디지털산업정보학회 논문지 제14권 제3호-2018년 9월
http://dx.doi.org/10.17662/ksdim.2018.14.3.045

보존연한 도래 및 법적기준 준수를 위한 개인정보 정책적 폐기시스템을 활용한 폐기 누적현황 데이터베이스 구축에 관한 방안 제안

서 우 석*

A Proposal of Methods for Building Databases about the Accumulation of Disuse Utilizing the Political System to Discard Private Information According to the Expiration of In-service Life and Observation of Legal Standards

Seo Wooseok

〈Abstract〉

The Personal Information Protection Act has been revised continuously since its establishment, and as a way to secure stability properly, the guidelines as well as enforcement ordinances and regulations have been changed, too. It seems that people's recognition and awareness of private information have already evolved to a certain level that is regarded to be fairly high. However, no one can exactly imagine how much ripple effect scrapping discarded paper regarded simply as waste material which is often and easily practiced in our everyday lives exerts and how many socially significant events it may arouse in our lives. Private information is produced, operated, preserved, utilized, distributed within the frame of law unidentified, and then discarded with a particular purpose. While going through a series of processes, each piece of that private information comes to be reproduced melting a lot of information. It is used and also changed beneficially sometimes to richen our lives or as basic material for welfare. Meanwhile, its importance is decided by its weight or mass and then often gets discarded after all. It means that the process of disuse is being done in a way to arouse the possibility of invasion of personal rights and also the second and third and also more exposure of private information. Therefore, approaching the meaning of automation politically, this study aims to suggest how to secure stability in the process of discarding private information in terms of logical automation.

Key Words : Correction Factor, Discard, Document Destruction, Objectivity, Personal Information, Quantitative Judgment, Verificatio

* Security 분야 Freelancer (주저자)

Ⅰ. 서론

일반 기업으로부터 공공 및 행정기관에 이르기까지 개인정보보호법이 제정된 이후 2018년 현재까지 법의 유권해석과 지침 및 준거성을 기반으로 하는 과정 속에서 개인정보에 대한 보유를 최소화 하고 대내외 서비스를 지원하는 정보시스템 및 행정 업무 등을 최적화 하는 일련의 과정들을 수년간에 걸쳐 시행하고 지금은 개인정보를 최소화하고 관련법에서 존치를 허용하는 범주내에서 관리와 안전성 및 기밀성 무결성을 위한 정보보안 인프라를 구현하고 있다. 하지만 개인정보는 특정한 목적을 위해 대부분 생성되고 때로는 비식별화 되어 기관 내부 또는 외부 유관기관으로의 불특정 다수 중 특정인을 지칭할 수 없는 정보로 변경 및 변형이 되어 사용되고 운영 및 법이 허용하는 범주 내에서 보존과 지속적 관리가 이루어지고 있다[1-3].

그리고 그러한 일련의 활용과 가치의 소멸 또는 법과 지침에서 요구하는 문서의 보존연한에 의해 개인정보가 포함된 문서 또한 동일한 문서의 보존연한에 의해 오프라인 문서의 경우 폐기 또는 파기의 정책적 폐기시스템의 흐름에 적용을 받는다. 물론 온라인 정보시스템에서 운영하고 있는 개인정보의 경우는 코딩되어진 법적 조건과 지침에 의한 또는 약관에 의한 철저한 파기과정과 재활용 및 복구과정을 할 수 없는 전자적 조치를 하고 있다. 하지만 오프라인의 경우는 온라인과는 다르게 폐기 대상을 확인해야하고 대상마다의 보유 개인정보의 형태와 내용, 용도, 폐기량, 폐기목적, 폐기기간, 폐기업체, 폐기방법, 폐기확인, 폐기 검증, 폐기검증 보증 과정 등 복잡도가 해당 업무를 수행하는 인력이 조직 전체적으로 참여를 독려하고 각 문서를 보유한 유기적인 부서들을 하나의 조직체로 재 구성하고 정확한 정책적 폐기시스템이 정해진 최적화 및 표준화된 프로세스에 의해 폐기 될 수 있도록 해야 하는 문제점이 항상 잔존하고 있다[4-5].

