정 보 보 호 학 회 지
제 33 권 제6호, 2023. 12

원자력 시설 취약점 정량화 평가체계 적용 방안 연구

김 가 경*, 윤 성 수*, 김 도 연*, 엄 익 채*

요 약

2023년 10월, 공통 취약점 평가체계의 신규 버전이 8년 만에 출시되었다. 공통 취약점 평가체계는 취약점의 심각도 점수 및 특성 정보를 제공하는 시스템으로, 취약점 관리활동의 바로미터로 활용되고 있다. 그러나 기존 공통 취약점 평가체계의 점수는 기반 시설에서의 실제 취약점 악용 가능성과의 불일치 및 운영 환경의 특성을 반영하지 못하는 한계점이 존재한다. 본 연구에서는 미국 등을 비롯한 국외 기반시설의 취약점 정량화 평가체계 선행 연구 및 적용 현황등을 분석하고, 이번에 신규 출시된 공통취약점 평가체계의 주요한 변경사항을 다룬다. 더불어 국내 원자력 시설의 운영 특성을 반영하여 개발되고 있는 취약점 정량화 평가시스템에 대해 소개한다.

Ⅰ. 서 론

2023년 10월 말, 공통 취약점 평가체계의 신규 버전이 게시되었다. 공통 취약점 평가체계는 산업 내 가장 보편적으로 활용되어 온 취약점 평가 시스템으로, 취약점의 위험이 아닌 심각도를 평가한다는 것에 초점을 두고 있다. 이러한 점에 기인하여 공통 취약점 평가체계에 따른 취약점 심각도 점수는 실제 취약점 악용 가능성이나 조직 특성에 따른 보안 영향을 반영하지 못한다.

최근 러시아-우크라이나 사이버전, 덴마크 에너지 기반시설 관련 기업 22곳이 사이버 위협을 받는 등 기반시설을 표적으로 하는 사이버 공격이 발생하고 있다. 기반시설은 특성상 사이버 위협으로 인한 피해는 전사회적으로 확산된다.

근무 환경의 디지털화, 전쟁 발발 등의 시점을 기준으로 기반시설을 타깃으로 하는 취약점 식별 건수가 증가하고 있어, 고도화된 취약점 대응체계가 필요한 시점이다.

따라서 본 연구에서는 국내외 기반시설 취약점을 관리하기 위한 동향을 조사하고, 결과적으로는 기반시설 취약점 대응 체계의 방향을 제시하고자 한다.

Ⅱ. 사이버 취약점 정보원 분석

본 절에서는 사이버 취약점 평가체계를 분석하기 위하여, 가장 보편화되어 사용되고 있는 관련 취약점 정보원들을 선정하고 취약점 정보원 간의 관계를 분석하였다.

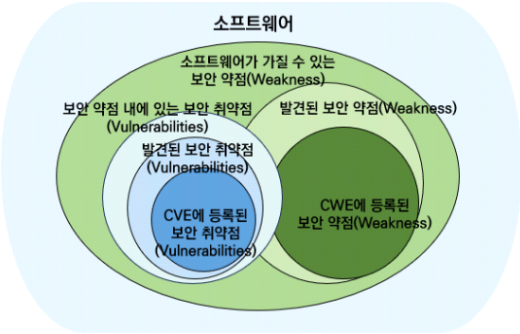
2.1. 취약점 정보원 선정 및 관계 분석

시스템에 존재하는 취약 구성 요소는 취약점 정보로 문서화할 수 있다. 취약한 시스템을 식별하기 위한 체계로 공통 플랫폼 정보(Common Platform Enumeration, CPE)를 활용할 수 있으며, 취약점 정보로는 NVD(National Vulnerability Database) 내 공개 취약점 정보(Common Vulnerability abd Expousere, CVE)를 활용할 수 있다. 따라서 CPE 정보의 취약 시스템 기반의 CVE 정보가 생성된다.

MITRE는 보안 약점을 특정 상황에서 취약점 발생에 기여할 수 있는 소프트웨어, 펌웨어, 하드웨어 또는 서비스 구성 요소의 상태라고 정의한다. 즉, 보안 약점은 보안 취약점이 될 수 있지만, 보안 약점이 존재하지 않는다면 보안 취약점은 존재할 수 없다. 따라서 보안 취약점보다 보안 약점이 더 포괄적인 범위이다. 보안 약점으로는 공개 보안 약점 정보(Common Weakness

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단 지원(No.2022R1G1A1010506)을 받아 수행한 연구결과입니다.

* 전남대학교 시스템보안연구센터(대학원생, kkk110306002@jnu.ac.kr, 대학원생, skymoonight@jnu.ac.kr, 대학원생, ehdus928@jnu.ac.kr, 부교수, iceuom@jnu.ac.kr)



〔그림 1〕 보안 약점과 보안 취약점 관계 분석

Enumeration, CWE)를 활용할 수 있다. 보안 약점과 보안 취약점 간의 관계는 [그림 1]과 같다.

공개 취약점 정보의 특성에 따라 취약점 정량적 심각도 점수를 측정할 수 있다. 취약점 정량적 심각도 점수를 측정하는 시스템은 공통 취약점 평가체계(Common Vulnerability Scoring System, CVSS)를 활용할 수 있다. 다만 신규 취약점 정보에 대하여는 심각도 점수가 측정되기 전의 기간이 존재하기에, CVE와 CVSS의 관계는 완전히 일치하지 않는다고 판단한다.

2.2. 공통 플랫폼 정보

공통 플랫폼 정보는 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)에서 제안한 SCAP(Security Content Automation Protocol)5의 일부로, 조직의 컴퓨터 리소스를 구성하는 IT 제품 및 플랫폼의 이름을 식별하고 문서화하기 표준 형식이다.

CPE 정보를 나타내는 규칙은 'cpe:/<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>' 으로 사용한다. 현재 NVD 내 공개 취약점 정보에 포함되어 함께 제공되고 있다.

CPE 표기 형식의 세부 내용은 [표 1]과 같다.

2.3. 공개 보안 약점 정보

2006년 MITRE는 보안 약점 정보를 처음 게시하였다. 초기에는 소프트웨어 약점에만 중점을 두었지만, 최근 산업제어시스템 및 의료 기기 등 하드웨어의 보안 문제가 IT, OT, IoT 영역에서 중요시 되면서 2020년부터는 하드웨어에 대한 약점 정보를 추가하여 제공하고 있다.

〔표 1〕 CPE 표기 형식

형식	설명
part	검색된 시스템의 종류 (하드웨어(h), 운영체제(o), 애플리케이션(a))
vendor	제품 제조사명
product	제품명
version	제품 버전 번호
update	제품 업데이트 나열
edition	소프트웨어 버전
language	식별된 언어

CWE 정보에는 'CWE-(단순 할당 고유 번호) : 약점 설명' 형식의 고유의 ID가 할당된다. 공개되는 CWE 정보에는 이름, 설명, 관련 CWE 정보, 플랫폼, 악용 결과, 관련 CVE 정보, 잠재적으로 완화가능한 방안, 참고 자료 등으로 구성된다.

2.4. 공개 취약점 정보

공개 취약점 정보는 MITRE Coperation이 제공하는 보안 취약점 식별, 정의 및 분류 정보이다. 미국 국립표준기술연구소의 NVD는 CVE 정보를 즉시 동기화하여 제공하고 있다.

CVE는 2002년 처음 출시되었으며, 2004년 DISA (Defense Information Systems Agency) 는 CVE ID를 사용하는 제품을 사용하여야 하는 정보보증 애플리케이션에 대한 작업 명령을 발표하였다. 2011년에는 국제전기통신연합(ITU-T)은 ITU-T X.1520 CVE 권장 문서를 발행하였으며, NIST 또한 CVE 사용을 권장하는 NIST SP 800-51을 발행하였다. 현재는 가장 보편화되어 사이버 보안 관리의 기반이 된 취약점 정보원이다.

