情 報 保 護 學 會 誌
第22卷 第8號, 2012. 12

스마트사회의 IT트렌드와 정보보호위협 및 대응방안

남 길 현*

요 약

세계는 더욱 효율적이고 인간중심적인 창조적 가치창출을 추구하는 스마트사회로 진화하고 있다. 스마트사회는 스마트 IT기술을 기반으로 모바일을 융합시켜 새로운 업무형태와 생활양식의 변화를 초래하고 있다. 본 연구의 목적은 스마트사회의 IT 트렌드를 중심으로 환경변화와 파생되는 정보보호위협을 분석하고 해결방안을 제시함으로써 다가오는 스마트사회를 보다 안전하고 신뢰성 있는 사회로 정착시키는데 도움을 주고자 한다.

Ⅰ. 서 론

최근 스마트폰의 확산과 함께 급변하는 모바일 환경은 지식정보사회를 뛰어넘어 스마트사회로 변화되고 있으며, SNS의 활성화는 개인과 그룹의 정보소통을 주도하고 있다. 이와 함께 주요정보와 개인정보유출 사건들이 빈번해 짐에 따라 국민들의 개인정보보호에 관한 관심은 급속도로 높아지고 있다. 그러나 스마트기기의 활성화에 따른 정보화의 순기능만을 강조하고 개인정보와 기업정보 유출, 자료의 변조와 악성코드의 유포, 청소년의 무분별한 유해사이트 접속 등 정보화 역기능에 대한 이해와 대응방안은 소홀하고 있는 실정이다.

한편 정부에서 추진하는 스마트 전자정부와 기업의 모바일 오피스는 IT분야의 핵심과제로서 반드시 성취되어야할 중요한 사업으로 인식되고 있다. 그러나 2011년 3월에 개인정보보호법이 제정됨에 따라 정부나 기업들은 조직의 중요정보 유출뿐만 아니라 관리하고 있는 고객의 개인정보에 대한 관리소홀 때문에 민·형사적인 책임 문제로 큰 손해를 감당해야 하는 경우가 빈번하게 발생하고 있다.

따라서 우리는 새로이 전개되는 스마트사회에 대비하여 파생되는 다양한 정보보호위협들을 도출하고 이들에 대응할 수 있는 요소기술들을 식별하고 분석함으로써 건전한 스마트사회로 진입할 수 있는 기반을 마련하도록 하여야 한다. 특히 스마트사회의 중요기술로 부각되고 있는 클라우드 컴퓨팅 환경구축을 위한 정보보호 요구사항은 스마트사회 진입을 위한 선결과제로 인식되고 있다.

또한 핵심 IT 트렌드로 인식되는 모바일 오피스 구축방안을 연구하여 우려되는 정보보호위협 요소들을 식별하고 구축방안을 제시함으로써 많은 중소기업들도 새로운 사회적 트렌드에 동참할 수 있도록 하여야 한다.

본 연구의 목적은 이와 같은 추세에 대비하여 스마트사회의 IT 트렌드를 중심으로 정보보호위협과 이에 대응할 수 있는 요소기술들을 분석하여 중소기업들도 스마트사회의 새로운 트렌드에 동참할 수 있도록 하는데 있다.

Ⅱ. 스마트사회의 IT 트렌드와 정보보호위협 분석

2.1 IT 기술진화와 스마트사회로의 환경변화

21세기는 지식정보사회에서 스마트사회로 진화하는 과정에 있다고 할 수 있다. 지난 2012년 5월에 개최된 서울디지털포럼 2012에서 세계의 석학들은 다가오는 미래의 사회 또는 현재 진행되고 있는 새로운 패러다임은 스마트사회로 변화하는 과정이라고 제시하였다[1]. 이제 IT기술을 기반으로 새롭게 전개되는 스마트사회의 개념을 파악하고 주요요소들을 식별하여 변화를 주도적으로 이끌어 갈 수 있도록 함으로써 글로벌 경쟁에서 우위를 점할 수 있는 국가사회의 선진화를 이루도록 하여야 한다.

* 한국과학기술정보연구원전문연구위원, khnammk@reseat.re.kr,

가. 스마트사회의 개념과 환경변화

스마트사회의 정확한 정의는 아직 공식화되어 있지 않은 상황이다. 다만 '스마트(smart)'의 의미가 멋있고 유능한 뜻을 지니고 있다고 볼 때 현재보다 진화된 더 나은 미래사회를 뜻한다고 할 수 있다. 스마트기술을 적용한 스마트기기들을 기반으로 인간중심, 창의성, 행복중심과 같은 새로운 가치를 창출함으로써 기존의 가치와는 다른 효율적이고 새로운 변화를 추구하는 사회라고 개념을 부여할 수 있을 것이다.

IT기술에서 진화된 스마트기술을 기반으로 스마트사회를 주도하는 핵심적인 요소는 융합과 모바일이라고 할 수 있다. 융합이란 다양한 요소기술들을 접목시켜 새로운 가치를 생산하는 복합적인 사고의 틀 속에서 발전하고 있으며 최근의 추세는 스마트폰의 확산과 더불어 모바일이 가장 중요한 요소로 인식되고 있다.

스마트사회는 인간중심의 지능형사회이며 스마트기기들을 활용하여 일하는 방식 및 생활양식, 사회문화 등 국가사회 전반에 걸쳐서 혁신을 통한 새로운 가치 창출을 도모하는 사회라고 할 수 있다. 우리의 일상생활은 스마트폰과 모바일앱을 활용한 새로운 문화를 창조하고 스마트워크, 소셜비즈니스, 모바일 뱅킹, 모바일 콘텐츠, 클라우드 컴퓨팅 등 다양한 모습으로 변화하고 있다.

그러나 스마트사회가 모든 면에서 순기능적인 역할만 수행한다고 할 수는 없다. 이와 같은 변화의 이면에는 정보화 역기능으로서 정보보호위협과 개인의 프라이버시 침해, 컴퓨터 중독과 인간성의 피폐 등 스마트사회가 성숙되기 이전에 반드시 해결되어야 할 선결과제들이 쌓여 있다.

따라서 본 연구에서는 스마트사회의 실현을 위한 순기능적인 주요요소들을 파악함과 아울러 해결해야 할 역기능적인 문제점들도 함께 제시하고자 한다.

나. 스마트사회의 새로운 IT 트렌드

첫째, 스마트사회의 가장 두드러진 특성은 스마트폰의 확산이라고 할 수 있다. 스마트폰의 세계시장은 애플사의 아이폰과 삼성전자의 갤럭시가 양분하고 있다고 볼 수 있으며, 두 회사는 주도권 확보를 위하여 디자인과 기능성 향상에 온 힘을 쏟고 있다. 최근에는 특허권 분쟁으로 세계의 이목을 집중시키고 있으며 국가 간의 보호무역주의라는 비판도 받고 있다. 우리나라는 스마트폰 사용자가 거의 3천만 명에 다가서고 있으며 인구대비 세계에서 가장 빠른 증가세를 보이고 있다. 음성전화기능에서 출발하여 메시지 전달기능을 첨가하는 형태에서 진화된 스마트폰은 이제 오히려 문자와 영상이미지를 더 많이 활용하는 기기로 변모하고 있다.

둘째, 소셜네트워크서비스(SNS)의 확산이라고 볼 수 있다. SNS(Social Network Service)란 인터넷을 기반으로 인적 네트워크 형성 및 인맥관리를 할 수 있게 해주는 서비스로 연결을 통한 사회적관계의 구축을 지향하는 서비스라고 할 수 있다. 개인 간의 인맥구축이라는 활용목적에서 출발하여 이제는 기업, 비즈니스, 정치 등 다양한 분야에 활용되면서 그 범위를 넓혀가고 있다. SNS의 대표 주자는 페이스북과 트위터라고 할 수 있으며 SNS의 등장으로 개인과 그룹의 의사소통이 급속도로 확대되고 새로운 정보교환과 소통의 문화를 만들어 가고 있다[2].

셋째, SNS가 활성화되면서 현재 포털 및 쇼핑몰을 통한 소비자의 정보습득과 구매활동을 벗어나서 SNS를 이용하는 방식으로 한 새로운 비즈니스가 소셜비즈니스 형태로 나타나고 있다. SNS를 비즈니스에 활용할 경우 비교적 저렴한 비용과 원활한 커뮤니케이션, 그리고 빠르고 광범위한 전파력을 장점으로 생각할 수 있다. 변화하는 소비트렌드를 반영할 수 있는 소셜비즈니스는 소셜커머스, 소셜러닝, 소셜게임, 소셜마케팅, 소셜고객관리 등 다양한 영역으로 확장되고 있다. 그리고 1인 기업이라는 새로운 창조적 기업영역을 개척하고 있다고 본다.

