Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.6, Dec. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.6.1183

국방획득체계 적용 한국형 보안위험관리 프레임워크

양 우 성,† 차 성 용, 윤 종 성, 권 혁 주, 유 재 원‡
한국형 사이버보안제도개발TF 국군방첩사령부

Korean Security Risk Management Framework for the Application of Defense Acquisition System

Woo-sung Yang,† Sung-yong Cha, Jong-sung Yoon, Hyeok-joo Kwon, Jae-won Yoo‡
K-RMF Dev. Task Force, Defense Counterintelligence Command

요 약

정보 및 정보를 생산, 처리, 폐기하는 시스템은 정보의 총수명주기에 걸쳐 일정수준의 보안이 유지되어야 한다. 일정수준의 보안을 유지하기 위해 소프트웨어 및 자동차 개발, 미국 연방정부 정보체계 등 시스템 수명주기의 보안관리 프로세스를 적용하고 있으나, 우리나라에는 이와 유사한 보안관리 프로세스가 전무한 실정이다. 본 논문에서는 국방 분야 정보 및 정보 처리시스템의 총수명주기에 걸쳐 일정수준의 보안을 유지하기 위한 한국형 보안위험관리 프레임워크를 제안한다. 국방 분야에 적용할 수 있는 한국형 보안위험관리 프레임워크의 개발 목적과 적용방안을 소개함으로써 향후 국방 보안업무가 나가야 할 방향을 제시하고 보안 패러다임의 전환을 유도하고자 한다

ABSTRACT

Information and Information processing systems must maintain a certain level of security during the total life cycle of Information. To maintain a certain level of security, security management processes are applied to software, automobile development, and the U.S. federal government information system over a life cycle, but theme of no similar security management process in Korea. This paper proposes a Korean-style security risk management framework to maintain a certain level of security in the total life cycle of information and information processing system in the defense sector. By applied to the defense field, we intend to present the direction of defense security work in the future and induce an shift in security paradigm.

Keywords: RMF(Risk Management Framework), SDLC(System Development Life Cycle), Risk Assesment, K-RMF

I. 서 론

AI, 빅데이터, IoT 사물인터넷, 클라우드 등 신기술이 등장하고 있다. 신기술은 정보 및 정보 처리를 위한 시스템을 기존 물리 영역으로 확장 연결하였고, 처리해야 할 정보도 증가함에 따라 연동되는 시스템도 비례해지면서 보안관리 영역과 비용도 Fig. 1.과 같이 증가하였다.

보안영역의 확대는 법규 준수여부를 확인하는 컴플라이언스 즉, 체크리스트 방식의 한계를 발생시켰다. 체크리스트 방식의 보안관리 프로세스는 알려진 기술과 공개된 보안취약점에 대한 대응이 가능하지만, 신기술 관련 보안취약점에는 한계를 보인다. 특히, 알려지지 않은 취약점을 노리는 제로데이(zeroday) 공격은 점검항목 및 보안대책이 마련되기 전까지 해당 시스템의 도입 및 활용이 제한되며 위험을 감내하고 있는 실정이다. 체크리스트 방식은 인증 및 인가(Certification & Accreditation)

Received(08. 18. 2022), Modified(11. 21. 2022), Accepted(12. 07. 2022)
† 주저자, themeblue79@gmail.com
‡ 교신저자, rickyoo1@naver.com(Corresponding author)

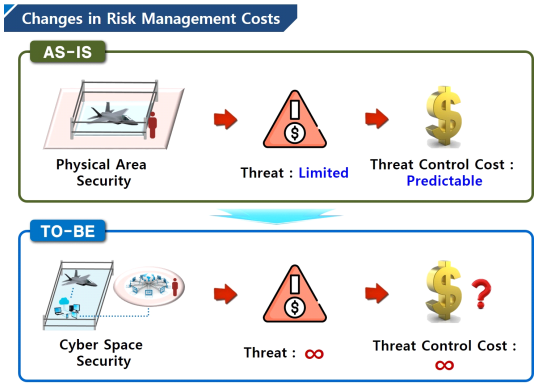

Fig. 1. Cost Increase Due to Expansion of Security Area

형식을 채택하고 있어 점검항목이 통과하면 안전하다고 인가해주는 것으로 신기술 등장과 더불어 발생하는 새로운 보안위협에는 적시적인 대응이 제한된다. 따라서 개발 간 미식별된 취약점이나 신규 취약점 등 새로운 보안위협을 식별하고 위험평가를 통해 보안수준을 일정하게 정보 및 정보 처리시스템의 총수명주기에 걸쳐 위험을 관리할 수 있는 보안위험관리 프레임워크가 필요하다.

본 논문에서는 현행 우리나라의 인증 및 인가(Certification & Accreditation) 형식의 보안관리 프로세스의 문제점을 해결하기 위해 시스템 개발부터 폐기 시까지 총수명주기동안 지속적인 위험평가 및 인가(Assessment and Authorization) 형식의 보안위험관리 프레임워크의 개발하고 이를 국방획득체계 단계에 따라 국방 무기 및 정보시스템에 적용함으로써 한국형 보안위험관리 프레임워크의 적절함을 증명하고자 하였다.

