ISSN 1976-5967
제14권
2021년 12월

군사과학정책연구

Military Science & Technology Annual Report

연구논문

RINSA
국 방 대 학 교
국가안전보장문제연구소

ISSN 1976-5967
제14권
2021년 12월

군사과학정책연구

Military Science & Technology Annual Report

국방대학교 국가안전보장문제연구소

목 차

연구보고 2021

무기체계 개발을 위한 딥러닝 기술 활용 방안

마 정 목

2021. 9.

국방대학교 국가안전보장문제연구소

목 차

그림목차

표 목 차

요 약 문

본 연구는 무기체계 개발을 위한 체계인 국방획득체계를 지원하기 위한 딥러닝 기술의 활용방안을 모색하기 위한 목표로 진행되었다. 먼저 국방획득체계를 이해하기 위해 국방획득의 역사 속에서 획득체계가 어떻게 형성되고 그 체계를 갖추어 갔는지 분석하였다. 1970년대부터 시대별로 구분하여 국방획득을 위한 중요한 정책들의 변화를 살펴보고, 이러한 환경의 변화 속에서 구축되고 발전해온 국방기획관리체계를 정리하였다. 특히 안보 상황 및 전략적 개념의 변화로 능력기반의 소요기획체계로의 변화가 진행되고 있으며, 4차 산업혁명과 같은 급속한 과학기술의 발전을 신속하게 받아들이기 위해 신속시범획득, 미래도전국방기술과 같은 사업을 진행하는 등 국방획득체계에 변화가 이루어지고 있다.

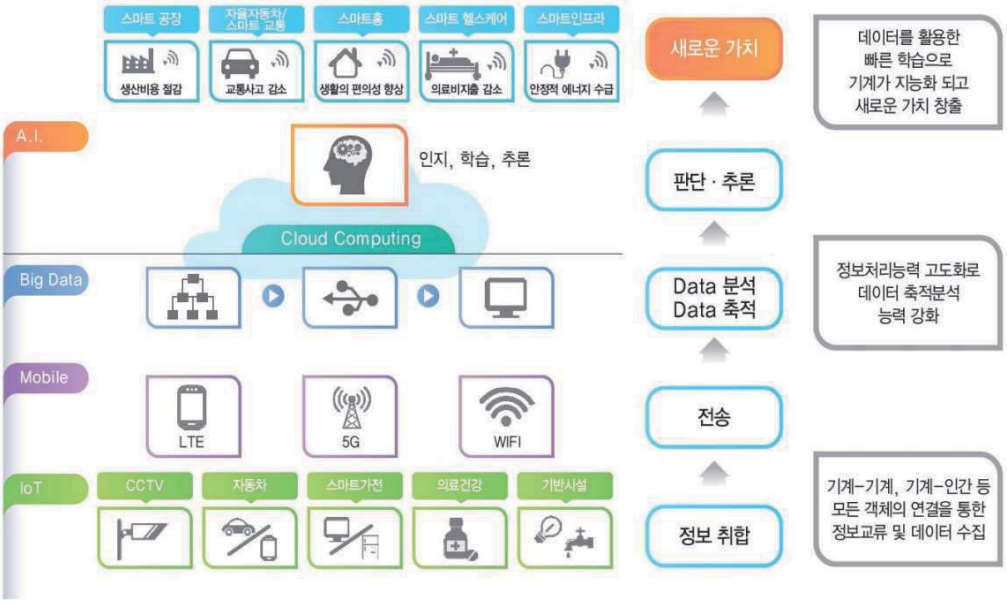
이러한 국방획득체계를 지원하기 위해 4차 산업혁명 기술 중 가장 핵심인 딥러닝 기술에 대해 살펴보았다. 딥러닝 기술이 출현하게 된 배경으로 인공지능과 함께 역사적 주요 사건들을 살펴보았고, 딥러닝 기술의 필수 개념을 정리하였다. 또한 본 연구를 통해 전력 업무를 담당하는 이들이 딥러닝 기술을 실제 적용할 수 있도록 데이터를 바탕으로 딥러닝을 구축하는 방법을 자세히 알아보았다.

국방획득체계의 동향과 딥러닝 기술의 이해를 바탕으로 진화하는 획득체계에서 딥러닝 기술이 활용될 영역을 분석하고, 딥러닝 기술의 적용을 위한 방안을 제시하였다. 활용될 영역으로는 소요기획 단계, 선행연구 단계, 연구개발 단계, 분석평가 단계로 구분하였고, 특히 연구개발 단계에서는 OODA Loop의 개념을 적용하여 제시하였다.

제1장 연구개요

1.1 연구 배경 및 필요성

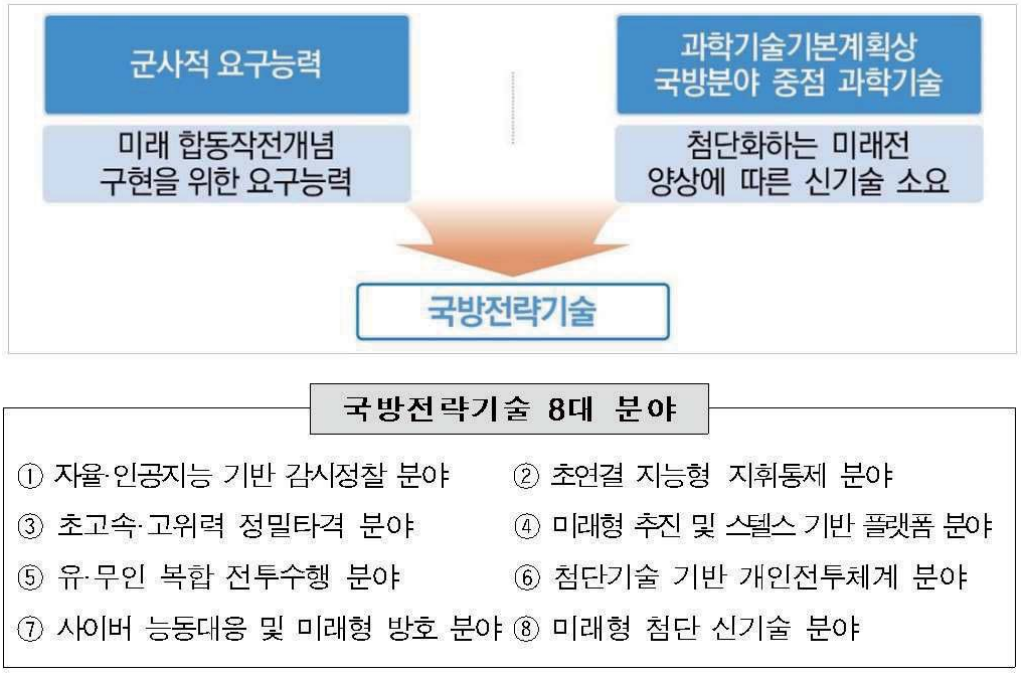
4차 산업혁명과 이를 이끄는 기술들은 이미 사회 전반은 물론이고 국방 영역에서도 변화를 자극하고 있다. 4차 산업혁명은 초연결, 초지능, 초융합으로 특징지을 수 있으며, 초지능을 바탕으로 한 자율능력을 갖춘 지능형 무기체계와 이들이 적시에 가용한 전력으로서 원하는 형태와 능력으로 필요한 국면에 집중될 수 있는 초연결과 초융합은 미래전을 그려나가는 핵심 요소이다. 이를 구현하기 위한 4차 산업혁명 관련 기술은 AI+ICBM으로 대표될 수 있다. AI는 인공지능을, ICBM은 사물인터넷(IoT), 클라우드, 빅데이터, 모바일을 각각 의미한다.



〈그림 1-1〉 AI+ICBM[1)]

1) 과기정통부. "지능정보사회 중장기 종합대책" 2016.

국방과학기술진흥정책서[2]에서도 미중 경쟁의 심화로 안보 유동성과 불확실성이 증대되고, 초국가적, 비군사적 위협 요인이 다양화되고 있는 가운데, 미국을 비롯한 주요 강대국들이 신개념 미래전에 대비하여 기술 분야에 집중하고 있음을 밝히고 있다. 특히, 미래전의 양상과 과학기술의 발전은 상호보완적인 특성을 가지고 있으며, 이에 따라 우리 군의 요구능력을 확보하기 위한 국방전략기술을 도출하여 제시하였다. 국방전략기술 8대 분야를 살펴보면 4차 산업혁명 관련 기술이 큰 역할을 차지하고 있음을 알 수 있다.

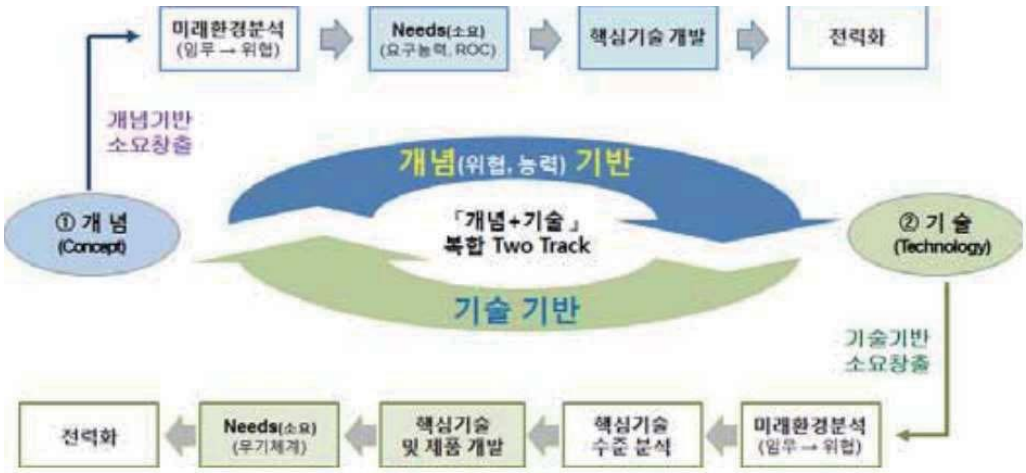


〈그림 1-2〉 국방전략기술의 도출[3]

이러한 변화의 물결 속에서 무기체계 개발의 틀이자 제도인 국방획득체계도 변화가 필요하다는 주장과 함께 다양한 시도가 일어나고 있다. 이종화와 심상렬

2) 2019-2033 국방과학기술진흥정책서(안)
3) 2019-2033 국방과학기술진흥정책서(안)

(2020)은 개념-기술 복합기반의 two-track 프로세스의 적용을 위한 안을 제시하면서, 기존의 싸우는 개념에 기초한 개념 기반과 기술주도형 전력증강 방식인 기술 기반이 병형될 수 있어야 한다고 주장하였다.



〈그림 1-3〉 개념기반, 기술기반 소요기획의 구분[4)]

방위사업청은 기존의 기본 획득체계가 철저한 계획과 검증을 통해 대형, 대규모 무기체계를 한정된 재원으로 확보하는데 최적화되어 있어, 기본 획득체계를 보완하여 4차 산업혁명 기술을 국방분야에 신속히 적용하기 위한 신속시범획득사업을 2020년부터 추진하고 있다. 국방과학연구소에서도 국방개혁 2.0 정책의 일환인 4차 산업혁명 기반의 국방연구개발 혁신을 추진하기 위해 제정된 '국방과학기술혁신 촉진법'을 바탕으로 혁신적이고 도전적인 미래도전국방기술을 기획하기 위한 노력을 기울이고 있다.

이에 따라 본 연구는 4차 산업혁명 기술 중 대표적인 기술인 딥러닝 기술이 신개념의 무기체계 개발을 위한 국방획득체계를 지원할 수 있는 방안에 대해 모색해 본다. 세부적으로는 획득체계의 역사와 현재를 이해하고, 최근 신기술 도입과 연계한 획득체계 발전 동향에 대한 분석이 필요하다. 다음, 딥러닝 기술의 역사와 동향

4) 이종화, 심상렬. "4차 산업혁명 첨단기술과 연계한 기술기반 소요기획체계 발전방안" 선진국방연구, 3(1), 2020.

을 이해하고, 실제 자료를 활용하여 딥러닝 기술을 적용하는 예를 살펴봄으로써 기술의 이해도를 높인다. 마지막으로 개선된 획득체계에서 딥러닝 기술이 활용될 영역을 분석하고, 딥러닝 기술의 적용을 위한 방안을 제시한다.

1.2 연구목표 및 범위

본 연구의 목표는 딥러닝 기술이 신개념의 무기체계 개발을 위한 획득체계를 지원할 수 있는 방안을 도출하는 것이다. 구체적으로는 다음의 3가지 중점분야에 대해 연구한다.

① 무기체계 개발을 위한 국방획득체계와 변화
② 딥러닝 기술의 이해와 실제
③ 딥러닝 기술의 획득체계 지원 방안

1.3 연구의 방법 및 기대효과

본 연구는 신개념의 무기체계 개발을 위한 획득체계를 지원하도록 딥러닝 기술을 적용할 수 있는 분야와 방안을 탐색하는 목적을 만족시키기 위하여 군 내외 문헌과 인터넷 공개자료로부터 획득체계와 딥러닝 기술에 대한 자료를 수집하고 분석한다. 또한 딥러닝 기술에 대한 실체를 명확히 이해하고 용용하는데 도움이 되도록 데이터를 활용하여 실제 인공신경망을 학습시켜보는 실습을 포함한다. 이를 바탕으로 전력업무를 담당하거나 관심이 있는 이들에게 획득체계를 이해하고, 딥러닝 기술을 활용할 수 있는 상태에서 획득체계를 지원할 수 있는 방법을 고민해 볼 수 있도록 하는 논의의 장을 제공할 수 있다.

제2장 무기체계 개발을 위한 국방획득체계

2.1 국방획득체계의 역사와 현재

2.1.1 국방획득의 역사

국방획득업무는 1945년 일본의 억압기에서 해방된 이후 미국의 군사원조에 의존하는 환경에서 1969년 닉슨독트린 발표, 1971년 주한 미 7사단 철수 등 안보환경의 변화에 따라 자주 국방력 확보의 필요성이 커지게 되면서 시작하게 된다. 이에 따라 1970년대를 시작으로 율곡사업(1974~1981), 전력증강사업(1982~1986), 전력정비사업(1987~1995), 방위력개선사업(1996~1999), 전력투자사업(2000~2005), 방위사업(2006~현재) 등 다양한 이름으로 군사력을 건설하기 위한 사업들이 진행되었으며, 이와 함께 국방획득체계가 갖추어지고 발전하게 된다. 크게 기간으로 구분해보면 1970년대는 모방개발과 기본병기 국산화에 중점을 둔 태동과 기반조성기였고, 1980년대는 정밀무기 개발의 도전과 방위산업의 안정화를 꾀하였으나 국내외적 상황으로 인한 정체기였으며, 1990년대는 정밀무기의 완성과 방위산업의 내실화로 재도약의 시기였고, 2000년대는 첨단무기 중심의 방위산업 신경제 성장을 추구한 경쟁과 도약의 시기였다. 획득이라는 용어는 1985년에 제정된 '무기체계 획득관리 업무절차(국방부훈령 245호)'에서 공식적으로 사용되었다.

구 분	1970년대	1980년대	1990년대	2000년대
서우덕	태동과 기반조성기	시련과 도전의 시기	안정과 성장의 시기	경쟁과 도약의 시기
최성빈 외	모방개발 및 기본병기 국산화	정밀무기의 도전과 방위산업 안정화	정밀무기의 완성과 방위산업 내실화	첨단무기 중심의 방위산업 신경제성장 동력화
정진태	기반조성기	정체기	재도약기	고도정밀 방위산업육성 및 신성장동력기
한용섭	기반조성기	정체기	발전기	혁신기

〈그림 2-1〉 방위산업 발전의 구분과 무기체계 발전[5)]

1970년 박정희 대통령이 자주국방의 의지를 실현하기 위한 방위산업 육성과 국방과학기술의 연구를 강조하면서 국방획득을 위한 근간이 마련되기 시작한다. 1970년 8월 국방과학연구소가 창설되었고, 번개사업을 통해 기본병기, 통신장비, 개인장구류 등의 품목 생산이 가능하게 되었다. 1973년에는 방위산업의 특수성을

5) 서용원, 김민욱. "한국 방위산업 2020년을 전환기로: 성장 위해 숨 가쁘게 달려온 50년, 미래 50년을 위해 준비할 것은?(1)" 국방과 기술 493, 2020.

고려하기 위해 '군수조달에 관한 특별조치법'이 제정되었고, 방산물자지정제도가 군수특조법에 명시된다. 1974년에는 방위성금과 방위세의 신설로 방위사업의 재원을 마련하여 1974년부터 1981년까지 1차 율곡사업(전력증강 8개년 계획)이 착수된다. 또한 1960년대에 미국의 맥나마라 국방장관이 도입한 기획예산제도(PPBS: Planning, Programming, Budgeting)를 1979년에 도입하여 최초로 국방기획관리제도(훈령 253호)로 정립하였다. 이후 1983년에는 집행 및 평가단계를 추가하여 PPBEES(Planning, Programming, Budgeting, Execution and Evaluation System)를 정립하였다.

1980년대에는 국내외 정치, 안보상황의 변화로 자주국방에 대한 절박성이 약화되었고, 민간 주도의 방위산업에 중점을 두게 된다. 1982년부터 1986년까지 2차 율곡사업이 추진되었고, 선진국의 무기를 개량하여 개발하려는 노력을 기울였다. 국외도입이 증가하는 상황에서 국내산업의 피해를 방지하고자 1982년에는 절충교역제도(military offset)가 시행되었으며, 1983년에는 전문화, 계열화 제도가 규정(2008년 폐지)되었다. 1983년 12월에는 이전 군수특조법이 '방위산업에 관한 특별조치법'으로 명칭을 변경하면서, 변화되는 제도들을 담았다.

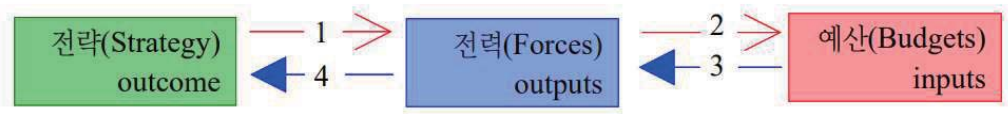
1987년부터 1995년까지 3차 율곡사업이 추진되었으며, 냉전체제의 해체에 따른 안보환경의 변화, 불확실한 위협의 증대, 정밀유도무기의 발전 등의 영향을 받게 된다. 문민정부가 들어서면서 1993년 감사원에 의한 율곡감사가 이루어지고, 그동안 총액만 국회에 제출하던 전력증강사업 예산도 1994년부터는 세부과목에 대한 예산 및 결산 심사를 받게 된다. 이후 1996년부터 전력정비사업이 방위력개선사업으로 명칭을 변경한다. 1990년대 후반부터는 제한적이지만 방산 수출을 통한 시장 확대로 눈을 돌리고 새로운 시장을 개척하는 활동을 시작한다.

2004년에는 '국방획득제도개선위원회'가 획득사업의 비리를 차단하면서도 전문성을 높이기 위해 구성되었으며, 획득전담기관의 신설을 결정한다. 2006년 국방부, 합참, 각 군, 조달본부 등의 기관에 분산되어 있던 획득업무를 통폐합하여 방위사업청이 창설되었고, 동시에 방위사업법이 시행되었다. 방위사업청은 국방부의 외청이며, 산하 출연기관으로 국방과학연구소와 국방기술품질연구원을 두었다. 2006년에는 또한 '국방개혁에 관한 법률'을 제정하여 국방개혁을 일관성있게 추진하도록 하였으며, 2007년에는 국방부가 '국방과학기술진흥정책서'를 발간하여 국방과학기술에 대한 가이드라인과 비전을 제시하기 시작하였다. 2020년에는 '방위

산업 발전 및 지원에 관한 법률'이 제정되면서 방위산업의 특성을 고려한 제도발전을 추진하고 있다.

2.1.2 국방기획관리체계

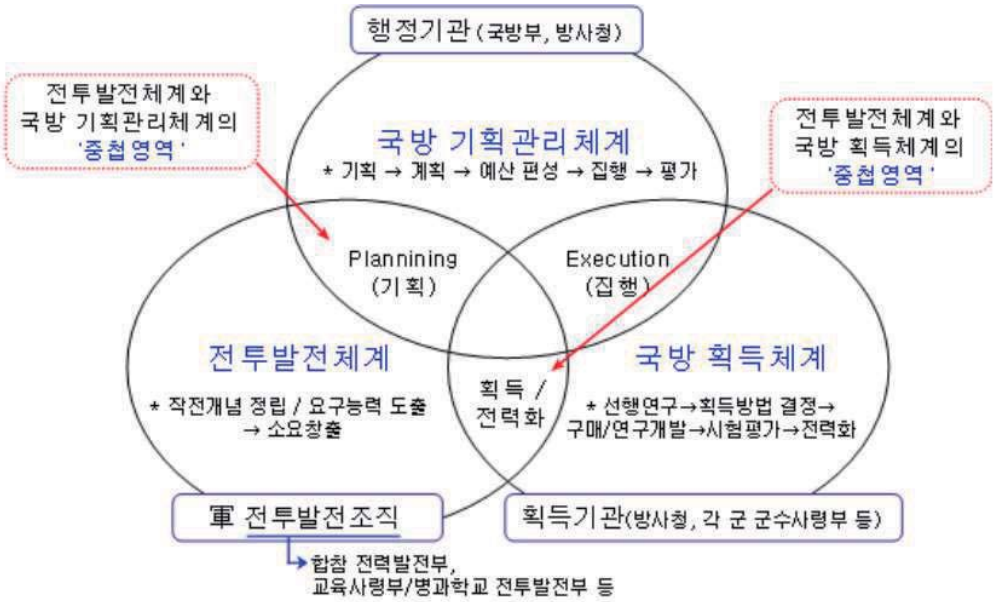
국방의 기본적인 임무인 평시 전쟁의 억제와 전시 전쟁의 승리를 달성하기 위해서는 어떻게 싸울것인가에 대한 전략과 그 전략을 이행할 전력, 그리고 전력을 획득할 재원인 예산의 관계가 매우 중요하다. 과거 대부분의 국가들이 전략과 전력 사이에서 각 군의 경쟁과 중복투자로 인한 비효율성을 겪어왔다. 국방기획관리체계(국방기획관리기본훈령, 국방부훈령 2513호)는 이러한 불균형을 중장기적으로 기획하여 해결하기 위한 제도로서 현재 무기체계 개발을 위한 국방획득체계를 제공한다.



〈그림 2-2〉 전략, 전력, 예산의 관계[6)]

국방기획관리체계는 넓은 의미의 획득에 해당하는 군사력 건설 시스템의 측면에서 보면, 획득기관들에 의한 획득사업이 관리되는 국방 획득체계, 작전개념과 요구능력으로부터 소요를 결정하는 전투발전체계와 함께 전체적인 군사력 건설 시스템을 이루고 있다.

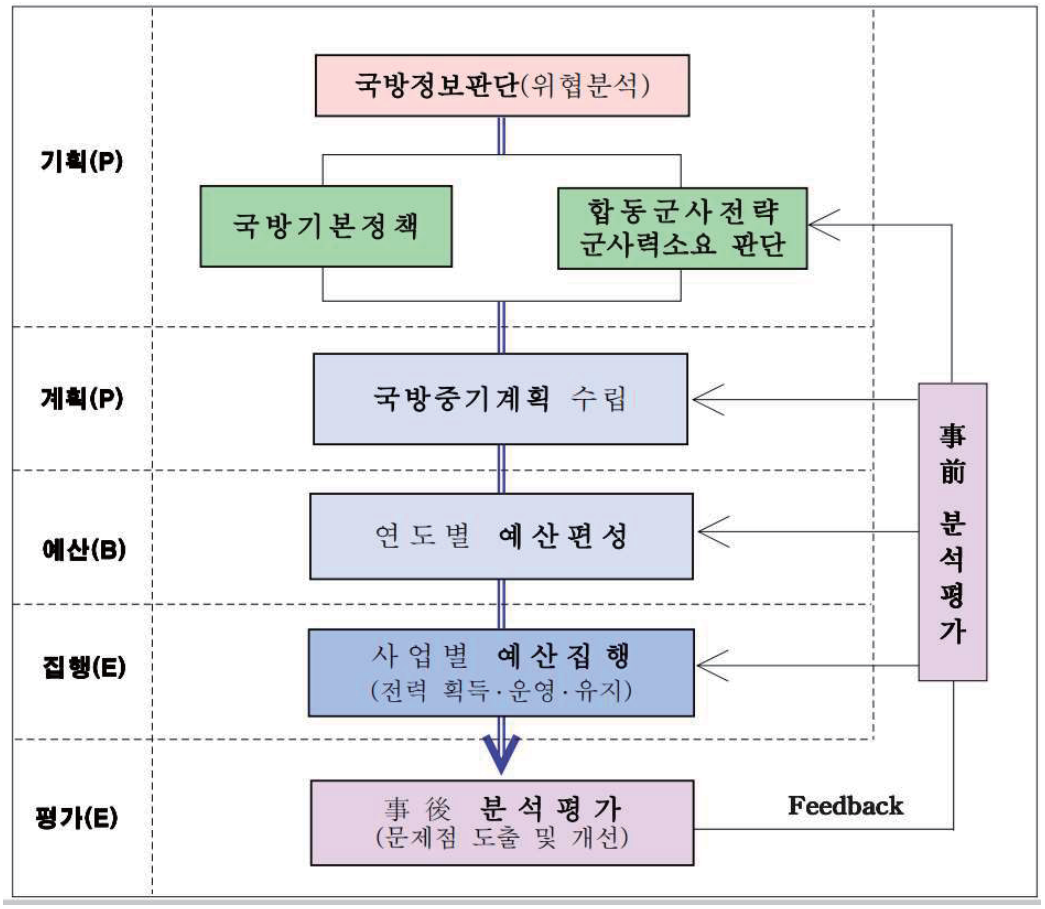
6) 전제국. "국방기획체계의 발전 방향: 문서별 적실성과 연계성을 중심으로" 국방정책연구 32(2), 2016.



〈그림 2-3〉 군사력 건설 시스템[7)]

국방기획관리체계는 위협을 분석하고, 국방정책, 군사전략을 바탕으로 소요기획체계에 따라 중장기 소요를 결정하는 기획단계, 가용한 재원을 고려하여 가까운 미래의 사업을 구체화하는 계획단계, 연도별 예산을 편성하는 예산단계, 예산을 집행하여 전력을 구매하거나 연구개발하는 집행단계, 이러한 단계들을 사전 및 사후에 분석지원하는 평가단계로 이루어진다.

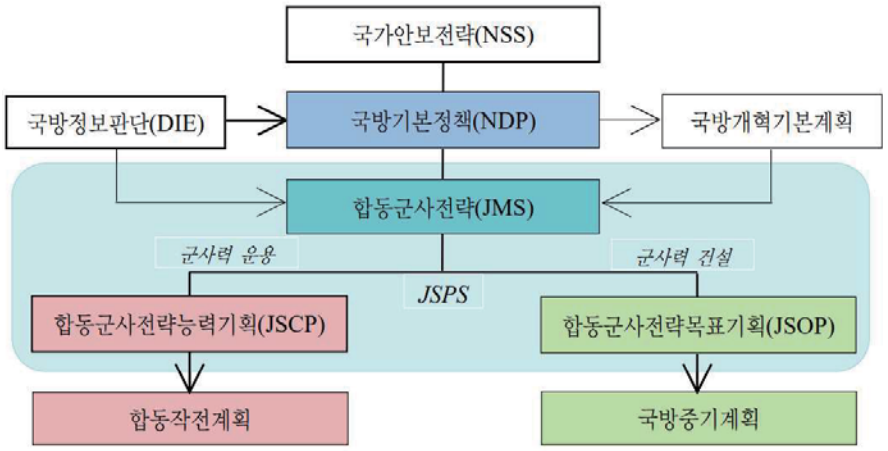
7) 서상국, 장세훈, 김용삼. "제4차 산업혁명기 한국군의 군사력 건설 시스템 혁신 방향: 소요창출을 위한 전투발전체계 혁신을 중심으로" 국방정책연구 33(1), 2017.



〈그림 2-4〉 국방기획관리체계[8)]

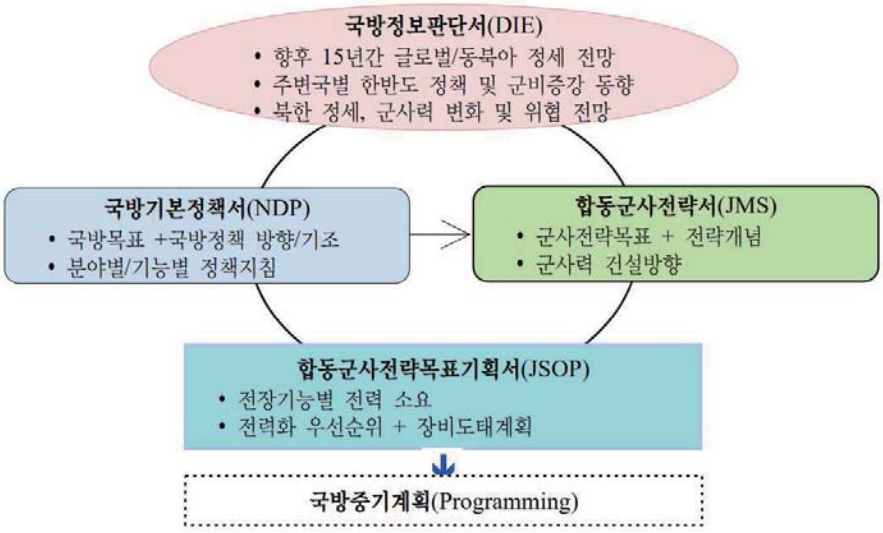
국방기획관리체계에서 기획체계는 합동전략기획체계(Joint Strategic Planning System)로 본다면 합동군사전략서(JMS: Joint Military Strategy)로부터 군사력 운용과 관련해서는 합동군사전략능력기획서(JSCP: Joint Strategy Capability Plan)에서 합동작전계획으로 이어지고, 군사력 건설과 관련해서는 합동군사전략목표기획서(JSOP: Joint Strategy Objective Plan)에서 국방중기계획으로 이어지는 두 축을 생각해 볼 수 있다.

8) 전제국. "국방기획관리제도의 이상과 현실: 제도 개선 방안을 중심으로" 국방연구 56(4), 2013.



〈그림 2-5〉 기획체계 구도[9)]

합동군사전략목표기획서로 이어지는 축을 중심으로 보면, 미래 위협과 정세분석을 바탕으로 국방정책과 군사전략을 수립하고 군사력 소요를 판단하여 국방중기계획을 작성하는 자료를 제공한다.



〈그림 2-6〉 군사력 건설의 위한 체계[10)]

9) 전제국. "국방기획체계의 발전 방향: 문서별 적실성과 연계성을 중심으로" 국방정책연구 32(2), 2016.
10) 전제국. "국방기획체계의 발전 방향: 문서별 적실성과 연계성을 중심으로" 국방정책연구 32(2), 2016.

국방획득의 기획을 위한 문서들은 다음과 같이 기존 10종의 문서에서 국방기획지침이 추가되면서 총 7종으로 통폐합되었다. 으며, 주관부서, 작성 시기 및 주기, 대상기간을 확인할 수 있다.

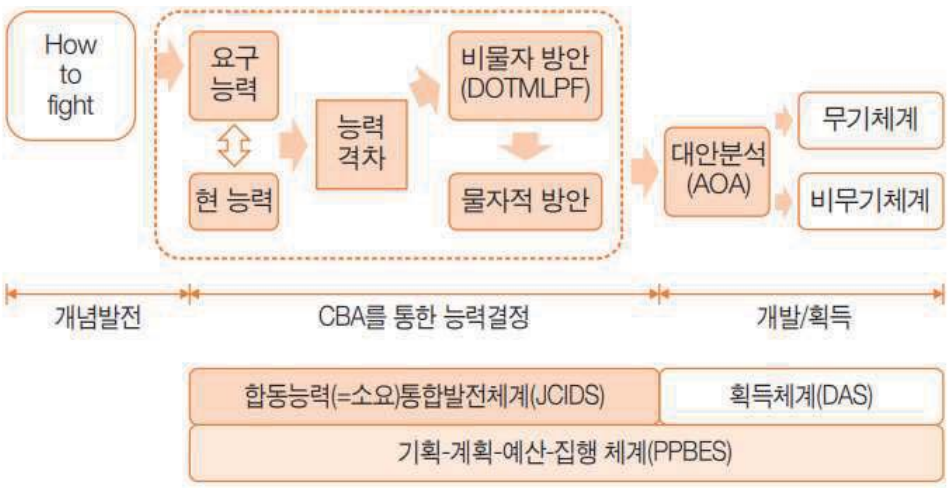
〈표 2-1〉 기획문서 종류[11)]

문서명	주관부서	작성 시기	작성 주기	대상기간
국방정보판단서	국방정보본부	2월	5년	F+1~15년
국방기본정책서	국방부(정책기획관실)	10월	5년	F+1~15년
국방개혁기본계획	국방부(국방개혁실)		2~3년	F+1~15년
합동군사전략서	합참(전략기획본부)	11월	5년	F+1~15년
국방기획지침	국방부(정책기획관실)	2월	매년	F+1~15년
합동군사전략목표기획서	합참(전략기획본부)	12월	매년	F+1~15년
합동군사전략능력기획서	합참(전략기획본부)	12월	매년	F+1~15년

2.2 국방획득체계의 발전 동향

국방획득체계의 발전 동향으로 먼저 2003년 미국에서 기존 소요생성체계(RGS: Requirements Generation System)를 대체하여 합동능력통합발전체계(JCIDS: Jonit Capabilities Integration & Development System)로 전환하였고, 우리 군도 이를 받아들여 능력(capability) 기반의 체계로 전환해나가고 있다는 점이 있다.

11) 국방부 훈령 2513호. "국방기획관리기본훈령"



〈그림 2-7〉 미국 국방기획관리체계 및 소요기획 개념[12)]

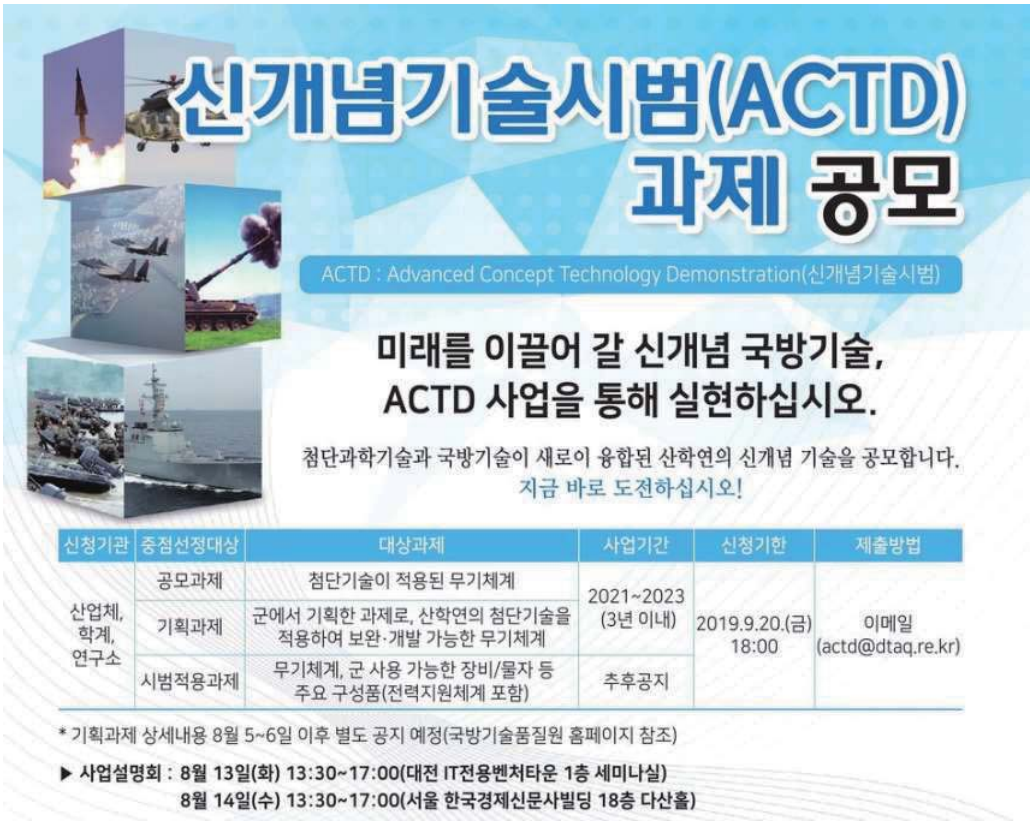
능력기반의 소요기획체계에서는 미래 작전개념을 구현하는데 필요한 능력을 기술하고, 현 능력과 요구되는 능력의 능력격차(capability gap)를 소요(requirement)로 기획하여, 전투발전요소(DOTMLPF: 교리(Doctrine), 구조 및 편성(Organization), 교육훈련(Training), 무기·장비·물자(Materiel), 간부개발(Leadership), 인적자원(Personnel), 시설(Facility))에 해당하는 비물자 방안(non-materiel solutions)과 물자적 방안(materiel solutions)을 모두 판단하도록 되어 있다.

JCIDS를 적용하기 위해서는 첨단 과학기술의 발전과 미래전에 대한 통찰을 바탕으로 합동 능력에 대한 체계적인 기획과 그 지침의 공유가 중요한데, 이러한 것들은 준비 없이 쉽게 이루어질 수 없다. 또한 대안분석의 절차도 필요한 무기체계를 창의적으로 개발하는데 필수적인 절차이나, 아직까지 우리의 실정에 맞게 어떻게 실행할지에 대한 논의가 부족한 것으로 보인다.

다음으로 미국의 신개념기술시범사업(ACTD: Advanced Concept Technology Demonstration) 제도를 2006년부터 우리 군도 도입하여 2008년부터 과제화하여 적용하고 있다는 점이다. ACTD제도는 무기체계 획득의 기간이 장기간 소요되고, 민간의 성숙된 기술을 적시에 도입하기 어렵다는 점을 개선하기 위해, 실용성 평

12) 안영수, 윤자영, 이재욱, 김윤태. "방위산업 발전과 선진강군을 위한 국방 전력소요기획체계 발전방향" 산업연구원, 2013.

가를 통해 3년 이내의 단기간에 우수한 기술개발 성과를 필요한 전력에 적용하겠다는 것이다.[13] ACTD제도를 통해 군에 전력화한 사례가 있어 전력발전에 기여하는 면도 있으나, 지속적인 제도 개선에도 불구하고 착수전 취소되거나 개발과정에서 실패하는 과제가 많아지고, 이에 따라 과제 지원수도 줄어들며, 궁극적으로 신속히 전력화하겠다는 목표가 희석되고 있는 실정이다.

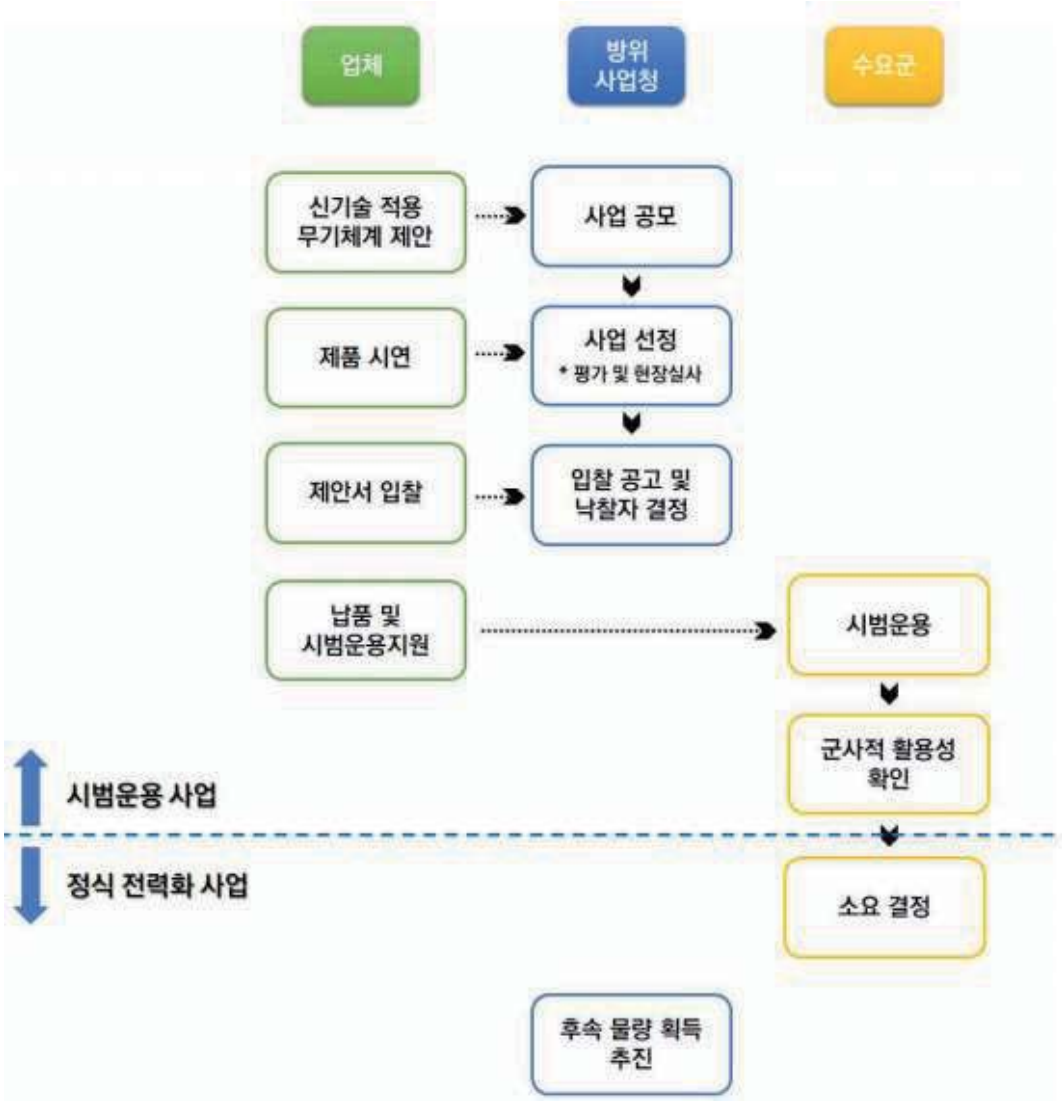


〈그림 2-8〉 ACTD 과제 공모 모습[14]

또한 4차 산업혁명 기반기술을 신속하게 적용하기 위하여 2020년부터 신속시범획득 사업이 시작되었다. 신속시범획득 사업 소개자료를 보면 4차 산업혁명 분야

13) 고관옥, 조수연. "신개념기술시범사업(ACTD) 이해 및 발전방향" 국방과 기술 456, 2017.
14) http://www.defensetoday.kr/news/articleView.html?idxno=113

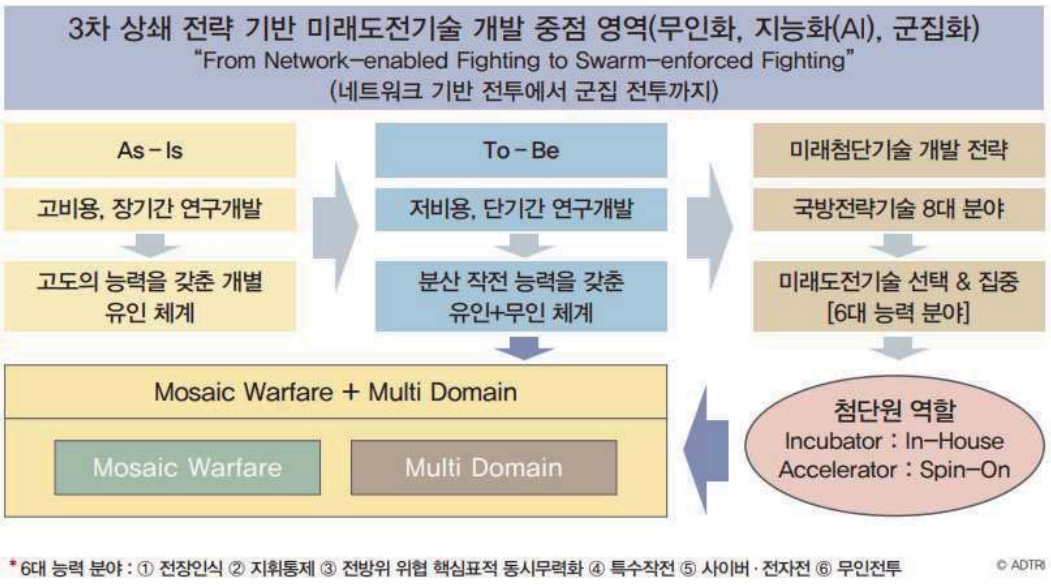
등 기술발전 속도가 빠른 분야는 업체 제안을 통해 이미 개발되어 있는 시제품을 소량 구매하여 그대로 군에서 시범운용하여 군사적 활용성을 확인하고, 이를 실적으로 국내외 시장 개척이 가능하도록 하는 개념으로 되어있다.



〈그림 2-9〉 신속시범획득 사업 절차[15)]

15) 신속시범획득 사업 소개자료, www.kbiz.or.kr

마지막으로 국방개혁 2.0 정책의 일환으로 와해적 신기술에 해당하는 4차 산업혁명 기반의 국방연구개발 혁신을 촉진하는 '국방과학기술혁신 촉진법'이 2020년에 제정되면서, '미래도전국방기술'을 기획하기 위한 전략을 국과연의 국방첨단기술연구원이 수립하고 추진하기 시작하였다.[16] 혁신적이고 도전적인 국방과학기술을 어떻게 기획하고 개발할지 관심이 모아지고 있다.



〈그림 2-10〉 미래도전국방기술 연구개발 전략[17]

16) 박병진. "미래 국방을 위한 우리의 준비, 미래도전국방 기술 연구개발" 국방과 기술 501, 2020.
17) 박병진. "미래 국방을 위한 우리의 준비, 미래도전국방 기술 연구개발" 국방과 기술 501, 2020.

제3장 딥러닝 기술의 이해와 실제

3.1 딥러닝 기술의 역사 및 동향 소개

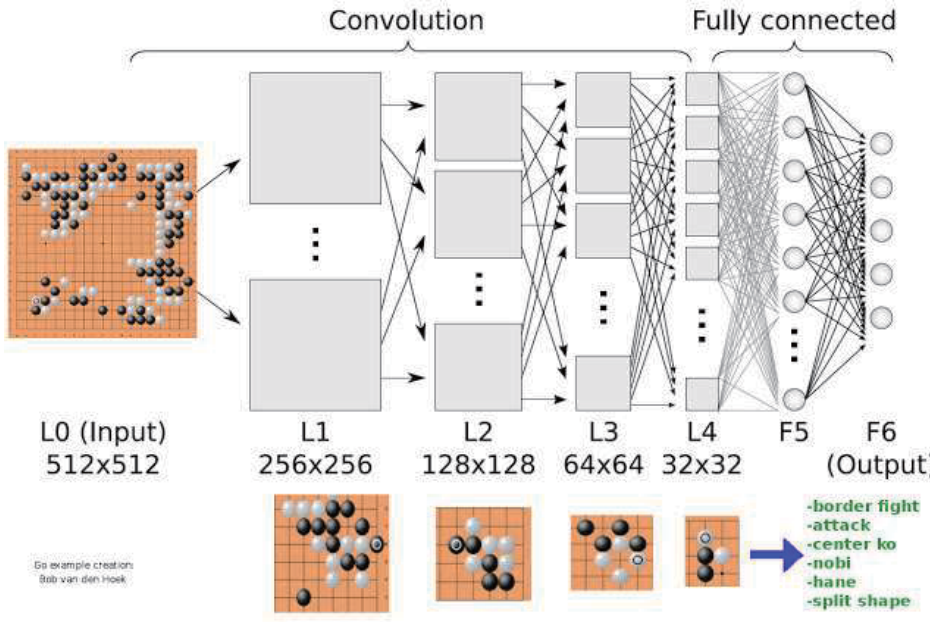
딥러닝 기술은 인공지능(AI: Artificial Intelligence)의 역사 속에서 이해해볼 수 있다. 인공지능은 인간의 지능을 인공적으로 만들어 내는 것으로 인간의 지각, 추론, 학습, 언어 능력 등 지적 활동을 컴퓨터나 기계가 모방하도록 하는 과학이다. 인공지능은 인간이란 다른 존재와 무엇이 다른가, 지능이란 무엇인가라는 철학적 문제에서 시작하였으며, 이는 컴퓨터의 출현과 더불어 기계가 인간과 같은 지능을 가질 수 있는가로 확장된다.

앨런 튜링(Alan Turing)은 1950년 튜링 모방 게임을 제시하여 지지부진한 논증을 피하고 기계가 인간과 같은 수준의 지능을 가진다는 것이 어떤 것인지에 대한 표준적인 시각을 제공하였다. 존 맥카시(John McCarthy)는 1956년 다트머스 대학에서 워크샵을 조직함으로써 인공지능이라는 새로운 분야가 탄생하는 계기를 만들었으며 이때 모인 연구자들은 향후 인공지능 연구를 주도하게 된다. 이후 1958년 인공신경망(ANN: Artificial Neural Network) 모형의 시작인 퍼셉트론(perceptron) 혹은 단층신경망을 중심으로, 1965년 퍼지집합이론(fuzzy set theory), 1970년 초 진화 연산(evolutionary computation)의 기초가 되는 유전알고리즘(genetic algorithm)까지 인공지능의 부흥이 시작되지만, 퍼셉트론의 제한점과 이를 실용화하는데 실패하며 첫 부흥기가 막을 내리게 된다.

