

# Barun ICT **1.2** 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.

## BARUN ICT EVENTS

### SW Welcomes Girls! 2016 2016.12.21 | 미래창조과학부

2016년 12월 17일에서 18일, 이틀에 걸쳐 미래창조과학부 주최, 한국정보화진흥원이 주관하고 바른ICT연구소가 후원하는 'SW Welcomes Girls! 2016'이 연세대학교 새천년관에서 성황리에 개최되었다. 이번 행사는 '엄마와 딸이 함께하는 SW 체험'과 '토크콘서트', '해커톤' 등의 참가자 특성에 따라 맞춤형된 프로그램으로 구성되었다.

바른ICT연구소의 임지선 박사 모녀를 비롯하여 130 가족이 참여한 '엄마와 딸이 함께하는 SW 체험'은 SW에 대한 학부모와 여학생들의 뜨거운 관심을 엿볼 수 있는 시간이었다. 참가한 학부모는 "딸과 함께 소프트웨어가 무엇인지, 왜 필요한 지에 대해 함께 배우고, 공감할 수 있는 뜻깊은 시간이 되었다."라고 밝히기도 하였다.

"Girls on Top! 소프트웨어로 세상을 놀라게 한 그녀들의 이야기"라는 주제로 진행된 토크콘서트에서는 200여 명의 여성들이 참석하여 급변하는 소프트웨어 환경 및 정보를 공유하는 자리를 가졌다.

이틀간 진행된 해커톤에서는 "Wonder Women"을 슬로건으로 내걸고, 일상생활에서 겪는 문제점에 대해 의문(Wonder)을 가지고 놀라운(Wonder) 해결책을 제시한다는 목표로 총 48명이 참여하여 선의의 경쟁을 펼쳤다. 🍀



## 인구통계 데이터를 활용한 PC/Mobile 플랫폼 이용행태 분석

안소영

연세대학교 바른ICT연구소

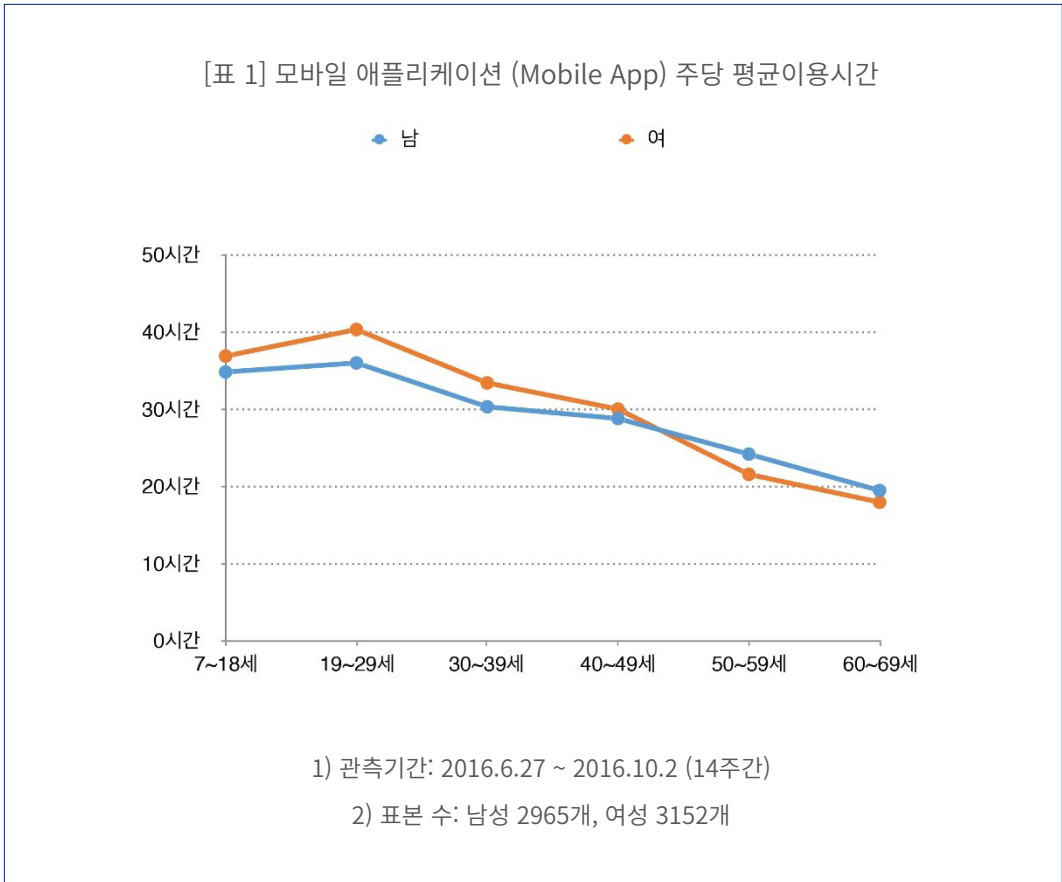
연세대학교 바른ICT연구소에서는 성별, 연령, 지역, 직업, 소득, 학력, 결혼여부 등 다양한 인구통계 데이터들을 활용하여 모바일/PC 플랫폼의 이용행태를 다각도에서 실증적으로 분석하고자 한다. 본 연구는 ICT사용 관련 사회적으로 중요하게 논의되고 있는 정보소외, 정보격차, 스마트폰 과몰입과 같은 다양한 이슈들에 대해 보다 객관적이고 심층적인 정보를 제공할 것이다. 모든 연구는 바른ICT연구소에서 자체적으로 구축한 데이터 셋을 기반으로 진행하였다.

