https://doi.org/10.33778/kcsa.2020.20.1.069

미래 지휘통제체계를 위한 보안 규정 개선 요구사항 분석★

강지원*, 문재웅*, 이상훈**

요 약

지휘통제체계는 인간의 두뇌와 신경 조직처럼 정보·감시·정찰(ISR)에서 정밀타격체계(PGR)를 연결하는 링커이며 전투력의 중심이다. 미래 한국군의 지휘통제체계 구축시 기술적 문제뿐만 아니라 제도적 문제를 함께 고려해야 한다. 미국 국방부는 지휘통제체계 개발에 앞서 보안 정책을 수립하고 이를 구체화하여 아키텍처 문서로 정리하며, 이를 토대로 보안 정책의 일관성과 지속을 유지한다. 본 논문에서는 미군의 지휘통제체계 구축시 적용하는 보안 아키텍처를 살펴보고 현행 한국군의 보안 관련 정책(규정)을 분석하여 미래 지휘통제체계 구축 시 보안 요구사항을 식별한다. 식별된 보안 요구사항을 그룹핑하여 현행 보안 관련 규정의 분야별 개선사항을 도출하여 제시하고자 한다.

Analysis of Improving Requirement on Military Security Regulations for Future Command Control System

Jiwon Kang*, Jae Woong Moon*, Sang Hoon Lee**

ABSTRACT

The command control system, like the human brain and nervous system, is a linker that connects the Precision Guided Missile(PGR) in information surveillance and reconnaissance (ISR) and is the center of combat power. In establishing the future command and control system, the ROK military should consider not only technical but also institutional issues. The US Department of Defense establishes security policies, refines them, and organizes them into architectural documents prior to the development of the command and control system. This study examines the security architecture applied to the US military command control system and analyzes the current ROK military-related policies (regulations) to identify security requirements for the future control system. By grouping the identified security requirements, this study identifies and presents field-specific enhancements to existing security regulations.

Key words : Cyber security, Weapon systems, Embedded software, Vulnerability

접수일(2020년 02월 29일), 수정일(1차:2020년 3월 16일), 게재확정일(2020년 3월 27일)

★ 이 연구는 국방과학연구소의 국방 지휘통제 통합·연동 기반 기술 특화연구실 과제의 지원을 받았습니다(UD180012ED)

* 세종대학교

** 국방과학연구소

1. 서 론

국방분야의 주요 정보체계 중에 군사작전의 계획(P)-실행(D)-평가(E)와 관련된 자동화 정보체계가 지휘통제체계(C4I체계)이다. 군의 지휘통제체계는 지휘관이 부여된 임무 달성을 위해 가용한 자원을 최적의 장소와 시간에 배열하여 전투력 상승효과를 발휘할 수 있도록 지휘·통제·컴퓨터 및 정보(Command, Control, Commuter, and Intelligence)의 각 요소를 유기적으로 통합, 연결하여 실시간에 정보 수집 및 분석-지휘결심-계획지시-작전수행(타격)이 가능하게 하는 모든 시설·장비·인원 및 절차로 구성되고 통합된 체계로 정의할 수 있다. [1]

이에 따라 우리 군은 2000년대 초반부터 합동지휘통제체계(KJCCS), 지상·해상·공중 C4I체계 등 많은 자동화 정보체계를 구축하여 군사작전 지휘·통제 업무에 활용 중이다. 그러나, 현행 지휘통제체계는 개별 획득(연구개발)과 체계별 구축으로 일부 정보보호 적용 기술(체계)이 상이하며 진부화되는 실정이다. 이에 따라 군은 최신 기술을 사용하고 미국 등 선진국의 지휘통제체계 구축 사례를 벤치마킹하여 미래 지휘통제체계를 구축하기 위한 개념연구가 진행 중이다.

작전 운영개념이 변화하고 정보기술이 발전하면 군의 지휘통제체계의 모습도 개선되어야 한다. 특히, 군 조직의 특수성과 임무의 기밀성을 고려할 때 주요한 요소가 보안 문제이다. 미군 통합정보환경(JIE : Joint Information Environment)의 단일보안구조(SSA : Single Security Architecture)가 의미하는 바와 같이 통합된 정보환경에서 표준화된 안전한 보안 서비스를 제공하도록 준비하여야 한다.[2]

이 과정에서 보안 기술의 적용과 함께 보안 제도의 틀을 개선하는 것이 중요하다. 본 논문에서는 보안 아키텍처 수립 과정에서 미래 지휘통제체계 운영개념의 변화와 선진국 사례 분석을 통해 보안 요구사항을 식별하고 현행의 규정 개정 방향을 제시하고자 한다.

