Journal of the Korea Academia-Industrial cooperation Society
Vol. 25, No. 8 pp. 341-349, 2024

https://doi.org/10.5762/KAIS.2024.25.8.341
ISSN 1975-4701 / eISSN 2288-4688

# K-RMF 보안 점검을 위한 美 RMF 보안 자동화 도구 분석

**최은진*, 노승일**
**국방기술품질원**

# Analysis of U.S. RMF Security Automation Tools for K-RMF Security Assessments

Eun-Jin Choi*, Seungil Noh
Defense Agency for Technology and Quality

**요 약** 최근 주요 정보기관을 대상으로 하는 보안 사고의 수가 급증하면서 정보를 송·수신하는 시스템의 보안을 지속해서 관리하는 방안이 중요해지고 있다. 미국 NIST(National Institute of Standards and Technology)에서는 IT 기술이 포함된 시스템을 대상으로 시스템 수명주기 전반에 걸쳐 보안을 내재화할 수 있는 NIST RMF(Risk Management Framework) 제도를 개발하였으며, 미국 국방부(DoD, Department of Defense)에서는 이를 IT 기술이 탑재된 군사 시스템에 도입할 수 있도록 관련 규정을 개발하였다. 한국에서도 군 환경에 적합한 보안 기능을 도입하기 위하여 한국형 위험관리 프레임워크(K-RMF) 제도를 개발하고 이를 국방 무기체계 내 적용 방안을 연구 중이다. 하지만 K-RMF 제도의 원활한 정착을 위해서는 K-RMF 보안통제항목별로 보안 기능을 구현 및 평가, 모니터링할 수 있어야 하며, 이를 위한 DoD RMF 보안 자동화 평가 도구에 관한 연구가 필수적이다. 본 논문에서는 DoD RMF 제도의 구현 및 평가, 모니터링 단계에서 활용 가능한 보안 자동화 평가 도구의 종류 및 기능을 살펴보았다. 보안 자동화 도구가 갖는 특징을 확인하고 K-RMF 제도에 활용하는 방안을 고려해보았으며, 분석 결과는 향후 K-RMF에 적용 가능한 한국형 보안 자동화 도구 개발 및 적용 시 활용할 수 있을 것이다.

**Abstract** As the number of security incidents targeting major intelligence agencies increases rapidly, managing system security methods is becoming increasingly important. In response, the National Institute of Standards and Technology (NIST) in the U.S. has developed the Risk Management Framework (RMF), which manages security throughout the life of systems incorporating IT technology. The U.S. Department of Defense (DoD) has adapted this framework to apply to military systems equipped with IT technologies. Similarly, South Korea has developed its Korean Risk Management Framework (K-RMF) tailored for military environments and is currently working on implementing this framework within the defense weapons system. On the other hand, the implementation, assess, and monitoring results of K-RMF security controls for effective application of K-RMF are important, so the list of security automation tools should be reviewed first. This study examined the types and functions of security automation tools under the DoD RMF Implementation, Assess, and Monitoring steps. The characteristics of the security automation tool were identified, and a plan to use it in K-RMF was considered. The analysis results can be used to develop Korean security automation tools applicable to K-RMF.

**Keywords :** Risk Management Framework, Security Controls, Cyber Security, K-RMF, Security Automation Tools, Vulnerability, Compliance

*Corresponding Author : Eun-Jin Choi(Defense Agency for Technology and Quality)
email: ejchoi@dtaq.re.kr
Received May 10, 2024 Revised June 21, 2024
Accepted August 2, 2024 Published August 31, 2024

## 1. 서론

최근 국제적 테러조직에서 일으키는 공격 기법이 고도화되면서 각종 해킹 및 보안 사고의 수가 급증하고 있다. 특히 주요 정보기관 및 군(軍) 정보기술(IT) 탈취를 목적으로 하는 공격의 수가 증가하였는데, 근래 보안 사고 유형 조사 결과에 따르면 국가 주요기관을 대상으로 하는 공격의 종류 및 횟수가 급격히 증가하였음을 확인할 수 있었다[1-3]. 군에서는 공세적 사이버 방어 활동을 강화함과 동시에 각종 보안 위협 이슈에 신속하게 대응할 수 있도록 관련 제도를 강화하였다[4,5].

미국 국방부(DoD, Department of Defense)는 일찍이 IT 기술이 탑재된 군사 시스템의 사이버보안을 강화하기 위한 보안제도를 개발하고 사이버 공간의 변화에 따라 발전시켜왔다. 초기에 도입된 보안 평가 및 관리 제도는 군 정보시스템(Information System) 데이터의 기밀성을 강화하기 위한 목적으로 개발되었는데, 대상 시스템에서 기밀 정보의 보호 수준을 평가하고 총 7단계 레벨 중 해당하는 영역을 평가 결과로 제출하였다. 이후 단순 분류만으로는 보안 평가가 어려워짐에 따라 평가 시기를 특정하는 것이 아닌 시스템 수명주기(Life-cycle) 전반에 거쳐 보안을 관리할 수 있는 제도로 발전하였다.

