

Online ISSN 2734-0376

정보처리학회지

Korea Information Processing Society Review

www.kips.or.kr



2023년 12월 | 제30권 제4호

국방 무기체계 사이버보안

사이버 복원력을 고려한 유무인 복합체계의 참조 아키텍처 설계

사이버 공격자 인프라 추적을 통한 선제적 대응방법

딥러닝 기반 SAR 표적 인식 모델의 적대적 공격에 대한 취약점 분석

FHSS 기반의 드론 무선통신 취약점 연구

적성국의 사이버 공격에 대응하는 위성통신 및 무선통신 시스템의 보안 강화 전략

국내 방산기술보호 통합실태조사와 미국CMMC 제도의 연계방안 연구

국방 RMF 연구 사례 분석



Bring digital to every person, home and organization
for a fully connected, intelligent world

www.huawei.com

Big Data



5G Network



Ai, Cloud



Smart Device



IoT



www.kips.or.kr



제 28대 임원명단

상임이사	장사익	문남미 (호서대학교)	이임영 (순천향대학교)	김준민 (제주대학교)	김현희 (동덕여자대학교)
	김정호 (배화여자대학교)	권태일 (빅센시스템즈(주))	권기룡 (부경대학교)	박종혁 (서울과학기술대학교)	박지수 (전주대학교)
	도경화 (고려대학교)	박능수 (건국대학교)	서승현 (한양대학교 ERICA)	유진호 (상명대학교)	윤주상 (동의대학교)
	백윤홍 (서울대학교)	임동혁 (광운대학교)	임유진 (숙명여자대학교)	한근희 (고려대학교)	장항배 (중앙대학교)
	이정원 (아주대학교)	최유주 (서울미디어대학원대학교)	김경아 (명지전문대학)	김미혜 (충북대학교)	
	강성희 (명지대학교)	권혁준 (순천향대학교)	이기용 (숙명여자대학교)	한성수 (강원대학교)	
	유동영 (홍익대학교)	윤혜정 (이화여자대학교)	김득중 (NIPA AI산업본부)	김성준 (Dell Technologies)	
	권혁상 (KCC정보통신(주))	권현오 (KISA)	김지훈 (썬케이티)	문정형 (한국정보산업연합회)	
	김세은 (한국생산성본부)	김정연 (KISDI)	방은주 (ZIDNet Korea)	신신애 (NIA)	
	민욱기 (ETRI)	박영민 (KLID)	이규복 (KETI)	이영상 (주데이터스트림즈)	
이사	유성철 (클로센(주))	이경록 (NIPA)	이준호 (한국화웨이기술(유))	이창열 (메타넷디지털(주))	
	이용우 (쌍용정보통신)	이재일 (중앙정보기술인재개발원)	조원영 (SPRI)	최호근 (한국T서비스산업협회)	
	전진욱 (슈퍼트컴퓨터)	전한수 (세립티에스지(주))	최병호 (KETI)	최종근 (썬마크에니)	
	최광남 (KISTI)	최광희 (KISA 사이버침해대응본부)	강지우 (숙명여자대학교)	고영웅 (한림대학교)	
	강승석 (서울여자대학교)	강운희 (백석대학교)	권순일 (세종대학교)	김경록 (호서대학교)	
	고진광 (순천대학교)	곽진 (아주대학교)	김병욱 (강릉원주대학교)	김성석 (서경대학교)	
	김기범 (국가보안기술연구소)	김미희 (한경대학교)	김승원 (전남대학교)	김영갑 (세종대학교)	
	김성환 (서울시립대학교)	김수균 (제주대학교)	김인철 (경기대학교)	김종길 (이화여자대학교)	
	김영종 (승실대학교)	김우성 (호서대학교)	김호원 (부산대학교)	노원우 (연세대학교)	
	김지희 (동국대학교)	김형준 (ETRI)	민홍 (가천대학교)	박광영 (승실대학교)	
협동부회장	민경식 (KISA)	민세동 (순천향대학교)	박정민 (KIST)	박진수 (순천향대학교)	
	박영호 (숙명여자대학교)	박용범 (단국대학교)	서영석 (영남대학교)	서화정 (한성대학교)	
	박진호 (동국대학교)	배호 (이화여자대학교)	송왕철 (제주대학교)	신동일 (세종대학교)	
	성연식 (동국대학교)	손태식 (아주대학교)	안상현 (서울시립대학교)	안진현 (제주대학교)	
	신병석 (인하대학교)	신승준 (호서대학교)	윤용익 (숙명여자대학교)	윤종희 (영남대학교)	
	원유재 (충남대학교)	유현창 (고려대학교)	이근호 (백석대학교)	이대원 (서경대학교)	
	이강만 (동국대학교)	이경현 (부경대학교)	이연 (인하대학교)	이원찬 (서울대학교)	
	이덕규 (서원대학교)	이승재 (선문대학교)	이종혁 (대구가톨릭대학교)	이현정 (중앙대학교)	
	이은서 (안동대학교)	이은영 (동덕여자대학교)	임신석 (배재대학교)	임승호 (한국외국어대학교)	
	이협근 (한국폴리텍대학)	이화민 (고려대학교)	정광식 (한국방송통신대학교)	정승원 (고려대학교)	
협동이사	장홍준 (강원대학교)	전재욱 (성균관대학교)	조준서 (한국외국어대학교)	조태남 (우석대학교)	
	정재화 (한국방송통신대학교)	정화영 (경희대학교)	추현승 (성균관대학교)	허준호 (한국해양대학교)	
	채상미 (이화여자대학교)	최민 (충북대학교)	황광일 (인천대학교)	황인준 (고려대학교)	
	홍성화 (목포해양대학교)	홍용근 (대전대학교)			
	Nasridinov Aziz (충북대학교)				
	김경원 (IPA)	김세종 (썬에스제이정보통신)	김윤철 (썬트라콤)	김은영 (썬투와이시스템즈)	
	문진현 (썬에이텍)	서준서 (메타넷디지털(주))	신재우 (비씨카드(주))	양현준 (썬지엘에이소시에이츠)	
	오경훈 (썬케이넷즈)	이윤재 (SK텔레콤)	이종근 (썬DST International)	이희천 (SK브로드밴드(주))	
	정은경 (한양대학교)	전상진 (서일대학교)	정문성 (SK브로드밴드(주))		

지회

강원지회	한성수 (강원대학교)	영남지회	서일수 (대구대학교)
제주지회	김형수 (제주한라대학교)	충청지회	김점구 (남서울대학교)
호남지회	이상준 (전남대학교)		

연구회 위원장

e-Bridge
IT정책
블록체인 기술 및 응용
소프트웨어공학
양자산업기술응용연구회
우정기술
인공지능
전산수학
정보통신응용
컴퓨터소프트웨어

이상근 (서강대학교)
오길록 (숭실대학교)
정영식 (동국대학교)
이은서 (한동대학교)
박종혁 (서울과학기술대학교)
정 훈 (ETRI)
전유부 (동국대학교)
박진홍 (선문대학교)
오진태 (ETRI)
박두순 (순천향대학교)

IT융합서비스
데이터과학연구회
빅데이터컴퓨팅
스토리지시스템
에너지그리드정보처리
웹3.0
전산교육
전자정부
지식 및 데이터공학
클라우드서비스

박석천 (가천대학교)
김현희 (동덕여자대학교)
이필규 (인하대학교)
신범주 (부산대학교)
박성준 (한전KDN)
민경식 (KISA)
김형진 (전북대학교)
이재두 (NIA)
진병운 (ETRI)
유진호 (상명대학교)

IT시니어봉사단

단 장 | 유기홍 (명지전문대학)
위 원 | 김홍진 (가천대학교)

여인갑 (한국IT전문가협회)

정진욱 (인터넷윤리실천협의회)

IT장학사업본부

본 부 장 | 이상범 (단국대학교)
부 본 부 장 | 박정호 (선문대학교)

인터넷윤리진흥본부

본 부 장 | 정진욱 (인터넷윤리실천협의회)
부 본 부 장 | 박정호 (선문대학교)

한민족IT평화봉사단

위 원 장 | 최 성 (남서울대학교)

선거관리위원회

위 원 장 | 강진모 (아이티센그룹)
위 원 | 강정호 (배화여자대학)
임유진 (숙명여자대학교)

길준민 (제주대학교)
장항배 (중앙대학교)

김현희 (동덕여자대학교)
최유주 (서울미디어대학원대학교)

이정원 (아주대학교)

연구윤리위원회

위 원 장 | 박지수 (전주대학교)
부 위 원 장 | 강정호 (배화여자대학교)
위 원 | 권혁준 (순천향대학교)
윤주상 (동의대학교)
간 사 | 유동영 (홍익대학교)

길준민 (대구가톨릭대학교)
임동혁 (광운대학교)

박종혁 (서울과학기술대학교)

신병석 (인하대학교)

인사위원회

위 원 장 | 문남미 (호서대학교)
위 원 | 최유주 (서울미디어대학원대학교)
간 사 | 유동영 (홍익대학교)

유진호 (상명대학교)

포상위원회

위 원 장 | 백윤홍 (서울대학교)
위 원 | 유진호 (상명대학교)
최유주 (서울미디어대학원대학교)

이정원 (아주대학교)

전임회장 운영위원회

위 원 장 | 이상범 (단국대학교)
위 원 | 성기중 (前 포스테이타)
오해석 (前 가천대학교)
최현규 (前 다우기술)
오경수 (前 제주도개발공사)
구원모 (전자신문)
이상현 (KCC정보통신)

조이남 (前 금융결제원)
김홍기 (케이티디에스)
이정배 (前 부산외국어대학교)
박석천 (前 가천대학교)
정영식 (동국대학교)
신용태 (숭실대학교)

오길록 (前 ETRI)
변재일 (더불어민주당)
금기현 (청년기업가정신재단)
조성갑 (세한대학교)
남석우 (인젠트)
강진모 (아이티센그룹)

정진욱 (前 성균관대학교)
김병기 (前 전남대학교)
정태명 (성균관대학교)
박두순 (순천향대학교)
김상훈 (한경대학교)

여성위원회

위원장	도경화 (고려대학교)			
부위원장	윤혜정 (이화여자대학교)			
위원	김경아 (명지전문대)	김미혜 (충북대학교)	김미희 (한경대학교)	김현희 (동덕여자대학교)
	문남미 (호서대학교)	박정민 (KIST)	성해경 (한양여자대학교)	송은하 (원광대학교)
	신은경 (날리자큐브)	안상현 (서울시립대학교)	안은영 (한밭대학교)	오수현 (호서대학교)
	윤희진 (협성대학교)	이유부 (성균관대학교)	이은영 (동덕여자대학교)	이정원 (아주대학교)
	이화민 (고려대학교)	임지영 (성서대학교)	조경은 (동국대학교)	최미정 (강원대학교)
	최수미 (세종대학교)	최유주 (서울미디어대학원대학교)	최은미 (국민대학교)	한영신 (성결대학교)
	한정란 (협성대학교)	홍헬렌 (서울여자대학교)		

30주년 준비위원회

위원장	최유주 (서울미디어대학원대학교)		
위원	김경아 (명지전문대)	김경록 (호서대학교)	유진호 (상명대학교)

학회지편집위원회

위원장	장항배 (중앙대학교)			
부위원장	유동영 (홍익대학교)			
위원	권혁준 (순천향대학교)	김대환 (울산대학교)	김수균 (제주대학교)	김윤기 (고려사이버대학교)
	김태규 (LIG넥스원)	박진수 (순천향대학교)	박필원 (동국대학교)	이기혁 (중앙대학교)
	이덕규 (서원대학교)	이송희 (한국폴리텍대학)	이원찬 (서울대학교)	이혜정 (순천향대학교)
	전미향 (수원여자대학교)	최연지 (이스트스프링자산운용코리아)	한성수 (강원대학교)	

JIPS 편집위원회

Editor-In-Chiefs	Jong Hyuk Park (Leading Editor) (Seoul National University of Science and Technology, Korea)	
	Vincenzo Loia (University of Salerno, Italy)	
Executive Editors	Doo-Soon Park (Soonchunhyang University, Korea)	Hamid R. Arabnia (The University of Georgia, USA)
	Young-Sik Jeong (Dongguk University, Korea)	
Advisory Editor	Han-Chieh Chao (National Ilan University, Taiwan)	Javier Lopez (University of Malaga, Spain)
	Jianhua Ma (Hosei University, Japan)	Giannong Cao (The Hong Kong Polytechnic University, Hong Kong)
	Laurence T. Yang (St. Francis Xavier University, Canada)	Mohammad S. Obaidat (Fordham University, USA)
	Mo-Yuen Chow (North Carolina State University, USA)	Qun Jin (Waseda University, Japan)
	Victor Leung (The University of British Columbia, Canada)	Witold Pedrycz (University of Alberta, Canada)
	Yang Xiao (The University of Alabama, USA)	
Managing Editor	Jisu Park (Jeonju University, Korea)	Neil Y. Yen (The University of Aizu, Japan)
Senior Editors	Houcine Hassan (Universitat Politècnica de Valencia, Spain)	Ka Lok Man (Xi'an Jiaotong-Liverpool University, China)
	Kim-Kwang Raymond Choo (The University of Texas at San Antonio, USA)	Luis Javier Garcia Villalba (Universidad Complutense de Madrid, Spain)
	Muhammad Khurram Khan (King Saud University, Kingdom of Saudi Arabia)	Muhammad Younas (Oxford Brookes University, UK)
	Naveen Chilamkurti (La Trobe University, Australia)	Jungho Kang (Baewha Women's University, Korea)
	Stefanos Gritzalis (University of the Aegean, Greece)	Youn-Hee Han (Korea University of Technology and Education, Korea)
	Yunsick Sung (Dongguk University, Korea)	
Associate Editor	Aditya Kumar Sahu (Amrita Viswa Vidyapeetham, India)	Aniello Castiglione (University of Salerno, Italy)
	Ankan Bhattacharya (Mallabhum Institute of Technology, Bishnupur, India)	Anna Formica (Istituto di Analisi dei Sistemi ed Informatica)
	Aziz Nasridinov (Chungbuk National University, Korea)	Byeong-Seok Shin (Inha University, Korea)
	Byoung-Soo Koh (Korea Creative Content Agency, Korea)	Byoungwook Kim (Gangneung-Wonju National University, Korea)
	Carlo Blundo (University of Salerno, Italy)	Changhao Plao (Chongqing University of Post and Telecommunication, China)
	Chao TAN (Tianjin University, China)	Deok Gyu Lee (Seowon University, Korea)
	Donghoon Kim (Arkansas State University, USA)	Dong-Hyuk Im (Kwangwoon University, Korea)
	Eunyoung Lee (Dongduk Women's University, Korea)	Fei Hao (Shaanxi Normal University, China)
	Fernando Bobillo (University of Zaragoza, Spain)	Goo-Rak Kwon (Chosun University, Korea)
	Hang-Bae Chang (Chung-Ang University, Korea)	Hoanh-Su Le (Vietnam National University Ho Chi Minh City (VNU-HCM), Vietnam)
	Hong-Jun Jang (Jeonju University, Korea)	Hossain Shahriar (Kennesaw State University, USA)
	Houbing Song (Embry-Riddle Aeronautical University, USA)	Hyejung Lee (Soonchunhyang University, Korea)
	Hyuk-Jun Kwon (Soonchunhyang University, Korea)	Hyunbum Kim (Incheon National University, Korea)
	Hyun-woo Kim (Baewha Women's University, Korea)	Imad Saleh (University of Paris 8, France)
	Jeonghun Cho (Kyungpook National University, Korea)	Jianbin Qiu (Harbin Institute of Technology, China)

Jiangshuai Huang (College of Automation, Chongqing University, China)
Jin Ho Park (Dongguk University, Korea)
Jong-Kook Kim (Korea University, Korea)
Joon-Min Gil (Catholic University of Daegu, Korea)
Ki Yong Lee (Sookmyung Women's University, Korea)
Kwang-il Hwang (Incheon National University, Korea)
Leandros Maglaras (De Montfort University, UK)
Marek R. Ogliela (AGH University of Science and Technology, Poland)
Mikael Gidlund (Mid Sweden University, Sweden)
Misun Kang (Soonchunhyang University, Korea)
Mohsen Toorani (University of South-Eastern Norway, Norway)
Ping-Feng Pai (National Chi Nan University, Taiwan)
Sangdae Kim (Soonchunhyang University, Korea)
Seung-Ho Lim (Hankuk University of Foreign Studies, Korea)
Seungwon Kim (Chonnam National University, Korea)
Soo-Kyun Kim (Jeju National University, Korea)
Sungsuk Kim (SeoKyeong University, Korea)
TAEGUEN KIM (Soonchunhyang University, Korea)
Vimal Shanmuganathan (Ramco Institute of Technology, India)
Wenhai Qi (Qufu Normal University, China)
Yeong-Seok Seo (Yeungnam University, Korea)
Young B. Park (Dankook University, Korea)
Yunsik Son (Dongguk University, Korea)
Journal Secretary | Dongwann Kang (Seoul National University of Science and Technology, Korea)
Yeongwook Yang (Hanshin University, Korea)

Jinhong Kim (Pai Chai University, Korea)
Jiwoo Kang (Sookmyung Women's University, Korea)
Jong-myon Kim (University of Ulsan, Korea)
Jun-Ho Huh (Korea Maritime and Ocean University, Korea)
Kuljeet Kaur (École de technologie supérieure, Université du Québec, Montréal)
Kyungbaek Kim (Chonnam National University, Korea)
Liangtian Wan (Nanyang Technological University, Singapore)
Michael Hwa Young Jeong (Kyung Hee University, Korea)
Min Choi (Chungbuk National University, Korea)
Minwoo Jung (Kyungpook National University, Korea)
Nam-Mee Moon (Hoseo University, Korea)
Samadhiya Durgesh (National Applied Research Laboratories, Taiwan)
Sayed Chhattan Shah (Hankuk University of Foreign Studies Korea, Korea)
Seung-Won Jung (Korea University, Korea)
Shanmugasundaram Hariharan (Shadan Women's College of Engineering and Technology, India)
Stelvio Cimato (Università degli studi di Milano, Italy)
Sun-Young Ihm (Pai Chai University, Korea)
Trung Duong (Colorado State University-Pueblo, USA)
Wenbing Zhao (Cleveland State University, USA)
Yan Li (Inha University, Korea)
Yonghoon Kim (Silla University, Korea)
Yu-Dong Zhang (Eugene) (University of Leicester, UK)
Zeeshan Kaleem (COMSATS Institute of Information Technology, Pakistan)
Pradip Kumar Sharma (University of Aberdeen, UK)

컴퓨터 및 통신 시스템(KTCCS) 논문지 편집위원회

위원장	윤주상 (동의대학교)	신종필 (The University of Aizu)	이덕규 (서원대학교)	최종명 (목포대학교)
부위원장	백상현 (고려대학교)	Nipon Theera-Umporn (Chiang Mai University, Thailand)	김원태 (한국기술교육대학교)	문병인 (경북대학교)
위원	홍용근 (대전대학교)	김경백 (전남대학교)	박재성 (광운대학교)	송두희 (한영대학교)
	강윤희 (백석대학교)	박능수 (건국대학교)	이태규 (평택대학교)	이화민 (고려대학교)
	박광진 (원광대학교)	이종혁 (세종대학교)	최영배 (Regent University)	최현영 (University of Pennsylvania)
	윤종희 (영남대학교)	최성근 (충북대학교)	허 경 (경인교육대학교)	허석원 (Qualcomm Technologies)
	이훈재 (동서대학교)	한영선 (부경대학교)		
	한연희 (한국기술교육대학교)			
	Weifeng Su (BNU-HKBU United International College)			

소프트웨어 및 데이터 공학(KTSDE) 논문지 편집위원회

위원장	박지수 (전주대학교)	박승중 (Louisiana State University)	이 연 (인하대학교)	이종혁 (대구가톨릭대학교)
부위원장	김병욱 (동신대학교)	Ka Lok Man (Xi'an Jiaotong-Liverpool University)	고명숙 (부천대학교)	길준민 (대구가톨릭대학교)
위원	임종범 (평택대학교)	강지우 (숙명여자대학교)	김영갑 (세종대학교)	김영철 (홍익대학교)
	김미선 (순천향대학교)	김성식 (서경대학교)	김중호 (순천대학교)	김한성 (고려사이버대학교)
	김상근 (성결대학교)	김정아 (가톨릭관동대학교)	신종필 (The University of Aizu)	안진현 (제주대학교)
	김우열 (대구교육대학교)	배지훈 (대구가톨릭대학교)	이공주 (충남대학교)	이성욱 (한국교통대학교)
	김태근 (순천향대학교)	오호정 (전북대학교)	이혜정 (순천향대학교)	임동혁 (광운대학교)
	양영욱 (한신대학교)	이한성 (안동대학교)	전재욱 (성균관대학교)	정광식 (한국방송통신대학교)
	이찬행 (경기대학교)	장홍준 (전주대학교)	조용운 (순천대학교)	최종선 (숭실대학교)
	임선영 (배재대학교)	정재화 (한국방송통신대학교)		
	정영애 (선문대학교)			
	최현영 (University of Pennsylvania)			
	Miti Ruchanurucks (Kasetsart University)			
	Weifeng Su (BNU-HKBU United International College)			

2023년 12월호 특집 담당위원

특 집 위 원 | 김태규 (LG넥스원)

2023년 12월 | 제30권 제4호 |

▶ 권두언

“국방 무기체계 사이버보안” 적성국의 사이버 공격에 대해 우리의 무기체계는 안전한가? / 김태규 2

▶ 특집명: 국방 무기체계 사이버보안

사이버 복원력을 고려한 유무인 복합체계의 참조 아키텍처 설계 / 김동환 4

사이버 공격자 인프라 추적을 통한 선제적 대응방법 / 김혁준 13

딥러닝 기반 SAR 표적 인식 모델의 적대적 공격에 대한 취약점 분석 / 한학수, 김민재, 임경섭, 이예형, 허준범 19

FHSS 기반의 드론 무선통신 취약점 연구 / 강재구, 최병철 25

적성국의 사이버 공격에 대응하는 위성통신 및 무선통신 시스템의 보안 강화 전략 / 정진우, 윤상범 32

국내 방산기술보호 통합실태조사와 미국OMMC 제도의 연계방안 연구 / 장항배, 김선영 42

국방 RMF 연구 사례 분석 / 조광수, 김예준, 안정근, 김정현, 박지원, 김해나, 백근우, 김승주 50

▶ 정기간행물 목차안내 62

▶ 학회동정 67

▶ 게시판 82



“국방 무기체계 사이버보안”

적성국의 사이버 공격에 대해 우리의 무기체계는 안전한가?

4차 산업혁명 이후 다양한 사물이 연결되고, 현실 공간과 가상공간이 교집합을 이루고 있습니다.

초 연결 기술로 대군사 작전의 공간은 지상, 해상, 공중, 우주, 사이버 등 5대 전장으로 구성되어 있습니다. 미래전은 5대 전장의 구분이 없어지고 있으며 지상·해상·공중뿐만 아니라, 우주, 사이버까지 모든 무기체계가 연결되고 있습니다. 사이버전 무기체계와 물리적인 무기체계가 연동되고 소프트웨어 기반 전쟁으로 발전됨에 따라, 무기체계 사이버보안의 중요성은 더욱 강화되고 있습니다.

전쟁에 참여하는 감시정찰 무기체계에서 수집한 정보를 빅데이터/인공지능 플랫폼 기반의 통합된 지휘결심을 통해 최고의 작전 효과를 달성하기 위한 타격 무기체계에 명령을 하달하여 작전하는 JADC2(Joint All Domain Command and Control)의 개념이 확대되고 있습니다. 사이버 위협은 더 이상 사이버 공간에 한정되지 않고, 육, 해, 공, 우주 무기체계 영역까지 위협이 확대되면서, 모든 무기체계에 접속하여 해킹, 탈취, 장악이 가능해졌습니다. 그리고, 러시아-우크라이나 전쟁에서 증명되었듯이 전쟁에 참여하는 무기는 IP Network를 넘어 위성통신 및 무선통신으로 확대되고 있습니다. 이런 전장환경 변화에서 사이버보안의 중요성 급격히 증가하고 있으며, 고도화되는 사이버 공격이 군사 작전에 미치는 영향을 최소화하기 위해 무기체계의 사이버보안이 중요시 되고 있습니다.

무기체계의 무인화, 기동화, 자율화에 따라 분실이나 탈취의 위협이 증가하고 있습니다. 비인가자가 악의적인 목적으로 접근하는 탬퍼링에 의해 막대한 비용으로 어렵게 개발한 우리의 첨단 기술이 너무나 쉽게 유출된다면 막대한 국력의 손실이 아닐 수 없습니다. 또한, 최근에 K방산 수출이 증가하고 있습니다. 세계시장으로 발을 넓히는 대한민국 방위산업에게 수출용 무기체계의 기술 보호는 기본 사항입니다.

지능화/고도화 되고있는 적군 사이버부대의 사이버 공격에 선제적으로 대응하기 위해 “인공지능 기반의 알려지지 않은 사이버 공격 상황인식 및 분석”, “CTI를 활용한 공격 원점 추적”, “휘발성 데이터 수집을 통한 공격 흔적 분석”, “유무인 복합 무기체계의 사이버 보안”, “위성통신 및 무선통신 사이버보안”, “안티탬퍼링”, “RMF”, “CMMC” 등 다양한 기술이 연구되고 있습니다.

본 12월호는 정치적, 금전적 목적의 초중급 해커조직이 아닌 라자루스나 김수키와 같은 국가의 지원을 받는 적군 사이버부대의 공격수준까지 고려하고, 사이버전과 물리전이 연동되는 동맹국과의 합동작전을 수행하기 위해 무기체계 사이버보안을 강화하기 위해 “국방 무기체계 사이버보안, 적성국의 사이버 공격에 대해 우리의 무기체계는 안전한가?”라는 주제로 기획 준비되었습니다. 그 결과 “사이버 복원력을 고려한 유무인 복합체계의 참조 아키텍처 설계”, “사이버 공격자 인프라 추적을 통한 선제적 대응방법”, “딥러닝 기반 SAR 표적 인식 모델의 적대적 공격에 대한 취약점 분석”, “FHSS 기반의 드론 무선통신 취약점 연구”, “적성국의 사이버 공격에 대응하는 위성통신 및 무선통신 시스템의 보안 강화 전략”, “국내방산기술보호 통합실태조사와 미국 CMMC제도 연계방안 연구”, “국방 RMF 연구 사례 분석” 등과 같은 좋은 글들이 모집되었습니다. 본 특집호를 통해 제공된 “국방 무기체계 사이버보안” 내용이 민,관,군의 모든 관계자가 국가 안보의 중요성은 인식하고 기술을 발전시켜 나가는데에 도움이 되었으면 합니다.

감사합니다.

2023년 12월

LIG넥스원 사이버전자전개발단장 김 태 규

사이버 복원력을 고려한 유무인 복합체계의 참조 아키텍처 설계

김동한 (LIG넥스원)

목 차	1. 서 론	4. 유무인 복합체계의 참조 아키텍처 설계
	2. 무기체계 개발방법론 및 문제점	5. 결 론
	3. 참조 유무인 복합체계의 요구사항	

1. 서 론

현대전에서의 유무인 복합체계는 무기체계의 여러 형태중의 하나가 아니라 궁극의 목표가 되는 필수적인 메가 트렌드(Mega Trend)이다. 유무인 복합체계는 기술적으로는 인공지능 소프트웨어를 적용하여 MUM-T(Manned-Unmanned Teaming)의 개념을 구현한 체계이며[1], 전술적으로는 작전시간 동안 동적으로 킬체인을 변경하는 모자이크전(Mosaic Warfare)을 실현하는 물리적 실체라고 할 수 있다[2].

인공지능 기반의 소프트웨어 중심 체계인 유무인 복합체계의 이러한 특징은 반대로 사이버 복원력(Cyber Resilience)을 고려한 개발이 필수적으로 요구된다. 이러한 이유 때문에 무기체계 개발시 RMF(Risk Management Framework)[3]를 적용하기 위한 논의들이 이루어지고 있지만, 전통적으로 무기체계 개발은 높은 신뢰성을 요구하는 System-of-Systems을 개발하는 엄격한 절차와 기준을 포함하고 있다.

본 논문에서는 MBSE(Model-Based System

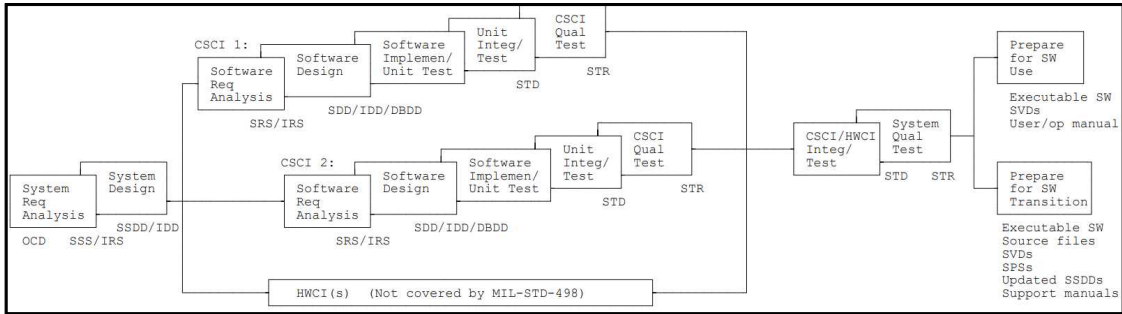
Engineering) 기반의 무기체계 개발방법론을 적용하여 사이버 복원력을 고려한 유무인 복합체계의 참조 아키텍처를 제안하고자 한다. 이를 통해 향후 개별적인 유무인 복합체계를 개발할 때 공통적으로 적용할 수 있는 가이드라인을 제시하고자 한다.

2장에서는 참조 아키텍처 개발을 위한 무기체계 개발방법론 및 문제점을 소개한다. 3장에서는 사이버 복원력을 고려한 참조 유무인 복합체계의 요구사항을 기능 및 비기능적 요구사항으로 구분하여 제안한다. 4장에서는 사이버 복원력을 포함한 다양한 품질속성을 반영한 최종 참조 아키텍처를 제안한다. 마지막으로 5장에서는 본 논문의 결론과 향후 연구 방향에 대해 제시하고자 한다.

2. 무기체계 개발방법론 및 문제점

2.1 무기체계 개발 프로세스의 소개 및 문제점

국내 무기체계 개발 프로세스는 MIL-STD-498[4]을 기반으로 하고 있다. MIL-STD-498은 현재 ISO 12207[5]에 통합되었지만, De-facto표준으로



(그림 1) MIL-STD-498의 무기체계 개발 프로세스

서 유럽과 미국의 방산업체에서 무기체계 개발에 적용하고 있다. (그림 1)은 MIL-STD-498에 기술된 대표적인 개발프로세스를 표현하고 있다. MIL-STD-498은 소프트웨어 시스템을 기반으로 개발 프로세스를 정의하고 있어 소프트웨어와 하드웨어가 통합된 체계관점에서의 분석으로부터 시작된다.

개발 프로세스는 체계분석 및 설계를 통해 체계를 구성하는 소프트웨어 형상항목(CSCI: Computer Software Configuration Item)과 하드웨어 형상항목(Hardware Configuration Item)을 식별하고 이들 간의 정적 및 동적인 관계를 설계하여 최종적으로 체계 아키텍처라는 산출물을 개발하도록 권고하고 있다. 그리고 각 형상항목별로 분석설계를 통해 최종 구현물을 제작하고 통합하여 시험평가를 실시하는 프로세스를 진행하며 개발이 진행된다.

MIL-STD-498에서는 이러한 절차들과 주요한 가이드라인을 포함하며, 가장 일반적인 폭포수형(Water-fall) 라이프사이클모델에서부터 점진적(Incremental), 진화적(Evolutionary) 라이프사이클모델까지 다양한 라이프사이클모델을 적용할 수 있다. 그러나 국내 무기체계 개발 매뉴얼[6]은 MI-STD-498을 기반으로 개발되었음에도 사이버 복원력과 같은 품질속성을 반영하기에는 여러가지 한계가 존재한다[7].

2.1.1 빈약한 요구사항의 관리

요구사항을 결정하는 것은 개발에서 있어서 가장 어려운 이슈 중에 하나이다. 시스템개발 프로젝트가 실패하는 원인으로 요구사항 관리의 실패가 큰 것으로 알려져 있다. 요구사항은 기능적 요구사항(Functional Requirements)과 품질속성으로 표현되는 비기능적 요구사항(Non-Functional Requirements)으로 크게 분류할 수 있다. 비기능적 요구사항은 기능을 수행하는 데 있어서 어느 수준으로 개발할 것인지에 대한 요구사항으로 품질에 가장 직접적인 영향을 주는 요구사항이다.

그러나 국내 무기체계 매뉴얼에서는 기능적 요구사항의 완전성과 일관성을 보장하기 어려운 문서 및 특정 사례 중심의 가이드라인을 제공한다. 또한 기능적 요구사항 분석에만 치중하고 비기능적 요구사항에 대한 분석 및 정의에는 매우 취약하다. 특히 명시적이지 않은 비기능 요구사항은 거의 정의되지 않아 테스트단계에서 이러한 정의되지 않은 요구사항이 새롭게 식별되어 최종적으로 구현된 시스템에 보이지 않는 결함을 내포하는 경우가 존재한다.

2.1.2 형식적인 품질관리

무기체계는 매우 높은 수준의 품질이 요구된다. 따라서 무기체계의 품질을 명확히 정의하고 엄격

하게 품질을 검증하고 확인하는 것은 매우 중요하다. 특히 요구사항을 검증 및 확인(Verification and Validation)이 가능하도록 정의하는 것은 품질관리에서 매우 중요하다. 따라서 IV&V(Independent V&V)를 통한 품질관리 활동을 강조하고 있다.

그러나 국내 무기체계 매뉴얼은 문서 존재유무 및 정성적인 체크리스트를 통해 주관적인 품질관리가 이루어지고 있어 품질의 정확한 관리가 매우 미흡하다. 실제 구현된 결과가 나오기 전까지는 개발과정에서의 시스템의 품질을 평가하는 것은 매우 어려운 실정이다. 문서 템플릿을 통해 상세한 가이드라인을 제공하고는 있지만 사실상 제공된 문서 템플릿이 한정된 분야에 국한되어 있고 무기체계에 적용하기 어려워 템플릿에 맞추다 보면 오히려 본질에서 벗어나 품질이 오히려 저하되는 경우가 많다.

2.1.3 기술부채의 증가

러시아-우크라이나 전쟁을 통해 상용기술의 신속한 활용이 승리의 요인이 되는 것을 직접 경험하였다. 전쟁에서 상용 드론의 활용, 저궤도 상용 위성을 이용한 정보 수집 및 통신, 모바일 앱을 통한 정보 교환 등은 기존의 전통적인 전쟁의 개념을 바꾸어 놓았다. 이것은 기술을 신속하게 전쟁에 활용해야 한다는 교훈을 우리에게 주고 있다. 특히 사이버공격에 대응하는 무기체계의 사이버 복원력이 OTA(Over-The-Air)를 통해 신속히 유지되는 것을 보면서 기술이 전장에 신속히 적용되는 것이 중요한 성공요인임을 알 수 있었다.

그러나 우리의 무기체계 개발은 전통적인 폭포수형 라이프사이클 모델에만 의존하고 있어 장기간의 개발기간이 소요되며, 운영 측면에서도 개발과 동일한 수준의 성능 개량 시간이 소요되어 기술부채가 매우 높은 무기체계를 개발하고 있다고 판단된다. 특히 기술문서 중심의 개발은 신속한

유지보수의 걸림돌로 작용하고 있으며, 동작하는 System Model을 기반으로 한 개발 및 유지보수가 중요하게 인식되고 있다.

2.2 PRISM 개발방법론

PRISM(Productive, Reliable and Intelligent Software Methodology)은 무기체계 개발매뉴얼의 문제점을 보완하기 위해 개발된 LIG넥스원의 소프트웨어 중심 무기체계 개발방법론이다[8]. MIL-STD-498의 무기체계 개발프로세스에 따라 다양한 라이프사이클모델을 지원하는 Model-Based System Engineering을 적용한 방법론으로 정량적으로 품질을 측정할 수 있도록 개발되었다.

PRISM은 SysML[9] 및 UML[10]이라는 모델링언어들을 이용하여 체계분석에서부터 소프트웨어 설계까지의 모든 단계를 정형화된 모델을 개발하는 모델링 가이드라인을 제시함으로써 MBSE를 지원한다. 본 논문에서는 PRISM을 적용하여 사이버 복원력을 고려한 아키텍처를 제안하며, 참조 아키텍처의 개발의 범위를 체계 아키텍처의 정적인 구조를 설계하기 위한 체계분석 및 설계 모델링으로 제한하여 소개한다.

