Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.5, Oct. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.5.1133

한국군 환경에 적합한 내부자(위협) 정의 및 완화방안 제안*

원 경 수,† 김 승 주‡
고려대학교 정보보호대학원

A Proposal for the Definition of Insider (Threat) and Mitigation for the Korea Military Environment*

Kyung-Su Won,† Seung-Joo Kim‡
Center for Information Security Technologies(CIST), Korea University

요 약

정보보호 분야 중 내부자 위협은 미국 카네기멜런대학 부설 연구소를 중심으로 연구가 꾸준히 이어오고 있을 정도로 중요도가 높다. 이에 반해 우리는 별도 연구기관이 없는 실정이며, 특히 국가 생존과 직결되는 국방 IT 환경에 대한 내부자 위협 연구가 보다 깊이 있게 진행되고 있지 않은 것이 현실이다. 그뿐만 아니라 군의 특수성으로 인해 국방 IT 보안은 학문으로서의 연구가 제한되며, 따라서 개념에 대한 정립조차도 제대로 이루어지지 못하고 있다. 뿐만 아니라 환경의 차이로 인해 미국의 기준을 그대로 빌릴 수 없기 때문에, 본 논문에서는 국방 IT 환경을 분석한 뒤 한국군 환경에 적합한 내부자(위협)를 정의하고, 내부자 위협 종류 및 완화방안에 대해 제안해 보고자 한다.

ABSTRACT

Insider threats in the field of information security are so important that the research is continuing centering on the institutes attached to the Carnegie Mellon University. On the other hand, we do not have any separate research institutes. In particular, insider threat research on the defense IT environment directly connected with the survival of the country is not proceeding in depth. In addition, due to the specificity of the military, defense IT security has limited research as an academic discipline, and even the establishment of concepts has not been achieved properly. In addition, because of differences in the environment, the US standard can not be borrowed as it is. This paper analyzes the defense IT environment and defines an insider (threat) suitable for the Korea military environment. I'd like to suggest the type of insider threat and how to mitigate it.

Keywords: Insider, Insider Threat, Mitigation, defense IT, military IT

I. 서 론

정보 공유시스템 접근 권한은 범위의 명확성이 없으면, 과대 또는 과소 권한 부여의 폐해가 발생한다. 과소의 권한은 정보공유 시스템 본연의 목적에 부합하지 못하기 때문에 공유로 인한 시너지 효과를 얻지 못하고, 과대의 경우는 매닝일병, 스노든 사건처럼 불필요한 사람에게까지 권한이 노출되어 정보가 유출되는 최악의 상황이 발생한다. 매닝사건은 기밀 정보의 디지털화와, 넓게 공유하려는 정부의 정책이 결합된 보안등급을 통해, 전례없이 자료가 유출된 대표적

Received(06. 13. 2019), Accepted(08. 27. 2019)
* 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2019-2015-0-00403)
† 주저자, numberwon@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

인 사건이다.

국방 IT에서의 정보공유는 넓은 작전영역을 연결하고, 육해공 및 연합군과의 다원화된 군/체계 간의 협동작전과 지휘관의 즉각적인 지휘결심을 위해서 반드시 필요하다. 그러한 필요성으로 탄생하게 된 것이 군의 지휘통제체계이다. 문제는 정보의 공유가 활성화될수록 정보누출 또한 증대된다는 것이다. 지휘결심을 위한 정보공유를 위해 도입한 지휘통제체계의 근본 목적을 위배하지 않고 정보누출을 최소화하기 위해서는, 발생할 수 있는 모든 내부자 위협을 도출하고, 그중에서 권한과 관련해서 발생할 수 있는 내부자 위협을 선별하여 대응하는 것이 필요하다.

따라서 본 논문은 서론에 이어 2장에서는 국방 IT 환경을 분석하고, 내부자 정의에 관련한 연구를 진행하며, 3장에서는 지휘통제체계에서의 내부자 위협 종류와 완화방안을 연구한 뒤, 그중에서 권한에 관련한 완화방안을 선별하고 마지막으로 결론을 맺는다.

II. 관련 연구

2.1 한국 국방 IT 환경 분석

외부환경분석과 내부환경분석 두 가지 관점 중에서 본 논문에서는 내부자에 대한 위협을 다루기 때문에 내부환경분석에 한정하였고, 사이버 분야에서의 내부자 위협이 중심이므로, 국방 분야 중 IT 환경에 초점을 맞추었으며, 국방 IT 분야 중 군의 특수한 IT 환경인 지휘통제체계 분석으로 제한하였다.

우선 국방 IT는 여러 각도에서 시각 차이가 존재하지만, 한국산업기술평가관리원과 한국산업기술진흥원에서 제시한 것에 따르면 '국가의 존속과 국민의 생명을 지키고, 국민의 지적, 신체적 활동의 보장을 위한 IT 기반의 융합기술'로 정의하고 있다.

국방 IT 환경을 구성하는 요소는 조직과 자산(무기/비무기체계)으로 나눠볼 수 있으며, 우선 국방 IT의 전반적인 정보화 프로세스를 운영하기 위한 각 조직 및 조직별로 이행할 세부 프로세스는 크게 다섯 가지로 나뉜다. 국방 비전 및 IT 비전에 해당하는 분야, 자원관리 분야, 전장관리 분야, 군사 정보관리 분야, 전사적 IT 관리로 구분된다[1].

이러한 국방 IT에 대한 정보보호 활동은 국방부 정보화기획관실, 합참, 국방정보본부, 군사안보지원사령부, 사이버작전사령부, 국군지휘통신사령부, 국방전산정보원, 각군 CERT 중심으로 이뤄지고 있다. 이중 각급 부대에 설치되어 운영되는 CERT는 국방 정보보호 업무 수행의 가장 중요한 실무조직으로 각 부대에 대한 침해사고 관제, 침해사고 발생 시 초동조치, 국방 사이버지휘통제센터 통제하에 제반 사이버위협 대응단계에 대한 조치사항 시행 등 각 군의 정보보호 대응 기능을 수행한다. 국방 사이버지휘통제센터는 사이버작전사령부에서 군 관련 사이버위협에 대응하기 위하여 운용하고 있는데 최초 안보지원사령부 국방정보전대응센터에서 수행하던 기능을 2010년부터 사이버작전사령부에서 이관 받아 해당 업무를 수행하고 있다. 국방 사이버지휘통제센터는 합참의 통제를 받아 각군 CERT에 사이버위협 관련 상황을 전파하고 각군 CERT는 침해사고 발생시 상위 CERT 및 최상위 CERT인 사이버지휘통제센터에 해당사항을 신고한다. 기타 한미 사이버위협 정보공유는 합참 및 연합사 정보작전방호태세 규정에 의해 수행된다[2].

국방 IT에서의 자산은 국방체계로 볼 수 있는데, 크게 무기체계 및 비무기체계로 나눌 수 있으며, "무기체계"라 함은 유도무기·항공기·함정 등 전장에서 전투력을 발휘하기 위한 무기와 이를 운영하는데 필요한 장비·부품·시설·소프트웨어 등 제반요소를 통합한 것으로 방위사업법에 따르면, 무기체계는 지휘통제/통신 무기체계, 감시/정찰무기체계, 기동무기체계, 함정무기체계, 항공무기체계, 화력무기체계, 방호무기체계, 기타 무기체계의 8가지로 다시 분류된다[3][4]. 비무기체계는 전력을 지원하기 위한 체계로 전력지원체계 명칭으로 변경되었고 정보체계라는 용어로도 사용된다.

국방 IT의 근간이 되는 국방망을 포함하고 있는 국방정보통신망은 국방정보화기반조성 및 국방정보자원관리에 관한 법률에 나온 정의 의하면 '전기통신기본법' 제2조 제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 국방정보를 수집, 가공, 저장, 검색, 송신 또는 수신하는 정보통신체제를 말한다. 국방정보통신망은 국방망과 전장망, 인터넷이 각각 물리적으로 분리되어있다. 전장망은 군 내부에서만 사용하는 별도의 네트워크망이다. 그리고 국방망은 인터넷과 수신연계모듈을 통해 연결되어있다[5].