2014년 DoD에서는 NIST(National Institute of Standard and Technology) 규격에 기반한 위험관리 프레임워크(RMF, Risk Management Framework) 제도를 국방 분야에 도입하였다. RMF 제도는 시스템 수명주기 간 발생하는 보안 위협을 식별할 수 있도록 관련된 보안 요구사항들을 보안통제항목(Security Controls) 단위로 관리할 수 있는데, RMF 대상으로 선정된 시스템은 선정된 보안통제항목의 보안 요구사항을 식별하여 기능을 구현하고 일정 주기마다 관리할 수 있어야 한다. 군 환경 내 RMF 제도가 정착함에 따라 미국 국방 환경에서 사용하는 IT 및 통신을 지원하는 기관인 국방정보시스템국(DISA, Defense Information Systems Agency)에서는 기능 구현이 요구되는 보안통제항목을 대상으로 기술적 구현 및 지속적인 모니터링이 쉽도록 보안 자동화 도구(Security Configuration Tools)를 개발하였으며, 보안 체크리스트를 분기별로 최신화한다.

2019년 4월, DoD에서 韓-美 연동체계를 대상으로 RMF에 준하는 보안제도를 적용할 것을 요구함에 따라 한국에서도 RMF를 한국화한 한국형 위험관리 프레임워크(K-RMF)를 개발하였다. K-RMF 제도는 2026년부터 전면 시행하는 것을 목표로 하고 있으며[6], 현재는 기존 보안제도와의 연계를 위한 연구가 진행되고 있다. 하지만 K-RMF 제도의 업무 효율성을 향상하기 위해서는 수명주기 간 보안통제항목을 관리하면서 지속해서 상태를 모니터링하는 보안 자동화 도구의 도입 방안이 고려되어야 한다.

본 논문의 구성은 다음과 같다. 2장에서는 연구의 배경이 된 DoD RMF 제도와 K-RMF에 관하여 차례대로 확인해보았으며, 3장에서는 DISA에서 DoD RMF 단계마다 사용할 수 있도록 개발 및 배포한 보안 자동화 도구들과 그 외 기관에서 개발한 보안 기능 자동화 도구에 관하여 살펴보았다. 이어 4장에서는 국내 보안 자동화 도구 도입을 위해 연구를 수행한 사례에 관하여 살펴보았다.

## 2. 위험관리 프레임워크(RMF)

### 2.1 DoD RMF

RMF는 NIST에서 개발한 제도로, IT 기술이 포함된 시스템을 대상으로 수명주기 관점 보안 평가 및 관리를 적용하는 프레임워크이다. DoD RMF에서는 NIST에서 개발한 RMF보다 더 엄격한 규격을 적용하기 위하여 NIST 규격 문서, FISMA(Federal Information Security Modernization Act)와 FIPS(Federal Information Processing Standards) 표준, DoDI 훈령 등을 활용한다. 이중 NIST 규격 문서는 컴퓨터 보안에 관한 각종 연구와 지침 등을 포함하는 문서로, NIST SP(Special Publications) 800 시리즈로 작성되었다.

DoDI 8510.01에 따르면 DoD 정보를 수신, 처리, 저장, 전송하는 모든 DoD 소유 또는 통제 IT를 DoD IT(DoD Information Technology)라 하며 개별 하드웨어 및 소프트웨어 제품부터 PIT(Platform-IT), 정보시스템, 대규모 컴퓨팅 환경, 엔클레이브(Enclave)를 포함한다[7]. 정보시스템과 PIT 시스템의 경우 DoD RMF 평가 및 인증 수행 대상으로 지정되어, 아래 6단계 프로세스를 차례대로 수행한다[8].

1) 시스템 보안 분류(System Categorize) : 시스템 보안 분류 단계에서는 대상 시스템에서 활용되는 정보의 보안등급을 확인해야 한다. 보안등급은 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability) 수준에 따라 H(High), M(Moderate), L(Low)로 나타낼 수 있으며 정보별 보안등급은 NIST SP 800-60 Appendix C에서 확인할 수 있다. 예를 들어 전자결제기능을 도입한 시스템에서는 [C.2.8.9 Personal Identity and Authentication

Information Type], [C.3.2.5 Payment Information Type] 등을 선정할 수 있는데, NIST SP 800-60에 따르면 [C.2.8.9 Personal Identity and Authentication Information Type]의 보안등급은 {M, M, L}, [C.3.2.5 Payment Information Type]의 보안등급은 {L, M, L}로 확인할 수 있다. 시스템 소유자(System Owner)는 정보 유형별 보안등급 확인이 완료되면 가장 높은 등급으로 최종 등급을 선정하는 HWM(High Water Mark) 기법을 적용하여 보안 시스템의 초기 보안등급을 결정하게 된다. 만일 앞서 살펴본 시스템에서 전자결제기능 외 추가할 정보가 없다면, 최종 등급은 {M, M, M}이 된다.

2) 보안통제항목 선정(Select) : 선정 단계에서는 앞서 결정된 보안등급에 따른 보안통제항목을 식별한다. 시스템 소유자는 최종 등급 이상의 보안등급을 요구하는 보안통제항목을 초기 보안통제항목으로 선정하고, 대상 시스템의 운용 환경과 특성을 고려하여 항목을 추가하거나 삭제한다. 보안통제항목 종류와 보안등급은 NIST SP 800-53, CNSSI 1253 문서에서 확인할 수 있다[9,10].

