개인정보 수명주기에 따른 개인정보관리모델에 관한 연구

김현철, 고재우, 최명길

인제대학교 시스템경영공학과
(621-749) 경상남도 김해시 어방동 607
Tel:055-320-3813, Fax:055-320-3632, E-mail: mgchoi@inje.ac.kr, hckim119@gmail.com, kokoko1111@nate.com

Abstract

인터넷은 개인과 조직간의 정보를 원활하게 유통시키는 역할을 하고 있지만, 개인정보를 노출시키는 부작용을 낳고 있다. 특히 개인정보의 가치가 증요시되고 있는 상황에서 개인정보를 보호할 수 있는 보호대책이 필요하다. 본 연구는 개인정보의 수집, 저장, 이용, 파기와 같은 수명주기에 따른 개인정보 관리모델을 제시하고자 한다. 개인정보 관리모델은 각 개인정보 수명주기에 따라 개인정보 관리자가 수립해야 할 개인정보보호정책, 개인정보보호를 위한 기술적 대책, 기술적 대책 및 프로세스를 관리할 수 있는 관리적 대책을 서술한다. 본 연구는 제안된 개인정보 관리모델을 구현할 수 있는 개념적인 아키텍처를 제시한다. 본 연구는 개인정보의 수명주기에 따른 개인정보보호를 위해서 필요한 개인정보정책, 기술적인 대책, 관리적인 대책을 제시했다는 데 의의가 있다.

Keywords :

개인정보 수명주기,개인정보침해,개인정보관리모델

1. 서론

인터넷의 발달과 더불어 인터넷 사용 인구는 기하급수적으로 증가하고 있는 상황이며, OECD 보고서에 의하면, 2006 년 우리 나라의 인터넷 보급률 전 세계의 1 위로 70.5%에 달하고 있다[3][4]. 그러나 인터넷의 확산과 더불어 개인정보의 유출이 급속히 확산되고 있어, 전자상거래를 위축시키고 있다. 개인 명의 도용 건수가 1 천 8 백 2 건이라는 보고가 있다[2]. 동 보고는 개인정보의 유출이 광범위하게 이루어지고 있음을 나타내고 있다. 정부는 개인정보보호를 위해서 개인정보보호법 등의 제정하여 제도적으로 개인정보를 보호하는 노력을 기울이고 있다[5][6]. 그러나 이러한 제도적인 노력을 뒷받침하기 위해서는 개인정보 제공자, 개인정보관리자, 개인정보활용자 등의 권익을 보호하고, 개인정보 유통을 추적할 수 있는 관리적 체계 및 기술적 체계가 필요하다.

본 연구는 개인정보관리 라이프사이클[1]인 개인정보의 수집, 저장, 이용, 파기 등을 지원할 수 있는 개인정보 관리모델 및 관리모델의 구현방안을 제시한다. 본 연구는 관리모델을 제시하기 전에 개인정보 각 라이프사이클에서 발생할 수 있는 보안 위협을 식별하고, 각 보안 위협에 대하여 서술한다.

2. 개인정보 침해 유형

[표 1]은 개인정보 라이프사이클별로 발생할 수 있는 침해 유형을 서술하고 있다. 침해유형은 불법수집, 오류, 부당한 접속, 2 차적 사용 등이며, 각각의 침해는 수집단계, 처리단계, 보관단계, 이용단계 등에서 발생할 수 있다[7].

[표 1] 개인정보의 침해 유형

발생 단계	침해 유형	구체적인 침해행위
수집 단계	불법 수집	- 정보주체의 동의 없는 개인정보 수집 - 개인의 사생활이나 권리를 침해할 수 있는 정보수집
처리 단계	오류	- 잘못된 정보의 기록 - 변경된 정보를 수정하지 않음
보관 단계	부당한 접속	- 자료의 불법유출(내부인의 유출, 업무상 취득한 개인정보비밀의 누설, 외부인의 물리적 침투에 의한 유출, 관리소홀로 인한 유출) - 자료의 불법열람 - 해킹 혹은 바이러스 감염 등에 의한 자료열람, 삽입, 변조, 파괴 - 해킹 등에 의한 자료의 도난
이용 단계	이차적 사용	- 수집목적 이외의 용도로 정보를 활용하는 행위 - 정보주체의 동의를 구하지 않은 채, 제3자에게 정보를 제공하거나 판매하는 행위 - 동의가 철회되거나 수집목적이 달성된 자료의 불법보유