### 스마트폰 덜 들여다보던 남성, 나이 들면 여성보다 더 오래 본다

- 스마트폰 애플리케이션 사용시간, 50대 이상 연령층에서 남성이 여성 추월
- 50대 이상의 남성, 커뮤니케이션, 소셜미디어, 금융, 부동산, 스포츠, 여행, 직업, 교육 등 다양한 애플리케이션에 관심 높아



연세대학교 바른ICT연구소의 조사 결과에 따르면 40대 이하 연령층에서 여성의 스마트폰 애플리케이션(이하 ‘앱’) 사용시간이 남성에 비해 더 많았지만 50대 이후에서는 남성의 사용시간이 여성보다 더 많은 것으로 나타났다. 50대 남성의 경우 주당 평균 약 2시간 37분, 60대 남성의 경우 약 1시간 31분 가량 여성보다 더 오래 스마트폰 앱을 사용했다. 남성이 50대 이후 은퇴하면서 상대적으로 여유시간이 증가한 것이 여성보다 스마트폰을 더 오래 사용하게 된 원인으로 분석된다.



50~60대 남성의 경우 대부분의 카테고리에 있어 여성보다 사용시간이 길었다. 다만 게임과 카카오톡과 같은 커뮤니케이션 영역에서는 여성이 남성보다 더 스마트폰을 더 오래 사용했다. 50대 이상 남성 스마트폰 사용자들은 같은 연령대의 여성 스마트폰 사용자들보다 평균적으로 더 다양한 카테고리의 스마트폰 앱을 이용하는 것으로 나타났다.

50~60대 남녀 모두 게임 카테고리의 모바일 앱 사용시간이 전체 모바일 앱 사용시간의 30%를 넘어섰다. 50~60대 역시 다른 연령층과 마찬가지로 특정 카테고리의 모바일 앱에 지나치게 편중된 사용패턴을 보인 것이다.

50대 남성은 커뮤니케이션, 소셜미디어(카페, 블로그, SNS, 게시판 등), 금융/부동산, 스포츠/레저/여행, 직업/교육관련 영역의 모바일 앱을 40대 남성보다 더 오래 사용했다. 50대 남성이 40대 남성보다 스마트폰 앱 주당 평균 사용시간이 무려 4시간 36분이나 적다는 점을 감안하면 상당히 이례적인 현상이다.

새로운 정보기술에 대한 적응력이 40대가 50대보다 뛰어나기에 전체 앱 이용시간은 40대가 더 많지만, 50대가 은퇴 등의 이유로 현실 세계에서 사회적 관계가 위축되는 경향이 있고, 이를 모바일 세계에서 보완하려 하다 보니 50대가 커뮤니케이션, 소셜미디어 등 모바일 앱을 더 오래 사용하게 된 것으로 보인다. 🤖

# BARUN ICT ESSAY CONTEST

2016년 12월 19일 연세대학교 청솔관에서 'Barun ICT Essay Contest'가 개최되었다. 본 섹션에서는 Barun ICT Essay Contest에서 Best Essay로 선정된 3편의 에세이를 매달 1편씩 소개한다.