3) 보안통제항목 구현(Implement) : 구현 단계에서는 대상 시스템 내 최종 선정된 보안통제항목 기능을 구현한다. NIST SP 800-53에서는 보안통제항목별 보안요구사항, 보충 설명(Supplemental Guidance), 관련 강화 항목(Control Enhancement), 관련 문서(Reference) 등을 제공하고 있으며, 보안통제항목의 이해를 높이기 위해서는 DISA에서 제공하는 CCI(Control Correlation Identifier)를 참고할 수 있다.

시스템 소유자는 관련 정책과 구현 간 예상되는 위협을 분석한 뒤, 분석 결과에 기반하여 보안계획서(SP, Security Plan) 문서 내 선정된 보안통제항목구현계획을 작성한다. 구현 단계는 작성된 구현계획에 기반하여 진행되어야 하며, 구현 종료 시점에서 조직의 ISSO(Information System Security Officer)와 ISSM (Information System Security Manager)는 개발 간 자체적으로 보안 평가(Self-Assessment)를 수행하여 구현 결과의 적절성을 확인할 수 있다[11].

4) 보안통제항목 평가(Assess) : 평가 단계에서는 구현된 보안통제항목의 구현 여부를 확인한다. 평가자(SCA, Security Control Assessor)는 평가계획에 기반한 평가를 진행하고 수행 결과를 보안 평가 결과서(SAR, Security Assessment Report)와 후속조치계획서(POA&M, Plan Of Action and Milestones)에 작성한다.

5) 시스템 인가(Authorize) : 인가 단계는 앞서 작성된 보안 인가 패키지(SP, SAR, POA&M)를 활용하여 시스템의 위험 정도를 판별한다. 조직의 인가책임자(AO, Authorizing Official)는 미구현 보안통제항목으로부터 발생 가능한 위험을 식별하고, 수용 여부를 결정한다.

Table 1. List of NIST RMF Security Controls [9]

| Identifier | Family |
|---|---|
| AC | Access Control |
| AT | Awareness and Training |
| AU | Audit and Accountability |
| CA | Security Assessment Authorization |
| CM | Configuration Management |
| CP | Contingency Planning |
| IA | Identification and Authentication |
| IR | Incident Response |
| MA | MAintenance |
| MP | Media Protection |
| PE | Physical and Environmental Protection |
| PL | PLanning |
| PS | Personnel Security |
| RA | Risk Assessment |
| SA | System and Services Acquisition |
| SC | System and Communications Protection |
| SI | System and Information Integrity |
| PM | Program Management |

6) 모니터링(Monitoring) : 모니터링 단계는 시스템 운영 간 발생할 수 있는 위협 요소를 지속적으로 모니터링하는 단계이다. 평가자는 모니터링 계획의 준수 여부와 신규 취약점 분석 결과 등을 토대로 평가 문서를 지속해서 업데이트한다.

NIST SP 800-53 revision 4 문서에 의하면 DoD RMF 제도에서 활용되는 보안통제항목은 표 1과 같이 접근통제(AC, Access Control), 형상관리(CM, Configuration Management) 등 18개 패밀리로 구성되어 있다. 각 항목의 보안 요구사항은 FIPS 200, NIST SP 800-53 등에서 확인할 수 있으며, NIST SP 800-53 보안통제항목별 관련 문서를 통해서도 항목에 대한 이해를 높일 수 있다.

## 2.2 K-RMF

NIST RMF 제도가 군 환경뿐 아니라 위험 식별, 평가 및 관리가 요구되는 각종 산업에서 활용되는 반면 K-RMF 제도는 한-미 연동체계에서 신규 개발되는 국방무기 및 정보시스템까지 적용 대상을 확장하는 것을 목표로 개발 중이다. K-RMF는 DoD RMF와 동일한 6단계 프로세스로 구성되어 있으며, 한국군 특성을 고려하기 위

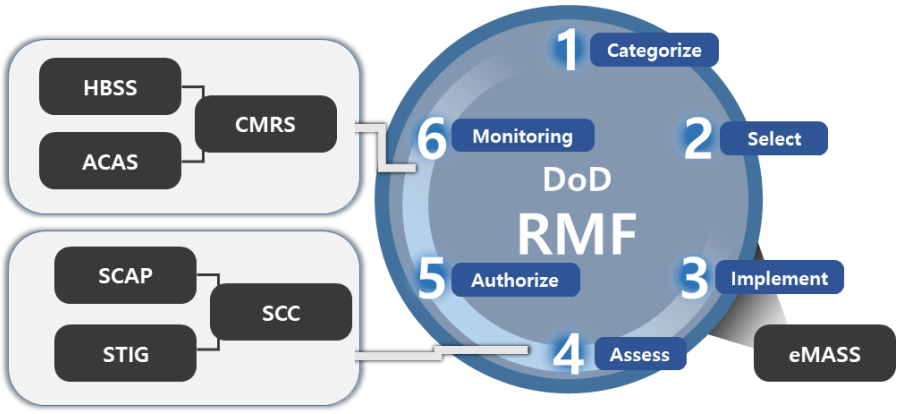


Fig. 1. DoD RMF procedures and related security automation tools

하여 시스템 보안 분류와 같은 초기 단계에서 K-RMF 제도를 적용하는 방안이 선행 연구되었다[12,13].

