논문 22-47-04-13 The Journal of Korean Institute of Communications and Information Sciences '22-04 Vol.47 No.04
https://doi.org/10.7840/kics.2022.47.4.671

K-RMF 기반 정보보증의 상호운용성 확보방안 연구

박 종 출◆, 최 용 훈°

A Study on How to Secure Interoperability of Information Assurance Based on K-RMF

Jong-Chool Park◆, Yong-Hoon Choi°

요 약

연합 및 합동 C4I체계 등 각종 체계 간의 막힘없는 정보교환 및 원하는 정보의 무결성을 보장하기 위해서 상호운용성 측면의 정보보호를 평가하고 있다. 또한, 전 세계적인 사이버 위협 증대에 따라 미군은 한·미 연동체계의 RMF 적용을 언급하였고 한국형 사이버보안제도(K-RMF)가 개발되었다. RMF는 사이버보안을 강화하기 위해 정보보호 및 정보보증 개념을 사이버보안 개념으로 대체하였다. 따라서 상호운용성 측면의 정보보호 평가도 정보보증이나 사이버보안으로 개념을 대체할 필요가 있다. 본 논문은 K-RMF 평가항목과 기존 상호운용성 정보보호 평가항목과의 중복성과 K-RMF 평가항목 중 상호운용성 측면에서 재검증이 필요한 항목을 식별하여 K-RMF 기반 정보보증의 상호운용성 확보방안으로 제시하였다.

Key Words : Interoperability, Information Assurance, Information Security, Cyber Security, K-RMF

ABSTRACT

Information security in terms of interoperability is evaluated to ensure seamless information exchange between various systems, such as combined and joint C4I systems, and the integrity of desired information. In addition, with the increase of cyber threats worldwide, the US military mentioned the application of RMF in the Korea-US linkage system, and K-RMF was developed. RMF replaced the concept of information protection and information assurance with the concept of cyber security to strengthen cyber security. Therefore, it is necessary to replace the concept of information security evaluation in terms of interoperability with information assurance or cyber security. This paper identifies items that require re-verification in terms of interoperability and redundancy between K-RMF evaluation items and existing interoperability information security evaluation items and suggested way to secure interoperability of information assurance based on K-RMF.

Ⅰ. 서 론

인터넷의 폭발적인 증가와 함께 대두된 4차산업혁명 시대를 맞이하여 이질적인 시스템 간의 막힘없는 정보교환을 위해서 상호운용성의 중요성이 증대되고 있다. 또한 금전 탈취나 국가 기간망 중단을 목적으로 하는 제3국 및 해커들의 활동으로부터 각국은 귀중한 정보와 자산을 보호하기 위한 노력을 하고 있으며, 더불어 사이버전과 사이버보안(Cyber Security)에 대한 개념이 발전하고 있다. 상호운용성과 사이버전은 상호

※ 본 연구는 정부 (과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2021R1F1A1064080).
◆ First Author : Kwangwoon University Department of Defense Acquisition Program, parkjc001@gmail.com, 학생회원
° Corresponding Author : Kwangwoon University Department of Robotics, yhchoi@kw.ac.kr, 종신회원
논문번호 : 202202-018-C-RN, Received February 6, 2022; Revised February 22, 2022; Accepted February 22, 2022

밀접한 관계에 있으면서도 서로가 장애를 가장 많이 제공할 수 있는 관계이다. 상호운용성 측면에서는 시스템 간 정보유통 보장을 위해 공통된 표준 등을 활용하기 위해 노력하지만 사이버전은 공통된 표준의 취약점 등을 활용하여 공격한다. 미국은 1998년에 정보보호(Information Security) 개념을 정보보증(Information Assurance) 개념으로 전환하였으며, 정보보증 개념도 2014년에 사이버보안 개념으로 대체되었다. 아울러 모든 연방정부 주요 기반시설에 대한 사이버보안을 강화하기 위해 위험기반의 전체수명주기 접근법인 위험관리프레임워크(RMF : Risk Management Framework)[1]를 도입하였다. 우리군은 상호운용성 측면에서 정보보호를 평가하고 있으나, 사이버보안에 대한 개념을 적용하지 못하고 있는 실정이다. 미국은 2019년 4월 지휘통제 상호운용성 위원회(CCIB : Command and Control Interoperability Board)에서 미측 체계와 연동되는 모든 한국 체계들에 대해서는 RMF를 적용해야 한다고 언급하였고 국방부는 2020년 TF를 구성하여 한국형 사이버보안제도(K-RMF)를 개발하였다. 현재 법령화 추진 중이며 AKJCCS에 대한 적용평가를 2021년에 실시하였고, 각군별로 확대 적용중에 있다. 그러나 상호운용성 정보보호 평가항목과 K-RMF 평가항목의 중복성 및 대체 가능성 또는 K-RMF 평가항목의 상호운용성 적용 필요성 등의 검토가 필요하다. 또한 K-RMF는 평가결과에 따라 주기적으로 평가 후 재승인을 득해야 하며 이때 상호운용성에 해당하는 항목에 대해서 상호운용성 평가를 재수행해야 하는 문제가 발생하고, K-RMF 평가결과 승인된 항목에 대해서 상호운용성 평가결과 부적합이 나왔을 경우 책임소재의 문제가 따른다.