2.1 불법수집

개인이 자신의 정보 제공을 동의하고, 개인정보를 제공하는 것이 당연하지만, 인가되지 않은 3 자는 바이러스, 웜, 트로이목마, 스파이웨어, 스팸 메일 등을 이용하여 사용자가 인지하지 못한 방식으로 불법적으로 개인의 정보를 수집한다. 이러한 개인이 인지하지 못하는 형태로 개인의 정보가 유출됨으로 개인 신용정보에 대한 무단 열람, 개인이 원하지 않은 스팸 메일 발송으로 인한 정보자원 낭비, 개인정보의 무차별적인 활용을 통해 개인의 경제 행위 및 법률 행위에 많은 손해를 발생시킬 수 있다.

2.2 오류

개인정보는 정적개인정보와 동적개인정보로 구분될 수 있다[9]. 동적개인정보는 시간이 경과함에 따라 내용이 변화하는 정보를 의미하며, 개인정보 수집자가 변화된 개인정보를 데이터베이스에 갱신하지 못하는 경우에 개인에 대한 부정확한 정보가 발생한다. 따라서 개인은 자신에게 적절한 정보를 제공자로부터 수신받지 못하는 경우가 발생한다. 정적개인정보는 시간이 지나도 변화지 않는 정보이다.

2.3 부당한 접속

비인가자가 개인정보를 저장하고 있는 데이터베이스 접속할 경우, 개인정보의 유출·변경·삭제가 발생한다[8]. 개인정보의 임의적인 변경 및 삭제는 개인정보 수집자 및 활용자가 개인정보를 더 이상 활용할 수 없는 피해가 발생한다. 개인정보의 임의적인 변경은 개인정보 제공자의 정보가 관련 활용자에게 잘못 전달됨으로 개인정보 제공자가 원하는 정보를 수신하지 못하는 기회 비용이 발생한다.

2.4 이차적 사용

특정한 목적을 위하여 수집된 개인정보가 정보제공자의 동의 또는 허가 없이 다른 목적으로 재사용되는 경우 개인정보 침해가 발생된다. 최근 개인정보가 기업 경영에 중요한 자원으로 인식됨에 따라 이를 상업적으로 사용하려는 경향이 증가하고 정보중개업을 전문으로 하는 기업이 발생함에 따라 개인정보의 이차적 사용은 더욱 심각한 문제로 대두되고 있다.

3. 개인정보 관리모델

3.1 수명주기에 따른 개인정보보호 관리모델

본 장은 개인정보 침해로부터 개인정보를 안전하게 관리할 수 있는 개인정보 관리 모델을 제시한다. 개인정보 관리 모델은 개인정보 수집, 처리, 보관 이용 등 일련의 개인정보 수명주기에 걸쳐 개인정보를 효과적으로 관리할 수 있는 방법을 제시하고 있다.

[표 4]는 본 연구가 제안하는 개인정보를 보호하는 관리 모델로서 개인정보 수명주기에 따라 발생할 수 있는 침해에 대응할 수 있는 정책적 대책, 관리적 대책, 기술적 대책을 제시하고 있다.

정보의 수집단계에서 발생할 수 있는 정책적 대책은 다음과 같다. 개인정보수집자는 개인정보제공자에게 개인정보 수집 목적을 명확하게 제시해야 한다. 명확하게 제시된 수집된 목적은 개인정보제공자가 자신의 개인정보를 제공할지 여부를 결정할 수 있는 판단 기준이 되며, 추후 자신의 개인정보의 불법적인 사용 여부를 판단할 수 있는 기준이 된다. 개인정보수집자는 개인정보제공자에게 개인정보관리 방침을 명확하게 명시해야 한다. 명확한 관리방침의 명시는 개인정보제공자가 추후 발생할 수 있는 침해에 대해서 개인정보수집자에게 항의할 수 있는 근거가 된다. 개인정보수집자는 수집단계에서 기술적인 대책과 관리적인 대책을 동시에 수립해야 한다. 개인정보수집자는 개인정보보호정책을 관련자들이 숙지할 수 있도록 XML, HTML 등을 이용하여 홈페이지, 메일 등을 이용하여 관련자들이 쉽게 접근할 수 있도록 한다. 개인정보보호정책이 서술해야 하는 내용은 개인정보의 수집의 명확한 목적, 개인정보 유효기간, 제공처, 수집에 대한 이력관리, 관리방법 및 절차 등을 명기한다.

