Regular paper http://dx.doi.org/10.13067/JKIECS.2013.8.8.1161

이원화된 계층적 개인정보 Life-Cycle 접근제어 방법론에 관한 연구

서우석* · 김계순** · 전문석***

Research on the Access Control Methodology for Dualised Hierarchical Personal Information Life-Cycle

Woo-Seok Seo* · Kye-Soon Kim** · Moon-Seog Jun***

요 약

2013년 현재 개인정보보호를 위한 사회적 합의결과로 도출되어진 관련법이 제정되고 수차례의 개정을 통해 IT분야를 비롯한 다양한 사회적 업무분야에 최종적인 정보보호를 위한 명확한 성문법적인 정책과 지침 등의 방향이 제시되어 졌다. 이러한 일련의 개인정보 중요성에 대한 사회적 이슈를 기반으로 새로운 개인정보 접근 패러다임이 나타났고 정보보호라는 거시적인 접근 방법에서 전문적인 접근방법의 필요성이 대두되어졌다. 물론 현재까지 모든 개인정보 형태의 자료들을 특정한 정보의 범주에 모두 제한하고 경계를 두는 것은 다소 무리수 있어 보이나 IT분야를 기반으로 하는 정보의 홍수 속에서 개인정보의 흐름을 확인하고 보안대상으로 선정하는 부분은 표준화되어 진 것은 사실이다. 다만 아직까지도 개인정보 Life-Cycle의 5가지 표준화된 흐름인 수집, 처리, 제공, 보관, 파기 등을 모든 기업과 기관이 보유한 정보들에 일상적으로 적용하기 어려운 경우도 발생하고 있다. 따라서 이원화된 계층적 개인정보 Life-Cycle 접근제어 방법론을 제안함으로써 표준화 방법론을 제안한다. 본 연구 결과는 개인정보 Life-Cycle에 최적의 접근제어 가능한 현실적인 자료를 제공하고자 한다.

ABSTRACT

Currently in 2013, a law that was drawn as a result of social agreement for personal information protection was enacted, and through several amendments, definite policy of written law and guideline were presented for definitive information protection in various fields of social business including IT field. Based on a series of social issues about the importance of personal information, a new access paradigm to personal information appeared. And from macroscopic access method called information protection, the necessity of technical access method came to the fore. Of course, it seems somewhat irrational to restrict all data in the form of personal information to a certain category of information until now. But in the deluge of information based on IT field, it is true that the part of checking the flow of personal information and selecting as security target has been standardized. But still there are cases in which it is difficult to routinely apply the five standardized flows of personal information Life-Cycle－collect, process, provide, store, and destroy－to information that all companies and organizations have. Therefore, the researcher proposes the standardized methodology by proposing the access control methodology for dualised hierarchical personal information Life-Cycle. The results of this research aim to provide practical data which makes optimal access control to personal information Life-Cycle possible.

키워드

Personal Information, Access Control, Methodology
개인정보, 접근제어, 방법론

* 주식회사 이지서티 개인정보보호센터 센터장(ssws2000@nate.com)
** 교신저자(corresponding author) : 한국SMC공압(주) 차장(kskimjw@naver.com)
*** 숭실대학교 컴퓨터학과 교수(ijcsns@gmail.com)
접수일자 : 2013. 07. 20 심사(수정)일자 : 2013. 07. 23 게재확정일자 : 2013. 08. 23

Ⅰ. 서 론

2011년 9월 개인정보보호법이 제정되어 3년 여간 지속적인 개인정보보호를 통한 전 국민 개인 사생활 보호를 위한 초석을 만들어가고 있다. 하지만 2013년 아직까지도 개인정보 유출 및 노출과 연관된 보안 사고는 잦은 빈도로 발생하고 있으며, 그 실례로는 불과 몇 개월 전인 지난 6월 25일에도 주요 정부기관 등에 사이버 공격으로 개인정보가 유출되는 사고가 했다.

