https://doi.org/10.33778/kcsa.2023.23.5.173

정보보안 위험관리를 활용한 사이버 위협 군사 대응 전략

유 진 철*

요 약

제4차 산업혁명 기술은 현재 우리 군이 처한 병력 감축과 국방예산 감소라는 장애물을 넘어 초연결 초지능화된 네트워크 중심 작전 환경을 구축하는 해결책으로 대두되고 있다. 그러나 최신 정보기술에 대한 복잡성 증대와 기 운용중인 정보시스템과의 영향성 검증을 포함한 전체적인 위험관리가 미흡하여 시스템 무결성과 가용성에 심각한 위협을 초래하거나 시스템 간 상호운용성에 부정적 영향을 끼침으로서 임무 수행을 저해할 수 있다. 본 논문에서 우리는 정보기술의 발전에 따라 발생할 수 있는 사이버 위협으로부터 군 정보화 자산을 보호하기 위해 미국의 정보보안 위험관리에 대한 내용의 고찰을 통해 우리 군이 사이버 위협에 대비하기 위한 사이버 위협 대응 전략을 제시하고자 한다.

Cyber Threat Military Response Strategy Using Information Security Risk Management

Jincheol Yoo*

ABSTRACT

The 4th Industrial Revolution technology has emerged as a solution to build a hyper-connected, super-intelligent network-oriented operational environment, overcoming the obstacles of reducing troops and defense budgets facing t he current military. However, the overall risk management, including the increase in complexity of the latest inform ation technology and the verification of the impact with the existing information system, is insufficient, leading to s erious threats to system integrity and availability, or negatively affecting interoperability between systems. It can be inhibited. In this paper, we suggest cyber threat response strategies for our military to prepare for cyber threats by examining information security risk management in the United States in order to protect military information assets from cyber threats that may arise due to the advancement of information technology.

Key words : cyber threat, information security risk management, enterprise architecture

접수일(2023년 11월 17일), 게재확정일(2023년 12월 26일)

* 육군사관학교 컴퓨터과학과(주저자, 교신저자)

1. 서 론

인공지능, 사물인터넷, 빅데이터, 클라우드 컴퓨팅과 같은 정보통신 기술 중심의 4차 산업혁명의 특징은 경제·사회 분야의 모든 제품과 서비스를 연결해서 사물을 지능화하여 혁신적인 변화를 초래한다는 것이다[1]. 이러한 첨단 기술은 현재 우리 군이 처한 병력 감축과 국방예산 감소라는 장애물을 넘어 초연결 초지능화된 네트워크 중심 작전 환경을 구축하는 해결책으로 대두되고 있다.

그러나 전체적인 위험관리가 미흡한 상태에서 정보시스템의 가용성만을 중시하여 시스템을 구축/운용하고 있는게 현실이다. 이는 정보기술에 내재된 취약점을 악용하여 정보유출뿐만 아니라 시스템 무결성과 가용성에 심각한 위협을 초래하거나 시스템 간 상호운용성에 부정적인 영향을 끼칠 수 있다. 따라서 최신 정보기술에 대한 복잡성 증대와 기 운용중인 정보시스템과의 영향성 검증을 포함한 전체적인 위험관리가 필요하다. 또한, 정보화 자산을 사이버 위협으로부터 보호하기 위해 위험관리에 대한 중요성 인식과 함께 조직 차원의 위험관리 프로세스 정립과 이를 준용하여 정보시스템을 구축하고 운용하는 노력이 필요하다.

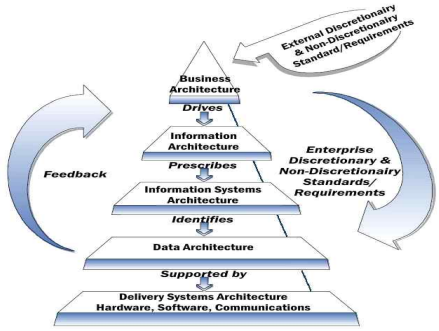
본 논문에서 우리는 먼저 체계적으로 표준화되어 있는 미국의 정보보안 위험관리(Information Security Risk Management, ISRM)에 대한 내용을 살펴보고 정보기술의 발전에 따라 발생할 수 있는 사이버 위협으로부터 정보화 자산을 보호하기 위해 정보관리 위험관리를 활용한 우리 군의 사이버 위협 대응 전략 방안을 제시하고자 한다.