3. 참조 유무인 복합체계의 요구사항

유무인 복합체계는 전투를 수행하기 위한 전투체계의 한 형태이다. 따라서 일반적인 작전주기를 설명하는 OODA(Observe, Orient, Decide, Act) Loop를 기반으로 우주, 공중, 지상, 해양 및 사이버의 5대 작전영역에서 공통적으로 적용할 수 있는 전형적인 킬체인을 기반으로 유무인 복합체계의 공통 요구사항을 도출하였다[11].

3.1 기능적 요구사항의 모델링

3.1.1 Context Model

체계 요구사항 분석은 시스템의 범위를 결정하는 것으로 시작한다. 시스템의 범위를 모델링한 분석모델이 Context Model이다. (그림 2)는 클래스 다이어그램을 사용하여 개발된 참조 유무인 복합체계의 Context Model이다.

흑백의 클래스로 표현된 “MUMT system”이 참조 유무인 복합체계를 의미하며 주변의 클래스들은 시스템의 액터(actor)로서 유무인 복합체계와 상호작용하는 외부 객체들이다. 그리고 상호작용은 객체 간의 관계(association)로 표현한다. 관계는 외부 객체들과의 인터페이스를 표현하며, 인터페이스를 통한 입출력되는 정보 또는 신호를 관계명으로 Interface Model에 별도로 모델링한다.

휴먼액터로 유무인 복합체계를 운영하는 운용자로서의 무인기통제관과 통제관에게 임무를 하달하는 상위 지휘관을 식별하였으며 시스템의 기술적 운영을 위한 체계관리자를 식별하였다. 그리고 연동하는 시스템을 2가지로 구분하여 지휘구

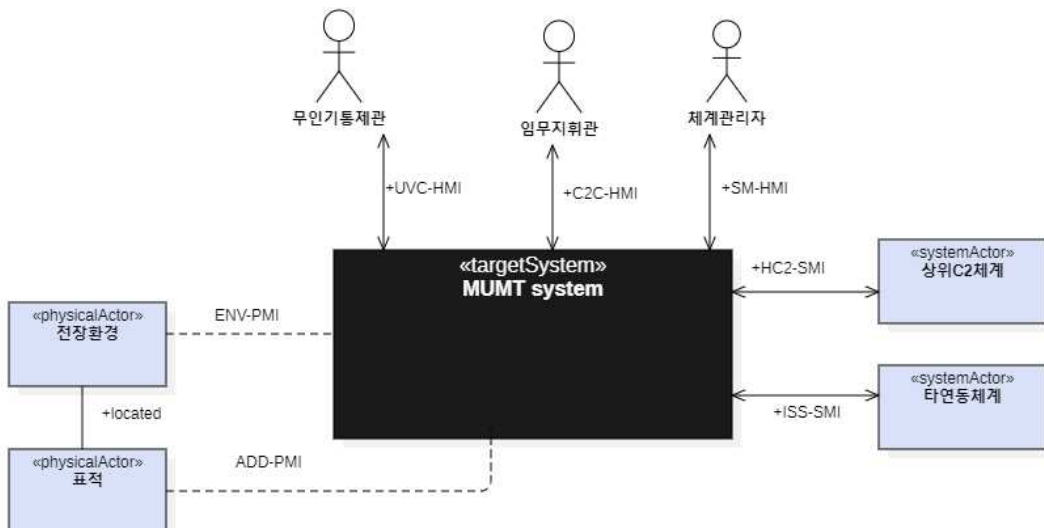
조에 따른 상위C2(지휘통제)체계와 지휘구조와 무관하게 연동하는 연동체계로 구분하였다. 나머지는 외부 환경 및 적의 위협을 표적이라는 객체로 모델링하였다.

3.1.2 Capability Model

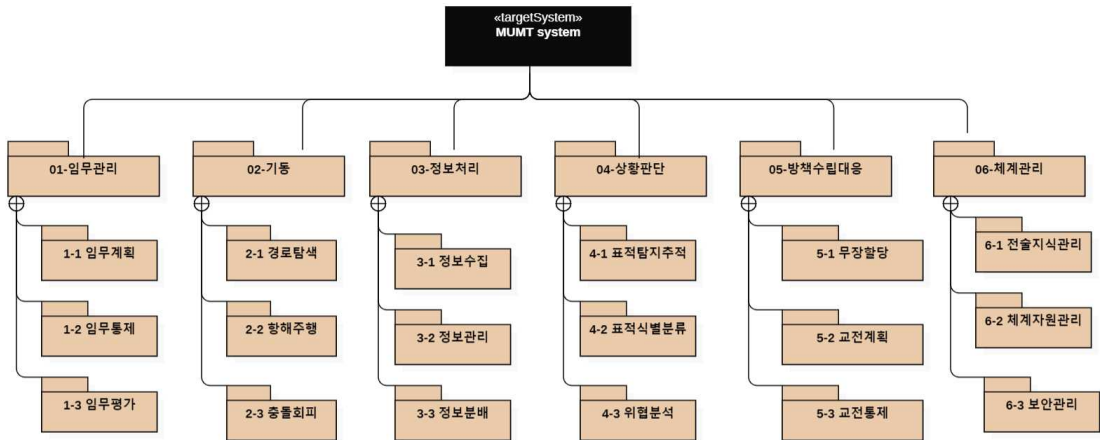
Capability Model은 체계가 수행할 기능 요구사항을 정의한 모델이다. 일반적으로 체계의 규모에 따라 체계수준에서의 최하위 기능을 결정하고 이들을 논리적으로 밀접한 관련이 있는 기능들을 통합하는 추상화를 통해 기능구조를 분석하고, 최하위 기능에 대해서는 세부적인 비즈니스 규칙을 유스케이스 시나리오(Use Case Scenario)로 정의한다. 일반적으로 추상화수준은 3단계로 제한하여 논리적 기능구조를 개발한다.

(그림 3)은 패키지 다이어그램으로 참조 유무인 복합체계의 기능구조를 표현한 Capability Model을 나타내고 있다. 최하위 패키지에는 하나 이상의 단위 기능들을 포함할 수 있다.

최상위의 추상화 기능들 중 정보처리, 상황판단, 방책수립대응은 킬체인을 구성하는 체계의 가



(그림 2) 참조 유무인복합체계의 Context Model



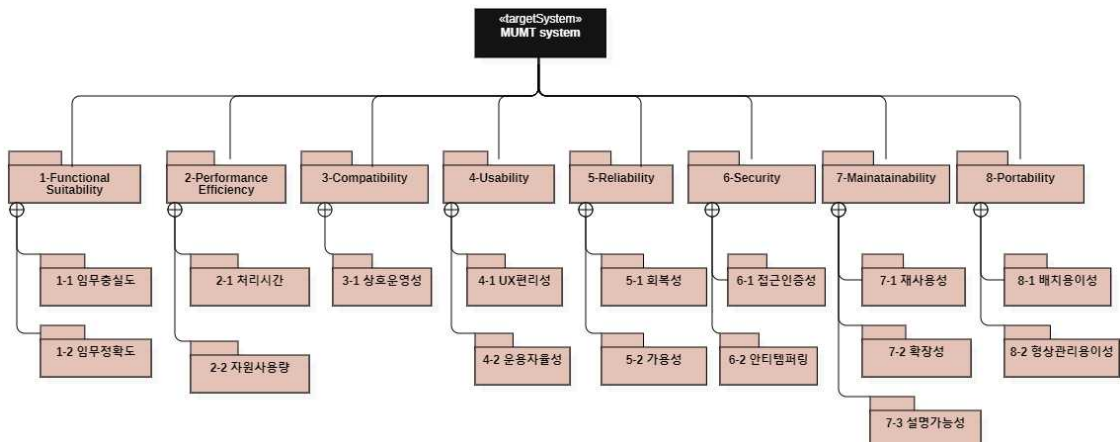
(그림 3) 참조 유무인 복합체계의 논리적 기능구조

장 핵심적인 전투기능이다. 정보처리는 외부로부터의 표적을 관찰하는 **Observe**의 기능, 상황판단은 표적을 식별하고 위협의 우선순위를 결정하는 **Orient**의 기능, 방책수립 대응은 교전을 위해 필요한 결정을 내리고 표적과의 교전을 수행하는 **Decide**와 **Act**의 기능을 의미한다.

그리고 임무관리는 임무 지휘관의 역할을 수행하는 기능들, 기동은 임무를 수행하는 무인체계가 이동과 관련한 기능들, 체계관리는 체계관리자를 지원하는 주요 기능들을 식별한 것이다.

3.3 품질 요구사항의 모델링

사이버 복원력과 직접적인 관련이 있는 신뢰성(Reliability) 및 보안성(Security)을 비롯하여 간접적으로 관계를 갖는 품질요구사항을 ISO 25000[12]의 8개의 품질속성을 기준으로 (그림 4)와 같이 패키지 다이어그램으로 모델링하였다. 사이버 복원력을 확보하기 위해서는 단순히 체계가 갖는 고유한 속성 뿐 만 아니라 체계를 운영 및 유지보수하는 관리적인 능력도 중요한 요인으로 인식되고 있다.



(그림 4) 참조 유무인 복합체계의 Quality Model

이러한 관점에서 8개의 제품과 관련된 품질의 대부분이 사이버 복원력과 직간접적으로 관계를 갖고 있다고 판단된다. 예를 들어 유지보수용이성(Maintainability)과 이식성(Portability)은 운용중인 시스템의 신속한 개선과 배포를 지원하여 급변하는 위협으로부터 체계의 생존성을 유지할 수 있는 중요한 속성이라고 할 수 있다. 최하위 기능의 경우 유스케이스시나리오를 작성하는 것과 같이 최종 품질속성에 대해서는 품질속성 시나리오(Quality Attribute Scenario)를 작성한다.

4. 유무인 복합체계의 참조 아키텍처 설계

4.1 사이버 복원력을 고려한 설계결정사항

아키텍처의 설계를 성공적으로 수행하는 것은 검증된 기존의 아키텍처 패턴(Pattern) 또는 스타일(Style)을 적용하는 것이다. 다시 말해 설계란 품질요구사항을 만족하기 위해 어떤 아키텍처 패턴을 적용할 것인가를 결정하거나 설계 가이드라

인을 기준으로 새로운 아키텍처 패턴을 식별하는 것이라 할 수 있다.

<표 1>은 목표로 하는 참조 아키텍처를 결정하기 위한 설계결정사항을 정리한 표이다. 설계결정사항을 개발한다는 것은 설계의 모든 의사결정을 수행하는 것이기 때문에 가장 중요한 활동이며 아키텍처는 이러한 설계결정사항의 부산물이라고 해도 과언이 아니다.

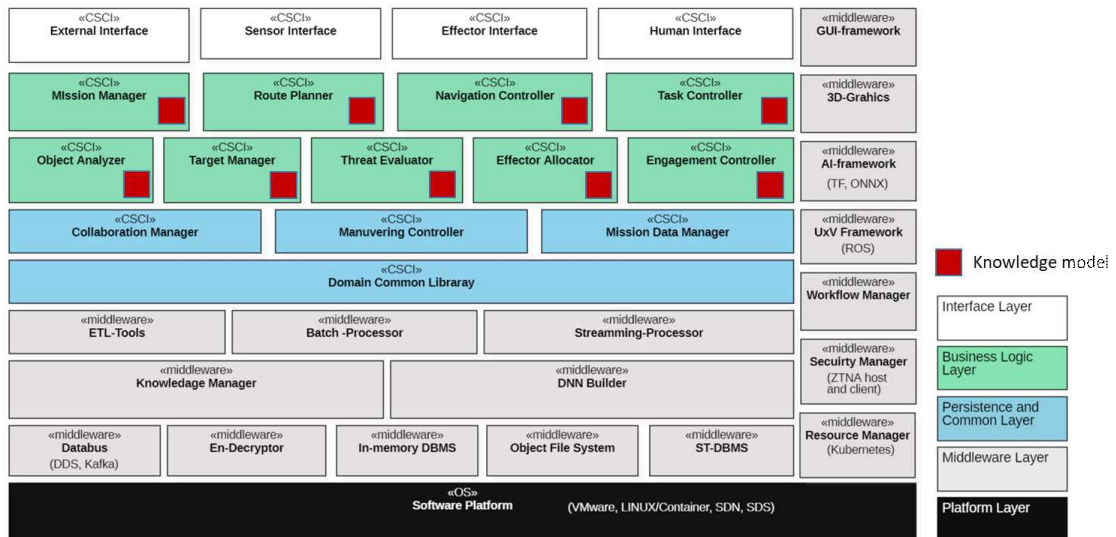
4.2 유무인 복합체계의 참조 아키텍처

4.2.1 소프트웨어 아키텍처

(그림 5)은 설계결정사항에 따라 최종 개발된 소프트웨어 레이어 아키텍처를 표현하고 있다. 제안한 아키텍처에는 본 논문에서 언급되지 않은 설계결정사항의 내용도 포함되어 있으나, 기본적으로는 크게 플랫폼 레이어, 미들웨어 레이어, 공통 및 데이터 담당 레이어, 임무서비스 순수기능을 담당하는 비즈니스 로직 레이어, 그리고 액터들과의

<표 1> 참조 아키텍처 설계를 위한 설계결정사항

아키텍처	구분	설계항목	설계결정사항	관련 품질속성
기술 아키텍처	컴퓨팅 플랫폼	임무분산구조	임무의 유형을 4개(coordination, collaboration, swarming, team)로 구분하여 분산구조 설계 [13]	운용자율성, 가용성, UX(User Experience)편리성
		SW 플랫폼	개방형플랫폼으로 쿠버네티스와 연동되는 Embedded LINUX Container 기반 플랫폼으로 설계[14]	재사용성, 회복성, 확장성, 배치용이성
		보안 플랫폼	TPM(Trust Platform Module) 또는 HSM(Hardware Security Module)[15]	접근인증성, 안티템퍼링, 상호운영성
	미들웨어 및 프레임워크	데이터베이스	실시간 Service-Oriented Architecture 패턴을 지향하는 DDS(Data Distribution Service) 적용[16]	확장성, 회복성 및 상호운영성, 실시간처리
		무인화 프레임워크	로봇분야에서의 개방형 프레임워크인 ROS2 적용[17]	확장성, 재사용성, 상호운영성, 임무정확도
		보안 프레임워크	Zero-trust architecture로 Software Defined Perimeter 구현[18]	접근인증성, 임무충실도, 상호운영성
응용 아키텍처	응용프로그램	레이어 아키텍처	논리적 기능구조를 기반으로 Interface layer, Business layer, Common 및 Persistence Layer를 구성	재사용성, 확장성, 형상관리용이성, 배치용이성



(그림 5) 참조 유무인 복합체계의 소프트웨어 아키텍처

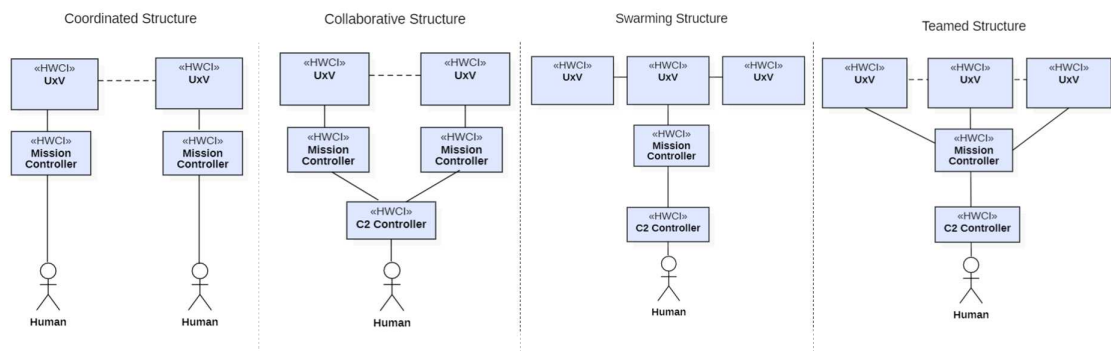
인터페이스를 담당하는 레이어로 구성되어 있다.

4.2.3 체계 아키텍처

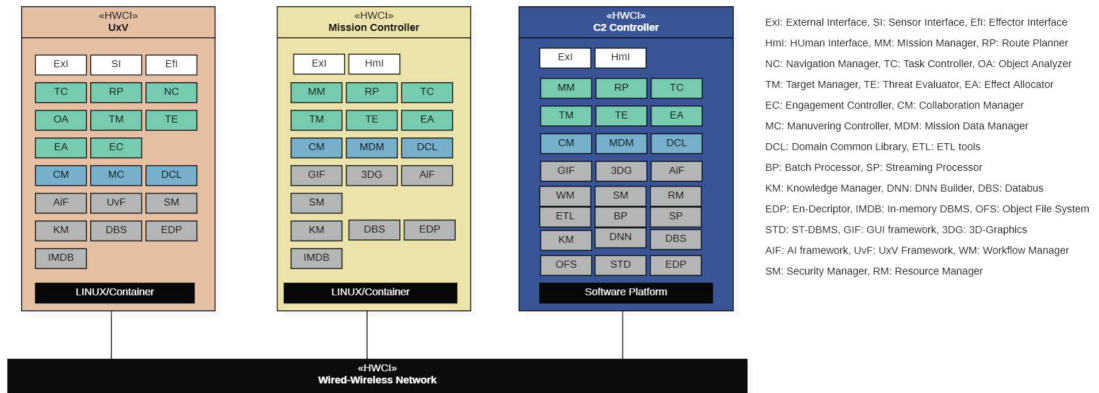
4.2.2 하드웨어 아키텍처

(그림 6)은 임무분산구조의 결정사항에 따라 4가지 형태의 하드웨어 아키텍처를 제시하고 있다. 실선의 연결은 특정 임무를 수행하기 위해 목적을 상호 공유하며 통제로 연결된 것을 의미하며, 점선의 연결은 통제가 아닌 단순 정보교환을 의미한다.

(그림 7)은 하드웨어 형상항목에 소프트웨어 형상항목을 배치하여 하드웨어와 소프트웨어가 통합된 최종 체계 아키텍처를 보여주고 있다. 미래의 유무인 복합체계는 Zero-Trust Architecture가 보장된 유무선 네트워크를 통해 특정 임무를 수행하기 위해 상호 연동하며, 사이버 복원력을 갖고 MUM-T를 성공적으로 실현하는 자율화 소프트웨어 형상항목들로 임무를 완수하게 된다.



(그림 6) 참조 유무인 복합체계의 하드웨어 아키텍처



(그림 7) 참조 유무인 복합체계의 체계 아키텍처

5. 결 론

미래의 무기체계는 인공지능을 적용한 소프트웨어 중심의 유무인 복합체계로 발전하고 있다. Software-Defined Weapon을 넘어 Software-Defined Warfare로 발전할 것이며, 이러한 발전은 오히려 무기체계에 대한 사이버공격의 위협이 증가될 것으로 예상된다. 이러한 이유로 RMF라는 사이버 위협에 체계적으로 대응하기 위한 체계개발 요구가 증대되고 있다.

본 논문에서는 RMF와 같은 사이버 복원력을 요구하는 가이드라인이 부재한 상태에서도 품질을 확보할 수 있는 개발방법론을 적용하여 사이버 복원력을 고려한 유무인 복합체계의 참조 아키텍처를 제안하였다. 제안된 참조 아키텍처는 유무인 복합체계의 공통적인 기능의 식별과 신뢰성, 보안성, 유지보수 용이성 등 사이버 복원력에 영향을 줄 수 있는 품질속성을 기반으로 설계되었다. 따라서 본 논문에서 제안한 참조 아키텍처 및 개발방법은 사이버공격에 강건한 기술적 및 관리적 요소들을 포함하고 있어, 특정 유무인 복합체계 개발에 가이드라인을 제시할 수 있을 것으로 기대된다.

향후 연구로는 RMF를 기반으로 추가적인 보안

통제항목을 기능적 및 비기능적 요구사항에 반영하여 개선된 아키텍처를 개발하는 것이다. 또한 유무인 복합체계는 인공지능을 적용하기 때문에 AI RMF[19]를 고려한 신뢰성(Trustworthiness)을 확보해야 하므로 이를 고려한 개선된 아키텍처의 개발도 향후에 연구해야 할 주제이다. 마지막으로 AI RMF를 고려할 때 제품의 품질속성 뿐만 아니라 데이터의 품질속성을 고려한 데이터 모델 및 아키텍처의 개발은 미래의 유무인 복합체계의 참조 아키텍처 연구에 또 다른 중요한 과제가 될 것으로 예상된다.

참 고 문 헌

- [1] Rajesh Uppal, DARPA(AI, XAI, and AI next) Developing "Third Wave" AI based adaptive military systems that are trustworthy, learn continuously, and explain their rationale, International Defense, Security & Technology, May 2021.
- [2] DARPA, DARPA Tiles Together a Vision of Mosaic Warfare, May 2018
- [3] NIST, Risk Management Framework for Information Systems and Organizations: A

- System Life Cycle Approach for Security and Privacy, NIST SP 800-37 Rev. 2, December 2018.
- [4] Department of Defense, Military Standard Software Development and Documentation, MIL-STD-498, February 1994.
- [5] ISO, Systems and software engineering — Software life cycle processes, ISO/IEC/IEEE 12207:2017, November 2017.
- [6] 방위사업청, 무기체계 개발 및 관리 매뉴얼, 방위사업청 매뉴얼 제2020-1호, 2020년 2월.
- [7] S. Lee, D. Kim, “Weapon Software: Challenge and Directions”, ICSE 2020 Korean Co-located Events, July 2020.
- [8] 김동환, 지능형 SW시스템 개발방법론, SDM-2023, 2023년 7월
- [9] Object Management Group, OMG System Modeling Language Specification, OMG SysML 1.6, December 2019.
- [10] Object Management Group, OMG Unified Modeling Language Specification, OMG UML 2.51, December 2017.
- [11] Frans Osinga, Science, Strategy and War-The Strategy Theory of John Boyd, January 2005.
- [12] ISO, Systems and software Quality Requirements and Evaluation, ISO/IEC/IEEE 25000:2014, March 2014.
- [13] Michael Woudenberg, George Walten-sperger, Troy Shideler, and Jerry Franke, “System Engineering of Autonomy: Frameworks for MUM-T Architecture”, DSAIC Journals Vol. 7, No. 3, Summer 2020.
- [14] Rob Woolley, Deploying Embedded Applications Faster with Containers, WNDRVR White paper, September 2021.
- [15] Microsoft, The right secure hardware for your IoT Deployment, Microsoft White pa-

per, November 2017.

- [16] Rajive Joshi, Data-Oriented Architecture: A Loosely-Coupled Real-Time SOA, RTI White paper, August 2007.
- [17] Vincenzo DiLuoffo, William R Michalson and Berk Sunar, “Robot Operating System 2: The need for a holistic security approach to robotic architectures”, International Journal of Advanced Robotic Systems, Vol. 15, Issue 3, May 2018.
- [18] Cloud Security Alliance, Software Defined Perimeter(SDP) and Zero Trust, CSA White Paper, 2020.
- [19] NIST, Artificial Intelligence Risk Management Framework, NIST AI 100-1, January 2023.

저 자 약 력



김 동 환

이메일 : kimdonghwan@lignex1.com

- 1984년 인하대학교 전산학과 (학사)
- 1986년 KAIST 전산학과 (석사)
- 1998년 KAIST 정보및통신공학과 (박사과정수료)
- 1995년 전자계산기조직응용기술사
- 2008년 정보시스템수석감리원
- 1986년~1995년 국방과학연구소 선임연구원
- 1995년~1996년 (주)한조엔지니어링 부장
- 1996년~2000년 대우통신(주) 부장
- 2000년~2003년 링크웨어(주) 상무
- 2003년~2009년 (주) 히어솔루션코리아 부사장
- 2010년~현재 LIG넥스원 C4ISTAR 연구개발2본부 연구위원
- 관심분야 : Dependable SW시스템 개발방법론 및 품질보증, 무인화 전투체계 및 자율주행 시스템

사이버 공격자 인프라 추적을 통한 선제적 대응방법

김혁준 (주)나루씨큐리티

목 차

1. 서 론
2. 현 사이버방어 체계의 문제점
3. 공격자와 방어자의 상호작용

4. 사이버 공격자 인프라 추적
5. 결 론

1. 서 론

사이버보안의 수준은 연결된 체계의 가장 낮은 수준으로 수렴하며 이는 국방 무기체계의 사이버 보안에도 동일하게 적용된다. 국내 방위사업의 22년 수주액은 약 95조원에 이르고 있으나 최근 발생하고 있는 방산기술 해킹사고는 대한민국의 사이버안보를 위협하고 있다. 최근 서울경찰청은 북한의 공격그룹 “안다리엘”이 국내 방산 업체 등을 상대로 해킹공격을 가해 레이저 대공 무기 등 관련 파일을 탈취하고, 방산 업체, 기술원, 연구소, 대학 제약회사, 금융기관 등을 공격하여 1.2테라바이트에 이르는 분량의 자료를 탈취 하였다는 수사결과를 발표하였고[1], 이는 21년 대우조선해양 및 한국우주산업주식회사를 등 대한민국 주요 방산업체를 대상으로 하는 조직적이고, 지속적인 사이버공격행위의 연속선 상에 있다. 이런 현실을 국방연구기관, 민간업체 및 소요군을 연결하는 국방무기체계 사이버보안 공급망 관점에서 본다면, 적성국의 사이버 공격에 대한 대한민국 무기체계 사이버보안 수준은 매우 취약한 것으로 판단된다.

2. 현 사이버방어 체계의 문제점

사이버보안체계의 문제점은 비단 대한민국에 한정된 것은 아니다. 세계 최고의 사이버보안 수준을 갖춘 것으로 알려진 미국의 사이버사령부 사령관이자, NSA 수장인 키스 알렉산더 장군은 미국 기업은 2012년 기준 매년 2천 5백억 달러의 지적재산권에 가치에 달하는 해킹사고가 발생하고 있으며 약 1,104억 달러에 달하는 사이버범죄 피해가 발생하며 이는 사이버공격으로 역사상 인류 최대의 부의 이동이 발생한 것이라고 말하였으며.[3] 이러한 현실은 결국 21년 5월 미국 백악관은 대통령 행정명령을 통해 위협정보 공유를 저해하는 요소를 제거하고, 연방정부와 클라우드 서비스 공급업체에 대한 제로트러스트 아키텍처 도입을 의무화 하였다. 2003년 미국 보안 엔지니어 클리프 리그 (Cliff Riggs)의 "Network Perimeter Security - Building Defense in-depth"의 출간 이후 지난 20년간 업계의 표준 여겨오던 경계선기반 방어는 진화하는 사이버공격에 대응하기에 적합하지 않다는 것으로 암묵적으로 선언하며 이의 대

3. 공격자와 방어자의 상호작용

에 50만대 이상의 봇넷을 구성하였다. 공격자는 이를 통해 대한민국의 인터넷 관문 중심의 경계선 기반 방어체계를 무력화 하여 모든 공격 대상 서버를 서비스거부상태에 빠지도록 하였다.

당시 공격자는 소프트웨어 공급망 공격을 통한 내부 자원 감염 전술로 관문중심의 경계선기반 방어체계를 무력화 하였고, 세션기반 공격전술을 차용하여 대역폭소진 방식의 서비스거부공격을 대응체계를 우회하였다. 7.7 DDoS 공격 발생 후 대한민국 정부는 공격에 대한 맞대응으로 국토해양, 국세, 국방, 외교, 경찰 등 5개 분야에 범정부 DDoS 대응체계 사업을 추진하여 HTTP 기반 서비스거부공격에 대한 국가적 방어체계를 수립 하였고 이는 2년후 다시 발생한 3.4 DDoS 공격을 성공적으로 방어하여 관련 공격에 대한 공격표면을 축소 하였고 국가정보보호백서에 따르면 7.7 DDoS 공격 후 만들어진 한국인터넷진흥원의 DDoS 대피소는 이후 발생한 800건 이상의 HTTP 세션기반 공격을 성공적으로 방어하고 있는 것으로 나타났다.

그림 1에서 초록색으로 표시된 공격은 새로운 공격 전술이 처음 사용된 침해사고로, 7.7 DDoS 공격은 소프트웨어기반 공급망 공격 및 공격자원 인프라의 구조적 사용이 처음 확인된 공격으로 이러한 전술은 웹하드 기반의 소프트웨어 공급망 공



(그림 1) 대한민국에서 발생한 주요 침해사고

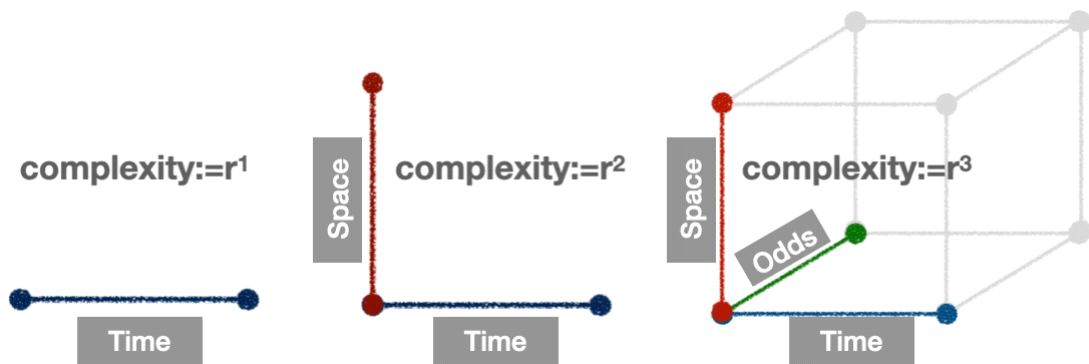
격 기법을 재 활용한 2011년 3.4 DDoS 공격, 정보 보호 소프트웨어에 대한 공급망 공격으로 방송, 금융 등 6개사 4만여대의 컴퓨터에 장애를 유발 하였고, 이는 2016년 다시 백신 소프트웨어에 대한 공급망 공격으로 발생한 국방망 해킹, 암호화 폐 거래소 빗썸에 대한 공급망 공격, 및 최근 발생한 맵식라인 취약점을 이용한 공급망 공격까지 동일한 전술이 반복적으로 사용 되고 있다.

2015년 11월 ADEX(서울 국제 항공우주 및 방 위산업 전시회) 운영본부를 사칭한 스피어피싱은 기존의 기술적 취약점 기반의 사이버공격 침투전 술을 넘은 사회공학적 해킹기법을 사용한 사례이 다. 이는 3.20 사이버테러이후 강화된 국내 사이버 방어체계를 우회하기 위한 것으로 기존의 공격이 경계선 기반 다단계 방어체계를 관통하는 형태를 가지고 있다면, 이메일은 이용한 공격은 당시 운 영되는 모든 방어체계를 우회하여 사용자에게 직 접 전달 되는 특징이 있으며, 기술적 방법으로 개 선될 수 없는 사회공학적 접근 방법을 사용하였다. 이때 사용된 피싱 공격은 8년간의 시간 동안 구조 적인 인프라를 갖추고 사용자의 인증정보를 탈취 하기 위해 지속적, 조직적으로 이루어지고 있다.

2022년 2월 발생한 카카오 클레이스왑 BGP Hijacking 공격은, 지역기반 방어체계로는 탐지가 불가능한 인터넷 라우팅 경로에 대한 공격으로 현

존하는 모든 사이버방어체계에서 탐지가 불가능 한 공격을 수행하여 사이버공격에 새 지평을 열었 으며 23년 7월 발생한 맵식라인 공급망 공격은 공 격목표에 대한 선택적 동작방식을 차용하여 원인 규명 방식의 방어체계를 무력화하며 시간적, 공간 적 방어공간의 확대에 확률 공간을 더하여 방어자 의 대응공간을 기하급수적으로 증가시키는 효과 를 발생시켰다.

그림 2는 사이버공격 전술의 변화에 따른 방어 공간의 확대를 나타내고 있다. 90년대 낮은 전송 속도 및 연구망 중심의 인터넷 환경에서는 발생하 는 모든 이벤트를 프린트로 출력하여 이를 육안으 로 확인하는 방식의 사이버공격을 탐지가 가능하 였으나[쿠크의 에그] 이후 연구망을 넘어 상업적, 개인적 컴퓨터 사용이 일반화 된 환경에서는 폭발 적으로 증가한 네트워크 및 컴퓨터 자원의 영향으 로 공격표면이 크게 증가 하였으며, 판테믹 이후 일반화된 글로벌 클라우드 서비스의 일반화, 재택 근무등의 변화로 기존의 방어체계의 선형적 확장 으로는 효과적 대응이 불가능게 되었다.이렇게 확 대된 공격 표면은 목표, 시기, 방법 선택에 이니셔 티브를 장악하고 있는 공격자에게는 다양한 선택 권을 주었으나 인터넷 기반 업무 환경의 확장과 더불어 시간적, 공간적 그리고 확률적 대응 공간 의 확대는 국가적 사이버방어전략의 수정을 요구



(그림 2) 공격전술 변화에 따른 방어 공간의 확대

하게 되었다

4. 사이버 공격자 인프라 추적

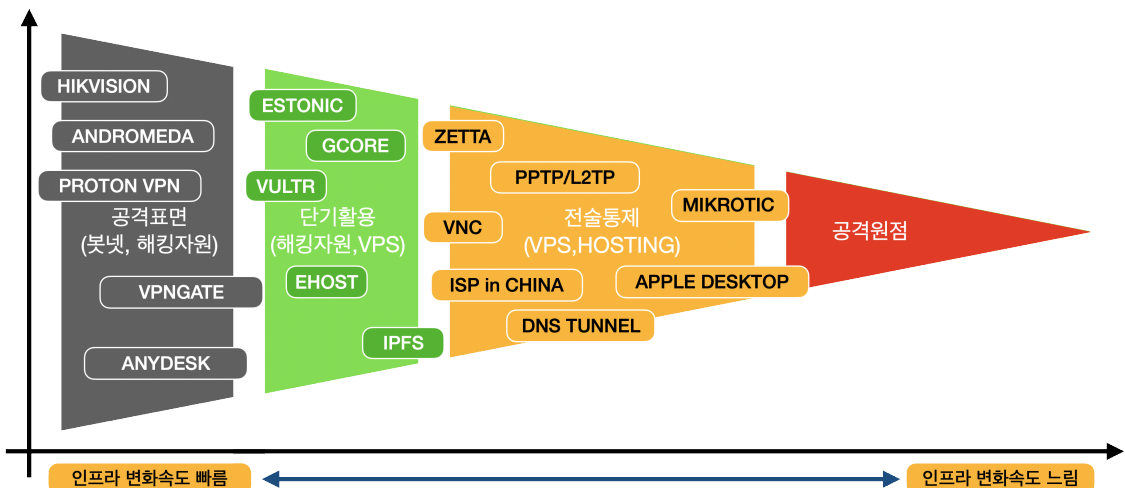
국가기반 사이버 공격그룹은 공격목표에 대한 지속적인 사이버작전 수행을 위해 인터넷 공간에 구조화된 공격 인프라를 구축하고 운영하고 있다. 사이버 작전운영을 위한 공격자원 배치는 원점, 전술통제, 단기활용 및 공격표면으로 구성된다. 이 그림에서 가장 왼쪽에 위치한 공격표면은 가장 휘발성이 높은 자원으로 개별 개체에 대한 추적이 어려우나 관리 체계를 갖추고 있어 관리 단위의 추적이 가능하다. 공격표면은 소유자와 이를 활용하는 그룹이 시점에 따라 상이하여 민감한 정보의 유통 보다는 IAB(Initial Access Broker)와 같이 정보수집, 권한확보 등의 초기 단계에 활용된다.

그림에서 녹색으로 표현된 단기활용자원은 해킹을 통해 확보한 국내 IT자원 및 특정 VPS 사업자 거점 및 국내에 위치한 해외 호스팅 사업자 자원을 활용하여 국내 수사기관의 및 방호체계의 탐지를 회피한다. 피싱 페이지, 악성코드 유포 혹은 최종 정보유출 경유지 구성 등 탐지 및 추적을 회

피하기 위한 목적의 작업에 활용된다. 마지막으로 전술통제 지점은 공격자 직접 운영하는 자원으로 국내 수사기관의 국가간 정보공유가 어려운 해외 지역 VPS 호스팅 사업자를 사용하거나 인터넷에 운용되는 특정 제품을 활용한 오버레이 통신망 구성/통제 등에 활용된다. 열거된 3개의 자원 중 휘발성이 가장 낮은 특성을 보인다.