넷째, GPS를 탑재한 단말이 확산되면서 위치기반과 융합된 다양한 위치기반서비스가 관심을 받고 있다. 위치기반서비스(Location-Based Service)란 무선통신망 및 GPS 등을 통해 얻은 위치정보를 바탕으로 사용자에게 위치에 따른 특정 정보를 제공하는 서비스를 의미한다. 위치기반서비스는 현 위치의 주변정보 제공, 길 찾기, 교통정보, 장애인 위치정보, 친구 찾기, 재난 위치, 특정 물체의 추적 등 다양한 용도로 범위가 확대되고 있으며 프라이버시 침해문제도 이슈화되고 있다[3].

다섯째, 현대의 업무형태와 생활양식에 큰 변화를 주고 있는 스마트워크도 인간중심의 새로운 문화를 만들어가고 있는 중요한 트렌드라고 볼 수 있다. 언제 어디

서나 필요한 정보를 얻을 수 있고, 하고 싶은 일을 할 수 있는 행복중심의 가치를 창출하는 중요한 형태라고 볼 수 있다. 일하는 방식의 획기적인 변화를 추구하는 스마트워크는 서류위주의 탁상업무를 현장중심의 즉시 처리로 결재를 간소화하고 칸막이 식 업무에서 비롯된 의사결정 지연현상을 원격협업을 통한 실시간 문제해결과 신속한 의사결정을 할 수 있도록 해준다. 또한 육아, 장애, 고령으로 인한 취업제한을 재택근무 또는 근무형태를 다양화시킴으로서 취약계층에게도 취업기회를 확대할 수 있는 방식이다.

여섯째, 클라우드 컴퓨팅의 확산이라고 할 수 있다. 지금까지 정보의 공유와 소통에 중점을 두었지만 이제는 정보뿐만 아니라 컴퓨팅 기기들과 분석능력까지도 공유할 수 있는 클라우드 컴퓨팅 환경은 국경을 초월하여 범세계적으로 인간사회를 통합시켜 나가는 촉매역할을 할 것으로 예상된다. 클라우드 컴퓨팅 환경이 정착된다면 최소사양의 모바일기기만으로서 편리하고 효율적으로 자료를 수집, 분석하고 업무에 활용할 수 있는 사회가 이루어지리라 생각된다. 이와 같은 클라우드 서비스에 대해서는 우리나라뿐만 아니라 EU, 캐나다, 영국, 호주, 싱가포르 등 여러 선진국들이 중요한 정책으로 추진하고 있다[4].

일곱째, 스마트기술을 탑재한 스마트 디바이스들이 새로운 생활양식의 변화를 유도할 것이다. 대표적인 디바이스로는 스마트TV를 들 수 있다. 스마트TV는 컴퓨터 운영체제가 탑재되어 인터넷의 모든 콘텐츠와 어플리케이션의 이용을 가능하게 하며 인터넷과 방송을 융합시켜 시너지 효과를 만들어 내는 TV라고 할 수 있다. 지금까지의 수신전용 TV에서 진화하여 양방향 통신이 가능하고 맞춤형 기능을 강화하여 개인의 취향에 맞는 프로그램의 설정까지 기능을 확장할 것으로 예상된다. 또한 스마트TV 뿐만 아니라 스마트 냉장고 등 가전기기와 스마트 홈시큐리티 제품도 등장할 것으로 생각된다.

여덟째, 마지막으로 앞에서 언급한 다양한 트렌드를 실현하기 위해서 가장 중요하다고 할 수 있는 정보보호와 개인의 프라이버시 보호가 중요한 선결과제로 주목받고 있다. 스마트사회를 견인할 원동력이 되는 IT기술은 항상 관련된 다양한 정보를 다루고 있다. 따라서 수집, 저장, 유통되는 정보를 보호하고 개인의 프라이버시를 보호하는 일은 개인과 기업 모두에게 중요한 분야이다. 최근 개인정보보호법이 제정되어 개인정보를 다루는 기업의 책임이 더욱 무거워지고 있으며 기업의 독자기술을 보호하는 일은 기업의 성패를 좌우하는 핵심 과제로 인식되고 있다[5].

다. IT기술과 모바일의 융합

지금까지 살펴본 스마트사회의 새로운 트렌드는 사실상 IT기술과 모바일의 융합에서 비롯된 트렌드라고 볼 수 있다. 즉 스마트폰과 태블릿 PC 등을 더욱 편리하고 손쉽게 구할 수 있는 환경이 되면서 모바일과 관련된 융합서비스와 제품이 급속도로 발전하게 된 것이다.

특히 모바일 콘텐츠 산업을 이끄는 핵심으로 떠오른 모바일 어플리케이션은 무선네트워크의 진화, 모바일 인터넷 환경의 확대, 스마트기기의 확산에 힘입어 사용이 급속도로 증가하고 있는 분야이다. 모바일앱으로 불리는 모바일 어플리케이션(Mobile Application)은 사용자가 모바일 디바이스를 이용하여 정보를 얻거나 필요한 특정기능을 실행할 수 있도록 해주는 응용소프트웨어를 말한다. 최근의 추세는 공공기관이 민간에게 보유하고 있는 양질의 정보를 개방하는 방향으로 나가고 있으며 기업뿐만 아니라 창의적인 아이디어를 갖고 있는 개인들도 적극적으로 모바일앱을 개발하는데 나서고 있다.

또한 스마트폰을 중심으로 모바일 기능을 탑재한 디바이스들의 확산에 기반을 둔 SNS를 이용하는 서비스들은 새로운 생활방식과 문화를 창출해 나가고 있다. SNS는 인터넷과 모바일 기능에 힘입어 빠른 전파력과 광범위한 정보전달을 장점으로 내세우고 있다. 이와 함께 페이스북, 트위터 등의 인간관계중심의 친근성을 바탕으로 실시간으로 전달되기 때문에 비즈니스 차원에서의 파급력과 동조화 세력을 규합하는 정치적인 파워까지 기대할 수 있는 막강한 파워집단으로 성장하고 있다.

금융서비스의 양상도 모바일과 융합된 대표적인 변화이다. 이제는 은행, 증권회사, 우체국과 같은 금융기관을 방문하여 시간과 노력을 소모하는 형태는 많이 달라지고 있다. 사무실에서 또는 이동 중에도 마음대로 손쉽게 금융 업무를 할 수 있고 다양한 분석자료 까지 제공받을 수 있다. 이러한 변화는 우리의 생활양식과 생각하는 방식에도 커다란 변화를 초래할 것으로 본다.

2.2 스마트사회의 정보보호위협 형태

지금까지 새로운 미래사회를 지칭하는 스마트사회의 변화된 모습들을 부분적으로 조명해 보았다. 스마트사회는 현재보다는 훨씬 효율적이고 인간중심의 살기 좋은 사회일 것이라고 누구나 예측하고 있으며 스마트사회의 성공적인 실현을 위하여 민간뿐만 아니라 정부에서도 기반구조를 확충하고 인력과 예산을 투입하는 등 적극적인 투자와 국가전략을 수립하고 있다. 그러나 스마트사회의 새로운 트렌드에서 살펴보았지만 스마트사회의 순기능적인 장점의 이면에는 항상 역기능적인 함정들이 내재되어 있다는 사실을 간과하여서는 안 된다. 이들 모든 스마트서비스들은 IT기술뿐만 아니라 다양한 정보를 인간과 결합시키고 있으며 이를 이용하여 불법적인 방식으로 개인 또는 집단의 이익을 도모하고자 하는 범죄적인 행위가 일어나고 있다. 여기에서는 스마트사회에서 파생되는 정보보호위협의 형태를 살펴보고자 한다.

가. 정보보호의 개념과 범위

○ 정보보호란 정보의 생성, 유통, 활용, 저장, 폐기 등의 생명주기 동안 정보시스템을 안전하게 보호하여 정보의 비밀성, 무결성, 인증성, 부인봉쇄와 가용성을 보장하여 신뢰성을 확보하는 것을 의미한다. 여기에서 정보시스템에는 정보(데이터)와 운영시스템을 포함하며 최근에는 관련되는 인적인 요소까지 포함하기도 한다.