K-RMF 시스템 보안 분류의 경우, NIST SP 800-60과 같이 정보 유형별로 작성된 보안등급 대신 대상 시스템의 임무 영역과 직무, 정보 유형이 표기된 문서를 활용하여 보안등급을 결정한다[13]. 보안등급은 기밀성, 무결성, 가용성 수준에 따라 상, 중, 하로 표기되며 관련 문서에 명시되지 않은 정보 유형이 식별된 경우 유관 부서에서 검토 의견을 받아 작성할 수 있다. 보안등급에 따라 초기 식별되는 K-RMF 보안통제항목은 NIST SP 800-53 revision 4에 한국군 훈령과 ISO 27001을 반영하여 총 17개 패밀리 761개 항목으로 구성되어 있으며[14], 이중 운용환경 등을 고려하여 최종 항목을 선정한다. 개발자는 최종 선정된 K-RMF 보안통제항목의 보안 요구사항에 기반하여 보안 기능을 구현하고, 평가자는 기능의 적절성을 평가해야 한다.

현재 군에서 적용되고 있는 보안 평가 방안은 방위산업보안업무훈령에 근거한 보안 측정과 방위산업기술보호법에 기반한 방산기술보호 통합실태조사가 있다. 반면 K-RMF 보안통제항목 평가 절차는 구현된 보안 기능의 적절성 평가와 위험의 수용 여부를 분석하는 업무를 포함한다. 따라서 선정된 K-RMF 보안통제항목의 구현 단계 이후부터는 현 보안 평가 방안과의 연관성을 고려하되, DoD RMF 절차와 같이 구현 결과의 적절성을 확인하고 평가 결과 위험도를 분석하여 모니터링 주기를 계획할 수 있는 연구가 진행되어야 한다. 이를 위하여 DoD RMF 보안 평가 방안을 적절히 활용할 수 있어야 하며 단계마다 활용할 수 있는 보안 자동화 도구에 대한 이해가 요구된다.

## 3. DoD RMF 보안 자동화 도구

DoD RMF에서 평가자는 보안 자동화 도구를 활용하여 보안통제항목별 기능의 구현 여부와 위험의 심각도를 파악할 수 있다. DISA에서는 군 관련 기관을 대상으로 점검 절차를 간소화하기 위해 SCAP(Security Content Automation Protocol) 기반의 보안 자동화 도구를 개발하여 배포하고 있다. 이 도구들은 표준화된 규격과 프로토콜을 사용하여 취약점 및 컴플라이언스(Compliance) 점검, 환경 설정 검사 등을 자동화하는 목적으로 사용된다.

2018년 2월 공개된 SCAP 1.3 버전에서 SCAP의 구성요소는 총 12개로, 언어, 보고형식, 식별체계, 측정 및 채점 시스템, 무결성으로 분류된다[15]. 이중 취약점 및 컴플라이언스 점검에 주로 활용되는 요소들은 다음과 같다.

- XCCDF(Extensible Configuration Checklist Description Format) : 보안 설정이나 정책 준수를 위한 보안 체크리스트를 작성
- OVAL(Open Vulnerability and Assessment Language) : 보안 기능의 구체적인 점검 방안 제공
- CVE(Common Vulnerabilities and Exposures) : 제품의 공개된 보안 취약점을 평가
- CVSS(Common Vulnerability Scoring System) : 취약점의 심각도를 평가

DoD RMF에서는 보안통제항목 단위로 보안 기능을 구현하므로 SCAP의 활용 범위는 보안통제항목 구현 종료 시점부터 모니터링 단계까지 가능하다. 따라서 DISA에서는 SCAP의 검증 방안을 OVAL로 작성된 체크리스트 파일 형태로 구현하여 시스템별로 배포한다. 사용자는 DoD RMF 대상 시스템의 SCAP 기반 체크리스트 파

일을 내려받은 후, 자동화 도구를 사용해 기능의 구현 여부를 확인한다. 본 장에서는 DoD RMF에서 사용되는 각종 자동화 도구와 그 활용 방안에 대하여 살펴보았다.

### 3.1 eMASS

DISA에서 개발한 eMASS(Enterprise Mission Assurance Support Service)는 정부기성품(GOTS, Government-off-the-Shelf)를 대상으로 DoD RMF 전 단계 보안 관리 서비스를 자동화하는 도구이다. eMASS 접근 권한을 부여받은 사용자는 각 단계 종료 시점마다 수행 결과를 프로그램 내 업로드해야 하며, 업로드된 산출물을 최신화 시점마다 확인할 수 있다. 따라서 사용자는 자료를 한눈에 확인하는 것이 가능하며 추후 프로세스 추적에 용이하다.

### 3.2 구현 지침

DISA에서는 DoD RMF 전 단계를 관리할 수 있는 eMASS를 개발하면서 각 단계 산출물을 eMASS에 등록하여 결과를 가져올 수 있도록 Fig. 1과 같이 단계별 활용 가능한 자동화 도구를 개발하였다. 구현 단계에서는 조직이 시스템 내 보안통제항목 기능이 올바르게 구현되었는지 확인하기 위하여 장치별 또는 대상별 구현 지침 파일과 비교할 수 있는데, 이때 사용 가능한 파일이 바로 SCAP Benchmark, STIG(Security Technical Implementation Guides), SRG(Security Requirements Guide)이다.