본 논문은 상호운용성 정보보증 평가항목에 대해 K-RMF 평가와 중복된 항목과 K-RMF 평가항목의 상호운용성 측면에서의 재검증 필요항목을 선정하여 효율적인 인력 및 예산 운영이 가능하고 책임소재를 명확히 하는 K-RMF 기반 정보보증의 상호운용성 확보방안을 제시한다. 2장에서는 정보보증과 사이버보안 개념연구 및 상호운용성 정보보증 평가와 위험관리프레임워크(RMF) 평가에 대해 살펴보고, 3장에서는 상호운용성 정보보증 개념 훈령 반영, 상호운용성 정보보증 평가항목 조정, K-RMF 평가항목 상호운용성 평가시 재검증 등 정보보증의 상호운용성 확보방안을 제안하고, 4장에서는 결론 및 향후 연구방안을 제시한다.

Ⅱ. 관련연구

2.1 정보보증과 사이버보안 개념 연구

정보보호 개념의 발전[2]을 살펴보면 1970년대 통신기술의 발전으로 기밀성 중심의 통신보안(COMSEC, Communication Security)이라는 용어를 사용하였고, 1970년 후반부터는 컴퓨터의 군사적 활용이 확대되면서 기밀성, 무결성, 가용성 중심의 컴퓨터보안(COMSEC, Computer Security)이라는 용어를 사용하였다. 또한 1980년대 초반부터 통신과 컴퓨터가 통합되고 통신보안과 컴퓨터보안의 구분이 모호해지면서 기밀성, 무결성, 가용성 중심의 정보체계보안(INFOSEC, Information System Security) 용어를 사용하였다. 1990년대 중반부터는 인터넷 보급 확대 및 역기능 인식확산으로 정보와 정보체계의 생존성 및 신뢰성까지 강조한 정보보증이라는 용어를 새롭게 사용하였다. 정보보증은 기밀성, 무결성, 가용성 뿐만 아니라 인증, 부인봉쇄, 탐지 및 대응 등의 서비스로 영역이 확대되었다. PC Magazine은 정보보증을 '정보 및 정보 시스템의 기밀성, 소유 또는 통제, 무결성, 신뢰성, 가용성 및 유용성을 보장하기 위해 설계된 기술 및 관리 조치'라고 정의하였다[3]. 표 1은 정보보호와 정보보증 개념을 비교한 것으로 정보보증은 적절한 보안 수준과 이를 달성하기 위한 최선의 방법을 파악하는 것을 목표로 하는 반면 정보보호는 달성 자체를 다루는 것을 볼 수 있다[4].

사이버보안은 '사이버 공격으로부터 사이버 공간 사용을 방어하거나 보호하는 능력'으로 미국 국립표준기술연구소(National Institute of Standards and Technology)는 정의하였다[5]. 2014년 3월 DoD 최고정보책임자(CIO)는 두 가지 중요문서를 발표하였다. DoDI 8500.01 Cyber Security와 DoDI 8510.01, Risk Management Framework(RMF) for DoD Information Technology(IT) 문서이다. 전자를 통해서는 정보보증을 사이버보안으로 대체하였고, 후자를 통해서는 국방부 IT에 대한 수명주기 사이버방호 리스크관리 과정으로서 기존의 정보보증 인증·인가 프로세서(DIACAP : Defense Information Assurance Certification and Accrediation Process)을 사이버보안 위험관리 프레임워크(RMF)로 대체하였다. RMF의 도입으로 DoD는 기존의 준수사항에 기반한 프로세스를 위험기반의 전체수명주기 접근법으로 전환하였다[6].

DoDI 8500.01[7]에서 '사이버보안은 컴퓨터, 전자통신시스템, 전자통신서비스, 유선통신, 전자통신 및

표 1. 정보보호와 정보보증 비교
Table 1. Comparison of Information Security and Information Assurance

Discipline Characteristics	Information Security	Information Assurance
Dates (approx.)	Since the 1980s	Since 1998
Subject of protection	Information and information systems	Business as a whole
Goals	Confidentiality, Integrity, Availability (Authenticity, Accountability, Non-repudiation, Reliability)	Overall business protection
Type of information	Primarily electronic	All types
Approach	Domination of the technical approach, initial attempts to consider soft aspects (e.g.human factor, administration)	All-encompassing multi-disciplinary systematic approach
Security Mechanisms	Primary focus is on technical security mechanisms; initial consideration of organizational and human-oriented mechanisms	All available (technical, organizational, human-oriented, legal)