전장망에서 핵심적인 기능을 하는 것은 전술 데이터링크(TDL, Tactical Data Link)이다. 전술 데이터 링크는 무기체계, 지휘통제체계간의 전술자료 교환을 통한 실시간 전장 상황정보의 공유와 무기체

계 교전 행위 통제를 위한 통신체계로써 네트워크 중심전을 달성하기 위한 핵심수단이다.

2.2 미국 국방 IT 환경 분석

미국의 국방 환경을 보면 현역군인 130만명, 국가방위군과 예비군에서 복무하는 민간인 74만 2천명, 5,000여개 이상의 다른 작전지역이 있으며, 개별 건물 및 구조물은 3천만 에이커 이상의 땅을 사용한다[6]. 이들은 인수, 명령 및 통제, 글로벌 물류, 보건 및 의료, 인텔리전스, 시설 관리에 이르기까지 다양하며 각각 사이버 보안에 중요한 역할을 한다. 네트워크 규모에서도 보면, DoD(Department of Defense)의 일부 IT 통계에는 2015 회계연도 360억 달러 이상의 국방성 IT 예산이 포함되어 있으며, 약 10억 달러 규모의 운영 체제, 수백 개의 데이터 센터, 수천 개의 서버, 4백만 대의 컴퓨터 및 IT 장치, 수십만 개의 상용 모바일 기기가 포함되어 있다.

또한 15,000개 이상의 분류/비분류 네트워크, 7백만대 이상의 컴퓨터/IT 기기, 17만 명 IT 인력을 보유하고 있다[7].

각 부서의 네트워크는 전 세계 거의 모든 곳에서 임무를 지원할 수 있을 만큼 충분히 이동 가능해야 하며, 임무가 요구되거나, 예상되거나, 예상되지 않은 어떤 파트너와의 협업을 촉진할 수 있을 만큼 충분히 유연해야 한다. 극복해야 할 단점으로는 이러한 네트워크 및 컴퓨팅 환경의 불필요한 복잡성으로 인해 가시성이 제한되고 정보를 안전하게 공유하고 미션 파트너와 전 세계적으로 운영을 실행할 수 있는 기능이 방해된다는 것이다. 또한, 방어하기 어렵고 운영과 유지 비용이 많이 든다. 그뿐만 아니라 동적 미션 환경을 완벽하게 지원하는 데 필요한 대처 능력도 부족한 실정이다.

또한, 미군의 사이버 작전업무는 연방 DHS U.S Federal Cybersecurity Operations Team과 DoD National Roles and Responsibilities 간의 업무 연계성도 중요한 요소로 다루고 있으며[8], 미 사이버공간에서의 사이버 전략 목표는 아래와 같다[9].

- 사이버공간 환경에서 합동군 임무 완수 보장
- 미국의 군사적 이점을 강화하는 사이버공간 운영을 통해 연합군 강화
- 단독으로 또는 캠페인의 목적으로 미국의 중요 인프라를 악의적인 사이버 활동으로부터 보호하는 것은 중대한 사이버 사고를 야기 가능
- 비 DoD 소유 네트워크에서 DoD 정보를 포함한 악의적 사이버 활동으로부터 DoD 시스템 보호
- 기관 간, 산업간, 국제 파트너와의 DoD 사이버 협력 확대

2.3 한·미 간 국방 IT 환경의 차이점 분석

이상으로 한미간의 국방 IT 환경에 대해 살펴보았다. 이러한 국방 IT 환경에서 한측과 미측의 주요 차이점을 한측 관점에서 보면 다음과 같다.

- 보다 좁은 임무와 범위를 가지고 있다
- 이동성이 높으며, 유연성을 가지고 있다.
- 가시성이 높다.
- 안전한 정보공유를 이룰 수 있다.
- 방어가 쉽고 유지비가 상대적으로 적게 든다.
- 동적 미션 지원 능력이 우수하다.

그러나 국방의 규모에 있어서 차이는 있지만, 목표는 동일하다. 또한, 이러한 차이점에도 불구하고 한미간의 국방 IT에서는 공통의 변화가 존재한다. 전쟁의 양상이 네트워크가 중심이 된 NCW(Network Centric Warfare)로 변화되었다는 것이다. 육군대학에서 발간한 C4I 체계 교재(2008)[10]에는 국방 환경의 변화를 다음과 같이 기술하고 있다.

- 전쟁개념이 화력, 기동 중심 전쟁에서 정보·지식 중심 전쟁 수행으로 변화
- 전장 영역은 영토 개념을 벗어나 우주 및 사이버 공간으로 확대
- 첨단 과학기술의 발전으로 전장 가시화와 정보 공유, 시·공간적으로 네트워크에 의해 통합된 시스템 중심의 전쟁 수행
- 사이버 무기에 의한 적의 정보체계 및 네트워크 마비, 파괴 등 활동을 통한 정보 우위 달성 추구

현대전은 네트워크화된 전력으로 정보와 상황인식을 공유하고 전 전력의 통합 활용을 가능하게 하여 극적인 작전 수행 효과를 창출하는 NCW(Network Centric Warfare) 개념을 근간으로 운용되고 있다. NCW를 구현하기 위한 근간은 모든 무기체계를 네트워크로 연결하고 실시간 상황인식과 작전지시, 평가분석을 가능하게 하는 지휘통제체계이다. 지휘통제체계는 감시-판단-타격이라는 Kill-Chain 단계에

있어 판단을 수행하는 머리 부분에 해당한다[11].

- 지휘통제체계 정의 및 분류 : 지휘통제체계는 지휘관이 임무달성을 위해, 지휘·통제·통신·컴퓨터 정보체계 등을 유기적으로 통합 및 활용하여 실시간으로 정보수집 및 분석·지휘결심·계획·지시·작전 수행을 효과적으로 가능하게 하는 모든 시설·장비·인원 및 절차로 구성된 통합체계를 일컬음. 지휘통제체계는 부대 구조별, 임무별, 작전단계별로 분류
- 운용개념 : 지휘통제체계는 전장 인식을 위하여 네트워크 기반의 신속·정확한 정보의 수집, 처리, 전파 및 지식관리 체계를 구축하고 의사결정자에게 작전환경에 대한 체계적 지식을 제공함으로써 전장을 가시화하고 전장 상황을 공유하는 것을 목표로 함.

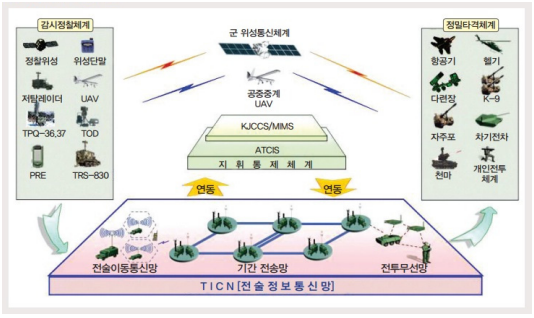

Fig. 1. Command&Control System, Tactical Information Communication Network

지휘통제체계의 세부 분류 및 내용은 아래와 같다.

이러한 NCW로의 패러다임 변화에 따라, 무기체계 IT 환경에 큰 변화가 왔고, 따라서 지휘통제체계의 내부자 위협은 중요한 보안 요소가 되었다.