개인정보의 저장 및 관리 단계에서 개인정보수집자는 저장되는 데이터의 안전한 저장 정책 및 저장 기간 정책을 수립한다. 수립된 정책의 구현을 위해서 수집자는 기술적 대책 및 관리적 대책을 수립해야 한다. 기술적 대책은 저장된 데이터의 안전한 보관을 위해서 데이터베이스 암호화 및 네트워크 암호화 대책, 데이터베이스에 대한 접근 관리 대책 및 인가 관리 대책을 수립한다. 수립된 기술적 대책의 관리를 위해서 개인정보관리자는 데이터베이스의 접근 권한의 관리 및 문서화한다. 을 관리하고 이를 문서화 한다. 개인정보관리자는 수집한 개인정보의 유효기간을 정책에 명시하고, 개인정보정책에 따라 운영한다. 그리고, 관리자는 여러 가지 침해 요인으로부터 개인정보의 보호를 위해 정기적인 점검 및 유효성 검증을 실시한다.

개인정보의 이용 및 제공단계에서는 개인정보 관리자는 다음과 같은 3 가지 정책을 수립한다. 첫째, 명시된 목적 외의 수집된 정보와의 혼합을 억제한다. 둘째, 분석의 결과의 실제 활용을 위해서는 사전 동의 및 사후 승인을 반드시 하도록 명시화한다. 셋째, 제 3 자에게 개인정보를 이전을 금지하는 정책을 수립한다. 개인정보관리자는 수립된 정책의

구현을 위해서 침해차단기술, DB 및 네트워크의 암호화 및 관제 기술, 개인정보 유출차단 기술, 접근 및 인가관리 기술을 사용할 수 있다. 동 기술의 관리를 위해서 개인정보관리자는 기타 정보와 개인정보와의 혼합을 허용하지 않고, 분석 결과를 로그형태로 기록한다. 분석 결과를 사용할 경우, 사전 동의 및 사후 승인을 득해야 한다. 그리고, 제 3 자에게 수집한 정보가 제공되지 않도록 모든 조치를 취하고, 이를 운영한다.

개인정보파기단계에서의 개인정보관리자는 정보의 유효기간 및 완벽하게 정보를 파기할 것을 명시하는 정책을 수립한다. 이 단계에서 개인정보관리자가 수립해야 하는 기술적 대책은 접근 및 인가관리이다. 이 단계에서 개인정보관리자가 수립해야 하는 관리적인 대책은 유효기간이 경과한 개인정보(백업포함)를 파기하는 절차 및 책임을 개인정보 관리방침으로 만들고, 파기할 때에는 복구가 불가능한 형태로 파기할 수 있도록 한다.

[표 2] 개인정보관리모델

구분	정책적 측면	기술적 측면	관리적 측면
정보의 수집	-개인정보 수집 목적의 명확성 -개인정보 수집 후 관리방침을 명시	-개인정보보호정책 설정 및 운영관리 -개인정보인증기술	-개인정보 수집의 명확한 목적을 개인정보보호정책에 명시한다. -수집된 개인정보는 목적, 유효기간, 제공처 등의 사항을 명시한다. -개인정보 수집에 대한 이력관리를 한다. -개인정보의 관리방법 및 절차를 명시한다.
정보의 저장/관리	-저장되는 데이터베이스 및 기타 유해성에 대한 보호 -개인정보의 유효기간 준수	-DB 및 네트워크의 암호화 및 관제 -개인정보관리 -개인정보보호정책 설정 및 운영관리 -접근 및 인가에 대한 관리	-DB의 접근권한을 관리하고 이를 문서화 한다. -수집한 개인정보에 대한 유효기간을 정책에 명시하고, 기간 후, 개인정보 처리지침을 설정/운영 한다. -접근과 인가에 관한 절차를 운영하며, 기타 여러 가지 침해 요인으로부터의 보호를 위해 정기적인 점검 및 유효성 검증을 한다.
정보의 이용/제공	-명시된 목적 외의 수집된 정보와의 혼합 억제 -분석의 결과의 실제 활용을 위해서는 사전 동의 및 사후승인이 필요 -제3자의 정보 이전 불가	-개인정보보호정책 설정 및 운영관리 -프라이버시 침해 차단 -DB 및 네트워크의 암호화 및 관제 -개인정보 유출 차단 -접근 및 인가에 대한 관리	-목적 외 수집된 정보와의 혼합은 허용되지 않으며 분석의 모든 결과는 로그형태로 기록한다. -분석 결과로 인하여 어떠한 실행을 할 경우, 사전 동의 및 사후승인을 득해야 한다. -제3자에게 수집한 정보가 제공되지 않도록 모든 조치를 취하고, 이를 운영한다. -접근이 허가된 작업자에 한하여 분석되며, 이를 유출할 수 없도록 운영 및 관리한다.
정보의 파기	-정보의 유효기간 준수 -완벽한 정보 파기	-개인정보 관리 -개인정보보호정책 설정 및 운영관리 -접근 및 인가에 대한 관리	-유효기간이 경과한 개인정보(백업포함)를 파기하는 절차 및 책임을 개인정보 관리방침에 명시하고 이를 이행한다. -파기할 때에는 복구가 불가능한 형태로 파기한다.

