SSE-CMM 기반 기술적 보안 성숙도 수준 측정 모델 연구

김점구* · 노시춘**

요 약

정보보호수준 검증방법은 프로세스를 중심으로 정보보호 제품, 시스템, 서비스를 개발하려는 조직의 개발능력을 평가하는 SSE-CMM(System Security Engineering-Capability Maturity Model)모델이 있다. CMM은 소프트웨어 개발업자의 개발능력을 평가하고 개선시키며 조직 전체의 성숙도 수준을 측정하는 모델이다. 그러나 이 방법은 보안엔지니어링 프로세스의 개선과 능력을 평가하는데 조직차원이 아닌 개별 프로세스의 능력수준 평가에 그치고 있다. 본 연구과제에서는 이들 기존연구를 근간으로 기술적 관점에서 정보보호수준 성숙단계를 정의하고자 한다. 연구방법은 정보보호취약점 진단, 기술보안체계 검증, 기술보안 이행실태 진단으로 구성한다. 제안하는 방법론은 업무현장 에서의 범위와 수준에서 정보시스템의 현재 상태, 취약점 실태, 정보보호 기능 이행과 기능만족도 수준을 평가한다. 제안된 방법에 의한 평가결과는 정보보호 개선대책 권고모델 수립 근거로 활용하여 정보보호 개선의 활용을 목표로 하고 있다.

A Study on Models for Technical Security Maturity Level Based on SSE-CMM

Jeom Goo Kim* · Si Choon Noh**

ABSTRACT

The SSE-CMM model is how to verify the level of information protection as a process-centric information security products, systems and services to develop the ability to assess the organization's development. The CMM is a model for software developers the ability to assess the development of the entire organization, improving the model's maturity level measuring. However, this method of security engineering process improvement and the ability to assess the individual rather than organizational level to evaluate the ability of the processes are stopped. In this research project based on their existing research information from the technical point of view is to define the maturity level of protection. How to diagnose an information security vulnerabilities, technical security system, verification, and implementation of technical security shall consist of diagnostic status. The proposed methodology, the scope of the work place and the current state of information systems at the level of vulnerability, status, information protection are implemented to assess the level of satisfaction and function. It is possible that measures to improve information security evaluation based on established reference model as a basis for improving information security by utilizing leverage.

keywords : Evaluation Methodology, Maturity Level, Technical Security, SSE-CMM Network

접수일(2012년 8월 25일), 수정일(1차: 2012년 9월 6일),
게재확정일(2012년 9월 7일)

* 남서울대학교 컴퓨터학과
** 남서울대학교 컴퓨터학과 (교신저자)

1. 서 론

정보보호 수준 성숙단계란 정보보호가 조직에 기여하거나 정보보호 활동을 통하여 조직의 정보보호 수준이 발전하여 가는 과정을 단계화한 것 이다. 대표적으로 프로세스 중심으로 정보보호 제품, 시스템, 서비스 개발 조직의 개발능력을 평가하는 SSE-CMM(system security engineering-capability maturity model) 모델이 있다. SEI(software engineering institutes)의 CMM이 소프트웨어 개발업자의 개발능력을 평가하고 개선시키며 조직 전체의 성숙도 수준을 측정한 모델인 반면 SSE-CMM은 공학, 보증, 위험 프로세스 3가지 요소로 보안 엔지니어링을 다루며 성숙도 평가 모델과 수준을 제시하고 있다. 이 방법은 보안 엔지니어링 프로세스의 개선과 능력 평가에서 조직원이 아닌 개별 프로세스의 능력수준을 평가하는 측면이 있다. 본 연구과제는 이들 기존 연구를 근간으로 기술적 분야 정보보호수준 '성숙단계' 측정 모델을 개발하고자 한다. 이 연구가 필요한 이유는 업무현장에서 보안대책 수립 시 가장 필요한 기술적 영역의 보안수준 측정 기준을 발굴하기 위한 것 이다. 연구는 관련연구, 문제점, 정보보호 성숙도 수준 측정 방법론 개발, 결론의 순서이다.