2. 전사적 아키텍처와 위험관리

2.1. 전사적 아키텍처

IEEE 1471(소프트웨어 집약 시스템의 아키텍처 설명에 대한 권장 사례)은 하드웨어 측면의 아키텍처 개념을 소프트웨어 측면의 아키텍처에 대한 사고로의 이전을 가져 왔으며, 아키텍처에 대하여 “시스템을 이루고 있는 구성요소와 구성요소들 사이의 관계, 구성요소와 환경과의 관계, 설계 원칙 등으로 표현되는 기본적인 구성”이라고 정의하였다[2].

전사적 아키텍처(Enterprise Architecture, EA)는 이러한 IEEE 1471의 아키텍처 개념에서 나아가 조직의 성공적인 임무 수행을 위하여 비즈니스, 데이터, 정보기술, 보안 등의 핵심적인 요건을 분석하여 조직의 현재 상태를 확인하고 미래를 설계하는 체계적인 기술을 의미한다[3]. 미국의 국립표준기술연구소(National Institute of Standards and Technology, NIST)는 전사적 아키텍처를 위한 참조모델을 통하여 조직의 비즈니스, 정보, 그리고 기술 환경 요소들 간의 관계를 (그림 1)과 같이 정의하였다.



(그림 1) NIST의 전사적 아키텍처 모델
(출처 : https://en.wikipedia.org/wiki/NIST_Enterprise_Architecture_Model)

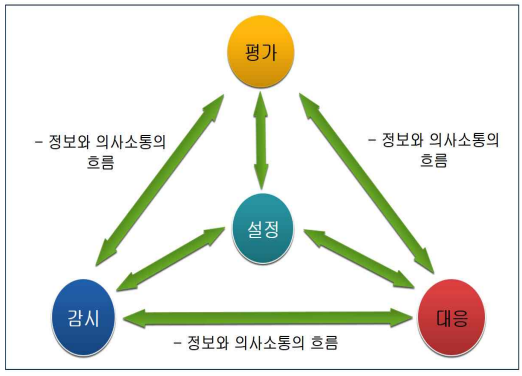
전사적 아키텍처의 기본적인 핵심 개념은 조직의 비즈니스 전략을 설정하고 이를 위한 IT 전략을 수행하는 것이다. 특히 정보시스템에서 사용되는 정보기술의 복잡성과 잠재적 위험이 조직의 성공적인 임무 수행을 위한 관건이 된다. 이러한 문제를 효과적으로 해결하기 위해 아키텍처의 개발과 구현은 필수적이라 할 수 있다.

또한, 전사적 아키텍처는 조직의 정보 자원을 최대한 활용하고 정보보호를 극대화하여 성공적인 임무 수행을 위한 관리기법으로 사용된다. 잘 설계되고 구현된 전사적 아키텍처는 조직이 효과적으로 임무 기능을 보호하고 위험을 관리할 수 있도록 일관성있고 상호운용이 가능한 정보보호 기능을 촉진한다. 이를 위해서 정보보안 아키텍처가 조직의 전사적 아키텍처에 있어서 통합적인 부분이 되어야 한다.

정보시스템의 효율적 도입 및 운영 등에 관한 법률에서는 정보보안 아키텍처를 '정보시스템의 무결성, 가용성, 기밀성을 확보하기 위해서 보안요소 및 이들 간의 관계를 식별하고 정의한 구조'라고 정의하고 있다[4]. 정보보안 아키텍처의 주요 목적은 조직의 정보시스템이 위험관리 전략에 따라 운용되는 환경에서 임무 중심의 정보보안 요구사항이 일관되고 효과적으로 비용을 절감하도록 보장하는 것이다[5].