Table 1. Command&Control System(CCS) classification

Classification		Type
Unit	CCS(Joint)	KJCCS, MIMS
	CCS(Army)	ATCIS, B2CS
	CCS(Navy)	KNCCS, KNTDS
	CCS(Air)	AFCCS, MCRC
Mission	Strategy	KJCCS, AKJCCS
	Tactics	ATCIS, KNCCS, AFCCS
	Battle	B2CS
Operat-ion	Information	MIMS
	Command control	KJCCS,AKJCCS,ATCIS,KNCCS,AFCCS,B2CS
	Fire Operating	JFOS-K

2.4 내부자(위협) 정의

다음으로는 국방 IT에서의 내부자 위협 대응방안을 다루기 위해서 내부자(위협)의 정의에 대해서 살펴본다. 실제로 내부자로 간주 될 수 있는 사람은 조직에 따라 다르며 시스템별 특성뿐만 아니라 조직의 정책과 값에 의해 결정되기도 한다[12].

내부자 정의에 이어 내부자에 의한 위협에 대한 정의를 살펴보면, 내부자 위협과 내부자 공격 두 가지 형태로 나눠볼 수 있다.

Table 2. References to the definition of an insider

Reference	Insider Definition
Bishop (2005) [13]	"Anyone with access, privilege, or knowledge of information systems and services". But also: "[…] anyone operating inside the security perimeter."
Butts et al.(2005) [14]	"[…] an insider is any individual who has been granted any level of trust in an information system. […] What is important is that once users have been granted any authorized explicit right to the information system, they are now considered an insider".
Carroll (2006) [15]	"[…] what is meant is any and all persons that have access to an organizations information including people such as contractors, temporary employees and the like".
Predd et al. (2008) [16]	"Insider:someone with legitimate access to an organization's computers and networks. For instance, an insider might be a contractor, auditor, employee, temporary business partner, or more".
Schultz (2002) [17]	"[…] insiders would usually be employees, contractors and consultants, temporary helpers, and even personnel from third-party business partners and their contractors, consultants, and so forth".

Table 3. References to the definition of insider attacks and insider threats

Refere-nce	Term	Definitions
Anderson et al. (2000) [22]	Insider attack	"Any authorized user who performs unauthorized actions that result in loss of control of computational assets".
Bishop (2005) [13]	Insider attack	"malevolent (or possibly inadvertent) actions by an already trusted person with access to sensitive information and information systems"
Carroll (2006) [15]	Insider threat	"Insider threats can be either intentional or unintentional".
NIST SP800-30(2001)	Insider threat	"the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability"
Predd et al.(2008) [16]	Insider attack	"[…] an insider's action that puts an organization or its resources at risk".
Schultz (2002) [17]	Insider attack	"An insider attack is considered to be deliberate misuse by those who are authorized to use computers and networks". […] "inside attackers are those who are able to use a given computer system with a level of authority granted to them and who in so doing violate their organization's security

III. 한국군 환경의 내부자(위협) 정의 및 완화 방안 제안

3.1 한국군 환경의 내부자 위협

3.1.1 한국군 환경의 내부자(위협) 정의

내부자 개념을 정립하여 보호 대상을 명확히 선정해야 내부자 위협을 완화하는 방안 수립이 가능하다. 또한 환경의 차이로 인해 미국의 기준을 그대로 차용할 수 없으며, 한국군은 특별한 규정 및 정의가 마련되어 있지 않아서 본 논문에서 제안한다. 단지 현역 장병과 군무원이라는 식의 신분 관련 용어만이 사용되고 있을 뿐이다.

관련 연구에서 언급한 내부자에 대한 논의의 주요 관점은 "legitimately, authorized, privilege, relatively, perimeter, intentional" 이며, 국방 분야에서 내부자 관점은 비밀 취급 인가 등급에 따른 접근 권한이다. 따라서 국방 IT에서의 내부자(insider)에 대한 정의를 다음과 같이 특정해 볼 수 있다.

"국방부(where) 법률에 따라 합법적으로(legitimately), 인가된(authorized) 권한(privilege)을 가지고, 그 권한의 범위(perimeter) 내에서 허용된 비밀 취급 인가 등급의 정보만을(relatively), 해부대 조직의 목적에 의해서만(intentional) 접근(access)하는 군인 또는 군에 종사하는 민간인(user)"

또한, 위에 정의한 내부자에 의해 초래될 수 있는 모든 위협을 내부자 위협으로 정의해 볼 수 있다.

3.1.2 내부자 위협 보호 대상 식별

서론에 언급한 대로 본 논문에서는 국방이라는 특수성에 따른 IT 환경 무기체계인 지휘통제체계를 분석 대상으로 한다. 분석 대상 식별을 위해 DFD(Data Flow Diagram)를 이용하였다. DFD를 이용하면 분석 대상의 구성요소와 데이터 흐름을 추상적으로 파악할 수 있다. DFD를 작성할 때 객체 요소를 활용하는데, 각 요소는 다음 표와 같다. DFD 작성을 위해 Microsoft사에서 공개 소프트웨어로 배포한 Microsoft Threat Modeling Tool 2016[23]을 사용하였다.

객체 및 프로세스를 통한 내부자 위협요소 식별을

Table 4. Elements of DFD

Element	Symbol	Description
Entity		People or code
Process		Any running code
Data Flow		Communication between processes.
Trust Boundary		Anyplace where various principles come together

위해, 주요 서버를 운용하는 합참 DFD 개념도를 그림 2에 나타내었다. 단, 이중화 및 시스템 관리/유지보수 flow, 다른 서버와 위협이 중복되는 일부 서버, 정보보호체계는 복잡성 및 보안으로 인해 제외하였다.

주서버에서 운용되는 공통작전상황도에는 부대명, 부대 코드, 부대 위치, 부대 규모 등이 도시되며, 위치보고접속장치 및 아군/적군의 위치 정보와 송수신 메시지가 반영된다[24]. 또한, 전자결재 및 전문 송수신을 위하여 시스템 기초자료(부대, 부서, 사용자, 직책 등)를 동기화하고 있다[25].

사용자 및 시스템은 E(Entity), S(System)로 표현하였고, 업무 흐름에 따른 프로세스는 P(Process)로 표현하였다.

Table 5. DFD Element Description

Type	No.	Name	Description
Entity	E1	staff	users who input/search data
	E2	commander	users with operational control
	E3	system manager	users with system admin rights
	E4	maintenance	maintenance business users
	E5	supplier	Developers/suppliers
System	S1	terminal	for staff
	S2	terminal	for commander
	S3	terminal	form maintenance
	S4	terminal	key insert/distribute
	S5	terminal	key policy
	S6	main server	operational condition, COP
	S7	link server	interworking between systems
	S8	spare server	for malfunction
	S9	backup server	backup
	S10	intelligence server	Intelligence System
	S11	interworking server	Allied data linkage
	S12	DB server	database server
	S13	vaccine	anti virus system
	S14	fire	Fire Operating System
		operating server	
	S15	key management server	Authentication
	S16	Crypto Device	crypt/decrypt
	S17	dongle	Authentication
	S18	media	for Air gap
Process	P1	input/search	data input/search
	P2	operational work	unit location, situation report
	P3	command	command, order
	P4	management	system management
	P5	copy	for malfunction
	P6	DB process	data process
	P7	backup/ recovery	System backup/restore
	P8	vaccine	vaccine update, logging
	P9,10	interwoking	interworking between systems
	P11	encrypt	encrypt
	P12	decrypt	decrypt
	P13	authentication	user authentication
	P14	key management	authentication, distribute
	P15	send	data send(Air gap)
Flow	F1~6	input	key authentication
	F7~12	result	authentication
	F13~15	input	authentication
	F16~17	input	command
	F18~19	input	management
	F20~22	result	authentication
	F23~24	search	report
	F25~26	result	management
	F27~28	copy	copy infomation

Type	No.	Name	Description
	F29~30	input	data processing
	F31~32	result	data processing
	F33~34	input	backup information
	F35~36	result	recovery info
	F37~38	logging	logging result
	F39~40	patch	patch info
	F41~53	interworking	send interworking
	F54~66	interworking	receive interworking
	F67~73	authentication	authentication input
	F74~80	authentication	authentication result
	F81~82	key management	key management info
	F83~84	policy	authentication policy management
	F85	supply	supply info
	F86	maintenance	maintenance info

3.1.3 보호 대상에 따른 내부자 위협 종류

지휘통제체계는 이전 지휘소자동화체계로부터 변화되는 과정에서 지휘관의 임무달성을 위해서 체계간의 연동 범위가 대거 확장되었다[26]. 이러한 연동 범위의 확장과 정보공유의 확대의 문제점의 대표적인 예를 들면, 종이지도가 디지털 지도가 되면서 실시간 정보공유가 가능해졌지만, 체계에 접근하는 누구나 열람할 수 있다는 문제 또한 발생했다는 것이다.