따라서 본 논문에서는 온라인이 아닌 정책적인 논리적인 그리고 물리적인 개인정보를 보유한 또는 포함하고 있는 문서에 대한 정확한 폐기 절차와 절차에 대한 결과를 보증할 수 있도록 하는 방안을 제안하고자 한다. 이와 같은 논문의 방향성을 이해하고 서술하는데 있어서 1장에서는 연구 개요를 언급하고 2장에서는 현재 시장에서 개인정보와 일반문서가 혼용되어 폐기되는 상황을 파악하는 관련연구와 3장에서는 법적기준 준수를 위한 개인정보 폐기 시스템을 활용한 폐기 누적현황 데이터베이스 정책적 구축 방안 제안하고 4장에서는 폐기 누적현황 데이터베이스 구축현황에 대한 검증과 구현을 정책적으로 오프라인 상황에서 시연하도록 할 것이다. 마지막으로 5장에서는 최종 결론을 통한 논문에서 제시하고자 한 정책적 폐기시스템에 대한 효율성과 안전성을 제시하고자 한다.

Ⅱ. 관련연구

연구과제 또는 과제로써 본 논문의 제안과 아이디어를 기술하기 보다는 개인정보의 안전성과 기밀성 그리고 무결성을 보존하는 가운데 재활용을 당함으로써 개개인에게 침해되는 인권 또는 민감정보 등을 활용한 인신공격, 금전적 손해 등과 같은 일련의 사건사고를 막고자하는데 그 의의가 있다[6]. 따라서 현시점에서 개인정보가 포함된 일반문서와 개인정보의 현황을 철저히 분리하고 분리된 정보를 가지고 정확한 누적 데이터베이스를 구축함으로써 정책적 폐기시스템을 기업마다 구동 시에 적절하게 표준절차로써 활용 가능하도록 제안하고자 한다[7].

2.1 문서 보존 연한에 관한 법 또는 지침 현황

공공기간 및 행정기관의 경우는 주간 문서 보존을 위한 행정기관에서 주도적으로 지침과 관련 방침 등을 제정하고 이를 각 기관에서 활용하고 표준화를 하는 과정을 통해 모든 일반문서를 비롯하여 개인정보를 포함한 문서 일체에 대해 영구, 반영구, 30년, 10년, 5년, 3년, 1년 단위로 현재는 문서의 보존연한의 기준이 있다[8-9]. 물론 관련 법 또는 보전을 위한 폐기기간 연장 관련 법률이 우선하는 경우는 해당 지침 상의 보존연한을 연장해서 보관 및 활용 가능하기도 하다. 하지만 기본적으로 일반문서와 개인정보가 포함된 모든 문서는 <표 1>과 같이 주어진 일정기간의 폐기를 위한 기본 보존연한을 가진다[10].

<표 1> 공공기관 문서보존을 위한 보존연한에 관한 법률 또는 지침현황

조항	보존연한	관련법률
제26조(보존기간)	영구	공공기록물 관리에 관한 법률
	준영구	
	30년	
	10년	
	5년	
	3년	
	1년	

우선 모든 문서의 생성은 일반문서를 기준으로 생성되고 이후 개인정보 등이 해당 문서의 내용에 추가되는 경우 별도의 개인정보보호법에 의거 각 법률 보장에 의한 특별문서로 분류되고 취급자 및 책임자와 기록물 관리자에 의해 별도의 보존연한과 관련 법률에 의거 이원화된 관리를 받아 보존 및 폐기 과정을 거친다. 따라서 향후 정책적 폐기시스템에 따른 처리에도 별도의 심의와 선정, 의안 상정 및 결의에 의한 폐기가 진행된다[11].

