情 報 保 護 學 會 誌
第23卷 第4號, 2013. 8

정보보호 및 개인정보보호 국제표준화 동향

박 대 하*

요 약

본 논문에서는 국제 표준화 기관인 ISO/IEC JTC 1에서 정보보호 분야의 표준화를 담당하고 있는 SC 27이 최근 작업 중인 정보보호 표준화 문건에 대한 상태와 공표 예정시기 등의 활동 정보를 작업그룹별(WG)로 정리하여 최신 정보보호 분야의 표준화 동향을 제시하고자 한다. 신규 표준으로 개발 중인 클라우드 컴퓨팅 서비스의 보안 통제, 경량 암호화 메커니즘, 보안시스템 설계 원칙 및 기법, 무선 네트워크 접근 보안, 개인정보 영향평가 등은 전세계적인 정보보호 및 개인정보보호의 최신 이슈를 반영하고 있어 국내 정보보호 표준의 개발과 정보보호 산업의 활성화 방향을 모색하는데 중요한 역할을 한다.

Ⅰ. 서 론

최근 무선 인터넷의 사용과 모바일 단말기의 보급, 클라우드 서비스의 대중화 등에 따른 새로운 정보보호 위협이 등장하고 있어서 이에 따른 위험을 감소시키기 위한 공공기관과 민간기업의 정보보호 기술에 대한 요구사항도 복잡해지고 있다. 새로운 정보보호 기술의 등장은 필연적으로 안전성과 효과성에 대한 검증과 호환성 및 상호운영성의 보장을 필요로 하며, 국내외의 다양한 표준화 조직(예: ISO/IEC, ITU, IETF, ETSI 등)에서는 정보보호 분야에 대한 전문가 활동을 통하여 이러한 필요성을 만족시킬 수 있는 표준 문서를 지속적으로 개발하고 있다.

본 논문에서는 정보기술(IT) 분야의 대표적인 국제표준화 기관인 ISO/IEC에서 최근 표준 문건으로 개발하고 있는 정보보호 표준화 작업에 대해서 살펴보고자 한다. 일반적으로 ISO/IEC는 5년을 주기로 정기 검토를 통해 국제표준의 개정 작업을 수행하고 있지만 회원국의 요구사항과 시장의 수요를 반영하여 더 짧은 주기로 개정이 이루어지거나 6개월 정도의 스터디 기간을 거쳐 신규 작업항목으로 등장하고 있다 [1].

따라서 국제 표준화 기관의 정보보호 분야의 표준화 작업 내용을 살펴봄으로서 전세계적인 정보보호 및 개인정보보호 관련 이슈를 이해하는 기초를 제공하며, 국내 정보보호 표준의 개발과 정보보호 산업의 활성화 방향을 모색하는데 기여하고자 한다.

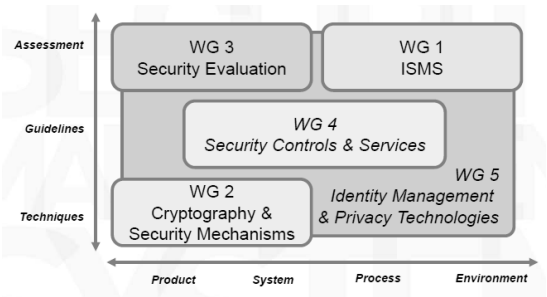
Ⅱ. ISO/IEC JTC 1/SC 27 표준화 동향

대표적인 공적(de jure) 표준화 기관인 국제표준화기구(ISO)와 국제전기위원회(IEC)는 정보보호기술 전반에 대한 국제표준을 개발하기 위하여 공동으로 표준화 절차와 규정을 제정하여 ISO/IEC JTC 1(공동기술위원회)을 중심으로 긴밀하게 협력하고 있으며, 특히 JTC 1의 소위원회(sub-committee) 중 하나인 SC 27(Information Technology, Security Techniques)은 5개 작업그룹(WG; Working Group)으로 구성되어 정보보호 관리 및 기술 표준화를 담당하고 있다 [2].

WG 1은 정보보호관리체계(ISMS)에 관련된 표준을 정의하고 있으며, WG 2은 암호기법 및 보안 메커니즘에 대한 연구 및 표준화 작업에 필요한 관련 기술의 표준을 제정하고 있다. WG 3은 IT 시스템과 구성 장치 및 제품의 보안평가와 인증을 위한 평가 기술의 표준을, WG 4는 알려진 보안 이슈의 발생을 막고 관리하기 위한 필요성, 정보보호시스템의 고장 또는 자연재해로 인한 사고나 정보보호 이슈를 포함하는 관리에 대한 표준을, WG 5는 아이디 관리와 프라이버시 기술, 프라이버시 연관 바이오인식 기술에 대한 표준을 제정하고 있다 [3].

* 고려사이버대학교 정보관리보안학과 (summer69@cyberkorea.ac.kr)

SC 27은 정보보호 제품, 시스템, 프로세스, 환경을 대상으로 기술, 지침, 평가에 이르는 활동의 표준화를 위해 노력하고 있으며, 각 작업그룹은 새로운 암호 알고리즘, 사이버 보안, 프라이버시, 아이디 관리 및 바이오 인식 등과 같이 시장의 요구에 따라 지속적으로 범위를 확장하고 있다(그림 1 참고) [4].



〔그림 1〕 SC 27 작업그룹의 활동 범위

2.1 WG 1(정보보호관리체계) 표준화 활동

WG 1의 작업 범위는 주로 국제적인 ISMS 인증에 사용되는 ISO/IEC 27000 시리즈를 개발 및 유지하는 것이며, 현재(2012년 10월 기준) 진행 중인 작업 문서를 중심으로 현황을 정리하면 표 1과 같다 [5].

ISMS 구축 및 운영에 필요한 요구사항을 명시한 ISO/IEC 27001과 정보보호 통제의 최적 실무를 제공하는 ISO/IEC 27002는 현재 국제표준안(DIS; Draft International Standard) 상태이며, 2013년도에 개정된 표준 문건으로 공표(publish)될 예정이다. ISO/IEC 27000은 ISMS에 대한 개요와 관련 표준 문건에 대한 간단한 소개 및 용어에 대한 정의를 제공하며 2015년도에 공표를 예정으로 개정 중이다.

ISMS 구현 지침을 제공하는 ISO/IEC 27003, 효과성 측정을 위한 ISO/IEC 27004, 위험 관리를 위한 ISO/IEC 27005은 2015년도 개정 문건의 공표를 목표로 작업이 진행 중이며, 기술보고서(TR; Technical Report) 형태로 공표할 ISO/IEC TR 27016은 정보보호의 경제성 측면에 따른 의사결정을 돕기 위한 지침으로 개발되고 있다.

ISMS 감사 및 인증기관에 필요한 요구사항을 명시한 ISO/IEC 27006이 작업초안(WD; Working Draft) 상태로 개정되고 있으며, 클라우드 컴퓨팅 서비스의 정보보호 통제를 위한 최적 실무를 ISO/IEC 27017로 신규 표준으로 제정하고 있다. 최근 신규 작업항목 제안(NP; New work item Proposal)으로 추가된 ISO/IEC 27009는 개인정보보호, 클라우드 컴퓨팅, 그리드 컴퓨팅 등 다양한 섹터와 서비스에서 ISO/IEC 27001 인증을 부여하기 위한 방법의 일환으로 개발을 진행하고 있다.

〔표 1〕 WG 1 작업 문서 현황

문서 번호	제 목	현재 상태	공표 시기
27000	Information security management systems - Overview and vocabulary	DIS (개정)	2015.05
27001	Information security management systems - Requirements	DIS (개정)	2013.10
27002	Code of practice for information security controls	DIS (개정)	2013.10
27003	Information security management system implementation guidance	NP (개정)	2015.10
27004	Information security management measurements	WD (개정)	2015.10
27006	Requirements for bodies providing audit and certification of information security management systems	WD (개정)	2015.05
27009	Use of ISO/IEC 27001 for sector-service specific Third-Party accredited certifications	NP (신규)	2016.04
TR 27016	Information security management - Organisational economics	PDTR (신규)	2013.11
27017	Code of practice for information security controls for cloud computing services based on ISO/IEC 27002	WD (신규)	2015.10

2.2 WG 2(암호화 및 보안 메커니즘) 표준화 활동

WG 2는 IT 시스템과 어플리케이션에 필요한 보안 기법과 메커니즘의 표준화를 담당하며, 주로 암호화 기술을 작업 범위로 다루고 있지만 기밀성, 개체 인증, 부인방지, 키 관리, 데이터 무결성(예: 메시지 인증, 해쉬 함수, 전자서명 등)에 관련된 다양한 기법과 메커니즘도 포함한다. 현재 WG 2에서 진행 중인 작업 문서를 중심으로 현황을 정리하면 표 2와 같다 [5].