2.2 위험관리

위험관리는 가지고 있는 자산과 자산에 대한 위협과 취약점을 파악하여 위험을 평가하고 보안대책을 수립하는 일련의 과정으로 보안 관리에 있어서 가장 핵심적이며 전체 조직, 즉 전사적 참여가 필요한 복잡하고 다각적인 활동이다.



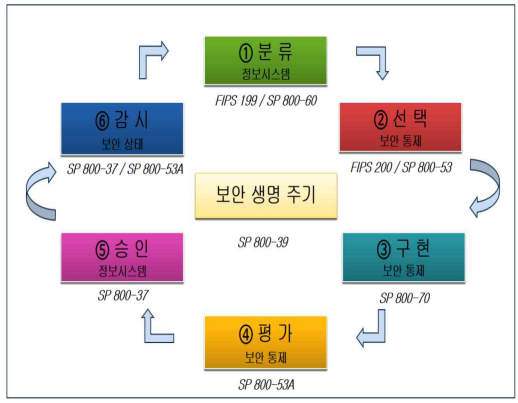
(그림 2) 위험관리 프로세스[5]

위험관리는 (그림 2)와 같이 ① 위험설정, ② 위험평가, ③ 위험 대응, ④ 위험 감시와 같은 4개의 구성요소로 이루어지는 프로세스이다. <표 1>은 위험관리의 구성요소에 대한 설명이다. 이러한 위험관리 프로세스 활동은 조직의 전략적 수준의 위험에서부터 구체적인 전술적 수준까지의 위험을 다루는 전체적인 활동으로 수행되어야 한다. 또한, 위험기반의 의사결정이 전사적 차원에서 통합되고 수행되도록 보장되어야 한다[5].

<표 1> 위험관리 구성요소

요 소	내 용
위험설정	현실적인 위험을 설정 또는 위험 상황을 다루는 신뢰성 있는 전략 수립
위험평가	조직의 위험설정 맥락에서 조직에 대한 위협이 일어날 가능성 평가
위험대응	위험평가 결과에 따른 조직의 대응 방식 (수용, 회피, 완화, 공유, 전가 등)
위험감시	조직이 시간 경과에 따라 위험을 감시하는 방법

위험관리는 (그림 3)과 같은 위험관리 프레임워크(Risk Management Framework, RMF)를 통해서 소프트웨어 개발 생명주기에 의한 명확한 정보보안에 관련된 직무 수행이 가능하다.



(그림 3) 위험관리 프레임워크[6]

위험관리 프레임워크[6]는 다음과 같은 프로세스로 구현된다.

① 정보시스템 분류 : 잠재적인 최악의 상황을 고려하여 보유하고 있는 자산에 대해 정보시스템의 중요도/민감도에 따라 분류

② 보안 통제 선택 : 위험을 해소하기 위한 기본 보안 통제를 선택하고 필요에 따라 위험평가를 통한 추가적인 통제를 적용

③ 보안 통제 구현 : 건전한 시스템공학 관행을 사용하여 전사적 아키텍처 내에서 보안 통제를 구현하고 보안 구성 설정을 적용

④ 보안 통제 평가 : 보안 통제의 효과성을 결정하기 위해 보안 통제가 올바르게 구현되었는지 또는 의도한 대로 동작이 되었는지 등과 같은 정보시스템에 대한 보안 요구사항을 충족하였는지 평가