2.2 일반 문서 및 특화된 개인정보 기록 문서에 대한 법적기준과 보관사례

일반문서의 경우는 기록물관리에 관한 법률에 준하여, 보존연한이 선정되고 각 해당 문서의 분류에 따른 보존연한이 도래하거나 연장을 목적성의 기반한 기록물 심의위원회의 심의에 의해 연장하여, 재관리 및 활용 후 폐기를 진행한다. 물론 영원한 영구문서는 현재로써는 그 기간의 제한을 두고 자제하고 있는 상황으로 해당 문서에 별도의 개인정보가 포함되는 경우는 또 다른 법률의 영향을 받아 보존연한의 연계 및 확대와 폐기의 연장이 이루어지기도 한다[12]. 다만, 기록을 연장하고 보존연한에 대한 확실한 기간연장의 법률에 근거하는 경우는 기존의 일반문서로써 보존하던 방법과는 달리 물리적, 논리적 그리고 정책적으로 별도의 안전성 확보를 기반으로 하는 일련의 기술과 방법을 제공하고 암호화 등과 같은 유출과 노출의 위험성 배제 기술까지도 적용해서 관리해하기도 한다[13]. 따라서 <표 2>와 같이 연장되는 법률에 의한 보존과 폐기는 특별한 제3의 과정과 절차를 확보해야 한다.

<표 2> 개인정보보호법에 의한 개인정보 파기에 관한 법률 요약현황

법률	조항	법률요약
개인정보 보호법	제21조 (개인정보의 파기)	[요약] 보유기간의 경과, 처리 목적 달성으로 개인정보의 사용이 불필요하게 되었을 때, 즉시 파기. 다만, 다른 법령에 따라 보존하여야 하는 경우는 제외. 또한, 파기할 때에는 복구되지 않도록 조치하고 보존하여야 하는 경우에는 다른 개인정보와 분리하여 저장 및 관리하여야 한다. 이외 법률에 준한다.

이러한 추가적인 폐기 연장은 안전성확보조치 기준에 의한 물리적 보호조치까지 그 범주를확대해서 문서의 폐기 이전까지의 라이프사이클에 대한 보안성을 확보해야 한다[14].

2.3 다양한 온라인 및 오프라인 문서 파기를 위한 폐기시스템 활용 현황

이제 일반문서와 개인정보가 포함된 문서의 차이점을 명확히 구분 가능하고 이를 관리하는 부분에 대해서도 보존과 폐기라는 2가지 범주로 대분류함으로써 관리의 형태를 <표 3>과 같이 별도의 형태로 분리 운영한다. 이는 복잡한 문서의 이원화를 통한 번거로운 기록물 관리의 또 다른 행정업무의 확대가 아니라 절차적 관리의 편의성 확보를 위한 시작으로 판단하고 접근하면, 된다[15-16].

<표 3> 개인정보보호법 등 관련법에 의한 일반문서와 개인정보 보유 문서 파기 및 폐기시스템 운영현황과 사례

구분	보존연한	처리방법	사례
일반문서	영구, 준영구, 30년, 10년, 5년, 3년, 1년 (* 단, 보존 관련 법률 존재 및 근거에 의거)	공공기록물 관리에 관한 법률에 의거 심의, 판단, 집행	기록물 처리 시에 혼합 중량 기준으로 일괄 파기 (* 개인정보 파기대장을 보유하고는 있으나, 세부적인 파기 내역을 정확히 기록하기에는 현실적 어려움 발생)
개인정보 보유문서		개인정보 보호법 및 관련법에 의거 심의, 판단, 집행	

