http://dx.doi.org/10.14400/JDC.2015.13.2.115

클라우드 개인정보보호를 위한 SLA 지표 개발

김정덕*, 박대하**, 염흥열***
중앙대학교 산업보안학과 교수*, 고려사이버대학교 정보관리보안학과 교수**, 순천향대학교 정보보호학과 교수***

A Study on development of privacy indicators in the context of cloud service level agreement

Jungduk Kim*, Dae-Ha Park, Heung-Youl Youm*****
Dept. of Industrial Security, The College of Business & Economics of Chung-Ang Univ.*
Dept. of Information Management & Security, The Cyber Univ. of Korea**
Dept. of Information Security, The College of Engineering of Sunchunhyang Univ***

요 약 디지털융합 환경의 기반 기술인 클라우드 컴퓨팅이 확산되면서 개인정보보호가 중요한 이슈로 대두되고 있다. 국내 개인정보보호법에서도 개인정보처리자가 클라우드 컴퓨팅을 통해 개인정보를 처리하는 경우, 계약서 또는 서비스 수준 협약(SLA, Service Level Agreement) 작성을 명시하고 있으나 일반적인 클라우드 SLA에서는 주로 가용성 측면의 지표가 포함되어있으며 개인정보보호에 대한 지표는 찾아보기 어렵다. 본 논문에서는 클라우드 환경에서의 개인정보보호 대책 분석 및 SMART 모델 활용을 통해 SLA에 포함할 수 있는 총 7개의 개인정보보호 지표와 13개의 척도를 개발하였다. 도출 된 지표는 전문가 그룹을 대상으로 포커스 그룹 인터뷰를 실시하여 중요도 및 실현 가능성을 평가하였다. 본 논문은 클라우드 환경에서의 개인정보보호 대책 확립과 향후, 개인정보보호 수준 측정을 위한 자료로 활용될 것으로 기대된다.

주제어 : 클라우드 서비스, 개인정보보호, 서비스 수준 협약, 개인정보보호 수준 협약, 개인정보보호 지표

Abstract As the cloud services, the underlying technology of the digital convergence environment, have been widely adopted in the business, personal information protection has been recognized as one of the major issues to resolve. When cloud services are used to process the personal information, the personal information protection law speculates the establishment of a contract or service level agreement(SLA).

This research presents 7 privacy indicators and 13 metrics which can be included in cloud SLA, based on the analysis of related regulation and standards and the SMART(Specific, Measurable, Action-oriented, Relevant and Timely) model. The proposed indicators are examined using the Focus Group Interview method in terms of materiality and feasibility. The results show that all the proposed indicators are meaningful and useful.

Key Words : Cloud service, Privacy, SLA(Service Level Agreement), PLA(Privacy Level Agreement), Privacy indicator

* 본 논문은 2014년 순천향대학교 산학협력단의 위탁 연구과제에 의하여 지원되었음
Received 6 December 2015, Revised 15 January 2015
Accepted 20 February 2015
Corresponding Author: Heung-Youl Youm
(Dept. Information Security, The College of Engineering of Sunchunhyang Univ.)
Email: hyyoum@sch.ac.kr
ISSN: 1738-1916

1. 서론

디지털융합 환경을 주도하는 주요 기술은 사물인터넷, 클라우드, 빅데이터, 모바일(ICBM: IoT, Cloud, Big data, Mobile) 기술이라고 한다. 이 중 클라우드는 인프라 역할을 하는 기반 기술로서 그 중요성을 강조할 필요가 있다. 클라우드 환경이 확산됨에 따라 빅데이터 수집·분석이 가능해졌고, 사물인터넷과 모바일 환경 역시 클라우드 기술을 이용한 데이터 저장 및 처리가 기반이 될 것이다. 이와 같이 디지털융합 환경의 기반 역할을 수행하는 클라우드 서비스의 확산과 함께 개인정보보호가 시급히 해결해야 할 이슈로 부각되고 있으나 현재 클라우드 환경에서의 개인정보보호는 미흡한 상태이다[9,12].

실제 아마존, 구글 등 주요 클라우드 서비스 제공자의 개인정보보호 관련 계약/약관을 조사한 결과, 개인정보 파기절차나 개인정보 관리책임자가 게시되어있지 않는 등 개인정보보호가 미흡한 상태로 분석되었다[18]. 일반적으로 개인정보보호는 정보보호와 달리 고객이라는 권리 주체를 추가적으로 상대해야하기 때문에 개인정보 유출 시 손해배상 및 기업의 이미지 실추가 발생할 수 있으며 나아가 기업 경영에 타격을 받을 수 있다[13]. 따라서 클라우드 서비스 제공자는 이러한 손실을 방지하기 위해 개인정보보호의 수준을 보장하는 것이 필요하며, 이를 명시하여 개인정보보호에 대한 신뢰를 조성해야한다.

