편집위원 : 진병문 (TTA)

스마트 사회의 보안위협과 정보보호 정책추진에 관한 제언

이기주
한국인터넷진흥원

요 약

우리는 지금 스마트 사회에 살아가고 있다. 언제 어디서든 스마트 디바이스를 통해 기존에 PC에서 하던 작업들을 손쉽게 하고 있다. 한편 스마트폰의 확산으로 이용자 수가 급증하고 있는 소셜네트워크 서비스(SNS)는 이용자들이 자신의 일상적인 이야기를 사이버공간에 게시함으로 인해 개인의 사생활 정보들이 노출되고, 그러한 정보들이 범죄에 악용되는 사례들이 눈에 띄게 증가하고 있다. 또한 SNS를 이용한 악성코드의 유포 및 빠른 전파 등도 새로운 보안위협으로 나타나고 있다. 그 밖에 스마트 기기를 대상으로 한 해킹 및 악성코드 감염 등 위협이 증가하고 있는 형편이다.

본고에서는 스마트 사회의 주요 보안위협을 살펴보고 미국, 유럽, 일본, 호주 등 선진국의 관련 정책 동향과 국내 정책과 실태를 분석하여 새로운 정보보호 정책 수립 방향을 제언하고자 한다.

스마트 사회 위험 요소로 가장 보편적으로 사용되고 있는 스마트폰과 스마트폰을 통해 이용되고 있는 소셜네트워크 서비스, 클라우드 서비스의 보안위협을 제기하고 최근 글로벌 이슈로 떠오르고 있는 빅 데이터 환경의 보안위협을 분석하였다.

스마트 사회의 위협을 대비하고 있는 주요국 정책을 살펴보면, 미국의 경우 사회적 합의를 바탕으로한 감시와 통제를 강화하는 정책을 추진 중에 있으며 유럽의 5개국 EU5(영국, 독일, 프랑스, 스페인, 이탈리아)는 스마트폰 위협을 중심으로 공동대응 방안을 마련하고 있다. 일본은 스마트 워크중심의 보안대책을 강구하고 있으며 호주는 스마트 사회 보안위협에 대한 국민의 인식제고에 주력하고 있다.

국내의 경우도 스마트 사회의 보안위협에 선제적 대응을 위하여 「스마트 모바일 시큐리티 종합계획」을 수립하여 추진중에 있다. 하지만 보안 실태를 보면 스마트 사회 보안위협에 대한 이용자들의 우려는 높은 반면 기업의 보안 대책 마련에 대한 투자는 여전히 미흡한 상황이다.

향후 우리 사회가 디바이스간 융합을 넘어 모든 사물이 연결되는 超연결(Hyper-Connectivity) 시대로 진화되어 가면 편리성이 증대되는 만큼 더 많은 위협에 우리의 일상이 노출되는 문제가 발생하게 될 것이다. 안전한 미래 사회로 진입하기 위해서는 보다 체계적이고 종합적인 정보보호 정책마련이 필요하다. 본고에서는 이를 위한 정책수립의 방향을 제언했다.

Ⅰ. 서 론

지금은 ICT를 활용하여 새로운 가치들이 창출되면서 우리의 삶의 형태가 바뀌고 있는 스마트(Smart) 시대이다. 스마트(Smart)라는 개념은 소프트웨어나 하드웨어에 관하여 말할 때 정보 처리 능력을 가지고 있다는 것을 나타내는 것으로서 특히 지금까지는 기대할 수 없었던 정도의 정보 처리 능력을 가지고 있다는 의미를 나타낸다. 지능화된 또는 지능형(intelligent)이라는 용어와 같은 의미로 이해할 수 있다.

최근 폭발적인 스마트폰의 보급과 이용으로 다양한 분야에서 '스마트'가 화두로 등장하면서 스마트한 생활, 스마트한 일처리, 스마트한 경영이 각광받고 있다. 또한 스마트폰 사용자 3천만 시대를 넘어서 스마트는 우리 삶의 중요한 부분을 담당하게 되었다.

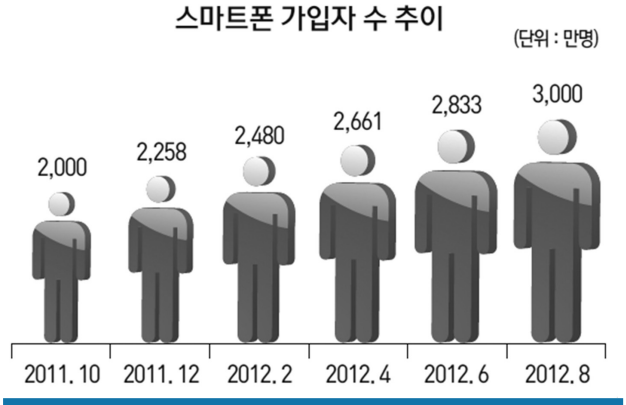

그림 1. 국내 스마트폰 가입자 추이
※출처: 한국인터넷진흥원, 『한국인터넷백서』, 2012.10

한편 스마트폰의 확산으로 이용자 수가 급증하고 있는 소셜네트워크 서비스(SNS)는 이용자들이 주로 자신의 일상적인 이야기를 사이버공간에 올림으로 인해 개인의 사생활 정보들이 노출되고, 그러한 정보들이 범죄에 악용되는 사례들이 눈에 띄게 증가하고 있다. 또한 SNS를 이용한 악성코드의 유포 및 빠른 전파 등도 새로운 보안 위협으로 나타나고 있다. 그 밖에 스마트 기기를 대상으로 한 해킹 및 악성코드 감염 등 위협이 증가하고 있는 상황이다.

독일의 사회학자인 울리히 벡(Ulrich Beck, 1986)은 근대화가 진전된 현대 산업사회의 특성을 '위험사회(Risk Society)'라는 개념으로 설명했다. 과학기술의 발전으로 합리적이고 풍요로운 그리고 효율적인 현대사회는 다른 한편으로 불안과 위험, 재난과 불확실성에 노출되어 있다는 것이다. 그의 문제제기는 산업사회에 대한 통찰에 그치지 않고 정보통신기술의 급격한 발전에 근거하고 있는 현재의 정보화 사회에서도 유효하게 나타난다고 할 수 있다.

