情 報 保 護 學 會 誌
第22卷 第2號, 2012. 4

프라이버시 참조 구조 국제표준화 동향

신 용 녀*, 김 학 일**, 전 명 근***

요 약

프라이버시 참조구조(privacy reference architecture)는 구현 및 배치 상황을 바탕으로 해야 하며, 독립적으로 존재할 수 없다. 구조 설치는 프라이버시 인지 및 가능 ICT 시스템을 배치할 구조와 조화를 이루어 운영되며 정책을 반영하는 업무 관리 기능, 프로세스 및 절차를 종합적으로 고려하여 이루어진다. 업무 및 데이터 처리 모델 또는 인벤토리의 공식적인 구축 및 유지는 해당 조직에 적용되는 모든 프라이버시 및 정보 보호 요건에 부합해야 한다. 업무 프로세스 모델이 구축되고 데이터 처리 모델과의 비교가 완료되면 동의 취득 기능, 개인식별정보 범주화 및 태깅 기능, 감사 및 기록 절차, 보존 일정, 고지 및 보안 경보와 같은 프라이버시 통제수단을 정하고 필수적인 프라이버시 보호 요건과 비교할 수 있다. ISO/IEC JTC1 SC27 WG5의 프라이버시 표준화는 프라이버시 프레임워크, 프레임워크 기반 구현을 위한 프라이버시 레퍼런스 아키텍쳐를 중심으로 이루어지고 있다. 본 논문에서는 프라이버시 표준화를 위한 국외 표준화 동향을 소개하고, 향후 추진해야할 중점 표준화 항목을 도출한다.

Ⅰ. 서 론

프라이버시 참조구조(privacy reference architecture)는 구현 및 배치 상황을 바탕으로 해야 하며, 독립적으로 존재할 수 없다. 구조 설치는 프라이버시 인지 및 가능 ICT 시스템을 배치할 구조와 조화를 이루어 운영되며 정책을 반영하는 업무 관리 기능, 프로세스 및 절차를 종합적으로 고려하여 이루어진다.

식별된 프라이버시 보호 요건을 충족시킬 수 있는 보다 종합적이고 전반적인 솔루션의 일부로서 적절한 기술적 보호수단을 찾기 위해 업무 프로세스 및 처리될 각각의 개인식별정보(PII, personally identifiable information)를 검토해야 한다. 개인식별정보를 처리하는 조직은 예를 들어 스프레드시트, 목록 또는 그래픽 소프트웨어 등의 익숙한 툴을 사용하여 다양한 프로세스 및 이들 프로세스 간의 관계를 차트로 작성해야 한다. 프라이버시 참조구조는 업무 프로세스에서 도출 가능한 원칙, 요건, 구조 계층 및 관점을 정하는 접근방식과 이들을 관리 구조 형태로 구현하는 방안을 설명하고, 기술적 구조의 설계, 구현 및 배치를 제시한다[1][2].

ISO/IEC JTC1/SC27 워킹그룹(Working Group) 5에서는 이러한 개인의 기본권인 프라이버시 보호를 위한 표준화 작업에 착수하여, 프라이버시 프레임워크(Privacy Framework)와 프레임워크 구현을 위한 프라이버시 레퍼런스 아키텍쳐(Privacy Reference Architecture)에 대한 표준화에 주력하고 있다. 국내에서도 개인정보보호법이 시행되어 개인정보보호 시장이 크게 확대되고 있다. 개인의 프라이버시 보호에 대한 이러한 발전추세에는 국내외 표준화기구를 통한 활발한 표준화작업이 밑바탕이 되고 있으며, 프라이버시에 대한 관심은 더욱 높아지고 있다. 정보통신기술의 발전과 더불어 대두되고 있는 정보보호 기법의 표준화에 대한 요구에 부응하여, 암호화 기법 등을 이용한 정보보호기법과 이들 기술에 대한 평가 등을 담당하였던 SC27이 개인정보보호와 관련이 있는 프라이버시 분야, 바이오정보보호, 신원(identity) 관리 분야로 그 영역을 넓혀나가는 것은 우리나라를 포함하여 각국에서 대두되고 있는 프라이버시 및 개인정보보호 관련 사회적 이슈를 해결하는데 크게