○ 비밀성은 외부로 공개되어서는 안 되는 주요정보가 허가되지 않은 제3자에 의해서 외부로 유출되지 않도록 하는 것이다. 지금까지 금고 속에 보관하던 중요한 자료가 이제는 디지털화되어 정보시스템에 저장되기 때문에 해커나 악의적 범죄자에 의해서 외부로 유출되는 것을 막아야 한다. 특히 기업 고유의 특허나 기술정보가 유출된다면 기업에 치명적인 손해를 입힐 수 있으며, 정부나 공공기관의 비밀정보가 누출될 때도 국가정책이나 안보에 미치는 파급효과가 막대하게 된다.

○ 무결성이라 함은 정보시스템에서 취급되고 있는 정보가 허가되지 않은 사람에 의해서 변조되거나 생성, 삭제되지 않고 항상 정확한 상태로 유지됨을 의미한다. 컴퓨터의 기본적인 특성은 속도가 빠르고 정확하다는데 있다. 여기에서 속도보다는 정확성이 더 중요한 특성이다. 아무리 빠르고 편리하다고 해도 답이 틀리거나 거짓정보가 제공된다면 오히려 해악이 되는 결과를 초래할 수 있다. 이와 같은 무결성을 보장하기 위해서는 해커들의 침입을 방지하고 입출력시스템에 오류가 발생하지 않도록 주의하여야 하며 관련 소프트웨어를 잘 관리하여야 한다.

○ 인증성은 서로 정확한 상대를 확인하는 것을 의미한다. 통상 우리가 전화통화에서 상대방을 확인하기 위해서는 전화번호나 목소리 또는 영상통화 모습으로 한다. 이와 마찬가지로 컴퓨터와 컴퓨터, 컴퓨터와 사람 또는 프로세서 간에 정보를 교환할 때는 상대방을 정확하게 확인할 수 있어야만 받은 정보의 출처를 알 수 있고 또한 보내는 정보의 안전성을 확인할 수 있게 된다. 요즈음 난무하는 스팸 메일이나 메시지 또는 보이스피싱 등은 인증성을 보장하지 않은데서 발생한다고 볼 수 있다.

○ 부인봉쇄라 함은 송수신된 정보에 대하여 추후에 송수신 사실 자체를 부정하거나 송수신된 정보에 고의 또는 실수로라도 오류가 발생했을 때 진위와 책임 소재를 명확히 하여 함부로 거짓 행위를 할 수 없도록 하는 것이다. 중요한 문서를 송수신하거나 쌍방 간에 계약문서를 체결할 때 추후에 분쟁이 발생하지 않도록 하기 위함이며 전자서명법에 의하여 기록된 전자서명은 법적인 효력을 갖게 된다.

○ 가용성은 정상적으로 정보시스템을 사용하도록 허가된 사용자는 필요한 때 항상 필요한 정보를 사용할 수 있도록 해주는 것이다. 앞에서 논의된 사항이 대부분 허가되지 않은 범죄적인 시스템 침해 행위로부터 보호하는 것인데 반해 가용성은 시스템과 정보의 안정성에 중점을 두고 있다. 따라서 가용성 보장을 위해서는 우선적으로 정보시스템을 다중화하고 데이터의 백업이 가장 중요하게 다루어진다. 특히 지난번 미국의 9·11 테러사건 이후에는 원격 실시간 데이터 백업이 중요하게 인식되고 있다. 9·11 테러에서 손상을 입었던 기업들 중에서 실시간으로 원격 백업을 시행했던 기업들은 대부분 원상을 회복하였지만 그렇지 못했던 기업들은 거의 도태되었다는 보고가 있었다.

나. 스마트사회의 개인정보보호위협

개인정보란 살아있는 인간 개인에 관한 정보로서 성

명, 주민등록번호, 여권번호 등 개인을 식별할 수 있는 고유의 정보뿐만 아니라 정보시스템에 접근하는데 필요한 ID나 패스워드 또는 지문과 같은 생체정보 등을 지칭한다. 또한 광의의 개인정보는 유일하지 않더라도 서로 조합되어서 개인을 식별할 수 있는 정보까지 포함한다. 이러한 개인정보는 유출되거나 남용되었을 경우에 개인의 프라이버시를 침해하고 명예훼손이 발생할 수 있으며 개인을 사칭하여 범죄적인 목적에 악용될 소지가 있으므로 법적으로 강력한 규제를 하고 있는 실정이다.

따라서 스마트사회에서 개인정보는 반드시 보호되어야할 필수적인 사항이다. 스마트사회의 큰 특징은 IT기술이 모바일과 융합되어 편리한 서비스를 제공하는데 있다. 그러나 이러한 모바일서비스에 접속하기 위해서는 대부분 사용자나 회원 등록을 해야 하며 이러한 등록과정에서는 개인이 소지하고 있는 스마트기기 정보나 개인정보가 사용되고 있다. 또한 서비스제공자는 수집된 개인정보를 안전하게 보관하고 관리할 책임을 지게 된다.

지난 2011년 3월에 제정된 개인정보보호법은 기업이나 서비스제공자가 개인정보를 수집, 이용, 제공 및 파기 등 단계별로 준수해야 할 법적인 요구사항을 명시함으로써 개인정보주체의 자기결정권을 강화하고 이를 위반하거나 나태하여 개인정보가 유출되거나 남용되었을 때는 형사적 또는 민사적 책임을 지도록 규정하고 있다[5]. 이는 개인정보가 외부로 유출되었을 때는 개인의 명예훼손이나 타 범죄적 목적으로 오용될 소지가 크기 때문이다.

최근 헌법재판소는 인터넷서비스를 제공하는 포털업체에서 블로그나 게시판에 의견을 게시할 때 개인 실명을 요구하는 것은 헌법에 보장된 표현의 자유를 억압하는 행위로 헌법에 위배된다는 판결을 내린바 있다. 그러나 요금을 부과하거나 금융서비스와 같은 민감한 서비스를 이용하기 위해서 처음으로 등록할 때는 개인을 식별할 수 있는 인증과정이 필수적인 것으로 인식된다. 그러므로 어떤 형태로든 서비스제공자는 개인정보를 수집할 수밖에 없는 실정이다. 다만 어떤 방법으로 수집되는 개인정보를 최소한으로 하고 안전하게 관리하도록 할 것이냐가 중요한 과제가 되고 있다.

먼저 개인정보가 불법적인 해킹이나 실수로 외부에 유출되었을 때 발생할 수 있는 피해를 살펴보자. 현재 대부분의 회원가입은 인터넷상에서 비 대면으로 개인을 확인하여 인증하기 때문에 다른 사람을 사칭하여 회원에 가입하여 서비스를 받을 수 있으며 만약 금융업무와 관련된 개인정보가 패스워드와 함께 도용되면 금전상의 손해도 발생할 수 있다. 또한 원격 접속하여 타인의 접근권한을 이용하여 중요정보를 유출하거나 손상시킬 수 있는 위험을 안고 있다.

최근에 발생되고 있는 개인정보관련 사고들은 회원정보를 관리하도록 위탁받은 자회사 직원이 판매를 목적으로 고의적으로 고객정보를 대량으로 유출하거나 해킹에 의해서 대량으로 유출 되는 것, 또는 관리소홀로 고객정보가 유출되는 경우가 많으며 수집된 정보를 목적이외의 용도로 사용하는 경우도 많다. 이러한 경우에 대부분 금전적 또는 정신적 피해보상을 요구하는 민사소송으로 진행되고 있으며, 이제는 개인정보보호법에 의해 단체소송이 가능해짐에 따라 소송규모가 더욱 확대되는 추세이다.

다. 스마트폰과 모바일앱의 정보보호위협

스마트폰은 가장 대표적인 스마트사회의 모바일기기로 정착되고 있다. 가장 빈번한 위협은 분실 및 도난이라고 할 수 있다. 최근에는 불법적 거래를 위하여 스마트폰을 훔치거나 분실된 스마트폰을 수집하여 판매하는 사례도 적발되고 있다. 그러나 스마트폰 자체의 재산적 가치보다 속에 내장되어 있는 정보의 가치가 훨씬 크다고 볼 수 있으며 내장된 정보가 유출되거나 분실된 스마트폰으로 외부에 접속하여 사용자를 사칭할 수도 있다. 모바일 쇼핑을 통하여 금전적 손해 가능성도 있지만 내장되어 있는 개인의 사진이나 동영상, 또는 사적인 비밀자료가 유출될 때는 심각한 프라이버시 침해와 명예훼손으로 확대될 수도 있다.