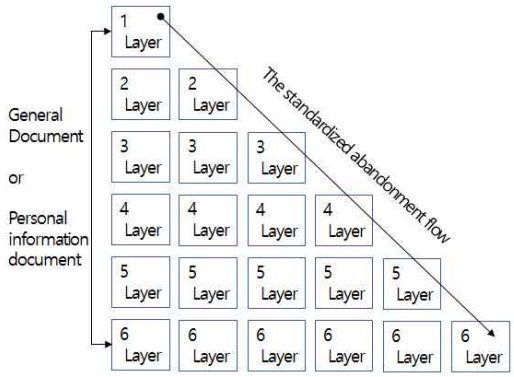
Ⅲ. 법적기준 준수를 위한 개인정보 폐기시스템을 활용한 폐기 누적현황 데이터베이스 정책적 구축 방안 제안

개인정보를 포함한 일반문서를 파기하는 방법으로는 우선 인력적인 추가 증원이 필수적인 조건으로 지속적인 인력 부족의 문제점으로 도출된다. 즉 정책적 폐기시스템은 단순히 일반문서에 어떠한 개인정보가 있었느냐 라는 단순한 확인과정이 아니라 반드시 기업마다 주기적 지침에 따른 문서연한 기준을 준수하고 일반문서와 개인정보가 포함된 문서를 이원화하는 과종을 시작으로 보존, 관리, 운영, 활용, 이관, 폐기까지 별개의 정책적 폐기시스템은 프로세스를 구현해야 한다. 물론 현 시점에서의 인력과 물리적, 관리적 자원의 투입은 경비와 비용면에서 큰 부담으로 작용되어질 여지는 있으나, 표준화된 프로세스를 구축하는 기술적인 측면으로 본다면, 과도기적인 정책적 프로세스 구현을 위한 컨설팅과 같은 부분이다. 따라서 반드시 시행하고 연구해야 할 학문적 부분일 것이다.

3.1 객관성 및 기밀성, 무결성 보증의 폐기 정보에 대한 정책적 구현 방안 환경 제시

개인정보를 담고 있는 특수 관리가 필요한 문서로의 변화는 <그림 1>과 같이 다수의 불특정 다수의 문서를 대상으로 정책적 폐기시스템 6단계에 대한 적용 단계를 결국에는 순차적인 생성으로부터 판단과 검증이 이루어진 최종 폐기 결과까지의 방안을 표준화로 제시하고 있다. 다만, 3단계에 준하는 안정화 시점에 따른 개선 및 폐기에 대한 안전성 보증사항과 선정을 위한 정확한 개인정보 폐기 상황 증명, 폐기내역에 대한 현황 검증, 기업별 보유 개인정보 누적 데이터베이스 관리, 향후 필수 보유 개인정보

에 대한 범주 파악, 폐기 보정 계수 파악, 일괄폐기로 인한 미폐기 개인정보 현황 파악, 일반 문서파기로부터 개인정보 파기 과정 분리를 통한 전문성 및 객관성 확보, 무게 및 중량 중심의 정성적 판단 지양, 개인정보 폐기대장과 일반 문서 폐기대장과의 분리, 일반 문서관리의 개념 탈피, 개인정보 파기에 대한 책임과 역량에 관한 조직 및 인력 양성 가정을 준수해야만 한다.



<그림 1> 현재 시행하는 폐기방식의 정책적 시스템 운영의 문제점 도출 환경 파악

따라서 단일 문서의 특수문서로의 변화와 보존 및 폐기의 절차는 정책적인 폐기시스템의 순차적 절차에 기반하는 단계를 거쳐서 업무를 적용한다면, 별도의 기록물 관리와 같이 또 다른 문서관리의 프로세스로 분리되어 이원화된 업무의 추가로 이어지지는 않는다는 것이다.