보안업무규정 시행규칙(대통령 훈령 제341호, '15.4.13) 별표 기본분류지침서에 보면 기상 및 계획 제원, 적 능력의 정보판단, 병력구성 및 운용은 Ⅰ급 비밀에 해당하는 사항으로 명시되어있었으며, 17년 2월에 개정된 보안업무규정 시행규칙('17.2.22)에도 I급 비밀은 아래와 같이 명시되어있다.

- 국가 차원의 전쟁전략 및 정책(전략 제대급의 전쟁 수행 계획, 극히 보안이 필요한 특수 정보활동 계획)
- 국가정보작전 및 특수적인 국내정보활동에 필요한 사항(국가의 중요한 정보수집 활동 사항, 전반적이고 종합적인 특수한 치안활동)

따라서 KJCCS로 공유되는 전군 상황도 및 작전상황 정보는 단순 Ⅱ급 비밀의 수준을 넘어설 수 있다. 그러나 KJCCS는 거의 모든 사용자가 상황도를 볼 수 있고, 공유되고 있으며 실시간으로 관련 정보가 전파되고 있다. 이뿐만이 아니라 합동 및 연합 C4I체계로는 통합된 군사정보(적 상황 등)가 최신화하여 탑재되며 또한 부대 위치는 실시간 자동 연동이 보장되며, 정기적인 보고자료는 모든 사용자에게 전평시 공유된다. 웹을 기반으로 체계를 구축하여 광범위한 정보가 공유되는 것이다.

ATCIS가 구축되지 않는 부대의 경우 과거의 스파이더망 개념상 별도 서버를 구축하지 않고 인근부대(상급 작전사가 될수도 있음) 서버에 접속하여 타 부대의 단말기 기능과 동일한 기능을 수행할 수 있는 것또한 공유의 범위를 넘어설 수도 있다.

군 오프라인상에서는 문서화된 비밀을 열람하기 위해서, 비밀을 보유한 부서에 출입 할 수 있어야 하며, 비밀을 소유한 사람의 승인이 있어야 하고, 비밀이 보관되어있는 비문함을 오픈할 수 있어야 하며, 이러한 일련의 절차에 대한 승인 및 비밀 취급인가가 있어야 한다. 오프라인에서 위와 같은 비밀 취급을 위한 인원에 대한 비밀 취급인가는 부대별 직위 책정표에 명시되어있다. 하지만 국방 IT 상에서는 구체적인 내부 등급이 명시되어있지 않다. 단지 부서에 따른 일반적인 사용 권한만 부여되어 있으며 주요 권한의 종류는 아래와 같다[10],[27].

- 일반사용 권한 :체계 등록된 사용자는 일반사용 권한을 가짐. 상황도 도시 SW 시작 권한
- 체계관리 권한 :체계 상태 및 체계 사용자 관리 등 수행, 주/백업센터/작전사 체계관리로 세분화
- 상황도 도시 권한 :상황도 도시의 자료관리 범위에 따라 상황도 관리, 군대부호 관리, 상황DB 갱신, 지도관리 등으로 세분화

또 한 가지의 위협요소는 무중단/이중화를 기본으로 해야 하는 체계 특성상 체계관리자의 권한이 더욱 막강해졌다는 것이며, 추가적인 위협으로는 수시로

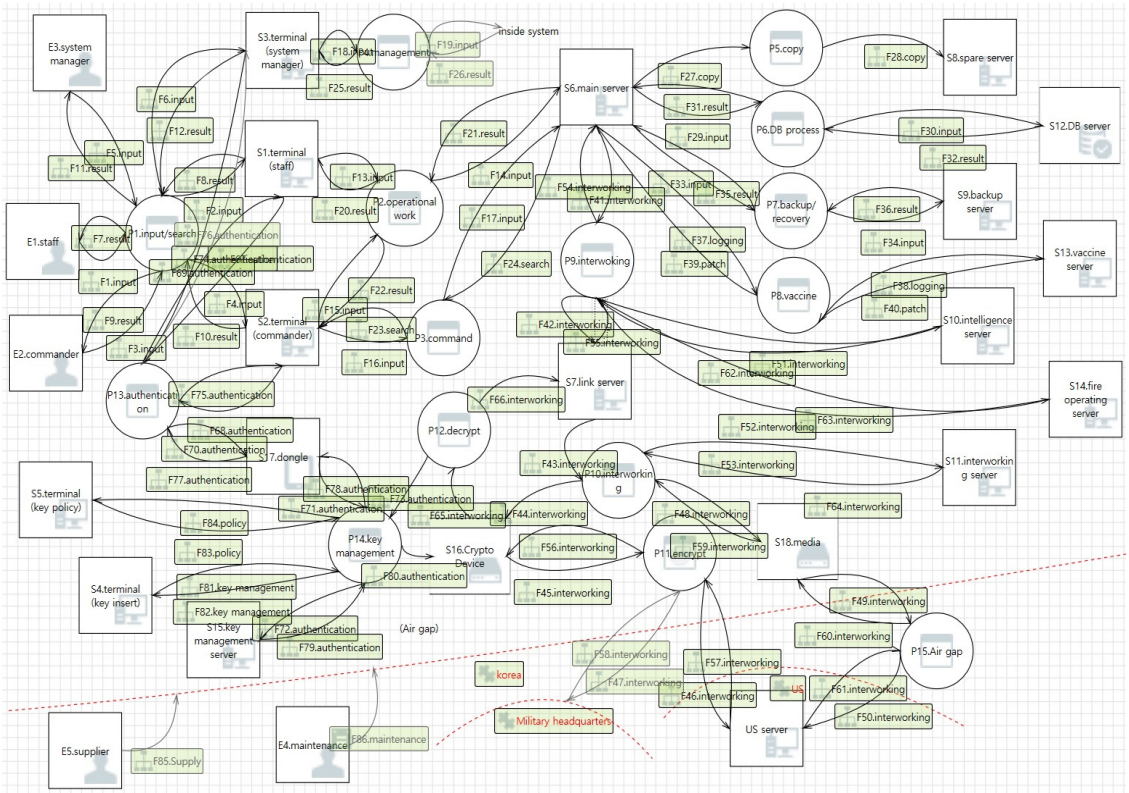

Fig. 2. Command&Control System DFD(Joint Chiefs of Staff)

이뤄지는 성능개선에 따라 방대한 소스코드의 오류에 따른 위협 또한 상존한다는 것이다. Table 6은 객체에 따른 내부자 위협 종류를 나열했다.

비무기체계에서는 정보탈취(기밀성)가 주목적이라면, 무기체계에서는 주로 변조(무결성)와 특히 거부(가용성)가 보안의 주목표이다. 체계를 사용하는 일반 사용자는 정보탈취, 허위정보입력 등의 대표적인 취약점이 있으며, 체계관리자/유지보수 인원에 의한 위협은 대용량자료탈취/시스템 마비/실시간 자료탈취가 있을 수 있다.

유지보수뿐만 아니라 제조사에 의한 공급망 위협도 내부자 위협이 될 수 있다. Left of Launch로 표현되는 위협이 그 예이다. 내장 SW가 늘어가면서 내부자의 범위가 외부개발자/제품제조자로 확대되었다. Left of Launch로 중요성이 증대되는 것이 사실이다. 그러나 이 부분은 정보보증(assurance) 영역으로 운용 간 발생 가능한 위협에 대해 다루는 이번 내부자 위협논문에서는 배제하기로 한다.

