[정보보호] 당신은 스마트 시대의 스마트인입니까?

요즘 서점에 가면 다양한 분야의 다양한 베스트셀러들이 우리 눈을 사로잡곤 한다. 많이 찾을 수 있는 단어들이 융합이니 행복이니 성공과 같은 단어들이다. 그러나 어느 때부터인가 항상 베스트셀러의 한 켠을 차지하고 있는 단어에 스마트라는 용어를 찾아볼 수 있게 되었다. 여기서 지칭하는 스마트는 '사람이 스마트하다'에서부터, 스마트폰 등 스마트 기기를 이용하는 교육까지, 우리가 생활을 편리하게 영위할 수 있도록 하는 현재의 모든 분야를 망라한다. 컴퓨터 정보화 시대를 넘어 스마트 세상으로 가는 길목에 서 있는 우리는 그 누리는 혜택 못지않게 스마트 기기가 끼칠 수 있는 역기능에는 주목하지 못하는 것 같다. 최근 들어 몇 년 새에 네트워크를 통한 해킹 소식이 심심치 않게 들려오며 최근에는 개인 정보가 새어나가 온 나라가 큰 홍역을 앓고 있는 실정이다. 그럼에도 일반 사용자들은 설마 나에게도 식의 감정을 가지고 적절하게 스마트한 기기를 사용하지 못하는 경향이 잇는 것 같아 정보보호를 전공하는 사람으로 안타까울 때가 종종 있다.

이러한 걱정과 근심으로 시작된 작업 중의 하나가 아태지역 표준화기구인 ASTAP forum 정보보호 전문가 그룹에서의 정보보호 핸드북 작성 작업이다. 이미 2012년 8월에 개최된 제20차 ASTAP forum 회의에서 정보보호 전문가 그룹(EG IS)은 정보보호 관련 유용한 정보를 제공할 수 있는 정보보호 핸드북(Security handbook)을 작성하기로 동의하였다. 그 후속 작업으로 한국 주도로 2013년 3월의 제21차 ASTAP forum 회의와 2013년 9월에 열린 제22차 ASTAP forum에서 스마트폰 보안 고려사항, 안전한 전자금융거래를 하기 위해 사용자가 주의해야 할 사항 등이 제안되었고, 향후 이를 기반으로 전자금융 거래를 안전하게 하기 위한 사용자 측면의 주의 사항들을 추가 수정하기로 결정하였다. 이와 더불어 최근 개최된 제23차 ASTAP forum(개최 장소: 태국 파타야, 기간: 2014.3.3 ~ 2014.3.7)에서는 정보보호 핸드북 작성을 위해 한국 측에서 다음과 같은 내용을 추가 제안하였다. 이를 자세한 내용을 생략하고 소개하면 다음과 같다.

1) 안전성이 높은 패스워드 선택 및 이용방법

- 패스워드는 영문자(대문자, 소문자), 숫자, 특수문자들을 혼합한 구성의 문자열로 설정한다. 이때 가급적 8자리 이상으로 한다.
- 다음과 같은 패스워드는 사용하지 말아야 한다.
  - 7자리 이하인 문자열
  - 특정 패턴을 갖는 패스워드
  - 제3자가 쉽게 알 수 있는 개인정보를 바탕으로 구성된 문자열
  - 사용자 ID (로그인 계정)를 이용한 패스워드
  - 사전의 단어로 구성된 패스워드
  - 특정 인물의 이름이나 널리 알려진 단어를 포함하는 패스워드
  - 시스템에서 초기에 설정되어 있거나 예제로 제시되고 있는 패스워드

• 안전한 패스워드 이용방법
  - 사용자는 위의 항목을 참조하여 안전한 패스워드를 설정한다.
  - 초기 패스워드가 시스템에 의해 할당되는 경우, 사용자는 빠른 시간 내에 해당 패스워드를 새로운 패스워드로 변경하여야 한다.
  - 사용자는 패스워드를 주기적으로 변경하여야 한다.
  - 패스워드 변경 시, 이전에 사용하지 않은 새로운 패스워드를 사용하여야 하며, 변경된 패스워드는 이전 패스워드와 연관성이 없어야 한다.
  - 제3자에게 노출되지 않도록 하여야 한다.
  - 제3자에게 노출된 경우에는 즉시 변경하여야 한다.

