정 보 보 호 학 회 지
제 30 권 제5호, 2020. 10

발전시설 사이버보안 평가 방법론 TAM(Technical Assessment Methodology) 분석

정 다 운*, 신 지 호**, 이 채 창***, 권 국 희***, 서 정 택*

요 약

최근 주요정보통신기반시설 대상의 사이버 공격이 급격하게 증가하고 있다. 특히, 발전시설 주요정보통신기반시설에 사이버 공격 발생 시 전력 공급 중단으로 인하여 대규모 정전사고가 발생할 수 있다. 따라서, 발전시설 대상의 사이버보안 관리가 중요하며, 주기적인 사이버보안 평가가 필요하다. 미국 EPRI(Electric Power Research Institute)에서 발전시설 대상 사이버 보안조치 평가 방법론인 TAM(Technical Assessment Methodology)을 개발하였고, 최근 아랍에미리트(UAE, United Arab Emirates) 바라카(Barakah) 원자력발전소에서 사이버보안 평가를 위해 TAM을 활용하였다. 본 논문에서는 발전시설 사이버보안 평가 방법론인 TAM을 분석하고, 국내 발전시설 사이버보안 평가에 활용 방안을 제시하고자 한다.

Ⅰ. 서 론

IBM 2020 report에 따르면, OT(Operational Technology) 공격이 전년 대비 2,000% 증가하고 있어 [1], 사이버 공격 대상이 점점 기반시설로 확대되고 있음을 확인할 수 있다. 발전시설에 사이버 공격이 발생할 경우 경제적 손실뿐만 아니라, 인명피해 또한 발생할 수 있다. 따라서 발전시설에 사이버보안을 적용하고 평가하는 것이 필요하다. 사이버보안 규제는 사이버 공격으로부터 발전시설을 보호하기 위한 사이버보안 요구사항을 제시하고 있으며, 사이버보안 요구사항 이행여부를 평가하여 발전시설의 사이버보안을 평가한다. 그러나 이러한 구조는 사이버 보안조치를 어떤 방식으로 적용해야 하는지 구체적으로 기술하고 있지 않으며, 사이버 보안조치 자체를 평가할 수 없어 발전시설에 충분한 사이버 보안조치를 적용하였는지 평가할 수 없다. 또한 정보보호 자원은 한정되어 있어 모든 사이버보안 요구사항을 적용하기에는 어려움이 존재한다. 따라서 발전시설에 적용된 사이버 보안조치 자체를 평가하여 발전시설에 충분한 보안조치가 적용되었는지 평가할 수 있는 방안이 필요하고, 한정된 정보보호 자원을 효율적으로 활용하기 위해 효과적인 사이버 보안조치를 적용할 수 있도록 하는 방안이 필요하다. 미국 EPRI(Electric Power Research Institute)는 발전시설의 사이버보안을 평가하기 위하여, 사이버 보안조치 평가 방법론인 TAM(Technical Assessment Methodology)을 개발하였다. TAM은 발전시설의 잠재적인 위협 요소를 고려하여 사이버 보안조치를 식별하고, 식별한 사이버 보안조치의 효과성과 적합성을 정량화하여 사이버 보안조치의 성능을 평가할 수 있는 방법론으로, 최근 TAM은 아랍에미리트의 바라카 원자력발전소에서 사이버보안 평가에 활용되고 있다.

본 논문은 2장에서 사이버 보안조치를 평가하는 TAM의 절차에 대해 분석하고, 3장에서 TAM의 이점과 활용 방안을 제시하며, 4장에서 결론을 맺는다.

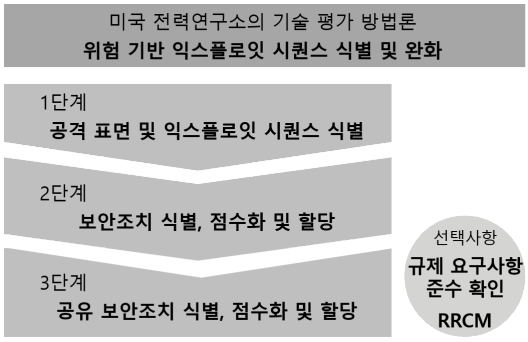
Ⅱ. EPRI TAM 분석

TAM은 미국 EPRI 에서 개발한 발전시설 대상 사이버 보안조치 평가 방법론으로, 자산의 기술적 구성을 검

본 연구는 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다. (No.1605007)