3.2 폐기 및 말소에 따른 재활용 불가를 위한 법적 제도적 안전장치에 대한 기준 설정

기록물관리에 관한 법률과 게인정보보호법에서는 두 가지 주요한 문서를 대상으로 하는 <표 4>와 같은 조항을 갖는데, 이는 첫 번째로는 파기를 위한 방안으로는 두 법률 모두 명확하게 법률 상에서 기록물의 안전성을 확보하기 위해 어떠한 문서든 개인정보가 포함된 경우는 파기할 때에는 복구 또는 재생되지 아니하도록 조치해야 한다는 기술적 접근과 행위를 요구하고 있으며, 또한 보존에 있어서도 반드시 보존에 대한 명확한 관련 법률을 요구하고 이를 기반으로 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장 및 관리해야 한다는 별도의 안전성확보조치기준을 요구한다.

<표 4> 문서 폐기 및 파기에 대한 법적 제도적 안정장치 현황과 기밀성과 안전성 확보를 위한 기준

법률	구분	처리방법
개인정보보호법	파기	개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치
	보존	개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장 · 관리 (* 안전성확보조치 기준에 의거)

Ⅳ. 폐기 누적현황 데이터베이스 구축현황에 대한 검증과 구현

개인정보가 폐기 되는 시점에 가장 중요한 기록관리 정보로써 발생 가능한 부분인 개인정보의 형태와 내용, 용도, 폐기량, 폐기목적, 폐기기간, 폐기업체, 폐기방법, 폐기확인, 폐기 검증, 폐기검증, 보증과정 결과의 정량적 객관성을 가진 결과 값을 반드시 데이터베이스하 함으로써 향후에도 어떠한 자료가 어떠한 정책적 폐기시스템의 프로세스에 의해서 폐기가 정상적으로 폐기되었고 ㅈ활용 및 재생산되거나 재가공되는 등의 불법적인 인용은 있을 수 없음에 대한 보증을 대외적으로 신뢰성 기반하에 확인

할 수 있도록 해야 한다.

4.1 보존연한과 법적기준에 의한 개인정보 데이터베이스 분류

개인정보가 포함된 일반문서의 경우 기록물관리에 관한 법류의 적용 범주에서 개인정보보호법률로 이관되어 법률의 조항을 적용 받게 되는데, 본 논문에서 제안하는 부분은 단순히 개인정보가 들어 있는 문서를 분류하고 이를 분류별 속성에 맞추어 다시 세부분리를 하고 일괄 중량에 따른 폐기를 하는 방법으로 향후 폐기 이후에 어떠한 문서와 문서 내에 존재했던 개인정보의 실체가 아닌 정확하고 안전하게 그리고 기밀성과 무결성에 위배되지 않은 상태로 적절한 폐기가 이루어졌는지를 확인 가능하도록 하는 정책적 폐기시스템의 프로세스를 제시하고 제안하는 이유는 <표 5>와 같이 폐기된 개인정보가 포함된 문서의 형태, 내용(단, 내용은 암호화 또는 직접적인 개인정보를 삭제되고 개요만을 비식별화 한 상태로 정보화된 내용을 의미), 관려근거(법률), 보존연한, 관리부서, 취급자, 책임자, 용도, 폐기량, 폐기목적, 폐기기간, 폐기업체, 폐기방법, 폐기확인, 폐기검증, 폐기보증에 대한 각각의 하나의 문서에 정책적 폐기시스템 프로세스 적용에 따른 하나의 폐기정보 레코드가 누적되어 최종 데이터베이스로 향후 기관 또는 기업의 누적 정보를 보존함으로써 개인정보의 기밀성과 무결성을 확보한 상태에서의 정확하고 안전한 폐기과정이 이루어졌는지에 대한 검증을 진행하는 것을 계량화 하는 것이다.

