Barun ICT 8 August KOR newsletter

바른ICT연구소는 ICT 관련 사회 현상 연구 및 대안을 모색하고 바람직한 사회적 가치 만들기에 기여할 수 있는 정책 방향을 제시합니다. 빠른 IT의 가치보다는 바른 IT 연구, 정책, 교육을 통하여 건전한 사회와 IT 문화 구축에 기여하는 것을 목표로 2020년 세계가 인정하는 융합 ICT 연구소를 준비하고 있습니다.

EVENTS

바른ICT연구소 International Student Ambassador 1기 출범

바른ICT연구소는 'International Student Ambassador' 1기를 출범했다. International Student Ambassador 1기는 미국, 아르헨티나, 베트남 등 다양한 국가의 연세대학교 학생들로 이루어져 각 국의 ICT 이슈를 공유하고 바른ICT연구소와 관련한 다양한 홍보활동을 하게 된다.

바른ICT연구소 김범수 소장은 "이번 International Student Ambassador 1기를 시작으로 ICT에 관심 있는 세계 각국의 학생들과 각 국가별 IT 과몰입, 프라이버시, 정보가치 등의 현황을 조사하고, 바른ICT연구소 연구원들과 바른ICT를 위한 방안을 함께 모색함으로써 각 국가에 적합한 바른ICT 추진 모델과 전략방향을 제시할 것이다. 이러한 국제활동을 통해 바른ICT연구소가 올바른 ICT 세상을 만들어 가기 위한 선도적인 역할을 하게 될 것을 기대한다"고 말했다.

한-EU 개인정보보호 세미나 개최

7월 18일(월) 여의도 전경련회관에서 **한-EU 개인정보보호 세미나**가 열렸다. 이날 세미나는 행정자치부와 방송통신위원회, 개인정보보호위원회가 공동 주최하고 한국인터넷진흥원이 주관하여 개인정보보호제도의 세계적인 기준을 공유하고 한국의 법제에 대한 관심과 이해를 높이기 위한 프로그램이 진행되었다.

특히, 이번 행사에서는 올해 EU 적정성 평가를 앞두고 EU집행위원회와 EU개인정보보호 감독기구 관계자, 아태지역 개인정보 관련 전문가가 다수 참석하여 국내 개인정보보호제도 및 정책 등을 국제적 시각에서 점검해보는 기회가 마련되었다. 국내에서는 개인정보 분야의 전문 변호사와 삼성전자, LG전자와 같은 산업계에서 참석하여 국제사회에 한국만의 제도적 특징을 알리고 발전방향에 대한 의견을 교류하였다.

EU에서 2018년 5월부터 시행할 단일화된 개인정보보호법인 '일반정보보호규정(General Data Protection Regulation, 이하 GDPR)'과 최근 EU와 미국 정부의 개인정보보호 협약인 '프라이버시 쉴드(Privacy Shield)'를 채택한 것에 대해 글로벌 개인정보보호 트렌드를 살펴보는 시간을 가졌다. 이러한 국제사회의 움직임에 따라 한국의 개인정보보호법과 이들 협약 간 충돌 가능성을 검토하고, 보완 장치에 대해 토론했다.

오후 세션의 「한국 개인정보보호법 체계」에서는 한국 개인정보보호의 헌법적 연원과 개인정보보호 기본원칙을, 「개인정보보호 관련 법집행 현황」에서는 사례와 판례를 중심으로 빅데이터, 비식별화, 사물인터넷 등 새로운 이슈에 대한 개인정보보호법 활용 방안을 제시했다.

이어진 「국내 기업의 개인정보보호 실태」에서는 **바른ICT연구소 김범수 소장**이 좌장을 맡아 삼성전자와 LG전자의 개인정보 보호현황과 글로벌 기업으로서의 대응 방안을 소개하는 발표에 이어 토론을 진행했다.

본 세션에서는 개인정보보호를 위한 조직 운영과 기술적 보호조치, 그리고 해외 근로자 및 글로벌 시장을 타겟으로 각국의 개인정보관련 법령을 준수하기 위한 기업의 대응과 예방활동 등이 소개되었다.

한편, 김범수 바른ICT연구소 소장은 2015년 12월, OECD SPDE(정보보호 작업반)의 부의장으로 선출되어 개인정보보호, 사이버 보안 등 온라인 정보보호에 관련된 정책 검토, 가이드라인 제정, 국제규범을 마련함에 있어 우리나라가 국제사회에서 정보보호 분야의 주도성을 가질 수 있도록 힘쓰고 있다.

