情 報 保 護 學 會 誌
第18卷 第2號, 2008. 4

개인정보 DB 관리기술의 보안 요구사항 연구

최 향 창*, 김 현**, 박 해 룡**, 전 길 수**, 이 형 효***

요 약

인터넷을 통한 공공 및 민간 부분 서비스 제공이 활성화됨에 따라 이들 서비스를 제공받기 위해 사용자들은 자신의 개인정보를 서비스 제공자에게 제공하게 되고, 서비스 제공자들은 가입자들의 개인정보를 관리하기 위해 일반적으로 데이터베이스를 이용하고 있다. 최근 개인정보에 대한 중요도와 필요성이 증가함에 따라 정보보호 제품에 대해 일반 보안기능 및 신뢰성 평가뿐만 아니라 개인정보 소유자의 프라이버시가 보장되는지를 평가할 수 있는 평가기준 마련 필요성이 제기되고 있다.

본 논문에서는 OECD, 미국 FTC, 유럽연합 등 정보보호 선진국에서 제정한 프라이버시 보호원칙과 기존 DBMS 보안 요구사항을 함께 반영한 개인정보 DB 관리기술에 대한 보안 요구사항을 개발하였다. 개발된 보안 요구사항은 TTA 개인정보 생명주기 관리모델(안)의 생명주기 단계를 기준으로 각 생명주기 단계에서 수행되는 기능 특성에 따라 DBMS 보안 측면과 프라이버시 보호 측면을 함께 고려하여 작성되었다.

Ⅰ. 서 론

인터넷으로 대표되는 정보통신망 및 컴퓨터를 이용한 개인정보의 수집 및 이용이 경제적 및 사회적으로 일반화됨에 따라 이의 역기능으로 개인의 프라이버시가 침해되는 사례가 점차 증가하고 있다. 향후에는 u-City, u-Healthcare 등 유비쿼터스 서비스가 일반화되면 사용자들은 자신들이 인식하지 못하는 사이에 수많은 개인정보가 다양한 기기 및 센서에 의해 수집될 것이다[1,2,3]. 이 대량의 데이터는 일반적으로 개인정보-DB에 체계적으로 저장, 관리되면서 인증, 인가된 데이터 이용자에 대해서만 데이터 접근을 허용한다[10].

일반적으로 데이터베이스 시스템은 데이터의 비밀성, 무결성, 가용성을 지원하지만 개인정보 보안을 제공하는 주체가 서비스 제공자인 개인정보 DB의 운용자임으로 인해 개인의 프라이버시가 위협받을 수 있다[10]. 따라서 데이터베이스 시스템도 현재의 공통평가기준(CC: Common Criteria) 기반의 데이터베이스 보안 지침을 기반으로 OECD[4], 미국의 FTC(Federal Trade Commission)[5], EU 등에서 제정한 프라이버시 가이드라인[8]을 준수하면서 데이터베이스에 저장된 개인정보 소유자의 프라이버시를 보장하는 기능 또한 추가되어야 할 것이다[6,7]. 본 논문은 개인정보 DB의 보안성 제공을 위한 일반적인 접근통제 요구사항과 개인정보의 주체인 소유자의 프라이버시 측면을 고려하는 프라이버시 보호 요구사항이 함께 고려된 개인정보 DB 관리기술 보안 요구사항을 제안한다. 제안된 요구사항은 개인정보 DB 관리기술을 새롭게 개발할 때 사용될 수 있으며 이미 만들어진 개인정보 DB 관리기술을 평가하는 데에도 활용될 수 있을 것이다.

Ⅱ. 관련 연구

개인정보 보호는 정보사회에서 개인들이 보장받기를 희망하는 기본적이며 필수적인 요구사항이다[8]. 예를 들어 개인은 자신과 관련된 정보를 정보사회의 시스템에 제공하고 이를 제공받은 정보시스템은 개인들에게 편리하고 이득이 되는 서비스를 제공하고는 있으나, 이 개인정보의 사용은 개인에게 프라이버시 침해를 일으킬 수도 있다. 예를 들어 개인정보를 제공한 정보 소유

본 연구는 한국정보보호진흥원 위탁과제(KISA-WP-2007-0031) 지원사업의 연구결과로 수행 되었습니다.
* 전남대학교 시스템보안 연구센터 (hcchoi@lsrc.chonnam.ac.kr)
** 한국정보보호진흥원 암호응용팀 ({hkim, hrpark, kschun}@kisa.or.kr)
*** 원광대학교 정보·전자상거래학부 (hlee@wonkwang.ac.kr), 교신저자

자에게 허가 받지 않은 개인정보 사용은 스팸메일을 발생시킬 수 있으며 개인에게 민감한 정보를 정보통신 환경에 배포함으로써 개인에게 피해를 야기할 수 있다. 본 장은 개인정보 DB를 안전하게 보호할 근간이 될 수 있는 개인정보 DB 관리기술 보안 요구사항을 제안하기 위해 개인정보 프라이버시 정의 및 관련 가이드라인[4,5,6,7] 및 개인정보 DB 관리기술[11,12,13,14,15]을 조사하고 분석한다.

2.1 주요 프라이버시 보호원칙

1980년 경제개발 협력기구(OECD)는 '사생활 정보 보호와 개인정보의 국제적 유통에 관한 개인정보 보호의 8원칙'을 규정했다. 이것은 개인정보보호에 관한 국제적인 기준이 되었다. OECD 8원칙은 정보 수집제한의 원칙, 정보내용 정확성의 원칙, 목적 명확화의 원칙, 이용제한의 원칙, 안전 확보의 원칙, 공개의 원칙, 개인참가의 원칙, 책임의 원칙으로 정의된다[4]. 이것은 정부나 기업 등 다양한 사용자에 의해 개인정보가 사용될 때는 반드시 개인정보 소유자가 동의하는 범위의 사용자, 사용목적, 사용기간, 의무사항에 따를 것을 권고하고 있다.