⑤ 정보시스템 승인 : 정보시스템은 조직 운영, 자산, 그리고 개인 기타 조직에 대한 위험을 결정하고 수용 가능한 경우 운영을 승인

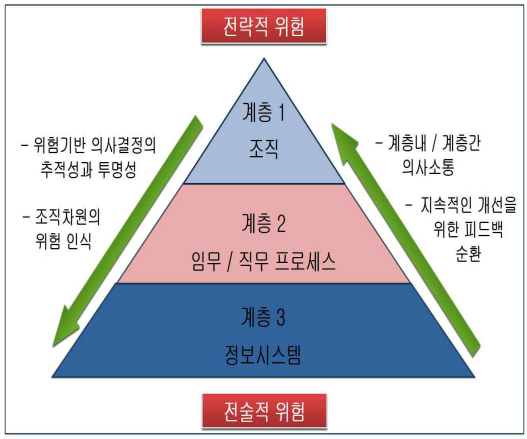
⑥ 보안 상태 감시 : 보안 통제에 영향을 미칠 수 있는 정보시스템의 변경사항을 추적하고 통제 효과를 재평가

최근에는 RMF의 중요성을 인식하여 국내에서도 미국 국방획득체계에 적용된 RMF를 한국 군에 맞게 적용하는 연구[7], 무기체계 개발을 위한 한국형 국방 RMF 구축 방안 연구[8], RMF에 기반한 정보보증의 상호운용성 연구[9]와 같은 RMF를 기반으로 하는 응용 연구가 활발히 진행되고 있다.

3. 위험관리 접근 절차

NIST SP 800-39[5]에서 제시하는 위험관리에 대한 접근은 3단계 계층에 따라 수행되며, 각 단계는 조직 수준에서의 계층 1, 임무 프로세스 수준의 계층 2, 정보시스템 수준의 계층 3으로 구분된다. 각 계층에서는 조직의 성공적인 임무 달성을 위한 유기적인 관계를 유지하기 위해 계층 간 또는 계층 내에서의 의사소통과 위험 관련 활동에 대한 지속적인 개선을 위한 피드백 순환과 같은 전사적인 방식으로 원활하게 수행되는 것이다. (그림 4)는 계층화된 위험관리에 대한 접근 방식과 주요 특성을 보여준다[5].

계층 1은 조직의 관점에서 모든 위험을 관리해야 하는 전략적 위험에 가장 근접한 계층이다. 따라서 조직 내의 현실적인 위험 상황을 분석하여 위험설정(위험관리의 첫 번째 요소)을 하고, 임무의 우선순위를 제공하므로 계층 2와 계층 3에 영향을 끼칠 수 있으므로 신중하게 결정해야 한다. 예를 들면, 계층 2에는 정보보안 아키텍처를 포함한 전사적 아키텍처 개발을 어떻게 하느냐의 문제로, 계층 3에는 기술적 보안 통제 및 운영과 같은 문제에 영향을 끼칠 수 있다.



(그림 4) 계층화된 위험관리[5]

계층 2는 임무 프로세스의 관점에서 위험을 다루고 있고 계층 1에게는 지속적인 개선을 위한 피드백 제공으로 위험결정을 유지 또는 수정할 수 있도록 하는 역할을 한다. 반면에 계층 3에게는 계층 2에서 개발된 전사적 아키텍처와 관련된 정보시스템 설계에 직접적인 영향을 끼친다. 계층 2의 위험관리 활동에는 다음과 같은 내용이 포함된다.

① 조직의 임무 프로세스 정의
② 조직의 전략적 목표와 연관된 임무 우선순위
③ 임무의 성공적 수행을 위한 정보의 유형
④ 정보보안 요구사항
⑤ 조직의 전략적 목표를 이룰 수 있는 효율적인 전사적 아키텍처 구축

계층 3은 정보시스템의 관점에서 위험을 다루고 계층 1의 위험결정과 계층 2의 위험관리 활동에 의해서 유도된다. 또한, 계층 3에서의 활동이 계층 1과 계층 2에게 피드백이 되어 정보보안 아키텍처의 수정 또는 위험설정 변경까지도 가능한 통합적인 구조를 이루게 된다. 계층 3의 위험관리 활동은 다음과 같다.

