

<http://dx.doi.org/10.7236/IIBC.2016.16.4.1>

IIBC 2016-4-1

인공지능 기술/서비스 기반의 개인정보 보호 모델에 대한 연구

A study on Model of Personal Information Protection based on Artificial Intelligence Technology or Service

이원태*, 강장묵**

Won-Tae Lee*, JangMook Kang**

요 약 인공지능은 빅데이터 분석 기술에서 보다 인간적인 기술로 진화하고 있다. 인공지능은 사물인터넷의 센싱 기술로 말미암아 인간의 오감보다 더 정교한 감각 기관을 가질 것으로 예측된다. 그리고 인공지능은 클라우드 네트워크 기술로 언제 어디서나 인터넷에 접속하여 컴퓨팅 자원을 지원받을 수 있을 것이다. 이처럼 인공지능은 최신 기술들의 총아로 발전 중에 있다. 이와 동시에 인공지능에 대한 불안과 미래 시대에 대한 암울한 전망도 높아지고 있다. 대부분의 기술 디스토피아적 미래상은 현상을 객관적으로 조망하는 관조적 시야를 잃어버렸을 때 발생한다. 또한 이러한 비관론은 기술 발전의 미래상을 인간 의지의 주관적 미래상으로 전환시킬 능력과 자신감의 부재를 반영하기도 하다. 이 같은 인공지능 기술과 서비스의 발달에 따른 대량해고와 실업, 기계에 의한 인류 종말 등 일반적 주제를 다루기보다는 가까운 지금 일어나고 있는 개인정보보호 침해의 이슈를 다루고자 한다. 더 나아가 이 논문은 개인정보보호를 보장하면서 인공지능 산업을 발전시킬 수 있는 도덕적/법제도적 모델에 대해서도 고찰하였다.

Abstract A.I. has being developed from the technology for Big data analysis to the technology like a human being. The sensing technology of IOT will make A.I. have the more delicate sense than human's five senses. The computer resource is going to be able to support A.I. by clouding networking technology wherever and whenever. Like this A.I. is getting developed as a golden boy of the latest technologies At the same time, many experts have the anxiety and bleak outlook about A.I. Most of dystopian images of the future come out when the contemplative view is lost or it is not possible to view the phenomena objectively. Or it is because of the absence of confidence and ability to convert from the visions of technology development to the subject visions of human will. This study is not about the mass dismissal, unemployment or the end of mankind by machinery according to the development of A.I. technology and service, but more about the occurrent issue like the personal information invasion in daily life. Also the ethical and institutional models are considered to develop A.I. industry protecting the personal information.

Key Words : Artificial Intelligence, Privacy, Personal Information, Big Data, Cloud Computing

1. 서 론

유엔 미래포럼의 제롬 글렌(Jerome Glenn) 회장은

“2020년에는 뇌과학 또는 의식기술 시대(Conscious Technology)가 온다”고 예측했다.^[1] 이미 암호전문가인 튜링(Alan Turing)은 1950년에 ‘튜링 테스트’라는 것을

*정희원, 정보통신정책연구원 연구위원

**정희원, 고려대학교 교수 (정보창의교육연구소)

접수일자 : 2016년 5월 9일, 수정완료 : 2016년 7월 8일

게재확정일자 : 2016년 8월 5일

Received: 9 May, 2016 / Revised: 8 July, 2016 /

Accepted: 5 August, 2016

**Corresponding Author: kangjm@korea.ac.kr; mooknc0331@gmail.com
Korea University, Korea

발표하여 인공 의식(synthetic consciousness)의 존재를 둘러싼 논쟁을 촉발시켰다.^[2]

그 후 66년이 지난 2016년 우리나라에서는 인공지능 알파고와 이세돌 9단 간의 세기의 바둑 격돌이 있었다. 2016년 구글의 ‘알파고’와 이세돌 9단의 대국은 인터넷에 흩어진 정보를 실시간으로 분석한 알파고의 승리로 끝났다.^[3]

우리나라에서는 이세돌과 인공지능 알파고의 대국 이후, 인공지능에 대한 관심은 드라마틱하게 성장하였다. 그와 동시에 인공지능에 대한 불안감, 기술 오남용에 대한 염려, 인간 종말에 대한 우려, 인공지능으로 말미암아 직장을 잃을 걱정 등 여러 기술 디스토피아적 미래상들이 펼쳐지기도 했다.