그 안에 담긴 정보에 대한 피해를 예방하고 이를 보호, 복구하여 가용성, 무결성, 인증, 기밀성, 부인방지를 보장하는 것'으로 정의하였다. 기밀성은 해당정보에 대한 접근 인가가 없는 이상 시스템 개체(사용자, 프로세스, 기기)에 정보를 공개하지 않는 특성으로 NIST SP 800.53에는 '개인 사생활 및 신용정보 보호 조치 등 정보공개 및 공개 제약 승인을 유지하는 것'으로 정의하였다. 무결성은 인가되지 않은 방식으로 개체가 변경되지 않는 특성으로 NIST SP 800.53에는 부적절한 정보변경 또는 파괴로부터 보호, 정보 부인방지와 인증을 포함한다. 가용성은 인가를 받은 개체의 요구에 따라 접근 및 사용할 수 있는 특성으로 NIST SP 800.53에는 '정보의 시의적절하고 신뢰할 수 있는 접근 및 사용을 보장하는 것'으로 정의하였다.

그러나 일반적인 관점에서의 정보보증과 사이버보안의 차이를 살펴보면 표 2와 같이 사이버보안의 개념이 정보보증의 한 부분으로 표현한 것을 볼 수 있다[8,9]. 또한 그림 1은 HITRUST[10]에서 연구한 정보보호와 정보보증, 사이버보안의 관계를 나타낸 것으로

표 2. 정보보증과 사이버보안 비교
Table 2. Comparison of Information Assurance and Cyber Security

구 분	정보보증	사이버보안
보호대상	정보	데이터
정보유형	모든 유형의 정보	디지털 형식의 보관 정보
보호수준	전략적, 설계	실용적, 구현
위험관리시기	과거, 현재, 미래	현재
성격	방어적	공격적, 방어적

정보보증 개념에 정보보호와 사이버보안이 포함된 것으로 표현하였다.

그러나 미국은 앞서 설명한 것과 같이 정보보증 개념을 사이버보안으로 대체하였다. 따라서 우리군도 일반적인 개념의 관점보다는 미국의 개념을 적용하는 것이 타당할 것이다.

2.2 상호운용성 정보보증 평가

상호운용성 측면에서 정보보증이 필요한 이유는 체계간 정보흐름의 무결성을 보장하는 것이다. 현재 우리군은 정보보호를 정보보증 개념과 혼용하여 쓰고 있는 것으로 보인다.

국방정보화업무훈령[11]에 '정보보호는 정보의 생산·처리·저장 및 유통과정에서 정보의 훼손 변조 유출 등을 방지하기 위한 관리수단 및 기술적인 수단을 강구하는 것을 말한다.' 라고 정의하였다. 또한 '국방 정보보호는 국방정보통신망에 대한 전자적 침해 행위의 거부 정지 제한 예방 확인 점검 역추적 및 봉쇄 등 군의 작전능력을 제고하기 위한 모든 활동을 말한다.'

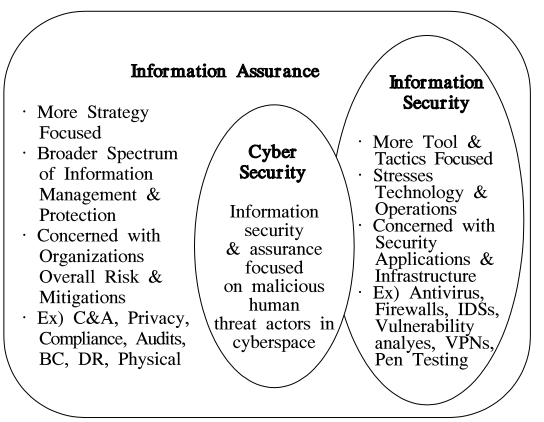

그림 1. 정보보호와 정보보증, 사이버보안의 관계
Fig. 1. Relationship between information security, information assurance, and cyber security

라고 정의하였다. 또한 상호운용성 이론과 실무[12]에 따르면 상호운용성 측면의 정보보호는 상호운용성과 대응되는 개념으로 네트워크 중심 정보공유 환경구축 및 상호운용성 확보를 위한 Net-Readiness의 핵심 요구사항이며, 아군간 정보공유의 범위를 최대화하여 복합체계의 시너지 효과를 극대화 하고자 하는 상호운용성과 대응되는 개념으로써 적에게 정보의 노출 가능성 및 피해를 최소화 하고자 하는 역할로 표현하였다. 아직까지 국방정보화 업무훈령 등에는 정보보증에 대한 개념은 없다.