1) SCAP Benchmark

DoD RMF에서는 각 기능의 구현 여부를 판단하기 위해 SCAP Benchmark 파일을 체크리스트로 사용한다. 이 파일들은 특정 시스템, 애플리케이션 또는 기기의 보안 설정과 점검 방법을 정의하며, XML 형식으로 작성되어 있다. SCAP Benchmark 파일과 호환되는 보안 자동화 도구를 이용하면 정의된 요구사항과 체크리스트에 따라 시스템을 자동으로 스캔하고, 각 항목의 준수 여부를 효과적으로 평가할 수 있다.

2) STIG

STIG는 군에 납품되는 IT 상용제품을 대상으로 개발한 보안 가이드이다. 제품별로 개발된 STIG 파일은 제품에 요구되는 보안 설정, 취약점, 관련 규정, 심각도, 점검사항 등을 포함하며 DISA 홈페이지에서 다운로드할 수 있다. 사용자는 이 문서를 활용하여 제품의 보안 준수 상

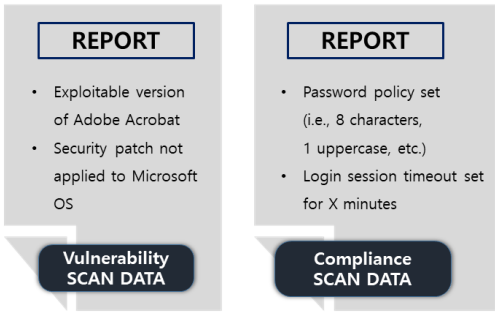


Fig. 2. Example of scanned data

태를 수동으로 평가하고, 권장 보안 기준의 준수 여부를 검증할 수 있다.

3) SRG

STIG가 제품 단위의 보안 요구사항을 다룬다면, SRG는 제품군 단위의 보안 요구사항을 포함한다. SRG는 보다 광범위한 보안 요구사항을 제공하며 다양한 환경에서 적용 가능한 범용성을 갖추고 있다. 예를 들어, 특정 정보보호제품에 적용되는 구체적인 보안 조치와 구성 방법을 다루는 것이 STIG라면, 정보보호제품군이 일반적으로 준수해야 하는 기본적인 보안 조치사항을 포함하는 것이 SRG이다.

### 3.3 평가 및 모니터링 자동화

보안 기능의 평가와 취약점 관리는 크게 두 가지 주요 방법으로 이루어진다. 첫 번째 방법은 앞서 살펴본 체크리스트 파일을 업로드하여 해당 항목의 구현 여부를 자동으로 확인하는 것이다. 두 번째 방법은 취약점을 주기적으로 모니터링하여 필요한 조치를 취하는 것이다. 이 두 가지 방법은 Fig. 2와 같이 SCC(SCAP Compliance Checker), OpenSCAP, STIG Viewer와 같은 체크리스트 기반 보안 평가 도구와 ACAS(Assured Compliance Assessment Solution), HBSS(Host Based Security System), CMRS(Continuous Monitoring Risk Scoring)와 같은 취약점 모니터링 및 관리 도구로 분류할 수 있다.

1) SCC/OpenSCAP

SCC는 DISA에서 개발한 SCAP 기반 도구로, 운영체제 및 소프트웨어의 구현 결과를 점검하여 조직이 연방정부의 보안 규정 및 표준을 준수하는지 확인한다. 사용자는 원하는 환경 설정을 선택하고 준비된 체크리스트 파일을 업로드하면 SCC는 보안 항목별로 점검을 수행하

고 결과를 심각도(Low, Medium, High)와 성공/실패(Pass/Fail)로 나타낸다.

OpenSCAP은 오픈소스 프로젝트로 개발된 SCAP 기반 도구로, 서버, 가상머신, 워크스테이션 등 다양한 환경에서 취약점 및 보안 구성 점검을 수행할 수 있다. 사용자가 체크리스트 파일을 업로드하면 OpenSCAP에서는 체크리스트 항목별 매핑된 CCI를 활용하여 구현 여부를 제공한다. 따라서 DoD RMF 절차에서 OpenSCAP은 시스템의 보안 요구사항을 충족하는지 정밀하게 분석하고 보안 관련 결함을 수정할 때 활용할 수 있다.

2) STIG Viewer

STIG Viewer는 SCC 및 OpenSCAP에서 생성된 XCCDF 파일을 분석하고, 점검 결과를 더욱 명확하게 이해할 수 있게 도와주는 소프트웨어이다. 점검 결과는 위험 수준에 따라 CAT 1~3으로 분류되며, 사용자는 분류된 위험 수준을 활용하여 보안 위험을 우선순위에 따라 관리하고 대응 계획을 수립할 수 있다.