3.2 개인정보보호 관리 아키텍처

개인정보 관리 모델을 구현할 수 있는 개념적인 아키텍처는 [그림 2]와 같이 나타낼 수 있다. 아키텍처는 개인정보 수명주기 각각을 MODULE 로 할당하였다(단, 파기단계는 시스템내부로 할당).

쉬운 이해를 위해 개인정보 흐름(개인정보 생명주기)에 따른 단계적 설명은 아래와 같다.

Step 1(수집): 개인정보수집자(Collect Module)는 개인정보 필요시 개인정보제공자/제공대상자(Person / Privacy Data)에게 개인정보보호 정책을 주지시킨다. 개인정보제공자/제공대상자(Person/Privacy Data)는 개인정보보호정책을 토대로 제공여부 결정한다.개인정보보호정책은 개인정보의 수집 및 이용 목적, 개인정보의 관리 방침, 유효기간 등을 명백하게 제시한다. 수집된 개인정보는 원본이 되는 개인정보에 시스템에서 부여한 정보를 추가한다. 추가되는 정보는 출처, 유효기간 등과 같은 관리에 필요한 정보에 한정해야 한다.

Step 2(저장/관리): 수집된 개인정보는 Encryption Module에 의하여 암호화 되어 Collect Repository에 저장된다. 암호화된 개인정보는 다시 DB Sector 로 나누어져 저장된다. (즉, 앞서 언급한 X=A+B+C; X 는 수집된 정보)

Step 3(저장/관리/이용): 개인정보는 종합/분석하기 위해 흩어진 각 개인정보들을 Mixing 하여, (즉, A+B+C=X; A, B, C 는 분할된 정보) Decryption Module 서 복호화 과정을 거쳐 Analysis Module 로 이동하게 된다. Analysis Module 은 분석을 위한 여러 툴들을 가지고 있다.

Step 4(저장/관리): 분석된 결과들은 Analysis Repository 에 암호화 되어 저장된다. Analysis Repository 는 분야, 목적/동기 등으로 분류된 DB들의 집합이라 할 수 있다.

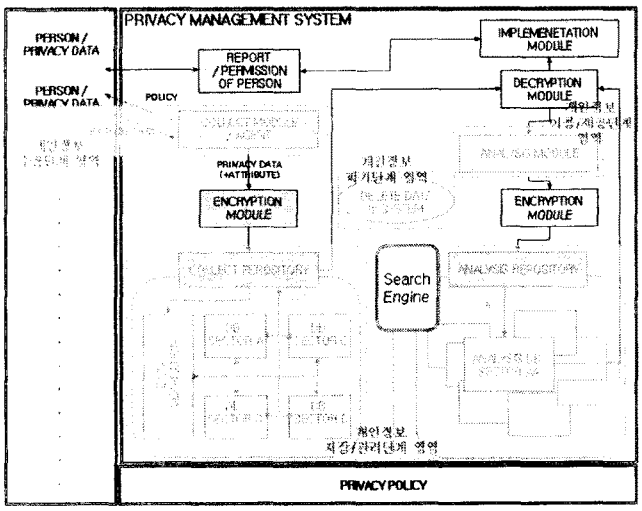
Step 5(이용/제공): 분석은 결과에 따라 시스템 안에서만 실행이 될 수도 있지만, 다른 시스템이나 조직에서 실행될 수도 있다. 여기서 주의해야 할 사항은 개인정보 수집단계에서 그 목적이 실행의 구체적인 명시를 하지 않았다면, 개인정보제공자를 대상으로 실행에 대한 승인을 득해야 한다. 즉, 수집단계에서는 시스템 안에서만 명시하였지만, 실제적으로 다른 시스템(다른 조직)에서 실행하게 되는 경우에는 사후승인을 개인정보제공자에게 해야한다.