우리군의 상호운용성 평가는 획득단계별로 소요기획/소요제기단계의 소요평가, 탐색개발 및 정보화전략계획수립단계의 수준측정Ⅰ 및 운용성확인, 체계설계단계의 수준측정Ⅱ, 개발시험평가단계의 표준적합성시험, 운용시험평가단계의 상호운용성시험평가, 운영유지단계의 운영유지단계 평가로 구분된다. 국방정보화업무 훈령상 평가항목에는 운용개념 및 체계 특성, 연동성 및 정보교환, 표준 및 아키텍처, 정보보호, 주파수 등 5개 항목이 있으며 항목별 세부항목을 평가한다. 표 3과 같이 정보보호 평가는 정보보호 수준 등이 있고, 네트워크 정보보호, 관제체계 구축, 키 관리체계 구축, 응용체계 정보보호, 서버 및 단말기 정보보호, 암호장비 적용, 사이버위협 대응능력, SW취약점 제거 항목 등에 대해 수행하고 있다. 사이버위협 대응능력과 SW취약점 제거 항목은 사이버전에 대비한 추가 평가항목으로 국방정보화업무훈령에는 미포함되어 있으나, 국방상호운용성관리지시[13]에는 포함되어 있다.

표 3. 상호운용성 정보보호 평가 항목
Table 3. Interoperability information security evaluation items

구 분	평가항목
정보보호 수준	정보보호 수준의 적절성
네트워크 정보보호	네트워크 정보보호 대책 수립/구현의 적절성
관제체계 구축	관제체계 구축방안 수립/구현의 적절성
키 관리체계 구축	키 관리체계 구축방안 수립/구현의 적절성
응용체계 정보보호	응용체계 정보보호 대책 수립/구현의 적절성
서버 정보보호	서버 정보보호 대책 수립/구현의 적절성
단말기 정보보호	단말기 정보보호 대책 수립/구현의 적절성
암호장비 적용	암호장비 적용계획/적용의 적절성
사이버위협 대응 능력	사이버위협 대응능력
	신분위장 위협 대응능력
	데이터 변조 위협 대응능력
	공격행위 부인 위협 대응능력
	정보유출 위협 대응능력
	서비스거부(DoS) 위협 대응능력
	권한상승 위협 대응능력
SW취약점 제거	SW취약점 제거
	시큐어코딩 규칙적용 적절성
	오픈소스 취약점 제거 적절성

표 4. 획득단계별 정보보호 평가 비교
Table 4. Comparison of information security evaluation by acquisition stage

구 분	소요기획	개발/전력화	소 관
보안대책 평가	보안대책 검토	보안측정	국방부 (안보사)
상호운용성 평가(정보보호)	소요평가	시험평가	합참(통신사/사이버사)

표 4와 같이 체계별 상호운용성 평가시 정보보호 항목에 대해 수행하며, 안보지원사에서는 별도로 보안대책과 보안측정을 수행한다. 안보지원사에서 선 수행한 항목에 대한 평가결과를 상호운용성 평가시에는 그대로 적용하고 있다. 또한 2019년부터 상호운용성 측면에서 정보보호 평가항목에 사이버전 대비능력 항목를 추가하여 사이버작전사에서 평가수행하며 결과를 상호운용성 위원회에서 검증하고 있으나, 미군의 DIACAP이나 RMF 개념을 적용하여 평가하지 않는 실정이다.

2.3 위험관리 프레임워크(RMF) 평가

미군은 정보보호에서 정보보증, 사이버보안 개념의 발전과 더불어 평가체계도 함께 발전시켰다. 정보보호 관점의 평가는 1997~2007년까지 DITSCAP(Defense Information Security Certification and Accrediation Process)으로, 정보보증 관점의 평가는 2007~2014년까지 DIACAP로, 사이버보안 관점의 평가는 2014년부터 현재까지 RMF로 수행되었으며 대체 되었다[14].

DIACAP과 RMF의 차이를 살펴보면, 과정을 명확히 하기 위해 DIACAP의 인증 및 승인(인가)을 RMF는 평가 및 승인으로 변경하였고, RMF는 3년 인증 및 승인 주기를 없애고 지속적인 모니터링과 권한 부여로 대체하며, 일단 ATO(Authorization to Operation)가 수여되면 전체적인 보안 태세를 유지하기 위해 보안조치를 지속적으로 평가해야 한다는 개

념으로 변경하였다. 임시운영권한(IATO: Interim Authority to Operate)이 제거 되었고, RMF는 IATO를 조건이 있는 ATO로 대체하였으며, 또한 DIACAP 임무보증 범주(MAC: Mission Assurance Category) 레벨 Ⅰ, Ⅱ, Ⅲ을 충격수준 낮음, 보통, 높음으로 대체하였다. RMF 시스템 분류는 MAC 대신 영향수준으로