미국과 유럽의 온라인 고객정보 보호 정책과 관련된 규정들은 고객정보 FIPP(Fair Information Practice Principles)[5]와 OPA(Online Privacy Alliance)[6]의 내용에 부합해야 한다. 미국 FTC(Federal Trade Commission)에서 제정한 FIPP는 고객정보 수집방법, 수집된 정보에 대한 고지 의무, 고객정보의 올바른 사용을 보장하는 기업의 보안 의무 등이 명시되어 있으며, OPA는 기업의 고객정보보호 정책을 개발하고 이 정책을 공개하기 위한 필요조건에 대한 지침을 제공한다[5,6]. 1995년 EU는 개인정보를 보호하기 위해서 개인정보 보호원칙을 제정하였고, 또한 기본적으로 개인정보 보호가 미흡한 제 3국에 대한 개인정보 이전을 금지하고 있다. 유럽의 프라이버시 원칙에는 정보에 대한 공정하고 적법한 처리와, 정보의 수집과 처리 목적이 명백하고 정당한 경우에만 가능하도록 제한하고, 정확한 최신의 정보 유지가 요구된다. 또한 현재는 ISO/IEC JTC 1/SC27 Working Group 5에서 Identity 관리와 관련된 프라이버시 표준개발을 위해 개인정보 보호원칙을 제안하고 있다. [표 1]은 OECD, FIP, EU, ISO/ETC, CSA(The CSA International. Privacy Code) 개인정보 보호 원칙들의 특징을 비교, 정리하고 있다[4,5,6,7,8,16].

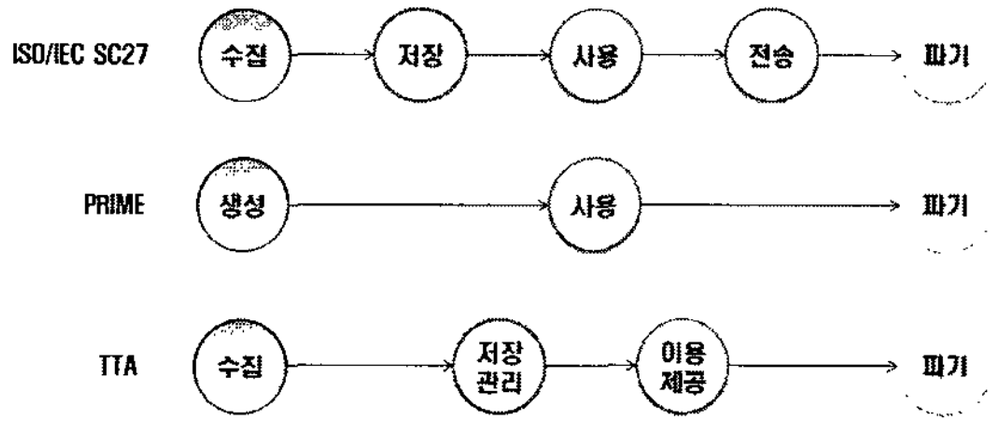
〔표 1〕 주요 프라이버시 보호 원칙간 특징 비교

항 목	OECD	FIP	EU	ISO/IEC	CSA
Consent		○	○	○	○
Choice		○		○	
Accountability	○		○	○	○
Purpose Specification	○		○	○	○
Collection Limitation	○			○	○
Use Limitation	○			○	○
Retention Limitation				○	○
Disclosure Limitation			○	○	○
Data Frugality				○	
Data Accuracy				○	○
Data Quality	○			○	
Openness	○			○	○
Transparency				○	
Notice & Awareness		○	○	○	
Individual Participation & Access	○	○	○	○	○
Security Safeguard	○	○	○	○	○
Compliance				○	
Challenging					○
Enforcement & Redress		○			

2.2 개인정보 생명주기 모델

정보시스템에서 운용하는 개인정보 DB는 개인정보를 DBMS에 기반을 두어 운용하는 개인정보의 집합체이다. 정보시스템에서 운용하는 개인정보는 개인의 신상정보, 연락정보, 금융정보 등이 있고[3] 본 논문은 이 개인정보를 운용하는 모든 기술을 개인정보 DB 관리기술로 명명한다. 개인정보 DB 관리기술은 개인정보 관리에 관련된 기술로 개인정보를 개인정보 DB에 입력할 수 있으며 개인정보 DB를 운용하고 접근하고 관리할 수 있는 권한 생성, 개인정보 사용자 신원 인증, 인가를 수행한다. 이러한 개인정보 DB 관리기술을 세분화하기 위해서는 개인정보 생명주기를 고려해야 한다[3].

개인정보 생명주기는 개인정보의 생성에서부터 사용되고 파기되는 단계를 의미한다. [그림 1]과 같이 ISO/IEC SC27의 개인정보 생명주기 단계는 수집, 저장, 사용, 전송, 파기의 5단계로 구성된다[16]. 수집단계는 개인



〔그림 1〕 주요 개인정보 생명주기 모델

정보를 필요로 하는 자가 필요한 개인정보를 소유한 소유자에게 개인정보를 수집한다. 저장단계는 수집된 개인정보를 수집했던 개인정보 수집의 주체가 재사용의 필요성을 고려해 자신의 영역에 개인정보를 저장한다. 사용단계는 수집한 개인정보를 필요한 목적으로 사용한다. 전송단계는 수집된 개인정보를 필요로 하는 곳에 전송한다. PRIME의 개인정보 생명주기 단계는 생성, 사용, 파기 단계로 구성하고 있고 한국정보통신기술협회(TTA: Telecommunications Technology Association)에서는 수집, 저장관리, 이용제공, 파기 단계로 개인정보 생명주기 모델(안)를 제안하고 있다(그림 1 참조).

본 논문에서 제안하는 개인정보 DB 관리기술 보안 요구사항은 TTA에서 제안한 개인정보 생명주기 모델을 기본으로 하고 있으므로 TTA 개인정보 생명주기 관리모델의 주요 특징에 대해 간단히 기술한다.

TTA의 수집 단계의 개인정보 DB 관리기술은 개인정보 소유자로부터 개인정보를 요청하여 개인정보 DB에 저장관리하기위해 개인정보를 수집하는 단계를 수행한다. 개인정보를 요청하는 정보시스템은 개인정보 사용자에게 개인정보의 요청을 알리는 메시지를 보이고 필요한 정보를 수집하기위해 요청되는 항목들을 다양한 유형의 입력 폼에 기초하여 요청한다. 정보시스템은 개인정보 소유자가 입력한 개인정보를 전송받고 개인정보 DB에 저장한다. 수집 단계의 개인정보 DB 관리기술은 이러한 수집과정에 관련된 일체의 DB 관리기술을 의미한다.

