

---

# MobiSec 2025 워크숍 참석을 위한 일본 해외출장 결과 보고

---

2026. 1.

## I. 출장 개요

### □ 개요

- (출장목적) 「양자보안 기반 5G특화망 기기 식별 기술 및 시험검증 기술개발」 사업 연구 성과 점검 및 실증 업무 논의와 보안 분야 최신 기술(양자 컴퓨팅, AI 등) 동향 및 국내외 연구 성과 조사
- (출 장 자) 디지털융합본부 이음5G사업팀 손세일, 박연규
- (출 장 지) 일본 삿포로
- (출장기간) 2025년 12월 15일(월) ~ 12월 19일(금), 4박 5일

### □ 주요일정

#### < 일자별 업무 일정 >

일 자	출발지	도착지	업무수행내용
12.15.(월)	인천 (13:10)	삿포로 (16:00)	○ 나주 → 인천국제공항 → 삿포로 도착
12.16.(화)	삿포로		○ <b>MobiSec 2025 참석</b> - eqSIM 도입에 따른 5G특화망 성능 영향 요소 식별을 위해 AI 기반 보안(세션1B), 네트워크 위협 감지(세션2C), 양자보안(세션3A) 세션 등 참석
12.17.(수)			○ <b>MobiSec 2025 참석</b> - 5G 특화망 보안 요구사항 조사를 위한 6G 및 차세대 네트워크 보안(세션4A, 5A) 세션 등 참석
			○ 「TTA eqSIM Project Workshop」 참석 및 양자보안 관련 공동 연구 아이템 발굴 - 특화망용 eqSIM 기반 기기 식별, 키 관리 기술 및 시험검증 개발을 위한 모바일 보안 관련 국제 표준화 개발 논의 - 특화망용 eqSIM 도입 및 실증을 통한 개발 기술 검증을 위해 국내외(한국, 일본, 중국 등) 특화망 관련 산학연 간 협력 연구사업 발굴
12.18.(목)			○ <b>MobiSec 2025 참석</b> - 5G 특화망용 eqSIM 검증환경 구축 방안 마련을 위한 적응형 지능 및 시스템 보안(세션7B, 8B) 세션 등 참석
12.19.(금)	삿포로 (17:30)	인천 (20:55)	○ 삿포로 → 인천국제공항 → 나주 도착

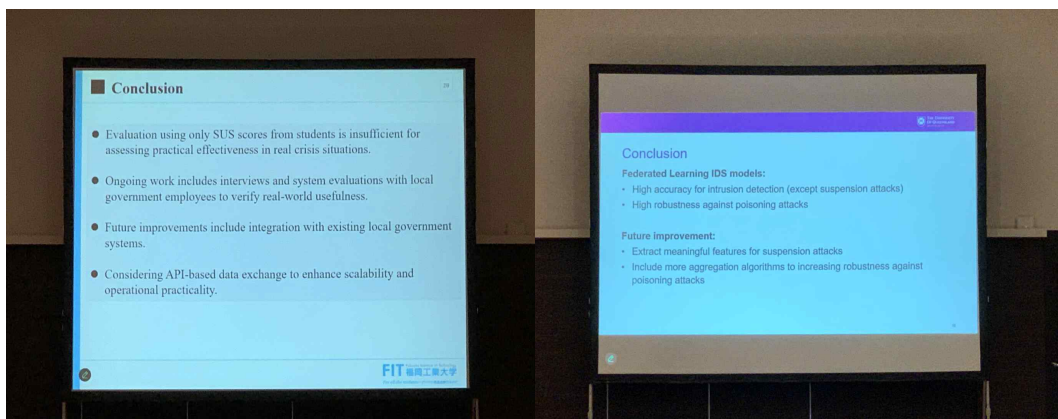
## II. MobiSec 2025

### □ 컨퍼런스 개요

- 기간/장소 : 2025년 12월 15일(월) ~ 12월 19일(금) / 일본 삿포로
- 주요 내용 : 모바일 인터넷 보안과 사이버 보안 분야에서 직면한 보안 문제의 해결을 위한 산·학·연 연구내용 발표 등
- 참가자 : 한국, 일본, 중국, 대만, 유럽 등 14개국에서 378명 참가