2. 선행 연구

2.1 미군의 보안 정책

미국 국방부 보안 정책의 총아는 아키텍처이다. 우리와 달리 미국은 보안 정책을 구체화하여 아키텍처 문서로 정리하여 정책의 일관성과 지속성을 유지하고 있다.

- 단일보안구조(SSA)

JIE SSA(Joint Information Environment Single Security Architecture)는 국방 사이버 인프라 운용 및 보안을 위해 보안 네트워크를 구축하고 네트워크에 대한 관제를 통해 사이버 위협에 공통된 대응을 할 수 있도록 설계된 미국 국방부(DoD) 보안 아키텍처이다. [6]

분산된 서버 및 서비스들을 핵심데이터센터를 중심으로 통합한 후, 분산된 보안 구조를 표준화된 단일보안구조로 전환한 것이다. 우리 말로 번역하면 단일보안구조 또는 통합보안구조라 불리운다.

SSA는 표준화된 보안 제품군을 최적의 위치에 적용하여 군 전체의 데이터센터 및 서비스 방어 기능을 수행하며 기존의 각 군 보안제품의 중복을 제거하고, 기존 보안제품을 운용하는 인력 및 장비들을 타 목적으로 전용할 수 있게 한다. 또한, 중복된 보안대책을 제거하여 중첩되고 중복된 역할과 책임의 복잡성을 최소화하며 정보체계에 대한 사이버 공격의 노출을 최소화하는 역할을 한다.

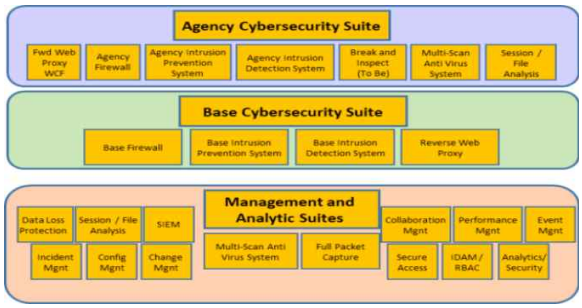
SSA의 목표는 ①사이버공격에 직면하였을 때 정보 및 정보 인프라에 지속적인 접근성 및 가용성을 보장하여 인프라에 대한 신뢰성을 확보하여 지속적 임무 수행 능력을 보장, ② 국방부와 임무 파트너와의 빠르고 안전한 데이터 공유를 위한 시스템 보안 기술 및 보안 네트워크 기술 적용, ③ 민감한 기밀 정보 보호, ④ 사이버 공간에서 시간과 장소에 제한없이 임무 지휘관의 임무 수행을 위한 접근성 보장, ⑤ 효율적인 프로세스를 통해 적은 위험으로 민첩하게 새로운 신기술을 삽입하고 배포하는 것이 가능, ⑥ 중앙 집중화, 중복성 제거 등을 통해 국방 사이버 인프라에 대한 사이버 위협에 대하여 효율적으로 보호 및 방어하는 것이다.

• 합동지역보안스택(JRSS)

JRSS(Joint Regional Security Stack)는 각 군 조직(육·해·공군)의 네트워크 보안관제를 중앙 집중화하여 중앙 집중방식으로 보안을 제공하고 네트워크 위협에 대처하기 위한 보안 스택(=계층별 보안 장비 집합)이다.[7] JRSS는 Agency, Base 2개의 계층(tier)이 존재하며 각 계층에서 제공하는 기능의 차이가 있어서 평문망 라우터인 NIPRNet의 JRSS와 비문망 라우터인 SIPRNet의 JRSS의 계층 구성이 상이하다. [8][9]

JRSS의 주요 기능은 보호, 관리, 작동하는데 사용되는 JMS(Joint Management System)를 통해 부대별 네트워크의 성능, 이벤트, 사고, 보안, 설정, 자산, 수정, 접근 등에 대한 시각화를 제공, 네트워크를 통해 활동하는 악성코드, 네트워크 자체에 대한 사이버 공격 등과 같은 보안 위협을 사전에 탐지하고 이에 대한 방어 조치, 자산 보안 관리, 및 중앙 집중식 네트워크 관리 및 방어이다.