해쉬 함수에 대한 일반적인 정의와 요구사항을 포함한 ISO/IEC 10118-1은 NP로 개정 작업이 시작되었으

며, 데이터 전송 및 저장에 기밀성을 제공하는 암호화의 특징과 일반적인 측면을 소개하는 표준인 ISO/IEC 18033-1는 WD 상태로 개정이 진행 중이다. 또한 ISO/IEC 18033-5는 식별자 기반의 암호화를 위한 인터페이스와 기능 및 암호문 양식의 명세를 제공하기 위한 표준으로 신규 제정 작업을 수행하고 있다.

〔표 2〕 WG 2 작업 문서 현황

문서 번호	제 목	현재 상태	공표 시기
10118-1	Hash-functions - Part 1: General	NP (개정)	2016.10
11770-3	Key management - Part 3: Mechanisms using asymmetric techniques	CD (개정)	2014.05
18014-4	Time-stamping services - Part 4: Traceability of time sources	CD (신규)	2014.05
18033-1	Encryption algorithms - Part 1: General	WD (개정)	2014.11
18033-3/ Amd.1	Encryption algorithms - Part 3: Block ciphers - Amendment 1	WD (신규)	2013.11
18033-5	Encryption algorithms - Part 5: Identity-based ciphers	WD (신규)	2014.11
18370-1	Blind digital signatures - Part 1: General	WD (신규)	2015.10
18370-2	Blind digital signatures - Part 2: Discrete logarithm based mechanisms	WD (신규)	2015.10
20008-1	Anonymous digital signature - Part 1: General	DIS (신규)	2014.05
20008-2	Anonymous digital signature - Part 1: Mechanisms using a group public key	DIS (신규)	2014.05
20009-1	Anonymous entity authentication - Part 1: General	DIS (신규)	2014.05
20009-2	Anonymous entity authentication - Part 2: Mechanisms based on signatures using a group public key	DIS (신규)	2014.05
20009-3	Anonymous entity authentication - Part 3: Mechanisms based on blind signatures	NP (신규)	2014.05
29192-4	Lightweight cryptography - Part 4: Mechanisms using asymmetric techniques	FDIS (신규)	2013.05

비대칭키 암호 기술을 기반으로 키 관리 기법을 정의하고 있는 ISO/IEC 11770-3은 위원회안(CD; Committee Draft) 상태로 개정 중이며, RFID 또는 스마트 카드와 같이 제한된 환경에서 비대칭키 기법을 사용하는 경량 암호화 메커니즘을 명세하고 있는 ISO/IEC 29192-4는 최종국제표준안(FDIS; Final DIS) 상태로 신규 제정이 진행 중이다.

ISO/IEC 18370-1과 18370-2는 전자화폐 또는 전자투표 시스템에 사용될 수 있는 블라인드 전자서명을 표준화하기 위하여 WD 상태로 신규 진행 중이며, 그룹 공개키를 이용한 익명 전자서명에 대한 신규 표준인 ISO/IEC 20008-1과 20008-2도 DIS 상태로 2014년도 공표를 예정하고 있다.

그 외에도 인증 개체의 식별자를 숨기는 익명 인증을 위한 ISO/IEC 20009-1, 20009-2, 20009-3과 타임스탬프 서비스에서 시간 출처의 추적성을 확보하기 위한 ISO/IEC 18014-4가 신규 표준으로 제정되고 있다.

2.3 WG 3(보안 평가, 시험, 명세) 표준화 활동

WG 3는 IT 시스템과 컴포넌트 및 제품에 대한 보안 명세, 평가, 시험, 인증 등의 정보보호 공학을 주로 다루며, 컴퓨터 네트워크, 분산 시스템, 관련 어플리케이션 서비스, 바이오인식 등도 포함하고 있다. 현재 WG 3에서 진행 중인 작업 문서 현황을 정리하면 표 3과 같다[5].