CVE 정보에는 CNA(CVE 번호 부여 기관)에 의해 고유한 식별 번호가 생성되어 관리되고 있다. 'CVE-(연도)-(순서)'라는 규칙을 가진다. 공개되는 CVE 정보에는 취약점 설명, 심각도 점수, 관련 참조 링크, 관련 CWE 정보, 관련 CPE 정보, 게시 및 수정 날짜, 출처 등으로 구성된다.

최근 10년 동안 식별된 CVE 건수는 아래 그림과 같다. 점차 취약점 식별 건수가 증가하는 추세이며, 2023년 3분기까지는 21,085건의 취약점이 식별되어 NVD에 공개되었다.

2.5 공통 취약점 평가체계

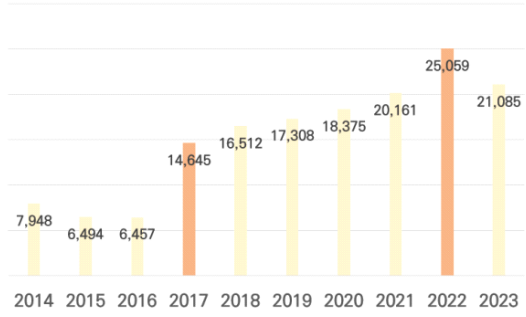
공통 취약점 평가체계는 FIRST(Forum of Incident Response and Security Team)에 의해 2005년 처음 게시된 취약점의 특성과 심각도를 전달하기 위한 개방형 프레임워크이다. 취약점의 심각도 및 영향을 논의할 수 있는 공통 기준을 장려하기 위한 궁극적인 목적으로 제안되었다.

FIRST에 의한 취약점은 기밀성, 무결성, 가용성의 묵시적 또는 명시적 실패로 이어질 수 있는 애플리케이션, 시스템, 장치 또는 서비스 내의 버그, 결함, 동작, 출력, 결과 또는 이벤트로 정의된다.

취약점 심각도 및 영향을 평가하는 해당 체계는 2005년 CVSS v1.0을 시작으로, 2007년 v2.0 개정, 2015년 v3.0 개정, 2019년 v3.1 개정, 2023년 v4.0 개정이 이루어졌다. 주요 개정 원인 및 배경, 지표 변화는 [그림 3]와 [표 2]과 같다.

주요 기반시설에서는 측정된 심각도 점수가 '7.0' 이상인 취약점을 우선적으로 대응하고 있다. 그러나 CVSS v3.0 개정 이후로는, 심각도 점수가 7.0 이상인 취약점이 다수의 비중을 차지한다.

심각도 점수가 7.0 이상인 모든 취약점을 대응하는 것은 매우 비효율적이며, 현실적인 어려움도 존재한다. 또한 심각도 점수가 높다고 해서 무조건적으로 악용되



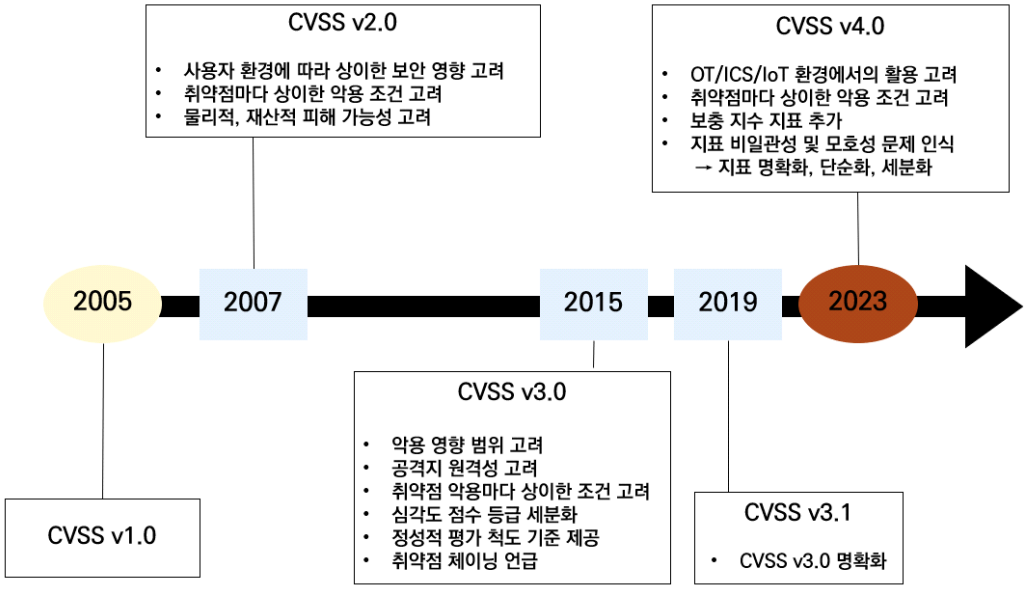
〔그림 2〕 연도별 CVE 식별 건수

는 것이 아니며, 반대의 경우에도 악용될 가능성이 존재한다.[24]

가용성이 중시되는 기반시설의 경우 즉각적인 취약점 제거가 어렵다. 효율적인 취약점 대응을 위하여는 기반시설의 특성을 반영한 특화된 취약점 정량화 평가체계가 필요하다. 다음 절에서는 산업별 제안된 취약점 평가체계를 분석하고자 한다.

Ⅲ. 산업별 사이버 취약점 평가체계 분석

본 절에서는 산업별 취약점 평가체계 활용 상황을 분석하기 위하여 제조[14], 로봇[15], 방위[16], 건설[17], 자동차[18], 의료[19], 금융[20], 내부망[21], 클



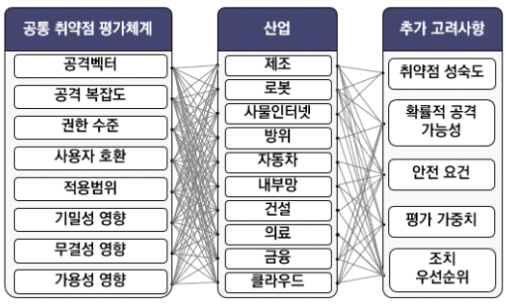
〔그림 3〕 CVSS 개정 원인 및 배경 분석

〔표 2〕 공통 취약점 평가체계 개정에 따른 지표 변화 비교

CVSS v1.0		CVSS v2.0		CVSS v3.0(1)			CVSS v4.0	
기본 지수	영향 편향	기본 지수	공격 벡터	기본 지수	악용 가능성	공격 벡터	기본 지수	공격 벡터
	공격 복잡성		공격 복잡성			공격 복잡성		공격 복잡성
	인증		인증			필수 권한		공격 요구사항
	공격 벡터		기밀성			사용자 상호작용		필수 권한
	기밀성		무결성		영향	기밀성		사용자 상호작용
	무결성		가용성			무결성	위협 지수	악용 성숙도
	가용성	시간 지수	악용가능성			가용성		
시간 지수	악용가능성		교정 수준		범위		환경 지수	수정된 기본지수
	교정 수준		보고 신뢰도					기밀성 요구사항
	보고 신뢰도	환경 지수	부수적 피해 가능성	시간 지수	악용 코드 성숙도			무결성 요구사항
환경 지수	부수적 피해 가능성		대상 분포		교정 수준			가용성 요구사항
	대상 분포		기밀성 요구사항		보고 신뢰도		보충 지수	자동화
			무결성 요구사항	환경 지수	수정된 기본지수			회복
			가용성 요구사항		기밀성 요구사항			안전성
					무결성 요구사항			값 밀도
					가용성 요구사항			취약점 대응 노력
								공급자 긴급성

라우드 산업[21], 사물인터넷[22]을 대상으로 하는 관련 연구들을 조사하였다. 공통 취약점 평가체계 지표와 추가 고려사항을 연결하여 [그림 4]와 같이 나타내었다.

[14]~[22]에서 제안한 산업별 취약점 평가체계 지표를 분석하였다. 대부분 공통 취약점 평가체계를 활용하고 있었으나, 활용하지 않는 산업도 존재하였으며 이를 구분한 세부 내용은 [표 3]과 같다.