본 논문은 지식경제부 산업융합원천기술개발사업(10039149)으로 지원된 연구결과입니다.
* 한양사이버대학교 컴퓨터공학과/주저자 (ynshin@hycu.ac.kr)
** 인하대학교 정보통신공학과 (hikim@inha.ac.kr)
*** 충북대학교 전자공학부 (mgchun@chungbuk.ac.kr)

도움이 되리라 생각된다. 이에, 본 논문은 프라이버시 보호 기술과 관련된 표준화 워킹그룹(Working Group) 5의 프라이버시 주요 표준화 동향에 대하여 간략하게 소개하고자 한다. 본 논문의 구성은 다음과 같다. 본 논문의 2장에서는 정보보호 분과인 ISO SC27워킹그룹(Working Group) 표준화 동향에 대해 살펴보고, WG5에서 추진중인 개인정보보호 참조 아키텍쳐 표준에 대해 살펴본다. 3장에서는 프라이버시 레퍼런스 아키텍쳐에 대해 살펴보고, 4장에서 본 논문의 결언을 맺는다.

Ⅱ. ISO/IEC JTC1/SC27 WG5 표준화 동향

2.1 ISO/IEC JTC1 SC27 WG5

WG5는 ID 관리(Identity management)와 프라이버시 기술(Privacy technologies)에 대해 표준화 하고 있으며, Published 된 표준은 일본에서 주도한 ACBio (Authentication Context for Biometrics)와 한국 주도의 Biometric Information Protection이다. WG5내에서 사용되는 용어를 위한 harmonization of vocabulary Standing Document(SD3)를 만드는 목적에 대한 비규범적(non-normative)인 베이스라인 정의를 내리고, 총 25개의 대상 용어를 선정하여 추후 문서의 revision을 통해 용어정의가 이루어질 것으로 판단된다. [표 1]는 ID리 및 프라이버시관련 WG5의 표준화 추진화 현황이다[7].

2.1.1 프라이버시 프레임워크(Privacy Framework)

PII(개인식별정보) 프로세싱에 있어서, 데이터 프로세싱의 라이프 사이클은 제 삼의 기관, PII 정보를 가진 개인 혹은 어떤 목적에 의해서 PII controller로부터 이미 제어를 받고 있는 PII로부터 PII를 수집하는 것부터 시작한다[3]. 따라서, ICT의 context내에 프라이버시 이슈를 다룰 때 일반적으로 PII Principle(개인)과 PII controller(제어자, 예를들어 정부)의 두 개의 주요 액터과 관련되어있다. 프레임워크내에서 PII의 프로세싱을 개념화하기 위해서는 이 두 액터간의 여러 가지 역할(role)에 대해 차별화 시킬 수 있다. [표 2]는 PII 제공자와 수신자에 대하여 도식화한 것이다[4].

역할 :

(a) PII 소유개인은 단지 수신자에게 PII를 제공한다. PII 소유는 PII 제공자에게 있다.

