2

# 개인정보 이슈 및 메커니즘

## - 개인정보 정책 및 접근제어 중심으로 -

성신여자대학교 ▌홍승필 · 장현미

### 1. 서 론

개인정보란 "생존하는 개인에 관한 정보로서 성명 · 생년월일 · 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호 · 문자 · 음성 · 음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)"를 말한다[1,2].

개인정보는 표 1과 같이 개인의 신상 관계성에 기반한 정보이며, 유형별로 구분될 때 다음과 같다.

개인정보의 가장 두드러진 특징은 정보통신 기술의 발전과 범세계적인 서비스기반이 확대됨에 따라 디지털화된 개인정보의 가공 및 활용이 용의해졌다는 것이다. 그에 따라 정부나 민간단체로부터 정보주체의 어떠한 동의 없이 무한대로 수집 · 축적 · 처리 · 가

표 1 개인정보 유형별 종류

| 유형구분 | 개인정보의 종류 |
|---|---|
| 일반정보 | 이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 성별 |
| 가족정보 | 가족구성원들의 이름, 출생지, 생년월일, 직업, 전화번호 |
| 교육정보 | 학적사항, 기술자격증 및 전문면허, 상벌사항 |
| 병역정보 | 군번 및 계급, 제대유형, 주특기, 근무부대 |
| 부동산정보 | 소유주택, 토지, 자동차, 기타 소유차량, 상점 및 건물 등 |
| 동산정보 | 보유현금, 저축현황, 현금카드, 주식, 채권, 예술품, 보석 |
| 소득정보 | 현재 봉급, 봉급경력, 보너스 및 수수료, 이자소득, 사업소득 |
| 기타수익정보 | 보험(건강, 생명 등), 가입현황, 회사의 판공비, 퇴직프로그램 |
| 신용정보 | 대부잔액 및 지불상황, 저당, 신용카드, 압류 통보 기록 |
| 법적정보 | 전과기록, 자동차교통위반기록, 구속기록, 이혼기록, 납세 |
| 의료정보 | 가족병력기록, 과거의료기록, 정신질환기록, 각종 의료정보 |
| 신체정보 | 지문, 홍채, DNA, 신장, 가슴둘레 등 |

표 2 개인정보 침해 유형

| 개인정보 침해유형 | 현 행 | 향후 발생가능한 문제점 |
|---|---|---|
| 부적절한 접근과 수집 | 정보주체의 동의 없는 개인정보의 수집 | 정보주체가 인식할 수 없는 상황에서 완전한 자기 정보 통제권을 상실할 가능성이 큼 |
| 부적절한 분석 | 부적절하게 수집된 정보의 분석, 동의 없는 사적정보의 분석 | 부적절하게 수집된 정보의 분석을 통해 개인 지배 또는 개인에 대한 통제행위가 심화될 가능성이 큼 |
| 부적절한 모니터링 | 동의 없는 개인의 인터넷 활동 모니터링 | 부적절한 모니터링을 통한 개인의 라이프스타일 등 개인의 생활 전반이 노출될 가능성이 큼 |
| 부적절한 개인정보 유통 | 개인정보를 제 3자에게 양도하는 등 불법적 거래 | 개인정보를 제 3자에게 양도하는 등 다양한 유형의 개인정보가 불법적으로 거래되거나 유통될 가능성이 큼 |
| 원하지 않은 영업행위 | 동의 없는 상품광고, 광고성 정보 전송행위 | 개개인의 특성에 정확하게 대응하는 구체적 상품 광고가 동의 없이 무차별적으로 유통될 수 있음. |
| 부적절한 저장 | 정보수집 목적 달성 후 개인정보를 파기하지 않는 행위 | 한번 수집된 정보는 파기되지 않고 수차례의 분석을 통해 다양한 용도로 재활용될 가능성 큼 |