II. 관련 연구

2.1 소프트웨어 개발주기 보안관리 프로세스

소프트웨어 개발방법론은 소스코드 혹은 컴퍼넌트 재사용을 기반으로 소프트웨어위기(Software Crisis)를 극복하며 발전해 왔다[1]. 전통적인 폭포수 모델[1]부터 XP(Agile Process)[2]의 일종인 DevOps 모델[3]까지 생산효율성을 극대화하기 위한 방향으로 발전하였다.

소프트웨어 위기는 시스템의 규모가 커짐에 따라 발생하였다. 생산성 향상을 위한 검증되지 않은 소스코드 혹은 컴퍼넌트 재사용은 잠재적 보안취약점을 시스템이 내재하게 만들었다.

이를 해결하기 위해 기업과 학계에서는 MS-SDL(Microsoft Secure Development Lifecycle)[4, Fig.2.], DevSecOps 방법론[5, Fig.3.]을 제시하고 개발주기에 맞추어 보안을 강화하였으나, 소프트웨어 분야에 한정되어 하드웨어 등 다른 구성품에는 적용하기는 제한이 되었다.

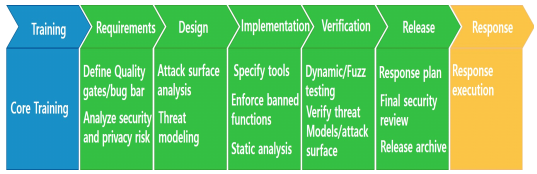

Fig. 2. Microsoft Security Development Lifecycle

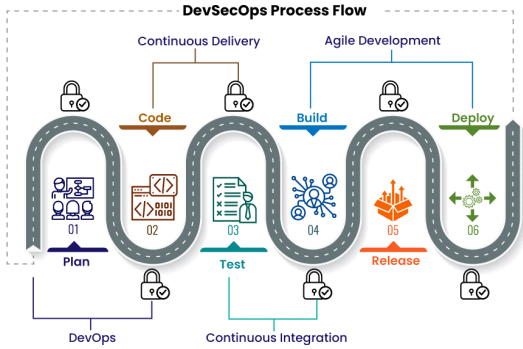

Fig. 3. DevSecOps Process Flow

2.2 자동차 개발 프로세스의 보안관리

자동차 개발 간 보안성 확보를 위한 자동차 사이버보안 규제인 ISO/SAE 21434 및

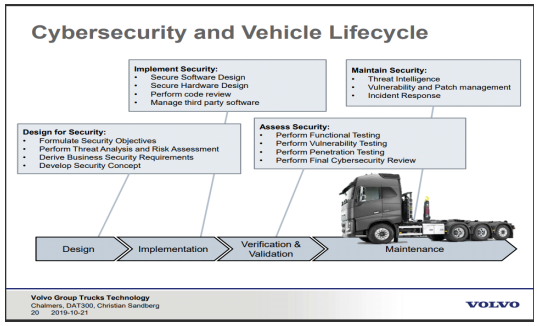

Fig. 4. Connected Vehicle Cybersecurity Volvo Group Trucks Technology

SAEJ3061[6]을 구체화한 Volvo사의 CVL (Cybersecurity and Vehicle Lifecycle) 모델[7, fig.4.]은 앞서 살펴본 소프트웨어 개발주기에 따른 보안관리 프로세스와 유사하게 자동차 개발 수명주기별 보안관리를 포함하고 있다.

소프트웨어와 하드웨어가 결합된 단일 체계에 보안관리 활동을 적용한 바에 의의가 있으나, 각종 정보 체계들이 결합되는 국가 혹은 정부 차원의 보안관리 제도로 적용하기는 한계가 있다고 판단된다.

2.3 미국 연방정부 RMF

미국 연방정부는 소속 기관의 정보 및 정보시스템에 대한 정보보안을 강화하기 위해 NIST(National Institute of Standards and Technology)에서 개발한 Risk Management Framework(이하 RMF)[8]를 발표하였다.

RMF는 물리적, 사이버, 단일 구성품 혹은 플랫폼을 제공하는 공급망에 대한 보안활동을 정의하고 있으며, 정보 및 정보시스템의 수명 주기에 맞추어 수행해야 될 Task를 Fig.5.와 같이 단계별로 제시하였다.

또한, 위험관리기법을 적용하여 잠재된 보안위협과 미충족 보안통제항목(Security Controls)을 관리하도록 하고 있다. 평가방식을 기존 체크리스트 방식(Certification and Accreditation, C&A)을 지속적 위험평가 및 인가(Assessment and Authorization, A&A)방식으로 변경하여 새로운 보안취약점에 대한 위험을 조기 식별하고 대응할 수 있도록 설계하였다.

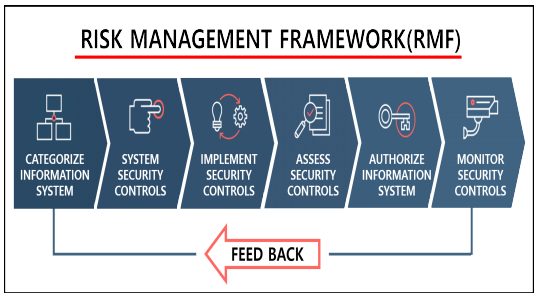

Fig. 5. For more information on each RMF Step, including Resources for Implementers and Supporting NIST Publications, select the Step below

2.4 우리나라 국방무기체계 획득과정간 보안활동

국방보안업무훈령 및 국방사이버안보훈령, 국방전력발전업무훈령에 의거 방위사업청은 무기체계의 정보시스템 및 내장형SW 연구개발 시 탐색개발 단계에서 국군방첩사령부에 보호대책 검토를 의뢰하고 검토 결과를 체계개발 계획에 반영하게 되어 있으며, 전력화 이전 단계에서 보안측정을 실시한다.