2. 기존 모델 사례

2.1 성숙도 모델 (CMM:capability maturity model)

CMM은 ISO SPICE와 함께 Software Process Improvement를 위한 대표적 모델중 하나이다. 80년대 중반 미 국방성에서 소프트웨어 개발 프로젝트 외주시 외주 업체들의 프로젝트 수행 결과가 품질측면에서 만족스럽지 못하자 SEI의 Watts S. Humphrey가 소프트웨어 개발능력이 우수한 업체를 선정할 기준을 연구 했다. 품질은 제품을 생산하는 프로세스가 우수하면 양질의 제품이 나올 수 있다는 가정을 소프트웨어 개발에 적용한 것이다. CMM은 SW-CMM(software CMM), P-CMM(people -CMM), SE-CMM(system engineering CMM) SA-CMM(software acquisition CMM), SSE- CMM(software security CMM) 모델로 계속 진화가 진행되고 있다. SW-CMM은 크게 다섯 단계로 분류 되며 소프트웨어 개발 조직 단위를 개발 프로세스 관점에서 평가하고 개발 프로세스를 향상시키기 위한 전략 모델이다[1].

2.2 시스템보안공학 성숙도 모델 (SSE-CMM:system security engineering capability maturity model)

SSE-CMM은 보안시스템의 효과적 개발을 위한 보안공학적 원칙이 개발기관에 얼마나 잘 내재 되어 있는지를 평가하기 위한 방법이다. 영역(domain)과 능력(capability) 두 측면으로 나뉘며 영역 측면에서는 11개로 구분된 보안공학 공정분야 이외에 11개 프로젝트 및 조직 공정분야로 구성된다. SSE-CMM을 이용한 평가방법으로 SSAM(SSE-CMM appraisal method)이 개발되었는데 계획수립-준비-현장실사-보고 단계를 거친다. SSE -CMM이 보안공학 공정에 대한 평가뿐 아니라 자체적인 공정 향상 노력에도 이용할 수 있도록 하기위한 접근법이 제안 되었다. SSE-CMM은 보안공학을 보장하기 위해 존재하는 조직의 보안공학 공정(security engineering process)의 필수적 특성을 서술한다. SSE-CMM이 특정 공정 또는 처리 순서를 규정하는 것은 아니며 일반적 보안공학을 커버하기 위한 표준 계량 도구이다[2][3][4].

3. 기존 모델의 실무 적용 어려움

정보시스템의 보안성에 대한 접근 방법론은 제품 중심의 CC, 관리 중심의 BS7799(ISO 17799), 정보보안시스템 개발기관의 프로세스에 대한 평가방법 SSE-CMM이 있다. 세가지 방법 중 SSE-CMM은 정보보호 제품, 시스템, 서비스를 개발하는 조직의 개발능력을 평가한다. CMM이 소프트웨어 개발업자의 개발능력을 평가하고 개선시키며 조직 전체의 성숙도 수준을 측정한 모델인 반면 SSE-CMM은 공학, 보증, 위험 프로세스 3가지 요소로 보안 엔지니어링을 나누고 성숙도 평가 모델과 수준을 제시한다. SSE-CMM은 보안직차원이 아닌 개별 프로세스의 능력수준을 평가

한다. 그러나 국내 보안업무 현장에서는 일반적으로 관리적, 기술적 보안에 중점을 두고 업무체계가 구성되고 있다. 따라서 기존 모델을 현장업무 적용 시는 조직 전체적 정보보호 위험도, 정보보호 수준 측정지표, 취약점 점검방법, 성숙도 수준 측정기준에 대한 실무적 가이드라인 도출에 다음과 같은 어려움 이 있다.

<표 1> 기존 방법론 적용시의 어려움

제 목	내 용
정보보호 위험도 측정방법의프레임워크	- 위험분석 상세분석 이론 - 관리적, 물리적, 기술적 분야 측정방법 - 단계별 보안수준 평가 방법
정보보호수준 측정지표개발 문제	- 관리적, 물리적, 기술적 보안분야 측정 지표 - 어떤지표를 사용해야 하나
취약점 점검방법의 문제	- 모의침투 방법 - 공개용소프트웨어 사용방법
정보보호성숙도 수준측정기준의 문제	- 관리적, 물리적, 기술적 보안 측정 - 성수도의 등급 결정 기준

4. 성숙도 수준 측정방법 개발

4.1 측정 목적

성숙도 측정의 주목적은 시스템 도입, 운영 및 활용 능력을 진단, 분석해 기업별로 보안수준을 발전시키기 위한 개선방향을 수립이다. 민간기업 과 달리 공공부문은 법적으로 보안수준을 체크 받도록 하고 있지만 민간기업은 보안수준 자체 진단의 문화가 조성되지 못하고 있다. 성숙도 측정을 통해 기업의 자체적으로 취약점 을 진단하면 업무에 대한 문제점과 개선방향을 도출해 발전방향까지 수립할 수 있다. 이를 통해 향후 기업의 시스템 구축 및 고도화, 관리, 운영, 활용 시 시행착오를 줄일 수 있다.