국내 “개인정보의 안전성 확보조치 기준”[20]에서는 개인정보처리자가 클라우드 컴퓨팅을 통해 개인정보를 처리하는 경우, 계약서 또는 SLA(Service Level Agreement)를 작성할 것을 명시하고 있다. SLA는 서비스 제공자와 이용자 간 법적 효력이 존재하는 계약서로, SLA 작성을 통해 대상 서비스의 책임소재를 명시하고 제공하는 서비스에 대한 신뢰감을 형성할 수 있다[4]. 그러나 현재 일반적인 클라우드 SLA에서는 주로 가용성 측면에서 주요 지표를 포함하고 있으며, 개인정보보호에 대한 지표는 찾아보기 어렵다[19].

따라서 본 논문에서는 개인정보보호 위험 및 대책에 대한 조사·분석을 통해 개인정보보호 주요 지표를 도출하고, Harbour[6]가 제시한 SMART 모델을 적용하여 실질적으로 SLA에 포함할 수 있는 척도(metric)를 선정하였다. 제시된 SLA 지표는 전문가 그룹을 대상으로 포커스 그룹 인터뷰를 실시하여 지표의 중요성과 현실 적용 가능성을 검토하였다.

2. 관련 연구

본 장에서는 클라우드 SLA에서의 개인정보보호 현황 파악과 클라우드 개인정보보호 대책의 비교·분석을 통해 클라우드 SLA에 포함될 수 있는 개인정보보호 대책을 조사하였다.

2.1 클라우드 SLA

클라우드 보안 전문기관인 CSA[10](Cloud Security Alliance)는 2013년에 클라우드 개인정보보호 SLA지침을 발표하였다. SLA에 포함될 내용으로 개인정보 유형, 처리방식, 전송, 보호대책, 모니터링, 개인정보 보유 및 폐기, 책임추적성, 분쟁해결, 손해배상 등으로 구성되어 있다. 클라우드 환경에서의 개인정보보호대책을 SLA 형태로서 도출하였다는 것에 의의가 있으나 대부분의 지표를 측정하기 위한 객관적 척도가 제공되지 않아 실제 적용하기에는 미흡하다는 한계를 가지고 있다.

방송통신위원회[19]는 클라우드 컴퓨팅 확산을 위해 클라우드 SLA 가이드를 제시하였으며 클라우드 환경에서 고려해야할 SLA 지표를 제시하고 있다. 하지만 SLA 지표에 개인정보보호에 대한 내용이 포함되어있지 않아 개인정보보호 수준을 협의할 수 없다는 한계가 있다.

2.2 클라우드 개인정보보호 대책

클라우드 개인정보보호 SLA 지표를 도출하기 위해서는 클라우드 환경에서의 개인정보보호 대책을 기반으로 해야 한다. 따라서 클라우드 개인정보보호에 대한 대표적 참고자료인 국제표준 ISO/IEC 27018[11]과 국내 방송통신표준인 KCS.KO-10.2001[21]을 비교·분석하였다.

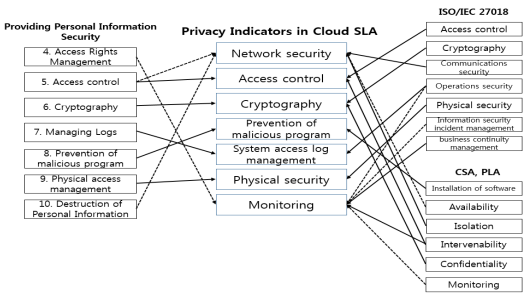
ISO/IEC 27018은 클라우드 환경에서의 개인정보보호 대책에 대한 국제표준으로 ISO/IEC 27002를 기반으로 14개의 통제 영역을 제시하며, 추가적으로 클라우드 환경을 고려한 개인정보보호 통제 항목을 제시하고 있다,

국내 방송통신표준인 KCS.KO-10.2001은 클라우드 환경에서의 개인정보보호 지침으로 개인정보보호대책을 개인정보 관리와 개인정보 생명주기관리 영역으로 구분하여 제시하고 있다.