전력화 후 보안감사, 기관평가, 보안점검 등을 통해 보안수준을 관리하고 있으나, 소요제기단계에서 보안설계 및 비용 미반영, 신규 취약점에 대한 위험관리 개념은 제도상 부족한 실정이다.

III. 한국형 보안위험관리모델(K-RMF)

3.1 연구 추진 경과

3.1.1 미국 RMF 연구 및 우리 국방 보안환경 고려

한국형 보안위험관리 프레임워크는 미국 연방정부 및 국방부의 RMF를 연구하고 벤치마킹하여 개발하였다. 정보 및 정보 처리시스템의 총수명주기에 걸쳐 보안위험을 단계별로 관리하는 절차는 거의 동일하다.

하지만, 우리나라와 미국의 보안 법령과 정책, 조직과 인력, 예산, 보안기술 등 양국의 보안 거버넌스는 물론, 보안에 대한 인식수준도 상당한 차이가 나기에 미국 RMF를 그대로 우리나라에 적용하는 것은 불가능하였다.

우리나라 국방 보안 거버넌스 및 환경에 대한 분석을 통해 현재 산재되어 중복 수행되고 있는 보안활동을 통합 및 간소화하고 효율성을 제고 할 수 있는 전사적 보안관리 방안을 도출하고자 하였다.

미국의 국방획득체계는 소요제기부터 개발, 운영, 폐기까지 획득과 운영이 일원화되어 연속적인 보안관리가 이루어지는 반면, 우리나라는 획득(개발)과 운영(소요제기, 전력화 이후 폐기까지)이 이원화된 국방획득체계로 사업단계별 보안관리 활동과 주체가 불분명하여 누락되거나 축소되는 문제점이 식별되었다. 이를 해결하고자 시스템 소요제기부터 폐기 시까지 보안관리 활동과 주체를 명시하고 각 기관별 독립적 보안활동 수행여건을 보장함으로써 보안요구사항이 미구현되는 것을 방지하는 한편, 앞서 2.4. 절의 문제점을 보완하고 위험관리 개념의 보안활동을 적용하고자 하였다.

또한, 시스템(체계) 단위의 모호한 보호요구수준 등 미흡한 보안관리 활동을 보다 강화하고 구체화하기 위해 미국 NIST SP 800-53 Rev.4의 Security Controls[9]와 국제 정보보호 표준 ISO 27001, 우리나라의 국방보안 관련 법령을 접목하여 우리나라 국방 무기 및 정보시스템에 적용 가능한 한국형 보안통제항목을 개발하였다.

3.1.2 기존 한국형 RMF 연구와 연관성

본 논문에 앞서 한국형 RMF에 관한 연구가 발표되었으나 우리나라 국방 조직의 보안환경과 임무 특성을 반영하고 무기 및 정보시스템의 총수명주기에 적용할 수 있는 구체화된 전사적 보안위험관리 프레임워크를 제시한 연구는 없었다.

조현석 등(2019)[10]은 미국 국방획득체계의 RMF를 우리나라 국방획득체계에 적용할 수 있는 한국형 RMF 적용방안을 제시하였다. 국방획득체계의 개발단계에 한하여 RMF 1, 2, 3step 적용방안을 구체적으로 제시함으로써 본 연구 진행에 참고할 수 있는 유용한 결과를 도출하였으나 특정 무기체계와 RMF step 1, 2, 3에만 국한된 연구 결과이었다.

이용석과 최정민(2020)[11]은 미군의 RMF에 대한 문헌연구를 바탕으로 한국군 적용방안을 제시하였으나 우리나라 국방 보안환경과 현실에 대한 구체적인 대안을 제시하지 않은 채 조직 구성, 국방 RMF MKS(Military Knowledge Service), 전문가 양성 및 확보, 한미 협력 등 원론적인 내용만 기술하여 활용이 제한되었다.

박종출과 최용훈(2022)[12]은 한국형 보안통제항목과 현행 국방 상호운용성 정보보호 평가항목과의 중복평가 문제점 및 해소방안을 제시하였다. 본 연구의 산출물인 한국형 보안통제항목을 상호운용성 평가로 국한 지어 연구된 결과로 조현석 등(2019, 재인용)과 동일하게 국한된 연구 결과라고 할 수 있다.

상기 연구들과 직접적인 관련성이 있다고 볼 수 있으나 전사적 보안관리 활동과 위험관리 개념 적용한 본 논문과의 상당한 차이가 있다.

3.2 총수명주기 연계 위험관리 보안 프로세스

국방획득체계와 연계한 6단계의 보안위험관리 수행절차, 한국형 보안통제항목, 전사적 보안관리 활동체계 구성 등 군 보안환경을 고려한 한국형 보안위험관리 프레임워크를 제시하였다.