개인정보 보호라는 주제 하에 법이 제정되고 해마다 상상하기 힘든 예산과 경비가 투여되어 정보보안 분야의 한 범주로 자리 잡는 전문 기술로 성장하고 있음에도 개인정보는 아직까지도 많은 문제점을 가지고 있다. 이는 단순한 하드웨어적인 접근과 소프트웨어적인 접근 이라는 단순한 1차원적인 환경 보안에 대한 접근이 아닌 정책과 접근방법론 등의 지식정보가 많은 비중을 차지함에도 이를 크게 확대 해석하고 접근하지 못한 부분이 지금의 정책과 환경의 적절한 조합을 이끌어 내지 못한 것이다[1][2].

따라서 다양한 개인정보에 대한 침해유형과 Life-Cycle 접근방법에 대한 재해석을 통해 현재까지의 개인정보보호를 위한 접근 방법론의 적정성을 객관적으로 문제점을 확인해 보고 본 논문에서 제안하는 계층적 성격의 인위적인 분리 영역 조건하에 개인정보 Life-Cycle 접근제어 표준화 방법론을 제안하고 이를 증명함으로써 안전기를 거친 확대기라는 새로운 개인정보 보호를 위한 패러다임을 제안하고자 한다.

본 논문의 구성은 2장에서는 개인정보 침해유형과 개인정보 Life-Cycle 접근방법과 분류, 국내외 주요 개인정보 관리유형 분석에 대해 분석하고, 3장에서는 이원화된 계층적 개인정보 Life-Cycle 접근제어 방법론을 제안하고, 4장에서는 방법론 접근 방식과 사고에 대한 이해결과를 도출한다. 마지막으로 5장에서는 논문의 결론과 향후 연구 과제를 제시한다.

Ⅱ. 관련연구

2.1 개인정보 침해유형

개인정보에 대한 인식과 보호를 위한 안전성 조치 등의 일련의 법안이 발의되고 이를 준수하기 위한 절차는 불과 3년 밖에 되지 않았다. 물론 그 전의 다양한 개인정보에 대한 침해에 대한 객관적인 정보를 취합하고 이로 인한 제2, 제3의 파급되는 문제점에 대한 분석과 인식도 이루어지지 못한 것 또한 사실이다.

개인정보에 대한 침해는 단순히 개인의 신상정보가 인터넷이라는 온라인 공간에 공개되어진다는 미시적인 의미에서 벗어나 해당 개인정보가 속하고 저장되어진 기업 또는 기관의 내부 네트워크가 제3의 불법적인 접근 또는 내부 유출자에 의해 망 전체가 침해피해를 받았다는 의식의 변화가 이루어졌다[3].

표 1과 같이 2012년 한국인터넷진흥원의 최근 개인정보 침해신고 및 상담현황을 통해 2013년 현재 정보보호를 위한 꾸준한 정책과 법안 및 기술적인 안전성 조치 등이 발전해온 만큼 침해도 꾸준히 방어라는 범주의 핵심기술과 비례하는 수준 이상으로 심한 정보침해 기술 기반의 장애와 문제점 현황을 보이고 있다[4][5].

따라서 단순한 개인정보의 유출 또는 노출로 인한 특정 개인의 피해만이 사회적 이슈가 아니며, 정보보호를 위한 존재하는 모든 데이터 유출 방지를 위한 새로운 기술과 정책의 변화가 절실히 필요한 시점이다.

표 1. 개인정보 침해신고 및 상담 접수 현황
Table 1. Cases of personal information violation reports and consulting service request

Type of Service Request	'10	'11	'12
Requirements for personal information collection	1,267	1,623	3,507
Obligation to notify and specify at the time of personal information collection	75	53	396
Excess personal information collection	146	379	847
Use for other purposes than specified or provision to a third party	1,202	1,499	2,196
Damage, violation, etc. of personal information by its manager	158	278	941

Entrusted processing of personal information	25	36	125
Business transfer and assignment	22	64	44
Person in charge of personal information protection	21	38	48
How to make sure the safety of personal information	1,551	10,958	3,855
Failure of personal information destruction	323	488	779
Rights of data subjects (request for reading and correction, etc.)	826	662	717
How to make reading and correction easier than collection	630	800	660
Collection of children's personal information	35	71	47
Damage, violation, and theft of others' information including Korean ID No.	10,137	67,094	139,724
Cases of personal information relating to other laws	38,414	38,172	12,915
Total	54,832	12,2215	166,801