<표 5> 개인정보를 보유한 기관 보유 전체 문서에 대한 데이터베이스 분류기준

구분	구성	운영	구현
데이터베이스	형태	주요 검색 주요 핵심 키	하나의 데이터베이스로 구성하되 각 레코드 구성 필드별 특성화 값을 보유. SQL 쿼리로 질의 및 통계관리 가능 코딩
	내용		
	관련근거(법)	KEY에 연계된 레코드 상의 관리 포인트	
	보존연한		
	관리부서		
	취급자		
	책임자		
	용도		
	폐기량	레코드 상의 폐기에 관한 세부 쿼리	
	폐기목적		
	폐기기간		
	폐기업체		
	폐기방법		
	폐기확인		
	폐기검증		
	폐기보증		

4.2 구축 데이터베이스 운영에 따른 개관적 및 안전성 보장 기반의 폐기 검증

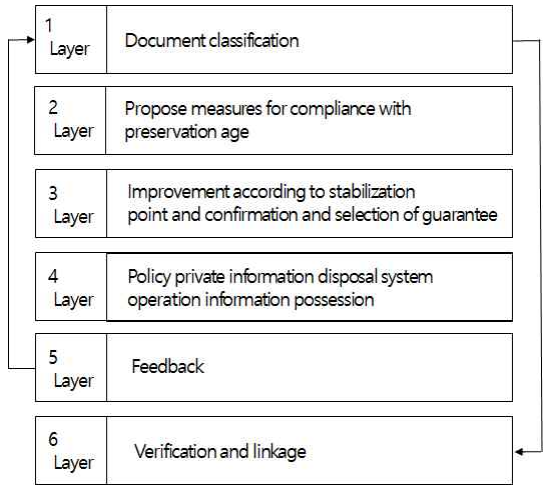
최종적으로 본 논문에서 지속적으로 폐기에 대한 안전성과 기밀성, 무결성에 준하는 폐기정보 데이터베이스를 위한 일련의 절차는 총 6단계로 <표 6>과 같이 1단계는 문서 구분, 2단계 보존연한 준수를 위한 방안 제시, 3단계 안정화 시점에 따른 개선 및 보증사항 확인과 선정, 4단계 정책적 개인정보 폐기시스템 운영, 5단계 피드백, 마지막 6단계는 검증과 연계를 통해서 제안의 완성도를 높이고자 한다. 완성도는 폐기의 안전성을 보증하는 계량적, 정량적 척도이기도 하다.

<표 6> 최종 데이터베이스 분류에 의한 보유연한 만료 정책적 문서 폐기시스템 검증

단계	핵심 행위	주요 내용
1	문서 구분	- 구분대상 : 일반문서, 개인정보 문서 - 구분보유 : 각 부서별 대장 및 파일을 이용한 1단계 분류 기록 관리
2	보존연한 준수를 위한 방안 제시	미파기 장기 보유하는 문제점 지속 발생에 따른 1단계 각 부서별 개인정보취급자가 파악한 기 부서내의 문서를 시점에 준하는 기간에 개별 파기 및 안건 상정으로 확인 및 검증과 보증 인지
3	안전화 시점에 따른 개선 및 보증사항 확인과 선정	정확한 개인정보 폐기 상황 증명, 폐기내역에 대한 현황 검증, 기업별 보유 개인정보 누적 데이터베이스 관리, 향후 필수 보유 개인정보에 대한 범주 파악, 폐기 보정 계수 파악, 일괄폐기로 인한 미폐기 개인정보 현황 파악, 일반 문서파기로부터 개인정보 파기 과정 분리를 통한 전문성 및 객관성 확보, 무게 및 중량 중심의 정성적 판단 지양, 개인정보 폐기대장과 일반 문서 폐기대장과의 분리, 일반 문서 관리의 개념 탈피, 개인정보 파기에 대한 책임과 역량에 관한 조직 및 인력 양성
4	정책적 개인정보 폐기시스템 운영	개인정보의 형태와 내용, 용도, 폐기량, 폐기목적, 폐기기간, 폐기업체, 폐기방법, 폐기확인, 폐기 검증 등 데이터베이스화
5	피드백	
6	검증과 연계	운영하는 기록관 비전자문서 및 서고관리 시스템 등을 활용한 최종 결과 데이터베이스 보존