## Privacy In the Face of Little Brothers | You Jin Kwak(연세대학교 UIC)

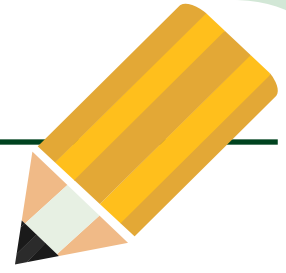
These days, we are bombarded with new devices that has the word “smart” attached to their names- smart TV, smartphones, smart refrigerators... you name it. Virtually anything can be embedded with sensors and software that enable the collection and exchange of data within your own house, workplace, and so on. We’ve reached an era where your “smart” clock could signal your coffeemaker that it’s time to brew the morning coffee. Have you ever thought about what we are trading for this increased convenience? In this quid pro quo world that we live in, we have to be conscious of the fact that as we gain more convenience through these devices, we’re doing it at the cost of our own privacy.

The physical objects now connected to the Internet and having the ability to autonomously collect data is called IoT, or “the Internet of Things”. In my investigation of how technology impacted the way privacy is viewed and defined regarding IoT, I came across 3 articles regarding this issue: an article titled “Privacy in the Internet of Things” by Jamie Lee Williams, “Protecting Privacy in an IoT-Connected World” by Michael S. Smith, and “The Half-Baked Security of Our Internet of Things” by Kashmir Hill.

Although all three articles focus on the susceptibility of IoT and the privacy issues at stake, they differ on their views on who should take measure against these problems. While Hill and Smith both call for tighter security measures on the individual/company level, Williams focuses more on the need to revise the legal framework on the state level. The discussion of the vulnerability

of IoT made me wonder how Korea is currently handling this situation and if the arguments by the three authors could be applicable to the case of Korea.

Hill and Smith both agree that companies should be aware of the threats that IoT poses and take necessary action against them. In her article, Hill puts the blame on the companies by describing how companies lacking in necessary security capability are just mass producing devices that are connected to the Internet. Since they don’t have knowledge on how to ensure their product’s security, it is very costly for them to do so, which means that the company will choose not to do anything about it unless an incident that severely affects a brand’s name value occurs. Hill continues with her cost-benefit analysis of the problem by mentioning, “There will be more and more hacks, not just of cameras but of lots of things. Eventually it will make people care and it will be more expensive to be insecure than secure.” Hill’s paper is effective in uncovering the liability of IoT producing companies by providing a specific case that reveals companies’ ineptness in implementing preventive measures or damage control. Along the same lines, Smith focuses on what the organizations within companies can do to prevent this. On the organizations’ part, he states that IG (Information Governance) professionals in each company should ensure its compliance to “U.S. Fair Information Practice Principles (FIPP)” which is in line with OECD guidelines on the protection of privacy (38).



Also, he recommends data minimization as a way to balance data use with privacy protection. He suggests that organizations could decide not to collect data at all or collect only the data necessary to the product or service being offered.

In contrast, Williams focuses more on the state's responsibility to reconstruct its legal frameworks to cover the realm of IoT. She attempts to raise awareness on the lack of effectively enforced regulations by listing potential danger situations that are not covered by existing laws. As Williams states, "when you make a device smart, you dramatically increase the number of things that can wrong" (3). Her argument is that there are evident loopholes in the existing legal framework, and she effectively illustrates this by giving a specific example of how the government can use this to its advantage. According to the Fourth Amendment of the U.S. Constitution, the government cannot access any detail of what goes on in an individual house without a search warrant issued on a probable cause. This also applies to an individual's cell phone even if the data in it were obtained outside of the house because it carries intimate information of an individual's private life. However, this does not apply to data that are available to the public or a third party. Williams explains that as the information inside the home gathered by the IoT ends up in the hands of the companies and possibly a third party, this could be turned over to the government, which renders the Fourth Amendment ineffective. Therefore, unlike Hill and Smith, Williams calls for a fundamental restructuring of the legal framework because the realm of IoT is unprecedented and too complex for the existing one to cover effectively.