이후 지능형 기계를 만들기 위해 해결해야 할 문제의 영역을 매우 제한하면서 전문가시스템(expert system)이 실용적 관점에서 관심을 받게 되나, 비용 및 확장 제한성 등의 제한사항으로 일부 분야에만 활용되는 한계에 부딪혔다. 1980년대 중반에 인공신경망에 대한 연구가 부활하게 되는데, 폴 워보스(Paul Werbos)에 의해 제안되고 제프리 힌튼(Geoffrey Hinton)에 의해 실제 적용된 오차역전파(error backpropagation) 알고리즘 혹은 후진 방식 자동 미분 기법에 의한 다층구조 퍼셉트론(MLP: Multi-Layer Perceptron)이 퍼셉트론의 단점을 보완할 수 있게 되었으며, 컴퓨터 기술의 발전으로 대규모 연산을 신속히 처리할 수 있게 되었기 때문이다.

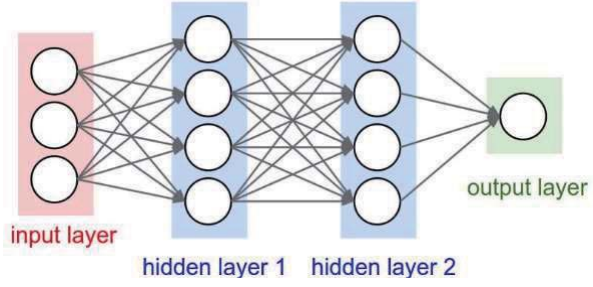
1980년대의 부흥기는 1990년대에 이르며 신경망이 복잡한 구조를 가질수록 과잉학습의 문제가 심각해지고 오차역전파 알고리즘 또한 제대로 작동하지 않는다는 문제가 발생하면서 다시금 암흑기를 맞이하게 된다. 2000년대에는 인공신경망 대신 다른 기계학습(machine learning) 방법들(결정나무(Decision Tree), 베이지안 망(Bayesian Networks), 서포트 벡터 머신(Support Vector Machine), 가우시안 프로세스(Gaussian process) 등)이 활발히 연구된다. 다시 찾아온 암흑기 속에서 제프리 힌튼은 2006년 데이터의 전처리 과정을 통해서 과잉학습과 오차역전파 문제를 해결할 수 있다고 밝힘으로써 현재와 같은 딥러닝(Deep Learning)의 큰 관심을 불러왔다. 딥러닝을 활용한 모델들이 각종 경쟁적 대회에서 우수한 성적을 거두면서 학계에서 큰 주목을 받기 시작한다.

그 후 급속도로 발전하기 시작한 딥러닝 기술은 2016년 바둑으로 대중의 큰 관심을 받게된다. 구글 딥마인드(DeepMind)가 개발한 인공지능 바둑 프로그램인 알파고(AlphaGo)와 이세돌 9단의 대결은 기계가 인간을 압도하였다는 표면적인 요인 말고도, 단 1년 만에 인간을 뛰어넘는 경이로운 학습속도와 인공지능 분야에서 난제로 인식되던 일반문제해결기(general problem solver)에 근접한 모습을 보여주었다. 특히, 알파고는 업데이트와 새로운 버전으로 불확실성과 자유도가 훨씬 큰 게임에서도 인간 전문가를 뛰어넘는 결과를 보여주었으며, IBM의 인공지능 왓슨(Watson)처럼 의료 및 헬스케어 분야에도 진출을 하고 있다.



〈그림 3-1〉 알파고와 딥러닝 엔진[18)]

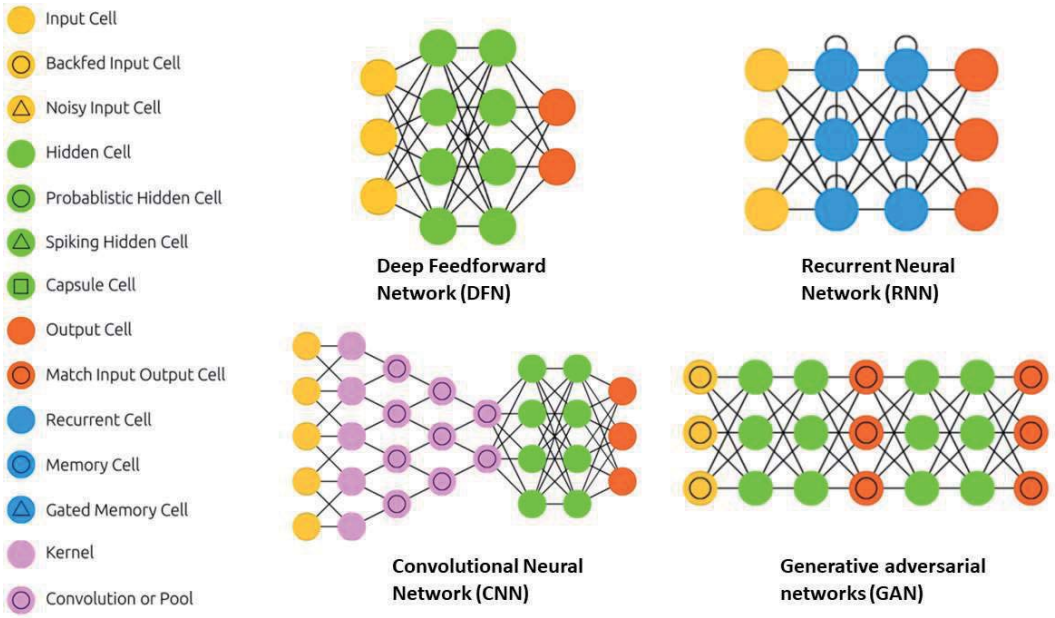
인공지능 기술의 근간이 되는 인공신경망의 기본 구조는 아래와 같으며, 딥러닝은 보통 2개 이상의 hidden layer를 가지는 다층신경망을 의미한다.



〈그림 3-2〉 인공신경망의 기본 구조[19)]

18) http://deeplearningskysthelimit.blogspot.com/2016/04/part-2-alphago-under-magnifying-glass.html
19) https://www.digitaltrends.com/cool-tech/what-is-an-artificial-neural-network/

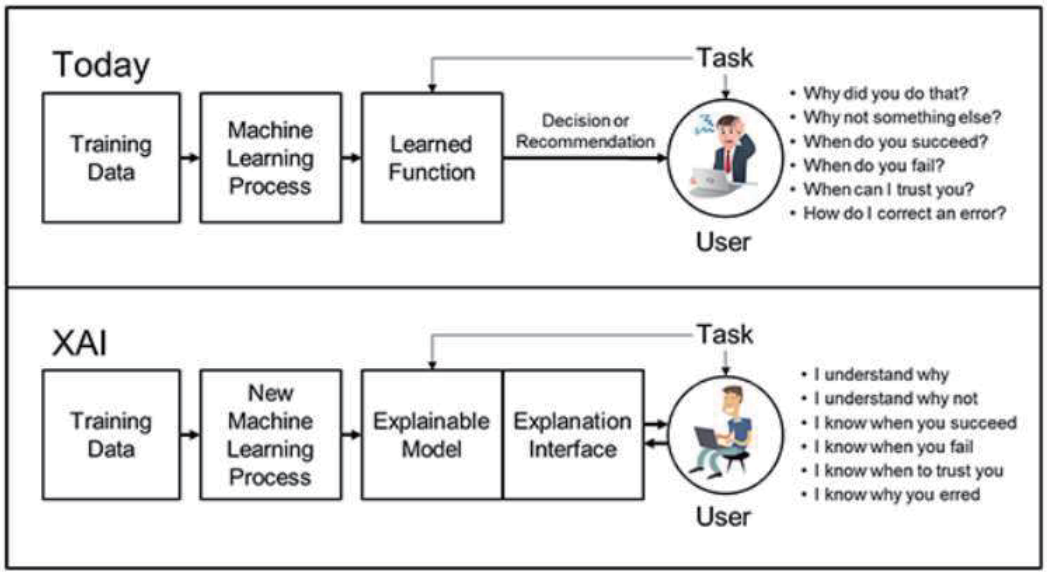
인공신경망은 계속해서 발전하면서 새로운 구조가 만들어지고 있어 전체를 분류를 하기는 어렵지만 대표적인 구조들은 다음과 같다. DFN(Deep Feedforward Network)은 딥러닝의 가장 기본이 되는 인공신경망이고, RNN(Recurrent Neural Network)은 입력 정보를 저장하여 전파할 수 있어서 순차적 정보를 다루어야 하는 문제(시계열 데이터나 문자열 예측)에 사용될 수 있다. CNN(Convolutional Neural Network)은 합성곱(convolution) 연산을 통해 패턴을 추출하여 학습할 수 있어 이미지 처리 분야에서 대표적으로 알려진 인공신경망으로 학습 및 예측이 빠른 장점이 있다. 2016년 알파고도 CNN 기반의 구조를 사용하였다. GAN(Generative adversarial networks)은 두 개의 인공신경망을 경쟁시켜 학습을 진행하며, 특히 새로운 이미지를 생성할 수 있는 능력으로 잘 알려져 있다.



〈그림 3-3〉 인공신경망의 종류[20]

20) https://www.asimovinstitute.org/neural-network-zoo/

특히 국방 분야에서는 설명가능한 인공지능(XAI: eXplainable AI)에 대해 적극적으로 연구가 이루어지고 있다. 딥러닝과 같이 데이터 적합 시 성능이 매우 뛰어난 반면 그 내부에서 어떤 일이 벌어지고 있는지 설명력이 떨어지는 모델을 블랙박스 모델(Black Box Model)이라고 부르며, XAI는 블랙박스 모델의 내부를 인간이 들여다볼 수 있도록 만들어주는 개념이다. XAI는 미국의 방위고등연구계획국인 DARPA의 프로젝트로도 널리 알려져 있다.



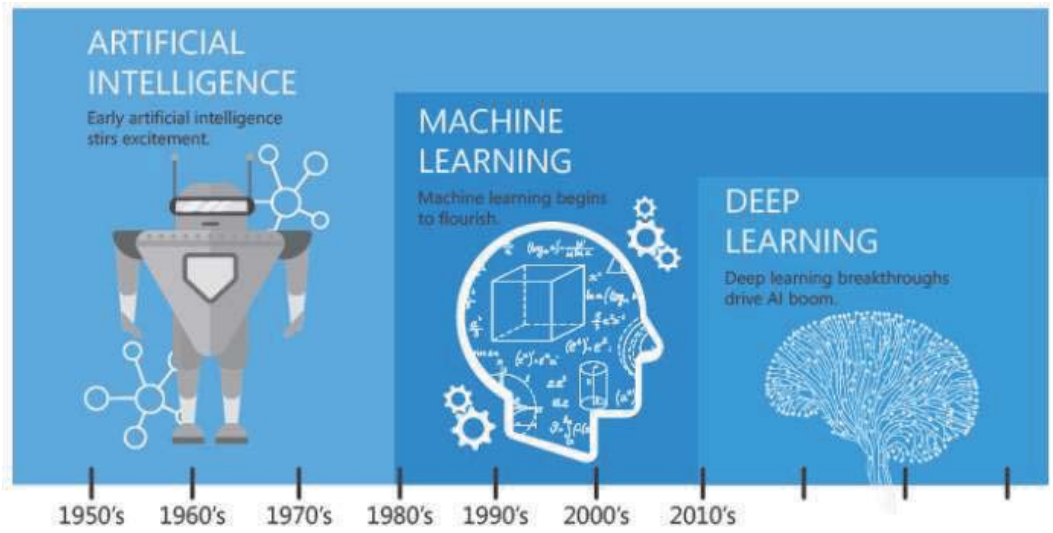
〈그림 3-4〉 설명가능한 인공지능 개념도[21]

3.2 데이터를 바탕으로 딥러닝 기술 적용

인공지능, 머신러닝, 딥러닝을 단어의 범위로 나타내어보면 아래와 같다. 인공지능의 범위 아래 머신러닝은 컴퓨터 공학의 주요 연구 분야 가운데 하나로 데이터를 이용해서 컴퓨터가 어떠한 지식이나 패턴을 학습하는 것이고, 그 중 딥러닝은 인공신경망(Artificial Neural Networks)을 여러 층 쌓아 올려 학습하는 것을 의

21) https://www.darpa.mil/

미한다. 머신러닝 알고리즘의 학습 방법은 크게 지도학습(supervised learning), 비지도학습(unsupervised learning), 강화학습(reinforcement learning)으로 분류할 수 있다. 지도학습은 컴퓨터에 정답을 제공하고 학습을 시키는 방식이고, 이때 학습하고자 하는 값이 이산 값이면 분류(classification) 문제에 해당하고, 연속값이면 회귀(regression) 문제에 해당한다. 비지도학습은 정답 레이블 없이 입력데이터만으로 학습하는 것으로, 비슷한 특성을 가지는 데이터들끼리의 군집(clustering)이 예가 될 수 있다. 강화학습은 학습의 대상이 어떤 행동을 취하면, 그 행동의 좋고 나쁜 정도를 학습 알고리즘에게 알려주어 그 정보를 컴퓨터가 이용하는 것을 의미한다.

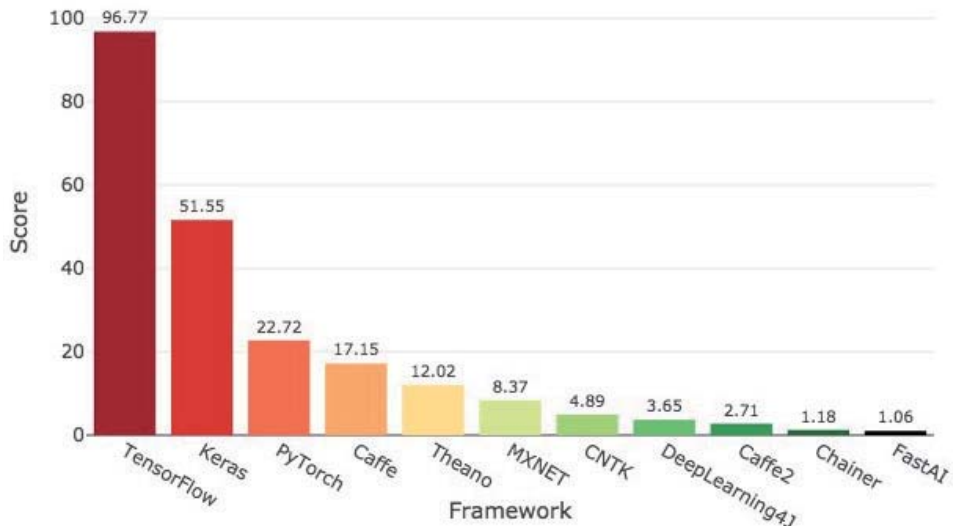


〈그림 3-5〉 인공지능, 머신러닝, 딥러닝[22]

다음으로 딥러닝을 실제 구현하기 위한 환경을 설명한다. 텐서플로는 구글에서 개발한 라이브러리(library)로 머신러닝/딥러닝을 쉽게 구현할 수 있도록 다양한 기능을 제공해 준다. 딥러닝 라이브러리는 텐서플로 외에도 파이토치, CNTK 등이

22) https://medium.com/@alanb_73111/artificial-intelligence-vs-machine-learning-vs-deep-learning-ai-vs-ml-vs-dl-e6afb7177436

존재하지만 텐서플로가 현재 가장 인기 있는 라이브러리의 위치를 차지하고 있다. 한편, 딥러닝 라이브러리 외에도 이를 한 단계 더 추상화한 라이브러리가 존재하는데, 이러한 라이브러리들은 보다 간결하고 직관적으로 코드를 이해할 수 있게 해준다. 추상화 라이브러리에는 케라스, 패스트AI, TF-Slim, Sonnet 등이 있고, 아래와 같이 프랑수아 숄레가 만든 케라스가 가장 인기있는 추상화 라이브러리이다.



〈그림 3-6〉 2018년 딥러닝 라이브러리 순위[23)]

앞서 케라스는 한 단계 더 추상화된 라이브러리라고 언급한 것처럼 케라스에서는 미분과 같은 저수준의 연산은 여러 가지 백엔드 엔진(backend engine)에서 수행하고, 이 백엔드 엔진은 케라스와 매끄럽게 연동되게 된다. 케라스의 백엔드 엔진으로 사용되는 것이 텐서플로, 씨아노, CNTK이며, 그중 텐서플로가 가장 널리 사용되는 것이다. 케라스와 텐서플로의 이 같은 관계는 텐서플로가 2019년 9월 텐서플로 2.0 정식 버전을 출시하면서 더욱 깊어졌다. 텐서플로는 2.0 버전부터 사용자의 친화성을 위해 텐서플로에 내장된 고수준 API(Application Programming

23) J. Hale, "Deep Learning Framework Power Scores 2018," September 20, 2018, https://towardsdatascience.com/deep-learning-framework-power-scores-2018-23607ddf297a (accessed Apr.12, 2020.)

Interface)로 케라스를 tf.keras란 이름으로 고정적으로 사용하기 시작했으며[24], 케라스 홈페이지에서는 유지보수와 텐서플로와의 통합성을 이유로 기존 여러 가지 백엔드 엔진을 사용하던 케라스 보다는 tf.keras 사용을 권장하고 있기도 하다[25].

텐서플로를 설치하기 위해서는 파이썬을 먼저 설치하여야 한다. 파이썬은 공식홈페이지에서 다운받을 수 있다. 파이썬을 설치한 후 텐서플로를 설치하기 위해 윈도우의 명령 프롬프트에서 다음과 같은 명령어를 실시한다.

```
C:₩Users₩user>pip install tensorflow
```

설치 후 명령 프롬프트에서 아래와 같이 파이썬 인터프리터를 실행시킨다.

```
C:₩Users₩user>python
```

아래와 같이 파이썬 코드를 입력해 'hello,TensorFlow!' 가 출력된다면 텐서플로 설치에 성공한 것이다.

```
>>> import tensorflow as tf
>>> hello=tf.constant('hello.TensorFlow!')
>>> sess=tf.Session()
>>> print(sess.run(hello))
b'hello.TensorFlow!'
>>>
```

케라스 설치가 정상적으로 완료된 것을 확인하기 위해 파이썬 인터프리터를 실행시킨 후 케라스를 import 시킨다.

```
C:₩Users₩user>python
```

```
>>> import keras
```

주피터 노트북은 명령 프롬프트가 아닌 웹 브라우저 상에서 프로그래밍 언어들을 시각적으로 확인할 수 있게 하는 프로그램이다. 주피터 노트북의 설치를 위해서는 명령 프롬프트에서 다음과 같은 명령어를 실시한다.

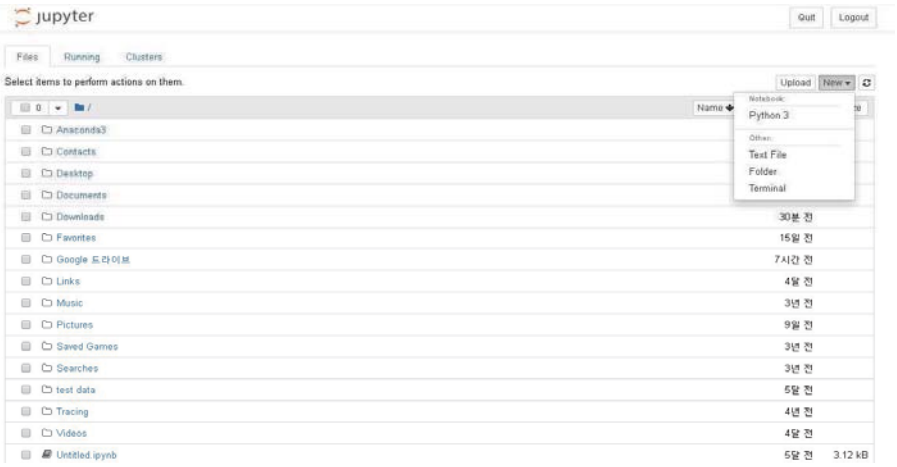
---

24) M. Heller. "떠오르는 심층 신경망 API, 케라스 알아보기," 2.12.2019, http://www.itworld.co.kr/news/116583.
25) Keras, "Multi-backend Keras and tf.keras," https://keras.io/#multi-backend-keras-and-tfkeras.

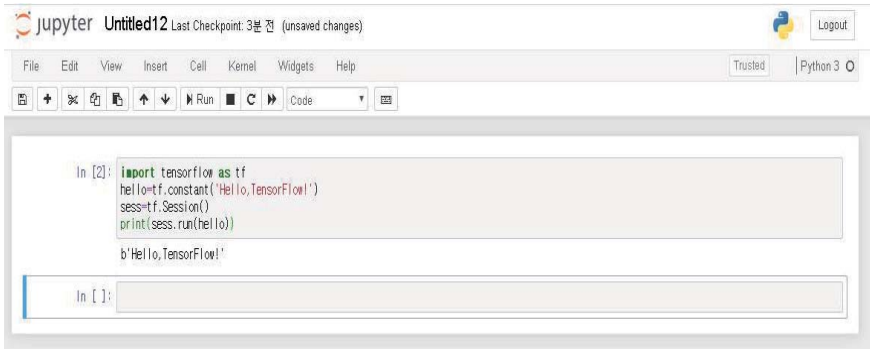
```
C:₩Users₩user>pip install jupyter
```

설치가 완료 후 아래와 같이 jupyter notebook을 입력하면 웹 브라우저가 열리면서 실행되는 것을 확인할 수 있다.

```
C:₩Users₩user>jupyter notebook
```



실행된 창에서 오른쪽 상단의 [NEW] 〉 [Python 3] 메뉴를 선택하면 새로운 창이 열리는 것을 확인할 수 있다. 새로 생성된 프로젝트에 코드들을 입력하고, Shift + Enter키를 누르면 바로 아래에서 실행결과 확인이 가능하다.



이처럼 주피터 노트북은 긴 코드를 짧게 나누어서 실행할 수 있으므로, 작업 중

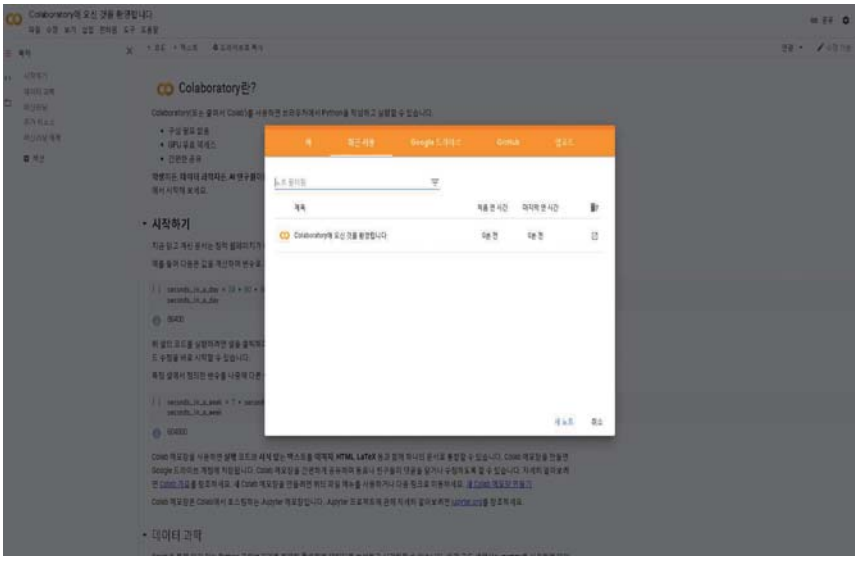
일부 코드가 잘못되었을 때 전체 코드를 다시 실행할 필요 없이 독립된 코드만 재실행하면 되며, 그 실행 결과를 바로 확인할 수 있다.

텐서플로 설치과정은 간단하지만 의외로 많은 사람이 난관에 부딪힌다. 호환성의 문제로 인해 라이브러리가 설치되지 않을 가능성이 있는데, 파이썬 3.8에서는 텐서플로를 지원하지 않아 파이썬을 다운그레이드 시킨 후 텐서플로를 설치해야 하는 문제가 있다. 또한 텐서플로 설치과정을 거친 후 텐서플로를 import 시킬 때 DLL load failed 오류를 접하게 되는 경우도 있다. 이 오류는 AVX Support 오류로 텐서플로 1.6부터는 AVX 지원 데스크탑 및 노트북에서만 설치가 가능하다[26].

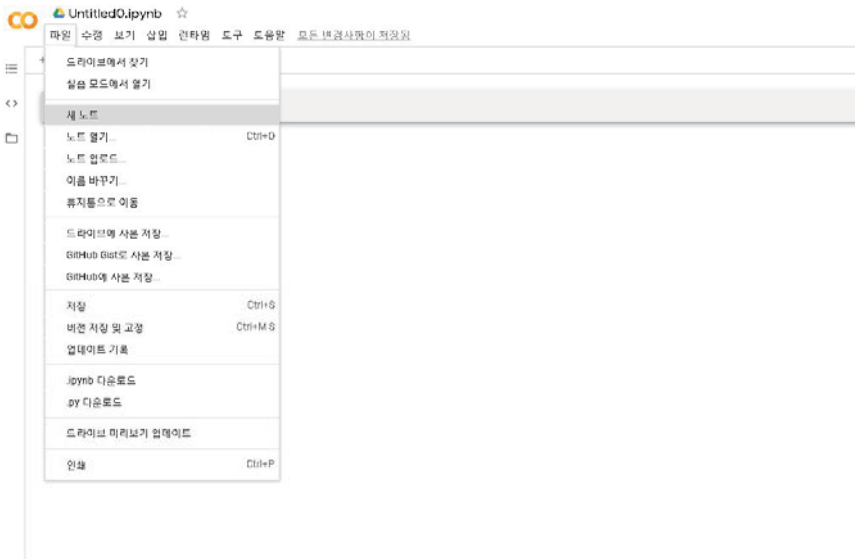
이와 같이 최신 버전의 텐서플로를 설치하지 못하게 되는 경우에는 Google Colaboratory을 사용할 수 있다. Google Colaboratory는 Google에서 제공하는 클라우드 서비스로 gmail 계정을 가지고 있는 사람이라면 누구나 무료로 사용이 가능하다. Google Colaboratory는 파이썬, 텐서플로, 케라스와 같은 딥러닝 라이브러리가 미리 설치되어 있어, 앞서 말한 호환성 문제로 인한 설치의 어려움을 겪지 않아도 되며, 주피터 노트북 환경을 기반으로 하고 있어 시각적으로도 편리하다. 무엇보다도 Google Colaboratory가 가장 널리 사용되는 이유는 GPU를 제한된 시간 내에서 무료로 사용할 수 있다는 점이다. Google Colaboratory는 흔히 Google Colab이라 부르며,

https://colab.research.google.com에 접속한 후에 Gmail 계정으로 로그인하면 아래와 같은 시작페이지가 뜬다.

26) R. Patal, “Install instructions for TensorFlow and Keras using CUDA 9 and cuDNN 7with GPU enabled, on Windows 10,” February 27,2019, https://github.com/rohit-patel/Install_Instructions-Win10-Deeplearning-Keras-Tensorflow



오른쪽 하단의 [새노트] 선택하거나 혹은 취소를 선택하더라도 왼쪽 상단의 [파일] 〉 [새노트] 메뉴를 선택하여 주피터 노트북을 실행할 수 있다.



GPU 사용을 위해서는 왼쪽 상단의 [런타임] 〉 [런타임 유형 변경] 메뉴 선택을 통해 아래와 같이 하드웨어 가속기를 GPU로 변경하는 것이 가능하다.

학습을 위한 파일을 Colab에서 읽기 위해서는 Google Drive를 활용하는 방법이 유용하게 사용될 수 있다. 이를 위해서는 Google Drive를 Colab에 연동시켜야 하는데, 다음 코드를 입력하면 URL 링크가 제시되고,

URL 링크로 연결하면, 문자열로 구성된 비밀키를 알려주고, 그 비밀키를 코드란에 붙여넣으면 Drive가 Colab에 성공적으로 연동된다.

다음으로 텐서플로의 동작과정을 살펴본다. 텐서플로는 기본적으로 텐서(tensor)라는 다차원 배열을 계산 그래프 구조(computational graph) 안에서 흘려보내면서(flow) 처리하는 것을 의미하고, 계산 그래프 구조는 노드(node)와 엣지(edge)로 이루어져 노드와 노드 사이로 엣지들을 통해 텐서들이 이동한다. 노드는 상수(constant), 변수(variable), 연산(operator) 세 가지 중 한 가지로 정의될 수 있다. 정의된 노드를 출력하기 위해서는 한 가지 추가적인 절차를 거쳐야 하는데, 세션을 열어서 실행하는 것이다. 노드를 정의하는 것은 그래프를 생성하는 것까지만 수행한 것이기 때문에, 실제 텐서 값들을 흘려보내기 위해 그래프 실행 단계를 수행해야 하는데 이를 세션을 열어 실행할 수 있다.

```
>>> import tensorflow as tf
>>> hello=tf.constant('hello.TensorFlow!')
>>> sess=tf.Session()
>>> print(sess.run(hello))
b'hello.TensorFlow!'
>>>
```

첫 번째 줄에서 텐서플로를 import 한 후에 두 번째 줄에서 tf.constant라는 명령어로 상수 노드를 정의하였고, 이때 노드의 이름을 hello라고 지정하였다. 세션을 열어 그래프를 실행시켜주고, print라는 명령어로 실행한 sess 값을 출력한다. 지금까지의 절차는 constant라는 명령어를 이용하여 노드에 상수 값을 직접 지정해 주었다. 추가적으로 placeholder라는 명령어는 노드에 지정된 값을 고정시키는 것이 아니라 필요할 때 feed_dict라는 명령어를 통해 다양한 값을 제공할 수 있다.

```
import tensorflow as tf

a=tf.placeholder(tf.float32)
b=tf.placeholder(tf.float32)
add=a+b

sess=tf.Session()
print(sess.run(add, feed_dict={a:1, b:2}))
print(sess.run(add, feed_dict={a:[1,2], b:[3,4]}))

sess.close()
```

```
3.0
[4. 6.]
```

첫 번째 줄에서 텐서플로를 import 한 후에 두 번째 줄과 세 번째 줄에서 tf.placeholder라는 명령어로 임의의 값을 받을 수 있는 노드를 정의하였고, 이때 노드의 이름을 a와 b라고 지정하였다. tf.placeholder API는 인자로 데이터 타입을 의미하는 dtype, 데이터 형태를 의미하는 shape, 연산의 이름을 의미하는 name을 받으며[27], 데이터 타입은 정수를 의미하는 integer, 실수를 의미하는 float, 복소수·실수·허수를 의미하는 complex 등이 있다. 즉, tf.placeholder(tf.float32)은 32비트 실수의 데이터 타입을 갖는 데이터를 feed_dict로 받는 임의의 노드를 지정하는 명령어이다. 네 번째 줄은 정의된 a와 b를 더하는 노드를 생성한다. 세션을 열고, sess.run을 실행할 때는 첫 번째 인자로는 실행하고자 하는 연산인 add를 명시하고, feed_dict를 통해 placeholder에 보낼 값을 지정해 준다.

다음으로 케라스에서 모델을 정의하는 방법은 Sequential 클래스와 함수형 API 두 가지 방법을 활용한다[28]. Sequential 클래스가 많이 사용되는 방법인데, 층을 순서대로 쌓아 올린 네트워크이다. 반면, 함수형 API는 하나의 텐서를 만들고, 이 텐서를 층으로 보내준다. 같은 모델을 Sequential 클래스와 함수형 API의 두 가지 방법을 활용해서 작성해본다. 먼저 Sequential 클래스 방법으로 작성한 모델이다.

27) 솔라리스, "텐서플로로 배우는 딥러닝," 서울:영진닷컴, 2018
28) F. Chollet, "케라스 창시자에게 배우는 딥러닝," 박해선 옮김, 서울:길벗출판사,, 2018

```
[5]  from keras import models
     from keras import layers

     model=models.Sequential()    # 새로운 모델 생성
     model.add(layers.Dense(256, activation='relu', input_shape=(224,224,3)))    # 층 추가
     model.add(layers.Dense(2, activation='softmax'))    # 층 추가
```

model.summary() 명령어를 입력하면 설계된 모델의 구조를 아래와 같이 확인할 수 있다.

```
[6]  model.summary()

     Model: "sequential_3"
     _________________________________________________________________
     Layer (type)                 Output Shape              Param #
     =================================================================
     dense_2 (Dense)              (None, 224, 224, 256)     1024
     _________________________________________________________________
     dense_3 (Dense)              (None, 224, 224, 2)       514
     =================================================================
     Total params: 1,538
     Trainable params: 1,538
     Non-trainable params: 0
     _________________________________________________________________
```

이번에는 함수형 API 형식으로 작성한 모델이다.

```
[7]  input=layers.Input(shape=(224,224,3))                    # 입력 텐서 생성
     x=layers.Dense(256, activation='relu')(input)            # 층에 입력텐서를 적용
     output=layers.Dense(2, activation='softmax')(x)          # 새로운 층에 텐서를 적용

     model=models.Model(inputs=input, outputs=output)
```

model.summary() 명령어를 이용해서 설계된 모델의 구조를 확인해보면 앞서 Sequential 클래스를 활용하여 작성한 모델의 결과와 동일한 구조를 확인할 수 있다. 입력과 출력이 하나인 다소 간단한 모델은 Sequential 클래스 모델만으로도 충분히 작성이 가능하다. 하지만, 다중 입력모델이나 다중 출력모델을 작성할 때는 Sequential 클래스 모델로 작성하는 것이 제한되어 좀 더 복잡한 방식의 함수형 API 모델을 활용한다.

텐서플로를 활용한 딥러닝 모델을 생성하기 위해서는 딥러닝 모델에 대한 기초적인 이해가 필요하다. 딥러닝을 포함한 머신러닝 모델은 모두 다음과 같은 과정을 거친다.

① 학습하고자 하는 데이터를 표현할 수 있는 가설함수(hypothesis function)를 가중치(weigh)와 바이어스(bias)로 표현되는 수학적 표현식으로 나타낸다.

② 가설함수가 실제 데이터와 얼마나 차이가 나는지를 표현하는 비용함수(cost function)[29]를 정의한다.

③ 비용함수를 최소화할 수 있는 알고리즘을 통해 비용함수가 최소일 때의 가설함수의 가중치와 바이어스를 찾는다.

가장 단순한 선형회귀 모형으로 예를 들어(1,3), (2,5), (3,7)의 (x, y) 집합이 있다면, x, y의 관계가 $f(x) = 2x + 1$이고, (4,9)를 쉽게 예측할 수 있다. 머신러닝 모델은 이를 학습하는 방법은 다음과 같다.

① 컴퓨터는 우선 $H(w,b) = wx + b$라는 가설함수에서 w, b의 값을 임의로 형성한다.

② 임의로 형성한 w,b 값이 목표값인 w=2, b=1과 얼마나 차이가 나는지를 $\mathrm{cost}(w,b)$ 함수로 구하는데, 흔히 $\mathrm{cost}(w,b)$ 함수는 최소제곱법을 활용하여

$\mathrm{cost}(w,b) = \frac{1}{m} \times \sum_{i=1}^{m} (w \cdot x_i + b - y_i)^2$ 와 같이 나타낼 수 있다.

③ 위 문제는 결국 $\min \sum_{i=1}^{m} (w \cdot x_i + b - y_i)^2$로 나타낼 수 있다. 이러한 간단한 문제에서는 w, b값과 비용함수는 2차방정식의 형태를 띠므로, 인간이라면 위 식의 w, b에 대한 기울기를 0으로 하는 값을 찾음으로써 최적해를 찾아낼 수 있다. 하지만 문제가 복잡해질수록 위 방식은 유용하지 않는데, 컴퓨터가 이를 해결하기 위한 최적화 기법 중 주로 사용하는 방법은 경사하강법(gradient descent)이다. w에 대한 기울기와 b에 대한 기울기를 아래와 같이 구한 후,

29) 손실함수(loss function)라고도 한다.

$$\frac{\partial \mathrm{cost}(w,b)}{\partial w} = \sum_{i=1}^{m}(2x_i^2 \cdot w + 2x_i \cdot b - 2x_i \cdot y_i) \times \frac{1}{m}$$

$$\frac{\partial \mathrm{cost}(w,b)}{\partial b} = \sum_{i=1}^{m}(2x_i \cdot w - 2y_i + 2b) \times \frac{1}{m}$$

기울기가 음수라면 w, b를 증가시키고 기울기가 양수라면 w, b를 감소시키면서, 반복적으로 변수인 w, b의 값을 변경해 나가며 기울기가 0이 되는 w, b를 찾는 것이다. w, b와 같이 기계가 학습해서 찾아나가는 값을 파라미터(parameter)라고 하는데, 이를 보다 일반화해서 θ_i로 표현하고, 경사하강법의 파라미터가 어떻게 업데이트 되는지를 수식으로 나타내면 다음과 같다.

$$\theta_i = \theta_i - \alpha \frac{\partial \mathrm{cost}(\theta_0, \theta_1)}{\partial \theta_i}$$

여기에서 α는 파라미터를 얼마의 크기만큼 업데이트 할지를 조절하는 학습률(learning rate)이다. α가 너무 크면 파라미터가 최적의 지점으로 수렴하지 못하고 발산할 수 있고, α가 너무 작으면 학습 속도가 지나치게 느린 문제가 발생할 수 있어 적절한 α 값을 찾는 문제가 중요하다.

이제 위의 머신러닝 기본 프로세스를 바탕으로 실제 명령어로 위의 선형회귀 문제를 구현시켜보도록 하자. 텐서플로의 기본 동작과정과 머신러닝의 기본 프로세스를 종합하면 아래의 ①~③ 단계로 정리할 수 있다.

① 텐서플로를 이용해서 가설함수와 비용함수를 설계

② sess.run을 이용해 설계된 계산을 실행

③ 비용함수 최소화를 위해 가중치와 바이어스라는 파라미터를 업데이트

이때의 파라미터 업데이트는 비용함수가 최소화 되었다고 판단될 때까지로 설정한다. 위 절차 중 ①단계의 가설함수와 비용함수 설계는 다음과 같은 명령어로 수행된다.

```
import tensorflow as tf

# 임의의 가중치(w), 바이어스(b) 생성
w=tf.Variable(tf.random_normal([1]), name='weight')
b=tf.Variable(tf.random_normal([1]), name='bias')

# 데이터를 입력받을 placeholder 지정
X=tf.placeholder(tf.float32, shape=[None])
Y=tf.placeholder(tf.float32, shape=[None])

# 가설함수 정의
hypothesis=X*w+b

# 비용함수 정의
cost=tf.reduce_mean(tf.square(hypothesis-Y))

# 최적화 기법으로 경사하강법, 학습률 지정
optimizer=tf.train.GradientDescentOptimizer(learning_rate=0.01)

# 최적화 할 노드로 'cost' 지정
train=optimizer.minimize(cost)
```

tf.random_normal([1])은 값이 하나인 1차원 array를 랜덤으로 형성하는 명령어이며, tf.reduce_mean은 여러 개의 수치 텐서의 평균값을 제공하는 명령어이다. ②~③단계로 세션을 구성하고, 비용함수의 최소화를 위해 파라미터 업데이트를 1001회 실시토록 설계하여, 세션을 실행하였다.

```
# 세션 구성
sess=tf.Session()

# Variable 초기화
sess.run(tf.global_variables_initializer())


# cost, w, b, train 노드를 실행시켜 파라미터 업데이트 루프 설정(1001회)
for step in range(1001):
    cost_val, w_val, b_val, train_=sess.run([cost, w, b, train], # 실행값을 cost_val, w_val, b_val, train_에 저장
        feed_dict={X:[1,2,3], Y:[3,5,7]}) # 위 placeholder에 데이터를 제공
    if step % 50 == 0:    # 50회마다 step, cost_val, w_val, b_val 출력
        print(step, cost_val, w_val, b_val)
```

tf.global_variables_initializer은 위에서 w, b를 정의하기 위해 사용한 Variable 명령어를 실행하기 위해서는 항상 global_variables_initializer를 통해 초기화 시켜야한다. 실험 결과는 아래와 같이 확인할 수 있다.

```
0 12.834915 [0.89086574] [0.16413948]
50 0.009731204 [2.1102436] [0.7399972]
100 0.0075706816 [2.1008034] [0.77082324]
150 0.005951228 [2.0893826] [0.79681194]
200 0.004678195 [2.0792477] [0.81985]
250 0.0036774715 [2.0702627] [0.84027624]
300 0.0028908218 [2.0622962] [0.85838616]
350 0.0022724483 [2.0552328] [0.87444276]
400 0.0017863469 [2.0489705] [0.88867867]
450 0.0014042482 [2.0434184] [0.9013004]
500 0.0011038772 [2.038495] [0.9124907]
550 0.0008677286 [2.0341303] [0.9224131]
600 0.00068211835 [2.0302606] [0.9312101]
650 0.0005361958 [2.0268297] [0.9390099]
700 0.00042150437 [2.0237877] [0.94592506]
750 0.00033134304 [2.0210907] [0.95205605]
800 0.0002604567 [2.0186992] [0.9574924]
850 0.00020474377 [2.016579] [0.9623122]
900 0.00016094699 [2.0146992] [0.9665853]
950 0.00012651918 [2.0130324] [0.97037405]
1000 9.945404e-05 [2.011555] [0.97373307]
```

설계한 선형 회귀 모델에 새로운 X 값인 4를 입력하고 출력되는 가설함수의 값을 확인해보자. 예측한 값인 9와 거의 유사한 값이 출력되는 것을 확인할 수 있다.

```
[24] print(sess.run(hypothesis, feed_dict={X:[4]}))

[9.019953]
```

앞에서 선형회귀를 통해 머신러닝의 기본 프로세스를 확인해보았다. 하지만, 선형회귀만으로 문제해결을 할 수 없는 경우가 많다. 예를 들어 학습시간에 따라 합격과 불합격이 발표되는 이항분류(binary classification)가 있다고 하자. 선형회귀에서는 학습시간에 따른 성적 등이 결과값이 될 수 있지만, 이항분류에서는 학습시간에 따른 결과값은 오직 합격 또는 불합격이다. 이항분류의 결과 값은 합격 또는 불합격 외에도 종양, 미종양 등 0 또는 1의 값으로 변환할 수 있는 값으로 선형회귀의 가설함수 $H(w,b) = wx + b$로는 더 이상 이를 표현할 수 없게 되며, 이때 사용되는 가설함수가 S자 형태로 그려지는 함수인 시그모이드(Sigmoid

function)이다. 시그모이드 함수를 그려가는 과정을 로지스틱 회귀라고 하며, 시그모이드 함수를 나타내는 방정식은 아래와 같다.

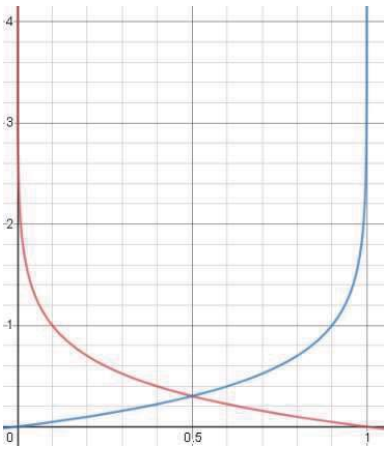
$$H(w,b) = \frac{1}{1+e^{-(wx+b)}}$$

그런데 시그모이드 함수를 이용해 선형회귀의 cost 함수식인 $\cos t(w,b) = \frac{1}{m} \times \sum_{i=1}^{m} (H(x_i) - y_i)^2$ 를 구하면, 선형회귀에서처럼 오목한 형태의 cost 함수가 형성되지 않기 때문에 전체의 최소점(Global minimum)에 도달할 수가 없다. 따라서 로지스틱 회귀에서는 아래와 같은 새로운 비용함수를 사용하는데, 이러한 비용함수가 다항분류에서 사용될 때 크로스 엔트로피 함수(cross entropy function)라 한다.

$$\cos t(H(x), y) = -ylog(H(x)) - (1-y)\log(1-H(x))$$

이 함수는 $y=1$ 일 경우와 $y=0$ 일 경우로 구분하여 아래와 같이 작성할 수 있고 그래프로 나타내면, 아래와 같은 형태를 확인할 수 있다.

$$\cos t(H(x), y) = \begin{cases} -\log(H(x)) & : y=1 \\ -\log(1-H(x)) & : y=0 \end{cases}$$



그래프를 살펴보면, $y=1$일 경우는 빨간색 그래프를 따르게 되고, 가설함수에서 $H(x)=1$라고 예측하게 되면 올바른 예측이며 비용함수 값은 0이 된다. $H(x)=0$이라고 예측하게 되면 잘못된 예측이며 비용함수 값은 무한대가 되어 적절한 비용함수 값이 부여되었다. 반대로 $y=0$ 인 경우는 파란색 그래프를 따르게 되고, 가설함수에서 $H(x)=0$ 이라고 예측하게 되면 올바른 예측이며 비용함수 값은 0이다. $H(x)=1$ 라고 예측하게 되면 잘못된 예측이며 비용함수 값은 무한대가 되어 함수식이 적절한 비용함수 역할을 할 수 있음을 알 수 있다.

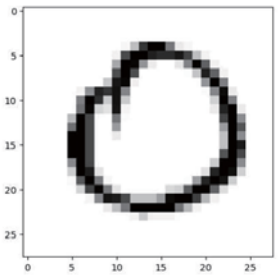
이항분류에서 $wx+b$ 값에 시그모이드 함수를 적용시켜 0~1 사이의 값으로 변환시켜준 것과 유사하게 클래스의 수가 2개를 초과하는 다항분류(multinominal classification)에서는 $wx+b$ 결과값(이를 logits 이라 함)을 아래와 같은 소프트맥스(Softmax) 함수에 적용시킨다.

$$Softmax(y_i)=\frac{\exp(y_j)}{\sum_j \exp(y_j)}$$

소프트맥스 함수의 출력 값은 0~1 사이의 값이며, 클래스별 총합이 1인 형태이기 때문에 각 클래스별 소프트맥스 함수의 출력 값은 결국 해당 클래스가 정답일 확률을 의미한다. 확률이 가장 높은 클래스만 1, 나머지 클래스는 0으로 바꾸어 출력할 수도 있는데 이를 원-핫 인코딩이라고 한다[30].

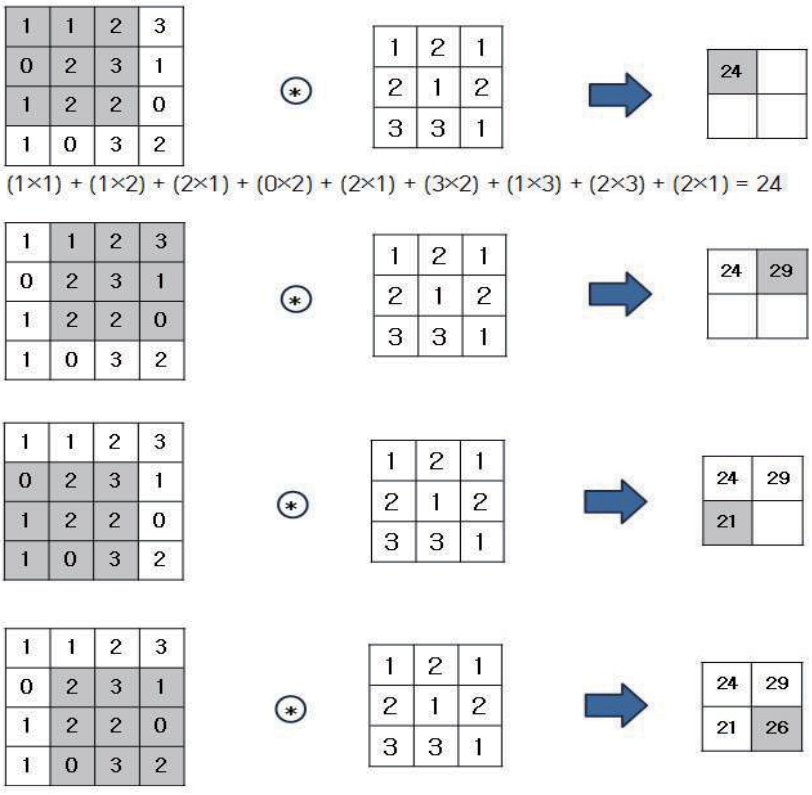
30) 조태호, "모두의 딥러닝," 서울:길벗출판사, 2017

데이터를 바탕으로 딥러닝을 적용해보기에 앞서 컴퓨터가 이미지를 어떻게 인식하는지를 살펴본다. 컴퓨터는 이미지를 크기에 따라 가로×세로의 픽셀로 인식한다. 예를 들어 아래 그림과 같이 28×28 픽셀의 이미지가 있으면, 총 784의 픽셀로 인식하는 것이다. 각 픽셀은 밝기에 따라 0~255까지의 수치를 부여한다. 가장 검은색 배경은 0이고 나머지 픽셀은 1~255의 숫자로 이루어진다. 즉 컴퓨터는 이미지를 0~255까지의 숫자로 채워진 행렬로 인식하는 것이다[31].