또한, 내부자 위협은 정보누출이 주목적이다. 거의 모든 내부자 위협은 STRIDE 모델링 기법 중에서 Information disclosure를 주목적으로 한다. 일부 Tampering이 발생할 수 있으나, 상식적으로 노출의 위험이 있어서 쉽게 시도하지는 않는다.

내부자 위협에서의 Spoofing, Elevation of privilege는 정보유출 목적 범주에 포함된다. 따라서 STRIDE 모델링을 통한 분류는 제외한다.

3.2 내부자 위협 완화방안

3.1절에서 도출된 내부자 위협에 대한 완화방안을 Table 7에 명시하였다. 모든 내부자 위협 완화 항목이 권한에 따른 위협과 무관할 수는 없으나, 특히 M01~03, M47, M53, M54, M58~63, M65, M66, M74, M75, M77~83은 권한 위협을 완화하는 방안이다. 또한, IT 환경에서의 최고 권한은 체계관리자에게 부여되어 있으며, 체계관리자에 따른 위협 완화방안은 주로 M69, M72, M77~85 완화방안으로 위협을 완화 시킬 수 있다.

Table 6. Insider threat types

Threat No.	Insider threat	Object No.	Ref.
TH01	Delete log through privileges, Disable system logs	S6~15,P1,P4~5,F6,F11~12,F18~19,F25~26	[27] [37]
TH02	Physical access to distribute information	S1~3,S6,P1~4,P9~10,F1~6,F13~17,F41~53	[12]
TH03	Physical access to view information	S1~3,S6,P1~4,F7~12,F20~26	[12]
TH04	Physical access to sabotage information	S6~15,P1,P4,P14,F1~6,F18~19	[12]
TH05	Unintentional destruction of information	S1~3,S6~15,P1~4,P14,F1~6,F13~19	[12] [38]
TH06	Unintentional misuse of information system	S1~5,P1~4,P14,F1~6,F13~19,F81,F83	[12] [38]
TH07	Accidental install of malicious software	S1~15,P1,P4,P14,F1~6,F13~19,F81,F83	[12]
TH08	Unintentional use of unauthorized access	S1~15,S17~18,P1~10,P14~15,F1~6,F13~19,F81,F83	[12]
TH09	Virus-laden CD and/or USB flash drive and/or floppy	S1~5,P1~4,P14,F1~6,F13~19,F81,F83	[18]
TH10	Administrator lockout	S3,S6~15,P1,P4,P14,F18~19,F81,F83	[18]
TH11	Social engineer passwords	E1~5	[18]
TH12	Smuggling out USB flash device or other media(exfiltration)	E1~5,S18,P13,P15,F48~50,F59~61,F67~69	[18]
TH13	"Missing" laptops/hardware	S1~5	[18]
TH14	Targeted acquisition of surplus equipment	S1~5,S18,F48~50,F59~61	[18]
TH15	Unpatched systems	S1~15,P8~10,F39~53	[18] [38]
TH16	Sabotaged patches	S1~15,P8~10,F39~53	[18] [37]
TH17	False positives on anti-virus	S1~15,P1~10,P14,F1~84	[18]
TH18	Use of unattended terminal	S1~5,P1~4,P9~10,P14,F1~26	[18]
TH19	Targeting database "adjustments"	S6~15,P1~4,P6,P9~10,F1~6,F13~19,F27~30,F33~34	[18]
TH20	Extra copy of DB backups	S6~15,P4~7,F18~19,F27~30,F33~34	[18]
TH21	Cell phone/PDA/voice recorder in classified meeting, Wireless telephone cameras to capture information	E1~3	[18]
TH22	Mislabeled paper	E1~3	[18]
TH23	Copy and paste between classifications (from high to low)	E1~3	[18]
TH24	Analyst changes workflow to exclude other analysts	E1~3	[18]
TH25	Analyst changes workflow to include himself/herself	E1~3	[18]
TH26	Insert bad content into report upon inception (e.g. translation)	E1,E3	[18]
TH27	Delete/withhold content into report upon inception	E1,E3	[18]

Threat No.	Insider threat	Object No.	Ref.
TH28	Identity theft or copy, fraud	E1~5,P13,F67~69,F72	[28] [29]
TH29	Antivirus self-protection disabling	S1~15,F1~86	[30]
TH30	Non-technical staff (threat) with access to sensitive information and IT assets, executives such as CFO/CEO	E2,P1,P3,F3~4,F9~10,F14~17,F21~24	[31]
TH31	theft of IP	S1~5,P1~4,P14,F1~6,F13~19,F81,F83	[29]
TH32	An officer who has the authority to confidential information about the main technology prints and attempts to leak it to the outside	E2,P1,P3,F3~4,F9~10,F14~17,F21~24	[32]
TH33	Copying sensitive file	S1~3, S6,P1~4,F1~26	[33]
TH34	Performing large file or folder copy	S1~3,S6~15,P1~4,F1~26	[33] [37]
TH35	Printing large number of pages during irregular hours	S1~3,P1~4,F1~26	[33]
TH36	Data Exfiltration(Printing sensitive documents)	S1~3,S6,P1~4,F1~26	[33]
TH37	Running CD or DVD burning tools), Data Infiltration(Connecting USB Storage Device	S1~3,S6,P1~4,F1~26	[33]
TH38	Logging in locally to sensitive Windows Server by unauthorized user	S1~15,P1~4,F1~26	[33]
TH39	Logging in remotely (RDP) to sensitive Windows Server during irregular hours	S1~15,P1~4,F1~26	[33]
TH40	Logging in remotely (RDP) to sensitive Windows Server by unauthorized user	S1~15,P1~4,F1~26	[33]
TH41	Logging in to sensitive machine using a shared account	S1~15,P1~4,F1~26	[33]
TH42	Running a remote PC access tool	S1~15,P1~4,F1~26	[33]
TH43	Accessing unauthorized folder	S1~15,P1~4,F1~26	[33]
TH44	Trying to access a system that requires credentials	S1~15,P1~4,F1~26	[33]
TH45	Adding Windows Firewall Rules	E3,S3,F5~6,F18~19	[33] [37]
TH46	Changing computer data or time	S1~15,P1~4,F1~26	[33]
TH47	Configuring Windows Firewall Status	S1~15,P1~4,F1~26	[33] [37]
TH48	Configuring Windows LAN or Proxy Settings	S1~15,P1~4,F1~26	[33]
TH49	Careless Behavior(Enabling Windows Remote Assistance)	S1~15,P1~4,F1~26	[33]
TH50	Careless Behavior(Running software to enable sharing and remote access)	S1~15,P1~4,F1~26	[33]
TH51	Careless Behavior(Storing passwords in clear text)	S1~15,P1~4,F1~26	[33]
TH52	Time Fraud	E1~5	[33]
TH53	Unauthorized Activity on Servers(Installing software on Server)	S6~15,P1,P4,P14,F1~6,F18~19	[33]
TH54	Running hacking tools, Install software on host computer to capture keystrokes logger	S1~15,P1~4,F1~26	[33] [18]