국가기반 공격그룹은 알려지지 않은 공격기법을 활용하여 공격대상 네트워크에 침투하여 정보 탈취, 시스템파괴 등의 작업을 수행하지만 전통적 정보보호 방어체제로 이를 탐지하기 위해서는 지속적인 데이터 수집, 분석 등의 작업이 소요되며 또한 방어환경에 따라 지속적으로 변화하는 공격자의 전술(TTPs)로 대부분의 공격은 공격자의 침투목적이 발생한 이후 탐지되어 왔다.

국가기반 사이버 공격은 조직적 협업을 통해 이루어 지기에 이를 위해 인터넷 구간에 사이버공격 인프라를 구축하고 빠르게 변화하는 공격표면 정보만을 노출시키는 방법으로 방어체계의 탐지를 회피해 왔다. 그러나 수년간의 작업을 통해 구축된 공격 인프라는 공격원점에 가까워 질수록 그 변화 속도가 느려지는 특성이 있으며, 공격 원점



(그림 3) 공격자 인프라 구조도

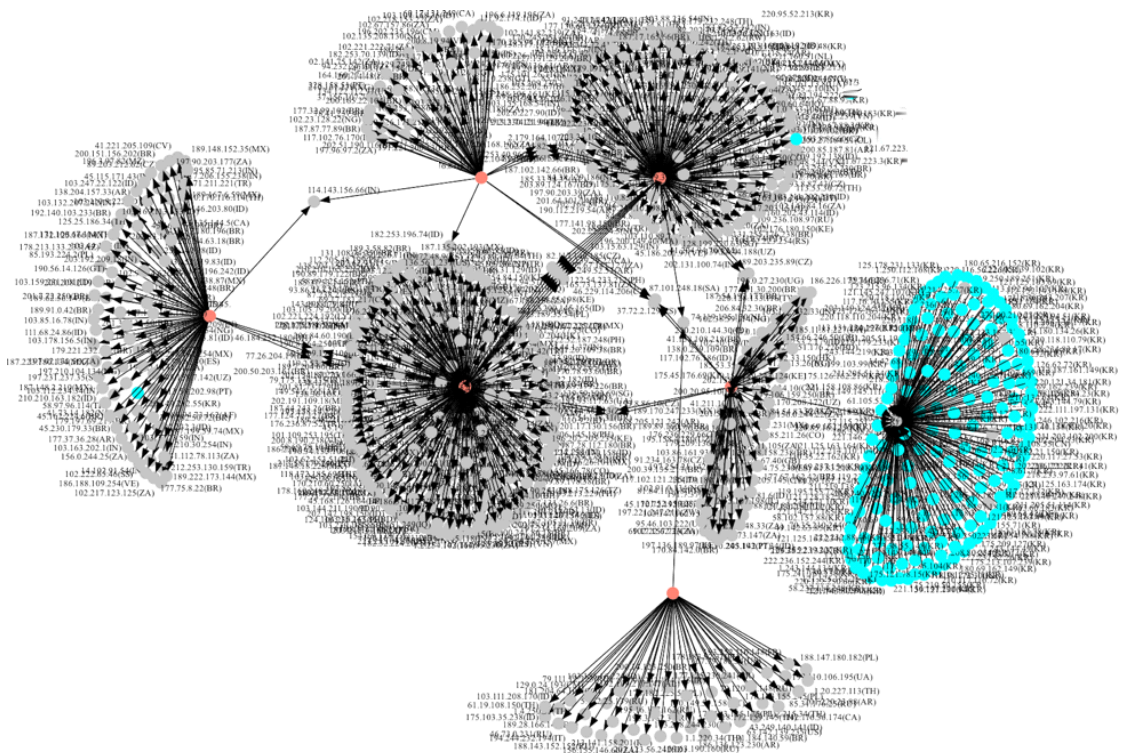
에 가까운 공격 인프라의 모니터링을 통해 공격자가 목적을 달성하기 전 이를 탐지하고 대응할 수 있다.

그림 4는 인터넷서비스제공자(ISP) 수준에서 수집된 네트워크 플로우 데이터 분석을 통해 공격 원점(그림에서 적색으로 표시)에서 타깃 네트워크(그림에서 청색으로 표현)까지의 연결도를 구성한 것으로 그림에 표시된 각각의 점은 연결지점의 공개 IP를 나타내며, 각 노드를 연결하는 선은 두 점 사이에 통신사실이 발생한 것을 나타낸다.

통신 플로우 기반의 연결도는 특정 공격 그룹이 인터넷 공간에 분산되어 있는 취약한 라우터에 불법적으로 획득된 권한을 이용해 구축한 오버레이 네트워크로 공격 원점에서 타깃 네트워크까지 구성된 경로를 보여주고 있다. 국가 기반 공격자는 임의의 시점에 공격 목적을 달성하기 위해 다수의

국내 기업/기관 네트워크를 점유하고 특정 시점 발생한 필요에 따라 실질적인 공격을 수행하는 것으로 분석된다. 따라서 이러한 공격 그룹의 사이버 공격 인프라를 모니터링하는 것으로 실질적인 피해가 발생하기 전 선제적인 대응이 가능할 것이다.

이러한 접근방법을 통해 현장에서 실질적인 대응이 가능하도록 하기 위해서는 먼저 인터넷공간에서 발생하는 통신사실에 대한 지속적인 수집, 사고분석을 통해 획득된 기초자료를 통해 구성된 공격자 인프라를 식별하기 위한 분석작업, 분석된 결과의 처리 및 시각화 과정이 지속적으로 이루어져야 하며 이를 통해 축적된 데이터를 기반으로 공격자 인프라 정보를 기반으로 하는 공격그룹 프로파일링 작업이 이루어 진다면 현재 운영되는 사이버 방어체계의 한계를 넘어 대한민국을 목표로



(그림 4) 통신 플로우 분석을 통한 공격자 인프라 추적

하는 국가기반 공격자의 인프라에 대한 선제적 대응이 이루어 질 수 있을 것이다.

5. 결 론

대한민국의 사이버 전쟁의 시작은 2009년 7월 7일 북한이 수행한 대규모 분산서비스거부공격에서 시작되었다고 볼 수 있으며 지난 13년 동안 국가기반 사이버 공격자는 대한민국에 대한 사이버 공격을 수행하기 위해 대한민국 내부는 물론 전 세계 각지에 매우 조직적으로 구성된 사이버 공격 인프라를 운영하고 있는 것으로 나타났다. 공격의 수준이 변화하면 이에 대응하는 방어 체계의 수준 역시 변화하여야 한다. 공격자는 방어 시야 밖에서 긴 준비 기간을 거쳐 침투 준비를 한 후 모든 것이 준비된 후 추적 가능한 모든 증거자료를 삭제한 후 공격의 마지막 단계인 목적 수행을 실행하기에 공격 라이프사이클 전 과정에 대한 대응 시야를 확보한다면 방어자는 비로소 공격자에 대한 대응 우위를 확보할 수 있게 된다.

빠르게 변화하는 공격 표면의 효과적 관리를 위해 인터넷 공간에 사이버 공격자들의 협업 도구로 구축된 사이버 공격 인프라는 공격 원점에 가까울수록 쉽게 변화할 수 없게 된다. 이러한 접근 방법을 통해 공격자 움직임과 공격 의도를 예측하고, 구축된 사이버 공격 인프라를 관측하는 것으로 기존의 수동적 대응방식에서 벗어나 선제적 사이버 공격 대응으로의 획기적인 전환이 이루어 질 수 있다

참 고 문 헌

- [1] 2023 국가정보보호백서, 2023-06-02, 4283
- [2] Riggs, Cliff, Network perimeter security: building defense in-depth, CRC Press,

2003.

- [3] Stafford, V. A. "Zero trust architecture." NIST special publication 800 (2020): 207.
- [4] <https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/>
- [5] <https://www.sedaily.com/NewsView/29YE4DM2W1>
- [6] <https://m.boannews.com/html/detail.html?idx=102043>
- [7] <https://www.donga.com/news/Politics/article/all/20210709/107867900/1>

저 자 약 력



김 혁 준

이메일 : joonkim@narusec.com

- 2003년 캐나다 알버타 주립대학교 컴퓨터공학(학사)
- 2003~2004년 캐나다 알버타 주립대학교 PINTS 센터 연구원
- 2004~2005년 RandomKnowledg Inc. 연구원
- 2005~2009년 한국인터넷진흥원 침해사고대응센터 연구원
- 2014~현재 정보통신망 침해사고 민관합동조사단 전문가
- 2017~현재 경찰청 사이버범죄 전문가 그룹 위원
- 2020~현재 성균관대학교 법과대학 과학수사와 검임교수
- 2010~현재 (주)나루씨큐리티 대표이사
- 관심분야: 사이버 보안, 침해사고대응, 위협 모델링, 인공지능, 빅데이터

딥러닝 기반 SAR 표적 인식 모델의 적대적 공격에 대한 취약점 분석*

한학수 · 김민재 · 임경섭 · 이예형 · 허준범 (고려대학교)

목 차	1. 서 론	4. Target과 Shadow의 취약점 분석
	2. SAR 표적 인식 모델의 적대적 공격 연구동향	5. 결 론
	3. SAR 이미지 영역별 취약점 분석	

1. 서 론

최근 CNN 기반의 SAR(Synthetic Aperture Radar) ATR(Automatic Target Recognition) 시스템이 사이버 보안 위협으로 간주되는 Adversarial example에 대한 관심이 높아지고 있다. SAR 이미지는 고유한 이미징 메커니즘으로 인해 광학 이미지와 다른 Target, Shadow 및 Speckle 영역이 있다. 최근 공격 패턴은 SAR-ATR에서 표적 지역 내에서만 섭동을 집중시키는 방식으로 개발되는데, 이는 물리적 구현이 표적 지역에서만 가능하기 때문이다. 더욱이 실제 시나리오에서는 CNN 기반 SAR-ATR에 접근 하기가 어렵기 때문에 적대적 사례에는 높은 전달성이 필요하다. 최근 연구에서는 SAR-ATR의 적대적 사례에 초점을 맞추고 물리적으로 실현 가능한 목표와 모델 간 전달 기능성의 중요성을 강조하고있다. 그러나 이전 연구에서는 SAR 이미지 영역 간 전송 가능성 및

취약점을 분석하는 데 제한이 있었다. 따라서 우리는 블랙박스 조건에서 전체 SAR 이미지에 대한 공격과 Target 집중 공격을 수행했다. 또한 이 논문에서는 다양한 SAR 이미지 영역(예: Speckle, Target 및 Shadow)이 전송 가능성에 미치는 영향을 조사한다. 향후 기술 발전을 예측하기 위해 Target과 Shadow 영역을 결합한 공격의 전이성을 분석했다. MSTAR 데이터 세트와 4가지 주요 공격 기법인 FGSM, CW, DeepFool 및 PGD를 사용하여 각 SAR 이미지 영역별 전이 공격의 취약점을 분석했다.

2. SAR 표적 인식 모델의 적대적 공격 연구동향

Synthetic Aperture Radar (SAR) 이미지는 지면이나 대상의 표면에 마이크로파를 발사하여 반사된 신호를 얻어 생성된 고해상도 레이더 이미지

※ 본 연구는 국방암호기술 특화연구센터(UD210027XD)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다

대[1]. SAR-ATR은 SAR 이미지에서 자동으로 대상을 식별하고 분류하기 위해 설계된 시스템으로, 군사, 지리학 및 민간 응용 분야에서 활용되고 있다[2].

최근 많은 연구자들은 적대적 예제를 실제 환경에서 Target 영역에 중점을 둔 공격 환경을 고려하여 개발했다. 이는 공격자가 적대적 예제에 필요한 변형을 물리적으로 생성할 수 있는 유일한 부분이기 때문이다[4,5,6]. 또한 실제 세계에서 공격자가 SAR-ATR의 CNN 모델에 접근하는 것은 불가능하므로, 블랙 박스 공격에 중점을 두었다[7]. 블랙 박스 공격에서는 공격자가 대상 모델의 입력과 출력에만 접근할 수 있다. 따라서 공격자는 대상 모델의 입력과 출력을 사용하여 서로 모델이라는 다른 모델을 훈련한다 [8]. 그런 다음 공격자는 서로 모델의 적대적 예제를 생성하여 대상 모델을 속인다. 전이성은 블랙 박스 공격에서 중요한 요소로, 대리 모델에서 생성된 적대적 예제가 대상 모델에 효과적으로 적용되는 것을 의미한다 [9-12].

2.1 적대적 공격

적대적 공격은 인간의 눈으로 감지하기에는 매우 작은 변형을 입력 이미지에 삽입하여 모델이 샘플을 잘못 분류하도록 한다[14].

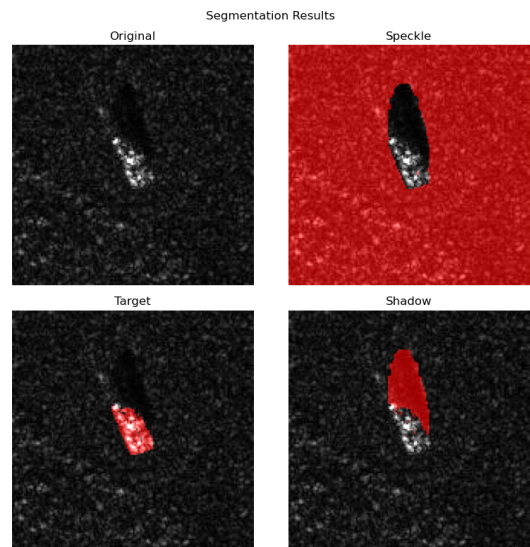
위의 공격 모델에서 공격자는 대상 모델의 구조, 입력, 출력 및 가중치에 대한 정보가 필요하며, 이 공격 상황은 화이트 박스로 간주된다. 그러나 블랙 박스 모델에서는 공격자가 대상 모델의 입력과 출력에만 접근할 수 있다[8]. 직접적으로 대상 모델을 공격하는 대신 공격자는 대리 모델을 별도로 훈련한다. 그 다음에는 대리 모델에 대해 화이트 박스 공격을 수행하고, 생성된 적대적 예제를 사용하여 대상 모델을 속이게 된다.

2.2 SAR ATR에서의 적대적 공격

최근에는 SAR-ATR 도메인에서 물리적으로 실현 가능한 공격 방법 및 현실적인 공격 시나리오에서 발생할 수 있는 블랙 박스 공격에 중점을 둔 연구가 진행됐다[4-7]. 실제 공격 환경을 고려하여 전자파 산란 반응 형태의 적대적 교란을 생성함으로써 물리적으로 공격 가능한 대상 영역에 초점을 맞춘 공격 방법이 개발되었다.[6]

또한, SAR-ATR을 위해 생성된 적대적 예제들은 장치에서 포착된 후 교란을 수정할 수 없기 때문에 CNN 모델들 간에 높은 전이성을 가져야 한다[3]. 또한, 실제 세계에서 공격자들이 CNN 기반 SAR-ATR에 직접 접근하기 어려워 SAR-ATR에서 전이성은 필요하다. 따라서 최근 노력에서는 전이성을 개선하기 위한 공격 방법들이 개발되었다.[5]

본 논문에서는 미국 방위고등연구계획국(DARPA)에서 공개한 MSTAR 데이터 세트로 실험을 진행했다. 8개의 CNN 모델은 2747개의 gray scale 이미지로 훈련 되었고, 입력 이미지의



(그림 1) SAR 이미지 분할 구역

크기는 224×224 이다. 대리 모델인 VGG16의 그라디언트를 사용하여 FGSM($\epsilon=8/255$, iteration=1), CW(iteration=50), PGD($\epsilon=8/255$, iteration=10), DeepFool(iteration=50)에 대한 섭동을 생성하였고 Target, Shadow, Speckle로 분할한 이미지에 생성된 노이즈를 입혔다. 각 영역의 적대적 사례를 7가지 모델에 공격하여 전송 공격 성공률을 측정하였다. (그림 1)은 SARBake[13]를 이용하여 분할한 이미지이다.

3. SAR 이미지 영역별 취약점 분석

<표 1>은 VGG16 모델을 대리 모델로 사용하는 블랙 박스 공격이 7개 모델에 적용될 때의 전이 공격 성공률을 보여준다. 또한, 네 가지 알고리즘을 사용하여 블랙 박스 공격이 구현되었으며 ALL, Target, Shadow, Speckle로 나누어 각 공격에 대한 전이 공격 성공률을 기록했다.

<표 2>는 네 가지 공격 각각에 대한 평균 전이

<표 2> ALL Pixel과 Target의 평균 전송 공격 성공률(%)

SORT		Average
FGSM	ALL	70.5
	Target	5.55
CW	ALL	5.92
	Target	4.36
DeepFool	ALL	7.31
	Target	4.4
PGD	ALL	62.37
	Target	5.21

공격 성공률을 나타낸다. 각 공격 알고리즘은 ALL 픽셀과 Target에서 다른 전이 공격 성공률을 보여준다. FGSM과 PGD 공격에서 ALL 픽셀에 대한 평균 전이 공격 성공률은 Target보다 61.05% 높았다. CW와 DeepFool 공격에서는 ALL 픽셀에 대한 평균 전이 공격 성공률이 Target보다 2.23% 높았다.

또한, <표 3>은 각 영역이 전이성에 미치는 영향을 보여준다. Speckle의 평균 전이 공격 성공률

<표 1> Target, Shadow, Speckle, ALL Pixel에 대한 전송 공격 성공률(%)

SORT		Alexnet	Densenet	Inception	Mobile	Resnet50	Resnext	Shuffle
FGSM	ALL	40.44	83.43	66.07	85.31	79.18	69.27	69.79
	Target	4.47	1.16	4.81	6.49	15.41	3.59	2.89
	Shadow	14.65	4.28	13.67	20.34	15.08	10.92	10.63
	Speckle	32.47	78.87	63.11	86.21	78.2	65.94	67.52
CW	ALL	3.85	0.72	5.34	8.52	15.47	4.01	3.5
	Target	2.5	0.63	3.93	5.14	13.55	2.68	2.08
	Shadow	2.84	0.67	4.21	6.22	13.66	3.28	2.5
	Speckle	2.56	0.61	4.24	5.82	14.2	2.83	2.28
Deepfool	ALL	5.57	0.95	6.68	11.37	15.56	5.67	5.39
	Target	2.48	0.73	4.04	5.18	13.55	2.68	2.12
	Shadow	3.73	0.63	4.88	7.86	13.85	4.38	3.58
	Speckle	2.6	0.61	4.15	5.76	14.22	3.16	2.43
PGD	ALL	40.37	64.95	58.39	82.76	70.35	56.69	63.06
	Target	3.89	1.02	4.7	5.98	14.61	3.32	2.95
	Shadow	13.75	4.07	11.62	18.35	15.09	8.87	8.49
	Speckle	31.33	59.12	52.83	79.74	67.93	50.1	54.3

〈표 3〉 Target, Shadow, Speckle의 평균 전송 공격 성공률(%)

SORT		Average
FGSM	Target	5.55
	Shadow	12.8
	Speckle	67.47
CW	Target	4.36
	Shadow	4.77
	Speckle	4.65
DeepFool	Target	4.4
	Shadow	5.56
	Speckle	4.7
PGD	Target	5.21
	Shadow	11.46
	Speckle	56.48

이 33.32%로 가장 높고, 그 다음이 Shadow 8.64%, Target 4.88% 순이다.

우리의 실험은 SAR 이미지의 Speckle, Target, Shadow가 다른 전이성을 가진다는 것을 확인했다. 각 SAR 이미지 영역에 대한 전이성이 가장 높았던 순위는 Speckle, Shadow, Target 순이었다.

4. Target과 Shadow의 취약점 분석

또한, 우리는 대상 영역에 물리적으로 교란을 생성하는 것이 그림자 영역에 영향을 미칠 것이라고 생각했으며, 그림자 영역에도 의도적으로 교란을 생성할 수 있을 것이라고 생각했다. 따라서, 우리는 대상과 그림자에 의도적 교란을 생성하는 새로운 공격의 전이성에 대해서도 실험을 진행했다. 표 4는 대상과 그림자의 결합된 영역에 대해 일곱

모델에 대한 블랙 박스 상황에서 네 가지 공격의 전이 공격 성공률을 보여주며, Target과 Shadow의 평균 전이 공격 성공률은 10.46%로 Target만 공격했을때보다 5.58% 높게 나타났다.

Target과 Shadow에 동시에 적대적 공격을 수행함으로써 전이성을 높일 수 있다. 최근 대상 중심의 적대적 공격에 충분한 전이성을 보장하기 위해, Target뿐만 아니라 Shadow에도 적용할 수 있는 방법을 고안함으로써 더 전이 가능한 적대적 공격 방법이 개발될 수 있다.

5. 결 론

이 논문에서, 우리는 블랙박스 조건에서 SAR 이미지를 All 픽셀, Target, Shadow, Speckle 영역으로 나누어서 영역별 전이 공격성의 취약점을 분석했다. 결과적으로, 공격이 대상에만 집중될 때, 전체 SAR 이미지에 대한 공격과 비교하여 모든 네 가지 공격에서 전이 공격 성공률이 감소하는 것으로 나타났다. 또한, 우리는 SAR 이미지 내의 다른 영역(Target, Speckle, Shadow)이 전이성에 미치는 영향을 분석하고, 영역에 따라 전이성이 다름을 확인했으며 Speckle 영역에서 공격을 하는 것이 가장 높은 전이성을 갖는다는 것을 확인하였다.

또한, 우리의 실험은 대상 영역만 공격하는 것과 비교하여 Target과 Shadow 영역을 동시에 공격할 때 물리적 공격이 가능한 경우 전이성에 더 취약함을 확인했다.

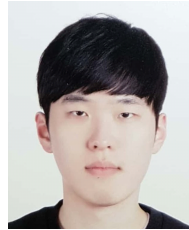
〈표 4〉 Target & Shadow 전송 공격 성공률(%)

SORT	Alexnet	Densenet	Inception	Mobile	Resnet50	Resnext	Shuffle
Target+Shadow	11.06	3.47	10.92	15.18	15.88	8.77	7.94
Target	3.34	0.89	4.37	5.7	14.28	3.07	2.51

참 고 문 헌

- [1] Anagnostopoulos, Georgios C. "SVM-based target recognition from synthetic aperture radar images using target region outline descriptors." {Nonlinear Analysis: Theory, Methods & Applications} 71.12 (2009): e2934-e2939.
- [2] Kechagias-Stamatis, Odysseas, and Nabil Aouf. "Automatic target recognition on synthetic aperture radar imagery: A survey." IEEE Aerospace and Electronic Systems Magazine 36.3 (2021): 56-81.
- [3] Li, Haifeng, et al. "Adversarial examples for CNN-based SAR image classification: An experience study." IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing 14 (2020): 1333-1347.
- [4] Peng, Bowen, et al. "Scattering model guided adversarial examples for SAR target recognition: Attack and defense." IEEE Transactions on Geoscience and Remote Sensing 60 (2022): 1-17.
- [5] Qin, Weibo, Bo Long, and Feng Wang. "SCMA: A Scattering Center Model Attack on CNN-SAR Target Recognition." IEEE Geoscience and Remote Sensing Letters 20 (2023): 1-5.
- [6] Zhou, Junfan, et al. "Attributed scattering center guided adversarial attack for DCNN SAR target recognition." IEEE Geoscience and Remote Sensing Letters 20 (2023): 1-5.
- [7] Peng, Bowen, et al. "An Empirical Study of Fully Black-Box and Universal Adversarial Attack for SAR Target Recognition." Remote Sensing 14.16 (2022): 4017.
- [8] hakraborty, Anirban, et al. "Adversarial attacks and defences: A survey." arXiv pre-print arXiv:1810.00069 (2018).
- [9] Su, Jiawei, Danilo Vasconcellos Vargas, and Kouichi Sakurai. "one pixel attack for fooling deep neural networks." IEEE Transactions on Evolutionary Computation 23.5 (2019): 828-841.
- [10] Xiao, Chaowei, et al. "Generating adversarial examples with adversarial networks." arXiv preprint arXiv:1801.02610 (2018).
- [11] Xie, Cihang, et al. "Improving transferability of adversarial examples with input diversity." Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2019.
- [12] Wang, Xiaosen, and Kun He. "Enhancing the transferability of adversarial attacks through variance tuning." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2021.
- [13] Malmgren-Hansen, David, and Morten Nobel-J. "Convolutional neural networks for SAR image segmentation." 2015 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT). IEEE, 2015.
- [14] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, "Intriguing Properties of Neural Networks," in ICLR, 2014.
- [15] Goodfellow, Ian J., Jonathon Shlens, and Christian Szegedy. "Explaining and harnessing adversarial examples." arXiv pre-print arXiv:1412.6572 (2014).
- [16] Moosavi-Dezfooli, Seyed-Mohsen, Alhussein Fawzi, and Pascal Frossard. "Deepfool: a simple and accurate method to fool deep neural networks." Proceedings of the IEEE conference on computer vision and pattern recognition. 2016.

- [17] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards Deep Learning Models Resistant to Adversarial Attacks," in ICLR, 2018.
- [18] Carlini, Nicholas, and David Wagner. "Towards evaluating the robustness of neural networks." 2017 ieee symposium on security and privacy (sp). leee, 2017.



임 경 섭

이메일 : gslim@isslab.korea.ac.kr

- 2021년 고려대학교 컴퓨터학과 (학사)
- 2021년~현재 고려대학교 컴퓨터학과 석박통합과정

저 자 약 력



한 학 수

이메일 : hshan@isslab.korea.ac.kr

- 2013년 공군사관학교 우주공학과 (학사)
- 2022년~현재 고려대학교 컴퓨터학과 석사과정



이 예 형

이메일 : yhlee@isslab.korea.ac.kr

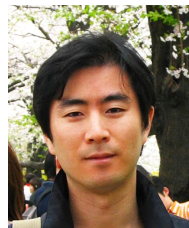
- 2023년 광운대학교 컴퓨터정보공학부 (학사)
- 2023년~현재 고려대학교 컴퓨터학과 석사과정



김 민 재

이메일 : mjkim@isslab.korea.ac.kr

- 2021년 고려대학교 컴퓨터학과 (학사)
- 2021년~현재 고려대학교 컴퓨터학과 석박통합과정



허 준 범

이메일 : jbhur@isslab.korea.ac.kr

- 2001년 고려대학교 컴퓨터학과 (학사)
- 2005년 한국과학기술원 전산학 (석사)
- 2009년 한국과학기술원 전산학 (박사)
- 2009년~2011년 University of Illinois at Urbana-Champaign (박사후 연구원)
- 2001년~2015년 중앙대학교 컴퓨터공학부 (조교수)
- 2015년~2016년 고려대학교 컴퓨터학과 (조교수)
- 2016년~2021년 고려대학교 컴퓨터학과 (부교수)
- 2021년~현재 고려대학교 컴퓨터학과 교수
- 2021년~2022년 ETH Zurich 방문교수

FHSS 기반의 드론 무선통신 취약점 연구*

강재구 · 최병철 (한국전자통신연구원)

목 차

1. 서 론
2. 드론 무선통신 체계
3. 드론 FHSS 무선통신 취약점
4. 결론 및 향후 연구

1. 서 론

반도체 집적 기술과 배터리, 무선조종 및 제어 기술이 발전하면서 해당 기술들을 기반으로 하는 무인기의 일종인 멀티콥터/드론이 보편화 되었다. 상당히 가볍고 작은 크기이지만 전문 장비 못지않은 고해상도/고배율 카메라를 장착하고, 적게는 수십분에서 많게는 수시간까지 비행이 가능해진 현대의 드론들은, 그 운용의 편리성과 원격지 정보 취득의 용이성이 더해져 개인의 사생활 침해뿐만 아니라 공항과 같은 비행 금지 구역의 허가되지 않은 비행으로 많은 재산 피해를 발생시키고 있다. 이뿐만 아니라, 살상을 위한 자폭용 드론 무기체계까지 개발되어 실전에 사용되는 사례(2022년 러시아-우크라이나 전쟁)까지 발생 되고 있다. 크기가 워낙 작고 빠르게 움직이는 드론의 특성상 탐지와 탈취, 무력화가 상당히 난해하다. 그러나 이러한 피해를 줄이기 위한 안티드론(Anti-Drone) 기술은 꾸준히 개발되어 오고 있으며, 시장의 크기도 계속하여 증가하고 있는 추세이다[1].

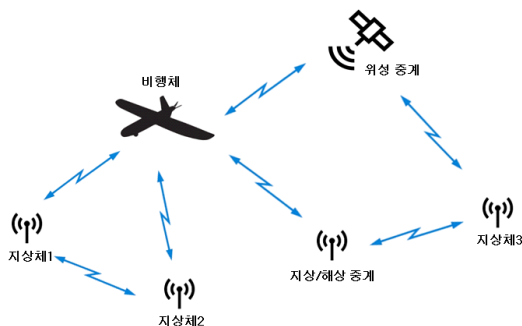
안티드론 기술은 크게 탐지와 무력화의 두가지 범주로 요약 할 수 있다. 탐지의 경우 적외선/가시광선등을 사용하는 전자광학적탐지 방법과, 드론 비행시 발생하는 특유의 소리를 탐지하는 음파탐지 방법, 전통적인 레이더를 사용하는 방식 그리고 드론 혹은 드론 조종자가 발생시키는 통신용 전자파를 탐지하는 RF스캔방식 등으로 구분할 수 있으며 한가지 방식만으로는 탐지에 어려움이 있으므로 보통 2개 이상의 방법을 동시 혹은 순차적으로 사용한다. 무력화의 경우 초기에는 물리적 접촉을 통한 무력화 또는 드론에서 사용하고 있는 같은 주파수 대역에 방해전파(RF Jamming)를 송출하여 드론을 추락시키거나 조종 불능 상태를 유도하였으나, 최근에는 GPS 기만 기법을 사용하거나 해당 드론에 직접 조종 신호를 송출하여 드론의 조종 권한의 탈취를 통해 안전한 장소로 이동시켜 착륙을 유도하는 무력화 기술도 개발이 진행되고 있다. 드론 조종권 탈취 방식의 경우 전자파 방해 방식에 비해 주변 통신 장비들의 광범위한 잠정적인 피해를 최소화할 수 있고, 무력화 대상

드론만을 목표로 하므로 유사 주파수 대역을 사용하는 아군 통신 장비의 피해도 최소화할 수 있다. 뿐만 아니라, 추락으로 인한 추가 피해를 방지할 수도 있다는 장점이 있어 기술에 주목을 받고 있다.

3G 혹은 LTE 통신의 변형된 방식을 사용하는 것으로 추정되는 DJI사의 드론 대상 안티드론과 관련된 연구로는, 드론과 조종기에서 발신하는 Drone-ID 무선 패킷을 해석[2][3]하는 최근의 연구를 비롯하여 탑재 펌웨어 조작을 위한 dji-firmware-tools[4] 그룹 등이 있고, DJI 드론 조종권의 직접 탈취가 가능한 이스라엘의 D-Fend Solution[5]과 Eclips[6]가 존재한다. 다만 DJI 드론 조종권 탈취 솔루션의 경우 어떠한 방식으로 탈취가 가능한지에 대해서는 현재까지 알려진 바가 없다. DJI를 제외한 나머지 드론들은 대부분 FHSS(Frequency Hopping Spread Spectrum) 혹은 DSSS(Direct Sequence Spread Spectrum) 다중접속방식을 주로 적용하고 있으며, 본 연구에서는 안티드론 기술개발 관점에서의 FHSS 무선통신 방식의 취약점에 대한 연구 결과를 제시하고자 한다.

2. 드론 무선통신 체계

일반적인 드론은 (그림 1)과 같이 지상체 혹은 조종자에 의해 원격으로 조종되며 지상중계, 해상

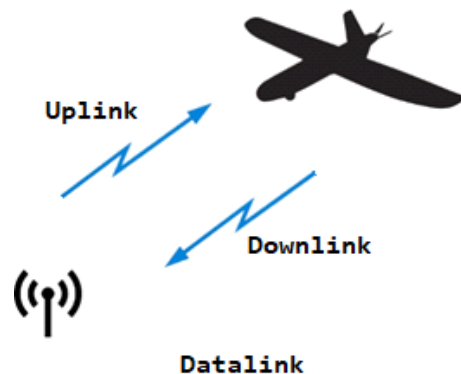


(그림 1) 드론 무선통신 체계

중계 혹은 위성중계 장비들을 체계에 추가 적용하여 그 임무 범위의 확장이 가능하다. 또한 한 개의 지상체/조종자가 아닌 다수의 지상체/조종자가 드론을 통제할 수 있는 복수통제 개념과 한 개 이상의 지상체에서 다수의 비행체를 통제하는 복수기체통제 개념도 존재 한다.

드론과 지상체 혹은 중계기간 통신을 ‘데이터링크’라고도 하며 이 데이터링크는 (그림 2)와 같이 비행체로 데이터를 올려 보내는 상향 링크(Uplink)와 비행체로부터 데이터를 수신하는 하향 링크(Downlink)로 구성된다. 이때 상향 링크는 보통 C2(Command & Control), TC(Tele-Command) 혹은 RC(Radio/Remote Control) 신호 라고도 부르며, 이름에서도 알 수 있듯이 주로 비행체의 제어와 통제를 위한 지상체의 명령 데이터를 담고 있다. 하향 링크는 비행체에 대한 원격계측정보(Telemetry)와 EO/IR(Electro-Optical/Infra-Red), SAR(Synthetic Aperture Radar)등과 같은 임무장비의 데이터를 지상체로 내려 보내준다.

전통적인 민수용 무선 조종 주파수는 초기에 AM 변조 방식의 27 MHz 대역을 사용하였으며, FM 변조 기술이 적용되면서 40 MHz와 72 MHz 대역을 사용해 왔다. 디지털 신호처리 기반의 변복조 기술이 주로 적용되는 최근에는 2.4 GHz 혹은 5.8 GHz의 ISM(Industry Science Medical) 대



(그림 2) 데이터링크 구성

역을 사용한다. 변/복조에는 FSK(Frequency Shift Keying) 혹은 PSK(Phase Shift Keying)가 주로 사용되며 이때 이 ISM 대역을 사용하기 위해서는 같은 대역을 사용하는 다른 기기와의 간섭 회피를 위해 다중접속기술중 하나인 주파수 확산 기법을 적용하게 되는데 대표적으로 주파수도약확산기법(FHSS - Frequency Hopping Spread Spectrum) 직접확산기법(DSSS - Direct Sequence Spread Spectrum) 두가지가 사용된다.

DSSS 방식의 경우 데이터신호와 확산코드 혹은 의사잡음코드(PN Code - Pseudo Random Noise Sequence)의 배타적 논리합(XOR) 신호를 반송파에 담아 송출하는 방식으로 이 의사잡음코드를 알지 못하면 도감청이 원칙적으로 불가능하다. 반면 FHSS 방식의 경우 ISM 대역 내에서 일정 간격으로 할당된 채널을 송신기와 수신기만이 알 수 있는 도약 순서로 초당 수~수십회 도약해가며 송수신을 하는 방식으로, 이 도약 순서를 알지 못하면 역시 신호 도감청이 불가능하다는 특징이 있다. 3G 혹은 LTE의 변형을 사용하는 것으로 추정되는 DJI사의 드론을 제외한 현재 시장에서 판매중인 ISM 대역의 드론 혹은 드론 조종용 송수신기의 경우 대부분 FHSS와 DSSS 방식중 하나이며, DSSS 방식의 Near-Far 문제로 인해 DSSS 방식보다는 FHSS 방식을 주로 선호하는 편이다.

3. 드론 FHSS 무선통신 취약점

전술한 바와 같이 FHSS 방식은 송신기와 수신기가 사전에 서로 약속된 도약 순서를 따라 주파수 채널을 바꿔가며 통신을 수행하는 방식으로, 해당 채널로의 데이터 전송시 송신기의 가용 전력 스펙트럼을 모두 사용하므로 상대적으로 낮은 전력 스펙트럼 특성을 보이는 DSSS 방식에 비해 Near-Far 문제로부터 자유롭다. 또한 특정 채널

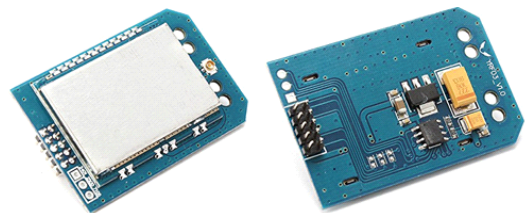
근처의 강한 신호가 나타나더라도 다른 채널로 능동적으로 바뀌가며 통신 연결 유지가 가능하므로, 진보된 적응형 채널 도약 알고리즘을 적용할 경우 전파 간섭 또한 최소화가 가능하다는 장점이 있어 시중에 판매되고 있는 드론과 드론용 무선 송수신기 들은 FHSS 기법이 많이 적용되어 있다.

FHSS 기법이 적용된 드론 혹은 무선 송수신 장치들의 경우 보통 Low-Cost, Low-Power를 강조하는 상용 RF Front-End SoC 혹은 RF Transceiver 칩들을 사용하는 경우가 대부분이며 자체 조사를 통해 대표적인 아래 4가지의 SoC가 주로 사용되는 것을 파악 할 수 있었다.

- 1) CC2500/CC2510 (Texas Instruments)
- 2) CYRF6936 (Cypress Semiconductor)
- 3) nRF24L01 (Nordic Semiconductor)
- 4) A7105 (AMICCOM)

대규모 글로벌 반도체 기업에서 판매하는 CC2500/CC2510 및 CYRF6936의 경우 중급기 이상의 제품에 주로 탑재가 되고 상대적으로 비용의 경쟁력을 갖추고 있는 nRF24L01 및 A7105등과 같은 칩셋은 주로 저가 및 보급형 드론과 무선 송수신기에 탑재되어 판매 되고 있는 것을 확인할 수 있었으며, 이 4개의 모든 SoC를 한데 모아 FHSS기반의 많은 프로토콜에 대응이 가능한 4IN1 모듈[7]을 시장에서 쉽게 구매 가능함을 확인하였다 (그림 3), (그림 4).

FHSS 패킷 스케줄링은 각 제조사와 모델마다



(그림 3) 4IN1 모듈

송신이 가능함도 확인 하였다.

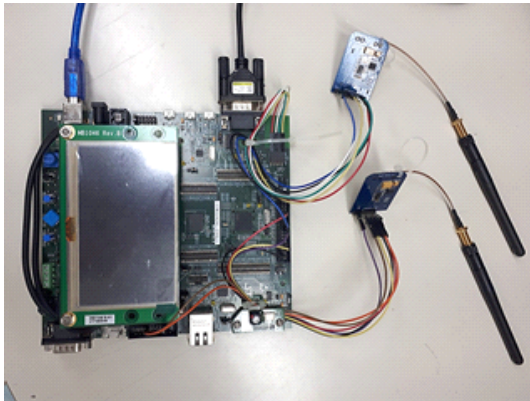
3) 일부 모델의 경우 C2 패킷에 다음 도약 채널을 연산 할 수 있는 정보를 담고 있음

- 1) 대부분의 FHSS 드론 무선 패킷의 데이터가 암호화 되어 있지 않음
- 2) 제조사별 FHSS 도약 알고리즘의 상당수가 공개정보[7]로 취득 가능

해당 취약점들을 직접 확인하고 검증하기 위해 (그림 7)과 같이 임베디드시스템 평가보드와 4IN1 모뎀을 연동하여 간단한 도구를 구성해 위 3가지

〈표 1〉 Multiprotocol TX Module github를 통해 파악 가능한 프로토콜 일부

Name	Sub 0	Sub 1	Sub 2	Sub 3	Sub 4	Sub 5	Sub 6	Sub 7
Assan	ASSAN							
Bayang	Bayang	H8S3D	X16_AH	IRDRONE	DHD_D4	QX100		
Bugs	BUGS							
BugsMini	BUGSMINI	BUGS3H						
Cabell	Cabell_V3	C_TELEM					F_SAFE	UNBIND
CFile	CFile							
CG023	CG023	YD829						
Corona	COR_V1	COR_V2	FD_V3					
CX10	GREEN	BLUE	DM007		J3015_1	J3015_2	MK33041	
Devo	Devo	8CH	10CH	12CH	6CH	7CH		
DM002	DM002							
DSM	DSM2_1F	DSM2_2F	DSMX_1F	DSMX_2F	AUTO			
E010 R5								
E016H v2								
E01X	E012	E015	E016H					
E129								
ESky	ESky	ET4						
ESky150	ESKY150							
ESky150V2								
Flysky	Flysky	V9x9	V6x6	V912	CX20			
Flysky AFHDS2A	PWM_IBUS	PPM_IBUS	PWM_SBUS	PPM_SBUS	PWM_IBUS16	PPM_IBUS16		
FQ777	FQ777							
FrSkyD	D8	Cloned						
FrSkyL	LR12	LR12_6CH						
FrSkyR9	R9_915	R9_868	R9_915_8CH	R9_868_8CH	R9_FCC	R9_FCC_8CH		
FrSkyV	FrskyV							
FrSkyX	CH_16	CH_8	EU_16	EU_8	Cloned	Cloned_8		
FrSkyX2	CH_16	CH_8	EU_16	EU_8	Cloned	Cloned_8		



(그림 7) FHSS 무선통신 취약점 분석용 간이 도구

취약점을 모두 확인 하였다.

Multiprotocol TX Module[7] 단체에서 공개한 자료들의 경우 시중에 판매되는 약 170여가지의 FHSS 통신 프로토콜과 관련된 정보를 소스코드 수준에서 취득할 수 있으며, 연구[8]에서는 FHSS 기반 드론의 조종권 탈취를 직접적으로 수행한 결과를 보여 주고 있다. 주파수 도약 방법이 바인딩 시 상수로 고정되는 드론의 경우 SDR(Software Defined Radio)과 같은 장치들을 활용하여 손쉽게 도약 정보를 파악 할 수 있으며, 위 1)의 취약점과 같이 패킷에 암호화가 되어 있지 않으므로 시행착오 방법 혹은 Multiprotocol TX Module github에 공개된 패킷 포맷에 따라 비행제 조종 명령을 만들어 송신하게 되면 원 조종자와 경쟁상태에서 드론의 조종권 일부 획득이 가능하다. 또한 위 취약점 3)과 같이 무선 패킷에 다음 도약 정보가 포함된 FHSS 프로토콜의 경우 원 조종자와 상이한 다음 도약정보 패킷을 만들어 송신하게 되면 좀더 개선된 조종권 탈취가 가능해짐을 보여주고 있다.

FHSS에서의 도약 방법은 가능한 난수에 가까운 수목 간섭이 최소화 되므로, 각 드론 및 송수신기 제조사들은 보다 진보된 도약 알고리즘들을 개발 하고 있으며, 패킷에 도약과 관련된 정보가 없

는 모델이거나, 도약을 위한 난수 발생 알고리즘을 알 수 없는 경우 FHSS 특성에서 설명한 바와 같이 FHSS 조종명령을 통한 조종권 탈취는 쉽지 않다.

<표 1>은 Multiprotocol TX Module github에서 확인 가능한 170여가지 FHSS 통신 프로토콜 중 일부 항목의 예시를 보여주고 있다.

4. 결론 및 향후 연구

안티드론 기술개발의 관점에서 드론의 무선 조종에 많이 사용되는 ISM 대역의 FHSS 확산기법에 대한 취약점 연구를 수행하였다. 그 결과 대부분의 FHSS 무선 패킷은 암호화가 되어있지 않으므로 대표적인 4가지 RF SoC인 CC2500/CC2500, CYRF6936, nRF24L01, A7105의 데이터시트를 참고하여 임의의 주파수 채널을 통해 목표 드론에 송신되는 패킷을 수신하여 그 내용을 분석할 수 있었으며, 공개된 정보를 기반으로 송신기의 복제와 수신기의 복제도 가능함을 확인 할 수 있었다. 또한 초기 바인딩과정에서 상수로 고정되는 도약 알고리즘들의 경우 전술한 취약점의 활용과 더불어 SDR과 같은 도구를 활용해 그 도약 정보를 쉽게 유추해 낼수 있으며, 드론 조종패킷을 기반으로 다음 도약 채널을 연산해 낼수 있는 프로토콜의 경우 해당 연산 알고리즘이 확보된다면 역시 도약 정보의 취득이 가능함을 확인 하였다. 다만, 어떠한 방법으로도 도약 정보를 확인할 수 없는 기존의 경우 해당 FHSS 패킷으로의 조종권 탈취는 거의 불가능하며, 연구[8]에서와 같이 취약점을 이용해 조종권한을 탈취하더라도 원 조종자의 조종신호가 공존하는 한 영구적 혹은 장시간 드론 조종권 탈취는 쉽지 않다.

향후에는 본 연구를 통해 확인된 FHSS 취약점과 더불어 다수의 모델을 활용하여 원 조종자의

조종신호를 무력화시키는 방법을 동원, 좀더 진보된 드론 조종권 탈취를 위한 연구를 진행할 계획이다.

Drones, Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, Pages 526-536, May 2021.

참 고 문 헌

- [1] Grand View Research, Anti-drone Market Size, Share & Trends Analysis Report By Component, By Type, By Range, By Technology, By Mitigation Type, By Defense Type, By End-use, By Region, And Segment Forecasts 2023-2030, 2023.
- [2] Nico Schiller, Merlin Chlosta, Moritz Schloegel, Nils Bars, Thorsten Eisenhofer, Tobias Scharnowski, Felix Domke, Lea Schönherr, Thorsten Holz, Drone Security and the Mysterious Case of DJI's DronelD, Network and Distributed System Security Symposium, Feb. 2023.
- [3] Bender, C. DJI drone IDs are not encrypted. arXiv 2022, arXiv:2207.10795. [Google Scholar].
- [4] dji-firmware-tools, Available online: <https://github.com/o-gs/dji-firmware-tools>, accessed on 6 Dec. 2023.
- [5] D Fend Solutions, Available online: <https://d-fendsolutions.com>, accessed on 6 Dec. 2023.
- [6] NSO Group Eclips, Available online: <https://www.nso-group.com/News/nso-group-launches-drone-defense-system-eclipse>, accessed on 6 Dec. 2023.
- [7] Multiprotocol TX Module, Available online: <https://github.com/pascallanger/DIY-Multi-protocol-TX-Module> (accessed on 6 Dec. 2023).
- [8] Sebastian Plotz, Frederik Armknecht, Christian Bunse, How to Take Over

저 자 약 력



강 재 구

이메일 : kangjaegu@etri.re.kr

- 2004년 전북대학교 전자제어계측공학 (학사)
- 2003년~2005년 KEC-메카트로닉스연구소 연구원
- 2007년 과학기술연합대학원대학교 HCI 및 로봇응용공학 (석사)
- 2007년~2010년 한국로봇융합연구원 연구원
- 2010년~2012년 (주)한화종합연구소 연구원
- 2012년~2022년 (주)대한항공 항공기술연구원 연구원
- 2023년~현재 한국전자통신연구원 연구원



최 병 철

이메일 : corea@etri.re.kr

- 1999년 서울시립대학교 제어계측공학과 (학사)
- 2001년 서울시립대학교 전자전기공학부 (석사)
- 2012년 충남대학교 컴퓨터공학 (박사)
- 2019년~2022년 한국전자통신연구원 보안취약점분석연구실 실장
- 2001년~현재 한국전자통신연구원 책임연구원
- 2020년~현재 한국정보보호학회 이사
- 관심분야: 사이버보안, 사이버전, 사이버전자전

적성국의 사이버 공격에 대응하는 위성통신 및 무선통신 시스템의 보안 강화 전략

정진우 · 윤상범 (LIG 넥스원)

목 차	1. 서 론	4. 사이버 보안 강화 전술 및 기술적 대응 전략
	2. 위성통신과 무선통신의 기술적 구조 및 운용 방식 개요	5. 정책 제언 및 미래 전망
	3. 고도화된 사이버 위협과 탐지 기술	6. 결 론

1. 서 론

사이버 안보의 중요성은 현대 사회에서 더욱 강조되어야 할 필수 요소다. 특히, 북한과 같은 적성국에 의한 사이버 공격은 전 세계적으로 심각한 위협으로 부상하고 있다. 북한은 2015년부터 금융기관에 대한 사이버 공격을 세계적으로 수행해 왔으며, 이는 베트남의 티엔퐁 은행에 대한 공격과 같은 사례에서 명확히 드러난다[1]. 또한, 유엔 전문가들은 최소 17개국에서 북한이 불법적인 자금 조달을 위해 사이버 공격을 시도한 적이 있다고 보고하고 있다[2].

특히, 북한은 최근 남한의 조선소를 대상으로 한 집중적인 사이버 공격을 감행, 이를 통해 남한의 국가 안보에 직접적인 위협을 가한 바가 있다[3]. 이러한 사이버 공격은 단순히 정보 탈취에 그치지 않고 군사적, 경제적 파급효과를 목표로 하고 있다. 북한의 사이버 공격 능력은 많은 이들에게 과소평가 되고 있으나, 이는 물리적인 피해뿐만 아니라 국가의 핵심 인프라를 위협하는 수준에

이르렀다[4].

더불어, 북한은 사이버 공격을 통해 약 20억 달러를 조달하여 대량살상무기 프로그램에 자금을 지원하는 등, 사이버 영역에서의 범죄 활동을 통해 국가적 차원의 이익을 추구하고 있다[5-6]. 이처럼 북한의 사이버 공격은 단순한 해킹 활동을 넘어서 국가 안보에 중대한 위협을 제기하며, 위성통신 및 무선통신 시스템의 보안 강화가 절실하게 요구되는 배경이 된다.

2. 위성통신과 무선통신의 기술적 구조 및 운용 방식 개요

위성통신 시스템은 지상의 기지국과 우주에 위치한 인공위성을 활용하여 데이터를 전송하는 복잡한 기술 체계이다. 이 시스템은 전 세계적인 커버리지를 제공하며, 글로벌 포지셔닝 시스템(GPS), 통신, 기상 관측 등 다양한 목적으로 활용된다. 위성통신은 특히 광범위한 지역 커버리지가 필요한 해양, 항공, 군사 및 재난 관리 분야에서

중요한 역할을 수행한다. 이 시스템은 지리적으로 접근이 어려운 지역에서도 통신 서비스를 제공할 수 있어, 원격 지역의 연결성과 응급 상황에서의 통신 능력을 향상시킨다.

무선통신 네트워크는 전파를 통해 정보를 전송하는 현대적인 통신 방식으로, 이는 고도화되고 지능화된 기술을 기반으로 한다. 이러한 네트워크는 휴대폰, 무선 인터넷, 위성통신 등 다양한 형태의 통신에 사용되며, 일상생활에서 중요한 역할을 담당한다. 무선 네트워크 기술은 계속 발전하고 있으며, 5G와 같은 최신 기술은 더 빠른 데이터 전송 속도, 낮은 지연 시간, 그리고 높은 네트워크 효율성을 제공한다. 이러한 기술은 스마트 시티, 자율주행 차량, 원격 의료와 같은 미래 기술의 발전에도 중요한 기반을 제공한다[7]. 다음의 <표 1>은 위성통신과 무선통신의 기본적인 공통점과 차이점, 그리고 각각의 장단점을 요약한 것이다. 위성통신은 주로 원거리 통신과 광역 커버리지를 제공하는 반면, 무선통신은 주로 근거리 및 지역적 커버리지를 제공한다. 또한, 위성통신은 지형에 구애받지 않는 광범위한 서비스를 제공하는 반면, 무선통신은 설치 및 유지보수의 편의성과 빠른 데이터 전송 속도를 제공한다. 그러나 위성통신은 신호 지연, 보안성 문제, 고비용과 같은 단점이 있으며, 무선통신은 간섭, 제한된 대역폭, 지리적 제한 등의 단점을 가지고 있다.

2.1 현재 시스템의 취약점과 과거 사례

위성통신은 외부 신호 교란에 취약할 수 있으며, 과거 우크라이나 사태에서 GPS 신호와 상업용 위성통신이 교란된 사례가 있었다[8]. 또한 무선통신 네트워크의 취약점으로는 해킹, 데이터 유출, 네트워크 침입 등이 있으며, 이는 사이버 공격 기법의 진화와 연관이 깊다[9]. 미국 GPS 시스템이 사이버 공격을 받은 사례는 이러한 시스템들의 취약성을 잘 보여준다[10]. 2023년 기준으로 위성통신 시스템과 무선통신 시스템의 취약점에 대한 사이버 공격 사례를 살펴보면 다음과 같다.

2.1.1 위성통신 시스템에 대한 사이버 공격 사례

위성 해킹은 실제로 발생 가능한 사이버 위협이다. 위성 시스템은 국방, 외교, 안보 분야의 핵심 자산이 되었기 때문에 전 세계 여러 국가들이 위성 전용 보안 정책과 기술을 개발하고 있다. 위성 시스템에 대한 사이버 공격은 주파수 대역에 간섭 신호를 방사하는 주파수 재밍, 민감한 데이터 도청, 비인가자의 위성 신호 도용, 데이터 불법 변경 또는 허위 데이터 전송, 탈취한 신호 재전송 등의 형태로 발생할 수 있다. 실제로, 러시아 군용 통신 위성과 위성통신 업체 비아셋이 악성 소프트웨어를 이용한 해킹을 당한 사례가 있었다. 이와 함께 위성 항법 시스템 탈취로 테슬라의 레벨2 자율주

〈표 1〉 위성통신과 무선통신의 특징

구분	위성통신	무선통신
공통점	정보 전송에 전파 사용	정보 전송에 전파 사용
차이점	우주에 위치한 위성을 이용 대부분 장거리, 광역 커버리지	지상 기반 장비 이용 주로 근거리, 지역적 커버리지
장점	광범위한 지역 커버리지 지형에 구애받지 않음	설치와 유지보수가 상대적으로 간단 빠른 데이터 전송 속도, 안정적 연결
단점	신호 지연, 보안성 문제, 전파 간섭 문제 고비용, 불안정한 데이터 전송 속도	간섭, 제한된 대역폭, 보안 문제 지리적 제한 (신호 범위 내에서만 사용 가능)

행 차량 오동작을 유도하는 시도도 있었다[11].

2.1.2 무선통신 시스템에 대한 사이버 공격 사례

최근 랜섬웨어, 가상화폐, 국가 안보는 사이버 보안의 주요 키워드로 부각되었다. 랜섬웨어 그룹의 활동은 개인, 기업, 국가 안보, 글로벌 경제시장에 영향을 미쳤으며, 러시아와 미국 및 서방 국가 간의 이해충돌은 사이버 보안에 새로운 도전을 제시했다. 러시아의 우크라이나 침공은 물리적 충돌과 사이버 공격이 결합된 하이브리드 전쟁의 사례로, 다양한 분야에서의 사이버 공격 효과가 나타났다[12]. 서비스형 랜섬웨어(RaaS)의 출현은 사이버 범죄의 전문화와 조직화를 촉진했으며, 공공, 금융, 제조, 교육, 국방 등 다양한 산업에 대한 공격이 확대되었다. 공급망 공격의 증가 추세는 Microsoft Exchange Server 취약점, Solarwinds 해킹, Kaseya 사례 등을 통해 공급망 보안의 중요성을 강조했다. 이러한 사이버 공격 사례들은 위성통신 및 무선통신 시스템의 취약점을 이용하며, 국가 안보, 사회기반시설, 경제적 안정성에 직접적인 영향을 미치고 있다. 이는 지속적인 대응과 보안 강화의 필요성을 시사한다. 다음의 <표 2>는 위성 통신 및 무선통신을 대상으로 하는 다양한

사이버 공격 유형과 이러한 공격에 대처하기 위한 보안 대책들을 요약하여 보여준다.

<표 2>에서 보는 바와 같이 위성 통신과 무선통신이 공통적으로 직면할 수 있는 사이버 공격 유형들에 대해서 각 통신 방식에 특화된 대응을 해야 한다. 두 시스템 모두 공통적인 위협에 직면할 수 있으나, 위성 통신의 경우 우주 환경과 같은 특별한 요소들을 고려해야 하고, 무선통신은 더 다양한 형태의 네트워크 침입과 인프라 공격에 노출될 수 있다. 따라서, 각각의 시스템에 적합한 보안 대책을 수립하는 것이 중요하다.

2.2 적성국의 사이버공격 유형 및 가능한 시나리오

적성국은 위성통신과 무선통신 시스템을 대상으로 한 다양한 형태의 사이버 공격을 시도할 수 있으며, 이는 국가 안보에 직접적인 위협이 될 수 있다. 이러한 공격에는 신호 교란, 데이터 해킹, 서비스 거부 공격(DoS) 등이 포함될 수 있다. 예를 들어, 북한의 정찰총국이나 라자루스와 같은 조직은 사이버전을 통해 타국의 통신 시스템에 침입하고, 이를 통해 정보를 유출하거나 군사적 목적으로 신호를 방해하는 등의 활동을 할 수 있다.

<표 2> 위성 통신에 대한 사이버 공격 유형과 그에 대한 대응 방안

사이버 공격 유형	일반적 대응방안	위성 통신 대응방안	무선통신 대응방안
신호 방해 (Jamming)	간섭 회피 기술 사용	주파수 이동 (Frequency Hopping)	신호 강도 강화
스푸핑 (Spoofing)	암호화된 신호 사용	위성 위치 인증 메커니즘	강력한 인증 프로토콜 적용
트래픽 분석 (Traffic Analysis)	트래픽 패턴 마스킹	랜덤 트래픽 생성	네트워크 트래픽 암호화
네트워크 침입 (Network Intrusion)	침입 탐지 및 방지 시스템 (IDS/IPS)	추가적인 물리적 보안 조치	다중 계층 보안 (Multi-Layer Security)
서비스 거부 공격 (DoS/DDoS)	분산 서비스 거부 (DDoS) 대응 전략 구축	대역폭 확장 및 관리	탄력적 네트워크 인프라 구축
물리적 공격 및 파괴 (Physical Attack)	물리적 보안 강화 및 감시 체계 구축	위성 장비의 강화된 보호 설계	무선통신 장비의 보안 강화

국가 간의 갈등 상황에서는 통신 시스템을 통한 정보 유출이나 군사적 목적을 위한 신호 방해가 더욱 증가할 가능성이 높다[13]. 위성통신과 무선 통신의 중단은 국가의 중요한 인프라 및 서비스에 심각한 영향을 미치며, 이는 국가 안보를 심각하게 위협할 수 있다. 이러한 위협에 대응하기 위해서는 탈린 매뉴얼과 같은 국제적인 사이버전 법률 및 규범을 참고하여 효과적인 대응 전략을 수립하고 실행하는 것이 중요하다. 따라서, 위성통신 및 무선통신 시스템의 보안을 강화하는 것은 국가 안보를 보장하는데 필수적이다[14-15]. 이를 위해서는 지속적인 보안 평가, 기술적 대응 전략의 개발 및 업데이트, 그리고 국제 협력을 통한 정보 공유와 공동 대응이 필요하다. 이러한 조치들은 사이버 위협을 효과적으로 관리하고, 국가 안보를 보호하는 데 있어 중요한 역할을 한다. 다음의 <표 3>은 적성국이 위성통신 및 무선통신 시스템을 대상으로 수행할 수 있는 다양한 사이버공격 유형과 시나리오를 나타낸다. 이러한 공격에는 신호 교란, 데이터 해킹, 서비스 거부 공격(DoS) 등이 포함되며, 이들은 국가 안보와 중요 인프라에 직접적인 영향을 미친다[16-18]. 국가 간 갈등이나 군사적 목적을 위한 신호 방해의 가능성은 통신 시스템의 보안 취약점을 드러내며, 이에 대한 적절한 대응

과 보안 강화 조치가 필수적이다.

3. 고도화된 사이버 위협과 탐지 기술

사이버공격 탐지는 현대의 사이버 보안 분야에 서 매우 중요한 위치를 차지하고 있다. 최신 기술과 방법론의 발전은 사이버 위협에 대응하는 데 필수적인 요소로 자리 잡았다.

3.1 최신 사이버공격 탐지 기술 및 방법론

위성통신과 무선통신 분야에서는 네트워크 트래픽 분석과 행위 기반 탐지를 통해 사이버 보안을 강화하고 있다. 이들 기술은 네트워크 유입 트래픽을 분석해 해킹을 탐지하고 대응하며, 빅데이터, 딥러닝, 인공지능을 결합해 정교한 보안 체계를 구축하고 있다. 또한, SUN 무선 센서 네트워크와 원거리 무선통신을 활용한 스마트 시티 기술 개발에 기여하고 있다. <표 4>에서는 이러한 사이버공격 탐지 기술을 요약하고 있다. <표 4>에서 보는 바와 같이 위성통신과 무선통신 분야에서 사용되는 주요 사이버공격 탐지 기술은 고급 네트워크 모니터링, 이상 징후 탐지 시스템, 그리고 인공지능 및 머신 러닝을 기반으로 한 탐지 알고리즘

<표 3> 적성국의 사이버공격 유형 및 시나리오

사이버공격 유형	설명	영향 및 중요성
신호 교란	통신 신호를 방해하여 정상적인 운영을 저해하는 공격.	국가 안보와 관련된 중요한 통신이 방해 받을 수 있음.
데이터 해킹	정보를 불법적으로 접근하거나 조작하는 공격.	정보 유출로 인한 보안 위협이 증가함.
서비스 거부 공격 (DoS)	대량의 트래픽을 발생시켜 정상적인 서비스 제공을 방해하는 공격.	필수적인 서비스와 인프라에 심각한 영향을 미칠 수 있음.
정보 유출	적성국이 통신 시스템을 통해 중요한 정보를 빼내는 행위.	국가의 기밀 정보가 외부로 유출되는 위험 존재.
군사적 목적의 신호 방해	국가 간 갈등 상황에서 특정 목적을 위해 통신 시스템의 신호를 방해하는 행위.	군사 작전의 효율성 저하 및 안보 위협 증가.
위성통신 및 무선통신 보안 강화	위성통신 및 무선통신 시스템의 보안을 강화하는 조치.	국가 안보를 보장하고 중요 인프라를 보호하는데 필수적임.

〈표 4〉 위성통신과 무선통신 분야의 사이버공격 탐지 기술

분야	기술적 적용	목적 및 기능
위성통신	트래픽 분석, AI 기술 적용	이상 징후 수집 및 분석, 해킹 침해 탐지 및 대응
무선통신	빅데이터, 딥러닝 기술 적용	보안 체계 강화, 실시간 모니터링, 스마트 시티 기술 개발 지원

을 포함한다. 이 기술들은 무단 접근, 데이터 유출, 및 기타 사이버 위협을 식별하고 대응하는데 중요한 역할을 한다.

3.2 암호화, 인증, 네트워크 모니터링 방법론

사이버 보안에서 암호화, 인증, 네트워크 모니터링은 중요한 역할을 한다. 암호화는 민감한 정보를 변조하기 어려운 형태로 바꾸어 데이터 기밀성을 유지한다. 예를 들어, 공개 키 암호화는 메시지를 안전하게 전송하는 데 사용되며, 금융 거래부터 전자 메일 보안에 이르기까지 다양한 분야에서 활용된다. 인증은 사용자의 신원을 확인하고 액세스 권한을 부여하는 과정이다. 다단계 인증은 해킹과 같은 무단 액세스를 방지하는 데 효과적이며, 금융 서비스와 기업 네트워크에서 널리 사용된다. 네트워크 모니터링은 활동을 감시하고 분석하여 보안 위협을 식별한다. 이상 징후 탐지 시스템은 비정상적인 활동을 조기에 감지한다. 이 방법론들은 상호 보완적으로 작용하여 포괄적인 보안 체계를 구축하는 데 기여한다.

3.3 인공지능 및 머신러닝을 활용한 사이버 위협 분석 사례

인공지능(AI)과 머신러닝(ML)은 사이버 보안 분야에서 중요한 역할을 하고 있다. 이 기술들은 대규모 데이터 분석, 복잡한 패턴 인식, 예측 모델링을 통해 보안 위협 탐지와 대응을 개선한다. 머신러닝 알고리즘은 기존의 사이버 공격 패턴을 학습하여 새로운 공격 유형을 예측하고, 네트워크 트래픽 분석을 통해 비정상적인 데이터 흐름을 감

지한다. 이는 기업이나 금융기관의 데이터 보호에 중요하다. AI와 ML은 또한 피싱 공격 식별 및 차단에도 활용된다. 예를 들어, Palo Alto Networks와 같은 보안 솔루션 제공업체들은 AI와 ML을 활용하여 사이버 위협을 효과적으로 탐지하고 대응한다. 이 기술들은 또한 사이버 보안 분야에서의 자동화와 효율성 증대에 기여하며, 전문가들이 더 중요한 과제에 집중할 수 있게 한다.

이와 같은 고도화된 사이버 위협 탐지 기술은 지속적인 발전과 혁신을 통해 사이버 공간의 안전을 확보하는 데 중요한 역할을 하고 있다. 이러한 기술들의 발전은 사이버 보안의 미래를 밝히는 중요한 열쇠가 될 것이다.

4. 사이버 보안 강화 전술 및 기술적 대응 전략

위성통신 및 무선통신 시스템의 보안 강화는 사이버 안보의 핵심 요소로, 전술적 및 기술적 대응 전략의 개발이 필수적이다. 이러한 전략은 광범위한 위협에 대응하고, 효과적인 보안 체계를 구축하기 위한 핵심적인 부분이다.

4.1 전술적 접근

위성통신 및 무선통신 시스템의 보안 강화를 위한 전술적 접근 방법은 다양한 위협으로부터 통신 인프라를 보호하는 데 중점을 둔다. 이러한 접근 방식에는 몇 가지 중요한 요소가 포함된다.

4.1.1 위험 평가 및 감시

첫 단계는 위협과 취약점을 정확하게 파악하는 것이다. 이를 통해 특정 위협에 대한 대비책을 마련할 수 있으며, 시스템이 어떤 공격에 취약한지를 파악할 수 있다. 다음의 <표 5>은 위험 평가 및 감시 과정에서 중요한 단계들을 정리해 놓은 것으로, 각 단계에서 필요한 활동과 목표를 설명하고 있다. 이 표는 위협을 체계적으로 식별, 평가, 감시하고 이에 대응하는 과정을 단계별로 구체화하여 보여준다.

4.1.2 데이터 암호화

위성통신 및 무선통신에서 데이터 암호화는 보안을 강화하는 핵심적인 요소이다. 암호화는 제3자로부터 데이터 도청을 방지하고, 데이터 무결성을 유지하여 변조를 방지한다. 이렇게 함으로써 통신 네트워크의 안정성과 신뢰성을 확보할 수 있다. 따라서 위성통신 및 무선통신 분야에서는 데이터 암호화 기술의 중요성이 더욱 부각된다.

4.1.3 네트워크 접근 제어

네트워크 보안의 중요성을 강조하고 있다. 엄격한 인증 및 권한 부여 절차는 무단 접근을 예방하며, 더 높은 수준의 네트워크 보안을 제공한다. 이러한 절차는 사용자와 장치가 신뢰할 수 있는지 확인하고, 필요한 권한만 부여하여 데이터 및 시스템의 안전성을 유지한다. 이는 방어 산업과 같

이 민감한 분야에서 특히 중요한데, 정보 유출 및 해킹으로부터 보호하기 위해 필수적이다.

4.1.4 지속적인 모니터링 및 대응

보안 시스템의 효과를 지속적으로 모니터링하는 것은 중요하다. 이를 통해 시스템의 작동 상태를 실시간으로 파악하여, 어떠한 문제가 발생하더라도 빠른 조치를 취할 수 있다. 또한, 위협이 발견되었을 때 신속하게 대응함으로써 중요한 정보나 시스템을 보호할 수 있다. 이러한 신속한 대응은 잠재적인 보안 사고의 효과적인 예방과 조기 탐지를 가능하게 한다. 따라서 보안 시스템을 효과적으로 관리하고 감시하는 것은 모든 조직에게 필수적인 요소이다.

4.1.5 보안 업데이트 및 유지보수

위성통신 및 무선통신 시스템의 정기적인 업데이트는 매우 중요하다. 이것은 현대 전자전에서 핵심적인 역할을 한다. 첫째, 보안 패치와 소프트웨어 업데이트를 통해 시스템의 취약성을 최소화할 수 있다. 이는 위협에 대한 강력한 방어를 제공할 수 있다. 둘째, 새로운 기술과 표준을 통합하여 효율성을 향상시킬 수 있다. 이것은 통신 시스템의 성능을 향상시키며 새로운 기회를 창출한다. 따라서 시스템의 정기적인 업데이트는 보안과 성능 개선을 위해 필수적이다.

<표 5> 위험 평가 및 감시의 중요 단계

단계	설명
위협 식별	현재 및 잠재적 위협 파악 (해킹, 물리적 침입, 소프트웨어 취약점 등 포함)
취약점 분석	시스템의 취약한 부분 찾기 (소프트웨어, 하드웨어, 프로세스, 인적 요소 검토)
위험 평가	위협과 취약점을 바탕으로 위험 수준 결정 (위험 가능성과 영향 평가)
모니터링 및 경보 시스템	지속적인 감시 및 경보 메커니즘 구축 (비정상 활동과 잠재적 위협 감지)
지속적인 개선	보안 환경 변화에 따른 위험 평가 및 감시 방법의 지속적인 개선

4.2 기술적 솔루션

4.2.1 암호화 기술의 발전

암호화 기술은 현대 정보 보안에서 중요한 역할을 한다. 이 기술은 데이터의 기밀성을 보호하여 무단 접근으로부터 보호하고, 데이터의 무결성을 유지하여 변경 또는 변조로부터 방지한다[19]. 특히, 퀀텀 컴퓨팅의 발전으로 인해 고전적인 암호화 방법들이 취약해질 우려가 있으므로, 현대 암호화 기술은 퀀텀 컴퓨팅에 대응할 수 있는 수준으로 발전해야 한다. 이는 미래의 정보 보안을 위해 매우 중요한 과제 중 하나이다.

4.2.2 효과적인 네트워크 모니터링 시스템 구축

실시간 네트워크 모니터링과 데이터 분석은 정보 보안을 강화하기 위한 필수적인 단계이다. 이를 통해 비정상적인 트래픽 패턴을 식별하고 대응함으로써, 잠재적인 위협을 미리 탐지할 수 있다. 또한, 이러한 접근 방식은 네트워크 활동에 대한 투명성을 제공하며, 보안 사고의 효과를 최소화하는 데 도움이 된다. 더불어, 이러한 실시간 감시와 분석은 조직의 데이터 자산을 보호하고 비인가된 액세스를 방지하는데 중요한 역할을 한다. 따라서 네트워크 보안에 있어서 이러한 접근 방식은 반드시 필요한 단계이다.

4.2.3 무선통신 시스템의 안전한 아키텍처 설계

무선통신 시스템의 아키텍처는 공격에 대한 내성을 가질 수 있도록 설계되어야 한다. 이는 통신망의 분산화, 중요 데이터의 분산 저장, 장애 허용 시스템 설계 등을 포함할 수 있다.

4.3 다층적 방어 전략 및 장기적 보안 체계 구축

다층적 방어 전략은 다양한 보안 계층을 통합하여 전체 보안 체계를 강화하는 방법으로, 단일 솔루션에만 의존하지 않는다. 이 전략은 공격자가 방어를 우회하거나 해체하기 어렵게 만들기 위해 지속적인 위협 평가, 기술 업데이트, 인원 교육 및 정책 개정을 포함한다. 네트워크, 애플리케이션, 물리적 보안을 통합하고, 방화벽, 침입 탐지 시스템, 암호화 등 다양한 보안 요소를 운용해야 한다. 이와 더불어, 정부, 산업, 학계 간의 협력은 정책 개발과 기술 표준 설정에서 중요하다. 국제적 협력 및 표준화를 통한 지속 가능한 보안 체계 구축은 위성통신 및 무선통신 시스템의 보안을 강화하고 사이버 위협에 대응하는 데 필수적이며, 국가 안보에 중요한 역할을 한다[19]. 대한민국 합동참모본부에서 사이버 경보 체계를 인포콘(Infocon)에서 CP콘(Cyber Protection Condition)으로 변경하고, 국가정보원의 NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) 가입은 대한민국이 사이버 공간에서의 적성국의 공격에 대응하기 위한 정부 차원의 국제 공조 및 세계적인 공동 대응 노력을 강화하는 중요한 전략적 움직임이다.

5. 정책 제언 및 미래 전망

정부와 관련 산업 간의 협력은 사이버 보안을 강화하기 위한 기반을 제공한다. 이를 위해, 정부는 다부처 간 협력 체계를 강화하여 사이버 보안 문제에 통합적으로 대응해야 한다. 이를 통해 정보 공유, 정책 조정 및 자원 배분의 효율성을 높일 수 있으며, 더욱 강력한 보안 체계를 구축할 수 있다[20]. 또한, 정부와 산업계는 보다 넓은 관점에서 협력하여 사이버 보안 인식을 높이고 관련

교육 프로그램을 확대해야 한다. 이는 사용자의 보안 행동을 개선하고 전반적인 보안 문화를 조성하는 데 중요한 역할을 한다.

미래 사이버 보안 환경을 예측하고 대응 전략을 수립하는 것은 매우 중요하다. 미래의 사이버 위협을 예측하고 분석하는 연구를 강화하여 미래 사이버 보안 환경을 이해하고 적절한 대응 전략을 마련해야 한다[21]. 또한, 끊임없이 변화하는 사이버 보안 환경에 적응하기 위해 유연한 사이버 보안 기술의 개발이 필요하다. 이는 인공지능과 머신러닝을 활용한 자동화된 위협 탐지 및 대응 시스템 개발을 포함하며, 보다 효과적인 사이버 보안 대책을 구축하는 데 기여할 수 있다[23].

기술 혁신은 사이버 보안을 변화시키고 있으며, 이에 맞춘 정책의 개발이 필요하다. 기술 발전과 정책의 조화는 사이버 보안의 지속 가능성을 보장하는 핵심 요소이다[24]. 또한, 장기적인 관점에서 전략을 수립하여 글로벌 사건이 사이버 보안 환경에 미치는 영향을 고려해야 한다. 이를 통해 미래의 다양한 도전에 대비하는 강력하고 유연한 보안 체계를 마련하는 것이 중요하다.

정부와 산업계의 협력, 미래 사이버 보안 환경의 예측 및 대응 전략, 그리고 기술 혁신과 정책의 조화는 사이버 보안의 미래를 위한 중요한 축이다. 이러한 요소들은 통합적인 접근을 통해 사이버 보안의 지속 가능성을 보장하고, 국가 안보를 강화하는 데 기여할 것이다.

6. 결 론

위성통신과 무선통신 시스템의 보안 강화는 적성국의 사이버 공격에 대응하는 데 필수적이다. 이를 위해 첫째, 인공지능과 머신러닝을 활용한 첨단 사이버 보안 기술 개발과 신속한 대응 메커니즘 구축이 중요하다. 둘째, 글로벌 사이버 보안

협력과 정보 공유를 통한 국제적 위협 인식과 협력 체계 구축이 필요하다. 셋째, 정부, 산업계, 학계 간 협력을 강화하고 사이버 보안 인력 양성 및 교육에 주력해야 한다. 마지막으로, 지속적인 보안 평가와 시스템 업그레이드를 통해 취약점을 식별하고 해결하는 것이 중요하다. 이러한 전략적 접근을 통해 시스템 보안을 강화하고 사이버 공격에 대응할 수 있다.

참 고 문 헌

- [1] K. C. Woo and C. Polito, "The Evolution of North Korean Cyber Threats," The Asan Institute for Policy Studies, Feb. 20, 2019.
- [2] E. M. Lederer, "UN probing 35 North Korean cyberattacks in 17 countries," AP News, The Associated Press, Aug. 13, 2019.
- [3] S. M. Oh, "N. Korea intensifying cyber attacks against S. Korean shipbuilders: spy agency," Yonhap News Agency, Oct. 4, 2023.
- [4] M. H. Jung, "Experts warn of North Korea's evolving cyberattack capabilities," _The Korea Times_, Aug. 30, 2022.
- [5] "North Korea Cyber Threat Overview and Advisories," Cybersecurity & Infrastructure Security Agency (CISA), Dec. 3, 2023.
- [6] M. Nichols, "North Korea took \$2 billion in cyberattacks to fund weapons program: U.N. report," Reuters, Aug. 5, 2019.
- [7] S. Joo, S.-Y. Kim, and I.-G. Lee, "차세대 무선통신 네트워크 기술 동향 및 보안 이슈 분석," Review of KIISC, Korea Science, Jun. 30, 2021.
- [8] S. Park, "[우주산업 리포트]인공위성 겨냥한 사이버 공격이 현실화되고 있다," DongA Science, Mar. 25, 2022.

- [9] H.S. Yoon, M.W. Yun, Joshua Freilich, Steven Chermak, Robert G. Morris, and I. S. Kim, "Cyberterrorism : Trends and Reponses," Korean Institute of Criminology and Justice, Dec., 2012.
- [10] Ministry of National Defense, "해군지휘통제체계 성능 고도화 및 발전방안," Republic of Korea Navy Education Command, School of Information and Communications, Dec. 2012.
- [11] H. Song, "위성 해킹, 이미 시작됐다. 핵심 보안 기술 조속히 확보해야," Newsis, Dec. 3, 2023.
- [12] "2023년 사이버 보안위협 및 대응기술 전망," Security & Intelligence, Igloo Corporation, 2023.
- [13] Y. K. Jin, Y. J. Kim, J. S. Lee, and C. S. Choi, "디지털 안심국가 실현을 위한 중장기 로드맵," DUDUIT Co., Ltd., KISA, Dec. 8, 2021.
- [14] "인공위성과 사이버 안보," SPACE ISSUE No. 20, 항공우주연구원 미래전략본부, May 8, 2015.
- [15] G. Y. Moon, "Attacks on Satellite Communication Systems Are Actually Happening," Boannews, Aug. 10, 2018.
- [16] Y. Jung-Ho, K. Yoon-Sun, O. Jin-Young, L. Joo-Ho, "Methods and Devices for Signal Transmission and Reception in a Satellite Communication System," KR20210133109A, filed Nov. 24, 2020, and published Nov. 5, 2021.
- [17] P. Kim, J. Yoo, and W. Byun, "Research Trends in Global Wireless Communication Technology Based on the LEO Satellite Communication Network," in Electronics and Telecommunications Trends, vol. 35, no. 5, pp. 83-91, Oct. 01, 2020.
- [18] G. Shibuya, "위성통신을 이용한 효율적 원격감시시스템," 계장 (A025), vol. 46, no. 15, pp. 54-58, 2003.
- [19] A. Scrase and K. C. Koo, "Cybersecurity for Consumer IoT Standardisation and De-identifications solutions," ETSI and TTA Webinar, Nov. 10, 2021.
- [20] D. Kim, I. Choi, E. Lee, H. Cho, and W. Jang, "2030 Future Society Change and Cyber Threat Forecast Study," Nexintelligence Inc., KISA, Dec. 2021.
- [21] D. Lee, "Cybersecurity Technology and Standardization Trends in the Pandemic Era," in Convergence Research Review, Nov. 2022.
- [22] C. Park and H. Yim, "10 Emerging Technologies in the Era of Data Security," KISTEP Brief, 2023.
- [23] J. S. Lee, S. M. Choi, C. M. Ahn, and Y. Yoo, "Trends and Implications of Cybersecurity Policies in Major Countries," Electronics and Telecommunications Trends, 2023.
- [24] A. Kim, '[2023 AI Security Monitoring Report] A Major Counterattack on Security Threats with ChatGPT, the Hot AI Technology,' Boannews, Jun. 30, 2023.

저 자 약 력



정 진 우

이메일 : jinwoo.jeong@lignex1.com

- 1999년 한양대학교 전자통신공학과 (공학사)
- 2001년 한양대학교 전자통신공학과 (공학석사)
- 2016년 한양대학교 전자통신공학과 (공학박사)
- 2001년~2007년 LG전자 디지털미디어연구소 선임연구원
- 2016년~2017년 한양대학교 신호정보특화연구센터 연구 교수
- 2017년~2022년 국방정보본부 000사령부 00팀장
- 2023년~현재 LIG넥스원 사이버전자전개발단 수석연구원
- 관심분야: 신호정보, 사이버전자전, 안티드론 시스템, 위성통신, 무선통신



윤 상 범

이메일 : sangbom.yun@lignex1.com

- 1999년 고려대학교 제어계측공학과 (공학사)
- 2002년 고려대학교 전기공학과 (공학석사)
- 2002년~현재 LIG넥스원 사이버전자전개발단 수석연구원
- 관심분야: 신호정보, 사이버전자전, 안티드론 시스템, 위성통신, 무선통신

국내 방산기술보호 통합실태조사와 미국CMMC 제도의 연계방안 연구

장항배(중앙대학교), 김선영(아주대학교)

목 차

1. 서 론
2. 방위산업기술보호 통합실태조사
3. 미국의 사이버보안 성숙도모델 인증(CMMC) 제도
4. 결 론

1. 서 론

우리나라는 선택과 집종의 국방 R&D 투자를 통해 첨단 무기체계의 독자개발 능력을 확보해가고 있다. 국방기술진흥연구소는 국방분야 선진 16개국의 기술수준을 분석한 「2021 국가별 국방과학기술 수준 조사서」에서 우리 국방과학기술 수준을 세계 9위로 평가하였다. 2012년 10위권으로 진입한 이후 꾸준히 성장하고 있는 것이다. 이러한 국제경쟁력 확보를 통해 수출도 세계 10위권에 진입하는 등 꾸준한 성장세를 이어가고 있다.

이러한 기술 발전에 따른 보호 체계 구축과 대외적 신뢰도 제고를 위해 정부는 2015년 12월 「방위산업기술보호법」을 제정하고 이듬해 6월 동 법 「시행령」과 시행규칙을 제정하면서 기술보호체계를 구축하였다. 즉, 동 법의 제정으로 방산업체에 대한 실태조사, 기술유출자 처벌 및 방위산업기술 지정·고시 등 기술보호를 위한 근거를 마련한 것이다. 또한 방산업체를 대상으로 「방위산업기술보호법」의 실태조사와 「방위산업보안업무훈령」의 보안감사를 각각 실시하다가 기업의 부담 경감을 위해 2019년부터 통합하여 시행하고 있다. 또

한 방위산업과 관련한 국방과학기술 중 국가안보를 위하여 특별히 보호되어야 하는 방위산업기술을 지정 고시하고 있는데 2023년 현재 센서·정보통신·탄약 등 8개 분야 128개 기술이 지정된 상태이다

그러나 2020년 대우조선해양 핵추진 잠수함 기술, 2021년 한국항공우주산업의 KF-21 전투기 기술 등 첨단 방산기술을 노리는 사이버 해킹 사고가 연이어 발생하는 등 사이버 보안 역량이 취약한 것으로 평가되었다. 이런 가운데 2020년 세계 최고의 방산수출국이며 기술 주도권을 쥐고 있는 미국이 자국 국방사업 참여 기업에게 강력한 사이버보안 체계인 CMMC(CyberSecurity Maturity Model Certification) 프레임워크를 구축할 것을 요구하고 있어 이에 대한 대비가 필요한 상황이다

본 연구에서는 미국 CMMC 시스템을 살펴보고 방위사업청 주도로 매년 실시하고 있는 통합실태조사와 연계함으로써 CMMC 도입에 따른 대응책을 제시하고자 한다

2. 방위산업기술보호 통합실태조사

2.1 방위산업기술보호 정책

방산기술보호 주무부처인 방사청은 「방위산업 기술보호법」 제4조와 동 법 시행령 제3조를 근거로 2017년부터 5년 단위로 「방위산업기술보호 종합계획」을 수립하여 시행하고 있다. 동 종합계획은 국내외 기술 보호 환경을 분석하여 추진과제를 선정하고 세부 추진계획을 제시하는 중기계획으로서 국방부장관 주재로 방위산업기술보호위원회 심의를 거쳐 확정된다. 현재 「2022-2026 방위산업기술보호 종합계획」이 시행되고 있다.

「2022-2026 방위산업기술보호 종합계획」에서는 '방산업체 대상 사이버 위협이 증가하고 있으나 전문기관 부재 등 효과적 대응책이 부족한 실정이며, '기술유출 예방 차원에서 실태조사를 수행하고 있으나, 인력 부족으로 심층적 조사는 제한적임'을 문제점으로 지적하였다. 이에 대한 대책으로 향후 ①사이버위협 대응역량 강화 ②정부역량강화를 통해 방위산업기술 보호 기반을 강화할 것을 세부 과제로 선정하고 있다.

방위산업기술보호 목표 및 추진방향

방 향	추진과제
방위산업기술 보호기반 강화	① 사이버위협 대응역량 강화 ② 기술관리 체계 고도화 ③ 방산기술 수출 및 도입 시 보호기반 구축 ④ 방위산업기술보호 정부역량 강화
기술보호 대내외 협력 활성화	⑤ 기술보호 공조체계 내실화 ⑥ 기술보호 국제협력 활성화
기술보호 인식 제고 및 인력 관리 강화	⑦ 기술보호 교육 활성화 및 교육체계 고도화 ⑧ 국방연구개발 핵심인력 관리 강화 ⑨ 기술보호 인식 확산
자율적 보호체계 구축 유도 및 지원 확대	⑩ 기술보호체계 구축 지원 확대 ⑪ 방위산업기술보호 대상기관 책임성 강화 ⑫ 기술보호 지식 및 정보 공유 활성화

(그림 1) 방위산업기술보호 목표 및 추진방향(2022-2026 방위산업기술보호 종합계획, 방사청)

(그림 1) 방위산업기술보호 기반강화 중 '①사이버위협 대응역량 강화 ④방위산업기술보호 정부역량강화'가 통합실태조사와 관련된 추진과제라고 하겠다.

2.2 방위사업기술보호 통합실태조사

통합실태조사는 「방산기술보호법」 제12조(방위산업기술보호를 위한 실태조사)와 동 법 시행령 제17조에 근거하여 매년 방사청·국정원·방첩사 등 3개 기관 합동으로 방산업체를 대상으로 전수조사를 실시한다. 조사결과는 종합분석되어 해당 방산업체 및 유관기관에 통보되며 향후 기술보호 정책 뿐 아니라 해당 기업의 정부 무기체계 사업 참여 여부에도 영향을 미친다.

실태조사는 2020년도 이전에는 방위사업청이 「방산기술보호법」을 근거로 하는 실태조사와 방첩사에서 「군사기밀보호법」과 「방위산업보안업무훈령」을 근거로 하는 보안감사가 별도로 실시되었다. 그러나 업체 입장에서 유사한 내용의 점검을 이중으로 받는다는 불만이 표출되자 업체 부담을 경감시키기 위해 2020년부터 방위사업청 주관으로 3개 기관이 합동으로 실시하게 된 것이다. 매년 3월 초 정부터 사업장의 규모 또는 중요도에 따라 3~5일간씩 점검하고 있다.

통합실태의 핵심인 조사항목은 비공개이므로 방산기술보호지침으로 배포되어 사용하는 자가진단표를 통해 점검항목을 살펴보겠다. 2023년 자가진단표는 기술의 식별·관리, 인원통제, 시설보호, 정보보호, 연구개발 등 5개 분야로 구성되어 있다.

이중 CMMC와 직접 관련되는 정보보호 분야 점검항목은 <표 1>에서 보듯이 9개분야 38개항목이며 세부적으로 분류하면 79개 항목으로 증가한다. 정보보호 분야 점검은 점검관은 물론 피점검관까지 관련 분야에 대한 특별한 전문성을 요구하고 있다. 통합실태조사에서 정보보호 점검은 국정

〈표 1〉 정보보호분야 자가진단표 점검항목

구 분	점검 항목 (★) 핵심요소
① 정보보호시스템 설치 및 운용 (7개항목)	① UTM 또는 방화벽, IPS 설치·운영(★) ② 바이러스 백신 프로그램 설치·운영(★) ③ DRM 설치 운영(★) ④ 자료유출방지시스템(DLP 등) 설치 운영(★) ⑤ 네트워크 접근제어 인증시스템설치(★) ⑥ 보안정책이력 등 관련 로그 존안(★) ⑦ 보안취약점 분석 및 평가(★)
② 외부망 차단 (6개항목)	① 외부망 차단체계 구축 운영(★) ② 패치관리시스템 및 백신서버 분리 운용 ③ 네트워크 접근제어(NAC)를 설치하여 비인가 기기 접속 통제(★) ④ 관리대상기술 전산자료 반출시 망간 자료교환시스템 운용 ⑤ 망간자료교환시스템 이용시 압축파일 전송 불가토록 조치 ⑥ 분기별 취약점 분석 평가(★)
③ 보안관제 (3개항목)	① 보안관제 시스템 설치·운영(★) ② 보안관제시스템 관리 ③ 관제결과 이상 발생시 유관기관 통보 및 이행조치
④ 긴급사태 예방 및 복구대책 (2개항목)	① 긴급사태 발생에 대한 관리대상기술자료 백업 및 복구계획 수립(★) ② 긴급사태 발생시 유관기관 신고
⑤ 정보통신망 원격 관리 및 외부업체 관리 (4개항목)	① 지정된 단말기에서만 원격관리(★) ② 외부업체의 정보통신망 유지보수 보안대책 수립(★) ③ 외부업체 정보통신망 접속 통제 ④ 외부업체 반입 정보통신기기 관리
⑥ 정보통신기기 및 저장매체 관리 (6개항목)	① 지정된 정보통신기기 및 저장매체 도입 총괄(★) ② 정보통신기기 개별 등록 ③ 정보보호시스템 설치 후 정보통신망 연결 ④ 녹음,촬영 등 정보보호시스템이 통제할 수 없는 행위 통제 ⑤ 정보통신기기 및 저장매체 외부 반출시 포맷 등 보안대책 ⑥ 정보통신기기 및 저장매체 분실시 유관기관 신고
⑦ 관리대상기술 접근범위 제한 (3개항목)	① 관리대상기술 자료별 접근범위 및 권한에 대한 정책수립(★) ② 기술자료 보관 주컴퓨터(서버) 접속기록 생성 유지(★) ③ 관리대상기술 관련 시스템 접근시 경고문구, 출력시 이력표시
⑧ 관리대상기술 전산자료 반출 (3개항목)	① 외부 전자메일 발송시 해당 부서장 승인 전송(★) ② 파일 첨부메일 발신시 일시, 발신자, 수신자 및 파일내용 기록(★) ③ 저장매체를 활용한 전산자료 반출 통제
⑨ 자료유출 관리 대응 (4개항목)	① 전자메일을 통한 무단자료반출 확인 및 추후조치(★) ② 이동식 저장매체 관리(★) ③ PC·노트북 등 자산관리(★) ④ 인터넷 PC에서 업무자료 작성 및 저장금지(★)

출처 : 방위산업기술보호지침

원이 전담하다가 올해부터 중소·중견기업에 대해서는 방첩사도 참여하고 있다. 한편 방사청은 실태조사관의 전문성 제고를 위해 산하에 「방위산업 기술보호센터」를 설립하고 실태조사 전문 인력(5명)을 투입하고 있다.

통합실태조사는 각 점검 항목별로 정성·정량 이행여부 등을 구분하여 확인한다. 조사결과에 따라 개선권고·시정명령 및 최고 3000만원의 과태료 부과 등 행정조치도 따른다. 또한 조사결과 우수한 점수를 획득한 기업은 무기체계 제안서에서

가점을 받는 등 인센티브도 주어지고 있다. 즉, 통합실태조사가 방산업체 규모나 참여사업 수준 등에 무관하게 동일한 보호수준을 요구하고 협력업체의 경우는 체계업체에서 자체적으로만 점검하는 등 문제점도 지적되고 있지만 통합실태조사는 방산업체가 기술보호를 위해 관심과 노력을 투자하도록 유도하는 결정적인 역할을 하고 있는 것이다

3. 미국의 사이버보안 성숙도모델 인증(CMMC) 제도

3.1 CMMC(CyberSecurity Maturity Model Certification) 도입 배경

미국 대통령 경제자문위원회CEA, Council of Economic Advisors)는 악의적인 사이버 활동이 2016년 미국 경제에 570억 달러에서 1,900억 달러의 손실을 입힌 것으로 추정한 가운데 2018년도에는 중국에 대한 무역적자가 4,192억 달러에 이르는 등 사상 최고치에 이르게 된다. 미국 정부는 막대한 무역적자의 원인 중에서 기술 및 지식재산권에 대한 중국의 불법적인 침해가 있다고 보고 이에 대한 대응으로 「수출통제개혁법(Export Control Reform Act: ECRA)」을 제정한다. 「수출통제개혁법」은 신형기술과 기반기술을 새로이 수출통제 대상으로 포함시키고, 기술의 식별 및 통제 절차를 강화하는 법이다. 또한 미국 정부는 첨단산업 분야 중국 유학생의 비자 단축(5년→1년, '18) 중국 군부 관련 연구인력 입국금지(1,000명

비자취소, '20비자취소) 등 인적교류도 제한한다.

특히 미국 국방부는 악의적인 사이버 범죄자들이 지속적으로 방위산업계(DIB, Defence Industrial Base)와 국방부(DoD, Department of Defence)의 공급망을 표적으로 삼고 있다고 분석하고 미 국방사업에 참여하는 해외업체를 포함한 모든 업체에 일정 수준의 사이버 보안 체계 구축을 의무화하는 CMMC 제도를 도입키로 한다. 이를 위해 2020년 1월 사이버보안제도 운영을 위한 인증기관(CMMC-AB, Accreditation Body)을 설립하고 2020년 3월 CMMC 모델 1.0을 발표한다. CMMC 모델1.0은 5등급으로 구성되며 17개 도메인(Domain)과 171개 프랙티스(Practice)로 구성되었다. 그러나 미국 방산업체들이 CMMC 프레임워크 구축에 반발하자 이를 수용한 미국 국방부는 2021년 12월 3개 등급 14개 도메인 110개 프랙티스로 구성된 모델 2.0을 발표하였다. CyberAB에서는 CMMC 모델 2.0이 모델1.0에 비해 5개에서 3개로 등급이 간소화되었고 사이버보안 역량을 강화시키면서 중소기업이 구현할 수 있는 비용 효율적이고 합리적으로 설계되었다고 강조하고 있다.

즉, CMMC는 점점 더 빈번하고 복잡해지는 사이버 공격으로 부터 미국 방위산업계(DIB)를 보호하기 위해 그동안 특별하게 기밀로 분류하지 않고 공유되었던 통제된 미분류정보(CUI, Controlled Unclassified Information) 및 연방계약정보(FCI, Federal Contract Information)의 보



(그림 2) CMMC 타임스케치

호를 강화하는 것을 목표로 미국 국방부(DoD)에서 구축한 프로그램인 것이다. 2026년부터 미국 국방사업에 참여하기 위해서는 CMMC 인증 요구 레벨을 RFP상에 포함시켜야 할 것으로 예상된다

- 연방계약정보(FCI, Federal Contract Information) : 제품 또는 서비스를 개발하거나 정부에 제공하기 위한 계약에 따라 정부가 제공하거나 정부를 위해 생성한 정보로서 공개할 목적이 아닌 정보를 의미. 정부가 공공 웹사이트 등에서 대중에게 제공하는 정보나 결제 처리에 필요한 단순 거래 정보는 포함하지 않는다(출처: 48 CFR§ 52.204-21, cyberab.org, CMMC 용어집 및 약어)
- 통제된 미분류정보(CUI, Controlled Unclassified Information) : 법률, 규정 및 정부 차원의 정책에 따라 보호 또는 배포 통제가 필요한 정보(2009년 12월 29일자 행정명령 13526호, 국가 기밀 보안 정보, 또는 그 이전 또는 후속 명령이나 개정된 1954년 원자력법에 따라 기밀로 분류되는 정보는 제외). (출처: NIST SP 800-171 Rev 2, cyberab.org, CMMC 용어집 및 약어)

3.2 CMMC(CyberSecurity Maturity Model Certification) 등급

CMMC는 가장 널리 인정되고 있는 미국 국립 표준기술연구소(NIST) 사이버보안표준을 사용하

고 있고 국방사업 참여 계약업체의 수준을 3개 등급으로 구분해서 인증을 요구하고 있다

업체가 정부에 의해 제공되거나 생산된 정보인 FCI(연방계약정보)만을 취급하면 가장 낮은 수준인 1등급 인증을 요구되며 연 단위로 자체 심사한다. 업체가 CUI(통제된 미분류정보) 까지 취급하게 되면 2등급 이상의 인증이 요구되며 국가 중요 보안 정보에 대해서는 3년 주기로 제3자에 의해 심사를 받는다. 최고 전문등급인 3등급은 NIST SP 800-172에 기반하는데 아직 발표되지 않은 상태이다.

3.3 미국의 CMMC와 통합실태조사

CMMC 실행을 위해 미국 국방부가 승인한 유일한 인증기관은 CyberAB이다. CyberAB는 국방부로부터 자금지원을 받지 않는 비영리법인으로서 수익원은 시스템 내 참가자로 부터 자격 등록 및 갱신 수수료 등으로 유지된다.

CMMC의 시스템내에는 인증기관인 CyberAB를 중심으로 심사기관 C3PAO(CMMC 3rd Party Assessor Organization), 컨설팅 기관 RPO(Registered Provider Organization), 교육 훈련기관 LTP(Licensed Training Provider), 교육커리큘럼 개발기관 LPP(Licensed Publishing Partner) 등이 주요 구성기관이다

특히 CMMC 등급 취득의 핵심인 심사기관 C3PAO 로 승인받기 위해서는 미국의 신용조사 전문회사인 Dun & Bradstreet 로 부터 배경 조사

(표 2) CMMC 2.0 등급별 프랙티스 및 심사

등 급	프랙티스 / 모델	심 사
3등급 (전문, Expert)	• 110+개 프랙티스 • NIST SP 800-172에 기반	• 3년주기 정부 주도심사
2등급 (고급, Advanced)	• 110개 프랙티스 • NIST SP 800-171(r2)에 연계	• 국가중요보안정보는 3년주기 제3자 심사 • 일부 프로그램은 연 단위 자체심사
1등급 (기본, Foundational)	• 17개 프랙티스 • 48 CFR 52.204-21에 명시된 기본적인 이행과제	• 연 단위 자체 심사

〈표 3〉 CMMC의 14개 도메인과 2등급 110개 프랙티스 요약 (NIST SP 800-171)

도메인	프랙티스
❶ 접근통제 (AC)	- 시스템 접근 요구사항 설정 - 원격 시스템 접근통제 - 내부 시스템 접근통제 - 무선, 모바일 장치, 휴대용 저장장치 통제
❷ 인식및교육훈련 (AT)	- 역할 기반 위험인식, 교육훈련 - 내부자 위협 인식
❸ 감사및책임추적 (AU)	- 감사 요구사항 정의 - 감사정보 식별 및 보호 - 감사 수행 - 감사로그 검토 및 관리
❹ 구성관리 (CM)	- 구성 기준 설정 - 최소 기능만 구성 - 구성 및 변경관리 수행 - 사용자 설치 통제
❺ 신원확인및인증 (IA)	- 신원 확인 - 비밀번호 관리 - 인증, 다단계 인증, 재생방지 인증
❻ 사고대응 (IR)	- 사고대응 계획 - 사고대응 테스트 - 이벤트 감지 및 보고
❼ 유지관리 (MA)	- 유지보수 관리 - 원격 유지관리 통제 - 장비 소거 및 미디어검사
❽ 미디어보호 (MP)	- 미디어 식별 및 표시 - 미디어 처리 - 백업 보호 - 미디어 보호 및 통제 - 운송 중, 미디어 보호
❾ 인원보안 (PS)	- 신원조사 - 인사조치 중 통제필요정보 보호
❿ 물리적보안 (PE)	- 물리적 접근 제한 - 시설 모니터링 - 방문자 에스코트 - 대체 작업장 보안
⓫ 위험평가 (RA)	- 위험 식별 및 평가 - 취약점 보완 - 취약점 진단
⓬ 보안평가 (CA)	- 시스템보안 계획수립 및 관리 - 보안통제 모니터링 - 보안통제 평가
⓭ 시스템 및 통신 보호 (SC)	- 시스템 및 통신에 대한 보안 요구사항 정의 - 시스템 경계에서 통신 통제 - 암호키 관리
⓮ 시스템 및 정보 무결성 (SI)	- 정보시스템 결함 식별 및 관리 - 비인가 사용 식별 - 악성코드 보안 - 통신 모니터링

를 받은 후 비즈니스 고유 식별 코드이며 이미 미국 정부와의 계약 프로세스에서 중요한 역할을 하고 있는 DUNS 번호를 받아야 한다. 그리고 무엇보다도 100% 미국 시민권자 소유의 기업이어야만 한다. 또한 CMMC 인증심사원(CCA)도 미국 시민권자이어야 취득할 수 있도록 제한되어 있다. 우리 정부와 방산업체 입장에서 CMMC 진입장벽이 너무 높을 뿐 아니라 기술 보호를 위한 인증심사 과정에서 우리 기업 내부 중요 정보가 외국 기업에게 노출될 우려가 있는 것이다.

이러한 문제를 해소하기 위해 방사청은 매년 실시하고 있는 통합실태조사를 미국 CMMC 인증과

연계시키는 방안을 추진하고 있다. 즉 우리 정부가 주관하는 통합실태조사를 완료하면 미국 CMMC 1등급에 해당하고 2등급의 경우는 필요시 추가 인증하는 내용으로 2024년 중 미국과 상호인정(MRA) 체결할 계획이다.(참고 : 2023 전반기 방산기술보호 합동설명회, 방위사업청)

이를 위해 방사청은 통합실태조사와 CMMC 등급 취득을 연계하기 위해 통합실태조사를 분석하여 점검항목 보완 연구를 진행중이다. 즉 통합실태조사 점검항목 내용과 이행 점검을 CMMC 프랙티스와 매칭시킴으로써 CMMC가 요구하는 보안수준을 확보한 것으로 인정 받겠다는 계획이다.

〈표 4〉 CMMC 시스템 및 통신보호(SC)와 통합실태조사 자가진단표 대응분석

CMMC 시스템 및 통신보호 (이행과제 번호/내용)	실태조사 자가진단 항목 (점검번호/ 점검내용)	대응결과
SC.L1.3.13.1 경계 보호	4.1 정보보호 시스템 설치 및 운용	대응 가능
SC.L1.3.13.5 공개접근 시스템 분리	4.2.1 외부망차단체계 구축 운용	대응 가능
SC.L2-3.13.2 보안 공학적 원칙사용	아키텍처 설계, S/W기술 개발 및 시스템 공학 원칙 적용	대응 부족
SC.L2-3.13.3 역할 분리	4.6 정보통신기기 및 저장매체관리	대응 가능
SC.L2-3.13.4 공유 자원 통제	4.7 자료별 접근범위 제한	대응 가능
SC.L2-3.13.6 예외에 의한 네트워크 통신	4.1 정보보호 시스템 설치 및 운용	대응 가능
SC.L2-3.13.7 분할 터널링	4.2 정보통신망 외부망과 차단 4.4 긴급사태 대비	대응 가능
SC.L2-3.13.8 전송 자료 보호	4.6 정보통신기기 및 저장매체관리	대응 가능
SC.L2-3.13.9 연결 종료	4.7 자료별 접근범위 제한	대응 가능
SC.L2-3.13.10 암호키 관리	4.1 정보보호 시스템 설치 및 운용	대응 가능
SC.L2-3.13.11통제필요정보 암호화	4.1 정보보호 시스템 설치 및 운용	대응 가능
SC.L2-3.13.12 협업 장치 통제	협업 컴퓨팅장치 원격활성화 금지 및 사용중지 표시	대응 부족
SC.L2-3.13.13 모바일 코드 통제	자바스크립트, 액티브엑스 등 모바일코드 사용 통제 및 감시	대응 부족
SC.L2-3.13.14 인터넷전화기술통제	인터넷전화 기술의 시스템 위협 대비 통제 및 감시	대응 부족
SC.L2-3.13.15 통신 진본성 보호	4.1 정보보호 시스템 설치 및 운용 4.6 정보통신기기 및 저장매체관리	대응 가능
SC.L2-3.13.16 저장된 자료 보호	4.1 정보보호 시스템 설치 및 운용	대응 가능

그런데 통합실태조사의 자가진단표와 CMMC 프랙티스를 비교했을 때 가장 큰 차이가 나는 도메인은 CMMC의 「시스템 및 통신보호(SC)」이다. 아직 CMMC 프랙티스를 실제 적용한 사례와 정보가 제한적이라서 판정에는 제한이 따르지만 「시스템 및 통신보호(SC)」16개 프랙티스 중에서 ‘보안 공학적 원칙 사용’ (SC.L2-3.13.2) “협업 장치 통제”(SC.L2-3.13.12) ‘모바일 코드 사용 통제와 감시’(SC.L2-3.13.13) ‘인터넷 전화 기술 사용 통제 및 감시’ (SC.L2-3.13.14) 등은 자가진단표의 항목과 매칭하기 어렵다. 게다가 모두 고난도의 보안 수준을 요구하는 내용으로서 현장에서 일시에 반영하는 것은 부담이 큰 프랙티스이다. 다음 <표 4>는 CMMC ‘시스템 및 통신보호’ 프랙티스와 자가진단표의 점검항목을 매칭시킨 후 대응 가능 여부를 판정한 내용이다

4. 결 론

미국 국방부는 미국의 국방사업을 지원하는 외국기업이 민감한 국가안보 정보를 보호할 수 있도록 CMMC 프레임워크를 갖추도록 요구하고 있다. 이에 주무부처인 방위사업청도 국내방산업체들이 순조롭게 CMMC에 대비할 수 있도록 통합 실태조사 완료가 미국 CMMC 등급 인증 취득으로 연계되도록 추진하고 있다. 이를 위해서는 CMMC를 충족할 수 있도록 통합실태조사 항목을 추가적으로 보완하는 작업이 선행되어야 할 것이다.

그리고 무엇보다도 미국 국적자 또는 미국 소유 기업만 심사관 및 심사기관 자격이 부여되는 현재의 CMMC제도는 우리의 사이버안보 주권을 위협할 수 있다. 따라서 방위사업청은 미국과 CMMC 상호인정협약(MRA) 체결과 병행하여 CMMC 인준기준과 절차를 준수하되 CMMC 심사원에 한

국 국적자에 의한 인증심사가 가능하도록 해야 할 것이다. 또한 공정성과 객관성 확보를 위해 CyberAB와 같은 독립된 비영리법인으로 인증기관을 설립하는 등 관련 체계도 갖추어 나가야 할 것이다.

끝으로 방산업체들은 CMMC 도입으로 통합실태조사 과정에서 난이도가 가장 높은 정보보호 비중이 더욱 높아지는데 부담을 갖고 있다. 더구나 CMMC 제도 초기인 관계로 관련 전문가도 부족한데다 CMMC 프랙티스 구현에 대한 경험 사례도 없는 등 정보가 매우 제한적이다. 따라서 정부는 제도 개선과 더불어 방산업체를 대상으로 CMMC 인증제도와 등급별 프랙티스 등을 충분히 이해할 수 있는 다양한 교육·훈련 프로그램을 개설하여 방산업체들이 CMMC 도입에 대비할 수 있도록 지원해야 할 것이다.

참 고 문 헌

- [1] 한국산업보안연구학회, “산업보안학” pp. 437-453, 박영사, 2019.
- [2] 이민재 역, “CMMC의 이해”, pp.115-345, 2021
- [3] 박언경, 왕상한, “미국 수출통제개혁법 제정의 함의”, 법제연구제 61호, pp.300-304, 2021
- [4] 김동선, 류연승, “미국 CMMC제도 대응을 위한 통합실태조사 제도개선연구”, 한국방위산업학회지, 제29권, 제3호, pp.54-57, 2022
- [5] 방위사업청(www.dapa.go.kr) “2022-2026 방위산업기술보호 종합계획” pp.6-13,
- [6] 방위사업청, “2023 전반기 방산기술보호 합동설명회”, 방위사업청, 국정원, 방첩사
- [7] 한국산업기술보호협회, 2023년 통합실태조사관 직무역량강화 교육, 2023.8,
- [8] 한국산업기술보호협회, 2023년 방위산업기술보호 책임자교육, 2023.6

[9] 산업보안실무위원회, “국가공인 산업보안관리사”, pp.60-61, 케듀아이, 2023

[10] 김혜정, “기술보호에 관한 주요 국내법분석 및 시사점, 한국지식재산연구원, pp.4-13, 2022-29호

저 자 약 력



장 항 배

이메일 : hbcchang@cau.ac.kr

- 2014년~현재 중앙대학교 산업보안학과 교수
- 현재 한국공학한림원 회원 (기술경영정책)
- 전 방위사업청 방위산업기술보호 실무위원회 위원
- 전 국가과학기술자문회의, ICT융합전문위원회 위원
- 관심분야: 산업보안, 방산기술보호, 데이터보안



김 선 영

이메일 : syk4590@gmail.com

- 2019년~현재 아주대학교 지식정보공학과 교수
- 2023년 10월~현재 CMMC RP
- 현재 한국산업보안관리사협회 부회장
- 전 한국산업기술보호협회 센터장
- 관심분야: 기술보호 실태조사, 방위산업보안, 보안지식경영

국방 RMF 연구 사례 분석

조광수·김예준·안정근·김정현·곽지원·김해나·백근우·김승주 (고려대학교)

목 차

- | | |
|--|--|
| <ul style="list-style-type: none"> 1. 서 론 2. RMF 개념 및 단계 3. 국외 RMF 동향 | <ul style="list-style-type: none"> 4. 국내 RMF 동향 5. 결 론 |
|--|--|

1. 서 론

소총, 기관총, 전차 및 야포 등의 다양한 무기체계들이 점차 네트워크로 연결되기 시작하였다. 이는 지휘관이 전장 상황을 빠르게 인지하고 신속하게 결심 및 지휘통제 할 수 있도록 만들기 위함이다. 하지만, 무기체계가 네트워크에 연결됨으로써 무기체계에 침투할 수 있는 공격 표면이 확대되었으며 확대된 공격 표면으로 인한 사이버 위협의 발생 가능성도 함께 증가하였다. 무기체계에 대한 사이버 위협이 늘어남에 따라 자연스럽게 공격자로부터 무기체계를 안전하게 보호하기 위한 무기체계 사이버보안의 중요성 또한 대두되고 있다[1]. 미 국방성은 증가하는 사이버 위협으로부터 무기체계를 안전하게 보호하기 위해 과거부터 평가 및 획득 체계를 개발하여 국방획득체계에 적용하였다. 통칭 Orange Book으로 불리던 TCSEC (Trusted Computer System Evaluation Criteria) 부터 DITSCAP (Defense Information Technology Security Certification and. Accreditation Process), DIACAP (Department of Defense Information

Assurance Certification and Accreditation Process)을 거쳐 가장 최신에 개발된 RMF A&A (Risk Management Framework Assessment & Authorization)까지 다양한 제도를 발전시키며 사용하고 있다[2]. 현재 사용되고 있는 RMF A&A의 가장 큰 특징은 잔존위험도를 기반으로 획득 여부를 결정한다는 것이다. RMF A&A 이전의 평가 수단은 체크리스트 형식으로 구성되어 전체 평가항목에 대해 통과하도록 요구되었다. RMF A&A의 경우 무기체계 개발에 필요한 막대한 비용 등을 고려하여 통과하지 못한 평가항목이 존재하더라도 임무 수행의 관점에서 위험도를 판단한 후 획득 여부를 결정하게 된다. 물론, 통과하지 못한 평가항목은 추후 보완 조치가 올바르게 취해질 수 있도록 요구된다[3].