GLOBAL BARUN ICT ISSUES

#1. 한국 정부와 르완다 정부의 ICT 협력 MOU 체결

Xandra Wihogora (연세대학교 정보산업공학과)

르완다의 정보통신기술(ICT) 발전을 위한 노력으로 이제 도시 곳곳에서 IT 인프라를 볼 수 있게 되었고 이후 지속적인 발전을 위해 르완다는 ICT 발전 국가 중 하나인 한국과 손을 잡기로 하였다.

2016년 6월 2일, 르완다 청소년정보통신부는 한국정부를 통해 한국정보화진흥원(NIA)과 아시아 ICT 협력 MOU를 체결했다. NIA는 르완다의 ICT 정책 시행기관인 르완다정보화진흥원(RISA)과 기술혁신허브, ICT 교육 및 훈련을 강화하기 위한 봉사프로그램인 World Friends IT Volunteers Program 활동을 지원하고 ICT 발전을 위한 정책 및 법규의 노하우도 공유할 예정이다.

또한, 2016년 6월 10일에 르완다 보건부와 한국은 건강분야의 기술 향상을 위한 노력의 일환으로 MOU를 체결했다. 이 MOU를 통해 르완다는 한국의 의료기술, 병원정보시스템(HIS), ICT 기반 의료 서비스 분야에서의 협력이 강화될 것으로 기대된다. 더불어 이 협정은 디지털 헬스케어에 관하여 KT, 연세대학교 의료원 그리고 키갈리 대학교육병원의 협력을 가능하게 할 것이다.

이와 같은 르완다와 한국간의 MOU를 통해 국가간 디지털 격차를 해소할 수 있기를 기대한다.

#2. 디트로이트의 실업자, 디지털 격차에 갇히다

Laurel Maelynn Alley (연세대학교 국제학대학원)

시골에서 인터넷 접속이 잘 안 되는 것은 일상적인 일이다. 하지만 도시에서 인터넷 접속이 잘 안 된다면 어떤 일이 벌어질까? 뉴욕타임즈 2016년 5월 22일자에 실린 “Unemployed Detroit Residents are Trapped by a Digital Divide”라는 기사는 미국의 미시건 주 디트로이트의 대표적인 사례를 통해 도시에서의 디지털 격차가 어떤 결과를 불러오는지에 대한 사회적 관심을 불러일으켰다.

디지털 격차는 인터넷 접속이 가능한 지역과 제한되거나 불가능한 지역 간의 분리로 인해 발생한다. 2015년, 미국의 연방통신위원회(FCC)는 초고속 인터넷을 공익사업으로 선언했지만 여전히 전체 디트로이트 거주민의 10명 중 4명이 인터넷 접속에 어려움을 겪고 있다. 충분하지 못한 인터넷 환경은 사람들이 구직활동, 보험 신청, 대출 같은 중요한 일이나 심지어 아주 간단한 학교 숙제를 하는데도 어려움을 겪도록 한다. 이렇게 제한된 환경에서, 가난한 지역의 거주자들은 기본적인 디지털 리터러시와 대안적인 교육 자원들을 얻기 위해 고군분투하고 있다.

하지만 디지털 격차 이슈는 인터넷 접속에만 국한되지 않는다. 사람들은 인터넷을 사용하기 위해 컴퓨터나 그외 디지털 디바이스, 그리고 이러한 장치들을 완전히 활용할 수 있는 지식을 필요로 한다. 기술에 관한 충분한 경험 없이는 기술적인 능력을 요구하는 일자리를 가질 수 없으며 이는 결국 디지털 격차라는 극복할 수 없는 장벽을 만듦으로써 경제적 불평등 이슈를 악화시킬 것이다. 돌이킬 수 없는 상황을 만들기 전에 이러한 장벽이 생성되는 것을 예방할 수 있도록 노력해야 할 것이다.

#3. 인터넷으로 인해 우리의 몸과 마음엔 어떤 일이 일어날까?

Julieta Salvo (연세대학교 국제학대학원)

인터넷과 디지털 기기들은 적절히 사용할 때 우리의 삶을 편리하고 윤택하게 하지만 과이용할 경우 신체적 정신적으로 부정적인 효과를 가져올 수 있다.

Mexican Internet Association에 의하면 2007년부터 오늘날까지 인터넷 사용시간은 한 주에 평균 2시간에서 하루에 6시간 사용으로 급격히 늘어났다. 웹 보안기술, 웹 필터링, 콘텐츠 운영 전문 멕시코 회사인 SAINT는 이러한 현실에서 발생할 수 있는 사이버 폭력이나 사이버 범죄를 예방하기 위한 교육의 필요성을 제고하기 위해 “Por un Internet seguro (for a safe Internet)” 캠페인을 시작했다.

이 캠페인은 인터넷(일반적으로 컴퓨터)의 과이용으로 인해 직접적으로 야기될 수 있는 신체적, 정신적 상태에 대해 알리고 이를 경고하고 있다.