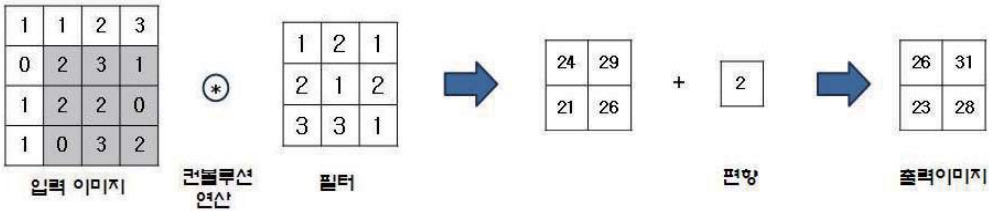


이제 컨볼루션 층과 풀링 층에 대해 알아보자. 컨볼루션 층은 이미지와 필터(filter)와의 컨볼루션 연산을 한 후 바이어스를 더해줌으로써 이미지의 값들을 압축하여 특징을 추출하는 층이다. 여기서 필터는 커널(kernel)이라고도 불리는데, 가로·세로 방향의 차원을 갖는 가중치들의 집합이라 할 수 있다. 컨볼루션 연산은 필터를 일정 간격으로 이동해가며 입력 이미지에 적용하는데, 입력 이미지와 필터에 대응하는 원소끼리 곱한 후 그 총합을 구한다. 그리고 그 결과를 새로운 출력으로 저장한다. 이 새로운 출력에 바이어스까지 더해주면 컨볼루션 층의 결과 값을 얻게 된다[32]. 여기에서 필터를 이동해가는 일정 간격을 스트라이드(stride)라고 하고, 컨볼루션 연산으로 인해 이미지가 줄어드는 것을 방지하기 위해 이미지 주변을 0과 같은 특정 값을 채운 후 컨볼루션 연산을 하기도 하는데, 이를 패딩(padding)이라고 한다. 아래 그림은 컨볼루션 연산의 절차를 보여주는데, 스트라이드가 1이고 패딩은 없는 경우이다.

31) 조태호, “모두의 딥러닝,” 서울:길벗출판사, 2017
32) 사이토 고키, “밑바닥부터 시작하는 딥러닝,” 개앞맵시 옮김, 한빛미디어:서울, 2017



아래 그림은 컨볼루션 연산과 바이어스를 더하는 컨볼루션 층의 전반적인 연산 절차를 보여준다.



이제 어떻게 필터가 컨볼루션 연산을 통해 이미지의 특성을 감지하는지 확인해 보자. 아래와 같이 그레이스케일(grayscale)의 6×6×1의 이미지가 있다. RGB 이미지라면 6×6×3이겠지만 그레이스케일이기 때문에 6×6×1이다. 이 이미지는

왼쪽 절반은 밝고 오른쪽 절반은 어두운 이미지를 나타낸다. 이 이미지는 가운데에 세로 경계선이 있는 이미지로 볼 수 있다.

10	10	10	0	0	0
10	10	10	0	0	0
10	10	10	0	0	0
10	10	10	0	0	0
10	10	10	0	0	0
10	10	10	0	0	0

이 이미지에 아래와 같은 필터를 컨볼루션 연산하면,

1	0	-1
1	0	-1
1	0	-1

다음과 같은 결과를 얻을 수 있다.

0	30	30	0
0	30	30	0
0	30	30	0
0	30	30	0

이는 가운데가 밝고 양쪽이 어두운 이미지를 나타내는데, 즉 입력이미지의 세로 경계선 부분이 밝게 나타남으로써 세로 경계선을 감지할 수 있는 것이다.

컨볼루션 층이 가중치와 바이어스를 적용하는 반면, 차원을 축소하는 역할을 담당하는 풀링 층은 단순히 값들 중 하나를 선택해서 가져오는 방식을 취한다. 풀링

의 종류에는 최대풀링(Max pooling), 평균풀링(Average pooling), 최소풀링(Min pooling)이 있는데, 최대풀링은 이미지의 픽셀에서 가장 큰 값을, 평균풀링은 평균 값을, 최소풀링은 가장 작은 값을 취하는 방법이다. 풀링을 통해 연산량을 감소시킬 수 있고, 이미지의 특징적인 부분만을 선별해 낼 수 있다. 아래는 풀링의 종류를 나타낸 것이다.

컨볼루션 층과 풀링 층을 거친 출력 값은 1차원으로 펼쳐진 후 인공신경망의 하나의 층과 같은 완전연결 층(fully-connected layer)을 거쳐 소프트맥스 결과값으로 최종 판단을 한다.

컨볼루션 신경망을 학습한다는 것은 설계한 신경망의 구조 내의 필터의 가중치 값과 바이어스 값, 완전연결 층의 유닛들을 연결하는 가중치 값과 바이어스 값 등을 찾아가는 과정이다. 하지만 적절한 가중치와 바이어스 값을 찾기 위해서는 대량의 데이터세트가 필요하다. 뿐만 아니라, 대량의 데이터세트가 있다 하더라도 원하는 문제 해결을 위해 컨볼루션 층을 어떻게 쌓을 것인지, 필터의 크기는 어떻게 할 것인지, 완전연결 층의 퍼셉트론의 개수는 몇 개를 할 것인지 등 가장 적절한 구조의 모델을 설계하는 것은 어려운 문제이다. 이 문제를 해결하는 좋은 방법은 사전 학습된(pre-trained) 모델을 사용하여 전이학습(transfer learning)을 실시하는 것이다. 사전 학습된 모델이란 대량의 데이터세트에서 미리 훈련되어 저장된 네트워크로, 일반적으로 ILSVRC(Image-net Large Scale Visual Recognition Competition)에서 100만장이 넘는 이미지 데이터세트인 이미지넷(Imagenet)을 이용하여 학습한 모델이 사전 학습된 모델로 사용된다. 이 모델에서 학습된 가중치, 바이어스와 네트워크의 구조를 이용하면 상대적으로 작은 데이터세트만으로도 이미지 분류 모델을 학습시킬 수 있다.

이제 crack 데이터로 컨볼루션 신경망을 통해 crack이 포함된 데이터와 crack이 포함되지 않은 데이터를 학습 후 테스트 데이터를 통해 학습된 모델의 정확도를 확인해 본다. crack 데이터는 캐글(kaggle)에서 다운로드 받을 수 있다. 캐글은

2010년에 설립된 예측모델 및 분석대회 플랫폼으로 기업 및 단체에서 데이터와 해결과제를 등록하면, 데이터 과학자들이 이를 해결하는 모델을 개발하는 곳이다. 여러 머신러닝 경연대회 뿐만 아니라 많은 데이터들이 탑재되어 있기 때문에, 머신러닝을 학습하는데 필요한 다양한 데이터세트들을 확보할 수 있다.

데이터세트는 surface-crack-detection이라는 폴더 안에 Positive와 Negative라는 하위 폴더로 구성되어 있고 두 개의 폴더는 아래와 같이 각각 20,000장의 crack 데이터와 crack이 아닌 데이터로 구성되어 있다.

〈그림 3-7〉 crack 데이터 세트[33)]

이를 훈련과 테스트를 위해 폴더 재구성을 아래와 같이 한다. 훈련데이터와 테스트데이터의 수를 8:2로 구성해 train 폴더 하의 Positive와 Negative 폴더 안에는 각각 16,000장의 이미지 데이터를 구성하고, test 폴더 하의 Positive와 Negative 폴더 안에는 각각 4,000장의 이미지 데이터를 구성해준다. 분류는 지도학습에 속하기 때문에 컴퓨터에 정답을 제공해 주는 것이 필요한데, Positive와 Negative라는 폴더의 명칭이 레이블의 역할을 담당한다.

33) A. pandian R, "Surface Crack Detection," November, 2019, https://www.kaggle.com/arunrk7/surface-crack-detection

전이학습에 활용한 사전 학습된 모델은 VGG16[34]이다. VGG16은 2014년 ILSVRC에서 준우승한 모델로 13개의 컨볼루션 층과 5개의 풀링 층, 3개의 완전 연결 층으로 구성되어 있다. VGG란 이름은 이 모델을 최초로 설계한 연구자들이 속해 있던 옥스퍼드 대학의 Visaul Geometry Group의 첫 자를 따온 것이고, 16은 딥러닝에서는 일반적으로 학습시켜야 하는 가중치와 바이어스의 파라미터를 가진 층만을 층으로 세기 때문에 풀링 층을 제외한 16개의 층으로 구성되어 있다고 하여 16이라 이름 붙여졌다. VGG16은 3×3의 균일한 크기를 가진 필터와 패딩을 이용해 이미지의 크기가 유지될 수 있도록 컨볼루션을 수행한다. 이전 CNN 모델에 비해 작은 필터를 깊은 네트워크에서 반복적으로 사용하여 효과는 동일하게 하되 파라미터 수를 적게 사용하였다는 특징이 있다.

34) K. Simonyan, A. Zisserman, "Very deep convolutional networks for large-scale image recognition," International Conference on Learning Representations, pp.1-14, 2015.

〈그림 3-8〉 VGG16 구조

이제 전이학습을 활용해 학습하는 과정을 살펴본다. 먼저 ImageDataGenerator를 활용하여 데이터를 불러들인다. 일반적인 파이썬 작업시 데이터는 부동 소수 타입의 텐서로 적절하게 전처리 된 후 네트워크에 제공되어야 하므로, 이미지 파일을 읽은 후 RGB 픽셀 값으로 디코딩하고 부동 소수 타입의 텐서로 변환하여야 한다. 하지만 케라스의 ImageDataGenerator를 활용하면 이 절차를 간단하게 해결할 수 있다.

```
[ ]  # 학습에 사용될 이미지데이터 생성
     from keras.preprocessing.image import ImageDataGenerator
     train_dir='./surface-crack-detection/train'
     batch_size=32
     image_size=224

     train_datagen=ImageDataGenerator()

     train_generator=train_datagen.flow_from_directory(
         train_dir,
         target_size=(image_size,image_size),
         batch_size=batch_size,
         class_mode='binary',
         shuffle=True)

     # 학습에 사용될 클래스 갯수와 클래스의 이름 지정
     class_num=len(train_generator.class_indices)
     custom_labels=list(train_generator.class_indices.keys())

     from keras import optimizers
     from keras.models import Sequential
     from keras.layers import Flatten, Dense
     from keras.models import Model
     from keras import models
     from keras import layers
     import keras.backend as K

     K.clear_session()
```

batch_size는 한번의 배치(batch)마다 넣어주는 데이터 수를 의미한다. 컴퓨터의 메모리 한계와 속도 저하 문제 때문에 모든 데이터세트를 한 번에 학습하는 것이 아니라 데이터를 나누어서 넣어주게 되고, 배치란 나누어진 데이터세트, batch_size란 몇 개의 데이터를 한 번에 학습하는지를 의미하고 데이터를 몇 번 나누어 주는지는 iteration이라고 한다. image_size는 VGG16이 입력으로 받는 이미지 사이즈가 224×224 이기 때문에 224로 설정하였다. class_mode는 이항분류이기 때문에 binary로 설정하였고, 다항분류일 경우에는 categorical을 설정하면 된다. 아래와 같이 훈련데이터 32000장이 정상적으로 읽힌 것을 확인할 수 있다.

```
Found 32000 images belonging to 2 classes.
```

다음 절차는 사전 훈련된 모델을 불러온 후 추가로 모델을 구성하는 부분이다. VGG16을 불러온 후 weights는 이미지넷 데이터세트로 학습된 가중치를 불러오겠다는 뜻이다. include_top은 VGG16의 완전연결 층을 포함할지 여부를 결정하는 명령어로 False을 설정하면 완전연결 층을 포함하지 않은 네트워크만을 불러오게 된다. input_shape로는 image_size(224), image_size(224), 3을 설정하는데 3은 RGB 이미지를 의미하고, 그레이스케일일 경우는 1로 설정한다. 불러온 VGG16의 네트워크를 conv_layers란 이름으로 지정한다. layer.trainable=False는 conv_layers의 파라미터(가중치, 바이어스)는 학습되지 않도록 고정하는 명령어이다.

이제 새로운 모델을 생성해보자. 우선 models.Sequential() 선언을 한 후 model.add() 함수를 통해 필요한 층을 차례로 쌓아올릴 수 있다. 가장 먼저 앞서 구성한 conv_layers를 쌓고 Flatten() 함수를 활용하여 이를 1차원 값으로 펼친다. Dense() 함수로 완전연결층을 쌓아주는데 1024는 유닛 수를 의미하며, 활성화함수는 relu이다. 마지막 완전연결 층의 유닛 수는 sigmoid 활성화함수를 사용하는 이항분류에서는 1로 설정하며, 다항분류일 경우에는 유닛 수는 클래스의 수, 활성화함수는 softmax로 설정한다.

```
[22] # VGG16 불러오기, VGG16의 dense층을 제외한 구조를 conv_layers 로 저장
     from keras.applications import VGG16
     conv_layers=VGG16(weights='imagenet', include_top=False, input_shape=(image_size, image_size, 3))

     # VGG16에서 불러온 conv_layers 의 파라미터는 학습되지 못하도록 지정
     for layer in conv_layers.layers:
         layer.trainable=False

     # 새로운 모델 생성
     model=models.Sequential()
     # 생성한 모델에 VGG16모델로 구성한 conv_layers 추가
     model.add(conv_layers)

     # model의 fully Connected layer 부분을 재구성
     model.add(layers.Flatten())
     model.add(layers.Dense(1024,activation='relu'))
     model.add(layers.Dense(1, activation='sigmoid'))

     # 모델 저장
     VGG16_model_path='VGG16_1024.h5'
     model.save(VGG16_model_path)
```

아래와 같은 명령어로 모델이 생성된 결과를 확인해 볼 수 있다. VGG16 모델의 3차원 출력값을 1차원 출력값으로 변경하고, 유닛 수는 7×7×512=25088임을 알 수 있다. 다음 두 개의 층은 재구성 한 대로 Dense 층이며, 유닛 수는 설정한 것과 같이 1024, 1이다.

```
[13] model.summary()
```

```
Model: "sequential_1"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
vgg16 (Model)                (None, 7, 7, 512)         14714688
_________________________________________________________________
flatten_1 (Flatten)          (None, 25088)             0
_________________________________________________________________
dense_1 (Dense)              (None, 1024)              25691136
_________________________________________________________________
dense_2 (Dense)              (None, 2)                 2050
=================================================================
Total params: 40,407,874
Trainable params: 25,693,186
Non-trainable params: 14,714,688
_________________________________________________________________
```

다음은 설계한 모델을 학습시키는 과정이다. 모델을 로딩한 후 모델의 손실함수와 최적화 기법, 성능지표를 선택해준다. 손실함수는 binary_crossentropy로 설정하고, 다항분류일 경우에는 categorical_crossentropy로 설정한다. 아래의 예제에서 최적화 기법은 RMSprop을 사용하였는데, 최적화 기법은 앞서 확인한 경사하강법 외에도 SGD(Stochastic Gradient Descent), 모멘텀(Momentum), Adagrad(Adaptive Gradient) 등 다양한 방법이 있으며, 예제에서는 많이 사용되는 RMSprop을 사용하였다. 최적화 기법 선택시 인자로는 학습률을 지정하였으며, 예제에서는 10^(-5)로 선택하였다. 성능지표(metrics)로는 정확도(accuracy)를 선택하였다. 모델 학습 시 학습세대(epochs)는 동일한 데이터를 몇 번 반복적으로 학습할지를 의미하는데, 예제에서는 10회로 선택하였다.

```
from keras.models import load_model

# 모델 로딩
model=load_model(VGG16_model_path)

# 모델 컴파일
model.compile(loss='binary_crossentropy',
              optimizer=optimizers.RMSprop(lr=1e-5),
              metrics=['acc'])

# 모델 학습
history=model.fit_generator(
    train_generator,
    steps_per_epoch=train_generator.samples/train_generator.batch_size,
    epochs=10)

# 모델 저장
model.save(VGG16_model_path)
```

아래와 같이 학습세대별 학습경과가 출력되면, 학습에 성공한 것이다. 학습이 반복되면서, 손실은 줄어들고, 정확도는 높아져, 학습률이 적절하게 부여되어 수렴하고 있음을 확인할 수 있다.

```
Epoch 1/10
1000/1000 [==============================] - 11951s 12s/step - loss: 0.0519 - acc: 0.9875
Epoch 2/10
1000/1000 [==============================] - 170s 170ms/step - loss: 0.0084 - acc: 0.9986
Epoch 3/10
1000/1000 [==============================] - 170s 170ms/step - loss: 0.0038 - acc: 0.9994
Epoch 4/10
1000/1000 [==============================] - 170s 170ms/step - loss: 0.0023 - acc: 0.9998
Epoch 5/10
1000/1000 [==============================] - 169s 169ms/step - loss: 0.0012 - acc: 0.9998
Epoch 6/10
1000/1000 [==============================] - 169s 169ms/step - loss: 5.9886e-04 - acc: 0.9999
Epoch 7/10
1000/1000 [==============================] - 169s 169ms/step - loss: 8.5926e-05 - acc: 1.0000
Epoch 8/10
1000/1000 [==============================] - 169s 169ms/step - loss: 7.1525e-05 - acc: 1.0000
Epoch 9/10
1000/1000 [==============================] - 169s 169ms/step - loss: 9.5119e-07 - acc: 1.0000
Epoch 10/10
1000/1000 [==============================] - 169s 169ms/step - loss: 1.8485e-08 - acc: 1.0000
```

이제 사전에 분류한 테스트 데이터를 활용하여 모델의 테스트 정확도를 확인해 보자. 약 99.56% 라는 매우 높은 정확도를 확인할 수 있다.

```
# 테스트 정확도 확인
from keras.preprocessing.image import ImageDataGenerator
test_dir='./surface-crack-detection/test'
batch_size=32
image_size=224

test_datagen=ImageDataGenerator()

test_generator=test_datagen.flow_from_directory(
    test_dir,
    target_size=(image_size,image_size),
    batch_size=batch_size,
    class_mode='binary')

test_loss, test_acc=model.evaluate_generator(test_generator,steps=test_generator.samples/test_generator.batch_size)
print('test acc:', test_acc)
```

```
test acc: 0.9955506324768066
```

다음으로 동일한 데이터세트로 직접 네트워크를 구성하여 학습하는 절차를 진행하되, 텐서플로 2.0 버전을 활용한다. 텐서플로 2.0 버전이 나오면서 1.0 버전 사

용자의 혼란을 막기 위해 호환성 라이브러리인 tf.compat.v1을 제공하여 2.0 버전에서도 1.0 버전의 API를 불러올 수 있고, 업그레이드 스크립트인 tf_upgrade_v2로 1.0 버전의 코드를 2.0 버전으로 자동 변환할 수 있다[35]. 하지만 앞으로 텐서플로를 지속적으로 사용한다면, 텐서플로 2.0 버전을 익힐 필요가 있다. 전반적인 과정은 케라스를 단독으로 사용하는 것과 크게 다르지 않다. 케라스와 유사하지만 텐서플로를 import시키는 과정을 거쳐야 하며, ImageDataGenerator를 import하는 과정도 조금의 차이가 있다.

```
[6]  # 학습에 사용될 이미지데이터 생성
     from tensorflow import keras
     import tensorflow as tf

     from tensorflow.python.keras.preprocessing.image import ImageDataGenerator
     train_dir='./drive/My Drive/surface-crack-detection/train'
     batch_size=32
     image_size=224

     train_datagen=ImageDataGenerator()

     train_generator=train_datagen.flow_from_directory(
         train_dir,
         target_size=(image_size,image_size),
         batch_size=batch_size,
         class_mode='binary',
         shuffle=True)

     Found 32000 images belonging to 2 classes.
```

다음은 새로운 모델을 생성하는 과정이다. 새로운 모델은 VGG16과 유사하게 3×3의 필터와 패딩을 이용하여 이미지의 크기를 유지하면서 컨볼루션 연산을 실시할 수 있도록 설계하되, 4개의 컨볼루션층, 2개의 최대 풀링층과 2개의 완전연결층으로 구성하였다. Sequential() 함수를 선언 후 사전 학습된 모델을 불러오는 절차 없이 층을 쌓아준다. Conv2D는 컨볼루션 층을 의미하고 MaxPool2D는 최대풀링 층을 의미한다. kernel_size는 필터의 가로 세로 크기를 의미하고, filters는 적용하는 필터의 개수를 의미한다. padding에서 same은 입력 이미지와 출력 이미지의 사이즈가 동일하도록 입력 이미지에 패딩을 적용하는 것이고 valid는 패

35) 김환희, "시작하세요! 텐서플로 2.0 프로그래밍," 위키북스:파주, 2020

딩을 적용하지 않는 것을 의미한다.

```
[ ]  from keras import optimizers
     from keras.models import Sequential
     from keras.layers import Flatten, Dense
     from keras.models import Model
     from keras import models
     from keras import layers
     import keras.backend as K

     # 새로운 모델 생성
     model=tf.keras.Sequential([
         tf.keras.layers.Conv2D(input_shape=(224,224,3), kernel_size=(3,3), filters=32, padding='same',
                                activation='relu'),
         tf.keras.layers.Conv2D(kernel_size=(3,3), filters=64, padding='same', activation='relu'),
         tf.keras.layers.MaxPool2D(pool_size=(2,2)),
         tf.keras.layers.Conv2D(kernel_size=(3,3), filters=128, padding='same', activation='relu'),
         tf.keras.layers.Conv2D(kernel_size=(3,3), filters=64, padding='valid', activation='relu'),
         tf.keras.layers.MaxPool2D(pool_size=(2,2)),
         tf.keras.layers.Flatten(),
         tf.keras.layers.Dense(1024, activation='relu'),
         tf.keras.layers.Dense(1, activation='sigmoid')
     ])

     # 모델 저장
     New_model_path='New_1024.h5'
     model.save(New_model_path)
```

model.summary()를 통해 설계된 모델을 확인한다.

```
[ ]  # 모델 컴파일
     model.compile(loss='binary_crossentropy',
                   optimizer=tf.optimizers.RMSprop(lr=1e-5),
                   metrics=['acc'])

     # 모델 학습
     history=model.fit_generator(
         train_generator,
         steps_per_epoch=train_generator.samples/train_generator.batch_size,
         epochs=10)

     # 모델 저장
     model.save(New_model_path)
```

```
Epoch 1/10
1000/1000 [==============================] - 139s 139ms/step - loss: 0.0070 - acc: 0.9989
Epoch 2/10
1000/1000 [==============================] - 140s 140ms/step - loss: 0.0121 - acc: 0.9984
Epoch 3/10
1000/1000 [==============================] - 138s 138ms/step - loss: 0.0018 - acc: 0.9996
Epoch 4/10
1000/1000 [==============================] - 140s 140ms/step - loss: 0.0029 - acc: 0.9993
Epoch 5/10
1000/1000 [==============================] - 138s 138ms/step - loss: 0.0046 - acc: 0.9993
Epoch 6/10
1000/1000 [==============================] - 140s 140ms/step - loss: 0.0012 - acc: 0.9997
Epoch 7/10
1000/1000 [==============================] - 139s 139ms/step - loss: 0.0051 - acc: 0.9996
Epoch 8/10
1000/1000 [==============================] - 140s 140ms/step - loss: 3.1813e-04 - acc: 0.9999
Epoch 9/10
1000/1000 [==============================] - 139s 139ms/step - loss: 0.0017 - acc: 0.9998
Epoch 10/10
1000/1000 [==============================] - 139s 139ms/step - loss: 0.0017 - acc: 0.9998
```

이제 테스트 정확도를 확인해보면, 전이학습을 할 때 보다는 낮지만, 97% 이상의 높은 정확도를 확인할 수 있다.

```
from tensorflow.python.keras.preprocessing.image import ImageDataGenerator
test_dir='./drive/My Drive/surface-crack-detection/test'
batch_size=32
image_size=224

test_datagen=ImageDataGenerator()

test_generator=test_datagen.flow_from_directory(
    test_dir,
    target_size=(image_size,image_size),
    batch_size=batch_size,
    class_mode='binary')

test_loss, test_acc=model.evaluate_generator(test_generator,steps=test_generator.samples/test_generator.batch_size)
print('test acc:', test_acc)
```

```
test acc: 0.9755240678787231
```

지금까지 살펴본 것처럼 딥러닝은 입력변수에 대한 주관적인 개입 없이도 이미지 인식, 자연어 처리, 패턴 추출 등에 있어서는 매우 우수한 성능을 보이는 강점을 가지고 있다. 그러나 딥러닝도 만능도구는 아니며, 대량의 데이터를 필요로 한다는 점, 블랙박스 모델처럼 처리과정에 대한 설명이 어렵다는 점, 그리고 많은 연산량을 필요로 한다는 약점을 가지고 있다.

제4장 딥러닝 기술의 국방획득체계 지원 방안 제시

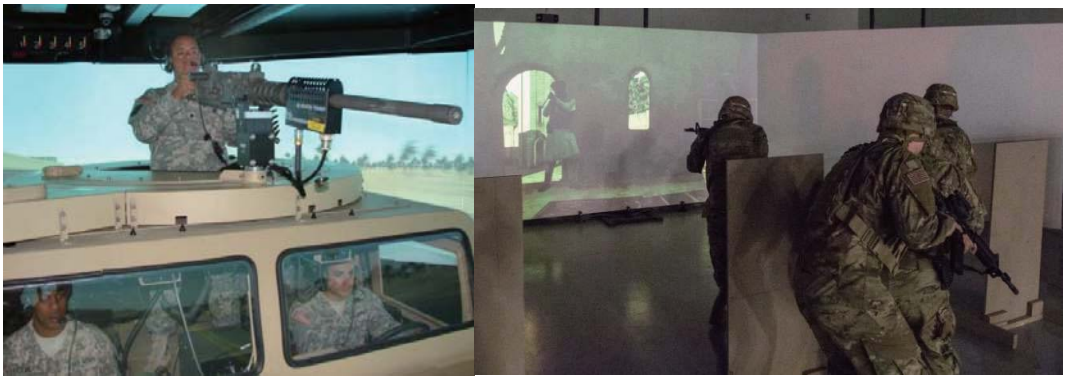
2장에서 살펴본 것처럼 기존의 국방획득체계가 절차의 누락이 없이 꼼꼼하고 체계적으로 대규모의 무기체계를 연구개발하거나 구매하여 획득하는데 중점을 두고 공고히 발전되었던 반면, 현재 동향을 종합해볼 때 앞으로는 미래전에 적합한 신기술을 신속하게 전력화할 수 있는 방향으로의 진화를 모색하고 있는 것으로 보인다. 이를 고려할 때 본 장에서는 딥러닝 기술이 국방획득체계의 어떤 단계에서 어떻게 활용될 수 있을지 살펴본다. 다만 3장의 기초적인 딥러닝 기술을 넘어서는 미래지향적인 관점에서 기술의 응용 가능성을 적용하였다.

〈그림 4-1〉 국방획득의 전반적인 단계

4.1 소요기획 단계

소요기획 단계에서는 소요를 발굴해 내는 것이 가장 중요하다. 이를 위해 작전개념이 형성되면 시뮬레이션을 통해 작전적 불일치 요소나 가능한 물자적 방안을 실험해 볼 수 있다. 이때 딥러닝 기술을 활용하여 아군과 적군이 모두 인공지능으로 구현하여 강화학습을 시키거나 실제 병력을 연계하여 다양한 작전의 조합과 상황을 워게임해 볼 수 있다.

〈그림 4-2〉 인공지능 활용 워게임[36)]



〈그림 4-3〉 실병력과 연계한 워게임[37)]

대안분석을 위해서는 딥러닝 기술을 이용하여 가능한 요소들을 다양하게 조합하여 물자적 방안의 요구성능을 만족하면서도 최적의 대안이 무엇인지 실험해 볼 수 있다. 또한 기존 및 개발중인 무기체계에 대한 형상 데이터가 구축되어 있다면 딥러닝을 통한 유사체계 및 필요 형상 자료에 대한 신속한 검색을 도울 수 있다.

36) https://www.artificial-intelligence.blog/entertainment/wargames
37) https://breakingdefense.com/2019/05/let-the-war-games-begin-army-buying-high-tech-training-sims/

4.2 선행연구 단계

선행연구 단계에서는 사업추진기본전략을 수립하기 위한 많은 분석이 요구된다. 먼저 경제성 분석을 위해 비용분석에 활용할 수 있다. 비용분석을 위한 기초자료가 구축되어 있다면 딥러닝 구조를 회귀 문제로 구성하여 비용에 대한 공학적 분석을 실시할 수 있다. 연구개발 가능성에 대해서도 비용분석과 유사하게 주어진 요인에 따른 개발 성공 확률에 대한 모델을 구축해 볼 수 있다. 기술성숙도 분석도 기술성숙도에 영향을 미치는 요인들을 분석하고 구축된 데이터로부터 딥러닝 모델을 만들어 최종 기술성숙도가 어떻게 될지 예측해 볼 수 있다. 그 외 소요량, 전력화 시기, 파급 효과 등 전문가의 정성적인 평가가 중요한 부분이 많은데, 전문가 그룹 데이터 안에서 가장 적합한 전문가들을 분석하고 추천하는 모델을 생각해 볼 수 있다.

4.3 연구개발 단계

연구개발 단계에서 실제 무기체계의 핵심기술이 연구되고 체계개발이 이루어진다고 볼 때, OODA Loop에 따라 딥러닝 기술을 활용한 무기체계를 생각해 볼 수 있다. OODA Loop은 Observe(관찰), Orient(상황 분석과 종합), Decide(결정), Act(행동) 이라는 일련의 의사결정 순환과정으로 미국의 John Boyd 대령에 의해 제시되었다. OODA Loop을 기준으로 가장 핵심적인 기술을 살펴보면, 먼저 Observe(관찰) 분야에서는 초소형 무인기, 무인수상정 등 다양한 플랫폼을 활용한 지능형 감시정찰지원체계가 있다. 또한 항공과 우주 영역에서 촬영한 이미지를 판독하는 체계나 시각적으로 가려져 있거나 탐지하기 어려운 환경에서도 인공지능을 통해 자동 식별하는 기술이 활용될 수 있다.

〈그림 4-4〉 지상형 지능형 감시정찰지원체계 예[38]

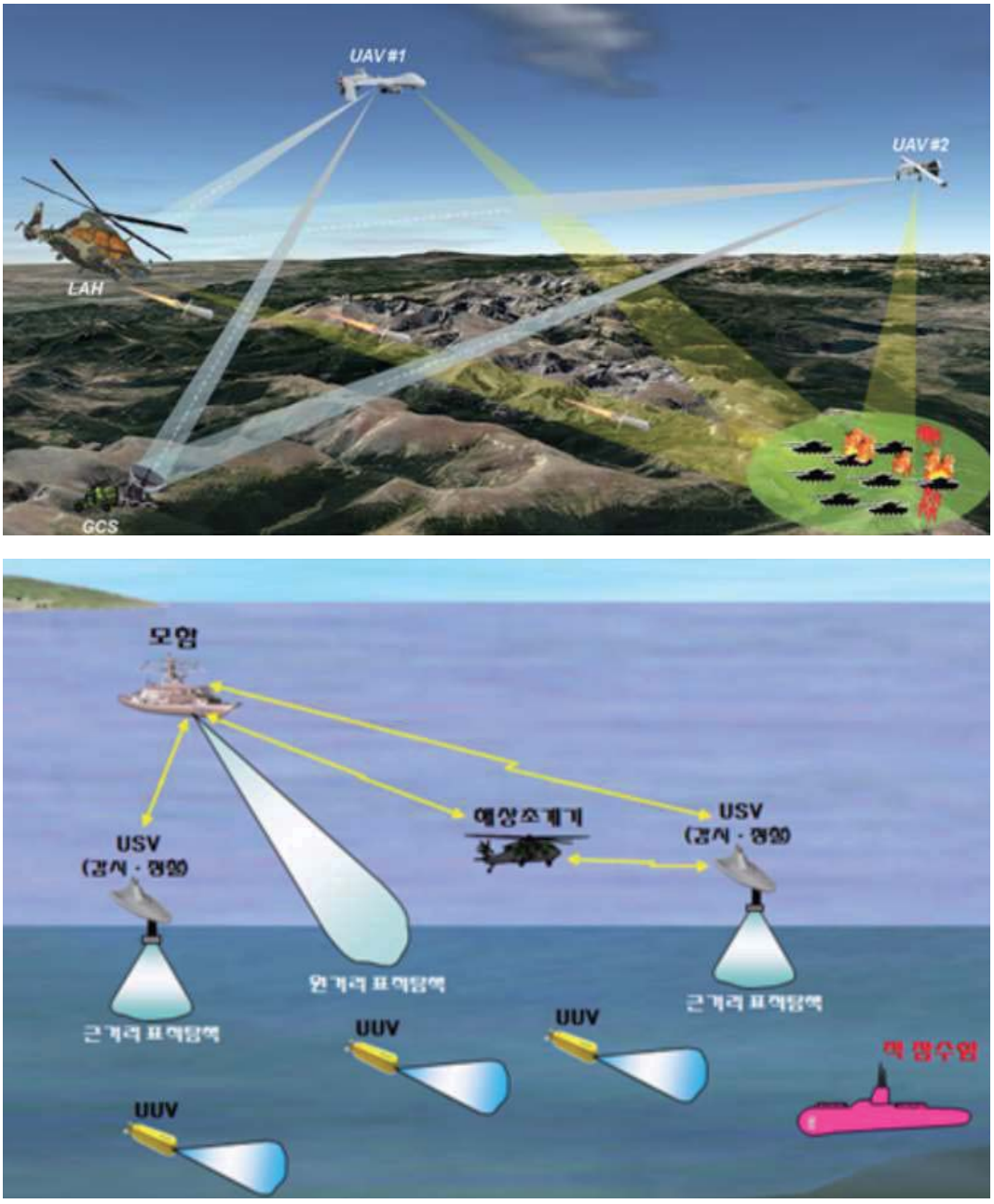
Orient(상황 분석과 종합)과 Decide(결정) 분야는 함께 살펴보면, 각종 센서정보들을 통합하여 적의 의도를 분석하고 최적의 의사결정을 지원하는 지능형 지휘결심지원체계가 있으며, 제대별 의사결정체계에 맞도록 실시간 현장에서의 전술지휘자는 물론 전략적 차원에서의 고등 결심 지원을 포함할 수 있다.

38) http://www.apple-economy.com/news/articleView.html?idxno=63556

〈그림 4-5〉 지능형 지휘결심지원체계 예[39]

Act(행동)에서는 무인체계 단독 자율행동, 무인체계 군집간 자율행동, 유무인 복합체계에서의 협업체계를 구현할 수 있도록 딥러닝 기술이 활용될 수 있다. 특히 유무인 복합체계에서의 협업체계를 구현하기 위해서는 무인체계의 지능이 자율행동이 가능할 정도로 향상된 상태에서 유인체계 혹은 인간과의 신뢰성 있는 상호작용이 가능해야 한다. 또한 모자이크전이나 다영역작전의 개념을 지원하기 위해서는 상위 영역에서의 인간에 의한 지휘 및 통제 외에도 하위 영역에서는 인공지능에 의한 통제가 필수적일 수 밖에 없을 것이다.

39) https://www.aitimes.kr/news/articleView.html?idxno=18378

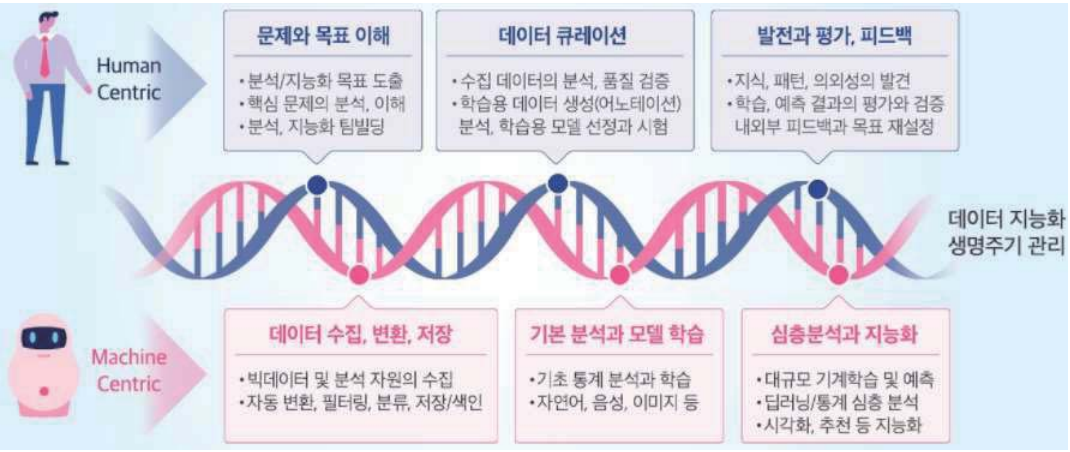


〈그림 4-6〉 공중과 해상에서의 유무인 복합체계 예[40)41)]

40) https://m.blog.naver.com/jhst3103/221858911644
41) 이종용. "해상작전을 위한 유·무인전투체계 협업방안 연구" 해양안보포럼 E-저널, 35, 2018.

4.4 분석평가 단계

분석평가는 획득체계의 단계별로 의사결정을 지원하는 것으로 기본적으로 연구개발 단계에서 제안한 지능형 체계가 필요한 분석평가를 돕는데 사용될 수 있다. 획득체계에서 발생할 수 있는 데이터가 제한되고 폐쇄적일 가능성이 높다는 점을 고려해 볼 때 이를 원활히 하기 위해서는 충분한 학습이 가능하도록 대량의 데이터 구축이 필수적이다. 따라서 학습에 필요한 데이터 구축을 도울 수 있는 딥러닝 모델을 생각해 볼 수 있다. 지능형 데이터 생성체계는 정형적 자료 외에도 음성, 동영상 등 다양한 비정형 데이터를 통합하여 수집하는 지능형 데이터 수집을 넘어 분석에 유리하도록 데이터를 생성시킬 수 있는 체계로 생각할 수 있다.



〈그림 4-7〉 지능형 데이터 생성[42)]

42) http://www.saltlux.com/cloudService/dataMixiDefine.do?menuNumber=4

연구보고 2021

사이버전에서의 머신러닝 기술의 악용 분석과 대응 방안

김 영 안

2021. 10.

국방대학교 국가안전보장문제연구소

목 차

〈그 림 목 차〉

〈표 목 차〉

요 약 문

4차 산업혁명 시대 발전에 따라 사이버 영역 공격자들은 핵심기술인 머신러닝 기술을 활용한 지능화된 알고리즘을 이용해 신·변종 사이버 공격과 자동화 기법을 활용하여 다양한 사이버 공간에서 공격을 시도하고 있다.

기술의 발전 추세가 점차적으로 고도화되고 다양해지는 사이버 공격에 효율적이고 정확하게 대응할 수 있는 기존 사이버보안 솔루션들로는 많은 한계를 보인다. 사이버보안 위협에 대해서 능동적으로 대비하기 위해서 사이버보안 분야에도 머신러닝 기법 적용이 주목하게 되었다.

사이버보안에 머신러닝을 적용함으로써 위협 인텔리전스, 실시간 탐지 및 대응, 네트워크, 악성코드 분석 및 취약점 분석 등 다양한 사이버보안 분야에서 성과가 획기적으로 향상될 것이다[1].

사이버보안 분야에서 활용되고 있는 머신러닝은 보안전문가의 역할을 침해하는 오버피팅 오류와 성향적 오류가 있으며, 이들을 극복하기 위한 노력으로는 방대한 사이버보안 분야 데이터를 그동안은 인간의 경험과 지식을 토대로 분석해 온 분야를 머신러닝을 적용하여 학습 과정을 통한 결과들이 점점 더 악용과 지능화로 인한 사이버보안 위협을 보다 효율적이고 정확하게 탐지하여 빠르게 대응할 수 있다.

또한, 여러형태의 사이버보안 프로세스 자동화로 사람의 개입을 최소화하고 미탐 및 오탐을 최소화를 위해 수집된 수많은 보안 데이터를 장기간 분석해 온 보안전문가의 경험과 지식들을 머신러닝에 적용해서 학습할 수 있도록 해야 한다. 뿐만 아니라 행위 및 시그니처 분석기술 등을 적용하고 머신러닝 기반의 지능화된 공격에 대해서도 실시간으로 탐지와 대응을 제공하도록 해야 한다.

본 연구의 목적은 날로 지능화로 진화되고 있는 사이버보안 위협과 기하급수적으로 증가하는 보안 정보들에서 지능화된 보안 위협을 정확한 분석과 보안 사고들을 실시간으로 대응이 가능한 머신러닝을 사이버보안 분야에 적용이 증가하고 있는 현 시점에 수많은 보안 데이터 및 로그분석 자동화로 필요한 핵심 데이터를 선별적으로 분석하고, 기존 규칙 및 시그니처 기반의 탐지가 제한된 지능화된 사이버보안 위협을 보다 정확하고 효율적으로 탐지하기 위한 머신러닝과 사이버보안

1) CCTV뉴스, “인공지능 보안, 대응 강화와 악성코드 분석 효율 지원”, 2019. 7.

위협 및 머신러닝의 적용사례와 국방 사이버보안 영역의 머신러닝 기반 공격 위협 모델과 공격기술에 대해 설명하고, 국방 사이버보안 영역의 머신러닝 기술에 대한 대응방안으로 통합보안관제체계 운영, 해킹 침해사고 대응 방안, 네트워크 보안 분야 대응방안, 악성코드 분석 분야 대응방안, 분산 서비스공격 대응방안, 취약점 분석 분야 대응방안 및 컴플라이언스 분야 대응방안을 제안한다.

1. 서 론

1.1 연구 배경

4차 산업혁명시대는 초연결성(Hyper-Connected), 초지연성(Hyper-Delay), 초지능화(Hyper-Intelligence)의 특성으로 IoE(Internet of Everything) 환경의 특성을 띠고 있다. 또한 초연결성과 더블어 급격한 컴퓨팅 성능 향상으로 데이터 생성 규모와 순환 주기가 급격히 빨라지면서 더블어 빅데이터(Big Data) 생태계는 그동안 주춤하던 인공지능(AI, Artificial Intelligence)의 발전을 가속화 했으며 사이버보안 기술 또한 머신러닝 기반의 고도화로 연결되고 있다.[2)]

최근 공공, 민간기업 및 국방영역의 핵심 사업에서 인공지능 기술을 활용한 분야가 증가하면서 비즈니스 분야에 대한 머신러닝(ML, Machine Learning) 알고리즘의 의존성이 증가하고 있다. 그러나 인공지능 알고리즘의 결과에 대한 일반적인 확신은 부족한 상황이다.

사이버보안에서의 기관들의 가장 큰 고뇌는 공격자와 방어자 모두 머신러닝을 이용한 도구를 배포하고 있으므로 이들 간의 역량의 차이에 대해서 예측하기 어렵다는 것이다.

따라서 방어자가 지능화된 머신러닝 기술을 적용한 다양한 형태의 위협에 대응하기 위해서는 상호협력과 머신러닝 기반 프로세스를 보호하기 위한 알고리즘들을 개발해야 한다. 안전한 설계, 수명 주기 관리, 사고관리 관련한 인공지능 보안원칙이 필요한데 보안원칙은 인공지능과 관련된 사이버 위험의 거버넌스를 지원하는 강력한 보증체제의 기반을 제공할 수 있다.[3)]

머신러닝 기술을 개발하기 위한 글로벌 경쟁이 가속화되고 있으며 세계 경제 전반의 머신러닝 활용이 빠르게 확산하고 있다. 전 세계적으로 머신러닝 기술 연구 등 AI분야 연구개발에 투자가 활발하게 진행되고 있다.

시장 조사기관인 IDC에 따르면 “AI에 대한 글로벌 지출은 2019년에 375억 달러로 추산되며, 중국과 미국이 글로벌 인공지능을 주도하며 2023년에는 979억 달

2) KISA Report, “디지털 감시(Digital Surveillance)”, 2020년 Vol. 12.
3) KISA Report, “2021년 인공지능 기술과 산업을 전망하며”, 2020년 Vol. 11.

러에 이를 것으로 전망되고 있다". AI 관련 수많은 기술은 기업들의 상황을 정확하게 분석하여 의사결정을 지원하고, 빅데이터 분석을 통한 의료, 교통, 제조 운송, 금융과 같은 다양한 분야에서 지능화된 서비스들을 창출하고 있다. 프로세스 개선, 데이터 활용, 고객 경험 및 효율성 향상 등 다가오는 미래에는 인공지능 시스템이 다양한 활용 분야에서 많은 역할을 할 것이다.[4)]

민간영역의 사이버보안과 국방영역에서의 사이버보안과의 차이점은 크게 다르지 않음을 인지하고 국방영역에서도 인공지능을 적용하려는 움직임이 활발해지고 있으며 점차 더욱 증가할 것으로 예상되며, 특히, 악성코드 탐지, 스팸메일 식별 및 침입 탐지 등 사이버전에서의 머신러닝 기술의 활용성이 커지고 있다.

한편, 머신러닝 기술 자체 또는 머신러닝 기술이 적용된 정보체계의 취약점을 통해 해당 체계의 파괴, 오작동 및 중요자료 유출 등을 목적으로 수행되는 머신러닝 기술 기반의 사이버 공격이 수행될 위험 역시 커지고 있어 이에 대한 대비가 필요하다. 머신러닝 기술과 활용체계의 취약점을 분석하고 관련된 사이버 공격 기술을 이해하는 것은 취약점 제거 및 예방, 관련 사이버 공격을 방어하기 위해서 매우 필수적이다.

하지만, 국방 사이버보안 영역에서 머신러닝 기술에 의한 피해 가능성을 조사하고 대응방안을 제시하는 연구는 아주 미흡한 상황이다.

따라서, 본 연구에서는 국방 사이버보안 영역에서의 머신러닝 기술에 대한 적용 분야를 조사하고, 머신러닝 기반의 공격 위협 사례에 관한 연구와 국방 사이버보안 영역에서의 머신러닝 기반의 공격 위협 모델과 관련 공격기술에 대한 조사를 바탕으로 머신러닝 기술에 대한 대응방안을 수립하고자 한다.

1.2 연구내용 및 범위

본 연구는 해마다 기하급수적으로 진화되고 있는 보안 위협과 날로 증가하고 있는 보안 정보 속에서 인공지능의 머신러닝 기반의 보안 위협을 정확하게 분석해서 보안 사고에 빠르고 조기에 대응이 가능한 인공지능을 국방 사이버보안 분야에서도 적용하려는 시도가 증가하고 있다.

---

4) KISA, "2021년 주요 이슈 전망", KISA Report, 2020. 11. 30.

다양하고 수많은 사이버보안 관련 데이터와 로그를 자동으로 분석한 핵심 정보를 추출하여 기존 룰·시그니처 방식의 단점인 지능화된 보안 위협에 대해 제한된 탐지 영역을 정확하게 탐지가 가능한 머신러닝 기술과 보안위협, 적용사례와 향후 전망 및 대응방안에 대해서 제시하고자 한다.

이를 위해 2장에서는 국방 사이버보안 영역의 머신러닝 기술 적용분야의 사용사례와 국방 사이버보안 분야의 머신러닝 기술 적용 분야에 대해서 제시하고, 3장에서는 인공지능 및 머신러닝 기술에 관해서 설명하고, 머신러닝 기반의 공격위협 사례로 오버피팅, 잘못된 학습 알고리즘 및 적대적 사례 제작에 관해서 설명한다.

4장에서는 국방 사이버보안 영역에서의 머신러닝 기반의 공격 위협 모델과 공격기술에 대한 제시를 위헤 분야별 머신러닝 기반 공격 위협 모델에 대한 설명과 국방 사이버보안 영역의 머신러닝 기반 공격기술인 악성코드, 데이터 공격, 생성적 대립 신경망, 스마트 봇넷, 첨단 스피어피싱 이메일 등에 대한 공격기술을 제시한다.

5장에서는 국방 사이버보안 영역의 머신러닝 기술에 대한 대응방안으로 통합보안관제체계 운영, 해킹 침해사고 대응 방안, 네트워크 보안 분야 대응방안, 악성코드 분석 분야 대응방안, 취약점 분석 분야 대응방안 및 컴플라이언스 분야 대응방안을 제안한다.

마지막 6장에서는 결론으로 사이버전에서의 머신러닝 기술의 악용 분석과 대응방안에 관한 연구 결론을 맺고, 연구 결과를 토대로 향후 국방 사이버보안 영역의 머신러닝 기반 보안 위협 대응방안을 위한 자료를 제공한다.

2. 국방 사이버보안 영역의 머신러닝 기술 적용 분야

2.1 사이버보안 분야 머신러닝 사용 사례

"머신러닝은 기관 및 조직의 보안 위협을 분석, 구성원들이 업무를 추진하는데 가치 있고 효율적이며 진취적인 업무에 초점을 맞출 수 있도록 해준다. 또한 차세대 워너크라이(WannaCry)에 대한 해결책이 될 수도 있다."[5)]

머신러닝은 '컴퓨터가 명시적인 프로그래밍 유무와 관계없이 학습할 수 있는 기능'이며. 방대한 데이터셋과 머신러닝 알고리즘을 적용해서 구축된 모델을 기반으로 학습된 데이터로 미래를 예측한다.

활용분야인 의료분야의 경우 인공지능이 질병에 대한 관리는 물론 진단까지 하고, 자율주행 자동차는 도로의 보행자나 움직이는 물체 등 위험 데이터를 토대로 도로 환경과 상태를 학습한다.[6)]

사이버보안 분야의 머신러닝은 기업의 위협에 대해서 더 효과적이고 정확하게 분석하고, 보안 사고에 대해서 효과적으로 대응 및 대처를 할 수 있도록 한다. 또한 과거 사람이 처리해야 하는 수많은 데이터 및 중요하지 않은 업무들의 많은 분야를 자동화할 수 있다.

