

개인정보보호의 신경향

- 프라이버시 중심 디자인(Privacy by Design)을 중심으로 -

최 해 선*

목 차

I. 서 론	2. EU에서 프라이버시 중심 디자인의 개정 논의
II. 프라이버시 중심 디자인(Privacy by Design)의 의의	3. 미국
1. 프라이버시 중심 디자인의 개념	4. OECD
2. 프라이버시 중심 디자인의 적용범위	5. 일본
3. 프라이버시 중심 디자인의 목표	IV. 개인정보보호 법제 현황 및 우리 법제도에의 시사점
4. 프라이버시 중심 디자인(Privacy by Design)의 7원칙	1. 현행 개인정보보호 법제 현황
III. 새로운 세계표준으로서의 프라이버시 중심 디자인(Privacy by Design)	2. 우리 개인정보보호 법제에의 시사점: 프라이버시 중심 디자인으로의 전환
1. 프라이버시 중심 디자인의 제안 경위	V. 결 론

I. 서 론

프라이버시가 권리로서 주장된 지 약 120년이 경과했다. 약 120년간 프라이버시는 크게 나눠서 2개의 세대가 시대를 구축해 왔다. 제1세대는 ‘보호받을 권리’¹⁾로 시작된 사생활의 보장에 관한 프라이버시권이며, 제2세대는 자기의 정보를 컨트롤할 수 있는 권리²⁾로 이해되는 프라이버시

* 건국대학교 법학연구소 책임연구원, 법학박사

1) Samuel D. Warren / Louis D. Brandeis, “The Right to Privacy”, 4 HARV. L. REV. (Harvard Law School, 1980), 194-196쪽.

2) ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (The Atheneum, 1967), 12쪽.
제1세대의 연장선상에 제2세대의 프라이버시를 명확하게 인정한 판결로서 Whalen

권이다. 소셜미디어의 보급이나 스마트폰의 이용확대로 인해 텍스트의 업로드, 위치정보, 행동이력추적 등의 다양한 정보가 매일 대량 생성되어 가고, 이러한 데이터를 활용한 비즈니스 서비스의 움직임도 활발해지고 있다. 그러나 데이터의 활용이 프라이버시 침해로 이어지는 사례가 자주 발생됨에 따라 프라이버시 보호의 올바른 방향정립이 요구되고 있다.

개인정보보호법이 시행된 후, 많은 기업은 개인정보보호법이 정의하는 ‘특정한 개인을 식별할 수 있는 정보’에 대해서 관리하고 있다. 그런데, 최근에는 여러 가지 데이터의 조합이나 분석에 의해 지금까지의 개인정보로는 간주되지 않았던 정보로도 쉽게 개인을 식별할 수 있게 되었다. 즉, 종래의 개인정보보호법에서는 대처할 수 없는 사태가 일어나고 있는 것이다. 개인정보를 보호한다는 것은 본래 개인의 프라이버시를 존중한다는 것이다. 정부의 정책적 차원이나 기업의 프라이버시정책 차원에서 개인정보를 보호하려는 어느 정도의 노력은 하고 있다고는 볼 수 있으나, 이용자의 입장에서는 그러한 노력이 실제로 개인정보가 제대로 보호받고 있다고는 잘 느껴지지 않는 것이 현실이다.

프라이버시가 침해되고 있는 예의 하나가 웹 검색·열람·구매나 이동의 이력정보를 수집·이용하여 본인의 선호에 맞춘 광고전송이나 서비스를 제공하는 ‘행동타겟팅’서비스의 남용이다. 본인에게 동의를 얻지 않고 여러 가지 이력정보가 수집되고 다른 사업자에게 이러한 여러 가지 정보가 제공되고 있다. 게다가 프로파일링은 소셜미디어 등에서 개인으로부터 발신되어진 정보를 수집해서 프로파일을 자동생성하고 판매하는 것인데, 판매된 정보는 기업의 채용활동이나 금융신용정보 등에 이용되는 것도 있다.

또한, 최근에는 빅 데이터³⁾의 분석이라는 새로운 기술을 통하여 개

v. Roe, 429 U.S. 589(1977)(宮下 紘, “プライバシー・個人情報保護の新世代”, 駿河台法学 25卷 1号(駿河台大学, 2011), 111-112쪽에서 재인용).

3) 빅 데이터는 기존에 대용량 자체를 의미하였으나, 점차 대용량 데이터를 이용하여 정보를 수집, 발굴, 분석하는 개념까지 확대되고 있으며, 정보의 성격은 개인화된

인의 일상에서 발생하는 막대한 양의 정보를 분석함으로써 기업의 영업 활동에 필요한 개인정보를 얻고, 이를 통하여 점차 정보화되어가는 소비자⁴⁾에 대한 영업활동을 강화하는 것도 경제계의 중요한 이슈로 떠오르고 있다.

그러면 프라이버시를 지키기 위해서는 무엇을 해야만 할까. 우선, 개인이 프라이버시에 대한 자각의식을 높이는 것이다. 젊은층이나 어린이의 프라이버시에 관한 지식의 향상도 필수적이다. 서비스사업자에는 자사의 서비스에 있어 프라이버시 침해가 발생할 가능성을 사전에 점검하고 위험을 최소화하는 ‘프라이버시 중심 디자인’(Privacy by Design)의 실시가 필요하다. 서비스의 제공시에는 사용자 개인이 프라이버시에 관해서 동의 등에 대한 판단을 하기 쉬운 구조를 도입할 필요도 있다. 더욱이 사업자의 프라이버시정책에 관해서는 제3자가 제대로 지키고 있는가를 감시하는 것도 필요하다.

II. 프라이버시 중심 디자인(Privacy by Design)의 의의

1. 프라이버시 중심 디자인의 개념

프라이버시 중심 디자인(Privacy by Design)은 Ann Cavoukian⁵⁾에 의

비정형 데이터(구조화된 데이터가 아닌 테스트, 음성, 영상, 소셜미디어) 등의 다양한 유형의 데이터를 말한다.

- 4) “소비자들이 과거에는 판매하는 물품을 구매하는 소극적인 지위에 있었지만, 생산에 참여하는 프로슈머(Prosumer)의 단계를 거쳐, 전시회의 큐레이터처럼 기존 제품을 꾸미고 다양하게 활용하는 편집형 소비자인 큐레이슈머(Curasumer)로 진화하고 있다고 한다.”(전경근, “개인정보의 활용범위에 관한 고찰”, 아주법학 제6권 제1호(아주대학교 법학연구소, 2012), 482쪽).

- 5) Ann Cavoukian, Ph. D., Information and Privacy Commissioner, Ontario, Canada.

해 주장된 개념으로서 프라이버시 정보를 취급하는 모든 측면에 있어 프라이버시 정보가 적절하게 취급되는 환경을 ‘사전적’(事前的)으로 만드는 것을 의미한다. ‘Privacy by Design’을 직역하면 ‘디자인(설계)에 근거한 프라이버시’라고 할 수 있을 것이나, 용어사용의 편이 및 적정성을 유념하여 ‘프라이버시 중심 디자인’⁶⁾이라고 번역하고 싶다.

Ann Cavoukian 박사는 프라이버시 중심 디자인의 개념은 네트워크에 연결된 대용량의 데이터시스템과 정보통신기술의 지속적인 성장과 그 영향을 체계적으로 설명하기 위하여 고안한 개념이라고 설명한다.⁷⁾

‘Privacy by Design’이라는 개념은 1990년대 중반에 탄생한 것이다. 개인정보를 확실히 보호하기 위해서는 법령 준수에 의지하는 것만으로는 불충분하다. 따라서 조직(정부) 또는 기업은 설계 단계에서 기술적으로 프라이버시를 보호하는 구조의 구축을 추진해 가는 것이 필요하다. 최초의 단계에서부터 확실히 프라이버시를 보호하는 것이 요구되고 있는 것이다. 즉, 개인정보보호를 위한 시스템을 ‘처음부터 구축한다’⁸⁾

6) ‘Privacy by Design’의 번역은 그 의미와 내용 및 범위를 고려하여 ‘프라이버시 중심 디자인’이라는 번역을 제안하며, 이 글에서는 의미의 정확한 전달을 위하여 영어표기와 한글표기를 동시에 사용하기로 한다.

7) Ann Cavoukian, *Privacy by Design—The 7 Foundational Principles* (Information and Privacy Commissioner, Ontario, Canada, 2011), 1쪽.