그러나 대부분의 기술 디스토피아적 미래상은 현상을 객관적으로 조망하는 관조적 시야를 잃어버렸을 때 발생한다. 또한 그러한 비판론은 기술 발전의 미래상을 인간의 의지의 주관적 미래상으로 전환시킬 능력과 자신감의 부재를 드러내는 것이기도 하다.

이 글은 인공지능 기술과 서비스의 발달에 따른 대량 해고와 실업, 기계에 의한 인류 종말 등과 같은 일반적 주제보다는 가까운 지금 일어나고 있는 개인정보보호 침해의 이슈에 초점을 두고자 한다. 더 나아가 이 논문은 개인정보보호를 보장하면서 인공지능 산업을 발전시킬 수 있는 도덕적/법제도적 모델에 대해서도 고찰할 것이다.

II. 인공지능의 함의와 조건

1. 기계가 생각할 수 있는가.

튜링은 ‘기계가 생각할 수 있는가?(Can machines think?)’라는 질문에 대해 긍정적이라고 답변하였다.^[4] 동시에 튜링은 ‘컴퓨터가 생각할 수 있다면 그것을 어떻게 표현해야 하는가?’라는 질문을 연구 주제로 삼았다. 튜링은 컴퓨터로부터의 반응이 인간과 구별할 수 없다면 컴퓨터는 생각할 수 있는 것이라고 주장하였다.

이후 튜링은 Computing machinery and intelligence 저널의 Mind을 통해 기계가 지능적이라고 간주할 수 있는 조건을 언급했다.^[5] 그리고 튜링은 튜링머신으로서 알고리즘과 계산 (computation)의 개념을 형식화 하였는데 이는 Church-Turing thesis 라고 불리기도 한다. 인공지능의 조건은 다음 절에서 다룬다.

2. 인공지능의 조건

튜링은 컴퓨터가 뇌를 모방할 수 있다고 주장하였다. 그는 어떤 문제에 대한 대답이 컴퓨터에서 나왔는지, 인간의 머리에서 나왔는지 구분할 수 없을 정도로 뇌의 모조품인 컴퓨터가 훌륭하다면, 기계도 생각할 수 있음을 인정해야 한다고 주장했다.^[5] 그리고 앞선 질문을 명쾌하게 풀기 위해, 장구한 철학적 토론 대신 구체적인 테스트를 제안했다.

표 1. 튜링 머신과 형식체계 [6]

Table 1. Turing Machine and Formal system

튜링머신		형식체계
기계 학습	입력	공리
	프로그램	추론규칙
	출력	정리

위 조건(입력-프로그램-출력/공리-추론규칙-정리)은 어떠한 실질적인 컴퓨터 모델도 튜링머신의 성능과 동등하거나 그것에 포함된다는 명제이다. 이 명제를 기준으로 만약 어떤 회사가 생산한 기계가 ‘인간처럼 생각한다’라고 주장을 한다면, 다음과 같은 논리적 추론을 통해 이를 확인할 수 있다.

실제 생산 회사의 의견대로 생각의 요소를 갖는다는 것을 확인하기 위해서는 주어진 조건들에 대하여 ‘단순히 인간처럼 반응하는가’ 또는 ‘인간인지 기계인지 구분하기 어려운가’ 하는 것만을 알아보면 될 것이다. 만일 구매자가 필요로 하는 서비스에 만족스럽게 답한다면 생산 회사에 대하여 불평할 근거가 없다. 또는 수리나 교체를 위하여 컴퓨터를 반환할 필요도 없다.^[7]

따라서 인간과 기계를 구분하기 위한 잣대로서 사고와 인식의 유무를 판단하는 것 자체가 무의미해진다. 오히려, 인공지능의 ‘인간적 요소’는 인간의 지능이나 행동양식을 인공지능이 동일하게 수행할 것인지의 문제를 다루는 것 보다는 인간 본연의 가치에 어떠한 영향을 미칠 것인가의 문제를 탐색하는게 더 나을 수도 있다는 것이다. 즉 인간과 유사한 인공지능으로 실현될 서비스의 특성을 파악하고 그 내재적 원리가 갖는 프라이버시 침해 또는 개인정보의 위협 요소 및 이에 대한 규제모델을 고려하는 것이 인공지능 연구의 더 중요한 과제라는 것이다.

III. 3장 인공지능 기술/서비스와 개인정보

1. 인공지능 기술과 의사결정

앞장에서 다룬 ‘튜링 테스트’는 철학자와 사회학자 등으로부터 많은 비판을 받았으나, 공학자가 생각할 수 있는 분명한 시사점을 가지고 있다. 그것은 인간의 인지적 능력과 의식 그리고 사고라는 것과 일치하는 ‘기계를 제작할 수 있는지의 여부’를 넘어서는 것이다.

문제의 요점은 인간 의식과 일치하는지 여부를 떠나 이용자가 인간과 기계의 사고판단 그리고 행위에 구분을 못 느낀다면, 그것으로 기계의 의식을 인정해야 한다는 주장이다. 이 주장은 기계의 사고, 인지 그리고 의식이 존재함에 대해서 인정하고 이에 대해 실용적인 준비를 하자는데 초점이 있다.

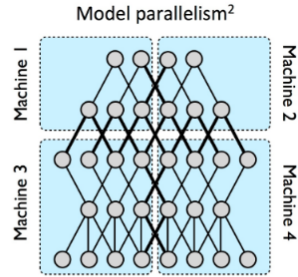
여기서 실용적인 준비란 본 글에서 밝히고자 하는 프라이버시에 대한 염려와 개인정보 보호를 위한 합리적인 제도적/기술적 안전 장치에 관한 것이다. 이에 대한 논의를 다음 절에서 하고자 한다.

2. 인공지능 기술과 개인정보

초연결 사회가 도래하면서 점차 인공지능 기술은 자율성과 독립성을 점점 확대해나갈 전망이다. 인공지능이 스스로 알아서 학습하고 판단하는 이른바 딥러닝(deep learning)의 정도에 따라, ‘강한 인공지능’과 ‘약한 인공지능’으로 구분된다. 아래 그림 1은 딥러닝 모델 중 하나의 사례이다. 이 모델에서는 여러 노드가 딥러닝 머신을 통해 학습한 결과, 새로운 상관관계(그림에서 진한 실선)로 재구성되는 과정을 보여준다. 이 모델의 특징은 4개의 머신을 병렬적으로 처리하는 기법을 통해 딥러닝 머신의 효율성을 높이는데 있다. 이처럼 다양한 방식으로 딥러닝을 통한 인공지능의 자체 성능을 향상시키는 연구가 진행 중에 있다.

그러나 단위 로봇 또는 기계 수준의 CPU에서 처리되는 분석 능력과 실시간 판단 능력으로 ‘강한 지능이냐 약한 지능이냐’를 구분하는 것은 무의미해 질 것이다. 오히려, 인터넷에 연결되어 실시간으로 빅데이터 처리 및 분석 가능한 상태에서는 무선 네트워크 속도와 클라우드 분석 능력이 더 중요해질 것이다. 물론 실세계로 의사결정을 전달할 때, 탁월한 의사결정을 신속하게 할 수 있는 인메모리 분석 능력이 탁월한 로봇 또는 기계의 운영체

제와 인공지능 플랫폼의 성능 역시 중요한 변수가 될 전망이다.



¹Courtesy N Rao
²Large Scale Distributed Deep Networks, Jeff Dean et al., Google, Inc.

그림 1. Deep Learning 모델 [8]
 Fig. 1. Deep Learning Model

그러나 클라우드 컴퓨팅 자원을 통해 개별 인공지능의 실세계 움직임과 판단을 블랙박스(black box)처럼 기록하고 사후적으로 이에 대처하는 Root 레벨의 조정자 역할이 필요할 수 있다. 바로 이 점은 본 연구의 목적인바, Root 영역에서 개인정보보호에 대한 규칙(rule)이 정의되고 제도적/규범적으로 적용되어야 함을 제안하는 것과 관련된다.

IV. 인공지능과 법제도적 함의

1. 인공지능과 프라이버시 위협

앞에서도 언급했듯이, 프라이버시(privacy)라는 광의의 사적 영역을 보호하기 위해서는 개인의 움직임과 판단을 블랙박스처럼 기록하고 사후적으로 이에 대처하는 Root 레벨의 조정자 역할이 필요하다. 개별 인공지능은 출시 시기와 제품 등에 따라 최신화 상태 및 오류 등의 발생 확률이 서비스마다 상이할 수 있다.

통상 iOS는 OS의 업데이트를 자동으로 해주지만, 컴퓨터 시스템(하드웨어 성능) 등이 따라주지 못할 경우, 최신 OS를 설치하지 않는 것이 더 나을 수 있다. 예컨대 MS의 경우, OS는 새로운 버전이 나올 때 마다 비용을 지불하고 구입해야하는 라이선스 개념의 비즈니스 모델이라는 점에서 차이가 있다.

앞으로 인공지능은 그러한 운영체제 위에서 미들웨어(여러 센서를 하드웨어적으로 구동하고 센싱 값을 직접

받아오면서 인공지능 연동의 애플리케이션과 작동) 또는 애플리케이션에서 구동되거나 그렇지 않으면 운영체제 자체가 인공지능의 플랫폼 형태로 개발될 것으로 전망된다.

아래 표 2.는 인공지능이 구현되는 수준 별로 프라이버시의 영역이 어떻게 변화할 지를 정리한 것이다.

표 2. 인공지능과 프라이버시 위협
Table 2. Artificial Intelligence and Privacy

인공지능 작동 위치와 핵심 기술		프라이버시 위협
애플리케이션	빅데이터 기반 개인화 서비스	해당 앱 서비스 (도메인 특정 서비스)
미들웨어/운영체제	센싱 기반 비정형데이터 분석	센싱값의 결합
네트워크	분산환경 하의 빅데이터 분석	비식별정보의 재결합 등

결국 인공지능 기반이란 사물인터넷, 로봇, 검색엔진, 관광/의료/교육 등 서비스, 자율주행차량 등에 직접 설치되어 구동되거나 인터넷으로 연결되어 실시간으로 인공지능적 의사결정을 돕는 서비스를 뜻한다. 따라서 단위 디바이스의 특징과 센싱에 최적화된 프라이버시 보호 방안과 더불어 Root 단위(네트워크 최상단)에서의 기본적인 개인정보보호 가이드라인이 요구된다.

2. Root레벨의 개인정보 가이드라인 모델

앞 절에서 인공지능이 위치하는 영역 (네트워크, 운영체제 또는 미들웨어, 애플리케이션)에 따라 프라이버시의 위협이 달라짐을 살펴보았다. 프라이버시는 이용자 개인이 느끼는 주관적 영역을 포함하는 반면, 개인정보는 식별 가능 여부를 중심으로 객관화가 가능한 또 다른 보호의 영역이다.

초연결사회에서 인공지능은 이용자와 ‘희노애락(기쁨, 노여움, 슬픔, 즐거움)’을 공감하면서도 이용자의 주관적 감정 또는 홀로 있을 권리를 언제든지 침해할 소지가 있다. 예를 들어 보다 지능화된 정크메일(opt-out 방식)을 발송하는 인공지능이 있다고 할 때, 이 인공지능은 이용자가 홀로 시간을 향유할 때 ‘팝업(pop-up)창’ 등의 지능화된 방식으로 광고를 발송하여 이용자가 고독할 시간을 가지지 못하도록 할 수 있는 것이다.

초연결 사회에서는 인터넷에 연결되는 허리띠, 바지, 양말, 목도리, 안경, 책상, 걸상, 모니터, 키보드 등에서 홀

로그램 형태든 소리든 이미지는 팝업창이든 어떤 식으로든 이용자의 의식과 시간을 빼앗을 수 있다. 점차 프라이버시는 존재하는 이용자를 둘러싼 외부 환경 모두로부터 포위되고 있다. 그래서 프라이버시의 위협이 개인정보보다 더 광범위하고 폭넓을 것이지만, 현행법 상 개인정보보호의 위협으로부터 이용자를 보호하고 관련 산업을 발전시키기 위해서는 협의의 프라이버시 영역인 개인정보보호에 대한 고찰이 필요하다.

다음 그림 2은 이상의 논의와 앞에서 고찰한 내용을 축약하여 법/제도가 인공지능 처리에서 어떤 영역에서 이루어져야 하는지를 도식화한 것이다.

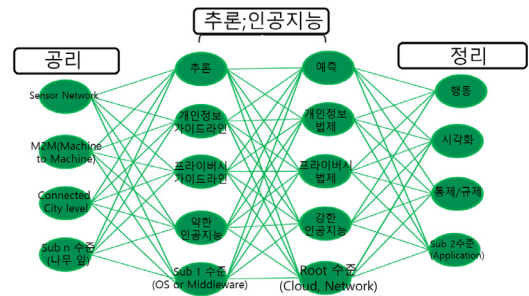


그림 2. Root 수준의 개인정보보호 모델
Fig. 2. Personal Information Security Model for Root Level

인공지능은 크게 세 가지 영역으로 구분한다. 첫째가 입력 영역(input level)이다. 둘째가 숨겨진 영역(hidden level)이다. 셋째가 표현 영역(output level)이다. 위 각 영역은 ‘인공지능의 아버지’라고 불리는 튜링의 테스트에서 ‘입력-처리-출력’에 해당하며 이 부분은 ‘공리-추론/예측-정리’라는 형식체제(2.2.절 표 1참조)로도 대응된다.

‘입력 영역-숨겨진 영역-출력 영역’의 트리(tree)는 세부 노드(node)들의 상호작용으로 이루어진다. 이때 각 노드와 링크가 인공지능에 의해 새로운 군집 또는 유형으로 재분류된다. 그 세부 알고리즘은 딥러닝으로 처리되며 개별 서비스와 기술의 도메인별로 상이하다.

여기서는 이들을 담아낼 수 있는 개인정보 보호 영역이 어느 레벨에 위치해야 하고 트리구조 상 왜 root 영역에 있어야 하는지를 도식화하고 이를 분석하고자 한다. 본 연구는 초연결 사회에 있어 개인정보는 ‘숨겨진 영역(hidden level)’에서 처리되어야 하며, 이 영역에는 기존의 개인정보보호 법제와 이를 구현하는 과정에서 지켜야 할 가이드라인 등이 포함되어야 한다고 본다. 통상 딥러

닝은 입력값을 통해 학습을 진행하게 되는데, 이때 개인 정보보호 규칙 또는 예외 조항 등이 프로그래밍되어야 할 필요성이 제기된다. 또한 개인정보보호는 딥러닝이 처리되는 숨겨진 영역에서 수행됨으로 그 과정의 무결성을 보장받을 수 있을 것으로 기대된다.

입력값으로는 사물인터넷의 센싱값, 비정형 데이터인 기계간 소통, 도시(공간) 간 연결 외 다수의 sub node들이다. 숨겨진 영역인 추론과 예측은 대표적인 인공지능 처리 영역이다. 이 영역은 sub1으로 운영체제 또는 미들웨어 수준에서의 인공지능이 설치된 영역이다. 또는 클라우드(Cloud)와 네트워크 상태에 있는 인공지능에 의한 예측 기능인 Root 수준이기도 하다. sub 1은 실세계에 존재하는 자율주행차량, 의료용 로봇, 살상용 로봇 등의 의사결정을 스스로 하는 자율적이고 독립적인 컴퓨터 자원(CPU 등이 인메모리 기술 등으로 처리되는 인공지능)이다. 이때 인공지능은 네트워크 없이 스스로의 센싱으로 작동하고 판단한다. 반면 Root 수준은 네트워크에 연결된 거대 인공지능의 합이다. 이 경우에는 실세계의 로봇이 네트워크에 연결된 인공지능의 의사결정에 따른다. 따라서 살상 로봇, 민감한 의사결정 등은 강한 인공지능 기반의 네트워크 인공지능으로 처리된다. 이때 인공지능은 개인정보와 프라이버시의 법적 수준에서 판단한다. 반면, 약한 인공지능 또는 개별화된 로봇 차원에서 의사결정은 프라이버시와 개인정보의 가이드라인을 준수한다.

마지막으로 정리 영역은 실제 행동하거나 통제 받거나 시각화되는 애플리케이션 영역이 담당한다.

V. 결 론

본 연구는 최근 급부상하고 있는 미래기술의 하나인 인공지능을 다루면서, 향후 인공지능이 더욱 보편화되는 미래 시점의 초연결사회에서 프라이버시와 개인정보는 어떤 방식(모델)으로 보호할 것인지의 이슈를 분석적으로 검토하였다. 이를 위해 과거 튜링이 주장한 '인공지능을 인간의 인지적 능력 또는 의식과 동일시할 수 있는 조건'을 예비적으로 고찰하였다. 그래서 본 연구에서는 튜링 테스트에서 다룬 '입력-프로그램-출력'과 '공리-추론/예측-정리'를 'Root 수준의 개인정보보호 모델'로 차용하였다.

또한 본 연구는 인공지능이 실제 처리되는 딥러닝 과정에서 다수의 노드가 상호작용하는 네트워크 상에서 학습을 통한 추론이 이루어지는 과정에 대해서도 분석하였다. 그리고 그 과정 중 '숨겨진 영역'에 프라이버시 또는 개인정보의 법제를 배치하는 것의 정책적 중요성을 강조하였다. 특히 운영체제와 미들웨어 수준에서 일체화된 자율판단형 인공지능의 경우에는 가이드라인 준수를 통해 로컬 차원의 부분적 문제해결 및 약한 인공지능의 제한된 성능에 최적화시키는 방법론도 제안하였다.

그와는 달리, 본 연구는 인터넷에 연결된 강한 인공지능의 경우 미래의 초연결 사회에서 절대적으로 필요한 통제/규제 시스템 속에서 의사결정이 이루어지는 과정을 모델링 하였다. 이는 사물인터넷과 기계의 비정형 데이터가 입력되는 과정과 이를 분석하여 정리하는 각 단계에서 개인정보가 어떤 영역에 어떻게 배치되어야 바람직한 것인지를 고찰하기 위함이며, 실제 개인정보보호에 대한 프로토타입을 설계할 때 유용한 시사점을 줄 것으로 기대된다.

지금까지의 논의는 주로 인공지능이라는 추상적 기술에 국한되었다는 한계점을 안고 있다. 따라서 향후 인공지능 기반의 개인정보보호 모델을 적용한 연구는 구체적인 기술이슈를 중심으로 추진되어야 할 것이다. 예컨대, 구글 글라스 등과 같은 웨어러블 디바이스의 출현에 따라 Touch 기술은 Watch 기술로 전환되고 이에 따라 시선의 이동, 동공의 확장, 시선이 갖는 인문학적 함의, 인문학적 메타포와 기술적 메타 태그의 연결 등이 매우 중요한 혁신전략이 될 것으로 예측되는 바,^[9] 향후 보편화될 웨어러블 디바이스의 인문학적 이해와 더불어 본 연구에서 제안한 인공지능 기반의 개인정보 보호 모델을 접목시키는 연구로 구체화한다면, 제안 모델에 대한 유의미한 검증 사례가 될 것으로 기대된다.

References

- [1] Jerome C. Glenn, Elizabeth Florescu, and The Millennium Project Team, 2015-16 State of the Future, <http://www.millennium-project.org/millennium/201516SOF.html>
- [2] Stephen L. Thaler, "The Emerging Intelligence and Its Critical Look at Us," Journal of

Near-Death Studies, March 1998, Volume 17, Issue 1, pp 21-29

- [3] Jang-mook KANG, A match of artificial intelligence, Sisa Journal, 2016, url: <http://www.sisapress.com/news/articleView.html?idxno=76417>
- [4] http://www.aistudy.co.kr/ai/turing_test.htm (검색일: 2016.05.01.)
- [5] A. M. Turing, "Computing Machinery and Intelligence", Computing machinery and intelligence. Mind, 59, 433-460. URL: <http://www.loebner.net/Prize/TuringArticle.html>
- [6] http://www.aistudy.co.kr/computer/turing_machine.htm (검색일: 2016.04.10.)
- [7] Roger Penrose, Various critical reactions to be found in Behavioral and Brain Sciences vol. 13 #4 (1990), 643 - 705, and vol. 16 #3 (1993), 611 - 622, e.g. M. Davis "How subtle is Godel's theorem? More on Roger Penrose, URL: <http://journals.cambridge.org/action/displayAbstract?aid=674880> (검색일 2016.04.22)
- [8] <http://www.nervanasys.com/deep-learning-and-the-need-for-unified-tools/> (검색일: 2016.05.14.)
- [9] Won-Tae Lee, Jang-Mook Kang, Deduction of Humanistic Metaphor based on Searching, Participation, Sharing and Analysis of Wearable Device, The journal of the institute of internet, broadcasting and communication : JIIBC, v.14 no.3, 2014, pp.125-130

강 장 목(정회원)



- (현) JM Code Group 대표
 - (현) 고려대 정보대학 정보창의교육 연구소 교수(연구)
 - (현) 경실련 소비자주권국 위원
 - (현) 국가인권위 정보인권국 자문 교수
 - (현)함께하는 시민행동 운영위원
 - (현) 시사저널 '강장목의 테크로깅' 칼럼리스트
 - 고려대학교 공학 박사(정보보호)
- <주관심분야 : ICT 융합 발명 및 특허, 프라이버시, 빅데이터>

저자 소개

이 원 태(정회원)



- (현) 정보통신정책연구원 ICT전략연구실 연구위원
 - (현) 정보문화포럼 지능정보사회윤리분과위원
 - (현) IT정치연구회 회장
 - 한국사이버커뮤니케이션학회 부회장, 정보문화포럼 부의장 등 역임
- 서강대학교 정치학 박사(정치커뮤니케이션)
<주관심분야 : ICT융합정책, 개인정보보호, SNS>