Step 6(관리/파기): Repository 에 있는 모든 DB들은 정보 제공자나 유효기간 등과 같은 시스템 안에서 확인되고 있는 Attribute(시스템이 부여한 정보)를 가지고 있다. 특히나 유효기간이 만기된 정보는 자동적으로 DB에서 삭제되도록 되어야 한다.

Step 7(이용/관리): Search Engine 을 통하여 이전에 분석되었던 결과 값들을 인증관리를 통해 허가된

사람에 한하여 검색을 통해 알 수 있다. 제 3 자나 다른 시스템에서 활용하기 위해서는 목적을 명백하게 명시하여 개인정보제공자의 승인을 득해야 한다.

개인정보 관리 모델의 구현을 위한 아키텍처는 개인정보 생명주기 각 단계의 순차적 진행이 아닌 복합적으로 구성된다. 하지만 이러한 복합적 구성은 시스템 전체의 관리에 더 강한 요소로 작용될 것이다.



[그림 2] 개인정보보호 관리 아키텍처

4. 결론

인터넷 및 전자상거래의 발달로 인해 개인정보의 중요성이 크게 높아지고 있다. 개인정보는 그 목적에 따라 개인정보를 제공하는 제공자(Privacy Data or Person)와 개인정보를 이용하는 이용자(Privacy Management System)로 구분된다. 개인정보제공자는 스팸메일과 같은 불편을 사전에 막을 수 있으며, 이용자 측면에서의 개인정보는 비용절감과 더 나은 고객관리의 기틀을 마련하는 계기를 지원하기 위해 개인정보를 이용한다.

이렇게 중요시 하는 개인정보는 개인정보의 유출 및 침해(즉, 바이러스, 웜, 범죄 등)로 인하여 물질적/정신적으로 큰 피해를 입히게 되며, 결국에는 인터넷 및 전자상거래의 발전을 저해하는 근본적인 원인이 될 수도 있다. 따라서 본 연구에서는 개인정보의 안전한 사용 및 관리를 위해 개인정보보호 관리 모델을 제안과 모델 구현을 위한 아키텍처를 제안하였다. 개인정보 관리 모델은 개인정보 수명주기에 따라 발생할 수 있는 침해에 대응할 수 있는 정책적 대책, 관리적 대책, 기술적 대책을 제시하고 있다. 개인정보 관리 모델은 개인정보 정책과 침해요인 및 보호에 관련된 연구를 바탕으로 한 개인정보 특성을 중심으로 하였으며, 기술적 측면, 관리적 측면, 정책적 측면을 고려하여 관리하는 모델이다. 그리고 개인정보관리모델을 구현화 시키기 위해 제안된 아키텍처는 개인정보 생명주기 각 단계를 복합적으로 구성하였으며, 개인정보관리모델에서 제시된 기술적, 관리적, 정책적 대책을 통해 개인정보관리에 더 나은 방법을 제시하고 있다.

참고문헌

[1] 「개인정보의 안전한 수집, 저장 및 관리, 이용, 제공, 파기를 위한 개인정보 관리모델 연구」, 한국정보보호진흥원, 2006.12

[2] 「개인정보보호 기술의 동향」, 송유진외, 주간기술동향, 1218 호, 2005.10

[3] 「인터넷과 개인정보의 보호」, 최정열, 한국정보법학회, 2002

[4] 한국정보보호진흥원, 「정보시스템과 네트워크의 보호를 위한 OECD 가이드라인」, 한국정보보호진흥원, 2003. 1

[5] 정보통신부, 「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」, 정보통신부, 2004.1

[6] 「개인정보보호」, 김연수, 사이버출판사, 2001

[7] 「개인정보 침해에 관한 조사 연구」, 김성언, 한국형사정책연구원, 2001

[8] 「개인정보보호 개선방안에 관한 연구」, 김정훈, 동국대 국제정보대학원, 2003

[9] 「개인정보 침해사례분석과 방안에 관한 연구」, 이종호, 동국대 국제정보대학원, 2001