〔그림 4〕 산업별 취약점 평가체계 지표 분석

산업별 취약점 평가 목적에 따라 추가적인 접목 기술이 존재하였다. 접목 기술에 따른 목적을 분석한 결과는 [표 4]와 같다.

또한 산업별 중시하는 보안 요소에 따라 특화된 추

〔표 3〕 산업별 접목 기술 및 목적 분석

산업	접목 기술	목적
제조	-	영향성
로봇	-	안전성
방위	CWSS	취약점 대응
사물인터넷	Baysian Network	영향성
건설	-	공격자 수준 평가
자동차	HEAVENS Model	안전성
내부망	CWSS	취약점 대응
의료	Logic Tree	영향성
금융	-	영향성
클라우드	Markov Chain	취약점 대응

〔표 4〕 산업별 공통 취약점 평가체계 활용 여부

산업	CVSS v3.1 지표		
	Base Metrics	Temporal Metrics	Environmental Metrics
제조	O	O	O
로봇	O	O	O
방위	O	O	O
사물인터넷	O	O	O
건설	O	X	X
자동차	X	X	X
내부망	O	O	O
의료	O	O	O
금융	X	X	X
클라우드	O	X	X

가적인 지표가 존재하였다. 추가된 지표를 공통 취약점 평가체계의 지수 그룹을 기반으로 기본 점수, 시간 점수, 환경 점수로 구분하였다. 이에 대한 결과는 [표 5]와 [표 6]과 같다.

〔표 5〕 추가 지표 구분

구분	추가 지표
기본 점수	① 취약점 성숙도 ② 안전 영향
시간 점수	③ 내결함성
환경 점수	④ 시스템 가시성 ⑤ 시스템 모니터링 ⑥ 시스템 제어 ⑦ 시스템 영향도 ⑧ 시스템 진행 절차 ⑨ 시스템 지속성 ⑩ 긴급성 ⑪ 자산 가치 ⑫ 취약점 연쇄 작용 ⑬ 시스템 안전성 ⑭ 시스템 조작

〔표 6〕 산업별 공통 취약점 평가체계 활용 여부

산업	추가 지표
제조	②, ④, ⑤, ⑥, ⑦, ⑧, ⑨, ⑬
로봇	①, ②
방위	⑭
사물인터넷	①, ②, ③, ④, ⑩, ⑪, ⑫, ⑬
건설	-
자동차	-
내부망	⑭
의료	-
금융	-
클라우드	-

해당 분석을 통하여 조직의 환경마다 중시되는 보안 요소가 다르며, 공통 취약점 평가체계를 보완하기 위한 접목 기술을 추가적으로 사용하고 있음을 파악할 수 있다. 특히 사람의 안전과 관련있는 산업의 경우 추가적인 안전 지표를 도입하여 활용하고 있었다.

Ⅳ. 기반시설에 적용 가능한 취약점 평가체계 분석

4.1. 원자력 시설 취약점 관련 규제 동향

국내 원자력 시설 사이버 보안 규제 기준인 KINAC/RS-015에서는 주기적으로 원자력 시설에 존재하는 취약점을 식별 및 관리할 것을 요구하고 있다.

최근 개정된 미국 원자력 시설 보안 규제 기준의 R.G 5.71에서는 지난 미국 가동 원전의 전체 사이버 보안 점검의 Lesson Learned를 반영하였는데, 이중에서도 주기적인 취약점 관리를 중요한 인사이트로 언급하고 있으며, 원자력 시설 자산의 취약점 관리에 정량적 지수 적용을 권고하고 있다.

4.2. 미국 원자력 시설 취약점 관리 규제 Lesson Learned

미국 원자력 시설은 2017년분터 2021년까지 57개 시설에 대한 사이버보안 특별검사를 완료하였으며,규제기관인 NRC에서는 취약점 관리에 대해 아래와 같은 Lesson Learned를 도출하였다.

첫째, 취약점 점수가 7.0이하인 취약점 중에서도 방화벽이나 데이터 다이오드, 이동형 저장매체 스캐닝 키오스크등 상속 취약점 악용이 우려되는 설비에 대해서는 4.0 이상이 취약점도 관리할 것을 요구하고 있다.

둘째, 취약점 우선 순위에 대한 기준 변경을 요구하고 있다. 초기에는 단순히 취약점 점수에 의한 조치 우선 순위등을 산출하였지만, 취약점이 존재하는 자산에 존재하는 공격 벡터와 악용가능성등을 판단하여 우선 순위화 할 것을 요구하고 있다.

셋째, 공급망 관리 및 소프트웨어 명세(Software Bill of Material)등을 이용한 아웃소싱되는 필수디지털자산의 취약점 관리를 요구하고 있다.

마지막으로, 데이터 다이오드(일방향 장비)나 키오스크등을 통한 네트워크/이동형 저장매체 통제 활동이 취약점을 완벽히 제거하지 못한다는 점을 제시하여 피수디지털자산단위의 취약점 관리 활동을 강조하고 있다.

4.3. 미국 원자력 시설 사업자의 취약점 관리 활동

대부분의 IT시스템에서는 주기적인 취약점 발견 및 관리를 위해 스캐닝(scanning)을 가장 효율적인 도구로 사용하고 있다.

하지만 원자력 시설 안전계통등의 설비에 스캐닝을 시도할 경우 이상 동작 등을 유발할 수 있는 등의 문제점도 상존한다. 이러한 점을 고려하여 초기 미국 원자력 시설의 사이버 보안 규제 이행 가이드인 NEI 08-09등에서는 취약점 스캐닝등을 국소적으로 권장하고 있었지만, 특별검사를 통하면서 삭제되었다.

미국 원자력 시설 운영 사업자 중의 하나인 TVA(Tennessee Valley Authority)의 자료에 의하면, 해당 사업자가 소유한 필수디지털 자산 중 취약점 스캐닝이 가능한 자산은 10%이하로 간주되고 있다. 이는 원자력 시설등의 기반시설에서는 Active Scanning 보다는 SBom기반의 소프트웨어 컴포넌트 취약점 식별이 보다 유효하다는 점을 시사한다.

더불어 미국 원자력발전협회(Institute of Nuclear Power Operations, INPO)에서는 민간 원자력발전사등이 공통으로 보유하고 있는 필수디지털자산의 취약점 정보를 기반으로 원자력 시설 환경의 특성에 맞게 재평가하는 ALNOTS라는 시스템을 개발하여 운영하고 있다.

이 시스템을 통해 대부분 원자력 시설 사업자가 공통으로 보유한 필수디지털자산에 대한 취약점 평가 시간을 절감하는 장점이 있다. 하지만 네트워크 기반의 공격벡터 유무로 폐쇄망으로 운영되고 있는 원자력 시설 자산의 취약점 점수를 낮추는 방식이어서 규제 관점에서는 적합하지 않다.

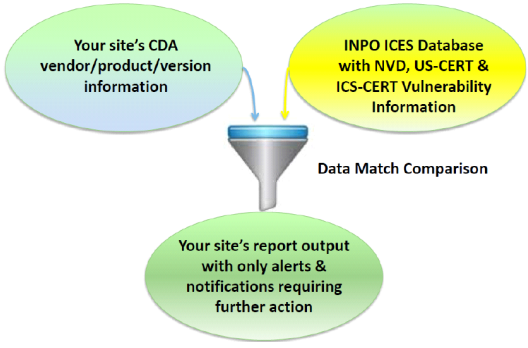
4.4. EPSS(Exploit Prediction Scoring System)

EPSS는 취약점이 실제로 악용될 가능성을 예측하여 제공하는 시스템이다. 2019년 Blackhat에서 처음 발표한 후, 2021년 FIRST가 첫 시스템을 게시하였다.