8) “각각의 조직은 프라이버시원칙에 특징적으로 관여하고 혁신적이고 현명하게, 그리고 제대로 된 정보관리를 해나가야 한다. 이 ‘Privacy by Design’의 생각은 중요한 조직적 적정평가절차(due diligence)의 실천이다. 그리고 불운한 사태가 일어났을 때에 필요한 시스템디자인의 변경이나 복구에 들어가는 막대한 비용을 줄일 수 있다. 제대로 프라이버시를 고려한다면 디자인의 설계가 보다 간단하고 신뢰할 수 있는 것으로, 효율이나 비용삭감이 크게 개선되는 것이다. 위험은 용이하게 정량화할 수 있는 것은 아니다. 이를 위해 ‘Privacy by Design’의 효과도, 그 측정이 어려운 경우가 있다. 거기에 중요한 것이 프라이버시의 문제에 상당한 주의를 기울이고 있다는 것을 보여주는 것이다. 적절하게 선견적인 행동을 취한 덕으로 프라이버시에 관한 사고가 발생하지 않는다면, 그 실적은 이익으로 이어진다. 프라이버시나 보안침해가 공표되는 빈도가 높았던 작년, 프라이버시보호책을 바르게 실시하고

는 것을 의미한다.

프라이버시 중심 디자인의 근간은 기술에 있다고 할 수 있으나, 그 개념의 적용은 점차 책임 있는 비즈니스 프로세스 및 물리적 스페이스나 네트워크 인프라스트럭처의 설계에도 미치는 것이다. 단순히 기술(특히, 정보시스템)만을 대상으로 삼는 것이 아니라, 비즈니스 프로세스 전반을 대상으로 한다. 그중에서도 Ann Cavoukian 박사는 구체적인 대상으로 다음의 세 가지를 제시한다. 첫째, IT 시스템(기술분야) 분야이며, 둘째로 책임 있는 비즈니스 관행, 셋째로 물리적 설계와 네트워크 인프라이다.⁹⁾

2. 프라이버시 중심 디자인의 적용범위

프라이버시 중심 디자인의 개념이 적용되는 범위는 어디까지인가에 대하여 살펴보기로 한다.

기술은 IT를 시작으로 여러 가지 기술분야가 해당되며, 비즈니스 관행은 사업활동을 생각하면 될 것이다. 또한, 물리설계에는 대상이 되는 서비스 그 자체에 관한 설계는 물론, 그 이용 시에 기반이 되는 네트워크 인프라 등도 포함된다.¹⁰⁾

어떠한 면에서는 이러한 내용을 단순한 발상으로 생각할지도 모르나, 이러한 광범위한 영역을 대상으로 하고 있는 것 자체가 중요한 지적을 포함하고 있음을 주의할 필요가 있다. 프라이버시 정보의 취급에 관한 종래의 프레임워크는 다수가 정보시스템의 정보이용을 염두에 두고 생각되어 왔다. 그러나 프라이버시 중심 디자인은 정보시스템을

있는 것을 보여주기 위해 점점 비밀주의나 태만을 피하지 않으면 안 된다.” 宮下 紘, 앞의 논문, 116쪽.

9) Ann Cavoukian, op. cit., 1쪽.

10) 堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC)編, プライバシー・バイ・デザイン (日経BP社, 2012, 10), 11쪽.

중요한 요소로 하면서 그 자체에 머물지 않는 비즈니스관행(사업활동), 또 네트워크 인프라 등의 정보시스템이 전제로 되는 환경에 대해서도 마찬가지로 의식해야만 한다는 것을 명확하게 하고 있다.¹¹⁾

[프라이버시의 개념]



〈그림 1〉 Privacy by Design의 적용범위

다음으로 ‘사전적’이라는 요소는 프라이버시정보를 이용하려고 하는 단계에서가 아닌, 그 이용이 예상되는 시점에서 대응을 구체화하는 필요성을 제시한다. 프라이버시 중심 디자인에서 ‘Design’이라는 단어가 사용되는 것도 그 때문이다. 즉, 프라이버시 정보를 ‘사용하는 단계에 이르러서 고려하는 것’이 아닌, ‘프라이버시 정보사용이 예정된 최초의 설계단계부터 포함시켜야 한다’라는 것이다.

다만, 프라이버시 중심 디자인의 ‘사전적’(事前的)인 의미에는 정보 시스템이나 비즈니스 프로세스의 설계단계의 의미도 내포되어 있다. 이러한 관점에서는 프라이버시 중심 디자인은 당해 시스템을 운용한

11) 堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC) 編, 위의 책, 11쪽.

후의 절차, 즉 이용자로부터 동의를 얻는 프로세스(opt-in)나 프라이버시 정보의 이용을 정지하는 프로세스(opt-out)¹²⁾와는 독립된 개념이다. 실제로 미국에서는 프라이버시 중심 디자인과 opt-out이 동일한 프라이버시 정보에 관한 규칙내에 공존하고 있다.¹³⁾

마지막으로, 프라이버시 중심 디자인의 위치나 성격을 정하고 있다. 프라이버시 중심 디자인에 관심을 가지는 사람들은 ‘이것이 법제도의 일종인가’라는 의문을 가지기도 하는데, 프라이버시 중심 디자인 자체는 특정의 정부나 기관에 의해 정해지는 것이 아닌, Ann Cavoukian 박사와 캐나다 온타리오주 Information & Privacy Commissioner 사무국(IPC)의 연구원이 제창한 프라이버시 정보취급에 관한 콘셉트 또는 지침이라고 할 수 있다.

현재는 프라이버시 중심 디자인의 콘셉트를 하나의 근거로 하여 일부 국가에서 법제화를 진행하고, 또한 기업이 프라이버시 정책의 지침으로 채용하고 있다. 그러한 의미에서는 오늘날에 있어서는 연성법¹⁴⁾의 일종으로 볼 수도 있을 것이다.¹⁵⁾

기술혁신도 이러한 패러다임의 변화를 받아들여 왔다. 특히, 프라이버시 중심 디자인의 검토부터 구체화된 1990년대 후반부터 정보통신분야를 시작으로 영상처리, 데이터베이스, 저장공간 등의 기술이 현저하

12) 옵트인(Opt-in)·옵트아웃(Opt-out) 방식은 불특정 다수인에게 무작위로 보내지는 스팸메일을 규제하는 방식으로, e-메일을 비롯해 전화나 팩스를 이용한 광고성 정보 전송 등에서도 적용된다.

‘옵트인’(Opt-in)이란 수신자의 사전 동의를 얻어야 메일을 발송할 수 있도록 하는 방식을 말한다. 반대로 수신자가 발송자에게 수신거부 의사를 밝혀야만 메일 발송이 안 되는 방식은 ‘옵트아웃’(Opt-out)이라고 부른다.

13) 堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC) 編, 위의 책, 12쪽.

14) 법적인 강제력이 없음에도 불구하고 현실의 경제사회에서 국가나 기업이 어떠한 구속감을 가지고 있는 규범으로 한 사회가 가진 윤리, 도덕, 종교적 교리 등과 같은 것으로 구체적으로 규제하지는 않으면서도 당위성을 수반하는 법이라고 볼 수 있다.

15) 堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC) 編, 위의 책, 13쪽.

게 고도화·대중화되었다. 이는 프라이버시 보호에 있어서도 기쁜 소식이 되어 간단한 조정으로 프라이버시 보호 수준을 높일 수 있게 되었다. 프라이버시 중심 디자인에서는 이러한 기술이 ‘교화가능한 기술’로 자리매김하고 있다.

정보시스템이나 비즈니스의 설계 단계부터 프라이버시를 의식하는 것으로 이용자에 대한 설명이 가능하게 되고, 이용자들의 이해나 신뢰를 받기 쉽게 된다. 이미 도입된 정보시스템에 있어서도 프라이버시 보호의 수준을 높이는 것이 가능하고, 결과적으로 이용자는 반드시 제공자의 사업을 지키게 된다. 이렇게 생각하면 프라이버시 중심 디자인이 보호하는 것은 단순히 이용자의 프라이버시 정보만이 아니라 기업활동 그 자체라는 이해도 가능할 것이다.¹⁶⁾

3. 프라이버시 중심 디자인의 목표

프라이버시 중심 디자인은 이용자(시민, 소비자, 고객)의 프라이버시 정보와 그 정보의 주체인 이용자의 프라이버시 자체를 지키고자 하는 것이다. 프라이버시 중심 디자인의 근원은 PETs(Privacy Enhancing Technologies: 프라이버시 보호 기술)¹⁷⁾이며, 기본적인 요건은 PETs의 개념이 진화해가는 과정에서 나타난 것이다. PETs는 정보시스템에 있어 개인의 프라이버시보호를 강화하는 기술의 총체라고 할 수 있다. 원래는 개인정보의 불필요 또는 불법적인 수집·이용 및 제공을 방지하

16) 堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC) 編, 위의 책, 13쪽.

17) PETs는 프라이버시 중심 디자인(Privacy by Design)을 실천하는 데에 필요한 기술이다. PETs는 개인정보가 불필요하게 또는 불법적으로 처리되지 않도록 하거나, 개인이 자신의 정보에 대해 제어를 강화하기 위해 톨이나 제어기능을 겸비한 정보시스템이다. 이 개념에는 정보시스템 아키텍처의 디자인도 포함된다(Kenny S. / Borking J., “The Value Privacy Engineering”, *The Journal of Information (Law and Technology; JILT 2002 (1))* <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/kenny/> 검색일 : 2012.12.29.

고, 개인이 자기정보결정권을 강화하기 위한 것이다. 구체적으로는 쿠키나 스파이웨어를 삭제하는 기술, 스팸메일의 필터 등을 그 예로 들 수 있다.