(b) 개인의 목적에 의해 PII를 단순히 가공하기 위해 PII 소유개인은 수신자에게 PII를 제공한다. PII

〔표 1〕 WG5 (ID 관리 및 프라이버시 보호) 표준화 추진 현황

표준화 상태	표준 번호	표준명	에디터(국가)	비고
IS	24745	Biometric Information protection	전명근 한국	
IS	24761	Authentication context for biometrics	Yamada Asahiko 일본	
FDIS	24760	part1 : Technology and Concept	Christophe Stenuit (이탈리아)	A framework for identity management
WD (1st)		part2 : Reference Frameworke and Requirements	Edward de Jong, José Fernando Carvajal	
WD (1st)		part3 : Practice	Edward de Jong, José Fernando Carvajal	
FDIS	29100	Privacy framework	Stefan Weiss(독일)	co-editor : sujan(미국)
CD (3nd)	29101	Privacy reference architecture	Hans Hedbom 미국	co-editor : Dan Bogdanov
CD (3nd)	29115	Entity authentication assurance	Brackney 미국	ITU-T SG17 Q.6 공동 추진 (X.eaa)
WD (5nd)	29146	A framework for access management	José Fernando Carvajal Vion 스페인	co-editor Yasuo Miyakawa 일본
CD (2nd)	29191	Requirements on relative anonymity with identity escrow	Kazue Sako 일본	

〔표 2〕 서로 다른 액터간의 가능한 객체식별정보의 흐름

	PII 제공자(provider)		PII 수신자(recipient)
역할 a	PII 제공자 & PII 제어자(controller)	→	PII 수신자(recipient)
역할 b	PII 소유개인 & PII 제어자(controller)	→	PII 가공자(processor)
역할 c	PII 소유개인	→	PII 제어자(controller) PII 가공자(processor)

소유는 PII 제공자나 제어자에게 있다. PII 수신자가 PII 가공자이다.

(c) PII 소유개인은 PII 제어자(controller)에게 PII를 제공한다. 따라서, 수신자는 어떤 의미에서 일정량의 제어권을 위임받고 있고, 수신자가 PII 제어자(controller)이다.

[표 2]의 핵심은 컨트롤 권이 어디에 있는지이다. 역할(a), (b)는 제공자측에 제어권이 있고, (c)는 제어권이 수신자 측에 있다. PII 가공자(processor)는 이와 같은 시나리오에서 분명한 역할이 있다. PII 가공자(processor)는 PII 제어자(controller)의 감독아래 PII 제어자(controller)를 위해 PII를 수집하고, 처리하고, 사용하고, 전송한다. PII 가공자(processor)는 법적 계약에 의해 이와 같은 프로세싱 절차를 PII 제어자(controller)의 제어에 의해 정확하게 집행해야 하는 의무가 있다. PII 제어자(controller)는 프라이버시 요구사항들이 법적 계약에 명기되어 있는 지를 감시하고, 관련 프라이버시 컨트롤에 알맞게 집행되고 있는지를 감시하기 위해 관련 통제 기관이 될 수 있다. [표 3]은 PII 제어자(controller)와 제3의 기관간의 가능한 PII의 흐름(flow)이다.

〔표 3〕 제어자와 제3의 기관간의 가능한 객체식별정보의 흐름

	PII 제어자(controller)		제 3의 기관
역할 d	PII 제공자(provider)	→	PII 수신자(recipient)
역할 e	PII 제공자(provider)	→	PII 가공자(processor)
역할 f	PII 수신자(recipient)	←	PII 제공자(provider)

역할 :

(d) 제 3의 기관은 단순히 수신자이다.

(e) 제 3의 기관은 PII 제어자(controller)의 제어하에 약간의 추가적인 프로세싱을 수행한다.

(f) 제 3의 기관은 PII 개인과 관련된 추가적인 PII를 만들어낸다.

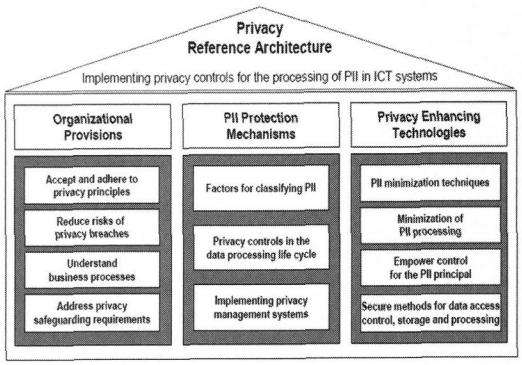
많은 경우에 PII 제어자(controller)와 PII 개인과의 역할이 일치하지 않는다. PII 개인은 PII 수신자에게 PII를 제공한다. PII 수신자는 다음 두 가지와 같이 행동할 수 있다.

(i) PII 개인의 제어 하에 PII를 가공한다

(ii) 처리를 위해 제 3자에게 PII를 전송할 권리를 포함하는 프라이버시 선택규정(preference)에 일치하고, PII 개인이 수신자가 PII를 프로세싱 할 권리를 수신자에게 허락한다면 PII 수신자가 제어자로서 행동할 수 있다.

Ⅲ. 프라이버시 레퍼런스 아키텍쳐(Privacy Reference Architecture)

프라이버시 레퍼런스 아키텍쳐 표준안은 정보 통신 시스템에서 개인식별 정보를 처리하는데 관여된 프라이버시 요구 조건의 일관적이고 기술적인 구현을 위한 참조모델을 기술한다[5]. 본 표준안은 프라이버시를 다루는 모든 부문의 역할과 책임을 구명할 뿐만 아니라, 데이터의 수명주기 관리기간내의 다양한 단계와 각 데이터 수명 주기에서 요구되는 개인정보를 위한 프라이버시 기능 구현을 포함한다[5].



〔그림 1〕 프라이버시 레퍼런스 아키텍쳐

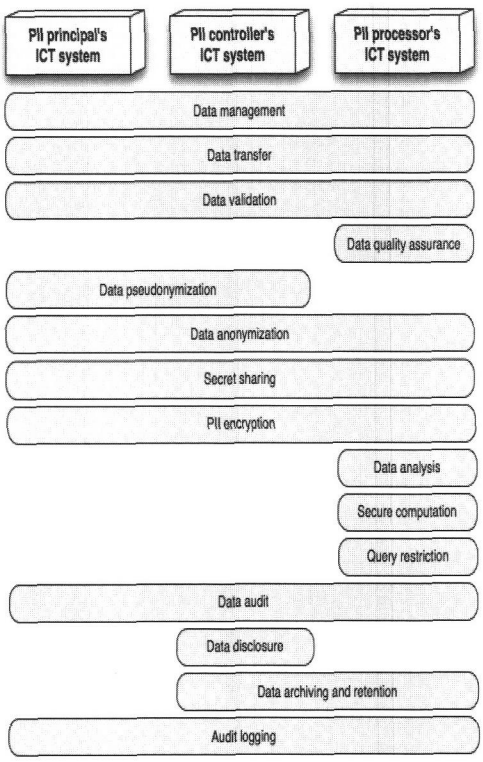
[그림 1]은 일반적인 Software Engineering 관점에서 프라이버시 보안 요구사항에 적합하고, 프라이버시를 보장할 수 있도록 하는 개발방법론 내지는 데이터 설계 방법론을 설명하고 있다. PII 제공자가 요구하는 프라이버시 요구사항에 대하여 PII 수용자는 프라이버시 보호

〔표 4〕 프라이버시 제어와 제어 보증의 예

프라이버시 요구 사항	프라이버시 제어	구현증거	제어 보증
옵트인 방법을 사용하여 PII 개인의 특정 동의를 획득	인터넷이나 문서로 동의를 획득할 수 있는 방법을 제공해야 함. PII 개인은 정보 수집, 사용, 전송, 저장, 아카이빙, 폐기에 대한 질문에 답변해야 함. 인터넷 하에서 체크박스의 형태로 옵트인 제어를 사용할 수 있음	동의에 대한 문서화와 서명된 동의에 대한 아카이빙	정기 감사
PII 정보 수집, 사용, 전송, 저장, 아카이빙, 폐기에 대한 목적에 대하여 전달하고 명시	각 PII가 수집, 사용, 노출될 때 PII를 포함하는 데이터 처리는 리스트 내 명시되어야 한다. 또한 이 리스트는 특정 목적에 따라 보완되어야 함	PII 개인의 동의 획득 관련 의견교환 뿐 아니라 정보 수집의 특정 목적과 각 데이터 처리의 문서화	정기 프라이버시 영향 평가 및 감사
명시된 목적만을 위한 PII 수집 제한	PII 수집 전에, 해당 작업과 관련된 수집의 범위와 정보의 필요성에 대해 정의해야 함	명시된 목적을 수행하기 위하여 왜 이 정보가 선택되었고 필요한지에 대하여 문서화	정기 레포트 혹은 공지
데이터 최소화 절차를 구현	PII 수집과 관련된 프로세스들은 가능한 최소한의 데이터를 수집하고 특정 업무에 독립인 방식으로 정의되어야 함	프로세스와 정의 가이드라인의 문서화	정기 프라이버시 영향 평가 및 감사
명기된 목적으로 PII 사용 완료 후 안전한 폐기	해당 업무 종료 후 PII의 폐기 혹은 익명화가 PII 프로세싱의 일부로 명시 되어야함	프로세스 정의 내 폐기 시간의 문서화	정기 프라이버시 영향 평가 및 감사
개인에게 PII 프로세싱과 관련된 정보 접근을 제공	PII 개인에 의해 요청된 정보를 다루는데 효과적으로 프로세스는 정의되어야 함 요청된 정보의 안전한 전송에 대한 수단과 더불어 요청자의 신원과 권한을 고려해야 함	프라이버시 정보요청 정책과 프로세스의 문서화, 전송 가이드라인의 문서화	정기 감사
PII의 정확성과 질의 검사	해당 업무 종료 후 PII의 폐기 혹은 익명화가 PII 프로세싱의 일부로 명시 되어야 함	프로세스 정의 내 폐기 시간의 문서화	정기 프라이버시 영향 평가 및 감사

방안 및 정책을 수립하여 Privacy Reference의 수집, 전송, 사용, 저장, 장기보장, 삭제되는 모든 유통기간을 만족시켜야 한다. Privacy Reference 아키텍처는 실질적인 개발, 구현, 운영, 통신 시스템의 프라이버시 보호의 측정이 가능하도록 Privacy Framework를 확장하였다. Privacy Reference 아키텍처는 실질적인 사례중심으로, 포털 이나 원격 의료 등에서 프라이버시 정보를 취급하는 구현 사례를 조사하여, 실질적으로 구현을 어떻게 했는지에 대한 사례를 설명하는 표준이 될 것 이다. Privacy Reference 아키텍처는 SE 개발 방법론 기반의 구성도를 그리고 실질적인 아키텍처를 설계하는 것을 목표로 한다. PI 제공자의 프라이버시 요구사항과 프라이버시 권리인 policy(정책)를 만족하기 위한 safeguarding controlling(프라이버시 보호절차) 동시에 보장하는 프레임워크에 따라서 실질적인 아키텍처를 표준화하고 있다. [표 4]는 프라이버시 제어와 제어 보증 예이다[6].

프라이버시 레퍼런스 아키텍처에서 데이터 레이어는 종합 데이터 관리 및 데이터 감사와 같이 전체적으로 사용되는 서비스를 포함한다. 그러나 이 레이어에는 모든 행위주체에 대해 배치될 수도 있지만 설계에 따라 특정 행위주체에 배치하는 것이 더 이득이 될 수 있는



〔그림 2〕 데이터 레이어 내에서의 구성요소 배치

서비스도 있다는 점에 유의해야 한다. 예를 들어, 비밀 공유는 개인식별정보 주체의 ICT 시스템에 직접 배치될 때 가장 큰 효과를 발휘한다. 그러나 비밀공유는 개인식별정보 처리자의 ICT 시스템에 데이터를 전달하기 전에 개인식별정보 관리자의 ICT 시스템에 의해서도 수행될 수 있다. [그림 2]는 데이터 관련 구성요소가 배치되는 방식을 나타낸 것이다.

Ⅳ. 결 론

조직이 고객의 구매 습관 동향을 분석하고자 하는 경우, 데이터 처리와 관련된 위험을 줄이기 위해 분석을 수행하기 전에 데이터베이스에 있는 레코드를 가명화할 수 있다. 그러한 가명화된 레코드에서는 개인식별정보가 가명인 코드로 대체된다. 코드 또는 가명은 비밀 테이블이나 알고리즘을 통해 재식별 가능하여 개인별로 재식별할 수 있다. 예를 들어, 데이터베이스에 성명, 신용카드 번호, 구매 품목 및 구매 일자가 포함된 경우, 성명이 삭제되고 신용카드 번호에 일방향 기능이 사용된 데이터베이스 복사본을 만들 수 있을 것이다. 도출된 데이터세트를 데이터 분석을 수행하는 개인에게 전달하면 신용카드 소지자의 식별 위험을 크게 줄일 수 있다.

또 다른 예로는 건강검진 결과를 연구 분석에 사용하는 경우가 있다. 구별 가능한 모든 개인식별정보 영역을 제거하고 별도의 고보안 시스템에 위치하는 교차 참조 테이블에 연결된 무작위 가명 데이터를 사용하여 환자의 ID 번호를 은폐할 수 있다. 원래의 (완전한) 개인식별정보 레코드를 재구성할 수 있는 유일한 수단인 교차 참조 테이블에 대한 접근은 반드시 인가된 개인으로 제한되어야 한다.

또한, 가명화 혹은 신원 내역이 삭제된 데이터는 비교 분석, 동향 분석 또는 유형 식별과 같은 통계 분석의 목적으로 집계할 수 있다. 여러 유형의 학자금 대출 프로그램 평가를 위해 신원 내역이 삭제된 복수의 데이터세트를 취합 및 사용하는 것이 한 가지 예이다. 이러한 데이터는 연령, 성별, 지역 및 대출 잔액과 같은 대출 수여자의 특징을 보여준다. 분석자는 이와 같은 데이터세트를 사용하여 특정 수의 특정 연령대에 있는 여성이 특정 금액보다는 많은 대출 잔액을 갖고 있음을 보여주는 통계치를 산출할 수 있다. 원래 데이터세트가 구별 가능한 각 개인의 신원 정보(개인식별정보로 간주되는 정보)를 포함하고 있었지만, 신원 내역을 삭제한 다음 집계된 데이터세트는 어떠한 개인에 대해서도 연결 혹은 구별 가능한 데이터를 포함하고 있지 않다. 개인을 그와 같은 구별 가능한 데이터에 연결시키는 속성을 연결성(linkability)라고 한다. 연결성은 공격자가 둘 이상의 관심 항목(예: 주체, 메시지, 행위 등)이 시스템(이들 항목 및 다른 항목들로 구성된 시스템) 내에서 연계되어 있는지 여부를 충분히 구분할 수 있는 상황을 나타낸다. 다른 속성들을 결합하여 개인의 레코드와 관련된 신원을 도출하는 것이 가능하다는 점에 유의해야 한다. 이와 같은 공격은 자동화하기 쉽지 않으며, 공격자는 데이터베이스에 데이터가 있는 개인식별정보 주체에 관한 추가 지식이 필요할 수 있다.

프라이버시 프레임워크(Privacy Framework)는 개인식별 정보를 처리하는데 있어서의 정보와 통신 기술의 요구 사항에 의해 가이드라인을 제시하고자 하는 것을 목표로 하고, 프라이버시 참조 구조(Privacy Reference Architecture)는 프라이버시 안정보장을 위한 제어를 갖춘 정보통신 시스템을 개발하고, 구현하고, 동작시키기 위한 가이드라인을 제시하고자 하는 것이다. 이러한 프라이버시 분야 국제 표준화 동향을 파악하고 국내 Personal Information Management System(개인정보보호관리체계) 제도의 효율성 제고 및 프라이버시 분야 한국 주도 국제표준화 전략 수립이 필요한 시점이다.