다음으로는 모바일 악성코드에 감염되어 개인정보가 유출되거나 기기의 동작에 오류가 발생하고 비정상적 과금이 발생할 가능성이 높다. 악성코드로서는 바이러스, 트로이 목마 등 PC에서 감염될 수 있는 모든 위협이 그대로 상존한다고 볼 수 있다. 특히 좀비 컴퓨터와 같은 악성코드에 감염되면 DDoS 공격과 같은 공격행위에 가담하여 엉뚱한 피해자를 양산하는데 참여하게 된다.

스마트폰의 기능성을 향상시키기 위한 위치기반 서

비스가 다른 목적으로 오용되어 개인정보를 유출하거나 프라이버시 침해를 받을 수 있다. 또한 마이크나 블루투스의 비인가적 접속으로 정보를 유출하는 경우도 발생되며 근거리 전파도청장치의 표적이 되기도 한다. 한편 분실 했을 때 정보가 유출되는 것을 방지하기 위하여 만들어진 원격 정보삭제 기능이 제3자에 의해서 실행되어 내부정보가 손상될 수도 있다.

스마트폰의 또 다른 장점은 수십만 건에 달하는 다양한 어플리케이션 프로그램 즉 모바일앱을 이용하거나 다운로드 받아 편리한 업무나 기능을 수행할 수 있다는 것이다. 그러나 모바일앱은 신뢰성이 검증되지 않은 경우가 많아 홍보된 기능과는 다른 역할을 실행할 수도 있다. 악성코드를 전파하는 매체로 활용되기도 하며 스파이웨어로 둔갑하여 스마트폰의 내장정보를 유출시킬 수 있고, 외부접속 시 실시간정보를 특정 사이트로 전송할 수도 있다.

라. SNS 기반의 서비스와 비즈니스에서의 정보보호위협

SNS의 장점으로서는 자유스럽게 자기 개인의 생각이나 경험을 표현할 수 있고 취득한 정보를 서로 공유하며 사람들과 더욱 친밀한 인간관계를 맺고 이렇게 맺어진 인적 네트워크를 관리할 수 있다는 것이다. 누구나 콘텐츠를 만들 수 있고 이를 관계를 맺고 있는 사람들에게 빠르게 전파할 수 있기 때문에 소셜미디어의 대표적인 페이스북과 트위터의 가입자는 4-5년 만에 수억 명을 초과하는 엄청난 속도로 확산되고 있다. 이제는 국내 네티즌들은 절반 이상이 소셜미디어를 이용하여 의사소통을 하는 것으로 조사되고 있다.

이러한 장점을 기반으로 SNS를 이용하여 정치 또는 경제적 이익을 추구하는 새로운 소셜비즈니스가 확산되고 있다. 정치적으로는 시민들의 선거참여를 독려하고 여론을 주도하며 오프라인상의 군중효과를 확대하여 새로운 정치세력으로 군림하는 경우가 발생하고 있다. 지난해 아프리카의 이집트와 리비아의 반정부 시위에서는 트위터 등을 이용한 정보의 공유와 여론조성이 결정적인 역할을 했다고 평가되고 있다. 또한 기업의 노사분쟁에서도 여론을 수렴하고 특정방향으로 유도하며 유리한 분위기 조성에 활용되기도 한다.

경제적인 분야에서는 소셜미디어가 더욱 활발하게 이용되고 있다. 새로운 전자상거래 형태인 소셜커머스를 시작으로 다양하고 창의적인 비즈니스모델이 발굴되고 개인의 창의적 아이디어를 더욱 중요하게 인식하게 되었다. 특히 소셜미디어를 활용한 제품 및 서비스의 제작과 판매 그리고 홍보까지 책임지는 소셜비즈니스가 등장하고 있다. 이러한 비즈니스의 확산은 개인과 기업의 일자리를 창출하고 새로운 기업전략과 창조의 정신을 중시하는 새로운 가치변화를 주도하고 있다.

그러나 이러한 SNS의 확산에서도 우려되는 역기능은 다양하게 나타나고 있다. 제일 먼저 우려되는 것은 개인정보의 유출문제이다. 처음 가입할 당시에 제공되었던 개인정보와 서로의 인간관계가 더욱 친숙해짐에 따라 상대방의 개인정보와 행동을 서로 알게 되고 공유함에 따라 고의 또는 실수에 의해서 개인정보가 유출되기 쉬어진다. 사적인 정보와 공적인 정보의 경계가 불분명해지고 국민의 알 권리와 표현의 자유를 앞세워 무분별한 폭로나 사이버 폭력 등은 개인의 프라이버시 침해와 명예훼손 등의 위협이 되고 있다.

또한 개인과 기업/정부 간에 소셜미디어를 통한 감시사회가 되는 측면을 생각할 수 있다. SNS를 이용하여 편의성과 효율성을 창출할 수 있지만 한편으로는 그것 자체가 활동을 제약하는 족쇄로 작용할 수 있다. 개인의 행동반경이나 행위가 노출되고 통신내용이 도청되어 어떠한 불이익을 받을 수도 있는 것이다.

그리고 과도한 SNS는 새로운 스트레스와 불안의 원인이 되고 있다. 소셜미디어에 가입한 순간부터 개인정보의 유출과 오남용에 대한 불안감이 증대된다는 사실은 여러 가지 설문조사에서 확인되고 있다. 더 나아가서는 SNS에 너무 심취되어 중독 현상으로 빠져드는 사례가 많이 발생하고 있다. 이러한 중독 현상은 그룹화 되어 그들만의 폐쇄된 가치관과 비도덕적인 또는 범죄적인 행위로 까지 연결될 수 있다. 중독이 되면 정상적인 일상생활을 유지하기 어렵게 되고 학생은 공부에 전념할 수 없는 정신상태가 될 수 있다. 또한 리더의 생각이나 지시에 맹종하는 습관으로 이성적 판단이 어렵게 되어 잘못하면 나쁜 방향으로 쉽게 탈선할 수 있게 된다.

SNS는 미래사회의 새로운 소외계층을 양산할 수 있는 가능성도 갖고 있다. SNS의 특성상 기존의 개별적인 인터넷 환경보다 이용자의 능력과 노력 또는 적극성에 따라 인맥활동의 범위와 경제적 이익 혹은 계급적 신분이 차이가 날 수 있으며 그룹에 동조화되지 못하거나 자신의 취향에 맞지 않을 때는 오히려 소외계층으로

전락하거나 격리될 수 있다. 소셜미디어로 인한 사회적 고립감과 소외감은 더욱 집착과 중독으로까지 발전될 수도 있어서 양극화 현상을 더욱 부추길 수도 있다.

그러나 가장 우려되는 상황은 정보왜곡, 미확인정보 유포, 악의적인 선동 등으로 파생되는 사회적인 혼란과 경제적 손실을 유발하는 SNS의 효과라고 할 수 있다. 특히 정부기관이나 국가안보와 관련되는 사실을 왜곡하여 거짓정보를 퍼뜨리고 사회불안을 조성하거나, 특정 집단이나 개인의 목적을 위하여 편향되게 SNS를 이용하며, 여기에 합리적인 판단이나 비판 없이 맹목적으로 수용하는 행태는 건전한 사회발전을 저해하고 공공의 신뢰성을 떨어뜨리는 위협이 되고 있다.

마. 스마트워크와 위치기반서비스의 정보보호위협

스마트워크란 언제 어디서나 시간과 장소에 구애받지 않고 업무를 수행할 수 있도록 해주는 선진화된 근무체제를 뜻하며 모바일 오피스, 재택근무, 스마트워크센터 등이 복합적으로 이루어진 선진화된 근무체제이다. 정부는 공공부문에 먼저 스마트워크를 도입한 후 민간부분으로 확대시킨다는 전략을 수립하였다[6]. 스마트워크가 활성화 된다면 시간과 공간의 제약 없이 네트워크를 통하여 상호 교류하고 협력하는 수평적 협업문화가 확산되어 더욱 효율적인 업무가 이루어지며 수직적인 현재의 근무행태에 변화를 주는 것이라고 볼 수 있다.