스마트 환경으로의 변화와 신기술 패러다임의 잇따른 등장은 정부, 기업, 개인들에게 예측 불가능한 위험을 증가시키는 사이버위험 사회로의 진입을 더욱 촉진하고 있는 상황이다. 곳곳에 산재한 컴퓨터를 시간과 장소에 상관없이 자유롭게 이용함으로써 편리하고 쾌적한 정보이용환경을 구현하게 해주는 스마트 사회(Smart Society)는 동시에 예측 불가능한 위험이 곳곳에 산재한 '사이버 위험사회'로의 진입을 의미한다고 할 수 있다.

Ⅱ. 스마트 사회의 보안 위협

스마트 시대가 가져온 다양한 편익에 비례해 해킹을 통한 개인정보의 유출, 서비스 중단 등과 같은 보안 위협 또한 함께 수반되고 있다. 다음에서는 스마트 시대의 대표적 보안 위협을 살펴보도록 하겠다.

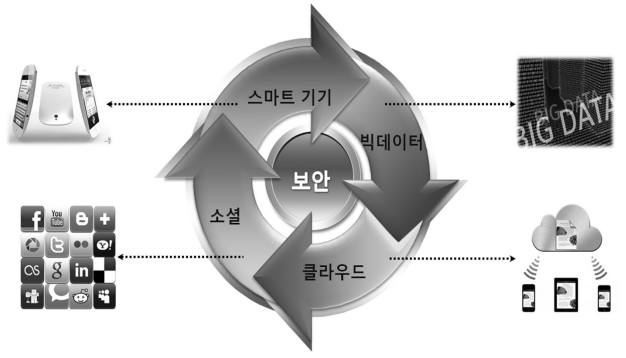

그림 2. 스마트 시대 대표적 보안 위협

1. 스마트폰 보안위협

최근 들어 스마트폰 사용자가 많아지고 다양한 스마트폰 OS가 선보이고 있다. 국내에도 본격적인 스마트폰 시대를 맞이하여 PC에서 하던 일을 스마트폰을 통해 언제 어디서든 할 수 있게 되었다. 이러한 편리성의 이면에는 PC 환경에서 일어나고 있는 많은 보안위협들이 그대로 스마트폰에서도 일어날 수 있다. 현재까지 알려진 모바일 악성코드의 주요 특징은 통화 기록이나 전화번호, 사진 등의 개인정보 탈취, 비정상 트래픽을 유발하여 과다요금을 유도하거나 배터리 소진시키는 것이 대부분이다.

그림 3. 스마폰을 중심으로 한 다양한 위협

악성코드뿐 아니라 휴대용 단말이 가지는 특성 등으로 인한 스마트 폰의 보안 위협은 크게 세 가지로 구분할 수 있다.

첫째, 단말기 보안 이슈이다. 스마트 폰 단말기의 도난 · 분실로 인한 개인정보 또는 업무 정보의 유출, 업무용 서버에 불법 접속하여 업무정보 유출, 스마트폰 소유자가 악의적으로 업무정보의 외부유출 가능성 존재 등이다.

둘째, 악성 코드나 악의적 앱 보안 이슈이다. 스마트폰의 악성코드 감염이나 악의적 목적의 앱으로 인해 개인정보 유출, 장치이용 제한, 부정 과금 유발, 모바일 DDos 공격 등의 발생할 수 있으며, 플랫폼 또는 펌웨어(Firmware)[1] 변조에 따라 보안 기능을 약화시킬 가능성 존재이다.

셋째, 네트워크 보안 이슈이다. 스마트폰을 와이파이 등의 무선 인터넷에 접속하여 사용함에 따라 무선구간에서 패킷 스니핑(Sniffing)[2], 상용인터넷 망을 통한 해킹, 스마트 폰을 경유

1 컴퓨터의 하드웨어(hard ware)와 소프트웨어(soft ware)의 중간에 위치하는 것으로 소프트웨어의 처리순서를 읽기 전용의 기억장치에 고정시켜 프로그램을 통해 일종의 하드웨어로 이용하는 구조를 말한다. 말하자면 소프트웨어의 하드웨어화이다

2 스니핑은 네트워크상의 데이터를 도청하여 네트워크상에 돌아다니는 패킷의 내용을 들여다보는 것을 말한다.

하여 인트라넷 서버에 접속하는 등의 보안 위협이 발생하게 된다.[3]

2. 소셜 네트워킹 환경의 보안위협

스마트 기기의 보급 확대와 함께 소셜 네트워크 서비스는 참여하는 구성원 개개인의 다양성을 존중하며 개인과 기업의 새로운 소통의 도구로 자리매김하고 있다. 하지만, SNS의 인기가 높아지면서 그에 대한 보안위협도 증가하고 있다. 인터넷을 사용하는 사람이면 누구나 블로그, 트윗, 웹사이트, 카페 커뮤니티 등의 다양한 소셜 네트워크 서비스를 통해 자기 홍보나 소속된 집단과의 소통을 향유하게 된다. SNS의 속성상 소속, 연락처, 취미, 활동내역, 사진 등의 대부분의 개인정보를 공개된 상태에서 소통하기 때문에 이러한 과정에서 의도하지 않게 많은 개인 정보들이 노출될 수 있다. 이외에도 SNS 플랫폼을 이용한 유해 컨텐츠 유통이 활발하게 전개될 것으로 예상된다.[4]

유럽의 정보보호 전문기관인 ENISA(European Network and Information Society Agency)는 SNS 관련 보안위협을 다음과 같이 분류하였다.[5]

프라이버시 보안위협: 개인 프로파일 수집, 2차 데이터 수집, 안면 인식과 개인정보 연계로 인한 초상권 침해와 익명성 약화, 콘텐츠 기반 이미지 검색, 이미지 메타 데이터와 개인정보의 연계, 완전한 계정삭제의 어려움이 있다.

네트워크상의 보안위협: SNS를 이용한 스팸증가, 크로스사이트 스크립팅, 웜 · 바이러스 등에 대한 취약성 증가. 다양하게 통합되는 SNS 포털들이 정보수집기로 이용되어 보안 취약성이 증가될 수 있다.