4.3 최종 누적 데이터베이스 최적화 및 표준화 폐기정책 적용

정책적 폐기시스템은 실제 물리적인 기술 기반의 프로세스가 아닌 관리적 측면에서의 논리적 업무 프로세스로써 <그림 2>와 같이 5단계의 문서 구분으로부터 검증 이전의 피드백까지의 반복적 폐기 데이터베이스 확인과 생성을 기반으로 하고 마지막 폐기 완료시에 최종 6단계 검증과 타 기록물 관리 및 서고관리 시스템과의 정략적 연계를 통해 확실한 폐기가 이루어졌음을 재확인하는 과정을 갖는다.



<그림 2> 최적 및 표준화 개인정보 보유 문서 폐기를 위한 절차를 포함한 정책적 폐기시스템 구현

Ⅴ. 결론

본 연구에서는 단순한 물리적인 파기를 정책적 폐기시스템이라는 펴현으로 기술한 것으로 개인정보 파기과정을 단순하게 그 범주를 이해할 수도 있으나, 이해와 노력 및 연구의 대상으로 언급한 부분은 총 6단계에 걸친 정책적 폐기시스템의 프로세를 구동하고 유관기관 또는 표준화 정책을 제안하고 관장이 가능한 기관이나 기업이 최적화 및 표준화 과정을 제시하고 이를 배포함으로써 개인정보가 파기되는 순간부터 다시 개인정보는 실제 폐기되어진 것이아니라 언제든 재활용, 재사용, 재운영이 될 수 없는 향태로 완벽하게 그리고 철저한 폐기 프로세스에 의한 파기되었음을 증명하고 보증할 수 있어야 한다. 현재 가장 단순한 문서파기 방법으로 지급도 사

용하고 있는 중량에 따른 무게에 따른 일괄파기 방법을 통해서 물론 어떠한 내용이 개인정보가 있는 문서인지도 확인할 필요성 없이 무조건 내용연한에 따라 전문성과 전문인력, 전문장비를 가지고 파기하기 때문에 어떠한 개인정보의 재활용은 있을 수 없음을 증명하기도 한다. 하지만 본 논문에서 연구하고 제안하는 부분은 단순한 파기의 명확성과 객관성 보존이 아니라 폐기된 개인정보의 데이터베이스를 구축하고 다양한 정보인 형태와 내용, 용도, 폐기량, 폐기목적, 폐기기간, 폐기업체, 폐기방법, 폐기확인, 폐기 검증, 폐기검증, 보증과정과 같은 기록을 누적하고 향후 수십년 이후에도 기업 또는 기관에서 현황을 파악하고 개인정보뿐만아니라 이외의 중요정보 또는 신기술에 의해 파생되는 정보들과 데이터들에 대한 새로운 정책을 적용하고자 할 때 반영가능한 최적의 과정과 누적정보를 공유하고 활용함으로써 또 다른 환경에서도 적응성을 가진 정책적 폐기 시스템 프로세스와 데이터베이스를 구축하고자하는 것이다. 따라서 향후 연구방향으로는 개인정보뿐만 아니라 다양한 정보와 데이터 뿐만아니라 실제 물리적인 정보자산에 이르기까지 그 대상을 확대해서 운영함으로써 확대 연구가 이루어져야 한다.

참고문헌

[1] 김태경, “개인속성 정보의 결합을 통한 강화된 인증방안에 대한 연구,”디지털산업정보학회논문지, 10권, 2호, 2014, pp.83-89.

[2] 민소연, 장승재, “익명 게시판 환경에서 가상 아이디를 이용한 개인정보보호에 관한 연구,” 한국산학기술학회논문지, 13권, 9호, 2012.

[3] 민소연, 진병욱, “U-Health환경에서 안전한 개인정보 관리를 위한 통합 인증스키마 설계,” 한국산학기술학회논문지, 15권 6호 pp.3865-3871, 2014.