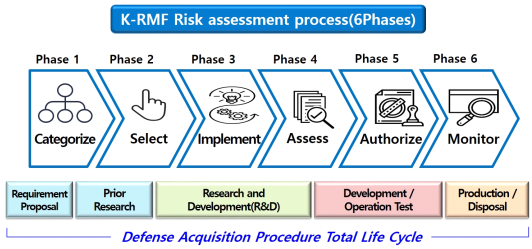

Fig. 6. K-RMF 6 steps process flow

국방획득체계는 Fig.6.과 같이 소요제기-선행연구-탐색/체계개발-시험평가-전력화/폐기로 이루진다. 국방획득체계 단계별 한국형 보안위험관리 프레임워크를 결합하여 총수명주기에 걸쳐 보안수준을 관리할 수 있도록 설계하였다.

3.2.1 보안분류(1단계)

보안 분류는 한국형 보안위험관리 프레임워크 수행절차의 1단계로 도입 또는 운영하고자 하는 정보시스템 및 무기체계의 보호요구수준을 결정하고 보호요구수준에 맞는 2단계 보안통제항목을 선택할 수 있는 기준을 Fig.7.과 같이 제시한다.

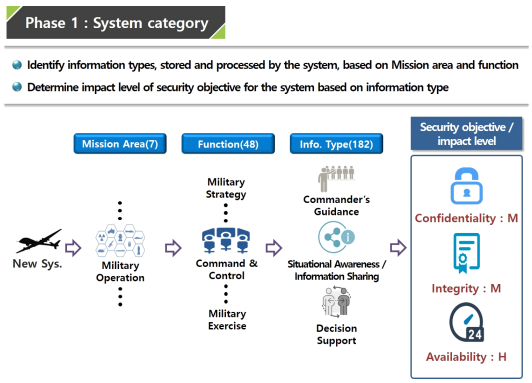

Fig. 7. K-RMF Categorize Step

3.2.2 보안통제항목 선정(2단계)

보안통제항목 선정은 보안 분류에서 결정된 정보시스템 및 무기체계의 보호목표와 보호수준을 달성하기 위해 보안통제항목을 선정하는 과정으로 국방획득주기의 선행연구 단계에서 수행하는 보안활동이다.

Fig.8.과 같이 정보시스템의 보안 분류 결과가 기

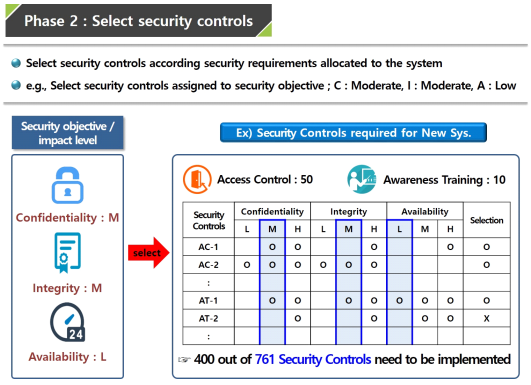

Fig. 8. K-RMF Select Step

밀성 '중', 무결성 '중', 가용성 '하' 이라면 이에 해당하는 보안통제항목을 선정한다. 선정된 보안통제항목은 보안정책, 정보 및 정보체계의 특성과 운용환경, 위협기반 위험평가 결과 등을 반영하여 필요한 보안통제항목을 추가하거나 제거하는 조정 과정(Tailoring)을 거쳐 최종 선정한다.

3.2.3 보안통제항목 구현(3단계)

선정된 보안통제항목을 보안계획에 따른 보안요구사항을 고려하여 보안기술을 구현 및 개발하는 단계이며 국방획득체계 중 탐색/체계 개발에서 수행하는 보안활동이다.

Fig.9.와 같이 선정된 보안통제항목을 구축하고자 하는 시스템에 실제 적용하는 단계이며, 실제 개발을 통해 구현할 분야와 운용 간 구현할 분야로 구분하여 시스템 설계·구현 간 반영하거나 운용지침서에 포함시키는 과정이다.

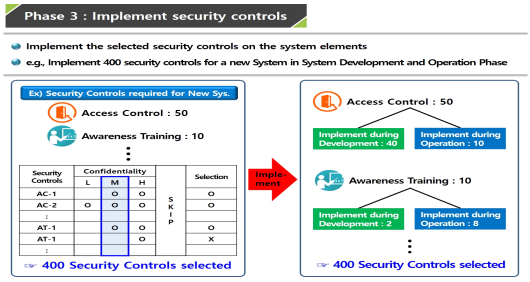

Fig. 9. K-RMF Implement Step

3.2.4 보안평가(4단계)

보안평가는 개발 또는 운영하고자 하는 정보 및 정보시스템의 보안요구사항에 맞게 보안통제항목이 올바르게 구현되었는지, 의도한 대로 보안기능이 작동하는지에 대한 적절성을 평가하는 단계이다. 국방획득체계 중 탐색/체계개발과 개발/운용시험평가 단계에서 수행한다.

Fig.10.과 보안통제항목 중 미충족 보안통제항목을 식별하여 추가 개발 등을 보완하거나 후속조치계획에 통해 운용절차를 보완한다. 체계 수준에서 미충족 보안통제항목으로 인해 발생하는 위협분석을 통해 시스템의 위험평가를 실시하게 된다.