특히 기억상실, 대인 상호작용의 어려움, 인터넷 중독, 우울, 기술 장치에 의존 등은 정보통신기술발전으로 야기된 심각한 정신적 결과이다. 비록 심리적인 효과는 그 증거가 명확하지 않아 진단 내리기가 어렵다 할지라도, 신체적인 문제와 마찬가지로 중요하게 다루어야 할 필요가 있다.

비만
인터넷 이전에는 볼 수 없었던 만큼 앉아 있는 생활을 촉진시켜 비만을 유발한다.

수면장애
컴퓨터, 스마트폰, 그리고 그 외 휴대용 디바이스 스크린에 의해 나오는 빛이 우리의 몸이 완전히 수면 상태로 들어가는 것을 방해한다.

컴퓨터화면증후군, 손목터널증후군
이 두 가지 상태 모두 일반적으로 하루의 거의 모든 시간을 컴퓨터 앞에서 살아가는 직업군에서 나타난다.

#4. 싱가포르 사이버보안침해 - 해커집단 ANONYMOUS

Ho Jia Ren Jan (연세대학교 전기전자공학부)

최근 싱가포르에 위치한 아시아 최대규모의 재무관리 센터가 지속적인 사이버 공격에 노출되어 일반 시민의 개인정보가 유출되는 사고가 일어났다. 사고에서 유출된 정보는 이름, 주소, 신분증 번호뿐 아니라 민감 정보까지 포함되었다.

싱가포르에서는 2016년 상반기 동안 몇몇의 큰 보안 침해 사건들이 발생했다. 2016년 초반에는 스탠다드차타드 은행의 부유층 고객 데이터가 대중에게 유출되었으며 2016년 4월에는, 싱가포르 최대 노래방 체인이 사이버 공격을 당해 30만 명 이상의 고객 개인정보가 온라인 상으로 유출되었다.

싱가포르의 개인정보보호위원회(Personal Data Protection Commission; PDPC)는 개인정보유출 사고의 주요 원인을 사이버 보안 절차 미흡에 기인한 것으로 보고 있으며, 해커집단은 이러한 특성을 가진 조직을 쉽게 타깃으로 삼는다고 하였다. 실제로 위에 언급된 사례를 보면, 한 조직의 데이터베이스에 접속하기 위한 비밀번호가 관리자 ID인 “admin”과 동일했다.

그리고 2016년 6월, 싱가포르는 역사상 가장 큰 규모로 알려진 보안 침해를 겪었다. 모든 싱가포르 거주자들이 세금신고, 연금저축, 그 외 금전적인 서비스를 거래하고 있는 싱가포르 정부의 e-서비스 플랫폼인 **‘싱패스(Singpass)’**가 사이버 공격의 대상이 된 것이다.

싱패스에는 기밀 정보를 포함한 340건 이상의 개인거래정보가 들어있었다. 이 사건으로 천 개가 넘는 계정이 자동접속되었으며 일부 계정의 비밀번호가 불법적으로 변경되거나 계정이 조작된 것으로 추정되고 있다.

이러한 싱가포르 사이버 공격의 배후로는 “Anonymous”라고 불리는 해커조직이 지목되었다. 2013년, 이 그룹의 일원이 싱가포르에서 체포된 후, Anonymous는 싱가포르 정부의 모든 정보를 누설할 것이라고 선언했다. 그 이후 싱가포르의 정부 산하기관뿐만 아니라 그 외 다양한 기관들이 지속적으로 사이버 공격을 받고 있다.

포켓몬GO로 인한 안전사고, 예방할 수 있다!

이건택 박사 (연세대학교 바른ICT연구소)

최근 포켓몬GO가 선풍적인 인기를 끌게 되면서 **증강 현실 (Augmented Reality, AR)**이 가진 가능성과 앞으로 일으킬 변화에 대한 관심이 점점 더 높아지고 있다. 증강 현실이란 사용자가 보는 현실세계에 3차원의 가상물체를 겹쳐 보여주는 기술을 말한다.

포켓몬GO의 성공에 힘입어 향후 유사한 형태의 게임을 비롯한 다양한 증강 현실 어플리케이션들이 계속 등장할 것으로 보이며 이에 따라 증강 현실 어플리케이션 사용자 수도 급증할 것으로 예상된다.

그러나 아직까지 증강 현실 환경에서의 사용자 안전에 대한 고려가 미흡한 실정으로 이미 포켓고GO 게이머들이 지나치게 게임에 몰입하여 사고로 인한 부상을 입는 등 안전 사고가 발생하고 있다.

앞으로 증강 현실 어플리케이션과 그 사용자 수가 증가할수록 더 다양하고 많은 사고들이 일어날 가능성이 커지기 때문에, 증강 현실 환경에서 사용자의 안전을 제고할 수 있는 방안이 필요하다.