표 3 2006년 개인정보 피해구제현황

| 침 해 유 형 | 2005년 | | 2006년 | | 증가율 |
|---|---|---|---|---|---|
| | 건수 | 비율 | 건수 | 비율 | |
| 이용자 동의없는 개인정보 수집 | 1,140 | 6.3 | 2,565 | 10.99 | ▲125 |
| 개인정보 수집시 고지 또는 명시의무 불이행 | 15 | 0.1 | 27 | 0.12 | ▲80 |
| 과도한 개인정보 수집 | 33 | 0.2 | 61 | 0.26 | ▲85 |
| 고지·명시한 범위를 초과한 목적 외 이용 또는 제3자 제공 | 916 | 5.0 | 917 | 3.93 | ▲0.1 |
| 개인정보 취급자에 의한 훼손·침해 EH는 누설 | 186 | 1.0 | 206 | 0.88 | ▲11 |
| 개인정보처리 위탁시 고지의무 불이행 | 4 | 0.05 | 5 | 0.02 | ▲25 |
| 영업의 양수 등의 통지의무 불이행 | 7 | 0.05 | 11 | 0.05 | ▲57 |
| 개인정보관리책임자 미지정 | 25 | 0.2 | 23 | 0.09 | ▼8 |
| 개인정보보호 기술적·관리적 조치 미비 | 290 | 2.1 | 632 | 2.7 | ▲62 |
| 수집 또는 제공받는 목적 달성 후 개인정보 미파기 | 152 | 0.8 | 266 | 1.2 | ▲75 |
| 동의철회·열람 또는 정정 요구 등 불응 | 771 | 4.2 | 923 | 3.96 | ▲20 |
| 동의철회 열람· 정정을 수집방법보다 쉽게 해야할 조치 미이행 | 285 | 1.6 | 484 | 2.1 | ▲69 |
| 법정대리인의 동의없는 아동의 개인정보 수집 | 71 | 0.4 | 23 | 0.1 | ▼67 |
| 주민번호 등 타인 정보의 훼손·침해·도용 | 9,810 | 53.9 | 10,835 | 46.4 | ▲10 |
| 기타(정보통신망법 규정 외의 침해유형 | 4,401 | 24.1 | 6,355 | 27.2 | ▲44 |
| 합 계 | 18,205 | 100 | 23,333 | 100 | ▲28 |

공·이용하여 개인정보통합관리시스템이 구축이 가능해지면서 개인정보 도용 및 유출에 따른 피해가 끊임없이 발생하고 있다[2,4].

본 논문의 구성은 다음과 같다. 1장에서는 논문의 개요를 간략하게 소개하였으며, 2장에서는 사회적으로 이슈화되고 있는 개인정보 침해현황 및 개인정보 이슈에 대해 설명하였다. 3장에서는 개인정보보호 관련 기술 및 표준에 대한 동향을 제시하였으며, 4장에서는 사례연구를 통한 개인정보 쓰임새와 현황을 알아보고, 5장에서는 개인정보 정책 설정 방안과 시스템 환경 내 효과적인 접근제어가 가능한 메커니즘을 제시하였다. 마지막으로 6장에서 결언 및 향후연구를 소개하였다.

## 2. 개인정보 침해현황 및 이슈

### 2.1 개인정보 침해 현황

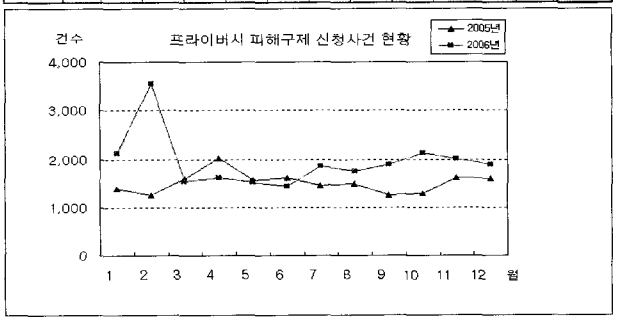
개인정보는 인터넷, 각종 마케팅 행사, 다양한 커뮤니티, 설문조사 등의 방법으로 각 개인이 원하지 않음에도 불구하고 각종 저장매체에 기록되고 유통되고 있다. 위 표 2는 현행 개인정보 침해유형을 분류하였다.

