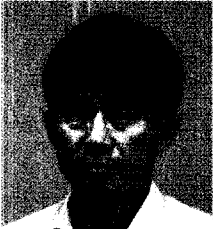


스마트 모바일 시큐리티 정책 방향

박철순 방송통신위원회 네트워크정보보호팀장



1. 머리말

지난 1년간 스마트폰, 스마트패드(태블릿 PC)를 비롯한 각종 모바일 단말의 급속한 보급과 다양한 신규 모바일 비즈니스 모델의 등장은 과거 10년간의 '유선 인터넷 패러다임'에서 '유·무선 통합 인터넷 패러다임'으로 변화를 이끌고 있다. 프랑스의 사회학자 자크 아탈리가 그의 저서 <21세기 사전>에서 21세기형 신인류의 모습으로 '디지털 노마드(Digital Nomad)', 즉 '디지털 유목민'을 언급한 것처럼 이제 우리는 스마트폰으로 촉발된 최첨단 정보통신 환경을 통해 시간적·공간적 제약으로부터 자유로울 수 있게 되었다.

비록 해외의 경우보다 그 변화가 늦게 시작된 감이 있으나, 최근 우리의 변화는 해외 어느 나라보다 그 속도가 빠르게 진행되고 있다. 2010년 12월 말 기준 국내 스마트폰 가입자 수는 725만여 명이 동통신 가입자 수의 약 14% 수준에 이르고 있으며, 올해는 더욱 많은 스마트 디바이스가 다량 보급

되고 2013년에는 스마트폰 가입자수가 3천만 명을 상회할 것으로 전망된다. 향후 스마트폰, 스마트패드, 스마트TV 등 다양한 스마트기기를 활용한 스마트 라이프가 진전되면 머지 않은 장래에 '스마트사이어티(Smartciety)¹⁾'가 본격적으로 도래할 것으로 보인다.

그러나 이러한 모바일 인터넷으로의 패러다임 전환에서 우리는 소위 해킹, 바이러스, 스팸 같은 유선상에서의 인터넷 역기능이 무선 인터넷상으로 전이될 수 있다는 점을 간과하기 쉽다. 과거 2003년 1.25 인터넷 대란, 2009년 7.7 DDoS(디도스) 공격이 모바일 인터넷에서 벌어진다면, 스마트기기 오작동과 통신 불능 등 그 피해는 상상을 초월할 것이다. 이러한 잠재적인 사이버 위협에 대하여 우리는 미리 대책을 마련하고, 관련 기술을 개발하며 제도를 정비함으로써 만일의 사태에 대비해야 한다.

이에 따라 방송통신위원회(이하 '방통위')는 2010년 상반기부터 '스마트폰 정보보호 민·관 합동대응반'(1월), '모바일 시큐리티 포럼'(4월), '미래융합 IT

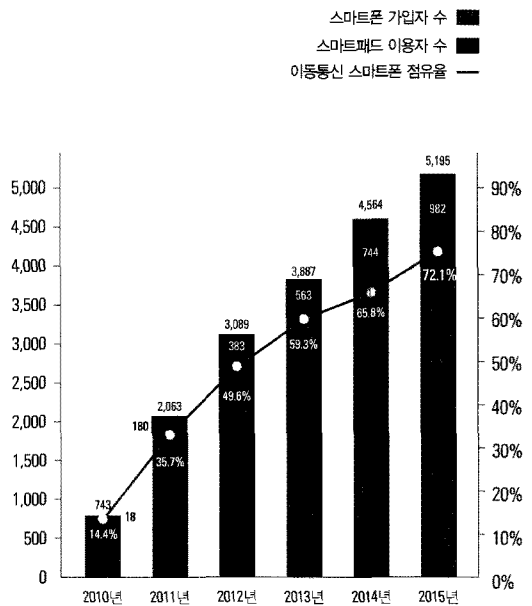
1) 스마트사이어티(Smartciety, Smart+Society의 합성어) : 스마트폰 등 각종 스마트기기로 대화와 소통이 이루어지고 업무처리, 학습, 의료진료 등 사회 전반에 스마트기술이 활용되는 사회를 지칭(금번 방통위 종합계획에서 처음 사용)

서비스 보안연구회'(5월) 등을 구성·운영해 오면서, 향후 '3천만 스마트폰 이용자 시대'의 폭발적인 모바일 인터넷 이용 확산에 따른 잠재적 보안위협에 선제적으로 대비하고, 글로벌 모바일 보안시장에서의 국가경쟁력을 확보해 모바일 보안강국이 되기 위한 중장기(2011~2015년) 「스마트 모바일 시큐리티 종합계획」을 수립(2010.12.24)하였다. 본 고에서는 모바일 인터넷에 관한 정부 차원 최초의 선제적인 보안 종합대책에 대해 알아보고, 그 시사점에 대해 살펴보고자 한다.