① 조직 정보시스템 분류
② 정보보안 아키텍처에서의 보안 통제 할당
③ 할당된 보안 통제의 선택, 구현, 평가, 권한 부여 및 지속적인 감시 관리

4. 정보보안 위험관리 관점의 사이버 위협 대응 전략 방안

본 장에서는 지금까지 살펴본 미국의 정보보안 위험관리에 대한 고찰을 통해 위험관리의 필요성을 인식한 가운데 사이버 위협 대응을 위한 우리 군의 정보보안 위험관리 전략을 제시하고자 한다.

4.1 정보보안 위험관리 단계화 추진

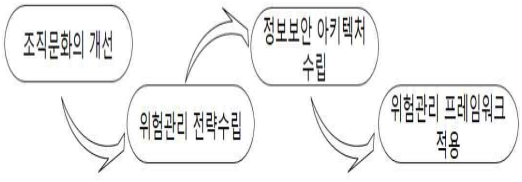
전사적인 관점의 정보보안 위험관리를 위해서는 (그림 5)와 같은 Top-down 방식의 단계적인 절차를 통해서 조기에 정보보안 위험관리 시행 여건 조성이 가능하다.

① 사이버 위협을 정보화 자산의 책임 부서가 중심이 되어 처리하려는 조직 문화가 우선적으로 조성되어야 한다.

② 조직 차원의 전사적인 관점에서 통합적인 위험관리 전략을 수립하고 기능별 위험 우선순위를 설정한다.

③ 정보시스템의 위협을 대비하기 위한 정보보안 아키텍처를 구축하고 위험 대응 전략을 수립한다.

④ SW 생명 주기에 기반한 위험관리 활동을 위해 위험관리 프레임워크를 적용한다.



(그림 5) 軍 정보보안 위험관리 단계화 추진

4.2 정보보안 위험관리 계층별 수행 내용

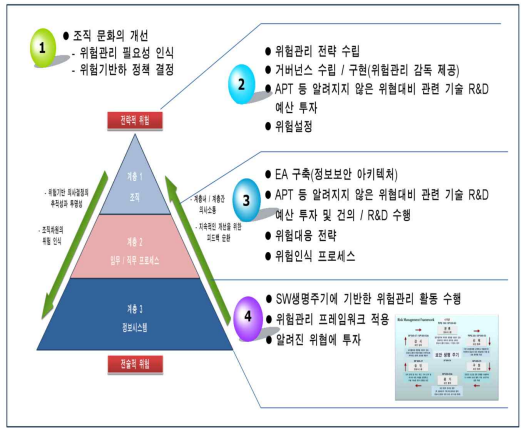
정보보안 위험관리를 위해 요구되는 계층별 주요 수행 내용은 (그림 5)와 같은 아키텍처 관점하에서 계층별 수행 내용을 결정해야 중복되지 않고 개별적이지만 체계적인 기능을 발휘할 수 있다. <표 2>는 계층별 포함되어야 할 주요 수행 내용이다.

<표 2> 계층별 수행 내용

구분	주요 수행 내용
공통	- 위험관리 필요성 인식 - 위험 기반하 정책 결정 등
계층1 (조직)	- 위험관리 전략 수립 - 거버넌스 수립/구현(위험관리 감독) - 알려지지 않은 위협대비 기술 R&D 예산 투자 - 위험설정 등
계층2 (임무)	- EA(정보보안 아키텍처) 구축 - 알려지지 않은 위협대비 기술 R&D 예산 건의 및 R&D 수행 - 위험대응 전략 - 위험인식 프로세스 등
계층3 (정보시스템)	- SW 생명주기에 기반한 위험관리 활동 수행 - 위험관리 프레임워크 적용 - 알려진 위협에 투자 등

4.3 정보보안 위험관리 관점의 軍 추진 전략 방안

전사적 관점의 정보보안 위험관리를 軍에 적용하기 위해 제안하는 추진전략은 (그림 6)과 같다. 이는 ① 단계 공통적인 관점에서의 조직문화 개선에서부터 ② 단계 조직 관점에서의 위험관리 전략 수립, ③단계 임무 관점에서의 정보보안 아키텍처 수립, 그리고 ④단계 정보시스템 관점에서의 위험관리 프레임워크 적용까지의 계층화된 Top-down 방식의 단계적인 절차이다.