개인정보 수집이라는 Life-Cycle 상의 첫 단계를 통해 다양한 정보가 수집되고 이를 기반으로 제공, 운영, 파기의 과정 속에서 개인정보의 기본속성 변화가 또 다른 개인정보를 이끌어 내고 있다. 이를 파급정보라 칭하기도 하며, 따라서 이러한 지속적인 형태의 변화를 통해 엄청난 속도로 증가되는 개인정보의 관리를 위한 세계 각국에서는 표 2와 같이 빠르게는 70년대부터 현재까지 개인정보보호를 위한 법안을 제정하고 개정과정을 통해 완벽성을 높이고자 하고 있다[6][7].

표 2. 주요 국가별 개인정보보호를 위한 관련 법률
Table 2. Personal information protection-related laws of major countries

Country	Related Law	Year of Legislation	Description
Korea	Personal Information Protection Law	2011	Law that provides for how to handle personal information to realize dignity and values of individuals
USA	Federal Privacy Act	1974	Act to protect personal information retained by federal government agencies
Japan	Act on Personal Information Protection	2003	Act on protection, etc. of information retained by individuals
China	Draft of Personal Information Protection Law (recommended by experts)	-	Draft to legislate a law on protection, etc. of information retained by individuals

* 최초 제정 및 개정의 경우는 해당 국가자료 도 참조

2.2 개인정보 Life-Cycle 접근방법과 분류

현행 국내에서 관련법에 의거한 개인정보를 취급하는 순차적인 Life-Cycle은 법에 명시된 총 15가지 용어 정의로 법문 안에 명기되어 있다. 따라서 가장 최근에 개인정보를 취급하는 흐름인 Life-Cycle은 표 3과 같이 접근방법을 기준으로 구성분류의 2차적인 접근방법과 분류를 구성 가능하다.

표 3. 개인정보 취급 Life-Cycle 접근방법과 분류
Table 3. Approaches and classifications of personal information handling Life-Cycle

Approach	Description	Classification	Related Laws	Related Provisions
Collection	1. Upon the consent of data subjects. 2. In case that it is inevitable subject to a special provision of laws or in order to meet legal obligations. 3. In case that it is inevitable to do so in order for a public agency to perform its duties as set forth in laws. 4. In case that it is mandatory in order to conclude a contract with data subjects and perform the contract. 5. Deemed necessary to do so for urgent life or physical and financial benefits of data subjects or a third party in case that data subjects or their legal representatives cannot express their opinion or it is impossible to obtain a prior consent due to wrong addresses. 6. In case that it is necessary to do so in order to achieve due profits of Personal Information Manager, which clearly is more important than rights of data subjects to the extent of being significantly related to due benefits of Personal Information Manager and not exceeding a reasonable range.	Creation	Personal Information Protection Law and its Enforcement Decree & Rules	Article 15 (Collection and Use of Personal Information)
Use		Record, storage, retention, processing, compilation, retrieval, printout, correction, restoration		
Provision	1. Upon the consent of data subjects. 2. In case of providing personal information in line with the purpose of its collection, subject to Sections 15.1.2, 15.1.3 and 15.1.5.	Release		Article 17 (Provision of Personal Information)
Destruction	① In case that any personal information becomes useless due to elapse of retention period, achievement of the purpose to process personal information, etc. Personal Information Manager shall destroy the personal information without delay, except that it is mandatory to retain the information subject to other laws. ②In case of destroying or reproducing personal information pursuant to Item 1, Personal Information Manager shall take every action to prevent its restoration or reproduction. ③ In case that it is required to retain personal information in accordance with the provisory clause as set forth in Item 1, Personal Information Manager shall store and manage the said personal information or personal information file separately from other personal information. ④Matters regarding methods and procedures of destroying personal information, etc. shall be in line with Presidential Decrees.	-		Article 21 (Destruction of Personal Information)

※ 개인정보보호법 상의 접근방법 연관 법률 일부 발췌

2.3 해외 개인정보 관리유형 분석

국내 개인정보보호법 이외의 대외적인 개인정보보호를 위한 정보법 등을 제정하고 이를 준수하기 위해 노력하는 다수의 국가가 개인정보를 관리하고 운영하는 정책은 표 4와 같이 그 예를 참고할 수 있는 문헌 등에 수록되어 있어 쉽게 그 내용을 파악 가능하다 [8][9].

