J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

국방 사이버보안을 위한 RMF-CMMC 공통규정준수 메타모델 개발방안 연구☆

A Research on RC3(RMF-CMMC Common Compliance) meta-model development in preparation for Defense Cybersecurity

황 재 윤[1] 권 혁 진[2*]
Jae-yoon Hwang Hyuk-jin Kwon

요 약

사이버보안 정책을 선도하는 미 국방부의 사이버보안 제도는 크게 2가지 방식으로 대외 군납업체 보안인증을 위한 CMMC와 내부기관대상 보안평가를 위한 RMF가 있다. 우리 군의 경우, 2026년부터 한국형 RMF(K-RMF)를 적용할 예정이다. 더불어 미 국방부가 발주하는 사업에 참여하는 국내 방산업체들은 2025년 10월전까지 CMMC인증을 사전 취득해야 하는 입장에 있다. 본 논문에서는 CMMC와 RMF 보안감사 준비업무를 동시에 지원할 수 있는 새로운 표준 컴플라이언스 메타모델(R3C) 개발방법론과 R3C메타모델을 기초로 한 컴플라이언스 솔루션 구현 결과물에 대해 소개하고 있다. 본 연구는 2022년 이후 국방부 합동참모본부 주관 한/미 국방 사이버보안 업무지원 자동화 솔루션 개발프로젝트를 수행하면서 얻은 미 국방 사이버보안 제도에 대한 실무 노하우를 토대로 진행되었다. 개발된 컴플라이언스 솔루션기능은 한/미 연합모의훈련 실무에 활용되고 있다. 본 연구를 통해 개발된 컴플라이언스 솔루션은 민간에도 제공할 예정이며, CMMC인증을 취득해야 하는 국내 방산업체에게 매우 유용하리라 예상한다.

☞ 주제어 : 사이버 보안감사, 컴플라이언스, 위험관리 프레임워크, 사이버 보안 성숙도 모델 인증

ABSTRACT

The U.S. Department of Defense, leading global cybersecurity policies, has two main cybersecurity frameworks: the Cybersecurity Maturity Model Certification (CMMC) for external defense industry certification, and the Risk Management Framework (RMF) for internal organizational security assessments. For Republic of Korea military, starting from 2026, the Korean version of RMF (K-RMF) will be fully implemented. Domestic defense industry companies participating in projects commissioned by the U.S. Department of Defense must obtain CMMC certification by October 2025. In this paper, a new standard compliance meta-model (R3C) development methodology that can simultaneously support CMMC and RMF security audit readiness tasks is introduced, along with the implementation results of a compliance solution based on the R3C meta-model. This research is based on practical experience with the U.S. Department of Defense's cybersecurity regulations gained during the joint project by the South Korean and U.S. defense ministries' joint chiefs of staff since 2022. The developed compliance solution functions are being utilized in joint South Korean-U.S. military exercises. The compliance solution developed through this research is expected to be available for sale in the private sector and is anticipated to be highly valuable for domestic defense industry companies that need immediate CMMC certification.

☞ keyword : Cybersecurity Audit, Compliance, RMF, CMMC

1. 서 론

전 세계 사이버보안 정책을 선도하는 미국 국방부(DoD)의 사이버보안(Cybersecurity)제도는 크게 2 가지 방식으로 이원화되어 있다. 사이버보안성숙도 인증모델 CMMC(미국 방부가 개발한 대외 기관용 사이버보안 인증 제도)와 내부기관용 사이버보안 평가/승인 제도인 위험 관리 프레임워크 RMF(Risk Management Framework)가 그것이다[2].

미 연방조달규정(FAR)에 의거 2025년 10월부터 미국

1 eVolcano Inc, Seoul, 05836, Korea.
2 Department of Protection and Safety, Seoul National University of Science and Technology, Seoul, 01811, Korea.
* Corresponding author (kwonhj@seoultech.ac.kr)
[Received 4 October 2023, Reviewed 24 October 2023(R2 15 November 2023), Accepted 4 December 2023]
☆ This study was supported by the Research Program funded by the SeoulTech(Seoul National University of Science and Technology)

국방부가 발주하는 사업에 참여하는 모든 방산업체들은 CMMC인증을 사전 취득해야 하며[3], Five Eyes(미국 외 영국·캐나다·호주·뉴질랜드)등 미국의 주요 동맹국들은 이미 자국 내 고유 CMMC인증제도를 마련하고 이를 미국과 등가대우(reciprocity)하기 위한 협정 체결을 논의중에 있다[4].

RMF의 경우, 우리나라도 F-35전투기 구매 이후 미 RMF에 근거해 한국군이 미 사업관리기관의 직접적인 감독과 통제를 받고 있는 상황인데, 우리나라의 사이버보안 감사제도가 미 국방부의 사이버보안관리 요구수준을 충족시키지 못하고 있기 때문이다[5]. 이에 우리군도 국군방첩사령부 주도로 2019년부터 한국형 K-RMF 개발에 착수, 2026년 적용을 목표로 추진중이다[6].

이제 국내 방산업체들도 CMMC와 RMF라는 생소한 국방 사이버보안감사제도에 미리 대비하지 않는다면 2025년부터는 방산무기 해외수출이 2026년부터는 국내 판매(군납)조차도 제한되는 최악의 상황에 직면할 수 있다. 특히, 한국형 K-RMF 라는 대체 제도가 준비되고 있는 국내 판매(군납)시장과 달리 방산수출용인 CMMC는 미 국방부가 정한 매우 엄격한 사이버보안관리 요구수준을 충족시켜야 한다는 점에서 가히 '새로운 방산무기 수출 장벽'이 될 수도 있다.

2019년 개발에 착수한 한국형 K-RMF는 최초 2025년 전면 적용에서 1년 연장되어 2026년 전면 적용으로 7년이란 오랜 준비기간이 소요되고 있다. 한국형 CMMC 제도가 만들어지고 미 국방부로부터 등가대우(reciprocity)를 위한 협정(MRA, Mutual Recognition Arrangement)이 체결될 때까지 많은 시간이 소요될 것으로 예상된다. 더욱이 미 국방부가 주도하는 CMMC는 최초 2026년 시행에서 2025년 10월 시행으로 앞당겨졌다. 만약 방산업체가 미국과 미동맹국에 방산무기 수출을 준비한다고 하면, 미국과의 MRA체결을 기다리기 보다는 CMMC인증 취득을 위한 준비에 본격적으로 착수해야 한다.

특히, 방산업체들은 전통적으로 "해외방산업체에 대한 미국의 수출 통제 준수 및 보안 요구 사항은 미국 내 방산업체에 부과된 기준보다 훨씬 높은 수준을 요구해 왔다."는 사실에 유념해야 한다[8]. CMMC인증과 상당부분 상호 호환되는 ISO 27001국제 인증 선임심사원으로 활동해온 경험에서 보면 미 국방부가 주도하는 CMMC인증에 필요한 준비기간에 6개월이 소요될지, 1년 이상 소요될지 정말 예측하기가 어렵다.

CMMC와 RMF 모두 새로운 국방 사이버보안감사에 대비한 준비과정에 있어 가장 큰 애로사항 중 하나가 "연중 사이버 보안통제 업무를 지속적으로 수행하였는지 여부에 대한 연속성과 추적성을 입증해야 한다."는 점이다. 이를 위해 상용 지원도구(컴플라이언스 솔루션) 활용은 필수적이다.