3) ACAS

ACAS는 DISA에서 제공하는 종합적인 네트워크 보안 평가 솔루션으로, 네트워크와 연결된 모든 IT 제품의 취약점을 식별하고 분석한다. ACAS는 Tenable 社의 Nessus 기술을 활용하여 제품을 스캐닝하고 실시간으로 네트워크 트래픽을 모니터링할 수 있다. 사용자는 스캔 결과를 분석하여 효과적인 보안 조치계획을 수립할 수 있다.

4) HBSS

HBSS는 DoD에서 사용하는 호스트 기반 보안 시스템으로, 사용자 단말, 서버 등에서 발생할 수 있는 보안 취약점을 감지한다. HBSS에서 감지할 수 있는 보안 위협에는 악성코드 감염, 무단 액세스 시도 등이 해당하며, 사용자는 감지된 보안 위협으로부터 공격을 방어할 수 있다.

5) CMRS

CMRS는 조직 내의 보안 위협과 취약점을 지속해서 모니터링하고 위험 평가 및 점수화하는 소프트웨어이다. CMRS에서는 위협 인텔리전스(Threat Intelligence) 기능을 활용하여 사이버 공격자의 의도와 목적을 분석하고 이를 바탕으로 위험 수준을 결정한다. 사용자는 CMRS에서 실시간으로 평가한 보안 상태를 활용하여 관리자가

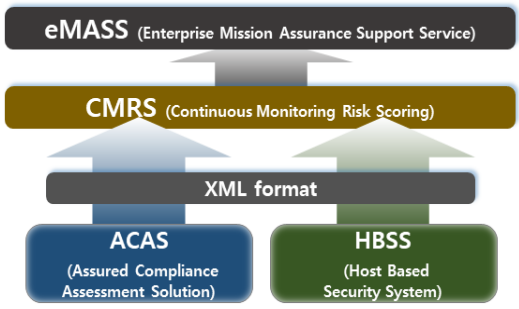


Fig. 3. Monitoring process

적절한 보안 조치를 취할 수 있도록 정보를 제공하고 분석 결과를 eMASS에 업로드한다.

### 3.4 기타 자동화 도구

DISA에서 제공하는 보안 자동화 도구들은 DoD RMF의 각 단계에서 효과적으로 활용될 수 있다. SCC와 OpenSCAP을 사용하면 시스템에 구현된 보안통제항목이 기준에 부합한 지를 검증할 수 있으며, STIG Viewer를 사용하여 평가 결과를 분석할 수 있다. ACAS와 HBSS를 활용하여 식별된 위험 요소들을 분석할 수 있고, 시스템의 전반적인 보안 상태에 대한 승인 결정을 내리거나 보안 취약점과 위협을 지속적으로 모니터링하는 데 활용할 수 있다. 이러한 도구들은 객관적인 분석 지표를 제공하므로 DoD RMF 단계별 효율성을 향상할 수 있다.

DISA에서 DoD RMF 관련 기관을 대상으로 자동화 도구를 배포하고 있었다면 근래 위험관리의 중요성이 증가함에 따라 DoD RMF나 NIST RMF를 적용하는 기관에서도 IT 제품의 보안 평가를 자동화하기 위한 도구를 적용하고 있다. 이러한 도구들은 NIST RMF뿐 아니라 보안 프로세스 효율화 및 일관된 보안 환경 조성 목적으로 활용할 수 있다.

1) Xacta 360

Xacta 360은 Teals 社에서 개발한 보안 관리 도구로 군 환경뿐 아니라 기업, 클라우드 및 하이브리드 환경에서 폭넓게 사용된다. eMASS와 유사하게 NIST RMF 전 단계에서 활용될 수 있으며 보안 위험 평가, 관리, 문서화 절차를 자동화하는데 탁월하다.

2) OpenRMF

OpenRMF는 DISA의 체크리스트를 활용하여 NIST RMF 전반을 관리하는 도구이다. 보안 설정과 정책의 구

Table 2. List of security automation tools

| Manufacturer | Software | Price | RMF process |
|---|---|---|---|
| DoD/DISA | SCC | - | Implement, Assess |
| | OpenSCAP | - | |
| | STIG Viewer | - | |
| Soteria Software | OpenRMF Professional | $247,477.77 (1 PC/Year) | Implement, Assess |
| Splunk | Splunk | $70,176<br>*Variation based on usage | Assess, Monitor |
| RSA | RSA Archer A&A | $14,000 (1 PC/Year) | Assess, Authorize |
| Telos | Xacta 360 | $76,800 (10 Project) | All |
| Rapid7 | Rapid7 InsightVM | $7.34 (hourly) | Assess, Monitor |

현을 검증하고, NIST RMF 관련 문서와 보고서를 생성하는 과정을 간소화할 수 있어 구현 및 평가 단계에서 활용할 수 있다. 다만, 무료 버전의 경우 입력 데이터의 수가 제한된다.

3) Splunk

Splunk는 데이터 로그와 서버 활동을 분석하여 NIST RMF의 평가 및 모니터링 단계에서 요구되는 컴플라이언스를 지원하는 도구이다. 실시간으로 데이터를 분석하여 보안 위협을 식별하고, 로그 데이터를 처리하는 데 활용할 수 있으나, 사용량에 따라 가격이 상이하다.