Threat No.	Insider threat	Object No.	Ref.
TH55	Performing Unauthorized Admin Tasks(Editing Registry Editor entry)	S1~15,P1~4,F1~26	[33]
TH56	Editing User Account Control (UAC) Settings	S1~15,P1~4,F1~26	[33]
TH57	Running Command Line Shell programs	S1~15,P1~4,F1~26	[33]
TH58	Running DBA tools	S1~15,P1~4,F1~26	[33]
TH59	Running Windows management tools	S1~15,P1~4,F1~26	[33]
TH60	Running unauthorized command by admin in command line tools	S1~15,P1~4,F1~26	[33]
TH61	Installing advanced monitoring tools	S1~15,P1~4,F1~26	[33]
TH62	Installing file transfer applications	S1~15,P1~4,F1~26	[33]
TH63	Installing non-standard software	S1~15,P1~4,F1~26	[33]
TH64	Installing password cracking tools	S1~15,P1~4,F1~26	[33]
TH65	Installing Remote Access and Sharing Desktop tools	S1~15,P1~4,F1~26	[33]
TH66	Installing Tunneling tools	S1~15,P1~4,F1~26	[33]
TH67	Uninstalling a program on Windows Desktop	S1~15,P1~4,F1~26	[33]
TH68	Uninstalling a program on Windows Server	S3,S6~15,P1,P4,F5~6,F18~19	[33]
TH69	Unauthorized DBA Activity(Executing SQL update command)	S3,S6~15,P1,P4,F5~6,F18~19	[33]
TH70	Opening a shell by unauthorized application user	S1~15,P1~4,F1~26	[33]
TH71	Opening root shell using SUDO command	S3,S6~15,P1,P4,F5~6,F18~19	[33]
TH72	IT Sabotage(Deleting a local user)	S1~15,P1~4,F1~26	[33]
TH73	IT Sabotage (Deleting files from sensitive directory)	S1~15,P1~4,F1~26	[33]
TH74	IT Sabotage(Overwriting files using SFTP or SCP in sensitive configuration directories)	S3,S6~15,P1,P4,F5~6,F18~19	[33]
TH75	Identity Theft(Changing own password by currently logged in user)	S1~15,P1~4,F1~26	[33]
TH76	Editing sensitive system configuration files	S3,S6~15,P1,P4,F5~6,F18~19	[33]
TH77	Editing network configuration files	S1~5,P1~4,P14,F1~6,F13~19,F81,F83	[33] [37]
TH78	Elevate users privileges	S3,P4,F18,F19	[37]
TH79	Use of defective HW	S1~5,P1~4,F1~26	[37]
TH80	System outage and destruction	S1~18,P1~15,F1~86	[39]

Table 7. Insider Threat Mitigation plan

No.	Mitigation	Threat No.	Ref.
M01	Security policy, Integration of Security Policy	Overall	[12] [34]
M02	Communicate accountability and "acceptable use" policies and expectations, and enforce the established guidance.	Overall	[35]
M03	Legally binding documents	Overall	[12]
M04	Pre-employment screening	Overall	[12]
M05	Use appropriate screening processes to select new employees.	Overall	[36]
M06	Conduct recurring workshops on technological approaches to mitigating the insider threat and reducing information system vulnerabilities.	Overall	[35]

No.	Mitigation	Threat No.	Ref.
M07	Consolidate, into a single electronic source, basic information assurance training material, customized or enhanced to address the insider threat and made accessible to all authorized users, security managers and training professionals.	Overall	[35]
M08	Establish mandatory minimum standards for security education, awareness and training programs related to the insider threat.	Overall	[35]
M09	Provide non-threatening, convenient ways for employees to report suspicions.	Overall	[36]
M10	Employ maximum use of "data mining" to enable continual online review of personnel security information.	Overall	[35]
M11	Manage organizational culture	Overall	[12]
M12	Process-Based Analysis	Overall	[34]
M13	Assignment of Risk Budget	Overall	[34]
M14	Use firewalls internally to enforce compartmentation of information systems and assets.	Overall	[35]
M15	Best Practices & Guides, Develop a database of insider events, characteristics, lessons learned and statistics.	Overall	[34] [35]
M16	Create a comprehensive list of system and user behavior attributes that can be monitored to establish normal and abnormal patterns to enable anomaly and misuse detection.	Overall	[35]
M17	Conduct research on means of reacting to suspected insider malicious activity.	Overall	[35]
M18	Incident registration	Overall	[12]
M19	Develop and implement metrics tailored to the insider threat.	Overall	[35]
M20	Develop a threat awareness package for all users of information systems.	Overall	[35]
M21	Ensure that security (including computer network security) personnel have the tools they need. Achieve defense-in-depth through use of multiple protection tools.	Overall	[36] [35]
M22	Assess technologies currently available for dealing with the insider problem.	Overall	[35]
M23	Direct the appropriate Defense agencies to accelerate the development of new tools for information systems security.	Overall	[35]
M24	Centralize coordination of activities addressing the insider problem.	Overall	[35]
M25	Ensure that management invokes minor sanctions for low level infractions of the stated security policy, in order to demonstrate the organization's commitment to the policy.	Overall	[35]
M26	Mandate periodic use of existing tools for vulnerability assessment on systems and networks.	Overall	[35]
M27	Conduct independent vulnerability assessments.	Overall	[35]
M28	Establish a broad-based, long-term research program in anomaly and misuse detection addressing specifically the insider threat.	Overall	[35]
M29	Conduct a long-range research program on reaction to insider threats.	Overall	[35]
M30	Develop capabilities to do forensic analysis of intrusions.	Overall	[35]
M31	Build a Threat Hunting Team	Overall	[41]
M32	Apply virus scanners to centralized server computers and routers within an installation's local area network(s).	7,9,17,29,54,79	[35]
M33	Antivirus, Configure virus scanners to test all floppy diskettes and other removable media when introduced; the scanners should not be capable of being disabled by the end user.	7,9,16,17,29,79	[12] [35]

No.	Mitigation	Threat No.	Ref.
M34	Restrictions on use of removable media, Use existing technology under DoD IT operating systems(OS) to disable writing to and booting from floppy disks or other removable media(e.g.offline storage hard disks) for critical and sensitive systems.	7,9,12,21,33~34,37	[12] [35]
M35	Investigate the current availability of tools to enable uniform security conscious configuration of application programs (such as Internet browsers, email packages and office support software) within an installation, and monitoring of the configurations once installed.	7,15,29,53~54,61~68,79	[35]
M36	Implement a new version of the Acquisition System Protection Program.	7,15,16,79	[35]
M37	Application controls	6,17,79,80	[12]
M38	Intrusion Detection Systems, Configure and deploy existing intrusion detection systems to monitor the activity of insiders.	5,6,17,31,38~48,76~80	[12] [35]
M39	Implement use of network mapping tools to detect any alterations in the configuration of a network.	31,45,48,77	[35]
M40	Encryption, Deploy media or file encryptors that transparently encrypt sensitive data, data recovery mechanisms to ensure that encrypted data can be recovered	3,33~34,37	[12] [35]
M41	Watermarking	3,32,35~36	[12]
M42	Data Loss Prevention (DLP) suites, DataLeakagePrevention.	3,20,32~36	[34]
M43	Disinformation by Decoys	3,12,37	[34] [40]
M44	Clear screen policy	2~5,11,18,33~36,75	[12]
M45	Continue research on developing a system security architecture sensitive to the demands of the insider threat.	2~4,6,7,9,13,14,32,39~48,55~68,70~78	[35]
M46	Create tools for a rapid and effective audit of a host computer system, to detect any anomalies in its programs and files.	2~4,6,17	[35]
M47	Revocation of authorizations, Enforce policy that requires immediate information system access removal for separated employees.	2~4,22	[12] [35]
M48	Clean desk policy	2~4,11,12,33~36	[12]
M49	Enforce established password policy and procedures, and require mandatory use of strong passwords, one-time passwords or encrypted passwords; bolster this requirement via the use of system features forcing strong password compliance.	2~4,10,11	[35]
M50	Perform research and development on the concept of "honeypots" specifically tailored to attract insiders.	2~4	[35]
M51	Mandate use of tools for effective destruction of information/media waste products so that they are unavailable to insiders (or outsiders).	2,7,9,21,53~54,61~68	[35]
M52	Monitoring and logging	17,38~48	[12] [40]
M53	Third party contracts, Require contractors who use information systems to meet the same requirements, contractually, as government insiders regarding accountability, random computer audits, timely access changes, and password policy.	15,16	[12] [35]
M54	Develop solutions to the problem of "temporary insiders."	15,16	[35]
M55	SIEM	10,38~44,80	[34]

