한 개인정보 또는 업무 정보의 유출, 업무용 서버에 불법 접속하여 업무정보 유출, 스마트 폰 소유자가 악의적으로 업무정보를 외부로 유출할 가능성 존재 등이다. 둘째, 응용 프로그램 및 플랫폼 보안 이슈이다. 스마트폰의 악성코드 감염으로 인해 개인정보 유출, 장치이용 제한, 부정과금 유발, 모바일 DDos 공격 등의 위협 가능, 플랫폼 또는 펌웨어[5] 변조에 따라 보안 기능을 약화시킬 가능성 존재이다. 마지막으로, 네트워크 및 서버 보안 이슈이다. 무선구간에서 패킷[6] 스니핑[7](가로채기), 상용인터넷 망을 통한 해킹, 스마트 폰을 경유하여 인트라넷 서버에 접속하여 발생하는 보안 위협의 존재이다.

최근 국내에서도 무단으로 국제전화를 걸어 비싼 요금이 나오게 하는 악성코드에 감염된 피해사례가 150건 이상 보고되었다. 또한 국외에서도 미국 은행 등의 이름을 이용해 개인정보와 금융정보를 빼가는 피싱 애플리케이션이 등장하였다. 이외에도 스마트폰의 주소록을 빼내거나 특정번호로 문자를 무작위로 보내고, 사용자의 데이터를 숨기는 등 다양한 악성코드가 출현하였다. 김기연 & 조성제(2010: 90-94)의 연구에 의하면, 악성 코드의 증가에 대해 미국의 한 모바일 보안업체의 조사 에 따르면 2005년 131개였던 모바일 악성코드는 2009년 600여 개로 늘어났다. 이러한 스마트 폰의 보안위협

4) 쉘코드(Shellcode)는 취약점을 이용해 특정 코드를 실행하게 할 때 사용되는 코드를 말한다.
5) 펌웨어(Firmware)는 컴퓨팅과 공학 분야에서 특정 하드웨어 장치에 포함된 소프트웨어로, 소프트웨어를 읽어 실행하거나 수정되는 것도 가능한 장치를 뜻한다. 펌웨어는 ROM이나PROM에 저장되며 하드웨어보다는 교환하기가 쉽지만, 소프트웨어보다는 어렵다(ko.wikipedia.org).
6) 패킷(Packet)은 네트워크를 통해 전송하기 쉽도록 자른 데이터의 전송단위이다. E-mail 등으로 파일을 보낼 때 패킷으로 분할해 보내면 받을 때는 원래의 파일로 재조립된다. 패킷으로 분할될 때는 각각 별도의 번호가 붙여지고 목적지의 인터넷 주소가 기록된다(http://joins.com).
7) 스니핑(Sniffing)은 스니퍼(Sniffer)를 이용하여 네트워크상의 데이터를 도청하여 네트워크 상에 돌아 다니는 패킷의 내용을 들여다 보는 것을 말한다(정보통신망이용촉진및정보보호등에관한법률, 2008).

요소는 스마트 폰의 가장 큰 장점인 시간과 장소의 구애를 받지 않고 무선인터넷을 통해 실시간으로 사용 가능한 인터넷 환경에 노출되어 있다는 점이다. 인터넷에 접속할 수 있으나, 아직까지 보안의 위협에 있어서 큰 관심을 가지고 있지 않다는 점이다.

이러한 스마트폰 보안의 위협요소는 다음과 같이 정의 내릴 수 있다. 첫째, 개방성이다. 스마트 폰은 일반 폰보다 월등히 뛰어난 성능을 가지고 있으며 멀티미디어 처리도 우수하다. 하지만 최근에는 일반 폰들의 사양이 스마트 폰과 거의 차이가 없을 정도로 개선되어 이를 기준으로 스마트 폰과 일반 폰을 구분하기는 어렵다. 스마트 폰과 일반 폰을 구별 짓는 가장 큰 특성은 개방성이라 할 수 있다. 스마트 폰은 일반 폰과는 다르게 무선인터넷 및 외부 인터페이스를 개방하여 제공하고 있다. 스마트 폰의 다양한 외부 인터페이스는 사용자에게 다양한 네트워크 서비스를 지원하고, 내부 API 인터페이스 제공은 개발자에게 편리한 개발환경을 제공한다. 하지만 이를 보안적인 측면에서 해석하면, 다양한 외부 인터페이스 제공은 악성코드 전파 경로의 다양성을 제공하고, 내부 인터페이스는 악의적인 개발자에 의해 악성코드가 은닉된 모바일 애플리케이션 제작을 용이하게 만드는 취약점을 가지고 있다.

둘째, 휴대성이다. 스마트 폰의 휴대 편의성으로 인해 발생하는 분실·도난 사고는 월평균 20만 대에 이르고 있다. 스마트 폰 분실·도난에 따른 직접적인 경제적 피해와 더불어 스마트 폰에 저장된 개인 정보 및 모바일 오피스를 지원하는 스마트 폰의 특성으로 인한 기업의 중요한 기밀 정보 유출은 심각한 사회문제를 야기 시킬 수 있다. 이에 따라 스마트 폰에 저장된 정보를 암호화하거나 분실·도난시 저장된 정보를 원격에서 소거하는 기술들이 등장하고 있다.

셋째, 저성능이다. 스마트 폰은 PC에 비해 저전력, 저성능 기기이다. 따라서, PC 환경에서 제공하는 보안 소프트웨어를 스마트 폰에 적용하기에는 무리가 있다. 강동호 외(2010: 72-74)에 따르면 PC 환경에서는 다양한 보안 위협에 대응하기 위해서 지속적인 모니터링을 통해 악성코드를 탐지해야 하지만 스마트 폰은 전력 및 성능적인 제약으로 인해 백신을 비롯한 보안 소프트웨어의 적용에 어려움이 있다.

Ⅲ. 유럽의 스마트 시대와 보안 문제의 대두

PC, PDA, 그리고 스마트 폰 등은 스마트 시대를 주도하는 스마트 디지털 기기들이다. 이중에서 스마트 폰은 '스마트 시대'의 주연이라고 볼 수 있는 정보통신기술의 총아(寵兒)이다. '스마트 모바일'(smart mobile)의 개념으로 보면, 이용자가 원하는 정보를 상황을 기반으로 정확히 선별하여 빠르고 편리하게 제공하는 이동성을 갖춘 단말기 및 서비스이다(나성욱 외, 2010: 4). 스마트 폰은 편리하고 직관적인 이용자 인터페이스(User Interface, UI), 빠른 반응 속도, 멀티 포인트 터치, 개방형 응용서비스 모델(앱스토어[8] , 안드로이드 마켓[9] 등) 활용이 가능하다. 즉, 다양한 애플리케이션의 자유로

8) 앱스토어(App store)는 애플(Apple)이 운영하고 있는 아이폰(iPhone), 아이패드(iPad) 및 아이팟 터치(iPod

운 설치 및 실행이 스마트 폰의 가장 큰 특징이자 장점이다. PC와 같이 멀티미디어 서비스 기능과 인터페이스를 지원하며, 디지털 컨버전스[10] (Digital convergence), 인터페이스 간편화와 터치 폰은 확산 추세이다.

영국, 독일, 프랑스, 이태리, 그리고 스페인은 유럽연합(EU)을 구성하는 주요 회원국이며, 동시에 정치·경제적 측면에서 가장 큰 영향력을 행사하는 국가이다. 즉, 유럽대륙(러시아 제외)에서 인구와 경제 규모가 다른 국가들에 비해 크므로 인해 지역 내에서 주도적 입장에 있다. EU5 국가는 정보화에서도 다른 회원 국가들에 비해 앞서고 있고 다양한 서비스를 제공하고 있다[11]. 따라서 이들 5개국은 인터넷과 모바일(스마트 폰 포함) 보급율에서 타 국가들에 비해 높다. 2010년 1월에 EU5 국가들은 단말기[12] 기준으로 약 7.9% 감소했지만, 스마트 폰 사용자의 수는 전년대비 약 32% 성장을 기록한 5천 1.6백만 명이었다(Roper, 2011). 특히, 영국의 경우에는 2009년과 비교해 70% 이상의 스마트 폰 사용자가 증가하였다(<표 3> 참조).