4.2 측정작업의 목표

목표는 기존 방법론 적용 시 어려움을 해소 할 수 있는 기업 자체 진단의 성숙도수준 측정 방법론을 개발한다. 그 내용은 기술적 보안 측면에서 실무 현장에서 접근 가능한 방법론 개발이며 정보시스템의 정보보호 취약점 진단 방법론 도출, 기술보안 이행실태를 분야별로 진단이다. 이 취지에 부합 하는 범위와 수준에서 시스템의 현재 취약점 실태 및 정보보호기능 이행과 기능만족도 수준을 평가 한다. 그 결과는 정보보호 성숙 수준으로 평가 되며 평가결과는 정보보호개선 대책 권고모델 수립 근거로 활용 한다.

4.3 측정작업 프레임워크

측정작업 프레임워크는 정보보호 침해사고 전체구조를 대상으로 상위구조 -> 하위구조 톱-다운 식 평가용 연관도 메커니즘을 구성한다. 본 연구에서 제시하는 프레임워크는 다음과 같은 6개 단계의 측정 프레임워크이다.

1) 자산평가 : 정보시스템 운용자산에 대한 종류분류와 자산 가치를 평가
2) 위협평가 : 정보시스템 자산에 대한 내외부 로부터의 보안 침해위협을 점검, 평가
3) 취약성평가 : 운용중인 정보자산이 위험에 노출될 수 있는 가능성과 수준 평가
4) 보안체계진단 : 정보보호침해 위험을 회피 또는 감소시키는 기술적 분야의 현행 대응체계 평가
5) 위험도측정 : 조사된 정보시스템 자산에 가해지는 위협과 내부적인 취약성 및 대응 체계를 연계 분석하여 현재의 위험수준 평가
6) 정보보호성숙도 수준측정 : 이상의 산출결과 를 바탕으로 정보보호성숙도 수준 종합적 평가

<표 2> 기본작업 구도

작업단계	자산평가	위협평가	취약성평가	보안체계진단	위험도측정	정보보호수준측정
표기	A	T	V	P	R	L

* 표기 : A:asset,T: threat, V:vulnerability, R:risk, L:level

4.4 측정작업의 수행단계

측정방법은 기술적영역의 정보보호 위험도를 측정하되 측정방법은 보안사고 발생 유형과 특성, 사고와 관련되는 보안취약성, 정보보호 수준 측정 방법론 도

출이다. 정보보호 수준평가 는 평가체계와 절차, 수행내용, 실용화된 국내 기술의 종류 및 사용방법을 통해 평가지표를 선정하고, 평가지표를 작성한다. 측정대상 분야는 기술적 보안 측면을 중점으로 하며 물리적 보안, 관리적 보안 분야는 기술적 보안 연관분야를 포함한다. 측정영역은 정보보호 전체영역 중 가능한 핵심요소 측정방법을 도출하여 적용한다. 절차적, 기술적 측면의 핵심요소 측정 방법론 이며 핵심 프로세스로부터 긴급개선 요구사항을 도출한다.

<표 3> 단계별 수행방법

위협 평가	취약점 평가	보안체계 진단	위험도 측정	측정지표 결정
• 모의침투 • 보안체크리스트 점검 • 측정방법 개발	• 측정툴사용 • 보안체크리스트점검 • 현장실사 • 측정방법 개발	• 보호체계 점검개발	• 자산, 위협, 취약점, 보안체계단계 산정 • 위험도 산출방법 개발	• 취약점, 기술보안이행기술보안체계, 단계 측정 • 측정체계, 지표개발