ID 관련 위협: SNS를 이용한 특정이용자 그룹에 대한 스피어 피싱, 침입을 통한 ID정보 유출, ID 도용을 통한 허위정보 생산 또는 명예훼손 등 각종 범죄가 증가 할 수 있다.

사회적 위협: 사이버 스토킹, 사이버 괴롭힘, 산업 스파이 등에 관한 위협 등이 있다.

3. 클라우드 서비스 보안위협

클라우드 서비스는 크게 클라우드 서비스를 제공하는 서비스 제공자 부분과 클라우드 서비스를 이용하는 이용자 부분의 2가지로 나누어진다. 특히 클라우드 서비스가 인터넷을 이용하여 제공되지만 기존 웹과는 다르게 다양한 형태의 서비스를 제공할 수 있는 컴퓨팅 환경으로써 새로운 기술을 이용함에 따라 그에 상응하는 다양한 보안문제가 제기되고 있다.

클라우드 서비스에서 일어날 수 있는 보안 위협으로는 다음의 7가지가 있다.[6]

클라우드 오용과 비도덕적인 사용: 악의적인 목적으로 클라우드를 도입하는 경우, 가상의 공간에 정보가 존재하는 특성이 있기 때문에 기존의 봇넷보다 더욱 높은 보안위험을 가지게 된다.

불안전한 인터페이스와 응용 프로그래밍 인터페이스: 부가 가치를 높이기 위해 기존 코드를 재사용 또는 합성 등을 통해 응용 프로그램을 개발하는 경우 프로그램 복잡도가 증가하여 이에 따른 보안 취약성이 발생할 수 있다.

악의적인 내부자: 클라우드 서비스 업체에서 실수로 해커, 조직범죄자, 기업 스파이 등 악의적인 목적을 가진 사람을 채용하는 경우 클라우드 시스템 내에 존재하는 데이터가 유출될 수 있다.

기술 공유 문제: 인프라 서비스(IaaS) 사업자는 공유 기술을 바탕으로 시스템 확장성을 제공하지만, 다중 애플리케이션 아키텍처 사용을 위한 효과적인 자원의 분리가 이루어지지 않는 경우가 있을 수 있다.

데이터 유실이나 유출: 클라우드 환경의 구조적, 운영적인 특성으로 데이터 유출의 위험이 증가하며, 그 원인도 보다 다양해진다.

계정이나 서비스 갈취: 피싱, 사기, 소프트웨어 취약점 등을 이용한 계정의 도용은 일반적인 상황이지만, 클라우드 환경에서 계정 정보의 유출은 기존의 경우보다 문제가 훨씬 더 심각해진다.

알려지지 않은 위험 프로파일: 클라우드 환경에서는 지금까지 알려지지 않은 보안위험 요소가 있으며, 이에 대한 대응을 위해 소프트웨어 버전 업데이트, 취약점 프로파일 및 침입시도에 대한 점검, 보안을 고려한 설계 등은 알려지지 않은 보안위험요소를 통한 피해를 최소화하기 위한 기본적인 방법이 된다.

또한 전통적으로 고려되고 있는 주요 보안 문제들처럼, 클라우드 서비스에서도 가상환경에서 보안, 기밀성과 무결성 문제, ID 관리, 접근통제와 프라이버시 문제가 발생할 수 있다.[7]

이것을 다시 이용자 관점에서 개인 사용자와 기업 사용자로 바라보면 개인 사용자는 E-mail, 블로그, 동호회, 사진 및 파일 저장과 공유 서비스를 주로 이용하며, 무료로 제공하는 서

3 임상규 외, "스마트 시대의 보안 위협; EU5의 대응과 시사점", 한국위기관리학회, 제7권, 4호, 2011.8.

4 김지훈, 조시행, "사이버 환경에서의 보안위협", 정보보호학회지, 제20권, 4호, 2010.8.

5 김성열, 소셜 네트워크 서비스 보안 위협요인에 관한 연구, 산업과학연구, 제30권 1호, 2012.1.

6 남기효, 김윤홍, "클라우드 서비스 분석 및 보안 이슈", 주간기술동향, 2012.4.

7 홍진근, "스마트 환경의 주요 정보통신 기술과 정보보호 동향", 한국 인터넷 정보학회, 제13권 1호, 2012.3.

비스를 선호하는 특성을 갖는다. 개인 사용자 관점에서 우려하는 보안 문제를 열거하면, 개인정보 노출, 개인에 대한 감시, 개인 데이터에 대한 상업적 목적의 가공 등이 있다. 한편 기업 사용자는 자신이 소유하던 IT자산을 클라우드 형태로 제공받기를 원하지만, 자신의 데이터가 타인과 공유되기를 원하지 않는다. 기업 사용자는 안전성을 제공하면 비용을 지불할 의사가 있으며, 때에 따라서는 Private Cloud와 같이 자신이 직접 운영하기도 한다. 기업 사용자 입장에서 우려하는 보안 문제를 열거하면, 서비스 중단, 기업 정보 훼손 · 유출, 고객 정보 유출 등이 있다.[8]

4. 빅 데이터 환경의 보안위협

다양한 IT서비스와 플랫폼이 등장하면서 엄청난 양의 데이터가 쏟아지고 있다. 이른바 '빅 데이터(Big Data)' 시대가 도래 하면서 기업들은 빅 데이터 솔루션 도입을 고려하고 있는 추세다. 빅 데이터 도입이 적극 고려되기 시작한 이유는 모바일 기기의 진화와 트위터, 페이스북 등과 같은 소셜네트워크 서비스의 출현으로 기업 내 데이터를 폭발적으로 증가시켰기 때문이다.