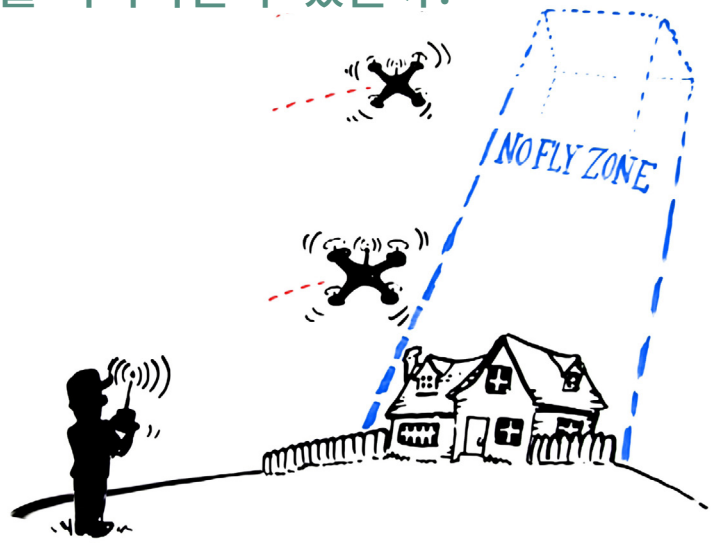
대부분의 안전 사고는 사용자가 증강 현실 어플리케이션에 지나치게 몰입하여 주변 상황에 대한 인지력이 떨어짐으로써 발생한다. 해안 절벽 근처에서 포켓몬GO를 플레이하다 추락하거나 게임 플레이 도중 교차로를 건너다 차에 치이는 사고가 이런 현상을 잘 보여주는 예이다. 사용자가 증강 현실 어플리케이션에 몰입하고 있을 때 사용자의 모든 관심은 스마트폰에 집중되어 있다. 따라서 스마트폰을 통해 주변의 위험 요소를 감지하고 사용자에게 위험에 대한 경고를 전달하는 것이 사용자가 효과적으로 위험을 인지할 수 있도록 하는 방법이 될 것이다. 그렇다면 어떻게 스마트폰을 통해 위험 요소를 감지할 수 있을까?

연세대학교 바른ICT연구소 이건택 박사는 횡단보도, 계단, 공사중인 지역, 접근 금지 지역 등 위험 지역 및 요소에 설치된 Bluetooth beacon의 신호를 스마트폰을 통해 인식하여 사용자에게 경고해주는 앱을 개발하였다. 개발한 앱은 다른 앱이 실행 중일 때에도 백그라운드에서 동작하며 경고음, 진동, 팝업 메시지 등을 통해 사용자에게 주변에 어떤 위험 요소가 있는지 경고해준다. 스마트폰에 집중하고 있는 사용자에게 스마트폰을 통해 직접 경고해주기 때문에 효과적으로 사용자의 주위를 환기시키고 위험을 인지하도록 하여 사고 위험을 줄이고 사용자가 돌발 상황에 잘 대응할 수 있도록 도울 수 있을 것으로 기대된다. 또한 향후 GPS 정보 및 지도 정보와 결합하여 더 정확하고 효과적으로 사용자에게 경고해줄 수 있도록 개발을 진행 중이다.

Bluetooth beacon은 Bluetooth 신호를 주기적으로 발신하는 장치이다. Bluetooth beacon의 신호 반경은 최대 70m에 달하며 이 신호는 스마트폰이 쉽게 인식하여 신호 세기를 통해 대략적인 거리도 파악이 가능하다. 또한 Bluetooth beacon은 작고 가벼워 설치 및 제거가 용이하며 저전력으로 동작하여 최장 2년까지 사용할 수 있다는 장점이 있다.

카테고리에 대한 단서와 배경 이미지가 드론에 대한 프라이버시 염려를 희석시킬 수 있을까?

박용완 박사 (연세대학교 바른ICT연구소)



6월 24일, 연세대학교 경영관에서 개최된 TPM (Theory + Practice in Marketing) Asia 2016 Conference에서 **박용완 박사(연세대학교 바른ICT연구소)**는 무인 항공기인 드론(Drone)의 사생활 침해에 대한 논문을 발표하였다.

드론은 디지털 카메라를 내장하고 있으면서 하늘 높이 떠올라서 촬영이 가능하기 때문에 일반적인 카메라로는 찍을 수 없는 각도와 장소까지도 쉽게 촬영할 수 있다. 그렇기 때문에 사람들은 드론에 의해 자신의 사생활이 쉽게 노출되거나 침해될 가능성에 대해 염려하고 있으며, 사람들이 가지고 있는 드론의 사생활 침해에 대한 염려는 향후 드론 시장 성장의 저해 요소로 작용할 수 있다.

박용완 박사는 사람들이 가지고 있는 드론의 사생활 침해에 대한 염려를 줄이기 위한 방안으로써 광고에서 제품의 특성과 배경 이미지를 활용할 것을 제시하였다. 연구 결과, 드론은 무선조정 장난감 비행기와 디지털 카메라가 합쳐진 융합형 IT 제품으로 볼 수 있기에, 디지털 카메라가 아닌, 무선조정 장난감 비행기의 성격을 광고에서 강조함으로써 소비자의 사생활 침해 염려가 상대적으로 감소함을 확인하였다. 또한 광고의 배경이 자연경관일 때보다 도시일 경우 사생활 침해에 대한 염려가 증가함을 보여줌으로써 드론을 제작, 판매하는 회사들이 홍보 및 광고를 제작할 경우, 소비자들의 사생활 침해 염려를 자극하지 않기 위한 방법을 제시하였으며, 이는 역으로 정책 입안자 및 시민단체들이 향후 드론에 의한 사생활 침해를 경고하는 캠페인을 할 경우에도 활용될 수 있다.

* 2011년 콜롬비아대학 비즈니스 스쿨에서 시작된 TPM Conference는 마케팅 이론들이 실무적 관점에서 다양한 이슈들과 어떻게 연관되는지와 그 시사점에 대한 활발한 토의를 이끌어내기 위해 기획되었으며, 이후 하버드 비즈니스 스쿨, 런던 비즈니스 스쿨, 켈로그 비즈니스 스쿨 등에서 매년 개최되었다. 그리고 2016년에 이르러 처음으로 아시아 컨퍼런스를 한국마케팅학회와 연세대학교 경영대학이 주관하여 개최하게 되었다. TPM conference는 학계의 연구자들뿐만 아니라 실제 업계의 전문가들이 연사 및 토론자로서 참여함으로써 여타 학술대회와는 확연히 구별되는 차별성을 가지고 있다.

이번 TPM Asia Conference는 “창의적 콘텐츠, 정보통신기술, 그리고 마케팅”이라는 주제로 진행되었으며, 학술 논문 발표는 총 16개의 세션으로 구성되어 창의성, 문화 콘텐츠, 온라인 마케팅, 브랜드, 소비자행동, 마케팅 전략 등의 다양한 주제를 중심으로 진행되었다.

SPECIAL SERIES: The Digital Divide in Smart Technology

노년층 스마트 교육 현장 속으로 - 첫 번째 이야기

김수정 인턴 (연세대학교 바른ICT연구소)

Introduction

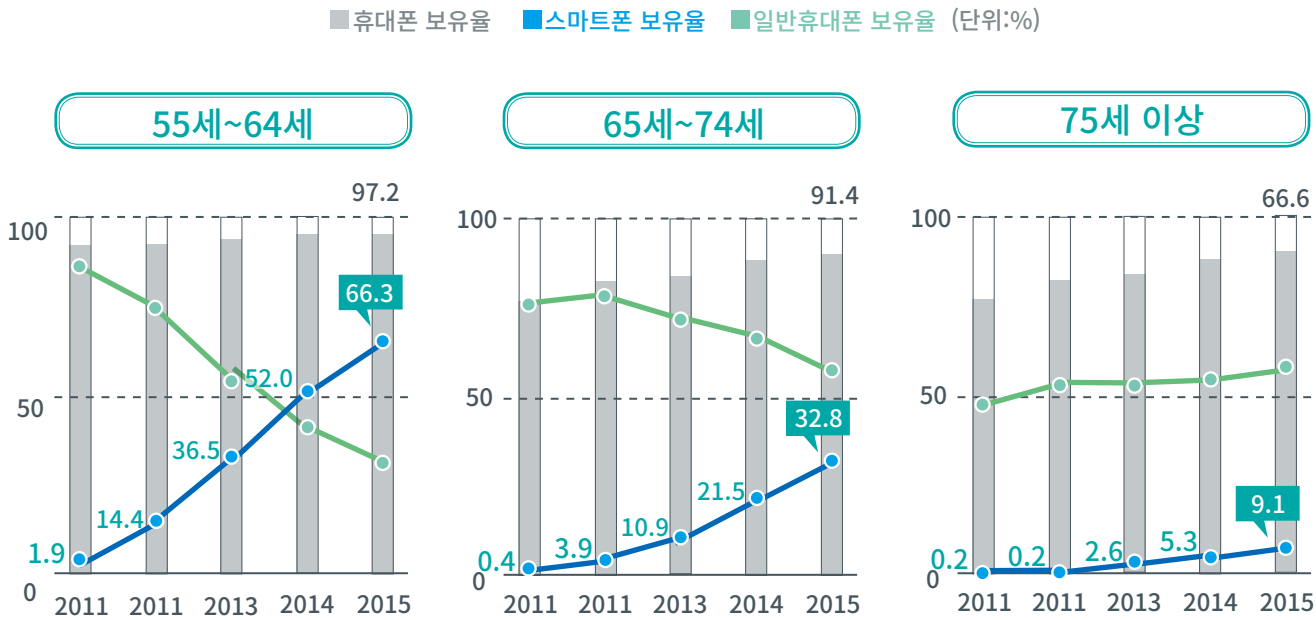
본 기획 연재는 연세대학교 바른ICT연구소 김수정 인턴이 서울특별시 내 두 곳의 복지관에서 노년층을 대상으로 하는 스마트폰 활용 교육 자원 봉사에 참여한 내용을 바탕으로 한다.

