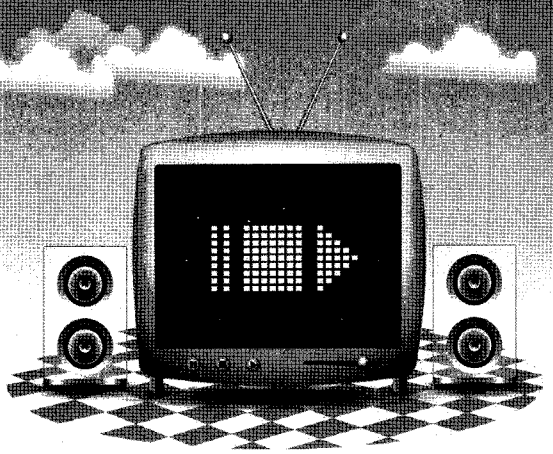
스마트폰 정보보호 정책방향



박철순 | 방송통신위원회 네트워크정보보호팀장

1. 머리말

2009년 11월 말 국내에 아이폰이 상륙하면서 촉발된 스마트폰 열풍은 2009년 말 100만 가입자를 돌파한 이후 올해에도 지속되어 그 이용자 수가 폭발적으로 증가하고 있다. 스마트폰이 본격적으로 활용되면 개인 이용자 측면에서는 생활밀착형 콘텐츠를 통한 생활 편의성 증대 및 다양한 스마트폰 애플리케이션을 활용한 '생활의 스마트화'가 가능하며, 기업의 측면에서는 모바일 오피스를 통한 업무 효율성 증대 및 비용 절감 효과를 기대할 수 있다.

그러나 스마트폰은 이러한 편의성 · 효율성에도 불구하고 인터넷 침해공격, 바이러스 · 웜 감염, 개인정보유출 등 기존 PC 상에서의 보안위협이 재현될 수 있으며, 무선랜, 이동통신서비스(3G, 4G), GPS 통신 등 복수의 통신기능이 기본 탑재됨에 따라 침해 경로가 다변화되어 새로운 유형의 보안위협에 노출되어 있기도 하다.

이에 따라 방송통신위원회는 이러한 스마트폰의 보안위협에 적극적으로 대응하기 위해 올해 초부터 '스마트폰 정보보호 민 · 관 합동대응반'을 구성 · 운영하는 등 스마트폰 보안위협에 대한 예방적 · 선제적 대응체계를 구축해 나가고 있다.

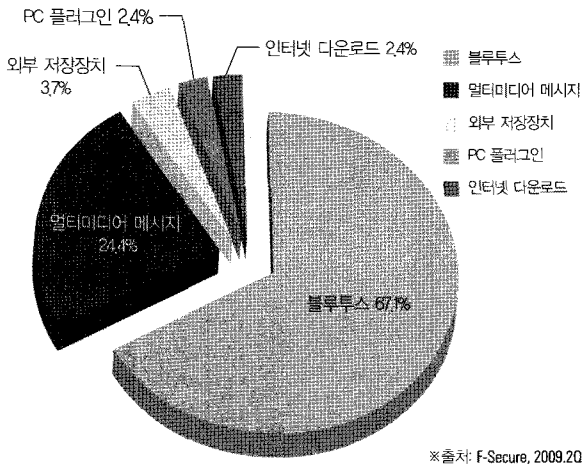
2. 스마트폰 보안위협 현황

현재 국내 스마트폰 가입자 수는 2010년 10월 말 기준 525만 명으로 전체 이동통신 가입자의 10.4%를 차지하고 있으며, 2010년 말까지는 스마트폰 가입자 수가 700만 명에 육박할 것으로 예상되고 있다. 또한 스마트폰 가입자 수가 2014년에 3천만 명을 넘어서고 2015년까지 4천만 명에 육박하여 전체 이동통신 가입자의 70% 정도를 차지할 것으로 전망되고 있다.