2. 모바일 인터넷 환경 현황 및 전망

모바일 인터넷 이용은 얼마전까지만 해도 비싼 무선 인터넷 요금, 무선 통신 인프라 투자 부족, 모바일 단말기 보급 미흡 등으로 대중화가 되기에는 어려움이 있었다. 하지만, 스마트폰의 도입과 함께 무제한 무선 요금제 출시, 무선랜(Wi-Fi) 및 이동통신 인프라의 투자 및 구축 확대, 국내외 제조사로부터의 다양한 모바일 단말기의 보급 증가 등으로 인해 모바일 인터넷의 이용이 크게 증가하고 있다. 현재 국내 스마트폰 가입자 수는 스마트폰 보급 이전의 예상보다 빠르게 증가 추세를 보이고 있는 중이며, 2012년에 국내 스마트폰 누적 가입자는 3천만 명에 육박하고 2015년에는 4천만 명을 훨씬 상회할 것으로 전망된다. 또한 2015년 국내 무선데이터 트래픽 규모는 모바일 멀티미디어 콘텐츠 및 소셜네트워크서비스(SNS) 커뮤니티의 데이터 통신량 증가로 인하여 2010년 대비 약 40배 이상 증가할 것으로 예상된다.

특히, 스마트폰은 '손안의 PC'로 불리며 사람들의 생활과 업무환경, 교육, 가사, 의료 등 사회 모든 분



※ 'Mobile voice and data forecast pack: 2010-15' OVUM(2010.5월) 및 '2010 국가정보화백서(NIA, 2010.7월)' 등을 기반으로 KISDI·KCC 예측(2010.11월)

【그림 11】 국내 스마트폰 및 스마트패드 (누적) 보급 전망

야에 걸쳐 대혁신('Mobile Big Bang')의 기회를 제공할 것이다. 산업·경제적 측면에서 폐쇄적 산업구조가 개방되며 그동안 뒤쳐져 있던 국내 S/W, 콘텐츠, 서비스 부문에서 선진화 계기가 제공되고, Web 2.0의 개방·공유·참여의 정신과 모바일 기반의 이동성이 결합되어 이용자의 새로운 생산소비 문화를 창출하고 국내의 시장에 LBS, 소셜커머스 등 신규 모바일 비즈니스 모델을 확산시킬 것으로 예상된다. 사회·문화적 측면에서는 원격으로 가사활동, 학습, 진료가 가능해지고 SNS를 통한 광범위한 정보공유를 토대로 새로운 사회적 관계가 형성될 것이다. 특히 종래의 사무실 개념을 탈피하여, 언제 어디서나 편리하고 효율적으로 업무에 종사할 수

있도록 하는 스마트 워크(Smart Work)의 정착을 통해 기업·행정 부문의 업무환경 개선 및 업무효율의 극대화가 추후될 것이다.²⁾ 뿐만 아니라 환경·에너지 측면에서 모바일 부문의 친환경 활동과 모바일을 활용한 에너지 수요공급 관리, 환경 감시 등 생활환경의 에너지 절약을 가능하게 하는 그린 ICT 서비스의 활성화로 '저탄소 녹색성장'의 국가 비전을 달성하는데 기여할 수 있을 것이다.

3. 모바일 시큐리티 위협

앞으로 급속도로 확장될 모바일 인터넷 환경에서도 인터넷 침해공격, 바이러스·웜 감염, 정보유출 등 기존의 보안 위협이 재현될 수 있다. 특히, 해외의 모바일 악성코드 유포 사례를 통해 유추해 볼 때 국내의 경우도 2011년 하반기부터 급전적 이득을 노리는 스마트폰 악성코드의 출현이 예상되고

2012년부터 본격적으로 악성코드가 유포될 것으로 전망된다. 2010년 4월, 원도 모바일 운영체제를 사용하는 스마트폰을 대상으로 국제전화 무단발신을 유발하는 모바일 악성코드가 국내에서 처음 발견되었으나, '스마트폰 정보보호 민·관 합동대응반'의 사전조치 및 신속한 대응으로 다행히 피해를 사전에 예방하였던 사례는 우리의 경각심을 일깨우기에 충분하였다.³⁾