이러한 스마트워크에서도 정보보호위협은 기업에게 큰 손실을 안겨줄 수도 있다. 외부에서 이용하는 스마트워크센터나 모바일 오피스 환경의 정보보호시스템이 조화가 이루어지지 않거나 미흡하여 송수신되는 정보가 도청되어 기업비밀이 외부로 누출될 수 있다. 외부에서 사용하는 정보시스템에 악성프로그램이 장착되어 회사 고유의 기업비밀이 경쟁상대에게 유출되거나 공개되면 회사에게 치명적인 손실을 입히게 된다. 또한 기업에서는 외부에서 모바일 근무를 하는 직원의 행동반경을 감시하는 수단으로 사용될 수 있으며 이는 개인의 프라이버시 침해로 간주될 소지를 안고 있다.

GPS 기능을 탑재한 스마트기기들의 증가에 힘입어 위치기반 서비스를 이용하는 비즈니스모델들이 많이 나타나고 있다. 위치기반 서비스는 대부분 편의성과 재난방지와 같은 분야에서 많이 활용되고 있다. 그러나 본래의 목적과는 다르게 오히려 프라이버시를 침해하거나 개인정보가 누출되는 상황이 발생할 수 있다. 영유아의 납치를 방지하고 길을 잃어버리지 않도록 하기위한 장비가 오히려 납치를 용이하게 만들거나 상대방을 감시하고 프라이버시를 침해하는 수단으로 변질될 수 있다. 흥신소에서 배우자나 타인의 약점을 추적하기 위한 도구로 사용되기도 한다. 또한 GPS는 인공위성에서 제공하는 위치정보를 수신하여 위치를 확인하기 때문에 의도적인 GPS 전파 교란 장비나 천둥번개와 같은 외부적인 상황에 의하여 잘못된 정보를 수신할 수 있다. 만약 GPS정보에 완전 의존적인 경우에는 심대한 피해를 유발할 수도 있다. 특히 비행기나 유도미사일과 같은 경우에는 GPS 교란에 대한 대비책이 필요하다.

바. 클라우드 컴퓨팅과 빅데이타의 정보보호위협

클라우드 컴퓨팅은 인터넷기술을 활용하여 소프트웨어, 스토리지, 서버, 네트워크 등의 IT 자원을 서비스로 제공하는 컴퓨팅 형태로서 IT 자원을 필요할 때 필요한 만큼만 빌려서 사용하고 사용한 만큼의 비용을 지불하도록 하는 방식이라고 볼 수 있다. 2010년 Gartner 보고서에 따르면 최근의 추세는 차세대 IT 기반구조와 응용분야에서 클라우드 컴퓨팅은 매우 빠르게 시장규모를 확장할 것으로 예측되고 있다. 클라우드 컴퓨팅의 편리성과 확장성을 기반으로 다양한 디바이스들을 연계하여 서비스를 제공하는 오픈환경의 플랫폼 및 운영체제들이 나오고 있다.

특히 모바일 클라우드 컴퓨팅은 기존의 데스크탑 클라이언트와 서버 관계에서 벗어나서 모바일 단말을 이용하는 클라우드 컴퓨팅 개념을 더욱 효율적으로 실현할 수 있는 방식이다. 그러나 클라우드 서비스 제공자들이 범세계적이고 이를 사용하는 사용자들도 전 세계적으로 분포되어 있기 때문에 각 국가별로 법과 제도가 상이하며, 국제적인 표준도 아직 미흡한 상황에서 정보보호위협은 여러 곳에 산재되어 있다.

먼저 서비스 제공자가 갖고 있는 서버의 정보보호기능이 요구되는 수준에 부합하지 못하거나 고의로 또는 부주의해서 악성코드에 감염되어 있으면 개인정보가 유출될 수도 있으며 거짓정보가 혼돈을 초래할 수 있다. 특히 서비스 제공자와 사용자가 최초 접속할 때 사용되는 인증방식에 차이가 있을 때는 효율성이 떨어지고 분

쟁의 소지가 될 수 있다.

기본적으로 클라우드 컴퓨팅은 서비스 제공자 규모면에서 양극화 현상이 심화되고 대형 서비스 제공자는 서비스 과정에서 수집되는 다양한 정보를 바탕으로 다양한 분석방법을 활용하여 소비자가 원하지 않은 내부정보를 양산할 수 있다. 이를 바탕으로 소규모 서비스 제공자와 사용자를 압도하는 빅브라더 또는 빅데이터의 위협을 초래할 수 있으며 장차 심각한 사회적인 문제로도 발전될 수 있다. 2012년 3월 구글이 발표한 정보의 통합정책은 클라우드 컴퓨팅 분야에서도 나타날 수 있는 유사한 빅데이타의 위협을 경고하는 사례라고 할 수 있다[7].

2.3 모바일 전자정부의 보안 취약점

가. 인증과 접근권한의 통제

안전성, 편리성, 다양성을 추구하는 모바일 전자정부는 다양한 모바일 접속 기기들이 정부의 컴퓨터시스템에 접속하기 때문에 기존의 전자정부에서 보다 더 큰 위협에 직면하게 된다. 모바일 전자정부는 서비스를 관리하고 정보를 업데이트하는 공무원뿐만 아니라 정보와 서비스를 사용하는 온 국민을 상대로 서비스를 시행하기 때문에 접속 시 개인에 대한 인증과 서비스 요청 시 해당하는 권한 여부를 명확히 하여야 한다. 개인 인증을 위하여 실명과 주민등록번호를 이용하는 기존의 방식은 모두 헌법에 불합치하거나 개인정보보호법에 저촉된다는 판결이 나왔다. 따라서 이를 대신할 수 있는 새로운 시스템이 갖추어져야 한다.

정부 게시판에 익명의 사용자가 헛소문이나 왜곡된 정보를 전파한다면 그 파급효과가 막대한 피해를 유발할 수 있다. 단순한 기업이나 개인의 블로그에 게시된 의견과는 비교할 수 없는 사회적 혼란을 예상할 수 있다. 또한 개인의 가족관계나 재산현황을 파악할 수 있는 데이터베이스가 허가되지 않은 제3자에게 공개된다면 프라이버시 침해는 물론 범죄에 악용될 가능성이 높아진다. 분실된 스마트폰을 이용하여 타인을 사칭하고 정부시스템의 권한관리의 취약점을 공격하고자 하는 공격수들이 모바일기기들의 익명성을 이용하여 시스템에 접속하는 위협은 훨씬 증가할 것으로 예상된다.

나. 모바일기기 상호운용성과 모바일앱 위협

모바일 전자정부는 국민편의성 제고를 위한 대 국민 서비스와 공무원의 효율적인 업무수행을 위한 행정업무서비스 구축을 위하여 모바일 공통기반을 구축하였다. 여기에는 다양한 모바일 기기들과의 상호운용성이 중요하게 다루어지고 있다. 그러나 이들 모바일 기기들은 서로 다른 운영체제를 갖고 있으며 아직 표준화된 지침이 없기 때문에 보안기능도 상이하다고 볼 수 있다. 모바일 기기에 내재되어 있는 정보보호 취약점을 이용하여 전자정부시스템의 보안기능을 약화시킬 가능성이 존재한다.

또한 모바일 전자정부는 모바일웹과 모바일앱을 개발하여 여러 가지 민원업무와 행정서비스의 질적 향상을 도모하고 국민과의 소통강화, 업무 생산성의 극대화를 추진하고 있다. 국가대표포털(m.korea..go.kr)을 통해 2012년 6월 현재 정부가 제공하는 모바일앱은 408건, 모바일웹은 329건으로서 계속 큰 폭으로 증가하고 있다[8]. 그러나 모바일앱을 사용하는 기기가 악성코드에 감염되어 있을 때는 심각한 위협을 주는 공격방법이 나올 수 있다. 아직은 완전한 보안기능을 확인하기 어렵기 때문에 개발된 모바일앱의 취약점을 이용한 정보보호위협이 끊임없이 발견되고 있다.