표 3은 2006년 개인정보 피해구제현황으로써, 가장 많이 접수된 침해유형으로는 고객확보를 위해 통신사 및 금융사 등의 업체가 개인정보를 데이터베이스화하기 위해 음성적인 경로로 수집 후 악용에 따른 "타인정보 훼손·침해·도용"이 46.4%를 차지하였으며, 두 번째로는 "이용자 동의 없이 개인정보 수집" 유형이 10.99% 차지하고 있음을 보여주고 있다[3,4].

아래 표 4 현재 우리나라 개인정보처리에 대한 2005~06년 동안 접수된 개인정보 피해구제 및 상담 신청 현황으로 무려 28% 증가한 것으로 보아 프라이버시 보호에 따른 대책의 필요성이 증가되고 있다.

표 4 2005~2006년 피해구제 신청현황

| | 1월 | 2월 | 3월 | 4월 | 5월 | 6월 | 7월 | 8월 | 9월 | 10월 | 11월 | 12월 | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2005년 | 1,387 | 1,253 | 1,601 | 2,031 | 1,555 | 1,618 | 1,462 | 1,500 | 1,253 | 1,285 | 1,620 | 1,591 | 18,206 |
| 2006년 | 2,131 | 3,561 | 1,538 | 1,613 | 1,521 | 1,439 | 1,859 | 1,746 | 1,885 | 2,133 | 2,018 | 1,891 | 23,333 |




### 2.2 개인정보 이슈

개인정보 보호 측면에서 고려하여야 할 주요 이슈 및 대응방안은 아래와 같이 정리될 수 있다.

▪ **익명성(Anonymity) 또는 아호(Pseudonymity)**: 사용자 정보는 불법적 또는 악의적 목적으로서의 인용 측면에서 보호하고자 필요시 사용자 정보에 대한 책임추적성(Accountablity)이 보장되어야 하며, 적용되는 목적에 따라 다른 등급 차원에서의 익명성이 보장 되

표 5 개인정보보호 기술 활용

| 개인정보 이슈 및 정보보호 기술 활용 | 주 요 메커니즘 | | 관 련 기 술 |
|---|---|---|---|
| 익명성 or 아호 | • Strong Authentication | | • WPKI<br>• Smart Card<br>• Mobile 환경 내 Authentication 기술 |
| 사용자 동의 | • Agrement<br>• Prevention/Detection Control | | • Monitering<br>• Notice 기능<br>• Log 분석 |
| 정보의 수집 및 제어 | • Access Control<br>• Logical Flow<br>• Privacy Policy | | • Privacy Policy/Procedure/Statement/Guideline<br>• Privacy related to law, ethics, Investigation |
| 정보보호 기술 및 활용 | Application 기술 | – 전자지불 | • e-Payment(Credit Card, E-Cash/E-Check) |
| | | – 컨텐츠 보안<br>– 개인정보응용기술 | • 바이러스<br>• 전자메일<br>• PET(Privacy Enhanced Technology) |
| | | – IC 카드 | • Smart Card |
| | | – 개인정보보호 | • P3P(Platform for Privacy Preferences) |
| | Network 기술 | – 응용기술 | • 방화벽(Firewall)<br>• 침입탐지시스템(IDS)-N/W 기반<br>• 가상사설망(VPN) |
| | | – 전송계층 | |
| | | – 네트워크 | |
| | | – 데이터링크 | |
| | System 기술 | – 소프트웨어 | • 침입탐지시스템(IDS)-Host 기반 |
| | | – 하드웨어 | |
| | 데이터 기술 | – 예방(Prevention) | • DB접근제어, 그룹통제 |
| | | – 탐지(Detection)/ 교정(Correction) | • DB Backup |
| | 암호화 | – 비밀키, 공개키 | • Crypto Toolkit |
| | | – 암호화 알고리즘 | |

어야 한다.

• **사용자 동의(Notice)**: 웹 시스템 환경 내 점점 개인정보가 분업화, 다각화 되어 지면서, 한번 입력 된 개인정보가 필요한 곳에 효과적으로 사용 되어 지는 방법과 정보가 필요한 곳에서만 사용자의 동의아래 사용되어 질 수 있는 방안이 필요하다.

• **정보의 수집 및 제어(Information gathering and Access)**: 사용자는 필요시 자기 정보에 대하여 접근 및 변경이 용이하여야 한다. 혹 사용자의 동의 없이 개인정보에 접근하고, 수집하려 할 때를 고려하여 제도적, 기술적 측면에서 개인정보를 보호하기 위한 접근 제어 방안은 매우 중요한 개인정보 해결방안 중의 하나이다.

• **정보보안(Security)**: 개인정보를 활용(수집 및 관리· 운영) 측면에서 기술적, 제도적, 관리적 측면에서 혹 발생 될 수 있는 위험 요소에 대하여 그 피해를 최소화하기 위한 예방이 필요하며, 모니터링 · 교정 측면에서 정보보안 기술 및 정책, 절차 및 지침 등을 활용하여야 한다.

위의 사례를 기반으로, 개인정보에 대한 침해유형은 크게 다음 6가지로 구분해 볼 수 있다[5]. 1) 부적절한 접근과 수집, 2) 부적절한 모니터링, 3) 부적절한 분석, 4) 부적절한 이전, 5) 원하지 않은 영업행위, 6) 부적절한 저장 등이 있으며, 이는 지식정보사회의 발달과 더불어 점점 증가하는 웹 시스템 환경 내 사용되는 개인정보들은 개인적으로나 사회적으로 1) 개인의 사적 공간, 2) 개인의 안전성, 3) 사회적 배제(Social Exclusion) 초래, 4) 기업과 소비자 사이에 힘의 불균형 측면에서 중대한 위협이 될 수 있다[5,6].

## 3. 관련연구

### 3.1 개인정보 관련기술

개인정보보호 기술(Privacy Enhancing Technology: PET)은 크게 웹기반의 익명성 제공 기술, Agent 기술과 네트워크 기반 기술의 3가지 범주로 나눌 수 있다[7].

#### 3.1.1 웹 기반의 익명성 제공 기술

정보의 노출 자체와는 무관하게 정보와 소유자간의 관계나 송수신 자간의 관계를 비밀로 하여 사용자

의 개인정보보호를 제공하는 기술로 상세 기술은 표 2와 같이 정리 할 수 있다.

#### 2.1.2 에이전트 기술

개인정보보호를 위한 에이전트(agent)는 사용자가 파악하기 어려운 인터넷상에서의 정보 유출에 대해 사용자를 대신하여 통제해 주는 역할을 하며 쿠키매니저(cookie manager), 에드 브로커(ad blocker), 스파이웨어 필터(spyware filter) 등의 기술이 있다.

#### 2.1.3 네트워크 기반 기술

현실적으로 가장 빈번하게 일어나는 개인정보 침해 사고들은 네트워크 환경에서 정보를 전달할 때 중간에 가로채거나 수정하거나 또는 단순히 그 데이터를 보기만 하는 행동들에 의해 발생되며 신뢰할 수 있는 네트워크를 구성하기 위하여, Proxy, Firewall, IDS, IPS 등이 있다[7].

그 외 개인정보의 가용성, 무결성 등을 고려하여 암호화나 접근제어 등과 같은 정보보호 기술이 고려되어야 한다.

### 3.2 관련 표준 및 동향

■ P3P(Platform for Privacy Preferences)

P3P(Platform for Privacy Preferences)는 지난 2002년 국제 웹 표준화 기구인 W3C(World Wide Web Consortium)가 웹사이트 이용 시 프라이버시를 보호하기 위해 정한 표준 기술 플랫폼으로, 개인 사용자는 자신의 Privacy 보호 Preference를 주어진 프로그램이나 에디터 등을 통해 명시하고 사용자 브라우저는 이 보호정책과 맞지 않는 웹서버를 차단하여 개인정보유출을 사전에 방지하는 기술이다[9].

■ OECD

프라이버시에 대한 논의는 OECD에서 이미 1978년 대부터 시작하여왔다. 그리고 이러한 논의의 결과1980년 "프라이버시 보호와 개인 데이터의 국제유통에 관한 가이드라인에 관한 이사회 권고"라는 가이드라인을 채택하였고, 개인정보의 사생활권 보호, 정보의 자유로운 유통 장려, 국내사생활보호입법에 의한 자유로운 정보유통에 대한 부당한 제한방지, 관련국내법규정과의 조화를 주목적으로 하고 있는 가이드라인의 8가지 원칙은 다음과 같다[10].

■ 국가별 개인정보보호 동향

표 7은 각 국가별 개인정보 보호를 위한 가이드라인의 현황 및 특징을 제시하고 있다[11].

## 4. 사례연구 - HIPAA

HIPAA('Health Insurance Portability and Accountability Act of 1996'19)는 미국이 제정한 프라이버시 규정으로써, 의료정보의 사용과 공개에 대한 표준을 규정하는 개인정보보호에 관한 대표적인 프로젝트라고 할 수 있다. 이를 통해 사람들의 이해를 도모하고 통제권을 보장하여 질 높은 건강관리 서비스를 제공하는 것을 목적으로 하며 의료보험기관, 의료서비스제공자, 요금청구 수납조직 등과 같은 의료정보취급기관에 적용된다. 프라이버시 규정에서 보호하는 것은 PHI

표 6 OECD의 개인정보 보호원칙

| 원 칙 | 내 용 |
|---|---|
| 수집제한 | 개인데이터의 수집에는 제한을 두어야 한다. 어떠한 개인 정보도 합법적이고 공정한 절차에 의하고 가능한 경우에는 데이터주체에게 알리거나 동의를 얻은 연후에 수집하여야 한다. |
| 정확성확보 | 개인데이터는 그 이용목적에 부합되는 것이어야 하며 이용 목적에 필요한 범위 안에서 정확하고 완전하며 최신의 것이어야 한다. |
| 목적명시 | 개인정보는 수집 시 그 수집목적이 명확히 제시하고, 그 후의 이용은 수집목적의 실현 또는 수집목적과 양립되어 목적이 변경될 때마다 명확화 될 수 있는 것으로 제한되어야 한다. |
| 이용제한 | 개인정보는 목적명확화의 원칙에 의하여 확인된 목적 이외의 다른 목적을 위해 개시, 이용, 그 밖의 사용에 제공되어서는 안 된다. 다만 정보주체의 동의가 있거나 법률의 규정에 의한 경우에는 예외로 한다. |
| 안전성확보 | 개인데이터는 그 분실 또는 불법적인 액세스, 파괴, 사용, 수정, 개시 등의 위험에 대하여 합리적인 안전조치를 함으로써 보호하여야 한다. |
| 공 개 | 개인데이터와 관련된 개발, 실시, 정책에 대하여는 일반적인 공개정책을 취하여야 한다. 개인데이터의 존재, 성질 및 그 주요 이용 목적과 함께 데이터관리자의 식별, 주소를 명확하게 하기 위한 수단은 용이하게 이용할 수 있어야 한다. |
| 개인참여 | 자신에 관한 정보를 합리적인 기간 내에 합리적인 비용과 방법에 의해 알기 쉬운 형태로 통지 받을 권리를 갖는다. 이러한 권리가 거부된 경우에 개인은 그 이유를 구하고 거부에 대하여 이의를 제기하거나 데이터의 폐기, 정정 및 보완을 청구할 권리를 갖는다. |
| 책 임 | 데이터관리자는 위의 제 원칙을 실시하기 위한 조치에 따를 책임이 있다. |

표 7 국가별 프라이버시 현황

| 국 가 | 운영기관 | 법 · 제도 현황 | 특징 |
|---|---|---|---|
| 프랑스 | ▪ 국가정보처리자유위원회 CNIL (The National Commission on Information and Freedom) | ▪ 1978년 프랑스의 개인정보법 The Data Protection Act No. 78-17 정보처리축적 및 자유에 관한 법률 제정 | ▪ 공공부분, 민간부분 통합형 |
| 독일 | ▪ Bundesministerium der Justiz | ▪ 1977년 연방정보보호법과 주의 정보보호법제정<br>▪ 1990년 연방데이터보호법 시행<br>▪ 2001년 EG-정보보호지침에 따라 연방데이터 보호법 개정 | ▪ 공공부분, 민간부분 분리형 |
| 영국 | ▪ ICO(Information Commissioner's Office) | ▪ 1998년 7월 데이터보호(Data Protection Act) | ▪ 공공부분, 민간부분 통합형 |
| 미국 | ▪ 대통령 주요기반시설보호위원회 (Presidents's Critical Infrastructure Protection Board) | ▪ 1974년 프라이버시법 (Federal Privacy Act)<br>▪ 1978년 금융프라이버시권법<br>▪ 1994년 전기통신 프라이시법<br>▪ 1996년 통신법 및 의료기록 비밀보호법 | ▪ 공공부분, 민간부분 분리형 (공공부분- 법 적용 민간부분- 윤리적 통제) |

표 8 개인정보 아키텍처 구현 방안 예

| 단계 | 단계별 분류 | 주 요 내 용 | | 적 용 방 안 | |
|---|---|---|---|---|---|
| I | 개인정보 수집 | - OECD의 개인정보 보호원칙 수집제한, 정확성확보, 목적명시, 이용제한, 안정성확보, 공개, 개인 참여, 책임의 8대 원칙을 통해 정보주체의 동의절차에 대한 명시를 포함하고 있다. | | 활용 방안 | ▪ 개인정보 보호 및 국제적 유통에 관한 지침서<br>▪ 개인정보 등급별에 준한 정책 기반 확립 (P1, P2, P3. P4. P5) |
| II | 개인정보 정책에 준한 접근제어 방안 | 개인 정보 정책 | - 개인정보를 위한 중심축으로서 전반적이고 선언적인 내용으로 정책은 목적, 적용 및 책임 범위 등을 고려하여 5단계로 등급으로 정의한다. | | 예) - P1 개인정보 관련한 기밀정보<br>- P2 개인정보 관련 취급 시 주의를 요하는 정보<br>- P3 개인정보관련 적절한 통제가능아래 공개 기능 여부가 가능한 정보<br>- P4 개인정보관련 어느 정도 공개 가능한 정보<br>- P5 국민 공개 가능정보 |
| | | 개인 정보 절차 | - 개인정보 정책애서 정의 된 세부 사항을 달성하기 위해 관련분야를 세부적으로 명시한다. | | 예) - P_100: 개인정보보호 관련 부서의 역할과 책임<br>- P_200: 개인정보보호에 관련된 자들의 역할과 책임<br>- P_300: 개인정보보호 사고 시 대응 절차<br>- P_400: 개인정보보호 서비스 제공시 고려 절차<br>- P_500: 개인정보관련 사용자 인증 관리 규정 |
| | | 개인 정보 가이드 라인 | - 개인정보 시스템을 다루는 운영자, 관리자 측면에서 역할 대비 실행 할 수 있는 가이드를 절차에 준하여 제시 한다. | | 예) - P_100_A_001: 사용자 개인정보 발급/신청/폐기 절차<br>- P_100_A_002: 개인정보 입력 발생 시 처리 절차<br>- P_100_A_003: 사용자 정보 공유 및 2중 사용시 확인 절차 |
| III | 개인정보 기반 프레임웍 구축 | 정책/ 관리 통제 기반 | - 개인정보보호정책기술 | 적용 기술 [표5 참조] | ▪ P3P<br>▪ HTML 기반 |
| | | | - 개인정보보호 정책관리 | | ▪ 개인정보보호정책 운영관리<br>▪ 개인정보 관리 (쿠키관리, 개인정보 제거) |
| | | 운영/ 기술 통제 기반 | - data 보호<br>- 접근통제 | | ▪ DB 접근제어, 그룹통제<br>▪ DATA Access Control |
| | | | - 전송 · 오남용 방지 (Network 기반) | | ▪ 방화벽<br>▪ 침입탐지시스템(IDS)<br>▪ 침입방지시스템(IPS)<br>▪ 위협탐지시스템(TMS) |
| | | | - 정보 · 오남용 방지 (응용/System 보안) | | ▪ 암호화(Crypto Toolkit.), PKI, PMI, 접근통제, (Access Control List. Access Control Matrix) |

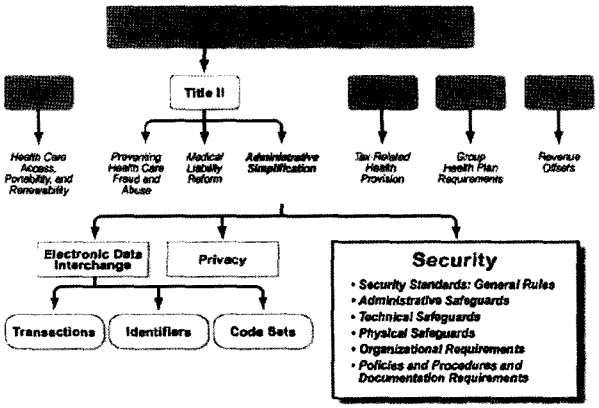



그림 1 HIPPA 구성도

(Protected Health Information)로 개인 식별이 가능한 모든 의료정보를 보호 대상(전자, 종이, 음성 등)으로 하며, 개인 식별이 가능한 의료정보는 각 개인의 과거, 현재, 미래의 신체적, 정신적 상태나 개인의 진료 및 치료내역과 의료비 발생내역을 포함한다[12,13]. 위 그림 1은 HIPPA의 구성도를 제시한 그림이다[14].

최근 혁신적인 기술 발전과 건강하고 윤택한 삶에 대한 욕구가 부합하면서 의료 서비스 분야에서도 의료정보 시스템과 비즈니스 애플리케이션 등 관련 기술이 다양화 및 고도화되어 짐에 따라 의료정보 기술에 대한 표준화가 활발하게 이루어지고 있는 실정이다.

현재 미국 내에서는 이러한 기술에 맞춰 HIPPA를 기준으로 정보화 정책 범위에 대한 명확한 정의부터 시작하여 정부와 민간, 서비스의 공급자와 소비자, 관련 산업 내 이해관계자들을 사이에서 진행되고 있다. 하지만 우리나라의 경우 의료분야에서의 IT 활용도는 전체 산업 분야에 비해 매우 낮은 실정이며, 보안 관리의 인식부족은 물론 민감한 의료정보를 보호함에 있어 명확한 기술적, 법 제도적 방안이 HIPPA와 비교하여 볼 때 좀 더 체계적인 연구의 필요성이 요구되어 지고 있다.

## 5. 개인정보정책기반의 아키텍처 구현 방안

본 논문에서는 신뢰할 수 있는 개인정보보호 정책 확립 및 아키텍처 구현 방안을 3단계로 제시하였다. 그에 대한 주요 구성으로 1단계 - 개인정보 정책에 준한 정보의 분류 및 정의, 2단계 - 주워진 개인정보 정책에 따른 효과적인 역할별 접근제어 방안 확립, 3단계 - 지정된 접근제어 기반의 개인정보 시스템 확립 및 관련 정보보호 기술 연동 방안 수립이며, 상세 내역 및 적용방안은 표 8과 같다.

위와 같이 제시된 개인정보 아키텍처는 실제 협업에서 관련 정보보호 기술과 적용되며, 아래 그림 2와 같이 보여질 수 있다[표 5 참조].