또한, 악성코드 탐지 기술에 머신러닝을 활용하여 랜섬웨어(Ransomware) 와 지능형 지속 위협(APT, Advanced Persistent Threat) 등을 탐지하고 차단하며, 사용자 행위 및 네트워크에 대한 모니터링으로 이상행위를 감지하여 조기에 보안 위협을 예방한다.

머신러닝의 학습 방식은 지도학습(Supervised Learning), 비지도학습(Unsupervised Learning) 및 강화학습(Reinforcement Learning)으로 구분되며, 사이버보안 분야에서도 머신러닝의 연구 및 적용으로 지도학습의 가장 대표적인 사례는 스팸 필터링(Spam Filtering)이 있다. 이외에도 학습방법과 특징에 따라 악성코드 탐지(Malware Detection), 사용자 행위 분석(UBA, User Behavior Analytics), 인증(행위분석을 통한 개인 식별), 이상행위 탐지(Anomaly

5) IT WORLD, "보안을 위한 머신러닝 사용 사례 5가지", 2017.12.15
6) 상게서, pp. 1

Detection), 포렌식, 보안관제 등 다양한 분야에서 학습분석 및 특징에 따라 적용되고 있다.

최근 기하급수적으로 지능형 위협이 APT 및 랜섬웨어 등에 의해 증가함에 따라 기존의 룰·시그니처 및 패턴 기반의 백신 제품이 탐지 및 대응능력에 한계가 있는데 이를 해결할 대책은 필요하며, 대안으로 머신러닝에 대한 관심이 더욱 높아지고 있다.

독일의 도이치 텔레콤 혁신 연구소(Deutsche Telekom Innovation Laboratories)와 이스라엘 벤-구리온 대학 사이버보안 연구소의 두두 밈란은 "넓은 의미에서 머신러닝과 딥 러닝이 포함되는 AI는 사이버 방어에 도움을 주기 시작했다. 가장 명백한 사용 사례는 엔드포인트와 네트워크의 악성 행위, 부정 행위 탐지 또는 SIEM의 패턴 분석이다".[7]

사이버보안 분야의 머신러닝 사용 사례를 분류해 보면 비정상 행위 탐지와 공격 저지, 모바일 엔드포인트 분석, 사람의 능력 보강, 반복 작업에 대한 자동화, 제로데이 취약점 제거가 있다.

① 비정상 행위 탐지와 공격 저지

기업에서의 사이버보안 분야의 가장 중요한 과업은 사전에 공격을 저지하하거나 조기에 악성행위를 탐지하는 것이다. 이를 머신러닝 알고리즘이 가능하도록 도움을 준다.

머신러닝은 다양한 인터넷 환경에서의 비정상 접근 및 악성코드에 대한 비정상 SW를 구분하기 위해서는 시스템에 접근해오는 수많은 사용자의 다양한 IP를 분석하고 대처하기 위한 학습적 검토가 필요하다. 머신러닝 알고리즘은 비정상 탐지 및 악성 행위를 조기에 탐지하고, 사전에 공격을 저지할 수 있도록 시스템을 이용한 체계구축으로 기관의 충분한 능력을 갖추게 된다.

② 모바일 엔드포인트 분석

머신러닝은 모바일 및 사이버 환경에서 주요한 기술로 자리를 잡고 있다. 하지만 음성에 기반을 둔 아마존 알렉사, 애플 시리, 구글 나우 등 환경 및 사용자 경험에 초점으로 분류되어 있다.

---

7) IT WORLD, "보안을 위한 머신러닝 사용 사례 5가지", 2017.12.15

사이버보안 분야에도 이들의 사례가 존재한다. 구글은 모바일 엔드포인트에 해당하는 위협을 분석하는 데 머신러닝을 활용하고 있다. 또한 기업들은 머신러닝이 계속 증가하는 BYOD(Body Your Own Device)와 CYOD (Choose Your Own Device)로 발생되는 위협을 더 안정적으로 보호하고 해결할 수 있는 대책으로 평가하고 있다.

모바일아이언과 짐페리움은 기관(업)들이 인공지능이 다양화된 모바일 바이러스 백신 솔루션을 적용할 수 있도록 하여 머신러닝 기반 위협 탐지 기술과 보안 및 컴플라이언스 엔진을 통합하고, 제품화하는데 이는 네트워크, 기기, 애플리케이션에서 발생하는 위협을 탐지해서 즉시 자동으로 기업 데이터를 보호하는 역할을 할 전망이다.[8)]

③ 사람의 능력 보강

사이버보안 분야의 머신러닝은 사람의 분석 능력에 도움을 주는 역할을 하는 것이 중요하다. 악성 행위에 대한 공격을 탐지하고, 네트워크와 엔드포인트 상태 분석을 하고, 취약점에 대한 평가가 대표적인 일들이다. 현재 위협 인텔리전스 분야에서 사람의 분석 능력 및 결과 보강을 위해 가장 필요로 하는 분야는 반복작업이다.

2016년, MIT CSAIL(Computer Science and Artificial Intelligence Lab)은 분석가가 “짚 더미에서 바늘'을 찾을 수도 있도록 도움을 주는 어댑티브 머신러닝 보안 플랫폼(AI2)을 개발했다. AI2 플랫폼은 매일 수백 만의 로그인 정보를 확인, 데이터를 분류한 후 분석가에게 전달하는데 경고 수를 매일 약 100개로 줄여준다. MIT CSAIL과 신생 업체인 패턴EX(PatternEx)의 테스트 결과 공격 탐지율이 85%로 향상되고, 오탐지율은 5배가 감소했다”.[9)]

④ 반복 작업에 대한 자동화

단순 반복 작업으로 인한 사용자의 피로도는 가장 업무의 능률 저하하는 일중 하나이다. 보안분야에서도 위협 인텔리전스에서와 같은 반복적이고 업무 가치가 저하되는 의사결정을 자동화하는 방식은 머신러닝의 활용효과 중 하나로 〈그림 2-1〉과 같이 사용자들의 반복 작업을 자동화하여 그시간을 활용하여 또 다른 중요한

8) 상게서, pp. 2.
9) 상게서, pp. 2.

일들을 처리할 수 있도록 도움을 주는 것이다.

〈그림 2-1〉 사용자 반복작업

머신러닝이 보안분야의 단순 반복 작업을 자동화함으로써 공격 탐지들이 향상되고, 오탐지율은 감소시키는 결과를 얻을 수 있다. 이에 대한 효과는 정보보호 종사자들이 그시간에 또다른 중요한 일을 처리할 수 있도록 도울 것이며 보안 분야의 인적 자원을 더 효율적으로 활용할 수 있도록 한다.

머신러닝은 위협 인텔리전스에서와 같은 반복적이고 업무 가치가 저하되는 의사결정을 할 필요가 없도록 자동화하는 것이다.

파머는 "머신이 랜섬웨어 공격dmfh '전술적' 부분이나 반복 작업을 처리하면, 사람들은 윈도우 XP 업그레이드 등 전략적인 문제에 더 많은 시간을 투자할 수 있다"고 강조했다. 부즈 알렌 해밀톤(Booz Allen Hamilton)은 사이버보안 분야에서 인적 자원을 효율적으로 사용하기 위해 머신러닝 도구를 활용하고 있으며 머신러닝은 위협에 대한 분류 업무보더 중요한 업무로 공격에 대해서 대비토록 도와준다.[10]

10) 상게서, pp. 3.

⑤ 제로데이 취약점 제거

제로데이 취약점(Zeroday exploit)이란 “소프트웨어의 취약점에 대해 공격하는 기술적 위협인데 해당 취약점에 대한 패치가 나오지 않은 시점에서 이루어지는 공격으로 이러한 시점에서 만들어진 취약점 공격(익스플로잇)을 제로데이 취약점 공격이라 한다”[11].

머신러닝을 이용하여 제로데이 공격 위협이나 보호되지 않고 안전하지도 않은 IoT 장치에 대한 표적 공격에 대한 취약점 제거을 해결할 수 있을 것이다.

포브스(Forbes) 보도에 따르면, 애리조나 주립 대학(Arizona State University)의 연구팀은 “다크 웹의 트래픽 분석을 위해 머신러닝을 사용해서 제로데이 익스플로잇에 관한 데이터를 수집하는 연구를 진행하고 있는데 이런 인사이트는 기업과 기관이 데이터 침해가 발생하기 전에 취약점을 없애도록 도움을 준다”.[12]

2.2 국방 사이버보안 분야 머신러닝 기술 적용 분야

① 위협 인텔리전스

위협 인텔리전스는 사이버 보안 전문가가 사이버 공격에 대해 정리하고 분석한 증거 기반 정보이다. 이 정보에는 공격의 메커니즘, 공격이 발생 중인지 파악하는 방법, 다양한 유형의 공격이 비즈니스에 영향을 미치는 경로 및 공격을 방어하는 방법에 대한 행동 위주의 조언이 포함된다.

오늘날 제로데이 공격, 맬웨어, 피싱, 중간자 공격, 서비스 거부 공격 등 다양한 형태의 사이버 공격이 일상적으로 발생한다.

사이버 범죄자가 공격할 새로운 취약점을 발견함에 따라 컴퓨터 시스템과 네트워크에 대한 다양한 공격 방법은 끊임없이 진화하고, 조직은 사이버 위협 인텔리전스(CTI)를 활용하여 새로운 위협에 대한 정보를 계속해서 인지하면서 스스로를 보호할 수 있다. 사이버보안 전문가는 공격에 관해 수집한 정보를 정리, 분석, 개선하여 새로운 내용을 학습하고 이를 활용하여 보다 효율적으로 비즈니스를 보호한다.

11) 위키백과 용어정의
12) 상게서, pp. 3.

또한 위협 인텔리전스(또는 보안 인텔리전스)는 진행 중인 공격을 중단하거나 완화하는 데 도움을 주기도 하며, IT 팀에서 공격에 대해 더 잘 이해할수록, 그 대응 방법에 대해 정보를 기반으로 한 더 나은 의사결정을 내릴 수 있다.

위협 인텔리전스는 인텔리전스 사이클을 거쳐 정보로부터 생성되는데 〈표 2-1〉에서와 같이 필수적인 5가지 단계를 포함하게 된다.

〈표 2-1〉 위협 인텔리전스 필수 단계

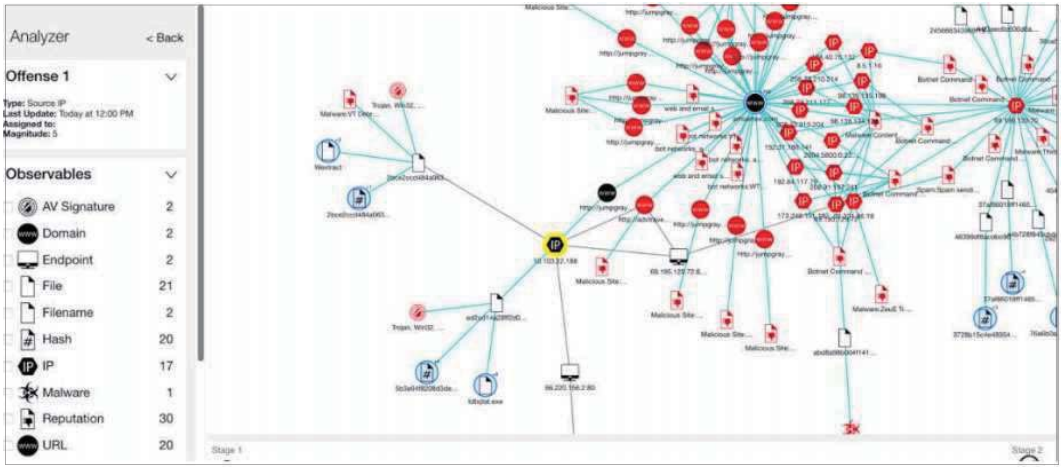
단계	세부 내용
① 계획 및 요구 사항	- 프로그램 목표을 적용한 명확한 CTI 임무 정의 - 실행 관리를 토대로 요구 사항에 기반한 접근방법 - 라이프사이클 프로세스를 이끌고 정보 기반 리소스 사용 방안을 통해 조직 위험 경감
② 수집 및 처리	- 수집 전략으로 요구 사항 충족을 위해 What, When, How, Why 수집하는지 판단 - 위협 데이터를 표준화, 중복 제거 및 보강으로 이용과 적용 가능한 정보 생산 - 처리시간을 절감하기 위해 위협 인텔리전스 플랫폼(TIP) 자동 수집시스템 사용 증가
③ 분석	- 처리 완료된 정보를 해당 프로그램 요구 사항과 비교, 분석, 평가해서 신뢰도, 연관성, 발생 가능성과 위협 영향 파악하기 위한 건전한 분석 판단 제공 - 요구 사항 충족토록 제한된 수집에 대한 평가
④ 생산	- 운영부터 전략, 전술까지 적절성, 관련성, 실행 가능성, 이해관계자들의 필요성까지 반영한 완성된 인텔리전스 제품(브리핑, 기술 보고서 등) 생산 - 이해관계자가 제시한 요건과 비교 모든 제품 결함 문서화
⑤ 유포 및 피드백	- 정해진 주기와 방법으로 내·외부 이해관계자들에게 완성된 인텔리전스 제품을 제공한다. - 제품은 조치 방안 기술과 이해관계자들이 받은 제품 평가 위한 수단 제공

공격자들은 그들의 전술, 행동에 대해서는 변화가 가능하기 때문에 이전 단계의 결과에 따라 새로운 사이클이 적용된다.[13]

사이버보안 분야에서 머신러닝은 전문가들이 정확하고 신속하게 분석하고 새로운 위협을 식별할 수 있도록 도움을 준다. 새로운 패턴의 제로데이 공격 탐지는 빅데이터 분석으로 수집된 새로운 악성 패턴을 식별할 수 있다. 또한, 지능화 기반의 제로데이로 예측 성공률을 향상하게 시킨다면, 전 인류의 위협 인텔리전스를 적용하여 지역적인 위협 동향을 예측도 가능하다.[14]

② 통합보안관제

머신러닝 기술을 활용하여 생성된 위협 인텔리젼스로 통합보안관제 운영 기관(업)의 정보기술 자산, Log, 이벤트, 보안분석에 대해 데이터 마이닝으로 보안체계, 서비스나 솔루션에서 탐지하지 못한 위협에 대해 머신러닝으로 탐지 및 식별하는 방식이다. (〈그림 2-2〉 참조)



〈그림 2-2〉 통합보안관제 개념도[15]

13) FIREEYE, "사이버 위협 인텔리전스 101"
14) 김영중, "머신러닝 기반 정보 보안 기술", MONITIRAPP 최신보안뉴스, 2021. 1.5.
15) IBM 통합 보안 관제 솔루션 소개 자료

통합보안관제에서 수집되는 로그와 다양한 이벤트를 직접 머신러닝에 학습시켜서 관제 담당자가 거의 실시간으로 파악하지 못한 공격징후인 이상 로그나 이벤트에 대해서 탐지 및 오탐을 줄여주기 위해 활용하는 사례도 있다.

대부분의 ESM 및 SIEM 솔루션은 전문 정보보호 관련 기관에서 매우 활발하게 개발하고 있다. ESM과 SIEM 기능보다 향상된 위협 판단 행위나, 상관 분석을 위해서나 그리고 다차원 분석 분야와 통계적인 베이스라인 제시에 머신러닝에 대한 기술들이 적용된다.

머신러닝을 통합보안관제에 활용한 결과 "기존 위협 분석보다 60배 더 빨라졌고 분석 속도도 수시간에서 수분 이내로, 보안 운영 업무 부담이 25배 절감되었으며, 식별되지 않았었던 새로운 위협의 탐지가 10배 증가되었다고 한다".[16]

〈표 2-2〉에서와 같이 보안 패러다임 변화에 따른 보안관제는 계속적으로 진화되고 있으며 가용 인력, 자원과 주어진 시간으로 기하급수적으로 증가하고 있는 방대한 자료를 정확하고 신속하게 분석할 수 있는 머신러닝을 통합보안관제에 적용하려는 기관들이 늘고 있다.

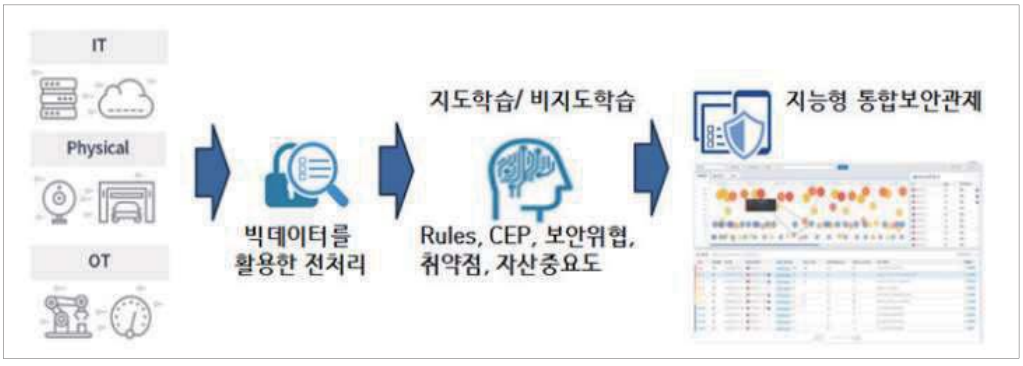
매일 생성되는 방대한 양의 보안이벤트 분석을 자동화해 우선순위가 높은 위험 이벤트를 선별함으로써, 엄청난 양의 보안 데이터 분석에 소요되는 시간을 절약하고 고도화되고 지능화된 보안 위협에 능동적으로 대처할 수 있기 때문이다.

16) SOGETI, FIDUCIA GAD, SCANA 등 인공지능 기반 통합보안 관제 솔루션 적용 기업 피드백

〈표 2-2〉 보안 패러다임 변화에 의한 보안 관제 주요 전략[17)]

구분	주요 내용
1세대: 단위 보안관제 (Perimeter Security)	- 네트워크 기반 보안(방화벽, 침입탐지시스템 등) 장비 활용 초기 구축단계 - 인프라 안정화 단계
2세대: 통합 보안관제 (Data Security)	- 종합분석시스템, 정보공유분석센터(ISAC) 등을 구축 - 취약점 관리, 트래픽 관리, 웹 변조 모니터링 등 관제 범위 확대
3세대: 빅데이터 보안관제 (Trust Security)	- 사이버 보안위협 고도화·지능화 - 다수의 Log, 이벤트, 웹 변조 관제, 네트워크 등 관제 범위 확대
4세대: 인공지능 보안관제 (Zero Trust)	- SOAR(Security Orchestration Automation and Response) - 머신러닝, 딥러닝

지능형 통합보안관제시스템은 〈그림 2-3〉과 같이 각종 디지털 데이터가 Phyical, IT(정보통신), OT(ICS/SCADA)의 보안 시스템에서 발생하는데 데이터를 수집하게 되는데, 독립된 플랫폼에서 빅데이터 분석을 통해 전처리 및 분석하고, 머신러닝 기반의 지도학습과 지도학습을 통해 Rules, CEP, 고위험도, 취약점 및 자산중요도 이벤트를 집중분석하여 통합보안관제에 적용함으로써, 실시간 침해 처리, 시간 단축 및 범위 확대가 가능하며, 처음 발견되는 위협도 탐지가 가능하다.



〈그림 2-3〉 지능형 통합보안관제 시스템[18)]

17) 김미희, "보안관제 + 인공지능", 이글루시큐리티, 2019. 2.
18) 아이티데일리, "AI 기반 보안관제, 철저한 준비가 필요하다", 2018. 10

③ 네트워크 패킷분석 및 침입탐지

기존의 침입탐지시스템은 탐지 대상 공격에 관련된 정보(흔적)와 시그니처가 있어야 하고, 정보와 시그니처가 없는 공격은 대상을 인지하기까지는 많은 시간과 분석이 필요하다.

그러나, 패킷 분석 시스템의 인공지능의 머신러닝 기반 기술을 활용해 기존 네트워크 관련 활동을 학습시키고, 평상 시 운용 중인 네트워크 활동 으로부터 이상 행위에 대한 분석 및 추론을 할 수 있다.

네트워크 상의 동일 디바이스들의 행위에 대한 문맥 학습과 분석 그리고 정상과 비정상 행위에 대한 위험도 산정의 수행, 연결 관계에 대한 통계와 추이를 이용하여 네트워크에서의 이상 징후를 판단한다.

침입탐지에서 문제들은 실시간으로 자동화된 지식(Knowledge)를 생성하는 문제인데 이는 인공지능애서 분류(Classification)의 시각과 전문가 시스템(Expert System)으로 접근할 수 있다.

정상 및 비정상적인 네트워크에서 패킷들을 수집하고, 수집된 패킷에 다양한 머신러닝 알고리즘을 활용하여 자동적으로 지식을 생성한다. 이렇게 학습된 지식으로 실시간 발생하는 패킷들을 정상과 비정상에 관한 결과를 판단하는 문제로 볼 수 있다.[19]

머신러닝 기반의 이상 행위 분석은 이용자들의 활동에 대해 로그, 이벤트, 자산 중요도, 수행명령 등 다양하게 수집 완료된 정보에 대해 데이터들의 저장소 및 데이터들의 마트를 구성하고, 다양한 룰과 모델을 기반으로 머신러닝의 학습 단계가 수행된다.

기본적으로 정상과 이상 분류에 대해서 사용된 대표 모델 베이지안(Bayesian), Holt-Winters, LDA(Latent Dirichlet Allocation) 모델 등이 주로 적용된다. 이후에 실제로 이용자 데이터를 분석하여 룰과 모델을 확인하며 이상 이용자를 탐지하여 위험 점수 등을 조정한다.[20]

네트워크 침입 탐지 시스템(Network Intrusion Detection System, NIDS)에서는 네트워크의 트래픽 감시를 이용한 DoS 공격, 컴퓨터 크랙 시도, 포트 스캔 등과 같은 악의적인 동작들을 탐지하는 시스템이며, 네트워크 침입 탐지 시스템은

19) 이창훈, "인공지능 기법을 이용한 네트워크기반 침입탐지 기술 동향", ICT Standary Weekly
20) 형근, "정보보안에서의 인공지능 도입 분야와 주요 사업자", 시큐티티플러스, 2018. 12, pp.6-7.

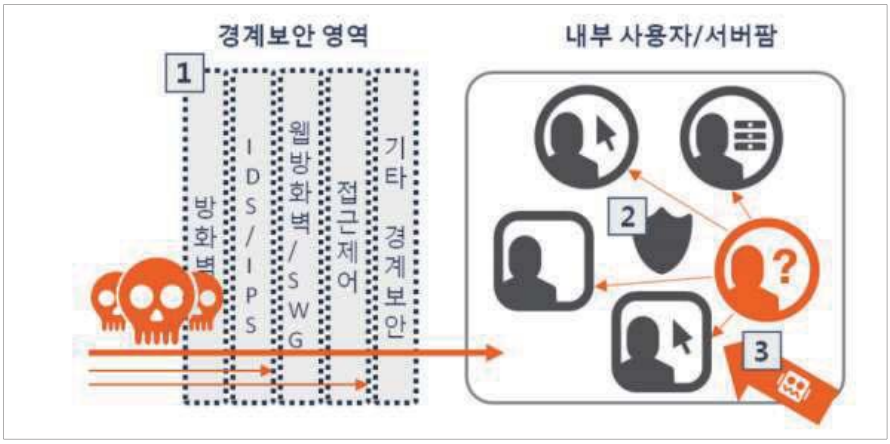
네트워크상의 수신 패킷 전부를 읽고 의심스러운 패턴을 찾는다. 예를 들어, 수많은 TCP 연결 요청이 다양하게 다른 포트를 이용하여 연결 시도를 발견했다면, 수상한자가 포트 스캔을 시도한다고 추측할 수 있으며, 이런 경우는 대부분 침입탐지 시스템에서처럼 수신되는 셸코드를 찾는 행동도 한다.

현재 운용하고 있는 대부분 NIDS 상용제품은 〈그림 2-4〉와 같이 룰 및 시그니처 기반의 시나리오에 의하여 공격을 차단하고 있다.

효율성에 대해서는 조금 보장이되나 각종 공격유형을 분석하여 패턴을 만드는 데는 추가적인 비용 발생과 기존 패턴을 우회하거나 변형된 공격에 대해서는 감지가 제한된다.

기존에는 사용자들에 대한 정상적인 네트워크 사용 통계자료를 기준으로 그 범위에 있지 않을 때에는 침입으로 간주하는 통계를 기반으로 비정상 행위 탐지(Statistics-Based Anomaly Detection) 기법을 많이 사용했다.

최근 사이버 보안 환경은 위협이 고도화 및 지능화됨으로 네트워크에서 발생하는 모든 데이터로부터 위협을 식별하고 실시간 관리을 위해서는 한계가 있다. 이를 위해 머신러닝을 적용하면 정상 및 비정상적 환경에서 네트워크 패킷을 수집하고, 각각의 패킷들에 대해 알맞은 머신러닝 알고리즘을 이용하여 학습한 지식 결과를 가지고, 정상· 비정상 여부를 실시간으로 생성되는 패킷들에 관해 판단할 수 있다.



〈그림 2-4〉 현재까지의 위협방어에 대한 한계[21)]

21) 아이마켓코리아, “인공지능 머신러닝 기반 보안 솔루션 알아보기”, 2019. 2.

④ 악성코드 분석

악성코드의 발생량은 지속적이며 꾸준하게 증가하고 있으며, 공격자들도 기존에 사용 코드를 조금만 변형하여 단순 규칙 기반의 탐지 시스템 및 안티바이러스 체계를 우회한다. AVTest에서 발표에 의하면 "매달 발견되는 새로운 악성코드의 개수에 대한 통계가 매달 평균 천만 개 이상이 수집되고 있으며 이는 분석 전문가의 수동 분석이 가능한 수준을 넘어선 것이다. 따라서 인공지능에 의한 자동 분석 기술 개발이 이제는 선택이 아닌 필수가 되었다."

인공지능을 데이터 분석 기술 영역에 사용할 때는 데이터 특성 분석이 머신러닝 알고리즘이나 모델 최적화 기술만큼이나 중요하다.

최근에 악성코드 데이터의 큰 특징 중 하나는 굉장히 유사한 악성코드들이 지속적이고 반복적으로 등장하고 있다는 것이다. 유사하다는 의미가 공학적으로 명확한 정의가 어렵지만, 데이터 특성에 따라 크게 달라진다. 예를 들어 유사도 특정 지표 중 가장 많이 사용하는 자카르드 인덱스(Jaccard index)에서는, 미리 주어진 데이터들의 형태를 집합 형태로 변형시킨다.

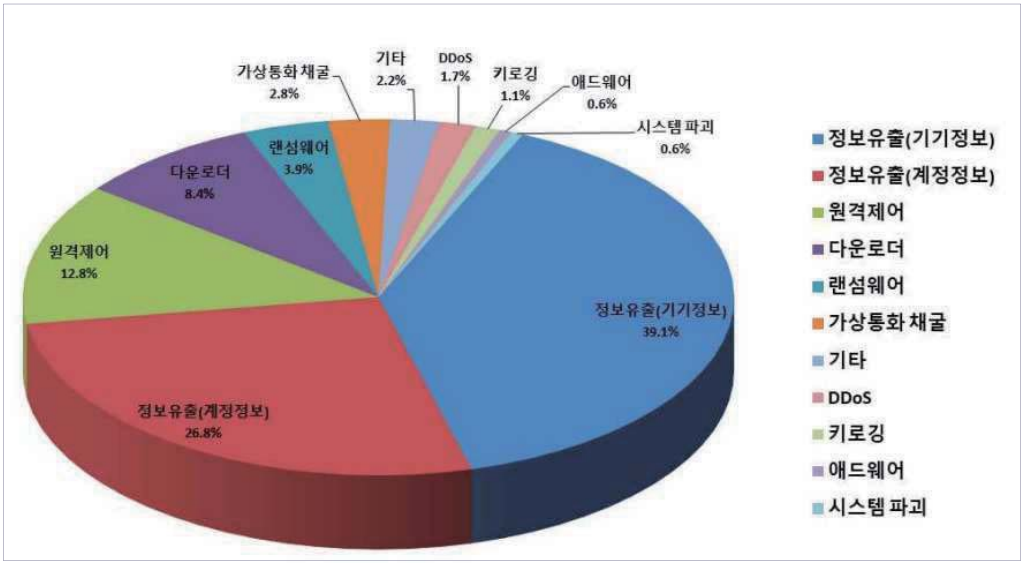
주어진 두 개 데이터 유사도는, "각 데이터로부터 생성된 집합들의 교집합과 합집합을 구하고, 교집합의 크기를 합집합의 크기로 나눔으로써 측정될 수 있다".[22]

물론 기존의 안티바이러스에서도 보안 기법을 적용하여 행위 분석 및 위협 정보를 적용하지만, 패턴 및 서명 업데이트에 크게 의존하고 있는 기존의 한계점에 대해서는 여전히 극복되지 않았다.[23]

한국인터넷진흥원(KISA)에서 발표한 "2019년 하반기 악성코드 은닉사이트 탐지 동향 보고서"에 의하면, 〈그림 2-5〉와 같이 "악성코드 유형 중 정보유출(기기정보)이 39%의 비율로 가장 높았으며, 그 다음으로는 정보유출(계정정보) 27%, 원격제어 13%, 다운로더, 랜섬웨어, 가상통화 채굴 등의 순으로 유형이 다양하게 나타났다."

22) 이식, 김동훈, 조영훈 등. "머신러닝 기반 보안데이터 분석 연구", 정보보호학회지, 제 29 권 제3호, 2019. 6

23) 박형근, "정보보안에서의 인공지능 도입 분야와 주요 사업자", 시큐리티플러스, 2018. 12, pp.7..



〈그림 2-5〉 악성코드 유형별 비율[24]

참고로 2019년 상반기 악성코드 유형은 "원격제어(31%), 정보유출(계정정보)(22%), 다운로더(15%), 랜섬웨어(14%), 정보유출(기기정보)(10%), 가상통화 채굴(4%) 순으로 나타났는데" 후반기와 비교했을 때 유형별 변화가 많이 나타났다.

또한 2019년 하반기의 악성코드 유포지에 대한 탐지 및 조치 현황은 "전년 하반기 대비 12%(276건→243건) 감소하고, 2019년 상반기 대비 25%(323건→243건) 감소했다".

머신러닝을 정상 파일과 악성파일로 구분하고자 하는 시도는 이런 한계점 극복 방안으로 활용되고 있으며, 실제 머신러닝을 악성코드에 적용해도 우선은 속도에서 가장 빠른 기존의 안티바이러스 시그니처 기반의 진단을 가장 먼저 적용한다.

우선 안티바이러스 엔진을 패스한 출처를 알 수 없는 악성코드에 대해 자동화 안티 리버싱으로 프로그램을 코드화해서 "6개의 악성 로직 ①취약점 공격 로직(Exploit) ②감염 및 전파 로직(Infect) ③시스템 호출 변경 및 가로채는 로직(Hook) ④동적 프로그램 삽입(Injection) ⑤비정상 시스템 자원 접근 로직(Access) ⑥정보 유출 로직(Theft)에 대한 변이를 포함하는지 분석하며", 이러한 분석에도 탐지되지 않았을 때는 샌드박스 내에서 시스템 행위 기반 분석을 병행해

24) 한국인터넷정보원(KISA), "악성코드 은닉사이트 탐지 동향 보고서", 2019. 1.

서 수행한다.[25]

악성코드의 위협 모델을 기반으로 IoC(Indicator Of Compromise), 블랙 IP 리스트, C&C IP 리스트와 같은 인텔리젼스 정보를 적용하여 악성코드에 대한 비정상 여부를 판별한다. 이 분야의 있어 대표적인 기업은 마이크로소프트, 딥 인스틱트, 사이랜스, 세이트시큐리티, 아바스트, 등이 있다.

⑤ 사용자 이상 행위분석

사용자의 이상 행위분석은 "광범위한 IT와 보안 인프라에 대한 분석과 비즈니스 혹은 사용자 패턴에 대한 이해라는 어려움으로 인해 이 분야의 해결 방안으로 머신러닝에 대한 관심이 높은 영역 중 하나이다."[26]

사용자의 이상 행위가 악의성에 대한 평가는 수행하는 기존의 업무 패턴을 장기간 분석해서 같은 그룹 사용자와 비교가 요구되며, 기준치 부재로 룰을 정해서 할 수가 없기 때문에 인공지능의 머신러닝 기법을 이용한 위험 점수 기반 시스템이 가장 많이 사용된다.

머신러닝 기반의 이상 행위 분석은 사용자들의 활동에 대한 로그, 다양한 이벤트, 자산중요도, 수행명령 등에서 수집된 다양한 정보에 대해 감사 데이터 저장소 및 데이터 마트를 구성하고, 다양한 룰과 모델을 기반으로 머신러닝에서 학습한다.

이때 사용되는 모델로는 Bayesian, Holt-Winters, LDA(Latent Dirichlet Allocation) 모델 등이 주로 활용되고 있으며, 사용자 데이터를 실제로 분석하고, 규칙과 모델을 확인하며 이상 행위 사용자를 탐지나 위험 점수를 조정한다.

사용자 이상 행위의 주요 카테고리로는 동일 그룹에서 거의 알려지지 않은 새로운 패턴의 발생, 비정상적인 에러 패턴, 이전에 보이지 않던 새로운 패턴, 비정상적인 많은 패턴 등으로 구분할 수 있다. 또한 인공지능의 학습 결과에 대해 사용자 이상 행위로 분류되는 것에 대해 타당한 이유와 행위들에 대해 근거를 제시하여야 한다.

25) 박형근, "정보보안에서의 인공지능 도입 분야와 주요 사업자", 시큐리티플러스, 2018. 12,
26) 상게서, pp 8.

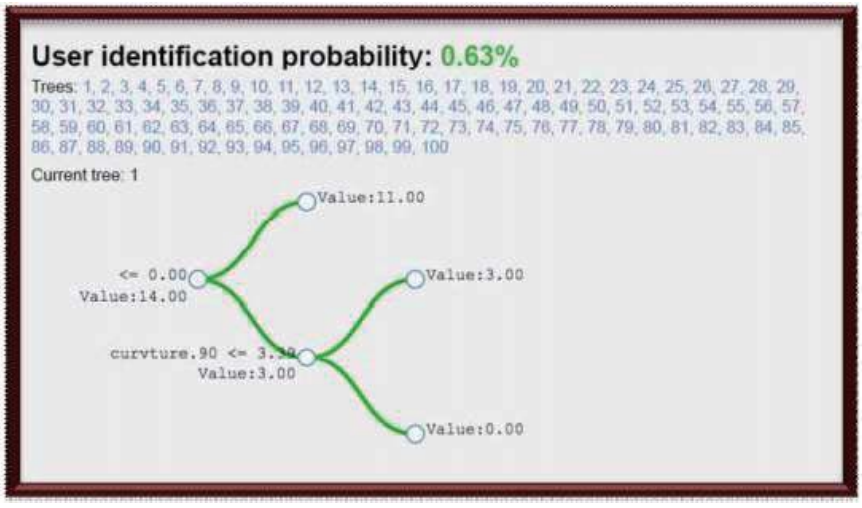
⑥ 사용자 인증과 사기(Fraud) 탐지[27]

사용자 인증과 사기 탐지에 머신러닝 기술의 활용은 매우 새로운 접근 방법이다. 스마트폰이나 PC에 있어 머신러닝의 활용은 다양한 패턴을 학습하여 사용자의 행위 기반 아이덴티티를 만들기 위해서이다. 사용자의 평소 마우스 사용 패턴, 클릭 습관, 클릭 시의 힘의 세기, 클릭과 클릭 사이 시간 등의 여러 사용 패턴을 DB화하여 사용자 행위 기반 아이덴티티를 만든다. (〈그림 2-6〉 참조)

이렇게 만들어진 아이덴티티로 사용자에게 있어서는 매우 단순하고 쉬운 인증 방식을 사용하지만 실제로는 그 사용자가 아니면 시스템과 서비스에 접근이 제한되는 난해한 시스템을 만들 수 있다. 인공지능의 분석 대상은 사용자의 행위 특성, 접근 디바이스 특성 및 세션과 트랜잭션 모니터링 등이다.

인공지능에서 사용자의 이해는 행위 생체 모델을 기반으로 한게 되는데 세션과 트랜잭션에 대한 비정상 행위 식별을 위해 세션을 평가하게 되며, 디바이스 활동을 분석하여 악성코드나 조작된 비정상 앱에 의한 요청인지를 판단하기도 한다. 그리고, 자동적인 보호 활동을 수행을 위해 관련되는 위협 인텔리젼스를 수집한다.

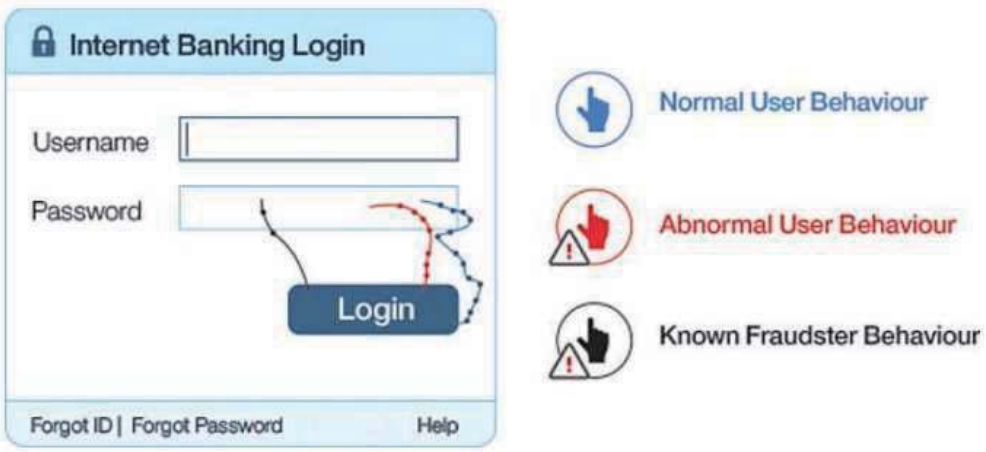
사용자 접속과 세션 정보를 이용해 사용자 아이덴터티를 조심스럽고 자연스럽게 평가하며, 다양한 증거를 기반으로 한 사기 지표(Fraud Indicator)로 행위 기반 생체 분석 결과를 실시간으로 상관 분석한다.



〈그림 2-6〉 사용자 행위 기반 특성 식별 학습 그래프[28]

27) 상게서, pp.8-9.

위의 결과를 토대로 오탐을 줄이고, 탐지 효과의 최대화 및 사용자의 불편을 최소화하면서도 위험을 감소시키기 위한 생체인증을 최적화 기법을 적용할 수 있다. (〈그림 2-7〉 참조)



〈그림 2-7〉 사용자 행위 기반 바이오 식별 정보의 활용의 예

⑦ 취약점 분석

악의적인 공격으로 인한 다양한 침해사고 중에서 응용 계층에서의 침해사고 건수가 가장 많은데 이는 응용 계층의 코드 자체 취약, 테스팅 및 수동 분석 등 문제점이 있어서 사이버 위협에 취약하다.

최근 머신러닝을 기반으로 한 웹 취약점 분석 보안 플랫폼으로 어플리케이션 맞춤형 자동화 테스트 시나리오를 기반으로 취약점을 분석 및 식별하는 솔루션들로 사이버 위협을 해결하는 제품들도 많다.

인공지능과 머신러닝 알고리즘을 적용하여 여러 종류의 애플리케이션 소스 취약점 진단 결과에 대한 자동 분석과 검토를 통해 비지도 학습과 전문가에 의한 지도 학습을 병행하여 분석을 할 수 있으며, 애플리케이션에 대한 초기 개발과 반복되는 취약점 분석에 대해 수정 비용도 절감할 수 있다.

또한, 자동화된 학습을 이용하면 다양한 언어와 프레임워크에 대해 동일한 애플리케이션 취약점 진단이 가능하며, 애플리케이션 취약점 분석을 위해서는 프로그래

28) Trusteer, User Behavior Biometric

밍 언어 이해와 데이터 입출력과 취약점 발견 지점에 대한 정확한 분류로 취약점을 찾아야 한다.

효율적인 결과를 위해서 발견 취약점의 검토, 무의미한 결과와 이중 오탐 제외, 중복된 취약점을 축약하여 최적의 해결방안 제시가 되어야 한다.

이러한 결과가 인공지능에 의해 수초, 수십초 이전에 기대하지 않을 정도로 빠르고, 광범위하게 취약점 진단과 결과에 대한 방안을 제시한다.

실제 머신러닝 기반으로 "프로그램을 진단해 본 결과, 98.6%의 정확도로 프로그램의 구조 파악(데이터 입출력 및 취약점 발현점 탐지) 및 분류를 할 수 있었으며, 98.91%로 오탐을 감소할 수 있다".[29]

인공지능 기반으로 대상 애플리케이션에 대해 취약점 진단, 수정 권고 사항, 불필요 및 중복 탐지 정제에 대해 시험한 결과는 〈표 2-3〉과 같다. 애플리케이션을 포함하여 이와 비슷하게 IT 인프라 전반에 걸쳐서 취약점 탐지와 공격위한 다양한 시나리오를 실행하는 인공지능이 있다.

이들은 이전과 다르게 사이버 무기체계로써 개발되기 위해서 시스템의 보안 취약점을 경고하는 차원보다도 더 강하게 직접 공격하여 증명하는 데 초점이 맞춰지고 있다.[30]

〈표 2-3〉 머신러닝 기반 웹 애플리케이션 취약점 진단 결과

Real-World App;ications	Scan Findings	IFA Vulnerabilities	Fix Groups
App;ocatiom 1	12k	1k	35
App;ocatiom 2	247k	1.2k	103
App;ocatiom 3	746k	483k	42

29) IBM AppScan의 인공지능 모듈인 ICA(Intelligent Code Analytics)와 IFA(Intelligent Finding Analytics) 의 테스트 결과 인용

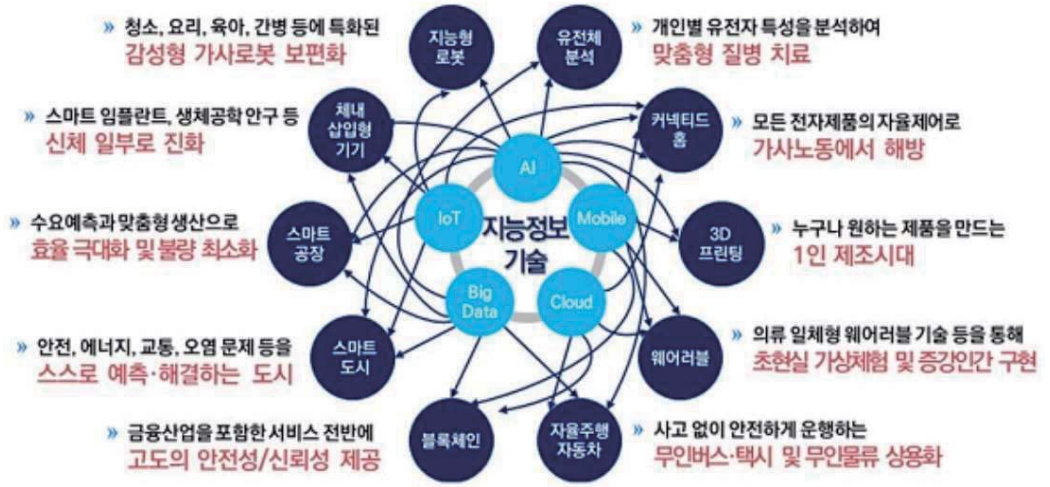
30) 박형근, "정보보안에서의 인공지능 도입 분야와 주요 사업자", 시큐리티플러스, 2018. 12, pp 9-10.

3. 머신러닝 기반의 공격 위협 사례

3.1 인공지능 및 머신러닝 기술

인공지능은 인간의 지능적 능력을 컴퓨터로 구현하는 과학기술이다. 즉 “학습, 문제 해결, 패턴 인식 등과 같이 주로 인간 지능과 연결된 인지 문제를 해결하는 데 주력하는 컴퓨터 두뇌 라고도 한다”.[31]

인공지능의 활용분야도 〈그림 3-1〉에서와 같이 단순히 인지능력에서 벗어나, 인공지능의 머신러닝과 딥러닝을 활용해서 문제를 스스로 학습하고 해결하는 단계를 달성하기 위한 기술 선도를 위해 로봇, 자율주행, 스마트 공장, 스마트 도시. 웨어러블 등 활발하게 다양한 분야에 연구와 투자가 추진되고 있다.[32]



〈그림 3-1〉 인공지능 활용 분야[33]

31) 워키백과 용어정의
32) 이승훈, “최근 인공지능 개발 트렌드와 미래의 진화방향”, LG경제연구원, 2017. 12.
33) 권용현, “AI,지능정보기술의 방향”, 카카오정책산업연구, 2017.4.

세계 각국에서도 사이버보안에 대한 국가 전략을 수립하고 사이버 공격 대응 전략을 추진하고 있다.

미국의 경우 "2018년 9월에 국가 사이버 전략과 2019년 12월에 국가 최상위 사이버보안 연구개발 전략계획을 발표했으며, 영국은 2016년 11월 국가 사이버보안 전략 발표에 이어 2020년까지 사이버 보안에 대한 예산을 2배 확대(총 19억파운드, 2조8000억원 규모)한다는 계획을 내놓았다.".[34]

우리나라도 국가 사이버 안보 계획 수립과 사이버보안 강화 계획을 발표했다. 2019년 9월에 사이버 안보 환경의 변화와 안보 위협 증대에 따라 국가 사이버 안보 기본계획을 관계부처 합동으로 발표했다.

국가 사이버 안보 기본계획은 안전하게 사이버 공간을 구축해 국가 안보와 경제 발전을 뒷받침하고 국제 평화에 기여를 목표로 3가지 비전으로 첫째 국가 주요 기능의 안정적 수행과 둘째 사이버 공격에 빈틈없는 대응, 마지막으로 강건한 사이버 안보 기반 구축을 목표로 설정했다.

또한 이들 비전과 목표에 따라 6개 추진전략과제로 "국가 핵심 인프라 안전성 제고, 사이버 공격 대응역량 고도화, 신뢰와 협력 기반 거버넌스 정립, 사이버 보안 산업 성장 기반 구축, 사이버보안 문화 정착, 사이버 안보 국제협력 선도" 등의 추진이다.[35]

최근에는 국방분야의 사이버보안에서도 공격이 더욱 고도화 및 지능화되고 있어, 이에 대해 정확하게 대응하기가 어려운 상황이며, 이러한 보안위협에 효과적이고 정확하게 대응하기 위해 머신러닝을 주목하고 있으며, 많은 정보보안 제품에서 인공지능의 머신러닝 기술을 적용해서 사용하고 있다.

사이버보안은 전산장비, 모바일 기기 및 전자 시스템과 지능형 네트워크(스마트 차량, 스마트홈) 그리고 수집되는 데이터들에 대한 악의적인 사이버 공격으로부터 보호하는 총체적인 활동으로 승인되지 않은 사용자들의 로그인과 악의적 코드로부터 자산 보호 활동을 말한다. 4차 산업혁명 핵심기술인 A-ICBM의 디지털 발전 및 전환은 사이버 공격에 대한 대상이 증가하는 원인이며, 결론적으로 보면 사이버보안의 중요성과 필요성이 더욱 강조될 것이며, 머신러닝은 공격자·방어자 둘 모두에 사용될 수 있다.

---

34) 정보통신신문(http://www.koit.co.kr)
35) 정보통신신문(http://www.koit.co.kr)

머신러닝을 방어로 활용하기 위해서는 먼저 머신러닝의 단점인 최소화된 오류를 추진해야 한다. 이를 개선하기 위해 비지도(unsupervised learning) 학습기법을 적용하여 효율적이고 정확하게 탐지하고, 지도 학습기법을 사용하여 공격자 의도의 공격을 식별 및 자동 분류하여야 하며, 작동(Operation)과 각종 사이버 위협과 다중 소스와 단일보기(Multi Source But Single View)에 대한 침해 대응의 요소별로 최적화된 알고리즘, 기법 및 학습 방법 지원과 이들을 기술을 활용해 통합이 필요하다.

3.2 인공지능 보안 위협

인공지능은 빅데이터와 머신러닝으로 영상분류, 자연어 처리, 객체 탐지, 실시간 자료 분석 등 다양한 분야에서 관심과 성능을 보여준다. 머신러닝을 활용한 서비스들이 우리 생활에 편리함과 안정을 주는 반면, 역기능으로 많은 보안 취약점을 가지고 있어 인공지능에 대한 보안 위협에도 많은 관심도가 증가하고 있다.

인공지능의 머신러닝 및 딥러닝은 현재 사이버보안의 기술단계를 빠르게 발전시켜, 이를 통해 기관(기업)에 안정적인 업무 환경의 연속성을 보장해줄 뿐 아니라, 효율적으로 인력 및 자산관리가 가능하다는 장점이 있다.