다만, 최근에는 서비스제공자 측이 ‘설계 시부터 고려’, ‘이용자의 피드백을 받아 기술의 고도화에 반영’을 중요시하고 보다 능동적으로 프라이버시보호에 대응이 가능한 툴이나 시스템환경을 요구하게 되었다.

다양한 서비스가 존재하는 가운데 이용자로부터 신뢰를 잃는 것은 사업을 존속시키는 데 치명상이 되기 때문이다. 실제로 대응을 어떻게 하느냐에 따라 사업은 물론 기업자체가 파탄에 이르는 것은 종종 볼 수 있다.

이러한 관점에서 ‘이용자 대 제공자’라고 하는 대립개념에 의한 제로섬 게임의 개념을 대신하여, ‘이용자를 보호하는 것으로 제공자도 지키는 것’이라는 포지티브섬(Positive-Sum)¹⁸⁾의 개념이 서서히 퍼졌다. 프라이버시정보의 보호를 이용자 자신에게 맡기는 것이 아니라 서비스제공자가 사전보호에 협력함으로써 제공자는 이용자로부터 신뢰를 얻을 수 있고, 사업상의 관계를 강화할 수 있다는 개념이 있는데 이러한 새로운 패러다임이 곧 프라이버시 중심 디자인의 기본 내용이다.

기술혁신도 이러한 패러다임의 변화를 반영하고 있다. 특히, 프라이버시 중심 디자인의 검토가 보다 구체화된 1990년대 후반부터 정보통신 분야를 시작으로 영상처리, 데이터베이스, 저장공간 등의 기술이 현저하게 고도화하고 더욱 대중화되었다. 이것은 프라이버시 보호에 있어서도 희소식이 되어 간단한 수리 또는 수정으로 프라이버시보호의 수준을 높일 수 있게 되었다. 프라이버시 중심 디자인에서는 이러한 기술은 ‘변환가능한 기술’이라고 규정하고 있다.

18) 포지티브섬이란 개인 또는 조직을 둘러싼 이해관계자들과의 협력을 통한 상생전략을 말한다. 시장의 가치를 증대시켜 구성원들이 서로 이득을 볼 수 있다는 장점이 있으며 제로섬과 대비되는 용어이다.

정보시스템이나 비즈니스의 설계단계부터 프라이버시를 의식하는 것으로 이용자에 대한 설명이 가능하게 되고, 이용자로부터의 이해나 신뢰를 얻기 쉽게 된다. 이미 도입된 정보시스템에 있어서도 프라이버시보호의 수준을 향상시키는 것이 가능하고, 그것이 결과적으로는 이용자만이 아니라 제공자의 사업도 보호할 수 있게 되는 것이다. 이는, 즉 프라이버시 중심 디자인이 지키는 것은 단순히 이용자의 프라이버시 정보뿐만 아니라, 기업 활동 그 자체이기도 하다는 것이다.¹⁹⁾

4. 프라이버시 중심 디자인의 7원칙

프라이버시 중심 디자인은 대규모로 네트워크화된 정보시스템에 있어 적절하게 프라이버시보호를 실현해가기 위한 개념이다. 정보통신기술이 급격히 발전되어 있는 현재, 이제 프라이버시정보의 안전은 단순히 규제를 하는 방식만으로는 보장될 수 없다. 조직 활동의 모든 면에서 표준적으로 보장할 필요가 있다. 프라이버시 보호에 관해 종래에는 프라이버시 강화기술(PETs)을 이용하는 것이 해결책으로 여겨져 왔지만, 현재에는 더욱 실질적인 접근이 필요하다는 인식이 있다. 예를 들면, PETs를 이용하는 것보다 편리함이 희생되는 것 없이(양자택일형의 제로섬 모델), 필요한 조건을 동시에 만족시키는 포지티브섬 모델을 지향하는 것이다. 그것이 PETs를 대신할 PETs Plus²⁰⁾의 기본적인 개념이 된다.²¹⁾

프라이버시 중심 디자인의 목적은 프라이버시를 확보하는 것과 자기

19) 堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC) 編, 앞의 책, 14쪽.

20) PETs Plus는 IT의 디자인과 그 이용에 ‘포지티브섬’ 패러다임을 추가하여 PETs를 개량한 것이다. 개인의 이익의 보호라는 의도를 더하여 그 목적을 달성하는 것을 목적으로 한다.

21) Ann Cavoukian, *Privacy by Design: Take the Challenge* (Information and Privacy Commissioner, Ontario, Canada, 2009), 24쪽.

정보결정권을 가지는 것, 조직을 위해 지속가능한 경쟁적 이점을 갖는 것, 그리고 이것은 7개의 기본원칙²²⁾에 의해 달성될 수 있다. 이 원칙은 모든 종류의 개인정보에 적용된다.²³⁾ 기본원칙의 7가지 내용을 살펴보면 다음과 같다.

기본원칙

- ① 사후적이 아닌 사전적, 구제책이 아닌 예방적인 것
프라이버시 중심 디자인은 수동적인 것이 아니라 선견적으로 대응하는 것이 특징이다. 프라이버시 침해가 발생하기 전에 그 침해를 예상하고 예방하는 것을 목적으로 한다. 이 때문에 사후가 아닌 사전에 작용하는 것이다.
- ② 프라이버시 보호는 초기설정에서 유효화되는 것
프라이버시 보호의 구조는 시스템에 최초부터 설계된다. 개인데이터는 개인이 아무것도 하지 않아도 그대로 보호된다. 개별적 조치는 불필요하다.
- ③ 프라이버시 보호의 구조가 시스템의 구조에 포함되는 것
프라이버시 보호의 구조는 IT시스템 및 비즈니스 관행의 디자인 및 구조에 포함된다. 사후적으로 부가기능으로서 추가하는 것이 아니다. 즉, 프라이버시 보호의 구조는 IT시스템 및 비즈니스 관행에 불가결한 중심적 기능이 된다.
- ④ 전기능적인 것과 제로섬이 아닌 포지티브섬
프라이버시 중심 디자인에서는 프라이버시 보호의 구조를 설계하는 것으로 편리함을 방해하는 등의 관계를 만드는 제로섬의

22) 堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC) 編, 앞의 책, 195-197쪽.

23) 특히, 의료정보나 재무데이터 등의 중요한 데이터에는 강력하게 적용되지 않으면 안 된다.

접근이 아닌, 모두 정당한 이익 및 목표를 거두는 포지티브섬 접근을 지향한다.

- ⑤ 데이터는 라이프사이클 전반에 걸쳐 보장될 것
프라이버시정보는 생성되는 단계부터 폐기되는 단계까지 보안이 철저하게 지켜져야 한다. 모든 데이터는 데이터 라이프 사이클관리하에 안전하게 보유하고 그 과정의 종료시에는 확실하게 폐기된다.
- ⑥ 프라이버시 보호의 구조와 운용은 가시화되어 투명성이 확보될 것
어떠한 비즈니스 관행 또는 기술이 관계되고 프라이버시 보호의 구조가 제대로 기능하는 것을 모든 관계자에 의해 보증한다. 이때, 시스템의 구성 및 기능은 이용자 및 제공자에게 항상 가시화되고 검증이 가능하여야 한다.
- ⑦ 이용자의 프라이버시를 최대한 존중하는 것
설계자 및 관리자에 대해 프라이버시 보호를 실현하기 위한 강력하고 표준적인 수단과 적절한 통지 및 권한부여를 간단하게 실현할 수 있도록 옵션수단을 제공하고, 이용자개인의 이익을 최대한 유지한다.

법적인 관점에서의 프라이버시 보호의 구조는 프라이버시의 권리침해에 대한 사후적인 구제가 주된 대응이 되어 왔다. 판례에서는 프라이버시 침해에 대한 불법행위책임을 묻는 사례가 일반적이며, 법령에서도 개인정보보호법은 개인정보취급 사업자의 의무에 위반한 경우의 제재를 사후적인 대응으로서 주무부처의 권한행사의 형태로 정하고 있는 것에 불과하다.

원칙	개요	실시 및 보급을 위한 방법
1. 사후(Reactive)대응이 아닌 사전(Proactive) 대응	프라이버시 침해사건이 일어날 때부터가 아닌, 발생을 방지하는 것을 목표로 함. 이를 위해서는 설계 및 개발단계에서 리스크를 파악해둘 필요가 있음.	개발자가 웹 애플리케이션에 대한 전형적인 프라이버시리스크를 파악하고, 설계나 개발을 함. 이용자는 DNT(Do Not Track)나 이력의 관리 등 프로바이더가 제공하는 기능을 파악하고 적절하게 설정할 수 있도록 함.
2. 프라이버시 보호는 표준	애플리케이션에서 개인정보가 자동적으로 지켜지는 것으로, 이용자에게 프라이버시보호를 위한 특별한 행동은 요구되지 않음.	DNT를 표준상태로 함.
3. 프라이버시 보호가 설계 단계에서 포함	프라이버시 보호의 구조가 애플리케이션의 설계나 아키텍처 안에 포함되고, 기본기능으로 제공	DNT도 광의적으로 파악하면 프라이버시보호기능이 프로바이더나 웹 애플리케이션에 설계단계에서 포함되어 있는 것을 의미함. Microsoft의 Security Development Lifecycle(SD L)이나 IBM의 Secure Engineering Framework(SEF)라는 보안제품개발의 수법이 있음. 프라이버시에 관해서도 이것과 같은 개발수법이 필요함
4. 제로섬(Zero-Sum)이 아닌 포지티브섬(Positive-Sum)	프라이버시보호가 다른 요건과 전환되는 것이 아닌, 이른바 win-win의 관계가 되도록 함.	필요최소한의 정보를 수집하고, 암호화나 익명화데이터보안기술을 이용한 애플리케이션을 개발
5. 라이프사이클 전체에 대한 개인정보 보호	정보의 생성, 유통, 이용, 삭제라는 전 과정에서 강력한 보안기준과 컨트롤이 필요	직접기술에 관련한 것뿐만 아닌, 이용자 프라이버시 관리장치이나 표준화활동을 통해서 개인정보를 end-to-end로 보호하기 위한 구조를 만드는 것이 필요
6. 가시화와 투명성	관련조직이 프라이버시에 관해서 보장하고 있는 조항과 방침을 명확화하고, 공개된 보안 및 프라이버시의 Best Practice를 준수함.	웹사이트 제공자가 프라이버시조항을 명확하게 알기 쉽게 제시하여, 이용자가 자신의 어떤 정보가 어떤 서비스에 사용되고 있는 가를 파악할 수 있도록 함.
7. 개인의 프라이버시를 존중함	안전 측에 옮겨진 디폴트, 적절한 통지, 이용자에게 친절한 옵션을 통해 개인중심을 중시하는 것을 설계자나 운용자에게 철저히 준수하도록 함.	설계자나 운용자가 프라이버시 보호를 기능요건이라고 하여 알기 쉽게 GUI 등을 사용하여 IT에 대해 잘 알지 못하는 이용자가 안심하고 사용하도록 그 방법을 제공함.

출전: 堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC)編, プライバシー・バイ・デザイン (日経BP社, 2012. 10), 197쪽.

사후적인 대응에 그치지 않는 개인정보의 적정한 취급과 보호를 달성하기 위해 기업은 위험관리의 관점에서 경영시스템 등을 활용하는 것으로 사전에 필요한 대책을 세워야 한다.

Ⅲ. 새로운 세계표준으로서의 프라이버시 중심 디자인(Privacy by Design)

1. 프라이버시 중심 디자인의 제안 경위

프라이버시 중심 디자인(Privacy by Design)의 개념은 최근 수년간 급속하게 논의가 활발해지고 있다. 예를 들면, 2010년 10월에 개최된 ‘제32회 국제개인정보보호기구회의²⁴⁾’에서는 프라이버시 중심 디자인(Privacy by Design)을 필수적 요소로 인식하는 것으로 결의 되었다.²⁵⁾ 국제개인정보보호기구회의는 세계의 정보보호·프라이버시 보고 기관이 매년 데이터보호나 프라이버시 보호에 관한 문제를 검토하는 국제 회의이다. 국제개인정보보호기구회의에서 결의된 것은 프라이버시 중심 디자인이 ‘새로운 국제 프라이버시 표준’(new global privacy standard)으로서 인식된 것이다. 실제로 이 회의에서 결의된 것에서도 프라이버

24) ICDPC(International Conference of Data Protection and Privacy Commissioner).

25) ‘제32회 데이터보호·프라이버시·Commissioner 국제회의 결의’

1. Privacy by Design은 기본적인 프라이버시 보호의 필수 요소로서 인식한다.
2. 조직의 위반상태로서의 프라이버시를 확립시키는 지침인 Privacy by Design의 기본원칙의 채용을 장려한다.
3. 데이터보호·프라이버시·Commissioner에 대해서 이하의 사항을 권유한다.
 - a. 자료의 배포, 교육, 개인의 지원운동 등을 통해 가능한 한 널리 Privacy by Design을 촉진한다.
 - b. 각각의 관할구역내에서 프라이버시 정책 제안과 입법에 있어 Privacy by Design의 기본원칙을 반영한다.
 - c. 적극적으로 Privacy by Design의 조사를 장려한다.
 - d. 국제프라이버시의 날(1월 28일)에 행해지는 행사의 의제로 Privacy by Design개념의 추가를 검토한다.
 - e. 베스트 프랙티스를 제공한다는 관점에서 필요에 의해 각각의 관할구역 내에서 행해진 Privacy by Design 활동이나 구상에 대해서 ‘제33회 데이터보호·프라이버시·Commissioner 국제회의’에서 보고한다.

시 중심 디자인의 기본원칙의 채용을 장려하고 있다. 이러한 국제적인 프라이버시에 관한 검토구조의 추진과 호응으로 세계 각국에서도 프라이버시 중심 디자인의 채용이 진행되고 있다. 이에 관하여 유럽과 미국, 일본의 경우를 살펴보기로 한다.

2. EU에서 프라이버시 중심 디자인의 개정 논의

2.1 논의 과정

유럽에서도 프라이버시 중심 디자인의 채용이 진행되고 있다. 유럽 연합(EU)은 현재 1995년에 제정된 ‘개인정보보호 관리 지침’²⁶⁾을 대폭 개정한 ‘일반정보보호규칙’(General Data Protection Regulation)의 검토를 하고 있다. 이 규칙의 전문에는 ‘관리자는 특히 정보보호에 기한 디자인 및 정보보호에 기본원칙에 합치하는 내부정책을 채택하고 이와 관련한 원칙에 맞는 조치를 실시하지 않으면 안 된다’고 하고 있다. 이 조문 중에서도 제23조와 제30조²⁷⁾에서 프라이버시 중심 디자인 및 그 개념을 전제로 한 문언이 포함되어 있다. 이 규제의 검토를 진행한

26) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

27) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) of the European Commission of 25 January 1995. Article 23 sets out the obligations of the controller arising from the principles of data protection by design and by default. Article 30 obliges the controller and the processor to implement appropriate measures for the security of processing, based on Article 17(1) of Directive 95/46/EC, extending that obligation to processors, irrespective of the contract with the controller.

유럽위원회의 정보보호관찰관, 정보보호에 관한 제29조 작업반은 이전부터 프라이버시 중심 디자인의 개념에 대하여 동의하는 의견을 표명하고 있었다. 이 규칙안의 검토를 살펴보면 유럽에 있어서도 프라이버시 중심 디자인은 프라이버시를 검토하면서 기초적인 개념의 하나로 위치하고 있음을 알 수 있다.²⁸⁾

2010년 11월 4일 유럽연합집행위원회(EC)는 ‘EU 개인정보보호전략에 대한 전략커뮤니케이션’²⁹⁾을 채택하였다. 이 발표의 내용에서 주목

28) 堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC) 編, 앞의 책, 20쪽.

29) ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS’(A comprehensive approach on personal data protection in the European Union)

1. NEW CHALLENGES FOR THE PROTECTION OF PERSONAL DATA 개인정보 보호에 대한 새로운 도전
2. KEY OBJECTIVES OF THE COMPREHENSIVE APPROACH ON DATA PROTECTION 정보보호에 관한 포괄적 어프로치의 주요 목적
 - 2.1. Strengthening individuals’ rights 개인의 권리 강화
 - 2.1.1. Ensuring appropriate protection for individuals in all circumstances
사전에 개인의 적절한 보호의 확보
 - 2.1.2. Increasing transparency for data subjects 정보 주체에 대한 투명성의 증진
 - 2.1.3. Enhancing control over one’s own data 자기정보에 대한 컨트롤의 향상
 - 2.1.4. Raising awareness 의식 계발
 - 2.1.5. Ensuring informed and free consent 정보에 근거한 자유로운 동의의 확보
 - 2.1.6. Protecting sensitive data 민감한 정보의 보호
 - 2.1.7. Making remedies and sanctions more effective 구제 및 제재의 효율화 향상
 - 2.2. Enhancing the internal market dimension 역내 시장 특성의 강화
 - 2.2.1. Increasing legal certainty and providing a level playing field for data controllers 법적 실효성의 증진 및 정보관리자에 대한 공평한 경쟁 제공
 - 2.2.2. Reducing the administrative burden 관리상 부담의 경감
 - 2.2.3. Clarifying the rules on applicable law and Member States’

되는 점은 프라이버시 중심 디자인(Privacy by Design)의 개념이 반영되어 있다는 것이다. 어떤 의미에서 언급되어 있는지를 살펴보기 위해 전체 구성을 살펴보면 다음과 같다.

이 내용 중 ‘2.2.4 정보관리자의 책임 강화’에서는 1) 정보보호 관리자를 둘 것을 의무로 하는 것, 2) 민감한 정보를 취급하는 정보관리자에 대해서 법적인 틀 안에서 개인정보영향평가(DPIA)의 실시를 의무로 할 것을 언급하고 있다. 3) 프라이버시 강화 기술(PETs)의 이용 및 프라이버시 중심 디자인(Privacy by Design)의 개념 구체적 실현을 위한 새로운 촉진으로서 프라이버시 중심 디자인(Privacy by Design)을 다루고 있다.

2.2 주요 내용

2012년 1월 25일에 개인정보보호규정(안)(Proposal for a General Data Protection Regulation)³⁰⁾이 발표되었다.

responsibility 준거법에 관한 제원칙 및 가맹국의 책임 명확화

2.2.4. Enhancing data controllers' responsibility 정보관리자의 책임 강화

2.2.5. Encouraging self-regulatory initiatives and exploring EU certification schemes 자율규제의 장려 및 EU인증제도의 심화

2.3. Revising the data protection rules in the area of police and judicial cooperation in criminal matters 형사사건에 있어 경찰·사법협력분야 정보보호 제원칙의 개정

2.4. The global dimension of data protection 정보보호에 관한 세계적인 관점

2.4.1. Clarifying and simplifying the rules for international data transfers 국제정보이전을 위한 제원칙의 명확화 및 단순화

2.4.2. Promoting universal principles 보편적 원칙의 촉진

2.5. A stronger institutional arrangement for better enforcement of data protection rules 정보보호규칙의 보다 나은 집행을 위한 제도정비 강화

3. CONVLUSION: THE WAY FORWARD 장래의 방향성

30) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF

이 규정(안)과 현행 EU개인정보보호지침의 형식적인 면에서의 다른 점은 현행 EU개인정보보호지침은 지침(directive)의 형식인 것에 비해 새로운 안은 규정(regulation)의 형식이다. 지침은 구속력을 가진 회원국의 국내법의 제정에 의해 효력이 있게 되는 반면, 규정은 가맹국에 직접 적용된다. EU의 지침하에서는 회원국간의 보호수준에 차이가 있어서 다국적기업이 국가마다 다른 대응을 하여야 하며, 이는 기업활동의 방해요소가 되고 있다. 규정에 대한 회원국의 보호수준은 균등하다. 새로운 규정(안)을 보면 개인정보보호에 관한 현재 EU의 개인정보보호규정(Directive 95/46/EC)은 개인정보보호에 대한 기본적 권리를 보장하는 것과 회원국 간의 개인정보의 자유로운 유통을 보장하는 것, 이 두 개의 목적을 염두에 두고 1995년에 채택된 것이다.

새로운 규정(안)에서는 기존 지침의 채택(1995년 10월 24일)에서 현재에 이르는 동안 기술의 급속한 발전에 대한 배경을 설명하고 있다. 간략히 서술하면 급속한 기술발전은 개인정보보호에 있어 새로운 과제를 가져왔다. 정보의 공유 및 수집의 방식은 급속히 확대되었고, 기술의 발전에 의해 민간기업 및 공공기관이 업무수행을 위해 개인정보를 이용하게 되었다. 개인정보는 공공연하게 세계적 규모로 이용된다. 기술은 경제와 사회생활 모두를 변화시키고 있다. 온라인 환경에 대한 신뢰 구축은 경제발전의 열쇠이다. 신뢰가 결여되면 소비자는 온라인상에서 물건을 사거나 새로운 서비스를 선택하는 것을 망설이게 된다. 이것은 새로운 기술의 이용·발전을 저해할 위협이 있다. 따라서 개인정보보호는 ‘유럽디지털아젠다’(Digital Agenda for Europe) 및 ‘유럽2020발전전략’(Europe 2020 Strategy)에서도 중심적 역할을 차지하고 있다.

THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data(General Data Protection Regulation) <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>, 검색일 : 2012.12.30.

이 규정(안)은 ‘일반 개인정보보호규정’(General Data Protection)과 ‘형사범죄의 방지, 수사, 탐지 또는 소추·형벌의 집행을 목적으로 하여 관할기관의 개인정보보호 및 당해 정보의 자유로운 이동에 관한 유럽의 회 및 이사회의 지침’ 제안으로 구성되어 있다.

2.3 프라이버시 중심 디자인 관련 규정

이 규정(안)에서 프라이버시 중심 디자인(Privacy by Design)에 관한 규정을 살펴보면 ‘제4장 관리자 및 프로세서’(Chapter IV Controller and Processor)의 ‘제2절 정보보안’(Section 2 Data Security)에서 ‘제30조 보안 취급’(Article 30 Security of processing)에서 프라이버시 중심 디자인(Privacy by Design)의 내용을 포함시켜야 한다는 내용이 있다.

3. 미국

미국에서도 프라이버시 중심 디자인의 개념에 대하여 그 논의가 활발해지고 있다.

미국 연방거래위원회(FTC)는 2010년 12월 2일에 발표한 ‘급속한 변화시대의 소비자프라이버시보호: 비즈니스 및 정책입안자를 위한 구조의 제안’(Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers)³¹⁾이라는 보고서를 발표했다. 이 보고서의 서두에 ‘프라이버시 중심 디자인’에 대한 언급이 있다. “이 보고서의 프레임워크는 특정의 소비자, 컴퓨터 또는 그 외의 디바이스와 합리적으로 링크하는 소비자의 정보를 수집·이용하는 모든 사업자에게 적용된다”라고 하며, 다음의 세 가지 원칙을 명시하고 있다.

31) <<http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>>, 검색일 : 2012.12.30.

- ① 프라이버시 중심 디자인(Privacy by Design)
- ② 선택의 단순화
- ③ 투명성의 확보

또한, 보고서에서는 “사업자는 그 조직 전체적으로 제품 및 서비스 개발의 사전단계에서 소비자프라이버시를 촉진하지 않으면 안 된다”라고 하며, 프라이버시 중심 디자인을 다음과 같이 설명하고 있다.

- 사업자는 정보보안·합리적인 수집 제한·건전한 보존업무 및 정보의 정확성과 같은 실질적인 프라이버시 보호책을 그 업무 내용에 포함시키지 않으면 안 된다.
- 사업자는 그 제품 및 서비스의 전체과정(life cycle)을 통해 포괄적인 정보관리절차를 정비하지 않으면 안 된다.

또한 FTC는 2012년 3월에 ‘급격한 변화시대의 소비자프라이버시보호: 비즈니스 및 정책입안자를 위한 권고’(Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Business and Policymakers)³²⁾를 발표하였다. FTC의 권고 내용을 살펴보면, 최종의 프라이버시 프레임워크는 소비자의 정보를 수집하고 이용하는 사업자에 의해 베스트프랙티스를 명확하게 명시하는 것을 목적으로 하고 있다. 이는 사업자가 내부의 프라이버시 및 정보보안의 업무를 행하기 위해 처리공정 및 시스템을 정비할 때, 유의한 것이 될 수 있다. 최종 프라이버시프레임워크는 연방의회가 프라이버시보호 입법을 할 때를 대비하는 것을 목적으로도 하고 있다. 이 내용에는 현행법의 요건을 넘는 부분이 있는데 이는 FTC가 현재 집행하고 있는 현행법에 기준한 집행조치 또는 규제의 기준으로서의 역할을 의도하고 있지는 않다.

보고서에서 최종 목적으로 하는 그 적용범위에 대하여 다음과 같이

32) <<http://ftc.gov/opa/2012/03/privacyframework.shtm>>, 검색일 : 2012.12.23.
 <<http://ftc.gov/os/2012/03/120326privacyreport.pdf>>, 검색일 : 2012.12.23.

한정하고 있다.

“이 프레임워크는 특정의 소비자, 컴퓨터 또는 그 외의 디바이스와 합리적으로 링크로 인해 얻는 정보를 수집, 이용하는 모든 사업자에게 적용된다. 다만, 사업자가 연간 5000명보다 적은 소비자로부터 정보를 수집하고 있을 뿐, 그 정보를 제3자와 공유하지 않는 경우에는 적용하지 않는다.”

예비 보고서³³⁾와 표현이 조금 다를 뿐이나 다음과 같이 프라이버시 중심 디자인(Privacy by Design)은 주요 내용³⁴⁾으로 다루어지고 있다. 특히, 프라이버시 중심 디자인에 관한 내용을 살펴보면 다음과 같다.

기본원칙으로서 “사업자는 그 조직전체에서 그 제품 및 서비스 개발의 전단계에서 소비자프라이버시를 촉진하여야 한다”는 것을 강조하고 있으며, 이에 대한 실체적 원칙으로 “사업자는 데이터보안, 합리적인 수집제한, 건전한 보존·처리업무 및 데이터의 정확성과 같은 실체적인 프라이버시 보호를 그 사업의 내용에 포함시켜야 한다”고 하고 있다. 또한, 이러한 원칙들을 보다 구체화하기 위한 절차적 원칙으로서 “사업자는 그 제품 및 서비스의 라이프사이클을 통해 포괄적인 데이터관리절차를 정비하여야 한다”는 것을 강조하였다.