이처럼 스마트폰 보급이 활성화됨에 따라 해외 스마트폰 악성코드의 국내 유입가능성 또한 증가하고 있는 것이 현실이다. 해외에서 2009년 6월까지 발견된 스마트폰 악성코드는 총 524종(출처: SMobile Systems)이며, 증가추세 및 국내외 보도 자료를 볼 때 2010년 3/4분기 기준 약 600여 종 이상으로 추정되고 있다.[1]

1) 최초의 스마트폰 악성코드는 Cabir로 2004년 8월 필리핀에서 발견

해외에서 발견된 스마트폰 악성코드는 개인정보 유출, 단말이용제한, 부정과금 유발 등의 피해를 발생시킬 수 있는 것으로 보고되고 있으며, 이러한 악성코드는 주로 단말기의 블루투스와 멀티미디어메시지(MMS)를 이용한 첨부파일 전달방식으로 전파를 시도하는 것으로 조사되고 있다.

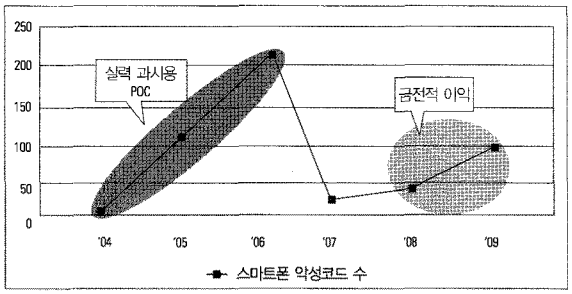


[그림 1] 감염경로별 악성코드 현황

국내에서는 지난 4월 윈도우모바일 운영체제를 사용하는 스마트폰을 대상으로 국제전화 무단발신을 유발시키는 모바일 악성코드가 최초로 발견되었다. 그러나 '스마트폰 정보보호 민·관 합동대응반'의 사전 조치 및 신속한 대응으로 피해는 발생하지 않았다.

초창기 스마트폰 악성코드는 해커의 실력 과시를 위한 개념증명코드(POC: Proof Of Concept) 수준이었으나 2008년에 들어서면서 금전적 이득을 목적으로 하는 스마트폰 악성코드(Smarm.b, Swapi.a, SMSFree.d 등)가 나타나고 있다.

최근 악성코드의 제작 목적이 금전적 이득임을 감안한다면, 국내 스마트폰 이용자 비율이 10% 중반대에 도달할 것으로 보이는 2011년 상반기에 금전적 이득을



※출처: SMobile Systems, 2009.6

[그림 2] 연도별 스마트폰 악성코드 발생 수

노린 스마트폰 악성코드가 유포될 것으로 예상되고 있다. 특히 스마트폰 보급 확산 시점으로 예상되는 2012년 상반기(국내 스마트폰 점유율 30% 이상 예상 시점)에는 악성코드가 본격적으로 제작·유포될 것으로 전망되고 있다.[2)]

스마트폰의 보안위협은 기존의 PC 및 유선인터넷 위협요소에 더해 신규 위협요소가 추가되어 나타날 수 있다. 스마트폰은 기능폰의 인터넷 접속환경 및 개인휴대 단말기로부터 오는 특징과 PC의 개방형 플랫폼이라는 특징이 혼합되어 있는 복합적인 형태로 나타나고 무선랜(Wi-Fi) 및 블루투스 기능 기본 탑재로 공중 또는 사설 무선랜 사용 빈도가 높아지게 되어 침해사고 위험성이 커질 수 있다.

또한 개방형 스마트폰 애플리케이션 마켓을 통해 누구든지 콘텐츠 제작과 유통, 사용이 가능한 반면 애플리케이션 검증체계가 미흡하여 악성코드가 삽입된 애플리케이션 유통 위협이 존재한다. 지난 1월에는 국외 스마트폰 애플리케이션 마켓(사이디아)에서 판매된 온라인 뱅킹 프로그램이 금융사기에 활용된 사례가 보도된 적도 있다.

단말기 제조사에서 제공하는 S/W 이외의 별도 S/W를 사용하기 위해 정품 스마트폰을 변형(예: Jailbreak, rooting)할 경우 해킹에 노출될 위험성이 커지며, 주요

2) 해외의 경우 스마트폰 시장이 전 세계 휴대폰 시장의 10%를 넘어선 시점(2008년) 이후부터 금전적 이득 등을 노린 악성코드가 출현하기 시작

정보를 담고 있는 개인화된 스마트폰의 분실 및 도난 시 개인정보, 금융정보 유출에 따른 사생활 침해 및 금전적 피해도 예상되고 있다. 이밖에도 위치기반서비스(LBS)에 의한 GPS 장소 노출 및 사생활 침해 가능성도 제기되고 있으며, 국내의 경우 미성숙된 스마트폰 시장 여건 등으로 백신 보급이 활성화되지 않은 것도 보안 취약성을 증가시키는 요인이 되고 있다.

3. 스마트폰 보안위협 대응 현황 및 정책 방향

방통위는 이와 같은 스마트폰 보안위협에 대한 대응을 위해 2010년 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. '스마트폰 정보보호 민·관 합동대응반'은 방통위를 비롯, KISA, ETRI, 이동통신사, 제조업체, 백신·보안업체, 애플리케이션 개발사 등이 참여하고 있다.[3]

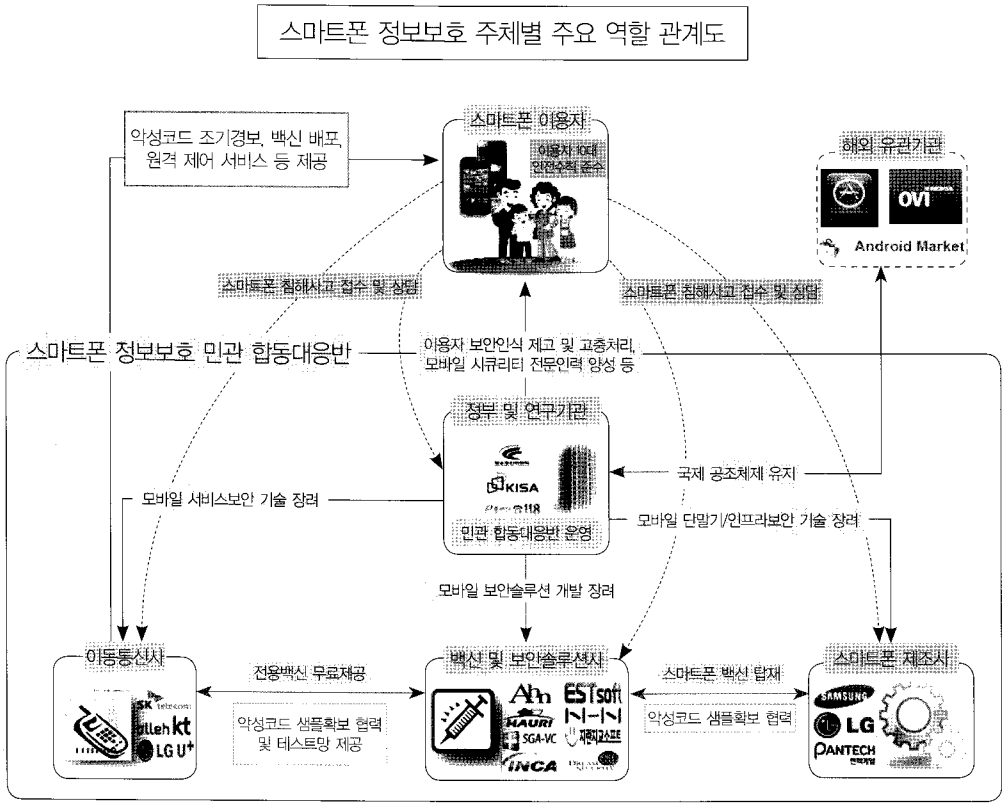
스마트폰 민·관 합동대응반은 우선 '스마트폰 이용자 10대 안전수칙'을 마련·제시하여, 이용자들이 평소에 악성코드 감염, 개인정보유출 등의 피해 예방을 스스로 실천할 수 있도록 하였다. 주요 내용으로는 악성코드 유포 경로로 악용될 수 있는 신뢰할 수 없는 애플리케이션 및 사이트 이용 주의하기, 발신인이 불명확한 메시지와 메일을 수신하였을 경우 바로 삭제하기, 스마트폰 운영체제 및 백신 프로그램을 최신 버전으로 업데이트 하기 등의 보안수칙을 담았다. 또한 단말기가 보안위협에 노출되지 않도록 스마트폰 플랫폼 구조를 이용자 스스로 임의로 변경하지 않도록 하고, 모바일 악성코드의 전파경로로 블루투스 기능 등의 무선 인터페이스가 악용될 수 있으므로 블루투스 및 무선랜 기능은 사용 시에만 켜놓도록 안내하였다.

스마트폰 민·관 합동대응반은 해외 악성 코드 발생에 대해서도 현황을 파악하는 등 지속적으로 대응하고 있다. 지난 4월에는 해외(영국)에서 '국제전화 무단발신을 유발하는 윈도우 모바일 기반의 악성 코드'가 발견됨에 따라 국내 유포 여부를 점검(4.16~20)하였으며, 이 과정에서 국내 첫 감염을 탐지하고 악성코드를 유포하는 모바일 게임을 차단하였으며, 전용백신 배포 등을 통해 확산을 방지했다.

또한 합동대응반은 지난 6월 말, 이통사, 제조업체, 백신업체, 정부 등 관련 주체별 스마트폰 정보보호를 위한 역할을 정립했다. 스마트폰 보안위협은 정부나 이용자 등 어느 한 주체의 노력만으로는 효과적인 대응에 한계가 있음을 공감하고, '이용자 10대 안전수칙' 발표의 후속조치로 이동통신사, 스마트폰 제조사, 백신사, 보안솔루션사와 같은 사업자와 정부 등 스마트폰 정보보호 각 주체가 선제적이고 체계적인 공동 대응이 가능하도록 주체별 필요한 상세 역할을 정립한 것이다. 스마트폰 정보보호 주체별 역할관계를 요약하면 [그림 3]과 같다.

한편 스마트폰 정보보호 민·관 합동대응반은 스마트폰 침해사고 발생 시 신속한 대응체계를 가동할 수 있도록 모바일 악성코드 공동대응 모의 훈련을 실시(2010.9.24)하였다. 안드로이드 마켓으로부터의 다운로드에 의한 악성 코드 감염을 가상하여 위협상황 발생에 따른 단계적 대응·조치방안이 신속하게 이루어지는지를 모니터링하고 악성코드 분석, 피해확산 방지, 전용백신 배포 등 대응절차를 점검했다. 올해의 모의 훈련

3) 스마트폰 정보보호 민·관 합동 대응반: 스마트폰 보안위협 관련 선제적 대응협력체제 구축 및 보안대책 마련 등을 위해 1월 21일 구성되었으며, 방통위와 KISA를 비롯, ETRI, 이통3사(KT, SK텔레콤, LG U+), 제조3사(삼성전자, LG전자, 팬택), 백신6사(안철수연구소, 하우리, 바이러스체이서, 이스트소프트, 잉카인터넷, NHN) 등의 전문가들이 참여



이용자 10대 안전수칙	이동통신사 주요 역할	스마트폰 제조사 역할	백신/보안솔루션사 역할	정부 및 연구기관 역할
① 의심스러운 애플리케이션 다운로드 하지 않기 ② 신뢰할 수 없는 사이트 방문하지 않기 ③ 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기 ④ 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기 ⑤ 블루투스 기능 등 무선 인터페이스는 사용시에만 켜놓기 ⑥ 이상증상이 지속될 경우 악성코드 감염여부 확인하기 ⑦ 다운로드한 파일은 바이러스 유무를 검사한 후 사용하기 ⑧ PC에도 백신을 설치하고 정기적으로 바이러스 검사하기 ⑨ 스마트폰 플랫폼의 구조를 임의로 변경하지 않기 ⑩ 운영체제 및 백신을 항상 최신 버전으로 업데이트 하기	① 모바일 악성코드 대응방안 수립 및 이행 ② 사고접수 및 처리절차 수립 ③ 악성코드 조기경보 서비스 제공 ④ 악성코드 감염 이용자 대상 서비스 이용 제한 기준 마련 ⑤ 중요 S/W 패치 및 업데이트 서비스 지원 ⑥ 안티스팸 서비스 제공 ⑦ 스마트폰 원격제어 서비스 제공 ⑧ 단말기 보안설정 정보 제공 ⑨ 네트워크 및 서버 관리 ⑩ 모바일 악성코드 테스트 망 지원 ⑪ WAP Push 서비스 관리 ⑫ 공조체제 유지	① 단말기 잠금 기능 강화 ② 블루투스 연결 가능 목록 관리 기능 제공 ③ 데이터 암호화 제공 ④ 데이터 및 시스템 접근 제어 ⑤ 데이터 및 시스템 백업 복구 기능 제공 ⑥ 안티스팸 기능 제공 ⑦ 안전성 검사 강화 ⑧ 단말기 보안설정 매뉴얼 제공 ⑨ 악성코드 샘플 확보 협력 ⑩ 신속한 보안패치 및 업데이트 제공 ⑪ 공조체제 유지	① 신속한 악성코드 샘플 확보 ② 모바일 환경을 고려한 백신 개발 ③ 신속한 백신 업데이트 ④ 악성코드 정보 제공 ⑤ 다양한 보안솔루션의 연구 개발 ⑥ 공조체제 유지	① 민 · 관 협의체 구성 및 지원 이용자 보안인식 제고 ② 모바일 위협정보 수집 및 ③ 악성코드 분석 채집기술 개발 ④ 모바일 콘텐츠 안전성 확보 방안 검토 ⑤ 모바일 인터넷 고충 처리 ⑥ 모바일 시큐리티 전문인력 양성 및 교육 강화 ⑦ 모바일 인터넷 환경에서의 보안강화 법제 개선 ⑧ 안전한 이용을 위한 모바일 단말, 인프라, 서비스 보안기술 개발 장려 ⑨ 모바일 서비스 침해예방 및 대응 체계 구축 ⑩ 모바일 보안위협 국제 대응 공조체제 마련

[그림 3] 스마트폰 정보보호 주체별 역할 관계도

은 방통위 및 KISA 주관으로 2007년부터 매년(1회) 실시하고 있는 '유관기관 공동대응 모의훈련'을 스마트폰 정보보호 민·관 합동대응반 참여기관(업체)으로 확대하여 실시한 것으로 스마트폰 정보보호 주체들이 참여하여 실질적인 훈련효과를 거두었다고 볼 수 있다.

방통위는 스마트폰 침해사고에 선제적으로 대응할 수 있도록 향후에도 스마트폰 정보보호 민·관 합동대응반의 지속 운영을 통해 선제적 보안위협 대응체계를 더욱 강화해나갈 계획이다. 또한 스마트폰 정보보호 민·관 합동대응반 및 기타 협의체(모바일시큐리티포럼, 인터넷정보보호협의회, 미래융합IT서비스보안연구회 등)와의 유기적 연계를 통한 스마트폰을 포함한 모바일 전반의 보안성 강화를 위한 제도 보완 및 기술적 대응능력을 강화해 나갈 수 있는 방안을 모색해 나가고 있다.

방통위는 스마트폰 보안위협 대응과 관련하여 ①스마트폰 이용자 보안인식을 제고하고, ②앱 스토어 및 애플리케이션 보안성 검증방안을 마련하며, ③민·관 합동대응반을 통해 스마트폰 침해사고에 효율적으로 대응하는 한편, ④중장기 모바일 시큐리티 종합계획을 마련하여 총체적인 대응이 이루어질 수 있도록 할 예정이다.

방통위는 우선 스마트폰 이용자 보안인식 제고를 위해 민·관 합동대응반을 통해 2011년 상반기에 이용자 스스로 스마트폰 백신을 손쉽게 설치·이용할 수 있도록 하는 보안 가이드를 마련·보급할 계획이다. '스마트폰 백신 설치 이용 가이드'(가칭)를 통해 스마트폰 단말기별 백신 설치 방법, 보안설정 가이드라인 등을 안내함으로써 이용자들의 보안인식이 제고될 수 있도록 할 예정이다.

그리고 스마트폰 앱 스토어 및 애플리케이션의 보안성을 검증할 수 있는 방안을 검토할 계획이다. 현재 국내 이동통신사업자들은 각사가 운영하는 앱 스토어에 대해서는 보안검증체계를 구축하고 있으나, 해외 개방형 애플리케이션 마켓에 대해서는 보안성 검증이 불가능한 것이 현실이다. 개방형 마켓을 통해 누구든지 콘텐츠 제작과 유통, 사용이 가능하며 애플리케이션 검증체계가 미흡하여 악성코드가 삽입된 애플리케이션이 유통될 위험성이 상존하고 있기에, 방통위는 스마트폰 정보보호 민·관 합동대응반을 통해 스마트폰 애플리케이션을 이용자가 안심하고 사용할 수 있도록 보안 검증 기준 및 절차를 마련하여 보안이 강화될 수 있도록 할 계획이다.

또한 스마트폰 민·관 합동대응반 운영을 지속적으로 강화해 나갈 계획이다. 스마트폰 정보보호 민·관 합동대응반을 통해 스마트폰 애플리케이션 악성행위에 대한 판단 기준을 마련하여 배포하고, 상호간 정보공유 등을 통해 스마트폰 전용백신 개발 등에 활용할 수 있도록 할 계획이다. 또한 모바일 악성코드 피해사례 및 대응 노하우 등을 공유하고 민·관 합동대응반이 참여하는 '모바일 악성코드 대응 모의훈련'을 정기적(예: 분기별)으로 추진할 수 있도록 하며, 범 정부 차원의 사이버위기 대응훈련과 연계하여 전반적인 사이버위기 대응훈련이 이루어질 수 있도록 할 예정이다.

마지막으로 '스마트 모바일 시큐리티 종합계획'을 수립하여 추진할 계획이다. 즉, 스마트폰 침해사고에 대한 단기적 대응을 넘어 모바일 전반에 대한 체계적·장기적 대응이 가능하도록 중장기(2011~2015년) 종합계획을 수립함으로써 스마트폰을 포함하여 모바일 전반의 보안 강화를 위한 기술 개발, 법·제도 개선, 단말·네트워크·서비스·콘텐츠 보호, 이용자 대상 홍보·교육 등의 세부과제를 마련하여 추진할 계획이다.