다음에서는 빅 데이터의 생성에서부터 서비스에 이르기까지 세 단계로 나누어 보안이슈를 살펴보도록 한다.[9]

데이터 생성단계: 다양한 경로를 통해 생성, 수집되는 많은 양의 데이터들은 곧 다양한 경로의 보안위협을 의미한다. 최근 장시간에 걸쳐 목적을 가지고 공격하는 지능형 지속 위협(APT, Advanced Persistent Threat) 등이 발생하면서 빅 데이터 생성 및 수집 과정에서 데이터 신뢰성 및 무결성에 대한 우려가 높아지고 있다. 또한 빅 데이터들은 많은 수가 개인 IT단말을 통해 생성되어 수집되는데 이때 의도하지 않게 개인정보가 노출되거나 개인 데이터가 무분별하게 상업적으로 이용되는 등 프라이버시를 침해할 수 있다.

데이터 저장 · 운영 단계: 빅 데이터가 생성되어 저장, 분석되어 서비스로 제공되기까지의 일련의 과정 중 가장 보안에 주의해야 하는 구간이 바로 빅 데이터의 저장 및 운영구간이다. 여기서는 다양한 사용자를 수용하는 클라우드 컴퓨팅을 활용하는 빅 데이터가 내 · 외부의 다양한 공격자에게 노출될 수 있어 사용자 인증 및 접근제어, 데이터 기밀성 · 무결성, 프라이버시 침해, 재해 · 물리적 침입, 네트워크 보안 등의 문제가 발생할 수 있다.

서비스 단계: 1차적으로 모여진 많은 양의 데이터를 산업별, 이용자별 각 필요와 요구에 따라 분석하는 과정은 빅 데이터 서비스를 위해 반드시 거쳐야 하는 절차이다. 이 과정에서 이전의 암호화 등을 통해 데이터의 기밀성과 익명화 과정을 거쳤다고 해도 사용자가 원하는 데이터를 추출하기 위해 데이터의 복호화 등 데이터 복구 과정을 수행하여야 한다. 따라서 분석 및 2차 데이터에서도 프라이버시 침해 및 데이터 의 기밀성이 노출될 위험이 있다.

예를 들어 금융업의 빅 데이터는 마케팅 효과 극대화, 고객에게 최적화된 맞춤형 상품 제안, 프로세스 효율화 등을 실현하는 데에 중요한 데이터베이스다. 만약 빅 데이터를 보유하고 있는 기업이 데이터를 손실 및 유출할 경우에 사회, 경제적인 피해뿐 아니라 개인의 프라이버시를 침해할 수 있다. 따라서 암호키와 암호화 데이터의 분리, 개인 식별번호 선별, 전송 데이터 암호화 등의 데이터 보호, 프라이버시 관리, 데이터 백업 등의 현실적인 대안이 필요하다.

Ⅲ. 스마트 정보보호를 위한 주요국 사례

전 세계적으로 스마트 시대의 진입과 함께 정보보호에 대한 다양한 사회 이슈가 제기되고 있으며 대응방안이 마련되고 있다. 여기서는 미국, 유럽, 일본, 호주의 주요국의 사례 분석을 통해 국가별 스마트 정보보호 대책을 살펴보고자 한다.[10]

1. 사회적 합의 바탕의 통제와 감시를 강화하는 미국

정보 보안의 강화는 스마트 시대로의 전환을 위한 필수 요소이다. 상대적으로 정보 보안의식이 높은 미국조차도 모바일 인터넷에서의 정보 유출을 심각한 도전으로 인식하고 다양한 대책을 모색하고 있다. 미국에서는 일찍부터 무선 인터넷으로 초래되는 새로운 유형의 정보유출 및 해킹에 대한 대책 마련에 고심하였으며, 그 해결책으로 정보 제공자의 네트워크 통제권(control)과 감시(monitoring) 기능의 강화를 제시하였다.[11]

정보 제공자의 감시 행위는 불가피하게 정보 이용자의 사생활(privacy)을 침해할 소지가 있다. 이러한 문제를 해결하기 위해 미국은 'Security Policy'를 문서화하고 이를 통해 감시와 사생활 보호 간의 균형을 유지하고자 한다. 개인생활을 중요시 하는 미국사회의 풍토로 생각하면 매우 아이러니한 해결책 이지만,

8 은성경,"클라우드 컴퓨팅 보안 기술 동향", 정보보호학회지, 제20권, 2호, 2010.4.

9 정교일 외, "빅 데이터와 정보보안", 한국정보기술학회지, 제10권, 3호, 2012.9.

10 Ⅱ장에서 언급한 보안위협 요소 중 각 국가의 대표적 정책사례를 중심으로 분석

11 미국 국립표준기술원(NIST)의 무선 인터넷 보안에 대해 제시한 13가지 정책 요소(Guide to Enterprise Telework and Remote Access Security)를 제시하였다.

오히려 정보 제공자는 네트워크 보호 및 정보 보안의 일차적 책임자이며, 통제와 감시의 권한 역시 'Security Policy' 등을 통해 사회적으로 허용 가능한 수준에서 결정된다.

이를 통해 얻을 수 있는 순기능은 첫째, 정보 제공자에 의한 감시 행위의 목적과 정당성을 명시함으로써 사생활 침해에 관한 이용자와의 갈등을 최소화할 수 있다. 즉, 네트워크 감시 활동에 관해 정보 이용자의 양해를 구하고, 감시의 목적을 규정함으로써 과도한 감시를 억제할 수 있다. 둘째, 은밀히 시행되던 이용자 감시를 공개함으로써 오히려 부당한 감시와 정보 제공자에 의한 정보 유출을 미연에 방지할 수 있다. 셋째, 이러한 문서화가 정보 유출의 심각성에 대한 사회적 경각심을 고취시킬 수 있는 기회로 작용할 수 있다고 평가된다.

통제와 감시의 부정적인 어감 때문에 미국의 대책은 개인 사생활의 희생을 가정하는 것처럼 보인다. 그러나 미국의 의도는 정보 유출 사고가 일시적이고 불가항력이었다는 정보 제공자의 변명은 더 이상 통용되지 못할 뿐더러, 해킹 등의 악의적 행위와 함께 이를 막지 못한 정보 제공자 역시 비난과 책임 대상으로 간주된다.[12]

이러한 측면에서 미국의 보안대책은 정보제공자의 네트워크 통제와 감시에 대한 새로운 해석, 그리고 이용자의 사생활과의 균형 등의 시사점을 제공하고 있다.