* 순천향대학교 정보보호학과 (대학원생, dauun999@gmail.com, 교수, seojt@sch.ac.kr)
** 경찰대학 치안정책연구소 과학기술연구부 (연구관, suchme@police.go.kr)
*** 한국원자력통제기술원 사이버보안실 (선임연구원, chiching@kinac.re.kr, 실장, vivacita@kinac.re.kr)

토하여 발생 가능한 사이버 공격을 식별하고 실제 공격 표면(attack surface)에 효과적인 사이버 보안조치를 식별한다. 그 후 사이버 공격의 잠재적인 결과를 고려한 위험 기반의 차등적인 접근방식을 사용하여 자산에 필요한 최소한의 보안수준을 제시하고, 최소한의 보안수준을 충족하였는지 평가한다. 또한 TAM은 NEI 08-09, R.G 5.71, NERC-CIP와 같은 발전시설 사이버보안 규제 요건 등과 매핑하여 발전시설의 규제 요건 준수 여부를 확인할 수 있는 프로세스를 제공한다. TAM은 각 자산에 존재하는 익스플로잇 시퀀스(exploit sequence)를 식별하고 익스플로잇 시퀀스를 완화시키기 위해 필요한 최소한의 보안수준을 설정하여, 자산에 적용된 모든 보안조치가 익스플로잇 시퀀스를 완화시킬 수 있는 최소한의 보안수준 이상이 되는지 평가한다. 그림 1은 TAM에 대한 전반적인 도식도이다. 보안조치 평가를 위한 3단계 절차로 구성되어 있으며, 선택적으로 규제 요건 준수 여부를 확인할 수 있다[2,3,4,5].

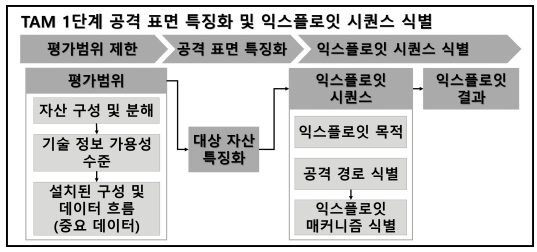


〔그림 1〕 EPRI의 TAM 도식도

자산 단위로 TAM을 적용하며, 동일한 모델의 자산이더라도 현장에서에 존재하는 자산의 역할이나 위치가 각기 다르기 때문에 자산 하나하나에 TAM을 적용해야 한다. 1단계는 자산에 존재할 수 있는 익스플로잇 시퀀스를 식별하기 위하여 자산 분석을 통해 평가범위를 제한 한다. 그 후 자산에 대한 공격 표면의 특징을 식별하고 익스플로잇 시퀀스를 도출한다. 2단계는 익스플로잇 시퀀스를 바탕으로 자산에 적용 가능한 보안조치를 식별 및 점수화하고, 익스플로잇 시퀀스의 잠재적인 결과에 따라 목표 수준(target level)을 설정한다. TAM에서 목표 수준은 익스플로잇 시퀀스를 완화시키는 기준으로 사용되며, 이는 해당 익스플로잇 시퀀스를 완화하기 위해 자산에 필요한 최소한의 보안수준이라고 해석할 수 있다. 보안조치의 점수를 고려하여 익스플로잇 시퀀스에 할당하는데, TAM에서는 익스플로잇 시퀀스를 완화시키기 위해 보안조치를 할당한다고 표현하며, 익스플로잇 시퀀스에 할당된 모든 보안조치의 점수 합이 목표 수준 이상이 되었을 때 보안조치가 완화되었다고 판단한다. 익스플로잇 시퀀스를 완화시킬 수 있는 보안조치를 모두 할당하였음에도 불구하고 익스플로잇 시퀀스가 완화되지 않은 경우, 해당 익스플로잇 시퀀스는 잔존하는 익스플로잇 시퀀스(residual exploit sequence)라고 하며, 3단계에서 완화한다. 3단계는 잔존하는 익스플로잇 시퀀스를 완화시키기 위해 자산 간의 관계를 관계집합(relationship set)으로 그룹화하고, 관계집합에 적용 가능한 보안조치인 공유 보안조치(shared control method)를 식별 및 점수화한다. 그 후 잔존하는 익스플로잇 시퀀스에 공유 보안조치를 할당하여, 잔존하는 익스플로잇 시퀀스를 완화시킨다. 자산에 적용된 보안조치가 사이버보안 규제 요건을 충족하였는지는 평가자가 선택적으로 수행할 수 있다[6].