미국의 경우, 국방 분야 대상으로 개발 및 활용되는 DoD (Department of Defense)의 RMF A&A, 연방정부 및 일반 산업 분야에서 활용할 수 있는 NIST (National Institute of Standards and Technology)의 NIST SP 800-37이 존재한다. 이 중 NIST SP 800-37은 전체 RMF 프로세스부

터 상세한 보안통제항목 Baseline까지 관련 문서가 모두 민간 영역에 공개되어 있기에 RMF를 적용하고자 하는 민간 업체에서 참조할 수 있는 충분한 자료를 획득할 수 있다. 반대로, 국방 분야에서 활용되는 RMF A&A의 경우 간단한 예시로 활용할 수 있는 극히 일부 자료만을 DoD 산하기관인 DCSA (Defense Counterintelligence and Security Agency) 등을 통해 공개하고 있다[4].

미 국방성은 RMF A&A를 개발하여 자국 내에서 적용하는 것뿐만이 아니라 외부 요인에 의해 미군의 중요 자원이 위협받지 않도록 2015년 국방 사이버 전략의 일부분으로 동맹국에 대한 사이버 보안 능력을 강화할 수 있도록 적극 지원할 것을 발표하였다[5]. 이러한 국방 사이버 전략 구현의 일환으로 우리나라를 포함한 동맹국들 중 미군의 무기체계와 직간접적으로 연동되는 무기체계 운용 국가에 대해 RMF 적용을 요구한 바 있다[6]. 이러한 요구에 대응하기 위해 우리나라에서도 국방부를 비롯한 유관기관에서 RMF 제도의 적용 및 대응하기 위한 연구와 시범 적용 사업을 수행하고 있다. 미국과 우리나라는 국방 획득체계의 제도적 기반과 요구되는 보안 수준이 상이하기 때문에 기존 미국의 RMF A&A를 그대로 도입할 수 없다[7]. 이에 우리나라에서는 미국의 RMF A&A와 NIST SP 800-37을 벤치마킹하여, 국방 사이버보안위험관리제도인 K-RMF (Korea-RMF)를 개발하고 있다. 하지만, 현재까지는 해당 K-RMF 제도와 관련하여 공개된 공식 문서는 존재하지 않으며 2026년 전면 적용될 예정에[8] 따라 추후 관련 자료들이 발표될 것으로 보여진다. 본 연구에서는 국내외에서 RMF와 관련하여 어떠한 연구들이 수행되었는지 조사한다. 이를 통해 추후 K-RMF 제도 개발 및 관련 연구를 수행함에 있어서 인사이트를 제공하고자 한다.

2. RMF 개념 및 단계

NIST에서 관리하고 공개하는 용어집인 NIST Glossary[9]에 따르면 RMF는 “A structured approach used to oversee and manage risk for an enterprise.”로 정의된다[10]. 즉, 어떠한 조직의 비즈니스 목표 달성 또는 주어진 임무 수행에 있어서 발생 될 수 있는 잠재적 위험을 미리 식별하고 완화 시키기 위해 수행해야 하는 일련의 활동들과 관련 바탕 자료들을 모아둔 하나의 방법론이다. 현재 공개되어있는 연방정부 및 일반 산업 분야 대상의 RMF인 NIST SP 800-37에 따르면 RMF 프로세스는 크게 총 7가지 단계로 구성되어 있으며, 점차 발전하고 정교해지는 공격 기법에 대응하고 이전에 미처 발견하지 못한 위험 요소를 지속적으로 추적 감시 할 수 있도록 7단계를 반복 수행하도록 만들어져있다. NIST SP 800-37 문서를 중심으로 RMF 각 단계에 대한 활동을 뒷받침할 수 있는 다양한 문서들이 존재한다. 대표적으로, 조직이 보안 목표를 달성하기 위해 필요한 보안 요구사항인 전체 보안통제항목을 NIST SP 800-53 문서로 작성하여 배포하고 있다. 다음 2.1 ~ 2.7절에서는 RMF 프로세스를 구성하는 각 단계에 대해 간략히 설명한다.

2.1 준비(Prepare) 단계

준비 단계는 RMF를 적용하고자 하는 조직이 체계 개발 프로젝트를 시작하기에 앞서서 이후 RMF 단계들을 원활히 진행하는데 필요한 사전 활동을 수행하는 단계이다. 준비 단계 활동을 통해 조직 구성원들의 RMF에 대한 이해도를 높이고, 보안 통제항목 baseline 및 공통 통제항목 등 추후 체계 보안 분류 단계 ~ 모니터링 단계에서 활용할 자원을 확보한다. NIST SP 800-37에 따르면 준비 단계는 다음 <표 1>과 같은 18개 활동으

〈표 1〉 준비 단계 세부 활동 목록

활동	활동 수행 결과 및 산출물
조직 수준의 준비 활동	
P-1 위험관리 역할 식별	- RMF에 따라 체계를 개발 및 획득하기 위한 중요 역할들이 식별되고 조직 구성원 개인에게 할당되어야 함
P-2 위험관리 전략 수립	- 조직이 감내(수용)할 수 있는 위험 수준에 관한 결정 및 표현을 포함하는 위험관리 전략이 수립되어야 함
P-3 위험평가 - 조직	- 조직 전체적인 관점에서 위험평가가 수행되고, 기존의 위험평가 결과가 최신화되어야 함
P-4 통제항목 baseline 구축 (Optional)	- 활용가능한 통제항목 baseline 및 사이버보안 프레임워크 프로파일 구축
P-5 공통 통제항목 식별	- 개발 또는 획득하고자 하는 체계가 상속할 수 있는 공통 통제항목의 식별 및 문서화, 배포
P-6 영향도 우선순위 선정 (Optional)	- 조직의 임무 및 비즈니스 목표에 대해 동일한 영향 수준을 지니는 체계에 대한 우선순위 선정
P-7 지속 모니터링 전략 수립 - 조직	- 조직 전체적으로 구현된 통제항목의 효과를 모니터링 하기 위해 필요한 통제항목 모니터링 전략을 개발 및 구현
체계 수준의 준비 활동	
P-8 임무 및 비즈니스 식별	- 개발 및 획득하고자 하는 체계가 지원해야 하는 조직의 임무, 비즈니스 기능, 및 프로세스를 식별해야 함
P-9 체계 이해관계자 식별	- 개발 및 획득하고자 하는 체계와 관련된 이해관계자를 모두 식별하고 목록화해야 함
P-10 자산 식별	- P-9에서 식별된 이해관계자들의 중요 자산 목록을 식별해야 함
P-11 인가 범위 식별	- 개발 및 획득하고자 하는 인가 범위(체계)를 식별해야 함
P-12 정보 유형 식별	- 개발 및 획득하고자 하는 체계에 의해서 처리, 저장, 및 전송되는 정보 유형을 모두 식별해야 함
P-13 정보 수명주기 이해	- P-12에서 식별된 정보 유형들에 대한 체계 내 수명주기(즉, 언제 생성되어 어떠한 과정을 거쳐 언제 소멸되는지)를 식별하고 이해해야 함
P-14 위험평가 - 체계	- 개발 및 획득하고자 하는 체계에 대한 위험평가가 수행되고, 기존의 위험평가 결과가 최신화되어야 함
P-15 요구사항 정의	- 보안 및 개인정보보호 요구사항이 정의되고 각 요구사항 간 우선순위가 선정되어야 함
P-16 조직 아키텍처 결정	- 개발 및 획득하고자 하는 체계가 조직 내 어느 위치에 설치되고 조직에 기존에 존재하는 타 체계와 어떻게 연동되는지 그 아키텍처가 결정되어야 함
P-17 요구사항 할당	- P-15에서 정의된 요구사항을 체계 또는 체계의 운영 환경에 적절히 배치해야 함
P-18 체계 등록	- 관리, 유지보수 및 모니터링 목적으로 조직 내 관리 체계(형상 관리 서버 등)에 개발 및 획득하고자 하는 체계가 등록되어야 함

로 구성되며, 7개의 “조직 수준”활동과 11개의 “체계 수준”활동으로 구분된다.

2.2 체계 보안 분류(Categorize) 단계

체계 보안 분류 단계는 RMF의 첫 번째 주요 단계로, 조직이 개발 및 획득하고자 하는 체계의 임무 영향도를 판단하는 단계이다. 이때, 임무 영

향도란 위험도와 유사한 의미를 가지며, 조직에게 주어진 임무 또는 비즈니스 목표를 달성하는데 있어서 해당 체계 또는 정보 유형이 얼마나 큰 영향을 미치는지 수치화 한 것을 의미한다. NIST SP 800-37에 의하면 RMF에서는 이러한 임무 영향도를 분석하는 기준으로 CIA(C: Confidentiality - 기밀성, I: Integrity - 무결성, A: Availability - 가용성)의 3가지를 활용한다. 본 체계 보안 분류

〈표 2〉 체계 보안 분류 단계 세부 활동 목록

활동	활동 수행 결과 및 산출물
C-1 체계 설명	- 조직이 개발 및 획득하고자 하는 체계의 특징이 모두 설명되고 문서화되어야 함
C-2 보안 분류 선정	- 체계 내에서 처리, 저장, 전송되는 정보를 포함하여 조직이 개발 및 획득하고자 하는 체계의 보안 분류가 선정되어야 함 - 체계 보안 분류의 결과가 보안 계획, 개인정보보호 계획, 공급망 위험관리 계획에 문서화되어야 함 - 체계 보안 분류의 결과가 조직의 임무, 비즈니스 기능, 임무 및 비즈니스 프로세스를 보호하기 위한 조직의 아키텍처 및 활동 목적과 일치하도록 조정해야 함 - 체계 보안 분류의 결과가 조직의 위험관리 전략을 충분히 반영하여야 함
C-3 체계 보안 분류 검토 및 승인	- 체계 보안 분류의 결과가 조직의 임원들에 의해 충분히 검토되고 최종적으로 승인되어야 함

단계에서 결정된 임무 영향도를 바탕으로 조직은 체계 개발 및 획득의 기준(즉, 보안 통제항목)을 선정하고 평가하게 된다. NIST SP 800-37에 따르면 체계 보안 분류 단계는 다음 <표 2>와 같은 3개 활동으로 구성된다.

2.3 보안통제항목 선정(Select) 단계

보안통제항목 선정 단계는 RMF의 두 번째 주요 단계로, 체계 보안 분류 단계에서 결정된 임무 영향도 및 체계 보안 분류에 따라 조직 및 체계를 보호하는데 필요한 보안통제항목을 선택, 교정, 할당하는 단계이다. NIST SP 800-37에 따르면 이전 단계에서 결정된 보안 분류에 따라 체계에 구

현되어야 하는 보안통제항목의 기본 목록이 결정되며, 이를 보안통제항목 **baseline**이라고 칭한다. NIST에서는 본 단계에서 활용할 수 있는 전체 보안통제항목을 NIST SP 800-53 문서로 공개하고 있으며, 임무 영향도별 구현되어야 하는 보안통제항목 **baseline**을 NIST SP 800-53B 문서로 공개하고 있다. 하지만 미 국방성에서 활용 중인 군용 RMF A&A의 경우 별도로 보안통제항목 **baseline**을 공개하고 있지 않다. NIST SP 800-37에 따르면 보안통제항목 선정 단계는 다음 <표 3>과 같은 6개 활동으로 구성된다.

〈표 3〉 보안통제항목 선정 단계 세부 활동 목록

활동	활동 수행 결과 및 산출물
S-1 통제항목 선택	- 결정된 위험도(체계 보안 분류)에 상응하여 체계 및 조직을 보호하는데 필요한 보안통제항목 baseline 을 선택해야 함
S-2 통제항목 교정	- 체계의 특성 및 조직 내 보안 정책에 따라 보안통제항목이 교정되어야 함
S-3 통제항목 할당	- 각 보안통제항목이 체계특정, 하이브리드, 또는 공통통제항목 중 한가지로 지정되어야 함 * <i>하이브리드 보안통제항목: 하나의 보안통제항목 내 세부 항목이 부분적으로 체계특정적, 공통적 특성을 모두 갖는 것</i> - 각 보안통제항목이 체계 내 적절한 위치에 할당되어야 함
S-4 통제항목 구현 계획 문서화	- 선택되고 교정된 보안통제항목이 보안 계획 문서, 개인정보보호 계획 문서 또는 이에 상응하는 문서에 기술되어야 함
S-5 지속적 모니터링 전략 수립 - 체계	- 준비 단계에서 수립된 조직적 모니터링 전략과 선택 및 할당된 보안통제항목을 반영하는 상세 체계 모니터링 전략이 수립되어야 함
S-6 계획 검토 및 승인	- 위험도(체계 보안 분류)를 충분히 고려하여 선택 및 교정된 보안통제항목이 체계와 조직을 충분히 보호할 수 있는지 인가 담당자(authorization official)에 의해 검토되고 승인되어야 함

〈표 4〉 보안통제항목 구현 단계 세부 활동 목록

활동	활동 수행 결과 및 산출물
I-1 통제항목 구현	- 보안 계획 및 개인정보보호 계획에 명시된 보안통제항목은 실제로 구현되어야 함 - 체계 보안 계획 및 개인정보보호 계획 내 통제항목을 구현하는데 체계 보안 및 개인정보보호 공학 방법론이 사용되어야 함
I-2 통제항목 구현 정보 갱신	- 통제항목의 계획된 구현에 대한 변화는 문서화 되어야 함 - 실제 구현 과정 중 발견된 정보 및 변경된 계획을 포함할 수 있도록 보안 및 개인정보보호 계획은 갱신되어야 함

2.4 보안통제항목 구현(Implement) 단계

보안통제항목 구현 단계는 RMF의 세 번째 주요 단계로, 보안통제항목 선택 단계에서 승인된 보안 계획 및 개인정보보호 계획에 따라 보안통제항목을 실제로 체계 또는 체계 운영 환경에 구현하는 단계이다. 본 단계에서는 보안통제항목을 구현하는데 필요한 소프트웨어를 개발하는 것뿐만 아니라 개발된 체계 소프트웨어 및 하드웨어를 실제 운영 환경에서 올바르게 설정 및 구현하고 잠재적 보안 위협이 존재하는지 확인 및 수정할 수 있는 상세 방법을 문서화하여야 한다. 이러한 구현 단계

에서 작성되는 문서 일체를 STIGs(Security Technical Implementation Guides)라고 칭한다. NIST SP 800-37에 따르면 보안통제항목 구현 단계는 다음 <표 4>와 같은 2개 활동으로 구성된다.

2.5 평가(Assess) 단계

평가 단계는 RMF의 네 번째 주요 단계로, 보안통제항목 구현 단계에서 개발되고 문서화된 보안통제항목이 최종적으로 제출된 보안 계획 및 개인정보보호 계획과 일치하는지, 잔존 위험도는 얼마나 존재하는지 검토하는 단계이다. 본 단계에서

〈표 5〉 평가 단계 세부 활동 목록

활동	활동 수행 결과 및 산출물
A-1 평가자 선택	- 보안통제항목 평가를 위한 평가자 또는 평가팀을 구성해야 함 - 구성된 평가자 또는 평가팀이 적절한 평가활동을 수행할 수 있도록 적절한 수준의 독립성이 보장되어야 함
A-2 평가 계획 수립	- 평가활동에 필요한 각종 문서 및 양식이 평가자 또는 평가팀에게 제공되어야 함 - 보안 및 개인정보보호 평가 계획이 개발되고 문서화되어야 함 - 보안 및 개인정보보호 평가 계획은 보안통제항목 평가 결과에 대한 기대치와 필요한 노력 수준을 설정하기 위해 검토 및 승인되어야 함
A-3 통제항목 평가	- 보안통제항목 평가는 보안 및 개인정보보호 평가 계획에 따라 수행되어야 함 - 비용 효율적으로 위험관리를 수행할 수 있도록 이전 평가 결과의 재사용 여부를 충분히 고려해야 함 - 가능한 경우 자동화 도구를 사용하여 보안통제항목 평가를 수행하여 평가의 속도, 효과 및 효율성을 향상시킬 수 있음
A-4 평가 보고서 작성	- 평가 결과와 수정 권장 사항을 제공하는 보안 및 개인정보보호 평가 보고서가 작성되어야 함
A-5 완화 활동 수행	- 구현된 보안통제항목의 결함을 해결하기 위해 즉각 수행할 수 있는 개선 조치를 취해야 함 - 평가 및 후속 개선 조치에 따라 변경된 보안통제항목 구현 변경 사항을 보안 및 개인정보보호 계획은 반영할 수 있도록 갱신하여야 함
A-6 보완 계획(PoA&M, Plan of Action & Milestone) 수립	- 보안 및 개인정보보호 평가 보고서에 기술된 허용 불가능 위험에 대하여 상세한 개선 계획을 문서화해야 함

〈표 6〉 인가 단계 세부 활동 목록

활동	활동 수행 결과 및 산출물
R-1 인가패키지 개발	- 인가패키지는 인가 담당자에게 제출하기 위해 개발되어야 함
R-2 위험 분석 및 결정	- 위험 분석 결과와 허용 가능한 위험도를 포함하는 위험관리 전략에 따른 인가 담당자의 위험 결정
R-3 위험 대응	- 결정된 위험에 대한 위험 대응이 제공되어야 함
R-4 인가 결정	- 공통 통제항목 또는 체계의 인가 결과가 승인 또는 거절로 결정되어야 함
R-5 인가 보고	- 인가 담당자는 인가 결정, 중대 취약점 및 위험 요소를 조직의 임원에게 보고해야 함

평가가 수행된 이후 미흡 항목이 발견되면 해당 미흡 항목에 대해 즉시 수정이 가능할 경우 수정 후 재검토를 받게 되며, 즉시 수정이 불가능할 경우 추후 보완 계획 수립과 함께 미흡 항목에 대한 잔존위험도를 측정한다. NIST SP 800-37에 따르면 평가 단계는 다음 <표 5>와 같은 6개 활동으로 구성된다.

2.6 인가(Authorize) 단계

인가 단계는 RMF의 다섯 번째 주요 단계로, 평가 단계 결과로 도출된 평가 결과를 바탕으로 인가 패키지를 개발하고 최종적으로 체계를 인가(획득)할 것인지 결정하는 단계이다. 인가 결정의 근거인 인가 패키지는 체계 보안 분류 단계부터 평가 단계까지 도출된 결과인 보안 계획, 개인정보보호 계획, 보안 평가 결과, 개인정보보호 평가

결과 및 보완 계획을 포함하는 문서 일체이다. 인가 담당자는 이러한 문서 일체를 바탕으로 잔존위험도를 감내하고 체계를 인가할 것인지 판단한다. NIST SP 800-37에 따르면 인가 단계는 다음 <표 6>과 같은 5개 활동으로 구성된다.

2.7 감시(Monitor) 단계

감시 단계는 RMF의 여섯 번째 주요 단계로, 인가한 체계에 추가적인 위협 또는 발견되지 않은 위험이 운영 중 발생되었는지 지속적으로 관찰하는 단계이다. 감시 결과에 따라 발생된 모든 변경 사항은 보안 계획 및 개인정보보호 계획에 지속적으로 반영될 수 있도록 해당 문서를 갱신해야 한다. NIST SP 800-37에 따르면 감시 단계는 다음 <표 7>과 같은 7개 활동으로 구성된다.

〈표 7〉 감시 단계 세부 활동 목록

활동	활동 수행 결과 및 산출물
M-1 체계 및 환경 변화 감시	- 정보 체계와 운영 환경은 지속적인 감시 전략에 따라 감시되어야 함
M-2 지속적 평가 수행	- 지속적인 감시 전략에 따라 보안통제항목 효과에 대한 지속적인 평가를 수행해야 함
M-3 지속적 위험 대응	- 지속적인 감시 활동의 결과를 분석하여 발견된 위험에 적절하게 대응해야 함
M-4 인가패키지 갱신	- 인가패키지에 포함된 위험관리 문서 일체는 지속적인 감시 활동을 기반으로 갱신되어야 함
M-5 보안 및 개인정보보호 보고	- 조직별로 정해진 절차에 따라 현재의 보안 및 개인정보보호 상태를 인가 담당자 및 기타 고위 경영진과 임원에게 보고해야 함
M-6 지속적 인가 수행	- 인가 담당자는 지속적인 감시 활동의 결과를 사용하여 지속적인 인가 활동을 수행하고 위험 결정 및 인가 결정의 변경사항을 전달해야 함
M-7 체계 폐기	- 필요에 따라 체계 폐기 전략을 개발하고 실행해야 함

3. 국외 RMF 동향

미 정부는 1980년대 초부터 제품 개발 시 사이버보안의 중요성을 인식하여 군을 중심으로 이와 관련한 기반 기술을 마련함과 동시에 각종 기준 및 지침 등을 개발하였다. 미 국방부는 1985년 신뢰성 있는 컴퓨터 시스템 평가기준인 TCSEC을 시작으로 제품에 대한 보안성 평가를 수행하여 안전한 제품을 개발하기 시작하였다. 이후 유럽의 평가기준인 ITSEC(Information Technology Security Evaluation Criteria)과 통합하여 CC(Common Criteria)가 제정되었다. CC는 전체 시스템이 아닌 단일 제품만 평가한다는 측면에서 평가방법을 무기체계에 직접 적용하기 어려운 부분이 존재한다. 따라서 무기체계를 운영하는 군에서는 사용하기에 적합하지 않다. 이에 미 국방부는 1997년 군에서 사용되는 제품, 환경, 시스템에 대한 통합적 보안 평가 및 인증을 위해 정보 기술 보안 인증 및 인가 프로세스인 DITSCAP을 수립하였다. 하지만 DITSCAP의 경우 독립적인 체계에 한정하여 평가가 가능하고, 표준화된 보안통제항목이 없기에 시스템별로 새롭게 정의한 보안통제항목을 사용한다는 문제점이 존재한다. 이러한 문제점을 해결하고자 미 국방부는 2007년에 DITSCAP을 DIACAP으로 대체하였다. DIACAP은 DoDI 8500.02의 표준 보안통제항목을 활용하는 것으로 DITSCAP의 문제점을 보완하였다. 이후 국방부는 타 정부기관과의 상호호환성을 높일 수 있는 인증 및 획득 제도를 구축하기 위해 NIST의 RMF를 바탕으로 RMF A&A 프로세스를 구축하였다. 이러한 흐름에 따라 2012년 미 국방부지침(DoDI) 8510.01 “Risk Management Framework(RMF) for DoD Information Technology(IT)”에서는 국방부 내의 RMF 사용을 의무화하고 있다[11]. DoDI 8510.01은 RMF를 이용하여 DoD IT의 수명주기 내 사이버 보안

위험을 관리하는 지침을 제공하고 있으며 무기체계 획득 시 관련기관이 개발·운용시험평가에 RMF 프로세스를 통합하도록 의무화하고 있다[12]. 또한 2015년 미 국방부는 ‘국방부 사이버 전략(The Department of Defense Cyber Strategy)’을 통해 군에서 사용하는 일반적인 전산 시스템뿐만 아니라 첨단 무기체계도 사이버보안을 개선해야 한다고 발표했다[13]. 이외에도 2019년 미 국방부는 ‘Risk Management Framework for Army Information Technology’을 통해 육군에 RMF를 적용하기 위한 지침을 제공하여 육군의 IT 개발자, 관리자 등이 해당 지침을 준수해야 한다고 명시하였다[14]. 이러한 흐름에 따라 현재 미 국방부는 첨단 무기체계의 소프트웨어 결함이나 사이버보안 위협에 대응하기 위해 무기체계에 RMF를 적용하고 있다. 이처럼 연방정부용 RMF는 관련 문서가 모두 민간 영역에 공개되어 있고, 특히 모든 보안 통제항목의 목록 및 세부 내용 또한 NIST SP 800-53 Rev.5에 상세히 기술되어 있다. 이 외에도 2023년 NIST에서는 AI 시스템을 설계, 개발, 배포, 사용하는 조직을 대상으로 RMF와 관련된 리소스를 제공하여 AI를 통해 발생할 수 있는 다양한 위험을 관리하는데 도움을 주고자 AI RMF에 대한 표준인 “Artificial Intelligence Risk Management Framework (AI RMF 1.0)”을 개발하였다[15]. AI RMF는 AI 기술이 지속적으로 발전함에 따라 이에 적응하고, AI를 통해 사회가 받을 수 있는 잠재적인 피해로부터 보호할 수 있도록 다양한 수준에 따라 조직 운영에서 사용될 수 있도록 개발되었다. 하지만, 무기체계를 개발 및 획득하는데 적용해야 하는 것은 NIST의 연방정부용 RMF가 아닌 DoD에서 관리하는 RMF A&A이다. DoD는 NIST와 달리 RMF A&A에 대한 문서 및 보안 통제항목 등을 민간 영역에 공개하지 않고 있다. DoD 산하기관인 DCSA에서 발행한 평가 및 인가 프로세스 매뉴얼(DAAPM,

DCSA Assessment and Authorization Process Manual)[16]에 극히 일부의 보안 통제항목 baseline만이 제시되어 있다.

Lockheed martin, BAE Systems, Boeing 등 세계 유수의 방위사업체에서는 방위사업 기술에 대한 사이버 공격에 대응하고 RMF를 준용할 수 있도록 위협 모델링 기반의 사이버보안 프레임워크를 독자적으로 개발하여 운영 및 서비스하고 있다. 대표적으로 Lockheed martin이 2020년 ‘An overview of the Lockheed martin Cyber Resiliency Level(CRL) framework for weapon, mission and training systems’문서를 통해 발표한 CRL Framework가 존재한다. 또한, 연방정부 산하의 비영리기관인 MITRE(The MITRE Corporation, 이하 MITRE)에서는 국방획득체계와 직접 연계될 수 있는 TARA(Threat Assessment and Remediation Analysis, 이하 TARA) 위협 모델링 방법론을 개발하였다[17]. 다음 <표 8>은 세계적인 방위사업체들로부터 개발된 사이버보안 프레임워크를 설명한다.

4. 국내 RMF 동향

K-RMF는 무기체계를 비롯하여 국방 정보체계에 대해 보다 높은 사이버보안 수준을 확보하기 위해서 새롭게 제정 및 시행될 국방 사이버보안 위험관리 제도이다. 2019년 미군에서는 CCIB(Command,

Control and Interoperability Board, 지휘통제상 호운용성위원회)에서 미군의 지휘통제체계인 CENTRIXS-K와 연동된 한국군의 지휘통제체계에 RMF를 적용할 것을 요구하였다[18]. 하지만 현재 미국과 우리나라는 제도적 기반과 기존 구축되어있는 보안수준이 서로 상이하기 때문에 미국의 DoD RMF A&A를 그대로 도입할 수 없다 [19]. 이에 따라 우리나라에서도 국방부가 당시 군사안보지원사령부(현 국군방첩사령부)에 한국현 위험관리 제도 개발 TF를 창설하고 미국의 국방 RMF인 DoD RMF A&A, 연방정부용 RMF인 NIST RMF 등을 참고하여 2020년 K-RMF를 제정하였다. 이어 2021년부터는 일부 무기체계를 대상으로 K-RMF를 시범 적용하고 평가를 진행하며 그 타당성을 검증하고 있다. 또한 국내 방위사업청은 2021년 ‘방위산업기술보호 종합계획’을 발표하며 미국의 사이버보안 인증제도 바탕의 한국형 기술보호 인증제도를 국내에 도입하여 방산업체의 한국형 기술보호체계 구축과 K-RMF 연계 여부를 검토해야 한다고 명시하고 있다[20]. 이러한 시범 적용 및 평가가 완료되면 오는 2024년부터는 국방부 및 군에서 새롭게 도입하는 모든 무기체계 및 정보체계와 기존 운용중인 주요 지휘통제체계를 대상으로 K-RMF를 전면 적용할 예정이며, 2026년부터는 K-RMF에 대한 전면 적용을 목표로 하고 있다. 하지만 현재 K-RMF와 관련된 자료는 제한적이며, 미국의 국방용 RMF는 외부

<표 8> 해외 방위산업체에서 개발된 RMF 기반 사이버보안 프레임워크

방위산업체	설 명
Lockheed martin	- 위험을 식별하고 효과적으로 관리하기 위해 RMF를 기반으로 무기시스템의 사이버 복원력 성숙도를 측정하는 CRL(Cyber Resiliency Level) 프레임워크 개발
BAE Systems	- 무기체계에 대한 정보보호 및 RMF 기능을 수행하는 정보 관리 솔루션인 Epiphany를 개발
Boeing	- RMF를 기반으로 하는 보안 인프라 모니터링 시스템인 SMIS(Security Monitoring Infrastructure System)을 개발
Northrop Grumman	- 사이버 위험관리를 위해 개발 프로세스에 대한 보안성 평가를 수행하는 도구인 Cyclope와 FAN을 개발

에 공개되지 않는 기밀자료에 속하는 등의 문제로 인하여 기존 국내에서 수행된 RMF 적용 연구를 실제 무기체계 개발에 적용하는데 한계가 있다. 이러한 한계점을 극복하고 K-RMF 제도를 구축할 수 있도록 국내 무기체계 대상의 RMF 적용 사례 연구를 바탕으로 한 한국형 국방 RMF 구축 방안 연구도 최근 수행되었다[6]. 이와 같이 국외 뿐만 아니라 국내에서도 무기체계에 RMF를 적용하기 위한 움직임을 보이고 있다.

국내 방위산업체인 한화시스템에서는 K-RMF에 대해 대비하기 위하여 “함정 전투체계에 대한 RMF 적용 방안 연구”과제를 통해 NIST RMF 및 DoD RMF A&A를 바탕으로 함정 전투체계를 대상으로 RMF 준비단계부터 구현단계까지에 대한 사례 연구를 진행하였으며, 현재 SRTOS(Secure Real-Time Operating System)를 대상으로 K-RMF를 준용하기 위한 “보안 실시간 SW 플랫폼 RMF 기반 보안 표준 준용 방안 연구”과제를 수행하고 있다. 또한 국내의 또다른 방위산업체인 LIG Nex1에서도 “무기체계 K-RMF 적용 대응 방안 연구” 과제를 통해 개발되는 무기체계에 대한 위협 식별, 위험 분석, 보안통제항목 선정 등에 대한 기술을 연구하고 적용하는 연구를 수행하고 있다. 이와 같이 국내 방위산업체에서는 K-RMF 준용을 위한 연구를 활발히 수행하고 있으며, 학계에서도 K-RMF에 대비하기위한 연구가 지속적으로 수행되고 있다. 2019년, 조현석 외 2명은 “국내 무기체계에 대한 RMF 적용 실 사례 연구”라는 주제로 당시의 한국형 RMF 연구를 활용하여 최근 개발된 실제 무기체계에 적용하고 RMF를 우리나라 무기체계에 적용할 수 있도록 상세한 가이드라인을 제시한 바가 있다[21]. 2021년, 조광수 외 1명은 “무기체계 개발을 위한 RMF A&A의 실증에 관한 연구”라는 주제로 상세한 정보가 공개되지 않아 실제 산업 환경에 적용이 어려운 RMF A&A를 분석하여, RMF A&A의 요구사항을 만

족시킬 수 있는 증거자료 작성방안을 제시하였다. 또한 제시한 방안을 실제 드론 시스템에 적용하여 제안된 방안이 RMF A&A의 요구사항에 부합하는지에 대한 검증을 수행하였다[22]. 이후 K-RMF에 대한 전면 적용에 대비하기위해 2023년에 안정근 외 5명은 “무기체계 개발을 위한 한국형 국방 RMF 구축 방안 연구”라는 주제로 우리나라 국방용 RMF인 K-RMF를 예측하여 무기체계의 보안 통제항목을 구축하기위한 방안과 이를 함정 전투체계에 적용하여 효용성을 입증하였다[6]. 이처럼 국내의 산업계 및 학계에서는 K-RMF 전면 적용에 대비하기 위해 K-RMF 제정의 기초가 된 RMF A&A와 NIST RMF 바탕의 K-RMF 연구가 활발히 수행되고 있다.

5. 결 론

기존에 독립적으로 운용되던 무기체계가 지휘관의 빠른 결심 및 실시간 전장 상황 공유 등의 목적을 위해 점차 네트워크로 연동되고 있다. 이러한 무기체계의 변화는 전장에서의 이점도 가져다줄 수 있지만, 동시에 사이버 위협에 노출될 가능성 또한 높이고 있다. 무기체계에 대한 사이버 보안 위협에 대응하기 위해 미국은 과거 TCSEC을 시작으로 현대에 이르러서 RMF라는 위협관리 및 평가 체계를 개발하고 적용하고 있다. 본 연구에서는 RMF에 대한 개념과 미 국방성의 RMF 적용 요구에 따른 국내외의 다양한 대응 노력에 대한 사례 조사를 진행하였다. 본 사례 조사를 바탕으로 추후 RMF와 관련한 연구가 더욱 심도있게 수행되고 우리나라의 K-RMF 제도 또한 올바르게 개발되고 안정적으로 정착되어 사이버 위협으로부터 안전한 무기체계를 개발할 수 있을 것으로 기대된다.

참 고 문 헌

- [1] 이지섭, 차성용, 백승수, 김승주, “무기체계의 사이버보안 시험평가체계 구축방안 연구”, 한국정보보호학회논문지, 제28권, 제3호, pp.765-774, 2018.
- [2] 차성용, “첨단 무기체계 획득 및 운용 시 사이버보안 강화방안 연구”, 고려대학교, 박사학위 논문, 2019.
- [3] 권혁진, 김성태, 주예나, “상호운용성을 고려한 RMF 기반의 위협관리체계 적용 방향”, 제22권, 제6호, pp.83-89, 2021.
- [4] “Defense counterintelligence and security agency assessment and authorization process manual”, Defense Counterintelligence and Security Agency, 2020.
- [5] “The DoD cyber strategy”, Department of Defense, 2015.
- [6] 안정근, 조광수, 정지훈, 정한진, 김승주, “무기체계 개발을 위한 한국형 국방 RMF 구축방안 연구”, 한국정보보호학회논문지, 제33권, 제5호, pp.827-846, 2023.
- [7] 양우성, 차성용, 윤종성, 권혁주, 유재원, “국방획득체계 적용 한국형 보안위험관리 프레임워크”, 한국정보보호학회논문지, 제32권, 제6호, pp.1183-1192, 2022.
- [8] 김하늬, “K-RMF 구축으로, 국내 사이버보안 수준 높인다”, 공학저널, 2023.11.25. 접속,
- [9] “NIST Glossary”, NIST, 2023.11.28. 접속, <https://csrc.nist.gov/glossary>
- [10] “risk management framework (RMF)”, NIST Glossary, 2023.11.28. 접속, https://csrc.nist.gov/glossary/term/risk_management_framework
- [11] DoD, “DoDI 8510.01 - Risk Management Framework (RMF) for DoD Information Technology (IT)”, 2016
- [12] DoD, “DoD Program Manager’s Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle”, 2015
- [13] DoD, “The Department of Defense Cyber Strategy”, 2015
- [14] Department of the Army. “Risk Management Framework for Army Information Technology”, 2019
- [15] Tabassi, Elham. “Artificial Intelligence Risk Management Framework (AI RMF 1.0).” (2023).
- [16] DCSA, Defense counterintelligence and security agency assessment and authorization process manual, DCSA, Aug.2020
- [17] MITRE, “Threat Assessment and Remediation Analysis(TARA) Overview”, MITRE Corporation, <https://www.mitre.org/sites/default/files/2021-11/pr-11-4987-presentation-tara-overview.pdf>, 2013
- [18] 안병오, “KIDA Brief - 미국의 新(신) C4I 정책과 연계한 연합 C4I체계 발전 방안”, 군사발전연구센터(KIDA), 2021
- [19] Woo-sung Yang, Sung-yong Cha, Jong-sung Yoon, Hyeok-joo Kwon and Jae-won Yoo, “Korean security risk management framework for the application of defense acquisition system,” Journal of the Korea Institute of Information Security & Cryptology, 32(6), pp.1183-1192, Dec. 2022
- [20] 방위사업청, “방위산업기술보호 종합계획”, 방위사업청, 2021
- [21] 조현석, 차성용, and 김승주. “국내 무기체계에 대한 RMF 적용 실 사례 연구.” 정보보호학회논문지 29.6 (2019): 1463-1475.
- [22] 조광수, and 김승주. “무기체계 개발을 위한 RMF A&A 의 실증에 관한 연구.” 정보보호학회논문지 31.4 (2021): 817-839.