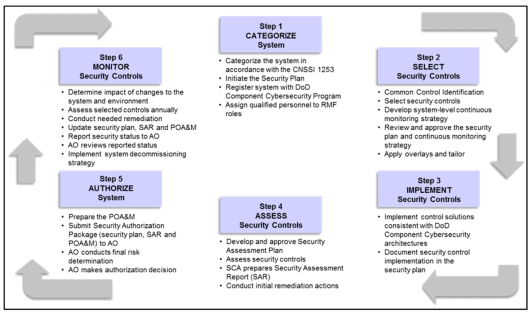

그림 2. RMF 프로세스 단계(출처 DoDI 8510.01)
Fig. 2. Steps in RMF Process

표 5. 보안 통제항목 식별자 및 패밀리 명칭
Table 5. Security control identifiers and family names

식별자	패밀리
AC	Acess Control(접근통제)
AT	Awareness and Training(의식제고와 훈련)
AU	Audit and Accountability(감사 및 책임성)
CA	Security Assessment Authorization (보안 평가 및 인가)
CM	Configuration Management(구성 관리)
CP	Contingency Planning(비상계획 수립)
IA	Identification and Authentication (식별 및 인가)
IR	Incident Response(보안사고 대응)
MA	MAintenance(유지보수)
MP	Media Protection(매체보호)
PE	Physical and Environmental Protection(물리적 환경적 보호)
PL	Planning(계획수립)
PS	Personnel Security(인적보안)
RA	Risk Assessment(리스크 평가)
SA	System and Services Acquisition (시스템 및 서비스 획득)
SC	System and Communications Protection(시스템 및 통신보호)
SI	System and Information Integrity (시스템 및 정보 무결성)
PM	Program Management(사업관리)

지정하였고, 또한 RMF는 DIACAP 분류수준을 보안목표인 기밀성, 민감성 및 가용성으로 대체하였다[15].

RMF 프로세스는 그림 2와 같이 6단계로 구성되어 있다. 6단계중 2단계는 분류된 보안등급에 따라 체계상 구현이 필요한 보안항목을 선정하는 단계로 NIST SP 800-53에 나온 표 5와 같은 보안통제항목 식별자를 기준으로 선정하게 된다. 여기서 보안통제항목 식별자를 살펴보면 상호운용성 정보보호 평가항목과 유사하거나 중복된 항목들이 있으므로 이에 대한 연관성 검토가 필요하다.

또한, 2019년 CCIB에서 미군은 한·미 연동체계에 대한 RMF 적용 필요성을 제기하였고, 그에 따라 국방부는 우리군 특성에 맞는 한국형 사이버보안제도(K-RMF)를 개발하였으나, 미측의 요구사항인 한·미 연동체계에 대한 RMF 적용을 위해서는 우리군의 체계 획득단계별 평가항목 재선정이 필요하고 신규 무기체계 뿐만 아니라 기존 무기체계에 대해서도 평가결과를 반영한 후속조치계획 등 산출물 작성 및 지속적인 관리가 필요하다.

Ⅲ. 정보보증의 상호운용성 확보방안

3.1 상호운용성 정보보증 개념 훈령 반영

국방정보화업무훈령상 상호운용성 평가항목에 정보보호가 있고, 국방상호운용성관리지시에도 정보보호 항목이 있다. 사이버위협을 대비한 사이버위협 대응능력과 SW취약점 제거 항목을 추가로 평가하고 있으나 정보보증에 대한 개념은 미흡하다. 미국은 정보보증을 사이버보안으로 대체하여 평가하고 있으나, 우리군의 정보보증에 대한 개념을 고려할 때 사이버보안 개념을 바로 적용하기에는 제한사항이 많을 것으로 본다. 그리고 일반적인 정보보증과 사이버보안 개념에서 볼 때 정보보증이 더 큰 개념으로 보는 경향이 있으므로 정보보증 개념을 먼저 적용하고 사이버보안 개념을 적용할지 추후 검토하는 것을 제안한다. 아울러 K-RMF 평가항목을 고려한 정보보증 평가항목 등을 선정하고 훈령 및 규정 반영이 필요하다.

3.2 상호운용성 정보보호 평가항목 조정

K-RMF를 전군으로 확대 적용하는 단계에 이르고 있는 현 시점에 상호운용성 정보보호 평가항목과의 유사성을 분석한 결과 평가항목 대부분이 표 6과 같이 K-RMF 평가항목에 포함되어 있다[16]. 따라서 K-RMF에서 평가하고 상호운용성 측면에서도 중복평가하는 사례가 발생하게 되므로 이들 평가항목에

표 6. 상호운용성 정보보호와 K-RMF 항목 매핑
Table 6. Interoperability information security and K-RMF mapping

평가항목		통제항목 식별
정보보호 수준		기밀성, 무결성, 가용성 기준
네트워크 정보보호		AC-2, IA-1,2, SC-8, PA-3
관제체계 구축		SC-8
키 관리체계 구축		IA
응용체계 정보보호		IA-1,4, AC-10, CP-8
서버 정보보호		SI-2,3, SC-10, AU, CP-8
단말기 정보보호		SI-2,3, MP, AC-19
암호장비 적용		CR
사이버 위협 대응 능력	신분위장 위협	AC-15, IA-1,4,8
	데이터 변조 위협	SC-9,10, CP-9
	공격행위 부인 위협	SC-9, AU-11
	정보유출 위협	MP, IA-2, SC-8,9,10, SI-13
	서비스거부(DoS) 위협	SC-6
	권한상승 위협	AC-6,14, IA-3,4
SW 취약점 제거	시큐어코딩 규칙적용	SA-3, SI-6
	오픈소스 취약점 제거	SI-6, CM-9,10

대한 중복성과 상호운용성 영향성을 살펴보았다.

상호운용성 정보보호 평가항목 중 상호운용성 측면에서 영향성이 크고 적은 항목에 대한 구분이 필요하며, 항목별로 K-RMF에서 중복평가 유무를 확인하고 평가결과를 확인하거나 재검증할 필요가 있다. 키 관리체계 구축, 응용체계 정보보호, 서버 정보보호, 단말기 정보보호, 신분위장 위협 대응능력, 정보유출 위협 대응능력, SW 취약점 제거, 시큐어코딩 적용 적절성, 오픈소스 취약점 제거 적절성 등은 K-RMF 평가항목에 포함되어 있고 상호운용성에 직접적인 연관성이 부족하므로 상호운용성 평가에서는 결과를 확인하는 수준으로 하고, 기타 항목들은 운용, 장애발생 복구, 성능보완 등 필요시 체계간의 상호운용성에 밀접한 연관성을 가지므로 K-RMF 평가항목에 포함되어 있어도 상호운용성 측면에서 재검증이 필요하겠다.

3.3 K-RMF 평가항목 상호운용성 평가시 재검증

상호운용성 평가에서는 정보보호 수준의 적절성을 평가하게 되어 있으나, K-RMF 평가시의 기밀성, 무결성, 가용성 등 보안등급을 시스템별로 소요제기 부서에서 제시된 수준을 같이 검증할 필요가 있다. 시스템상의 정보를 효과적으로 관리하기 위해 상호운용성 정보보호 수준과 보안등급 분류의 적절성을 확인하여야 한다.

아울러 보안통제항목 식별자 18개 중 상호운용성 측면에서 재검증이 필요한 항목에 대해서 분석한 결과 접근통제(AC), 형상관리(CM), 보안계획 및 평가(PA), 시스템 및 통신보호(SC), 시스템 및 정보 무결성(SI)에서 항목들을 도출하였다. 각 항목에 대한 설명은 [16]을 참조하였다.

접근통제는 정보에 대한 획득 및 사용, 특정시설에 대한 출입 등 요청을 처리하기 위한 통제 절차이다. 시스템에 기반한 접근통제는 논리적 접근통제로 해당 시스템 자원에 접근이 가능한 사용자(프로세스 포함) 및 접근 유형에 대해 규정한다. 계정관리, 직무분리, 최소권한, 세션잠금, 정보흐름통제 및 세션 종료 등이 있다. 접근통제에서 상호운용성 측면의 재검증이 필요한 항목으로 정보흐름통제를 검토하였다. 정보흐름통제는 정보가 시스템 내·외부에서 이동할 수 있는 위치를 통제한다. 정보가 외부로 전송되는 경우 외부 시스템이 서로 다른 보안정책을 적용할 수 있고, 시스템의 보안 수준이 상이할 수 있기 때문에 하나 이상의 보안 영역에서의 보안정책을 위반할 수 있다. 이러한 상황에서 정보 소유자는 시스템간의 정보흐름을 위한 지침을 제공해야 한다. 정보흐름통제를 제외한 계정관리, 직무분리 등의 항목들은 RMF 평가결과를 상호운용성 측면에서 확인만 하더라도 문제가 발생하지 않을 것이다. 그러나 정보흐름통제는 내·외부 체계간의 서로 다른 보안정책을 적용했을 경우 상호운용성의 문제가 발생한다. 따라서 RMF 평가결과를 토대로 상호운용성 측면에서 체계간 동일한 보안정책 여부와 상이할 경우의 해결방안이 적용되었는지를 재검증해야 한다.

형상관리는 획득수명주기 전 기간동안 시스템 및 구성요소들의 무결성을 유지하기 위해 최초 기준선을 설정하여 변경사항을 추적하고 관리하는 활동이다. 형상관리는 시스템에 적합한 형상을 설정하고 문서화함으로써 변경사항을 추적할 수 있고, 보안 영향성 분석을 통해 한 구성요소의 변경사항이 전체 시스템에 미치는 영향 등을 평가하여 관리할 수 있다. 형상관리 기준선, 형상변경 통제, 보안 영향 분석, 형상변경 접근제한, 형상 설정, 기능 최소화 등이 있다.

접근통제와 달리 형상관리는 형상관리 기준선 등 모든 항목들에 대한 RMF 평가결과를 상호운용성 측면에서 재검증이 필요하다. 형상관리 기준선은 현재

시점에서 승인 및 배포된 시스템, 소프트웨어, 시스템 구성요소, 네트워크 토폴로지 등의 형상을 포함한다. 기준선을 정하지 않았을 경우 체계 장애 발생시 복구할 시점이 상이하다면 상호운용성에 문제가 발생하게 된다. 형상변경통제는 형상변경시의 절차를 규정하여 임의적 시스템 변경을 방지하는 것으로, 운용자가 필요에 따라 임의로 수행하게 된다면 장애 발생 가능성 미검증 및 체계간 상이한 시스템 운영으로 상호운용성에 문제가 발생하게 된다. 형상설정, 형상관리계획, 보안영향성 분석, 형상변경제한, 기능 최소화, 시스템 구성요소 목록 등은 형상을 지속적으로 추적 및 관리하기 위한 것으로, 상호운용성 측면에서 형상의 변경과 변경될 수 있는 범위를 재확인해야 한다. 소프트웨어 사용제한 및 사용자 설치 소프트웨어는 저작권법에 따라 불법 소프트웨어 사용을 방지하고, 소프트웨어 설치전 인가 절차 및 설치후 점검절차를 수립하는 것으로, 불법/비인가 소프트웨어나 검증되지 않은 업데이트나 패치 등에 의한 체계 장애가 발생하지 않도록 재확인이 필요하다.

보안계획 및 평가(PA)는 사이버보안 제도를 확립하고 각 시스템에 대한 사이버보안 계획, 평가 활동을 체계적으로 수행하여 사이버보안 위험을 관리하기 위한 활동이다. 항목 중 시스템 연동은 서로 다른 시스템간의 연결시 보안 요구사항 및 통제사항이 다를 수 있기 때문에 사전 협의(연동합의서) 후 연결하여 보안 문제가 발생하지 않도록 만들기 위한 것으로, 평문 및 비밀 국방시스템과 연결, 공공 네트워크와 연결, 인가범위 외 시스템 연결 등을 평가하는데 상호운용성 측면에서도 승인된 시스템인지 여부와 연동시 문제 유무를 재검증해야 한다. 보안 아키텍처는 엔터프라이즈 아기텍처와 일관성을 가지고 일부로써 통합되어 개발되어야 한다. 심층방어는 적들이 시스템 공격을 달성하기 위해 여러 가지 보호조치를 극복하도록 하는 것이며, 공급업체 다양성은 개별 기술, 제품의 단점을 보완할 수 있도록 설계하는 것으로, 상호운용성의 아키텍처와 일관성 및 이들 적용으로 인한 문제 유무를 재검증해야 한다.

시스템 및 통신보호(SC)는 시스템 및 통신에 대한 저장, 처리, 전송되는 정보의 기밀성과 무결성을 보호하기 위한 물리적 또는 논리적 수단인 보호조치들로 구성된다. 이중 전송정보의 기밀성 및 무결성을 보호하기 위한 물리적인 방법과 논리적인 방법 등을 적용하였을 경우 시스템 또는 시스템간 연동제한 및 성능저하 등의 상호운용성 문제 유무를 재검증 해야 한다.

따라서 국방정보화업무훈령 및 국방상호운용성관리지시에 정보보호를 정보보증 평가로 수정하며, 표 7와 같이 기존 상호운용성 평가항목 중 키 관리체계 구축 등 9개를 제외하고 K-RMF 평가항목 중 형상관리의 적절성 등 4개를 재검증 평가항목으로 추가하는 방안을 제시한다.

표 7. 개선된 상호운용성 정보보증 평가항목
Table 7. Improved interoperability information assurance evaluation items

구분	평가항목
정보보호 수준	정보보호 수준의 적절성
네트워크 정보보호	네트워크 정보보호 대책 수립/구현의 적절성
관제체계 구축	관제체계 구축방안 수립/구현의 적절성
암호장비 적용	암호장비 적용계획/적용의 적절성
사이버위협 대응 능력	데이터 변조 위협 대응능력
	공격행위 부인 위협 대응능력
	서비스거부(DoS) 위협 대응능력
	권한상승 위협 대응능력
K-RMF 평가 재검증	가용성, 기밀성, 무결성 수준 적절성
	정보흐름통제의 적절성
	형상관리의 적절성
	시스템 연동 및 보안 아키텍처
	전송정보의 기밀성 및 무결성

Ⅳ. 결 론

본 논문에서는 상호운용성 측면의 정보보호 평가개념을 정보보증 평가개념으로 대체하였고, K-RMF 평가결과를 반영한 상호운용성 확보방안을 제안하였다. 정보보증 및 사이버보안에 대한 개념 연구를 통해 우리군의 현 실정에 맞게 국방정보화업무훈령 및 국방상호운용성관리지시, 합참 상호운용성관리규정에 정보보증 개념을 선 적용할 것과, 기존 상호운용성 정보보호 평가항목에 대한 분석결과 K-RMF와 중복 평가하는 항목을 제외하였고, K-RMF 평가항목 중 상호운용성 측면에서 재검증이 필요한 항목을 식별하여 제시하였다.

향후 K-RMF 평가항목들에 대한 상호운용성 측면의 재검증 필요항목에 대한 획득단계별 적용시기 추가 연구가 필요하나, 중복평가 수행에 따른 불필요한 시간과 예산낭비 해소가 가능하고 명확한 책임소재 식별 등 평가 및 운용 업무에 큰 역할을 할 것으로 기대된다.

References

[1] DoD Instruction 8510.01, *Risk Management Framework(RMF) for DoD Information Technology*(IT), Incorporating Change 3, Dec. 29, 2020.

[2] J.-W. Kang, H.-J. Choi, and H. Lee, "Semantic analysis of information assurance concept : A literature review," *Convergence security J.*, vol. 19, no. 1, pp. 31-40, 2019.

[3] *PC Magazine, information assurance*, Jan. 28, 2020, from https://www.pcmag.com/encyclopedia/term/information-assurance

[4] Y. Cherdantseva and J. Hilton, "Understanding Information Assurance and Security," *J. Organ. End User Comput.*, vol. 16, no. 3, Oct. 2015.

[5] NIST Special Publication 800-53, Rev. 4, "*Security and Privacy Control for Federal Information Systems and Organizations*," Apr. 2013.

[6] DoD, *Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*, Ver. 1.0, Office of The Under Secretary of Defense for Acquisition, Technology, and Logistics, Sep. 2015.

[7] DoD Instruction 8500.01, *Cybersecurity*, Mar. 14, 2014, Incorporating Change 1, Effective Oct. 7, 2019.

[8] Opentext Security & Protection Cloud Team, *Top 5 difference between information assurance vs. cybersecurity*(Jun. 7, 2021), Jan. 28, 2022, from https://blogs.opentext.com/information-assurance-vs-cybersecurity/

[9] Cyber Security Kings, *10 Differences for Cyber Security Vs Information Assurance?*, Jan. 28, 2022, from https://cybersecuritykings.com/2020/04/22/10-differences-between-cyber-security-and-information-assurance/

[10] HITRUST, *Healthcare's Model Approach to Critical Infrastructure Cybersecurity*(Jun. 2014, pp. 5), Jan. 28, 2022, from https://hitrustalliance.net/documents/csf_rmf_related/ImplementingNISTCybersecurityWhitepaper.pdf

[11] MNDI 2576, "*Defense Information Service Instruction*," Aug. 12, 2021.

[12] KJITC, "*Interoperability theory and practice,*" pp. 22-23, Jan. 2016.

[13] Order from the Ministry of National Defense 2020-003, "*Defense Interoperability Management Order*," Jan. 6, 2020.

[14] K. Lee, J. Lee, and H. Lee, "Development plan for information assurance evaluation in preparation for cyber warfare," *Defense Acquisition Develop. Conf. 2018*, Sep. 2018.

[15] Phoenix TS, *Transitioning from DIACAP to RMF*(Aug. 5, 2013), Jan. 28, 2022, from, https://phoenixts.com/blog/diacap-vs-rmf/

[16] K-RMF TF, "*K-RMF Security Control List(Final Draft)*," Dec. 14, 2020.

박 종 출 (Jong-Chool Park)

1989년 2월 : 공군사관학교 전자 공학과 졸업
1996년 2월 : 고려대학교 전자공학과 석사
2018년 3월~현재 : 광운대학교 방위사업학과 박사과정

<관심분야> Network, ICT융합, 상호운용성, 정보보호
[ORCID:0000-0002-6903-7237]

최 용 훈 (Yong-Hoon Choi)

1995년 2월 : 연세대학교 전자공학과 공학사
1997년 2월 : 연세대학교 전자공학과 공학석사
2001년 2월 : 연세대학교 전기전자공학과 공학박사
2001년 4월~2002년 3월: (미) 매릴랜드 주립대 Research Associate
2002년 6월~2005년 8월 : LG전자 책임연구원
2005년 9월~현재 : 광운대학교 로봇학부 교수
<관심분야> 통신 네트워크, 머신 러닝
[ORCID:0000-0002-1460-0520]