The discussion of the vulnerability of IoT made me wonder what the Korean government was doing about this issue. I assumed that as a nation with a leading IT industry, Korea would have some kind of protocols or technology to prevent this. However, when I read the 2014 IoT status report issued by the Ministry of Science, ICT, and Future Planning, it was an exact resonance of William's argument in that the report was full of what "should be" done, not what "is being" done. For example in chapter 3, "IoT's security measure status", of the report, it states that: 1. there currently exist no regulation or guideline applicable to companies manufacturing IoT products or services (except for a limited guideline on telemedicine), 2. There exists no privacy security framework for IoT, which makes safe implementation and management difficult. 3. There is a need for a structural policy that enforces privacy protection after service (A/S) and can reimburse customers in case of a breach (12). It went on to state that Korea is actually behind in the development of security algorithms, saying that the algorithms that have been developed domestically, such as LEA(Lightweight Encryption Algorithm) and HIGHT(High security and light weight), were all susceptible to a hacking technique that detects the password by analyzing electromagnetic waves from the IoT devices (13). The lack of a proper structural framework and technology to tackle these security issues in Korea made me think about what Korea should do in response to this.

---

Regarding this, we can go back to our previous discussion on Williams, Hill, and Smith. All three had argued for the need to change the status quo, but Hill and Smith were on an individual, company level whereas Williams was on a state level. I believe thinking on both levels is crucial and that a solution should incorporate both levels into the discussion. Therefore I thought of potentially comprehensive solutions to Korea's current situation. One solution I had thought of was to improve our R&D capacity through international cooperation. Since the U.S. has strength in the area of network security regarding Clouds and wireless technology and Europe in cyber security regarding industrial sectors, the Korean government could push for a joint research to learn from and utilize it. Another solution could be to push for a merger between security companies and these manufacturing companies, similar to what Cisco and Intel have done. Cisco had bought NDS, SourceFire, ThreatGrid Security Corps. in 2012, 2013, and 2014 respectively to increase their security capability in IoT products, and Intel had bought McAfee to develop an encryption that ensured their IoT's data security. Likewise, I think the government should encourage IoT manufacturers with incentives to actively merge with security technology companies in order to solve the privacy issues at risk.

Personally, I think that solving this problem is a focal imperative for Korea in order to boost its recently stagnant IT growth and claim a major share in the international market. Since no one has yet come up with an internationally standard protocol for IoT, the world is turning its head to the internal regulations of international companies like Google for guidance. Therefore, it will be a tremendous competitive advantage for

Korea to develop a systematic security framework that could be standardized. Like two sides of a coin, the seemingly grim future of privacy in the era of IoT might actually be an opportunity for Korea. 🌐

#### [References]

Richards, Neil M. "Four Privacy Myths." What Law Can and Should Do? A World without Privacy, Washington University in Saint Louis - School of Law, 2014, Print.

Smith, Michael S. "Protecting Privacy in an IoT-Connected World", Information Management Journal, Association of Records Managers & Administrators, 2015, Print.

Williams, Jamie Lee. "Privacy in the Internet of Things", Human Rights. 2016, Vol. 41 Issue 4, p14-22. 4p.

Ministry of Science, ICT, and Future Planning. "IoT Information Security Roadmap". [http://www.msip.go.kr/cms/www/open/go30/info/info\\_1/info\\_11/\\_\\_\\_icsFiles/afieldfile/2015/12/08](http://www.msip.go.kr/cms/www/open/go30/info/info_1/info_11/___icsFiles/afieldfile/2015/12/08)

## ICIS 2016 개최

지난 2016년 12월 11일, ICIS(International Conference on Information Systems) 2016이 아일랜드 더블린에서 개최되었다. ICIS는 매년 12월 개최되는 IS분야의 가장 명망있는 컨퍼런스로, IS 전문가들의 네트워킹을 제공하고 가장 최신 트렌드와 연구 역량을 공유하도록 한다.



비즈니스, 정책 관점의 연구도 많았지만, 기술의 어두운 관점을 조명하고 이에 대한 해결방안을 찾아나가는 연구자들의 노력을 엿볼 수 있었다. 특히 한국 연구자들이 모여 토론하는 KrAIS에서는 빅데이터 분야의 효율적인 교수법에 대한 심도있는 논의가 벌어졌다.

올해 2017년에는 한국에서 ICIS가 개최될 예정으로 국내외 IS 전문가들의 많은 참가가 기대된다.

## BARUN ICT ESSAY CONTEST 개최



지난 2016년 12월 19일 Barun ICT Essay Contest가 개최되었다. 이번에 처음으로 개최된 콘테스트는 프라이버시와 개인정보보호를 주제로 영문학 강의를 듣는 학생들을 대상으로 하여 가장 우수한 Best Essay를 3편 선정하는 방식으로 진행되었다. Best Essay 3편은 바른ICT 뉴스레터에서 3달에 걸쳐 소개할 예정이다. Best Essay Award 수상자는 다음의 3명이다.