다. 시스템의 효율성과 정보보호 대책의 불균형

모바일 전자정부의 일차적인 특성은 수많은 국민을 상대로 하는 서비스를 제공하기 때문에 시스템의 효율성과 편의성이라고 생각할 수 있다. 그러나 이들 서비스에서 정보보호 대책은 항상 효율성과 편의성에 제동을 거는 역할을 수행한다고 할 수 있다. 즉 정보보호 기능을 추가함으로써 시스템의 반응 속도가 느려지고 사용자 관리와 인증 및 권한확인 등을 위하여 까다로운 절차를 필요로 한다. 따라서 서비스 개발자들은 정보보호의 중요성을 잘 인식하지 못하는 사용자들의 설문이나 만족도 평가에서 좋은 결과를 얻기 위하여 고의적으로 절차를 단순화 시키는 경향이 있다. 이러한 현상은 결과적으로 정보유출이나 오남용의 사고로 연결되고 모바일 전자정부의 신뢰성을 떨어뜨리는 위협요소가 되고 있다.

현재 우리나라의 대부분의 기업이나 조직에서는 IT

를 담당하는 CIO(Chief Information Officer) 산하에 정보보호를 담당하는 책임자가 임명되는 조직구조를 갖고 있다. 시스템의 효율성을 강조하는 CIO의 입장과 시스템의 정보보호기능을 준비하는 보안담당자와의 사이에 이견이 생길 수 있는 상황에서는 시스템의 효율성과 정보보호 측면에서의 불균형으로 인한 위협요인이 생긴다고 할 수 있다.

Ⅲ. 스마트사회에서의 정보보호위협 대응책 분석

3.1 기본적인 정보보호 대책

가. 법/제도적 정보보호 대책

스마트사회는 지금 진행되고 있는 성숙한 미래사회를 뜻하고 있으므로 지금의 환경과는 여러 가지 분야에서 다른 사회 모습을 예상할 수 있다. 이러한 새로운 사회에서 파생될 수 있는 다양한 정보보호위협에 대비하기 위해서는 먼저 법/제도적인 측면에서의 대책을 갖추어야 한다. 기존의 관련법을 재정비하여 효율적이고 인간중심적인 스마트사회를 조기에 구축할 수 있도록 하여야 한다.

가장 대표적인 '정보통신망 이용 촉진과 정보보호 등에 관한 법률'과 '개인정보보호법'에서는 기준과 절차 및 방법을 제시하고 있지만 현실과 부합되지 못한 처벌 위주의 조항들이 많이 포함되어 있다. 또한 IT 기술은 발전 속도가 매우 빠르기 때문에 관련법이나 제도가 변화된 기술을 반영하지 못하는 경우가 많이 발생하고 있다. 따라서 법/제도와 기술을 함께 다룰 수 있는 전문가가 항상 개정 및 보완을 할 수 있는 체제를 갖추어야 한다.

개인정보보호법에서 언급되고 있지만 일정규모 이상의 조직에서는 정보보호를 담당하는 임원급의 CSO(Chief Security Officer)를 임명하여 IT를 담당하는 CIO와는 수직적인 관계가 아니라 수평적인 관계에서 협력하여 조직의 정보보호를 책임질 수 있도록 하여야 한다.

가장 중요한 사항으로서 정보보호정책이 올바른 방향을 제시할 수 있어야 한다. 이제는 정부가 PaaS (Policy as a Service)라고 하는 서비스 즉 정보보호정책을 사용자와 개발자에 대한 서비스 개념으로 진화시켜서 투명하고 효율적으로 문제점을 해소할 수 있도록 지원하여야 한다.

우리나라에서는 '지식정보보안산업협의회'가 정보보호 산업에 종사하는 기업들을 규합하여 정부에 산업발전을 위한 정책을 건의하고 건전한 경쟁을 통한 기업발전을 도모하고 있다. 정보보호 산업체에서 생산하는 정보보호 제품의 품질을 향상시키기 위해서는 세계적인 제품들과 경쟁뿐만 아니라 새로운 환경에 빠르게 적응할 수 있도록 공동의 노력과 정부차원의 지원이 필요한 실정이다. 대부분이 영세한 소규모의 기업이 독자적인 기술개발과 사업영역을 관리하는 데는 많은 어려움에 봉착하게 될 수 있다. 따라서 공공기관에서 개발한 신기술을 기업체에 전수하고 사업컨설팅을 제공하는 제도가 정착되어야 한다.

나. 기술적 정보보호 대책

일반적으로 기술적인 정보보호 대책은 하드웨어적인 장비를 개발하거나 또는 소프트웨어적인 프로그램을 이용하는 방법을 생각할 수 있다. 서비스 제공자는 방화벽, 침입탐지시스템(IDS), 침입방지시스템(IPS), VPN 등과 같은 정보보호제품을 사용하여 허가되지 않은 사용자들의 불법적 접근을 차단하고 안전한 암호알고리즘을 활용하여 전파를 타는 도중에 도청과 같은 피해를 방지하여야 한다.

스마트기기들의 컴퓨팅 능력이 거의 PC에 가깝게 발전되고 있으므로 지금까지 서버에게만 의존하던 정보보호기능을 스마트기기에서도 함께할 수 있도록 개발되어야 한다. 특히 새로운 기능을 탑재하거나 제품을 개발할 때는 기술적 뿐만 아니라 디자인 측면에서도 특허에 저촉되지 않도록 세심한 주의가 필요하다. 최근 삼성과 애플의 특허분쟁에서 보는바와 같이 대수롭지 않게 생각했던 부분에서 엄청난 곤경에 직면할 수도 있다.

다. 교육 및 관리적 정보보호 대책

일정한 규모이상의 조직에서는 책임자를 임명하고 정보보호관리 지침과 규정을 마련하여 시행하는 것이 관리적인 정보보호대책이다. 지침은 반드시 내용이 쉽고 명확하게 하여야만 하며 실제 환경에 부합되도록 하여야 한다. 현실을 무시한 너무 이상적이거나 실행이 어

려운 지침이나 규정은 아무런 도움이 되지 않는다.

핵심적인 사항은 조직에서 운영하는 정보시스템에 대해서 정보보호관리체계 인증제도를 활용하는 것이다. 국제적으로는 영국의 BS7799가 있으며 우리나라도 한국인터넷진흥원(구 한국정보보호진흥원)에서 2003년부터 시행하고 있는 KISA ISMS 인증제도가 있다. 공신력 있는 제3자가 기업에서 운영되고 있는 정보시스템을 평가하여 정보보호관리체계 인증을 함으로써 최고경영자와 고객이 함께 안심하고 개인정보를 위탁 관리할 수 있으며 대외적으로도 신뢰성을 확보할 수 있게 된다.

관리적인 측면에서 조직원에 대한 정보보호교육도 필수적인 사항이다. 대부분의 정보보호 대책이 허가되지 않은 자의 불법적인 침해를 막고 정보시스템의 안전성에 중점을 두고 있지만, 정상적으로 고용된 내부직원이 나쁜 마음으로 불법행위를 하는 것을 방지하는 것은 실제적으로 매우 어려운 일이다. 따라서 내부자에 의한 정보유출과 불법적인 금융행위 등은 적절한 교육과 감사가 가장 효율적인 정보보호 대책이 될 수 있다.

3.2 스마트폰과 모바일앱의 정보보호 대책

가. 표준화와 정보보호 기반구조

표준화는 스마트기기들 간의 상호운용성을 확보하고 국제적인 경쟁에서 뒤지지 않기 위해 필수적인 사항이다. 그러나 국제표준이나 국내표준을 막론하고 개인이나 기업의 노력만으로는 표준화에 참여하여 유리하게 이끌어 가기는 매우 어려운 일이다. 정부와 산학연의 여러 조직이 함께 표준화에 동참하는 적극적인 활동이 정보보호와 산업발전에 중요한 것이다.

또한 기술의 변화에 맞추어 서비스 제공자들이 안전하게 서비스를 개발할 수 있도록 국가적인 차원에서 서비스로서의 정보보호 기반구조를 확립하여야 한다. 최근 이슈가 되고 있는 IaaS(Infrastructure as a Service) 개념은 스마트사회를 준비하면서 정보보호에 중점을 둔 기반구조를 서비스로 제공해야함을 강조하고 있다.

스마트기기들의 정보보호기능을 평가하여 인증서를 부여하는 제품의 평가/인증 제도를 활성화 시켜야 한다. 국제적으로 통용되고 있는 국제공통평가기준(CC : Common Criteria)에 근거하여 정보보호제품의 정보보호기능을 평가하여 인증을 받아야만 제품의 품질을 보증할 수 있고 세계에 수출할 수 있는 능력을 갖게 된다. 다행히 우리나라는 CC 인증서를 발행할 수 있는 국가이기 때문에 평가/인증 제도를 근거리에서 활용할 수 있다.