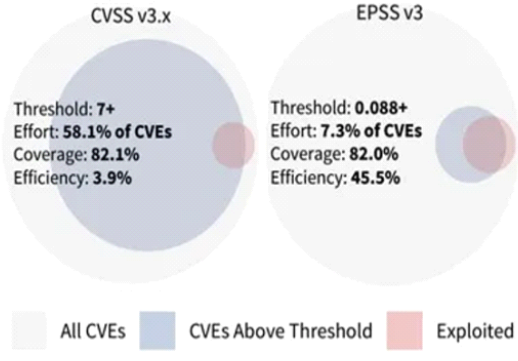
데이터 소스를 기반으로 향후 30일 이내 실제 악용될 가능성을 추정하며, 이 가능성을 'EPSS Score'라고 칭한다. 익스플로잇 코드, 웹사이트나 소셜 미디어 언급, 보안 스캐너, CVE, NVD, CVSS, CWE 등의 데이터 소스 수집하여, 하이퍼 파라미터 값을 설정하고 XGBOOST 알고리즘에 적용시키어 취약점 악용 가능성을 추정한다.

현재 공개된 모든 CVE에 대한 EPSS Score를 생성하여 제공하고 있다. 0에서 1(0~100%)사이의 확률 점수를 생성하며, 점수가 높을수록 취약점 악용 가능성이 높다는 것을 의미한다.

[25]에 따른 [그림 5]는, CVSS v3.x만 사용하였을 때는 커버리지 82.1%와 효율성 3.9%지만, EPSS v3을 사용하였을 때는 커버리지 82%와 효율성 45%로 측정된 것을 나타낸다. 커버리지(Coverage)는 실제 악용된 취약점 수 대비 대응하여 악용을 예측할 수 있었던 취약점 수의 비율이다. 효율성(Efficiency)은 임계값



〔그림 5〕 ALNOTS 시스템 알림 구조



〔그림 6〕 CVSS-EPSS 비교[25]

(Threshold) 점수 이상의 취약점 수 대비 실제 악용된 취약점 수의 비율이다. 해당 연구는 EPSS를 사용함으로써 유사한 커버리지 상에서 취약점 대응 효율성은 약 11배 이상 증가한 것을 입증하였다.

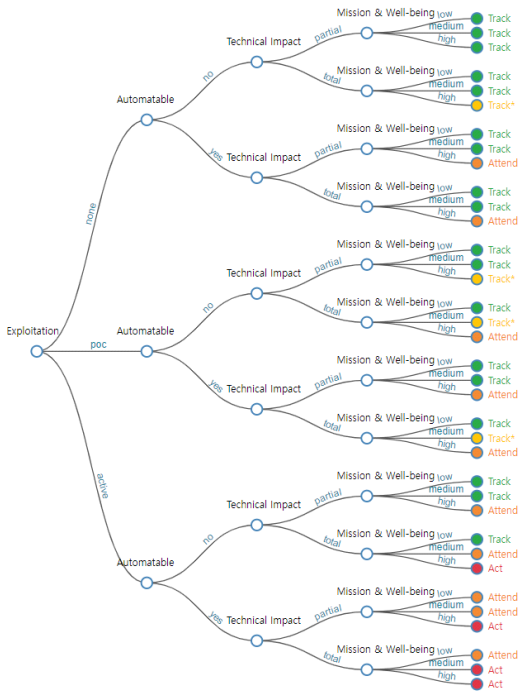
이처럼 EPSS의 점수가 곧바로 위험 점수로 직결되지는 않지만, CVSS를 보완하여 취약점 관리의 효율성을 돕는 하나의 구성요소로 활용 가능할 것이다.

4.5. SSVC(Stakeholder-Specifiv Vulnerability Categorization)

SSVC는 카네기 멜론 대학(Carnegie Mellon University)의 소프트웨어 엔지니어링 연구소에서 CISA(Cybersecurity Infrastructure Secutiry Agency)와 협력하여 개발한 이해관계자 관점에 따른 취약점 분류 프레임워크이다.

이 프레임워크에서는 시스템 개발자, 공급자, 조정자 3가지 역할에 따른 취약점 우선순위 판단을 위한 의사 결정 트리를 제공한다.

CVSS 점수의 정적 특성이라는 한계점을 보완하기 위하여, 취약점 관리자의 입장에서 시간적, 운영적 맥락을 고려하기 위한 목적으로 개발되었다.



〔그림 7〕 CISA-SSVC 의사 결정 트리

이후 2020년 CISA에서는 정부 관점의 맞춤형 의사결정 트리를 개발하였다. CISA의 의사 결정 트리는 '악용 현황(Exploitation status), 기술적 영향(Technical impact), 자동화 여부(Automatable), 자산 임무 중요도(Mission prevalence), 공공 복지에 미치는 영향(Public well-being impact)' 5가지 지표 값을 기반으로 '빠른 시일 내 조치 필요(Act), 기존 표준 계획보다 빠른 조치 필요(Attend), 주의깊은 모니터링 필요(Track*), 표준 계획대로 취약점 관리(Track)' 의 4가지 시급성을 판단할 수 있도록 한다.

Ⅴ. 필수디지털자산 취약점 분석 시스템 구축

기반시설의 효율적인 취약점 대응을 위하여는 특화된 필수디지털자산 취약점 정보 제공 시스템이 필요하다. 본 연구에서는 취약 자산 식별 체계에 따라, 필수디지털자산에 존재하는 취약점 정보를 관련 사업자에게 제공할 수 있도록 하는 데이터베이스 시스템(Nuclear Vulnerability Assessment System, NVAS)을 [그림 8]과 같이 구축하였다.

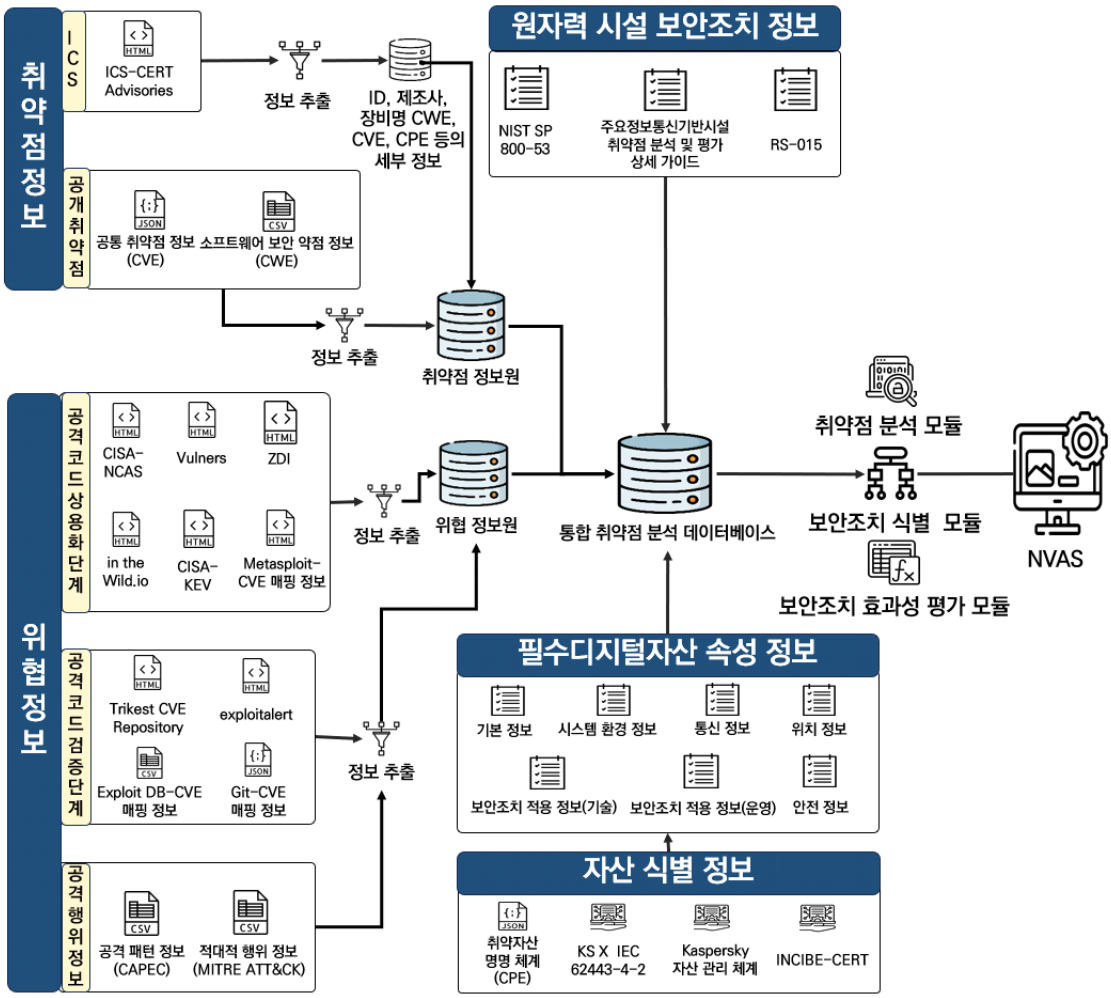
구축한 데이터베이스 시스템은 웹페이지 UI를 통하여 사용자에게 제공하는 것을 목적으로 한다.

5.1. 시스템 개발 환경 구성

구축한 데이터베이스 시스템은 웹페이지 UI를 통하여 사용자에게 제공하는 것을 목적으로 한다. 이에 해당 시스템 개발에 사용한 프레임 워크는 Django, MySQL, Python, HTML/CSS 등이며, 세부 내용은 [표 7]과 같다.

〔표 7〕 시스템 개발 프레임워크

분류	기술	설명
웹	Django	Python 기반 오픈 소스 웹 프레임워크
DB	MySQL	오픈 소스 관계형 데이터베이스 관리 시스템
개발언어	Python	Python, SQL
	HTML/CSS	HTML, CSS, Java Script



〔그림 8〕 NVAS 시스템 데이터베이스 구축 흐름도

5.2. 필수디지털자산 취약점 및 위협정보 수집

필수디지털자산에 대한 취약점 평가 및 보안조치 식별을 위해 다양한 성격의 정보원으로부터 데이터를 수집한다. 수집 정보원으로는 산업제어시스템 환경에서의 취약점 정보원을 포함한 취약점 정보원 4건, 실제 환경에서 악용되어지는 0-day 취약점, in-the-wild 취약점 정보 등을 포함한 위협 정보원 12건, 사이버 보안조치 정보원 3건 등이 존재한다.

해당되는 정보원에서 데이터를 수집하기 위해 Python의 크롤링 모듈인 Selenium과 BeautifulSoup를 활용하였다. 또한 수집되는 정보는 제공되는 데이터에 따라 특정되도록 모듈화 하였다. 이에 대한 흐름도를 [그림 8]에 나타내었으며, 정보원 별 수집된 세부 규모는 [표 8]과 같다.

〔표 8〕 수집 정보자원 규모

분류	정보자원명	개수(건)
취약점 정보	〔CISA〕 ICS-CERT	2,072
	CVE	219,471
	CWE	935
	CPE	735,646
위협정보	CAPEC	561
	MITRE ATT&CK	607
	Exploit DB	33,773

	Github	5,621
	〔CISA〕 Known Exploited Vulnerabilities(KEV)	1,042
	〔CISA〕 National Cyber Awareness System(NCAS)	262
	Metasploit	5,282
	Zero-day Initiative	11,906
	Vulners	1,419
	inthewild.io	95,217
	Trickest CVE Repository	5,621
	exploitalert	38,470
보안조치 정보	RS-015	101
	NIST SP 800-53	303
	주요정보통신기반시설 기술적 취약점 분석 및 평가 상세가이드	347

5.3. 필수디지털자산 취약점 재평가

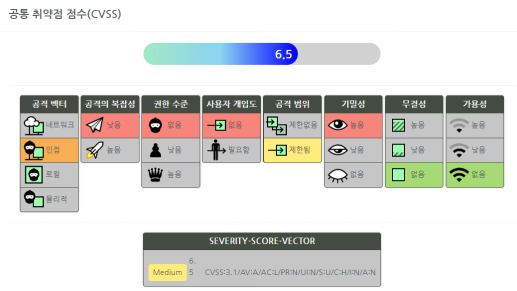
필수디지털자산에 대한 취약점 재평가를 수행하기 위해서는 자산의 특성 및 자산이 위치한 운영 환경을 이해할 필요성이 존재한다. 기존의 평가 기준으로 활용되어지는 CVSS의 평가 속성은 취약점에 대한 특성만을 반영하였기에 필수디지털자산이 위치한 환경의 특성을 반영한 점수라고 보기 어렵다.

〔표 9〕 평가 자산 속성 정보

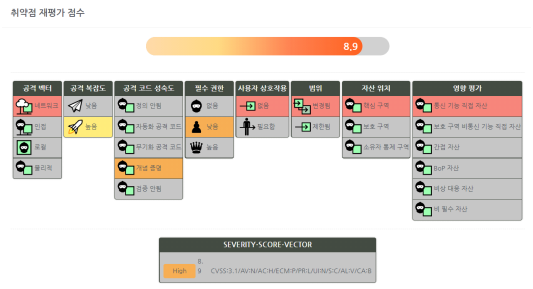
분류	자산 속성
기본 정보	자산 유형
	자산 유형 세부 사항
	제조사/공급자
	자산 등록 명칭
	모델 버전
	HMI 이용 여부
	매체연결 포트 물리적 차단 여부
	유지보수용 기기 연결 포트 물리적 차단 여부
	매체 연결(USB 등) 기능 여부
	유지보수용 연결 기기 사용 여부
통신	통신 연결성
	통신 프로토콜
	통신 인터페이스
	단방향 통신 여부
	무선 통신 활성화 여부
	무선 통신 유형
시스템 환경	애플리케이션 명칭
	애플리케이션 버전
	응용 서비스 이용 여부
	펌웨어 명칭
	펌웨어 버전
	운영체제 명칭
	운영체제 버전
위치	자산의 물리적 위치
	네트워크 보안 계층
보안정책 적용 여부 (기술)	호스트 방화벽 적용 여부
	암호화 통신 여부
보안정책 적용 여부 (정책)	자산 접근권한
	작업 승인 여부
	계정 관리 지원 여부
중요도 평가	Consequence Classification

따라서 이에 대한 한계를 보완하고, 필수디지털자산 속성에 기반한 취약점 평가를 수행하기 위해 자산 속성 정보 31개를 [표 9]와 같이 정의하였다.

또한 기존 CVSS 평가체계에 기반하여 평가 속성에 대한 기준 및 가중치를 개선하여 필수디지털자산에 특화된 취약점 평가 방안을 구성하였다. 이를 시스템에 적용하여 [그림 9], [그림 10]와 같은 결과를 사용자에게 제공한다. [그림 9]의 경우 필수디지털자산 내 기존 취약점인 'CVE-2020-7592'에 대한 CVSS 점수를 나타내며, [그림 10]는 본 연구에서 제시한 취약점 재평가를 수행한 결과를 나타낸다.



〔그림 9〕 'CVE-2020-7592' 취약점 CVSS 기본 점수



〔그림 10〕 'CVE-2020-7592' 취약점 재평가 점수

'CVE-2020-7592' 취약점은 SIMATIC HMI Comfort 패널 기기에서 발견된 취약점으로 연결 기기 간 암호화되지 않은 통신을 통해 평문으로 민감한 정보를 전송한다. 해당 취약점의 기존 평가 점수는 6.5점의 심각도 Medium이며, 재평가된 점수는 8.9점의 심각도 High이다. 이와 같이 재평가된 근거를 분석해보면 [그림 11]과 같다.

'CVE-2020-7592' 취약점은 기존 취약점 평가 결과 인접 네트워크 취약점이자, 공격 복잡도가 낮고, 영향을 받더라도 다른 시스템에 파급력이 없어 낮은 점수로 평가되었다.

하지만 해당 취약점이 발견된 자산의 속성을 반영한 재평가 결과, 해당 취약점에 기반한 악용으로 인해 다른 시스템에 영향을 줄 수 있음을 발견하였다. 또한

〔그림 11〕 'CVE-2020-7592' 취약점 재평가 수행 결과 비교

상위 계층의 네트워크와의 통신 연결이 존재하여 공격 벡터 속성이 가장 치명적인 네트워크로 변경되었다. 더불어 해당 자산이 위치한 곳이 핵심 구역이며, 악용을 위한 공격 코드 성숙도가 PoC로 평가되어 그 시급성이 반영되었다.