2. 스마트 시대 정보보호 문제를 공동 대응하는 EU5

스마트 시대의 대표기기인 스마트 폰 사용자의 증가는 이러한 정보보호 문제가 한 지역이나 국가에 머무르지 않고 공간을 초월한 글로벌 이슈임을 보여준다. 영국, 독일, 프랑스, 스페인, 이탈리아의 EU5 국가들은 증가하는 스마트 폰 사용자와 서비스에 대한 대비책을 마련하였다.[13]

급격하게 증가한 유럽 주요 5개국의 스마트 폰 사용자는 금융과 의료 서비스 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. EU5 국가는 스마트 폰 및 PDA 같은 정보기기의 사용으로 스마트 시대의 위험을 10가지로 분류하고 대처 방안을 제시하였다.[14]

EU5 국가들이 제시한 스마트 시대의 정보보호 문제들은 완벽하게 해결할 수는 없지만, 충분한 대비가 있다면 해결이 가능하다고 보고 있다. 또한 EU5는 10가지의 위험에 대한 대응방안으로 새로운 고도 기술이나 시스템의 도입보다 지금까지 간과한 간단한 방법들을 제시하였다. 이것은 보안 문제는 한 국가에 머무르지 않고 공간을 초월한 문제로 주변 국가들이 함께 논의의 장을 만들고 공공 대응한다는 취지이다.

표 1. EU5가 정의한 스마트 시대 정보보호 위협 10가지

구분	위험	세부 내용
R1	Data leakage	스마트폰 도난, 분실
R2	Improper decommissioning	정보보호 조치가 되지 않은 스마트폰을 타인이 사용/습득하여 생긴 피해
R3	Unintentional data disclosure	앱(apps)을 통해 사용자가 인지 못하는 사이 개인정보 데이터가 전달되는 경우
R4	Phishing	공격자가 위조 사이트를 통해 사용자의 개인정보를 탈취
R5	Spyware	Spyware를 활용한 개인 데이터의 파괴와 악용
R6	Network Spoofing attacks	악성 네트워크에 접근하도록 유도하여 위험을 초래
R7	Surveillance	공격 목표로 삼은 스마트폰 사용자를 속여 스파이 행위 수행
R8	Diallerware	서비스나 폰 번호를 알아내어 사용자 돈을 탈취
R9	Financial malware	악의적인 멀웨어를 통해 신용카드 번호와 인터넷 뱅킹 정보 탈취
R10	Network congestion	네트워크 정체가 발생해 스마트폰 사용을 방해

※ 출처: ENISA(2010)

현대 사회에서 가장 시급한 문제 중의 하나가 정보화에 따른 보안 문제라고 할 수 있다. 서비스의 제공과 기술 발전도 중요하지만, 이용자가 보다 편리하고 안전하게 이용할 수 있는 환경의 조성이 더 중요하다. EU5의 스마트 시대의 보안 문제에 대한 대책은 국가간 공동협력의 중요성을 강조한데 시사점이 있다고 할 수 있다.

3. 스마트워크 보안 대책을 추진하는 일본

성공적인 스마트 시대를 맞이하기 위해서는 기술적 발전을 뒷받침할 수 있는 보안 대책이 마련되어야 한다. 특히, 스마트 워크 영역의 경우, 다양한 스마트 기기와 인터넷을 활용하여 원격으로 작업하는 근무 환경의 특성상 바이러스 및 기밀 정보 유출 등으로 인한 사회적 손실 위험이 증대되고 있다. 따라서 정보보안에 대한 충분한 고려와 적절한 대책이 요구되고 있다.

일본 정부는 정보보호 관련 문제를 스마트 시대로의 발전을 위해서 해결해야 할 중요한 과제로 인식하고 있다. 스마트 시대 관련 정책은 총무성의 「텔레워크 추진 정책」을 시작으로 추진되었다.[15] 총무성은 「텔레워크 시큐리티에 관한 조사 연구회」의 검

12 윤창근 외, "해외동향 스마트시대의 보안대책", 지역정보화, 2011.5.

13 김종업, "스마트 시대의 보안과 유럽의 대응", 지역정보화, 2011.5.

14 자세한 내용은 European Network and Information Society Agency(enisa) (2010). "Smartphones: Information security risks, opportunities and recommendations for users," Brussels: enisa. 참조.

15 김유미, "스마트 시대, 일본의 텔레워크 관련 보안 대책", 지역정보화, 2011.5.

토를 거쳐 「텔레워크 시큐리티 가이드라인」을 제정하였다. 본 가이드라인은 효과적인 보안 대책 수립을 규칙, 사람, 기술의 세 가지 측면에서 접근하고 있다.

또한 일본은 국내의 스마트폰 보급 확대로 인한 스마트워크 환경변화에 대응하고자[16] '11년 10월부터 스마트폰과 클라우드 서비스 이용에 관한 정보보호 과제들을 도출하고 안전한 이용 환경 마련을 위한 「스마트폰, 클라우드 보안 연구회」를 운영하였다.[17] 본 연구회에서는 '12년 6월 최종보고서를 통해 이른바 '스마트폰 정보보호 행동계획'을 제안 하였다. 본 행동계획은 정부, 사업자, 이용자별 역할과 책임을 명시하고 이용자 보호관점의 기술개발 및 대책의 마련을 천명하고 있다.

일본은 일찌감치 모바일 오피스 환경의 보안대책에서 출발하여 스마트워크 환경으로 진화해 가며 체계적인 대응책을 마련하고 있다. 또한 최근에는 클라우드 등 신규 서비스에 대한 보안 대책마련까지 스마트 사회 위협에 대한 종합적이고 지속적인 정책 대응을 강구 하고 있는 것이 특징이다.

4. 스마트 사회 보안위협의 대국민 홍보에 주력하는 호주

호주에서는 범정부 차원에서 스마트 시대의 데이터 보안 및 프라이버시에 대한 대책마련에 주력하고 있다. 호주 정부는, 일례로 2011년 '프라이버시 인식 주간(Privacy Awareness Week)'을 선포했다. 또한, 스마트폰을 포함한 휴대전화의 사용 시 프라이버시와 보안에 대해 국민의 경각심을 일깨우기 위해 포켓 사이즈의 참고 지침을 휴대전화 이용자들에게 제공하였다.