- 곽유진(연세대학교 UIC), 'Privacy In the Face of Little Brothers'
- 김하늘(연세대학교 사회복지학과 & 영어영문학과), 'Workplace Needs Privacy Protection'
- 구연우(연세대학교 영어영문학과), Department of English Language & Literature, 'Social Networking Sites: Reflecting or Refracting Real-Life Privacy?'

## 사물인터넷(IoT) 환경에서의

## 개인정보 위험 분석 프레임워크 | 한국IT서비스학회지, 2016년 12월, pp.41-62

이애리, 김범수

연세대학교 바른ICT연구소

IoT의 등장으로 수집되는 정보의 종류가 점차 다양해지고, 정보를 이용, 유통, 처리하는 환경이 변화하고 있다. 특히 IoT가 확산되면서 새롭게 수집되는 정보의 양과 정보 수집 디바이스가 기하급수적으로 증가함에 따라, 개인정보보호 및 프라이버시 침해 이슈가 함께 부각되고 있다.

실제로 IoT 환경에서의 침해 사례가 다수 발생하고 있다. 그 사례에는 미국 제너럴 모터스의 텔레메틱스 서비스 온스타(Onstar)의 개인정보 무단 수집 사례, 웹 캠 제조사인 트랜드넷의 동영상 유출 사건, Baby Monitor 서비스 해킹 사건, 무인기(Drone)를 활용한 개인정보 유출, 글로벌 보안기업 카스퍼스키랩(Kaspersky Lab)의 스마트카 해킹 시연 사례 등이 있다.

이와 같이 IoT 환경에서의 개인정보 침해에 따른 개인적/사회적 위험 발생 가능성이 높아지고 있지만, IoT에서의 개인정보와 관련한 법·제도/관리적/기술적 위험 대응방안이 체계적으로 제시되지 못하고 있다(Choi 2015; Kang 2015; Shin 2015).

이에 연세대학교 바른ICT연구소 이애리 박사는 IoT에서 발생가능한 개

인정보 유출 및 프라이버시 침해 관련 위험 요인들을 파악하고, IoT 시대의 개인정보 위험을 분석할 수 있는 위험 분석 프레임워크를 제시하였다.

본 연구에서는 기존 연구 조사를 참조하여, IoT 활용 분야 중 높은 비중을 차지할 것으로 전망되는 서비스를 스마트 커뮤니케이션 디바이스(Smart Communication Device), 커넥티드 카(Connected Car), 스마트 홈(Smart Home), 스마트 헬스케어(Smart Healthcare), 스마트 인프라(Smart Infra)의 5부문으로 정리하였다.

IoT 환경에서의 위험 분석 프레임워크란 이러한 5가지 대표 IoT 서비스들이 상용화되어 보급되었을 때 발생할 수 있는 여러 위험을 사전에 인지하도록 하여 이를 위한 대안을 도출할 수 있는 프로세스를 의미한다.

본 연구에서는 IoT 환경에서의 위험 분석 프레임워크 개발을 위해 기존의 대표적인 위험 분석 기법인 미국표준기술연구소(NIST) SP800-30:2002와 한국산업표준인 KS X ISO/IEC 27005, 그리고 정보시스템 감사통제협회(ISACA) RISK IT의 3가지 위험측정방법을 위험 요인 파악

(식별)과 위험 분석 체계 구축에 있어 핵심이 되는 '위험 평가' 부분에 초점을 두고 분석하였다. 이 3가지 측정 방법 모두 조직 비즈니스 환경에서의 위험 관리 분석에 집중하여 특화되어 있기 때문에, IoT 환경에서의 개인정보 위험 분석에 부합하지 않는다. 따라서 이를 보완할 수 있는 새로운 프레임워크가 필요하다.

이애리 박사는 기존 프레임워크가 가지고 있는 위험 측정 방법을 참조하여 개인정보의 특성과 영향력이 반영되도록 변형 및 보완하였다. 새롭게 제안한 위험 분석 프레임워크의 구성 변수를 수식으로 표현하면 다음의 [그림 1]과 같다.

기존에 일반적으로 받아들여지고 있는 위험 측정 방식은 'IT Risk = (자산Asset, 위협Threat, 취약성Vulnerability)'이다.

본 연구에서는 자산(Asset)을 개인정보(Personal Information)로, 취약성(Vulnerability)을 영향도(Impact)로 대체하였다. 개인정보(Personal Information)는 개인정보의 종류와 민감도 측면을 포함한다.



- 기존 위험 측정 방식

IT Risk = (Asset, Threat, Vulnerability)

- IoT Risk to Personal Information = (Personal Information, Threat, Impact)

= PxPersonal Information + TxThreat + IxImpact

= Px(P1xType of Personal Information + P2xSensitivity of Personal Information)

+ Tx(T1xThreat to Device + T2xThreat to Network + T3xThreat to Server)

+ Ix(I1xNumber of Users + I2xFrequency of Use + I3xMarket Size + I4x2<sup>nd</sup> Market Size)

[그림 1] IoT 위험 측정 방식

그리고 IoT 환경에서는 서비스가 가질 수 있는 취약성을 분석하기 매우 힘들다는 점을 고려하여, 개인정보 유출이 미치는 취약성을 투영하는 변수로서 사회적 영향력(Social Impact)에 초점을 두고 위험을 측정하도록 하였다. 사회적 영향력은 사람(즉, 개인)에 대한 정보 유출 및 프라이버시 침해 사고 발생 시 사람들이 받을 피해와 이로 인한 사회적 충격과 관련된 변수이다. 사회적 영향력은 세부적으로 IoT 서비스 사용자 수, 사용 빈도, 시장 규모, 2차 결합 시장 규모로 구성된다.

위협(Threat)은 개인정보 유출 및 프라이버시 침해 위협 정보를 말하며, IoT 환경에서 개인정보가 생성/전달/처리되는 단말(Device), 네트워크(Network), 서버(Server) 영역에서의 침해 위험도가 모두 반영되도록 하였다.

도출된 프레임워크의 검증 을 위해 수행한 IoT 서비스 분야별 위험 분석 결과는 [표 1]과 같다. 예를 들어 식별가능한 개인정보 종류 측면에서 커넥티드 카와 스마트 커뮤니케이션 디바이스가 위험도가 높았지만, 개인정보

보의 민감도 측면에서는 커넥티드 카보다 스마트 홈이 더 높게 나타나는 등 비즈니스 영역 별로 위험 요인에 대한 위험 정도가 다르게 나타났다.

앞으로 IoT의 확대에 따라 개인정보보호법 보완 및 대책 방안에 대한 논의가 활발하게 전개될 것으로 예상된다. 본 연구에서 도출된 위험 분석 프레임워크는 향후 개인정보보호를 위한 개선 방안과 위험 관리 체계 마련에 참조가 될 수 있을 것이다. 🌐

[표 1] 서비스 분야별 IoT 개인정보 위험 분석 결과

\* 수준: H(높음), M(중간), L(낮음)  
\*\*숫자는 각 수준에 대한 점수를 나타냄

	Personal Information		Threat			Impact				IoT Risk Score
	Type	Sensitivity	Device	Network	Server	#of Users	Freq. of use	Market Size	2nd Market Size	
Connected Car	H(3)	M(2)	M(2)	H(3)	L(1)	M(2)	H(3)	H(3)	L(1)	20
Smart Home	L(1)	H(3)	L(1)	M(2)	L(1)	H(3)	H(3)	M(2)	M(2)	18
Smart Healthcare	M(2)	M(2)	M(2)	L(1)	L(1)	H(3)	H(3)	L(1)	M(2)	17
Smart Infra	L(1)	M(2)	L(1)	M(2)	M(2)	M(2)	H(3)	M(2)	H(3)	18
Smart Comm.	H(3)	H(3)	M(2)	M(2)	L(1)	H(3)	H(3)	H(3)	H(3)	23

## 재난 상황에서의 SNS 정보, 믿을만한가?



Shiori Sano

International Student Ambassador 2기  
연세대학교 국제학대학원

스마트폰이 대중화된 이후로 일본에서는 2차례의 큰 지진이 있었다. 2011년 도호쿠 지진과 2016년 구마모토현을 중심을 발생한 지진은 각각 규모 9.0과 6.5로 규모만큼이나 큰 피해를 남긴 끔찍한 자연재해였다. 강진으로 집이 허물어지고 도로에 구멍이 생기는 혼란 속에 통신망은 마비되고 일부 지역에서는 전화연결도 불가능했다.