4) RSA Archer A&A

RSA Archer A&A(Assessment and Authorization)는 다양한 정보시스템 전반에 대한 컴플라이언스 및 위험관리를 지원하는 도구이다. 정보시스템의 위험 평가 결과를 점수화하고 위험 등급을 결정할 수 있어 평가 단계 이후 활용할 수 있다.

## 4. K-RMF 보안 점검 방향

DoD RMF 보안 자동화 도구들은 대체로 보안통제항목의 구현, 평가, 모니터링 단계에서 보안 위험을 감소시키고 규격을 준수하였음을 보장하는 객관적인 기준을 제공할 수 있다. 한국에서도 K-RMF 제도의 원활한 정착을 위하여 보안 기능을 점검하는 방안을 연구 중이지만, K-RMF 제도의 적용 대상은 IT를 포함하는 군 정보시스템으로 한정하며 공개된 문서로부터 확인 가능한 사실이 많지 않은 관계로 DoD RMF에서 사용 중인 보안 자동화 도구를 가져다 바로 도입하는 데에는 어려움이 있다. 다만 국내 연구 결과 중 보안 기능 점검 자동화를 위하여 SCAP을 분석한 연구 사례가 있으므로, 이를 활용하여 향후 K-RMF 보안 점검을 수행하는 방향을 제시하려 한다[16-18].

[16]에서는 정보보호 및 개인정보보호 관리체계(ISMS-P, Information Security Management System-P)에서 제시한 보안 평가 기준을 활용하여 서버 보안 평가를 자동화하는 방안을 연구하였다. [17]에서는 Red Hat 8 STIG 파일을 활용하여 국내 보안 평가체제 관련 항목을 선별하고 보안 자동화 도구에 적용하였다. [16]과 [17] 모두 대상별 기술적 구현이 요구되는 보안 기능을 도출하는 절차의 중요성을 강조하였는데, 이를 위해 향후 보안 평가 기준을 세분화하여 체크리스트로 활용하기 위한 연구가 요구된다.

[18]에서는 공공기관 정보시스템을 대상으로 SCAP을 활용하기 위한 세 가지 방안을 제시하였다. 보안 설정을 SCAP 기반 점검 항목으로 작성하는 방법, 보안 요구사항과 보안 설정을 매핑시키는 방법, 취약점을 효과적으로 평가할 수 있는 체계를 구축하는 방법이 있으며 이를 국내 공공기관에 적용하기 위해서는 K-SCAP을 개발하여 상시 점검체계를 구축해야 한다. 다만 이를 국내 공공기관에 적용하기 위해서는 국외 공공분야를 대상으로 하는 평가제도에 관한 연구가 선행되어야 하며, K-RMF 보안통제항목 또한 DoD RMF 제도를 채택한 나라들의 사례를 검토하는 절차가 필요하다는 점을 확인할 수 있었다.

기존 연구 결과를 통해 K-RMF 보안 점검 절차에 DoD RMF와 같은 보안 자동화 도구를 도입하기 위해서는 미국과 한국에서 사용 중인 보안 정책 간 연계성을 분석하고 기술적으로 구현 결과를 점검할 수 있는 항목을

도출해야 함을 확인하였다. 도출된 기술적 항목은 체크리스트 형태로 세부적으로 작성되어야 하며 점검 결과는 NIST SP 800-53 항목과 연계하여 보안통제항목별 보안성을 검증하는 목적으로 활용할 수 있다. 다만 기술적 항목으로 분류되지 못한 보안통제항목의 검증 방안의 연구가 별도로 진행되어야 하며, K-RMF용 eMASS 프로그램이 개발된다면 보안 자동화 도구의 산출물을 등록할 수 있는 절차까지 고려해봐야 한다. 또한, 기존 연구 결과에서는 취약점 모니터링보다 컴플라이언스 진단에 비중을 두고 있으므로 K-RMF 모니터링 업무에 적용하기 위한 취약점 진단 도구에 관한 추가 연구가 진행되어야 하며 향후 환경 및 제도의 발전 과정에서도 적절한 방향으로 최신화될 수 있도록 주기적으로 관리 및 업데이트할 수 있어야 한다.

## 5. 결론

본 논문에서는 K-RMF 구현 이후 단계를 구체화하기 위하여 DoD RMF에서 활용 중인 보안 자동화 도구에 관하여 살펴보았으며, 이를 K-RMF 보안통제항목 보안 점검 절차에 접목하는 방안을 고려해보았다. DoD RMF 제도에서 활용되는 보안 자동화 도구는 제품별 체크리스트를 활용하여 구현 수준을 진단하는 컴플라이언스 자동화 도구와 운용 중 주기적으로 취약점을 분석할 수 있는 취약점 자동화 도구로 구분할 수 있다. 사용자는 DoD RMF 적용 대상에서 사용 가능한 자동화 도구 및 체크리스트 파일을 활용하여 보안 점검 절차를 간소화하고, 평가 결과의 객관성을 확보할 수 있다.