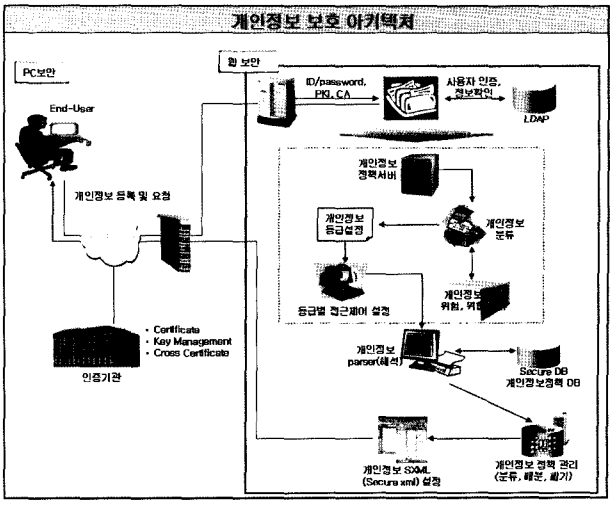



그림 2 정보보호기술과 접목된 개인정보 아키텍처

## 6. 결 론

혁신적인 기술 발전과 인터넷을 통한 서비스 기반이 확대되어짐에 따라 민감한 개인정보의 보호와 정보시스템에 따른 보안문제가 사회적 이슈로 떠오르고 있다. 하지만 국내에서는 이를 보완할 수 있는 기술적, 법 제도적인 정책이 실제 활용 부분에서의 어려움이 있으며, 특히 개인정보보호를 위한 시스템 인프라 구축이 시급한 실정이다.

본 논문에서는 개인정보보호정책에 따른 지침, 절차에 준한 사용자별 등급을 설정하고, 그에 따른 적합한 역할대비 접근통제를 부여함으로써, 보다 안전하게 개인정보를 관리·통제할 수 있는 방안을 제시하였다. 또한 제시한 방안을 기존의 정보보호 기술과 접목한 시스템 환경 측면에서의 신뢰를 기반으로하여 개인정보 공유 및 활용할 수 있는 아키텍처를 제시하였다. 향후 유비쿼터스 환경에서 사용자 정보를 효율적으로 보호하기 위한 기술적 방안에 대해 연구할 계획이다.

## 참고문헌

[1] Springer-Verlag New York "Information Security and Privacy" Australasian Conference, Acisp 2006 Melbourne, Australia, July 3-5, 2006.

[2] P. W. Warren, "From Ubiquitous Computing to Ubiquitous Intelligence", BT Technology Journal, Volume 22 Issue 2, pp.28-38, April, 2004.

[3] 한국정보보호진흥원, 2005년 개인정보 피해구제 및 상담 사례분석, 2005.

[4] 한국정보보호진흥원, 2006년 개인정보 피해구제 및 상담 사례분석, 2006.

[5] 조화순, "IT혁명과 개인정보보호", 한국전산원, 05,

2004.
[6] 개인정보보호백서 2003, 한국정보보호진흥원, 2003.
[7] 홍승필, "유비쿼터스 컴퓨팅 보안", 2006.
[8] 홍승필, "유비쿼터스 컴퓨팅 환경내 개인정보보호 프레임웍 적용방안", 2006.
[9] A list of privacy surveys, Available at http://www.w3.org/P3P/p3pfaq.html.
[10] Jean-Philippe Cotis, "Economic Policy Reforms : Going for Growth 2006", OECD Publishing2, 7, 2006.
[11] 서혜석, "개인정보 이용의 해외 사례와 시사점", 정책자료집 2006.
[12] Joan Hash. Pauline Bowen, Arnold Jognson, Carla Dancy Smith, Daniel I. Steinberg, "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act(HIPPA) Security Rule." http://csrc.nist.gov/publications/nistpubs/800-66/SP800-66.pdf, 9, July, 2006.
[13] OCR HHS(United States Department of Health Human Service), "Summary of the HIPPA Privacy Rule." http://www.hhs.gov/ocr/privacysummary.pdf, 17, July, 2006.
[14] 정영철 외 9명, "e-Health의 영향 및 주요이슈", 한국보건사회 연구원, 2005.

**홍 승 필**

1993 Indiana State University(학사)
1994 Ball State University(석사)
1997 Illinois Institute of Technology(박사수료)
2002 한국정보통신대학교 (박사)
1997~2004 LG CNS Systems, Inc.
2005~현재 성신여자대학교 컴퓨터정보학부 전임강사
관심분야 : 접근제어, 정보보호 아키텍처, 유비쿼터스 보안, 프라이버시 보호
E-mail : philhong@sungshin.ac.kr

**장 현 미**

2006 서울산업대학교 산업정보시스템학과 졸업 (학사)
2006~현재 성신여자대학교 대학원 전산학과 (석사)
관심분야 : 프라이버시 보호, 유비쿼터스 보안, 접근제어
E-mail : nicemiya@sungshin.ac.kr