다만 다소 전체 개인정보를 위한 법률에 있어서 극히 정책적인 부분인 법 존재 유무와 법을 제정하고 이를 관리 및 운영 가능한 전담조직에 대한 현황만을

보이고 있으나, 이외의 관련 보호조치는 법안에 존재하는 각 조, 항, 호를 그 시행과 준수조건과 기능으로 판단해도 문제는 없다.

표 4. 국내외 개인정보 관리유형
Table 4. Types of local and overseas personal information regulations

Classification	Direct-Regulatory Type	Self-Regulatory Type
Country	France, UK, Germany	USA, Japan
Personal Information Protection Basic Law	Legislation of basic laws (general law)	Legislation of individual laws
Organization responsible for personal information protection	Independent body	Government agencies

국내 개인정보보호법은 2011년 제정되고 정보보호의 대상을 확대하는 최종 법안이 발의되었다. 다만 최종 법안이 나오기까지 대상의 확대를 위한 노력은 1995년 이후 계속적으로 일어났다.

**** 개인정보보호를 위한 관련 법률 제정과 개정 내역(법률만 명시) - 법제처 해당법률 공포법령 일부발췌***

- *공공기관의 개인정보보호에 관한법률[시행 1995.01.08.][법률 제4734호, 1994.01.07.]*
- *공공기관의 개인정보보호에 관한법률[시행 1999.1.29.] [법률 제5715호, 1999.1.29., 일부개정]*

<개인정보의 이용 및 제공요건을 강화하는 한편, 본인의 열람제한사유를 완화하는 등 규제를 완화하고 기타 현행제도의 운영상 나타난 일부 미비점을 개선·보완하려는 것임>

- *공공기관의 개인정보보호에 관한 법률[시행 2007.11.18.] [법률 제8448호, 2007.5.17., 일부개정]*

<공공기관이 범죄예방·교통단속 등의 필요에 따라 설치·운영하고 있는 폐쇄회로 텔레비전의 설치 및 화상정보보호 등에 관한 법적 근거를 마련함으로써, 공공업무의 적정한 수행을 도모함과 아울러 사생활의 비밀과 자유 등 국민의 기본권을 보호하고, 공공기관이 보유하고 있는 개인정보의 안전성 확보에 대한 필요성이 증대됨에 따라 처리정보 보유기관의 안전성 확보조치 의무를 규정하며, 공공기관에 의한 개인정보의 수집·처리 등에 관한 정보를 공개하는 등 공공기관에서 처리되는 개인정보의 보호제도를 개선·보완하려는 것임>

- *공공기관의 개인정보보호에 관한 법률[시행 2010.3.22.] [법률 제10142호, 2010.3.22., 일부개정]*

<현행 양벌규정은 문언 상 영업주가 종업원 등에 대한 관리·감독상 주의의무를 다하였는지 여부에 관계없이 영업주를 처벌하도록 하고 있어 책임주의 원칙에 위배될 소지가 있으므로, 영업주가 종업원 등에 대한 관리·감독상 주의의무를 다한 경우에는 처벌을 면하게 함으로써 양벌규정에도 책임주의 원칙이 관철되도록 하려는 것임>

- *개인정보 보호법[시행 2011.9.30.] [법률 제10465호, 2011.3.29., 제정]*

III. 이원화된 계층적 개인정보 Life-Cycle 접근제어 방법론 제안

현재 관련 법률에 의한 개인정보 Life-Cycle 정책 접근과 해석적인 논리적 방법론 구성에 따른 제어는 기본적인 4대 흐름인 수집, 이용, 제공, 파기라는 정해진 순차적 절차에 의거 개인정보 Life-Cycle 접근제어 정책을 구성하고 있다.

하지만 기존 법률의 기초적인 적용만을 우선시하는 Life-Cycle은 최초 생성되는 기업 또는 기관에 적용하기에 가장 적합한 법률적 준수 기반의 형태이다.