(그림 6) 위험관리 관점의 추진전략

① 공통사항 : 사이버 위협에 대한 전사적 인식을 갖기 위한 조직 문화의 개선이 필요하다. 지금까지 적의 사이버 위협으로부터 자산을 보호하기 위한 정보보안 위험관리는 정보화 부서가 정보화 추진의 일환으로 실시하는 것으로 인식되었다. 그러나 이제는 정보화 부서의 적극적이고 주도적인 주요 임무로 변화되어야 한다. 정보보안 위험관리가 기존의 기반 환경 조성 및 위협 상황 관리라는 협의의 위협 대응 수준에서 벗어나 위험관리를 통해 전사적 가치 창출을 위한 작전적 관점에서 해당 위험을 임무 또는 직무 기능에서 어떻게 의사결정을 할 것인지에 대한 주체가 되어 논의하고 결정해야 한다.

② 조직 관점 : 전사적 관점의 정보보안 위험관리를 위한 거버넌스 운영을 통해 위험관리 전략을 수립하여 기술적인 문제보다는 기능별 조직의 적극적인 참여와 협의를 할 수 있는 출발점을 제공해야 한다. 위험관리 전략과 같은 공통의 기준문서를 통해 전사적 위협에 대한 공통된 상황인식이 전제되어야 해당 기능 영역에서 각 기능에 맞는 능동적 정보보안 위험관리가 가능하며 기능별 위험 우선순위 등을 고려한 예산 편성으로 제한된 예산의 효과적인 사용을 촉진시킬 수 있다.

③ 임무 관점 : 전사적 관점의 위험관리를 위해 정보시스템 구축 간 단편적인 보안 관리수준을 벗어나 정보보안 아키텍처에서 보안 요구사항과 해당 요구사항을 충족하기 위해 위험 대응 전략에 따라 편성된 통제조치를 할당하여 보안과 관련된 공통된 기준문서를 산출하여 활용한다. 이 기준문서는 조직의 정보보안 위험관리 전략을 반영할 뿐만아니라 타 시스템과의 정보 교환시 보안 요구사항에 대해 이해 당사자 간 공통된 언어로 사용 가능하며 이러한 정보보안 아키텍처의 산출물을 통해 최종 솔루션 아키텍처에서 최종 보안 요구사항을 만족했는지 여부를 추적할 수 있도록 해준다. 이러한 운영 여건을 조성하기 위해서는 정보보안 아키텍처 수립을 위한 관련 예산을 개발 예산에 포함을 시켜서 개발 단계에서 요구되는 관련 산출물을 정보보안 아키텍처로 대체할 수 있도록 관련 지침 등을 검토할 필요가 있다.

④ 정보시스템 관점: 정보시스템 구축 간 소프트웨어 생명주기 기반의 위험관리 프레임워크를 적용하여 관련자에게 명확한 절차와 지침을 제공하여야 한다. 이를 활성화하기 위해 초기 추진 단계에서는 조직 차원의 지원을 통해 Best Practices를 산출하여 타 정보시스템 구축 간 실무 규약으로 활용토록 포털시스템에 탑재하는 등 전사적 기반 환경 조성을 위한 정책적 뒷받침과 함께 위험관리 통제권 안으로 단계적으로 유입될 수 있도록 법제화 방안도 모색할 필요가 있다.

5. 결 론

현재 군은 사이버 위협에 대한 심각성을 인식하고 과거의 정보보호 차원을 넘어 사이버전을 새로운 전장 영역으로 규정하고 적으로부터 군의 자산을 지키기 위한 많은 노력을 하고 있다. 그 일환으로 사이버 위협에 대한 정보보안 위험관리를 어떻게 하고 있는지 면밀한 진단을 통해 사이버 전장에서의 우위를 확보하기 위한 올바른 방향으로 투사해야 한다.

2019년 미국이 중국의 화웨이社에 대한 규제조치를 시행하였던 것을 보면 사이버 위협에 대한 문제를 국가적 수준에서 결정하고 조치를 시행하는 모습이 우리에게 전달해 주는 시사점은 명확하다[10]. 이제 사이버 위협에 대한 기존의 관행인 정보시스템 중심의 관점에서 벗어나 전사적 관점으로 접근하여 거버넌스와 기반환경을 조성해 나가기 위해 대전환이 필요한 시점이다.

이를 위하여 본 논문에서는 미국의 정보보안 위험관리에 대한 고찰을 통하여 조직문화의 개선, 위험관리 전략 수립, 정보보안 아키텍처 수립, 위험관리 프레임워크 적용이라는 단계화 추진과 각 단계에서는 다음과 같은 수행 내용이 이루어져야 한다는 전략을 제안하였다.

- 1단계(조직문화의 개선) : 사이버 위협에 대한 인식의 전사적 전환에 따른 위험관리를 통한 의사 결정
- 2단계(위험관리 전략 수립) : 거버넌스 운영을 통한 위험관리 전략 수립으로 기능별 위험 설정
- 3단계(정보보안 아키텍처 수립) : 위험 대응 전략에 따라 편성된 통제 조치를 할당하고 공통된 기준문서를 산출하여 활용

- 4단계(위험관리 프레임워크 적용) : 위험관리 프레임 워크에 따른 명확한 절차와 지침 제공

제안된 전략방안을 구현하기 위해서는 우리 군의 실정에 맞는 위험관리에 대한 정책과 전략이 먼저 수립되고 제도적인 정책 변화가 추진되어야 할 것이다. 이러한 기반 위에 정보시스템 환경이 단계적으로 조성되어야 한다. 이를 위해 향후 아키텍처 관점의 위험관리 개념이 사이버작전 수행체계의 기본적인 프레임 워크가 될 수 있도록 관련 작전 수행절차 연구를 통해 사이버 위협에 대비하여야 한다.

참고문헌

[1] “4차산업혁명과 한미동맹”, 쿠키뉴스(http://www.kukinews.com/newsView/kuk202001060062.html).

[2] IEEE 1471-2000, IEEE Recommended Practice for Architectural Description for Software-Intensive Systems.

[3] 전사적 아키텍처, IT위키(https://itwiki.kr/w/전사적_아키텍처).

[4] 최경호, 이동휘, 김귀남, “Multi-level 보안 아키텍처(MLSA) 구축 방안”. 융합보안논문지, 제7권, 제4호, pp. 107-114, 2007.

[5] NIST SP 800-39, ‘Managing Information Security Risk - Organization, Mission, and Information System View’, U.S. Department of Commerce, 2011.

[6] NIST SP 800-37 Rev.2, ‘Risk Management Framework for Information Systems and Organizations’, U.S. Department of Commerce, 2018.

[7] 이용석, 최정민, “한국군에 RMF 적용방안 연구”, 한국통신학회논문지, 제45권, 제12호, pp. 2132-2139, 2020.

[8] 안정근, 조광수, 정한진, 정지훈, 김승주, “무기체계 개발을 위한 한국형 국방 RMF 구축 방안 연구”, 정보보호학회논문지, 제33권, 제5호, pp. 827-846, 2023.

[9] 박종출, 최용훈, “K-RMF 기반 정보보증의 상호운용성 확보방안 연구”, 한국통신학회논문지, 제47권, 제4호, pp. 671-678, 2022.

[10] “미국, 中화웨이·70개 계열사 거래제한...안보침해 위협제기”, MK뉴스(https://www.mk.co.kr/news/world/8816570)

〔저 자 소 개〕

유 진 철 (Jincheol Yoo)
1989년 3월 육군사관학교 학사
1993년 8월 미국 아이오와 주립대학교 (Iowa State Univ.) 석사
2003년 5월 미국 펜실베니아 주립대학교 (Pennsylvania State Univ.) 박사
email : jyoo@kma.ac.kr