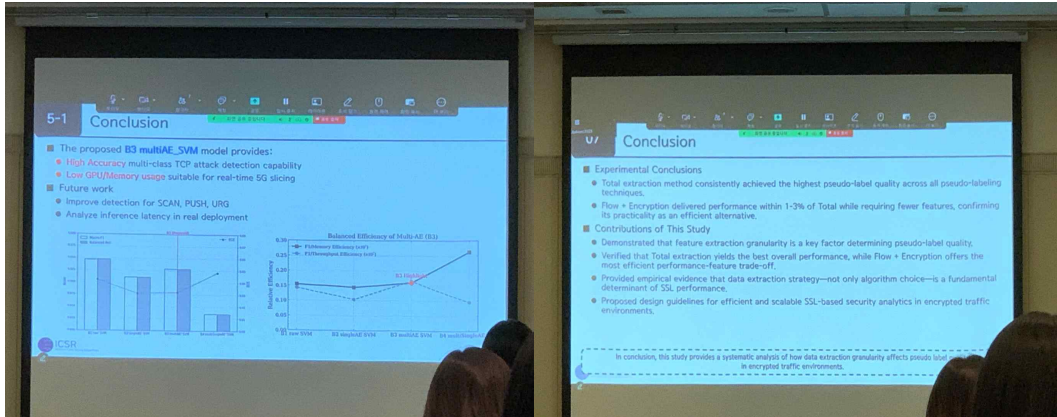
### □ 주요 내용

- (AI 기반 보안) 기존 사이버 보안 패러다임이 'AI를 활용한 보안 (AI for Security)'에서 'AI 자체를 보호하기 위한 보안(Security for AI)'으로 전환되고 있음
  - (자동화) 외부 API 기반 대규모 언어모델(LLM)에 의존하지 않고, 소형 언어모델(SLM)을 instruction-tuning하여 폐쇄망·특화망 환경에서도 취약점 식별 및 보안 분석이 가능함
  - (취약점) AI 모델의 학습·운영·출력 과정 자체가 데이터 중독 (Poisoning), 자기출력 재활용 등 새로운 보안 위협의 대상이 될 수 있음



- (네트워크 위협 감지) 암호화 트래픽 증가, 네트워크 슬라이싱 및 다양한 서비스 운용으로 인해 기존 단일 특징·단일 모델 기반 탐지 방식에는 한계가 있으며, 지능형 위협 감지 기술이 필요함

- 네트워크 위협은 정상 행위와 유사한 형태로 은닉될 수 있음
- 따라서, LLM 기반 행위 모델링, 자원 효율형 실시간 탐지, 암호화 트래픽 중심 분석을 통해 기존 탐지 기법의 한계를 보완해야 함



- (양자보안) 5G 특화망 보안은 '단일 양자내성 알고리즘 채택'이 아니라, 암호 체계의 다층적·다양화된 단계적 전환 전략이 필요함
- 공개키·대칭키 암호, 인증·키 교환 전반에 걸쳐 PQC 적용이 필요함
- 특히, 핵심 프로토콜 영역에서는 PQC와 QKD의 병행 적용 및 격자계와 비격자계 암호의 공존을 고려한 단계적 전환이 요구됨

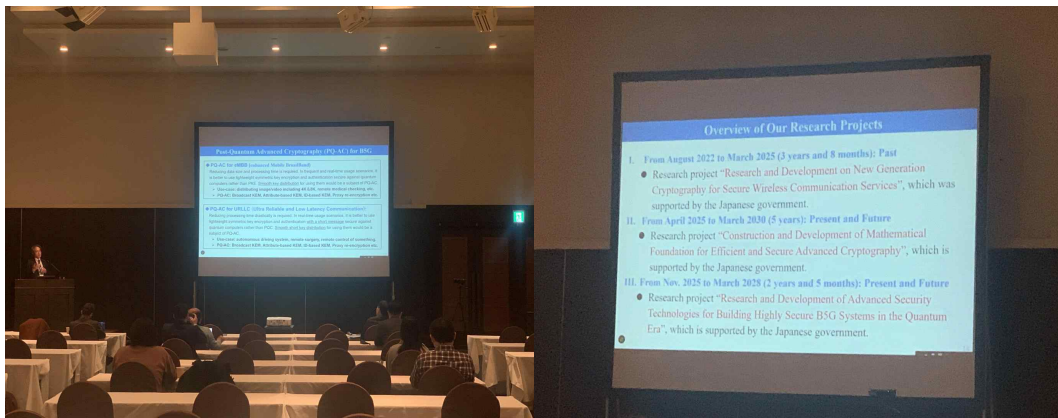


- (차세대 네트워크 보안) 개별 암호 기술이나 특정 공격 대응을 넘어, 신호·서비스·AI를 포괄하는 통합적 보안 체계로의 전환이 필요함
- 공격을 완전히 차단하는 예방 중심 접근만으로는 한계가 있음
- ① 사전 위협 분석, ② 지능형 탐지, ③ 서비스 연속성 확보, ④ 신속한 복구를 포함한 회복탄력성 중심의 보안 전략이 필수적임

- 보안 분석 대상을 네트워크 트래픽이나 프로토콜 수준을 넘어 정책·요구사항·서비스 영역까지 확장해야 함
- 오픈소스를 활용해 5G-AKA 절차에서 발생 가능한 재전송·재생 공격, SQN 비동기화, NF 연쇄 장애를 재현 및 정책·가이드라인 수준에서 적용 가능한 보안 통제 항목을 도출함



- (적응형 지능 및 시스템 보안) 가상화 환경, 모바일 엣지 컴퓨팅(MEC) 등 다양한 계층에서 지능형 의사결정, 자동화를 보안에 접목하여 보안성을 강화함
- (지능형 의사결정) 그래프 기반 시공간 적응형 강화학습을 통해 MEC 환경에서 작업 오프로딩을 지능적으로 결정하는 등 자원 제어를 통한 보안·신뢰성을 향상함
- (자동화) KVM 기반 가상화, procfs 기반 인터페이스 등 가상화·시스템 레벨에서의 정보의 추적·제어 자동화를 통해 기밀정보 확산 및 내부 위협을 대응함





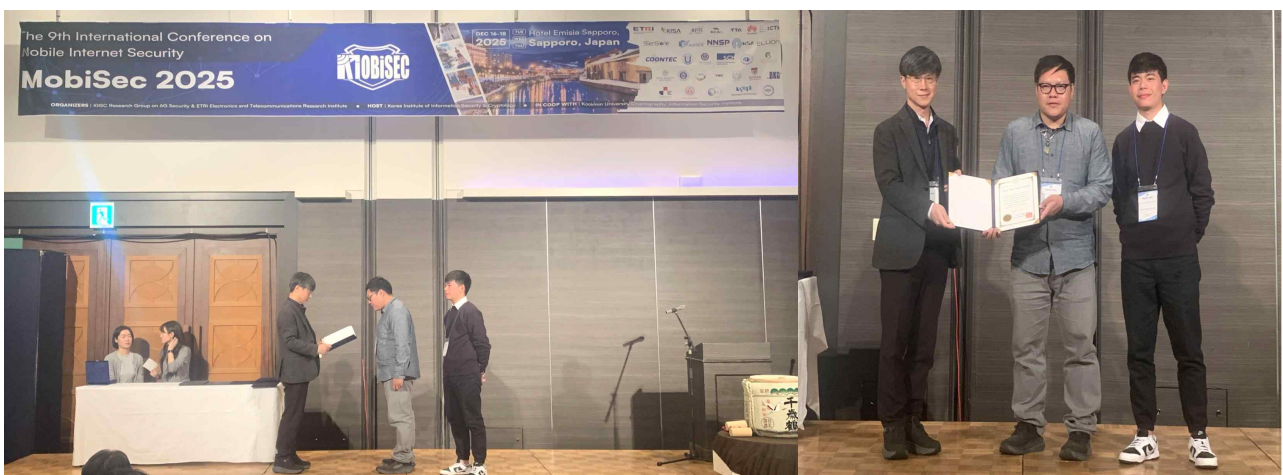
- (포스터 세션) 5G/6G, IoT, 클라우드 환경을 포함한 시스템 및 네트워크 보안을 주제로 총 78편의 포스터가 발표됨



- (KCA 원장상 시상) 모바일 인터넷 보안 분야의 총 178편의 최신 연구 논문 중 우수논문 2건을 선정하여 KCA 원장 명의로 'KCA 원장상' 2건 대리 시상

< 우수논문 내역 >

구 분	논문명	저 자
1	Secure Satellite Communication Using Shamir's Secret Sharing-Based Frequency Hopping Technique	Kim Su-Kyoung, Kim So-Yeon and Lee Il-Gu
2	Multi-Keyword Searchable Identity-Based Proxy Re-Encryption with Validity Period Control from Lattices	Er-Shuo Zhuang, Kai-Him Lam, Ming-Feng Tsai, Wei-Cheng Hung and Chun-I Fan



### III. TTA eqSIM Project Workshop

#### □ 워크숍 개요

- 일자/장소 : 2025년 12월 17일(수) / 일본 삿포로
- 주요 안건 : 「양자보안 기반 5G특화망 기기 식별 기술 및 시험검증 기술개발」 사업 성과 점검, eqSIM 서비스 실증 방안 및 성능 분석 방안 논의 등
- 참가자 : 국민대학교, TTA, KCA 등 공동연구개발기관



#### □ 주요 내용

- (해외 동향) 국외 주요국들은 2023년부터 모바일 및 네트워크 보안과 데이터 기밀성 보장을 위해 PQC 체계로 전환 예정
  - 미국 국립표준기술연구소(NIST)는 레거시 암호화 알고리즘의 폐기를 공식화하며 중요한 마일스톤을 제시함
  - RSA, ECDSA, EdDSA, DH, ECDH를 포함하는 기존의 비대칭 암호화 알고리즘은 2030년부터 사용이 중단되고, 2035년에는 완전히 사용이 금지됨
- (도입 방안) 성공적인 PQC 배포를 위해서 하이브리드 접근 방식, 암호화 민첩성 확보 및 5G 성능 제약 조건 간의 조화로운 균형이 필요함
  - (하이브리드 모델) NIST와 5G Americas에서 승인한 산업계의 합의는 전환 단계 동안 하이브리드 PQC 구성을 의무화함

## &lt; 기존 암호와 양자 내성 암호 비교 &gt;

구 분	기존 암호(예: X25519)	양자 내성 암호(예: Kyber)
양자 공격	취약함 (Shor 알고리즘 등에 의해 붕괴)	강력함 (내성 있음)
기존 공격	매우 강력함 (수십 년간 검증)	아직 충분히 검증되지 않음 (수학적 결합 가능성)
결합 (HPQC)	양자 공격이 발행해도 PQC가 막아주고, PQC에 예상치 못한 결함은 기존 암호가 막아줌	

- (암호화 민첩성\*) PQC 전환의 주요 목표이며, 이를 위해 시스템은 듀얼 스택 모드(전통적 암호화, PQC 강화 연결)로 운영되어야 함
- \* 알고리즘을 쉽게 교체하거나 업데이트할 수 있는 능력

인터페이스	도메인	보안 메커니즘	PQC 목표 알고리즘	PQC 전환 방안
UE 인증	접속	5G-AKA 키 교환	ML-KEM	ECIES/ECDH KEM 대체
코어 NF 간 통신	SBA	상호 TLS	ML-KEM & ML-DSA	하이브리드 PQ-TLS 확장
PLMN 간 로밍	SBA/도메인	N32-c	ML-KEM & ML-DSA	하이브리드 PQ-IPsec/PQ-TLS
gNB/UE 무선링크	접속	무선 인터페이스 키 파생	대칭 PQC에 의해 키잉	양자 안전 K <sub>{gNB}</sub> 입력

- (실증 시나리오) 이음5G 테스트베드를 활용하여 무암호 대 PQC 적용 비교와 고부하 트래픽 혼재 테스트를 통한 eqSIM 도입에 따른 성능 분석
- (목적) PQC가 추가하는 순수 지연시간(Overhead) 측정과 PQC로 인해 커진 패킷이 5G특화망 업링크 대역폭을 포화시킬 때 제어 신호 생존성을 확인함
- (테스트베드 현황) 모바일코어(3종), 4.7GHz gNB(2종), 단말(5종) 및 물류 서비스 데모설비와 5G 메시지 분석을 위한 DM SW 1식







## 붙임1

## MobiSec 2025 워크숍 참석 요청

ICT 표준화와 시험인증의 글로벌 리더

청정@서상


**한국정보통신기술협회**  
 Telecommunications Technology Association

수신자 수신자참조

(경유)