ISO/IEC 27018, KCS.KO-10.2001의 비교·분석 결과, 클라우드 개인정보보호 대책을 특정 클라우드 서비스와 관계없이 공통적으로 적용될 수 있는 개인정보보호 프로그램 영역과 클라우드 서비스 개별적으로 적용할 필요가 있는 영역으로 구분할 수 있다. 개인정보보호 프로그램 영역은 개인정보를 체계적·지속적으로 관리하기 위한 영역으로 개인정보보호 정책, 조직 구성, 인적 자원 보안, 자산 관리, 시스템 개발과 도입 및 유지보수, 공급자 관계 관리, 컴플라이언스 관리가 개인정보보호 프로그램 영역에 포함된다. 개인정보보호 프로그램 영역은 모든 클라우드 서비스에 공통적으로 적용되기 때문에 클라우드 서비스 제공자의 개인정보보호정책 또는 약관에 포함시키는 것이 일반적이다. 개인정보보호 서비스영역은 개별 서비스 성향이 강한 개인정보보호 대책들로 구성되어있으며 서비스 계약 당사자 간 선택적으로 제공이 가능하며 서비스의 수준 설정이 가능한 항목들이 포함되어있다. 접근통제 암호화, 물리보안, 운영보안, 통신보안, 사고 관리, 비즈니스 연속성 관리가 개인정보보호 서비스영역에 포함된다.

3. 클라우드 개인정보보호 SLA 지표 개발

SLA에서 서비스 수준을 협의할 수 있는 지표와 척도를 개발하는 것은 핵심적인 활동이다. SLA 지표는 계약 당사자의 요구사항과 이해관계가 반영되어야한다 [5, 15, 16]. 본 장에서는 클라우드 개인정보보호 대책을 비교·분석하여 계약 당사자 간 요구사항과 이해관계를 반영할 수 있는 클라우드 개인정보보호 SLA 지표를 도출하였으며 Harbour의 SMART 모델을 적용하여 세부적인 SLA 척도를 개발하였다.



[Fig. 1] Development of Privacy indicators in Cloud SLA

3.1 클라우드 개인정보보호 SLA 지표 도출

개인정보보호법에서 요구하는 법적 준수사항과 2장에서 분석한 클라우드 개인정보보호 대책을 비교·분석하여 [Fig. 1]과 같이 총 7개의 클라우드 개인정보보호 SLA 지표를 도출하였다. 국내 현실에 적용가능하고 실질적인 지표를 개발하기 위해 개인정보보호법을 기반으로 한 "개인정보의 안전성 확보조치"[20]에서 요구하는 필수 개인정보보호 항목을 기반으로 개인정보보호 관련 국제표준(ISO 27018)과 CSA의 PLA(Privacy Level Agreement)[10]에서 제시하는 개인정보보호 대책을 중심으로 구성하였다. 클라우드 개인정보보호 대책은 개인정보보호 정책 등 개인정보보호 프로그램 영역은 제외하고 클라우드 서비스별로 개인정보보호 수준을 협의할 수 있는 대책 영역만을 대상으로 지표를 도출했다.

[Fig. 1]에서, 클라우드 개인정보보호 SLA 지표에 직접적 내용이 포함되어 있을 경우 실선으로 표시하였고 부분내용이 포함되어 있으면 점선으로 구분하였다.

3.2 클라우드 개인정보보호 SLA 척도 개발

3.1절에서 도출된 총 7개의 지표를 측정하기 위한 실질적인 척도를 도출하기 위해 Harbour의 SMART 모델을 활용하였으며 <Table 1>과 같이 SLA 척도를 개발하였다. SMART 모델은 구체성(Specific), 측정가능성(Measurable), 실행가능성(Action-oriented), 연관성(Relevant), 적시성(Timely) 등 척도 개발에 적용될 수 있는 대표적 모델이다[7,14,17]

〈Table 1〉 Privacy metric in Cloud SLA

Privacy indicators	Privacy metrics
Network security	Network security solutions
	Type of network separation
Access control	Access right management
	Account management
Cryptography	Encryption system for transfer
	Encryption system for storage
Prevention of malicious program	Anti-virus SW installation & update
System access log management	Log storage method
	Log retention period
Physical security	Data-center location and facilities
	Physical access control system
Monitoring	Monitoring scope
	Monitoring review period

‘네트워크 보호대책’ 지표는 개인정보처리시스템에 대한 비인가 접근 및 침해 사고 방지를 위한 개인정보보호 대책으로 ‘네트워크 보안시스템 유형’ 및 ‘망분리 유형’이 네트워크 보호대책에 대한 척도로 제시될 수 있다. 네트워크 보안시스템은 방화벽, 침입탐지시스템(IDS), DDOS (distributed denial of service) 방지시스템 등과 같은 보안시스템의 구축 여부가 SLA 체결 시 협의될 수 있다. 망분리 유형은 비용과 보안 요구사항을 고려하여 물리적 또는 논리적 망분리 방법 중 선택될 수 있을 것이다.