K-RMF 제도는 NIST RMF 제도를 한국군 환경에 맞게 벤치마킹한 제도로, 시스템 수명주기와 연계하여 보안을 내재화할 수 있다. 현재 국내에서 사용 중인 보안측정 및 방산기술보호 통합실태조사는 모두 보안성이 취약한 요인을 진단하고 보안 기술을 보호하기 위한 대책을 수립하는 제도로, K-RMF 보안 점검에 적용하기 위해서는 보안 기능 단위의 적절성을 판단할 수 있는 보안 자동화 도구가 추가로 개발되어야 한다. DoD RMF 자동화 도구 기능 및 국내 관련 연구 결과를 통해 K-RMF 보안 자동화 도구 적용을 위해서는 보안 기능 세분화 및 관련 규정의 연구가 선행되어야 하며, 추후 DoD RMF에서 사용 중인 자동화 도구의 활용 범위를 토대로 K-RMF에 적용하기 위한 도구를 식별하고 체크리스트를 개발하는 연구가 진행되어야 할 것이다.

## References


[1] "In 2023, domestic public institutions received an average of 1.62 million cyberattacks per day", Boannews, Retrived from: http://www.boannews.com/media/view.asp?idx=126047

[2] "2021-2023, maximum DDoS attacks explode by more than 100% each year", Boannews, Retrived from: http://www.boannews.com/media/view.asp?idx=126201

[3] "Cyber Attack on Public Data Surges…40% increase in government agencies, 95% increase in legal practice", Global Trend & Technology (GTT KOREA), Retrived from: https://www.gttkorea.com/news/articleView.html?idxno=8481

[4] "It will be added to cyber, cryptography, electromagnetic waves, satellites, and military security", Boannews, Retrived from: https://www.boannews.com/media/view.asp?idx=111603

[5] "National Security Office Establishes 'National Cyber Security Strategy' Of Yoon Suk Yeol Government", Retrived from: https://www.president.go.kr/newsroom/press/gdXzwtKB

[6] "Policy and technical support is urgently needed to settle the Korean RMF early", Gukbangnews, Retrived from: https://www.gukbangnews.com/news/articleView.html?idxno=6437

[7] "Risk Management Framework (RMF) for DoD Information Technology (IT)" DoDI 8510.01, Mar.2014

[8] "Guide for Conducting Risk Assessment," NIST SP 800-30 Rev.1, Sep.2012

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

[10] "Security Categorization and Control Selection for National Security Systems", CNSSI 1253, Mar.2014

[11] "Defense Counterintelligence and Security Agency Assessment and Authorization Process Manual", Ver.2.1, Mar.2020

[12] J. Kim and S. Jeong., "The first step toward the success of the Korean risk management framework (KRMF): System Classification Orientation Study," Journal of Advances in Military Studies, vol. 5, no. 2, pp. 73-106, Aug. 2022. DOI: https://doi.org/10.37944/jams.v5i2.151

[13] G. Jeong, K. Kim, S. Yoon, D. Shin, and J. Kang., Exploring Effective Approaches to the Risk Management Framework (RMF) in the Republic of Korea: A Study. Information. 2023; 14(10):561. DOI: https://doi.org/10.3390/info14100561

[14] W. Yang, S. Cha, J. Yoon, H. Kwon, and J. Yoo., "Korean Security Risk Management Framework for the Application of Defense Acquisition System," Journal of the Korea Institute of Information Security & Cryptology, vol. 32, no. 6, pp. 1183-1192, Dec. 2022. DOI: https://doi.org/10.13089/JKIISC.2022.32.6.1183

[15] "The Technical Specification for the Security Content Automation Protocol", NIST SP 800-126, Feb.2018

[16] D. Shin and S. Kim, "SCAP Applicability for Vulnerability Management of Server-Oriented System," Journal of Information Technology Applications and Management, vol. 26, no. 4, pp. 19-30, Aug. 2019.
DOI: https://doi.org/10.21219/jitam.2019.26.4.019

[17] S. Kim, H. Park, and H. Ahn., "A Study on the Classification of OVAL Definitions for the Application of SCAP to the Korea Security Evaluation System," Korean Institute of Smart Media, vol. 11, no. 3. Korean Institute of Smart Media, vol. 11, no. 3, pp. 54-61, Apr. 2022.
DOI: https://doi.org/10.30693/SMJ.2022.11.3.54

[18] Y. Jee, Y. Lee, D. Yoon, and Y. Shin., "A Study on the Improvement of Information Security Management Condition Evaluation in Public Sector through the SCAP Analysis by NIST in U.S.," Journal of Information Technology Applications and Management, vol. 26, no. 4, pp. 31-39, Aug. 2019.
DOI: https://doi.org/10.21219/jitam.2019.26.4.031

최 은 진(Eun-Jin Choi) [정회원]

- 2019년 2월 : 한국기술교육대학교 컴퓨터공학부(공학사)
- 2021년 2월 : 성균관대학교 전자전기컴퓨터공학과(공학석사)
- 2022년 7월 ~ 현재 : 국방기술품질원(DTaQ) 연구원

〈관심분야〉
국방품질경영, 사이버보안, K-RMF

노 승 일(Seungil Noh) [정회원]

- 2019년 8월 : 광운대학교 수학과(이학사)
- 2023년 8월 : 고려대학교 정보보호대학원 정보보호학과(정보보호학 석사)
- 2023년 7월 ~ 현재 : 국방기술품질원(DTaQ) 연구원

〈관심분야〉
국방품질경영, 사이버보안, K-RMF