 『양자보안 기반 5G 특화망 기기 식별 기술 및 시험검증 기술개발』 과제 관련  
 제 목 MobiSec 2025 워크숍 참석 요청

1. 귀 기관의 무궁한 발전을 기원합니다.
2. 우리 협회는 “양자보안 기반 5G 특화망 기기 식별 기술 및 시험검증 기술개발” 과제를 주관하고 있습니다.
3. 위와 관련하여, MobiSec 2025에서 과제의 워크숍을 개최하고 아래와 같이 진행할 예정이오니, 귀 기관의 참여를 요청드립니다.
  - 가. 과 제 명: 양자보안 기반 5G 특화망 기기 식별 기술 및 시험검증 기술개발
  - 나. 주관기관: 한국정보통신기술협회
  - 다. 참여기관: 국민대학교 산학협력단, 한국방송통신전파진흥원, ㈜이루온, ㈜리임씨에스아이
  - 라. 일 자: 202.12.17.(수), ※ Mobisec 2025, 12. 16.(화) ~ 18(목) 기간 중 개최 예정
  - 마. 장 소: Hotel Emisia Sapporo(일본 삿포로)
  - 바. 주요논의사항
    - 최신 보안 트렌드에 따른 양자보안 기기식별 기술 및 시험검증 기술 발전 방향 논의
    - 1/2년차 연구 성과 발표 및 공유
    - 1단계 평가를 위한 실증관련 업무 협의

붙임, MobiSec 2025 행사 및 워크숍 개최안, 끝.

한국정보통신기술협회 회장



수신자 국민대학교 총장, 한국방송통신전파진흥원장, (주)이루온 대표이사, (주)리임씨에스아이사

간결 11/19

선임 이주승 행정 전속형

협조자

 시행 정보통신시험인증연구소-국방 ( 2025. 11. 19. ) 접수 ( )  
 ICT-25.177

우 13691 경기도 성남시 분당구 분당로 47 / http://www.tta.or.kr

전화 010-5110-2297 /전송 / jslee@tta.or.kr / 공개

## 붙임2

## MobiSec 2025 프로그램

## □ 컨퍼런스 개요

- (일자/장소) 2025년 12월 16일(화) ~ 19일(금) / 일본 삿포로 에미시아 호텔
- (주요 내용) 모바일 인터넷 보안 관련 최신 기술(6G, AI, 양자보안 등)과 위협 탐지 및 암호 기술에 관한 연구 동향

## □ 프로그램(안)

Tuesday, 16th December 2025			
Time	Palace Ball Room (East)	Palace Ball Room (West)	Crown Room
09:00 ~ 10:30 (1H 30M)	<b>Session 1A</b> System Operation Security Chair: -	<b>Session 1B</b> AI-driven Security 1 Chair: -	<b>Session 1C</b> Industry Security Chair: -
10:30 ~ 10:45	Break (15M)		
10:45 ~ 12:00 (1H 15M)	<b>Session 2A</b> IoT Security Chair: -	<b>Session 2B</b> Advanced Cryptography Chair: -	<b>Session 2C</b> Network Threat Detection Chair: -
12:00 ~ 13:40	Lunch – Complement of MobiSec conference (1H 40M)		
13:40 ~ 14:00 ( Opening )	Opening Ceremony		
14:00 ~ 15:00 (1H)	Keynote 1 Prof. Yongdae Kim (Korea Institute of Science and Technology, Korea) TBD		
15:00 ~ 15:15	Break (15M)		
15:15 ~ 16:15 (1H)	Panel Discussion TBD		
16:15~ 16:30	Break (15M)		
16:30 ~ 18:00 (1H 30M)	<b>Session 3A</b> Quantum/Post-Quantum Security Chair: -	<b>Session 3B</b> Key Exchange & Management System Chair: -	<b>Speicla Session</b> Chair: -
Time	Wednesday, 17th December 2025		
09:00 ~ 10:30 (1H 30M)	<b>Session 4A</b> 6G and Next Generation Network Security 1 Chair: -	<b>Session 4B</b> AI-driven Security 2 Chair:-	<b>2025 MobiSec Workshop 1</b>
10:30 ~ 10:45	Break (15 min)		
10:45 ~ 12:00 (1H 15M)	<b>Session 5A</b> 6G and Next Generation Network Security 2 Chair: -	<b>Formal Verification Session 1</b> Chair: -	<b>2025 MobiSec Workshop 2</b>
12:00 ~ 13:30	Lunch – Complement of MobiSec conference (1H 30M)		
13:30 ~ 14:30 (1H)	Keynote 2 Prof. Junji Shikata (Yokohama National University, Japan) TBD		
14:30 ~ 15:00	Break (30M)		
15:00 ~ 16:15 (1H 15M)	<b>Session 6A</b> Air & Space Security Chair: -	<b>Formal Verification Session 2</b> Chair: -	<b>TTA eqSIM Project Workshop</b> (14:30~16:15)
16:15 ~ 16:30	Break (15M)		
16:30 ~ 18:00 (1H 30M)	<b>Poster Session 1&amp;2 (Offline)</b>		<b>Global Research Collaboration Forum</b>
19:00 ~ 21:00	Banquet – Complement of MobiSec conference (2H)		
Time	Thursday, 18th December 2025		
09:00 ~ 10:45 (1H 45M)	<b>Session 7A</b> Cryptographic Applications and Analysis Chair: -	<b>Session 7B</b> Adaptive Intelligence and Syst em Security 1 Chair: -	<b>Session 7C</b> Blockchain/Distributed Trust Chair:
10:45 ~ 11:00	Break (15M)		
11:00 ~ 12:00 (1H)	<b>Session 8A</b> Digital Asset Protection Chair: -	<b>Session 8B</b> Adaptive Intelligence and System Security 2 Chair: -	<b>Session 8C</b> Covert Threat Analysis Chair: -
12:00 ~ 13:30	Break (1H 30M)		
13:30 ~ 15:30 (2H)	AirGap Project Workshop		
15:30 ~ 17:00 (1H 30M)	E-Business Information Systems & Cyber Security Insight Hour		
Time	Friday, 19th December 2025		
09:00 ~ 11:00 (2H)	Roundtable on Research Challenges in the 6G, Quantum, AI, and E-Business Information Systems, etc.		



## 붙임3

## 모바일인터넷보안 국제학술대회 KCA 원장상 협조

KIISC

# 한국정보보호학회

Korea Institute of Information Security & Cryptology

수 신 : 한국방송통신전파진흥원장

참 조 : 디지털융합본부장  
(경 유)

제 목 : 제9회 모바일인터넷보안 국제학술대회 (MobiSec 2025) 우수논문 수상작 선정 결과

1. 귀 기관 의 무궁한 발전을 기원합니다.
2. 한국정보보호학회 6G 보안연구회는 올해로 9회째를 맞이한 'MobiSec 2025(모바일 인터넷 보안 국제 학술대회)'을 오는 12월 16일(화) - 18일(목) 일본 삿포로에서 국제컨퍼런스 행사로 개최합니다.
3. 금번 행사는 한국, 일본, 대만, 중국, 스페인 등 전세계 전문가들이 운영 및 프로그램위원으로 참여 하여 아래와 같이 수상작 선정 결과를 안내 드리며, 귀 기관의 협조에 감사드립니다.

- 아 래 -

가. 수상작 선정결과 : 2편(Best Paper)

유형	논문 제목	저자	소속
Best Paper	Secure Satellite Communication Using Shamir's Secret Sharing-Based Frequency Hopping Technique	Kim Su-Kyoung, Kim So-Yeon and Lee Il-Gu	Sungshin Women's University, Korea
Best Paper	Multi-Keyword Searchable Identity-Based Proxy Re-Encryption with Validity Period Control from Lattices	Er-Shuo Zhuang, Kai-Him Lam, Ming-Feng Tsai, Wei-Cheng Hung and Chun-I Fan	National Sun Yat-sen University, Taiwan

나. 상장 수령처 : (02707) 서울특별시 성북구 정릉로 77, 국민대학교 과학관 104호 정보보안암호수학과 학과사무실

다. 문 의 처 : 한국정보보호학회 사무국 T. 02-564-9333 (내선 0)

붙임 1) 영문 상장 문구(안)

사단법인 한국정보보호학회



담당자 : 최 윤 정

시 행 : 정보보호 2025 - 611 (2025. 12. 2.) 접 수 :

우 06132 서울시 강남구 논현로 507 909호 (역삼동, 성지하이츠 3차) / www.kiisc.or.kr

Tel. 02-564-9333 (내선 0) Fax. 02-564-9226 / kiisc@kiisc.or.kr