4. OECD

OECD는 프라이버시·개인정보보호의 분야에서는 1980년 9월 23일

33) FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers <<http://www.ftc.gov/opa/2010/12/privacyreport.shtm>>, 검색일 : 2012.12.23.

<<http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>>, 검색일 : 2012.12.23.

34) 본 보고서는 프라이버시 보호를 위하여 다음의 세 항목이 반드시 지켜져야 한다는 것을 주요 내용으로 서술하고 있다. ① 프라이버시 중심 디자인(Privacy by Design) ② 단순화된 소비자의 선택 ③ 투명성

에 ‘프라이버시보호 가이드라인’³⁵⁾을 채택하였다.

이 가이드라인은 채택된 지 30년이 경과한 2010년에 그 동안의 개정 논의 등에 대한 내용을 정리하여 ‘OECD 프라이버시 가이드라인 그 후 30년’³⁶⁾이라는 보고서가 발행되었다. 이 보고서의 내용에서는 각각의 요소에 프라이버시 중심 디자인의 개념이 언급되고 있다. 예를 들면, 보고서의 내용 중 “Chapter 2의 프라이버시에 관한 현상의 전개”에서 7가지의 중요 요소를 거론하고 있는데, 그중 7번째³⁷⁾에서 “프라이버시 가이드라인 이후의 중요한 혁신적인 발전의 예로 프라이버시 중심 디자인”을 거론하고 있다. 또한 “현재의 프라이버시 접근의 검토와 과제”에서 “정보관리와 프라이버시 중심디자인”을 거론하고 있다. 제4장의 “프라이버시 보호와 개인정보의 국제유통에 대한 가이드라인에 관한 이사회 권고의 검토를 위한 자문사항”³⁸⁾에서 프라이버시 중심 디자인을 개발하고 실시와 조직을 통해 관여하는 노력을 할 것을 언급하고 있다.

35) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data <<http://www.oecd.org/internet/interneteconomy/oecdguidelinesonthe protection of privacy and transborder flows of personal data.htm>>, 검색일 : 2012.12.30.

36) Thirty Years After the OECD Privacy Guidelines <<http://www.oecd.org/sti/interneteconomy/49710223.pdf>>, 검색일 : 2012.12.23.

37) OECD, *Thirty Years After the OECD Privacy Guidelines* (OECD, 2011), 13쪽.
7. There is interest by the global privacy community and commitment within international organisations, governments, and privacy enforcement authorities to addressing current challenges.

Important and innovative developments since the privacy guidelines—for example, the emergence of a privacy profession, privacy by design, privacy impact assessments, and data breach notification—offer encouraging signs of a broad multi-stakeholder commitment on the part of privacy advocates, the technical community, businesses and governments to protecting privacy.

38) OECD, *Thirty Years After the OECD Privacy Guidelines* (OECD, 2011), 93쪽.

5. 일본

일본 총무성은 2012년 8월에 공표한 ‘스마트폰 프라이버시 이니시아티브’³⁹⁾라는 보고서에서 그 기본원칙의 하나로써 프라이버시 중심 디자인 개념을 채택하였다. 일본 정부가 공표한 지침 중에서 프라이버시 중심 디자인 자체를 거론한 것은 이것이 처음이다.

스마트폰이 급속하게 보급되는 현상에서 일부 스마트폰 애플리케이션에 의해 프라이버시 침해 사건이 다발하고 있다. 한편으로는, 애플리케이션 개발자나 플랫폼사업자 측의 프라이버시 보호에 관한 의식은 충분하다고 말할 수는 없는 실정이다.

이러한 상황으로 인해 총무성이 2012년 1월에 ‘이용자의 관점을 감안한 ICT서비스에 관계된 제반문제에 관한 연구회’ 내에 ‘스마트폰을 경유한 이용자정보의 취급에 관한 워킹그룹’을 설치하여 이후 워킹그룹에서는 프라이버시 정보를 포함하여 이용자정보가 안심·안전하게 활용되고 편리한 서비스 제공으로 이어지도록 제외국의 동향을 포함한 현상과 과제를 파악하고, 이용자정보의 취급과 대응에 대해 검토를 거듭하였다.⁴⁰⁾

‘스마트폰 프라이버시 이니시아티브’의 내용을 살펴보면 다음과 같다.

이 보고서에서는 이용자를 보호함과 동시에 스마트폰 어플리케이션 비즈니스를 건전하게 발전시켜나가기 위해서 시켜야 할 항목으로 ‘업체단체의 자주적인 가이드라인 작성을 위한 지침’을 정하고 있다. 내용면에서는 크게 두 가지의 주요점이 있다. 첫째, 애플리케이션 제공자등에게 프라이버시정책의 작성을 요구한 점 둘째, 전화번호부와 단말 ID 등 프라이버시성이 높은 이용자정보의 취급에 대해서 구체적인 제시를

39) スマートフォン プライバシー イニシアティブ—利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション-, <http://www.soumu.go.jp/main_content/000171225.pdf>, 검색일 : 2012.12.30.

40) <http://www.soumu.go.jp/menu_sosiki/kenkyu/11454.html>, 검색일 : 2012.12.30.

하고 있는 점이다.⁴¹⁾

또한, 이 지침의 실효성을 높이기 위한 제안도 포함되어 있는데, 그 중 하나가 애플리케이션 지침에의 대응을 체크하는 제3자기관의 정비이다. “민간주도로 정립되는 것이 바람직하다.”라고 서술하고 있으며, 청소년보호를 위해 모바일사이트의 심사를 진행하는 모바일콘텐츠심사·운용감시기구(EMA: Content Evaluation and Monitoring Association)와 같은 구조를 요구하고 있다.

이외에 스마트폰 애플리케이션은 국가를 넘어 유통되고 이러한 경우에 대한 배려가 필요하다는 것에 대해서도 언급하고 있다. 구체적으로는 국제적인 정책협의의 장에서 휴대전화에 대한 논의의 필요성도 강조하고 있다.⁴²⁾

‘스마트폰 프라이버시 이니시아티브’에서 주목되는 것은 그 내용에 프라이버시 중심 디자인이 명시적으로 도입되어 있는 점이다. 프레임워크의 일부로서만이 아니라, ‘스마트폰 프라이버시 이니시아티브’의 기본원칙의 하나로서 받아들여지고 있다.

‘스마트폰 프라이버시 이니시아티브’에 프라이버시 중심 디자인이 도입된 것은 해외의 법제도나 프라이버시 보호의 프레임워크를 검토한 결과이다. 해당분야에서 전례가 있는 것부터 도입이 용이하다고 판단된 것도 강하게 영향을 미쳤다. 예를 들면, 유럽을 시작으로 세계의 통신사업자가 가입하는 업계단체 세계이동통신사업자협회(GSMA)가 2011년 1월에 발표한 ‘모바일 프라이버시 원칙’(Mobile Privacy Principle)에서는 GSMA에 가입하는 통신사업자가 프라이버시에 관한 정책이나 대응을 검토할 때, 기본자료가 되는 지침을 정하고 있다. 이 원칙의 기본적인 구조가 프라이버시 중심 디자인에 근거하고 있는 것은 해당 문서에서도 명시되어 있다. 이 근거의 기준의 배경이 되는 것이 2010년 12월에 발표

41) 堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC) 編, 앞의 책, 200쪽.

42) 堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC) 編, 위의 책, 201쪽.

된 FTC보고서(Staff Report)⁴³⁾이다. 이용자 프라이버시의 보호를 위해 소비자에게 선택사항을 제공하고 투명성의 증진, 모바일을 포함한 주요 분야에의 적용 등에 대한 내용이 원칙에 명기되어있고, 이 원칙은 바로 프라이버시 중심 디자인에 근거하고 있는 것이다. 이러한 경위가 같은 모바일분야를 목표로 한 스마트폰 프라이버시 이니시아티브에서 프라이버시 중심 디자인을 적용하는 것으로 이어진 것이다.

게다가 이를 뒷받침한 것이 2012년 1월에 공표된 ‘EU개인정보보호 규칙안’이다. 여기에서도 프라이버시 중심 디자인이 명시적으로 포함되어 있다. 이러한 외국의 동향에 따라 일본은 그 기준으로 무엇이 필요 한가를 검토한 결과 ‘스마트폰 프라이버시 이니시아티브’에서 기본원칙의 6번째에 “Privacy by Design”을 용어 그대로 채택하고 있다.

IV. 개인정보보호 법제 현황 및 우리 법제도에의 시사점

1. 현행 개인정보보호 법제 현황

현행 개인정보보호법은 2011년 3월 29일 제정되어 2012년 3월 30일부로 시행되고 있다. 이 법률은 공공분야와 민간분야에서의 개인정보보호에 관한 사항을 통합하는 내용으로 제정되었다.

개인정보보호법에서는 정보주체의 권리, 대통령 소속의 개인정보보호위원회, 개인정보의 처리, 개인정보의 처리제한(민감정보·고유식별정보, 영상정보처리기기), 개인정보의 안전관리(개인정보파일의 등록

43) FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers.