저장·관리 단계의 개인정보 DB 관리기술은 개인정보 DB에 개인정보 소유자로부터 수집한 개인정보를 저장하고 관리하는 단계를 수행한다. 수집단계에서 개인정보 소유자로부터 제공되며, 개인정보는 DB 관리기술에 의해 무결성, 가용성과 특정한 개인정보에 대해 비밀성을 유지하면서 관리된다. 저장·관리 단계의 개인정보 DB 관리기술은 이 저장·관리과정에 관련된 일체의 DB 관리기술을 의미한다.

이용·제공 단계의 개인정보 DB 관리기술은 개인정보 DB에 저장·관리되는 개인정보를 이용하거나 또는 다른 개인정보 이용자 제공하는 단계를 수행한다. 개인정보를 이용·제공하는 DB관리기술은 DB에 저장된 개인정보를 SQL의 Select문을 통해 필요한 개인정보를 검색하고 개인정보 이용자에게 제공한다. 이용되거나 제공되는 개인정보 DB는 개인정보 보호정책에 기반을 두어 개인정보를 이용제공 한다. 이용·제공 단계의 개인정보 DB 관리기술은 이 이용·제공과정에 관련된 일체의 DB 관리기술을 의미한다.

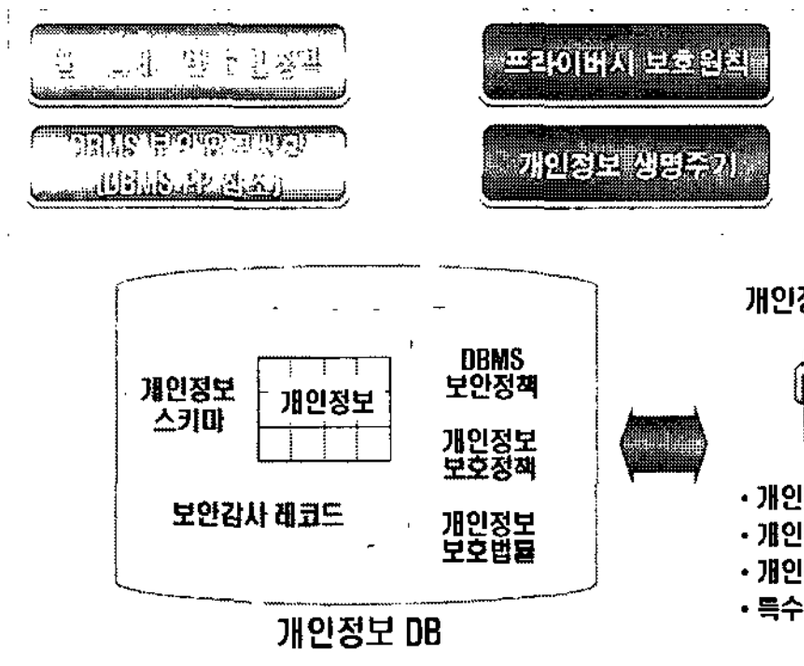
파기 단계의 개인정보 DB 관리기술은 개인정보 DB에 저장·관리되는 개인정보를 파기하는 단계를 수행한다. 개인정보를 파기하는 DB관리기술은 개인정보 저장·관리 단계에서 저장되고 관리되고 있는 개인정보를 SQL의 Delete문을 통해 파기할 개인정보를 삭제한다. 파기되는 개인정보는 DB관리기술에 의해 개인정보 소유자와 개인정보 관리책임자에 의해 보안과 프라이버시를 보장하기위해 유효하지 않은 데이터는 삭제한다. 파기 단계의 개인정보 DB 관리기술은 이 파기과정에 관련된 일체의 DB 관리기술을 의미한다.

Ⅲ. 개인정보 DB 관리기술 보안 요구사항 작성원칙

3.1 보안 요구사항 개발 방법

본 논문에서 제안하는 생명주기 기반 개인정보 DB 관리기술 보안 요구사항은 TTA 개인정보 생명주기 모델(안)을 기반으로 DBMS PP에서 정의하고 있는 보안기능 요구사항과 프라이버시 보호원칙을 함께 반영하여 작성되어 있다(그림 2).

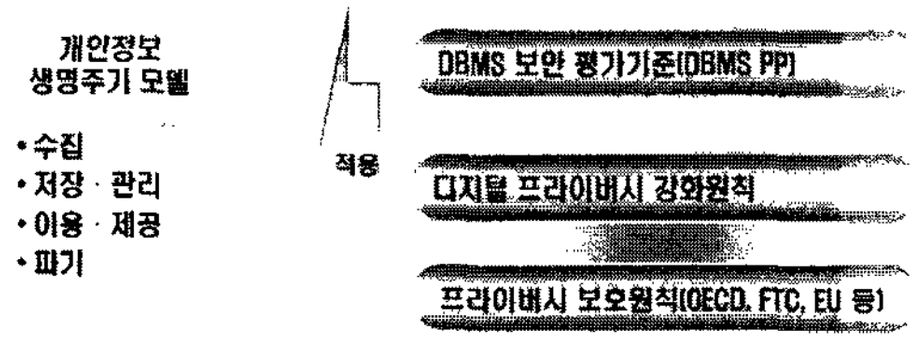
[그림 2]에서 개인정보 DB 관리기술 보안 요구사항은 접근통제기반 보안정책, CC 표준 DBMS 보호프로파일(PP: Protection Profile)의 보안기능 요구사항, 개인정보 자기통제권 강화 기술 및 원칙, 프라이버시 보호법 및 원칙들에 기반을 두어 도출되고 있음을 보여주고 있다. 불법적인 접근 및 프라이버시 침해로부터 보호되어야 하는 개인정보 DB는 개인정보, 개인정보 스키마, 감사레코드 및 보안정책, 개인정보 보호정책 등으로 구성되어 있다. 개인정보를 사용하는 주체들로는 개인정보 소유자, 개인정보 관리책임자, 개인정보 이용자, 특수 이용자 등이 있다.



〔그림 2〕 개인정보 DB 관리기술 보안요구사항 작성 시 고려사항

3.2 개인정보 DB 보호 측면 요구사항

개인정보 DB의 안전한 관리는 개인정보에 대한 보안과 개인정보 소유자의 프라이버시를 안전하게 보장할 때만 가능하며, 이를 위해서는 [그림 1]과 같은 개인정보 DB 생명주기 각 단계에서 보안과 프라이버시를 고려해야 한다. 즉 개인정보 DB 관리기술 보안은 DBMS PP 보안기능 요구사항을 충족시키면서 프라이버시 보호를 보장하기 위해 디지털 프라이버시 보호원칙이 적용되어야 한다(그림 3)[4,8,9].