김수정 인턴은 봉사활동을 통하여 노년층에게 있어 스마트 세상의 진입 장벽은 무엇인지, 어떻게 넘어야 할지에 대한 인사이트를 얻고자 하였으며, 이를 통해 본 섹션에서는 노년층의 스마트 정보격차 해소를 위한 교육의 현황과 어려움을 살펴보고 해결 방안을 모색하여 향후 연구 과제를 제안하고자 한다.

스마트 정보격차 왜 중요한가?

한창 좋을 커플도 카페에 나란히 앉아 스마트폰만 바라보는 시대가 되었다. 그리고 이러한 모습은 비단 젊은이들에게만 해당 되는 것은 아니다. 최근 정보통신정책연구원(KISDI)이 발간한 '은퇴 연령 계층의 미디어 이용' 보고서에 따르면 중장년 이상 연령층의 휴대폰 사용은 매년 크게 늘고 있다.

휴대폰 사용자 가운데 50대 이상 스마트폰 이용자 비율은 2011년 3.6%에서 작년에는 50.35%로 이미 절반을 넘어섰다. 그러나 50대 이상의 스마트폰 이용자 비율이 절반을 넘어섰다고 해서, 이들 모두가 스마트폰을 능숙하게 사용하는 것은 아니다. 여전히 상당수 노년층은 스마트폰을 가지고 있어도 사용법을 모르거나, 배울 곳이 없어 사용에 어려움을 겪고 있어 젊은층과 노년층 사이의 스마트 정보격차가 발생하고 있다.



고령자 핸드폰 및 스마트폰 보유현황 (정보통신정책연구원, 2015)

스마트 정보격차 문제가 가지는 중요성을 크게 세 가지로 생각해 보았다.

1 사회 통합

첫째, 사회 통합에 있어서 스마트 정보격차가 가지는 중요성이다. 각종 스마트 기기 및 서비스가 우리 생활에서 차지하는 부분은 지속적으로 늘어날 것이다. 따라서 노년층이 정보기술로부터 소외되지 않아야만 보다 독립적인 생활과, 젊은세대와의 온전한 소통을 가능하게 하여 사회통합에 한 걸음 더 나아갈 수 있을 것이다.

2 비즈니스 측면

둘째, 스마트 정보격차는 **비즈니스 측면에서도 중요성**을 지닌다. 앞서 언급한 바와 같은 스마트 정보격차 해소의 필요성은 필연적으로 새로운 시장을 창출할 것이다. 스마트폰 활용 교육 현장에서도 볼 수 있었듯 현재 스마트 정보격차 해소를 위한 정책은 물론이고 기기나 서비스 또한 충분하지 않다. 고령화 추세는 지속될 것이고 현행대로라면 스마트 정보격차를 겪는 세대는 축적될 것이다. 즉, 이러한 사용자 층이 스마트 세상에 쉽게 적응할 수 있도록 새로운 기기나 서비스를 제공하는 시장에 대한 가능성이 존재한다. 이 뿐만 아니라 이를 바탕으로 해당 사용자 층을 향후 더 나은 사용 단계의 다른 시장으로도 유입 시킬 수 있는 여지 또한 존재한다.

3 상품 및 서비스 기획

셋째, 스마트 정보격차를 겪는 사용자 층이 상품 및 서비스 기획 등에 있어 주는 인사이트이다. 이는 향후 다양한 미래 기술의 대중화에 있어 기술을 처음으로 수용하는 소비자가 제품 및 서비스의 효율성과 필요성을 이해할 수 있게끔 디자인하는 데 도움이 될 것이다. 이를 테면 스마트폰 활용 교육에서도 너무 많은 디폴트(기본 값)를 경계해야 한다는 디자인적 사고를 체감할 수 있었다.