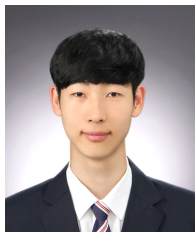
저 자 약 력



조 광 수

이메일 : cks4386@korea.ac.kr

- 2019년 호서대학교 컴퓨터공학과 (학사)
- 2021년 고려대학교 정보보호대학원 정보보호학과 (석사)
- 2021년~현재 고려대학교 정보보호대학원 정보보호학과 (박사과정)
- 관심분야: 보안공학, RMF, DevSecOps



김 예 준

이메일 : v3locy@korea.ac.kr

- 2019년 순천향대학교 정보보호학과 (학사)
- 2019년~현재 고려대학교 정보보호대학원 정보보호학과 (석사통합과정)
- 관심분야: 보안공학, 위협모델링, 보안성 평가/인증, 취약점 분석, 역공학



안 정 군

이메일 : stable_root@korea.ac.kr

- 2014년 육군사관학교 지역연구학과 (학사)
- 2019년~현재 국군방첩사령부
- 2023년~현재 고려대학교 정보보호대학원 정보보호학과 (석사과정)
- 관심분야: 보안공학, 위협관리, 보안성평가/인증



김 정 현

이메일 : letter@korea.ac.kr

- 2018년 순천향대학교 정보보호학과 (학사)
- 2020년 순천향대학교 정보보호학과 (석사)
- 2020년~현재 고려대학교 정보보호대학원 정보보호학과 (박사과정)
- 관심분야: 보안공학, 자동차보안, CSMS



박 지 원

이메일 : jwkwak4031@korea.ac.kr

- 2017년 중앙대학교 전자전기공학부 (학사)
- 2019년 고려대학교 일반대학원 사이버국방학과 (석사)
- 2019년~현재 고려대학교 정보보호대학원 정보보호학과 (박사과정)
- 관심분야: 보안성분석평가, 정형기법, 고신뢰시스템개발



김 해 나

이메일 : haena0114@korea.ac.kr

- 2021년 서울여자대학교 정보보호학과 (학사)
- 2021년~현재 고려대학교 정보보호대학원 정보보호학과 (석사과정)
- 관심분야: 제로트러스트, 보안공학, 위협모델링, RMF



백 군 우

이메일 : sinse100@korea.ac.kr

- 2023년 한국항공대학교 소프트웨어학과 (학사)
- 2023년~현재 고려대학교 정보보호대학원 정보보호학과 (석사과정)
- 관심분야 : 블록체인, 보안공학



김 승 주

이메일 : skim71@korea.ac.kr

- 1994년~1999년 성균관대학교 정보공학과 (학사, 석사, 박사)
- 1998년~2004년 한국인터넷진흥원(KISA) 팀장
- 2004년~2011년 성균관대학교 정보통신공학부 부교수
- 2011년~현재 고려대학교 정보보호대학원 정교수
- 2004년~현재 한국정보보호학회 이사
- 2014년~2015년 육군사관학교 초빙교수
- 2016년~2018년 개인정보분쟁조정위원회 위원
- 2017년~현재 고려대학교 국방RMF연구센터(ARC) 센터장
- 2018년~현재 고신로 보안운영체제 연구센터(CHAOS) 센터장
- 2018년~2020년 대통령직속 4차산업혁명위원회 위원
- 2023년~현재 대통령직속 국방혁신위원회 위원
- 2023년~현재 고려대학교 디지털정보처 처장
- 2023년~현재 (사)한국국방혁신기술보안협회 협회장
- 관심분야 : 보안공학, 위협모델링, 보안성 평가/인증, DevSecOps, 암호학, 블록체인

정보처리학회지 게재 목차

■ 2023년 9월 (제30권 제3호)	■ 특집명 : 디지털 금융 서비스와 보안
♦ 권두언	
본 9월호는 "디지털 금융서비스와 보안"이란 주제로 구성하였습니다. / 이기혁	2
♦ 특집	
컨조인트 분석을 이용한 금융소비자의 인증서 선택에 대한 연구 / 강환철	4
디지털 금융의 클라우드 보안 강화를 위한 공동 책임 모델 설계 / 민경조	14
금융 빅데이터 처리를 위한 비식별 처리 기술의 국제 표준화 동향 / 황송이, 임형진	20
가상자산의 글로벌 투자현황 및 국가별 법제와 향후 시장 전망 / 도영환	27

정보처리학회논문지(KTCCS) 게재 목차

■ 제12-CCS권 제9호(통권 제132호) 2023년 9월	
▶ 차세대 통신시스템 및 네트워크	
• MEC 산업용 IoT 환경에서 경매 이론과 강화 학습 기반의 하이브리드 오프로딩 기법 / 배현지, 김승욱	263
▶ 사물인터넷	
• 인공지능 기반 컨테이너 적재 안전관리 시스템 연구 / 김상우, 오세영, 서용욱, 연정흠, 조희정, 윤주상	273
▶ 블록체인	
• DSLR을 이용한 효율적인 스택스메싱 공격탐지 방법 / 황도영, 유동영	283

■ 제12-CCS권 제10호(통권 제133호) 2023년 10월	
▶ 컴퓨터 시스템 및 이론	
• 정보·컴퓨터 중등교사 임용시험의 프로그래밍 문항 분석 / 강오한	291
▶ 차세대 통신시스템 및 네트워크	
• 전송률 분할 다중 접속 기술을 활용한 비면허 대역의 트래픽과 공정성 최대화 기법 / 전장우, 김승욱	299
▶ 정보보호	
• 전기차 전과정평가를 위한 DID 기반 차량부품 데이터수집 모델 연구 / 권준우, 이수진, 김제인, 서승현	309

■제12-CCS권 제11호(통권 제134호) 2023년 11월

- ▶ 컴퓨터 시스템 및 이론
 - 예지 컴퓨팅 기반 객체탐지 서비스를 위한 이미지/동영상 데이터 처리 기법에 관한 연구
/ 장신원, 홍용근 319
- ▶ 차세대 통신시스템 및 네트워크
 - 수탁사 개인정보보호 강화를 위한 프레임워크 및 점검방법 연구 / 박유림, 신용태 329
- ▶ ICT 융합
 - 돌봄 제공자를 위한 디지털 돌봄 앱 개발 및 사용성 평가
/ 박종찬, 김재국, 정의재, 안창선, 정봉수, 김영주 337

■제12-CCS권 제12호(통권 제135호) 2023년 12월

- ▶ 기획특집: 디지털 전환을 위한 ICT 기술과 융합 사례
 - 저궤도 위성통신 분야의 ICT 디지털 전환과 데이터 융합 생태계 조성을 위한 SNS 감성분석과
니드마이닝 / 이병희, 김태현 347
 - 지능형 교량 안전성 예측 엣지 시스템 / 박진효, 이태진, 홍용근, 윤주상 357
 - 자원 제약적 기기에서 자율주행의 실시간 객체탐지를 위한 태스크 오프로딩 적용에 관한 연구
/ 장신원, 홍용근 363

정보처리학회논문지(KTSDE) 게재 목차

■제12-SDE권 제9호(통권 제132호) 2023년 9월

- ▶ 소프트웨어 공학
 - 한글 요구사항 기반 결정 테이블로부터 테스트 케이스 생성을 위한 메타모델링 구축화
/ 장우성, 문소영, 김영철 381
- ▶ 데이터 공학
 - 검색어 빈도 데이터를 반영한 코로나 19 확진자수 예측 딥러닝 모델 / 정성욱 387
- ▶ 인공지능
 - 멀티 에이전트 예지 컴퓨팅 환경에서 확장성을 지원하는 딥러닝 기반 동적 스케줄링 / 임종범 399
 - 멀티 모달 맥락정보 융합에 기초한 다중 물체 목표 시각적 탐색 이동 / 최정현, 김인철 407
- ▶ 인간 컴퓨터 상호작용
 - 부동산 유통화 NFT와 FT 분할 거래 시스템 설계 및 구현 / 김영근, 김성환 419

■ 제12-SDE권 제10호(통권 제133호) 2023년 10월

- ▶ 소프트웨어 공학
 - CodeBERT 모델의 전이 학습 기반 코드 공통 취약점 탐색 / 박찬술, 문소영, 김영철 431
- ▶ 데이터 공학
 - 위치정보 보호를 위한 이동 경로 기록 및 관리 서비스 앱 개발
/ 김서연, 김아영, 오민정, 오 샘, 김성욱 437
- ▶ 빅데이터
 - LSTM을 이용한 협동 로봇 동작별 진류 및 진동 데이터 잔차 패턴 기반 기어 결함진단
/ 백지훈, 유동연, 이정원 445
- ▶ 인공지능
 - 생성-선정을 통한 텍스트 증강 프레임워크 / 김경민, 김동환, 조성웅, 오홍선, 황명하 455
- ▶ 멀티미디어 처리
 - 딥러닝을 활용한 한국어 스피치 애니메이션 생성에 관한 고찰 / 강석찬, 김동주 461

■ 제12-SDE권 제11호(통권 제134호) 2023년 11월

- ▶ 인공지능
 - EPC 프로젝트의 위험 관리를 위한 ITB 문서 조항 분류 모델 연구: 딥러닝 기반 PLM 양상불 기법
활용 / 이현상, 이원석, 조보근, 이희준, 오상진, 유상우, 남마루, 이현식 471
 - 생성형 대규모 언어 모델과 프롬프트 엔지니어링을 통한 한국어 텍스트 기반 정보 추출 데이터셋 구축
방법 / 정영상, 지승현, 권다롱새 481
- ▶ 기획특집: 서베이 & 리뷰
 - 한반도에서 발생한 지진의 통계적 자기 유사성 분석 및 시각화 / 황재민, 임지영, 정해덕 493

■ 제12-SDE권 제12호(통권 제135호) 2023년 12월

- ▶ 인공지능
 - 멀티-뷰 영상들을 활용하는 3차원 의미적 분할을 위한 효과적인 멀티-모달 특징 융합
/ 배혜림, 김인철 505
 - 효율적인 이미지 검색 시스템을 위한 자기 감독 딥해싱 모델의 비교 분석
/ 김수인, 전영진, 이상범, 김원겸 519
 - 멀티모달 방식을 통한 가스 종류 인식 딥러닝 모델 개발 / 안서희, 김경영, 김동주 525

JIPS(정보처리학회영문지) 게재 목차

■ Volume 19, Number 5(Serial Number 83), October 2023	
• Improved Gauss Pseudospectral Method for UAV Trajectory Planning with Terminal Position Constraints <i>Qingquan Hu, Ping Liu, and Jinfeng Yang</i>	563
• Personalized Recommendation Algorithm of Interior Design Style Based on Local Social Network <i>Guohui Fan and Chen Guo</i>	576
• Research on the Sharing Strategy of Electronic Book Resources in Universities in the Internet Era <i>Guiya Gao</i>	590
• A Brief Survey into the Field of Automatic Image Dataset Generation through Web Scraping and Query Expansion <i>Bart Dikmans and Dongwann Kang</i>	602
• Automatic Detection of Dead Trees Based on Lightweight YOLOv4 and UAV Imagery <i>Yuanhang Jin, Maolin Xu, and Jiayuan Zheng</i>	614
• Research on Keyword-Overlap Similarity Algorithm Optimization in Short English Text Based on Lexical Chunk Theory <i>Na Li, Cheng Li, and Honglie Zhang</i>	631
• BERT-Based Logits Ensemble Model for Gender Bias and Hate Speech Detection <i>Sanggeon Yun, Seungshik Kang, and Hyeokman Kim</i>	641
• Ensemble Gene Selection Method Based on Multiple Tree Models <i>Mingzhu Lou</i>	652
• Vehicle Detection at Night Based on Style Transfer Image Enhancement <i>Jianing Shen and Rong Li</i>	663
• Transfer Learning-Based Feature Fusion Model for Classification of Maneuver Weapon Systems <i>Jinyong Hwang, You-Rak Choi, Tae-Jin Park, and Ji-Hoon Bae</i>	673
• A Network Intrusion Security Detection Method Using BiLSTM-CNN in Big Data Environment <i>Hong Wang</i>	688
• Research on the Application of Load Balancing in Educational Administration System <i>Junrui Han and Yongfei Ye</i>	702

■ Volume 19, Number 6(Serial Number 84), December 2023

• Research on Economic Performance of Mining Enterprises Based on Stakeholders <i>Yunxiang Peng and Guixian Tian</i>	713
• Visual Analytic for Intangible Cultural Heritage in China <i>Nan Zhang</i>	722
• Egocentric Vision for Human Activity Recognition Using Deep Learning <i>Malika Douache and Badra Nawal Benmoussat</i>	730
• Defect Detection of Steel Wire Rope in Coal Mine Based on Improved YOLOv5 Deep Learning <i>Xiaolei Wang and Zhe Kan</i>	745
• Reversible Multipurpose Watermarking Algorithm Using ResNet and Perceptual Hashing <i>Mingfang Jiang and Hengfu Yang</i>	756
• Machine Learning-Based Reversible Chaotic Masking Method for User Privacy Protection in CCTV Environment <i>Jimin Ha, Jungho Kang, and Jong Hyuk Park</i>	767
• A Density Peak Clustering Algorithm Based on Information Bottleneck <i>Yongli Liu, Congcong Zhao, and Hao Chao</i>	778
• Hot Spot Detection of Thermal Infrared Image of Photovoltaic Power Station Based on Multi-Task Fusion <i>Xu Han, Xianhao Wang, Chong Chen, Gong Li, and Changhao Piao</i>	791
• A Gradient-Based Explanation Method for Node Classification Using Graph Convolutional Networks <i>Chaehyeon Kim, Hyewon Ryu, and Ki Yong Lee</i>	803
• Quality Adaptation of Intra-only Coded Video Transmission over Wireless Networks <i>Shu Tang, Yuanhong Deng, and Peng Yang</i>	817
• Word-Level Embedding to Improve Performance of Representative Spatio-temporal Document Classification <i>Byoungwook Kim and Hong-Jun Jang</i>	830
• Research on Chinese Microblog Sentiment Classification Based on TextCNN-BiLSTM Model <i>Haiqin Tang and Ruirui Zhang</i>	842
• Multiple Mixed Modes: Single-Channel Blind Image Separation <i>Tiantian Yin, Yina Guo, and Ningning Zhang</i>	858



[학회 주최/주관 행사]

◆ 제3차 단기강좌 개최

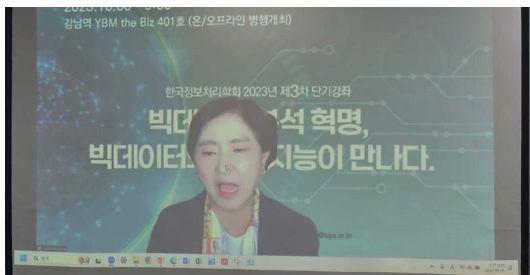
- 1) 일 시 : 2023년 10월 6일(금) 9:50
- 2) 장 소 : YBM the Biz 401호(온/오프라인 병행)
- 3) 주 제 : 빅데이터 분석 혁명, 빅데이터와 인공지능이 만나다.
- 4) 위원회
 학회장 : 문남미 교수(호서대학교)
 담당 부회장 : 김현희 교수(동덕여자대학교)
 프로그램위원장 : 윤혜정 교수(이화여자대학교)
- 5) 참가자 : 46명
- 6) 발표자 : 차경진 교수(한양대학교), 안성복 교수(이화여자대학교), 맹윤희 겸임교수(이화여자대학교), 이일섭 매니저(신한카드), 이장후(MLOps실전가이드 역자)



[제3차 단기강좌 발표 - 차경진 교수(한양대학교)]



[제3차 단기강좌 발표 - 안성복 교수(이화여자대학교)]



[제3차 단기강좌 인사말 - 문남미 회장(호서대학교)]



[제3차 단기강좌 발표 - 맹윤희 겸임교수(이화여자대학교)]



[제3차 단기강좌 사회 - 김현희 교수(동덕여자대학교)]



[제3차 단기강좌 발표 - 이일섭 매니저(신한카드)]

- 3) 위원회
학회장 : 문남미 교수(호서대학교)
조직위원장 : 권기룡 교수(부경대학교)
학술위원장 : 임동혁 교수(광운대학교)
- 4) 논문발표 : 총 497편
- 5) 참가자 : 총 775명
- 6) 시 상 : 총 58편
논문상(대학원생이상) : 총 21편 (최우수논문상 2편, 우수논문상 19편)
학부생논문경진대회 : 총 27편 (대상 1편, 금상 2편, 은상 2편, 동상 4편, 장려상 18편)
산학협동우수상 : 총 2편
정보통신산업진흥원 원장상 : 총 2편
정보통신정책연구원 원장상 : 총 2편
정충연합회 회장상 : 총 2편
부경대학교 총장상 : 총 2편
ICT멘토링상 : 22편
- 7) 행사내용 : 초청강연, 튜토리얼, 신진학자 워크숍, WicSE Workshop 등
- 8) 전체일정 :

11월 2일(목)		공학1관 1층 창의공작실	온라인
15:00~17:00	Social Events (Only for Invited Members) 초청강연 이경미 과장(부산의료원)		구두 (동영상) 스트리밍
17:00~18:00	“100세 시대. 인생은 지금부터!”	특별세션1	
18:00~19:00	Welcome Reception (Only for Invited Members)		

11월 3일(금)	공학1관										공학2관							온라인
	2층 로비	3층 로비	1층 창의공작실	209호	2층 소회의실	210호	211호	519호	722호	1219호	1319호	102호	103호	104호	106호	401호	402호	
09:30~10:30(60')			특별세션 2	특별세션 3	특별세션 4	특별세션 5	특별세션 6	특별세션 7	특별세션 8									
10:30~11:00(30')																		
11:00~11:30(30')																		
11:30~12:00(30')	포스터 1									Oral 1-1	Oral 1-2	Oral 1-3	Oral 1-4		Oral 1-5	Oral 1-6	Oral 1-7	
12:00~12:30(30')																		

11월 3일(금)	공학1관											공학2관						온라인
	2층 로비	3층 로비	1층 창의공작실	209호	2층 소회의실	210호	211호	519호	722호	1219호	1319호	102호	103호	104호	106호	401호	402호	
13:30~14:30(60')	포스터 2		여성위원회	특별세션 9	특별세션 10	특별세션 5		특별세션 11	특별세션 12	특별세션 13	특별세션 14		Oral 2-1	Oral 2-2	Oral 2-3	Oral 2-4	Oral 2-5	구두(동영상) 스트리밍
14:30~15:00(30')																		
15:00~16:30(90')																		

11월 3일(금)	공학1관 3층 다목적홀	온라인
15:00~15:30(30')	튜토리얼 운영찬 교수(제주대) “ChatGPT & LLM 동향분석”	구두(동영상) 스트리밍
15:30~16:00(30')	신진학자 워크숍 김승욱 교수(부경대) / 유지현 교수(광운대) / 권범 교수(동덕여대)	
16:00~16:10(10')	휴식	
16:10~16:40(30')	초청강연 윤석찬 테크에반젤리스트(아마존웹서비스) “생성형 AI 기반 기업 내부 활용 기술 동향”	
16:40~17:10(30')	기조강연 이경무 석좌교수(서울대) “Chat GPT시대의 인공지능 발전전략”	
17:10~17:20(10')	휴식	
17:20~18:00(40')	개회식 및 정기총회	

3일차 / 2023년 11월 4일(토)

11월 4일(토)		온라인
10:00~14:00	산학연 교류회	구두(동영상) 스트리밍
14:00~17:00	Post-Conference Meeting	



[구두(대면) 세션 발표 - 1]



[구두(대면) 세션 발표 - 2]



[포스터 세션 발표]



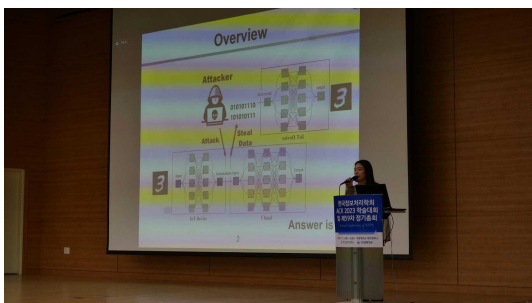
[기조강연 발표 - 이경무 석좌교수(서울대학교)]



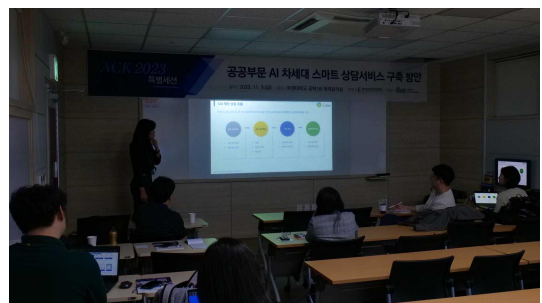
[신진학자 워크숍 발표 - 김승욱 조교수(부경대학교)]



[특별세션 발표 - 김병구(한국전자통신연구원)]



[신진학자 워크숍 발표 - 유지현 조교수(광운대학교)]



[특별세션 발표 - 김설아(서울시 120 다산 콜재단)]



[신진학자 워크숍 발표 - 권범 조교수(동덕여자대학교)]



[특별세션 발표 - 광운대학교]



[특별세션 발표 - 윤예중(성균관대학교)]



[축사 - 장영수 총장(부경대학교 - 김영복 부총장)]



[특별세션 발표 - 윤승용(한국전자통신연구원)]



[감사패 전달 - 장영수 총장(부경대학교)]



[특별세션 발표 - Mpyana Mwamba Merlec(고려대학교)]



[공로상 수상자 단체사진]



[개회사 - 문남미 회장(한국정보처리학회)]



[KISDI, NIPA 원장상 및 정총 회장상, 부경대 총장상 수상자 단체사진]



[(최)우수논문상 수상자 단체사진]



[학부생논문경진대회장 수상자 단체사진 - 1]



[학부생논문경진대회장 수상자 단체사진 - 2]



[ICT멘토링 (최)우수논문상 단체사진]

◆ 창립 30주년 기념식 및 2023년도 윤당학술상 시상식

- 1) 일 시 : 2023년 12월 1일(금) 16:00
- 2) 장 소 : 코리아나호텔 17F 글로리아홀
- 3) 위원회
 학회장 : 문남미 교수(호서대학교)
 위원장 : 최유주 교수(서울미디어대학원대학교)
 위 원 : 유진호 교수(상명대학교), 김경아 교수(명지전문대학), 김경록 교수(호서대학교)
- 4) 참석자 : 총 206명
- 5) 행사내용 : 환영사 및 축사, 학회 발자취 및 축하 영상 상영, 감사패 증정, 기념떡 커팅 및 기념촬영 학술상 시상식 등



[창립 30주년 기념식 환영인사 - 문남미 회장(한국정보처리학회)]



[창립 30주년 기념식 축사 - 오명 장관(前과학기술정보통신부)]



[창립 30주년 기념식 축하 -
조이남 전임회장(한국정보처리학회)]



[창립 30주년 기념식 축하동영상 상영 -
황종성 원장(한국지능정보사회진흥원)]



[창립 30주년 기념식 축하 -
이원준 회장(한국정보과학회)]



[창립 30주년 기념식 축하동영상 상영 -
신희동 원장(한국전자기술연구원)]



[창립 30주년 기념식 축하동영상 상영 -
이종호 장관(과학기술정보통신부)]



[창립 30주년 기념식 축하동영상 상영 -
방송찬 원장(한국전자통신연구원)]



[창립 30주년 기념식 축하동영상 상영 -
고진 위원장(디지털플랫폼정부위원회)]



[창립 30주년 기념식 축하동영상 상영 -
김형철 소장(소프트웨어정책연구소)]



[창립 30주년 기념식 비전 선포 -
문남미 회장, 백윤희 수석부회장(한국정보처리학회)]



[창립 30주년 기념식 차기회장 인사 -
백윤희 교수(서울대학교)]



[창립 30주년 기념식 감사패 수상 -
故)남궁석 전임회장, 조이남 전임회장]



[창립 30주년 기념식 단체사진]



[창립 30주년 기념식 감사패 수상 -
서승현 교수(한양대학교), 유현창 교수(고려대학교)]



[2023년 문당학술상 환영사 -
이상현 부회장(KCC정보통신)]



[창립 30주년 기념식 기념떡 커팅]



[2023년 문당학술상 경과보고 -
신용태 운영위원장 (숭실대학교)]



[2023년 윤당학술상 윤당학술대상 - 이경무 석좌교수(서울대학교)]



[2023년 윤당학술상 윤당논문대상 - 임유진 교수(숙명여자대학교), 손진곤 교수(한국방송통신대학교)]



[2023년 윤당학술상 윤당학생논문상 - 이수진(한양대학교), 김지흥(호서대학교), 유동연(아주대학교), 최종우(한국과학기술원)]



[2023년 윤당학술상 수상자 단체사진]

◆ 제4차 단기강좌 개최

- 1) 일 시 : 2023년 12월 15일(금) 10:00
- 2) 장 소 : 한국정보처리학회 회의실
- 3) 주 제 : 인공지능과 정보보안, 융합을 보다!
- 4) 위원회
 학회장 : 문남미 교수(호서대학교)
 수석부회장 : 백윤희 교수(서울대학교)
 담당 부회장 : 김현희 교수(동덕여자대학교)
 프로그램위원장 : 도경화 교수(고려대학교)
- 5) 참가자 : 19명
- 6) 발표자 : 백윤희 교수(서울대학교), 도경화 교수(고려대학교), 유인지 대표(코리아엑스퍼트), 박창현 프로(삼성SDS), 박영선 대표(두두아이티)



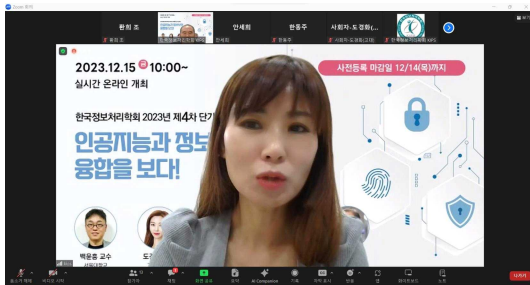
[제4차 단기강좌 인사말 - 문남미 회장(호서대학교)]



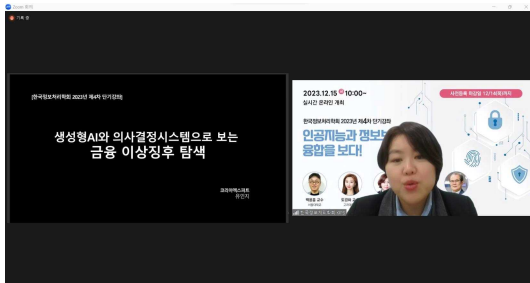
[제4차 단기강좌 사회 - 김현희 교수(동덕여자대학교)]



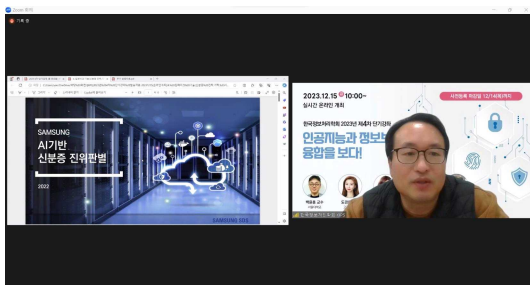
[제4차 단기강좌 발표 - 백윤희 교수(서울대학교)]



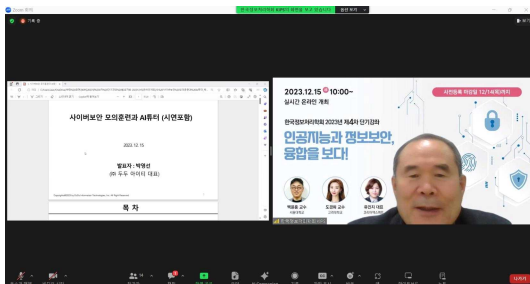
[제4차 단기강좌 발표 - 도경화 교수(고려대학교)]



[제4차 단기강좌 발표 - 유인지 대표(코리아엑스퍼트)]



[제4차 단기강좌 발표 - 박창현 프로(삼성SDS)]



[제4차 단기강좌 발표 - 박영선 대표(두두아이티)]

[대외활동]

◆ 학회 유관기관 방문

- 1) 일 시 : 2023년 10월 26일(목)
- 2) 장 소 : ETRI 원장실
- 3) 참석자 : 문남미 회장 외 2명



[한국전자통신연구원(ETRI) 방문 기념 촬영]

[제회의]

- 이사회

◆ 2023년도 제4차 이사회

- 1) 일 시 : 2023년 10월 4일(수) 17:00
- 2) 장 소 : 온라인 화상회의(Zoom)
- 3) 참석자 : 문남미 회장 외 24명
- 4) 내 용 : 2023년 수석부회장 보선에 관한 사항 외

◆ 2023년도 제5차 이사회 개최

- 1) 일 시 : 2023년 10월 13일(금) 17:00
- 2) 장 소 : 한국화웨이(유) 17층 회의실
- 3) 참석자 : 문남미 회장 외 20명
- 4) 내 용 : 제59차 정기총회 포상자 심의 외



[회의 참석자 단체사진]

[지회/연구회]

- 컴퓨터소프트웨어연구회

◆ The 9th JIPS/KIPS-CSWRG Workshop

- 1) 일 시 : 2023년 11월 9일(목)~10(금)
- 2) 장 소 : Gangneung-Wonju National University, Korea
- 3) 참석자 : 박종혁 위원장 외 24명
- 4) 내 용 : 논문발표 외

◆ CSA/CUTE 2023 개최

- 1) 일 시 : 2023년 12월 18일(월)~20(수)
- 2) 장 소 : Nha Trang, Vietnam
- 3) 참석자 : 박종혁 위원장 외 230명
- 4) 내 용 : 논문발표 외



[참가자 단체 사진]

[학술사업 추진 활동]

- ACK 2023

◆ ACK 2023 제1차 학술위원장단 회의 개최

- 1) 일 시 : 2023년 10월 11일(수) 15:00
- 2) 장 소 : 학회 회의실
- 3) 참석자 : 임동혁 학술위원장 외 5명
- 4) 내 용 : 행사 전체 프로그램 구성 외



[회의 진행 모습]

[각 위원회 활동]

- 여성위원회

◆ 2023년도 여성리더십/AllyShip 워크숍 개최

- 1) 일 시 : 2023년 11월 3일(금) 13:20
- 2) 장 소 : 부경대학교 공학1관 1층 창의공작실
- 3) 참석자 : 도경화 위원장 외 10명



[2023년도 여성리더십/AllyShip 워크숍 진행 모습]

신규회원 명단

가입기간 : 23.10.1~23.12.31

회원구분	회원번호	성명	직장명
종신회원	2023-23695-01	권태경	서울대학교
	2023-23691-01	최봉준	숭실대학교
	2023-23685-01	이경무	서울대학교
	2023-23678-01	최일석	LG전자(주)
	2023-23664-01	최선미	한국전자통신연구원
	2023-23584-01	오상진	고려대학교
	2023-23558-01	이상근	서강대학교
	2015-20349-01	김민철	펜타시큐리티시스템(주)
정회원	2023-23693-02	최원욱	안양대학교
	2014-19384-02	박소현	동국대학교
	2023-23694-02	한창욱	동의대학교
	2023-23692-02	고은비	한국정보통신기술협회
	2023-23690-02	나영국	서울시립대학교
	2021-22686-02	이신재	한국과학기술원
	2023-23684-02	정진우	LIG넥스원
	2023-23677-02	박지영	주식회사 데이터룩
	2009-16253-02	최종선	숭실대학교
	2023-23675-02	박중혁	국민대학교
	2023-23674-02	최규담	희래
	2023-23672-02	조영필	한양대학교
	2023-23670-02	김봉훈	한양대학교 에리카
	2018-21971-02	신영주	고려대학교
	2023-23669-02	김훈희	부경대학교
	2023-23668-02	이상민	광운대학교
	2014-19501-02	이태휘	한국전자통신연구원
	2000-6647-02	신상욱	부경대학교
	2023-23665-02	홍석재	성균관대학교
	2023-23663-02	문현곤	울산과학기술원
	2022-23101-02	Palash Ingle	세종대학교

회원구분	회원번호	성명	직장명
정회원	2017-21540-02	구자훈	세종대학교
	2021-22743-02	송미화	세명대학교
	2015-20104-02	김미혜	충북대학교
	2002-9168-02	명훈주	한국과학기술정보연구원
	2023-23659-02	김다솔	한국과학기술정보연구원
	2023-23658-02	송사광	한국과학기술정보연구원
	2023-23657-02	배병성	호서대학교
	2023-23656-02	이재학	고려대학교
	2022-23218-02	이상백	한국과학기술정보연구원
	2023-23653-02	유은지	한국과학기술정보연구원
	2023-23648-02	서지원	한국자동차연구원
	2023-23645-02	김찬민	한국자동차연구원
	2023-23640-02	김용국	세종대학교
	2023-23638-02	김성호	해양 IT융합기술연구소
	2023-23637-02	정현지	국립공주대학교
	2023-23636-02	안효원	고려대학교
	2023-23634-02	박준영	한국과학기술정보연구원
	2023-23633-02	원종호	한국전자통신연구원
	2023-23631-02	오현영	가천대학교
	2023-23630-02	김시진	쿠노소프트
	2021-22998-02	김서정	한국전자기술연구원
	2021-22912-02	장광선	한국과학기술정보연구원
	2017-21561-02	곽재혁	한국과학기술정보연구원
	2016-21057-02	권민우	한국과학기술정보연구원
	2023-23628-02	김병진	한국폴리텍대학 청주캠퍼스
	2023-23616-02	조영래	티쓰리큐(주)
	2002-9212-02	이석준	가천대학교
	2023-23620-02	공성곤	세종대학교
	2023-23613-02	이미라	한국전자기술연구원

회원구분	회원번호	성명	직장명
정회원	2023-23612-02	최필주	부경대학교
	2023-23609-02	이지현	한국전자기술연구원
	2023-23608-02	김병기	(주)코메스타
	2023-23604-02	고완진	구미전자정보기술원
	2023-23598-02	전상훈	한국전자통신연구원
	2023-23594-02	박민정	금오공과대학교
	2011-17180-02	정종진	한국전자기술연구원
	2001-8280-02	이용주	한국전자통신연구원
	2023-23603-02	이성희	한국과학기술정보연구원
	2023-23591-02	Ngo Thien Thu	Kyunghee University
	2023-23590-02	Jihyeon Ryu	광운대학교
	2006-13259-02	문경렬	한국소재융합연구원
	2023-23583-02	박유림	한국국방연구원
	2023-23574-02	정희진	한국과학기술정보연구원
	2023-23571-02	이재환	한림대학교
	2023-23570-02	정영상	텔레픽스 주식회사
	2023-23567-02	양창규	서울벤처대학원대학교
	2023-23566-02	오치민	(주)세이프모션
	2023-23565-02	유진승	한국과학기술정보연구원
	2023-23564-02	민무홍	성균관대학교
	2023-23562-02	윤정일	한국전자통신연구원
	2023-23559-02	김웅	에프아이시스
준(학생)회원	2022-23214-03	박진호	동의대학교
	2023-23686-03	정승민	순천향대학교
	2023-23687-03	담스문 리타나	순천향대학교
	2023-23689-03	이민섭	고려대학교
	2023-23688-03	Ielisa adeba jilcha	아주대학교
	2023-23683-03	민시온	경북대학교
	2023-23680-03	김동현	경북대학교
	2023-23679-03	최철훈	한양대학교