또한, 새로운 서비스 도입에 따른 신규 보안 위협이 출현할 수 있다. 단말기기에 무선랜(Wi-Fi), 블루투스, 이동통신서비스(3G), GPS통신 등 복수의 통신기능이 기본 탑재됨에 따라 침해경로가 다변화되고 IPTV, 클라우드 컴퓨팅 등 유선망의 신규 서비스가 무선 환경으로 이용됨에 따라 안전성을 위협하는 요인도 증가하고 있다. 또한 중요한 개인정보를 담고 있는 모바일 기기의 분실·도난 시 개인정보 노출, 사기범죄에 악용 등의 피해가 우려되고,



[그림 2] 모바일 4대 영역별 보안위협

2) 스마트워크 근무율을 2015년까지 전체 공무원과 노동인력의 30%까지 높이는 방안이 범 정부차원에서 추진(스마트 워크 활성화 전략, 2010. 7월)
3) 전 세계 모바일 악성코드는 2010년 2/4분기까지 약 600여 종 이상 추정

정품 스마트폰을 변형(예: jailbreak, rooting)할 경우 해킹에 노출될 위험성도 크다. 그 밖에도 위치기반 서비스(LBS)에 의한 개인 위치 노출 및 사생활 침해 가능성 및 모바일 단말기를 통한 불건전 정보 및 유해 사이트 접근의 위험성도 우려되고 있다.

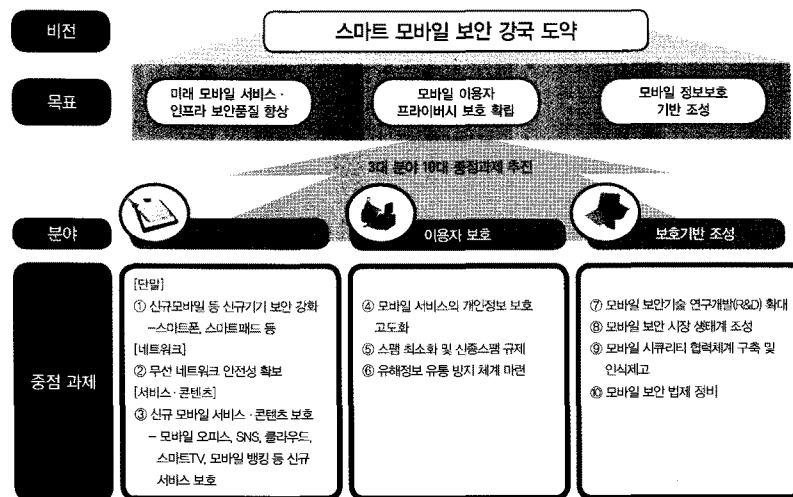
아래 ▶ 미래 모바일 단말·서비스 보안품질 향상, ▶ 모바일 이용자 프라이버시 보호 확립, ▶ 모바일 정보보호 기반 조성을 3대 목표로, 서비스·인프라 보호, 이용자 보호, 보호기반 확충 분야에 대한 10대 중점과제를 추진하기로 했다.

4. 모바일 시큐리티 정책방향 및 주요 과제

방통위는 작년 상반기부터 스마트폰 정보보호 위협에 대비한 국가차원의 전략 수립을 준비해왔다. '모바일시큐리티포럼', '인터넷 정보보호 협의회' 등을 통해 종합계획 수립방향을 정립하고(2010.5), 전담반 구성·운영, 전문가그룹 자문(8회), 방통위원장 주재 모바일 보안업체 CEO 간담회(2010.12) 등을 통해 '스마트 모바일 시큐리티 종합계획'을 마련했다. 그리하여 향후 '3천만 스마트폰 이용자 시대'에 대비해 '스마트 모바일 보안 강국 도약'이라는 비전

4.1 미래 모바일 서비스·인프라 보안품질 향상

방통위는 ① '한국형 앱 게놈 프로젝트'를 추진하여 유통 중인 앱을 분석해 악성행위 수행 및 개인정보 침해 여부를 파악하기로 하고, 애플리케이션 스토어에서는 자체적으로 표준화된 검증 기준 및 절차를 준수하여 사전 보안 검증이 가능하도록 '그린 마켓 인증 체계'⁴⁾ 마련을 검토할 예정이다. 또한 다양한 스마트폰 단말 및 플랫폼별 통합시험이 가능한 '모바일 백신 테스트베드'를 구축하여 중소 보안업체들이 백신의 성능을 측정할 수 있도록 지원하는 한편, 스마트폰 및 스마트패드에서 사용되