참고문헌

[1] Asia Pacific Economic Cooperation (APEC), “APEC Privacy Framework”, 2005.

[2] http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, 1980.

[3] http://www.law,cornell.edu/rules/frcp/index.html#chapter_v, “Federal Rule of Civil Procedure”.

[4] ISO/IEC JTC1 SC27 Privacy Framework, SC27 N9226, May. 2011.

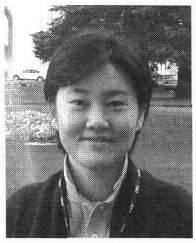
[5] ISO/IEC JTC1 SC27 Privacy Reference Architecture, SC27 N9228, May. 2011.

[6] ISO/IEC JTC1 SC27 WG5 StrudyPeriod Vocabulary, SC27 N9401, May. 2011.

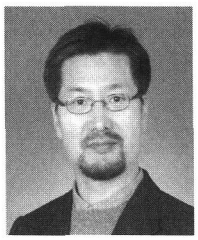
[7] ISO/IEC JTC1 SC27 WG5 Recommendation,

SC27 N9237, May. 2011.
[8] ISO/IEC JTC1 SC27 Buisiness Plan for JTC1 SC27 "Security Technique", SC27 N9463, Jun. 2010.
[9] ISO/IEC JTC1 SC27 WG5 Resolution, SC27 N9920, May. 2011.
[10] ITU-T SG17 Q.9 Summaries for work item under development in Question 9, TD1350, Dec. 2010.
[11] ITU-T SG17 Q.9 Meeting Report on Q.9/17, TD1425, Dec. 2010.
[12] HomelandSequrity Whitepaoer, "Computer Network Security & Privacy Protection", 2011.
[13] http://www.cs.ucdavis.edu/~hchen/paper/pas-sat09.pdf, "Nois Injection for Search Privacy Protection", 2011.

〈著者紹介〉



신 용 녀 (Yong-Nyuo Shin)
1999년 2월: 숭실대학교 컴퓨터학과 졸업
2001년 9월: 고려대학교 컴퓨터학과 석사
2008년 2월: 고려대학교 컴퓨터학과 박사
2002년 1월~2009년 6월: 한국정보보호진흥원 주임연구원
2009년 7월~2010년 7월: 한국은행 전자금융팀 과장
2010년 9월~현재: 한양사이버대학교 컴퓨터공학과 교수
<관심분야> 바이오인식, 프라이버시, 정형기법



김 학 일 (Hakll Kim)
종신회원
1983년 2월: 서울대학교 제어계측공학과 졸업
1985년 8월: Perdue University 전기컴퓨터공학과 석사
1990년 8월: Perdue University 전기컴퓨터공학과 박사
1990년 9월~현재: 인하 박사대학교 정보통신공학과 교수
2009년~현재: ITU-T SG17 Q.9 표준회의 라포처(의장)
<관심분야> 바이오인식, 영상처리, 컴퓨터비젼

전 명 근 (Myung-Geun Chun)
종신회원
1987년 2월: 부산대학교 전자공학과 졸업
1989년 2월: KAIST 전기 및 전자공학과 석사
1993년 2월: KAIST 전기 및 전자공학과 박사
1993년~1996년: 삼성전자 자동화연구소 선임연구원
2000년~2001년: University of Alberta 방문교수
1996년~현재: 충북대학교 전자공학부 교수
2008년~현재: TTA PG505 표준위원회 의장
2007년~현재: ISO/IEC SC27 정보보호표준화전문위원
<관심분야> 바이오인식, 개인정보보호, 지능시스템