본 논문은 2022년 이후 미 RMF를 토대로 국방부 합동참모본부 주관 한/미 연합연습 모의지원 사이버보안 자동화 솔루션 개발프로젝트를 수행하며 얻은 미 국방 사이버보안감사제도 준비에 대한 노하우를 토대로 하였다. CMMC와 RMF 보안감사 준비업무를 동시에 지원할 수 있는 상용도구(컴플라이언스 솔루션)의 공통 규정준수 메타모델 개발과정에 대해 기술하였다.

CMMC와 RMF를 동시에 지원할 수 있는 공통 규정준수 메타모델을 개발해야 하는 가장 큰 이유는 국내 방산업체 입장에서 향후 미래에 발생하게 될 국방 사이버보안감사 준비과정의 불필요한 중복업무 발생을 최소화하기 위함이다. 구체적으로 향후 국내 방산업체는 신형무기체계에 대한 시제품개발(선행연구)시 RMF(또는 K-RMF)에 근거해 사이버보안 평가/승인을 준비해야 하고, 양산단계 해외수출 시에는 또 다시 CMMC기준에 맞춰 인증심사를 준비해야 하기 때문이다.

다행히 CMMC의 보안심사항목(Security Requirements)은 ISO 27001과 RMF의 보안통제항목으로부터 도출되었다. 이에 가장 보안요구수준이 낮은 ISO 27001메타모델을 개발한 선행연구사례를 토대로 CMMC와 RMF를 공통지원할 수 있는 공통 메타모델을 새롭게 개발하였다.

2. 관련연구

국방 분야에서의 사이버보안은 단순한 정보 보호를 넘어서, 사이버작전(Cyber Operations)이라는 독립된 작전영역으로 존재한다. 따라서 국방 사이버보안과 관련된 연구는 민간 분야의 사이버보안 연구보다 훨씬 다양하고 광범위하다. 이에 본 논문에서 관련연구는 국방 사이버보안 규정준수(Cybersecurity Compliance)라는 단일 주제영역으로 국한하였으며, 군 내 국방 사이버보안 규정준수를 위한 제도인 RMF와 군 외 제도인 CMMC에 대해 평가방법론적 측면에서 우선 조사, 분석하였다.

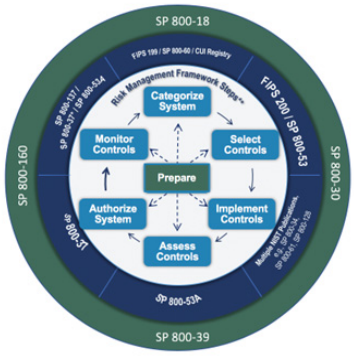
그 다음으로 본 논문의 연구 주제인 국방 사이버보안 규정준수를 돕는 효율적인 상용 지원도구(컴플라이언스 솔루션)개발을 위한 기반 토대인 '사이버보안 메타모델' 선행연구사례를 조사, 분석하였다. CMMC와 RMF 모두 새로운 사이버보안 평가제도로 표준 메타모델연구 사례가 존재하지 않으며, 이에 CMMC 및 RMF와 호완성이 좋

은 국제 표준 사이버보안 표준모델인 ISO 27001관련 메타모델 선행 연구사례를 조사, 분석하였다.

2.1 RMF에 대하여

미국 국방부는 방호(protection)적인 측면에서 기존의 물리적 수단에 의한 공격보다 사이버 공격이 국가 안보에 더 치명적일 수 있기 때문에, 보다 더 주목하기 시작하였다[9]. 이에 최초 소요기획단계에서 폐기단계에 이르기까지 총 수명주기 관리 관점에 사이버보안인증제도(DIACAP, DoD Information Assurance Certification and Accreditation Process)를 마련하였다. 2016월부터 DIACAP를 대체하는 군 내부기관용 사이버보안 평가/승인제도가 바로 RMF이다[10].

RMF는 현재 NIST표준으로 채택(자세한 내용은 NIST SP 800-37을 참조할 것)되었으며, 총 수명주기 관리 관점의 RMF 프로세스 7단계 수행절차는 아래 그림 1과 같다[11].



(그림 1) RMF 7단계 프로세스
(Figure 1) RMF 7 Steps

RMF의 1단계는 평가준비(Prepare)단계이며, RMF의 2단계 시스템 분류(Categorize System)는 예상되는 위협이나 취약성 수준에 따라 자산을 분류하는 단계이다. 3단계는 보안통제기준을 설정(Select Security Controls)하고, 4단계는 보안 통제를 구현(Implement Security Controls)한다. 5단계는 보안통제가 제대로 이루어지고 있는지를 평가(Assess Security Controls)하고, 6단계 시스템 인가(Authorize System)는 위험평가에 기초하여 새로 개발하거나 성능 개선된 시스템 운영을 승인한다. 마지막 7단계 보안통제 감시(Monitor Security Controls)는 지속적인 모니터링을 통해 위험평가를 업데이트하는 단계이다.

2.2 CMMC에 대하여

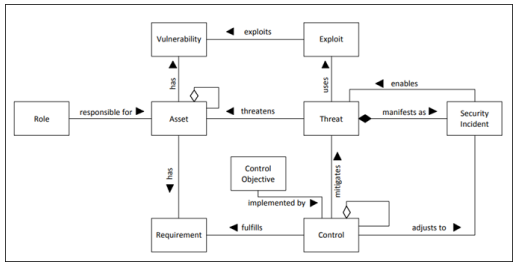
CMMC란 군납 민간업체의 사이버보안 품질관리 수준을 인증심사하는 제도이다. 군납 민간업체 중 단순 연방계약정보(FCI, Federal Contract Information)만 취급하는 경우는 CMMC 레벨1(자체심사) 인증 취득을 요구한다. 대외비 이상 비밀을 취급하는 방산업체들은 미 대통령 행정명령 13526에 의거하여 CMMC LEVEL 1, LEVEL 2 인증을 모두 취득해야 한다.

(그림 2) CMMC 인증심사제도
(Figure 2) CMMC Certification Audit System

상기 그림 2와 같이 [LEVEL 1] 자격취득을 원하는 업체는 연방조달규정(FAR) 조항 52.204-21에 명시된 기본적인 보호 요구사항 17개 항목을 충족(자체평가)시켜야 한다. [LEVEL 2] 자격취득을 원한다면 NIST SP 800-171에 명시된 110개의 보안요구사항을 충족(CYBER AB주관 인증심사에 통과)해야 하며, [LEVEL 3] 자격취득 기준은 아직 공식, 발표되지 않았다[12].

2.3 사이버보안 메타모델

사이버보안 실무에 있어 ISO 27001과 같은 정형화된 표준모델 외에 많은 비공식 모델들이 존재한다. ISO 27001과 같은 표준모델을 그대로 적용하기 보다는 조직의 특성 또는 보안 컨설팅 회사의 경험적 노하우를 반영한 비 표준모델을 사용한다. 비 정형화된 보안모델을 사용할 경우 내부 문서화 작업 간소화 등 사이버보안 실무에 있어서는 편리하다. 그러나 사이버보안업무를 자동화하거나 여러 개의 보안감사 프레임워크를 준수해야 할 경우에는 장애물로 작용한다. 이에 오래전부터 재사용 가능한 보안지식의 상호운용성을 제공하는 보안 온톨로지(보안 메타모델)의 필요성이 인식되어 왔다[13].



(그림 3) ISO 27001 메타모델
(Figure 3) ISO 27001 Meta-model

위 그림 3은 UML언어를 사용하여 정형화된 표준보안 모델인 ISO 27001을 메타 모델화한 사례 중 하나로 UML 클래스 다이어그램형식을 적용, 사이버보안 메타모델을 정의하였다[14]. 그림 3에서 주요핵심 요소로써 통제목표(Control Objectives)클래스는 공식적으로 충족되어야 하는 목표 또는 조건으로 ISO 27001인증을 위한 ISO27002과 같은 보안통제 프레임워크(Security Control Framework)을 지칭한다. 또한 통제항목(Controls)클래스란 통제목표(보안통제 프레임워크)에서 충족되길 원하는 요구하는 기술적, 관리적 또는 물리적 보호수단을 지칭한다.

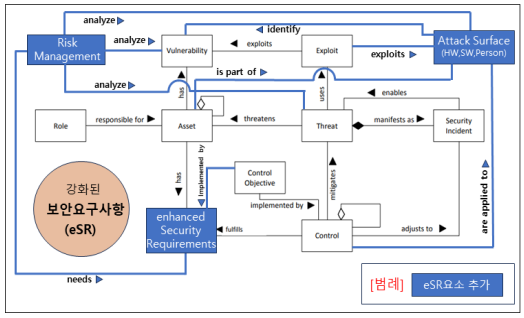
이와 관련하여, "Ontology-Based Evaluation of ISO 27001" 논문은 ISO 27001 보안 표준의 핵심 개념을 명시한 메타모델을 통해 정보보안 관리의 포괄성을 분석하고 있다. 이와 대비하여, 본 연구는 '컴플라이언스 메타모델 개발'에 중점을 두고 있으며, 이는 기존의 '사이버보안 메타모델' 연구와는 다른 차별적인 접근을 제시하며, 보안표준 및 규정 준수에 대한 새로운 시각을 탐구한다[15].

3. 컴플라이언스 메타모델 개발

앞서 관련 연구에서 소개했던 그림 3의 메타 모델은 근거 이론과 질적 데이터 분석(QDA, qualitative data analysis)방법을 기반으로 개발되었다[14]. 구체적으로 현장에서 경험적 데이터에 기반해 얻은 질적 데이터를 개념화하고, 개념적 라벨이 부여된 새로운 클래스에 대해 기존 클래스와의 관계를 식별함으로써 이론화하는 귀납적 방법으로 연구가 진행되며, 동일한 연구방법론을 본 논문의 연구에서도 채택하였다.

3.1 확장된 사이버보안 메타모델

다음 그림 4의 강화된 메타모델(enhanced Meta-Model)은 그림 3의 ISO 27001메타모델을 기본 토대로 RMF와 CMMC의 보안요구사항을 추가 지원할 수 있도록 강화된 사이버보안 메타모델로 본 연구 역시 근거 이론과 질적 데이터 분석방법에 기초해 메타 모델 확장을 진행하였다.



(그림 4) 강화된 메타모델
(Figure 4) Enhanced Meta-model

앞서 그림 3의 요구사항이란 클래스는 그림 4에서는 강화된 보안요구사항 eSR(enhanced Security Requirements)란 클래스명으로 새롭게 대체되었는데, eSR은 기존 ISO 27001의 요구사항 외에 CMMC와 RMF의 강화된 요구사항을 추가했음을 의미한다.

그림 4의 통제목표는 ISO 27001인증을 위한 ISO27002 외에 CMMC인증을 위한 NIST SP 800-171, RMF평가/승인을 위한 NIST SP 800-53의 보안통제 프레임워크를 추가로 지원한다.

그림 4에서는 공격표면(Attack Surface), 위험관리라는 새로운 클래스 2개를 더 추가하였는데, 공격표면이란 취약성이 발생할 수 있는 대상으로 하드웨어와 소프트웨어, 사람(페르소나)들을 지칭한다. RMF와 통합하여 운영되고 있는 미 국방부의 6단계 사이버보안 시험평가 과정중 2단계가 '사이버 공격표면 식별'이며, 3단계는 '협업을 통한 취약점 식별'이다[16].

미 국방부는 사이버 공간을 전쟁 영역으로 확대 인식하고 사이버 공격이 미래 전쟁의 일부가 될 것으로 예상하고 있다[17]. 이에 사이버 공간을 구성하는 물리계층(하드웨어), 논리계층(소프트웨어), 사회계층(페르소나)은 모두 위협의 대상이 될 수 있으며, 위험관리를 필요로 한다.

공격표면 및 취약점을 악용(exploit)한 위협발생 예방을 위한 위험관리의 핵심 중 하나로 식별된 위험에 우선순위

를 식별하는 위험평가 방법으로 아래 그림 5와 같이 CMMC와 RMF에서 공용으로 채택하고 있는 NIST SP800-30의 위험메트릭스기법이 대표적이다[18].

Overall Likelihood	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

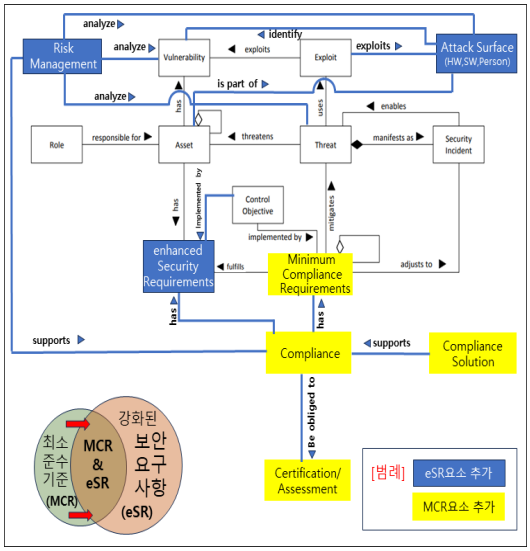
(그림 5) NIST SP800-30의 위험메트릭스
(Figure 5) Risk Matrix of NIST SP800-30

위험메트릭스기법을 현장 실무에 활용할 경우, 모호성 문제(주관적 판단을 최소화하고 보다 객관적인 위험우선순위 식별)와 중복성문제(식별된 서로 다른 위험요인이 동일한 위험우선순위가 부여)가 발생하며, 이를 해결하기 위해서는 전문적 경험 노하우가 필요하다.

필자는 위험메트릭스기법 적용 시 발생하는 모호성과 중복성 문제해결을 위해 시스템 공학분야에서 가장 널리 사용되어져 온 대표적인 위험관리 방법론인 FMEA(Failure Mode and Effect Analysis)와 인공지능 Fuzzy기술을 접목시킨 위험우선순위 식별 자동화방안을 연구, KIDA 국방정책연구논문에 구체적인 알고리즘을 공개하였다[19]. 또한 연구 결과물은 (주)이볼케이노의 상용도구(컴플라이언스 솔루션)내 CMMC와 RMF 위험관리 자동화 기능 중 하나로 구현되어 있다. 특히, 위험관리 자동화 기능은 CMMC인증심사를 위한 여러 평가항목들 중 증적자료 준비과정의 난이도가 높은 RA.L2-3.11.1(위험평가)와 RA.L2-3.12.1(보안통제 평가), RA.L2-3.12.3(보안통제 모니터링)을 위한 자동화된 증적자료 생성에 유용하게 활용될 수 있다.

3.2 RC3 컴플라이언스 메타모델

강화된 보안요구사항 요소가 추가된 그림 4에 RMF와 CMMC의 보안정책에 따라 근거해 규정준수 여부를 모니터링하고, 규정위반이 해결되었는지 확인하는 일련의 컴플라이언스업무 및 지원도구와 관련해 필요한 최소한의 메타데이터 요소(MCR, Minimum Compliance Requirements)를 새롭게 정의하고 추가하여 컴플라이언스 중심 메타모델 그림 6을 완성하였다.



(그림 6) RC3(RMF-CMMC Common Compliance) 메타모델
(Figure 6) RC3 (RMF-CMMC Common Compliance) Meta-model

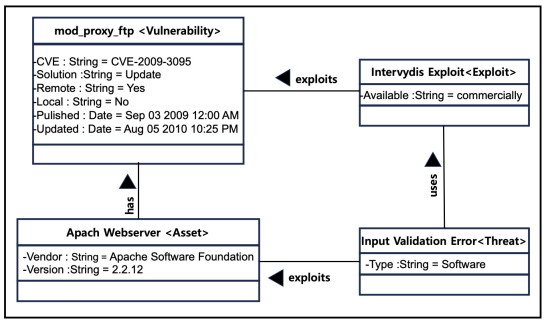
MCR요소들을 새롭게 추가 정의한 이유는 그림 3, 그림 4와 같은 사이버보안 메타모델과 차별화되는 그림 6의 컴플라이언스 메타모델의 특징을 정의하기 위해서이다. 사이버보안 메타모델과 달리 컴플라이언스 메타모델의 주요 목적은 CMMC와 RMF와 같은 보안감사 요구사항(eSR)을 충족시키기 위해 사전에 준비해야 하는 증적자료(MCR) 준비과정에 드는 시간과 노력을 최소화하는 것(MCR ⊆ eSR)에 있다.

그림 4의 통제항목 클래스는 MCR이란 클래스로 새롭게 대체되었는데, MCR클래스는 통제목표에 설정된 요구사항을 충족시키기 위한 최소한의 통제항목 이라고 정의한다. 컴플라이언스 클래스는 CMMC를 위한 인증 및 RMF를 위한 평가클래스를 공통 지원하며, 컴플라이언스 지원도구 클래스는 증적자료인 MCR을 준비과정에 드는 시간과 노력을 최소화하기 위한 방안(MCR ⊆ eSR)으로 컴플라이언스 업무 자동화관리 기능 및 자동화된 증적자료 생성기능을 제공한다.

3.3 RC3 구현

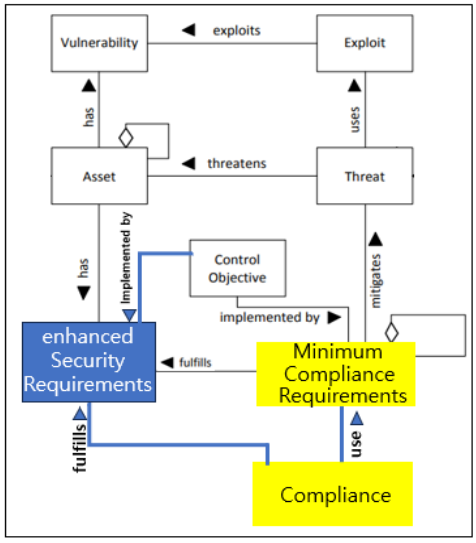
UML언어를 사용하여 정형화된 표준 메타모델은 MDA(Model Driven Architecture)개념에 기초해 자동화된 모델 변환 및 더 구체적인 수준의 모델로 변환할 수 있다

[14]. 구체적인 예로 그림 7은 그림 3의 ISO 27001기반 메타모델(UML클래스)의 4가지 핵심 개념을 인스턴스화 한 모습을 보여주고 있다.



(그림 7) 핵심개념의 인스턴스화
(Figure 7) Instantiation of Core Concepts

상기 그림 7의 사이버보안 메타모델은 Apache웹서버라는 자산(Asset)의 취약점 중 하나인 'CVE-2009-3095'는 입력 유효성 검사 오류를 이용한 사이버 위협에 악용될 수 있음을 보여준다.



(그림 8) RC3 핵심개념
(Figure 8) RC3 Core Concepts

그림 8은 사이버보안 메타모델 그림 7의 핵심 개념4가지(Vulnerability, Asset, Threat, Exploit)와 밀접한 관련이 있는 컴플라이언스 요소 3개만을 그림 6 RC3메타모델에서 발췌한 그림이다. 조직이 보유한 자산의 취약점 해소 측면에서 컴플라이언스 메타모델의 주요 목적은 CMMC와 RMF와 같은 보안감사 요구사항(eSR)을 충족시키기 위해 사전에 준비해야 하는 증적자료(MCR) 준비과정에 드는 시간과 노력을 최소화하는 것(MCR ⊆ eSR)에 있다. 다음은 보유한 자산의 취약점해소 측면에서 CMMC의 실제 보안감사 요구사항(eSR)인 SI.L1-3.14.1에 대해 'MCR ⊆ eSR'측면에서 RC3메타모델 구현방안에 대해 설명하겠다.

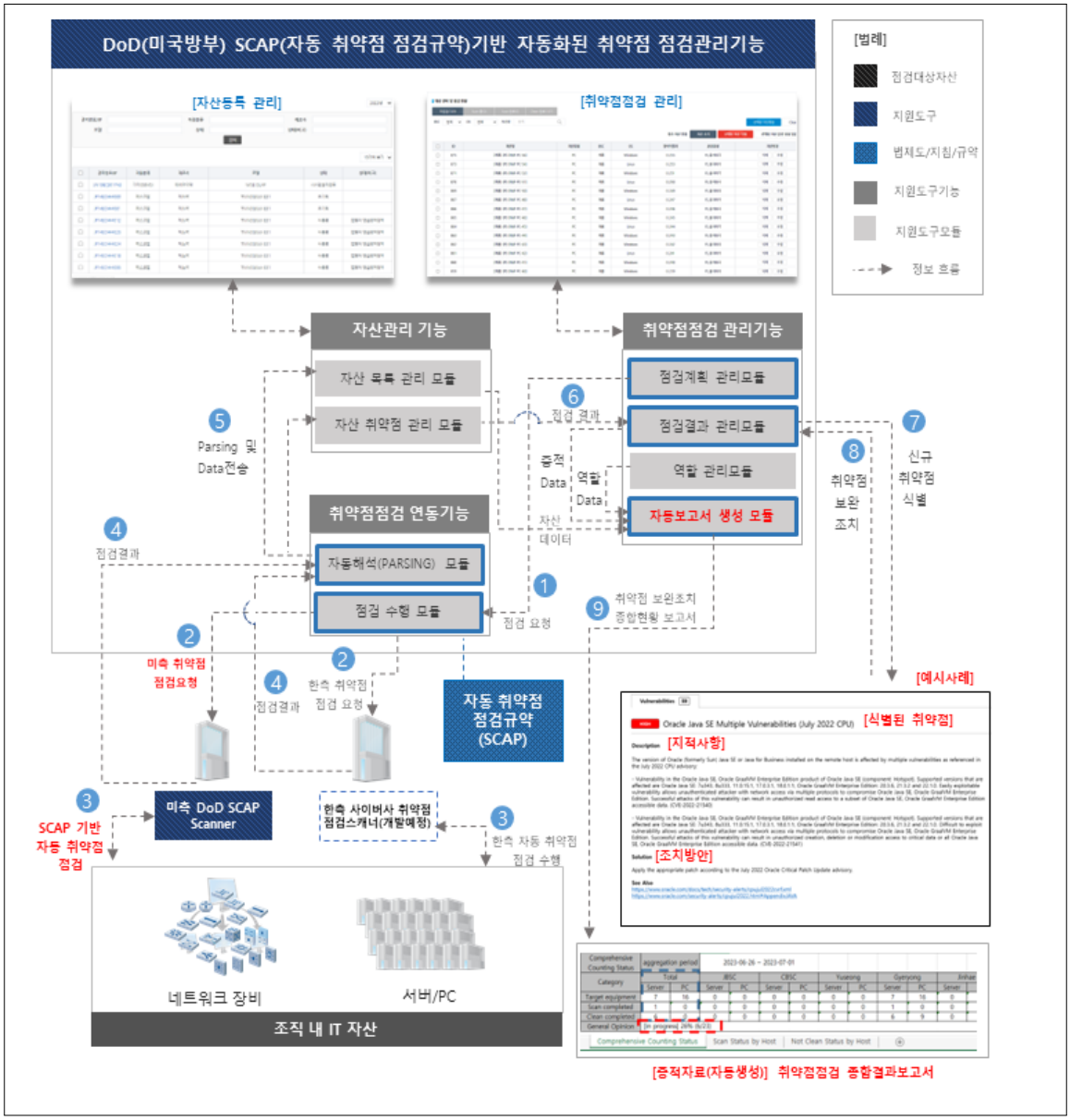
(레벨1) SI.L1-3.14.1 Flaw Remediation 결함시정

[평가항목]
Identify, report, and correct information and information system flaws in a timely manner. 정보 및 정보시스템 결함을 적시에 식별 및 보고하고 시정(보완)할 수 있는 체계를 갖추었는지를 입증(해야 합니다.)

[인증평가기준]
Flaw Remediation(결함 시정)에 대한 평가는 다음 6개 요구사항을 확인합니다.
[a] the *time* within which to identify system flaws is specified;시스템 결함(보안취약점)을 식별하는데 소요되는 시간
[b] system flaws are identified within the specified *time* frame; 결함이 지정된 시간프레임(마감시간) 내 식별되었는지 여부
[c] the *time* within which to report system flaws is specified; 식별된 시스템 결함을 보고하는데 소요되는 시간
[d] system flaws are reported within the specified *time* frame; 시스템 결함이 지정된 시간프레임(마감시간) 내 보고되었는지 여부
[e] the *time* within which to correct system flaws is specified; 시스템 결함을 보완조치하는 소요되는 시간
[f] system flaws are corrected within the specified *time* frame 시스템 결함이 지정된 시간프레임(마감시간) 내 보완되었는지 여부

(그림 9) CMMC의 실제 보안감사 요구사항 (eSR)
(Figure 9) Actual Security Audit Requirements of CMMC (eSR)

그림 9의 인증평가기준 6개 항목을 살펴보면 평가항목 6개 모두에서 적시성 측면이 강조되고 있음을 확인할 수 있다. 적시성을 충족시키기 위한 가장 효과적인 수단은 바로 취약점 해소의 '자동화' 이다. 그림 10는 미국방 사이버보안제도를 지원하는 컴플라이언스 솔루션 공급업체의 상용제품인 'SI.L1-3.14.1 결함 시정(Flaw Remediation)' 평가항목의 CMMC 인증심사지원을 위한 자동화된 취약



(그림 10) RC3메타모델에 기초한 자동화된 취약점 점검관리기능 구현

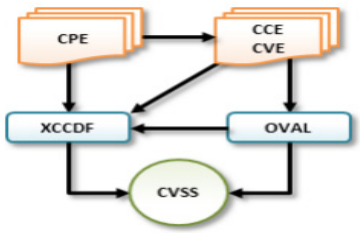
(Figure 10) Implementation of Automated Vulnerability Inspection Management Function Based on the RC3 Meta-model

점 점검관리기능을 보여주고 있다. NIST 표준(SP 800-171의 '부록 D')는 CMMC의 보안통제항목과 RMF를의 보안통제항목 간 매핑정보를 제공하며, 이를 토대로 CMMC와 RMF를 동시에 지원할 수 있는 프로세스 순서의 정합성 검증을 수행하였다. NIST RC3메타모델에 기초한 취약점 점검관리 자동화 방안 모색과정을 설명하겠다.

취약점 점검관리 자동화 방안으로 미국정부의 정보보안 자동화 프로그램의 일환으로 국제 표준 취약점 목록인

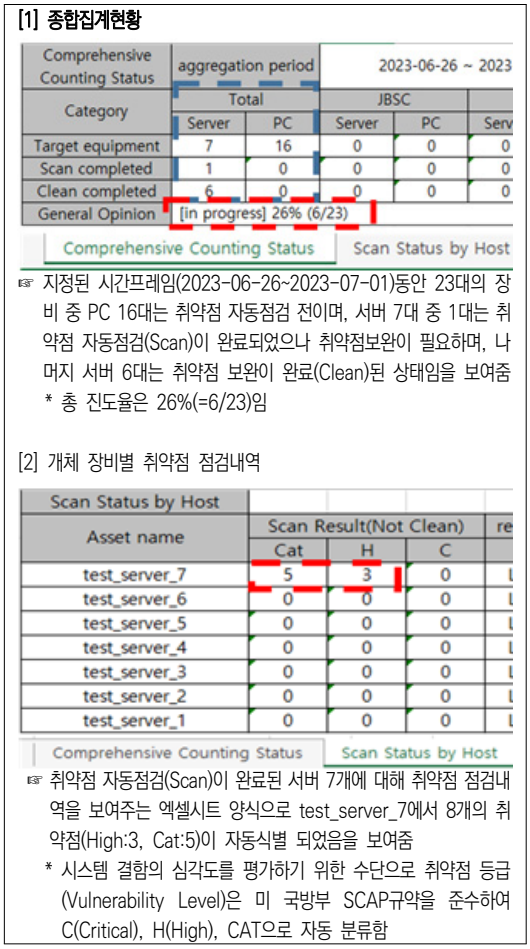
CVE (Common Vulnerabilities and Exposures)를 분석하여 데이터베이스화한 NVD(National Vulnerability Database) 활용을 우선적으로 모색해볼 수 있다[20].

그 다음단계로 NVD의 데이터를 이용하여 취약점을 자동으로 점검할 수 있도록 만든 NIST표준(NIST.IR.7511)인 보안요소자동화프로토콜 SCAP(Security Content Automation Protocol)을 채택하는 방법을 모색해 보았다[21]. 검토결과, SCAP은 CMMC와 RMF 모두에서 인정되는 공인된 취약점해소 및 위험예방 방법으로 RC3메타모델에 100% 부합됨에 따라 SCAP을 취약점 점검관리 자동화 방안으로 채택하였다.



(그림 11) SCAP의 6개 핵심 컴포넌트 요소
(Figure 11) Six Core Components of SCAP

그림 11은 SCAP의 6개의 핵심 컴포넌트 요소를 보여주고 있다[22]. 일반적인 취약점 및 노출CVE(Common Vulnerabilities and Exposures)는 IT자산의 취약점에 대해서 고유한 식별 번호를 부여하며, 공통구성목록CCE (Common Configuration Enumeration)은 보안 관련 시스템 설정 항목을 확인하기 위한 시스템 환경설정에 대한 공통 식별번호를 제공한다. 공통플랫폼목록CPE (Common Platform Enumeration)은 하드웨어, 운영체제, 응용 프로그램 등의 플랫폼을 식별하는 체계이다. 공통취약점점수산정체계CVSS(Common Vulnerability Scoring System)는 취약점 자체의 특성을 평가하여 심각도를 점수화한다. 확장가능한 구성 체크리스트 설명포맷XCCDF(Extensible Configuration Checklist Description Format)는 보안검증항목에 대한 내용과 결과를 작성을 작성하는데 사용되는 언어이다. 개방형 취약성 및 평가 언어 OVAL(Open Vulnerability and Assessment Language)은 시스템의 취약성을 자동으로 점검하기 위한 언어로 취약점점검의 자동화를 가능하게 한다.



[1] 종합집계현황

Comprehensive Counting Status	aggregation period		2023-06-26 ~ 2023		
Category	Total		JBSC		
	Server	PC	Server	PC	Serv
Target equipment	7	16	0	0	0
Scan completed	1	0	0	0	0
Clean completed	6	0	0	0	0
General Opinion	[in progress] 26% (6/23)				

Comprehensive Counting Status | Scan Status by Host

☞ 지정된 시간프레임(2023-06-26~2023-07-01)동안 23대의 장비 중 PC 16대는 취약점 자동점검 전이며, 서버 7대 중 1대는 취약점 자동점검(Scan)이 완료되었으나 취약점보완이 필요하며, 나머지 서버 6대는 취약점 보완이 완료(Clean)된 상태임을 보여줌
* 총 진도율은 26%(=6/23)임

[2] 개체 장비별 취약점 점검내역

Scan Status by Host				
Asset name	Scan Result(Not Clean)			re
	Cat	H	C	
test_server_7	5	3	0	
test_server_6	0	0	0	
test_server_5	0	0	0	
test_server_4	0	0	0	
test_server_3	0	0	0	
test_server_2	0	0	0	
test_server_1	0	0	0	

Comprehensive Counting Status | Scan Status by Host

☞ 취약점 자동점검(Scan)이 완료된 서버 7개에 대해 취약점 점검내역을 보여주는 엑셀시트 양식으로 test_server_7에서 8개의 취약점(High:3, Cat:5)이 자동식별 되었음을 보여줌
* 시스템 결함의 심각도를 평가하기 위한 수단으로 취약점 등급(Vulnerability Level)은 미 국방부 SCAP규약을 준수하여 C(Critical), H(High), CAT으로 자동 분류함

(그림 12) 자동 생성된 취약점점검 종합결과보고서(1/2)
(Figure 12) Comprehensive Vulnerability Inspection Report Automatically Generated (1/2)

앞서 그림 10의 기능은 RMF를 준수하며, 한/미 연합모의훈련 실무에도 실제 적용되어 활용되었다. 한/미 연합모의훈련에 참여하는 모든 IT자산들은 점검대상 장비의 특성에 따라 시스템 결함(예: 보안 취약점, 잘못된 시스템 환경설정)을 자동으로 식별하였다. 그림 10의 기능은 그림 12, 그림 13과 같이 자동 생성된 취약점점검 종합결과보고서(가상 예시)를 이용해 한측과 미측 지휘부에 보고되었다. 한/미 연합훈련의 경우, 참여하는 모든 IT자산들은 매번 훈련 시작 전 사전에 취약점 보완이 완료되어야 한다. 자동 생성된 취약점점검 종합한 결과는 주한 미군 담당부서에 전달된다. 통상적으로 취약점 점검(Scan) 후 해당 장비관리자는 1주 이내(time frame)에 보완조치를 완

[3] 취약점 유형별 세부내역

Not Clean Status by Host

Risk Rating	Identified Vulnerability Name	Asset name	Equipment Identifier
Cat	RHEL 7 : qemu-kvm (RHSA-2020:4079)	test_server_7	111.17
Cat	RHEL 7 : qemu-kvm (RHSA-2021:0347)	test_server_7	111.17
High	21 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities	test_server_7	111.17
Cat	22 / 1.8.0_321 / 1.11.0_14 / 1.17.0_2 Multiple Vulnerabilities	test_server_7	111.17
High	Oracle Java SE Multiple Vulnerabilities (April 2022 CPU)	test_server_7	111.17
High	Oracle Java SE Multiple Vulnerabilities (July 2022 CPU)	test_server_7	111.17
Cat	Oracle Java SE Multiple Vulnerabilities (October 2022 CPU)	test_server_7	111.17
Cat	Oracle Java SE Multiple Vulnerabilities (January 2022 CPU)	test_server_7	111.17

Comprehensive Counting Status | Scan Status by Host | Not Clean Status by Host

[예시사례]

Vulnerabilities 59

HIGH Oracle Java SE Multiple Vulnerabilities (July 2022 CPU) [식별된 취약점]

Description [지적사항]

The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is affected by multiple vulnerabilities as referenced in the July 2022 CPU advisory.

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2022-21540)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. (CVE-2022-21541)

Solution [조치방안]

Apply the appropriate patch according to the July 2022 Oracle Critical Patch Update advisory.

See Also

https://www.oracle.com/docs/tech/security-alerts/cpujul2022cvrf.xml

https://www.oracle.com/security-alerts/cpujul2022.html#AppendixJAVA

☞ 아직 미보완 조치(Not Clean)된 취약점 8개의 세부내역을 확인할 수 있음

(그림 13)자동 생성된 취약점점검 종합결과보고서(2/2)

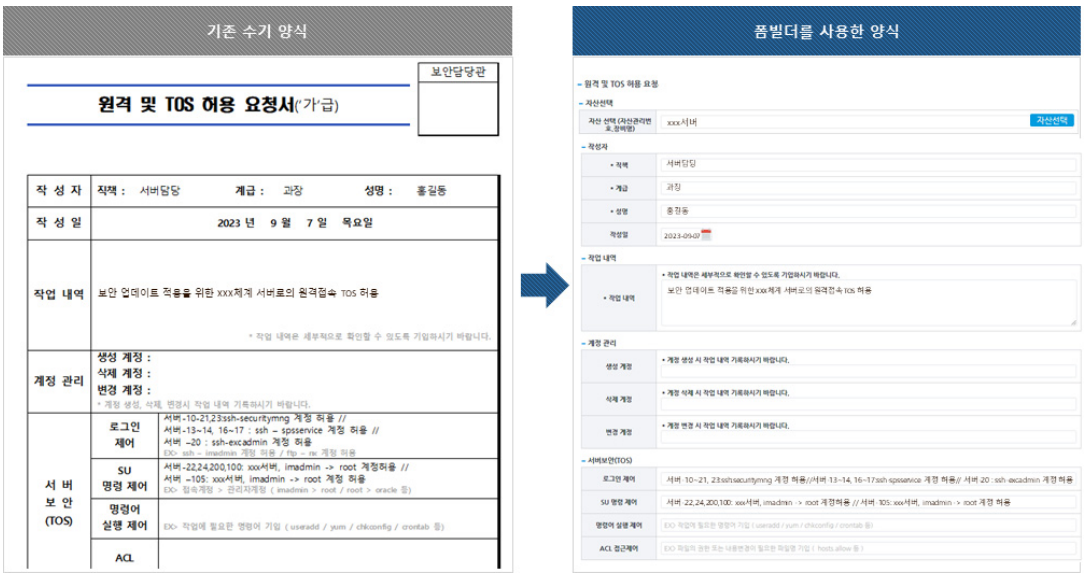
(Figure 13) Comprehensive Vulnerability Inspection Report Automatically Generated (2/2)

료(Clean)해야 한다. 보완조치시행에 별도의 비용이 발생하여 예산 확보를 위해 즉각 조치가 불가능한 경우에는 해당 장비관리자에게 보완조치 이행계획서를 제출받은 후 조치완료 상태로 재분류한다. 그림 13과 같이 미보완 조치(Not Clean)된 개별항목에 대해서는 그림 10의 [취약점점검 관리]화면에서 그림 13의 [예시사례]와 같이 상세 지적사항 및 조치방안을 제공하며, 보완조치과정에서 모든 활동들을 자산(Asset)과 증적자료(MCR)측면에서 이력이 남아 기록 관리된다.

예를 들어 사이버보안활동에 대해 지속적으로 관리하고 모니터링해야 하는 CMMC와 RMF에서는 그림 13과 같이 대상서버의 Oracle Jave SE보안취약점 해소를 위해 보안 업데이트를 적용하기에 앞서 서버로의 원격접속 허용 및 TOS(서버보안OS통과)허용을 요청한 후 보안담당관에 승인을 얻은 후 작업이 가능하다. 그림 14와 같이 신청 및 승인내역, 원격접속을 통해 이루어진 작업내역은 MCR측면에서 증적이력과 자산측면에서 자산이력으로 자동생성되어 추적/관리되고, CMMC인증심사와 RMF평가 시 제출할 증적자료 자동생성을 위한 기초데이터로 활용된다.

마지막으로 RC3 적용의 핵심 중 하나인 NIST 오버레이(overlay)정책에 맞춘 RC3 오버레이 아키텍처에 대해 설명하고자 한다. 피수검기관의 환경과 임무에 맞게 보안기준을 커스터마이징 할 수 있는 방법을 제공하는 오버

① 조직별 업무 특성에 맞춰 수기식 사이버보안 서식을 온라인 서식으로 쉽게 변환하는 것을 돕는 폼빌더 기능적용(예)

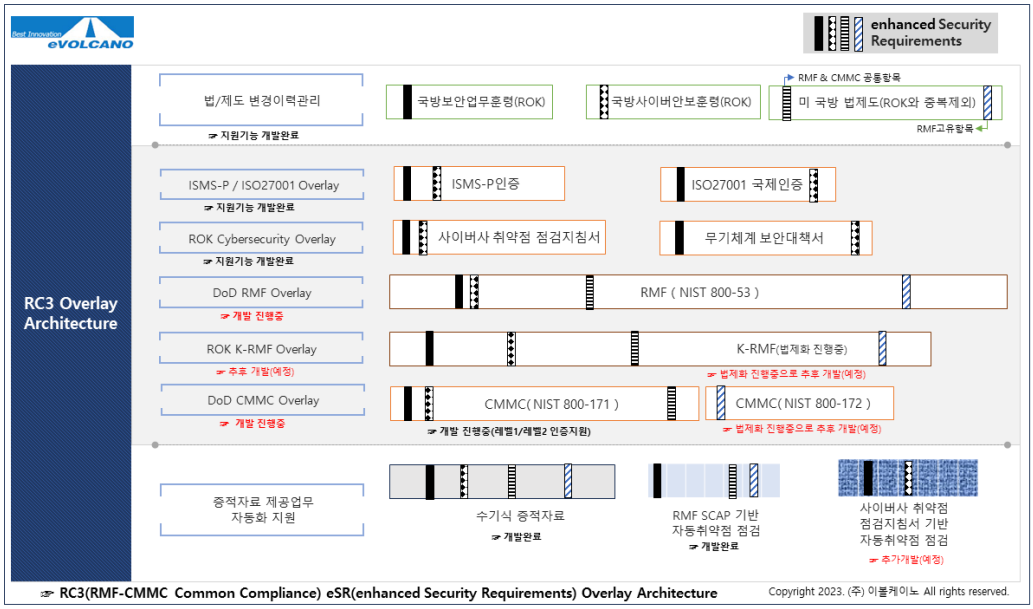


② IT자산별로 최초 도입부터 운영유지, 폐기까지 총 수명주기 사이버보안 관리를 위한 MCR증적이력 자동생성(예시)

(그림 14) 수기식 사이버보안활동의 온라인화 지원 및 자동 생성된 증적이력(예시)

(Figure 14) Support for Online Transformation of Manual Cybersecurity Activities and Automatically Generated Evidence History (Example)

레이 정책은 NISTIR 8183에서 처음 사용된 용어이며[23], RMF는 SP 800-53의 '부록 C'는 조직의 운영 환경, 시스템 유형 등에 맞춰 보안통제항목을 커스터 마이징(추가, 수정 또는 제외)할 수 있는 기회(지침)을 제공한다[24]. NIST SP 800-161서는 RMF(NIST SP 800-53)에서 추출한 오버레이를 토대로 NIST SP 800-161를 위한 확장 오버레



(그림 15) 국내외 다양한 국방 사이버보안 정책지원을 위한 RC3 오버레이 아키텍처

(Figure 15) RC3 Overlay Architecture for Supporting Various Domestic and International Defense Cybersecurity Policies

이를 만든 사례를 보여주고 있는데[25], NIST SP 800-161은 CMMC의 보안통제항목인 NIST SP 800-171의 모태가 되었다.

UML언어를 사용하여 정형화된 RC3 메타모델의 인스턴스화 개념은 NIST의 오버레이정책을 구현하기에 최적화되어 있다. 메타 모델링 관점에서 오버레이는 인스턴스화 과정을 거쳐 'deployment'하는 단계에 해당하며, 오버레이는 리눅스가 용도에 따라 여러 배포본이 존재하는 것과 유사하게 평가 목적(평가 지침)별로 선택적으로 적용할 수 있도록 미리 만들어놓은 보안 통제 항목의 집합을 의미한다. 컴플라이언스 실무(deployment) 단계에서 앞서 그림 7과 같이 인스턴스화된 모든 보안 취약점들에 대해 대응(보안 통제)하는 것은 현실적으로 불가능하다. 실제로 대다수 조직에서는 비용 대 효과 측면을 고려하여, 낮은 위험도의 보안 취약점들을 감내하고 개선하지 못하게 된다. 보안 담당자는 항상 어떤 우선순위에 의거해 보안 취약점들을 해결해야 하는지 고민하게 된다. 더욱이, 2025년~2026년 사이에 중견 규모 이상의 방산업체, 국방IT 사업 참여 업체의 보안 담당자는 그림 15과 같이 RMF, CMMC 등 새로운 보안 평가 지침들을 직면하게 될 것이다. 평가 지침별로 보안 통제 요구 수준은 모두 제각기 상이하며, 보안 담당자가1개 이상의 평가 지침을 동시에 준수해야 하는 상황이 되면 매우 큰 업무 혼란에 직면하게 될 것이다. 제각기 상이한 평가 지침들 사이에서 최소한의 노력으로 공통 대응이 가능한 보안 통제 항목 배포본을 제공하는RC3 오버레이 아키텍처는 컴플라이언스 실무 효율성을 향상시키는데 크게 도움이 될 것이다.

4. 결 론

국내 방산기업은 CMMC와 RMF라는 생소한 국방 사이버보안감사제도에 미리 대비하지 않는다면 어려운 상황에 직면할 수 있다. 특히 ,방산무기 수출에 주력하는 국내 방산업체들에게 CMMC인증 취득을 위해 남아 있는 시간적 여유는 많지 않다는 점은 매우 큰 어려움으로 대두 될 수 있다.

본 논문은 2022년 이후 미 RMF를 토대로 국방부 합동참모본부 주관 한/미 연합연습 모의지원 사이버보안 자동화 솔루션 개발프로젝트를 수행하며 얻은 미 국방 사이버보안감사제도 준비에 대한 노하우를 토대로 CMMC와 RMF 보안감사 준비업무를 동시에 지원할 수 있는 상용도구(컴플라이언스 솔루션)의 공통 규정준수 메타모델

개발과정에 대해 기술하였다.

메타모델의 개발 및 적용 과정에서 드는 비용과 소요시간은 조직의 규모와 장비 수, 시스템 복잡성 등 다양한 요인에 의해 결정된다. 효과적인 솔루션 공급 계획 수립은 비용과 시간을 절약하는 데 중요한 역할을 한다. 본 논문에서 제안하는 솔루션은 이러한 요인들을 고려하여 개발되었으며, 기존 시스템의 통합과 확장성을 용이하게 함으로써, 메타모델의 적용 기간을 상당히 단축시킬 수 있다. 특히, 대규모 조직이나 복잡한 시스템 환경에서는 이러한 접근 방식이 시간과 비용 측면에서 더욱 효과적일 것으로 예상된다. 이는 메타모델의 적용이 조직의 규모가 커짐에 따라 더욱 효율적이고 비용 효과적인 방식으로 진행될 수 있음을 의미한다.