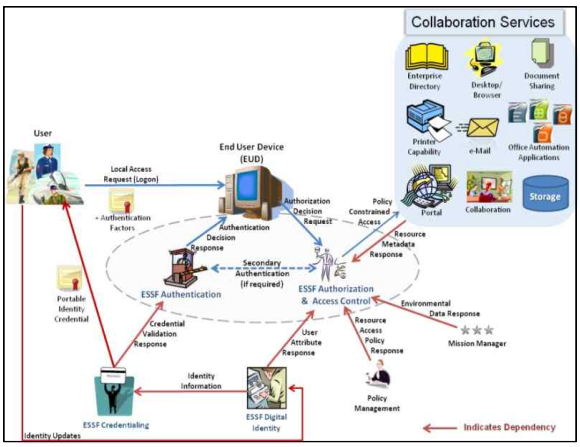
또한, JRSS의 목표는 ① 공개되서는 안되는 기밀 정보를 전송하는데 사용되는 네트워크인 Classified 네트워크와 평문 정보를 전송하는데 사용되는 네트워크인 Unclassified 네트워크를 통한 안전한 정보 교환 기능 제공, ② 네트워크 보안 관제에 대한 중앙 집중화 및 지속적인 모니터링을 통해 모든 시스템에 대한 상황을 지속적으로 인식하는 것, ③ 중앙 집중화 된 네트워크 관리를 통해 글로벌 네트워크를 운용하고 네트워크를 능동적으로 관리함으로써 사이버 공격에 효과적인 대응하는 것이다.



(그림 1) JRSS Logical Capabilities

• 전군네트워크접근및협업서비스(EANCS)

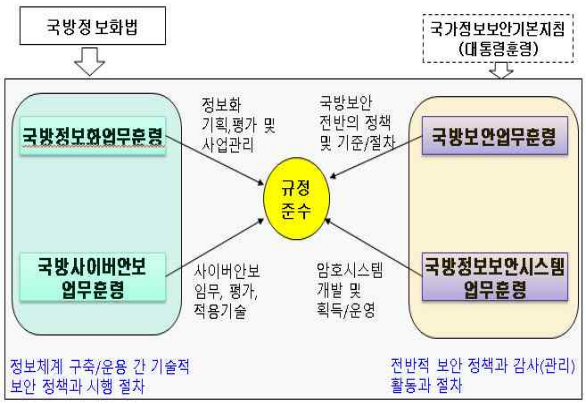
EANCS(Enterprise-wide Access to Network and Collaboration Services) RA(Referece Architecture)는 “DoD 내 모든 곳에서의 로그인하고 업무 수행을 원한다.”라고 한 합참부의장의 언급으로부터 시작되었으며, 이 요구사항과 관련하여 EANCS RA는 지정된 엔터프라이즈 서비스의 사용을 가능하게 하는 네트워크 로그인, 글로벌 인증, 권한부여 및 접근통제에 초점을 맞추고 있다. 또한 EANCS 구현 지침과 솔루션 아키텍처의 개발을 지원하며 이러한 개발 지원은 액티브 디렉터리와 엔터프라이즈 사용자 활동과 함께 글로벌 인증, 접근통제 및 디렉터리 서비스를 제공하는 것이다.[10]



(그림 2) OV-1 운영개념도

2.2 한국군의 보안 정책

현재 한국군의 국방 보안 관련 정책은 공개되지 않으나 보안 관련 규정으로 담아 실행의 구속력을 가지도록 하고 있으므로 규정을 살펴보기로 한다. 군 보안 관련 규정은 (그림 1)과 같이 네 개의 규정으로 요약할 수 있다. 국방부(정보화기획관실) 주관의 정보체계 구축·운영 간 기술적 절차를 규정하고 있는 좌측 그룹과 정보본부 주관의 일반 보안정책과 관리적 절차를 정한 우측 그룹으로 구분된다. 여기서 미래 지휘통제체계 구축을 위해 우선 적용될 것으로 예상되는 규정은 국방보안업무훈령과 국방사이버안보훈령 그리고 국방정보보안시스템훈령이다. [3][4]



(그림 3) 국방 보안 관련 규정 체계도

한편, 국방분야에 대한 사이버 위협이 고도화 됨에 따라 국방부는 '다계층 방어 전략(Defense in-depth)(출처 : 미 국방부 보보증 기술구조(IATF : Information Assurance Technical Framework R3.1, 2002, 9')에 따라 네트워크, 서버, 단말기, 응용체계(데이버 포함), 보호관리 등의 5개 영역별 보안 기술(체계)을 설치하여 중첩 방호하고 있다.

(그림 4) 정보체계 보안 구조

3. 미래 지휘통제체계 보안 요구사항 분석

3.1 미래 지휘통제체계의 보안 요구사항 식별

미래 지휘통제체계를 어떻게 운영해야 할 것인가에 대한 답은 현재 지휘통제체계 구축·운영의 경험을 통해 축적된 노하우와 미국과 같은 선진국의 지휘통제체계 운영 사례 연구를 통해 파악할 수 있다. 또한, 최근 국가적으로 4차 산업혁명에 대한 대비가 화두이므로 4차산업혁명 핵심요소인 AI-ICBM 기술을 군에 적용하는 것을 고려하여야 한다.

(그림 5) 국방 보안 관련 규정 개선 절차

현재 보안 관련 규정의 개선 방향은 앞서 연구한 미군의 SSA, JRSS, EANCS 등의 미군C4I체계 분석과 군의 요구를 종합할 필요가 있다. 현재까지 정리된 미래 지휘통제체계의 발전 방향의 요구사항은 다음과 같다.

- 통합 네트워크 운영
  - 전달망 통합 : 다계층 전달망(MBcN, Microwave망, 위성망)의 주(Main) 네트워크와 예비 네트워크로 구분하여 운용하던 것을 동시(Active-Active) 통합망으로 운용 필요.
  - 체계망 통합: 체계별 물리적으로 격리된 전달망을 통합하고 비도 또는 임무별로 가상화 기술을 적용(Virtual Enclave)하여 논리적으로 망을 분리 사용함. 또한, 전체 또는 일부 물리적 보안장비를 논리적(가상화) 보안장비로 대체하여 운용 필요
  * 미군 블랙코어, 민간 VPN과 유사
  - 망관리체계(NMS) 통합·고도화: 전달망별 또는 체계망별 운용중인 NMS를 단일의 NMS로 통합하고, 단순 모니터링 및 분석 수준에서 원격제어가 가능한 수준으로 고도화 필요.
  - 외부망 연결 확장: 향후 인터넷, 상용 모바일망, 퍼블릭 클라우드 등 외부망과의 연결 확장 운용 필요. (미군처럼 Access Point를

통해 향후 인터넷, 상용 모바일망 연결)

- 통합 단말 운영
  - 하나의 단말기를 사용하여 비도가 다른 다수의 네트워크나 체계를 동시 접근 필요.

- 공통기반구조/서비스/응용 통합
  - 체계별 공통기반구조, 서비스, 응용을 수행 중이나, 통합데이터센터에서 클라우드 서비스로 통합·공유 필요.

- 보안 통합 및 고도화
  - End-to-End 암호화: 현행 회선(Link)방식의 암호화 제거(대체)하고 E2E 암호화 필요.
  - 네트워크 보안장비 구축: 체계별/부대별 다수의 보안장비를 통합하고, 네트워크 보호를 위해 보안장비 추가 구축(외부망 연결 대비) 필요.
  - IdAM 통합: 전군 사용자/단말에 대한 인증 관리와 신원(권한) 관리 서비스를 통합 운용필요.

<표 1> 미래 지휘통제체체 발전 방향(요구사항)

구 분	현 행	개 선
네트워크 운영	전달망 분리 운영	전달망 동시 통합
	체계별 분리 망	통합 물리망 구성 후 논리적 격리 운영
	NMS 분리 운영	NMS 통합 운영
	외부망 비 연결	외부망 확장 연결
단말 운영	체계별 단말 운영	통합 단말 운영
체계 구조	체계별 독립 구조	체계 구조 통합
보안 체계	Link 암호화	E-to-E 암호화
	체계별 보안장비	통합 보안장비 운영
	체계별 인증/권한 관리	통합 인증/권한 관리
클라우드 적용	없음	관리적·기술적 보안 기준 마련

또한, 앞서 언급한 바와 같이 지휘통제체계는 중앙집중형 클라우드 컴퓨팅 서비스 개념으로 구축이 예상되므로 클라우드 신기술에 대한 보안 요구사항이 반영되어야 한다.