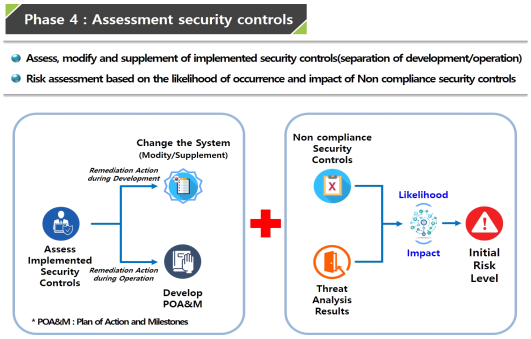

Fig. 10. K-RMF Assess Step

3.2.5 시스템 인가(5단계)

시스템 인가 단계는 해당 정보 및 정보시스템 위험 수준이 조직이 설정한 위험정책에 따라 위험 허용범위인 수용·완화·회피·전가를 결정단계이다.

Fig.11.과 같이 4단계에서 이루어진 보안평가 결과를 바탕으로 조직의 임무 우선순위, 평판도 등을

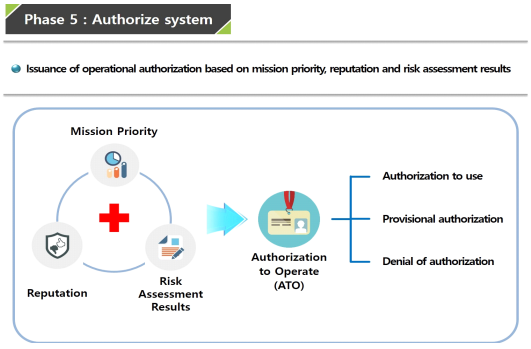

Fig. 11. K-RMF Authorize Step

고려하여 인가 여부를 결정한다. 국방획득체계의 전력화 결정 과정에 해당한다.

운영인가는 해당 정보 및 정보시스템 위험 수준에 따라 인가 기간을 차등적으로 부여한다.

3.2.6 보안 운용관리(6단계)

보안 운용관리 단계는 보안위험관리 프레임워크의 가장 핵심으로 운용환경 변화 및 새로운 취약점 식별 또는 인가기간 만료에 따른 재인가시 위험평가를 통해 일정수준 보안수준을 Fig.12.와 같이 유지하는 단계이다. 국방획득체계 중 전력화 이후 단계로 각 군에서 운용하는 단계로 볼 수 있다.

5단계 이후 보안 운용관리 전략에 따라 구현항목별 주기에 따라 보안 상태를 점검하고 미충족 보안통제항목의 후속조치 이행 및 구현상태 확인은 물론, 새로운 보안위협 식별, 보안정책의 변화, SW·HW 시스템 업그레이드 또는 교체, 실무자 변경 등 각종 보안환경의 변화 시마다 조직과 운용하는 정보시스템 또는 무기체계의 보안위협을 분석하고 보안평가와 위험평가를 실시하는 등 지속적인 보안위험관리활동을 통해 일정수준의 보안수준을 유지한다. 이 단계는 폐기 시까지 반복 시행하는 과업이다.

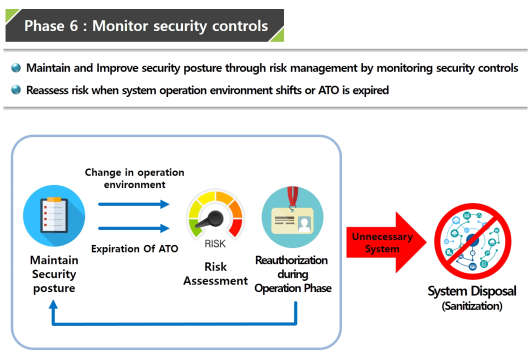

Fig. 12. K-RMF Monitor Step

3.3 한국형 보안위험관리의 핵심 요소

3.3.1 전사적 보안관리 활동

최근 증가하는 공격유형(공급망 공격, 내부자 위협, 사회공학적 공격 등)에 대한 대응을 위해서는 전사적 보안활동이 이루어져야 한다.

한국형 보안위험관리 프레임워크는 Fig.13.과 같

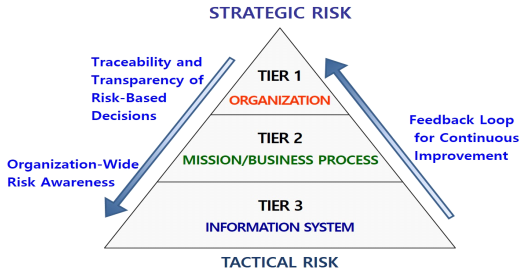

Fig. 13. ORGANIZATION - WIDE RISK MANAGEMENT APPROACH

이 전사적 수준의 3계층 위험관리 개념을 도입·적용하였다.

조직수준에서 보안위험 전략·정책을 수립하고 위험관리의 전반적인 조정·통제 역할을 수행하는 최상위 계층, 임무 및 사업관점에서 조직의 임무와 연계下 사업을 추진하는 계층, 실질적으로 체계를 운용하는 계층으로 구분하여 조직 전체가 보안활동에 참여하도록 설계하였다.

현재 체계를 운용하는 계층에게만 보안활동과 책임이 집중되어 있는 문제점을 해소하고 한국형 보안위험관리 프레임워크 적용 시 각 계층별 임무분장을 구분하여 조직 전체가 보안활동에 참여토록 하였다. 전사적 보안활동은 조직의 보안 인식을 일치화하고 각 계층 간 의사소통을 통해 보안정책 수립 및 시행 간 발생 가능한 보안 공백을 최소화하는 등 보다 효과적인 보안 관리를 추구할 수 있다.

3.3.2 기관별 독립적 보안활동

한국형 보안위험관리 프레임워크는 기능별 독립적 보안활동을 보장하기 위하여 Fig.14.와 같이 기관별 특성과 기능을 고려하여 인가, 평가, 사업, 운영, 정책기관으로 구성하였다.

또한, 제도의 절차에 상응하는 각 기관의 임무를

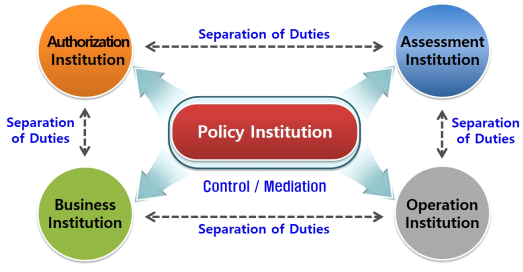

Fig. 14. Functional Isolation of K-RMF

명확히 구분하고 있다. 이는 조직 통제의 핵심이 되는 직무분리 개념을 적용하여 기관별 '이해상충 방지'가 수행될 수 있도록 설계하였다.

3.4 위험관리 기반의 보안관리

위험관리 기반의 보안관리는 미국 연방정부 NIST RMF와 매우 유사한 개념으로 경영과학의 위험관리와 정보보호의 보안관리 개념을 접목하였다. 정보 보안, 개인정보보호 및 위험관리 활동을 시스템의 총수명주기동안 시행하는 체계적인 보안관리 활동이다. 정보보호의 위험관리의 원칙은 정보 및 정보를 취급하는 체계에 피해를 유발할 수 있는 위협의 영향을 확인, 통제, 제거, 최소화하는 것으로 위험 분석, 위험의 처리에 대한 결정, 보호 대책의 선정 및 구현, 잔여 위험 분석 등의 위험평가 과정이 보안위험관리 프레임워크 전단계에서 반복적으로 수행되어야 보안 위험관리의 효과를 기대할 수 있다. 위험관리의 핵심인 위험평가는 획득하고자 하는 정보 또는 무기체계에 대한 위협을 식별하고 취약요인에 대한 영향성 평가를 통해 보안 위험수준을 결정하고 완화 방안을 마련하는 활동이며 인가기관의 위험 수용 여부의 판단 근거로 활용된다.

최초 한국형 보안위험관리 프레임워크도 미국 연방정부 NIST RMF와 동일하게 국방획득체계의 전단계에서 위험관리를 실시하는 것으로 개발하였으나 보안위험관리를 처음 도입하는 현실과 단계별 위험평가의 세부적인 사항에 대한 논의와 추가 개발 소요 등을 종합 고려하여 보안통제항목 선정 2단계의 위협기반 위험평가와 보안평가 4단계의 보안통제항목 기반의 위협평가로 축소하였다. 향후에는 모든 단계에서 위험관리와 평가를 실시할 수 있도록 추가 방안을 개발하여 확대 적용할 예정이다.

3.4.1 위협기반 위험평가

위협기반 위험평가는 보안위험관리 프레임워크의 보안통제항목 선정 2단계에서 시행된다. 획득하고자 하는 체계의 예상 위협과 운용 조직의 보안 위협을 바탕으로 시스템 분류 결과에 따라 선정된 보안통제항목의 위험도를 판단하게 된다. 사업주관 기관은 소요제기 기관의 보안요구사항과 인가기관의 위험 허용 수준을 충족할 수 있도록 위협을 분석하고 이를 선행연구 결과에 반영한다. 선행연구 기관은 인기가관에서 작성한 위협분석 결과와 소요제기 기관의 보안요구사항을 확인하고 사업주관 기관과 협조하면서 공개된 위협 정보를 실질적으로 분석함으로써 보안의 완전성을 기하게 된다. 각 기관은 반복적인 위협기반 위험평가를 통해 보안통제항목을 조정하는 테일러링을 거쳐 최종 보안통제항목을 선정하고 인가기관은 선정된 보안통제항목이 위험을 통제할 수 있다고 판단되었을 시 최종 승인한다.

3.4.2 보안통제항목기반 위험평가

보안통제항목기반 위험평가는 보안위험관리 프레임워크 4단계에서 독립적이고 전문화된 평가기관이 소요제기, 사업관리, 연구개발 기관에서 선정된 보안통제항목의 구현여부를 평가하고 미구현 보안통제항목에 대한 위협을 분석하여 위험완화 방안을 마련하여 인가기관에 제공하게 된다.

미구현 보안통제항목으로부터 발생할 수 있는 취약점 및 위협을 분석하고 식별된 위협의 발생 가능성과 체계에 미칠 영향성을 종합적으로 판단하는 초기 위험수준 평가를 통해 초기 위험도를 산출한다. 산출된 초기 위험도가 조직의 위험관리 허용 수준보다 높을 시에는 조정된 위험수준 평가를 통해 미구현 보안통제항목과 구현 보안통제항목과의 연관 관계를 분석하여 초기 위험수준 평가 결과의 가능성과 영향성을 완화할 수 있는 요인을 식별하고 초기 위험도의 수준을 재판단하여 조정된 위험도를 산출한다. 조정 위험수준 평가에도 불구하고 조정된 위험도가 조직의 위험관리 허용 수준을 초과한다면 다시 초기 위험도의 가능성과 영향성을 낮출 수 있는 위험완화 방안을 마련하여 인가기관에 권고안을 제시한다. 인가기관은 권고안을 참고하여 미구현 보안통제항목 구현 또는 연관 구현통제항목 보완을 통해 위험도를 낮추고 관련 결과를 평가기관에 제출하여 재평가를 실시하는 등 위험도를 낮추기 위한 반복적인 위험평가를 시행하게 된다.

보안통제항목기반 위험평가 결과는 인가기관의 체계 사용 인가 여부의 근거로 사용된다.

IV. 향후 연구 분야

미국 NIST는 2002년부터 법적 근거를 바탕으로 정부 및 군, 학계, 민간 보안기업 등으로 구성된 태스크포스를 조직하여 각종 보안 위협에 대응할 수 있

는 최적화된 보안정책과 최신 보안기술을 적용한 RMF를 개발하였으며 현재도 계속 업데이트하고 있다. 한국형 보안위험관리 프레임워크도 우리나라 국방 보안환경에 적합하고 쉽게 적용할 수 있도록 최적화가 필요하며 최신 보안정책과 기술을 개발하여 반영하는 등 지속적인 연구가 필요하다.

4.1 기존 보안제도와 연계연구

현재 국방보안업무훈령 및 국방사이버안보훈령, 국방전력발전업무훈령 등에 의거 보안대책 검토, 보안측정, 취약점 분석·평가, 신뢰성시험, 보안적합성 검증, 보안감사, 사이버보안기관평가, 방위산업실태조사 등 각종 보안 제도가 수행되고 있으나 각 제도가 개별적으로 시행되고 있으며 국방획득주기와의 연계성도 없는 등 전사적 보안 관리와는 거리가 멀다고 할 수 있다. 한국형 보안위험관리 프레임워크가 정상 시행된다면 현행 우리 군의 보안업무의 미흡점은 해소될 것이지만 현행 보안업무의 중복성, 기관별 보안제도 및 유사활동과의 연계성, 훈령과의 상충문제 등 선결해야 할 과제가 많다. 기존 보안업무 수행체계와의 효율적 통합방안에 연구가 추가되어야 한다.

4.2 위험평가론 개선발전 방안

우리나라 정부에서 시행하는 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증과 국제 표준인 정보보안 경영시스템(ISO27001) 인증제도의 중심에도 위험관리가 있다. 다만, 위험을 분석, 평가하여 적절한 정보보호대책을 선정하고 구현하는 개념은 동일하지만 한국형 보안위험관리 프레임워크의 위험평가는 미국 연방정부 NIST SP 800-30(Guide for Conducting Risk Assessments), 미국 국방부 Cyber security Risk Assessment Guide를 기반으로 MITRE의 CAPEC과 ATT&CK, Lockheed Martin의 Cyber-kill chain 등 위협모델을 접목하여 개발되었다. 현재 시행중인 제도와 한국형 보안위험관리 프레임워크의 위험평가는 보안개념과 위험평가 산정 방식이 다르기에 향후 한국형 보안위험관리 프레임워크가 국방분야에 정착되었을 시 위험관리에 대한 제도 표준화가 필요하다.

한국형 보안위험관리 프레임워크의 위험평가는 처음 도입되는 것으로 국내에는 관련 연구 및 참고자료가 부족하여 미국의 위험관리 및 평가 중심으로 개발되면서 개념을 이해하는데 중점을 두었다. 이로 인해, 위험관리 전략과 계획 수립, 위험 구성 요소 분석, 위험평가 방법론, 보호대책 선정, 구현 계획 수립 등 위험관리 5단계 과정과 이와 연계한 한국형 보안위험관리 프레임워크 수행단계별 위험평가 세부사항이 구체화되어야 하며 위험평가 및 수행방법이 추상적이거나 이해하기 어려운 부분이 있어 실무자들이 적용하기 어려운 실정이다. 보다 이해하기 쉽고 적용하기에 쉽도록 추가 연구가 필요하다.

V. 결 론

우리나라 국방 정보 및 무기체계에도 최신 기술이 도입됨에 따라 보안 위협도 증가하고 있다. 기존의 경계 기반 보안 중심의 보안정책과 공개된 취약점 제거 위주의 보안활동은 새로운 위협의 조기 식별 및 대응이 어려울 것으로 예상되는 바, 보안에 대한 과감한 인식 전환과 새로운 보안관리 제도 마련 및 적용이 필요한 시점이다.

우리 군의 직면하고 있는 보이지 않는 보안 위협을 대응하고자 미국 연방정부 NIST RMF 및 국제표준 정보보안 경영시스템(ISO27001) 인증제도, 현행 우리 군의 보안제도를 융합하여 국방획득체계와 연계한 6단계의 보안위험관리 수행절차 및 17개 패밀리 761개의 보안통제항목으로 구성된 한국형 보안위험관리 프레임워크를 개발하였다. 다만, 관련 연구에서 보았듯이 미국 연방정부 NIST RMF와 MS-SDL도 장기간에 걸쳐 변화하는 보안환경과 위협에 대응할 수 있는 보안관리 제도로 개발하고 지속적인 연구개발을 통해 완성도를 높여왔듯이 우리나라 국방 보안환경과 새로운 보안기술에 대한 계속적인 연구가 수행된다면 보다 나은 한국형 보안위험관리 프레임워크로 발전될 수 있을 것이다.

우리나라 국방보안의 새로운 보안제도로 정착되기까지 어려움과 시행착오가 예상되지만 전면 적용 전까지 시범적용과 각계각층의 의견 수렴, 미국 연방정부 및 국방부 RMF의 변화 모니터링 등 다양한 피드백을 통해 한국형 보안위험관리 프레임워크의 완성도를 높이고 조기 정착토록 노력하여 우리나라의 국방 보안수준을 한층 격상시키고자 한다.

References

[1] Jung Sejin, et al, "OOPT:An Object - Oriented Development Methodology for Software Engineering Education", Journal of KIISE, 44(5), pp. 510-521, May. 2017

[2] Kim tai-dal, "Software development project management using Agile methodology", The Journal of the Institute of Internet, Broadcasting and Communication, 16(1), pp. 155-162, Feb. 2016

[3] Son Kyung-A and Yun Young-Sun, "Introduction and Analysis of Open Source Software Development Methodology", Journal of Software Assessment and Valuation, 16(2), pp. 163-172, Dec. 2020

[4] Hur Junghun and Choi Jin-Young, "Practical use of MS SDLC for small mobile app development", Proceedings of the Korean Information Science Society Conference, 39(1C), pp. 292-294, Jun. 2012

[5] Cho Jihoon, "Data security 4.0 for next-generation data security", The Magazine of the IEIE, 48(5), pp. 16-25, May. 2021

[6] Jeong Seungyeon, Kang Sooyoung and Kim Seungjoo, "A Methodology for Integrating Security into the Automotive Development Process", KIPS Transactions on Software and Data Engineering, 19(12), pp. 387-402, Dec, 2020

[7] "Connected Vehicle Cybersecurity Volvo Group Trucks Technology", Volvo GTT Presentation material, 2019

[8] Kim So Jeong, "Information Security : A Comparative Study on Information Security Management Activity of Public Sector in USA & Korea", The KIPS Transactions:PartC, 13(1) pp. 69-74, Feb. 2006

[9] "Security & Privacy Controls for Federal Information Systems and Organizations", NIST SP 800-53 Rev.4, 2013

[10] Hyun-suk Cho, Sung-yong Cha and Seung-joo Kim, "A Case Study on the Application of RMF to Domestic Weapon System", journal of The Korea Institute of Information Security & Cryptology, 29(6), pp. 1463-1474, Dec. 2019

[11] Yongseok Lee and Jeongmin Choi, "Research for Application the RMF to the Korean Military", The Journal of Korean Institute of Communications and Information Sciences, 45(12), pp. 2132-2139, Dec. 2020

[12] Jong-chool Park and Yong-hoon Choi. "A Study on How to Secure Interoperability of Information Assurance Based on K-RMF", The Journal of Korean Institute of Communications and Information Sciences, 47(4), pp. 671-678, Apr. 2022

〈저자소개〉

양 우 성 (Woo-sung Yang) 정회원
2022년 8월: 세종사이버대학교 정보보호대학원 석사
2019년 12월~2020년 12월: 군사안보지원사령부(現 국군방첩사령부) 한국형 사이버보안 제도개발TF
2021년 1월~2021년 12월: 군사안보지원사령부(現 국군방첩사령부) 사이버보안평가TF
2022년 1월~현재: 국군방첩사령부 RMF평가팀
〈관심분야〉 정보보호, 사이버보안, RMF

차 성 용 (Sung-yong Cha) 정회원
2004년 2월: 육군 사관학교 전산학과 전공
2008년 8월: 뉴욕 주립 대학교 전자공학과 석사
2019년 8월: 고려대학교 정보보호대학원 박사
2019년 12월~2020년 12월: 군사안보지원사령부(現 국군방첩사령부) 한국형 사이버보안 제도개발TF
2021년 1월~현재: 국방부(국군방첩사령부)
〈관심분야〉 C4I, 위험관리, 무기체계 신뢰성/보안성 시험평가

윤 종 성 (Jong-seong Yoon) 정회원
2018년 3월: 고려대학교 정보보호대학원 정보보호학 박사
2019년 12월~2020년 12월: 군사안보지원사령부(現 국군방첩사령부) 한국형 사이버보안 제도개발TF
2021년 1월~현재: 공군본부
〈관심분야〉 디지털포렌식, 사이버보안

권 혁 주 (Hyeok-joo Kwon) 정회원
2015년 3월: 단국대학교 산업공학과 학사
2015년 6월~2019년 6월: 육군 정보통신 장교
2021년 12월~현재: 국군방첩사령부 RMF평가팀
〈관심분야〉 정보보호, 공급망관리, 사이버보안, RMF

유 재 원 (Jae-won Yoo) 정회원
1998년 3월: 공군 사관학교 전자공학과 전공
2008년 3월: 미국 오레곤 주립 대학교 컴퓨공학과 석사
2019년 3월: 호서대학교 융합공학 박사
2019년 12월~2020년 12월: 군사안보지원사령부(現 국군방첩사령부) 한국형 사이버보안 제도개발TF 보안제도개발팀장
2021년 1월~2021년 12월: 군사안보지원사령부(現 국군방첩사령부) 사이버보안평가TF장
2022년 1월~현재: 국군방첩사령부 RMF평가팀장
〈관심분야〉 정보보호, 사이버보안, RMF