이러한 정보보호 관련 정책 및 인식제고 활동은 '호주 연방 정보 커미셔너(Office of the Australian Information Commissioner)'가 주도적으로 추진하고 있다.[18] 또한 청소년을 대상으로 스마트 사회의 보안 수칙을 홍보하기위한 '사이버스마트(cybersmart)'사이트를 개설하여 인터넷, 모바일 보안에 대한 자료나 가이드라인 등 정보교육 자료를 제공 중에 있다.

또한 호주 국방부는 스마트 시대의 다양한 모바일 장비의 정보 보안의 문제를 중요 의제로 공공정보와 시스템의 보안 매뉴얼(Australian Government Security Manual)을 만들어 '10년 11월부터 운용 중에 있다.

호주의 정책적 특징은 공무원과 일반 시민들에게 정부가 나서

그림 4. 사이버 스마트 웹사이트
※ 출처: http://www.cybersmart.gov.au/

휴대전화 등 모바일 기기 시대의 정보보안 지침을 마련하는 등 적극적 대국민 인식제고 및 홍보에 있다.

Ⅳ. 국내 스마트 정보보호 현황과 실태

1. 스마트 사회위험에 대비한 정보보호 정책추진

'09년 이후 본격적으로 국내에서도 스마트 폰 등 각종 모바일 기기 활용이 증가하면서 국민의 인터넷 이용패턴도 모바일로 변화하기 시작하였다. 향후 스마트폰, 스마트패드, 스마트TV 등 다양한 스마트기기를 활용한 스마트 라이프의 가속화로 이른바 '스마트사이어티(Smartciety)'[19]가 본격적으로 도래하면서 스마트폰 누적 가입자 수는 '15년에는 4천만 명을 넘어설 것으로 전망된다. 이러한 모바일 인터넷으로의 패러다임의 전환은 새로운 정보보호 위협도 야기하여 모바일 정보보호에 대한 사

16 '11년 일본 국내 스마트폰 출하는 2,340만대로 전체휴대폰의 55.8%를 차지하고 있으며 동년 12월말 기준으로 스마트폰 중 안드로이드폰 58.1%, iOS가 37.2%를 차지하고 있다.

17 관련자료는 http://www.soumu.go.jp/main_sosiki/kenkyu/smartphone_cloud/index.html 를 참조

18 http://www.oaic.gov.au/

19 Smart+Society의 합성어로 스마트폰 등 각종 스마트기기로 대화와 소통이 이루어지고 업무, 학습, 진료 등 사회 전반에 스마트 기술이 활용되는 사회를 지칭한다.

회적 요구가 증대되고 있다.

따라서 정부는 향후 '3천만 스마트 폰 이용자 시대'를 대비한 안전한 모바일 인터넷 사회구축을 위한 선행적 준비로 「스마트 모바일 시큐리티 종합계획」을 2010년 마련하였다. 본 종합계획에서는 ①미래 모바일 서비스 · 인프라 보안품질 향상, ②모바일 이용자 프라이버시 보호 확립, ③모바일 정보보호 기반 조성을 3대 목표로, 서비스 · 인프라 보호, 이용자 보호, 보호기반 확충 분야에 대한 10대 중점과제를 추진하는 것으로 되어있다.

특히 스마트폰에 대해서는 스마트폰 보안위협에 대한 대응을 위해 '10년 1월 '스마트폰 정보보호 민 · 관합동대응반'을 구성하여, 스마트폰 보안위협에 대한 선제적 예방 및 신속 공동대응 체제를 구축했으며, 이용자 10대 안전수칙 마련, 국내 스마트폰 악성코드 발생 대응, 스마트폰 정보보호 주체별 역할 정립 등을 추진해 왔다.[20] '11년 6월 국내 스마트폰 이용자들을 대상으로 본인 스마트폰에 적합한 모바일 백신을 검색하고 직접 설치하여 사용할 수 있도록 '스마트폰 백신 이용 안내서'를 개발하여 보급하였다. 또한 스마트폰 이용자 보안인식 제고를 위하여 자신이 사용하고 있는 스마트폰의 보안수준을 점검하고 조치할 수 있도록 지원하는 '스마트폰 보안 자가점검 앱(App)'을 '11년 9월에 개발하여 보급하였으며 '12년에는 기능강화버전을 추가로 보급하고 있다.

2. 스마트 사회의 신규서비스에 대한 이용자 실태

한국인터넷진흥원의 「'11년도 정보보호 실태조사」에 따르면 국민의 대부분이 스마트폰, SNS, 무선인터넷 서비스에 대한 보안의 중요성을 인식하고 있으며 특히 스마트폰 보안에 대해서는 93.3%가 중요성을 인식하고 있는 것으로 나타나고 있다.[21]

스마트폰의 피해 유형별로 이용자의 인지정도는 개인정보 유출(71.1%), 피싱(61.6%) 등의 순으로 나타나 보안의 중요성 만큼이나 피해유형에 대해서도 많이 알고 있는 것으로 조사되었다. 다만, 실제 피해를 경험한 여부는 개인정보 유출 4.5%, 피싱 3.3%로 아직 일반인들이 느낄 만큼의 피해가 발생하고 있지는 않은 수준임을 알 수 있다.

그러나 국내외 관련 동향을 살펴보면, 스마트폰 관련 위협이 매우 심각해지고 있음을 알 수 있다. 스마트폰에 저장된 카드정보 등 금융정보를 도용하거나, 개인정보가 무단으로 유출된 사고들이 빈번히 보도되고, 특히 미국 보안업체 트렌드마이크로의 3/4분기 분석 보고서에 따르면 안드로이드 기반에서의 모바일 악성코드 발생이 당초 올 8월까지 3만건으로 예상하였으나, 안드로이드를 타깃팅한 악성코드의 폭증으로 9월까지 17만5천건의 악성코드를 발견한 것으로 나타났다.