<표 3> 스마트 폰 플랫폼(Platforms) in EU5(UK, DE, FR, ES, and IT)

(2010년 1월말 기준)

	Share (%) of Smartphone Subscribers					
	EU 5	UK	DE	FR	ES	IT
Total Smartphone Subscribers	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Symbian	60.9%	46.9%	55.1%	40.7%	73.5%	75.7%
Apple	14.5%	20.5%	15.3%	29.9%	6.5%	7.7%

Touch)용 응용 소프트웨어 다운로드 서비스이다. 아이폰(iPhone) 3G가 발표될 즈음인 2008년 7월 10일부터 아이튠즈(iTunes)의 업데이트 형태로 서비스가 시작되었다. '앱 스토어'란 이름은 '애플의 응용 소프트웨어 가게'(Apple Application Software Store)란 의미를 담고 있으며, 개인용 컴퓨터에서 아이튠즈를 이용하거나 아이폰 및 아이팟 터치의 메뉴에서 직접 3G 네트워크 혹은 WiFi를 경유하여(아이팟 터치의 경우는 Wi-Fi만 지원) 소프트웨어를 다운로든 할 수 있다. 다운로드할 수 있는 소프트웨어는 유료 및 무료가 있으며, 무료 소프트웨어를 다운로드할 때도 아이튠즈의 계정이 필요하다(http://enc.daum.net).

9) 안드로이드 마켓(Android Market)은 구글(Googple)이 운영하고 있는 구글 안드로이드용 응용 소프트웨어를 다운로드할 수 있게 해주는 서비스이다. 애플의 앱 스토어와는 다르게 안드로이드 마켓은 구글의 정책에 따라 사용자가 구입한지 15일 이내에 다운로드한 응용 프로그램의 환불을 요구하면 구매 금액을 모두 환불해 주어야 한다(http://enc.daum.net).

10) 영상·음성·데이터 등 서로 다른 종류의 미디어를 단말기·서비스·네트워크의 제약없이 자유롭게 융합하는 현상을 말한다. 디지털 컨버전스 현상은 디지털 기술이 발전하면서 기존의 산업·기술·서비스 등의 구분이 모호해지면서 이들 간에 새로운 형태의 융합 상품과 서비스들이 등장하며 시작되었다. 카메라·MP3·모바일뱅킹 등의 기능이 결합된 휴대전화, 방송과 통신이 결합된 DMB 등이 디지털 컨버전스의 한 예이다.

11) EU5 국가들을 제외하고 아일랜드(Republic of Ireland)와 핀란드(Finland)의 정보화 수준이 높은 편이다.

12) 단말기는 일반 모바일 폰(Feature phone)과 스마트 폰(smart phone)을 포함 것이다.

<표 3> 스마트 폰 플랫폼(Platforms) in EU5(UK, DE, FR, ES, and IT)(계속)

	Share (%) of Smartphone Subscribers					
	EU 5	UK	DE	FR	ES	IT
Microsoft	14.1%	10.7%	19.9%	20.0%	12.8%	11.4%
RIM	8.3%	18.7%	6.8%	5.4%	5.2%	4.7%
Google	2.0%	3.0%	2.2%	3.7%	1.8%	0.4%

※ 주: UK(영국), DE(독일), FR(프랑스), ES(스페인), IT(이탈리아)

※ 자료: com Score MibiLens

영국은 유럽 주요 5개국 중에서 스마트 폰 사용자가 가장 많은 1천 1백만 명인데, 전체의 1/4에 조금 미치지 못하는 22.6%이고, 급속하게 사용자가 증가하는 추세이다. 물론 여전히 3/4 이상이 피쳐폰[13](Feature phone)을 사용하고 있다(<표 4> 참조).

<표 4> EU5 국가들의 모바일 서비스 및 이용율

(2010년 1월말 기준)

	모바일 가입자(%)					
	EU5	UK	DE	FR	ES	IT
Sent an SMS/Text	83.5	90.3	81.6	81.7	84.5	79.5
Used Application (including games)	33.4	37.6	33.3	23.6	36.1	37.8
Listened to Music	22.7	21.4	24.6	19.9	28.7	20.4
Mobile Browsing	22.2	30.8	17.4	21.7	19.9	20.7
Accessed Social Networking Site or Blog	11.3	18.2	6.5	10.2	9.5	11.7
Accessed News	9.6	13.7	7.5	9.0	6.7	10.4
3G Device	42.4	41.7	38.3	36.7	53.3	45.2
Smartphone	22.6	22.9	16.5	15.2	28.3	32.0

※ 주: UK(영국), DE(독일), FR(프랑스), ES(스페인), IT(이탈리아)

※ 자료: com Score MibiLens

스마트 시대에 가장 적합한 폰으로 인식되고 있는 3G 폰의 경우 영국 전체 스마트 폰의 41.7%가 사용하는 것으로 조사될 정도로 스마트 폰을 이용한 서비스의 이용이 가능해졌다. 또한, 김종업(2011: 41)의 연구에 의하면 인터넷 이용자의 31%가 그들의 폰을 이용하여 인터넷 서비스를 이용하고, 18%

13) 유럽에서는 일반 핸드폰(Plain old mobile)이라고도 한다.

이상이 SNS에 접속하며, 13.7%가 다른 매체가 아닌 폰을 이용하여 뉴스 정보를 얻는 것으로 나타났다[14].

영국을 비롯한 유럽 주요 5개국의 스마트 폰 사용자는 매년 증가하고, 모바일 오피스의 확대, 그리고 인터넷 이용 증가로 인해 스마트 시대가 도래 했다고 볼 수 있다. 그렇지만, 스마트 폰을 사용하고 첨단 정보통신 기기들을 이용한다고 해서 사용자가 모두 스마트 한 것은 아니다. 스마트 폰과 인터넷 사용자가 증가하고 모바일 오피스(혹은 스마트 워크)의 확대는 해킹과 기기 도난으로 인한 정보 유출 등의 주요한 공격 목표로 떠올랐다. 다시 말해, 스마트 폰의 보급과 사용자의 증가는 기존에 인터넷을 통한 시스템 파괴나 정보 탈취 같은 해커의 공격이 빈번했다면, 이제는 스마트 폰 사용자가 해커나 테러 공격의 주요 목표가 되었다고 볼 수 있다. 스마트 시대의 도래로 스마트 폰 사용자를 위한 금융과 의료서비스 등의 뉴 어플리케이션(New Application)이 등장하면서 해커들은 이들을 대상으로 한 사이버 테러나 정보탈취, 그리고 시스템 파괴 같은 새로운 유형의 보안 위협이 등장한 나온 것이다.

IV. EU5 국가들의 보안 대책

급격하게 증가한 EU 5 국가들의 스마트 폰 사용자는 금융과 의료 서비스, SNS 등의 다양한 부문에서 이전에 누리지 못한 새로운 형태의 서비스 제공과 정보의 향유를 가능하게 했지만, 그와 함께 해커의 공격과 정보의 탈취, 시스템 파괴 같은 보안 문제를 함께 야기했다. 영국, 독일 등의 EU5 국가는 스마트 폰 및 PDA 같은 정보기기의 사용으로 스마트 시대에 스마트 폰의 사용자가 직면한 위험요인을 10가지로 분류했다(<표 5> 참조). 스마트 폰에 대한 정보보안 위험은 스마트 폰뿐만 아니라 PDA, 인터넷 사용 등을 통해 충분히 경험할 수 있는 위험 요인들까지 포함하는 스마트 시대의 보안 위험 분류라고 할 수 있다.

<표 5> 스마트 시대의 정보 보안 위험 10가지

	위험	세부 내용
R1	Data leakage	스마트 폰의 도난 & 분실로 인한 정보의 보안 문제
R2	Improper decommissioning	폰에 내장된 민감한 정보를 보호하지 않거나 방치한 채로 다른 사람이 폰을 사용하거나 습득함으로 인한 공격 피해
R3	Unintentional data disclosure	대부분의 앱(apps)은 개인 프라이버시 기능을 가지는데, 많은 사용자들이 인식하지 못하고 데이터가 전달되거나 정보의 존재를 인식하게 되는 경우
R4	Phishing	공격자가 사용자의 개인정보(패스워드, 신용카드 번호 등)를 사용하거나 위조하는 것

14) 유럽연합(EU) 전체 국가들의 22%가 폰을 이용하여 인터넷에 접속하고, EU5 국가의 11%가 폰을 이용하여 SNS 서비스에 접속하는 것으로 나타났다.

<표 5> 스마트 시대의 정보 보안 위험 10가지(계속)

	위험	세부 내용
R5	Spyware	Spyware를 활용한 개인 데이터의 파괴와 악용
R6	Network Spoofing attacks	공격자가 나쁜 네트워크를 만들어 사용자가 접근하게 하여 위험을 초래함
R7	Surveillance	공격 목표가 된 스마트 폰 사용자를 속이면서 스파이 행위를 하는 것
R8	Diallerware	공격자가는 서비스나 폰 번호를 알아내어 사용자의 돈을 탈취하는 것
R9	Financial malware	악의적인 소프트웨어(malware)를 통해 신용카드번호와 인터넷 뱅킹의 정보를 훔치는 것
R10	Network congestion	네트워크의 자료가 한계를 벗어나므로 인해 스마트 폰 사용을 못하게 하는 경우

※ 자료: European Network and Information Society Agency(enisa)(2010).

EU5 국가들이 제시한 스마트 시대의 정보보안 위협 문제들은 완벽하게 해결할 수는 없지만, 충분한 대비가 있다면 위협이 줄어들 수 있다고 보고 있다. EU5가 10가지의 위험에 대한 주요 대처 방안은 <표 6>에서 보는 것과 같다. 각각의 위험 요인에 대한 대응 방안은 새로운 고도기술의 도입이나 시스템보다는 쉽지만 이전에는 간과한 간단한 방법에서 출발하고 이들 방안들은 한국에게도 적용이 가능하다.

먼저, R1에 대한 대응은 자동 장금장치와 정기적인 백업, IEMI 번호의 기록, 그리고 스마트 폰 사용자 인증처럼 손쉽게 할 수 있다. 일반적으로 사용의 불편함 때문에 자동잠금장치와 백업을 잘 하지 않는 것은 동·서를 막론하고 쉽게 간과 하고 있다. 또한, R1과 더불어 R2의 개인정보 기본 설정과 면밀한 조사를 통한 승인 요구는 필요하다고 볼 수 있다. 스마트 폰을 위시한 디지털 기기들은 많은 개인정보를 담게 되고 이에 보다 높은 수준의 승인 과정이 함께 이루어져야 한다.

다음으로, R3의 경우 우리가 쉽게 간과하는 경향이 있는데, 핸드폰의 교체 시에 반드시 모든 정보를 삭제하여 개인정보의 유출을 막을 수 있다. 핸드폰을 교체할 경우 들어 있는 개인정보를 백업 받은 후에는 다른 이들이 핸드폰을 습득하더라도 남아 있는 개인정보를 활용하지 못하게 삭제나 초기화를 해야 한다.

마지막으로, R4의 위험에 대한 의식, R5, 8 & 9와 같은 서비스와 메커니즘에 대한 모니터링과 제어, R6, 7, 10의 공인되고 안전한 시스템 이용을 제시하고 있다. 개인이 보안 위협들에 대응을 해도 위협들이 사라지는 것은 아니다. 함께 공유할 수밖에 없는 기지국을 사용하기 때문에 위험에 대한 인식을 언제나 해야 하며, 안전하고 공인된 것인지 확인하는 것은 필수적이다. 또한, R5, 8 & 9의 위협은 지속적인 모니터링과 데이터 사용량에 대한 체크를 해야 한다. 간과하기 쉬운 보안이나 암호화 관련 소프트웨어를 구입하여 보안에 대한 철저한 대비가 필요함을 알려주고 있다.

<표 6> 주요 위험요인과 대응 방안

위험 요인	대 응 방 안
R1	- Automatic locking(자동 잠금장치) - Regular backups(정기적인 백업) - Note IMEI number(IMEI 번호의 기록) - User-to-smartphone authentication(스마트 폰 사용자 인증) - Certification of smartphone(예를 들어, FIPS140-2, 영국 CESG의 Product Scheme(CAPS))
R2	- Scrutinize permission requests(면밀한 승인 요구) - Review default privacy settings(개인정보 기본 설정)
R3	- Reset and wipe(before disposing or recycling the phone, wipe all the data and setting) (초기상태 & 모든 데이터 삭제) - Decommissioning(해체)
R4	- Be skeptical(다른 이의 사용을 막음) - IT officers should create awareness of this risk(위험의 인식)
R5, 8, and 9	- Check reputation(before installing or using new smartphone apps or services, check their reputation using app-store reputation mechanisms(안전하고 공인된 것인지 확인) - Check resource usage and phone bill(사용량을 체크) - Resource control(monitor resource usage of smartphones for anomalies(모니터링)
R6	- Cautious use of hotspots(use public WiFi hotspots with caution and configure the smartphone so that it does not connect automatically)(공인된 무선랜 기지국 이용) - Communications confidentiality(using VPN or SSL)(통신 비밀의 보장) - Pre-installing server certificates(사용전 서버 인증) - Encryption software(암호화 소프트웨어 구비)

※ 자료: European Network and Information Society Agency(enisa)(2010).

EU5 국가들이 내놓은 보안 위협 10가지에 대한 대응은 어렵고 비용이 많이 들어가는 기술적인 보안 대응보다는 쉽게 할 수 있는 것이다. 이들 국가들은 스마트 시대의 도래로 복잡한 디지털 기기들을 능숙하게 다룰 수 없다고 보고, 누구나 쉽고 간편하게 다양한 보안 위협에 대응할 수 있는 방안들을 강구한 것이다.