〔그림 3〕 개인정보 DB관리기술 보안 요구사항 작성원칙

DBMS PP는 정보를 데이터베이스에 저장, 관리하는 기업이나 조직의 데이터베이스에 저장된 정보의 비밀성, 무결성, 가용성 보장을 위한 보안요구사항을 명세하고 있다[12,13]. DBMS 보안을 위해 실행되는 사용자 인증인 OS 인증과 DBMS 인증의 두 가지 방법이 존재한다. OS인증은 DBMS가 설치되어있는 OS에 접속권한을 갖는 사용자가 자신의 계정으로 인증이 가능하며, DBMS 인증방법은 OS와 별도로 DBMS가 운용하는 인증 방식이다. DBMS는 이러한 인증방법에 기반을 두어 DBMS를 통해 기업이나 조직의 데이터베이스에 저장된 정보의 안전함을 제공한다. DBMS에 영향을 미칠

〔표 2〕 DBMS 위협 및 정책의 보안 요소 간 관계

보안요소 / T(위협)/P(정책)	O.I&A.TOE	O.ACCESS	O.AUDIT	O.RESOURE	O.ADMIN.TOE
T.ACCESS	YES	YES		YES	YES
T.DATA	YES	YES			YES
T.RESOURCE	YES	YES		YES	YES
T.ATTACK	YES	YES	YES		YES
T.ABUSE.USER	YES	YES	YES		YES
P.ACCESS		YES		YES	
P.ACCOUNT		YES	YES		

수 있는 위협과 정책의 보안 요소들 간에 관계는 DBMS PP에서 [표 2]와 같이 정의하고 있다[15].

[표 2]에서 T는 DBMS와 관련된 보안 위협을 의미하며 P는 정책을 의미한다. DBMS PP는 다루는 정보가 기업이나 조직의 데이터베이스에 저장된 정보들을 의미하나 본 논문의 목표가 개인정보 DB의 보안요구사항임으로 데이터베이스에서 다루는 정보를 개인정보로 한정하여 [표 2]를 논의한다. [표 2]에서 T.ACCESS는 데이터베이스에 저장된 개인정보를 접근권한 없는 비인가자가 정당한 방법이 아닌 방법으로 접근할 때 발생할 수 있는 위협을 의미한다. T.DATA는 데이터베이스에 저장된 개인정보에 대한 위협이다. 이 위협으로는 허가받지 않은 사용자가 개인정보 데이터를 확인할 수 있는 위협을 포함한다. T.RESOURCE는 DBMS와 관련된 자원에 대한 위협을 의미한다. 대표적인 T.RESOURCE와 관련된 위협은 자원에 대한 DoS(Denial of Service) 공격이다. T.ATTACK은 DBMS의 위협이 탐지되지 못한 공격을 의미한다. T.ABUSE.USER는 DBMS와 관련된 권한이 있는 사용자가 권한을 남용함으로써 발생할 수 있는 위협이다. P.ACCESS는 개인정보, 개인정보에 접근하려는 주체, 개인정보에 접근하려는 주체의 권한, 개인정보 데이터베이스의 관리권한, 주체에게 할당된 개인정보에 기반을 둔 정책규칙을 설립하여 개인정보의 인가를 수행한다. P.ACCOUNT는 데이터베이스의 개인정보 소유자 및 데이터베이스 관리자가 행사할 수 있는 연산을 정책으로 유지하여 인가시기에 적용한다[15].

보안요소인 [표 2]의 O.I&A는 개인정보 보안을 수행할 대상 시스템은 사용자를 식별하고 인증할 수 있어야 함을 의미한다. O.ACCESS는 최종 사용자 또는 관리자 그룹의 구성원들은 그들이 소유하거나 또는 관리책임이

있는 개인정보에 대해 접근을 제한할 수 있어야 함을 의미한다. O.ACCESS의 하위 메서드로는 OBJECT, CONTROL, RESIDUAL이 있다. O.AUDIT은 보안관련 이벤트를 TOE 관리자에게 도움을 줄 수 있도록 충분히 자세하게 기록하는 수단을 제공해야 함을 의미한다. O.RESOURCE 는 인가된 사용자에 의한 과도한 데이터베이스 자원 소비를 통제하는 수단을 제공해야 함을 의미한다. O.ADMIN은 개인정보 보안을 수행할 대상시스템은 효과적인 관리기능을 제공해야 하며 반드시 관리에 합당한 계정을 소유한 사용자만 관리기능을 행사할 수 있도록 제한되어야 함을 의미한다[15].

3.3 프라이버시 보호 측면 요구사항

프라이버시 보호를 위해 개인정보 소유자에게 자기정보통제권이 보장되어야 하며, 이 통제권은 개인정보 소유자가 자신의 개인정보를 어떻게 통제할 것인가를 기술하는 정책에 기반을 두는 경우가 많다. 이와 같은 개인정보 보호정책을 통해 개인정보 사용을 요청하는 모든 요구에 대해 개인이 직접 참여하여 그때의 상황을 판단하여 개인정보를 제공하거나 거부하는 등 개인정보 자기통제권 행사를 지원하게 된다.

프라이버시 보호는 개인정보가 수집, 저장 후 이용되고 마지막에 파기되는 생명주기 전 단계에 걸쳐 적용되어야 한다. 예를 들어, 개인정보의 수집단계에서는 수집되는 개인정보를 이용목적에 적합한 최소 정보만 수집되고 개인정보 보유기간, 관리 책임자 등에 대한 정보가 공개되어야 하며 개인정보 소유자가 자신의 정보에 대한 접근이 보장됨과 동시에 감사레코드를 통해 개인정보 오남용으로 인한 책임이 부과됨을 개인정보 보호정책에 포함, 반영되어야 한다.

Ⅳ. 개인정보 생명주기 기반 개인정보 DB 관리기술 보안 요구사항

이 장에서는 TTA의 개인정보 생명주기(안) 기반 개인정보 DB 보안 측면과 프라이버시 보호 측면을 함께 고려한 개인정보 DB 관리기술 보안 요구사항을 정리한다. 개인정보 DB 보안 요구사항은 DBMS PP 보안기능 요구사항에 준거하여 개발되었고, 프라이버시 보호 요구사항은 주요 프라이버시 보호원칙 중 각 생명주기에 해당되는 원칙들을 반영하도록 작성되었다. 본 논문에서는 지면 제한으로 개인정보 DB 관리기술 보안 요구사항 중 중요 내용만을 발췌하여 정리하였다.

4.1 수집단계 개인정보 DB 관리기술 보안 요구사항

4.1.1 개인정보 DB 보안 요구사항

수집 요구사항 1 : 수집 단계에서 생성되는 감사레코드는 다음 감사기능을 수행하는데 충분해야한다.
- 개인정보 수집사실과 수집되는 개인정보 항목, 보유기간 및 사용목적에 대한 개인정보 소유자 확인 여부 점검
- 개인정보 보호정책에 합당한 사용목적으로 개인정보 수집 여부 점검
- 개인정보 이용자(수집 응용) 및 개인정보 소유자 식별
- 수집되는 개인정보의 안전성과 비밀성 유무 점검
- 법률에 정의된 예외사항에 의한 개인정보 수집 여부 점검

수집 요구사항 2 : 수집 단계에서 생성되는 감사레코드는 최소한 다음의 정보를 포함해야 한다.
- 수집되는 개인정보 소유자 및 개인정보 이용자(수집 응용) 식별정보
- 수집되는 개인정보 식별정보, 수집목적 및 수집 시각 정보, 사전 동의정보
- 감사레코드의 생성 시각 정보, 무결성 점검 정보

수집 요구사항 3 : 감사레코드들은 무결성과 가용성이 보장되어야 하며 저장된 감사레코드는 정당한 권한을 가진 사용자에 의해서만 접근될 수 있다.

4.1.2 프라이버시 보호 요구사항

수집 요구사항 4 : 기관이나 조직의 개인정보 DB 관리기술은 개인정보의 수집 목적을 명시해야 하고, 정보가 수집되는 시점이나 그 이전에 개인에게 개인정보 수집 목적을 알려야 한다. 명시된 목적은 명확해야 하고 제한적이며 목적에 합당한 최소한의 정보를 수집해야 한다.

수집 요구사항 5 : 개인정보 DB 관리기술을 운용하

여 개인정보를 수집하는 기관이나 조직은 개인정보 처리에 관한 자신의 관례, 정책, 절차를 명확하게 기술하여 개인정보 소유자가 쉽게 접근할 수 있도록 제공해야 한다.

- 개인정보 DB 관리기술의 각 기능 동안 수집되는 개인정보 및 수집목적
- 개인정보가 공개되는 기관들의 종류
- 개인정보 관리자와의 연락방법
- 개인정보 소유자가 개인정보 관리기술 동안 수집되는 개인정보의 수집을 제약할 수 있는 방법
- 개인정보 소유자가 자신의 정보에 접근하고 수정할 수 있는 방법

수집 요구사항 6 : 개인정보 DB 관리기술을 운용하여 개인정보를 수집하는 기관이나 조직은 개인정보 저장으로 발생하는 개인정보를 안전하게 보호해야 할 책임이 부과되며 요구되는 기능은 다음과 같다.

- 데이터 보호 법령 및 보안, 프라이버시 정책을 준수하는 내부 접근 통제 및 감사 메커니즘
- 개인정보 이의제기 및 시정 메커니즘
- 개인정보 DB 관리기술의 수집과 관련된 개인정보 보호 정책이나 절차 및 책임사항이 공시될 수 있는 기능
- 개인정보의 보호 업무를 담당하는 인력을 위한 기능

4.2 수집단계 개인정보 DB 관리기술 보안 요구사항

4.2.1 개인정보 DB 보안 요구사항

저장·관리 요구사항 1 : 저장·관리 단계에서 생성되는 감사레코드는 다음 기능을 수행하는 데 충분해야 한다.

- 개인정보의 수집/저장, 이용 및 제공, 변경
- 개인정보의 수집, 이용 및 제공, 변경 이력 조회
- 개인정보 보호정책의 생성 및 변경
- 개인정보 보호정책의 생성 및 변경 이력 조회
- 개인정보 보호 정책관리자가 설정한 기본 개인정보 보호정책의 생성 및 변경 이력 조회

저장·관리 요구사항 2 : 저장·관리 단계에서 생성되는 감사레코드는 다음 정보를 포함해야 한다.

- 개인정보 이용자 식별정보
- 개인정보 또는 개인정보 보호정책 소유자 정보
- 개인정보 또는 개인정보 보호정책 대상 연산(조회, 변경, 제공, 이력조회 등) 식별정보
- 개인정보 또는 개인정보 보호정책 대상 연산 목적 및 결과
- 개인정보 또는 개인정보 보호정책 대상 연산 수행에 필요한 개인정보 소유자 사전동의, 사후통지 여부
- 감사레코드의 생성 시각 정보, 무결성 점검정보

저장·관리 요구사항 3 : 개인정보 DB에 저장된 개인정보는 개인정보 보호 정책에 의해 안전하게 관리되기 위해 다음과 같은 기능이 제공되어야 한다.

- 개인정보 보호정책은 개인정보 소유자 또는 개인정보 관리책임자에 의해 정의됨
- 저장·관리 단계에서 DB 관리기술과 관련된 개인정보 보호정책이 없을 경우에는 기본 개인정보 보호정책이 이를 대신할 수 있어야 함
- 개인정보 소유자의 개인정보 보호정책과 개인정보 관리책임자가 정의한 정책들 간에 충돌이 발생할 경우 해결방안이 제시되어야 함

저장·관리 요구사항 4 : 개인정보가 저장되는 DB 스키마와 개인정보 보호정책이 저장되는 스키마는 별도로 정의되어 관리되어야 하며, 각 개인정보에 대한 수집, 이용 및 제공, 파기에 적용되는 개인정보 보호정책이 존재해야 한다.

- 개인정보, 개인정보 보호정책, 감사레코드는 개인정보 소유자와 개인정보 관리책임자에 의해 접근이 허용되며 법률이 정한 경우에 한해 특수 이용자가 접근할 수 있음

저장·관리 요구사항 5 : 개인정보 소유자, 개인정보 관리책임자가 수행할 수 있는 권한은 명확히 정의되어야 한다.

- 개인정보 소유자는 개인정보 및 개인정보 보호정책을 생성, 조회, 사용이력 확인, 변경할 수 있는 권한을 가짐
- 개인정보 관리책임자는 기본 개인정보 보호정책을 생성, 조회, 변경할 수 있는 권한을 가짐

· 개인정보 관리책임자는 감사레코드에 포함되는 정보를 정의할 수 있으며 감사레코드를 조회할 수 있는 권한을 가짐
· 개인정보 관리책임자는 개인정보 DB의 백업, 복구 등의 권한을 가짐
· 단, 법률에 의해 권한이 부여된 특수 이용자에 의해 개인정보, 개인정보 보호정책, 감사레코드는 조회될 수 있음

4.2.2 프라이버시 보호 요구사항

저장·관리 요구사항 6 : 기관이나 조직의 개인정보 DB 관리기술은 법률에 의한 예외 경우를 제외하고 개인정보의 저장·관리에 개인정보 소유자의 선택적 동의를 제공할 수 있어야 한다.

저장·관리 요구사항 7 : 개인정보를 저장하는 기관이나 조직의 개인정보 DB 관리기술은 개인정보의 수집 목적과 일치하는 저장 목적을 명시해야 하고, 정보가 저장되는 시점이나 그 이전에 개인에게 개인정보 수집에 상응하는 저장 목적을 알려야 한다. 명시된 목적은 명확해야 하고 제한적이며 해당 상황에 연관성이 있어야 한다.

저장·관리 요구사항 8 : 개인정보를 저장·관리하는 조직이나 기관은 개인정보 소유자가 동의한 목적에 부합하는 동안에만 저장·관리됨을 보장해야 한다. 개인정보는 명시된 목적을 달성하기위해 유효한 기간만 저장·관리되어야 하고 목적이 달성되면 안전하게 파기됨을 원칙으로 한다.

저장·관리 요구사항 9 : 개인정보 DB 관리기술에 의한 개인정보 저장은 공정하고 합법적이어야 하며 명시된 목적에 부합하는 정확한 개인정보 만을 저장해야 한다. 저장되는 개인정보는 완전하고 최신으로 유지되어야 한다. 개인정보를 저장하는 기관이나 조직의 개인정보 DB 관리기술은 저장된 데이터의 정확성과 품질을 수시로 점검할 수 있는 내부 메커니즘을 갖추고 있어야 한다.

저장·관리 요구사항 10 : 개인정보 DB 관리기술을 운용하여 개인정보를 저장·관리하는 기관이나 조직은 수집단계에서 수집된 개인정보의 저장·관리에 관한 자신의 관례, 정책, 절차를 명확하게 기술하여 개인정보 소유자가 정확히 연산을 수행할 수 있도록 하는데 충분해야 한다. 공개하는 항목은 다음과 같다.

· 수집단계에서 수집된 개인정보의 저장 정책
· 개인정보 수집목적에 부합하는 저장목적
· 개인정보 관리자와의 연락방법
· 개인정보 관리자가 개인정보 소유자에게 제공하는 개인정보의 저장을 제약할 수 있는 방법
· 개인정보 소유자가 저장된 자신의 정보에 접근하고 수정할 수 있는 방법
· 이외에도 법률이 정하는 것을 저장해야 한다.

4.3 이용·제공단계 개인정보 DB 관리기술 보안 요구사항

4.3.1 개인정보 DB 보안 요구사항

이용·제공 요구사항 1 : 이용·제공 단계 감사레코드는 다음의 감사기능을 수행하는데 충분해야 한다.

· 개인정보 이용자가 접근하는 개인정보가 개인정보 소유자에 의해 설정된 개인정보 보호정책에 부합되는지 검사
· 개인정보 이용자가 타 개인정보 이용자에게 제공하려는 개인정보가 개인정보 소유자에 의해 설정된 개인정보 보호정책에 부합되는지 검사
· 개인정보 이용자가 개인정보를 접근한 후 실행해야 하는 의무사항 실행여부 검사

이용·제공 요구사항 2 : 이용·제공 단계에서 생성되는 감사레코드는 최소한 다음의 정보를 포함해야 한다.

· 개인정보 식별정보 및 소유자 정보
· 개인정보 이용자 식별정보
· 개인정보 대상 연산(조회, 변경, 제공, 백업, 복구 등) 식별정보
· 개인정보 대상 연산 목적 및 연산 결과
· 개인정보 대상 연산 수행에 필요한 개인정보 소유자 사전 동의 및 사후 통지여부
· 개인정보 이용자의 개인정보 대상 연산 후 실행하는 의무사항 식별정보 및 실행 결과
· 감사레코드의 생성 시각 정보, 무결성 점검정보

이용·제공 요구사항 3 : 개인정보 DB에 저장된 개인정보는 개인정보 보호정책에 의해 안전하게 이용되어야 하며, 이를 위해 다음과 같은 기능이 제공되어야 한다.

- 개인정보 소유자 의해 정의된 개인정보 보호 정책을 이행
- 개인정보 보호 정책은 개인정보 이용자가 개인정보를 사용하기 이전에 정책을 만족하는지 점검됨
- 개인정보 이용자는 개인정보 보호정책에 의해 정의된 목적으로 개인정보를 이용, 제공할 수 있으며 개인정보 보호정책에 명시된 의무사항을 실행할 의무를 가짐
- 개인정보를 다른 개인정보 이용자에게 제공할 경우 개인정보 외에 해당 개인정보에 대응하는 개인정보 보호정책이 함께 제공되어야 함
- 개인정보를 제공받은 개인정보 사용자는 개인정보와 함께 제공되는 개인정보 보호정책에 의거하여 개인정보를 사용해야 함

이용·제공 요구사항 4 : 개인정보 이용자는 정해진 목적동안 유효한 개인정보 DB 관리기술의 연산만을 수행할 수 있다. 이를 위해서는 다음의 기능이 추가로 요구된다.

- 개인정보 이용자의 식별
- 개인정보 DB에서 사용되는 개인정보의 식별
- 개인정보 이용자가 허가받은 목적동안 할당받을 수 있는 개인정보 접근 권한 식별
- 개인정보 이용자가 개인정보 사용에 수행할 기능들을 식별

이용·제공 요구사항 5 : 개인정보 DB 관리기술의 모든 연산들은 개인정보의 이용제공 단계를 수행하는 동안 합법적으로 제공되는 정당한 절차만을 수행해야 하고 정당하지 않은 우회로를 제공해서는 안 된다. 단, 법률에 의해 지정된 특수 이용자는 법률에 의해 명시된 목적으로 개인정보 보호정책을 점검하지 않고 개인정보, 개인정보 감사데이터에 접근할 수 있다.

4.3.2 프라이버시 보호 요구사항

이용·제공 요구사항 7 : 기관이나 조직의 개인정보 DB 관리기술은 법률에 의한 예외 경우를 제외하고 개인정보의 이용·제공에 개인정보 소유자의 선택적 동의를 제공할 수 있어야 한다.

이용·제공 요구사항 8 : 개인정보를 이용·제공하는 개인정보 DB 관리기술은 개인정보의 수집 목적과 일치하는 이용·제공 목적일 때만 수행가능하고, 정보가 이용·제공되는 시점이나 그 이전에 개인에게 개인정보 수집에 상응하는 이용·제공 목적을 알려야 한다. 명시된 목적은 명확해야 하고 제한적이며 해당 상황에 연관성과 일치성이 있어야 한다.

이용·제공 요구사항 9 : 개인정보 DB 관리기술을 운용하여 개인정보를 이용·제공하는 기관이나 조직은 수집단계에서 수집된 개인정보의 이용·제공에 관한 자신의 관례, 정책, 절차를 명확하게 기술하여 개인정보 소유자가 쉽게 접근할 수 있도록 제공해야 한다. 공개하는 항목은 다음과 같다.

- 수집 단계에서 수집된 개인정보와 수집과 저장
- 관리단계에서 생성된 이용·제공 정책
- 개인정보 수집목적에 부합하는 이용·제공 목적
- 개인정보 관리자와의 연락방법
- 개인정보 관리자가 개인정보 소유자에게 제공하는 개인정보의 이용·제공을 제약할 수 있는 방법
- 개인정보 소유자가 이용·제공된 자신의 정보가 안전하게 사용되었음을 검증할 수 있는 방법

4.4. 파기단계 개인정보 DB 관리기술 보안 요구사항

4.4.1 개인정보 DB 보안 요구사항

파기 요구사항 1 : 개인정보 파기 단계에서 생성되는 감사레코드는 아래 기능을 수행하는데 충분해야 한다.

- 개인정보 파기를 수행하는 개인정보 이용자가 개인정보를 파기할 수 있는 정당한 권한을 가지는지 점검

파기 요구사항 2 : 개인정보 파기 단계에서 생성되는 감사레코드는 최소한 다음의 정보를 포함해야 한다.

- 파기 개인정보 식별정보 및 소유자 정보

- 개인정보 DB 파기 수행자 식별정보
- 개인정보 파기 수준
- 개인정보 파기 수행에 필요한 개인정보 소유자 사전 동의 및 사후 통지 여부
- 개인정보 이용자의 개인정보 파기 후 실행하는 의무사항 식별정보 및 실행 결과
- 감사레코드의 생성 시각 정보, 무결성 점검정보

파기 요구사항 3 : 감사레코드들은 무결성과 가용성이 보장되어야 하며, 저장된 감사레코드는 개인정보 소유자 또는 개인정보 관리책임자 등 감사레코드 조회 권한을 가진 사용자에 의해서만 조회되어야 한다.

- 감사레코드는 어떠한 경우에서도 파기되지 않고 저장되어야 하며, 법률에 의한 경우 일정 기간이 지난 감사레코드는 파기될 수 있음

파기 요구사항 4 : 개인정보 DB에 저장된 개인정보는 정당한 절차만으로 사용되고 정당하지 않은 우회로를 제공해서는 안 된다.

- 개인정보의 사용이 완료되면 허가받지 않은 복제, 저장 연산을 수행해서는 안 됨
- 사용이 완료된 개인정보는 복원불가능 하도록 완전히 파기해야 함
- 파기된 개인정보가 저장된 기억장소가 다른 용도로 사용되기 위해 할당될 경우 파기된 개인정보가 전체 또는 부분적으로 복구되어서는 안 됨

4.4.2 프라이버시 보호 요구사항

파기 요구사항 5 : 개인정보 DB 관리기술은 개인정보의 수집 목적을 달성한 경우에 개인정보를 파기해야 한다.

파기 요구사항 6 : 개인정보 DB 관리기술에 의한 개인정보 파기는 공정하고 합법적이어야 하며 명시된 목적에 부합하는 정확한 개인정보 만을 파기해야 한다. 파기되는 개인정보는 완전하게 삭제되어야 하며 복구가 불가능해야 한다. 기관이나 조직은 개인정보가 정확히 파기되었음을 수시로 점검하고 파기 연산에 안전성을 보장할 수 있는 내부 메커니즘을 갖추고 있어야 한다.

파기 요구사항 7 : 개인정보 DB 관리기술을 운용하여 개인정보를 파기하는 기관이나 조직은 수집단계에서 수집된 개인정보의 파기에 관한 관례, 정책, 절차를 명확하게 기술하여 개인정보 소유자가 쉽게 접근할 수 있도록 제공해야 한다. 공개하는 항목은 다음과 같다.

- 수집단계에서 수집된 개인정보의 파기 정책
- 개인정보 수집목적의 달성을 명시한 규칙
- 개인정보 관리자와의 연락방법
- 개인정보 소유자가 제공한 개인정보를 합법적으로 파기할 수 있는 방법
- 개인정보 소유자가 제공한 자신의 정보가 안전하게 파기되었음을 검증할 수 있는 방법

V. 결 론

본 논문에서는 개인정보 관리 기능 특성에 따라 DBMS 보안 측면과 프라이버시 보호 측면을 함께 고려하여 생명주기에 기반을 둔 개인정보 DB 관리기술 보안 요구사항을 개발하였다. 개발된 보안 요구사항은 일반적인 DBMS 보안 요구사항 외에도 개인정보의 수집, 저장 및 관리, 이용 및 제공, 파기 단계에서 준수되어야 하는 개인정보 사용목적 명확화 및 제한적 수집, 개별참여, 개방원칙 등의 프라이버시 보호원칙이 반영되어 있다. 향후 제안된 개인정보 DB 관리기술 보안 요구사항은 개인정보보호에 대한 사회적 요구 증대와 안전한 개인정보보호를 의무화하는 금융, 의료, 교육, 기업회계 등 다양한 분야에 특화된 법률 시행에 따라 제품개발과 사용이 확대될 개인정보 데이터베이스 시스템에 대한 객관적이며 체계적 평가기준으로 활용될 수 있을 것으로 기대되며, 개인정보보호 서비스를 제공하는 정보시스템 또는 서비스 개발자에게 프라이버시 보호를 위한 개인정보 DB 개발기준으로 활용될 수 있을 것이다.

참 고 문 헌

[1] Camp, J.L., "Digital identity," Technology and Society Magazine, IEEE, Volume 23, Issue 3, 2004.

[2] Jonghwa Choi, Dongkyoo Shin, Dongil Shin, "Research and implementation of the context-aware middleware for controlling home appli-

ances," Consumer Electronics, IEEE Transactions on Volume 51, Issue 1, 2005.

[3] Philip J. Windley, Digital Identity, O'Reilly, 2005

[4] OECD, "OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data," http://www.oecd.org

[5] Federal Trade Commission, "Fair Information Practice Principles," http://www.ftc.gov/reports/privacy3/fairinfo.shtm

[6] Online Privacy Alliance, "Guidelines for Online Privacy Policies," http://www.privacyalliance.org/resources/ppguidelines.shtml

[7] Privacy Code, Canadian Standard Association, http://www.csa.ca/standards/privacy/

[8] PRIME(Privacy and Identity Manage ment for Europe), PRIME Project, https://www.prime-project.eu/

[9] PRIME Architecture V2, PRIME Project, 2007. https://www.prime-project.eu/

[10] "P3P: The Platform for Privacy Preferences," W3C, http://www.w3.org/P3P/,

[11] Paul Ashley, Satoshi Hahda, Gunter Karjoth, Matthias Schunter, "E-P3P Privacy Policies and Privacy Authorization," Workshop on Privacy in the Electronic Society 2002(WPES'02), 2002. 11.

[12] Thuraisingham, Bhavani M., "Database and Applications Security: Integrating Information Security and Data Management," Auerbach Publication, 2005.

[13] Elisa Bertino, Ravi Sandhu, "Database Security-Concepts, Approaches and Challenges," IEEE Transactions on Dependable and Secure Computing, VOL. 2, NO. 1, 2005.

[14] Howard Smith, "Database Management System Protection Profile," http://www.commoncriteriaportal.org/public/files/ppfiles/dbms.pp.pdf, 2005.

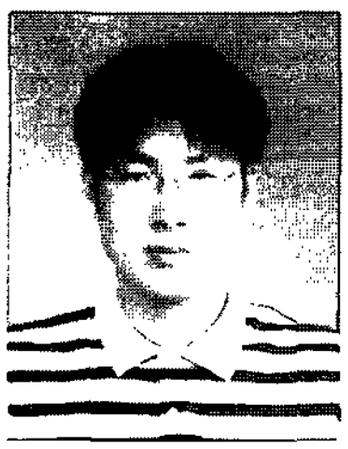
[15] Abdelmounaam Rezgui, Athman Bouguettaya, Mohamed Y. Eltoweissy, Virginia Tech, "Privacy on the Web: Facts, Challenges, and Solutions," IEEE Security and Privacy, 2003.

[16] "Information Technology - Security techniques - A Privacy framework, Working Draft 29100 (N5881)," ISO/IEC JTC 1/SC27, 2007. 6.

〈著者紹介〉

최 향 창 (Hyangchang Choi)
정회원

2002년 8월 : 전남대학교 대학원 전산학과 졸업(이학석사)
2005년 8월 : 전남대학교 대학원 정보보호 협동과정(이학박사)
2005년 8월~현재 : 전남대학교 시스템보안 연구센터 박사후 연구과정
<관심분야> 개인정보 DB 보호, 디지털 Identity 보안, 유비쿼터스 보안, 전자상거래 보안, 컴퓨터와 네트워크 보안



김 현 (Hyun Kim)
정회원

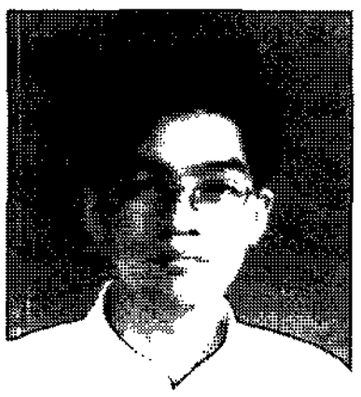
2005년 2월 : 고려대학교 수학과 학사
2005년 3월~현재 : 고려대학교 정보보호대학원 석사(수료)
2006년 4월~현재 : 한국정보보호진흥원 암호응용팀 연구원
<관심분야> 암호 알고리즘 분석, 개인정보보호

박 해 룡 (Haeryong Park)
종신회원

1999년 2월 : 전남대학교 수학과 학사
2001년 2월 : 서울대학교 수학과 석사
1999년 2월 : 전남대학교 정보보호협동과정 박사
2006년 4월~현재 : 한국정보보호진흥원 암호응용팀 선임연구원
<관심분야> 전자서명 알고리즘/암호프로토콜 설계 및 분석

전 길 수 (Kilsoo Chun)
종신회원

1991년 2월 : 서강대학교 수학과 이학사
1993년 2월 : 서강대학교 대학원 수학과 이학석사
1998년 2월 : 서강대학교 대학원 수학과 이학박사
1998년 10월~1999년 9월 : 서강대학교 기초과학연구소 박사후 연구원
2001년 3월~2001년 6월 : 서강대학교 컴퓨터학과 연구교수
2001년 7월~현재 : 한국정보보호진흥원 암호응용팀장
<관심분야> 암호학, PET, Digital ID Management



이 형 효 (Hyung-Hyo Lee)
종신회원

1987년 2월 : 전남대학교 계산통계학과(학사)
1989년 2월 : KAIST 전산학과(석사)
2000년 2월 : 전남대학교 대학원 전산학과(박사)
1990년~1992년 : 삼보컴퓨터 기술연구소
1993년~1997년 : 한국통신 연구개발원
2001년 3월~현재 : 원광대학교 정보·전자상거래학부 부교수
<관심분야> 프라이버시보호, Identity 관리시스템, 보안온톨로지, 응용보안