회원구분	회원번호	성명	직장명
준(학생)회원	2023-23681-03	정성욱	한양대학교
	2023-23682-03	장승완	순천향대학교
	2023-23676-03	홍정범	인하대학교
	2021-22954-03	일흠존	순천향대학교
	2023-23673-03	송동수	부산대학교
	2023-23671-03	유인식	서울시립대학교
	2021-22687-03	조경록	국립안동대학교
	2019-22350-03	권재환	송실대학교
	2023-23666-03	윤영은	순천대학교
	2023-23667-03	장민수	광운대학교
	2021-22787-03	강길욱	세종대학교
	2022-23269-03	김유준	세종대학교
	2023-23661-03	신정민	인하대학교
	2023-23662-03	신현호	성균관대학교
	2023-23655-03	LE THI KIM NGOC	Dept. of AI Systems Engineering, Sungkyunkwan University
	2023-23654-03	양희찬	아주대학교
	2015-20097-03	이선민	호서대학교
	2018-21831-03	정수민	부산대학교
	2021-22741-03	홍석민	송실대학교
	2022-23147-03	Cho Nwe Zin Latt	부경대학교
	2022-23160-03	팽소니	순천향대학교
	2023-23437-03	이정민	한양대학교
	2023-23621-03	신유석	서울과학기술대학교
	2023-23629-03	손영진	이화여자대학교
	2023-23632-03	박성빈	한양대학교
	2023-23635-03	김우재	전남대학교
	2023-23639-03	신재정	순천향대학교
	2023-23641-03	이유진	광운대학교
	2023-23642-03	차예원	호서대학교

회원구분	회원번호	성명	직장명
준(학생) 회원	2023-23643-03	김채윤	광운대학교
	2023-23644-03	Sheng Ying	한양대학교
	2023-23646-03	노유진	광운대학교
	2023-23647-03	강지연	광운대학교
	2023-23649-03	이재원	광운대학교
	2023-23650-03	이창열	한양대학교
	2023-23651-03	변규린	성균관대학교
	2023-23652-03	유사라	숙명여자대학교
	2023-23625-03	이수영	고려사이버대학교
	2023-23614-03	이봉준	한양대학교
	2023-23622-03	유민희	고려대학교
	2023-23624-03	장이완	한양대학교
	2023-23626-03	안자건	한양대학교
	2023-23627-03	Zhang Songming	한양대학교
	2019-21999-03	장경배	한성대학교
	2023-23619-03	채송화	숙명여자대학교
	2019-22237-03	김현준	한성대학교
	2022-23246-03	이주혁	한경국립대학교
	2023-23605-03	진명	경상국립대학교
	2023-23606-03	한상훈	부산대학교
	2023-23607-03	박준영	단국대학교
	2023-23610-03	Sinha Shrutika	국민대학교
	2023-23611-03	김대훈	부경대학교
	2023-23615-03	정현승	고려대학교
	2023-23617-03	김명준	고려대학교
	2023-23618-03	Tran Dao Huy Cuong	세종대학교
	2023-23623-03	강민우	고려대학교
	2022-23193-03	김양은	서울미디어대학원대학교
	2023-23585-03	백승준	광운대학교
	2023-23586-03	Khasanova Nodira Gayrat Kizi	부경대학교

회원구분	회원번호	성명	직장명
준(학생) 회원	2023-23587-03	하중수	서울미디어대학원대학교
	2023-23588-03	Vo Hoang Anh	세종대학교
	2023-23589-03	Ignacio, Marvin John	세종대학교
	2023-23592-03	Viet-Tuan Le	세종대학교
	2023-23593-03	Diep Giang Thuy Khuong	세종대학교
	2023-23595-03	박수연	전남대학교
	2023-23596-03	이정호	단국대학교
	2023-23597-03	최영찬	단국대학교
	2023-23599-03	장재훈	서울미디어대학원대학교
	2023-23600-03	김세영	단국대학교
	2023-23601-03	Wang Jia	세종대학교
	2023-23602-03	김태석	세종대학교
	2023-23582-03	Lyu Zhi	전주대학교
	2021-22988-03	정인수	아주대학교
	2023-23568-03	김우현	서울과학기술대학교
	2023-23569-03	김동섭	부산대학교
	2023-23572-03	박민서	아주대학교
	2023-23573-03	Seung-kyu Choi	서울과학기술대학교
	2023-23575-03	이석원	부산대학교
	2023-23576-03	장석준	순천향대학교
	2023-23577-03	김영훈	부산대학교
	2023-23578-03	전선함	고려대학교
	2023-23579-03	윤성철	순천향대학교
	2023-23580-03	김태훈	순천향대학교
	2023-23581-03	전지영	고려대학교
	2021-22935-03	신유진	상명대학교
	2021-22937-03	홍혜진	상명대학교
	2023-23561-03	김정혁	고려사이버대학교
	2023-23563-03	김지수	고려대학교

특별 법인회원 명단

구 분	대표자	주 소
델인터내셔널	김경진 대표	서울시 강남구 테헤란로 152 강남파이낸스센터 18층
삼성SDS(주)	황성우 대표	서울시 송파구 올림픽로35길 123(신천동) 삼성SDS타워
송암시스콤(주)	김도완, 이지학 대표	경기도 성남시 분당구 판교로228번길 17 판교세븐벤처밸리 2단지 1동 8층
(주)센스톤	유창훈 대표	서울시 동대문구 천호대로 329, 5층(답십리동, 도이치모터스빌딩)
(주)시티랩스	조영중 대표	경기도 안양시 만안구 예술공원로 153-32 3층
에스넷시스템(주)	유홍준, 장병강 대표	서울시 강남구 선릉로 514 (삼성동) 성원빌딩 10층
(주)LG CNS	김영섭 대표	서울시 강서구 마곡중앙8로 71 LG사이언스파크 E13, E14
클로센(주)	이석희 대표	서울시 마포구 마포대로 155 LG마포빌딩
정보통신산업진흥원	허성욱 원장	충청북도 진천군 덕산면 정통로 10
정보통신정책연구원	권호열 원장	충청북도 진천군 덕산면 정통로 18
(주)지란지교시큐리티	윤두식 대표	서울시 강남구 역삼로 542(대치동 신사S&G 5층)
(주)지엘어소시에이츠	이용렬 대표	서울시 강남구 봉은사로 449 밤부타워
KCC정보통신	이상현, 권혁상 대표	서울시 강서구 공항대로 665 KCC오토타워
(주)코리아퍼스텍	장영규, 김상직 대표	서울시 강서구 화곡로 222
티에스라인시스템(주)	최국현 대표	서울시 영등포구 영신로 220, 805호~806호
한국인터넷진흥원	이원태 원장	전라남도 나주시 진흥길 9
한국전자통신연구원	김명준 원장	대전광역시 유성구 가정로 218
한국지능정보사회진흥원	황종성 원장	대구광역시 동구 첨단로 53
한국화웨이기술(유)	Tian Feng, Gao Aozhan 대표	서울시 중구 세종대로9길 41(서소문동) 퍼시픽타워 9층
(주)시큐에버	변해진, 이준엽 대표	서울시 송파구 백제고분로9길 10 MBC아카데미 4층
(주)에이텍	이상훈 대표	경기도 성남시 분당구 판교로 289 에이텍빌딩
(주)케이넷츠	오경훈 대표	서울시 금천구 가산디지털2로 123 1107호
(주)동인시스템	곽동달 대표	부산광역시 해운대구 재송동 1216번지 6층 620호



한국정보처리학회 기관지 원고 집필 안내



한국정보처리학회는 학회지 「정보처리학회지」와 논문지 「정보처리학회논문지 A·B·C·D」를 발행하고 있습니다. 「정보처리학회지」는 새로운 기술동향을 비롯해서 각종 정보를 게재하고, 회원의 지식 향상을 목적으로 하며, 「정보처리학회논문지 A·B·C·D」는 회원의 연구 결과를 발표하는 장입니다.

본 안내는 학회 기관지의 원고 집필 요령을 정리한 것으로, 집필 시 참고로 하시기 바랍니다.

『정보처리학회지』 원고 집필 안내

- 제 1 조** 학회지에 게재할 원고의 종류는 특집, 특별기고, 기획기사, 정보 관련 기술 동향 및 편집위원회가 인정하는 것으로 한다.
- 제 2 조** 투고자는 원칙적으로 본 학회 회원으로 한다. 단, 회원과의 공동기고자 및 초청기고자는 예외로 한다.
- 제 3 조** 원고는 수시로 접수하며 접수일은 원고가 본학회 편집위원회에 도착한 날로 하고, 접수된 원고는 편집위원회에서 게재여부를 결정한다.
- 제 4 조** 원고는 가장 많이 사용되는 워드프로세서로 작성한 파일을 함께 제출한다.
- 제 5 조** 원고의 내용은 정보처리 관련자가 이해할 수 있는 정도로 작성한다.
- 제 6 조** 투고자는 200자 이내의 약력을 제출하여야 한다. 게재가 확정된 원고에 대해서는 추후 저자의 사진을 제출해야 한다.
- 제 7 조** 본 학회지에 게재된 내용은 본 학회의 승인없이 영리목적으로 무단 복제하여 사용할 수 없다.
- 제 8 조** 원고 작성 방법은 다음과 같다.
- (1) 1페이지 기술 분량 : A4용지 30행×40자 내외
 - (2) 원고분량 : 6~8페이지 내외
 - (3) 참고문헌 : 참고 문헌은 저자명에 의한 사전식으로 기술하되, 각 참고 문헌은 잡지의 경우 “번호저자명, 제목, 잡지명, 권, 호, 페이지, 연도”의 순으로 기술한다. 단, 참고문헌 인용시에는 대괄호를 이용할 것(예 [1], [2], [3], [4] 등)
- (예) [1] 김철수, 김수철, “한국 정보 처리 산업에 관한 연구”, 한국정보처리논문지, 제1권, 제1호, pp.23-43, 1997.
- [2] 이영희, 컴퓨터입문, pp.234, 출판사, 1997.
- [3] L. Lanomt, “Synchronization Architecture and Protocols”, IEEE Trans. on Comm., Vol. 23, No. 3, pp.123-132, 1997.
- [4] Steinmetz, Multimedia : Computing, Communications & Applications, PII, 1995.
- (4) 내용표기에 있어서, 장, 절 등의 표시는 ‘ 1, 1.1, 1.1.1, 가, 1), 가), (1), (가)’의 순서로 한다.
 - (5) 원고는 ‘제목-소속-성명-목차-본문-참고문헌’의 순으로 기술하며, 첫장 하단에는 회원 구분을 명기한다.
 - (6) 표의 제목은 “〈표 1〉대한민국” 과 같이 표의 상단에 기술하고, 그림의 제목은 “(그림 1)서울”과 같이 그림의 하단에 기술하며, 사진판으로 사용할 수 있도록 백지에 정서해야 한다.

본 규정은 1997년 1월 1일부터 효력을 발생한다.



기타 원고 모집 안내



당 학회지 편집위원회에서는 학회지 「정보처리학회지」에 게재할 각종 원고를 회원 여러분으로부터 모집하고 있습니다. 많은 투고와 참여있으시기 바랍니다.

1. 모집내용

다음에 대한 원고를 모집합니다.

- (1) 해설 : 정보처리에 관련된 신기술 또는 이론으로서 당 학회 회원의 관심도가 높은 내용
- (2) 외국기사 : 외국 잡지에 게재된 기사로서 당 학회 회원에게 유익한 내용
- (3) 서평 : 최근에 출판된 책으로서 당 학회 회원에게 유익한 도서의 소개 또는 비평
- (4) 뉴스 : 정보처리에 관한 국제규모의 회의, 대회의 보고 등 시사성이 높고 당 학회 회원에게 널리 알릴 가치가 있는 내용
- (5) 기관소개 : 국내 기관 또는 외국 기관
- (6) 기타 : 당 학회 회원에게 유익한 내용

2. 응모 자격

당 학회 회원으로 한다.

3. 응모 절차

원고는 학회지 편집위원회에서 정한 투고 규정에 의거하여 다음 순서로 기술하여 주시기 바랍니다.

- (1) 제목
서평의 경우에는 저자명, 책이름, 페이지수, 출판사, 발행년도, 가격 등으로 기술한다.
어느 장르에 속하는지를 첫페이지 오른쪽 상단에 표시한다.
- (2) 필자명, 소속, 필자 연락처
- (3) 본문
본문은 서평의 경우 2,000자 정도, 뉴스의 경우 1,000자 정도로 한다.
- (4) 참고문헌, 부록, 그림, 표
- (5) 필자 소개
이름, 경력과 학력을 기술한다.

4. 원고 취급

투고된 원고는 학회지 편집위원회에서 심사를 한 후 게재여부를 결정합니다. 게재가 결정되었을 경우에는 원고 수정을 부탁하는 경우가 있습니다. 서평의 경우에는 필자의 사진이 필요하므로 게재 결정 후 학회 사무국으로 우송해야 됩니다.

5. 원고료

학회지 규정에 의거하여 소정의 원고료를 지급합니다.

6. 보낼 곳

04376 서울특별시 용산구 한강대로 109, 1002호(한강로 2가 용성비즈텔)
한국정보처리학회 학회지 편집위원회
chh@kips.or.kr



정보처리학회 논문지 투고 규정

1. 원고의 전자 투고

모든 원고는 전자 형태(MS Word, 아래아 한글, 혹은 PDF 형태)로 학술지 웹사이트(<http://ktccs.kips.or.kr>, <http://ktsde.kips.or.kr>)를 통해 온라인으로 투고하여야 한다. 투고 규정은 해당 웹사이트에서도 볼 수 있으며, 본 학술지에 투고하는 모든 원고들은 이 규정을 준수하여야 한다. 그렇지 않을 경우 원고가 반송되게 되며 이로 인해 출판이 지연될 수도 있다. 원고 투고에 관한 문의는 이메일(kips@kips.or.kr)이나 전화(+82-2-2077-1414), 팩스(+82-2-2077-1472)를 통해 학회 사무국으로 한다. 저자 중에 1인은 학회 회원으로 가입되어야 함을 원칙으로 한다.

2. 연구 및 출판 윤리

본 학술지는 Guidelines on Good Publication(<http://publicationethics.org/node/11184>)에 기술된 연구 및 출판 윤리 지침을 따른다.

2.1 이해갈등관계 명시

저자는 기업으로부터의 재정적 지원 또는 연계, 이익집단으로부터의 정치적 압력 등과 같은 이해 갈등 관계가 있으면, 이에 관한 정보를 밝혀야 한다. 특히, 연구에 관계된 모든 지원금의 출처를 명백히 진술해야 한다.

2.2 저자 요건

1) 연구의 기본개념설정과 설계, 자료수집, 또는 자료분석과 해석에 지대한 공헌을 하고, 2) 원고를 작성하거나 내용의 중요 부분을 변경 또는 개선하고, 3) 최종 원고 내용에 대한 동의, 4) 연구 작업 각 부분 마다 관련된 정확성 또는 무결성과 관련된 질문이 적절하게 조사되고 해결되었음을 보장하는 해당 작업의 모든 측면에 대해 책임을 지는 계약에 관한 네 가지 조건을 모두 충족한 사람만이 논문 저자로서 원고에 나열되어야 한다. 원고의 최초 투고 후, 어떠한 저자 변경 사항(저자 추가, 저자 삭제, 혹은 저자 순서 변경)도 편집인에게 편지로 알려주고 승인을 받아야 한다. 이 편지에는 해당 논문의 모든 저자들의 서명이 포함되어야 한다.

2.3 이중게재/이중투고 금지

투고된 모든 원고는 다른 학술지에 이미 실렸거나 또는 심사 중이어서는 안된다. 채택된 원고의 모든 부분은 편집위원회의 허가 없이 다른 과학학술지에 이중게재 하여서는 안 된다. 본지에 실린 논문의 이중게재 발각 시에는 저자 및 소속기관에 이를 알릴 것이며, 저자에게 제재가 가해 될 것이다.

3. 상호심사 절차

모든 원고는 편집위원이 위촉한 2인 또는 3인의 심사위원들이 평가하며, 연구의 질과 독창성, 그리고 과학적 중요성을 바탕으로 심사하여 채택 여부를 결정한다. 원고투고 후 심사 의견과 결과를 온라인 투고시스템과 이메일로 통보한다. 교신저자는 수정된 원고를 온라인으로 재투고해야 하며 심사자의 지적에 따라 변경된 내용을 각 항목별로 진술해야 한다. 편집위원회 결정 이후 8주가 경과해도 수정된 원고를 재투고하지 않을 시에는 철회로 간주한다. 저자는 학술지 웹사이트에서 투고 논문의 심사 진행 현황을 확인할 수 있다.

4. 저작권

출판된 모든 원고는 한국정보처리학회의 자산이 되며, 서면허가 없이 다른 곳에 출판되어서는 안 된다. 출판이 결정되면 저자는 저작권양도 서식을 기재하여 팩스, 우편 또는 이메일로 학회 사무국에 보내야 한다.

5. 원고 작성

5.1 언어

모든 원고는 국문 또는 영문으로 작성하여야 한다. 국문 논문의 경우, 서지 정보(제목, 저자, 소속, 교신저자의 주소와 이메일), 표, 그림, 감사의 글, 참고문헌 등은 모두 영문으로 기술하여야 한다. 심사를 위한 초기 투고 원고에는 저자 정보를 포함시키지 말아야 한다. 하지만, 논문 수락 판정을 받은 후 제출하는 최종본에는 저자 정보를 포함시켜야 한다.

5.2 일반적인 사항

- 1) 원고는 MS Word나 한글문서로 작성한다.
- 2) 원고는 A4 (21.0×29.7cm) 용지에 10point 글씨크기로 행 사이를 2행 간격(double space)으로 하여 작성하되, 상하좌우 모두 2.5cm의 여백을 둔다.
- 3) 모든 단위는 International System(SI) of Units 에 따라 기술하여야 한다. 퍼센트(%)와 온도(°C)를 제외한 모든 단위는 한 칸의 공백 다음에 기술해주어야 한다.

5.3 출판 유형

한국정보처리학회논문지는 연구논문(research paper), 기획특집 논문(special issue paper) 등을 출판한다.

- 1) 연구논문(research paper): 본 학술지가 다루는 범위 안에서 새로운 학술적 발견들을 상호 심사과정을 거쳐 연구논문으로 출판할 수 있다. 연구논문에는 이론이나 실험에 관한 새롭고 중요한 결과들이 기술되어야 한다. 논문의 길이 제한은 20쪽 이내이다.
- 2) 기획특집 논문(special issue paper): 본 학술지가 다루는 범위안에서 필요시 최신 이슈나 새로운 아이디어를 주제로 하여 상호 심사과정을 거쳐 논문으로 출판할 수 있다. 논문의 길이 제한은 20쪽 이내이다.

5.4 연구논문

원고는 국문제목, 국문요약과 국문키워드, 영문제목, 영문요약과 영문키워드, 본문, 감사의 글(필요 시), 참고문헌을 순서대로 포함한다.

1) 요약과 키워드

요약은 무슨 연구를 어떻게 수행하였는지, 주된 연구결과와 그 중요성에 관해 간결하게 기술하여야 한다. 표나 참고문헌 번호를 포함하지 않은

하나의 문단으로 기술되어야 한다. 초록의 하단부에는 연구분야와 내용을 나타낼 수 있는 3 ~ 5단어 이내의 키워드를 기재하여야 한다.

2) 본문

- 장질 제목: 장이나 절의 제목은 1, 1.1, 1) 와 같이 4 단계 레벨로 표기할 수 있다.
 - 본문 중 참고문헌 인용: 참고문헌은 본문에서 처음 인용되는 순서대로 번호를 붙인다. 그리고 본문에서 참고문헌을 인용할 때는 해당 참고문헌의 번호를 [1, 4, 7] 혹은 [6-9]와 같이 각괄호 안에 기재한다.
 - 약어: 약어는 저자의 편의성보다는 독자에게 도움을 줄 수 있는 방식으로 사용되어야 한다. 따라서 약어는 가급적 제한적으로 사용하는 것이 바람직하다. 표와 그림을 포함해 본문에서 세 번 이상 등장하지 않는 약어의 사용은 가급적 피하라. 약어는 본문에서 처음 사용될 때 축약 이전의 형태로 정의되어야 한다.
 - 표: 표는 본문에서 인용되는 순서대로 아라비아 숫자로 번호를 붙인다. 표의 제목과 설명은 영어로 작성하며, 본문 내용을 읽지 않고도 이해할 수 있도록 간결 명료하게 작성한다.
 - 그림: 그림은 본문에서 인용되는 순서대로 아라비아 숫자로 번호를 붙인다. 동일한 번호에 두 개 이상의 그림이 있는 경우, Fig. 1A, Fig. 1B와 같이 아라비아 숫자 뒤에 알파벳 대문자를 기입하여 구분한다. 자신이 그린 그림이 아니면 저작권자의 허락을 받아야 하며 각주에 이를 밝혀야 한다.
- 3) 감사의 글
필요한 경우, 본문 뒤에 감사의 글을 포함시킬 수 있으며, 연구비 지원 또는 다른 지원에 대한 내용을 명시할 수 있다.
- 4) 참고문헌
모든 참고문헌은 영어로 기술하며, 제출 원고의 내용과 분명히 관련이 있는 것들이어야 한다. 참고문헌은 본문에서 처음 인용되는 순서대로 번호를 붙인다. 참고문헌들은 반드시 원저 확인을 통해 출처를 검증하는 것이 필요하다.
다음 예시들을 참고하여 참고문헌들을 작성한다.

Journal Article

- S. Y. Hea and E. G. Kim, "Design and implementation of the differential contents organization system based on each learner's level," *The KIPS Transactions: Part A*, Vol.18, No.6, pp.19-31, 2011.
- S. Y. Hea, E. G. Kim, and G. D. Hong, "Design and implementation of the differential contents organization system based on each learner's level," *KIPS Transactions on Software and Data Engineering*, Vol.19, No.3, pp.19-31, 2012.

Book & Book Chapter

- S. Russell and P. Norvig, "Artificial Intelligence: A Modern Approach," 3rd ed., New York: Prentice Hall, 2009.
- J. L. Hennessy and D. A. Patterson, "Instruction-level parallelism and its exploitation," in *Computer Architecture: A Quantitative Approach*, 4th ed., San Francisco, CA: Morgan Kaufmann Pub., ch. 2, pp.66-153, 2007.
- D. B. Lenat, "Programming artificial intelligence," in *Understanding Artificial Intelligence*, Scientific American, Ed., New York: Warner Books, Inc., pp.23-29, 2002.

Conference Proceedings

- A. Stoffel, D. Spretke, H. Kinnemann, and D. A. Keim, "Enhancing document structure analysis using visual analytics," in *Proceedings of the ACM Symposium on Applied Computing*, Sierre, pp.8-12, 2010.

Dissertations

- J. Y. Seo, "Text-driven construction of discourse structures for understanding descriptive texts," Ph.D. dissertation, University of Texas at Austin, TX, USA, 1990.

Online Source

- Thomas Clabum, Google Chrome 18 brings faster graphics [Internet], <http://www.techweb.com/news/232800057/google-chrome-18-brings-faster-graphics.html>.

6. 투고료 및 게재료

6.1 투고료

본 학술지에 원고를 투고할 때, 투고자는 1편당 일반 심사의 경우 50,000원(US \$50), 급행 심사의 경우 350,000원(US \$350), 기획특집 심사의 경우 100,000원(US \$100)을 학회에 납부하여야 한다.

6.2 게재료

채택된 논문의 투고자는 논문의 게재를 위해 다음과 같은 논문 게재료를 학회 사무국에 납부하여야 한다.

- 인쇄쪽수가 1 ~ 6쪽인 경우, 100,000원
- 인쇄쪽수가 7쪽 이상인 경우, 100,000원 + 50,000원 추가 / 쪽당

6.3 결제

- 계좌이체
 - KEB하나은행: 232-13-01249-5 (예금주: 한국정보처리학회)
 - 우체국: 012559-01-000730 (예금주: 한국정보처리학회)
- 온라인 결제
 - 온라인 투고시스템에서 로그인 후 결제

7. 본 투고 규정은 2020년 1월 31일부터 효력을 발생한다.



입회 안내

국가가 지향하는 첨단 정보처리 산업과 기술혁신의 시대에 부응하여 첫째, 정보처리 학술활동의 활성화, 둘째, 정보처리 기술의 산학연 협동의 내실화, 셋째, 정보처리 기술의 국제화와 표준화 등 회원봉사 활동에 역점을 두고 정보화사회를 선도하는 명실상부한 정보처리 분야의 정통학회인 사단법인 한국정보처리학회에서는 정보처리분야에 종사하고 계시는 여러분들의 많은 입회를 바라고 있습니다.

주요 목적 사업

1. 정보처리에 관한 각종 학술발표회 및 전시회 개최
2. 정보처리에 관한 지식 및 기술 보급에 관한 사업
3. 정보처리 기술의 상호 협조 및 정보 교환
4. 정보처리에 관한 표준화 사업
5. 국제적 학술 교류 및 기술 협력
6. 학회지 및 논문지 발간
7. 정보처리에 관한 문헌 발간
8. 기타 본 학회 목적 달성에 필요한 사업

(정관 제4조)

회원의 종류 및 자격

1. 특별회원 : 정보처리 분야 발전에 기여하고 본 학회의 취지에 찬동하는 법인 및 단체.
2. 명예회원 : 학식과 덕망이 높고 본 학회의 발전에 크게 기여한 자.
3. 정 회원 : 정보처리 관련 분야를 전공하여 학사학위 이상을 취득한 자 또는 정보처리 관련분야에서 2년이상 근무한 자.
4. 준 회원 : 정보처리 관련학과 학생 또는 대학원생
5. 단체회원 : 도서관 또는 초·중·고 교육기관

(정관 제6조)

회원의 혜택

1. 정보처리학회지(논설, 기술보고, 해설, 전망, 강좌, 단편정보 등 게재) 발행. 무료배포
2. 정보처리학회논문지 및 특집호(학술연구논문, 심사완료 후 게재) 발행.
3. 춘추계 학술발표회와 각종 학술행사에 참가 및 논문발표
4. 전문분과연구회의 활동자격과 각종 학술행사에 참가 및 논문발표
5. 국제 학술회의 활동 및 외국 학회에 참가 및 추천
6. 정보처리 및 기술발전에 업적이 있는 회원에게는 각종 학회상 수여

회비

1. 특별회원 회비는 이사회의 결정에 따르면 종신회원·정회원·준회원·단체회원 회비는 다음과 같다.

구 분	종 신 회 원	정 회 원	준 회 원	단 체 회 원
연 회 비	600,000원	60,000원	40,000원	300,000원

※ 논문 구독료 각권 별도 2만원 (필요시 구독)

2. 회원가입은 학회 홈페이지를 통하여 회원정보를 입력하신후 회비를 신용카드 결제 및 아래의 은행으로 입금하여 주시기 바랍니다.
 하 나 은 행 계좌번호 : 234-890011-51605 예금주 : (사단)한국정보처리학회
 우 체 국 계좌번호 : 012559-01-000730 예금주 : 한국정보처리학회

문의처 : 04376 서울특별시 용산구 한강대로 109, 1002호(한강로 2가 용성비즈텔)

사단법인 한국정보처리학회 사무국 귀하

전 화 : (02) 2077-1414(代) 팩 스 : (02) 2077-1472

홈페이지 : www.kips.or.kr

e-mail : chh@kips.or.kr



연구회 안내



당 학회에는 현재 다음과 같은 연구회가 구성되어 있으며, 이들 연구회는 위원장을 중심으로 하여 현재 활발한 연구 활동을 하고 있습니다. 연구회에 가입을 원하시는 회원은 연구회 가입 원서를 작성하셔서 당 학회 사무국 또는 각 위원장에게 보내주시기 바랍니다. 회원 여러분의 많은 가입을 부탁드립니다. 연구회 발족 등에 관한 의견이 있으시면 학회로 연락 주시기 바랍니다.

e - B r i d g e 연 구 회	우 정 기 술 연 구 회
위원장 : 이상근 교수 (서강대학교) 전 화 : 02)705-7987 e-mail : slee1028@sogang.ac.kr	위원장 : 정 훈 부장 (ETRI) 전 화 : 042)860-6470 e-mail : hoonjung@etri.re.kr
I T 융 합 서 비 스 연 구 회	웹 3.0 연 구 회
위원장 : 박석천 교수 (가천대학교) 전 화 : 031)750-5328 e-mail : scpark@gachon.ac.kr	위원장 : 민경식 팀장 (KISA) 전 화 : 061)820-1454 e-mail : kyoungsik@kisa.or.kr
I T 정 책 연 구 회	인 공 지 능 연 구 회
위원장 : 오길록 교수 (숭실대학교) 전 화 : e-mail : gilrokoh@paran.com	위원장 : 전유부 교수 (동국대학교) 전 화 : 02)2290-1444 e-mail : jeonyb@dgu.ac.kr
데 이 터 과 학 연 구 회	전 산 교 육 연 구 회
위원장 : 김현희 교수 (동덕여자대학교) 전 화 : 02)940-4595 e-mail : heekim@dongduk.ac.kr	위원장 : 김형진 교수 (전북대학교) 전 화 : 063)270-4783 e-mail : kim@chonbuk.ac.kr
블 록 체 인 기 술 및 응 용 연 구 회	전 산 수 학 연 구 회
위원장 : 정영식 교수 (동국대학교) 전 화 : 02)2260-3374 e-mail : ysjeong@dongguk.edu	위원장 : 박진홍 교수 (선문대학교) 전 화 : 041)530-2224 e-mail : chp@omega.sunmoon.ac.kr
빅 데 이 터 컴 퓨 팅 연 구 회	전 자 정 부 연 구 회
위원장 : 이필규 교수 (인하대학교) 전 화 : 032)860-7448 e-mail : pkrhee@inha.ac.kr	위원장 : 이재두 수석 (NIA) 전 화 : 02)2131-0370 e-mail : leejaeedu@gmail.com
소 프 트 웹 어 공 학 연 구 회	정 보 통 신 응 용 연 구 회
위원장 : 김정아 교수 (가톨릭관동대학교) 전 화 : 033)649-7801 e-mail : clara@cku.ac.kr	위원장 : 오진태 부장 (ETRI) 전 화 : 042)860-4977 e-mail : showme@etri.re.kr
스 토 리 지 시 스템 연 구 회	지 식 및 데 이 터 공 학 연 구 회
위원장 : 신범주 교수 (부산대학교) 전 화 : 055)350-5417 e-mail : bjshin@pusan.ac.kr	위원장 : 진병운 박사 (ETRI) 전 화 : 042)860-6544 e-mail : bwjin@etri.re.kr
양 자 산 업 기 술 응 용 연 구 회	컴 퓨 터 소 프 트 웹 어 연 구 회
위원장 : 박종혁 교수 (서울과학기술대학교) 전 화 : 02)970-6702 e-mail : jhpark1@seoultech.ac.kr	위원장 : 박두순 교수 (순천대학교) 전 화 : 041)530-1317 e-mail : parkds@sch.ac.kr
에 너 지 그 리 드 정 보 처 리 연 구 회	클 라 우 드 서 비 스 연 구 회
위원장 : 박성준 원장 (한전KDN) 전 화 : 061)931-6900 e-mail : jspark_96@kdn.com	위원장 : 유진호 교수 (상명대학교) 전 화 : 02)781-7574 e-mail : jhyoo@smu.ac.kr



◆ 납입방법 : 신용카드

◆ 결재내용 : 학회 회비 / 세미나 참가비 / 논문 구독료 / 논문 게재료

학 회 회 비	종신회원 ₩600,000() 정회원 ₩60,000()
	준 회 원 ₩40,000() 기 타 (₩)
행 사 등 록 비	(₩)
논 문 구 독 료 (각 권당 2만원)	☐ 소프트웨어 및 데이터 공학(KTSDE) ☐ 컴퓨터 및 통신 시스템(KTCCS) (₩)
논 문 게 재 료	()권 ()호 (₩)
기 타	(₩)

◆ 신용카드 사용내역서

카 드 명	☐ 신한카드 ☐ 국민카드 ☐ 비씨카드	결 재	일시불()	※ 타카드 사용 불가
카드번호	□□□□ □□□□ □□□□ □□□□			
지불금액	원	카드유효기간	년 월 전 화	
소 속		성 명	서 명	
“상기 금액을 정히 지불합니다” 사단법인 한국정보처리학회				

※ 신한카드, 국민카드 및 비씨카드만 사용이 가능합니다.

※ 반드시 팩스로 회송바랍니다.

※ 학회 연회비 및 논문 구독료는 홈페이지에서 로그인 후 모든 카드로 온라인 카드 결제가 가능합니다.

☞ 보내실곳 : 한국정보처리학회

전화 : (02)2077-1414

팩 스 : (02)2077-1472

http://www.kips.or.kr

e-mail : chh@kips.or.kr

04376 서울특별시 용산구 한강대로 109, 1002호(한강로 2가 용성비즈텔)

학 회 사 무 국

사무국장	김은순 (내선 2)	uskim@kips.or.kr	사무국 총괄 / 대외업무 / 재정 / 제회의 / 선거 / 각 위원회 / 지회 / 본부
부 장	이주연 (내선 1)	joo@kips.or.kr	포상 / JIPS / IT21 글로벌 컨퍼런스 / 윤당학술상 / 정총연합회
차 장	윤영숙 (내선 3)	ysyun@kips.or.kr	재무 / 연구회 / KTCCS / ASK / ACK / CUTE, 위탁과제 / KIPS-AOH
사 원	조환희 (내선 5)	chh@kips.or.kr	회원 / 회계 / 학회지 / KTSDE / 단기강좌 / 여성위원회 / 홈페이지 및 홍보 / 기타행사

- 사무국주소 : (04376) 서울특별시 용산구 한강대로 109, 1002호(한강로2가, 용성비즈텔)
- 전 화 : (02) 2077-1414
- 팩 스 : (02) 2077-1472
- 대 표 메 일 : kips@kips.or.kr
- 홈 페 이 지 : www.kips.or.kr

정보처리학회지

제 30 권 제 4 호

등록일자 : 1994년 3월 31일
서기 2023년 12월 28일 인쇄
서기 2023년 12월 30일 발행

발 행 인 : 문 남 미

편 집 인 : 장 항 배

발 행 처 :  **한국정보처리학회**
KIPS Korea Information Processing Society

(04376) 서울특별시 용산구 한강대로 109, 1002호(한강로 2가, 용성비즈텔)

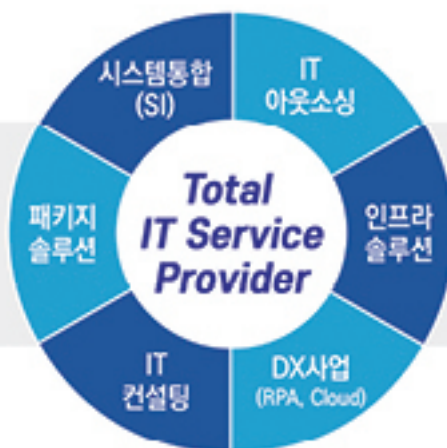
전 화 : (02)2077-1414(代) 팩 스 : (02)2077-1472

홈페이지 : www.kips.or.kr 이 메 일 : kips@kips.or.kr

* 제 작 : (주)이환디앤비 Tel : (02)2254-4301(代) <비매품>



상상을 현실로 ! ICT 혁신을 통한 **편리한 세상 !**



기술로 미래를 선도하는 **글로벌 ICT 전문기업**

KCC정보통신은 오랜 경험과 최신 ICT 기술력을 바탕으로 공공, 금융, 국방, 교육, 의료, 통신 등 다양한 분야에서 고객에게 최고의 IT서비스를 제공하고 있습니다. 편리함은 KCC정보통신이 고객에게 주고자 하는 소중한 가치입니다. 한 발 더 앞선 ICT 기술로 더 나은 미래를 만들어 가겠습니다.



Bring digital to every person, home and organization
for a fully connected, intelligent world

www.huawei.com

Big Data



5G Network



Ai, Cloud



Smart Device



IoT





**클라우드전환
쌍용정보통신과 함께
Non - Stop으로
할 수 있습니다**

**클라우드 너머의 미래
쌍용정보통신과 함께 설계하세요!**

**No.1 Cloud Native IT Service Company
DX Innovator, 클라우드 · AI 전문가 그룹**