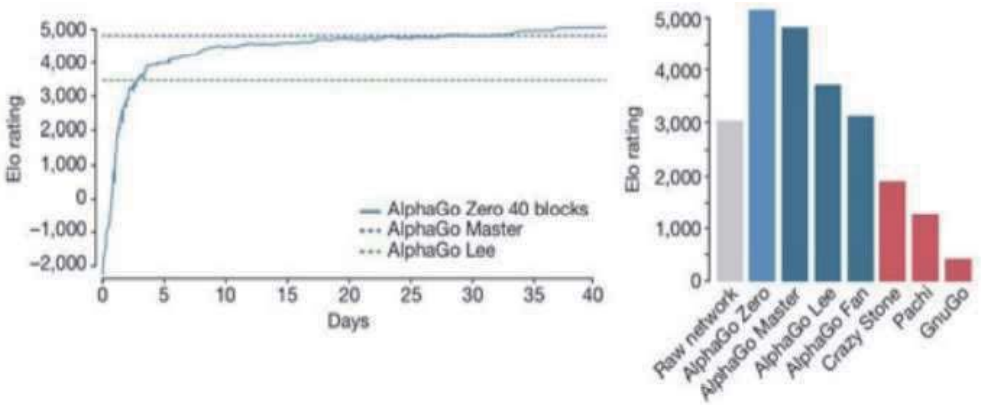
그러나 인공지능을 방어적 측면만을 생각하면 문제가 커진다. 인공지능을 적용하여 창과 방패처럼 공격측과 방어측에 동일하게 기술을 사용할 수 있다. 방어자로서는 인공지능이 여러 종류의 악성코드 공격유형을 머신러닝 기법으로 자동 분류 및 분석을 통하여 대응책을 마련해 주듯이 공격자로서도 운영되고 있는 정보시스템의 보안 취약점에 대해서 지속적으로 탐지하고 공격하여 시스템의 취약점을 탐지해서 공격함으로써 공격자를 효과적이고 안전하게 침입할 수 있도록 도움을 줄 수도 있다.

인공지능의 가장 큰 장점은 스스로 학습하며 진화할 수 있는 것이다. 인공지능 시대를 앞당겨준 알파고는 알파고 마스터로 진화한 후에 최종적으로는 알파고 제로까지 진화했다. 여기서 주목할 점은 기존에 최강이었던 알파고 마스터와 이를 훨씬 능가하는 능력을 갖춘 알파고 제로의 알고리즘이 기본 설계 구조는 같고, 다른 점은 “인간에게 학습했느냐, 하지 않았느냐”에만 차이인데, 결과적으로 보면 스스로 많은 시행착오를 겪으면서 많은 요령들을 터득한 알파고 제로가 더욱 뛰어난

성능을 가질 수 있다는 게 사실이다.

〈그림 3-2〉와 같이 제로상태에서 인공지능의 강화학습 방식으로 누구의 도움도 없이 바둑의 세부적인 원리를 깨우쳤던 알파고 제로는 단기간에 알파고를 능가했고, 약 1달 만에 알파고 마스터의 한계도 넘어섰다.

결론적으로 역기능으로 보면 인공지능은 어느 순간 인간의 도움 없이 스스로 학습하여 다양한 공격 패턴 및 기술을 만들어 낼 수도 있다는 것을 유추할 수 있다. 인공지능 기술의 발전은 방어측의 보안 시스템 강화와 더불어 공격측 시스템의 진화도 함께 된다는 사실을 망각해서는 안 된다는 것이다.



〈그림 3-2〉 인공지능 바둑 프로그램들과의 실력 비교[36]

인공지능에서 발생할 수 있는 보안 위협은 크게 학습단계와 활용단계로 나눌 수 있는데, 학습단계에서 발생할 수 있는 보안 취약점으로 Poisoning, Overfitting, Backdoor 공격이 있으며, 활용단계에서 발생할 수 있는 보안 위협은 적대적 공격(Adversarial attack)이 있다.

이런 공격들은 인공지능 모델이 잘못된 데이터를 학습하여 오동작을 하게 되는데 공격자가 학습 단계에서 공격하기 위해서는 학습 데이터에 대한 접근이 가능해야만 공격할 수 있으므로 공격하기가 쉽지는 않다.

아래에 대표적인 각 단계의 보안 위협에 대해서 제시한다.

36) 김대규, "머신러닝으로 진화하는 보안 위협과 대응", 컴퓨터 월드, 2018. 7.

① **오버피팅**

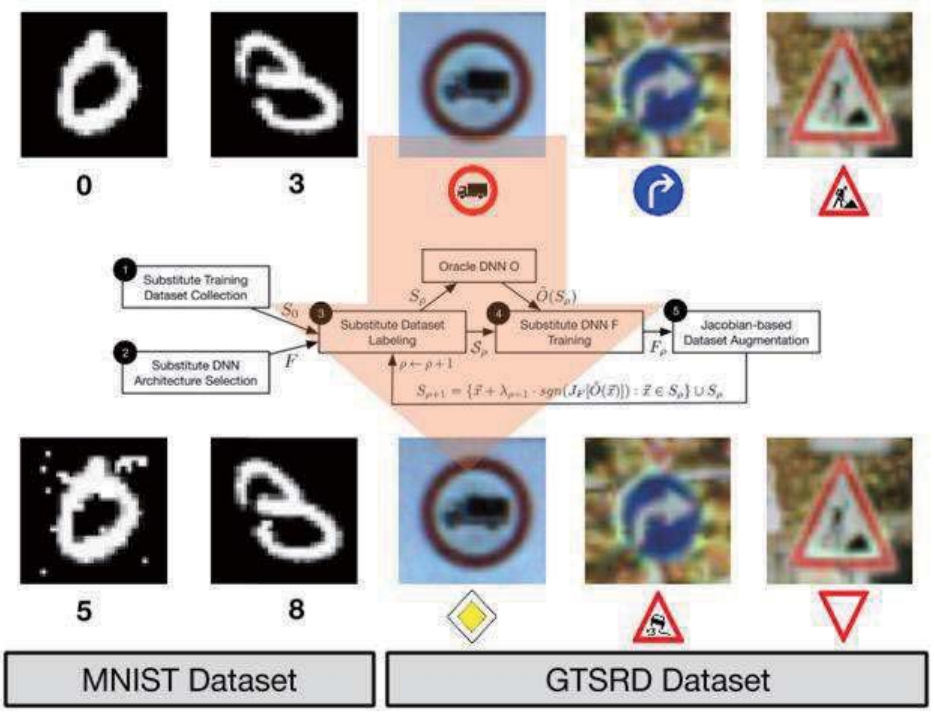
오버피팅(Overfitting, 과적합)이란 지능신경망이 훈련용 데이터만 과도하게 적응되어 일반 데이터에는 올바르게 예측하지 못하는 상태를 말한다.

머신러닝이나 통계학에서 주로 사용되는 용어로 훈련 데이터를 학습하는 모델에서 자주 나타나는 오류이며 원인은 훈련 데이터만 지나치게 학습하다 보니 새로운 데이터 또는 미래 발생할 데이터는 정확하게 예측하지 못해 발생하므로 신경망은 훈련하지 않은 데이터를 학습해도 바르게 식별해야 한다. 오버피팅은 매개변수가 많고 표현력이 높은 모델과 훈련 데이터가 적은 모델의 경우에 일어난다.

〈그림 3-3~4〉가 오버피팅에 대한 예인데 〈그림 3-3〉과 같이 "좌측의 갈색 고양이만 학습한 모델이 우측 검정색 고양이를 보고 고양이라 판단하지 못하는 경우가 대표적인 오버피팅 사례다".

〈그림 3-3〉 오버피팅의 오류 1[37]

37) 김대규, "머신러닝으로 진화하는 보안 위협과 대응", 컴퓨터 월드, 2018. 7.



〈그림 3-4〉 오버피팅의 오류 2[38]

이러한 결과를 이용한 공격기법으로 오버피팅 오류를 악용해 정상 이미지를 시스템에 학습시킨 후 이미지에 변형을 가하기 위해 특별한 기법을 적용시킨 후 이미지를 재인식 시킨 결과 전혀 다른 이미지를 출력하는 결과가 도출됐다. 이는 수많은 데이터를 통해 인증 정확도가 높게 학습된 모델도 결과적으로는 학습된 데이터와 무관하게 어떤 특정된 조건에서는 출력 데이터가 오류가 발생할 수 있다는 사실을 입증했다.

오버피팅 오류를 해결하기 위해서 과거부터 꾸준히 연구가 진행되고 있다. 리스트릭티드 볼쯔만 머신(Restricted Boltzmann Machine)을 통해 학습시킬 신경망의 각 층을 효과적으로 드랍아웃하여 오버피팅을 방지할 수 있다.[39]

38) Nicolas Papernot, 'Practical Black-Box Attacks against Machine Learning'
39) 강대기, "딥 러닝 기반 기계학습 기술 동향", IITP 기획시리즈, 2016.

② 학습 알고리즘 악용

인공지능 알고리즘에 대해 결과적으로 편견과 차별로 문제를 일으켰던 사례로 학습 알고리즘을 악용해 2016년 마이크로소프트에서 머신러닝 기반 스스로 학습 능력을 보유한 테이 챗봇을 공개했다. 테이 챗봇의 개발 목적은 정상적인 사용자들과의 대화를 통해 학습하려고 개발됐지만, 실제로는 부정적으로 사용하는 사용자들과 대화를 통해 성/인종차별, 히틀러 옹호, 욕설 등을 학습하도록 유도되어서 문제점을 일으키게 되었다. 어떠한 배경지식이나 판단 기준이 없는 상태로 시작했다가 결국 16시간 만에 서비스가 종료되었는데 역시 준비되지 않은 인공지능 알고리즘이나 서비스가 이렇게 큰 국가적 인종차별로까지 확대될 수도 있는 사례이다.

③ 적대적 사례 제작

머신러닝 모델의 학습에는 많은 수의 학습 데이터가 활용되지만 단순하게 생각할 때 방대한 양의 데이터로 학습되었다고 해서 학습모델의 안전을 보장할 수 없으며, 아무리 다계층으로 구성되고 복잡한 구조를 가진 인공신경망이라 해도 얼마든지 간단한 트릭으로 우회나 속일 수 있다.

적대적 사례는 원본 데이터에 대해서 최소한의 노이즈 추가로 생성되며 사람이 문제점에 대해서 발견할 수가 없지만 머신러닝에 의해서 잘못 오인식되는 데이터를 의미한다. 적대적 사례는 인공지능 분야와 사이버보안 분야에서 관심을 받고 있으며 텍스트, 음성, 이미지 등에서 활발하게 연구가 진행 되고 있다.

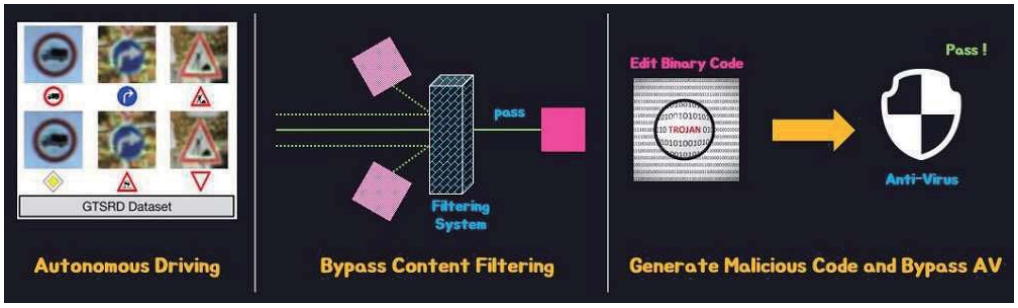
적대적 사례 제작은 원본 데이터에 오인식하도록 이미지에서 특정 부분만 변조하여 사람이 보기에는 문제가 없지만 머신러닝 모델에 의해서 잘못 오인식하게 하는 것으로 목표 모델에 여러 번의 질의(쿼리) 통해서 최적의 노이즈를 이용하여 모델에게 오인식을 일으키게 하는 샘플을 생성하게 한다.

예를 들어 이미지나 영상 등을 학습해 입력된 이미지가 사물인지 사람인지 판별하는 모델에서 사용자가 사물 이미지를 입력하게 되면 머신러닝 모델은 '사물'이라고 판별할 것이다. 여기서 만약 사물 이미지를 입력한 결과값을 '사람'으로 판별하게 속이려면 공격자는 입력 이미지의 픽셀을 조작해서 입력에 대응하는 출력값을 벡터 공간에 대응시켜서 출력값이 기준선으로부터 거리 차이, 방향성 및 이동에 대한 계산이 가능하다면 단순 픽셀 조작만으로도 결과값을 변경할 수 있다. 즉 사용자가 보기에 입력 이미지는 분명 '사물'이지만 머신러닝 모델이 보기에는 사물이

아닌 '사람'으로 보이도록 속일 수 있다.

〈그림 3-5〉 적대적 사례 제작 1[40]

이러한 적대적 공격 사례를 조금 더 응용하게 된다면 단순하게 이미지에 대한 결과값을 바꾸는 것보다 더 위험하게 적대적 사례 제작에서 콘텐츠 필터링 무력화, 교통 표지판 인식 오류 또는 안티 바이러스 제품 무력화 등에 악용될 수 있다.



〈그림 3-6〉 적대적 사례 제작 2[41]

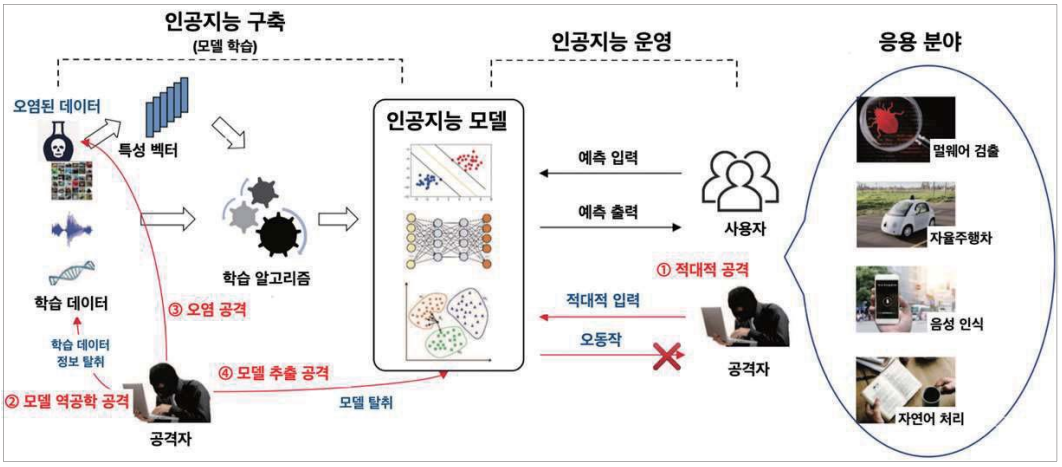
40) 김대규, "머신러닝으로 진화하는 보안 위협과 대응", 컴퓨터 월드, 2018. 7.
41) 상게서, pp 9-10.

4. 국방 사이버보안 영역에서의 머신러닝 기반의 공격 위협 모델과 관련 공격기술

4.1 사이버보안 영역의 머신러닝 기반 공격 위협 모델

사이버 영역을 국방 사이버 영역으로 한정해서 공격 위협 모델을 선정하기에는 제한사항이 있는 것 같으며, 머신러닝 기반의 보안 위협 모델은 특히 영역 구분없이 적용이 되고 있다.

사이버보안 머신러닝 기반의 공격 위협에 대해서 〈그림 4-1〉과 같이 ① 악의적으로 왜곡된 적대적 입력으로 오작동을 유발하는 적대적 공격, ② 반복된 질의의 출력을 역산하여 학습데이터 정보를 탈취하는 모델 역산 공격, ③ 학습데이터에 오염된 데이터를 삽입하여 모델의 오염을 유도하는 오염공격과 ④ 반복된 질의를 통해 모델 정보를 역산하여 탈취하는 모델 추출 공격이 있다.



〈그림 4-1〉 머신러닝 기반 공격 위협 모델

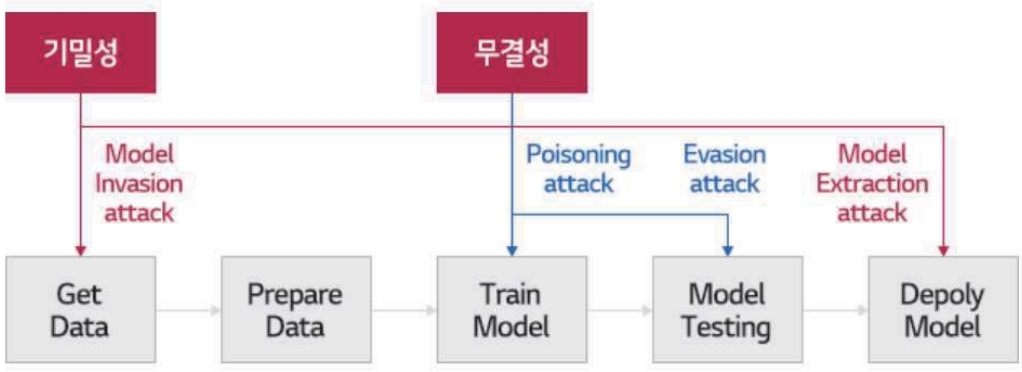
① 적대적 공격(Adversarial Attack)

적대적 공격은 머신러닝 모델의 높은 분류 정확도에도 불구하고 영상에 대한 분류 및 예측 결과를 완전히 변경할 수 있는데, 공격받은 모델은 잘못된 예측 결과에 대해 높은 신뢰도(confidence)로 확신해서 보고하게 된다.

머신러닝 모델은 컴퓨터 비전 분야에서는 정확도가 대단히 강하지만 이미지 분류에서는 약점을 보이고 있는데, 인간의 눈으로는 거의 확인할 수 없는 수준의 미세한 교란 신호가 입력 영상에 추가되는 것만으로도 영상의 분류가 달라지는 등 놀라울 정도로 머신러닝 모델이 취약하며, 적대적 공격에 이용된 변형된 영상을 적용하여 다양한 네트워크 분류 모델들을 동일한 메커니즘으로 속일 수도 있다.

새로운 적대적 공격은 머신러닝 알고리즘이 가지고 있는 취약점을 이용했다는 점에서 차이가 있으며, 머신러닝으로 하여금 엔진 자체가 잘못된 판단을 하도록 유도하는 공격 방식이다.

머신러닝 모델에서 〈그림 4-2〉에서와 같이 적대적 공격을 기밀성과 무결성 공격으로 구분하는데, 무결성 공격으로 초기 학습에서 악의적인 학습 데이터를 주입해 모델을 중단시키는 오염 공격(Poisoning Attack), 역공학으로 머신러닝 모델이나 학습 데이터를 탈취하는 모델 추출공격(Model extraction attack), 추론 과정에서 데이터를 교란하게 시켜 속이는 회피공격(Evasion attack)과 학습 데이터에 대한 추출 공격(Inversion attack)이 있다.

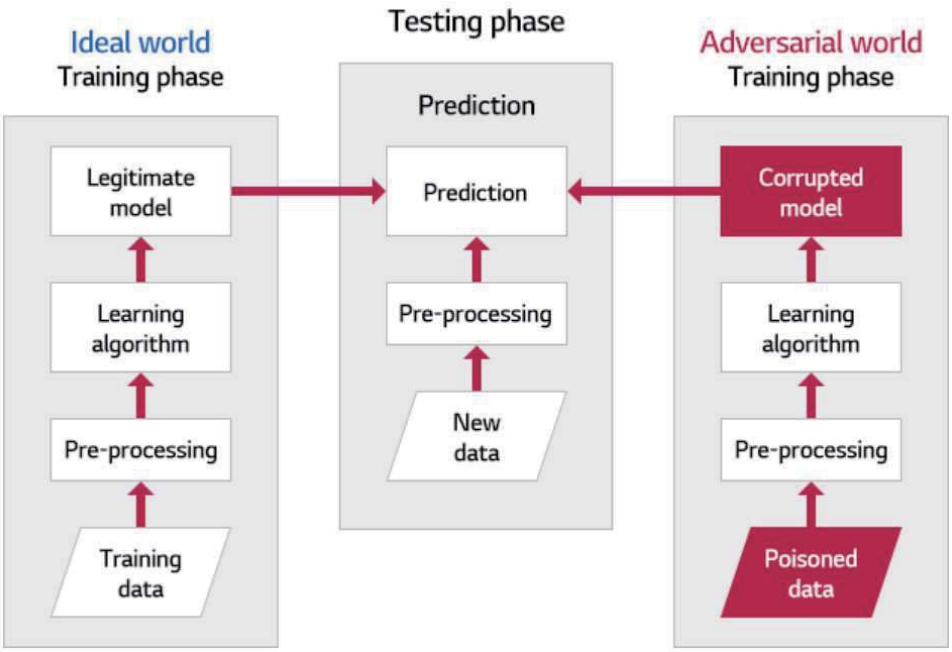


〈그림 4-2〉 머신러닝 기반 적대적 공격 유형

② 오염 공격(Poisoning Attack)

오염공격은 〈그림 4-3〉에서와 같이 의도적으로 악의적인 공격자가 학습데이터를 위·변조하여 주입해 머신러닝 모델을 망가뜨리는 공격을 말하는데 다른 머신러닝 공격 기법과 다른 점은 모델 자체를 공격해서 모델에게 영향을 준다는 것이다.

오염공격은 악의적인 데이터를 최소로 주입해 모델 성능을 망가뜨리는 것이 오염공격 평가 기준이 되며, 의료 분야에서 기계를 대상으로 오염공격 결과에서 장비의 오작동을 발생시키는 것을 확인했다.



〈그림 4-3〉 오염공격 기법

또한 오염공격의 사례로 〈그림 4-4〉에서와 같이 마이크로소프트사가 인공지능 챗봇 테이(Tay)를 공개하였다가 16시간 만에 운영 중단을 했는데. 악의적인 성향의 사용자들에 의해 테이가 욕설, 성/인종차별, 부정적인 정치적 발언을 학습해서 남발했기 때문이다.

〈그림 4-4〉 차별 발언중인 Tay[42)]

③ **회피 공격**(Evasion Attack)

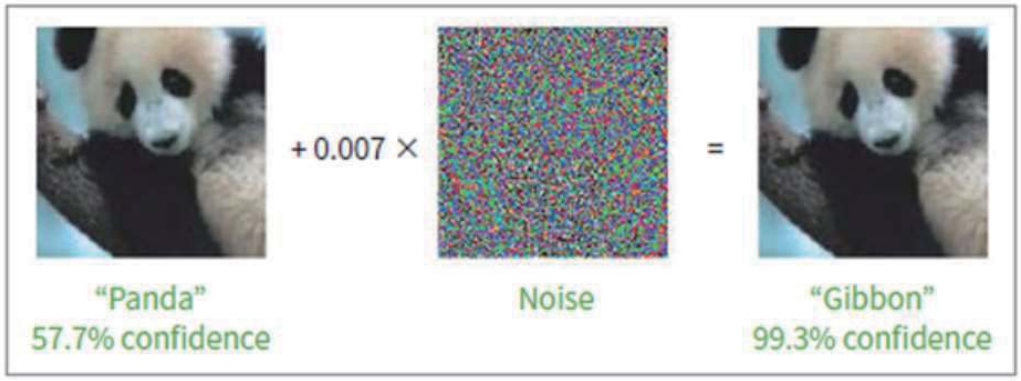
오염공격이 머신러닝 모델의 학습에 직접 관여 모델 자체를 망가뜨리기 위해 공격하는 개념이라면 회피 공격은 입력 데이터에 최소한의 교란으로 모델을 속이는 기법이다.

머신러닝 기법을 이용하여 이미지를 분류하는데 사람의 눈으로는 알 수 없을 정도로 이미지를 변조시켜서 머신러닝 모델이 착오하도록 만드는 수법이다.

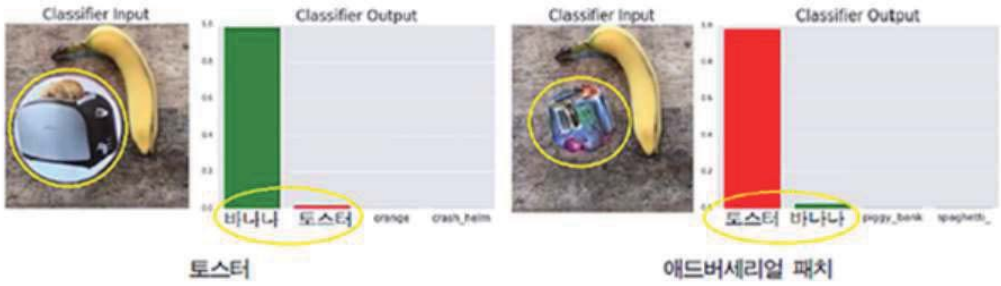
회피 공격에 의해 〈그림 4-5〉와 같이 팬더 이미지에 미세하게 분간이 힘든 노이즈를 추가하면 머신러닝이 이를 다른 동물인 원숭이로 착각하게 만드는 것이 가능하다.

〈그림 4-6〉에서와 같이 "적대적 스티커(Adversarial patch)를 바나나 옆에 붙이면 이미지 인식 앱이 바나나를 100% 확률로 토스터 기기로 인식했다. 적대적 스트커는 누구나 쉽게 인쇄해 사용할 수 있고 악의적인 공격인지 쉽게 발견하기 어려워서 악용되는 경우 크게 문제가 될 수도 있다".

42) Tay twitter catpure



〈그림 4-5〉 회피 공격 예시[43]



〈그림 4-6〉 적대적 스티커를 붙인 경우 결과 비교[44]

④ 전도 공격(Inersion Attack)

전도 공격은 모델에 수많은 질의(쿼리)를 해서 산출된 결과값을 분석해 머신러닝 모델에 학습하기 위해 사용될 데이터를 추출하는 공격이다.

〈그림 4-7〉에서처럼 전도 공격을 이용하면 얼굴인식을 위해 머신러닝 모델의 학습에 사용했던 얼굴 이미지 데이터에 대해서 복원도 가능하다.

머신러닝에서 데이터 분류는 부여된 입력 데이터 분류 결과와 신뢰도에 대해 함께 출력하게 되는데, 전도 공격은 결과값을 분석해 학습 과정에서 주입된 데이터를 복원하는 방식이다.

만약 머신러닝의 학습데이터에 군사적으로 중요한 군 기밀정보나 인사정보, 민감

43) Lan G., Joonathan S. and Christian S., "Explaining and harnessing adversarial examples", 2014
44) https://youtube/i1sp4X57TL4

정보 등이 포함된 경우라도 전도 공격을 이용하면 유출될 가능성이 존재한다.

〈그림 4-7〉 실제 학습데이터(우), 전도 공격 이미지(좌)[45]

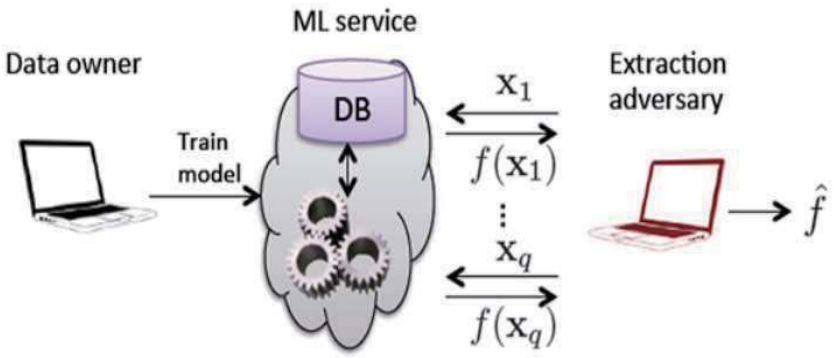
⑤ 모델 추출 공격(Model extraction Attack)

전도 공격이 결과 값을 분석해 학습 과정에서 주입된 데이터를 복원하는 방식의 공격이라면, 모델 추출 공격은 머신러닝 모델을 추출하는 공격이다.

전도 공격과 동일하게 머신러닝 모델을 쿼리를 계속 던지면서 결과값을 분석하는 방식의 공격이며, "이 공격 방법으로 70초 동안 650번 쿼리만으로도 아마존 머신러닝 모델과 유사한 모델을 만들어 내는 것이 가능하다".

모델 추출 공격은 〈그림 4-8〉에서와 같이 머신러닝 모델 서비스(MLaaS : Machine Learning as a Service)를 탈취하거나, 전도 공격, 회피 공격과 같이 2차 공격을 위해서 사용될 수 있다.

45) Matt Fredrikson,et.al, "Model Inversion attack that Exploit Confidence Information", CCS'15.



〈그림 4-8〉 모델 추출 공격[46)]

4.2 국방 사이버보안 영역의 머신러닝 기반 공격기술

① 악성코드

사이버보안 영역의 머신러닝 기반 공격은 해마다 기하급수적으로 증가할 뿐 아니라 사회 기반 시설이 모두 인터넷 기반이 되면서 피해가 사이버 영역뿐만 아니라 우리의 생활 전반에 큰 위협이 되고 있다. 마찬가지로 국방분야에도 예외는 아니다. 대부분의 사이버 침해 공격은 악성코드를 이용하고 있으며, 빠른 속도로 지능화된 형태로 발전하고 있다.

악성코드는 일 평균 200만개를 넘어서고 있는데 끊임없이 발생되는 대량의 악성코드를 대응하기 위해서는 머신러닝 기반의 자동화된 악성코드 분석기술이 매우 중요하다.

악성코드 분석기술의 결과물은 지능화 형태로 진화하는 악성코드에 맞춰서 보안 솔루션들을 실시간 또는 주기적으로 업데이트하고 이를 통해서 사전에 보안사고 대응, 예방 및 차단할 수 있어야 한다.

또한 악성코드 분석을 위한 목적으로 지능화된 형태로 나타나는 보안 위협에 대해서 사전 차단 및 대응에 있으며, 세부적으로 7개로 분류할 수 있다.[47)]

---

46) Florian Tramer et.al, “Stealing MAchine Learing Models via Prediction APIs”, usenix, 2016

47) Ucci, Daniele, Leonardo Aniello, and Roberto Baldoni. "Survey on the Usage of Machine Learning Techniques for Malware Analysis." arXiv preprint arXiv:1710.08189 (2017).

〈표 4-1〉 악성코드 분석 기법

분류	분석 내용
Malware Detection	- 파일이 악성인지 아닌지 판단결과 도출 - 악성코드 분석의 가장 기본적이면서 중요한 목적 - 악성코드의 다양한 생태계에서 다양한 요소기술 필요 - 악성여부 판단을 잘해서 보호하고자 하는 시스템 보호
Malware Variants Detection	- 기 제작된 코드를 활용하여 악성코드 재작 비용이 저렴 - Variants Selection과 Families Selection
Malware Development Detection	- 결과적으로 지향하고 있는 주요 핵심행위 (Prominant Behavior)와 목적(Objectives) 기준분류 - 복잡한 설계의 악성코드라도 이미 식별 및 분류된 Category에 대한 지식이 있다면, 대단히 분석에 유용한 방향성 제공
Malware Category Detection	- 2개의 파일에서 무엇이 유사한 부분인지, 무엇이 다른 부분인지 코드레벨에서 자동 분석
Malware Novelty and Similarity Detection	- 분석대상 파일의 공통된 부분을 식별하고, 그대로 의미를 부여할 수 있는 부분
Malware Development Detection	- 기존 분석된 지식에 없던부분을 모두 식별하고 의미를 부여하는 방식
Malware Attribution	- 공격자에게 장점은 신규 제작된 악성코드가 얼마나 방어 기술을 회피할 수 있는지 널리 쓰이는 Anti-Virus, Sandbox, On-line Scanning Service 등을 통해 사전 시험

머신러닝 기반으로 악성코드를 제작된 사례는 2017년 “GAN 기반의 블랙박스 공격을 위한 적대적 악성코드 예제 제작”이라는 논문을 통해 소개됐다. 이 논문에서 머신러닝 기반 탐지 시스템을 우회하는 적대적 악성코드 샘플을 생성하는 알고리즘을 기반으로 생성적 적대 신경망(generative adversarial network)을 구축하는 방법을 공개했다.

② 데이터 공격(Data Attack)

해커들의 공격 대상 중에 머신러닝 모델 학습에 활용되는 데이터도 포함이 된다고 미국 표준기술연구소 예하 정보기술 연구소 수석 연구원 엘햄 타바시(Elham Tabassi)가 말했다.

데이터 공격은 학습 데이터셋을 조작해, 훈련된 모델의 행동을 예상해서 제어하는 공격 행위이다. 해커들은 데이터 공격 과정에서 백도어를 활용해 머신러닝의 모델을 설계자가 알아차리지 못하는 알고리즘을 몰래 삽입한다. 결과적으로 머신러닝 모델이 훈련 데이터를 잘못 분류하도록 유도를 하는 것이며, 연구 결과에 따르면, "트레이닝된 데이터 중 3%만 해킹 공격을 당해도 업무수행 정확도가 11%가 감소한다고 했다".

타바시는 "데이터 공격이 특정한 모델에서 다른 모델로 이관될 수 있다고 설명했다". 이를 근거로 기업들이 안전성을 보장할 수 있는 데이터 품질의 표준과 가이드라인 제정을 하게 되는 것이다. 국가 차원에서 미국 표준기술연구소에서 인공지능의 신뢰성 확보를 위한 가이드라인을 제작 중이라고 했다.[48]

③ 생성적 대립 신경망(GAN)

GAN은 두 개의 시스템으로 구성되는데 하나는 확률 분포를 학습하는 생성모델과 다른 하나는 서로 다른 집합을 구분하는 판별모델로 대립한다. 생성모델은 판별모델을 최대한 속이도록 가짜 예제를 만들고, 판별모델은 생성모델이 생성한 가짜와 실제 예제를 정확히 구분하도록 훈련을 받는다. 이러한 과정을 거쳐, 콘텐츠 생성을 해서 두 개의 대립하는 시스템이 함께 신뢰할 수 있도록 한다.

디지털 가디언의 최고 정보보안 책임자인 팀 반도스(Tim Bandos)는 "해커들이 GAN을 이용해, 민감한 데이터를 순식간에 추출할 수 있다고 설명한다". 이때, 해커들은 트래픽 패턴을 모방하고 시스템 주위를 분산시켜 해킹 공격을 감지하지 못하도록 한다.

그는 "GAN을 악용한 해킹 공격에서 민감 데이터가 노출되는 시간은 30~40분이다. 해커들이 인공지능과 머신러닝을 한차례 공격하면, 이후 인공지능이 자동으로 해킹 공격을 개시할 수 있다. 따라서 사이버보안에 활용되는 인공지능 알고리즘은 수시로 훈련해야 한다"라고 말했다.

48) 코딩월드뉴스(https://www.codingworldnews.com)

GAN에서는 민감정보 유출 외에도 악성코드(멀웨어) 감지 방해, 패스워드 조작, 안면 인식 방해 과정에도 악용되기 쉽다.

④ 스마트 봇넷

4차 산업혁명 기술의 발전으로 자율 학습분야에 있어서 '스웜봇(Swarmbots)'과 '하이브넷(Hivenets)'의 집중이 예상된다. 이는 지능형 IoT 기기가 취약한 시스템을 공격하는 데 사용될 수도 있다는 것이다.

IoT 기기는 Ad-hoc 네트워크 개념으로 서로 통신하고 공유되는 엣지 지능을 바탕으로 작업을 수행한다. 좀비는 더 스마트해져서 지시를 하는 봇넷과 관계없이도 동작할 수 있다. 때문에 하이브넷은 스웜으로 급격히 성장하면서 다수의 목표물을 동시에 공격하고 보안 대책들을 지연시킬 수 있는 역량을 강화하게 될 것이다.

하이브넷은 스웜 기술을 사용해 과거 행동을 이용해 자율 학습이 가능해진다. 머신러닝의 하위 분야인 스웜 기술은 자율적 또는 인위적으로 분산된 자기 조직적 시스템과 함께 동작하며 로봇이나 드론에 사용되고 있다.

⑤ 스피어피싱 메일 공격

스피어피싱이란 창으로 찌르다는 스피어(Spear)와 사용자를 속이다를 의미하는 피싱(Phishing)의 합성어로 개인이나 조직에 대해서 은밀히 염탐하여 개인이나 조직에서 중요정보를 탈취하기 위해 유도 이메일로 위장한 악성 메일을 전송하여 메일 감염을 시킨 후 원격제어 및 정보 탈취 등을 시도한다.

역기능인 머신러닝의 명확한 능력 중 하나는 지능적인 소셜 엔지니어링을 위해 음성 인식, 텍스트-음성, 자연어 처리(NLP)와 동일한 알고리즘을 활용하는 것으로 반복적인 GAN을 통해 소프트웨어에 정교한 작문을 학습시킬 수 있서 피싱 이메일도 더 정교함과 교묘함을 가질 수 있다.

머신러닝 모델의 자동화 프로세스를 이용해서 대규모 목표를 겨냥하는 지능형 스피어피싱 이메일의 성능을 강화할 수 있다. 악의적인 집단에서 머신러닝을 이용해서 대량의 데이터를 훔쳐서 기록분석 및 잠재적 공격 목표를 식별하고 목표에 대해서 효과적으로 공격하는 정상적인 내용으로 이메일을 작성할 수도 있다. 이런 시스템은 정상 이메일을 이용해서 학습하고 설득력 있는 문장 작성도 가능하다.

예시로 존 세이무어와 필립 툴리의 논문에서 “소셜엔지니어링용 데이터과학의

무기화: 트위터에서 자동화된 E2E 스피어피싱"을 확인할 수 있다.

이 논문에서 타겟을 특정 사용자로 한 피싱 게시물을 SNS에서 반복적으로 하는 신경망 학습 방법을 제시했다. 또한 스피어피싱 펜 테스팅 데이터에 대해 학습을 한 SNAP_R 신경망은 목표 사용자의 타임라인 게시물에서 수집한 주제를 동적 입력으로 높은 클릭 가능성을 높여서 대량 피싱과 수동 스피어피싱의 결과가 향상됐다.

⑥ 머신러닝 엔진 중독

머신러닝 엔진 중독은 오염공격과 마찬가지로 공격자의 입장에서 머신러닝을 공격에 사용하기 위해 악성코드 탐지를 위해 사용되는 머신러닝 엔진을 중독시킨다.

머신러닝 모델의 라이프사이클은 입력 데이터를 학습하여 결과 데이터를 만드는데, 데이터 풀이 중독되면 출력 결과도 중독된다. 미국의 뉴욕 대학에서 CNN(Convolutional Neural Networks)을 적용해 학습한 후 잘못된 결과를 출력하도록 CNN을 백도어로 작동시키는 방법을 소개했다.

5. 머신러닝 기술에 대한 대응방안

5.1 통합보안관제체계 운영

머신러닝 기반 보안사고 대응체계는 실시간으로 정보자산 전체에 대한 모니터링이 수반되어야 하며, 침해의 징후에 대해서 끊임없이 추적과 분석이 필요하다.

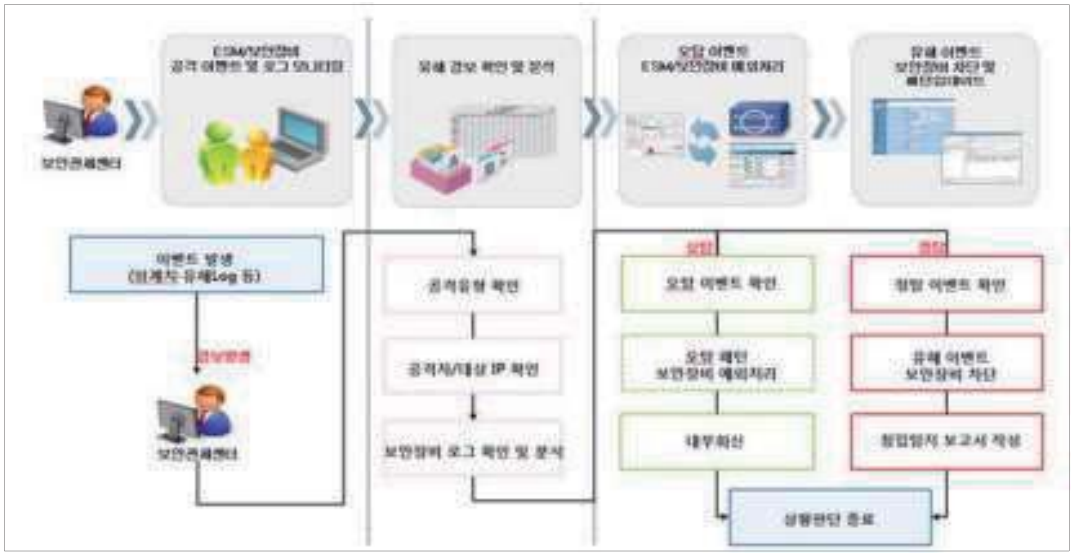
보안관제 대응 업무 프로세스는 〈표 5-1〉에서와 같이 예방, 관제, 대응 및 분석 체계의 유기적 순환구조인 보안관제체계와 탐지되는 새로운 위협에 대해 빅데이터 분석의 전처리를 적용해 범위 및 속도 향상을 하고 정상적인 학습모델을 적용해 비정상 행위 식별로 인해 알려지지 않은 위협에 대한 대응이 필요하다, 또한 머신러닝을 활용하여 분석 능력 강화와 최신 위협 정보에 대해 수집을 해야 한다.[49]

〈표 5-1〉 보안관제 대응 업무 프로세스

구분	주요 내용
예방	• 서비스/시스템/보안정책 보안 대응 수준 유지 강화 • 신규 위협정보 수집체계 기반의 공격 사전예측 서비스 • 위험평가 분석 서비스 제공
관제	• 보안대응 시스템 보안 수준 강화 • 접근통제 강화를 통한 사고예방 기능 강화 • 신규 보안정책 생성 및 권한 정책 변경사항 반영
대응	• 정상기반 이상행위 탐지와 잠재적 위협 탐지 서비스 • 사이버 위협 우선순위 부여 및 대응 • 노출된 위협요소 격리 및 차단
분석	• 외부 위협 인텔리전스를 활용한 침해 정밀분석 서비스 • 보안 정책 적용 자동화와 긴급 보안 정책 Push 기능 제공

49) 정기문, 박학수, “침해위협 상관분석 기반의 보안관제 시스템 설계,” 한국컴퓨터정보학회, 제19권, 제2호, pp.335-337, 2011

〈그림 5-1〉의 이벤트 대응 프로세스는 ① 관제시스템을 통한 실시간 경보 모니터링, ② 이밴트 상세 분석(IP(출발/목적지) 정보, 공격유형, 탐지규칙), ③ 정·오탐 분석(페이로드(Payload)), ④ 유해 IP 차단(방화벽 또는 정보보호 시스템), ⑤ 보고서(침입탐지) 작성 후 사건은 종료된다.[50]



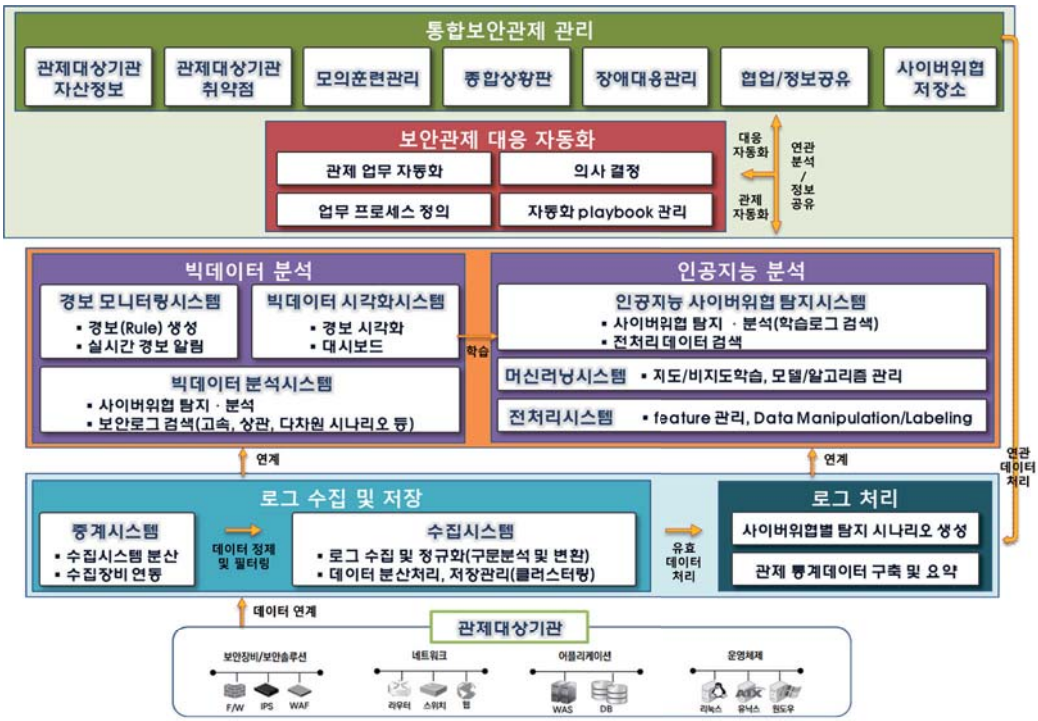
〈그림 5-1〉 이벤트 대응 프로세스[51]

국방분야 차세대 자동화 기반의 지능형 보안관제시스템을 원활하게 구축하기 위해 〈그림 5-2〉와 같이 빅데이터 분석 및 인공지능, 보안관제 대응 자동화, 통합보안관제 관리를 단일 플랫폼으로 구성하며, 이를 통해 사이버안전센터 업무 기능 간 제약없는 데이터 상호 연계·참조, Drill-Down을 구현하여야 한다.

보안 빅데이터는 센터의 관제시스템과 관제 대상 기관의 보안장비에서 발생한 로그를 중계시스템을 통해 수집 연동 및 분산 구성하며, 수집한 로그를 구문 분석과 변환을 통해 정규화하고 데이터 분산 처리와 저장 관리를 위한 클러스터링 구조의 수집시스템으로 구성하여야 하고, 빅데이터 분석은 보안 로그의 실시간 고속 검색과 상관 분석, 다차원 시나리오 기법 등 다양한 검색 기능 및 사이버 위협 탐

50) 홍준력, 이병엽, "인공기능기반 보안관제 구축 및 대응방안", 한국콘텐츠학회논문지, Vol. 21, No. 1
51) http://www.igloosec.co.kr/BLOG_SIEM을 통한 경보 설정과 이벤트 대응

지 분석의 빅데이터 분석시스템과 경보 설정, 실시간 경보 알람의 경보 모니터링 시스템, 경보 시각화 및 대시보드를 위한 빅데이터 시각화 시스템으로 구성해야 한다.



〈그림 5-2〉 통합관제체계 구성도

인공지능 분석은 수집된 데이터 추출을 위한 전처리, 학습을 위한 알고리즘과 모델 관리, 사이버 위협 탐지 분석과 검색 기능으로 구성하고 모델 관리를 위해 데이터 선택 및 모델 생성, 생성된 모델을 적용하는 단일화된 프로세스 및 마법사 기능이나 워크플로우 형태의 직관적인 UI를 통해 사용자 편의성을 제공해야 한다. 직관적인 모니터링을 위한 UI 및 사용자 피드백 기능을 구현하고 매뉴얼로 관리하거나 사용자에 따라 차이가 있는 관제업무 프로세스를 사이버 위협별 대응 업무관리를 위한 플레이북으로 통합 관리해야 한다.

수집된 로그 및 분석결과를 바탕으로, 플레이북 구성을 통해 사이버 위협의 분석 및 대응을 자동화하기 위한 보안관제 프로세스 자동화 WorkFlow 처리 기능을

구현하고 사이버사령부 상황센터↔관제대상기관 간 관제 대응 업무 및 사이버 위협정보, 기관 관제대상 자산 및 보안담당자 현황, 모의훈련 및 사이버교육 정보, 기관 작업 및 장애 처리 등 정보 공유는 상황판 및 게시판을 이용한다.

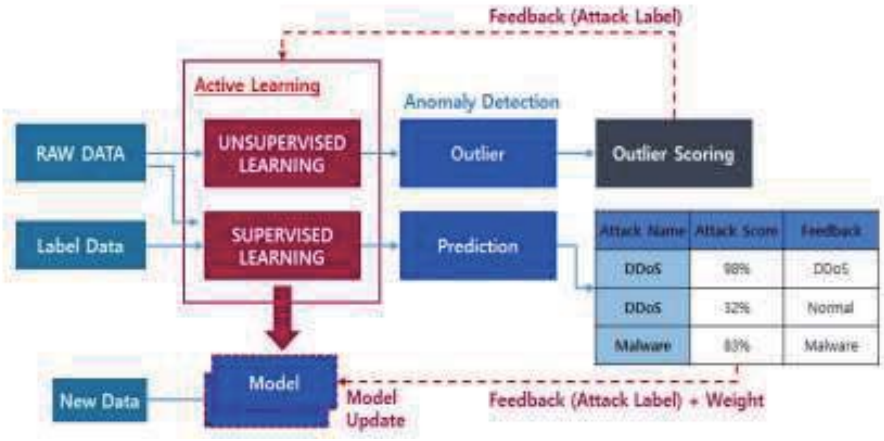
5.2 해킹 침해사고 대응방안

APT(Advanced Persistent Threat) 공격기법은 해커들이 오랜 시간 동안에 지능적이고 지속적으로 목표물을 설정해서 공격하는 기법이며, 해킹 침해사고의 대표적인 공격기법이다.

APT의 프로세스는 침입, 침투, 공격 프로세스로 단계별로 진행한다. 먼저 1단계의 침투 프로세스는 해커는 목표 대상의 관련된 정보를 조사하는데 악성 메일 제작 배포해서 사용자들이 수신된 메일을 열어볼 수 있게 하려면 관심 주제를 메일로 작성해서 메일에 악성코드를 침투시키는 것이다. 2단계는 잠입으로 목표시스템에 접속해서 목표물에 침투한 후에 악성코드를 해커의 지시로 2차 감염 프로세스는 새로운 패턴 및 유형의 악성코드를 지속해서 유입시키는 것이다. 3단계의 공격 프로세스는 해커가 필요로하는 정보 탈취를 위해서 백도어(Back door)를 설치해 시스템 및 보안 관리자에게 들키지 않고 장기간 공격을 수행한다.

해킹 침해사고의 대표적인 APT공격에 대응방안으로 보안전문가는 인공지능 기반 선순환 구조의 〈그림 5-3〉의 Active Learning 기술로 빅데이터 분석에서 발생하는 대용량의 보안 이벤트와 Log 중 라벨링 이전의 데이터를 효율적인 학습에 필요한 데이터를 보안담당자에게 요청을 하고 보안담당자는 요청에 의해 라벨링된 데이터를 머신러닝으로 학습에 적용한다면 보안전문가의 지식과 인공지능의 학습으로 APT기법에 의한 해킹 공격에 대응이 가능하다.[52)]

52) 김규일, 보안관제 효율성 제고를 위한 실증적 분석 기반 보안이벤트 자동검증 방법, 한국과학기술정보연구원, 2014.



〈그림 5-3〉 Active Learning Architecture

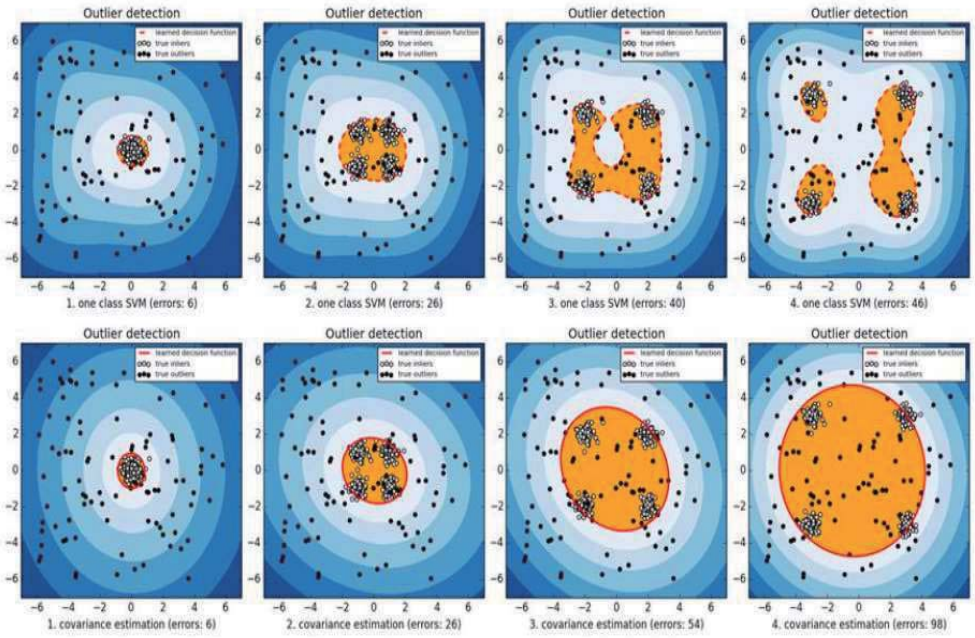
5.3 네트워크 침입탐지 대응방안

IDS(침입탐지시스템) / IPS(침입방지시스템)를 이용하여 네트워크의 침입 탐지에 대해서는 등록된 탐지 정책을 적용하여 네트워크 패킷이 정상인지 공격인지를 판별한다. 여기에 머신러닝 기술을 활용하면 네트워크에서 발생하는 트래픽 분석으로 비정상 행위 탐지 방식[53]을 사용할 수 있다.

예시로 평시에는 ○○ 부대 네트워크의 트래픽 변화가 부대원들이 출근 이후부터 점차 증가한다. 그러나 어느날 갑자기 부대원들이 출근 전에 갑자기 부대내 네트워크 트래픽이 증가하는 등 평소보다도 증가한 트래픽 탐지가 감지된다면 이는 네트워크 침입 등의 비정상 행위로 간주해 시스템이나 보안담당자에게 문자전송이나 경고이벤트로 전파를 하게 된다.

물론 탐지 정책(기준선 설정 등)에 따라 탐지율에 차이가 있을 수 있지만, 결과적으로는 비정상 행위 탐지 방식으로 기존에 알려지지 않은 새로운 네트워크 침입 공격에 대해서 신속한 탐지로 대응할 수 있다.

53) "정상적인 트래픽 데이터에 대해 학습을 통해 정상, 비정상을 구분할 수 있는 기준을 세우고 향후 수집된 트래픽이 기준으로부터 얼마나 차이가 있는지 측정하는 방식"



〈그림 5-4〉 비정상 행위 탐지

5.4 악성코드 침해사고 대응방안

정보보호 침해사고 대응지침은 “정보보호 침해사고에 의해 중요자료 유출 및 정보자산의 손실, 절도, 파괴 등으로 정상적인 업무수행에 지장을 초래하는 사고 발생 시 신속하게 대응하고, 그 과정을 기록 관리함으로써 정보보호 침해사고에 효과적으로 대응하는 것”을 목적으로 한다.[54]

국가기관들은 물론 일반기업들도 정보보호 침해사고 대응지침을 작성하여 활용하고 있으며, 대응절차는 〈표 5-2〉의 공격유형에 따라 〈표 5-3〉과 같이 대응절차에 의거 대응한다.

54) “정보보호 침해사고 대응지침”, 통계청예규 제78호, 2015. 5. 18.

〈표 5-2〉 공격유형

구분	내용
악성코드 공격	컴퓨터바이러스, 웜, 스파이웨어, 백도어, 트로이목마, 봇(BOT) 등이 악의적인 목저으로 컴퓨터에 침입 설치되어 컴퓨터 고장(오작동), 정보 탈취, 네트워크 마비 등 악의적인 행위
서비스거부 공격	네트워크 및 시스템에 고의로 과도한 부하를 유발시켜 서비스 및 정상적인 행위를 차단, 성능 저하하는 행위
비인가접근 공격	시스템, 프로그램, 데이터, 네트워크 및 기타 자원 등에 비인가자가 논리적, 물리적인 불법 공격
복합구성공격	악성코드공격, 비인가 접근공격, 서비스거부공격 등 요소를 복합으로 구성하는 공격유형

〈표 5-3〉 대응절차[55)]

구분	대응절차
악성코드 공격	1. 악성코드 공격 판단 2. 감염시스템 분리 및 감염경로 차단 3. 외부 네트워크와의 연결 차단 4. 미확인 악성코드 대처 및 사고통보
서비스거부 공격	1. 서비스거부공격 유형판단 및 추적차단 2. 정보통신서비스제공자(ISP) 차단규칙을 통한 차단 및 추적 3. 피해시스템의 자료백업 및 보안취약점 제거 4. 사고통보
비인가접근 공격	1. 피해시스템 격리 또는 관련 서비스 중지 2. 로그자료 백업 및 비인가 접근공격에 사용된 계정 제거 3. 사고통보
복합구성 공격	1. 사고별 대응 요령을 나열하고 중요도를 판별하여 우선순위에 따라 공격기법별 사고 대응절차 수행

기존의 악성코드 침해사고에 대한 대응은 SSL 암호화 탐지 제한, Zero-Day 공

55) 국가법령정보센터, “G-ISMS 인증 컨설팅”

격 취약, 실시간 네트워크 탐지 제한, 시그니처, SandBox 등의 기술에 대한 신·변종 악성코드에 대해서 탐지가 제한된다. 하지만 머신러닝 기반의 End-Point 보안기술(바이러스→HIPS→Anti-Exploitation→Sandbox→EDR→SIEM)이 발전하면서 악성코드 위협의 수준을 정량화했고, Stealth 엔진 기반 보안기술로 탐지할 수 있게 됐다.[56]

〈표 5-4〉 악성코드 침해사고 방지 기술

방지 기술	설 명
프로세스 패턴 탐지	• 라이브러리 로딩 시 파일검사 • 프로세스 모델링, 분류, 회귀
악성행동 분류	• 이상행동 악성여부 검사, 판단 • KNN, SVM, 베이지안 네트워크
익스플로잇 자동차단	• 코드 덮어쓰기, 랜 스크래핑 • 자체 판단기반 차단 수행
코드인젝션 실시간 방지	• 메모리 원격 할당, 매핑 차단 • 실시간 Over Flow 사전차단
Active Script 공격분석	• 악성 Power Shell 스크립트 분석 • 가상 실행 결과 악성여부 도출
VBA 매크로 공격 탐지	• File-Less기반 공격탐지/차단 • Office 문서 내 스크립트 분석
지능형 앱 리스크 관리	• 실행 가능한 APP리스크 관리 • APP 행위 시계열 분석
저장장치 자동 통제	• Driver 수준 DMA데이터 추적 • Cycle Stealing Word 단위 분석
신종 악성코드 탐지	• 행위기반 모데링/패턴화 수행 • 정상/악성행위 벡터 거리 측정
변종 악성코드 탐지	• 기존 시그니처 분석, 전이 학습 • Fine Tuning 기반 유사 코드 차단

56) Hong, Jun-Hyeok, Lee, Byoung Yup, “인공지능기반 보안관제 구축 및 대응 방안”, 한국콘텐츠학회 논문지, 20201, vol. 21, no. 1.

악성코드 탐지를 위해 〈표 5-4〉 분석기술 기반의 Precision[57], Recall[58]이 필요하며, 프로세스 패턴 탐지, 악성행동 분류, 익스플로잇 자동차단 등 다양한 방지 기술을 이용해서 학습을 수행하는 다차원 머신러닝 기술을 사용해야 한다.

데이터 수집에 대한 분류 모델은 위험 수준을 고려 확률적으로 예측할 수 있는 알고리즘을 적용해서 판단과 예측을 분리한 프레임워크 구성 예측 모델을 적용한다면 침해사고 예측, 위험도 분석 및 대응을 할 수 있다.

다양한 악성코드는 동일한 기능을 같는다고 하여도 프로그램 개발 도구나 컴파일러 환경에 따라서 내부 코드가 다르게 생성이 되며, 추가적으로 안티 가상머신(Anti-VM), 안티 디버깅(Anti-Debugging), 패킹(Packing) 등의 정보보호 기법을 적용하게 되면 악성코드 분석 시간이 더 증가하게 된다.

해결책으로 SandBox 기반으로 자동화된 분석기술과 머신러닝 기술을 결합하게 되면 효율적인 분석 결과를 도출할 수도 있다.[59]

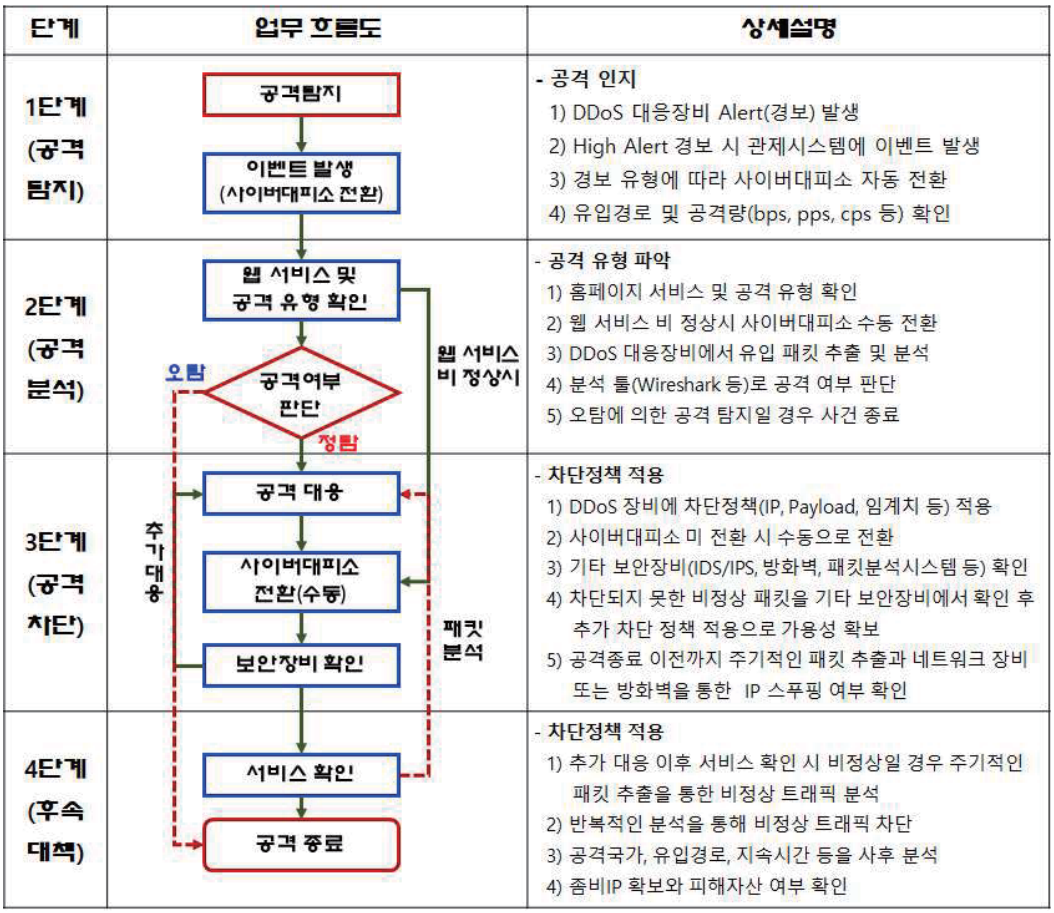
〈그림 5-5〉 행위 정보 기반의 군집화 예시

57) Precision(정밀도) : 모델이 True라고 분류한 것 중에서 실제 True인 것의 비율, Precision = TP / TP + FP
58) Recall(재현율) : 실제 True인 것 중에서 모델이 True라고 예측한 것의 비율, Recall = TP / TP + FN
59) 홍준력, 이병엽, "인공기능기반 보안관제 구축 및 대응방안", 한국콘텐츠학회논문지, Vol. 21, No. 1

5.5 분산 서비스거부(DDoS) 침해사고 대응방안

DDoS(Distributed Denial of Service) 공격은 “수십 대에 많게는 수백만 대의 좀비 PC를 원격 조종해 특정 웹사이트에 동시에 접속시킴으로써 단시간 내에 과부하를 일으키는 행위”를 뜻한다.[60]

〈그림 5-6〉에서와 같이 DDoS 공격 대응 절차는 공격 탐지, 공격 분석, 공격 차단, 후속조치 순으로 진행된다.



〈그림 5-6〉 DDoS 대응 절차[61]

60) 지식백과 용어 정의
61) 상게서, pp. 537-538

1단계로 공격 탐지를 위한 체크포인트로 이벤트 발생 당시 공격 유무의 명확한 판단이다. 2단계는 공격유형 분석으로 부대 네트워크에 유입되는 트래픽에 대해서 수집된 패킷을 분석하거나 시나리오 기반(Scenario Drawn)의 DDoS 유형에 대해서 파악을 한다.

3단계로 차단정책 적용에 의한 대응으로 공격유형을 명확히 판단하여 DDoD 차단을 위한 부대 내 정보보호 시스템이나 기타 보안장비에 차단 정책을 설정하여 서비스에 대한 가용성을 확보한다. 4단계로는 추가 대응 이후 서비스 확인 시 비정상일 경우 주기적인 패킷 추출을 통합 트래픽 분석 및 반복적인 분석을 통한 비정상 트래픽 차단 및 좀비 IP 확보와 피해자산 여부를 확인하는 후속조치이다.

지금까지는 보안담당자들에 의해서 DDoS 침해사고에 의한 대응을 DDoS 대응 절차 4단계에 의거해서 수행해 왔는데, 앞으로는 DDoS 침해사고 대응을 위해서 머신러닝과 결합을 해서 DDoS의 공격유형별 정보 및 특징들을 머신러닝 알고리즘에 학습시켜서 보안시스템에서 자동적으로 예방하거나 차단할 수 있는 시스템을 구축하는 것이다.

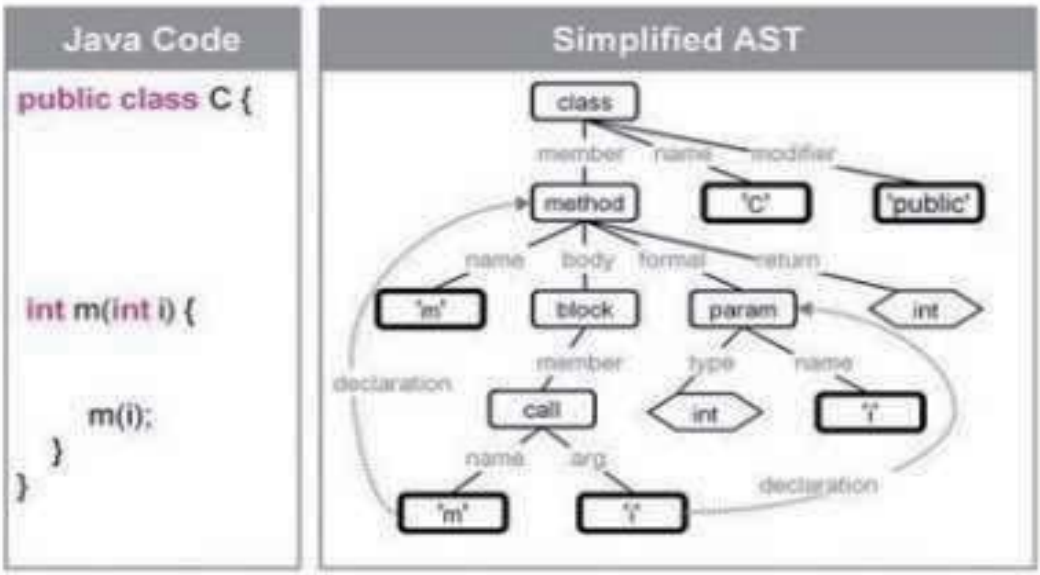
5.6 취약점 분석 분야 대응방안

취약점 분석은 광범위한 범위의 네트워크 이슈를 분석한 후 문제가 될수 있는 네트워크 보안 취약점을 정확히 찾아내는 과정이며 설정상의 오류나 정책의 불일치성과 같은 취약점을 모두 포함해서 발견하는 것이다.

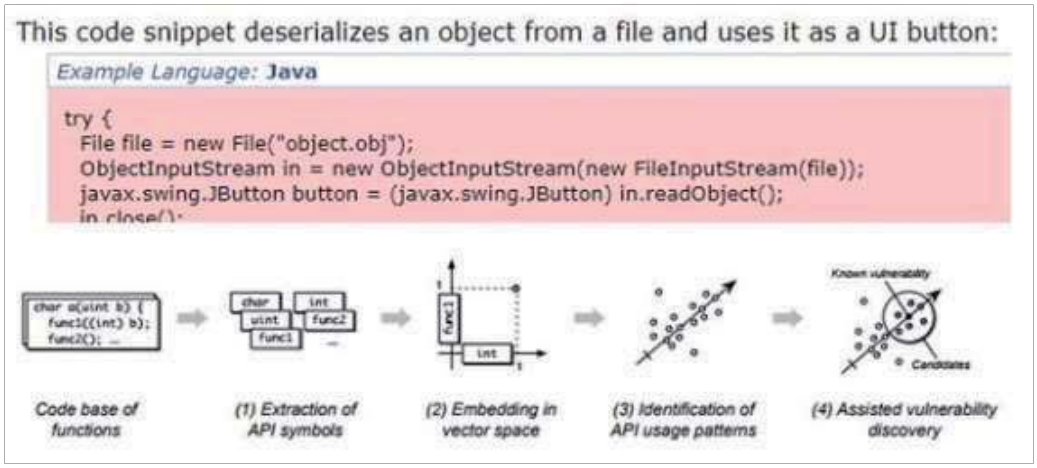
이러한 취약점 분석 분야에도 머신러닝을 활용하여 취약점 정보 공유 사이트의 방대한 양의 데이터를 학습시킨다면, 소프트웨어나 네트워크상의 취약점을 찾아내고 분석하는 분야에서도 활용하여 취약점 분석의 자동화를 달성할 수도 있다.

예를 들어 〈그림 5-7〉과 〈그림 5-8〉에서와 같이 소스 코드에서 이진 트리형식의‘구문 트리(Syntax Tree)’를 활용해서 프로그래밍 패턴을 식별과 학습을 통해서 새로운 취약점 존재여부를 탐지할 수 있다.

그러나 현재는 관련되는 취약점 데이터의 양이 불충분하고 개발과정에서 컴파일된 바이너리 분석 시 개발 및 컴파일러 환경의 차이로 인해 다양한 변수가 있으므로 정확도를 향상시키기 위한 노력도 병행되어야 한다.



〈그림 5-7〉 구문트리



〈그림 5-8〉 취약점 데이터 학습 과정

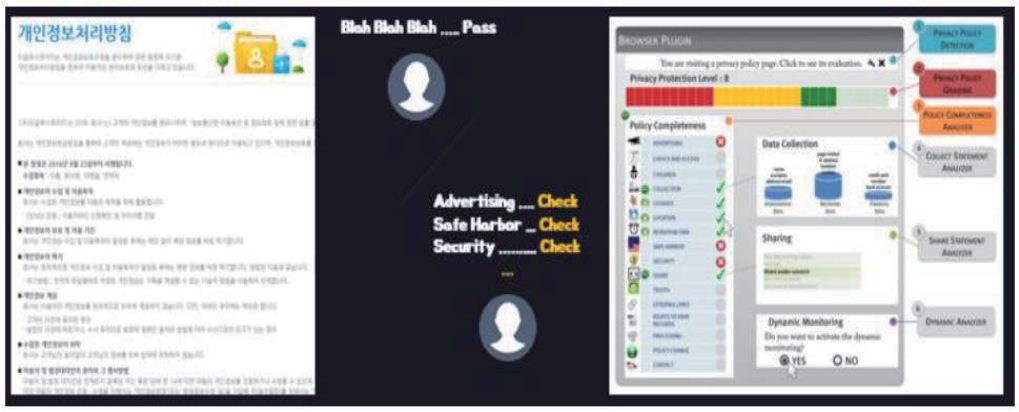
5.7 컴플라이언스 분야 대응방안

컴플라이언스[62] 프로그램(compliance program)이란 “사업 추진 과정에서 기업이 자발적으로 관련 법규를 준수하도록 하기 위한 일련의 시스템으로 컴플라이언스 프로그램을 기업윤리까지 포괄하는 의미도 있고, ethics and compliance program이라는 표현”이 사용되기도 한다.[63]

국방부 및 각군본부 등 일부 부대에서 인터넷 포털사이트를 이용하는데 〈그림 5-9〉에서와 같이 이용약관, 개인정보처리방침 등에 대해서 고지를 하고 있다. 이는 외부 사용자들이 포털사이트 회원가입을 해서 서비스를 활용할 때 주의사항 등에 대한 고지인데 이를 등한시해서 위반할 때는 법적인 분쟁까지 발생될 수도 있다.

대부분 이러한 고지를 일반 사용자들이 인식하기 어려운 위치에 배치하거나 어려운 용어 등을 사용해서 곤란하게 만드는 사이트들도 존재한다.

이에 컴플라이언스 분야에서 머신러닝 기반의 솔류션을 사용하여 이용약관이나 개인정보보호 관련 내용들을 학습시켜 사용자들이 이해하기 쉽게 체크리스 포맷으로 서비스를 할 수 있는 방법을 적용할 수 있다.



〈그림 5-9〉 컴플라이언스 분야 대응방안

62) 컴플라이언스(compliance)는 통상 법규준수/ 준법감시/ 내부통제 동의 의미
63) 지식백과 용어 정의

6. 결 론

4차 산업혁명 시대 발전에 따라 사이버 영역 공격자들은 핵심기술인 머신러닝 기술을 활용한 지능화된 알고리즘을 이용해 신·변종 사이버 공격과 자동화 기법을 활용하여 다양한 사이버 공간에서 공격을 시도하고 있다.

기술의 발전 추세가 점차적 고도화되고 다양해지는 사이버 공격에 효율적이고 정확하게 대응할 수 있는 기존 사이버보안 솔루션들로는 많은 한계를 보인다. 사이버보안 위협에 대해서 능동적으로 대비하기 위해서 사이버보안에서는 머신러닝 기법 적용에 대해서 주목하고 있다.

사이버보안에 머신러닝을 적용함으로써 위협 인텔리전스, 네트워크, 악성코드 분석, 실시간 탐지 및 대응, 취약점 분석 등 다양한 사이버보안 분야에서 성과가 획기적으로 향상될 것이다[64].

사이버보안 분야에서 활용되고 있는 머신러닝은 보안전문가의 역할을 침해하는 오버피팅 오류와 성향적 오류가 있으며, 이들을 극복하기 위한 노력으로는 방대한 사이버 보안분야 데이터를 그동안은 인간의 경험과 지식을 토대로 분석해 온 분야를 머신러닝을 적용하여 학습 과정을 통한 결과들이 점점 지능화되어 가고 있는 사이버보안 위협을 보다 효율적이고 정확하게 탐지하여 빠르게 대응할 수 있다.

또한, 여러형태의 사이버보안 프로세스 자동화로 사람의 개입을 최소화하고 미탐 및 오탐을 최소화를 위해 수집된 수많은 보안 데이터를 장기간 분석해 온 보안전문가의 경험과 지식을 머신러닝에 적용해서 학습할 수 있도록 해야 한다. 뿐만 아니라 행위 및 시그니처 분석 기술 등을 적용하고 머신러닝 기반의 지능화된 공격에 대해서도 실시간으로 탐지와 대응을 제공하도록 해야 한다

본 연구의 목적은 날로 지능화로 진화되고 있는 사이버보안 위협과 기하급수적으로 증가하는 보안 정보들에서 지능화된 보안 위협을 정확한 분석과 보안 사고들을 실시간으로 대응이 가능한 머신러링을 사이버보안 분야에 적용이 증가하고 있다.

현시점에 수많은 보안 데이터 및 로그분석 자동화로 필요한 핵심 데이터를 선별적으로 분석하고, 기존 규칙 및 시그니처 기반의 탐지가 제한된 지능화된 사이버보안 위협을 보다 정확하고 효율적으로 탐지하기 위한 머신러닝과 사이버보안 위

64) CCTV뉴스, “인공지능 보안, 대응 강화와 악성코드 분석 효율 지원”, 2019. 7.

협 및 머신러닝의 적용사례와 국방 사이버보안 영역의 머신러닝 기반 공격 위협 모델과 공격기술에 대해 제안했다.

국방 사이버보안 영역의 머신러닝 기술에 대한 대응방안으로는 통합보안관제체계 운영, 해킹 침해사고 대응 방안, 네트워크 보안 분야 대응방안, 악성코드 분석 분야 대응방안, 분산 서비스공격 대응방안, 취약점 분석 분야 대응방안 및 컴플라이언스 분야 대응방안을 제안했다.

앞으로 국방 사이버보안 분야도 더욱더 다양한 업무에서 머신러닝을 적용한 지능적이고 창의적인 접근 방식이 많이 활용되기를 기대하며 본 소고를 마친다.

참고문헌

[1] CCTV뉴스, “보안을 위협하는 양날의 검, 인공지능”, 2019. 7.
[2] 스트레이트뉴스, “전세계 CIO 가장 파괴적인 기술은 인공지능(AI)”, 2018. 10.
[3] CCTV뉴스, “인공지능 보안, 대응 강화와 악성코드 분석 효율 지원”, 2019. 7.
[4] 경찰청, “2018년 사이버위협 분석 보고서”, 2018. 8.
[5] 보안뉴스. “보안에서의 인공지능과 머신러닝, 어디까지 와 있나”, 2018. 1.
[6] IT월드, “사이버 보안 속 인공지능, 할 수 있는 일과 할 수 없는 일”, 2018. 8.
[7] 김광일, “인공지능의 과거, 현재 그리고 미래”, 에이콘출판, 2017. 12.
[8] 이승훈, “최근 인공지능 개발 트렌드와 미래의 진화방향”, LG경제연구원, 2017. 12.
[9] 박형근, “정보보안에서의 인공지능 도입 분야와 주요 사업자”, 시큐리티플러스, 2018. 12, pp.3-9.
[10] CCTV뉴스, “4차 산업혁명, 보안에 AI를 더했다”, 2018. 2.
[11] CCTV뉴스, “급증하는 신종보안 위협, 정보보안은 어떻게 나아가야 하는가”, 2018. 10.
[12] 이창훈, “인공지능 기법을 이용한 네트워크 기반 침입탐지 기술 동향”, 건국대학교, 2018. 5, pp.1-2.
[13] 아이마켓코리아, “인공지능 머신러닝 기반 보안 솔루션 알아보기”, 2019. 2.
[14] 연합뉴스, “알파고 제로, AI 창의성 확인…인간 한계 분야에 적용 가능”, 2017. 10.
[15] 한국정보화지흥원(NIA), “인공지능 악용에 따른 위협과 대응 방안”, Special Report 2018-12, 2018. 3.
[16] 나우뉴스, “인공지능, 이미 악용단계 돌입” 전문가들 경고“, 2018. 2.
[17] 국경완, “인공지능 기술 및 산업분야별 적용사례“, 정보통신기획평가원, 주간기술동향 1888호, 2019. 3.
[18] 데일리시큐, “RSA 컨퍼런스 2019 AP&J”, 2019. 7.
[19] 아이티데일리, “인공지능으로 공격하고 인공지능으로 막는다”, 2017. 8.
[20] SD아카데미, “클라우드 컴퓨팅(Cloud Computing), 과연 보안에 안전한가?”, 2018. 10.
[21] 정보통신산업진흥원(NIPA), “인공지능 확산의 핵심 인프라, 클라우드 산업 동향 분석과 시사점”, 2019. 6.
[22] 공병철, “정보보호 최고 책임자 자격요건과 역할론”, 한국 인터넷정보학회, 20권 1호, 2019. 7.

[23] 홍준혁, 이병엽, “인공지능기반 보안관제 구축 및 대응 방안”, 한국콘텐츠학회논문지, ‘21 Vol. 21 No. 1, 2021. 1.
[24] 김영중, “머신러닝 기반 정보 보안 기술“, MONITIRAPP 최신보안뉴스, 2021. 1.5.
[25] 이식, 김동훈, 조영훈 등. “머신러닝 기반 보안데이터 분석 연구”, 정보보호학회지, 제 29 권 제3호, 2019. 6
[26] 권용현, “AI,지능정보기술의 방향”, 카카오정책산업연구, 2017.4.
[27] “정보보호 침해사고 대응지침”, 통계청예규 제78호, 2015. 5. 18.
[28] 강대기, “딥 러닝 기반 기계학습 기술 동향”, IITP 기획시리즈, 2016.
[29] Ucci, Daniele, Leonardo Aniello, and Roberto Baldoni. "Survey on the Usage of Machine Learning Techniques for Malware Analysis." arXiv preprint arXiv:1710.08189 (2017).
[30] KISA Report, “ 2021년 인공지능 기술과 산업을 전망하며, 2020년 Vol. 11.
[31] KISA Report, “ 디지털 감시(Digital Surveillance), 2020년 Vol.12

연구보고 2021

미래 해군을 위한 스마트 해양정보체계 구축 방안

하 용 훈

2021. 9.

국방대학교 국가안전보장문제연구소

목 차

그림 목차

표 목 차

1. 연구 개요

1.1 연구배경

우리 해군은 “4차 산업혁명 첨단기술 기반의 「SMART Navy」구현”을 계획하고 있다. 미래의 해군력의 중점은 북한의 위협을 포함하여 해양주권 침해와 초국가적·비군사적 위협 등 다양한 해양안보 위협에 대응하는 것이며 이를 위해서는 연·근해뿐만 아니라 원해역까지 적극적이고 공세적인 전력 운용을 통해 관할해역과 관심해역에서의 임무형 기동작전과 성분작전을 수행할 수 있는 능력을 갖춰야 한다. 이러한 작전 수행능력은 작전을 수행하는 주체인 함정이나 항공기를 획득하는 것으로만 확보되는 것이 아니다. 플랫폼의 중추적 역할을 담당하는 첨단 전투체계와 탐지체계, 무장 등이 연동되어야 하고 현대전에서 필수적인 C4I체계의 연동도 필요하다. 그런데 이러한 체계들은 반드시 정확하고 적시적인 정보를 기반으로 운용되어야 한다. 특히, 대잠전, 대함 및 대공전, 기뢰전, 상륙전, 특수전, 구조전 등 성분작전을 중심으로 수행되는 해군작전에 해군의 독자적 정보 분야인 해양정보는 무엇보다 중요하다.

지난 30여 년간 우리 해군의 해양정보 업무는 다양한 분야에서 작전 지원을 극대화하기 위한 발전을 시도하였다. 체계 분야에서는 2000년 초반에 해양 데이터베이스 체계를 구축하였으며 2010년대에는 해군음향정보관리체계가 전력화되었고 부체계인 통합해양환경분석체계를 이용하여 다양한 해양정보를 제공할 수 있었는데, 이때부터 본격적으로 일일/주간/월간 단위의 광역 해양환경 예보[1]와 음향탐지거리 예보를 작전에 지원하였다. 해양특성조사 사업을 통해서는 수상함, 잠수함, 대잠항공기 등에서 사용 가능한 ‘음탐환경 예보체계’, ‘기뢰전 지원체계’, ‘지자기 환경 지원체계’, ‘부유물 표류경로 분석체계’, ‘해양·기상정보 지원체계’ 등 작전 지원을 위한 다양한 체계를 개발하였다. 그러나 개발된 해양정보 체계들은 대부분 독립체계이며 타 체계와 연동이 되더라도 체계 간 공유되는 정보는 다소 제한적이었다.

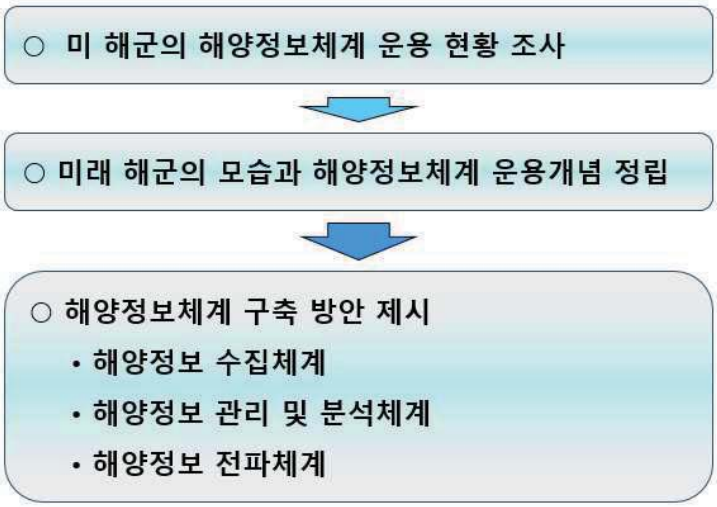
1) 해양환경 예보모델을 운용하여 동해 중·남부 해역, 서해 중·남부 해역, 남해 등에서 작전 시 활용할 수 있는 해양환경을 제공

2000년대 산업기술의 급격한 발전과 함께 인공지능, 빅데이터, 사물인터넷, 모바일, 클라우드 컴퓨팅 등 첨단 정보통신기술이 융합되면서 '4차 산업혁명'이라고 언급되며 우리 사회에 나타났다. 이러한 신기술은 경제, 사회뿐만 아니라 국방 영역에서도 커다란 영향을 미치고 있으며, 현재 육・해・공군의 비전 및 정책서에도 4차 산업혁명 기반기술의 적용을 명문화하고 있다. 향후 4차 산업혁명 기반기술은 군(軍)의 무기체계에 적용될 것이라는 단순한 예상을 넘어 군 작전의 기본 운용개념부터 세부적인 운용개념 전반에 걸쳐 커다란 변혁이 일어날 것으로 예상된다. 해군의 「SMART Navy」 구현 계획은 장기적 관점에서 이러한 변화를 반영한 것으로서, 전력, 작전, 대외협력 측면에서 새로운 시스템을 구축하는 것이며 「SMART Battleship」, 「SMART Operation」, 「SMART Cooperation」이라는 주제로 구체화 될 예정이다.

그러나 미래 해군을 위한 「SMART Navy」구현은 전력과 작전에 초점을 두고 있는데 향후 과학기술 발전과 해군의 무기체계 환경 변화에 대응하고 「SMART Navy」구현을 지원하기 위해서는 기존과 다른 새로운 해양정보체계 구축이 반드시 수반되어야 할 것이다.

1.2 연구 목표 및 범위

본 연구의 목표와 범위는 미 해군의 해양정보 운용 현황 조사를 통해 우리의 실정에 맞는 미래 해군의 모습과 해양정보체계 운용개념을 정립하고 이를 바탕으로 해양정보 수집, 관리 및 분석, 전파에 관한 업무 분야별 해양정보체계 구축 방안을 제시하는 것이다(〈그림 1-1〉 참조).



〈그림 1-1〉 연구 목표 및 범위

1.3 선행연구

해양정보는 해양환경정보, 음향정보, 해양기상정보를 포함하는 해군 고유의 정보 분야로서 연관된 학문 분야는 해양학(해양물리, 해양화학, 해양생물, 해양지질), 음향학(수중음향학), 기상학(해양기상학) 등이며 이러한 학문 분야에서 생산되는 해양 자료들은 모두 해양정보가 될 수 있다. 그러나 해군작전을 지원하는 해양정보와 해양정보체계의 세부사항에 대해서는 공개된 학술 연구가 많지 않으며 대부분 비공개로 연구가 진행되고 있고 체계 개발의 경우는 더욱 그러하다.

미 해군은 세계 2차대전 이후 미 해군의 작전지원을 위한 해양정보 업무 및 체계들을 발전시켜왔으며 전 세계 해군 중 가장 발전된 해양정보체계들을 구축하고 있다. 미 국립학술원(The National Academies)의 국가연구위원회(National Research Council, NRC)는 2004년 '해군작전을 위한 환경정보(Environmental Information for Naval Warfare)' 연구에서 해군 성분작전에 지원되는 해양정보의 가치를 평가하였으며 해양환경의 불확실성 제거를 통해 해양정보 발전방안 개념을 제시하였고 해양정보와 NCW 지원관계를 정립하였다. 미 해군은 해군작전 지원을 위한 해양정보를 〈표 1-1〉과 같이 해양·기상 물리적 특성 기준에 따라

분류하여 수집하고 있다.

국내에서는 하 등(2020)은 “해양특성조사 사업 개선 및 가시화 방안” 연구에서 해양특성조사 사업을 해양정보체계와 연계하여 발전방안을 제시한 바 있다.

〈표 1-1〉 해양 · 기상 물리적 특성 기준[2)]

항목	세부 사항	항목	세부 사항
대기학	날씨(구름, 안개, 강수량, 풍속 및 방향, 기온)	해양학	조석
	주변 광, 해양 경계층 속성 (온도, 습도, 굴절률)		내부파 (해류 : 표층 및 하층)
생물학	주변 소음		해수 전도도, 수온, 수심 및 염분
	광학 산란		해상상태
	생물 발광		파고 및 방향
측심학 /지형학	바닥 및 해변 경사		파도 조건
	해변과 바닥 구성		광학 특성(수직 및 수평)
음향학	산란		탁도
	주변 소음	지질학 /자기학	해저 거칠기 및 유형
인류학	오염		퇴적물 특성, 바닥 강도 및 안정성
	소음		주변 자기 및 전기 배경

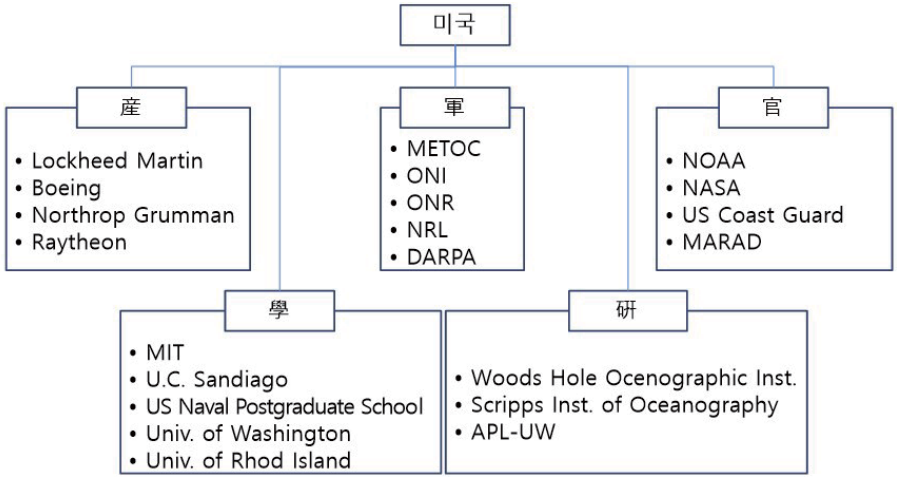
2) 1993년, 미국 National Research Council이 “Coastal Oceanography and Littoral Warfare"에서 정의

2. 미 해군의 해양정보 업무 및 체계 운용

제2장에서는 우리 해군의 해양정보 업무 및 체계를 발전시키기 위한 롤 모델로서 미 해군의 해양정보 업무 조직 및 업무수행 모델, 그리고 해양정보 운용체계 현황을 소개한다.

2.1 미 해군의 해양정보 업무 조직

미 해군에는 해양정보 업무를 전담으로 수행하는 기상해양병과인 METOC[3]이 있으며, 대잠전 및 대수상함전에서 음향정보를 지원하는 해군정보국(ONI[4]), 연구 및 체계 개발 프로젝트를 지원하는 해군연구국(ONR[5]), 해군연구소(NRL[6]), 등 군(軍) 기관뿐만 아니라 〈그림 2-1〉과 같이 이와 연계된 관(官)·산(産)·학(學)·연(硏)의 해양정보 유관기관이 매우 다양한데, 규모와 역량 면에서 세계 최고 수준의 해양정보 수집·분석·처리·전파 업무를 수행하고 있다.



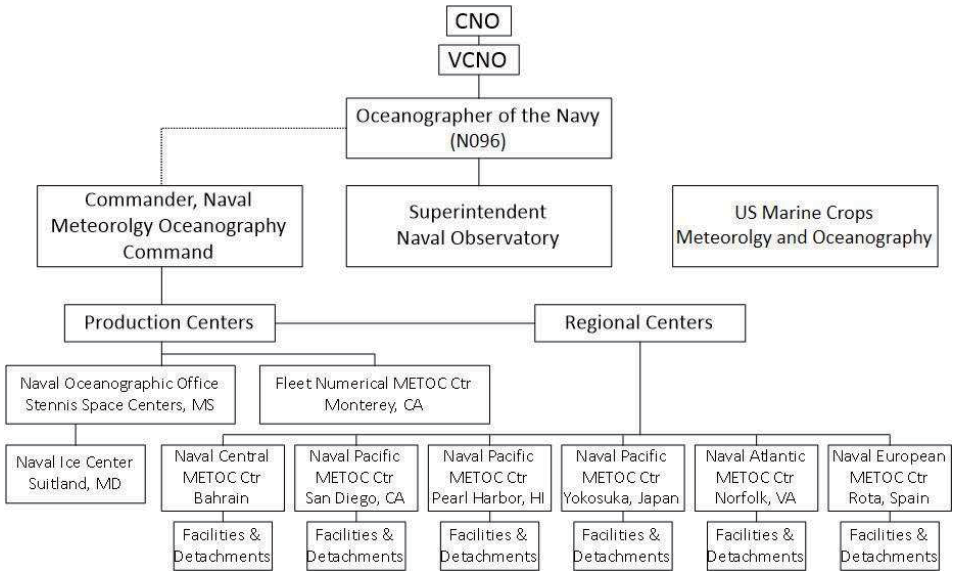
〈그림 2-1〉 미국의 해양정보 유관기관

3) METOC : Meteorology and Oceanography
4) ONI : Office of Naval Intelligence
5) ONR : Office of Naval Research
6) NRL : Naval Research Lab

2.1.1 해군 기상해양병과(Navy METOC)

기상학(Meteorology)과 해양학(Oceanography)을 의미하는 METOC은 전 세계에서 해양정보 분야에 가장 많은 전문인력과 장비를 가진 조직이며 400여 명의 장교와 1,300여 명의 부사관으로 구성되어 있고 전 세계 전구(戰區)에서 해군뿐만 아니라 전 미군을 지원하고 있다. 미 해병대도 별도로 구성된 450여 명의 METOC 조직을 운영한다. METOC은 미 국방성 예하 기관 외에도 국립과학재단, 항공우주국, 상무부 등 정부 조직과도 협력하며, 작전 지원은 물론 민간에도 다양한 정보를 제공하고 있어 정부·산업·학계에서도 높은 평가를 받고 있다.

METOC 조직은 〈그림 2-2〉와 같으며, 해군참모총장(CNO)의 참모이자 병과장(계급 : 소장)인 'N096 Oceanographer of the Navy' 예하에 기상해양사령부(CNMOC[7])가 있으며, 예하에 해양국(NAVOCEANO[8]), 함대수치기상해양센터(FNMOC[9]), 6개의 지역(미 동·서부, 하와이, 일본, 바레인, 스페인 등) 기상해양센터를 두고 있다.



〈그림 2-2〉 METOC 조직도[10]

7) Naval Meteorology and Oceanography Command
8) Naval Oceanography Office
9) Fleet of Naval Meteorology and Oceanography
10) National research council, 「Environmental Information for Naval Warfare」, 2004

가. 기상해양사령부(CNMOC)

미시시피주 Stennis Space Center에 있으며 사령관(준장)을 중심으로 약 70~80명이 전체 METOC 조직을 관리, 감독하는 임무를 수행하고 있고 미 해군의 대잠전, 기뢰전, 정보·감시·정찰(ISR), 공격 및 원정작전, 대함·대공작전에 있어 해양·기상·지형·천문 관련 정보를 적시에 제공하는 것을 주 임무로 하고 있다.

나. 해양국(NAVOCEANO)

기상해양사령부 예하의 규모가 가장 큰 해양정보 기관이며 METOC 장교와 부사관, 연구원, 군무원 등 약 950여 명 인원으로 편성되어 있고, 7척의 T-AGS급 해양조사선[11]을 보유하고 있다. T-AGS 해양조사선(〈그림 2-3〉 참조)은 매년 한미연합대잠전훈련(SHAREM)에 참가하여 해양·음향환경에 대한 조사와 분석 임무를 수행하고 있다. 또한, 해양국 예하의 Warfighter Support Center는 작전부대에 전술적 의사결정을 지원하는 맞춤형 보고서를 (근)실시간에 제공하고 있다.

〈그림 2-3〉 미 해양조사선 T-AGS 60 Pathfinder[12]

11) 만재 약 4,800톤, 107.6m(전장)×17.7m(전폭), 통상 승무원 27명, 과학자 39명 탑승, 가변심도소나(VDS), 사이드스캔소나, CTD(수온염분측정기), XBT, 해저지질 샘플러 등을 탑재하여 음향신호 수집, 지형 관측, 수온/염분 등 해양자료 수집 및 분석 업무 수행

12) https://www.msc.usff.navy.mil/Press-Room/Photo-Gallery/igphoto/2002508630/

다. 함대수치기상해양사령부(FNMOC)

약 270명의 METOC 요원과 연구원으로 구성된 FNMOC는 캘리포니아 Monterey에 위치하고 있으며, 여러 대의 슈퍼컴퓨터를 이용하여 기상 및 해양 수치 모델 운용 결과를 생산하고 지역 기상해양센터를 통해 全 세계 미군과 연합군에 기상·해양정보를 제공하고 있다. 특히 'Navy Global Environmental Model(NAVGEM)'이라 불리는 글로벌 수치기상모델과 'Hybrid Coordinate Ocean Model(HYCOM)'이라 불리는 글로벌 해양예보모델을 운용하며 작전에 해양정보를 제공하고 있는데, 전 세계 지역별 해양파 예보 차트, 표층수온 차트, 지역별 기상 예보 차트를 생산하며 미 공군과 함께 태평양 전역에 대한 합동태풍경보센터(Joint Typhoon Warning Center)를 운영하고 있다.

라. 지역 기상해양센터(Regional METOC Center)

지역 기상해양센터는 CNMOC의 지휘 통제를 받으며 FNMOC에서 제공되는 기상·해양정보를 미군 및 연합군에 적시 제공하고자 이동예보팀(MET)을 구성하여 해상작전을 수행하는 함정에 METOC 요원을 탑승시켜 실시간 예보를 지원하거나 작전요원에 필요한 해양정보를 제공하고 있다.

2.1.2 해군정보국(ONI : Office of Naval Intelligence)

해군정보국에서는 음향정보[13]를 취급하고 있으며 ONI 내 음향정보 관련 부처에서 함정의 음향정보를 수집, 분석, 식별 및 DB화하고 대잠작전을 수행하는 수상함과 잠수함, 대잠항공전력에 이러한 정보를 전파한다. 함정의 단독/연합 작전 및 훈련 간 잠수함 탐지를 위한 해양 및 음향신호 수집·분석은 METOC에서 수행하나 사후 정밀 분석하고 이를 DB화하여 관리하며 작전에 제공하는 것은 ONI가 수행하고 있다.

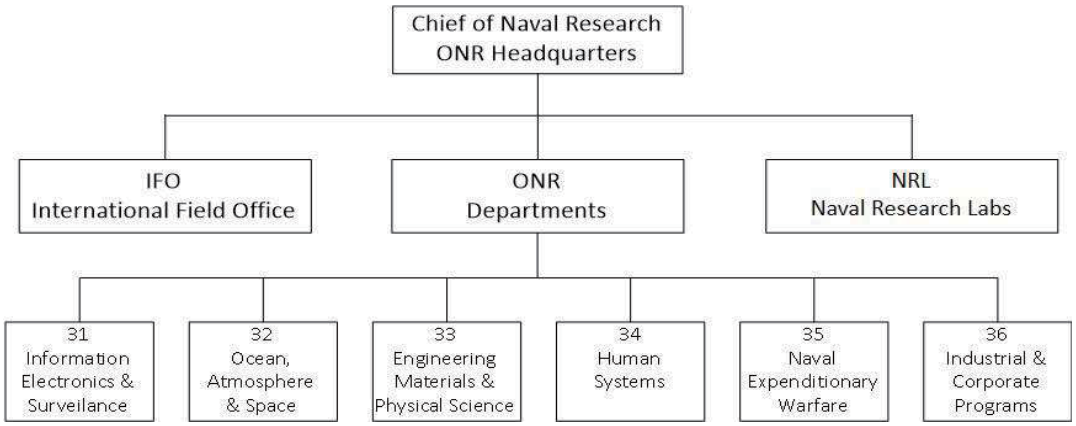
13) 표적 음향신호의 제원 특성인 음향특성(Acoustic Characteristic), 주파수 성분의 음향징표(Acoustic Signature), 그래픽 특성의 음문(Acoustic Gram)자료를 의미하며, 2급 비밀보다 수준이 높은 특수정보 수준으로 취급함.

2.1.3 해군연구국(ONR)[14]

METOC에 대한 최대 지원기관으로 정보전자·감시처, 해양·대기·우주처, 공학재료·자연과학처, 인간공학처, 해군원정전처, 산업협력처 등 6개 처로 구성(〈그림 2-4〉)된 해군성 장관(Secretary of the Navy) 예하의 기관으로서, 해군의 과학기술 연구·개발·획득 분야와 관련된 업무를 수행하며 연간 약 20억 달러의 R&D 예산을 해군연구소, 학계·산업계에 지원하고 있다

2.1.4 해군연구소(NRL : Naval Research Lab.)

1923년 설립된 해군연구소는 ONR 예하의 기관으로 80여명의 현역, 2,500여명의 연구원과 행정원으로 구성되어 있으며 해군과 관련된 기초과학 및 응용연구, 기술개발 등에 연간 10억 달러 규모의 예산을 집행하고 있으며 현재 연구분야는 〈표 2-1〉과 같다.



〈그림 2-4〉 ONR 조직도[15]

14) ONR 홈페이지 : www.onr.navy.mil
15) National research council, 「Environmental Information for Naval Warfare」, p.28., 2004

〈표 2-1〉 NRL 연구분야

구 분	연구 분야
기초과학	• Oceanography & Meteorology • Materials • Marine geosciences • Ocean acoustics
응용연구	• Computer science, cognitive science, and A.I. • Directed energy technology • Environmental effects on naval systems • Human-robot interaction, Information technology • Imaging research and systems
기술개발	• Advanced radio, optical and infrared sensors • Autonomous systems • Electronic electro-optical device technology • Electronic warfare • Enhanced maintainability, reliability and survivability technology • Space systems and technology • Surveillance and sensor technology • Undersea technology

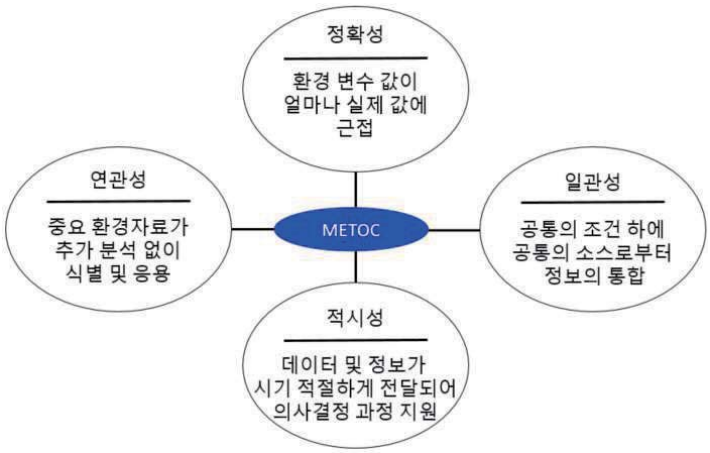
2.2 미 해군의 해양정보 업무 수행 모델

본 절에서는 2013년 미 해군(해병대)에서 발행된 “Operational Level Integration of METOC Capabilities”를 요약하였다.

2.2.1 해양정보 업무의 원칙과 프로세스

미 해군의 해양정보(METOC) 업무의 목표는 임무 지휘관의 의사 결정능력을 강화하고 정보 우위를 확보할 수 있는 해양정보를 제공하는 것이다. 해양정보 조직은 네 가지 기본 원칙(〈그림 2-5〉 참고)을 적용한 정보를 바탕으로 계획 및 의사결정 지원을 한다. 그 원칙은 해양정보 업무에 있어서 가장 중요한 특성을 정확성, 일관성, 연관성, 적시성으로 요약하고 있다. 해양정보는 작전 임무에 가능한 가장 정확한 데이터와 정보를 제공해야 하며 조건이 유사할 경우 일관성 있는 데이터를

생산 및 제공하고, 중요 데이터와 정보는 별도의 분석이나 가공 없이 신속히 식별 및 적용됨으로써 이들 데이터가 적시에 의사결정에 활용될 수 있어야 한다는 것이다. 이러한 특성은 독립적인 것이 아니며 상호 유기적 관계를 갖는데 결국 정확하고 일관성이 있으며 상호 연계되어 적시적인 해양정보를 제공하는 것으로 해양정보 업무의 목표를 성취하기 위한 기본 원칙이라 할 수 있다.



출처 : US Navy, Operational Level Integration of METOC Capabilities

〈그림 2-5〉 METOC 업무의 4가지 기본 원칙

앞서 설명한 기본 원칙을 바탕으로 해양정보 업무의 프로세스는 환경을 특성화하고 지휘관에게 의사결정 수준의 정보를 제공하며 다음과 같은 단계를 거쳐 처리된다.

① 정적 및 동적 데이터 수집
: 기상, 해양, 우주 환경 데이터의 감지, 획득 및 관찰
② 해당 데이터로부터 현재/과거 조건 분석
: 기상, 해양 및 환경 데이터를 정보 형태로 저장
③ 미래 환경 조건 예측
: 기상, 해양 및 우주 환경 관련 예측되는 미래의 상태에 대해 설명
④ 특정 부대의 작전 요구 사항이 충족되도록 환경 정보를 맞춤식으로 조정
: 환경 정보 파라미터로부터 관련성 있는 정보를 도출

⑤ 이 정보를 지휘관의 의사 결정주기 및 C2 시스템에 통합
: 의사결정자가 계획된 작전에 대한 환경 영향을 예상한 후 이를 완화하거나 오히려 활용할 수 있도록 보좌

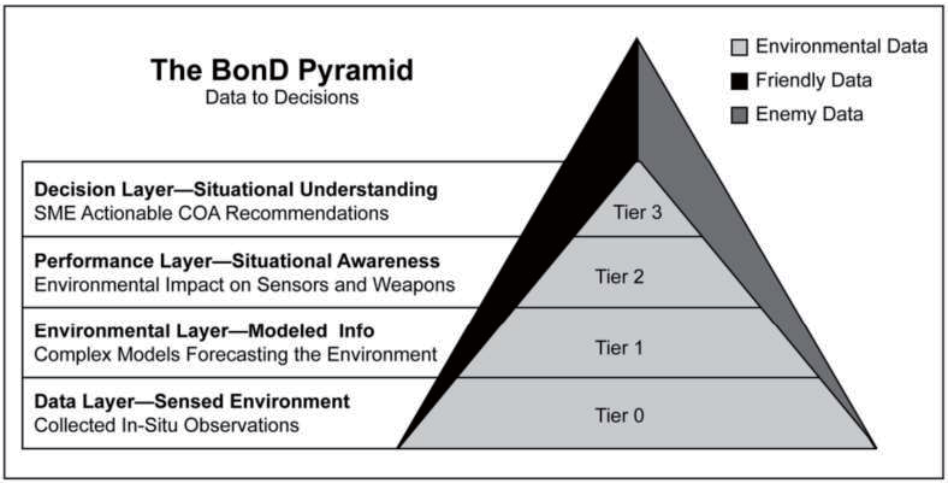
2.2.2 주문형 전장(BonD : Battlespace on Demand) 개념

해양정보 업무의 원칙과 프로세스는 'BonD'로 구체화된다. 'BonD'는 '2010년 미 해군의 정보 지배 비전'과 '21세기 해상 협력 전략'에 뚜렷하게 명시된 원칙들이 포함된 개념이다. 미 해군 해양력의 최적화를 위한 기상해양사령부의 비전 및 실행 전략은 BonD 개념을 통한 의사결정 능력 향상에 근거한다. BonD 개념은 복잡한 작전환경의 정확한 이해를 위해 해군, 합동전력, 정보기관, 그리고 전 세계 정보출처로부터 환경 데이터와 정보를 획득하고 분석하는 방법을 표현하는데 BonD 개념을 적용한 데이터 모델은 〈그림 2-6〉과 같다.

BonD 개념은 다음과 같이 설명될 수 있다.

① 환경 데이터 수집, 데이터 변환과 다른 데이터 소스와 정보 및 지식의 융합에 중점
② 전투원이 실제 환경을 이용하여 전술적, 작전적, 전략적 이점을 달성할 수 있도록 맞춤형 의사결정 지원 정보를 제공
③ 적시에 정보에 근거한 결정을 위해 환경 데이터를 연결함으로써 장거리 해군 해양전략 지원

BonD 데이터 모델은 4계층 피라미드 형태이며, 각 계층에 대한 설명은 다음과 같다.



출처 : US Navy, Operational Level Integration of METOC Capabilities

〈그림 2-6〉 Battlespace on Demand 모델

가. 데이터 계층(Data Layer)

'Tier 0'으로 알려진 데이터 계층은 대기와 바다를 위성, 고도계, 글라이더, 부표 등과 같은 현장 또는 원격 센서들을 통해 관찰하면서 수집된 정보로 구성된다. 이 데이터는 현재의 해양 및 대기 환경뿐만 아니라 천체 및 시간 기준 프레임을 정확하게 설명하는 초기 및 경계 조건을 제공하기 위해 동화 및 융합된다. 이에 대한 결과물은 물리적 환경 상태에 대한 원시 관측 데이터 모음이다.

나. 환경 계층(Environmental Layer)

'Tier 1'이라고도 하는 환경 계층에서 Tier 0의 데이터는 미래의 환경 상태를 예측하기 위해 고성능 컴퓨팅 시스템에서 작동하는 데이터베이스, 예측 시스템 또는 수치 모델로 분석, 처리 및 병합된다. 결과물은 진행 중인 작업에 대한 예상 물리적 환경에 대한 공간 및 시간 예측 집합이며 일반적으로 '신뢰 요소'가 포함된다.

다. 퍼포먼스 계층(Performance Layer)

'Tier 2' 퍼포먼스 계층에서는 환경 예측과 운영 환경에 대한 정보가 통합되어 특정 운영 조건에서 아군과 적군, 센서, 무기 시스템 및 플랫폼의 성능을 예측할 수 있다. 이 융합 정보들을 분석하면 계획, 부대 구조, 표적 지정, 타이밍, 기동 및

전술・기술・절차(TTP[16])에 미치는 영향과 같은 작전상의 함의를 제공할 수 있다. 적절한 신뢰성을 바탕으로 운영자가 이해할 수 있는 용어로 표현된 영향 평가 결과는 상황 인식 능력을 향상시킨다.

라. 결심 계층(Decision Layer)

'Tier 3'으로도 알려진 의사결정 계층에서는 Tier 2에서의 상황 인식을 특정 상황에 적용하여 전략, 작전 및 전술 수준에 대한 위험과 기회를 계량화한다. 이를 통해 안전성과 교전 효과를 직접적으로 향상시키는 부대 할당 및 배치에 관해 의사 결정자에게 실행 가능한 권장 사항이 제시된다. 최적의 방안을 마련하기 위해 Tier 3에서는 Tier 2에서 수행된 실행 예측에 대안 방책(COA : Courses Of Actions)을 추가하여 고려하는데, 그 이유는 다음과 같다.

① 위험과 성공 확률에 대한 이해
② 변화하는 물리적 환경에서의 비대칭 기회의 이점 극대화
③ 아군에게 최대 이점 제공
④ 적군의 불리(Disadvantage) 극대화

실제 환경에 대한 최적화된 이해를 기반으로 하는 의사결정 권장 결과는 의사결정자에게 매력적인 이론적 근거와 상황 이해를 제공한다.

요약하면, BonD 개념은 Tier 1의 고성능 환경 모델을 위해 Tier 0에서 수집된 현장 환경 데이터를 사용한다. Tier 3의 의사결정 프로세스를 개선하기 위해 해양정보 지원은 Tier 2의 의사결정 지원 도구에 대한 이해를 향상시킨다. 해양정보 전문가들과 지원 담당자는 해양정보 결과물에 대한 더 나은 이해를 제공하기 위해 실제 관찰 결과와의 일치 여부를 기준으로 모델 성능을 평가한다. 자산의 기능과 한계에 대한 환경 영향에 중점을 두고 해양정보 지원을 사령관의 의사 결정주기에 완전히 통합시킨다면 전투 효과는 즉시 향상될 것이다.

16) Tactics, Techniques, and Procedures

2.2.3 해양정보의 역할(결심과 계획 측면에서)

지휘·통제는 작전 지휘관에게 부대 작전을 동기화 또는 통합함으로써 노력의 통일성을 달성하는 방법을 제공한다. 이러한 지휘·통제에 해양정보의 핵심 임무 기능을 효과적으로 통합하고 해군의 다양한 전쟁 지역 내에서 작전적 수준의 임무 지원 기능의 활성화에 중점을 두어야 하며, 해양정보의 능력과 서비스를 해상작전센터(MOC[17])의 해군구성군사령부 및 함대사령부, 연합전투단(CTF[18]), 항모강습단(CSG[19]), 원정강습단(ESG[20]), 상륙준비단(ARG[21]), 항공·수상·수중·특수작전 부대, 연합군 사령관 등에 의해 수행되는 의사결정 프로세스에 효과적으로 통합하기 위해 지원할 수 있어야 한다. 이러한 지원은 해양정보 전문가 집단과 기상해양사령부의 노력을 통해 제공된다.

해군·해병의 계획 프로세스는 전역(Campaign) 또는 작전 전 분야에 지속되는 기능이다. 작전이 시작되면, 지휘관은 관련 계획과 후속 계획이 포함된 명령을 동기화하고 통합해야 한다. 이때 정보관리(IM : Information Management) 과정을 통한 통제력을 발휘하는 것이 기본이다. 이를 통해 지휘 구조 내에서 수직 및 수평으로 우선순위를 정하여 동기화 및 통합해야 하고 '대상', '위치', '시기' 및 '이유'에 대한 정보를 얻을 수 있다. 이러한 해군·해병의 계획 프로세스 상에서 해양정보는 중요한 작전환경정보를 지원하며 지휘관 의사결정에 관여하며 단기·중기·장기 계획을 지원하는데 이때 4개의 BonD 계층 단계별로 적용된다. 또한, 해양정보 전문가 그룹은 작전환경에 대한 지식을 적용하여 지능적 추정치를 생성하고, 적 의도를 분석하여 작전환경정보와 최상의 방책을 결정하기 위해 지원한다.

가. 결심 주기

해군의 의사결정 주기는 평가, 계획, 명령, 감시 등 4단계로 진행되는데, 해양정보는 지휘관이 작전 준비 및 실행 단계상에서 작전환경을 이해하고 작전을 설계할 수 있도록 지원한다. 지휘관들은 상황 평가를 통해 계획을 집행 및 지휘하며, 전력에 임무를 부여하고 적 상황을 감시한다. 모니터링 결과는 다음 평가의 입력값을 제공한다.

17) Maritime Operation Center
18) Combined Task Force
19) Carrier Strike Group
20) Expeditionary Strike Group
21) Amphibious Ready Group

나. 대상 기간

해군 내 모든 조직은 장기・중기・단기 목표가 있다. 이러한 목표에 따라 작전 지휘관은 작전계획을 작성하고 집행한다. 해상작전센터(MOC)에서는 작전을 수행하는 작전사령부를 조직하여 장기・중기・단기별 현행 작전계획과 장차작전 계획을 수립하는데 이는 지휘관의 의사결정과 관련이 있다. 해양정보 팀을 지휘관의 참모로 배치함으로써 작전계획 프로세스 전반에 걸쳐 해양정보를 통합할 수 있다.

작전계획은 일반적으로 장기 사이클에서 시작하여 이벤트 실행 단계에서는 중기 계획을 거쳐 단기 계획으로 전환된다. 장기・중기・단기별 작전계획에는 공통적으로 해양정보 요소들이 반영되며 여기에 지휘관의 의사결정이 결합된다. 각 의사결정 주기의 순환속도는 시간 기준에 따라 다르다. 일반적으로 단기 결정주기는 중기 및 장기 결정 주기보다 더 빠르게 회전한다. 각 기간 별 의사결정 주기의 주요 특성은 현행작전과 장차작전을 일치시키기 위한 지휘관과 참모 활동 주기인 배틀 리듬에서 확인된다. 이렇듯 다양한 계획 분할은 시간이나 이벤트과 연관되어 있으며, 지휘 수준과 상황에 따라 달라진다. 일반적으로, 해양작전센터는 24시간 내의 활동에 현행작전계획을, 24시간에서 96시간 사이의 활동에 장차작전계획을 적용한다. 또한 96시간 이상의 활동에 대한 향후 계획도 수립한다.

다. 대상 기간에 BonD 개념 적용

BonD 개념의 4개 계층은 다음과 같이 장기・중기・단기의 작전계획과 연계될 수 있다.

장기계획의 초점은 미래에 대한 작전운영이다. 이 단계에서는 광범위한 정보지원 데이터를 개발・분석한다. 장기 분석은 종종 정보생산에 오랜 시간이 소요된다. 분석 소요 시간은 요청 사안의 공간적, 시간적 복잡성과 필요한 독립적 분석의 양에 따라 달라진다. 일반적으로 수집 데이터는 데이터베이스의 환경정보 및 과거 수집 정보와 연동되는데, 해당 결과는 BonD Tier 1과 2에서 생성된다.

BonD Tier 0, 1, 2는 중기 계획 중에 채택된 정보를 제공한다. 방책에서 파악되지 않은 것을 제외하고, 실행 완료된 작전에 대해 중기 계획은 완료된다. 중기에 진행되는 정보생산에 상당한 노력이 요구되나, 필요에 따라서는 1~2일 이내에 지원될 수도 있다. 장기 단계에서는 중기 단계와 일반적으로 동일한 데이터 매개변수가 사용되지만, 모델링 또는 예측 데이터를 사용함으로써 주어진 영역에 대해

훨씬 더 심층적인 분석이 가능하다.

단기 작전은 이미 실행 중이거나 이제 시작하려는 단계로써 대부분 완성된 데이터를 사용하기 때문에 통상적인 작전과 서비스가 고려된다. 그러나, 임무 구역과 관심 표적 대상의 범위가 작을 경우, 작업 시간과 데이터 송·수신 시간이 감소될 수 있으며 현장 데이터를 사용할 수 있다. 단기 데이터에는 관심영역(AOI : Area of Interest)에 대한 정적(static) 해양·대기 마스터 라이브러리(OAML : Oceanographic and Atmospheric Master Library) 데이터베이스와 동적(dynamic) 예측 데이터가 모두 포함된다. 정적 데이터의 사용 연도 범위는 데이터 유형과 관심영역에 따라 크게 달라질 수 있다. 모델 입력자료(무인잠수정(UUV) 등의 현장 수집자료) 또는 선박과 해안에서 관측된 현장 기상 관측자료를 지속 수집함으로써 BonD Tier 0, 1, 2의 정보는 모두 적용 가능하다.

라. 작전환경 정보분석(IPOE[22]) 및 전장 정보분석(IPB[23])의 계획 통합

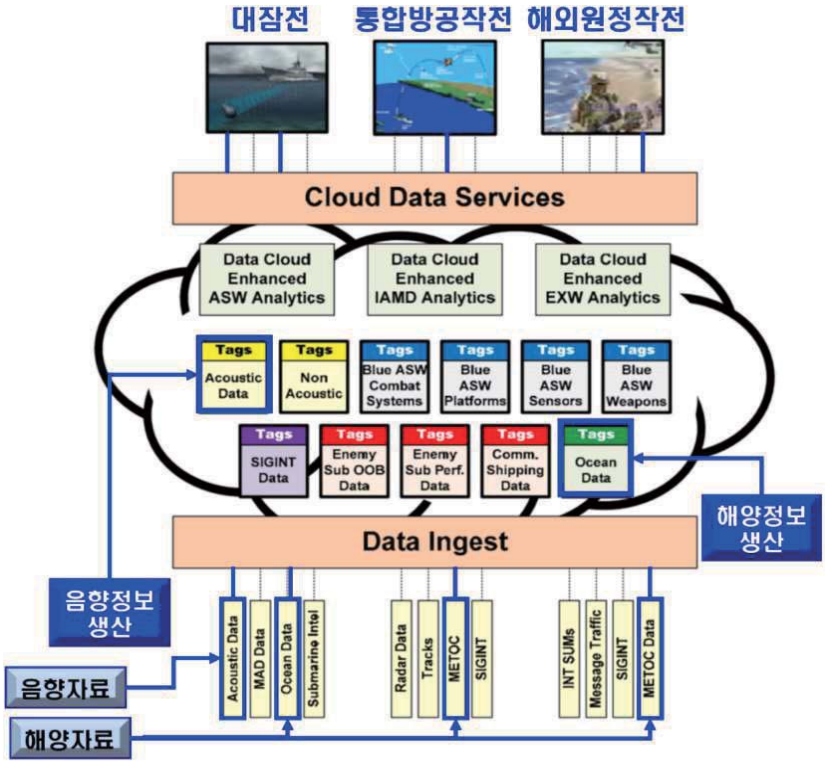
작전환경 정보분석과 전장 정보분석은 적·환경·시간·지형에 관한 불확실성을 줄이기 위한 것이다. IPOE 및 IPB는 계획 프로세스와 지휘관의 의사결정 주기에서 필수요소로서, 주로 장기부터 중기까지의 계획 프로세스를 지원한다. IPOE/IPB에 전체 환경에 대한 해양정보를 반영하여 지휘관의 상황인식을 향상시킨다. 해양정보에는 지휘관의 임무 수행 능력에 영향을 미칠 수 있는 지리적 제한사항 및 기타 물리적 특성이 강조되어 있다.

해병대 작전에서 IPB는 특정 지역의 위협과 환경을 분석하는 체계적이고 지속적인 과정을 수반한다. IPOE/IPB 과정 간에 전투력을 성공적으로 운용하거나 병력을 보호하고 임무를 완수하기 위해 이해해야 할 요소와 조건이 고려되어야 하는데 여기에는 항공, 육지, 바다, 우주, 적과 우호 세력, 시설, 날씨, 지형, 전자파 스펙트럼, 그리고 운용 영역, 관심 영역 및 영향 영역 내의 정보 환경이 포함된다.

22) Intelligence Preparation of the Operational Environment
23) Intelligence Preparation of the Battlespace

2.2.4 해양정보의 작전활용

미 해군은 '데이터 중심 해군전술클라우드(DF-NTC[24])' 체계를 구축하여 작전에 활용하고 있다. DF-NTC의 기본 개념은 해양정보, 음향정보, 지자기 자료, 레이다 신호, 표적정보, 신호정보, 영상정보, 정보요약 등 다출처 정·첩보자료를 클라우드 데이터 서비스를 통해 융합하고 대잠전, 통합방공작전, 해외원정작전 등 다양한 작전에 필요한 새로운 정보를 적시에 제공하는 것이다. DF-NTC는 미 해군의 빅데이터 시스템으로 개발되었는데, 지휘관의 의도 및 결심과 적·아 방책 구상을 위해 데이터를 통합하여 대잠전, 통합방공작전, 해외원정작전 등에서 효과적이고 신속한 계획, 평가 및 실행 지원을 위한 고급 분석을 수행하고, 전역(warfare domains)에서의 자동 예측 상황을 인지하고 최종 작전 판단을 지원한다.(〈그림 2-7〉 참조)



출처 : US Navy ONR, Data-Focused Naval Tactical Cloud

〈그림 2-7〉 DF-NTC에서의 해양정보 작전활용

24) Data-Focused Naval Tactical Cloud

3. 미래 해군의 모습과 해양정보체계 운용 개념

제3장에서는 해양안보환경과 해군력 운영개념 변화에 따른 우리 해군의 「SMART Navy」구현 계획을 통해 미래 우리 해군의 모습을 고찰하고 미 해군의 BonD 모델과 비교하여 향후 우리 해군의 해양정보체계의 운용개념을 수립한다.

3.1 해양안보환경과 해군력 운영개념 변화

지속적인 정부의 한반도 평화정착 노력에도 불구하고 여전히 북한에 의한 위협 불확실성이 상존해 있으며 한반도 주변국들은 비약적인 해군력 증강을 통해 영향력을 확대하고 있다. 중국은 해군력 증강을 위해 첨단 원양함대 전력을 강화하고 있는 가운데, 한반도 동・서・남해에서 활동을 증가시키고 있으며 일본은 공세적인 해양정책을 추구하면서 첨단 통합기동방위력을 강화하고 있고 독도에 대한 영유권 주장도 지속할 것으로 예상된다. 그리고 러시아도 원거리 해군 전력 투사 및 해상 작전능력을 보강하고 북극해 및 태평양에서의 활동을 강화하는 등 해군력을 발전시켜 나아가고 있다. 한편, 정치・경제・안보 등 전 분야에서 미・중 간 패권 경쟁이 심화되고 있는데, 미국은 중국을 전략적 경쟁자로 인식하고 공세적 행동에 나서고 있고 중국은 남중국해 영유권 확대 및 군사 거점화를 통해 미국의 항행자유작전에 대항할 것으로 예상된다. 이에 따라 미・중 간 해양 충돌 가능성은 확대되고 역내 안보상황의 불안정성은 심화될 것으로 예상된다.

이러한 안보상황과 맞물려 미래전의 양상은 매우 복잡하게 전개될 것으로 평가된다. 전장영역은 우주 및 사이버 공간으로 확대되면서 다영역에서 동시 또는 통합전이 수행될 수 있으며 인명피해를 최소화하고 저비용의 효과를 극대화하기 위해 무인체계를 발전시키는 등 유・무인체계가 융합된 복합전 형태로 전개될 가능성이 크다. 또한 ICT 기반의 첨단 네트워크를 활용하고 극초음속 미사일, 레일건 등 치명성을 갖춘 새로운 무기체계 개발을 통해 통합 정밀타격전을 수행할 것이다. 궁극적으로 미래전은 과학기술 발전과 함께 패러다임의 변화를 불러올 것이며 모든 수단이 동원되는 하이브리드전 형태로 전개될 것으로 예상된다.

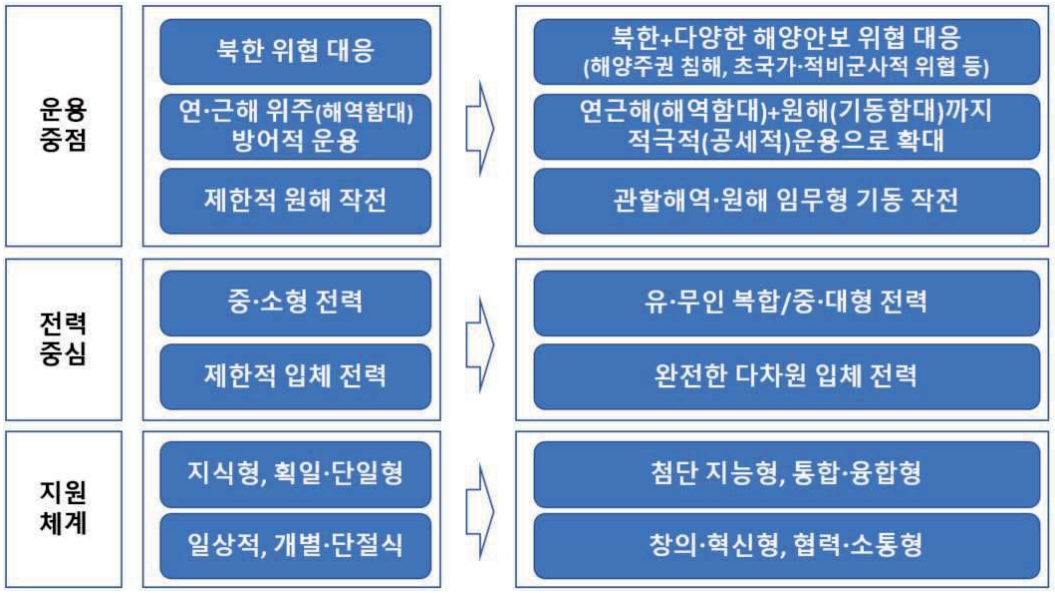
안보환경 변화와 미래전 양상의 변화에 따른 미래 해양안보의 과제는 직접적인 군사적 위협뿐만 아니라 국가 이익과 해양주권, 권익침해로 인한 다양한 분쟁 발

생 가능성을 고려하여 북한의 위협은 물론 주변국 등 잠재적 위협에 대비하여야 한다. 우리의 생존과 번영에 직결되는 해상교통로를 적극 보호할 수 있어야 하며 해적, 테러, 밀입국/난민, 밀수, 불법조업, 재해 및 재난 등 초국가적·비군사적 위협에 대해 능동적으로 대응해야 한다. 또한 향후 우리 군의 병력 부족, 인명 중시 등을 고려 시 인공지능, 빅데이터, 로봇 및 나노기술 등 첨단 과학기술 발전에 따라 무인 및 첨단 기술집약형 무기체계 개발에 노력해야 할 것이다. 국가적 차원에서 볼 때 대외 정책 지원을 위한 해군의 역할 증대가 예상되므로 미래 해양안보 위협과 국가 이익 수호를 위해 해군의 다양한 역할 수행과 능력을 구비해야 하며 해군 차원의 다양한 대·내외 협력체계도 구축해 나아가야 할 것이다.

따라서 해군력 운영개념도 패러다임의 전환이 요구되며 〈그림 3-1〉과 같다. 운용 중점은 북한의 위협을 포함하여 해양주권 침해와 초국가적·비군사적 위협 등 다양한 해양안보 위협에 대응하고 연·근해뿐만 아니라 원해역에서의 기동함대까지 적극적이고 공세적으로 전력 운용을 확대하여 관할해역과 관심해역에서 임무형 기동작전을 하는 것이다. 이를 위해 중·소형 전력 대신 유·무인 복합전력과 중·대형 전력으로 구성된 완전한 다차원 입체전력을 구축해야 할 것이다. 또한, 이러한 전력 운용 지원을 위해서는 첨단 지능형 통합 지원체계와 융합형 지원체계를 병행하여 구축해야 나아감으로써 향후 창의적이고 혁신적인 해군력 운용이 가능할 것이다.

우리 해군은 국가 및 정부의 해양비전과 연계하여 국가안보와 해양주권·권익을 수호하고 국제평화에 기여하기 위해 "해양강국, 대양해군"이라는 해군비전 2045와 "다양한 해양안보 위협에 대응하고 국제평화에 기여하는 해군"이라는 목표를 설정하고 있다. 해군비전 2045를 실현하기 위한 일환으로 "4차 산업혁명 첨단기술 기반의 「SMART[25] Navy」구현"을 계획하고 있다.

25) Strong Maritime forces Accomplished with Revolutionary Technology, '스마트(Smart)'라는 사전적 의미를 넘어 첨단기술로 미래 해군력을 달성하는 강한 의지를 함축한다.



출처 : 해군본부, 「해군비전 2045」(2020)

〈그림 3-1〉 해군력 운용개념 변화

3.2 「SMART Navy」추진 계획[26]

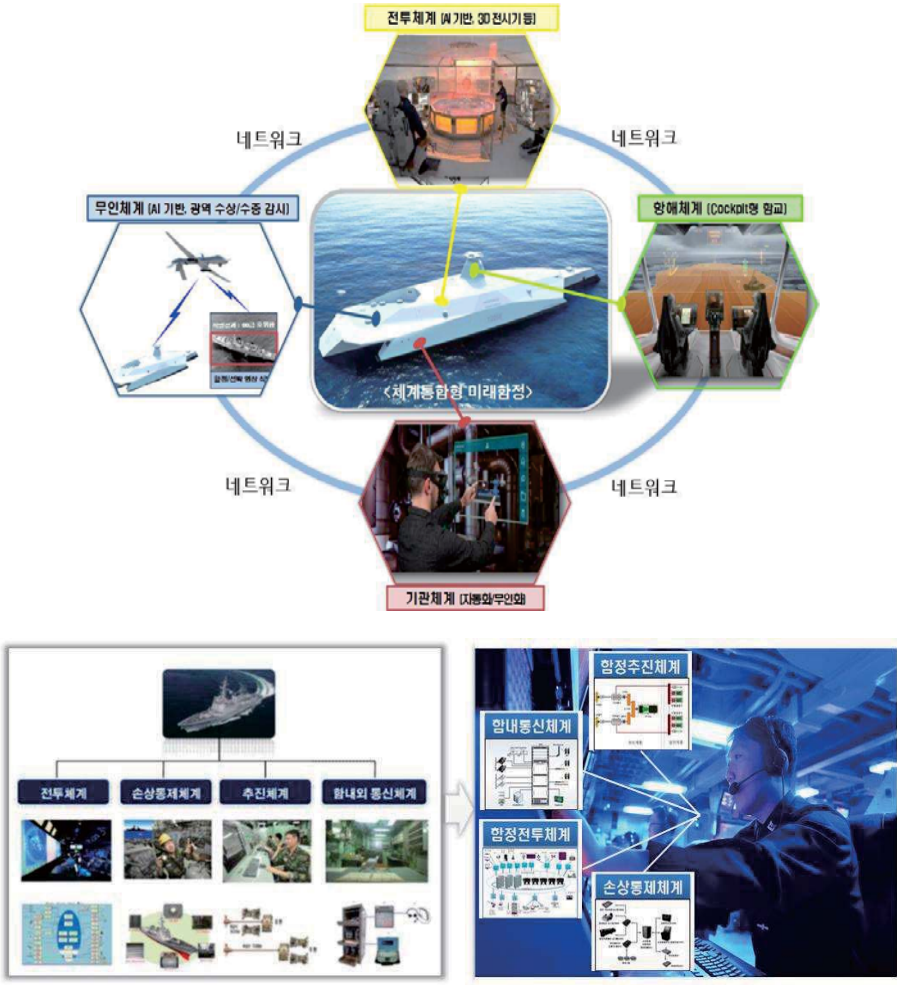
「SMART Navy」 2020년 3월 대한조선학회지에 게재된 "4차 산업혁명 첨단기술 기반의 'SMART Navy' 大항해 계획"을 요약하였다. 「SMART Navy」는 'SMART Battleship', 'SMART Operation', 'SMART Cooperation'이라는 3대 분야에 대한 추진 목표를 설정하고 있다.

3.2.1 SMART Battleship(스마트 전투함)

해군의 함정 및 항공기 등에 최신 첨단기술을 적용함으로써 전투성능을 극대화하는 것이며 이를 위해 다양한 탑재 장비를 통합 서버체계로 구축하여 전투 반응시간을 단축한다. 또한, 함정 자동화 기술을 적용하여 군수지원과 정비 효율성을 향상시킬 수 있다. SMART Battleship의 개념은 〈그림 3-2〉와 같다.

26) 박동선, "4차 산업형명 첨단기술 기반의 'SMART Navy' 大항해 계획", 대한조선학회지, 57(1), 7-10, 2020. 3.

SMART Battelship 구현을 위해 다음과 같은 목표를 설정하고 있다.



〈그림 3-2〉 SMART Battleship 개념도[27)]

① 선진형 함형 발전 : 선진 기술발전 고려한 함형 발전
② 신기술 적용 탐지감시장비 개발
: 디지털기술 기반 고성능 레이더 및 신기술 적용 표적처리체계 개발

27) 해군본부 홈페이지, "스마트 해군 건설 추진", 2018.

③ 차세대 지능형 통합 전투체계 개발
: 전투 지휘통제를 위한 체계 통합, 빅데이터 기반의 전투체계 관리
④ 함 운영 통합/자동화체계 구축
: IT 기반 함정 주요 통제시스템 및 인원절감형 통합 함교체계 구축
⑤ 함정 무기체계 자동화체계 구축
: 함정 탄약고 자동화 구축, 무기체계 관리의 디지털화
⑥ 함정 모바일 통신체계 구축
: 함내 무선네트워크 서버 구축, 승조원용 웨어러블 디바이스 개발
⑦ 함정 무기체계 사이버방호체계 구축
: 인공지능 기반 사이버보안 솔루션 구축

3.2.2 SMART Operations(스마트 작전운용)

함정, 항공기, 육상부대 간 네트워크화로 통합 전투력을 발휘하고 운용효과를 극대화한다. 이를 위해 입체적 감시능력을 확충하며 유·무인전력 통합운용 기반 조성과 네트워크 중심 지능형 지휘통제체계를 구축하고 다음과 같은 목표를 설정하고 있다.

① 해양무인체계 발전 : 무인체계 운용개념 정립
② 지능형 지휘통제체계 구축
: 지능형 통합정보분석체계 및 지능형 전술 C4I체계 구축
③ 광해역 전장감시체계 구축
: 광해역 수중감시체계 및 초수평선 레이더체계 구축
④ 지능형 군수지원/정비체계 발전
: 원격 정비체계 구축, 3D 프린팅 활용 수리부속 원격제작
⑤ ICT 기반 항만/기지 관리체계 구축
: 5G/드론 기반의 경계체계 및 지능형 항만/기지 근무지원체계 구축
⑥ 통합 교육훈련체계 발전
: 지역별 훈련체계 간 연동체계 및 실기동 전력과 연계한 통합체계 구축
⑦ 지능형 지식관리체계 구축
: 통합 검색엔진 개발, 클라우드 기반의 자료 공유체계 구축

3.2.3 SMART Cooperation(스마트 협력)

해양안보와 관련하여 국내・외 협업체계를 구축함으로써 비군사적 위협 대응능력을 강화하고 해양주권을 수호한다. 이를 위해 국제 협력체계를 강화하고 국내 민・관・군 해양 네트워크를 구축하는 것이다. 목표 설정은 다음과 같다.

① 국제 해양유관기관 협업 강화
: 국제 해양정보공유시스템 구축, 국가 간 국제해양정책발전 협업 강화

② ICT 기반 국내 해양재난관리체계 구축
: 행안부 PS-LTE 기반 재난안전통신망 및 해양 재난상황관리체계 구축

3.3 해양정보체계 운용 개념

해양정보업무의 최종 목표는 정확하고 적시적이며 효과적・효율적인 해양정보 지원을 통해 성공적인 해군작전을 보장하는 것이다. 그러나 현재까지 구축된 체계는 여러 측면에서 제한되는 부분이 많다. 수집자료의 정확성과 적시성, 분석체계의 정밀성, 관리체계 운용의 효율성과 효과성, 전파체계의 적시성 등 측면에서 여러 불확실성 요소들이 존재한다. 이러한 불확실성을 감소시키기 위해 미 해군이 발전시킨 BonD 모델을 우리 해군에 적용시킬 수 있는 방안에 대한 검토가 필요하다.

3.3.1. 미 해군 BonD 모델 적용

미 해군의 BonD 모델은 작전운용 개념을 기반으로 해양정보 지원 업무를 구성하였는데 각 계층별 해양정보 지원 업무를 정의하기 위해서는 미 해군과 같이 탄탄한 해양정보 업무 조직과 미 해군과 유사한 수준의 해양정보 수집・관리・분석 체계를 보유하고 해양정보를 원활하게 유통할 수 있는 전파체계 구축이 선행되어야 한다. 그러므로 BonD 모델을 우리 해군의 해양정보 업무 발전을 위한 모델로 적용하는 데에는 해양정보 업무 조직, 해양정보 및 작전지원체계, 위성통신 및 해군 C4I체계 측면에서 제한사항이 존재할 수밖에 없다.

제2장에서 언급한 바와 같이 미 해군은 참모총장의 해양참모와 기상해양 병과의 인력을 운용하고 있고 기상해양사령부 예하에 함대수치예보센터, 해양국, 전 세계에 다수의 기상해양센터 등 방대한 규모의 인력과 조직을 운용하고 있다. 우리 해군의 동일 업무 조직은 미국과 비교하여 비교하기 어려울 정도로 규모가 작다. 이

러한 작은 규모로 BonD 모델의 각 계층에서의 해양정보 업무를 정의하는 것은 각 계층 별 업무 수행 수준의 차이가 커서 무리가 있다. 특히, 작전 지원 능력의 차이는 매우 크다고 할 수 있다.

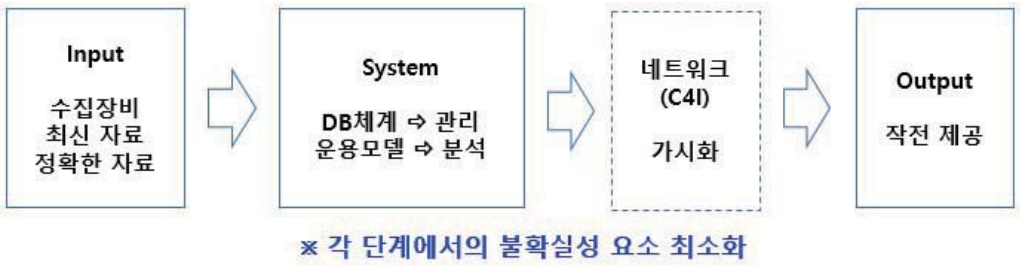
또한, BonD 모델은 미국과 같은 수준의 해군작전을 지원할 수 있는 해양정보 수집・관리・분석체계를 보유하고 있어야 한다. 미국은 해양국에 모든 해양환경 데이터를 수집할 수 있는 4,000톤급 이상의 해양조사선 7척을 보유하고 있으며 UUV, AUV, 수중글라이더 등의 무인체계, 관측 부이, 위성관측센서 등 실시간 해양 관측시스템을 보유하고 있다. 방대한 양의 데이터를 관리할 수 있는 데이터베이스도 구축하고 있어 이미 빅데이터 분석 시스템을 적용하고 있다. 해양정보 모델은 세계 최고 수준의 공학 모델과 함께 많은 수퍼컴퓨터를 운용하고 있다. 해양정보 관련 시스템은 타 작전지원체계와도 연동되고 있는데, 이와 같은 체계를 기반으로 Bond 모델의 '퍼포먼스 계층'에서의 상황 인식이 가능하며 작전 판단을 위한 결심 지원이 가능하다.

미 해군은 위성통신 및 해군 C4I체계를 기반으로 전 세계 해역을 전구로 하여 작전을 수행하고 있는데, 이는 단지 BonD 모델의 '결심 계층'에 국한된 것이 아니라 해양정보 지원 전체에 영향을 미친다. 즉, 각 단계별 수집・분석・처리・생산되는 해양정보가 다음 단계로 지원되기 위해서는 대용량의 정보를 송・수신할 수 있는 통신체계가 기반이 되어야 한다. 이러한 제한사항을 무시하고 BonD 모델을 우리 해군의 해양정보 업무 모델에 적용하는 것은 바람직하지 않을 것으로 판단된다. 대신, 미 해군의 BonD과 비교하여 또 다른 방식의 세부적인 프로세스로 구분하고 각 프로세스에 대한 체계를 구성함으로써 해양정보체계의 운용 개념을 수립하고자 한다.

3.3.2 해양정보체계 운용 개념

미 해군의 BonD 모델을 우리 해군의 해양정보 업무 모델로 설정하기에는 무리가 있으나 업무 조직과 보유하고 있는 체계의 수준이 미군보다 낮다고 하더라도 현재 보유하고 있는 체계를 기반으로, 해양정보의 유통 단계별 불확실성을 최소화할 방법을 마련하고 향후 새로운 체계 획득을 통해 우리 해군 규모의 수준에서 최대한 정확하고 적시적이며 효과적・효율적인 해양정보 업무 및 체계발전을 달성할 수 있을 것이다.

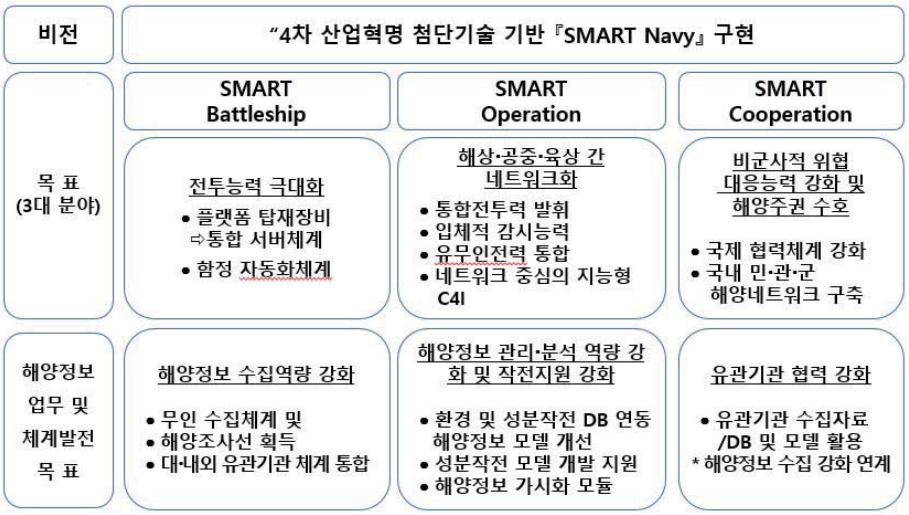
체계적 접근(Systematic approach)을 통한 사고를 통해 〈그림 3-3〉과 같이 BonD 모델이 아닌 정보순환 4단계 즉, 수집・분석・처리・전파 측면에서 단순화하여 해양정보 업무의 불확실성 요소를 식별하고 개선할 방안을 찾을 수 있을 것이다.



〈그림 3-3〉 체계적 접근을 통한 해양정보 업무 및 체계 운용 단계

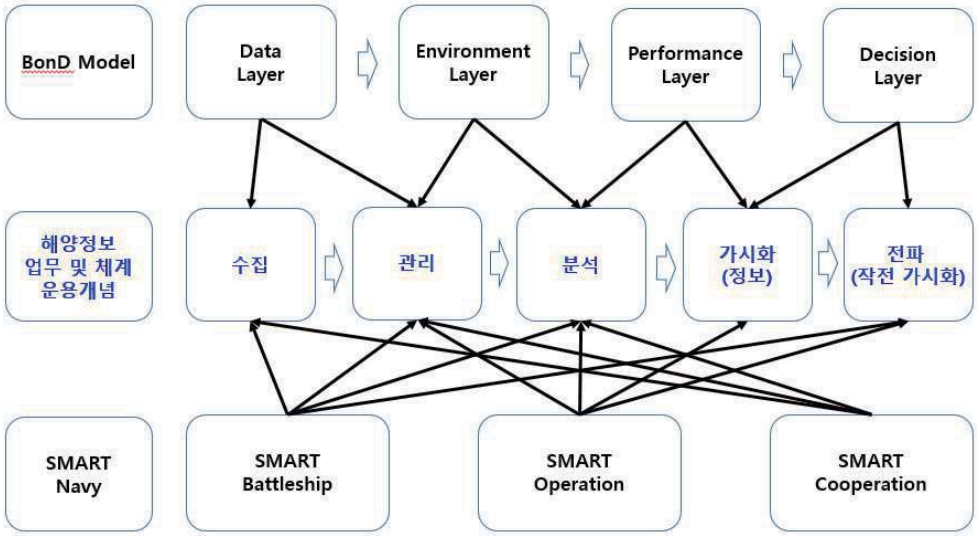
한편, 해군의 "4차 산업혁명 첨단기술 기반의 「SMART Navy」구현을 해양정보 업무 발전과 연계하고자 한다. 「SMART Navy」구현의 3대 분야인 'SMART Battleship', 'SMART Operation', 'SMART Cooperation' 측면에서 각각 '전투능력 극대화', '해상공중육상 간 네트워크화', '비군사적 위협 대응능력 강화 및 해양주권 수호'라는 목표가 있다. 이를 해양정보 업무 및 체계발전과 연계하면 〈그림 3-4〉와 같이 생각해 볼 수 있다.

'SMART Battleship' 분야에서는 해양정보 수집역량을 강화하기 위해 무인 수집체계와 해양조사선을 획득하고, 수집되는 해양정보는 향후 새롭게 구축할 해양정보 관리・분석체계에 통합되어야 할 것이다. 'SMART Operation' 분야에서는 해양정보 관리・분석 역량을 강화하고 작전지원을 확대해야 할 것이다. 이를 위해 해양・기상・해저지형 등 환경 데이터베이스와 성분작전 데이터베이스를 연동해야 할 것이며 성분작전 모델도 병행해서 개발해야 한다. 또한, 이들 체계로부터 생산된 해양정보를 작전에서 효과적으로 활용하기 위한 가시화 방안도 마련되어야 할 것이다. 'SMART Cooperation' 차원에서는 대내・외 유관기관과의 협력을 강화하여 방대한 규모의 실시간 수집자료를 해군 해양정보 관리・분석체계와 연동을 통해 유관기관의 수집자료와 데이터베이스, 모델을 활용할 수 있어야 할 것이다.



〈그림 3-4〉「SMART Navy」와 연계한 해양정보 업무 및 체계발전 목표

종합하면, 우리 실정에 맞는 해양정보 업무 및 체계 운용개념은 〈그림 3-5〉와 같이 해양정보 수집, 관리, 분석, 가시화, 전파 단계별로 정립해야 하며 미래 해군을 위한 스마트 해양정보체계 구축 방안도 이를 기반으로 제4장에서 제시하였다.