2011년 개인정보보호법이 제정되고 같은 해 9월 시행되는 시점에 이미 수많은 기업과 기관은 많게는 몇십만 개의 개인정보를 이미 보유하고 있었다는 부분에 대해서도 일괄적인 법의 적용이 이루어졌다. 물론 모든 법률을 모두 적용하는 부분이 아닌 순차적으로 단계별 적용은 이루어 졌다고 평가할 수 있다면, 그와는 반대의 결과인 3년이 지난 지금 무엇이 우선이고

무엇을 위한 보호가 이루어지고 있는지에 대한 목적과 정의가 다소 혼탁한 정책으로 이루어지고 있는 것 또한 사실이다.

따라서 본 논문에서는 기존 명확하게 법률로써 정하고 있는 준수해야 하는 모든 기준점을 순차적인 방법에서 비순차적인 이원화된 다차원의 Life-Cycle을 제안하고 있다.

3.1 이원화 계층 분류

제안하는 Life-Cycle의 접근제어 방법론에서 이원화 계층 분류에 대해서는 표현계층과 적용계층으로 분리하고 각 개인정보보호법을 근간으로 적용하고자 하는 정책 적용 Life-Cycle의 이원화 계층 분류는 단순 경우의 수(사례 적용 가능한 정책 접근 또는 적용 가능에 대한 경우의 수를 의미)로 표 5와 같이 정의한다.

표 5. 사례 적용 가능한 정책 접근 또는 적용 가능에 대한 경우의 수
Table 5. Number of cases of applicable policy approaches or applicable cases

Classification	Component	Remarks
Expression hierarchy	Collection, use, provision, destruction	* Reductive personal information life-cycle of dual hierarchy - Number of cases for personal information life-cycle access control For a reduction system of expression, how to adjust the number
Application hierarchy	Creation, record, storage, retention, processing, compilation, retrieval, printout, correction, restoration, release	

본 논문에서 제안하는 다차원 Life-Cycle 접근 제어는 단순한 산술적인 경우의 수를 도출해서 무작위 정책적용 시점의 난립이 아니라 개인정보가 어떠한 형태로 현 시점에 존재하든 접근이 가능한 정책과 방법론을 적용하기 위한 예시적인 경우의 조건 도출현애이며, 이외의 다른 다양한 접근 경우의 수를 도출 가능한 형태가 있다면, 접근 정책의 등급 또는 계층만의 차이가 있을 뿐 논문에서 제안하는 접근 제어의 다차원에 대한 목적성은 유지된다.

**** 개인정보 Life-Cycle 접근제어 경우의 수***

- *수집->생성/이용->생성/->제공->생성/파기->생성*
- *수집->기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구/*
  이용->기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구/
  제공->기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구/
  파기->기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구
- *수집->공개/이용->공개/제공->공개/파기->공개*

3.2 계층적 개인정보 Life-Cycle 접근 방법론 분석

계층적 개인정보 Life-Cycle 접근 방법론은 그림 1과 같은 이원화 계층 개인정보 Life-Cycle 환원 고리를 위미하며, 환원 고리는 현재 또는 미래의 개인정보를 수집으로부터 파기에 이르는 일련의 개인정보를 보유하게 될 기관과 기업의 이원화된 개인정보 운영과 관리 및 환원을 위한 방법론의 기초형태로써 접근제어 경우의 수를 논리적으로 기관에 적용 가능한지를 입증하고 구현하는 과정을 갖는다.

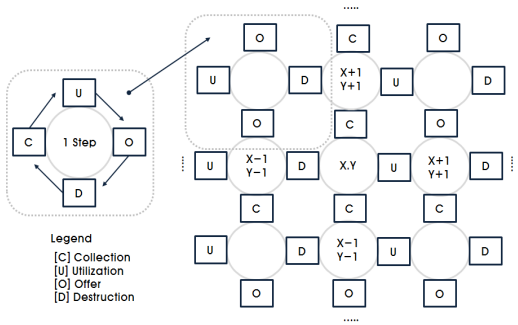

그림 1. 이원화 계층 개인정보 Life-Cycle 환원 고리
Fig. 1 Reductive life-cycle of personal information of dual hierarchy

계층적 개인정보 Life-Cycle 접근 제어 방법론의 시작은 4가지 경우의 수인 수집, 이용, 제공, 파기 1 Step 라운드 정책을 다차원의 시작 시점인(x, y)를 기점으로 접근 4면의 (x+1, y+1)', (x-1, y-1)', (x+1, y+1)", (x-1, y-1)" 4가지 근접 정책을 구현함으로써 환원 고리 구성을 이룬다.