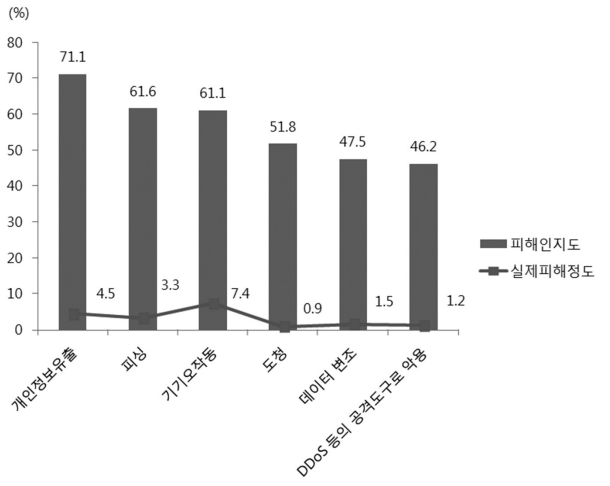

그림 5. 스마트폰 피해 유형별 인지도와 실제 피해
※ 출처: 한국인터넷진흥원(2011), 정보보호 실태조사.

반면에, 기업의 정보보호 수준을 살펴보면, 사업체 중 정보보호 전담조직을 설치 · 운영하고 있다고 응답한 업체는 12.6%, 개인 정보보호 전담조직을 설치 · 운영하고 있는 업체는 34.1%로 아직 기업들의 정보보호 대응수준을 미약한 형편이다. 스마트 사회위협에 대한 대응 정도를 살펴보면 SNS에 대한 공식적인 보안정책 및 가이드라인을 수립하고 있는 사업체도 11.4%로 낮게 나타나고 있다. 또한 클라우드 컴퓨팅 서비스를 이용하고 있거나 이용계획이 있는 사업체 중 41%만이 보안 대책을 수립하고 있으며 모바일 오피스를 도입했거나 계획 중인 업체 중 55.1%가 보안대책을 수립하고 있는 상황이다. 이상의 실태를 토대로 국내 스마트 정보보호의 문제점을 다음과 같이 정리 할 수 있다.

첫째, 개인 이용자 대부분은 스마트 정보보호의 중요성에 대해 인식은 하고 있으나 실제 피해발생은 낮아 심각성에대한 인지나 적극적인 보호행위가 부족한 상황이다.

둘째, 기업의 정보보호는 현재 보안 위협에 대응하기 위한 체계 구축 및 투자가 미흡한 수준이며, 스마트 시대의 보안위협에 대한 준비 또한 이용자가 느끼는 중요도에 비해 매우 낮은 상태이다.

Ⅴ. 결 론: 정책제언

현재 우리사회는 인터넷의 진화와 정보통신기술의 급속한 환경변화 속에 있다. 특히 스마트폰의 확산과 무선인터넷의 활성

20 '스마트폰 정보보호 민 · 관 합동대응반'은 방통위를 비롯, KISA, ETRI, 이동통신사, 제조업체, 백신 · 보안업체, 애플리케이션 개발사 등이 참여하고 있다.

21 정보보호 전반에 대한 중요성 인식은 97.4% 수준이다.

화, 새로운 융합서비스의 지속적인 등장으로 우리 생활방식과 업무방식, 소통방식 등 다양한 변화가 일어나고 있다. 향후 이러한 변화는 디바이스간 융합을 넘어서 모든 사물이 연결되는 超연결(Hyper-Connectivity)의 시대로 진화해 나갈 전망이다.

그러나 정보사회의 진화와 더불어 역기능 또한 다양해지고 심화되고 있어 주요한 사회 이슈가 되고 있다. 본고에서는 지금까지 살펴본 스마트 사회의 위협을 토대로 정보보호정책의 방향에 대해 몇 가지 제언을 하고자 한다.

첫째, 우리 사회의 특성을 반영한 정보보호 정책철학에 의거한 정책수립이 필요하다. 현재의 정보보호 정책들은 기술주도적 관점에서 위협들을 분석하고 대응방안을 강구하고 있으나 가장 중요한 정책철학이 결여되어 있다는 것을 지적하고 할 수 있다. 예를 들어 최근 사회적 이슈가 되고 있는 개인정보보호만 보더라도 우리사회의 정서상 미국이나 다른 선진국 사회와는 문화적 성향에서 차이가 난다.[22] 그러나 정책은 이러한 문화적 차이나 이용자 정서의 고려보다는 규제를 양산하는데 집중하여 다양한 반대 의견 및 구성원간 충돌을 양산하고 있다. 따라서 정책 수립에 앞서 심도 있는 사회 · 문화적 고찰, 다양한 사회구성원들이 참여하는 사회적 합의를 통하여 우리사회 전반의 방향성을 정하는 정책 철학을 마련한 후에 정책을 수립하고 추진하는 것이 중요하다.

둘째, 사전적인 정보보호 정책의 설계가 필요하다. 그동안 정보보호 정책은 그 특성상 정보화에 뒤따른 사후적인 성격이 강하게 작용하였다. 항상 새로운 기술, 서비스가 보급되고 그것이 확산되면서 문제점이 지적되거나 사고가 발생한 후에야 정책이 수립되는 것이 일반적이었다. 이러한 사후적 정책 수립은 역기능으로 인한 사회경제적 피해를 양산시키는 결과를 가져왔다. 특히, ICT의 패러다임이 스마트화로 변화되면서 이기종간의 융합화, 컨버전스화로 역기능이 발생하게 되면 그 피해는 급속히 확산될 수밖에 없는 구조가 되고 있다. 따라서 미래 사회변화를 예측하고 새롭게 나타날 위협들을 전망하여 사전적이며 체계적으로 대응해 나가야 할 것이다. 물론 울리히 벡의 지적과 같이 현대 산업사회에는 필연적으로 다양한 위협요소가 존재할 수밖에 없는 사고전제(事故前提)사회임을 인정해야 하나 사전적인 위기대응은 사고의 크기와 피해정도를 줄일 수 있다.