〈그림 3-5〉 해양정보 업무 및 체계 운용개념

4. 해양정보체계 구축 방안

4장에서는 3장에서 다루었던 미래 우리 해군의 모습과 그에 따른 해양정보체계 운용개념을 바탕으로 해군의 해양정보체계 구축 방안을 다루며 해양정보 수집체계, 관리 및 분석체계, 전파체계로 구분하여 해양정보체계 구축방안을 제시한다.

4.1 해양정보 수집체계

성공적인 성분작전 보장을 위해서는 작전에서 요구하는 해양정보를 적시에 수집하여 지원할 수 있어야 한다. 향후 우리 해군의 해양정보 수집체계 구축 목표는 작전해역을 포함한 관심해역에서 모든 해양·음향정보를 적시에 지원할 수 있는 환경자료를 수집할 수 있는 체계를 구축하는 것이다.

해군작전을 지원하기 위한 해양정보 분석에 활용되는 수집 데이터와 수집 장비/체계는 〈표 4-1〉과 같다. 해군의 대표적 성분작전인 대잠전, 잠수함전, 기뢰전, 상륙전, 특수전 및 구조전에 활용하기 위한 수집 데이터는 수심별 수온 및 염분, 배경 및 표적 소음, 해저 지형 및 저질, 유향 및 유속, 수중 시정 및 투명도 등이다. 그런데 이들 수집 데이터 중 기상청 또는 육상 관측소에서 수집되는 기상자료와 임무 중인 함정 및 항공기에 탑재된 (A)XBT[28]를 이용한 임무해역에서의 일일 단위 수심별 수온 데이터 등이 실제 해군에서 직접적으로 실시간 수집·활용이 가능하다. 배경 및 표적소음 등도 실시간 수집 및 분석이 가능하나 정밀 분석 등을 위해서는 임무 종료 후 사후 분석까지 상당한 시간이 요구된다. 기타 해양환경자료의 경우에는 해양조사원, 한국해양과학기술원 등 유관기관이 보유하고 있으나 데이터를 해군이 적시에 활용하는 측면에 있어 해군과 동 기관들과의 전용 구축망 미구축 등으로 제한이 있는 실정이다.

따라서 이러한 제한사항들을 극복하여 해양정보 수집 업무를 발전시키기 위해서는 최소한 (근)실시간 해양정보 수집이 가능한 수준의 체계를 확보함으로써 가능할 것으로 판단된다. 본 연구에서는 체계 개발 및 확보가 요망되는 해양정보 수집체계로서 대내·외 해양정보 연동체계, 해군이 독자 운용 가능한 해양조사선, 해양환

28) (Airborne)EXpendable Bathy Thermograph

경 수집장비를 탑재한 감시・정찰 무인체계 등을 제시한다.

〈표 4-1〉 작전 분야별 해양환경정보 수집 자료 및 장비

작전 분야	수집 해양환경자료	수집 장비
대잠전 잠수함전	수심별 수온	(A)XBT(함정/항공기)
	수심별 수온, 염분	CTD(잠수함/정보함)
	수심별 수온, 배경소음	수중글라이더
	표적소음 음원, 배경소음	함정/항공기 능・수동소나
기뢰전 구조전 상륙전 특수전	해저 지형 및 저질	멀티빔/사이드스캔 소나 Bottom Sampler
	유향, 유속	유속계, ADCP
	수중시정, 투명도	White disk

4.1.1 대내・외 해양정보 연동체계 구축

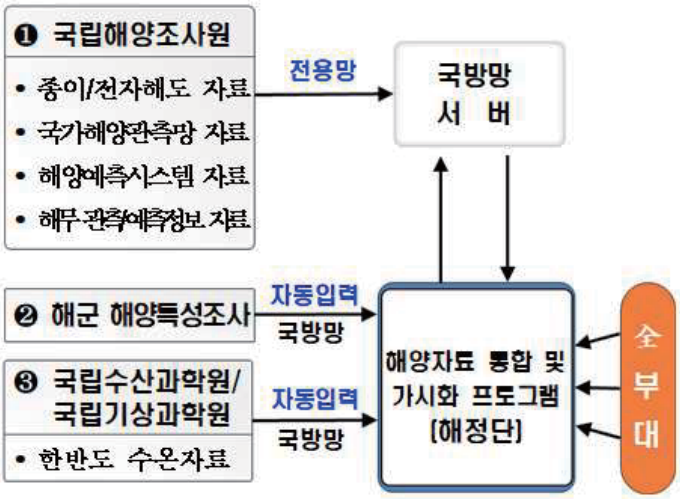
국립해양조사원은 해양관측에 관한 계획을 수립하고 수립된 계획을 바탕으로 해양 물리환경과 해양기상에 관한 조사를 수행하며 조석 및 조류 등 해양현상을 추산하고 예보한다[29]. 또한, 종합해양과학기지를 운용하고 있으며 국가 해양관측망을 구축하여 운용하고 있고 해양조사선과 다양한 해양조사장비를 운용하고 있다. 국립해양조사원은 이와 같이 다양한 수집체계를 통해 (근)실시간 해양정보 수집이 가능하며 이렇게 수집된 자료를 이용하여 다양한 해양수치모델의 입력자료로 활용하여 해양예보 업무를 수행하고 있다. 현재 우리 해군은 특정 사업을 통해 국립해양조사원의 아주 일부 자료만을 수신하여 이용하고 있다. 국립해양조사원 외에도 국립수산과학원과 한국해양과학기술원의 일부 해양환경자료를 off-line 상으로 수집하여 활용하고 있다.

국립해양조사원과 같은 국가기관에서 수집한 양질의 많은 해양환경자료를 해군이 자체적으로 수집하여 활용하기 위해서는 많은 예산이 투입되어야 하는데, 사업의 효율성 측면에서만 보더라도 이는 바람직하지 않다. 국립해양조사원은 우리나라의 해양과학조사자료 관리기관의 역할을 하고 있으므로 해양정보를 필요로 하는 기관에서 동 자료를 활용하는 것은 국가적 차원에서 자료를 공유하여 공동 활용도

29) https://www.khoa.go.kr/kcom/cnt/selectContentsPage.do?cntId=25401000

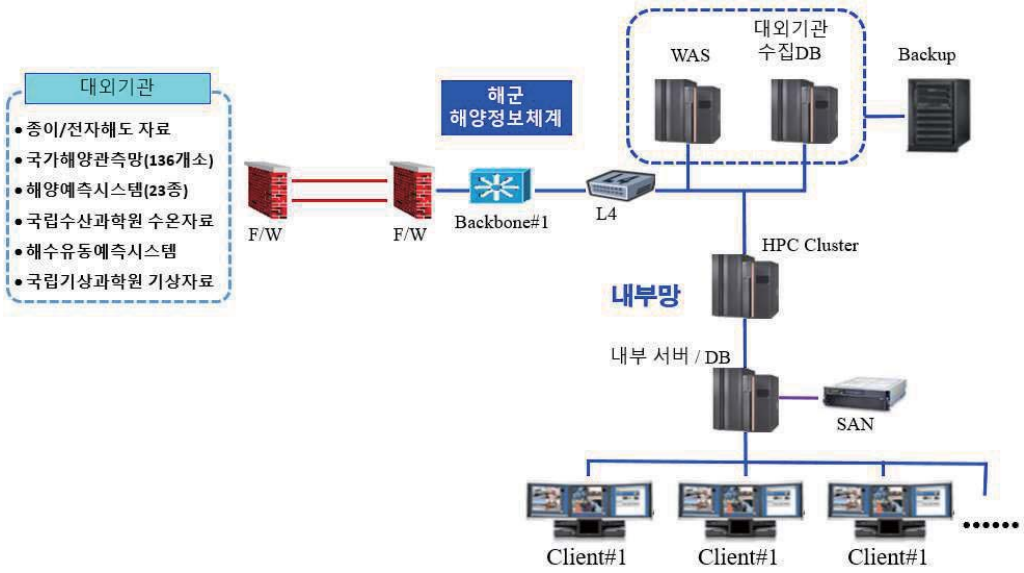
를 높이는 일이며 국가 예산 활용의 효율성도 증대시키는 것이라 할 수 있다. 따라서 국립해양조사원과 해군이 연동망을 구성할 수 있다면 (근)실시간 수집된 해양환경자료와 동 기관에서 확보하는 수치모델 운용 결과도 해군이 활용할 수 있을 것으로 판단된다.

2021년 3월 해군본부는『해양자료 통합 및 가시화 프로그램 개발』사업을 발주하였는데 동 사업을 통해 국립해양조사원 등 대외기관과 해군 간 해양정보 연동체계를 구성할 계획이며 〈그림 4-1〉와 같다. 체계 연동 기본 개념은 먼저 국립해양조사원과 해군 간 인터넷 전용망을 설치하고 국립해양조사원의 국가해양관측망 자료, 국립수산과학원 수온자료, 해양예측시스템 및 해수유동예측시스템의 해양수치모델 자료, 시정자료 등의 자료를 포함한 해양 데이터베이스 자료를 해군 보유체계에 수신하여 활용하는 것이다. 또한 웹서버 체계를 구축하여 국립해양조사원 수신자료와 해양특성조사 사업 결과자료, 기타 유관기관 수집 해양자료를 관리 및 활용할 수 있을 것이다. 동 사업을 통해 연동체계는 향후 〈그림 4-2〉와 같이 발전시켜야 할 것이다.



출처 : 해군본부, 제안요청서『해양자료 통합 및 가시화 프로그램 개발』, 2021. 3.

〈그림 4-1〉 해군과 국립해양조사원 간 해양정보 수집 연동 개념



〈그림 4-2〉 해군과 대외기관 간 해양정보 수집 연동 개념

4.1.2 해군 독자적 해양조사선 확보

한반도를 둘러싼 주변국들은 미래의 해양분쟁 가능성에 대비하고 있으며 자국의 해양주권을 공고히 하기 위해 해양환경조사 활동도 강화하고 있다. 중국은 일본에 대하여 조어대 영유권 분쟁에 대한 정기순찰을 지속하고 있고 일본은 중국의 움직임에 대한 대응의 일환으로, EEZ 관리강화법 추진 등을 통해 동중국해에서 발생하는 중국의 일방적 자원개발과 해양조사, 플랫폼 건설 등을 경계하고 있다. 실제, 동아시아에서 벌어지고 있는 국가 간 분쟁들의 대부분은 해양주권과 연관되어 있으며, 세력 간 충돌의 공간은 해양이 될 가능성이 매우 높다. 동아시아에서 국가 간 해양충돌 발생 시 대한민국은 직·간접적으로 분쟁에 개입될 소지가 다분할 것이며, 이에 따라 우리 해군도 동아시아 해역에서 작전을 수행할 준비가 필요할 것이다.[30]

해군의 요구에 부응하는 국외 관심 해역에 대한 해양환경조사가 원활히 이루어지기 위해서는 해양조사선 파견을 통한 해양정보수집이 가장 이상적이다. 작전 임무를 수행 중인 전투함을 통해 해양환경조사를 수행하기에는 과중한 임무 부담과 주변국과의 외교적, 군사적 마찰을 발생시킬 수 있기 때문에 해군 자체 해양조사

30) 양희철, "동북아 해양분쟁에서 해양안보의 중요성과 국제동향", 한국해양과학기술원, 2016.

선을 확보하는 방안이 마련되어야 할 것이다. 해양 선진국들은 해양환경조사를 국가 차원에서 장기간의 대형 사업으로 수행하고 있으며, 장차 발생할 해양에서의 물리적 충돌에 대비하고 해양영토(관할수역) 확장 협상을 자국에게 유리하게 이끌기 위해 경쟁적으로 조사에 매진하고 있다. 대양해군 건설에 매진하고 있는 우리 해군도 해양조사선 운용을 통한 국외 분쟁 해역에 대한 해양정보 수집은 장차작전과 해양 주도권 확보를 위해 필수적이다.

우리 해군의 해양환경 조사능력 확보를 위해서는 2가지 방안이 있는데 첫째는 차기 정보함 건조 시 해양조사장비 탑재를 반영하는 것이고, 둘째는 독자적 해양조사선을 확보하는 것이다. 첫 번째 방안은 예산 확보 및 운영 측면에서 매우 효율적일 수 있으나 현재 정보함의 임무를 고려 시 정보 수집 본연의 임무 외에 해양조사 임무를 부가적으로 수행하는 것이 효율적이고 효과적일지에 대해서는 부정적일 것으로 판단된다. 왜냐하면, 정보함의 임무는 합참(정보본부)과 해군 작전사의 정보수집 명령에 따라 함행동이 결정되는데 해양조사 임무를 부가 의무로 부여하는 것은 부적절할 수 있기 때문이다. 또한, 해양환경자료 수집이 필요한 시기와 필요한 해역이 정보함 고유의 임무 해역 및 시기와 상이할 때 과연 원활한 해양정보 수집이 가능할 것인지에 대해서도 부정적일 것으로 생각한다. 따라서 첫 번째 방안보다는 두 번째 방안인 해군 독자적인 해양조사선을 확보하는 것이 최상의 방안으로 판단된다.

우리 해군의 부족한 해양정보의 작전지원 능력 측면을 고려하여 획득이 요구되는 해양조사선의 제원과 특징을 제시하기 위해서 먼저 해양조사선의 임무, 운용요원, 함정제원, 탑재장비 등 네 가지 사항을 기준으로 분석하였다. 이를 위해 미 해군 해양국의 해양조사선과 한국해양과학기술원의 해양조사선 능력을 분석하였고 해군 해양조사선의 주요 특징 및 제원은 〈표 4-2〉와 같다.

〈표 4-2〉 해군 해양조사선의 주요 특징 및 제원(안)

구분		주요 특징 및 제원
임무	해역	· 한반도 주변 해역
	시기	· 연중, 작전사령부 지시에 의거
	내용	· 해군 성분작전 및 훈련 지원 · 연중 관심해역 해양정보 DB화 · 해양특성조사 사업 지원 · 수리 함정 음향측정 지원
운용 요원	인원수	· 함정 톤수 고려 * 한국해양과학기술원 온누리호(연구 25, 운용 16)
	인원 구성	· 함정운용 요원은 당직 및 정비인원을 고려 최소화 · 탑재장비 운용요원과 장비별 분석요원으로 구성
	기타	· 대외기관 연구인력 투입 가능
함정 제원	톤수	· 원해역 임무 고려 시 2,000톤 이상
	길이/폭	· 80m / 15m 기준
	속력	· 10~15 Kts
탑재 장비	무장	· 없음 * 임무를 고려하여 해양정보 관련 장비 위주 탑재
	기본	· 항해용 레이더 및 통신장비
	해양 정보 수집 장비	· CTD/XBT : 수심별 수온 측정
		· Multibeam Sonar : 고해상도 해저지형정보 수집
		· ADCP : 수층별 유향 및 유속 측정
		· Towed Hydrophone : 배경소음 측정
		· Acoustic Transmitter : 음원 발생기
		· Bottom Sampler : 해저저질 시료 채취
		· 모의 기뢰 : 기뢰 매몰률 측정
		· White Disk : 수중 시정 측정
		· 수중글라이더 등 무인체계 : 수중 해양정보 수집
		· 자동 기상정보 시스템 : 실시간 기상정보 수집

4.1.3 해양무인체계 확보

우리 해군의「SMART Navy」구현 목표 중 하나인 'SMART Battleship'의 과제 중에는 해양무인체계 운용이 포함되어 있는데, 향후 건조할 함정들에 무인체계 탑재를 고려하고 있으며 이를 위한 공간 확보, 무인체계의 지휘통제, 진수 및 회수를 위한 기술적인 방법이 연구되고 있다. 해양무인체계는 크게 무인수상정(USV)과 무인잠수정(UUV)으로 구분할 수 있다. 무인수상정은 모함 또는 육상 기지에서 원격조종되는 무인 고속선박으로 위험구역에 대한 정보수집, 대함전, 대잠전, 대기뢰전, 항만과 연안 정찰 및 감시, 상륙작전구역 정찰 등 다양한 임무를 수행할 수 있으며 임무에 따라 정보수집용, 정찰 및 감시용, 전투용으로 구분되며, 크기에 따라 소형, 중형, 대형, 초대형으로 구분된다.[31] 무인잠수정은 잠수함, 수상함, 항공기, 연안기지 등 다양한 플랫폼과 장소로부터 전개 및 회수가 가능하며 수중 저소음 무인 잠항능력 등 은밀성을 극대화할 수 있는 장점이 있다. 임무에 따라 감시 및 정찰용, 전투용, 기뢰처리용 등으로 구분하고, 크기에 따라 소형, 중형, 대형으로 구분된다. 해양무인체계 개발에 가장 앞서있는 미국의 개발현황은 〈표 4-3〉과 같으며 해양정보 수집은 휴대용부터 대형에 이르기까지 다양한 형태의 무인체계 개발이 진행되고 있다.

〈표 4-3〉 미 해군 해양무인체계 개발현황

임무	휴대용	소형	중형	대형
ISR (정보/감시/정찰)	O (근거리)	O	O	O
MCM (기뢰 탐색제거)	O	O	O	-
ASW (대잠전)	-	-	-	O
Oceanography (해양정보 수집)	O	O	O	O
개발장비	REMUS100 Bluefin-9	CETUS-II Bluefin-21	LMRS, MRUUV(21)	LDUUV, Manta

출처 : U.S. Navy,「Unmanned Underwater Vehicle Master Plan」

31) 이필승 외, "미래 해상무인/자율무기체계 개발 방향 연구", 제2장 제1절 1.미국(요약), 2018.11

해양무인체계는 성분작전 지원 및 수행뿐만 아니라 감시·정찰 임무 수행에도 향후 중요한 역할을 수행할 수 있을 것으로 예상된다. 그런데 우리 해군의 해양무인체계 계획에는 해군의 중요 정보 분야인 해양정보 수집 분야는 누락되어 있다. 해군작전의 성공 보장을 위해서는 정확하고 적시적이며 효과적인 해양정보를 지원할 수 있어야 하며 지금까지의 우리 해군의 부족했던 분야인 해양정보 수집 공백을 채우기 위해서는 해양정보 수집용 무인체계 개발 및 획득을 통해 해양정보 업무를 발전시켜 나아가야 할 것이다.

해양무인체계 중 해양정보 수집용 무인체계로 수중통신의 한계가 있는 무인잠수정보다는 무인수상정이 적합할 것으로 판단된다. 무인수상정은 통신능력에서 자유로울 뿐만 아니라 무인잠수정에 비해 선체 중량을 크게하여 다양한 해양장비 탑재가 가능할 것으로 평가된다. 국내에서는 2004년부터 민군 겸용 과제로 무인수상정 개발을 시작하여 해양탐색 등 다양한 임무를 수행할 수 있는 무인수상정이 개발되었다. 최근 동향으로 2019년에 한화시스템은 자율주행 복합 임무 무인수상정 'M-Searcher'를 개발하였고 LIG넥스원은 2020년 11월에 감시정찰 장비를 탑재한 '해검-Ⅲ'를 공개하기도 하였다. 현재까지 국내 무인잠수정 개발 동향을 고려 시 기술 수준은 성분작전 지원 측면에서는 일부 부족할 수 있으나 해양정보 수집 분야는 충분히 개발 가능할 것으로 평가된다.

해양정보 수집을 위한 무인수상정을 획득 방안은 ① 해양정보 수집용 무인수상정을 개발하는 방안과 ② 향후 신형 함정 탑재 예정인 무인수상정에 해양정보 수집장비를 탑재하는 방안이 있다. 운용 측면에서 보면 ① 육상 통제소 운용 방안과 ② 함정 탑재 운용 방안이 있다. 육상 통제소에서 운영하는 방안은 무인수상정의 크기에 제한이 없으나 원거리 운용에 제한이 있을 수 있다. 함정에 탑재하는 방안에는 신형 건조되는 전투함에 탑재하는 방안과 신형 정보함 등에 탑재하여 운용하는 방안이 있다. 각 방안 별로 여러 장·단점과 제한사항이 있는데, 특히 함정 탑재 운용방안과 관련해서는 기존의 함정 임무에 해양정보 수집 임무가 추가되는 부담이 생길 수 있어 무인수상정 운용을 담당하는 요원이 별도 편성되어야 하는 등 다각도의 검토가 필요할 것이다.

해양정보 수집을 위한 무인수상정의 주요 특징 및 제원을 〈표 4-4〉와 같이 분석하여 제시한다.

〈표 4-4〉 해양정보 수집용 무인수상정의 주요 특징 및 제원(안)

구분		주요 특징 및 제원
임무	해역	· 한반도 주변 해역, 함정 탑재 시 파견 수역 포함
	시기	· 함정 임무 중 · (육상 운용 시) 해양정보 수집지침 의거
	내용	· 임무 해역 내 실시간 해양정보 수집
운용요원		· 무인수상정 운용 자격 부여 인원
기본 제원	톤수	· 약 10톤
	길이/폭	· 12~15m / 2m(이내)
	속력	· 5~10 Kts
탑재 장비	기본	· 항해용 레이더 및 통신장비
	해양 정보 수집 장비	· CTD/XBT : 수심별 수온 측정
		· Multibeam Sonar : 고해상도 해저지형정보 수집
		· ADCP : 수층별 유향 및 유속 측정
		· Towed Hydrophone : 배경소음 측정
		· Acoustic Transmitter : 음원 발생기

4.2 해양정보 관리 및 분석체계

해양정보 수집체계로부터 수집된 데이터는 해양정보 데이터베이스에 저장되어 관리되어야 한다. 해양환경자료는 시간영역과 공간영역에 따라 변동성이 많기 때문에 끊임없이 지속적으로 수집하여 관리되어야 하므로 데이터베이스는 매우 중요한 역할을 한다고 할 수 있다. 예를 들어, 주간 단위 이상의 예보를 제공하기 위해서는 현재 이전의 관측자료가 체계적으로 잘 관리되어 있어야 특정 기간에 대한 환경의 경향성을 정밀하게 분석할 수 있을 것이다.

데이터베이스는 확장성도 있어야 하는데, 데이터가 체계적으로 잘 관리되고 있다면 데이터베이스는 타 체계와의 연동도 매우 용이할 것이다. 데이터베이스는 데이터 관리라는 측면에서 중요하지만 저장된 데이터를 추출하여 우리가 원하는 정보를 생산할 수 있는 분석모델과의 연동이 무엇보다 중요하다. 우리가 원하는 해양

정보는 분석모델을 통해 생산되며 분석모델의 기본 입력 데이터는 결국 데이터베이스로부터 추출되기 때문이다. 또한, 이러한 분석모델은 해양환경분석 모델만 있는 것이 아니라 기상환경분석 모델, 음탐환경분석 모델, 기뢰전 등 성분작전 별 분석모델도 있다. 이러한 다양한 분석모델들은 자체 데이터베이스뿐만 아니라 다른 데이터베이스와도 연동될 수도 있는데, 이를 통해 보다 정확하고 다양한 새로운 정보를 획득할 수 있다.

우리 해군이 추진하고 있는 4차 산업기술 기반의 「SMART Navy」 구현에도 데이터베이스 구축은 매우 중요하다. 빅데이터 및 인공지능 기술 적용을 위해서는 기본적으로 정형 데이터 관리가 제대로 이루어져야 하기 때문이다. 데이터베이스를 기반으로 우리 해군이 보유하고 있는 모든 센서 데이터, 보고서, 교리 및 교범 등의 자료 융합을 통해 해군의 빅데이터 분석 시스템을 구축할 수 있고 궁극적으로는 해군작전의 판단을 지원할 수 시스템을 구비하게 될 것이다. 결론적으로 해양정보 관리 및 분석체계의 목표는 해군작전 지원을 위한 확장성있는 최적의 해양정보 데이터베이스를 구축하고 이와 연계된 해양정보 분석모델 정확도를 향상시킬 수 있도록 분석모델을 고도화하는 것이다.

4.2.1 해양정보 데이터베이스 구축

기존에 해군에서 운용 중인 해양DB는 개발된 지 20여 년이 지나 향후 우리 해군이 구현하고자 하는「SMART Navy」와 연계된 체계와의 연동 문제가 대두될 수 있다. 특히 데이터 표준화 문제, 하드웨어 업그레이드 등 여러 복잡한 기술적 문제들이 상존할 수 있어 이를 고려 시 새로운 해양정보 데이터베이스 구축이 요구된다.

최상의 해양정보 관리를 위해서는 데이터베이스를 주요 분석체계와 같이 개발하여 연동하는 것이 매우 중요하다. 특히, 개발단계에서 분석에 활용되는 데이터의 형식을 잘 관리할 수 있고 이는 정보 가시화와 연결되며 타 체계와의 연동 및 체계 확장성 측면에서 중요하다고 할 수 있다. 최근 개발되는 무기체계는 상호운용성이 매우 중요한 요소 중 하나이므로 분석센터의 데이터베이스는 타 체계에서 활용하는 환경자료의 표준이 되도록 개발되어야 한다. 이를 통해 추후 신형 전투체계 개발 시 체계 연동을 시도할 때도 용이하게 진행할 수 있다. 향후 4차 산업 기반 기술인 빅데이터 기술을 적용할 때에도 이는 매우 도움이 될 것으로 판단된다. 따라서 앞으로의 해양정보 데이터베이스는 해양정보 분야의 표준형 데이터베이스

가 되어야 하고 새롭게 개발되어야 한다. 해당 데이터베이스는 주요 분석체계와 별도로 개발되어 연동하는 방안보다 동시에 개발되는 것이 가장 바람직할 것이다.

해양정보 데이터베이스에 포함될 데이터 구성과 해양정보 분석 및 관리체계 구성은 각각 〈표 4-5〉와 〈그림 4-3〉과 같다.

〈표 4-5〉 해양정보 데이터베이스 수집 데이터 구성(안)

구분	주요 특징 및 제원
해군 자산 수집 데이터	· 함정 및 항공기 (A)XBT · 잠수함 및 수중감시체계 CTD · 기상/해양장비 관측자료
대외기관 수집자료(국내)	· 국립해양조사원 · 국립수산과학원 · 한국해양과학기술원 · 기상청 및 국립기상과학원
해양특성조사(용역) 수집자료	· 해양환경 및 해저지형 DB
선진 해군 자료(인터넷)	· HYCOM/NCOM · MYOCEAN

〈그림 4-3〉 해양정보 관리 및 분석체계 구성(안)

4.2.2 해양정보 분석모델 고도화

해군작전 성공을 보장하기 위해서는 정확하고 적시적이며 효과적인 해양정보를 생산하여 지원할 수 있어야 한다. 그런데 해양환경 데이터가 적시적으로 수집된다고 하더라도 해양정보를 생산하는 분석모델이 정확한 결과를 산출하지 못한다면 제공되는 정보의 신뢰성이 저하될 수 있다. 생산된 해양정보의 신뢰성은 해양환경의 불확실성 요소와 분석모델 자체의 정확성에 의해 결정된다. 해양환경의 불확실성 요소는 분석모델에 입력자료로 활용되는 자료 자체의 오차뿐만 아니라 분석모델이 정의하고 있는 가정사항에 기인할 수 있다. 해양환경은 비선형적이기 때문에 이를 분석하기 위해서는 다양한 가정사항을 지정할 수밖에 없다.

예를 들면 대잠탐지거리 모델의 경우 기본적으로 식 (1)과 같은 소나방정식을 계산하는데 동 식에는 상당한 불확실성 요소들을 내포하고 있다.

$$SL - 2TL + TS - MAX(RL, NL) + DI \geq DT \qquad (1)$$

여기서 SL(Source Level) : 음원준위, TL(Transmission Loss) : 전달손실, TS(Target Strength) : 표적강도, RL(Reverberation Level) : 잔향음준위, NL(Noise Level) : 소음준위, DI(Directivity Index) : 지향지수, DT(Detection Threshold) : 탐지문턱이며 식 (1)의 좌변이 DT보다 크거나 같을 경우 탐지된다. 대잠탐지거리 모델 내에는 음파전달모델이 탑재되어 있어 TL 값을 계산하는데 이때 오차가 발생된다. 음파전달모델은 음파 파동방정식을 지배방정식으로 계산되며 기본적으로 유체모델이다. 즉, 해수와 해저저질의 전단응력을 고려하지 않으며 파동방정식 계산에 포함되는 수중 매질의 음속 값의 정확성도 동 모델의 불확실성을 증가시킨다. 또한, 수중에서의 잔향음 등도 세부적으로 고려하지 않는다.

이와 같이 가장 단순한 해양환경을 가정하더라도 분석모델은 모델이 자체적으로 가지고 있는 지배방정식의 제한사항과 해를 구하기 위한 조건, 환경변수, 가정사항 등 아주 다양한 불확실성 요소를 내포하고 있다. 이러한 불확실성 요소를 완벽하게 제거하는 것은 현재로서는 불가능하다. 우리에게 중요한 것은 이러한 불확실성 요소를 최소화할 수 있는 방안을 연구하고 모색하는 것이다. 해군의 연구 투자를 통해 대학과 연구소, 업체 등 산・학・연이 〈그림 4-3〉 해양정보 관리 및 분석체계 내 분석모델의 불확실성 요소를 최소화하기 위해 끊임없이 연구해야 할 것이다. 결국, 해양정보 분석모델 고도화를 통해 모델의 정확성과 신뢰성을 향상시키고 성공적인 해군작전을 보장할 수 있을 것이다.

본 연구에서는 분석모델 고도화를 위해 다음과 같이 제언한다.

1) 차기 통합해양환경분석체계 개발

① 기존 'Hindcast' 위주의 광역에보시스템을 'Nowcast'가 가능토록 현장 관측자료를 이용하고 정확한 해저지형 및 해저저질 정보를 연동

② 대잠전, 기뢰전, 구조전, 상륙/특수전 등 성분작전 별 모델을 고성능 컴퓨터에 탑재하고 해양정보 관리 및 분석체계 내 서버 구축

③ 상기 ②항의 각 체계들을 연동

2) 해양환경 분석 영역 정밀화

: 분석모델의 지배방정식에서 한 지점의 환경을 기준으로 계산하는 '거리독립' 방식이 아닌 '거리종속' 환경을 계산 가능토록 모델을 정밀화함으로써 세부적인 해양환경을 적용 가능토록 분석 영역 정밀화

* 아중규모(1~10km) 해양 변동 모델링 기술 적용 가능[32)]

3) 국립해양조사원 수치모델자료 활용

: 4.1.1.에서 언급한 대외기관 해양정보 수집 연동체계 구축 시 전용망을 통해 일부 수치모델 결과 활용 가능

⇨ 해군 보유 분석모델 결과와 상호 비교 및 보완 가능하며 생산된 해양정보의 정확성과 신뢰성 보장 기대

4.3 해양정보 전파체계

해양정보 관리 및 분석체계를 통해 생산된 해양정보를 작전에서 효과적으로 적시에 활용토록 하기 위해서는 제공되는 해양정보가 복잡하지 않고 단순 명료하게 가시화되어야 하며 이렇게 가시화된 해양정보는 데이터 크기에 상관없이 전파체계를 통해 적시에 전파될 수 있어야 한다. 따라서 제공된 정보를 효과적으로 활용할 수 있는 가시화 체계와 신속히 작전에 전파될 수 있는 전파체계 구축이 요구된다.

4.3.1 해양정보 가시화

'가시화'라는 것은 컴퓨터가 어떠한 모델에 의해 계산되고 시뮬레이션된 결과를

32)

사용자에게 보여주는 것을 의미한다. 해양정보체계에는 가시화되는 정보들이 매우 많다. 기본적으로 수온, 염분, 음속, 해·조류, 지형, 저질, 배경소음 등 다양한 환경자료를 가시화 해야 하고 이러한 환경자료들이 다양한 모델에 의해 새로운 결과를 산출하고 정밀분석을 위해 다양한 방식으로 가시화된다. 기존의 해양정보 가시화는 분석센터에서 전문 분석요원이 해양정보체계가 제공하는 복잡한 결과인데, 비전문가가 해석하기 어려운 그래프 등이 많아 작전에 전파하기 위해서는 단순한 계산 결과값으로 제공하거나 가시화 결과를 재처리하여 전파한다. 이는 매우 비효율적이고 비생산적인 업무 처리 방식이라 할 수 있는데 향후 해양정보체계에는 작전에서 정확한 작전판단을 용이하게 할 수 있는 새로운 해양정보 가시화 모듈이 탑재되어야 할 것이다. 이를 위해서는 기존 체계의 기능과 성능이 크게 향상되어야 한다.

차기 통합해양환경분석체계는 우리 해군의「SMART Navy」구현을 지원할 수 있어야 하고 고성능 하드웨어를 기반으로 빅데이터, 인공지능, 클라우드, 사물인터넷 등 다양한 4차 산업 기반기술 적용도 염두해 두어야 할 것이다. 기존 체계의 '해양환경' 및 '음탐환경'과 '대잠탐색분석' 등의 가시화를 기본으로 하되 새롭게 탑재되는 수집자료 연동 인터페이스, 수치모델의 기능 등을 고려하여 구성되어야 한다.

4.3.2 적시적인 해양정보 가시화 및 전파체계 구축

전파체계는 통신망과 통신망에 연동되는 체계를 포함한 체계를 통칭하는데 현재 해군의 대표적인 정보 전파체계로는 해군의 지휘통신체계인 전술C4I 체계가 있다. 2020년 9월 방위사업청은 해군 전술C4I체계 성능개량 사업을 완료하였다고 발표하였는데, 주요 성능은 〈그림 4-4〉와 같다. 해군 전술C4I체계의 성능이 개선되었다고 하나, 해상에서 수집한 고용량 음향신호 원음 데이터가 분석센터에서 실시간 분석되고 그 결과를 적시에 대잠전력에 전파하는 데에는 아직까지 통신속도 및 통신량 등의 통신능력 측면에서 제한이 따른다.

해양정보를 가시화하여 작전에 전파하기에 가장 쉬운 방법은 C4I체계에 해양정보 가시화 모듈을 탑재하는 방안이다. 그러나, 다양한 해양정보를 분석센터로부터 C4I체계에서 수신하기 위해서는 고용량 데이터 통신이 가능하여야 하는데 특히, 3차원 해저지형정보를 C4I체계에 전시하는 것은 현재로서는 매우 어려운 실정이다. 만약 해양정보를 C4I 체계에 직접 탑재하여 하부 모듈로서 가시화 기능을 수행하

도록 구성한다면 〈표 4-6〉과 같다.

구분	주요 성능 개량
체계 운용	• 기존의 KNCCS[33], KNTDS[34], DMHS[35], 실시간 문자망[36] 각 체계별 4개의 단말기로 운용되던 것을 체계통합하고 성능 개량된 1개의 단말기로 운용
표적 처리 능력 향상	• 탄도탄 표적(3차원/초고속/고고도) 부대간 실시간 공유 가능 • 표적 처리 용량 기존 대비 약 3배 이상
생존성 강화	• 주요 함정 및 주요 레이더 기계 이중화 확대 • 예비 지휘소 전환 약 10분 소요(기존 약 4시간 소요) • 全 운용 부대 보안관제 및 최신 보안 적용
연동체계	• 기존 23개 대비 57개 연동체계로 확대

〈그림 4-4〉 해군 전술C4I 성능 개량(출처 : 방위사업청)

33) KNCCS(Korea Naval Command and Combat System : 해군지휘통제체계) : 다양한 경로로 획득된 정보를 공유하고 전투 지휘 및 결심을 지원하는 체계
34) KNTDS(Korea Naval Tactical Data System : 해군전술자료처리체계) : 육상 지휘소와 함정 등 작전부대 간 전술 표적 정보를 수집, 분석, 전파(공유)하는 체계
35) DMHS(Digital Message Handling System : 디지털전문처리체계) : 해군 부대 간 컴퓨터를 이용한 자동화된 전문처리체계
36) 함정, 육상 지휘소 및 전탐 감시대 간 작전 수행 및 의사소통 수단으로 운용되는 문자메시지(채팅) 형식의 작전망

〈표 4-6〉 해군 전술C4I 체계 내 해양정보 탑재 시 지원 내용

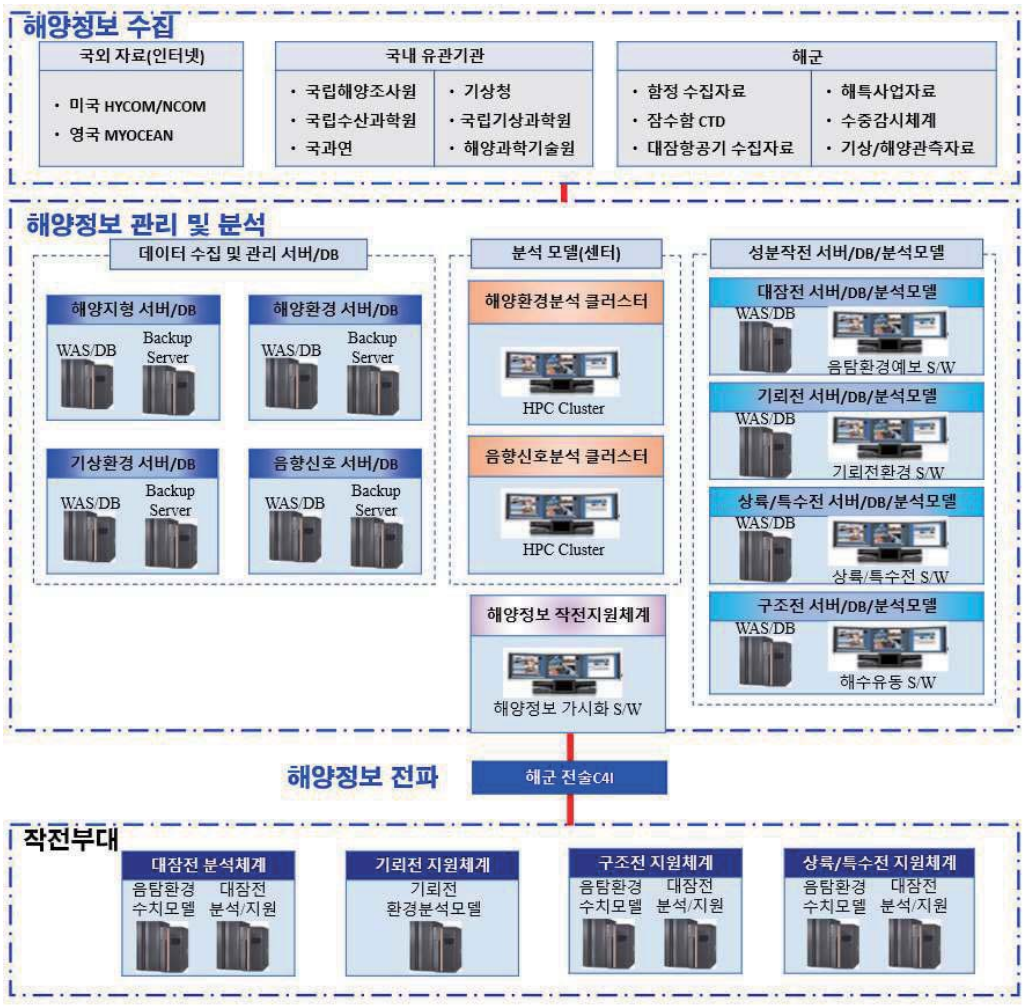
성분작전	작전판단 지원 해양정보	가시화 형태
대잠전	수온	수평 2D 이미지
	음속	수직 2D 이미지
	표층해류	수평 2D 이미지
	층심도	수치
	잠수함 최적심도	수치
	음탐 최대탐지거리	수치
	최적 탐색경로	수평 2D 이미지
	소노부이 최적배치	수평 2D 이미지
기뢰전	Q-route 해저지형	3D 이미지
상륙/특수전	상륙해안 해저지형	3D 이미지
구조전	부유물 표류경로	수평 2D 이미지

C4I체계 내에 해양정보 탑재가 가능하다 하더라도 이는 C4I 체계의 기능 수행에 과부하를 발생시킬 수 있어 정작 중요한 지휘·통제 기능에 부정적 영향을 미칠 수 있다. 해저지형 데이터뿐만 아니라 대부분의 해양환경자료는 넓은 공간영역상에서 정점별 시간별 계속해서 시공간적으로 변화하는 자료가 수신되고 처리되기 때문에 해양정보 관리 및 분석체계와 직접 연동을 하던 C4I체계 내 직접 탑재를 하던 해양정보를 가시화하여 작전에 전파하는 데에는 여러 제약이 따를 수 있다.

이러한 문제를 해결하기 위한 방안으로 해양정보 관리 및 분석체계에 해양정보 가시화 S/W를 탑재한 '(가칭)해양정보 작전지원체계'를 두고 작전에 필요한 해양정보만을 선별하여 해군 전술C4I 체계를 통해 작전에 전파하는 방안을 검토해 볼 수 있다. 통상 전술 C4I 체계를 운용하는 지휘통제실에서는 특정 상황이 없는 경우, 해양정보를 요구하지 않는다. 즉, C4I 체계 상에서 해양정보를 필요로 하는 경우는 주로 구조전 상황 발생 시 또는 대잠 경비 간에 미식별 수중표적 탐지 등의 상황이 발생하는 경우라 할 수 있다. 따라서 해양정보가 요구되는 상황 발생 시 또는 작전에서 요구 시에 동 체계를 이용하여 해양정보 관리 및 분석체계 운용자(해양정보 전문가)가 실시간에 작전에서 필요로 하는 해양정보를 영상을 통해 제공할 수 있을 것이다.

해군 전술C4I 체계에 새로운 해양정보 모듈을 구축하는 방안은 체계 상에서 직접적으로 상시 해양정보를 확인할 수 있다는 측면에서는 유용할 수 있다. 그러나 전술C4I 운용자가 해양정보 전문가가 아니라면 정보 판단 측면에서 작전을 지원하는 데 있어 정보의 해석 및 내용 파악에 일부 문제를 발생시킬 소지가 있다. 또한, 전술C4I의 지휘·통제 기능과 해양정보 모듈의 충돌로 기능이 제대로 활용되지 않을 경우, 체계 내 컴퓨팅 자원만 소모할 뿐 결국 효용성의 문제가 대두될 수도 있다. 체계 및 예산 운용 측면에서도 비효율적이다. 전술C4I 체계는 해양정보만을 위한 체계가 아니라 해군의 전 작전영역에서 활용되는 체계이다. 이러한 체계에 한번 탑재된 모듈은 지속적인 관리가 필요하며 추가적인 예산이 발생될 수 있다. 따라서 해양정보 가시화 및 전파 측면에서 볼 때, 정보지원의 효율성 및 정확성, 체계 및 예산 운용 등을 고려한다면 〈그림 4-5〉와 같은 방안이 가장 적합할 것으로 판단된다.

동 방안은 '해양정보 작전지원체계'를 24시간 운용함으로써 인적자원 소요가 요구되지만 해군작전을 성공적으로 지원하고 작전판단의 중요한 요소들을 제공한다는 측면에서 매우 효율적이고 효과적인 체계 운용이라 할 수 있다. 즉, 전문가가 분석한 해양정보를 지원함으로써 보다 신속하게 지휘부의 결심이 도출될 수 있다. 필요 시에는 전술C4I 체계의 VTC(Video Teleconference)를 통해 분석센터에서 일일, 주간, 월간 단위의 해양정보를 지휘관에게 실시간 보고할 수도 있을 것이다. 그뿐만 아니라, 성분작전을 수행하는 부대에서 운용하는 대잠전 분석체계, 기뢰전 지원체계, 구조전 지원체계, 상륙/특수전 지원체계에 직접적인 정보 지원이 가능함으로써 체계의 작전운용을 극대화할 수 있을 것으로 예상된다.



〈그림 4-5〉 해양정보 가시화 및 전파체계 구성(안)

5. 결론

본 연구에서는 미 해군의 해양정보 운용 현황 조사를 통해 우리의 실정에 맞는 미래 해군의 모습과 해양정보체계 운용개념을 정립하고 이를 바탕으로 해양정보 수집, 관리 및 분석, 전파에 관한 업무 분야별 해양정보체계 구축 방안을 제시하였다.

이를 위해 제2장에서는 미국의 해군 기상・해양병과(METOC)의 조직과 체계 등을 조사하였고 미 해군의 해양정보 업무 프로세스를 분석하였다. 특히, 주문형 전장(BonD) 모델에서 제시하고 있는 '데이터 계층', '환경 계층', '퍼포먼스 계층', '결심 계층'에서의 해양정보의 단계적 적용 및 활용 방안을 살펴보았다. 제3장에서 새로운 안보환경 변화에 따라 미래 우리 해군의 모습을 조망하였고 우리의 실정에 적합한 해양정보 업무의 프레임워크를 구상하였다. 미 해군의 BonD 모델과 비교하여 우리 해군의 해양정보 업무 발전 방향을 검토하였는데, 미 해군의 BonD 모델을 우리의 실정에 적용하는 데에는 해양정보 업무 조직, 각종 정보 및 작전 지원체계, 위성통신 및 해군 C4I체계 측면에서 많은 제약이 있음을 확인하였다. 이에 대한 대안으로서 우리 해군의 독자적인 해양정보 수집, 관리 및 분석, 가시화 및 전파 및 가시화 체계 구축의 필요성을 언급하였다. 또한, 정확하고 적시적이며 효과적・효율적인 해양정보 체계 구축을 통해 작전성공을 보장하고 미래 우리 해군의「SMART Navy」구현을 지원할 수 있을 것이라 강조하였다.

제4장에서는 먼저 해양정보 수집체계 구축을 위해 대외 유관기관과의 연동체계를 구축하여 해양정보 수집을 확대하고 작전활용성을 증대시키며 향후 수집 능력 확대를 위해 중・장기적으로 독자적인 해양조사선과 무인수상정 체계 확보 방안을 제시하였다. 해양정보 관리 및 분석체계 구축을 위해서는 차기 통합해양환경분석체계 사업과 연계하여 해양정보 데이터베이스를 신규 개발하고 해양정보 분석모델 고도화 방안을 다루었다. 해양정보 전파체계와 관련해서는 첫째 해군 전술C4I체계에 해양정보 가시화 모듈을 탑재하는 방안을 언급하였고, 두번째 방안으로 분석센터의 해양정보체계에 '해양정보 작전지원체계'를 구축하여 전문가가 해군 전술C4I체계를 통해 작전에서 요구시 지원하는 개념으로 구성하였는데 정보의 정확성, 정보지원의 효율성 및 효과성, 체계 및 예산 운용 등을 고려 시 두 번째 안이 적합

하다고 판단하였다.

현재 우리 해군의 해양정보 업무 및 체계 수준을 미 해군과 비교할 수는 없다. 그러나 우리는 우리 해군 실정에 적합하면서도 최적의 효과를 발휘할 수 있는 한국형 해양정보 체계를 구축함으로써 선진 해군의 해양정보 업무 수준에 근접할 수 있을 것이다. 아직까지는 군에서 연구 및 활용되고 있는 4차 산업혁명 기반 기술이 민간 영역에 비해 뒤처져있다. 미래 해군을 위한 스마트 해양정보 업무 체계를 구축하기 위한 핵심은 바로 4차 산업 기반 기술을 조속히 적용하는 것이다. 본 연구결과는 이를 위한 첫 단계라 할 수 있을 것이며 해양정보 체계 구축에 대한 해군 전체의 관심과 투자가 필요한 시점이다.

참고문헌

국립해양조사원, https://www.khoa.go.kr/kcom/cnt/selectContentsPage.do?cntId=25401000

김성용, “Regional underwater acoustical climatology under submesoscale ocean process", KAIST, 2020.

방위사업청, “해군, 최신예 신경망 해군전술C4I 성능개량사업 개발 성공”, 뉴스브리핑, 2020.9.

박동선, “4차 산업형명 첨단기술 기반의 ‘SMART Navy’ 大항해 계획”, 대한조선학회지, 57(1), 7-10, 2020. 3.

양희철, “동북아 해양분쟁에서 해양안보의 중요성과 국제동향”, 한국해양과학기술원, 2016.

이필승 외, “미래 해상무인/자율무기체계 개발 방향 연구”, 해군연구보고서, 2018.11.

하용훈 외, “해양특성조사 사업 개선 및 가시화 방안 연구”, 해군연구보고서, 2020.12.

해군본부, “스마트 해군 건설 추진”, 2018.

해군본부, 제안요청서「해양자료 통합 및 가시화 프로그램」, 2021.3.

해군본부,「해군비전 2045」, 2020.

https://www.msc.usff.navy.mil/Press-Room/Photo-Gallery/igphoto/2002508630/

National research council,「Environmental Information for Naval Warfare」, 2004

US Meteorology and Oceanography, https://www.metoc.navy.mil

US Navy and Marine Corps,「Operational Level Integration of METOC Capabilities」, 2013.

US Office of Naval Research,「Data Focused naval Tactical Cloud(DF-NTC)」, 2014.6.

유 의 사 항

1. 본 연구보고서 내용은 연구진의 개인적인 견해로서 국방대학교 국가안전보장문제연구소의 공식입장과 다를 수 있습니다.
2. 본 연구보고서는 정책입안시 참고자료로만 활용하고 타 기관에 불필요한 자료유출을 삼가 주시기 바랍니다.

군사과학정책연구 제14권

2021년 12월 29일 인쇄
2021년 12월 31일 발행

저 자 : 마정목 등 3명
발 행 처 : 국방대학교 국가안전보장문제연구소
TEL. (041) 831-6414
FAX. (041) 831-0000
인 쇄 : 청맥기획 (042) 487-2589

ISSN 1976-5967