No.	Mitigation	Threat No.	Ref.
M56	Develop tools for effective scanning and analysis of system and network audit logs to detect anomalous system and insider activity.	10,17,38,80	[35]
M57	Mandate use of "warning banners" or other on-line messages that serve to raise the awareness of insiders to the need for secure and appropriate system usage, and that highlight recent observed misuse and its consequences.	1~9,17,15,19,21,32~38,45~68,70~74,76~78,80	[35]
M58	Ensure that proprietary information is well protected.	1~9,11~15,20~23,26,27,32~37,45~74,76~78	[36]
M59	Physical access control	1~4,8,9,14,18,28,33~37,80	[12]
M60	Role Based Access Control	1~4,8,24,25,30,53,78	[12]
M61	Establish a mandatory program to randomly audit insider computer usage, the capability for intense monitoring of individual users, and for critical systems allow maintenance of a continuous map of selected users' activity.	1~4,6~8,10,23,28,45~48,55~75,78,80	[35]
M62	Enforce mandatory and discretionary access control mechanisms to ensure that only a user with the proper clearances and need-to-know is able to access classified or sensitive information.	1~4,6,8,30,33~36,78	[35]
M63	Assure that more than one individual is authorized to access vital system operations and modifications, or perform duties of a security officer.	1~4,6,10,12~17,19,20,24~27	[35]
M64	Authentication	1~4,10	[12]
M65	Establish personnel security vetting procedures commensurate with individuals'levelofinformationsystemaccess.	1~4,78	[35]
M66	Least privilege and need-to-know, ConstrainingNeed-to-Know	1,8,22,23,30,33~36,69,72~74,78	[12] [34]
M67	Security education	1,5,7~9,11~13,15,21,32,37,49~68	[12]
M68	Educate and regularly train employees on security or other protocols.	1,5,7~9,11~13,15,21,32,37,49~68	[36]
M69	Dual control	1,5,6,19,20,80	[12]
M70	Monitoring and Analysis of Incidents, Routinely monitor computer networks for suspicious activity. Audit, AuditTools	1,5,6,17,19,31,38~48,76~78,80	[12] [34]
M71	Contingency planning	1,4,5,13,19,80	[12]
M72	Backup	1,4,5,80	[12]
M73	Perform research on identifying critical information, automatically.	1,3~5,32~36	[35]
M74	Develop and use software tools that check file and access permissions within system and flag potential problem areas.	1,3~5,78	[35]
M75	Separation of duties	1,24,25,30	[12]
M76	Create technology providing a tamper-proof audit trail recording the actions of individuals authorized access to sensitive data and networks.	1,2~4,6~8,10,28,45~48,55~60,70~75,78,80	[35] [41]

No.	Mitigation	Threat No.	Ref.
M77	Create two distinct categories of information technology (IT) insider. *Category1(CAT1):Positions involving privileged access to IT systems with the capability to alter the intended operation or proper configuration of the system. *Category2(CAT2):Positions involving general access to IT systems with read/write permissions, and whose incumbents can receive information from, input information to or modify information on, a system without a reliable human review.	1,19,20,24~25,69	[35]
M78	Establish, as an investigative prerequisite, the requirement for a favorable specific Investigation (ex:SSBI) completed within the past five years for CAT1 insiders.	1,19,20,69	[35]
M79	Conduct minimum periodic reinvestigations (PRs) at a 5-year interval for Cat 1 IT positions and a 10-year interval CAT2 IT positions.	1,19,20,69	[35]
M80	Include appropriate questions in the specific Investigation (ex:SSBI) to address on-line behavior for CAT1 and CAT2 insiders.	1,19,20,69	[35]
M81	Mandate completion of minimum requirements prior to permitting a CAT1 insider to assume assigned duties.	1,19,20,69	[35]
M82	Require a written waiver approved by the head of the agency concerned before foreign nationals are permitted access to CAT1 IT functions.	1,19,20,69	[35]
M83	Develop and use procedures for random reviews of system administrator logs by another System Administrator, chosen randomly and anonymously.	1,19,20,24~25,45~48,53,69	[35]
M84	Remind employees that reporting security concerns is vital to protecting the organization, its reputation, its well-being and its future.	22	[36]

IV. 결 론

'18년 7월 9일 보안 저널에 따르면 美 육군은 내부자 위협을 완화하기 위하여 650만 달러를 투입하여 연방정부 정보 제공업체와 내부자 위협 모니터링 프로그램 구현을 위한 계약을 체결하였다. 또한, 실제로 연간 교육과정을 편성하여 운용하고 있다. NITTF(National Insider Threat Task Force) 내부자 위협 교육프로그램은 2019년에도 편성되었으며 현재 등록사항은 Table 8과 같다.

우리도 이와 같은 실질적인 대응방안이 필요하다. 국방 IT 환경에서는 주로 외부자에 대한 관제가 중심이며, 내부자 위협에 관한 관심이 미흡하다. 단지 감찰 목적으로 비위 여부를 감독하거나, 군사보안업무 시행규칙에 준해서 위반 여부를 감사할 뿐이다.

한국군은 내부자 위협에 대한 명확한 지침 및 업무처리 절차가 전무한 상태로 이번 제안은 의미가 있다고 할 수 있으며, 향후 내부자 위협 완화를 위한 실무에 구체적으로 적용할 수 있는 기술적/관리적 대응방안으로 구체화할 필요가 있겠다.

Table 8. NITTF Insider Threat education program

Date	Registration Availability
Jan. 29-31, 2019	Full/Wait list
Feb. 26-28, 2019	Full/Wait list
Apr. 9-11, 2019	Accepting Registrations
May 7-9, 2019	Accepting Registrations
Jun. 11-13, 2019	Registration Opens April 1
Aug. 20-22, 2019	Registration Opens April 1
Sep. 17-19, 2019	Registration Opens June 1
Oct. 22-24, 2019	Registration Opens June 1

References

[1] Hyeon Jo, Kiho Kwak, Soung-Hie Kim, and Byung-Chun Kim, "A Study on Defense IT Governance and Principle Establishment," Journal of

Advanced Information Technology and Convergence (JAITC) 10(9), pp. 153-162, Sep. 2012.
〔2〕 Choi Kwang-Bok, "A Study on the Analysis of Defense Information Protection Environment and the Research Direction of Security Management Model for Cyber Warfare Response," Review of KIISC21(6), pp. 6-14, Oct. 2011.
〔3〕 Lee Dong-hoon, "Defense IT Convergence Technology for Improved Interoperability of Weapon System-Non-Weapon Systems," 2012 Defense IT Convergence Support Center Result Report Appendix 2, Apr. 2013.
〔4〕 Jung Jong and Joongeup Kye, "Aspect a Future War and Development Direction of Weapon-system," The 8th Conference on National Defense Technology, pp. 306-318, Jul. 2012.
〔5〕 Kwon Oh Hun, Lee Myoung Hun, and Lee Jae Woo, Chae-ho Lim, "Real-Time Security Management System for Defense Network," Review of KIISC 23(6), pp. 54-66, Dec. 2013.
〔6〕 Chief Information Officer, "Environment", https://dodcio.defense.gov/Portals/0/Documents/JIE/DoD%20IT%20Environment%20Way%20Forward-%20DISTRO(Aug%202016).pdf, Feb. 2019.
〔7〕 Chief Information Officer, "Environment", https://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf, Feb. 2019.
〔8〕 Critical Infrastructure Resilience institute, "Cyber Warfare", https://ciri.illinois.edu/sites/default/file%20s/2018.2.27._Cyber%20Warfare.pdf, Feb. 2019.
〔9〕 U.S. Department of Defense, "CYBER STRATEGY", https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, Feb. 2019.
〔10〕 Army college, C4I system, National Library of Korea(print dept in army), daejeon, 202, 2008
〔11〕 Lee Ho Kyun, "National Defense Command and Control System (C4I) Development Trends," National defense and technology(429), pp. 58-71, Nov. 2014.
〔12〕 W Cornelissen, "Investigating insider threats:problems and solutions," Master thesis, essay.utwente.nl-, May. 2009.
〔13〕 Bishop, M., "Panel: the insider problem revisited," In Proceedings of the 2005 workshop on New security paradigms (Lake Arrowhead, USA), pp. 75-76, Jan. 2005.
〔14〕 Butts, J.W., Mills, R.F. and Baldwin, R.O., "Developing an insider threat model using functional decomposition In Proceedings of the Third international workshop on mathematical methods," models, and architectures for computer network security (St. Petersburg, Russia, September 25-27), pp. 412-417, Sep. 2005.
〔15〕 Carroll, M.D., "Information security: examing and managing the insider threat," In Proceedings of the 3rd annual conference on Information security curriculum development, Kennesaw, Georgia (USA), Sep. 2006.
〔16〕 〔16〕 Predd, J. et al., "Insider behaving badly", IEEE security and privacy 6 (4), pp. 66-70, Jul. 2008.
〔17〕 Schultz, E. E., "A framework for understanding and predicting insider attacks", Computers and Security 21(6), pp. 526-531, Oct. 2002.
〔18〕 Brackney, R.C. and Anderson, R.H., "Understanding the insider threat," In Proceedings of a March 2004 Work shop (March 2-4, 2004, Rockville, MD, USA), Mar. 2004.
〔19〕 Wood, B., "An insider threat model fo