국가·공공기관은 국가 정보보안 기본지침(제69조)에 따라 클라우드 시스템을 구축할 경우 '국가·공공기관 클라우드 컴퓨팅 보안 가이드라인'을 준수하고 중앙행정기관, 광역지방자치단체 등 상급기관에 보안성 검토를 의뢰하여야 하며, 국가정보원에 보안성 검토를 받도록 정하고 있다.

따라서 국방 클라우드 컴퓨팅 구축 시 보안 요구사항을 준수하여야 한다. 국방분야 클라우드 컴퓨팅은 군이 독자적으로 자원을 사용하며 통제권을 가지고 외부에서 접근이 불가하도록 완전한 "On-site Private 클라우드 컴퓨팅" 유형으로 구축하고 향후 서비스 개념 및 보안 기술 등을 고려하여 민간·공공 클라우드 컴퓨팅 개념으로 점진적 확장이 필요하며, 클라우드 컴퓨팅 시스템 구축 시 현행 정보체계의 보안 정책을 그대로 유지하면서 아래와 같이 클라우드 컴퓨팅의 고유 특성으로 인하여 발생할 수 있는 가상화된 자원에 대한 사용자간 공유로 발생할 수 있는 보안 위협 등에 대한 보안 통제 정책 마련이 필요하다.

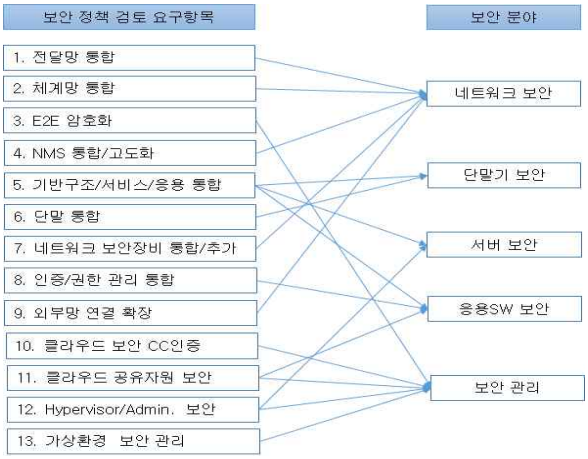
<표 2> 국방 클라우드 도입 시 보안 요구사항

구분	보안 검토항목	사 유
도입	CC인증 클라우드 제품 도입	도입시 안전성 확인
운용	클라우드 공유자원 목록 유지 및 무결성 유지	자원공유 시 보안관리
	2단계 인증, IP 필터링 등 하이퍼바이저 관리 및 관리자 콘솔 접근통제	하이퍼바이저 및 관리자 보안관리 강화
	가상환경 식별정보 관리, 이동저장매체 통제 및 가상 PC 보안관리	가상환경 보안관리 강화

3.2 미래 지휘통제체계의 보안 요구사항 분류

<표 1>의 軍 지휘통제체계 운영개념의 변화에 따라 개선이 요구되는 보안 정책 요구항목을 국방사이버안보훈령 부록의 "정보시스템 보호 구조의 5개 정보보호 분야"로 분류하여 한다. 이는 개별 요구사항이 중복을 제거하고 어느 분야에 규정으로 반영할 것인가 사전 검

토할 필요가 있다. (그림 2)와 같이 주어진 보안정책 검토 요구항목은 그 내용에 따라 5개 정보보호 분야에 1:1 또는 N:1로 매핑되는 경우도 있다.



(그림 6) 보안 요구사항을 5대 정보보호 분야와 매핑

3.3 보안 규정 개선의 필요성 분석

식별된 보안 정책 검토 요구사항에 대한 현행 규정 개선 필요성을 검토한 것이 <표 3>이다.

<표 3> 보안 요구사항의 규정 개선 필요성 분석

분야	보안 개선 요구사항	개선 필요성	
		중요성	영향성
네트워크 보안	•전달망 동시 통합운용	M	M
	•체계망 논리적(가상화) 분리 운용 •논리적(가상화) 보안장비 사용	H	H
	•망별 NMS를 단일 NMS로 통합 운용 •기능 고도화 (원격 제어)	H	H
	•네트워크 보안장비 통합/추가	H	H
	•외부망 연결 확장	M	H
단말 보안	•단일 통합단말기 운용	H	H
	•공통 기반구조(클라우드)와 통합/공유	M	M
서버 보안	•공통 기반구조(클라우드)와 통합/공유	M	H
	•클라우드 공유자원 보안	M	H
응용 SW 보안	•공통 기반구조(클라우드)와 통합/공유	M	M
	•인증/권한 관리 통합 운용	H	H
	•클라우드 공유자원 보안	M	M
보안관리	•외부망 연결 확장	M	H
	•End-to-End 암호화	H	H
	•클라우드 보안제품 도입시 CC인증	H	H
	•클라우드 공유자원 보안	M	M
	•클라우드 가상환경 보안 관리	M	M

[범례] H(High), M(Moderate), L(Low)

<표 2>의 규정 개선의 필요성은 요구사항의 중요도와 규정 개선시 영향성을 대상으로 NIST SP 800-37의 정보증 위험관리 평가시 영향 수준(Impact Level)을 기준으로 하였다.[5]

여기서 규정 개선 필요성이 H(High)이면 필요성이 높은 것을 의미하며 향후 규정 개정에 우선순위를 가지고 접근해야 할 항목이다.

4. 결 론

미래 지휘통제체계 구축을 위한 연구 중에 일부분으로 보안 규정 개선에 대해 연구하였지만, 정보체계 구축에 있어 보안 정책이 우선이며 보안 정책은 규정(훈령)으로 강제화하여 나타난다.

우리가 벤치마킹하는 미군의 경우는 보안 정책의 기본틀을 아키텍처화하여 각종 문서로 발간하여 구현의 용이성과 일관성을 유지하고 있다. 한국군의 지휘통제체계 구축 운영개념의 변화와 클라우드컴퓨팅 환경에서 보안 규정의 개선 요구사항을 식별하고 클러스터링하여 보안 요구사항을 정제하였다. 또한 각 보안 요구사항에 대해 중요성과 영향성을 기준으로 우선순위를 식별하였다.

향후 지휘통제체계는 전술이동망이 활용이 필수적이므로 무선이동망 보안 개선 요구사항을 추가 식별하고, 현행 규정의 조항별 개정여부 구체화 검토와 그 사유에 대해 추가 연구하는게 필요하다.

참고문헌

[1] 박규동 외, 한국군 지휘통제체계 발전방안 연구 최종보고서, pp. 6-7, 2017.6.30

[2] Danielle Metz, “Joint Information Environment Single Security Architecture (JIE SSA)”, May 12, 2014

[3] 국방부, '국방보안업무훈령', 국방부 훈령 제2258호, 2019.2.13

[4] 국방부, '국방사이버안보훈령', 국방부 훈령 제2234호, 2018.12.26

[5] Kevin Stine, “Vol.II: Appendices to Guide for

Mapping Types of Information and Information Systems to Security Categories", NIST SP 800-60 Vol.Ⅱ Rev.1, Aug. 2008

[6] Office of Deputy DoD CIO "Additional Information about the Joint Information Environment (JIE)", July 2017

[7] DISA, "Joint Regional Security Stack(JRSS)", 21 April 2016

[8] DISA, "Joint Regional Security Stack", 17 Jun 2015

[9] DISA, "Joint Information Environment Single Security Architecture(JIE SSA)", 12 May 2014

[10] Office of the DoD CIO, "Enterprise-wide Access to Network and Collaboration Services (EANCS) Reference Architecture Version 1.0", December 2009

〔저자소개〕

강 지 원 (Jiwon Kang)
1988년 2월 금오공과대학교 공학사
1997년 2월 연세대학교 컴퓨터과학 (정보보호 전공) 석사
2012년 8월 경기대학교 정보보호학 박사
2017년 9월～현재 세종대학교 컴퓨터 공학과 산학협력중점교수
email : jwkang@sejong.ac.kr

문 재 웅 (Jae Woong Moon)
2002년~2018년 (주)제이컴정보 CEO
2016년~2017년 한국정보보호산업협회 수석부회장
2019년 2월 세종사이버대학교 대학원 (공학석사)
2019년 3월～현재 세종대학교 정보보호학과 박사과정
email : jwmoon10@gmail.com

이 상 훈 (Sang Hoon Lee)
1978년 2월 : 한양대학교 전자공학과 공학사
1989년 2월 : 경북대학교 전자공학과 공학석사
2002년 2월 : 충북대학교 정보통신공학과 공학박사
1978년 3월~현재 : 국방과학연구소
<관심분야> C4I체계, 보안구조연구