나. 스마트폰의 정보보호 대책

스마트폰에서 사용하는 응용프로그램의 개발과 유통에서 악성코드가 감염되어 개인정보를 유출시키거나 하드웨어의 기능을 손상시키는 위협에 대응할 수 있어야 한다. 기본적으로 응용프로그램의 악성코드 감염여부를 검사하는 장치가 있어야 한다.

스마트기기를 사용하는 사용자들도 무분별하게 모바일앱을 사용하거나 불법적인 사이트에 접속하여 악성코드에 감염되는 경우가 발생하지 않도록 조심하여야 한다. 만약에 좀비 프로그램에 감염된다면 본인이 피해자가 되지만 한편으로는 자신이 타인을 공격하는 가해자가 되는 상황으로 변질될 수 있는 것이다.

스마트폰 자체의 하드웨어를 방어할 수 있는 기능이 강화되어야 한다. 단말기의 인증기능과 암호화 솔루션을 탑재하여 중요개인정보를 보호하고 통신 중에 전파도청에 의한 정보유출을 차단할 수 있어야 한다. 이때 패스워드나 암호화키에 대한 안전대책이 강구되어야 한다.

스마트폰은 제조회사마다 독자적인 운영체제를 사용하고 있기 때문에 운영체제의 보안취약점을 이용한 제로데이 공격에 대응할 수 있도록 하여야 한다.

스마트폰의 도난이나 분실에 대비하고 이동저장매체의 악성코드 감염을 방지하도록 하여야 한다. 항상 타인이 쉽게 사용할 수 없도록 암호 잠금장치를 사용하거나 비상시에는 원격으로 주요정보를 삭제하는 기능도 필요하다.

다. 모바일앱의 정보보호 대책

모바일앱의 무분별한 개발과 악의적인 정보보호 침해가 우려되고 있다. 우선 중요한 것은 개발된 모바일앱을 게시하여 서비스를 실시하기 전에 보안성검증을 받는 것이 중요하다. 행정안전부는 2012년 8월에 '모바일 전자정부 서비스 앱 소스코드 보안성검증 안내서'를 발간하여 모바일앱의 보안성을 사전에 검증하도록 권고하

고 있다[9]. 검증 절차는 준비 및 신청단계, 보안성검증 단계, 배포 및 서비스 단계로 이루어지며 검증에 합격해야만 앱 서비스를 할 수 있도록 하여야 한다.

한편 모바일앱 사용자는 신뢰성 있는 기관의 보안성 검증을 통과한 앱만 사용하도록 주의를 하여야 한다. 특히 신뢰성이 충분하지 못한 앱을 다운로드 받을 때는 반드시 바이러스 검사를 실시하고 이용 중에도 불법적인 정보유출이나 예상하지 않은 작동상태에 주의를 기울여야 한다. 보통의 바이러스 백신으로 찾아내기 어려운 악성코드 때문에 피해를 보는 사례도 발생하고 있다.

스마트폰의 가장 매력적인 장점으로 꼽히고 있는 다양한 기능의 모바일앱은 수십만 건에 이르고 있다. 따라서 이토록 많은 모바일앱을 정확히 검증하는 일은 매우 어려운 일이다. 이제 모바일앱을 개발하고 검증할 수 있는 좀 더 효율적인 절차와 기반구조 확립이 필요한 시점이다. 가. 개인정보보호 개요

3.3 모바일 오피스의 주요서비스와 정보보호 대책

가. 모바일 오피스의 요구사항

최근 빠르고 안정적인 무선네트워크 환경과 스마트폰과 같은 모바일기기들의 보급이 급속도로 증대됨에 따라 모바일 오피스를 구축하는 것이 기업 경쟁력을 강화할 수 있는 좋은 수단으로 주목받고 있다. 모바일 오피스는 모바일 기능을 이용하여 기업외부에서 기업내부와 실시간 정보공유 및 업무처리를 가능하게 함으로써 비용을 절감하고 업무의 효율성을 증진시킬 수 있다는 장점 때문에 공공기관과 대기업 또는 중소기업에게 까지 확대되고 있는 추세이다. 특히 외부 현장에서의 업무가 많은 기업은 더욱 큰 효과를 기대하고 있다. 이제 모바일 오피스는 기업이 필요로 하는 선택의 영역이 아니라 필수영역으로 자리매김하고 있다고 본다.

모바일 오피스의 기본기능은 이메일, 전자결재, 업무일정 조회 및 등록, 메신저, 자료검색, 사내 게시판 등 사무업무에 필요한 기능을 포함한다. 또한 모바일 오피스의 전문기능은 특정기업이나 조직에서 특화된 기능으로서 고객관리(CRM), 전사적 자원관리(ERP), 지식관리시스템, 시설 안전관리 등 전문적인 분야까지 확대되고 있다.

모바일 오피스의 요구사항으로서는 기업의 목표와 최고경영자의 경영철학, 기업의 규모와 업무행태, 투자예산 등을 고려하여 필요한 업무에 대한 구체적인 사항을 작성하여야 한다. 특히 업무환경의 변화와 기술발전과 고객 서비스의 변화와 같은 불확실성에 대한 확장성과 융통성도 고려하여야 한다.

나. 웹 및 앱을 이용한 모바일 오피스 구축방식

모바일 오피스를 구축하는 방식은 크게 웹을 이용하는 방식과 앱을 이용하는 방식으로 나누어진다. 이외에도 아주 간단한 서비스만을 제공하는 기본형과 많은 비용과 여러 가지 그룹웨어까지 제공할 수 있는 가상화 방식을 열거할 수도 있으나 본 연구에서는 가장 일반화된 웹과 앱을 이용한 방식만을 다루고자 한다.

웹(Web) 방식은 기존 운영하는 그룹웨어와 연계된 모바일 웹 서비스를 웹 서버에 탑재하여 스마트폰내의 인터넷 웹 브라우저로 접속하여 업무에 필요한 그룹웨어를 사용하는 방식이다. 통상 간단한 메뉴화면으로 생성되며 상대적으로 저렴한 비용과 다양한 단말기를 모두 수용할 수 있다는 장점을 갖고 있다. 그러나 동기화가 불가능하여 업무의 효율성이 저하될 수 있으며 상대적으로 정보보호 기능이 취약하다고 할 수 있다.

앱(Application) 방식은 그룹웨어와 연계된 모바일 서비스를 모바일 서버에 구축하고 각 단말별로 별도의 어플리케이션을 탑재하여 서비스하는 방식이다. 다양한 사무업무를 응용서비스로 개발하여 사용할 수 있으며 동기화가 가능하여 실시간 업무처리의 효율성과 데이터 암호화와 VPN 등을 이용하여 보다 수준 높은 보안기능을 제공할 수 있다. 그러나 상대적으로 높은 구축비용과 사용할 수 있는 단말기가 제한적이며 스마트폰용 별도 응용프로그램을 개발하여야 하는 단점을 갖고 있다.

따라서 모바일 오피스를 구축할 때는 기업의 근무 행태와 투자여건 등을 웹 또는 앱 방식의 장단점과 비교하여 가장 적합한 방식으로 구축하여야 한다. 경우에 따라서는 간단한 업무는 웹을 이용하고 특화된 업무는 앱 방식을 따른 혼합형식을 고려해 볼 수도 있다.

다. 사용자 식별 및 접근권한 통제

모바일 오피스에서 가장 중요한 정보보호위협은 원격에서 다양한 모바일기기들이 접속하므로 이들에 대한

식별 및 인증과 요구하는 서비스에 대한 접근통제 문제이다. 앞에서도 언급하였지만 중앙의 서버는 표준화된 인터페이스 방식으로 모바일 단말기를 식별하고 다시 사용자의 ID와 패스워드를 사용하여 개인을 식별하여야 한다.

사용자 식별 후에는 여러 가지 업무관련 서비스에서 사용허가에 관련된 권한 여부를 확인 하여야 한다. 특히 권한을 부여하거나 삭제 시에 권한관리자에 의한 오남용이 발생하지 않도록 지침이나 규정이 명확하여야 한다.

편의성을 위하여 여러 가지 서비스에 접속할 때 SSO(Single Sign On) 방식을 채용할 수도 있지만 이런 경우에는 OTP(One Time Password) 방식과 같은 더욱 보강된 식별방식을 사용하여야 하며 중요한 문서에 대해서는 전자서명과 공인인증서 방식을 혼합할 수도 있다.