r adversary simulation," In proceeding s of the conference on Research on Mi tigating the Insider Threat to Informa tion Systems #2 (Arlington, USA), Ap pendix B, pp. 41-48, Aug. 2000.
〔20〕 〔20〕 Magklaras, G.B. and Furnell, S. M., "Insider threat prediction tool: ev aluating the probability of IT misuse," Computers & Security 21 (1), pp. 62-73, Jan. 2002.
〔21〕 Neumann, P.G., "The challenges of in sider misuse," SRI Computer Science Laboratory, Paper prepared for the W orkshop on Preventing, Detecting, an d Responding to Malicious Insider Mis use, 16-18 August 1999, at RAND, Sa nta Monica, CA, Aug. 1999.
〔22〕 Anderson, R.H. et al., "Research on m itigating the insider threat to informa tion systems," In Proceedings of a Wo rkshop Held August 2000, Aug. 2000.
〔23〕 Microsoft, "Modeling", https://www.mi crosoft.com/en-us/download/details.as px?id=49168, Jan. 2019.
〔24〕 Jung Joo Bae, Jeong-Dong Kim, Youn g-Duk Seo, and Doo-Kwon Baik, "Defi nition and Implementation of an Onto logy Based Schema for Interoperability of Common Operational Pictures in a Battle Management System," Journal of KIISE : Database 40(1), pp. 62-78, Feb. 2013.
〔25〕 〔25〕 Park Hyun Jae, "Report(A Study on the Improvement and Develop ment of the Naval Command Control System)," Ministry of National Defen se(www.prism.go.kr), Dec. 2012.
〔26〕 Army Tactical C4I Development Team, Top 100 Questions 100 Answers to Gr ound Tactical C4I System, National L ibrary of Korea(print dept in army), d aejon, 172, 2005.
〔27〕 NIST, "Insider", https://csrc.nist.gov/c src/media/publications/conference-pap er/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande80.pdf, Jan. 2019
〔28〕 Kim Jong-Ki and Oh Da-Woon, "A Stu dy on Security Policy Violations of Or ganization Members," Informatization p olicy 25(3), pp. 95-115 , Sep. 2018.
〔29〕 Carnegie Mellon Univ.sei, "Insider Thr eat", https://resources.sei.cmu.edu/ass et_files/TechnicalReport/2019_005_001_540647.pdf, Feb. 2019.
〔30〕 Gu Samuel and Kim Seul-ki, "A Study on The Security Vulnerabilities in Sel f Protection of Anti Viruses," https://agz.es, Sep. 2011.
〔31〕 Hong Byung-jin and Lee Soo-jin, "Desi gning of The Enterprise Insider-Threats Management System Based on Tasks and Activity Patterns," Journal of Info rmation and Security 15(6), pp. 3-10, Oct. 2015.
〔32〕 Young-geun Kim and Jinyoung Choi, "A Study on the Korean company's red iness against to Insider Threat," Com munications of the Korean Institute of Information Scientists and Engineers 2017, pp. 1,087-1,089, Jun. 2017.
〔33〕 Observeit, "Insider Threat", http://pag es.observeit.com/rs/248-SYG-803/image s/ObserveIT-Insider-Threat-Manageme nt-Library-v7.0.0.pdf, Jan. 2019.
〔34〕 Ivan Homoliak, Falvio Toffalini, Juan Guarnizo, Yuval Elovicl and Martin O choa, "Insight into Insiders and IT:A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeas ures," ACM Computing Surveys, vol. 5 2, no. 30, May. 2019.
〔35〕 Defense Technical Information Center, "Insider Threat", https://apps.dtic.mil/dtic/tr/fulltext/u2/a391380.pdf, Jan. 2019.
〔36〕 U.S.Army Cyber Command, "Insider T

hreat", https://8tharmy.korea.army.mil/site/assets/doc/resource/information-assurance/ARCYBER-fact-sheet-Insider-Threats(2Sep2015).pdf, Jan. 2019.

[37] Brian M. Bowen, Malek Ben Salem, Shlomo Hershkop, Angelos D. Keromytis, and Salvatore J. Stolfo, "Designing Host and Network Sensors to Mitigate the Insider Threat," In IEEE Security & Privacy Magazine, vol. 7, No. 6, pp. 22-29, Nov./Dec. 2009

[38] exabeam, "Insider Threats", www.exabeam.com/ueba/insider-threats, Jan. 2019.

[39] N. Nostro, A. Ceccarelli, A. Bondavalli, and F. Brancati, "Insider threat assessment: A model-based methodology," SIGOPS Oper. Syst. Rev., vol. 48, no. 2, pp. 3 - 12, Dec. 2014.

[40] Carnegie Mellon Univ.sei, "Insider Threat", https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html, Jan. 2019.

[41] Kyungroul Lee, Sun-Young Lee, and Kangbin Yim, "Classification and Analysis of Security Threats in the Infrastructure," The Journal of Korean Institute of Communications and Information Sciences 43(3), pp. 572-579, Mar. 2018.

〈저자소개〉

원 경 수 (Kyung-su Won) 정회원
2002년 2월: 연세대학교 전산학과 졸업
2016년 9월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 내부자 위협, 악성코드 분석, 사이버 위협 인텔리전스

김 승 주 (Seung-joo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월: KISA(舊 한국정보보호진흥원) 팀장
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화전문가
2004년 3월~2011년 2월: 성균관대학교 정보통신공학부 조교수, 부교수
2011년 3월~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2004년~현재: 한국정보보호학회 이사
2005년~2006년: 교육인적자원부 유해정보 차단 자문위원
2007년 :국가정보원장 국가사이버안전업무 유공자 표창
2007년~2009년: 전자 정부 서비스 보안 위원회 사이버 침해사고대응 실무위원회 위원
2010년 :방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2012년 3월~2012년 6월: 선관위 디도스 특별검사팀 자문위원
2013년 4월~2013년 12월: IT보안인증사무국 자문위원
2013년 9월~현재: 중앙선거관리위원회 자문위원
2014년 3월~현재: 헌법재판소 자문위원
2014년 12월~현재: 카카오 자문위원
2016년 1월~현재: 한국정보화진흥원 자문위원
2018년 4월~현재: 원자력안전위원회 전문위원
2018년 9월~현재: 국방부 정보화책임관(CIO) 자문위원
2018년 11월~현재: 4차산업혁명위원회 위원
〈관심분야〉 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable security