산업 영역에서 빅데이터 개인정보 보호체계에 관한 연구

(A Study on Personal Information Protection System for Big Data Utilization in Industrial Sectors)

김진수*, 최방호, 조기환**
(Jin Soo Kim, Bang Ho Choi, Gi Hwan Cho)

요 약

4차 산업혁명 시대에 사물인터넷과 모바일을 통해 수집된 다양한 정보를 이용해 공공 및 민간영역의 새로운 비즈니스모델을 위한 빅데이터 산업이 각광을 받고 있다. 하지만, 개인정보 비식별화 조치를 통한 빅데이터 통합 및 분석를 수행하면서 개인프라이버시가 노출될 위험성을 여전히 가지고 있다. 최근 개인정보를 노출하지 않고 데이터의 가치를 유지하는 방법에 대한 연구가 진행되고 있다. 본 논문에서는 빅데이터산업 활성화를 위해 의료, 농업 등 산업별로 개인정보 보호체계가 필요함을 강조하였다. 비식별화된 개인정보의 적정성 평가 기준을 개인 민감정보 중심의 의료분야는 k-익명성 최소값을 일반적인 산업분야의 평균값 보다 높은 5 이상으로 설정해야하며, 농업분야에서는 개인별 민감정보범위에 개인소유 반려견이나 농지 정보를 포함시켜서, 산업별 특성에 맞게 개인정보 보호체계를 보완해야하며, 해당 산업의 특정지역을 대상으로 먼저 실증을 거쳐 전국적으로 확산하는 것을 제안한다.

■ 중심어 : 빅데이터산업 ; 개인정보보호 ; 비식별화조치 ; 데이터 거버넌스

Abstract

In the era of the 4th industrial revolution, the big data industry is gathering attention for new business models in the public and private sectors by utilizing various information collected through the internet and mobile. However, although the big data integration and analysis are performed with de-identification techniques, there is still a risk that personal privacy can be exposed. Recently, there are many studies to invent effective methods to maintain the value of data without disclosing personal information. In this paper, a personal information protection system is investigated to boost big data utilization in industrial sectors, such as healthcare and agriculture. The criteria for evaluating the de-identification adequacy of personal information and the protection scope of personal information should be differently applied for each industry. In the field of personal sensitive information-oriented healthcare sector, the minimum value of k-anonymity should be set to 5 or more, which is the average value of other industrial sectors. In agricultural sector, it suggests the inclusion of companion dogs or farmland information as sensitive information. Also, it is desirable to apply the demonstration steps to each region-specific industry.

■ keywords : Big data Industry ; Personal Information Protection ; De-Identification ; Data Governance

Ⅰ. 서 론

빅데이터 솔루션은 방대한 양의 데이터를 수집·가공 후 분석을 통해 의미있는 결과를 이끌어 내는 데이터관리 기술을 말한다. 고객 신상정보나 매출·회계 데이터 등 고정된 필드에 저장된 정형데이터뿐만 아니라 동영상·음악·소셜미디어 등 실시간으로 생성되는 비정형데이터를 포함한다. 대부분의 빅데이터의

* 학생회원, 전북대학교 정보보호공학과
** 정회원, 전북대학교 컴퓨터공학부

접수일자 : 2018년 08월 09일
수정일자 : 1차 2019년 01월 27일, 2차 2019년 03월 12일
게재확정일 : 2019년 03월 14일
교신저자 : 조기환, e-mail : ghcho@jbnu.ac.kr

형태가 정해지지 않은 비정형데이터이거나 반정형데이터로, 복잡하고 수준 높은 처리기술을 필요로 한다. 최근 경제적 가치창출, 범죄 예방 및 수사 등 빅데이터를 활용하는 비중이 높아지면서 새로운 경제적 가치의 원천으로 떠올랐다. 기업의 타켓 마케팅전략 뿐만 아니라, 범죄방지, 사회공헌 등 공공분야에서도 널리 활용되고 있는 것이다. 컴퓨터 단말기를 이용하는 전통적인 방법으로 자료를 수집하기도 하지만, 최근 발전된 정보기술인 인터넷, 모바일, 소셜미디어, 사물인터넷 등을 이용해서 필요한 대량의 데이터를 손쉽게 수집・저장하여 분석을 할 수 있기 때문이다[1].

하지만, 많은 데이터의 수집뿐만 아니라, 유의미한 결과를 도출하기 위해서는 데이터의 신뢰성을 높여야 한다. 빅데이터가 체계적으로 구축되지 않으면, 개인 프라이버시를 침해할 뿐만 아니라 데이터의 품질도 보장할 수 없다. 특히 기업과 공공기관 등이 개인정보를 침해하여 데이터를 수집·가공·이용·제공하는 과정에서, 「개인정보 보호법」 등 관련 법령을 위반하게 되면, 관계기관으로부터 법적, 행정적 처분과 함께 정보의 주인인 정보 주체로부터 손해배상 소송을 당하는 등, 심각한 위험에 직면할 수 있다.

개인정보와 가명 정보, 익명 정보의 구분이 모호하고, 개인정보를 비식별화해도 분석과 재조합을 통해 다시 식별 가능한 정보로 전환될 가능성도 있어서 여전히 개인정보보호와 빅데이터 활용 간에 충돌이 존재하고 있다[2].

애매한 개인정보 관련법도 빅데이터산업의 걸림돌이 되고 있다. 개인정보보호 법제가 산재돼있는데다, 개인정보 범위 또한 매우 포괄적이어서 데이터 활용 시 제약이 되고 있다. 다양한 데이터의 원활한 연결 및 융합을 위해서는 명확한 개인정보 보호법과 유연한 데이터 공유 환경이 선결 되어야 한다[3].

2장에서는 국내에서 빅데이터 활용을 위해 개인정보 보호 차원에서 취해지고 있는 조치와 문제점을 살펴보고, 3장에서는 이를 해결하기 위한 다른 국가들의 사례를 분석해 보았다. 4장에서는 현재의 포괄적 개념에서 벗어나 빅데이터 분석을 위해 산업별 특징을 고려한 개인정보 보호체계의 개선방안을 제안한다. 마지막으로, 5장에서는 결론을 정리하였다.

Ⅱ. 빅데이터산업과 개인정보보호

1. 빅데이터시장 동향

시장조사기관인 Wikibon에 따르면 소프트웨어, 하드웨어, 서비스를 모두 포함한 세계빅데이터 시장은 2026년에 총 922억 달러의 규모로 성장할 것으로 전망된다. 이는 2014년 기록했던 183억 달러에서 약 404% 증가한 수치이며, 2014년부터 2026년까지의 연평균 성장률은 14.4%에 달한다[4].

2016년도 빅데이터 및 분석시장 산업별 비중은 은행업(13.1%)이 가장 높았으며 뒤이어 조립제조(11.9%), 공정제조(8.4%), 연방/중앙정부(7.6%), 전문서비스(7.4%) 순이었다[4](표 1 참조).

2017년 기준 국내 빅데이터시장은 4,547억 원이다. 2016년 3,440억 원 대비 32.2% 성장한 규모이다. 4차 산업 기술에 대한 정부 투자확대 및 민간 산업계의 빅데이터 인식 개선, 금융권의 빅데이터 플랫폼 투자 본격화가 시장 주요 성장 요인으로 파악된다.

표 1. 2016년 빅데이터 및 분석시장 산업별 비중

산업	비중
은행업	13.1%
조립제조	11.9%
공정제조	8.4%
연방/중앙정부	7.6%
전문서비스	7.4%
기타	51.7%

서버 스토리지 네트워크 등 하드웨어 투자에 56%, 소프트웨어 23.2%, 서비스 분야는 20.9% 로 구성되어있다. 향후 2020년 9,000억 원 이상으로 시장이 대폭 확대될 것으로 예측되며, 연평균 약 25%의 성장률을 보일 것으로 전망하고 있다. 산업별 빅데이터에 대한 성장 전망을 보면, 제조업, 금융, 서비스, 물류유통 및 의료, 공공, 방송통신 분야가 성장률이 높은 편이고, 교육, 환경, 농축산 산업분야도 주목 할만 하다고 보고 있다. 글로벌 Industry 4.0트렌드에 대한 대응으로 국내 제조업에서 공정 자동화 및 위험예측 등의 스마트 팩토리 구축이 증가할 것으로 기대하면서 업종 중 빅데이터 활용이 가장 유망할 것으로 예측한다. 또한 잇따른 금융 대기업들의 빅데이터 도입에 따라 대량의 고객정보를 보유하고 있는 금융권에서의 빅데이터 활용이 확산될 것으로 기대하고 있다. 그리고, 아마존 등 글로벌 대기업이 빅데이터 분석을 통해 구매가능성이 높은 제품을 해당 지역 물류창고에 가져다놓는 예측 배송 서비스를 도입하는 등 물류유통 산업에서의 활용도가 높아짐에 따라 산업 내 활용이 더욱 증가할 것으로 전망된다. 이러한 상황에서 빅데이터산업 활성화를 위한 공급기업의 정책수요를 살펴보면 크게 국가 차원의 빅데이터 거래소 설립 및 과금 등의 관련 법제도 제정, 실무 적용이 가능한 전문인력 양성, 그리고 개인정보 비식별화 가이드라인에 대한 보완 및 산업별 성공사례 확산 등을 중점적으로 요구하고 있는 것으로 나타났다[5].

한편 빅데이터 솔루션의 대상특허 4860건에 대한 각 국가의 연도별 출원동향을 살펴보면, 2010년도를 시작으로 꾸준히 증가하는 양상을 보이고 있다. 전체 출원건수의 64%(3125건)를 차지한 최대 출원국인 미국이 빅데이터 기반 소프트웨어 기술

을 리드하고 있다. 그 뒤는 한국 25%(1203건), 일본 6%(289건), 유럽 5%(243건)순으로 나타났다. 한국의 경우 2010년이후 꾸준히 증가추세를 보였고, 특히 2013년 이후 급증하고 있다. 출원 주체도 70%이상이 내국인으로 기술자립도가 높은 편이다. 특히 중소기업의 경우 빅데이터산업에서 가장 큰 시장, 오픈소스를 주로 활용해서 새로운 제품 및 서비스를 제공하는 서비스 부문에 강세를 보이고 있다. 특허청에 따르면 최근 5년간 빅데이터 관련 중소기업 출원중 서비스부문 비중은 72.8%(377건)를 차지했다. 시장변화에 따른 신속한 의사결정이 가능한데다, 창의성을 갖추고 있어 가능했다는 평가다[6].

2. 개인정보보호에 가로막힌 빅데이터산업

휴대전화에 GPS 수신기가 내장되어 사용자의 위치가 시간별로 기록되고, 범죄를 예방하기 위하여 여기저기 설치하게 시작한 CCTV는 우리 생활 속에서 필수적인 존재가 되었다.

이러한 환경변화로 인해 이제는 우리 생활의 거의 모든 것이 기록되어 보관된다고 해도 이상할 것이 없는 상황이다. 개인정보에 대한 이슈가 사회적으로 부각되는 이유이기도 하다.

최근 기업들의 동향은 빅데이터를 이용하여 소비자들의 구매동향, 취향, 구매 시간대, 연령대별 일정한 구매 법칙을 발견함으로써 각 기업은 그들 스스로가 오래전부터 데이터를 가공하여 수집한 빅데이터를 보유하고 있으며, 그것들을 적극적으로 활용한 마케팅 전략을 펼치고 있다. 소셜미디어 이용이 확대됨에 따라 데이터 사용의 윤리적 맥락에 대한 시기적절한 논의들이 다양하게 이루어지고 있다.

프라이버시 보존형 데이터마이닝(PPDM: Privacy Preserving Data Mining)은 데이터 소유자의 프라이버시를 침해하지 않으면서도 데이터에 함축적으로 들어 있는 지식이나 패턴을 찾아내는 기술을 말한다. 데이터 마이닝은 많은 양의 데이터에 함축적으로 들어 있는 지식이나 패턴을 찾아내는 기술이다. 데이터를 모으고 이를 여러 가지 방법으로 분석하는 과정에서 프라이버시와 관련된 문제는 자연스럽게 대두된다. 특히, 데이터 마이닝이 전자상거래나 마케팅과 같은 분야에 주로 활용되면서, 개인프라이버시 침해 이외에도 경쟁 회사들 사이에 이윤추구를 위해 협력하는 경우 개별 회사가 수집한 정보의 노출이 문제시 된다[7].

데이터 소유자의 프라이버시를 침해하지 않으면서 유용한 정보를 추출하는 것은 정보를 공유하는 것과 프라이버시를 유지하고자 하는 것의 취사선택에 대한 문제로 볼 수 있다[8](그림 1 참조).

특정 개인임을 식별할 수 없다면 기업에서 동의를 받지 않아도 주고받을 수 있게 해서 '데이터' 활용을 가능하게 해야 한다.

스위스 국제경영대학원(IMD)이 발표한 디지털 경쟁력 순위에서 한국의 '빅데이터 사용 및 활용 능력'은 63국 중 56위로 최하위권이다. IMD는 한국의 빅데이터 활용 능력이 콜롬비아·터키·브라질·페루·멕시코 같은 신흥국보다도 떨어진다고 평가하고 있다. 기술에 대한 규제 강도도 63국 중 44위로 지나치게 과도하다고 분석하고 있다.

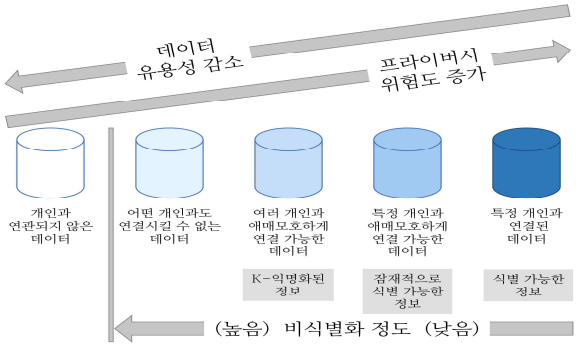

그림 1. 데이터 식별가능 스펙트럼

3. 개인정보보호 관련 이슈

가. 개인정보보호 관련법

빅데이터 산업을 활성화하기 위해서는 개인정보에서 가명 정보의 개념을 더욱 확실히 하고, 「가명 정보 입법화」를 추진하여 산업적 연구 및 상업적 통계 목적의 경우에는 가명 정보의 제삼자 제공이 가능하도록 해야 한다. 벤처협회는 "일부 정보만 감춘 가명정보 결합과 활용은 전문기관을 통해 제한할 수 있다"며 "다만 아예 누군지 알 수 없도록 한 익명정보 활용은 제한 없이 자율에 맡겨야 한다"고 말했다. 개인정보 보호가 소홀해지는 것에 대해서는 사후 처벌 강화 정책이 필요하다.

빅데이터 활용 과정은 수집에서 저장, 분석 및 시각화로 크게 4단계로 나눌수 있고, 사용후 파기 및 저작권에 대해서도 추가 고려해야한다.

이러한 단계에서 예상되는 개인정보보호 핵심이슈를 정리하여 보면 클라우드에 기반한 자료 통합시 가공정보에 대한 정보주체의 동의 판단여부나 개인정보 국외이전에 따른 목적별 세분화된 동의 절차 등이 필요하다[9](표 2 참조).

표 2. 빅데이터 라이프 사이클별 개인정보보호 이슈

단계	기존규정	핵심이슈
수집·이용	필요한범위내 수집 수집하는 개인정보에대한 동의 이용에관한 사항에대해서도 동의	가공정보 정보주체 동의 또는 이용사실에대한 고지여부
	영상정보처리시 과도한영상 수집방지	개인정보와 지리정보가 결합된 신규서비스 적용여부
활용	클라우드기반 집적화·가공정보는 정보주체에 공지, 동의	개인정보를 세부적인단위로 구분해 절차에따라 정보의 중요도에 관한 규정을두고

		동의를 받는데 한계
	개인정보의 국외이전시 정보주체의 동의 의무	국외이전의 목적,형태 등을 고려않한 획일적인 동의절차, 글로벌경제활동에 지장초래
	개인정보제공목적이외 용도로 이용 또는 제3자 제공금지	빅데이터를 구성하는 정보를 결합한 신규서비스창출에 제약
파기	개인정보처리자가 보유기간이 경과, 개인정보처리 목적 달성 등 으로 개인정보가 불필요할 때, 지체없이 파기 의무	개인정보가 가공돼 민감정보, 고유식별정보 등을 또다른 정보의 요소로 사용가능
저작권	창작물을 만든이(저작자)가 자기저작물에 대해 가지는 배타적인 법적권리	분석되는 가공정보에 한해 새로운 저작권 개념도입 및 법적보호

나. 비식별화조치 기법

국내에서는 2016년 6월 30일에 국무조정실 중심으로 「개인정보 비식별 조치 가이드라인」을 발표하였다[10].

개인정보 비식별 조치란 '개인을 식별할 수 있는 요소를 삭제하거나 대체하여 개인을 알아볼 수 없도록 하는 조치'로 가명처리, 총계처리, 데이터 삭제, 범주화, 마스킹 등의 기법을 활용한다(표 3 참조).

개인정보 비식별 조치 가이드라인에서 비식별정보 재식별 가능성 검토, 즉 적정성 판단을 위한 방식으로 k-익명성, ℓ-다양성, t-근접성을 제시하고 있다. 여기에서 k, ℓ, t값은 전문가들이 검토하여 적정한 값을 원본자료의 특성을 고려하여 설정할 수 있다.

k-익명성은 특정인임을 추론할 수 있는지 여부를 검토하는데 일정 확률수준 이상 비식별 되도록 하기위해 동일한 값을 가진 레코드를 k개 이상으로 하도록 한다. 이 경우 특정 개인을 식별할 확률은 1/k이다.

표 3. 개인정보 비식별화기법 종류

비식별화기법	대표사례	세부종류
가명처리 (Pseudonymization)	가명을 사용	.휴리스틱 가명화 .암호화 .교환방법
총계처리 (Aggregation)	평균값을 표기	.총계처리 .부분총계 .라운딩 .재배열
데이터삭제 (Data Reduction)	연단위 날짜만 사용	.식별자삭제 .식별자부분삭제 .레코드삭제
데이터범주화 (Data Suppression)	연령대를 사용	.감추기 .랜덤라운딩 .범위방법 .제어라운딩
데이터마스킹 (Data Masking)	자료에 마스킹표기	.임의잡음추가 .공백과 대체

ℓ-다양성은 특정인 추론이 안 된다고 해도 민감한 정보의 다양성을 높여 추론 가능성을 낮추는 기법이다. 각 레코드는 최소 ℓ개 이상의 다양성을 가지도록 하여 동질성 또는 배경지식 등에 의한 추론을 방지하도록 한다.

한편 t-근접성은 ℓ-다양성 뿐만 아니라, 민감한 정보의 분포를 낮추어 추론 가능성을 더욱 낮추는 기법으로 전체 데이터 집합의 정보 분포와 특정 정보의 분포 차이를 t이하로 하여 추론 방지하는 기법이다[11].

「개인정보 비식별조치 가이드라인」은 아직 법적 근거가 미흡하다. 가이드라인이어서 법적 구속력이 약했다. 또한 데이터들간 결합을 통해 개인정보 노출 위험성을 여전히 내재하고 있다[2].

다. 비식별화 적정성 평가절차

정부의 「개인정보 비식별화조치 가이드라인」에서 권고하는 적정성 평가 절차를 보면, 총 5단계로 구분되는데, 우선 기초자료 작성, 평가단 구성, 평가 수행, 추가 비식별 조치, 데이터 활용 등으로 구성되어 있다. 3명 이상으로 구성되는 평가단은 개인정보 처리자가 제공한 기초자료와 k-익명성 모델 등을 활용하여 비식별 수준의 적정성 여부를 평가한다.

적정성 평가 수행단계는 아래와 같다[12].

- (사전검토) 개인정보 처리자가 제출한 기초자료와 인터뷰 터뷰 등을 통해 평가대상 데이터의개인 식별요소 포함 여부, 데이터 이용 목적, 비식별 조치 기법 등 검토한다.
- (재식별 시도 가능성) 데이터를 이용 또는 제공받는 자의 재식별 의도와 능력, 개인정보보호 수준 등 재식별 시도 가능성 분석한다.
- (재식별시 영향 분석) 데이터가 의도적 또는 비의도적으로 재식별될 경우 정보주체 등에게 미칠 수 있는 영향 분석한다.
- (계량 분석) 개인정보 처리자가 제출한 k값의 정확성 여부 검증한다.
- (평가 기준값 결정) 평가단에서 '재식별 시도 가능성', '재식별시 영향', '계량 분석' 결과와 데이터 이용 목적 등을 종합적으로 고려하여 평가 기준값을(k-익명성 값) 결정한다. 미국 교육부 「프라이버시 보호 기술지원센터」의 기준으로 보면, 'k=3'은 안전도를 보장하는 최소한의 수준이며, '5≦k≦10'은 안전도가 높은 수준이다.
- (적정성 평가) '평가 기준값'과 '계량 분석'에서 산출된 값을 비교하여 비식별 조치의 적정성 여부를 최종 결정한다. 계량분석 결과의 k값이 4이고 평가 기준값이 3인 경우 '적정'으로 평가하고 계량분석 결과의 k값이 4이고 평가 기준값이 6인 경우 '부적정'으로 평가한다. '적정'한 경우에는 데이터 이용 및 제공 가능하고, '부적정'한 경우는 추가적인 비식별 조치 및 재평가를 수행하게 된다.

하지만, 적용되는 k값이 너무 단순한 기준으로 정해진다는 문

제점이 있다.

라. 차세대 비식별화 암호기법

기업들이 사용할 수 있는 여러 방법 중에는 테크놀로지 플랫폼을 이용하여 데이터 분포나 특정 요청을 '원래 데이터를 보지 않고도' 프로세스 하는 방법이 있다. 암호화된 데이터에 대한 컴퓨테이션을 허용하는 특정한 암호화 형식을 이용하는 것이다. 동형 암호와 같은 개념을 사용하든, 아니면 분산 보안 멀티-파티 컴퓨테이션 테크닉 등의 개념을 활용하든, 이들 플랫폼은 데이터의 암호화 된 버전을 운용하며, 해독 시 요청 결과와 꼭 들어맞는 암호화된 결과물을 생성하게 된다.

동형암호는 평문과 암호문에서 같은 성질이 유지된다는 의미로 평문에 대한 연산 결과와 암호문에 대한 연산 결과가 같은 값을 가지는 특징이 있다. 마치 원래 암호화되기 전 상태의 데이터를 사용한 것과 같은 결과이다[13].

이러한 기술은 상황에 따라서는 아주 강력한 힘을 발휘할 수 있다. 기관 전반에 걸쳐 애널리틱스를 추출하거나, 양자가 지니고 있는 정보를 공개하지 않아도 되기 때문이다. 이는 가능할 뿐 아니라 매우 강력하고 안전한 정보 공유 방식이 될 것이다. 민감한 데이터 세트를 다루는 기관에서는 프라이버시의 정의를 매우 넓고 엄격하게 해석해야 한다. 사소한 잔여 위험성조차도 간과해서는 안 되며, 잘 계량하여 파악하고 있어야 한다. 수학적으로 증명된 개인 데이터 공유가 가능한 알고리즘을 사용하고, 데이터의 '모양' 및 통계적 특성을 변형시키지 않는 방식과 정도까지만 데이터에 영향을 미쳐야 한다. 이러한 방식은 정보 공유에 수반되는 프라이버시 보호와 정보의 이용이라는, 언뜻 상충할 수밖에 없는 두 가지 가치들 간에 최적의 균형을 유지할 것이다.

차등 프라이버시와 같은 개념에 기반을 둔 입증 가능한 프라이빗 알고리즘들은 특히 IoT 데이터 스트리밍이나 에너지, 교통 관련 데이터의 취합 및 수집 등 여러 가지 상황에서 매우 유용하게 쓰인다.

Ⅲ. 개인정보보호 글로벌 동향

빅데이터 선도국은 빅데이터 산업 활성화를 위한 필수 조건인 개인정보보호 관련 규제를 비교적 명확하게 규정하고 있다. 다양한 산업 데이터의 원활한 융합을 위해서는 명확한 개인정보보호법 정비와 유연한 데이터 공유 환경이 필수적인 전제 조건이다[14](표. 4 참조).

표 4. 각국의 개인정보法 특징

구분	국가	내용
개인정보의 정의	EU	식별되거나 식별가능한 자연인에 관한 정보
	일본	다른 정보와 쉽게 조합하여 특정한 개인 식별이 가능한 정보
동의방식	미국	개별법에 따라 상이한 사전 사후동의 방식
	EU	사전 동의방식이 기본이나, 정당한 이익 추구시 사후동의 허용
	일본	사전 동의 및 사후동의 방식 동시 허용
제재	미국	개별법에 따라 상이한 형벌 , 행정벌 규정
	EU	개인정보처리 위반 시 형벌 적용
	일본	시정권고조치 후, 추가 위반 시 형벌

1. 일본의 개인정보 개념 명확화

2017년 1월부터 일본 정부는 IT종합전략본부를 중심으로 개인정보의 합리적 활용을 촉진하기 위해 개인정보 보호법을 시행하고 있다. 주요내용으로는 개인정보의 빅데이터 활용 확대를 위해 익명가공정보 개념을 정의하고, 익명가공정보는 복원 불가능도록 안전 조치를 함을 전제로 정보주체의 동의 없이 활용할 수 있도록 허용하고 있다. 또한, 익명가공정보 취급 사업자에게 일정한 기술적·관리적 조치 의무를 부여한다. 일본 정부는 관계 전문가와 함께 비식별 가이드라인 마련 추진 중이며, 전문가들은 '완전한 익명화'는 있을 수 없음을 인정하고, 익명화의 수준을 단계별로 구분·제시할 계획이다. 그중 익명화 수준을 가장 높도록 조치하기 위한 방법으로 k-익명성 모델을 활용하는 방안을 검토하고 있다[15].

2. 미국의 산업별 개인정보 적용

빅데이터산업을 주도하고 있는 미국은 산업분야별로 개인정보범위가 확립돼 모호한 해석에 따른 문제가 적고, 성과를 내기도 쉽다. 일반적으로 개인정보 보호에 관한 일반법이 없으며, 개별 법령에서 제한하지 않는 한 자유로운 데이터의 이용이 보장된다.

의료·교육 등 특정 산업별로 개인정보 보호에 관한 개별 법령 운영 중이며, 의료정보는 「건강보험 이전과 책임에 관한 법」(HIPAA: Health Insurance Portability and Accountability Act) 에 따른 「HIPAA 프라이버시 규칙」에서 비식별 조치 기준을 제시하고 있다. 비식별 조치된 의료정보는 제한 없이 이용 가능하다. 「경제적·임상적 보건에 대한 건강 정보기술법」에서는 비식별 조치된 건강정보에 대해 프라이버시 관련 규제를 적용하지 않는다. 비식별 조치 방법에 따라 '전면적 규율면제' 또는 '부분적 규율면제' 방식을 적용하고 있다. '전면적 규율면제'가 적용되는 비식별 조치방법에는 '전문가 결정방식'과 '세이프 하버방식'이 있다. '전문가 결정방식'은 통계적, 과학적 원칙과 방법에 대한 지식과 경험을 보유한 전문가가 개인식별 위험 최소화 방법 적용하는 것이다. '세이프 하버 방식'은 이름, 주소정보 등 18가지 주요 식별자를 제거하여 개인식별이 가능하

지 못하도록 하는 방식이다. 마지막으로 데이터 제공자와 제공받는 자 간에 데이터 이용 및 제공목적 등을 담은 계약을 체결하여 진행한다[16].

「가족의 교육적 권리 및 프라이버시 법」(FERPA: The Family Educational Rights and Privacy Act of 1974)은 비식별 조치된 학생기록에 대해 별도의 동의 없이 배포 가능하며, 평가절차에서 k-익명성 모델을 활용하고 있다[8].

3. EU의 국가 간 개인정보 적용

2018년 5월부터 EU에서는 단일한 개인정보 보호법(General Data Protection Regulation; GDPR)이 시행되고 있다. 기존 지침의 가명정보 규정이 법적 구속력이 있는 GDPR에 명문화하고 있다. 그러나 가명정보를 동의없이 처리할 수 있는 목적의 범위가 공익, 과학적 연구, 역사연구, 통계 목적으로 일부 한정하고 있다. EU 국민의 개인정보에 대해 국제적인 규칙을 강화하였다. EU 밖에 있는 기업이나 국가가 자국민의 정보를 취급할 경우에도 GDPR이 적용된다는 규정이다[17].

그리고, EU는 최근 일본의 개인정보보호 정책에 대해 적정성(adequacy decision) 여부를 판단하기로 결정하였다. 일본내 개인정보 처리 사업자가 EU로부터 받은 개인정보가 정보주체의 노조 가입여부, 성생활, 성적 취향에 대한 정보를 포함하고 있는 경우, 개인정보 처리 사업자는 해당 정보를 특별 보호가 필요한 개인정보로 취급해야 한다.

4. 뉴질랜드 농업빅데이터 정보

뉴질랜드의 농장자료처리규칙(Farm Data Code of Practice)에서는 자료를 필요로 하는 기관들이 농장에서 취득한 자료들에 대한 보안을 위해 필요한 단계들을 기술하도록 규정하고 있다. 자료에 대한 권리 및 처리 와 공유, 그리고 저장 및 보안에 대한 정책이나 규정을 농장주에게 알리도록 되어있다[18].

미국의 클라이밋 코퍼레이션은 농업현장에서 발생하는 다양한 데이터를 분석하여 농가의 의사결정을 지원하는 서비스 제공한다. 네덜란드에서는 사물인터넷, 빅데이터, 인공지능 및 농업로봇 등 디지털 농업분야에서 산・학・연・관 혁신형 연구를 활발하게 진행 중이다. 이스라엘의 프로스페라는 특화된 인공지능을 기반으로 최적화된 농업 솔루션 제공하며, 클라우드 기반의 데이터 축적으로 분석·예측 정밀도는 계속 향상 중이다. 오스트리아의 스막텍은 센서가 내장된 소형기기를 젖소의 체내에 삽입하여 질병과 건강상태 등을 개체별로 모니터링하면서 데이터를 축적 및 분석한다. 개별 가축의 정보와 지역별 기후정보를 실시간으로 클라우드에 전송, 전 세계목장의 데이터로 빅데이터를 만들어 활용하고 있다[19].

이와 같이, 농업의 빅데이터 대상은 단지 살아 있는 개인뿐만 아니라 반려동물 및 축산동물, 농지까지 포함되어 있다.

Ⅳ. 빅데이터 개인정보 보호체계 개선방안

1. 데이터 거버넌스 체계 수립

데이터 거버넌스(Data Governance)란 통상 기업에서 사용하는 데이터의 가용성, 유용성, 통합성, 보안성을 관리하기 위한 정책과 프로세스를 다루며 프라이버시, 보안성, 데이터품질, 관리규정준수가 중요하다. 광의의 개념으로 데이터 거버넌스는 데이터 자산 관리에 대한 권한, 통제 및 공유된 의사 결정의 행사를 의미한다[20].

빅데이터 가치를 높이기위해서는 많은 데이터의 수집과 함께 데이터 거버넌스 관리프로세스를 통해 데이터 신뢰성을 먼저 확보해야 한다.

빅데이터를 활용하기 위해서는 기초데이터 수집·저장에서 데이터 전처리·가공을 한 후 분석·활용, 시각화로 크게 4단계로 나눠진다.

빅데이터 분석을 위해 가장 먼저 선행돼야 할 것은 데이터 수집 및 저장이다. 이 단계에서부터 데이터의 가치를 높이기 위한 설계가 필요하며, 데이터 거버넌스를 고려해야 한다. 데이터 수집은 서비스의 품질을 좌우하기 때문에 수집 자료의 표준화가 전제되어야 한다. 저장단계에서는 웹 데이터, 소셜 미디어 데이터, 비즈니스 데이터 등 다양한 형식의 데이터를 실시간으로 저장하고 관리하여야 한다. 빅데이터 전처리·가공 단계에서는 개인정보익명화를 수행하게 된다. 수집·저장된 방대한 양의 데이터와 다양한 형태의 데이터 중 실질적으로 필요한 데이터를 걸러내고 적당한 형태로 변형하는 것이다. 최소한으로 편집된 데이터를 사용해 데이터의 최초형태보다 접근하기 편하게 가공하고, 직관적으로 분석해 쉽게 결과를 도출할 수 있도록 하는 게 핵심이다.

데이터 거버넌스의 필요성을 다음과 같이 다양한 관점에서 기술하고 있다.[21]

- 데이터 경영·분배·보호 프레임워크와 로드맵
- 데이터 통합과 기업 데이터 경영 프로그램을 지원하기 위한 데이터 수집 전략과 방법
- 산업의 특화된 규정에 정렬하기 위한 접근
- 전반적인 데이터 투명성과 사용을 향한 전략

이처럼 산업 분야, 조직, 학술 등 분야별 특성이나 관점, 연구목적 등에 따라 다양하지만, 데이터 통합을 위한 3가지 방향성을 정리하면 아래와 같다.

- 기관 등이 자산인 데이터를 효율적으로 관리하여 활용하

기 위한 원칙이 있어야 한다.

• 기관 등이 조직 내에서 인력, 절차, 기술 및 정책의 조정을 통하여 전사 데이터에서 최적의 가치를 도출하기 위한 방법론이 수립되어야 한다.

• 데이터로부터 야기될 수 있는 데이터의 불일치 등과 같은 다양한 문제로 유발되어 상충하는 정책 등을 조정·통제·관리하는 방법론을 가지고 있어야 한다.

또한, 공공기관이나 기업 등은 빅데이터 활용에 필요한 개인정보보호의 정책방향과 세부이행계획, 그리고 인력과 조직이 포함된 소위 '빅데이터 개인정보보호 기본계획'을 수립하여 추진하여야 한다. 첫째는 '규정준수'에 관한 사항으로 개인정보보호 정책방향 등에 관한 내용이고, 둘째는 '법·내부규칙'에 관한 사항으로 개인정보보호 담당 조직 및 인력에 관한 내용이며, 또한 '정보호보, 개인정보보호, 규정'에 관한 항목으로 구성 되어야 한다[19].

• (위험관리) 데이터로부터 유발되는 비즈니스 및 문화적 위험을 식별, 평가, 정량화, 회피, 수용, 완화, 나아가서는 양도하는 방법론이다.

• (규정준수) 개인정보보호, 정보보호, 기타 규정으로 구분하여 규정을 준수하도록 하는 정책 또는 기준이다. 특히 개인정보의 보호를 위해 개인정보의 수명주기별로 규정의 준수를 위한 정책을 포함한다.

• (가치 창출) 데이터 자산의 가치를 향상시키고, 평가하고, 계량화하는 절차이며, 비즈니스 이익의 극대화에 기여한다.

• (조직 구조) 비즈니스 조직과 IT 조직 간의 책임과 역할을 명확히 정의하고, 독립된 데이터관리 조직을 설계, 운영하는 방법론과 절차이다.

• (데이터 관리권 식별·담당자 지정·훈련) 데이터 품질관리의 한 분야로 데이터를 특성과 분야별로 분류하고, 각 분류별 데이터의 가치향상, 위험 완화 및 조직 통제 등을 위한 담당자를 지정하고, 해당 직무 또는 행동기준을 정한다. 그리고 필요한 사항의 훈련도 한다.

• (법·내부규칙) 규정준수에서 정의한 정책이나 기준을 관리·운영하는 조직을 정의하고 조직 구성원의 행동기준도 정한다.

• (데이터 품질관리) 데이터의 수집이나 생산, 데이터 정제, 테스트 등 데이터 품질의 확보를 위한 활동인 측정·품질향상·품질의 인증 등을 위한 절차이다.

• (데이터 수명주기 관리) 데이터의 수집·이용·저장·삭제에 대한 체계적인 정책이다. 특히 개인정보의 수명주기에 따른 파기와 관련되는 정책과 절차도 포함하여야 한다.

• (정보보호, 개인정보보호, 규정) 규정준수에서 정한 정책이나 기준을 이행하는 실질적인 방법이며, 데이터 자산을 보호하기 위한 세부정책이나 사례, 그리고 통제규칙 등이다.

• (데이터 품질관리) 기업 등이 부문별, 업무별로 별도의 정보시스템을 구축·운영함으로써 데이터의 중복과 불일치 등의 문제가 발생하게 된다. 이러한 현상을 완화하거나 제거하기 위한 활동을 데이터 품질관리라 하며, 이를 통해 데이터의 정확성·일관성·적시성 등의 확보하도록 하는 단계이다. 세부 단계로는 품질진단, 품질 측정, 품질 모니터링, 데이터 정제, 데이터 계보 및 임팩트 분석 등이 있다.

2. 비식별화 적정성평가

데이터와 관련된 이해 관계자들이 데이터 공유, 유출에 따르는 재식별(re-identification)의 위험을 인지하게 할 필요가 있다. 정보 이론 프레임워크를 이용하여 민감한 정보의 공유와 관련된 잔여 리스크를 정확하게 추정하는 방식이다. 정부기관과 기업, 그리고 비영리기관, 사설기관 등을 위한 데이터 프라이버시 관리 가이드를 제공해서, 획일화된 데이터 프라이버시를 강화하지는 못할 수 있다. 그러나 데이터 관리자들이 특정 데이터 공유나 공개 상황에 따르는 중요 위험 요소들을 이해하고 거기에 적절히 대처할 수 있다. 예를 들어 프라이버시 리스크 분석 및 통제, 이해 관계자의 참여, 그리고 리스크의 영향력 평가 등을 고려할 수 있다.

3. 개인정보 자기결정권 확대

개인정보 자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 해당 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리로 정의된다. 이러한 결정권을 활용하면 일방적이고 수동적인 현 제도의 단점을 보완 할 수 있다. 개인정보 자기결정권은 익명권, 정보열람청구권 등의 구체적인 권리들을 포함하고 있으며, 국내에서는 개인정보보호법, 정보통신망법, 위치정보법, 신용정보법에 규정되어 있다[2]. 개인정보 비식별화와 블록체인 기술들의 이용해서 개인데이터(MyData) 활용을 보편화해야 한다.

4. 개인정보보호 거버넌스 확립

개인정보보호 거버넌스 이슈도 법 개정이 필요하다. 정부내 조직적인 측면에서 보면 개인정보 침해를 우려하는 국민 불안을 해소하기 위해 개인정보보호위원회, 행안부, 방통위, 금융위 등 관련 부처 개인정보 보호 기능을 정리해 독립된 감독체계를 강화하는 방향으로 가야한다. 또한 지역특화산업의 특징을 반영할 수 있도록 지자체의 적극적인 참여도 필요하다.

데이터 거버넌스 관점에서도 를 공공과 민간 데이터를 포괄

한 국가 전체 데이터 자산 관리에 대한 권한, 통제, 의사 결정이 가능해야 한다. 대민 조사 환경 악화로 인한 대안 모색의 차원에서 행정데이터 또는 민간 데이터 활용이 불가피한 상황을 감안하면 행정자료와 국가통계 자료 등 공공 데이터는 물론 민간 데이터까지 포괄하는 국가 차원의 데이터 거버넌스 체계의 정립이 시급하다.

5. 산업별 개인정보 보호체계

비식별화 대상이 되는 개인정보는 통상 개인식별정보, 준식별정보, 민감정보 등이 있는데, 산업별로 요구하는 빅데이터 목적에 따라 주로 사용되는 세부 개인정보가 상이하다.

개인식별정보를 활용하는 맞춤형 광고분야는 이용자의 개인정보에 근거한 것이어서 개인정보보호법의 규제대상이 된다.

보건의료산업에서는 빅데이터 활용에 개인 민감정보와 준식별정보들 간의 연결을 통한 개인정보식별 가능성이 높다[22].

농업분야에서도 4차 산업혁명의 기회를 농업 재도약의 디딤돌로 활용하기 위해 유럽에서는 IoF2020 프로젝트로 사물인터넷을 기반으로 유럽의 농식품 모든 영역에 정보 네트워크를 구축하여 빅데이터를 수집・활용할 예정이다.

국내 「개인정보 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서는 죽은 자, 토지, 가축의 개인정보는 개인정보의 범위에 포함하지 않고 있다. 그 이유는 명확하지 않으나, 죽은 자, 토지, 가축 등은 「개인정보 보호법」에 의하여 처리정보의 열람, 정정 등을 청구할 수 있는 정보주체도 사실상 권리를 행사할 수는 없기 때문이다[23].

하지만, 살아있는 사람뿐만 아니라 사망한 사람에 대한 의료학적 빅데이터 분석이 필요한 경우가 있다. 사망원인 및 일정 의료치료 후 생존기간에 대한 분석이 한국인의 건강한 삶의 연장에 기여 할 수 있기 때문이다. 이러한 경우 현재는 직계가족 등에 대한 동의 없이 정보를 사용할 수 있게 되어 있다. 그러나 이러한 것들이 개인정보로 취급할 수 있는 방법은 있다. 이들을 관리하거나 보호하는 주체, 즉 유족이나 관리자를 정보주체로 하고, 이들의 정보를 해당 유족이나 관리자의 개인정보에 속하는 항목으로 한다면 개인정보로 볼 수 있다.

농업분야에서는 반려동물에 대한 인식이 인간과 함께하는 가족의 개념으로 정착되고 있는 상황에서, 반려견의 치료 및 건강기능식품 개발 등에 빅데이터의 활용성이 급격히 증대 되고 있다. 마찬가지로 질병 예방을 위한 건강한 사료개발 및 농지에 적합한 비료를 위해 농지 토양정보 대한 수집이 활발해 지고 있다. 반려동물 및 축산동물, 농지 소유주의 동의가 이 분야의 빅데이터 활성화를 위해 전제되어야 한다.

일반적으로 개인정보는 다음과 같은 형식으로 취한다. 개인정보 = A(a1, a2, a3, ,,, , an) 라고 하면, 여기서 A는 n개의 항목으로 구성하고 있으며, 이 항목들은 식별자, 준식별자, 민감정보, 그리고 기타 정보로 구성된다.

이 형식에서 죽은 자, 토지, 가축 등을 관리하는 자의 이름, 주소, 주민등록번호 등과 같은 식별자 정보와 함께 한 개의 레코드를 구성한다면, 죽은 자 정보, 토지 정보, 가축 정보는 관리자의 개인정보로 볼 수 있다. 그러한 방법으로 데이터를 구성하면, 유족이나 관리자의 개인정보는 보호해야 하므로 관련 정보도 보호의 대상이 된다.

유럽의 GDPR에도 자연인이라 하여 살아있는 사람의 정보를 보호대상으로 보고 있다. 다만, 호주의 정보공개법은 死者의 정보도 개인정보로 보호하고 있다.

유통, 의료, 농업 등 주요산업별로 개인정보범위를 탄력적으로 적용해야 할 뿐 만 아니라, 개인정보 비식별화의 적정성을 판단하는 k값의 경우에도 민감정보를 많이 취급하는 의료분야는 일반 산업분야에서 안정성이 있다고 판단하는 최소 'k=3'대신에 보다 높은 '5≦k≦10'을 적용해야 한다.

이들 산업별 개인정보 보호법을 지역별로 특화산업을 대상으로 각 지자체 조례를 통해 제정하여 시범적용 한 후 문제점을 추가로 보완 한 후 전국적으로 확대 시행 할 필요가 있다.

Ⅴ. 결론

빅데이터산업을 보다 더 활성화하기 위해서는 개인정보보호체계의 개선이 필요하며, 이를 위해 다음의 2가지의 경우에 대해서 산업별 특징을 고려해서 정의 되어야 한다.

- 비식별화 대상이 되는 개인정보의 범위
- 비식별화 적정성 판단기준 지표

통상 비식별화 개인정보는 개인식별정보, 준식별정보, 민감정보 등이 대상이 된다. 의료 ·농업 등 산업특성을 고려하여 별도로 정해져야 한다.

의료분야에서는 사망한 사람들에 대해 분석이 필요할 경우 유가족의 동의가 필요하다. 이런경우에는 유가족의 개인민감정보에 사망자의 정보가 포함되어야 한다.

농업분야에서는 사람이 아닌 가축이나 반려동물, 또는 농지에서 발생하는 정보가 소유주의 개인 또는 준식별정보로 포함되어야 한다.

산업별로 사용하는 개인정보 종류 및 결합용이성을 고려해서 비식별화 적정성여부를 판단하는 k-익명성의 기준값이 설정되어야 한다. 지금은 산업특성을 고려하지 않은 일반적인 k 기준값이 3 이상으로 제시 되어 있다. 그러나 민감정보을 많이 포함하는 의료분야에서는 5 이상으로 설정 되어야 한다. 이와 같이 비식별화정보의 노출 위험지표를 산업별로 정량화 해야 한다. 자료이용자의 전문성에 따라서 일반이용자와 심층이용자에 제공하는 비식별화 기준을 계층별로 구분하는 방법도 좋은 대

안이 될 것이다. 그리고, 빅데이터를 통합하는 과정에서는 수집, 저장, 그리고 이용하는 단계별로 산업별 특징을 분석하면 위치정보, 차량정보, 보행자정보 등도 추가 고려대상이 된다.

REFERENCES

[1] 정지선, "신가치창출 엔진, 새로운 가능성과 대응전략," *정보화진흥원 새로운 미래를 여는 빅데이터 시대*, 8-30쪽, 2012년 12월

[2] 이현승, 송지환, "개인정보 비식별화기술의 쟁점 연구," *소프트웨어정책연구소*, 50-64쪽, 2016년 8월

[3] 조성은, 이시직, "빅데이터 시대 개인 행태 정보수집 및 활용에 대한 정책 연구," *정보통신정책연구원 기본연구*, 22-27쪽, 2015년 11월

[4] 박선우, "빅데이터 시대와 데이터 융합," *정보통신정책연구원 정보통신방송정책*, 제30권, 제1호, 4-7쪽, 2018년 1월

[5] 권영일, 최영인, "2017년 BIG DATA 시장현황 조사," *정보화진흥원 시장현황 조사 보고서*, 22-24쪽, 2018년 5월

[6] 중소기업기술정보진흥원, "빅데이터 기반 SW," *중소기업기술로드맵 2018-2020*, 252-256쪽, 2018년 1월

[7] 유준석 외 2인, "암호학 기반의 프라이버시 보존형 데이터 마이닝 기술에 관한 연구," *한국정보처리학회*, 제12권, 제2호, 983-986쪽, 2005년 11월

[8] Simson L. Garfinkel, "De-Identification of Personal Information," *NISTIR 8053*, pp. 3-8, Oct., 2015.

[9] 중소기업기술정보진흥원, "중소기업 기술 로드맵 2018-2020 정보보호", *중소벤처기업부*, 38-42쪽, 2017년 12월

[10] 국무조정실, 행정안전부 등, "비식별 조치 기준 및 지원·관리체계 안내," *개인정보 비식별 조치 가이드라인*, 3-8쪽, 2016년 6월

[11] N. Le, et al., "t-Closeness: Privacy Beyond k-Anonymity and l-Diversity," *ICDE*, vol. 7, Apr., 2007.

[12] 개인정보보호지원센터, "개인정보 비식별화에 대한 적정성 자율평가 안내서," *한국정보화진흥원*, 28-44쪽, 2014년 12월

[13] 김영기, 홍충선, "맵리듀스를 적용한 동형 암호화 기법 연구," *한국정보과학회 학술발표논문집*, 749-751쪽, 2016년 12월

[14] 오정연, 선미란, "개인정보보호법제로 인한 빅데이터활용 한계 사례," *정보화진흥원*, 2015년 12월

[15] 한귀현, "일본 개정개인정보보호법의 주요내용과 그 시사점," *한국비교공법학회, 공법학연구*, 제18권, 제4호, 531-559쪽, 2017년 11월

[16] Bradley Malin, "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with HIPPA Privacy Rule," *the Office of Civil Rights, USA*, pp. 4-9, Nov., 2012.

[17] 이상윤, "빅데이터 관련 개인정보 보호법제 개선방안 연구", *한국법제연구원 용역보고서*, 73-78쪽, 2017년 10월

[18] Farm Data Code of Practice(2014). http://www.farmdatacode.org.nz (accessed Aug., 2, 2018).

[19] 민승규, 서현권, "빅데이터가 바꾸는 농업의 미래," *농진청 RDA Interrobang,* 199호, 7-23쪽, 2017년 7월

[20] John Ladley, "Data Governance," *Kaufmann Press*, Nov., 2012.

[21] 김석수, "EA를 위한 데이터 거버넌스 구축 사례 연구," *Journal of Information Technology and Architecture*, Vol.8. No3, pp. 255-265, Sep., 2011.

[22] 여광수, 김철중, 이재현, 김순석, "상관도를 이용한 국내 의료기관용 개인정보 비식별화 방안에 관한 연구," *스마트미디어저널*, 제5권, 제4호, 83-89쪽, 2016년 12월

[23] 임규철, "개인정보의 보호범위," *한독법학*, 제17호 224쪽, 2012년 2월

저 자 소 개

김진수(학생회원)

1985년 서울대학교 전자계산기공학과 학사 졸업.
1996년 연세대학교 전자계산학과 석사 졸업.
2016년 전북대학교 정보보호대학원 박사과정.

<주관심분야: 개인정보보호, 빅데이터, 데이터품질>

최방호

1998년 한밭대학교 전자공학과 학사 졸업.
2008년 전북대학교 컴퓨터정보학과 석사 졸업.
2016년 전북대학교 정보보호대학원 박사과정.

<주관심분야 : 컴퓨터네트워크, 정보보호, 무선인터넷>

조기환(정회원)

1985년 전남대학교 계산통계학과 학사 졸업.
1987년 서울대학교 계산통계학과 석사 졸업.
1996년 Univ. of Newcastle 전산학과 박사.
1999년 전북대학교 컴퓨터공학교수.

<주관심분야 : 컴퓨터네트워크, 정보보호, 무선인터넷>