Ⅴ. 결론: 시사점 및 한계

정보통신 기기를 활용한 서비스와 정보의 취득과 활용은 일상생활에서 의・식・주처럼 되어 가고 있다. 최근 빠르게 발전을 거듭하는 정보통신 기술로 인해 이전에 누리지 못한 편리함과 다양한 서비스는 정보화가 가져다 준 편익이고 스마트 시대의 선물이다. 하지만, 기술의 진보만큼이나 그에 따른

위험이 수반되고 있고, 그에 대한 대책 마련이 시급한 현안이 된지 오래다. 특히, 스마트 폰과 PDA 같은 스마트한 정보통신기기의 활용과 인터넷을 이용한 각종 서비스의 사용이 보편화 되면서, 이전에 비해 해커의 공격으로 인한 정보의 유출・탈취에 비해 훨씬 광범위하고 위험성이 증가하게 되었다.

스마트 시대의 대표기기인 스마트 폰 사용자의 증가와 다양한 애플리케이션의 제공은 이러한 정보보안 문제가 한 지역이나 국가에 머무르지 않고 공간을 초월한 글로벌 이슈가 될 수밖에 없음을 보여준다. 유럽에서 정보화를 선도하고 있고 정보기기의 활용과 다양한 서비스를 제공하는 영국, 독일, 프랑스, 스페인, 그리고 이탈리아의 EU5 국가들은 증가하는 스마트 폰 사용으로 인해 나타날 수 있는 대표적인 보안 위험 요인을 10가지로 분류하였고, 이들 위험 요인들에 대한 대응 방안을 제시하고 있다. 빠른 정보통신기술의 진보와 정보화를 통한 다양한 서비스에 맞게 안전하게 정보화가 주는 편익을 누릴 수 있게 해줘야 함을 EU5 국가들의 정보보안 위협에 대한 대응 방안에서 알 수 있다. 또한, 보안 문제는 한 국가에 머무르지 않고 공간적 벽을 초월한 문제이기 때문에 가까운 지역의 국가들이 함께 논의의 장을 만들고 공동 대응할 수 있어야 한다.

스마트 시대가 가져다주는 다양하고 편리한 서비스의 이용을 위해서는 취약한 보안 위험에 대응이 필요하다. 먼저 스마트 폰을 비롯한 스마트 정보통신 기기들을 사용하는 사용자의 대응이다. 스마트 폰과 PDA 같은 기기의 악성 코드 사고에 대한 책임은 전적으로 시스템에만 존재할 수 없고, 사용자들에게도 일정부분 책임이 있다. 특히, 피쳐폰(Feature phone)에서 스마트 폰으로 급속한 전환이 일어나는 시점에서 사용자들은 스마트 폰 보안에 대한 이해가 부족한 실정인데 각종 보안 사안별 위험에 대한 보안의식을 가질 수 있도록 해야 한다. EU5 국가들의 보안 위협 R1, R5, R8 그리고 R9의 대응 방안이 이 부문에 해당한다고 볼 수 있겠다.

둘째, 기술적인 대응 방안인데, 백신 소프트웨어의 한계이다. PC 환경에서 악성코드 검출 및 제거 방법으로 백신 프로그램의 설치를 최우선적으로 고려해왔던 것이 사실이다(이형찬 외, 2010: 67). 반면에, 스마트 폰은 일반 폰과 다르게 PC의 기능을 가지고 있기 때문에 기존 PC에서와 동일한 접근방법이 스마트 폰 환경에서도 그대로 적용할 수 있을지에 대한 검토와 함께 스마트 폰에 가장 적합한 환경을 만들어 주어야 한다. 더불어, 스마트 폰에 장착되거나 사용 가능한 소프트웨어 등록 및 검증이 필요하다. 아이폰(iPhone)의 경우 앱 스토어(App store)에서 개발자가 프로그램 등록시 이에 대한 보안성 검증 및 테스트가 이루어지는데, 검증과정이 폐쇄적으로 진행되어 어떤 검증과 테스트가 이루어지는지 알 수 없는데 투명성 있게 검증하고 그 결과를 사용자들에게 알려주어야 한다. EU 5 국가들이 제시한 R5, R8, R9의 위협에 대한 대응 방안으로써 앱이나 프로그램을 설치하기 전에 그 앱이나 프로그램에 안전・신뢰도를 알아보고 사용한다면 위협을 줄일 수 있다.