‘접근통제’ 지표는 개인정보처리시스템에 접근할 수 있는 권한 및 절차에 대한 개인정보보호대책으로 ‘개인정보처리시스템에 대한 접근권한 관리’와 ‘계정 관리’가 구체적인 척도로 제시될 수 있다. SLA 체결 시, 개인정보처리시스템에 대한 접근권한 관리에서는 계정에 대한 권한 변경 및 말소, 비밀번호 설정, 주기 및 잠금 정책 등에 대한 내용이 계약 당사자 간 협의가 이루어질 수 있다[1]. 계정 관리 방법에서는 비밀번호 보안 강도와 일정 수준 이하의 비밀번호는 설정되지 못하도록 하는 내용 등이 협의될 수 있다[3].

‘암호화’ 지표는 개인정보 저장 또는 송수신 시 기밀성을 유지하기 위한 개인정보보호대책으로, ‘개인정보 저장 및 전송 시 암호화방법’이 구체적인 척도로 제시될 수 있다. 개인정보 저장 시 암호화방법의 수준을 평가하기 위해 암호화 알고리즘, 키 길이 및 키 보관 방법 등이 객관적인 기준으로 제시될 수 있다. 개인정보 전송 시 암호화 방법은 SSL(Secure Socket Layer) 인증 설치 여부 등을 통해 SLA 체결 시 당사자 간 협의 가능하다[2].

‘악성 프로그램 방지’ 지표는 악성 프로그램의 유입 및 치료를 위한 개인정보보호 대책으로 SLA 체결 시 당사자 간 안티바이러스 S/W 선택 및 업데이트 주기 등을 협의할 수 있다.

‘개인정보처리시스템 접근기록 관리’ 지표는 접속기록의 무결성을 유지하기 위한 개인정보보호대책으로 ‘개인정보 접속기록 저장 방법’과 ‘개인정보 접속기록 저장 기간’이 구체적인 척도로 제시될 수 있다. 개인정보 접속기록 저장방법은 SLA 체결 시 접속·종료 시간, 접근 계정, 접속 후 수행 업무 등 세부 내용 정의, 접근 기록 보고 주기 설정, 암호화 등 접속기록 보관 방법 등이 협의되어야 하며 개인정보 접속기록 저장 기간은 또한 계약 당사자 간 협의 하에 설정되어야한다[3].

‘물리적 보호대책’은 개인정보가 보관/처리되는 클라우드 컴퓨팅 센터가 안전하게 보호되고 있음을 보장하기 위한 개인정보보호 대책으로 ‘데이터 저장 위치 및 시설 보안’과 ‘물리적 접근통제시스템 운영’이 구체적인 척도로 제시될 수 있다. 데이터 저장 위치 및 시설 보안에서는 데이터 저장 위치에 대한 내용을 클라우드 서비스 제공자가 고시해야하며 소방 시설 등 안전 관리 시설 여부를 SLA 체결 시 확인해야 한다. 또한 물리적 통제 장치의 설치 여부 및 방법 등이 고려되어야 한다.

‘모니터링’ 지표는 개인정보 처리이력의 무결성을 유지하기 위한 개인정보보호 대책으로 ‘모니터링 범위 설정’과 ‘모니터링 결과 보고 기간’이 구체적인 척도로 제시될 수 있다. SLA 체결 시 모니터링 범위 설정에서는 접속이력 개인정보 다운로드 이력 등 처리이력에 대한 관리범위가 협의되어야한다. 또한 SLA 체결 시 상호간 개인정보 처리이력 결과보고 주기를 설정할 수 있다[1].

4. 실증분석

본 논문은 클라우드 개인정보보호 대책의 비교·분석을 통해 총 7개의 지표와 13개의 세부적인 척도를 도출하였고 이에 대한 타당성을 검증하기 위해 포커스 그룹 인터뷰(FGI) 방법으로 지표의 중요성과 실현가능성을 검토하였다. 포커스 그룹은 총 10명의 학계 및 기업의 개인정보보호 분야의 전문가로 구성하였으며 전문가들을 대상으로 심층 인터뷰를 수행하였다. 심층 인터뷰는 개인정보보호 SLA 지표의 중요성과 실현가능성을 측정하기 위해 리커드 5점 척도를 이용하여 진행하였으며 인터뷰 종료 후 약 1시간에 걸쳐 참여자간의 의견 교류 및 토론을 진행하여 지표의 타당성을 분석하였다.

포커스 그룹 인터뷰 결과, 클라우드 개인정보보호 척도의 중요성은 ‘물리적 접근통제시스템 운영’ 척도를 제외하고 모두 3.5점 이상으로 높게 분석되었으며, 실현가능성은 3.5점 이하의 척도가 2개로, 일부 척도의 실현가능성에 대한 재검토가 필요하다는 의견이 제시되었다.

‘물리적 접근통제시스템 운영’ 의 평균 중요성 점수는 3.2점으로, 토론 결과 일반적인 정보보호대책과 중복되기 때문에 클라우드 SLA척도에 포함될 만큼 중요하지 않다는 의견이 제시되었다.

실현가능성이 낮게 평가된 척도는 '접근권한 관리'와 '모니터링 범위 설정' 척도로 분석되었다.

'접근권한 관리'에서 인사변경 시 접근권한의 변경·삭제가 즉각적으로 이루어져야하지만 서비스가 위탁되는 클라우드 환경 상 인사관리시스템 등 다른 정보시스템과 연계가 어렵기 때문에 실무적으로 한계가 존재한다는 의견이 제시되었다.

〈Table 2〉 Review of Privacy metrics in Cloud SLA using FGI

Privacy metrics in Cloud SLA	materiality	feasibility
Network security solutions	4.3	4.1
Type of network separation	4.6	4.3
Access right management	3.8	2.8
Account management	3.7	3.9
Encryption system for transfer	4.8	4.7
Encryption system for storage	4.8	4.5
Anti-virus SW installation & update	4	4.7
Log storage method	3.8	3.6
Log retention period	3.7	4
Data-center location and facilities	4.7	3.8
Physical access control system	3.2	3.8
Monitoring scope	3.8	3.2
Monitoring review period	3.6	4.2

'모니터링 범위 설정' 척도는 모니터링에 대한 범위가 넓기 때문에 이를 위한 협의과정이 어려울 수 있으며, 모니터링 방법 또한 협의가 어렵다는 의견이 제시되었다.

'암호화' 및 '네트워크 보호대책' 지표는 클라우드 환경에서 가장 중요하게 인식되는 클라우드 개인정보보호 대책으로 평가되었다. 클라우드 환경은 인터넷에서 접속할 수 있고, 특히 무선을 이용한 접속의 경우 보안에 취약하기 때문에 법에서 요구하는 수준 이상의 암호화 정책 및 방법을 수립하는 것이 중요하다고 평가되었다. 또한 '네트워크 보호대책' 지표는 클라우드 환경임을 고려하여 분산 환경 및 접근 통제 우회에 따른 해결책이 필요하며 이를 계약 시 명시하는 것이 중요하다고 평가되었다.

5. 결론 및 향후 연구

본 논문은 클라우드 SLA 체결 시 계약 당사자 간 협의가 가능한 클라우드 개인정보보호 SLA 지표를 도출하였다. 클라우드 개인정보보호 SLA 지표는 암호화, 네트워크 보호대책, 모니터링, 물리적 보호대책, 접근통제, 접속 기록 보관 및 위변조 방지 순서로 중요하다고 분석되었다. 특히 암호화, 네트워크 보호대책 같은 경우, 클라우드 환경임을 고려하여 법에서 요구하는 사항 이상으로 강조되어야 한다고 분석되었다.

본 연구의 한계점은 다음과 같다. 첫째, 본 연구는 학계 및 관련 기관의 전문가를 대상으로 조사하였으나 인원이 10명으로 한정되어 있어 연구결과를 일반화하는데 어려움이 있다. 향후 더 많은 표본 집단을 통한 연구 진행이 필요하다. 둘째, 본 연구 결과는 전문가 인터뷰 방법을 사용하여 전문가 경험에 의존한 가상 검토라는 한계가 있다. 제시된 지표와 척도의 유효성을 확보하기 위해서는 실제 SLA에 적용해 볼 필요가 있다. 따라서 연구결과의 시범적용을 통한 유효성 검증이 필요하다.

ACKNOWLEDGMENTS

This research was supported by Industry-Academic Cooperation Foundation of Sunchunhyang Univ. in 2014

REFERENCES

[1] Deyan Chen and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", Vol.1, No.1, pp.647-651, 2012

[2] Zhifeng Xiao and Yang Xiao, "Security and Privacy in Cloud Computing", Vol. 15, No. 2, pp.843-860, 2013

[3] Ian Goldberg, David Wagner and Eric Brewer, "Privacy-enhancing technologies for the Internet", Vol., No., pp., IEEE, 1997

[4] Andrew Hiles, "The Complete Guide to IT Service Level Agreements: Aligning IT Service to Business Needs", Rothstein Associates Inc, 2008

[5] I. S. Hayes, "Metrics for IT Outsourcing Service Level Agreement,", Vol., No., pp., Clarity Consulting INC, White Paper, 2004

[6] Harbour, Jerry L., "The Basis of Performance

Measurement", Quality Resource, 1997
[7] Kaseye, "SMART SLA", 2012
[8] ITU-T, "Privacy in Cloud Computing", 2012
[9] KPMG, "The cloud takes shape", 2013
[10] CSA "Privacy Level Agreement Outline" 2013
[11] ISO/IEC 27018, "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors" 2014
[12] D H Park and T S Baek, "Recent Trends and Issues on personal information protection", KIISC REVIE, Vol. 21, No.5 pp.37-44, aug 2011
[13] J D Kim and S H Hwang, "A Study on Critical Success Factors for Implementing Governance of Personal Information Protection", KIISC REVIE, Vol.21, No.5, pp.197-203, aug 2011
[14] H J Suh, M G Choi and S Y Son, "Establishing IT Outsorcing Performance Measurement Framework through the IT BSC", The Korea Society of Information Technology Services, Vol., No.27, pp.301-308, 2003
[15] K C Nam and J H KIm, "A Study of SLA's Maturity Level on Performance", Journal of Information Technology Applications & Management, Vol.14, No.1, pp.1-20, mar 2007
[16] C H Park, "Selection Methodology for SLA Evaluation Factors with End-user Perspective", Korea Information Processing Society, 2007
[17] H J Suh and M L Choi, "Establishing SLA Metrics Selection Framework for Maximizing Operation Efficiency and Satisfaction of IT Outsourcing, Establishing SLA Metrics Selection Framework, Vol.3, No.2, pp.101-115, 2004
[18] KISA, "The study on Providing Personal Information Security",2014
[19] Korea Communication Commission, "SLA guide in Cloud computing", 2011
[20] Ministry of Government Administration and Home Affairs, "Providing Personal Information Security", 2014
[21] TTA KCS.KO-10.2001, "Personal Information Protection Guidelines of Cloud Service Providers", 2014

김 정 덕(Kim, Jung duk)

- 1979년 2월 : 연세대학교 정치외교학과(학사)
- 1981년 8월 : 연세대학교 경제학과 대학원(석사)
- 1986년 8월 : Univ. of S. Carolina, MBA
- 1990년 12월 : Texas A&M Unv., Ph. D. in MIS
- 1995년 3월 - 현재 : 중앙대학교 산업보안학과 교수
- 관심분야 : 정보보호 거버넌스, 정보보호 관리, IT 감사
- E-Mail : jdkimsac@cau.ac.kr

박 대 하(Park, Dae Ha)

- 1992년 2월 : 고려대학교 컴퓨터학과 (학사)
- 1994년 2월 : 고려대학교 컴퓨터학과 (석사)
- 2004년 8월 : 고려대학교 컴퓨터학과 (박사)
- 2004년 3월 ~ 현재 : 고려사이버대학교 정보관리보안학과 교수
- 관심분야 : 정보보호관리체계, 개인정보보호, 소셜 네트워크 보안, 클라우드 컴퓨팅 보안, 데이터베이스 보안, PKI emd
- E-Mail : summer69@cuk.edu

염 흥 열(Youm, Heung Youl)

- 1981년 2월 : 한양대학교 전자공학과(학사)
- 1983년 9월 : 한양대학교 전자공학과 (석사)
- 1990년 2월 : 한양대학교 전자공학과(박사)
- 1990년 9월 ~ 현재 : 순천향대학교 정보보호학과 교수
- 관심분야 : 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜
- E-Mail : hyyoum@sch.ac.kr