〔표 3〕 WG 3 작업 문서 현황

문서 번호	제 목	현재 상태	공표 시기
17825	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	WD (신규)	2014.11
24759	Test requirements for cryptographic modules	CD (개정)	2014.05
29147	Vulnerability disclosure	DIS (신규)	2013.11
TR 29193	Secure system design principles and techniques	PDTR (신규)	2013.11
TS 30104	Physical security attacks, mitigation techniques and security requirements	PDTS (신규)	2013.10
30111	Vulnerability handling processes	DIS (신규)	2013.11
TR 30127	Detailing software penetration testing under ISO/IEC 15408 and ISO/IEC 18045 vulnerability analysis	WD (신규)	2014.11

취약성에 대한 정보를 관련 조직 간에 공유하고 관리하기 위한 방법을 표준화한 ISO/IEC 29147과 제품 또는 온라인 서비스에 대해 보고된 취약성을 처리하여 해결하는 방법을 지침으로 제공하는 ISO/IEC 30111이 DIS 상태로 신규 제정되어 조만간 공표될 예정이다.

암호 모듈의 보안 요구사항을 명세한 ISO/IEC 19790의 준거성 테스트를 수행하는 시험기관에서 사용할 수 있도록 ISO/IEC 24759를 CD 상태로 개정하고 있으며, 더 높은 보안 수준에서 요구하는 비침입 공격을 경감시키기 위한 시험 기법을 표준화하기 위하여 ISO/IEC 17825로 WD 상태의 신규 작업을 진행 중이다.

보안 시스템 설계의 원칙, 최적 실무, 기법에 대한 지침을 제공하는 ISO/IEC TR 29193과 암호 모듈에 대한 물리적 보안 기법을 제공하는 ISO/IEC TS 30104는 각각 기술보고서와 기술명세(TS)의 형식을 신규 작업을 진행하고 있다. 또한 소프트웨어 취약성 평가 표준인 ISO/IEC 15408과 ISO/IEC 18045에 따른 침투 시험을 계획, 개발, 실행하기 위한 지침으로 ISO/IEC TR 30127을 신규 제정하기 위하여 WD 상태로 진행 중이다.

2.4 WG 4(보안 통제 및 서비스) 표준화 활동

WG 4는 ISO/IEC 27001에서 정의한 통제 목적과 통제의 구현을 지원하기 위한 서비스와 어플리케이션에 대한 표준 및 지침을 개발하고 있다. 네트워크 보안, 보안사고 관리, IT 재해복구 서비스, 업무연속성, 사이버 보안, 아웃소싱(공급망) 보안 등을 포함한다. 현재 WG 4에서 진행 중인 작업 문서 현황을 정리하면 표 4와 같다[5].

〔표 4〕 WG 4 작업 문서 현황

문서 번호	제 목	현재 상태	공표 시기
24762	Guidelines for information and communications technology disaster recovery services	WD (개정)	2014.11
27033-1	Network security - Part 1: Guidelines for network security	WD (개정)	2015.10
27033-4	Network security - Part 4: Securing communications between networks using security gateways	DIS (18028-3 개정)	2013.11
27033-5	Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)	DIS (18028-5 개정)	2013.11
27033-6	Network security - Part 6: Securing IP network access using wireless	WD (신규)	2015.11
27034-2	Application security - Part 2: Organization normative framework	WD (신규)	2015.11
27034-3	Application security - Part 3: Application security management process	NP (신규)	2017.11
27034-4	Application security - Part 4: Application security validation	NP (신규)	2017.11
27034-5	Application security - Part 5: Protocols and application security controls data structure	WD (신규)	2016.11
27034-6	Application security - Part 6: Security guidance for specific applications controls data structure	WD (신규)	2016.11
27035-1	Information security incident management - Part 1: Principles of incident management	WD (27035 개정)	2014.11
27035-2	Information security incident management - Part 2: Guidelines to plan and prepare for incident response	WD (27035 개정)	2014.11
27035-3	Information security incident management - Part 3: Guidelines for incident response operations	WD (27035 개정)	2014.11
27036-1	Information security for supplier relationships - Part 1: Overview and concepts	DIS (신규)	2013.10
27036-2	Information security for supplier relationships - Part 2: Requirements	DIS (신규)	2013.10
27036-3	Information security for supplier relationships - Part 3: Guidelines for ICT supply chain security	DIS (신규)	2013.10
27036-4	Information security for supplier relationships - Part 4: Guidelines for security of cloud services	WD (신규)	2015.10

문서 번호	제 목	현재 상태	공표 시기
27038	Specification for digital redaction	CD (신규)	2013.11
27039	Selection, deployment and operations of intrusion detection and prevention systems (IDPS)	CD (18043 개정)	2014.11
27040	Storage security	CD (신규)	2015.04
27041	Guidance on assuring suitability and adequacy of investigation methods	CD (신규)	2014.10
27042	Guidelines for analysis and interpretation of digital evidence	CD (신규)	2014.10
27043	Incident investigation principles and processes	CD (신규)	2014.10
27044	Security information and event management (SIEM)	WD (신규)	2015.10

현재 IT 네트워크의 관리, 운영, 사용에 대한 보안을 지침으로 제공하기 위해 제정되어 있는 ISO/IEC 18028을 ISO/IEC 27033으로 대체하기 위한 작업이 진행 중이다. ISO/IEC 27033-4와 27033-5는 각각 보안 게이트웨이와 가상사설망(VPN)을 사용한 안전한 통신 방법을 DIS 상태로 표준화하고 있어서 조만간 공표가 예정되어 있다. 또한 무선 네트워크에 대한 위협, 보안 요구사항, 보안 통제, 설계 기법을 내용으로 하는 ISO/IEC 27033-5를 WD 상태로 제정 중이다.

업무 어플리케이션에 대한 적절한 보안 수준을 보장하도록 관리자, 개발자, 감사자, 최종사용자에게 지침을 제공하기 위한 표준으로 ISO/IEC 27036의 각 부문(part 2~5)을 WD 또는 NP 상태로 신규 제정하고 있다.

기존에 보안사고 관리를 위한 지침으로 공표된 ISO/IEC 27035를 사고관리 원칙(27035-1), 계획 및 준비 지침(27035-2), 운영 지침(27035-3)의 3 개의 문서로 분리하여 WD 상태로 개정을 진행하고 있다.

최근 이슈가 되고 있는 IT 아웃소싱이나 클라우드 서비스 등에 대한 정보보호를 공급망 관리 측면에서 다루기 위하여 ISO/IEC 27036-1(개요 및 개념), 27036-2(요구사항), 27036-3(ICT 공급망 보안), 27036-4(클라우드 보안)으로 구분하여 DIS 상태(27036-4는 WD 상태)로 신규 제정 중이다.

침입탐지/침입방지시스템(IDS/IPS)의 선택, 배치, 운영을 위한 지침으로 ISO/IEC 27039(기존 ISO/IEC 18043 대체)이 CD 상태로 개정 중이며, 보안정보 및 사건관리(SIEM) 시스템의 선택, 배치, 운영을 위한 지침으로 ISO/IEC 27044가 WD 상태로 신규 개발되고 있다.

그 밖에도 디지털 포렌식을 지원하기 위한 표준으로 ISO/IEC 27041(조사방법), ISO/IEC 27042(증거수집), ISO/IEC 27043(조사원칙 및 절차)을 CD 상태로 신규 제정 중이며, 전자문서 편집(redaction) 후 복구가 불가능하도록 보장하기 위한 ISO/IEC 27038과 저장 장치 및 서비스에 대한 보안 위험을 감소시키도록 보장하기 위한 ISO/IEC 27040이 CD 상태로 신규 제정이 진행되고 있다.

2.5 WG 5(ID관리 및 프라이버시 기술) 표준화 활동

WG 5의 활동 범위는 ID 관리와 바이오인식 및 개인정보보호를 주로 다루고 있다. ID 관리 프레임워크, 프라이버시 프레임워크, 접근관리 프레임워크, 프라이버시 참조 아키텍처 등 다수의 프레임워크와 아키텍처를 근간으로 바이오인식 정보의 보호 및 인증 지침으로 작업을 확대하고 있다. 현재 WG 5에서 진행 중인 작업 문서 현황을 정리하면 표 5와 같다 [5].

〔표 5〕 WG 5 작업 문서 현황

문서 번호	제 목	현재 상태	공표 시기
17922	Telebiometric authentication framework using biometric hardware security module	WD (신규)	2014.12
24760-2	A framework for identity management - Part 2: Reference architecture and requirements	WD (신규)	2014.05
24760-3	A framework for identity management - Part 3: Practice	WD (신규)	2015.05
27018	Code of practice for data protection controls for public cloud computing services	WD (신규)	2014.12
29003	Identity proofing	WD (신규)	2016.10
29101	Privacy reference architecture	DIS (신규)	2013.10
29134	Privacy impact assessment - Methodology	WD (신규)	2015.10
29146	A framework for access management	WD (신규)	2015.05
29151	Code of practice for the protection of personally identifiable information	NP (신규)	2016.04
29190	Privacy capability assessment model	WD (신규)	2015.11

ID 정보의 생명주기에 따른 관리 시스템의 요구사항에 대한 명세 및 구현 지침을 제공하고 있는 ISO/IEC 24760-2와 조직과 개인의 ID 관리 실무를 제공하는 ISO/IEC 24760-3이 WD 상태로 신규 제정되고 있다. 개체의 식별 설정과 확인에 필요한 최적 실무와 지침을 제공하는 ISO/IEC 29003을 신규로 제정하여 WD 상태로 진행 중이다.

ISO/IEC 29101로 신규 제정 중인 프라이버시 참조 아키텍처가 DIS 상태로 조만간 공표될 예정이며, 국내에서 에디터 활동을 주도하고 있는 개인정보 영향평가(PIA)는 ISO/IEC 29134로 WD 상태의 신규 표준으로 제정 중이다. 또한 프라이버시 관리 성숙도를 평가하기 위한 상위 수준의 지침으로 ISO/IEC 29190을 WD 상태로 작업을 진행하고 있다.

일반적인 범주의 개인정보(또는 개인식별정보)를 보호하기 위한 통제의 최적 실무와 클라우드 환경에 특화된 프라이버시를 보장하기 위한 데이터 보호 통제의 최적 실무를 각각 ISO/IEC 29151과 ISO/IEC 27018에서 WD 상태로 신규 제정이 진행 중이다.

Ⅲ. 결론

본 논문에서는 ISO/IEC JTC 1/SC 27의 5 개 작업그룹에서 진행 중인 표준 문서에 대한 상태와 공표 예정 시기를 중심으로 정리하여 최신의 국제 정보보호 표준화 동향을 살펴보는데 도움을 주고자 하였다.

국내의 보안 전문가를 대상으로 조사한 2013년도 정보보호 10대 이슈를 살펴보면, 빅데이터 보안, 모바일 앱 보안, 클라우드 컴퓨팅 보안, 지능형지속위험 공격, 개인정보보호법 확산 등을 포함하고 있다 [6]. SC 27의 WG 1에서 개발 중인 클라우드 컴퓨팅 서비스의 보안 통제, WG 2의 경량 암호화 메커니즘, WG 3의 보안시스템 설계 원칙 및 기법, WG 4의 무선 네트워크 접근 보안, WG 5의 개인정보 영향평가 등은 이러한 정보보호 및 개인정보보호의 최신 이슈를 반영하고 있으며, 국내 정보보호 이슈가 아울러 전세계적인 정보보호 추세와 일치하고 있음을 확인할 수 있다.

아울러 ITU-T와 IETF 등의 국제표준 기관의 정보보호 표준 기술 동향을 참고하면 [7] 국내 표준의 개발에 필요한 로드맵의 작성과 검증에 도움이 될 것으로 확신한다.

참고문헌

[1] “ISO, IEC, JTC 1 국제의장, 간사 및 컨비너 업무 매뉴얼, 국제표준화 쉽게 따라잡기”, *한국표준협회*, p.56, 2009.

[2] 김정덕, “정보보호관리 국제표준화 동향”, *정보보호학회지*, 21(2), pp.19-22, 2011.

[3] 신용녀, 김학일, 전명근, “개인정보보호 참조 아키텍처와 국제표준화 동향”, *정보보호학회지*, 21(5), pp.12-20, 2011.

[4] E. Humphreys 등, “SC27 Platinum Book”, *ISO/IEC SC27*, p.16, 2010.

[5] K. Passia, “SC27 N12057 Catalog of SC 27 Projects and Standards”, *ISO/IEC SC27*, http://www.jtc1sc27.din.de/sbe/SD7, 2013.

[6] “2013년 인터넷 및 정보보호 10대 이슈 전망”, *한국인터넷진흥원*, p.22, 2012.

[7] 오흥룡, 염흥열, “정보보호 표준 기술 동향 및 로드맵”, *한국정보보호학회 동계정보보호학술대회 논문집*, 13(2), pp.340-347, 2003.

〈著者紹介〉

박 대 하 (Park, Dae-Ha)
종신회원

1992년 2월 : 고려대학교 컴퓨터학과 학사
1994년 2월 : 고려대학교 컴퓨터학과 석사
2004년 8월: 고려대학교 컴퓨터학과 박사
<관심분야> 정보보호관리체계, 개인정보보호, 소셜 네트워크 보안, 클라우드 컴퓨팅 보안, 데이터베이스 보안, PKI, 신뢰 모델 등