마지막으로, 법・제도적인 미비점에 대한 대응이다. 스마트 폰의 사용자가 증가하고 다양한 정보통신 기기들을 이용한 서비스의 제공과 활용이 보편화 되고 있다. 스마트 시대에 접어 들면서, 일상생활뿐만 아니라 업무에서도 스마트 기기의 활용이 증대될 것이다. 즉, 모바일 워크를 넘어 스마트 워크(Smart work)가 일반화 될 경우 기반 구축과 서비스 제공 및 역기능 방지를 위한 법이나 제도적인

마련을 통해 스마트한 환경 조성이 필요하다. 또한, 스마트 시대는 지리적인 한계를 벗어나기 때문에 이웃한 국가뿐만 아니라 전 세계 모든 국가와 상호 협력을 통해 보안 위협을 줄여 나가야 한다. EU와 자유무역협정(FTA)이 발효되어 더욱 많은 교류가 예상되는데, 보안 위협 문제 역시 EU5 국가들을 중심으로 국제협력을 통해 해외로부터의 위협과 새로운 보안 문제에 대한 대응이 필요하다고 할 수 있겠다.

테러와 전쟁 같은 인위적인 재난, 지진과 태풍 같은 자연 재해와 함께 현대 사회에서 가장 시급한 문제 중의 하나가 정보화에 따른 정보 보안 문제라고 할 수 있다. 서비스의 제공과 기술 발전도 중요하지만, 사용자(이용자)가 보다 편리하고 안전하게 이용할 수 있는 환경의 조성이 더 중요하다. 유럽연합(EU)에서 주도적인 EU5 국가들의 스마트 시대의 보안 위험에 대한 문제 인식과 공동의 대응 방안은 디도스(DDOS)로 인한 공격과 농협의 정보보안 시스템 사태에서 보여준 허술한 대응으로 보안 부문에서 취약한 한국에 시사하는 바가 크다고 할 수 있다. 전통적인 재해·재난, 전쟁과 테러와 마찬가지로 스마트 시대의 보안 위협에 대해 새로운 인식의 전환과 중앙-지방정부간, 국가 간의 공동 노력이 필요하다.

더불어, 본 연구가 스마트 시대의 도래와 함께 보안 위협에 상대적으로 관심을 먼저 가진 유럽의 사례를 연구하다 보니 한국의 사례 분석이 부족한 한계를 가진다. 또한, 연구가 문헌연구를 중심으로 이루어져지면서 관련 전문가의 인터뷰나 설문조사 같은 정량적 연구가 함께 이루어지지 않은 아쉬움이 있다. 향후의 연구는 비록 선행연구가 많지 않다고 하더라도 이러한 문제에 대한 인식을 바탕으로 해외 사례와 한국의 현황과 문제점을 반영한 연구가 필요하다고 본다. 스마트 시대의 밝은 면을 더욱 활용하기 위해서는 어두운 면에 대한 대비와 보완은 충분조건이 아니라 필수조건이기 때문이다.

참고문헌

강동호 외. 2010. 스마트폰 보안 위협 및 대응기술. 전자통신동향분석. 25(3): 72-80.

김기연·조성제. 2010. 스마트폰 보안 취약점 동향. 한국정보과학회 추계 학술대회 발표논문집. 36(2B): 90-94.

김소정. 2006. 미국과 우리나라의 정보보안관리 활동 비교 연구. 정보처리학회지. 13(3): 69-74.

나성욱 외. 2010. 스마트폰과 모바일 오피스의 보안 이슈 및 대응전략. 한국정보화진흥원(NIA) 연구보고서. 서울: 한국정보화진흥원.

박광림. 2007. 웹 애플리케이션 보안의 도래와 전망. 지역정보화지. 42: 62-66.

손경호. 2010. 정보보안 산업 현황 및 전망. 정보처리학회지. 17(6): 67-75.

이형찬 외. 2010. 스마트폰 보안 기술 동향. 정보처리학회지. 17(3): 61-72.

장상근. 2010. 스마트폰 환경에서의 보안 위협. 정보처리학회지. 17(2): 64-69.

정익재. 2007. 정보보안 취약성 분석과 정책적 대응논리. 한국정책학회보. 16(2): 211-239.

정필운. 2011. 스마트 서비스 도입・확산을 위한 법제도 현황 및 개선방안. 지역정보화지. 68: 6-11.

정현철. 2006. 정보보호 침해사례 유형 및 보안대책. 지역정보화지. 40: 30-35.

행정안전부 외. 2011. 국가정보화백서 2011. 서울: 행정안전부, 방송통신위원회, 지식경제부.