〈<http://www.ftc.gov/opa/2010/12/privacyreport.shtm>〉, 검색일 : 2012.12.30.

〈<http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>〉, 검색일 : 2012.12.30.

및 공개 개인정보영향평가), 정보주체의 권리보장, 권익구제(개인정보 분쟁조정위원회, 개인정보 단체소송) 등이 주요내용으로 되어 있다.

개인정보보호법에서는 개인정보침해의 위험요인을 분석하고 이를 사전에 제거하고 개인정보의 유출 및 오·남용의 피해를 사전예방 하고자 하는 목적으로 개인정보 영향평가제도에 대하여 정하고 있다.

개인정보 영향평가의 대상은 1. 구축·운용 또는 변경하려는 개인정보파일로서 5만 명 이상의 정보주체에 관한 법 제23조에 따른 민감정보(이하 “민감정보”라 한다) 또는 고유식별정보의 처리가 수반되는 개인정보 파일, 2. 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만 명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일, 3. 구축·운용 또는 변경하려는 개인정보파일로서 100만 명 이상의 정보주체에 관한 개인정보파일 등이다(법시행령 제35조). 개인정보 영향평가를 담당할 업체선정 및 시행이 본격화된 가운데, 최근에는 관련 고시를 정하여 개인정보관리자의 교육에 관한 사항까지 제정되기에 이르렀다.

한편, 영국의 개인정보보호기구가 발표한 보고서⁴⁴⁾에서는 프라이버시 중심 디자인의 실시에 관하여 다음의 사항을 정해야 하는 것으로 명시하고 있다.

① 프라이버시 보호를 위한 경영책임, ② 시스템의 라이프사이클 전반에 대한 개인정보영향평가, ③ 부서를 횡단하여 행해지는 데이터공유에 관한 기준, ④ 구체적(현실적)인 프라이버시 기준, ⑤ 현재 및 장래에 대한 프라이버시 보호 강화 기술 활용을 위한 검토의 촉진, ⑥ 엄격한 허용 및 집행체제의 확립, 이상 6가지이다.

프라이버시 보호를 위한 경영책임, 부서를 횡단하여 행해지는 데이터 공유기준, 구체적인 프라이버시 기준, 엄격한 허용 및 집행체제의 확립에 관한 것은 개인정보보호의 매니지먼트시스템을 만드는 데 있어

44) UK Information Commissioner's Office, Privacy by Design, 26th November 2008.

서 이전부터 실현되어온 것이다.

여기에서의 시스템의 라이프사이클 전반에 대한 개인정보영향평가와 현재 및 장래에 대한 프라이버시 강화 기술 활용 검토는 프라이버시 중심 디자인의 사상이 반영된 것이라고 말할 수 있을 것이다. 이러한 관점에서 프라이버시 중심 디자인과 개인정보영향평가 및 PETs는 각각 개별적으로 소개되고 검토되는 경우가 많지만, 프라이버시 중심 디자인과의 관계에 있어서는 사전에 실시되는 개인정보영향평가의 결과를 받아서 PETs가 검토되고, 달성되는 프라이버시보호의 구조가 프라이버시 중심 디자인 개념이라고 말할 수 있을 것이다.⁴⁵⁾ 그러나 우리의 개인정보보호법제는 법개정을 통해 이전보다 강화된 사전적 개인정보보호체계를 갖추었다고는 평가할 수 있을지 모르나, 다른 선진 외국에 비하여 법의 체계 및 구체적 개인정보보호책이 법에 의해 충실히 구현되고 있다고 평가하기는 힘들다.

2. 우리 개인정보보호 법제에의 시사점: 프라이버시 중심 디자인으로의 전환

현행 개인정보보호법은 여러 가지 맥락에서 문제제기라든지 논란이 존재하고 있다. 예컨대 개인정보보호법에 대한 이해의 부족,⁴⁶⁾ 새로운 개인정보 보호 처리비용의 증가에 따른 부담감 등도 그중 하나이다.⁴⁷⁾

개인정보 보호는 헌법상의 기본권인 개인정보통제권을 실현하기 위

45) 堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC) 編, 앞의 책, 55쪽.

46) 특히, 개인정보보호법에 대한 이해의 부족에 대해서는 손형섭, “개인정보 보호법의 특징과 앞으로의 방향—업계의 반응에 대한 몇 가지 대안을 중심으로—”, 언론과 법 제11권 제1호(한국언론법학회, 2012), 104-109쪽 참조(황성기, “개인정보 보호와 다른 헌법적 가치의 조화”, 경제규제와 법 제5권 제2호(서울대학교 공익산업법센터, 2012), 20쪽에서 재인용).

47) 황성기, 위의 논문, 20쪽.

한 것으로 정부와 업계는 물론 모든 국민의 노력으로 보호할 수 있는 기본권이다. 나아가 개인정보 보호는 정보사회의 지속적인 순발전을 위해 중요한 기반 원칙이기도 하다. 개인정보를 보호하는 것은 정보사회에서 사는 우리 모두의 인격권을 보호하는 기반이 된다.⁴⁸⁾

프라이버시 중심 디자인(Privacy by Design)이라는 원칙으로 보호하고자 하는 것은 한마디로 이용자(시민, 소비자, 고객)의 프라이버시 정보이며, 또한 그 정보의 주체인 이용자의 프라이버시 자체이다. 이것은 프라이버시 중심 디자인의 근원이 PETs(Privacy Enhancing Technologies: 프라이버시 보호 기술)이며, 기본적인 요건은 PETs의 개념이 진화해 가는 과정에서 정리되었다는 경위는 분명하다.

2011년 2월에 세계경제포럼(World Economy Forum, 다보스포럼)에서 ‘개인정보: 새로운 자산가치의 출현’⁴⁹⁾이 발표되었는데, “전선에 전자를 통하게 하여 전력산업이 되고, 전화에 패킷을 흐르게 하여 인터넷이 되었다. 다음은 개인이 생산하는 정보(개인정보)를 구조화하여 유통되고, 새로운 사업이 생긴다. 이것이 퍼스널 데이터 에코시스템(Personal Data Ecosystem)이며, 그 근간을 이루는 것이 신뢰 프레임워크(Trust Framework)이다”라는 내용이다. 그리고 그 신뢰의 프레임워크로서 기획단계부터 프라이버시 보호의 설계를 하는 것(프라이버시 중심 디자인)이나 가시성과 투명성 등을 거론하고 있다.

또한, 2011년 5월에 미국 맥킨지가 ‘Big Data’라는 보고서를 발표하고, 큰 사회적 효용을 발생시키는 공적인 정보가 다양하게 존재하는 것을 지적했다. 그리고 그 다음 달인 6월에 개최된 OECD의 정보보안·프라이버시작업반(WPISP: Working Party on Information Security and Privacy)에서는 “정보보안과 프라이버시의 경제학”(Economics of Information

48) 손형섭, 앞의 논문, 109쪽.

49) <<http://www.weforum.org/reports/personal-data-emergence-new-asset-class>>, 검색일 : 2012.12.30.

Security and Privacy)의 섹션에서 개인정보의 경제적 가치의 계산이 발표되었다.⁵⁰⁾

프라이버시 중심 디자인은 이러한 이론적 가치를 설계단계에서부터 설치하여 개인정보보호를 실현하고자 하는 것이다. 이러한 국제적인 보호의무에 대한 개념발상의 전환을 우리도 재인식할 필요성이 있다고 생각된다. 또한, 일본에서는 개인정보보호법이 시행된 이후에도 크고 작은 개인정보 유출사건이 계속되어 법의 기능적 한계를 보이기도 하였다. 개인정보의 보호를 위해서는 개인정보 보호 및 프라이버시 보호를 위한 법적인 제도정비는 물론 기술적 보호시스템의 정비도 중요하다.⁵¹⁾

한편, 앞서 언급한 영국 ICO의 보고서에 “The privacy by design ecosystem”⁵²⁾이라는 내용의 소개가 있는데, 이것은 ‘전분야에서, 전체 레벨의, 전체 이용자 및 관계자가 시스템의 라이프사이클 전반을 보고, 조직에 있어서는 당연한 조치로서 프라이버시 보호의 취급이 행해지는 환경’이라고 설명하고 있다. 여기서 말하는 에코시스템이란 생태계를 말하는 것이며, 개인정보는 일상적으로 다양한 장소와 다양한 곳에서 다루어지고 우리 경제사회에서는 공기나 물과 같이 불가결한 것이다. 개인정보를 취급해야하는 관계자가 매일 최고의 개인의 프라이버시를 보호하는 환경이야말로 프라이버시 중심 디자인이 지향하는 사회일 것이다. 공기나 물을 사용하면 오염이 되듯이 개인정보도 그 운용에 따라 오염되는 것이다. 개인정보의 이용에 관해서는 모든 관계자에 의한 정보의 적정한 취급과 보호라는 ‘순환’을 유지할 필요가 있다. 이를

50) 일본에서도 이 조사에 영향을 받아 2011년에 경제산업성에서 ‘익명화기술 등을 활용한 대규모 개인정보의 활용에 관한 조사연구’를 실시하고, 조사보고서를 OECD의 정보보안·프라이버시작업반 및 정보경제작업반(WPIE: Working Party on the Information Economy)에 보고하였다.