예를 들어, 할머니께서 시력이 안 좋으시니 글씨 크기 조정법을 가르쳐드려야겠다고 쉽게 생각 할 수 있을 것이다. 그러나 이러한 추측 역시 너무 많은 사용자 경험으로 단련된 나의 디폴트 위에서 이루어진 것이기에 큰 도움이 되지 못했다. 막상 문제가 되는 것은 글씨 크기를 변경하는 것에 앞서 글씨 크기를 바꿀 수 있는 '설정'까지 찾아가는 것, 그리고 톱니바퀴 표시가 '설정'을 뜻하는 것임을 설명하는 것이었다. 이러한 스마트 정보격차 극복을 위한 노력은 좀더 편리한 사용경험을 제공하는 상품과 서비스를 위한 디자인적 인사이트를 제공할 것이다.

이와 같은 중요성으로 볼 때 스마트 정보격차 해소를 위한 제도 정비 및 각계각층의 노력이 필요할 것으로 생각된다. 이를 위하여 향후 제도적 측면의 보완 및 효과적인 학습 방법에 대한 연구와 관련 제품 및 서비스 개발이 이루어져야 할 것이다.

RESEARCH SEMINAR

6/23

클라우드 컴퓨팅에서 발생할 수 있는 정보보호 주요 이슈

양희동 교수 (이화여자대학교 경영대학)

클라우드 서비스는 IT 자원을 소유하지 않고 일부 또는 전체를 아웃소싱하는 형태이므로 필수적으로 보안 문제가 제기될 수 밖에 없다. 클라우드 보안협회(Cloud Security Alliance: CSA)에서는 클라우드 컴퓨팅에서 발생 가능한 보안 문제와 해결 방안에 대해 제시하고 있다.

1 데이터 유출 (Data Breaches)

클라우드를 업무시스템으로 사용하는 기업에게 가장 두려운 일은 자사의 데이터가 유출되는 것이다. 클라우드는 기존의 서버 기반 환경보다 네트워크 접근성이 확대되어 해커들에게 그만큼 다양한 공격 경로를 제공할 수 있다.

따라서 클라우드 데이터의 저장과 관리에 있어 이러한 가능성이 고려되어야 한다. 데이터 유출 예방을 위한 방법으로는 암호화, 키 관리, 인증과 접근제어 등이 있다.

2 데이터 소실 (Data Loss)

클라우드 서비스는 여러 채널과 경로를 통해 여러 사람이 동시에 접속할 수 있어 사용자에게 편리함을 제공하지만 누군가 삭제를 하거나 수정해버린 데이터는 다시 되돌릴 수 없다.

데이터의 삭제나 수정은 갱신으로 이해할 수도 있지만 기존 데이터의 소실이기도 하다. 데이터 소실을 예방하기 위해서는 이전 데이터를 백업해 두는 수 밖에 없다.

3 계정 또는 서비스 탈취 (Account or Service Hijacking)

클라우드 서비스는 계정 정보에 기반하여 사용자를 인식하여 정보를 제공한다. 만약 사용자의 계정 정보가 탈취된다면 기업의 기밀 정보를 엿볼 수 있고, 관리자로서 다른 계정을 삭제하거나 기업의 클라우드 서비스 계약 정보를 변경할 수도 있다.

이를 예방하기 위해 Two-factor 인증 등으로 인증을 강화하거나 사용자의 활동을 모니터링하여 대처할 수 있다.

4
안전하지 않은 APIs (Insecure APIs)

클라우드 서비스는 서비스 운영 및 관리를 위해 다양한 API를 제공하고 있다. 하지만 이러한 API의 취약점을 통해 사용자의 인증을 우회하거나 접근이 제한된 데이터에 접근하는 등의 보안 사고가 발생할 수 있다.

이는 클라우드 웹방화벽(Web Application Firewall) 설치를 통해 예방할 수 있다.

5
서비스 거부 (Denial of Servic : DoS)

클라우드 환경에서도 서버의 자원을 소진하여 서비스를 불가능하게 만드는 서비스 거부(DoS) 공격이 가능하다. 서비스 거부 공격은 클라우드 서비스를 이용하는 기업의 업무가 원활하게 이루어지는 것을 방해할 것이다.

DoS 공격은 백신 프로그램의 업데이트와 보안 패치 설치, 방화벽 및 침입탐지시스템(IDS) 등 네트워크 보안 시스템을 설치하여 예방할 수 있다.

6
악의적인 내부 사용자 (Malicious Insiders)

기업의 클라우드 서비스 사용에 있어 퇴사한 직원의 계정이 즉시 삭제되지 않았거나, 직무의 조정으로 접근 불가능한 권한이 아직 유효한 경우 이를 악용할 수 있다.

이러한 악의적인 내부 사용을 막기 위해서는 사용자의 계정과 권한에 대해서 지속적인 관리와 감사가 이루어져야 한다.