방송통신위원회 보도자료. 2011. 3. 24.

European Network and Information Society Agency(enisa). 2010. *Smartphones: Information Security Risks, Opportunites and Recommendations for Users*. Brussels: enisa.

Roger, Stephen. 2011. *Increase in Number of People Using Smartphones in the UK and Europe*. London: Mobile Phone.

Say, M.ark. 2011. *CESG Provides Smartphone advice for Public Sector*. London: Guardian Government Computing.

Green, Jon. 2008. *Building Global Security Policy for Wireless LANs*. Sunnyvale: ARUBA Networks.

http://ko.wikipedia.org (wikipedia 한국판)

http://www.gchq.gove.uk (Government Communication Headquarters in the UK)

http://www.itpro.co.kr

http://www.kcc.go.kr (방송통신위원회)

http://www.i-pravacy.kr (개인정보보호 포털 사이트)

林庠圭: 연세대학교에서 행정학 박사학위를 취득하고(논문명: 우리나라 중앙정부와 지방정부 성과의 영향요인에 관한 연구), 현재 연세대학교 사회과학연구소 연구원으로 재직 중이다. 주요 관심분야는 조직이론, 성과관리, 재난관리, 정보화 등이며, 주요논문으로 "공공부문의 정성적 성과측정에 관한 연구(2006)", "소방방재청 자체평가체계의 개선에 관한 연구(2011) 등이 있다(rsk0115@paran.com).

李昌吉: 연세대학교에서 행정학 박사학위를 취득하고(논문명: 한국의 전략적 성과관리정책에 관한 연구, 2007), 현재 인천대학교 도시행정학과 조교수로 재직 중이다. 주요 관심분야는 성과관리, 정책분석 및 평가, 인사행정 등이다. 주요 논문으로는 "공공부문과 민간부문의 성과관리도구 도입이 조직성과에 미치는 영향 요인 비교 분석(2007)," "통합성과 관리체계 구축을 위하 지방 자치단체 평가의 개선방안(2008)", "공공기관의 직무급 제도 도입 방안에 관한 연구(2009)", "지역사회 국제 운동경기장 경영위기 극복방안에 관한 연구(2010)," "생활안전 분야의 표준화 및 성과관리체계(2011)" 등이 있다(changkillee@incheon.ac.kr).

金鍾業: 영국 웨일즈 대학교(University of Wales) Political & Cultural Studies 박사과정을 수료하였으며, 경희대학교, 부경대학교, 동아대학교에서 시간 강의 중이다. 주요 관심분야는 지방정부의 역할, 정보화, 문화정책 등이며, 주요논문으로 "구청공무원 윤리적 판단의 성별 차이에 관한 연구(2009)", "지방공무원의 성별 정보격차와 컴퓨터 자기 효능감(2010)", "Immigrants and the National Security: A study of Philippines's territorial claim to Sabah, Malaysia(2010", "말레이시아 종족간의 갈등 원인과 현황 연구(2011)", "창조도시 구현을 위한 문화거리 활용 방

안(2011)" 등이 있다(kimje49@hanmail.net).

투 고 일: 2011년 08월 03일
수 정 일: 2011년 08월 20일
게재확정일: 2011년 08월 27일

The Information Security Risks of Smart Age and EU5's Responses

Sang Kyu Rheem, Chang Kil Lee, Jong Eop Kim

Smartphones are now an essential tool in all sections of European society, from top government officials to businesses and consumers. In EU5 countries (the UK, Germany, France, Spain, and Italy) alone, the number of smartphone users has increased to 61 million. Smartphone have a rich cocktail of feature: an array of sensors, multiple radio and network interface, as well as gigabytes of storage and powerful processors. They are often within a meter of their owner 24 hours a day. In fact, smartphones have already realized many aspects of the vision of ambient intelligence which includes, for example, providing augmented reality applications, applications that adapt to and anticipate the user's physical environment using smart sensors– even providing smart health applications using biometric monitoring. Overall, smartphone has led to 'Smart age' with other digital devices. However, many of the security and privacy issues raised in the context of ambient intelligence apply to smartphones as well. The objective of this study is to allow an informed assessment of the information security and privacy risks of using digital devices in smart age. Most importantly, we make practical recommendation on how to address these risks. In this study we give an overview of the key information security risks and smart age in chapter two. We also categorize the information security risk and provide practical advice to address the risk in chapter three and four. Finally, we conclude with some recommendations for the solution of information security risks in South Korea.

Key words: smart phone, information security risks, european union, EU5