[그림 3] 스마트 모바일 시큐리티 종합계획 비전 및 목표

4) 그린 마켓 인증체계 : 앱에 대한 표준화된 보안 검증 절차 및 가이드라인을 준수하고 지속적인 사후 관리를 수행하는 마켓을 선정하여, 신뢰할 수 있는 마켓임을 정부가 인증

는 보안 앱 및 솔루션을 검증할 계획이다. 그리고 스마트패드, e-Book, PMP 등 스마트화 되어가는 다양한 단말기와 향후 개인 단말과 연결될 홈네트워크에 대한 보안방안 등을 마련하고 홈네트워크 신뢰 보안 아키텍처 모델을 연구하기로 했다. ② 무선 네트워크에 대한 안전성 확보를 위해 공중 무선랜의 체계적인 보안 관리체계 수립 및 이용자 인식 제고 등을 통해 무선랜 보안수준을 강화하고, 모바일 인터넷망과 IP 백본망과의 연동망 구간에 네트워크 침입탐지 및 대응시스템 구축 등도 추진해나갈 계획이다.

그리고 ③ 최근 신규 모바일 서비스로 각광받고 있는 모바일 오피스의 성공적인 도입 기반 마련을 위해 예상되는 보안이슈에 대해 분석하고, 스마트워크 정보보호 모범사례를 발굴하여 이용 확산 환경을 조성하며, 안전한 모바일 SNS 환경 구축 및 이용을 위한 안내서를 개발·보급하고 홍보 및 교육을 통한 이용자 윤리 의식을 강화할 예정이다. 또한 모바일 클라우드 표준 SLA 가이드라인 마련 및 스마트TV 디바이스·콘텐츠 보안 솔루션 개발 지원, 모바일 बैं킹 보안 취약성 점검 지원 등 신규 모바일 서비스들의 보안 체계 강화를 통해 안전한 서비스 환경을 조성할 계획이다.

4.2 모바일 이용자 프라이버시 보호 확립

다양한 신규 모바일기기를 통해 보다 다양한 인터넷 접속환경이 제공되고 있으나 악성코드 감염 및 개인정보 유출 경로가 확대되고, 원하지 않는 스팸의 발송수단으로 악용되는 사례가 늘어날 것으로 예상된다. 이를 방지하기 위하여 ④ 모바일 서비스의 개인정보 및 위치정보 보호 강화를 위해 개인

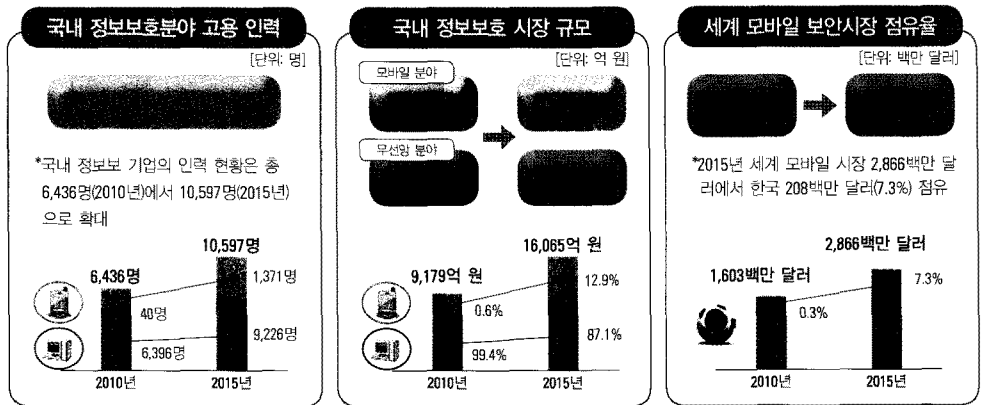
정보 암호화 등 보호수단을 제공하고, 애플리케이션 개발 및 모바일기기 제조 시 이용자가 이해하기 쉬운 개인정보보호 권고안을 제시하여 수집되는 개인정보 종류, 수집목적, 수집기간 등의 고지 및 이용자의 동의 획득 등의 절차를 마련해 관리책임을 강화할 예정이다. 또한, 앱 프라이버시 안전성 검증체계를 마련하고, 위치정보사업자와 위치기반 서비스사업자로 하여금 이용자 자신의 위치정보 사용 확인 및 설정 변경이 가능한 '개인위치정보 자기제어시스템'⁵⁾ 구축 등을 추진토록 할 계획이다.

또한 ⑤ 모바일 스팸 방지 및 최소화를 위해 신규서비스의 스팸 위험성을 분석하고 지능형 필터링 등 안티스팸 서비스 강화를 통해 모바일 스팸을 최소화할 것이며, ⑥ 모바일 유해정보 차단 앱 개발 및 보급을 추진하고, 애플리케이션 스토어 모니터링 체계를 마련하여 모바일 유해정보의 유통을 방지해 나갈 계획이다.

4.3 모바일 정보보호 기반 조성

모바일 정보보호 기반 조성을 위해서는 ⑦ 저전력·경량암호, 단말 및 플랫폼 보호, 무선망 인프라 보호, 모바일 콘텐츠 보호 등의 핵심 원천 보안기술 개발 지원을 강화할 것이며, ⑧ 모바일 보안업체와 단말 제조업체, 이통사 간의 협력 어려움 타개 등을 위한 '(가칭)모바일 시큐리티 협의회'를 구성·운영해 보안시장의 상생 생태계 조성을 위해 노력할 계획이다. 또한 산·학·연·관의 '모바일 보안표준 연구센터' 등의 설립을 통해 신규 보안기술의 민간이전 및 상용화를 지원하고 관련 모바일 보안기술의 국제 표준화(ITU-T 등)를 추진하기로 했다. 그리고 ⑨ 모바일 보안 분야 전문연구기관(Think-

5) 개인 위치정보 자기제어 시스템: 이용자가 PC나 스마트폰을 통해 언제나 자신의 위치정보 설정 변경 및 사용내역 확인을 할 수 있는 관리시스템



*출처 : [신규채용] KISIA(2009.12월), [국내시장규모] 한국IDC(2009.6월) 및 KISIA(2009.12월), [세계시장점유율] IDC(2010.5월) 기반으로 KISA 예측(2010.11월)

[그림 4] 산업·경제적 기대효과

Tank)을 지원하고 유관기관 간 모바일 시큐리티 협력체계 강화와 인식제고를 위한 노력을 확대해 나갈 것이며, 모바일 정보보호 취약계층 교육 및 정보보호 문화 확산 운동을 전개할 것이다. 한편, ⑩ ‘(가칭)스마트 모바일 보안 법제연구회’ 구성·운영을 통해 스마트기기, 신규 모바일 서비스의 안전한 이용 보장을 위한 법제도 개선도 추진하기로 했다.

5. 맺음말

방통위는 10대 과제를 이용자의 수요, 기반기술의 선도성, 신시장 창출 등과의 상승적 결합을 고려하여 단기·중장기 추진과제로 구분해 단계적으로 정책 추진을 해 나갈 예정이며, 이를 통해 모바일 보안시장 활성화 및 관련 산업경쟁력 제고에 기여함으로써 국내 모바일 보안시장 규모가 2010년 57억 원 수준에서 향후 2015년까지 2,078억 원으로 확대되어 세계 모바일 보안시장의 7.3%까지 차지할 수 있을 것으로 예측하고 있다. 또한 모바일

시큐리티에 대한 이번 방통위의 종합계획 수립 및 시행에 따라 미래 모바일 보안위협에 대한 사전적 예방으로 사회적 비용을 최소화시키고, 안전한 모바일 서비스 이용환경을 조기에 구축함으로써 국민들의 삶의 질이 향상되고 대한민국의 위상이 제고될 것으로 기대된다.

향후 모바일 인터넷 이용에서부터 스마트 그리드, 스마트 빌딩, 사물지능통신 등 새로운 유무선 융합 서비스 환경의 안전한 네트워크 기반 구축에 이르기까지 급변 ‘스마트 모바일 시큐리티 종합계획’이 과거와 달리 사후적 대응책이 아닌 신규 서비스의 보안위협에 대한 사전적 대비책 마련이라는 점에서 정책 패러다임 전환의 시금석이 될 것이다. 이를 통해 모바일 시큐리티가 사회적 비용이 아니라 국내 보안 기업들의 글로벌 모바일 보안시장 진출을 위한 투자 및 모바일 산업발전과 서비스 활성화를 위한 필요 불가결한 전제라는 인식으로 자리잡을 수 있을 것으로 기대된다. TTA