다소 정책의 방법론을 수치적인 해석으로 접근한 점도 있으나 이는 객관적인 명확성을 기반으로 하는 Life-Cycle의 접근 제어와 정책반영을 위한 방법론의 제시에 그 목적을 두고 있다.

3.3 개인정보 Life-Cycle 접근 제어를 위한 표준화 방법론 제안

본 논문에서 최종 제안하고 그 형태성 정책을 재정립하고 이를 조정하는 등의 다양한 운영과정의 효율성을 하나의 적정성을 갖는 개인정보 Life-Cycle을 구성하는 방법론을 제안한다.

제안하는 방법론은 기존 방법론과의 차별화를 두고 있는 가장 큰 정책 적용의 장점은 비순차적인 정책에 대한 접근으로 방법론의 요구제한이 없이 어느 기업 또는 어느 기관이든, 어떤 정보이든, 기존 개인정보의 존재 유무가 있는지 아니면 없는지도 절대 정책을 적용이 가능한 이원화된 계층적 개인정보 Life-Cycle이 표준화된 방법론으로 표출된다.

다만 다양한 기업과 기관에 적용하고 운영하는 과정들이 지속적인 방법론의 적용 결과의 누적이 필요함에 따라 방법론의 현존하는 개인정보를 가지고 환경을 구성하고 적용하는 방법을 통해 제안하는 방법론을 증명한다.

*** *표준화 개인정보 Life-Cycle 접근 제어 방법론 주요 제안사항***

- *개인정보 접근 정책의 시작은 미정*
- *수집과 파기 Life-Cycle는 동일한 개인정보 접근 정책 적용 시점*
- *환원 고리 형태의 개인정보 Life-Cycle 연결고리 확장*
- *단일 개인정보 Life-Cycle은 제한*
- *이원화(다수 Life-Cycle이 하나의 기업과 기관에 존재)*
- *계층화(Life-Cycle 내부에 또 다른 Life-Cycle을 구성)*
- *계층화 구성은 상위, 하위 높이를 기준으로 하는 등급 불가*
- *개인정보 접근 제어 정책 조건 : 개인정보 유무와 무관*

표준화된 개인정보 Life-Cycle 접근 제어 방법론으로 제안되는 본 논문의 목적에 준하는 방법론을 구성하고 적용하기 위한 8가지 주요 제안사항은 다차원으로 구성된 각 Life-Cycle 마다 존재하고 준수되어지는 일련의 규칙성을 갖는다.

Ⅳ. 방법론 접근 방식과 사고에 대한 이해결과

과거 단일 Life-Cycle 형태의 개인정보를 수집하고 파기 하는 시점까지의 접근 제어 방법론의 문제점을 인지하고 제안되어 지는 다중화 Life-Cycle 형태의 수집이 곧 파기라는 환원 고리 형태의 Life-Cycle 구성을 이해하고 적용하는 과정이 실무에서 지속적으로 표출되어야만 향후 최종 제안하는 방법론에 대한 객관성과 효율성을 확인하고 이를 증명하는 이해결과가 도출될 것이다

따라서 논리적 제안 방법론과 표준화 방안을 상호 비교하는 과정과 비교를 통한 상호 전근 제어 결과를 이끌어 낸다.

4.1 논리적 제안 방법론 구성과 표준화 방안 비교

최종 제안되어지는 방법론에 대한 증명결과를 표 6과 같이 기존 Life-Cycle 형태와 비교함으로써 다시 효율성을 확보한 이원화 계층적 개인정보 Life-Cycle 접근 제어 방법론에 대한 이해를 높인다. 가장 기본적인 방법론 비교의 기초자료는 Life-Cycle 구성을 4가지로 구분할 것인가 아니면, 관련법인 개인정보보호법에 명기되어진 전체 개인정보를 가지고 처리 가능한 일련의 단계 모두를 적용하느냐를 따른다.