5.4. 보안조치 식별 방법론

원자력시설은 필수디지털자산에 대한 취약점 및 보안조치 적용에 대한 지속적인 감시 및 평가가 필요하다. 하지만, 국내 원자력 시설에 대한 취약점 보안조치 검사 결과로 부적절한 항목이 도출되는 등의 지적사항이 존재한다.

이에 해당 시스템은 필수디지털자산에 대한 유효 보안조치를 식별하기 위하여 다음 [그림 12]과 같은 절차를 활용한다.

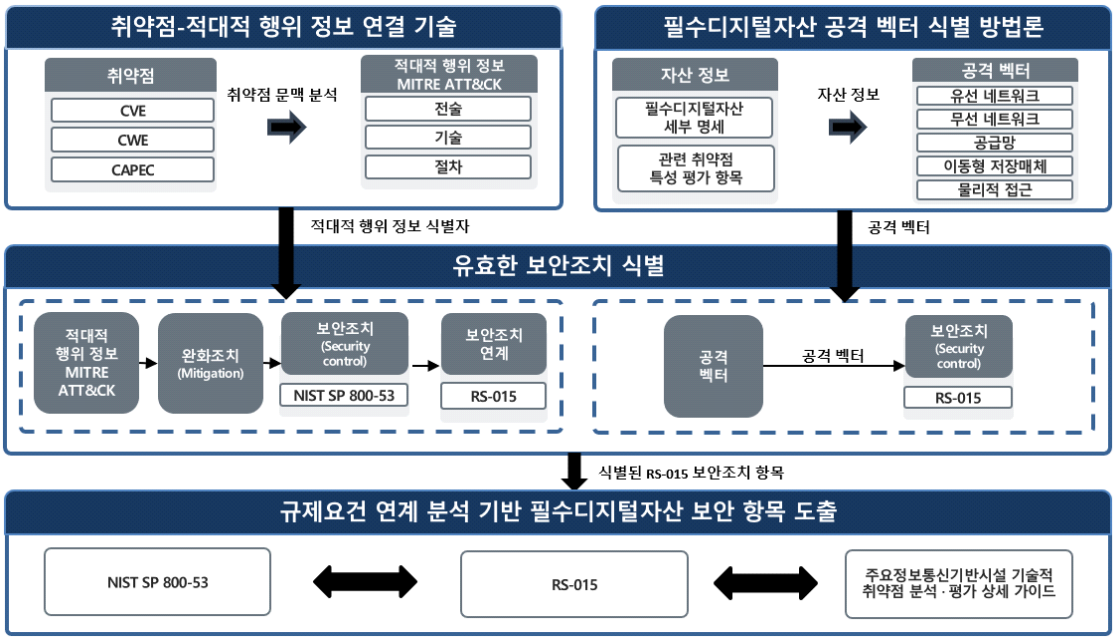
본 방법론은 크게 두 가지로 분류한다. 첫 번째는 취약점 특성을 기반으로 적대적 행위를 연계하고, 이에 따른 보안조치 항목을 식별하는 것이다. 적대적 행위 정보는 MITRE ATT&CK Technique 정보를 활용한다.

이후 MITRE에서 제공하는 Technique - Mitigation-NIST SP 800-53 연계 정보를 활용하여, 한국원자력통제기술원(KINAC)에서 개발한 원자력 시설 보안 규제로 최종 보안조치인 RS-015와의 연계를 수행한다.

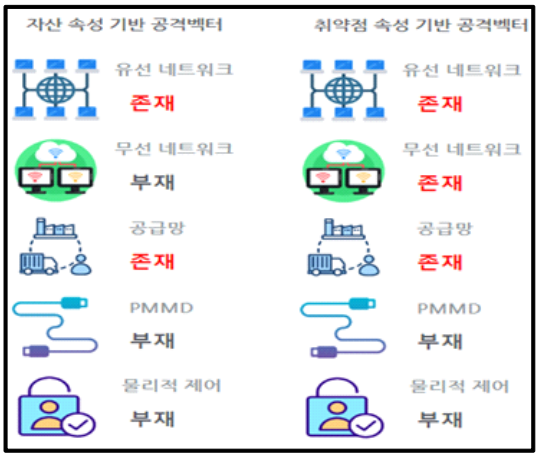
두 번째 방법론은 필수디지털자산 속성 정보와 자산에서 발생하는 취약점의 CVSS Vector String 정보를 활용하여 해당 취약점에 잔존 가능한 "유선", "무선", "공급망", "이동형 유지보수용/연결 기기","물리적 접근"등의 공격 벡터를 식별하는 방안을 기반으로 한다. 식별 결과를 NVAS 시스템에서는 [그림 13]와 같은 화면을 제공한다.

이와 같은 두 가지 방법론을 결합하여 필수디지털자산 공격 벡터 및 적대적 행위 정보를 모두 고려할 수 있는 유효 보안조치를 식별한다.

최종적으로 대안적 보안조치 항목을 제공하기 위하여, 본 시스템은 RS-015 보안조치 정보와 연계될 수 있는 NIST SP 800-53 및 주요정보통신기반시설 기술적 취약점 분석 및 평가 상세 가이드 정보를 [그림 14]과 같이 화면을 통해 사용자에게 제공한다.



〔그림 12〕 필수디지털자산 유효 보안조치 식별 프로세스



〔그림 13〕 필수디지털자산 잔존 공격 벡터 식별 화면

〔그림 14〕 대안적 보안조치 제공 화면

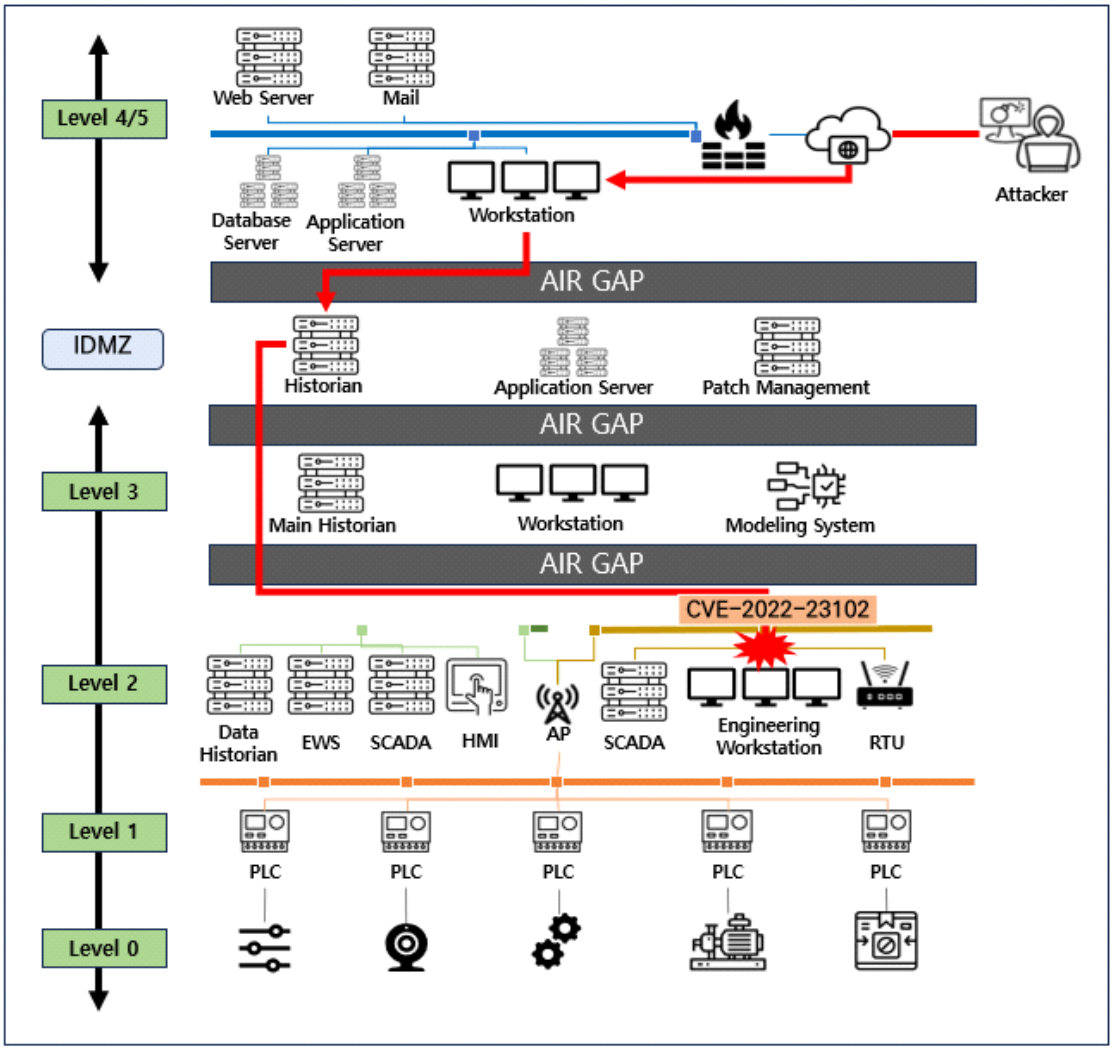
5.5. 사례 연구

본 장에서는 NVAS 시스템에 적용한 필수디지털자산에 유효한 보안조치 식별 방법론을 검증하기 위하여 가상의 환경을 구축하여 사례 연구를 진행하였다.

5.5.1. 환경 구축

본 연구의 보안조치 식별 방법론 사례 연구를 위하여 [그림 15]과 같은 가상의 원자력 시설을 설정하였다. Level 0부터 3까지는 ICS 영역이며, Level 4/5는 IT 영역으로 구성된다. ICS 영역과 IT 영역은 직접적인 통신이 불가하며, IDMZ를 통하여 간접적인 통신만 가능하다.

공격자는 ICS 영역의 Engineering Workstation을 타깃으로 한다고 가정한다. 공격자는 해당 시설의 외부에 위치하였기에 접근이 쉬운 IT 영역으로 먼저 침투한다. 이후 측면 이동을 통하여 ICS 영역으로 침투한다.



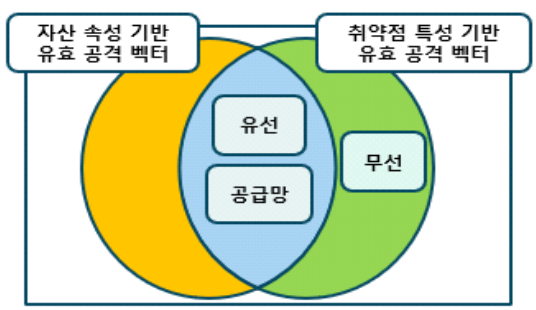
〔그림 15〕 가상 원자력 시설 시스템 구조도(사례 연구)

5.5.2. Engineering Workstation 분석

공격자가 타깃으로 하는 Engineering Workstation은 HP Z6 Tower Workstation을 사용하며, 해당 필수 디지털자산 세부 속성 정보는 [표 10]와 같다. 필수디지털자산 속성 정보에 따라 잔존하는 공격 벡터는 유선 네트워크, 공급망으로 식별하였다.

5.5.3. 원자력 시설 특화 취약점 재평가체계 적용

HP Z6 Tower Workstation에 존재하는 공개 취약점 정보 4개 중 'CVE-2022-23102'를 선정하였다 선정한 'CVE-2022-23102'에 원자력 시설 특화 취약점 재평가체계를 적용하였으며, 이에 대한 결과는 [표 11]



〔그림 16〕 유효 공격 벡터 식별

〔표 10〕 HP Z6 Tower Workstation 속성 정보

자산 속성 항목	HP Z6 G5 Tower Workstation
자산 유형	하드웨어
자산 유형 세부 사항	워크스테이션
제조사/ 공급자	HP
자산 등록 명칭	Z6 G5 Tower Workstation
모델 버전	-
HMI 이용 여부	-
매체연결 포트 물리적 차단 여부	O
유지보수용 기기 연결 포트 물리적 차단 여부	X
매체 연결(USB 등) 기능 여부	O
유지보수용 연결 기기 사용 여부	X
통신 연결성	O
통신 인터페이스	RJ45, RS-485
통신 프로토콜	TCP/UDP, TCP/IP
단방향 통신 여부	X
무선 통신 활성화 여부	X
무선 통신 유형	-
운영체제 명칭	windows
운영체제 버전	server_2019
펌웨어 명칭	-
펌웨어 버전	-
응용 서비스 제공 여부	O
애플리케이션 명칭	ecostruxure_control_expert
애플리케이션 버전	15.1
자산의 물리적 위치	핵심구역
네트워크 보안 계층	산업 영역
호스트 방화벽 적용 여부	X
암호화 통신 여부	O
자산 접근 권한	취급자
작업 승인 여부	O
계정 관리 기능 여부	X
Consequence Classification	통신 기능 직접 필수디지털자산

에 나타내었다.

‘CVE-2022-23102’는 AV(Attack Vector)가 ‘N(Network)’로 측정되면서, 잔존하는 공격 벡터는 유선 네트워크, 무선 네트워크, 공급망으로 식별하였다.

〔표 11〕 ‘CVE-2022-23102’ 정보 및 재평가 결과

구분	측정값	
설명	피싱 공격을 유도하여 신뢰할 수 없는 URL로 리디렉션	
CVSS v3.x	벡터열	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
	심각도 점수	6.1
재평가	벡터열	AV:N/AC:H/PR:L/UI:R/S:C/AL:V/CA:B/ECM:P
	심각도 점수	8.4

5.5.4. 잔존 공격 벡터 기반 보안조치 식별

HP Z6 Tower Workstation 속성 정보에 기반하여 잔존하고 있다고 식별한 공격 벡터는 유선 네트워크, 공급망이며, 취약점 ‘CVE-2022-23102’ 특성에 따라 잔존하는 공격 벡터는 유선 네트워크, 무선 네트워크, 공급망이다. 따라서 실제로 잔존하고 있는 공격 벡터는 유선 네트워크와 공급망이다.

유선 네트워크와 공급망 공격 벡터를 완화할 수 있는 관련 RS-015 보안조치 항목은 [표 12]와 같다.

〔표 12〕 잔존 공격 벡터 완화 보안조치 항목 수

구분	잔존 공격 벡터		
RS-015 보안조치 항목 수	유선 네트워크	공급망	중복 제거 총 보안조치 항목 수
	87	30	93

5.5.5. 취약점-적대적 행위 기반 보안조치 식별

‘CVE-2022-23102’에 대한 적대적 행위 식별 방법론을 적용한 결과, 관련 적대적 행위는 T1036, T1566.002, T1204.001 3가지 공격 기술이 식별되었다. 이에 대한 RS-015 보안조치 항목 수 [표 13]와 같다.

〔표 13〕 적대적 행위 완화 보안조치 항목

구분	RS-015 항목 수
T1036	8
T1566.002	5
T1204.001	6
중복 제거 총 보안조치 항목 수	11

5.5.6. 실제 유효한 보안조치 항목 식별

잔존하는 공격 벡터를 완화할 수 있는 보안조치 항목은 총 93개였으며, 적대적 행위를 완화할 수 있는 보안조치 항목은 총 11개였다.

잔존하는 공격 벡터를 완화하고, 적대적 행위에 대응할 수 있는 실제 유효한 보안조치 항목은 10개로 식별되었다.

기존 필수디지털자산에 잔존하는 공격 벡터를 완화하기 위한 보안조치 항목의 수는 93개였으나, 이를 모두 수행하는 것은 이론적인 이상이며 현실적으로는 비효율적일뿐더러 실현도 불가능하다.

잔존 공격 벡터를 완화할 수 있는 보안조치 항목을 기반으로 적대적 행위자의 공격 목적과 의도를 고려한 보안조치 항목은 10개로, 단순 공격 벡터 완화 보안조치 항목 수보다 약 10배 이상 줄었다.

본 사례 연구를 통하여 필수디지털자산의 보안조치 식별 방법론을 검증하였다. 필수디지털자산의 속성 및 공개 취약점 정보 기반 잔존 공격 벡터 식별, 취약점 정보와 적대적 행위 정보 연계, 원자력 시설 특화 취약점 재평가체계 적용, 잔존 공격 벡터와 적대적 행위자의 목적 및 의도를 고려한 필수디지털자산에 유효한 실제 보안조치 식별에 이름으로써, 본 연구가 기반시설의 취약점 정량화 평가체계 구축을 위한 참고자료로 활용될 수 있을 것이라고 사료한다.

〔표 14〕 방법론 단계별 보안조치 항목 수 비교

구분	총 보안조치 항목 수 (중복 제거)
공격 벡터 완화 관련	93
적대적 행위 완화 관련	11
최종 유효 보안조치	10

Ⅵ. 결 론

본 연구에서는 공통 플랫폼 정보, 공개 취약점 정보. 보안 약점 정보, 공통 취약점 평가체계 등의 취약점 관련 정보원를 살펴보고, 산업별 취약점 평가체계 활용안에 대한 지표를 분석하였다. 또한 자체적으로 구축한 NVAS 시스템 및 활용한 방법론을 제시하였다.

구체적으로는 원자력 시설의 특성이 반영된 취약점 정량적 평가체계, 필수디지털자산 속성 및 공개 취약점 특성에 따른 잔존 공격 벡터 식별 방법론, 취약점을 악용하는 적대적 행위자의 목적 및 의도 고려 방안, 필수디지털자산에 실제 적용 가능한 보안조치 식별 방법론 등을 다루었다.

이처럼 기반시설의 효율적인 취약점 대응을 위하여는 OT 환경의 특성을 반영한 취약점 정량적 평가체계가 필요할 것이다. 또한 정적인 특성을 보완할 수 있는 시스템을 보완적 목적으로 활용한다면, 기반시설별 특화된 효율적인 취약점 대응체계가 구축될 수 있을 것이다.

이러한 점에 기인하여 본 연구는 기반시설 취약점 정량적 평가체계 구축을 위한 참고 자료로 활용될 수 있을 것이라고 사료한다.

참 고 문 헌

[1] FIRST, ‘CVSS v4.0 Presentation’, June 2023

[2] Karen Scarfone , Peter Mell “An analysis of CVSS version 2 vulnerability scoring”, IEEE, November 2009.

[3] International Telecommunication Union, X.1520 : Common vulnerabilities and exposures, January 2014

[4] International Telecommunication Union, X.1521 : Common vulnerability scoring system, March 2016

[5] KISA, Information Security Management System-Personal Information, April 2022

[6] KISA, 주요정보통신기반시설 기술적 취약점 분석 · 평가 상세 가이드, March 2021

[7] International Organization for Standardization, ‘“ISO/IEC 27001‘, October 2022

[8] U.S. NIST, SP 800-53 Security and Privacy Controls for Information systems and Organization, rev. 5. September. 2020

[9] U.S. NIST, SP 800-82 Guide to Operation Technique System Security, rev. 3. April 2022

[10] KINAC, 원자력시설등의 컴퓨터 및 정보시스템 보안, 2014

[11] U.S.NRC, REGULATORY GUIDE 5.71, Cyber Security Programs for Nuclear Facilities, January

2010
[12] U.S. Nuclear Energy Institute, NEI 13-10 Cyber Security Control Assessments, November 2019
[13] U.S. Nuclear Energy Institute, NEI 08-09 Cyber Security Plan for Nuclear Power Reactors, April 2010
[14] Attiq Ur-RehmanIqbal, GondalIqbal GondalJoarder, KamruzzamanJoarder Kamruzzaman, Alireza JolfaeiAlireza Jolfaei, , “Vulnerability Modelling for Hybrid Industrial Control System Networks”, Journal of Grid Computing, 18(82), December 2020.
[15] Vilches, Víctor Mayoral et al., “Towards an open Standard for Assessing the Severity of Robot Security Vulnerabilities, the Robot Vulnerability Scoring System”, ArXiv abs/1807.10357, July 2018.
[16] 김경원, 장석민, 손윤식, 임선영, “무기체계 소프트웨어의 보안성 강화를 위한 보안약점 분석 및 평가 체계 연구”, 한국군사학논집 77(1), February 2021.
[17] Bharadwaj R. K. Mantha, Yeojin Jung, Borja García de Soto, “Implementation of the Common Vulnerability Scoring System to Assess the Cyber Vulnerability in Construction Projects”, Creative Construction Conference, June 2020.
[18] Y. Zhang, P. Shi, C. Dong, Y. Liu, X. Shao, C. Ma, “Test and Evaluation System For Automotive Cybersecurity”, IEEE International Conference on Computational Science and Engineering, December 2018.
[19] Steve Christey Coley, Penny Chase, “Rubric for Applying CVSS to Medical Devices”, The MITRE Corperation, September 2019.
[20] Carbon Black, “Understanding the FFIEC Cybersecurity Assessment Tool”, VMware, April 2017.
[21] Ngoc T. Le, Doan B. Hoang. “Security threat probability computation using Markov Chain and Common Vulnerability Scoring System”. IEEE, January 2018
[22] Pooja Anand, Yashwant Singh, Arvind Selwal, Pradeep Kumar Singh, Kayhan Zrar Ghafoor, “IVQFIoT: Intelligent vulnerability quantification framework for scoring IoT vulnerabilities”, Future Generation Computer Systems, 93, 814 - 821, September 2021
[23] Y. Choi and S. Lee, “A Study on the Implementation of Technical Security Control for Critical Digital Asset of Nuclear Facilities,” Journal of the Korea Institute of Information Security & Cryptology, vol. 29, no. 4, pp. 877 - 884, August 2019
[24] DHS, “BOD 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems”, CISA, April 2019
[25] Jay Jacobs, Sasha Romanosky, Octavian Sucium, Ben Edwards, Armin Sarabi, “Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights”, IEEE, July 2023

〈저자소개〉

김 가 경 (Ka-Kyung Kim)
학생회원
2022년 8월 : 충북대학교 정치외교학과 학사 졸업
2023년 3월~현재 : 전남대학교 정보보안융합학과 석사과정
<관심분야> 산업제어시스템 보안, 취약점 분석, 데이터 사이언스, 정보보호

윤 성 수 (Seong-Su Yoon)
학생회원
2021년 2월 : 전남대학교 소프트웨어학과 학사 졸업
2021년 3월 : 전남대학교 정보보안융합학과 석사과정 졸업
2023년 3월~현재 : 전남대학교 정보보안융합학과 박사과정
<관심분야> 산업제어시스템 보안, 인공지능, 취약점 분석, 정보보호

김 도 연 (Do-Yeon Kim)

2022년 8월 : 전남대학교 물리학과 학사 졸업
2022년 8월~현재 : 전남대학교 정보보안융합학과 석사과정
<관심분야> 산업제어시스템 보안, 인공지능, 취약점 분석, 정보보호

엄 익 채 (Ieck-Chae Euom)

종신회원

2003년 8월 : 전남대학교 컴퓨터정보학부 학사 졸업
2015년 2월 : 한국과학기술원 소프트웨어대학원 석사 졸업
2019년 2월 : 전남대학교 정보보안협동과정 박사 졸업
2003년~2007년 : LG이노텍, 주임연구원
2007년~2019년 : 한전KDN, 차장
2019년 10월~현재 : 전남대학교 시스템보안연구센터 소장, 데이터사이언스대학원 교수
<관심분야> 제어시스템보안, 스마트그리드 보안, 원자력 보안, 취약점 분석, 차세대인프라 보안, 스마트시티·공장 보안, AI기반 이상징후 탐지, 지능형 보안