4. 맺음말

스마트폰은 '손안의 PC'로 불리며 사람들의 라이프

스타일과 업무환경, 네트워크 시스템 등에 막대한 영향력을 미치면서 '스마트사이어티(Smartciety)'의 시대를 열고 있다. 최근 급속히 출현하고 있는 스마트 모바일 기술 및 신규 서비스는 우리 사회 전 분야에 걸쳐 대혁신('Mobile Big Bang')의 기회를 제공할 것이다. 산업 · 경제적 측면에서 폐쇄적 산업구조가 개방되어 그동안 뒤쳐져 있던 국내 SW, 콘텐츠, 서비스 부분의 선진화 계기가 제공되고, Web 2.0의 개방, 공유, 참여의 정신과 모바일 기반의 이동성이 결합되어 소비자의 새로운 문화와 행동을 창출하고 국내외 시장에 LBS, 소셜커머셜 등 신규 모바일 비즈니스 모델을 확산시킬 것으로 예상된다. 사회 · 문화적 측면에서는 원격으로 가사활동, 학습, 진료가 가능해지고 소셜네트워크 서비스(SNS)를 통한 광범위한 정보공유를 토대로 새로운 사회적 관계가 형성될 것이다. 특히 종래의 사무실 개념을 탈피하여, 언제 어디서나 편리하고 효율적으로 업무에 종사할 수 있도록 하는 스마트워크(Smart Work)정착을 통해 기업 · 행정 부문의 업무환경 개선 및 업무효율의 극대화가 추구될 것이다.[4] 뿐만 아니라 환경 · 에너지 측면에서 모바일 부문의 친환경 활동과 모바일을 활용한 에너지 수요공급 관리, 환경 감시 등 그린 ICT서비스의 활성화로 「저탄소 녹색성장」비전 달성에 기여할 수 있다.

그러나 모든 IT 단말이 그러하듯 스마트폰, 스마트패드 등의 스마트 기기 또한 다양한 역기능을 수반하고 있다. 복합 단말이기에 조작이 어려우며, 타인과의 소통도 스마트폰으로 해결하면서 전통적인 소통수단인 대화의 단절 현상도 나타나게 된다. 날씨 및 버스 도착정보, 길찾기 등 다양한 애플리케이션이 설치되어 있어 스마트폰이 없으면 초조함이나 불안감을 보이는 경우도 있으며, 작은 화면을 장시간 들여다보게 되면서 나타나는 시력저하 등 건강에도 악영향을 미칠 수 있는 것이다.

무엇보다도 스마트폰의 보안위협은 가장 심각한 역기능이라고 볼 수 있다. 앞으로 복잡하게 확장될 무선 인터넷 환경에서는 인터넷 침해공격, 바이러스 · 웜 감염, 정보유출 등 유선에서의 보안 위협이 재현될 수 있고 새로운 서비스 도입에 따른 신규 위협이 확산될 수 있다. 단말기기에 다양한 통신기능이 탑재됨에 따라 침해경로가 다변화되고 IPTV, 클라우드 컴퓨팅 등 유선망의 신규서비스가 무선 환경으로 확대됨에 따라 안전성을 위협하는 요인도 모바일 환경으로 함께 전이될 수 있으며 모바일 기기 분실 · 도난 시에 기본적 보안조치(패스워드 설정 등) 미비로 개인정보 노출, 사기 범죄에의 악용 등의 피해가 우려된다. 또한 이통사에서 SW안정성을 보장하는 폐쇄형 관리와 달리 사용자가 직접 개발하는 앱 SW의 안전성 보장이 미흡할 수 있다. 스마트폰 보안위협과 관련하여 다양한 악성코드의 종류와 감염경로, 피해유형 등이 조사되고 있어 철저한 예방과 발생 시의 신속한 대응이 매우 중요하다.

방송통신위원회는 급변하는 모바일 인터넷 환경에서 신규 보안위협에 사전 대비하고 전 국민이 안심하고 모바일 서비스를 이용할 수 있는 환경을 조성하기 위해 스마트폰 보안위협에 체계적으로 대응해 나가고 있으며, 향후에도 이통사, 단말제조사, 백신 및 보안업체, 앱개발업체, 이용자 등의 주체들과의 협력강화 및 보안인식 제고를 통해 지속적으로 대응능력을 강화해 나갈 것이다. TTA

4) 스마트워크 근무율을 2015년까지 전체 공무원과 노동인력의 30%까지 높이는 방안이 범정부차원에서 추진 중(스마트워크 활성화 전략, 2010.7월)