표 6. 단일 개인정보 Life-Cycle과 이원화된 계층적 개인정보 Life-Cycle의 상호 비교
Table 6. Comparison of personal information life cycle of single hierarchy & personal information life-cycle of dual hierarchy

Classification	Personal information life-cycle of single hierarchy	Personal information life-cycle of dual hierarchy
Components	Collection, use, provision, destruction	Creation, record, storage, retention, processing, compilation, retrieval, printout, correction, restoration, release
Hierarchy	N/A	Multi-dimensional (reduction cycle)
Flow	collection requiring destruction	Collection and destruction on the same line
Application	Good for a new organization	Applicable to and good for any organizations, whether existing data retaining ones or new ones
Input	Single expert system / excess work load	Each life-cycle (one-step) processed by a number of staffers
Category	Data of businesses or organizations at large [covering creation of one big data to destruction]	Data classified in detail by purpose

4.2 이원적 분리를 통한 계층화된 개인정보 Life-Cycle과 접근제어 결과분석

특정 기업의 경우에 있어서 15개의 부서로 구성되어진 조직에 대한 이원화된 계층적 개인정보 Life-Cycle 접근 제어 방법론 적용 시에 해당 제안에 대한 최적의 구현결과(제안결과 도출을 위한 예시)로써 그림 2와 같은 결과를 갖게 된다. 이는 제안하는 별개의 업무별 또는 원하는 개인정보 운영과 관리 범주에 대한 개별적인 Life-Cycle 적용함으로써 관리 주체의 편리성과 업무한계치 조정 등의 제반 방법론 구현을 위한 조정이 가능한 결과를 갖는다.

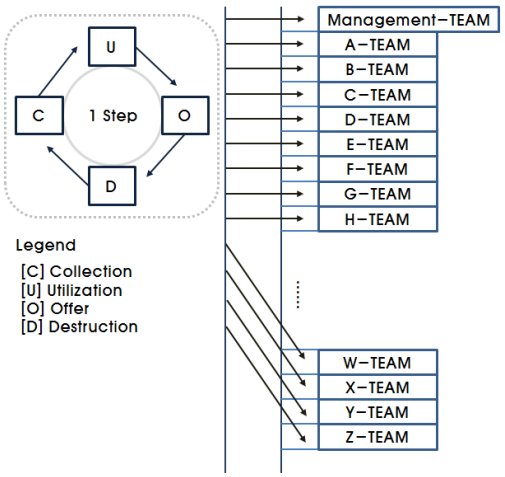

그림 2. 제안결과 도출을 위한 예시
Fig. 2 Template for proposal results

최종 제안되고 증명된 개인정보 Life-Cycle 접근제어 방법론은 기업 또는 기관을 대상으로 TEAM 단위 업무를 구분하여 다차원 환원 고리 형태를 적용하거나 또는 단위별 TEAM 내의 세부 업무를 구분해서 Life-Cycle을 적용 가능한 효율성을 갖는 방법론 성격을 갖는다.

V. 결 론

본 논문에서는 현행 적용중인 개인정보 Life-Cycle의 순차적인 기업 또는 기관의 정보보호를 위한 현황과 구성을 확인하고 이에 대한 문제점을 증명하고 이와 같은 기존의 순차적인 life-Cycle 접근제어 방법론의 적용으로 인한 문제점을 해소하고 다차원적으로 비순차적인 정책적용으로도 보유하고 있는 개인정보를 보호하기 위한 정책적인 Life-Cycle 접근제어 방법론을 제안하고 있다.