[4] 최철재, 이영식, 이태희, “개인정보보호를 위한 ELIS의 자치법규서식 개선방안,” 한국전자통신학회논문지, 11권, 11호, 2016, pp.1017-1024.

[5] 정혜인, 김성준, “개인정보관리체계계(PIMS)를 이용한 클라우드컴퓨팅 개인정보 보안 개선 방안 연구,” 디지털산업정보학회논문지, 12권, 3호, 2016, pp.133-155.

[6] 김윤식, “계정과 개인정보의 연관성 연구,” 디지털산업정보학회논문지, 2권, 4호, 2006, pp.1-7.

[7] 배윤조, 이소영, “환자 개인정보 보호에 대한 학생간호사의 지식과 인식의 연구,” 한국산학기술학회논문지, 17권, 1호, 2016, pp.36-44.

[8] 서동진, 김태성, “개인정보 보안취약성과 지각된 유용성이 지속적인 은행이용의도에 미치는 영향,” 한국통신학회논문지, 40권, 8호, 2015, pp.1577- 1587.

[9] 김태경, “호텔 이용 고객의 개인정보 비식별화 방안에 관한 연구,” 디지털산업정보학회논문지, 12권, 4호, 2016, pp.61-68.

[10] 차기정, 하영미, “의료기관 근로자의 환자 개인정보 보호 인식에 대한 평가도구 개발 및 검증,” 한국산학기술학회논문지, 16권, 2호, 2015, pp.1253-1263.

[11] 최보미, 채상미, 김민균, 강연정, “GDPR 환경에서 국내 개인정보보호 관련 인증제도 및 표준 발전방향에 대한 연구,” 한국통신학회논문지, 43권, 2호, 2018, pp.416-426.

[12] 최희식, 조양현, “빅데이터 개인정보 취급에 따른 문제점 분석,” 디지털산업정보학회논문지, 10권, 1호, 2014, pp.89-97.

[13] 장지혜, 복화정, 김연서, 최진식, 최철재, “지방자치단체 공공기관의 개인정보보호에 관한 인식 수준 분석,” 한국전자통신학회논문지, 11권, 3호,

2016, pp.345-350.

[14] 조성규, 전문석, “개인정보 영향평가 수행 사례에 기반한 기관의 개인정보보호법 대응방안에 관한 연구,” 디지털산업정보학회논문지, 8권, 1호, 2012, pp.89-98.

[15] 최희식, 조양현, “모바일 환경에서 개인정보 유출 방지를 위한 개선 연구,” 디지털산업정보학회논문지, 11권, 3호, 2015, pp.53-62.

[16] 전성철, 김인경, “인터넷 이용자의 개인정보 유출 가능성에 대한 심리적 불안에 관한 연구 : 성별, 이용량, 이용 빈도를 중심으로,” 한국전자통신학회논문지, 6권, 5호, 2011, pp.731~737.

■ 저자소개 ■

서우석
(Seo Wooseok)

2006년 8월 : 숭실대학교 정보과학대학원 정보통 신융합학과 석사
2013년 2월 : 숭실대학교 일반대학권 컴퓨터학과 박사
2006년 4월 ~ 2012년 12월 : 서울특별시용산구시설관리공단 전산총괄
2012년 12월 ~ 2017년 1월 : 주식회사 이지서티 보안사업본부 본부장(이사), 개인정보보호센터 센터장(이사)
2017년 2월 ~ 현재 : Security 관련분야 Freelancer

관심분야 : 4차 산업, ICT, IOT, 정보경영, 정보보안, 개인정보, 비식별화, 정보화 전략기획(ISP), 정보화 관리체계, 실태점검, 빅데이터, 인공지능(AI), PIMS, ISMS 인증
E-mail : ssws2000@nate.com

논문접수일 : 2018년 07월 27일
수 정 일 : 2018년 07월 31일
게재확정일 : 2018년 08월 01일