이러한 혼란스러운 상황속에서 많은 일본 국민들은 라인, 트위터, 페이스북과 같은 SNS를 적극 활용하며 크게 의존하는 모습을 보였다. 가족들은 라인 그룹채팅을 통해서 서로의 생사를 확인하고 트위터와 페이스북에서 재난관련 정보와 대피소, 구호물품에 대한 정보를 얻었다.

하지만 문제는 SNS상의 정보들이 모두 유용하고 정확한 것은 아니었다는 점이다. 일례로 구마모토 지진 당시 '지진때문에 동물원에서 사자가 탈출했다'는 루머가 트위터를 통해 삽시간에 퍼져나가 주민들에게 공포와 불안감을 불러 일으켰다. 사자가 탈출하는 조작된 사진과 함께 올라온 거짓 정보를 수많은 사람들이 리트윗하며 전국적으로 퍼졌던 것이다. 도호쿠 지진 당시에는 '방사능 피폭에는

요오드 성분이 있는 가글과 소독약을 음용하면 방사능 성분이 분해가 된다'는 루머가 트위터에서 확산되었다.

거짓 정보뿐만 아니라 시간이 맞지 않는 정보도 문제가 되었다. SNS를 통해 대피시설이나 구호물품에 대한 때지 난 정보를 확인한 사람들은 막상 해당 장소를 찾았을 때 물건들이 동이 나거나 해당 기간이 지나 적절한 도움을 얻지 못했다. 정보의 정확성 뿐만 아니라 적시성까지 고려해야 신뢰할 수 있는 정보를 선별할 수 있는 것이다.

패닉에 빠진 사람들은 SNS에 떠도는 모든 정보를 받아들이는 경향이 있다. 하지만 메세지가 신뢰할 수 있을만한 것인지에 대한 판단은 꼭 필요하다. 트위터 사용자들은 글 게시자의 계정이 트위터에서 공식적으로 인정받은 계정인지 여부를 확인함으로써 메시지의 진위여부나 신뢰성을 판단할 수 있다. 페이스북의 경우 프로필 사진이나 기본 정보들이 메세지의 신뢰성을 판단할 수 있는 요인들이 될 것이다. 특히 제 3자에게 메시지를 공유 받을 때는 메시지가 작성된 날짜와 시간을 확인해야 해당 정보가 가진 가치와 혜택을 적시에 얻을 수 있을 것이다. 🌐

おいふざけんな、地震のせいでうちの近くの動物園からライオン放たれたんだが  
熊本



구마모토 지진 당시 SNS 상에서 떠돌던 루머

### [Sources]

ICT活用の防災対策探る 災害情報、手元で確認 | 佐賀新聞LIVE. (n.d.). Retrieved December 7, 2016, from <http://www.saga-s.co.jp/news/saga/10101/380583>

日経プレスリリース. (n.d.). Retrieved December 7, 2016, from <http://release.nikkei.co.jp/detail.cfm?rellID=430416&lindID=1>

熊本地震でSNSが威力発揮! しかし、2つのデメリットも | 人命と財産を守る防災知恵袋. (n.d.-a). Retrieved December 7, 2016, from <http://www.saigairisk.com/999.html>

「災害時のSNS・デマに気を付けて」 (くらし☆解説) | くらし☆解説 | NHK 解説委員室 | 解説アーカイブス. (n.d.). Retrieved December 7, 2016, from <http://www.nhk.or.jp/kaisetsu-blog/700/242979.html>



## IoT 시장에서 기회를 엿보는 기업들


**Alexandra Stephenson**

International Student Ambassador 2기  
연세대학교 국제학대학원

초고속 인터넷의 발달, Wi-Fi의 접근성 향상과 같은 통신 네트워크의 발전과 더불어 센서를 포함한 많은 종류의 부품, 기기들의 가격과 유지비용이 감소했다. 모든 사람들이 스마트폰을 소유하는 문화와 SNS를 통한 실시간 정보교환 또한 많은 분야에 변화를 가져왔다. ‘가능한 모든 곳을 연결(connecting everything where possible)’ 하는 IoT의 출현으로 우리는 인터넷과 연결된 전등, 세탁기와 같은 가전제품, 자동차뿐만 아니라 항공기의 제트엔진, 원유 굴착기 등을 사용할 수 있게 되었다. 글로벌 리서치 기업인 Gartner는 2020년까지 260억 개의 장치가 인터넷에 연결될 것이라고 전망했다. 엄청난 양의 기기들이 IoT 기술을 접목하여 인터넷을 통해 상호작용하는 것이다. 이러한 변화에 전 세계 기업들은 IoT 시장에서 경쟁력을 구축하고 자사를 성장시킬 수 있는 비즈니스 기회를 찾기 위해 노력하고 있다.