CMMC와 RMF를 동시에 지원할 수 있는 공통 규정 준수 메타모델의 개발이 필요한 주된 이유는, 국내 방산 업체들이 향후 국방 사이버보안 감사 준비 과정에서 불필요한 중복 업무를 최소화하기 위함이다. 구체적으로 향후 국내 방산업체는 신형무기체계에 대한 시제품개발(선행연구)시 RMF(또는 K-RMF)에 근거해 사이버보안 평가/승인을 준비해야 하고, 양산단계 해외수출 시에는 또 다시 CMMC기준에 맞춰 인증심사를 준비해야 하기 때문이다.

CMMC와 RMF 모두 새로운 국방 사이버보안감사에 대비한 준비과정에 있어 연속성과 추적성을 입증해야 하는 점에서 상용 지원도구(컴플라이언스 솔루션) 활용은 필수적이다. 특히, 2025년 10월전까지 CMMC인증을 취득해야 하는 국내 방산업체들에게 있어 CMMC와 RMF 동시에 지원할 수 있는 상용 컴플라이언스 솔루션의 활용은 매우 유용할 것이라 예상된다.

그 이유로 태생적으로 RMF의 보안평가모델(NIST SP 800-53)은 800-161을 거쳐 CMMC(NIST SP 800-171)의 모태가 되었고, RMF를 준수할 경우 CMMC의 요구사항을 완벽히 충족시킬 수 있기 때문이다. CMMC의 실무 경험이 있는 전문가가 전혀 없는 국내 여건 상 미 RMF를 실무에 적용해가며 개발된 컴플라이언스 솔루션에 녹아들어가 있는 경험적 노하우는 CMMC인증심사과정에 있어서도 매우 큰 도움이 될 것이다.

참고문헌(Reference)

[1] Office of the USD A&S, “CMMC Self-Assessment Guide Level 1, Version 2.0,” DoD, 2021.12. https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_FinalDraft_20211210_508.pdf

[2] DoD, DoD Program Manager’s Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle VERSION 1.0, DoD, September 2015. https://books.google.co.kr/books/about/ DoD_Program_Manager_s_Guidebook_for_Inte.html?id=nbsjjwEACAAJ&redir_esc=y

[3] United States Government, “Basic Safeguarding of Covered Contractor Information Systems,” FAR 52.204-21, 2323.6.2. https://www.acquisition.gov/far/52.204-21

[4] “Key Cybersecurity Challenges and Proposed Solutions Faced by the Domestic Defense Industry,” news2day, 2023.8.13. https://www.news2day.co.kr/article/20230811500136

[5] Seungbae Lee, “Considerations for Information Security and Cybersecurity in U.S. Weapon Systems Acquisition Programs,” Defense Security Research Institute, Defense and Security, Volume 1, Issue 2, December 2019.

[6] Advancements in the Establishment of ’Security Risk Management System’ in the Defense Sector, Defense Daily, November 27, 2022.

[7] CYBER AB, CMMC IMPLEMENTATION CONSULTING, https://cyberab.org/CMMC-Ecosystem/Ecosystem-Roles/Consulting-and-Implementation

[8] Dr William Greenwalt, Tom Corben, “BREAKING THE BARRIERS: REFORMING US EXPORT CONTROLS TO REALISE THE POTENTIAL OF AUKUS,” UNITED STATES STUDIES CENTRE, 2023.5.17. https://doi.org/10.17606/2v6z-9j05

[9] Min-Hyo LEE. “A Study on the Tallinn Manual on the International Law Applicable to Cyber Warfare,” The Korean Journal of Humanitarian Law, pp. 9-42, 2017. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07365876

[10] DoD, “DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT),” 2014, 5. https://www.dau.edu/cop/stm/documents/dodi-851001-risk-management-framework-rmf-dod-information-technology

[11] NIST, NIST Risk Management Framework, Created November 30, 2016, Updated December 13, 2023 https://csrc.nist.gov/projects/risk-management/about-rmf

[12] DoD CIO, Cybersecurity Maturity Model Certification (CMMC) Model Overview, 2021.11. https://dodcio.defense.gov/CMMC/about/

[13] Tsoumas, B,Gritzalis, D, “Towards an Ontology-based Security Management,” AINA’06, IEEE, 2006. https://doi.org/10.1109/AINA.2006.329

[14] Danijel Milicevic, Matthias Goeken, “Model Driven Information Security Management - Evaluating and Applying the Meta Model of ISO 27001,” AMCIS 2011 Proceedings, 2011. https://aisel.aisnet.org/amcis2011_submissions/376/

[15] Danijel Milicevic, Matthias Goeken, “Ontology-Based Evaluation of ISO 27001,” in Proc. of 10th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society (I3E), Nov 2010, Buenos Aires, Argentina. https://doi.org/10.1007/978-3-642-16283-1_13

[16] Ik-jae Kim, KANG JI WON, Shin, Dong Kyoo, “A study on the application of mission-based weapon system cybersecurity test and evaluation,” vol.22, no.6, pp. 71-81, JICS, 2021. https://doi.org/10.7472/jksii.2021.22.6.71

[17] DoD, The Department of Defense Cyber Table Top Guidebook Version 1.0, 2018.6.

[18] NIST, “Guide for Conducting Risk Assessments,” NIST SP 800-30 Rev. 1, 2012. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

[19] Ye-Na Joo, Beomsoo Kim, HyukJin Kwon, “Suggestion of Risk Priority Identification Methodology for the Establishment of the Korean RMF System,” JDPS, vol.37, no.2, pp. 99-130, 2021. https://www.dbpia.co.kr/Journal/articleDetail?nodeId=NODE10653845

[20] NIST, NATIONAL VULNERABILITY DATABASE, https://nvd.nist.gov/

[21] NIST, “Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements,” NISTIR 7511 Revision 4, 2016. https://csrc.nist.gov/projects/scap-validation-program/scap-1-2-validation

[22] Mohammed Noraden Alsaleh, E. Al-Shaer, “SCAP based configuration analytics for comprehensive compliance checking,” 4th SAFECONFIG, IEEE, 2011. https://doi.org/10.1109/SafeConfig.2011.6111674

[23] NIST, “Cybersecurity Framework Version 1.1 Manufacturing Profile,” NISTIR 8183 Revision 1, 2020. https://csrc.nist.gov/news/2020/cybersecurity-framework-v1-1-manufacturing-profile

[24] NIST RMF, Security and Privacy Control Overlay Overview https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/overlay-repository/overlay-overview

[25] NIST, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,” NIST SP 800-161r1, 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

◐ 저 자 소 개 ◑

황 재 윤(Jae-yoon Hwang)
2009년~2012년 SK C&C, SK Infosec
2012년~2014년 대웅제약 IT 그룹웨어 ERP 사업부장
2014년~현재 ㈜ 이볼케이노 대표이사
관심분야 : Cybersecurity Audit, Compliance, RMF, CMMC
E-mail : rmkk@evolcano.co.kr

권 혁 진(Hyuk-jin Kwon)
2000년 성균관대학교 공과대학 산업공학과(공학박사)
2017년~2020년 국방부 정보화기획관
1991년~2021년 한국국방연구원 책임연구위원
2021년~현재 서울과학기술대학교 국방방호학과 주임교수
2023년~현재 서울과학기술대학교 국방인공지능응용학과 주임교수
2016년~현재 ISO27001 국제인증 선임심사원
관심분야 : 국방정보화, 국방사이버안보, 국방인공지능 etc.
E-mail : kwonhj@seoultech.ac.kr