51) 손형섭, 앞의 논문, 115쪽.

52) <http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf>, 검색일 : 2012.12.30.

위해 무엇이 요구되는지에 대한 것이 바로 ‘프라이버시 중심 디자인’의 의도를 이해하고 받아들여 향후 개인정보보호 정책에 있어 그 중심 개념으로 삼아야 할 것이다.⁵³⁾

V. 결 론

스마트폰을 비롯한 다양한 통신기기의 등장으로 사용자의 편의성은 점점 높아져가고 있지만, 이러한 편리함 속에 통신기기 및 인터넷을 통한 개인정보의 침해 문제는 아직 세계적 과제이다. 개인정보는 더 이상 한 개인만의 정보라고 할 수 없으며, 개인정보를 활용하고 재가공하여 엄청난 데이터, 즉 빅 데이터로서 기능될 수 있음은 이제 모두 인식하고 있는 바이다. 이러한 정보를 어떻게 관리하고 운용 및 활용을 하는 가는 국가와 기업의 이익과도 직결된다고 해도 과언이 아닐 것이다.

개인정보 침해문제에 대처하기 위한 새로운 대처방안으로서 사후적 대처방법이 아닌 사전적 대응방안으로 제안된 “프라이버시 중심 디자인”에 대하여 살펴보았다. 이 개념은 유럽을 비롯하여 미국, 일본 등지에서 적극적으로 검토되고 논의되어 정책적으로 프라이버시 중심 디자인의 개념을 채택하는 경향을 보이고 있다. 그러나, 우리나라에서는 아직 이에 대한 논의조차 적극적이지 않은 상태이다. 유럽과 미국에서의 적극적 논의 동향을 통해서도 그 시사성을 찾을 수 있으며, 특히 일본에서 프라이버시 중심 디자인의 개념을 도입하는 것에 관해 논의를 할 때 앞서 언급하였던 ‘스마트폰을 경유한 이용자정보의 취급에 관한 워킹그룹’에서는 이 개념에 대한 반론이나 의문이 거의 없었다는 것도 주목할 점이다. 프라이버시 중심 디자인의 개념(사전 예방적으로 대응을 진행하는 것)이 이제는 일반적으로 요구되는 개념으로서 이해되어

53) 堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC) 編, 앞의 책, 55쪽.

도 좋다고 생각한다. 적어도 현재의 일본 스마트폰 활용환경에 있어서 프라이버시 중심 디자인에 대해서 도입을 적극적으로 논의하고 있는 것을 보아도 우리의 정보통신기기의 아키텍처설계에 있어서 상당한 시사성이 있다고 보여진다.

한편, 조금 다른 관점에서 재산적 가치를 창출하는 개인정보에 대한 논의로 시야를 넓혀 어떠한 기술이 필요한지 그리고, 어떠한 데이터 취급 규정이 유효한 것인가를 검토하는 것도 필요할 것으로 생각된다. 이러한 제도설계와 기반정비를 함께해 가는 경우에도 프라이버시 중심 디자인을 지침으로 도입하는 것이 가능할 것이다.⁵⁴⁾⁵⁵⁾

우리나라에서는 프라이버시 중심 디자인에 대한 논의가 아직 적극적이지 않은 상태이나, 세계 각국의 동향을 인식하여 보다 적극적으로 개인정보보호 관련 규정들을 개선할 필요성을 제기한다.

더 나아가서는 법제 정비를 통한 개인정보보호를 위해 정보통신관련 법제도 및 관련 기기의 설계에 있어서 프라이버시 중심 디자인 개념을 적극 도입할 것을 제안한다. 이것은 빅데이터 활용을 시대적 중요성의 인식과 더불어 반드시 그 규범적 근거로서 반드시 도입하여야 하며, 이를 통하여 우리나라의 개인정보보호제도가 유효하고 실효성 있는 제도가 될 수 있을 것이다.

(투고일 2012년 12월 31일, 심사(의뢰)일 2013년 2월 5일, 게재확정일 2013년 2월 12일)

주제어 : 프라이버시, 프라이버시 중심 디자인, 개인정보보호, 프라이버시 강화 기술, 포지티브섬

54) 堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC) 編, 위의 책, 42-43쪽.

55) OECD에서는 2013년부터 2014년의 총예산 2406유로 중에서 빅데이터와 관련한 사항에 323만 유로를 할당하였다. 특히, 빅데이터의 활용에 의한 새로운 경제성장예의 기여를 분석에 223만 유로를 할당하고 있다.

참고문헌

1. 단행본

堀部 政男, 一般財団法人日本情報経済社会推進協会(JIPDEC)編, プライバシー・バイ・デザイン, 日経BP社, 2012. 10.

ALAN F. WESTIN, *PRIVACY AND FREEDOM* 7, The Atheneum, 1967.

Ann Cavoukian, *Privacy by Design-The 7 Foundational Principles*, Information and Privacy Commissioner, Ontario, Canada, 2011.

2. 논문

손형섭, “개인정보 보호법의 특징과 앞으로의 방향—업계의 반응에 대한 몇 가지 대안을 중심으로—”, 언론과 법 제11권 제1호, 한국언론법학회, 2012, 93-123쪽.

전경근, “개인정보의 활용범위에 관한 고찰”, 아주법학 제6권 제1호, 아주대학교 법학연구소, 2012, 481-502쪽.

황성기, “개인정보 보호와 다른 헌법적 가치의 조화”, 경제규제와 법 제5권 제2호, 서울대학교 공익산업법센터, 2012, 20-36쪽.

宮下 紘, “プライバシー・個人情報保護の新世代”, 駿河台法学 25卷1号, 駿河台大学, 2011, 111-136쪽.

Kenny S. and Borking J., “The Value Privacy Engineering”, *The Journal of Information, Law and Technology*, JILT 2002 (1), 1-29쪽.

Samuel D. Warren / Louis D. Brandeis, “The Right to Privacy”, 4 *HARV. L. REV.*, Harvard Law School, 1890, 1-16쪽.

3. 기타

FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Privacy by Design, UK Information Commissioner's Office, 26th November 2008.

Thirty Years After the OECD Privacy Guidelines.

Whalen v. Roe, 429 U.S. 589, 1977.

[Abstract]

New Trend of Personal Information Protection

—Concept on Privacy by Design—

Hye-Seon Choi*

In order to correctly keep privacy, increasing self cognition on privacy by individual is necessary first of all. Service provider needs to perform ‘Privacy by Design’ which is an privacy focused design examining possibility of privacy invasion and minimizing risk in own corporation service. In order to certainly protect privacy, relying on only regulation obedience is not sufficient. Hence, government or corporation needs to promote construction of a structure for technically protecting privacy in design stage. It is required to certainly protect privacy from initial stage. That is, it is to ‘construct from first stage’ the system for personal information protection. The base of ‘Privacy by Design’ can be said to be in the technology, but application of its concept also gradually affects design of responsible business process and physical space or network, infrastructure. This is not simply subject to only technology (especially, information system) but general business process. Among them, Dr. Ann Cavoukian mentioned the specific object as IT system (technical field) field, responsible business convention, physical design and network infra. Privacy by Design concept has been actively discussed recent years. Especially, in 32th International Personal Information Protection

* Ph.D.(Law) Researcher, Institute of Legal Studies, Konkuk University

Authority Conference¹⁾ opened on October, 2010, Privacy by Design was agreed to be recognized as essential element. What the International Personal Information Protection Authority Conference agreed on was that Privacy by Design is recognized as new global privacy standard. Actually, the agreement in this conference encourages acceptance a basic principle of Privacy by Design. Due to promotion and support for review structure about international privacy, application of Privacy by Design is proceeded worldwide. What the Privacy by Design try to keep is privacy information of user (citizen, consumer, customer) in a word and privacy of user itself who is a principal agent of that information. This is clear that the source of Privacy by Design is PETs(Privacy Enhancing Technologies) and the basic requirement is appeared while PETs concept is evolved. PETs is the whole technology enhancing personal privacy protection in information system. This was originally to prevent illegal collection, use and provision of personal data and enhance control on own personal information by individual. Specifically, a technology remove cookie or virus, filtering spam mail, etc. However, recently service provider lays a stress on ‘consideration at design stage’, ‘advancement of technology receiving feedback from user’ and requests tool or system environment more actively protecting privacy. A thought on the positive sum which ‘protects both user and provider’ has been widely applied. As service provider cooperates in protecting privacy information in advance with user not leaving it to user, he can obtain trust from user and the business relations can be enhanced. Such a new paradigm became the basis for Privacy by Design. On this new paradigm which each world nation is actively discussing and applying, our country should more positively discuss and cope actively with application environment (changes in technology and legal system) of Privacy by Design worldwide.

Key Words : privacy, privacy by design, personal information protection,
privacy enhancing technologies(PETs), positive sum