실제로 다양한 분야의 기업들은 새로운 기능의 추가나 기존 제품의 재창조 등을 시도하며 변화의 기회들을 잡고 있다. IoT를 통해 기업들은 기존 제품의 수익성 향상뿐만 아니라 새로운 제품 개발과 같은 혁신을 도모하는 것이

다. 많은 기업들이 비용절감, 고객서비스 개선, 효율적 프로세스 구축 등의 이유로 제품에 IoT기술을 도입하고 있지만 고려해야 할 이슈 또한 적지 않다.

IoT 기술을 적용하는 것의 단점은 상당히 많은 투자와 초기비용이 들어간다는 점이다. 선제적 투자가 진입장벽을 만들어 장기적으로 해당 기업에게 이점을 가져다 줄 수도 있지만, 초기 투자가 항상 옳은 결정이라고 말하기는 어렵다. 두번째로, **보안 이슈**는 제품에 IoT 접목하려는 기업들에게 또 다른 큰 장애물이다. 인터넷과 더 많이 연결될수록 정보들이 도용되거나 오용될 가능성 또한 커지기 때문이다. 특히 의료 또는 금융 분야 기업의 경우 이 부분을 신중히 고려할 필요가 있다. 급부상하는 IoT 비즈니스 기회를 포착하려는 기업들은 위와 같이 이미 지적된 문제들을 해결하는 것뿐만 아니라 자신의 경쟁사가 무엇을 하고 있는지 조사하며 시장 변화에 세심한 주의를 기울여야 한다. 더불어 성공적으로 IoT를 구현하기 위해서는 IT 부서와 비즈니스 리더 간의 긴밀한 협력이 필요하다는 것을 기억하자. 

[Sources]

Cindy Baker, “Time is of the essence to capitalize on the Internet of Things,” IT World Canada, November 17, 2016, <http://www.itworldcanada.com/article/time-is-of-the-essence-to-capitalize-on-the-internet-of-things/388507>

Jacob Morgan, “A Simple Explanation of the ‘Internet of Things’,” Forbes, May 13, 2013, <http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#6b74277b6828>

## 독일 인더스트리 4.0 추진현황과 우리의 과제 | 2016.12.20

김은

상근부회장 / 겸임교수


한국ICT융합네트워크 / 울산과학기술원(UNIST)

인더스트리 4.0은 독일의 제4차 산업혁명 정책으로 제품 라이프사이클 전반에 걸친 가치창출사슬 조직과 관리 그리고 통제의 새로운 단계를 말한다.

독일은 기계/설비분야에서 선도적인 포지션을 갖추고 있었고 제조업의 비중이 높은 편이었다. 높은 제조업 비중은 위기상황에서 크게 무너지기도 하지만 빠르게 회복 되는 기반이 되기도 한다.

독일이 인더스트리 4.0의 주요 특징으로는 Decentralization, Autonomy, Networking을 들 수 있다. 제조업에 있어서 이러한 특징은 기존의 조립 라인에서 추가 비용 없이 개인화된 상품 생산이 가능하도록 한다. 특히 인더스트리 4.0의 주요 기술인 가상물리시스템(CPS: Cyber Physical System)을 활용하여 두 가지 CPS 전략(dual CPS strategy)을 달성하기 위해서는 다음과 같은 인더스트리 4.0 특성이 실현되어야 한다.

- 1) 가치창출네트워크의 수평적 통합
- 2) 모든 가치창출사슬 전반 엔지니어링의 디지털 통합
- 3) 수직적 통합과 네트워크화 된 생산 체계

인더스트리 4.0 구현 시 대기업이 중소기업과 협력한다면 네트워크 효과는 최적화가 된다. 상호운용성이 최대화 됨으로써 투자 위험이 최소화되어 국내외 모든 기업이 이상적인 네트워킹이 가능하다. 이러한 협력 시나리오에서는 공동의 의사소통 형태 구현이 성공하여 규격과 표준을 통해 인더스트리 4.0은 큰 경제적인 잠재력을 확보할 수 있다. 

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

\* 바른ICT뉴스레터를 정기적으로 받아보고 싶으신 분은 [news@barunict.kr](mailto:news@barunict.kr) 로 이메일 주시기 바랍니다.