4.5 보안사고 코드체계

국내에서 발생하였거나 향후 발생가능성이 예상 되는 사고유형을 유형별로 모형화 하고 각각의 코드를 부여한다. 사고모형 코드설계는 시스템 구축 시 활용가능 토록 10진 분류방식의 코드체계로 구성하되 4단계 계층구조로 설계 한다. 대분류는 부문별 5개영역으로 구분하며 영역 중복시는 최초 발생 부문으로 분류한다. 중분류는 부문별 하부구조로 사고유형을 기준으로 코드부여 하되, 모형중복사고는 선행 행위를 기준으로 한다. 소분류는 중분류 하부 구조로 사고 유형별로 코드를 부여하되 두가지 유형 이외의 유형은 향후의 활용을 대비하여 소분류 단위 명칭까지만 설정한다. 일련번호는 소분류단위의 사고별 일련번호이다.

대분류 : 업무분류기준 4종과 예비1종
중분류 : 정보보호 1종, 전자 1종
소분류 : 정보보호침해, 세부 분류
일련번호 : 소분류사고의 일련번호

<표 4> 보안사고 코드체계

코드체계	대분류	중분류	소분류	일련번호
자릿수	3	1	2	3

4.6 측정 체크리스트

보안사고 코드체계를 기반으로 사고모형별 측정 체크리스트를 작성한다. 사고모형 설정은 특수 사례 사고가 아닌 일반적 대표적 정보보호 침해 사고 유형을 기준으로 최근 발생실적 기준 대표적 사고 유형을 작성한다.

1) 해킹위협 측정 : 위협측정방법으로 제시된 위협 점검, 취약점점검, 기술보안체계 기술보안이행 측정방법
2) 악성코드 감염도측정 : 각종 악성코드 감염여부측정, 감염수준 측정방법
3) 개별사고모형별 측정 : 개별 사고별로 보안수준 측정가능영역에 대한 측정방법
4) 공통영역측정 : 개별 사고별 측정불가 영역, 측정자체가 기술적으로 어려운 영역에 대한 정보시스템 사고 종합측정
5) 취약점점검과 기술보안이행점검은 각각6개의 기술영역으로 구성
6) 기술보안체계 점검은 7개 기술영역으로 구성

<표 5> 측정 체크리스트 구성 요약

영역	측정 범위	항목 구성수
기술보안체계	기술보안계획체계, 정보보호인프라체계, 위험관리체계	3개부문, 7개세부부문, 70개항목
취약점 보유	NW ,OS, DB, AP, CL, 정보보호시스템	6개기술영역, 35개항목
기술보안이행	NW, OS, DB, AP, CL, 정보보호시스템	6개기술영역, 8개세부영역,40개항목

4.7 측정결과 평가방법

성숙도 수준 산출방법은 1) 측정분야별 항목별로 취약점 및 정보보호 기능만족도 조사 2) 측정 분야별로 측정결과 집계 및 분석. 1.단계 집계, 2단계 평가, 3단계 등급판정, 4단계 종합의견 작성이다. 성숙도수준

영역별 점수배분 가이드라인은 평가대상 영역인 취약점보유, 기술보안 체계, 기술보안 이행 3개영역을 대상으로 영역별 점수배분을 결정한다. 영역별 점수배분 총 100% 범위를 부여한다. 반드시 현장업무 진단 평가 결과에 따라 영역별점수 적용여부를 결정 한다.

<표 6> 측정결과 분석방법

항 목	내 용
○정보보호위험관리 절차/ 측정방법 개발	○기존방법론 특화 -기술적분야 6개영역 -기술적분야 3개 카테고리 -5개단계 수준으로 평가
○정보보호측정지표 개발	○기존방법론 특화 -기술적분야만대상 기술적분야6개영역,3개카테고 리측정지표
○취약점 점검 방법 ○모의침투 방법	○기존방법론 특화 -공용소프트웨어사용 -점검방법 내용을 현행화 -점검방법을 실무용 작성
○정보보호성숙도수준측정기준 개발	○기존방법론 특화 -기술적분야만을측정,기술적분야6개영역,3개카테고리별 수준측정 개발 -5단계수준 측정

4.8 영역별 점수 배분

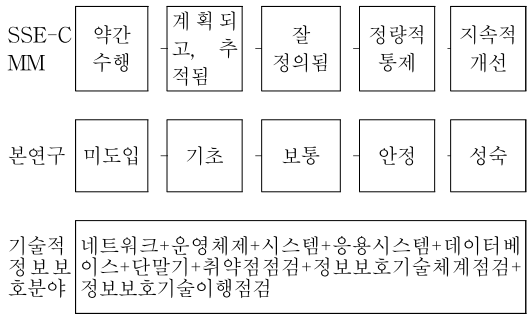
가중치는 선택적인 적용사항으로서 현장업무 전문가집단의 협의를 통해 적용여부, 적용대상, 적용수준을 결정한다(델파이법의취지). 가중치 값은 진단평가의 목적, 진단평가의 시기적 특성, 대상 업무성격, 업무규모, 업무프로세스 단계, 프로세스 중요도를 기준으로 부여한다. 가중치 값은 가변적인 데이터값 으로서 고정적 개념이 아니다. 가중치 값은 동일구룹 부여 대상 항목 전체를 대상으로 100%의 범위내 값을 부 항목간 상대적으로 배분한다. 본 연구에서 제시하는 가중치 값은 영역별 가이드라인 이다.

- 취약점보유 : 평가대상 기술영역 전체에 걸쳐 실제적인정보시스템취약점 보유실태를 나타내고 있으므로 가장중요한비중 부여.(권고기준50 %)
- 기술보안체계 : 기술보안이행에 대한 기본인프라 수준 (권고기준 20 %)
- 기술보안이행: 평가대상 기술전체영역 전체에 걸쳐 보인 이행실태를 나타내고 있으나 취약점 보유지표에서 정보보호수준을 평가 하므로 상대적 비중이 작음(권고기준 20 %).
- 가중치:3개영역별 점수배분 합계치 외에 권고기준10%를 가중치 값 부여

4.9 정보보호수준 성숙단계 부여

본 연구에서는 연구절차를 근간으로 기술적 관점에서 정보보호수준 '성숙단계'를 정의한다. 제시하는 정보보호수준 성숙단계 구도는 SSE-CMM과 비교하여 다섯단계 레벨로 구성된다. 산출된 정보보호 지수를 활용하여 정보보호수준 단계를 정의한다. 정보화가 진전 될수록 정보보호 수준 또한 진전되어야 한다. 초기단계 에서는 정보보호 의식이 점차 높아지며 이 영향으로 정보보호기술이 차츰 도입되고, 나중에는 조직의 체계적인 보안정책으로 이어진다.

- 미도입 단계 : 아직까지 정보보호활동이 구체적으로 추진되지 않는 단계. 정보 보호에 대한 인식 부족, 정보보호 기술도입 매우 미흡
- 기초단계 : 바이러스 백신 등 기본적 보안 기능만을 수행. 정보보호 의식은 미도입 단계보다 높지만, 정보보호 의지가 영향을 미치지 않는다.
- 보통단계 : 기업 구성원이 정보보호에 대한 관심이 높아지며, 여러 가지 정보보호 기술들이 도입되는 단계.
- 안정단계 : 구성원의 정보보안 의식이 높은 수준이며, 여러 기술로 인해 체계적인 정보보호 활동이 수행되는 단계.
- 성숙단계 : 정보보호 정책이 경영전략과 함께 추진되며, 정보보호 조직이 독립 운영 수준.



(그림 1) 정보보호수준 성숙단계

정보보호성숙도수준 등급 설정기준은 A-E 5개 단계의 등급명칭을 설정한다. 5개 단계는 정보보호 기능 만족도를 매우만족-매우미흡 구간으로 설정한다. 5개 단계의 정보보호성숙도 수준을 성숙-미도입 구간으로 설정한다. 5개단계 성숙도 수준별 점수범위를 0-100 구간으로 부여한다. 성숙단계는 정보보호 활동을 통하여 조직 및 국가의 정보보호 수준이 이상적으로 발전하여 가는 과정을 단계화한 것이다.

<표 7> 정보보호수준 성숙단계

단 계	점 수	특 징
미도입 단계	20점 미만	정보보호가 구체적으로 추진되지 않은 단계로. 정보보호의 필요성, 정보보호에 대한 의식, 기술도입 등 대부분 내용 미흡
기초 보호	20점 이상40점만	백신 등의 기본적 기술이 도입, 정보시스템이 부분적으로 보호되는 수준에 그치고, 보안의식, 조직전체의 보호정책 등은 미흡
보통 보호	40점 이상60점미만	정보보호에 대한 관심이 높아지며, 여러 정보보호 기능 도입이 진행되기 시작
안정적 보호	60점 이상80점미만	전사적 정보보호 정책이 수립되기 시작, 조직이 정보보호 체계를 갖추는 단계. 구성원 보안의식이 높아지며 기술 보안은 높은 수준.
성숙 보호	80점 이상	보안정책이 경영전략과 함께 추진, 정보보호 조직이 독립 운영 수준. 이 수준 기업은 탈 벤처의 현상 중견기업의 규모됨.