라. 주요서비스 개발

모바일 오피스에서 사용하는 기본 기능에는 이메일, 전자결재, 게시판, 일정계획, 연락처 등의 업무가 있다. 이와 같은 기본 업무는 대부분이 이미 사용하고 있는 그룹웨어에 포함되어 있으므로 특별한 개발비용이 필요하지 않다고 본다. 그러나 기업의 특수한 목적이나 환경에 특화된 전문서비스를 제공하기 위해서는 새로운 응용서비스 개발이 요구된다.

전사적자원관리(ERP : Enterprise Resourse Planning) 서비스는 기업제품에 대한 재고관리, 생산 및 원가관리, 영업 및 판매, 구매 및 발주 등 업무를 현장에서 실시간으로 정보를 파악하고 입력할 수 있도록 하여 업무의 효율성과 신속성, 편리성을 함께 도모할 수 있는 응용프로그램이다.

고객관계관리(CRM : Customer Relationship Management) 서비스는 고객과의 관계를 우호적으로 개선하여 영업관리, 서비스관리, 마케팅관리에 연동시킴으로써 기업의 이익을 극대화시키고자 하는 응용프로그램이다. 기업마다 업무영역과 행태에 따른 특화된 고객관리가 필요하다고 볼 수 있다.

모바일 시설안전관리 서비스는 현장을 이동하면서 시설물의 안전성을 점검하고 실시간으로 조치를 취함으로서 즉시대응력을 향상시키고 업무의 신속성을 유지할 수 있는 서비스이다.

이토록 모바일 오피스의 전문기능은 기업의 특성에 따라 다양하게 제공될 수 있으므로 응용서비스를 개발할 때는 반드시 수요자의 요구사항을 반영할 수 있도록 하고 기업의 요구사항에 맞도록 하여야 한다.

마. 모바일 오피스의 정보보호 대책

모바일 오피스의 기본적인 서비스 기능과 특화된 전문기능에 대해서는 차별화된 권한통제가 요구된다. 서비스 종류에 따라 사용자의 수준과 업무구분에서 차이가 있으므로 꼭 필요한 사람에게 꼭 필요한 업무만을 수행할 수 있도록 하여야 한다. 즉 최소권한의 원칙과 업무의 분리원칙이 적용될 수 있도록 하여야 한다. 이러한 모바일 오피스의 정보보호 대책은 크게 세 가지, 즉 단말기 정보보호, 네트워크 정보보호, 정보센터 정보보호로 구분할 수 있다[10].

단말기의 정보보호는 사용자 및 서버 인증, 악성코드 대응, 분실과 도난 대비, 데이터 보호로 구분한다. 사용자뿐만 아니라 서버에 대한 인증이 확실하여야만 불법접속을 차단할 수 있고 단말기 분실로 인한 위장접속을 예방할 수 있다. 또한 분실과 도난에 대비하여 개인정보와 같은 중요정보를 암호화시키거나 원격 정보 삭제 기능을 이용하여야 한다. 악성코드의 감염에 대비하여 안티바이러스 소프트웨어를 설치하고 항상 최신버전을 유지하도록 하여야 한다. 데이터보호를 위해서는 중요자료를 암호화하고 업무관련 정보만 조회할 수 있도록 하여야 한다.

네트워크 정보보호는 VPN을 적용한 안전한 네트워크 구성, 보안관제, 무선침입방지시스템, 스마트폰 인증 등이 있다. 통상 모바일 오피스는 경비절감을 위하여 전용선 보다는 공중인터넷망을 선호한다. 따라서 인터넷망을 전용선과 같이 활용할 수 있는 VPN 방식을 활용하여 안전한 네트워크를 구성하여야 하며, 해킹 및 바이러스 감염에 대응할 수 있는 보안관제를 실시하여야 한다. 또한 비인가 모바일기기나 AP 탐지를 위한 무선침입방지시스템을 설치하여 기기들을 인증하도록 하여야 한다.

정보센터 정보보호는 업무서버를 보호하는 대책을 강구하고, 사용자의 행위를 기록하며, 24시간 보안관제를 실시하여야 하고 불필요한 서비스와 포트를 차단하

여 비인가자의 침입을 막고 저장된 주요정보를 보호할 수 있도록 하여야 한다.

Ⅳ. 결 론

스마트사회는 인간중심적이고 창의성과 행복을 중시하는 미래사회로서 Beyond IT 즉 IT 기술 중심사회 이후에 도래하는 새로운 사회로 자리매김하고 있다. 아직 명확하게 정의되지는 않았지만 지금과는 다른 새로운 가치창출과 사회생활의 진화를 예상할 수 있다.

본 연구는 스마트사회의 다양한 환경변화와 그에 따른 정보보호위협 요소들을 도출하고 이러한 위협에 대응할 수 있는 요소기술들을 분석하여 정보화 역기능적인 위험에 대비할 수 있도록 함으로써 안전하고 신뢰성 있는 스마트사회 구축을 앞당기는데 도움이 되고자 하였다.

스마트사회를 주도하는 명제는 IT 기술과 모바일의 융합이라고 볼 수 있으며 IT기술의 트렌드는 여러 가지로 분류될 수 있다. 몇 가지 중요한 분야를 살펴보면 스마트폰을 비롯한 모바일기기들의 급증, SNS의 확산, 다양한 소셜비즈니스의 증가, GPS를 탑재한 위치기반서비스의 증가, 모바일 오피스와 스마트워크의 확산, 그리고 스마트기술을 융합시킨 스마트 TV와 같은 스마트기기들의 개발 및 보급 등 여러 가지가 주목을 받고 있다.

그러나 이 모든 트렌드에 앞서 정보보호와 개인의 프라이버시 보호라는 이슈가 가장 중요하고 시급한 선결과제로 인식되고 있다. 특히 해킹과 바이러스를 이용한 사이버테러와 국가 주요기반시설에 대한 위협은 국가안보와도 연결된 핵심요소이다.

따라서 각 트렌드별로 발생 가능한 정보보호위협들을 도출하고, 이러한 위협에 대응할 수 있는 대응책들을 분석하였다. 기본적인 정보보호대책과 함께 각 트렌드에 따른 특성에 따라 필요한 대응책을 제시하였으며 근본적으로 국민적 정보보호 의식의 중요성을 일깨우는 교육이 절실한 시점이다.

본 연구가 새로운 스마트사회의 특성과 정보보호 대응책을 이해함으로써 인간중심의 창조적이고 행복중심의 새로운 가치를 창출하고자 하는 스마트사회를 앞당기는데 도움이 되길 바란다.

참고문헌

[1] 서울디지털포럼, “공존-기술, 사람 그리고 큰 희망,” 서울디지털포럼 2012, 2012. 5.

[2] 한국정보문화진흥원, “스마트사회의 실현을 위한 전략과 과제,” 한국정보문화진흥원, 2012. 3.

[3] 방송통신위원회, “위치정보 이용 활성화 계획”, 방송통신위원회, 2010

[4] 신선영, “국내외 클라우드 컴퓨팅 추진동향 및 사례,” 한국정보문화진흥원, 2011.7.

[5] 국회, “개인정보보호법,” 법률 제10465호, 2011. 3. 제정

[6] 국가정보화전략위원회, “스마트워크 활성화 전략,” 행정안전부, 2010. 7.

[7] 한국개인정보보호협의회, “구글의 개인정보 통합정책에 관한 토론,” 한국개인정보보호협의회, 2012. 4.

[8] 행정안전부, “2012 국가 정보화백서,” 한국인터넷진흥원, 2012. 8.

[9] 행정안전부, “모바일 전자정부 서비스 앱 소스코드 보안성 검증 안내서,” 한국인터넷진흥원, 2012. 6.

[10] 이장수, “모바일 오피스 구축방안,” Smart Mobile Security 2010, 한국정보보호학회, 2010. 6.

〈著者紹介〉

남 길 현(Kil Hyun Nam)
정회원

1973년: 서울대학교 토목공학과 졸업
1979년: 미국 해군대학원 전산학 석사
1985년: 루이지아나 대학교 전산학 박사
1985년~2006년: 국방대학교 교수
2008년~2010년: 고려대학교 전문교수
1999년~2001년: 한국정보보호학회 회장
2010년~현재: 한국과학기술정보연구원 전문연구위원
<관심분야> 정보보호