셋째, 정보주체가 자발적으로 참여하고 자율적인 보호역량 높이는 정책 추진이 필요하다. 국가 주도하는 정보보호 정책만으로는 스마트시대에 다양한 위협에 효과적으로 대처하기 어렵다. 따라서 개인, 기업, 정부 모두가 스마트 시대의 보안위협이나 피해를 인식하고 자발적이고 지속적인 보호활동이 전개되어야 한다. 개인은 자기 방임적 정보보호 의식을 개선하여 실천하는 정보보호의 생활화가 정착되도록 하는 것이 필요하고, 기업은 사회적 책임의식을 기반으로 이용자 정보를 포함한 보유 정보가 비즈니스 대상이 아닌 사회 공동자산이라는 인식을 가지고 관리 · 유통할 수 있도록 해야 한다. 따라서 정부 정책도 이처럼 사회 모든 구성원의 인식을 높이고 정보보호 문화가 정착될 수 있도록 장기적 관점에서 수립되어야 한다.

넷째, 획일적 규제 정책의 탈피가 필요하다. 특정 서비스나 보호기술만이 허락되는 획일적인 규제를 탈피하여 이용자 선택권을 보장한 유연한 규제가 강구되어야 할 것이다. IT가 사회 전 분야와 결합하여 다양한 서비스와 기술이 개발되고 있으며, 서비스 이용 계층 또한 다양해진 만큼 많은 보호기술이나 서비스가 서로 경쟁해서 시장에서 선택받고 발전해나갈 수 있도록 하는 유연한 규제 정책이 마련되어야 한다. 하지만 유연한 규제가 시장의 혼란을 주어서는 안 된다. 즉 규제의 범위가 모호하거나 포괄적으로 된다면 오히려 많은 부작용을 양산할 수도 있다는 것을 명심해야 한다.

마지막으로 미래 환경에 대비한 정보보호측면의 전략적 연구정책이 필요하다. 지금까지 우리정부는 정보보호에 관한 다양한 정책을 수립해 추진해 왔으나 그동안의 정책들이 ICT 진흥정책을 보완하는 역할의 비중이 높았다. 하지만 앞으로의 정보보호 정책은 ICT 전체를 조망하고 선도하는 정책이 되어야 할 것이다. 그러기 위해서는 스마트 시대와 빅 데이터 환경의 보안위협 및 보호기술에 대한 전략적인 연구가 계속되어야 한다.

따라서 이러한 미래 사회 보호 정책을 기획하고 지원하는 전문기관의 역량 강화와 전문 인력의 확충이 동반되어야 할 것이며, 국내 최고의 정보보호 전문기관으로서 한국인터넷진흥원의 역할이 매우 중요하다고 할 것이다.

정보보호는 더 이상 우리 사회의 규제와 비용이 아니며 스마트 사회로 진입하기 위한 핵심 요소이다. 우리 사회가 불안한 스마트 사회로 진화하지 않도록 정부와 관계 전문기관이 정책 수립에 많은 고민과 노력이 필요한 시점이 되었다. 이러한 정책적 변화와 노력이야 말로 우리 사회를 '스마트 안전 사회'로 만들어 갈 첫 걸음이 될 것이다.

22 서양의 경우, 개인(Individual)의 어원은 '더 이상 나눌 수 없는 것'으로 '독립적 개체로서의 개인(절대 개인)'을 의미한다. 이러한 개념을 바탕으로 자유롭고 평등한 상호독립적인 존재로 개인을 통해서 「질서」, 「사회」, 「국가」가 설명된다는 사상적 바탕을 가지고 있다. 한편, 우리사회는 공동체문화(이른바 고맥락사회)에서 근대사회적 개인의식(프라이버시)은 매우 낮고 개인의 사생활정보를 공유하고 공개하는 것이 공동체 유지를 위해 필요하다는 의식 내재하고 있다.

참 고 문 헌

[1] 김성열, 소셜 네트워크 서비스 보안 위협요인에 관한 연구, 산업과학연구, 제30권 1호, 2012.1.

[2] 김지훈, 조시행, “사이버 환경에서의 보안위협”, 정보보호학회지, 제20권, 4호, 2010.8.

[3] 남기효, 김윤홍, “클라우드 서비스 분석 및 보안 이슈”, 주간기술동향, 2012.4.

[4] 이상우,서동일, 조현숙, “미래인터넷 보안 기술 동향”, 전자통신동향분석, 제26권, 5호, 2011.10.

[5] 이준호, “스마트 모바일의 발전과 정보보안”, 정보통신정책연구원, 제22권 13호, 2010.

[6] 은성경, “클라우드 컴퓨팅 보안 기술 동향”, 정보보호학회지, 제20권, 2호, 2010.4.

[7] 임상규, 이창길, 김종업, “스마트 시대의 보안 위협: EU5의 대응과 시사점”, 한국위기관리학회, 제7권, 4호, 2011.8.

[8] 윤창근, 김종업, 김유미, 이경래, “해외동향 스마트시대의 보안대책”, 지역정보화, 2011.5.

[9] 정교일, 박한나, 정부금, 장종수, 정명애, “빅 데이터와 정보보안”, 한국정보기술학회지, 제10권, 3호, 2012.9

[10] 홍진근, “스마트 환경의 주요 정보통신 기술과 정보보호 동향”, 한국 인터넷 정보학회, 제13권 1호, 2012.3.

[11] 방송통신위원회, 스마트 모바일 시큐리티 종합계획, 2010.12.

[12] 한국인터넷진흥원,『정보보호 실태조사』, 2012.3.

[13] 한국인터넷진흥원,『한국인터넷백서』, 2012.10.

[14] Beck, Ulrich(1986). Risk Society: Toward a New Modernity, Mark Ritter, ed., London: Sage.

[15] 内閣官房情報セキュリティセンター、平成23年度情報セキュリティ産業の活性化方策に係る調査、2012.3.

약 력

이 기 주

1982년 고려대학교 행정학사
1990년 서울대학교 대학원 행정학석사
1996년 미국 조지워싱턴대학교 대학원 통신정책학석사
2012년 미국 조지워싱턴대학교 대학원 정책학박사
2007년 정보통신부 통신전파방송정책본부장
2008년 방송통신위원회 이용자네트워크국장
2009년~2010년 방송통신위원회 기획조정실장
2011년~2012년 서강대학교 언론대학원 겸임교수
2010년~2012년 김앤장 법률사무소 고문
관심분야: 정보통신, 정보보호 정책