2) 최소한의 PC 보안 취약점 점검 항목

일반적인 개인용 PC나 노트북을 대상으로 하여 악성코드 공격이나 해커의 침입으로부터 방어를 하기 위한 최소한의 취약점 점검 항목은 아래와 같다. 이러한 항목들에 대해서는 수시로 점검하여야 할 것이다.

• 바이러스 백신 설치 및 실행 여부 점검
• 바이러스 백신의 최신 보안 패치 점검
• 운영체제의 최신 보안 패치 설치 여부 점검
• 로그인 패스워드 안전성 점검
• 로그인 패스워드의 변경 주기 점검
• 화면 보호기 설정 여부 점검
• 사용자 공유폴더 설정 여부 점검
• USB 자동 실행 허용 여부 점검

3) 공중 무선랜을 안전하게 사용하기 위한 주의사항

무선랜은 선 연결 없이 자유롭게 접속할 수 있으므로 악의적인 목적을 가진 사용자가 접속하여 개인정보 유출 등 다양한 보안 위협을 발생시킬 수 있다. 따라서, 사용자 관점에서 안전하게 공중 무선랜을 이용하기 위한 주의사항은 아래와 같다. 이러한 사용자 관점의 주의사항 이외에도 공중 무선랜을 구축하고 운영하는 측면에서는 별도의 더욱더 다양한 주의사항들이 존재한다.

• 제공자가 불분명한 공중 무선랜 사용에 주의한다. (사용하지 않기)
• 보안 설정이 없는 무선랜으로 민감한 서비스를 이용하지 않아야 한다.
• 무선랜 자동접속 기능 사용에 주의한다. (사용하지 않기)

또한 정보보호 핸드북의 본문 작성용 템플릿을 제안하여 추후 완성될 정보보호 핸드북의 형식을 확정하였으며 이번에 제안된 형식으로 정보보호 핸드북을 2015년까지 완성할 예정이다. ASTAP forum의 정보보호 전문가 그룹에서 작성 중인 정보보호 핸드북은 일반 말단 사용자들을 위해

작성되고 있으며 정보보호의 주제별로 작성된 것을 모아 사용자 가이드라인 형식으로 제공될 예정이다(2015년 완료 예정). 정보보호 전문가 그룹은 핸드북에 대한 작업을 2015년 완료를 목표로 전문가들의 참여와 의견 반영을 통해 만들어가고 있다. 정보보호 핸드북 작성은 지난 4-5년간 아태 지역 정보보호 전문가들의 관심사였으며 이에 대한 준비 작업으로 아시아태평양전기통신협의체(APT) 회원국들 전문가들의 설문 조사를 통해 이러한 문서의 필요성을 인식하고 ASTAP forum에서 이에 대한 준비 작업을 시작하였다.

이러한 문서 작업을 통해 ASTAP forum의 정보보호 전문가 그룹에서는 한국과 일본과 같은 통신과 정보보호 선진국뿐만 아니라 아태 지역의 낙후된 회원국들의 말단 사용자들도 안전한 통신 환경에서의 사용을 보장받을 수 있도록 할 예정이며 이러한 작업은 개인의 정보보호나 실제 통신 기기나 스마트 기기의 사용에서 발생할 수 있는 여러 가지 문제점을 예방할 수 있다는 차원에서 우리나라에도 절실히 보급하고 교육하여 모든 사용자가 안전하고 편리하게 사용할 수 있도록 되기를 희망한다.

류희수 (경인교육대학교 수학교육과 교수, hsryu@ginue.ac.kr)