<표 8> 정보보호 성숙도수준 등급 결정

등급명	A	B	C	D	E
정보보호기능 만족도	매우만족	만족	보통	미흡	매우미흡
정보보호 성숙도	성숙	안정	보통	기초	미도입
성숙도수준별 점수범위	81-100	61-80	41-60	21-40	0-20

5. 결 론

지금까지 프로세스를 중심으로 정보보호 제품, 시스템, 서비스를 개발하려는 조직의 개발능력을 평가하는 SSE-CMM 연구가 수행 되었다. SEI의 CMM이 소프트웨어 개발업자의 개발능력을 평가하고 개선시키며 조직 전체 성숙도 수준을 측정한 모델인 반면 SSE -CMM은 공학, 보증, 위험 프로세스 3개 요소로 보안 엔지니어링을 나누고 성숙도 평가 모델과 수준을 제시하고 있다. 이 방법은 보안 엔지니어링 프로세스의 개선과 능력을 평가 하는데 조직 차원이 아닌 개별 프로세스의 능력수준을 평가한다. 본 연구는 이들 기존연구를 근간으로 조직차원 기술적 분야를 대상으로 정보보호 수준 '성숙단계'를 제안 했다. 본 연구가 실무 현장에서 참고 모델로 활용되기를 기대한다.

참고문헌

[1] CMMhttp://www.freesoft.or.kr/osd/html/software/introduction3.htm

[2] SSE-CMM Org http://www.sse-cmm.org/

[3] CCRA(Arrangement on the Recognition of Common Criteria Certificates) http://www.commoncriteria.org.

[4] SSE-CMM, "Project, Systems Security Engineering Capability Maturity Model (SSE-CMM) - Model Description Document", V.2, http://www.sse-cmm.org, 1999. 4. 1.

[5] CC, Common Criteria for Information Technology Security Evaluation, Version 2.1, CCIMB-99-031, August 1999,

[6] British Standards Institution(BSI), "BS-7799", 1999.

[7] 정보통신부, 한국정보보호진흥원, 정보보호시스템 공통평가기준(정통부고시 제 2002-40), 2002.8.

[8] 한국정보보호진흥원, "공통평가기준 기반 평가기관 산정 방안 및 평가수수료 정책 연구," 수탁기관: 한국정보보호학회, 2003.11.

[9] TTAS.KO-12.004, "네트워크 보안 장비에 대한 성능 측정 방법", 한국정보통신기술협회, 2006

[10] 류재철외 2명, "국외 민간평가기관 평가 동향", 한국정보보호학회 학회지 특집, 보안성 평가 및 시험, 제 13권 6호, 2003.12

[11] 오흥륭외 1명, "국제 공통평가기준(CC)의 교육

동향 및 평가된 정보보호 제품 분석", 한국정보보호학회 특집, 사이버 범죄와 프라이버시, 제 13권 5호, 2003.10

[12] CC인증 제품 중 국제용은 15%에 불과, 보안뉴스 및 동향 2011.11.19

[저 자 소 개]

김 점 구 (Jeom Goo Kim)

1990년 2월 광운대학교
전자계산학과 이학사
1997년 8월 광운대학교
전자계산학과 석사
2000년 8월 한남대학교
컴퓨터공학 박사
1999년 3월~ 현재 남서울대학교
컴퓨터학과 교수
IT융합연구소장

email : jgoo@nsu.ac.kr

노 시 춘 (Si Choon Noh)

1987년2월 : 고려대학교
경영정보학 석사
2005년2월 : 경기대학교
정보보호기술 박사
2002년11월 : KT 시스템보안부장
2004년 12월 : KT 충청전산국장
2005년3월 ~ 현재 :남서울대학교
컴퓨터학과 교수
IT융합연구소연구위원

email : nsc321@nsu.ac.kr