이는 법에서 가장 단순하게 그 흐름을 지명하고 있는 수집과 이용, 제공, 파기의 가장 큰 범주의 운영항목에 대한 절대적인 순차적 접근을 통한 정책의 이행에 대해서 4가지 수행 정책에 대한 방법론을 개인정보 Life-Cycle이라는 흐름에서 다차원 형태로 변형해서 적용하고자 하는 용어로는 이원화된 다차원 개인정보 Life-Cycle이라는 또 다른 접근제어 방법론으로 변화를 통해 기업과 기관에서 개인정보에 대한 접근

Life-Cycle의 시작을 이용에서 제공, 파기 이후 수집의 비논리적이고 비순차적인 정보의 접근이 가능함을 기술했다. 이는 개인정보를 수집하는 과정을 통해서 관리해야하는 Life-Cycle이 생성되는 것이 아닌 어느 단계에서든 관리가 가능한 정보가 넘쳐나고 이를 수영 가능한 방법론을 제시하고 있는 것이다.

향후 연구방향으로는 중복되는 Life-Cycle의 교접 범주의 적용방안과 정책의 적용여부 및 영역의 한계를 파악하고 해당 정책의 재적용이 이루어지는지 또는 기 적용되어 있어 재적용이 불가피 한지 등의 행정적인 절차와 흐름을 면밀하게 확인하는 일련의 개관적인 확보조치가 필요하다.

참고 문헌

[1] K. S. Lee, H. B. A, S. Y. Lee, "A Study on a Prevention Method for Personal Information Exposure", The Journal of information and security, Vol. 12, No. 1, pp. 71-77, 2012.

[2] M. S. Kim, "The Study of Check-list based on Privacy Law in Korea for Private Company", The Journal of computing science and engineering (Proceedings of the 2010 Fall Conference), Vol. 37, No. 2B, pp. 37-42, 2010.

[3] D. j. Lee, "The Moderating Role of Site Usage Experience in Internet Users' Decision on Personal Information Disclosure", Information Policy, Vol. 19, No. 2, pp. 21-38, 2012.

[4] The Republic of Korea Ministry of Security and Public Administration · Korea Internet & Security Agency, Privacy counseling casebook", pp. 10-11, 2012.

[5] S. C. Jin, I. K. K, "A Study on the Psychological anxiety on Private information leakage to likelihood of internet users", The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 6, No. 5, pp. 731-738, 2011.

[6] C. I. Hwan, "A study on the Development of Personnel Security Management for Protection against Insider threat", The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 3, No. 4, pp. 210-220, 2008.

[7] E. J. Jun, H. B. Kim, H. Y. Youm, "Trends of laws and programs for personal information protection of Japan and China", The Journal of the Korea Institute of Information Security and Cryptology, Vol. 22, No. 5, pp. 90-105, 2012.

[8] D. K. Jeong, "Comparative study of the privacy information protection policy - Privacy information basic laws and dedicated organizations -", The Journal of the Korea Institute of Information Security and Cryptology, Vol. 22, No. 4, pp. 923-939, 2012.

[9] S. J. Lim, G. J. Kim, T. G. Kang, "Important Information Protection using Client Virtualization", The Journal of The Korea Institute of Electronic Communication Sciences, Vol. 6, No. 1, pp. 111-117, 2011.

저자 소개

서우석(Woo-Seok Seo)

2006년 8월 숭실대학교 정보과학대학원 정보통신융합학과 (공학석사)

2013년 3월 숭실대학교 일반대학원 컴퓨터학과 (공학박사)

2006년 4월~2012년 12월 서울특별시 용산구시설관리공단 전산총괄

2012년 12월~현재 주식회사 이지서티 개인정보보호센터 센터장

※ 관심분야 : 정보보호, 네트워크 보안, Network Design

김계순(Soon-Kye Kim)

1994년 9월~2008년 11월 리바이스 트라우스 코리아 인사부 과장

2008년 12월~현재 한국SMC공압(주)인사총무부 차장

※ 관심분야 : 행정학적 접근 정보통제, 개인정보 정책관리 방법론, 기업경영정책 등

전문석(Moon-Seog Jun)

1981년 2월 숭실대학교 전자계산학과 졸업
1986년 2월 University of Maryland Computer Science 석사
1989년 2월 University of Maryland Computer Science 박사
1986년 9월～1989년 12월 University of Mary 강사
1989년 3월～7월 Morgan State University 조교수
1989년 9월～1991년 2월 New Mexico State University Physical Science Lab. 책임연구원
1991년 3월～현재 숭실대학교 정교수
※ 관심분야 : 정보보호, 네트워크 보안, 전자여권, 암호학