7
클라우드 서비스의 남용 (Abuse of Cloud Services)

해커들은 클라우드의 거대한 전산자원을 활용하여 암호를 해독하거나 사용자의 패스워드를 획득하기도 한다. 또한 해커들은 클라우드 환경에서 여러 개의 가상머신이 동시에 동작하도록 하는 가상화 기술을 이용하여 다른 가상머신을 공격하는 기법을 연구하기도 한다.

이를 막기 위해서는 기술적인 방법보다는 클라우드 이용자에 대한 지속적인 모니터링과 운영 정책의 적용이 이루어져야 한다.

8
클라우드 서비스 이해 부족 (Insufficient Due Diligence)

기존의 업무 시스템을 가상화하여 가상머신으로 동작하게 되면 하드웨어나 네트워크의 직접적인 제어가 불가능해진다. 이러한 클라우드 환경에 대한 이해가 부족하다면 가상화 후의 시스템에 치명적인 취약점을 야기시킬 수 있다.

따라서 업무시스템이 클라우드의 가상화 환경에서 안전성을 충분히 확보할 수 있는지 여부를 사전에 충분하게 검토해야 한다.

9
공유기술의 취약점 (Shared Technology Vulnerabilities)

클라우드 기술 내부에는 상당히 많은 요소기술이 있다. 예를 들어, 하드웨어 측면만 해도 CPU, 메모리, 저장장치 등의 많은 요소들이 대량으로 서로 연결되어 있다. 따라서 내부의 요소기술이나 하드웨어에서 발견되는 취약점이 클라우드 전체의 취약점으로 연결될 수 있다.

이는 각 가상 머신마다 방화벽, 통합위협관리(UTM) 등 보안 장비를 설치하여 예방할 수 있다.

금융 IT 보안 컴플라이언스와 정보보호 통합관리 체계의 필요성

유영록 부문대표 ((주)씨에이에스)

6/30

금융 분야에 있어 각종 개인정보 유출사고, 특히 인가자에 의한 사고가 급증하고 있다. 이는 기업 구성원들의 정보자산과 자산의 프로세스에 대한 파악 미흡, 낮은 보안 인식 등으로 인한 것이다. 보안 사고의 증가로 관련 법·규제와 경영진의 책임이 강화되고 있으며, 보안 사고는 기업의 신뢰도와 평판에 직접적인 영향을 주어 큰 손실을 발생시키고 있다.

따라서 CISO와 보안담당자들은 보안위협에 선제적으로 대응하고 법·규제 준거성을 확보하기 위하여 정보보호 거버넌스를 강화해야 하는 문제에 직면하였다. 보안담당자들이 통제 결과를 검증하고 업무효율성을 향상시키며 임직원들과의 의사소통을 원활히 하기 위해서는 정보보호 통합관리 체계의 필요성이 대두된다.

정보보호 통합관리를 위해서는 다음과 같은 업무 요소들이 반드시 포함되어야 한다.

정보보호 거버넌스

지시, 평가, 모니터링의 거버넌스 활동을 보안 관점에서 놓고, 리스크와 컴플라이언스의 규정, 표준, 절차, 가이드를 보안활동에 결합하여 총괄적으로 관리하는 업무

리스크 관리

IT운영자산에 기반한 취약점 및 위협을 도출하고, 측정지표(영향도, 발생가능성)를 통해 리스크를 평가하고 대책수립 및 사후관리 지원

보안 컴플라이언스 관리

법령, 표준 및 지침 등 보안 관련한 요구사항들을 기반으로 정보보호 컴플라이언스 통합관리체계 및 통합점검체계를 제공함으로써 효율적이고 효과적인 통제점검 지원

보안 활동 관리

정보보호 통합관리 체계를 운영하기 위한 주요 활동들을 체계적으로 시스템화하여 정보보호 서비스를 지원

보안 상시 모니터링

보안통제위반 및 고객정보유출 이상징후 관점에서 핵심위험지표(KRI)를 도출하여 모니터링하고 소명절차를 수집하고 사후관리를 지원

바른ICT뉴스레터를 정기적으로 받아보고 싶으신 분은 barunict@barunict.kr 로 이메일 주시기 바랍니다.

* 본 연구소에서 제공되는 바른ICT뉴스레터는 국내외 우수 ICT 연구 동향 및 연구 결과를 정리하여 제공합니다.

연세대학교 YONSEI UNIVERSITY
바른 ICT연구소 Barun ICT Research Center

Publisher 김범수 | Editor 손수민 | Design 손민정

서울시 서대문구 연세로 50 연세대학교 302동 (연세·삼성학술정보관) 720호
Phone: +82-2-2123-6694 www.barunict.kr