2.1. 1단계 공격 표면 특징화 및 익스플로잇 시퀀스 식별

1단계는 자산의 기능과 특성을 분석하여 익스플로잇 시퀀스를 식별하기 위한 평가범위를 제한하고, 공격 표면의 특징을 식별하여 익스플로잇 시퀀스를 도출하는 단계이다. 그림 2는 1단계를 도식화한 것으로, 평가범위 제한, 공격 표면 특징화, 익스플로잇 시퀀스 식별과 같이 3가지 세부 절차로 구성된다.



〔그림 2〕 TAM 1단계: 공격 표면 특징화 및 익스플로잇 시퀀스 식별

2.1.1. 평가범위 제한

자산에 존재할 수 있는 익스플로잇 시퀀스를 식별하

기 위하여, 자산의 평가범위를 제한한다. 이를 위해, 표 1과 같이 자산의 구성(composition)을 파악하고 세부적인 단위로 분해(decomposition)를 수행하며, 기술 정보 가용성 수준(TIA level, Technical Information Availability level) 이라는 평가자가 자산의 공격 표면에 대한 정보를 얻기 위해 기술적으로 분석할 수 있는 수준을 파악한다. 또한 자산에서 실제 사용 중인 설치된 구성(installed configuration), 중요 데이터(critical data), 해당 데이터 흐름(data flow)을 식별한다. 평가범위를 제한하기 위해서는 자산의 구성요소(모듈 및 칩셋 단위)와 기능, 자산의 기능 중 활성화 및 비활성화 제어가 가능한 기능, 현장에서의 자산 식별자, 자산이 처리 및 저장하는 데이터 유형, 발전시설의 각 데이터 흐름도, 실질적으로 자산에 보안 테스트를 수행할 수 있는 정도 등에 대한 정보가 필요하며, 이에 따라 평가범위가 다르게 제한된다.

〔표 1〕 평가범위 제한을 위한 분석 유형

분석 유형	설명
자산 구성요소	• 평가범위 결정을 위한 자산 단위 결정 • 자산 구성요소, 제조업체 및 모델 변호, 현장 식별자 등 파악 • 자산의 특정 기능이나 구성을 제거하거나 비활성화하도록 설정한 강화된 기본 구성(hardened baseline configuration) 식별 • 분석 가능한 범위 내에서 분석
자산 분해	• 자산을 세부적인 단위(회로보드 또는 칩 단위)로 분해 • 자산이 중요 데이터를 저장 및 전송하는 방법을 알기 위함 • 분석 가능한 범위 내에서 분석
기술 정보 가용성 수준	• 자산의 공격 표면 정보를 얻기 위해 기술적으로 분석하는 수준 (수준 1 ~ 수준 3) • 수준 1: 현장 또는 워크벤치(workbench)에서 공격 표면 분석을 수행할 수 있으며, 법적 또는 운영상 제약 때문에 자산을 내부적으로 검사하거나 직·간접적으로 조사할 수 없음 • 수준 2: 현장 또는 워크벤치에서 공격 표면 분석을 수행할 수 있으며, 법적 또는 운영상 제약 내에서 자산을 내부적으로 검사하거나 직·간접적으로 조사 가능 • 수준 3: 실험실에서 공격 표면 분석을 수행할 수 있으며, 자산을 내부적으로 검사하거나 직·간접적으로 조사 가능 (리버싱을 통해 자세한 OEM과 설계정보 파악)
설치된 구성 및 데이터 흐름	• 자산의 익스플로잇 시퀀스를 식별하기 위한 중요한 단계 • 실제 사용 중인 구성 및 데이터 흐름 식별 • 정상 운영, 유지보수, 기타 임시 운영에 대한 구성 분석 • 중요 데이터의 저장 및 전송 위치를 나타내는 데이터 흐름도 작성
중요 데이터	• 6가지 중요 데이터 유형 존재 (저장 또는 전송 형태를 가짐) • 데이터 유형을 파악하는 것보다 모든 데이터 흐름을 파악하는 것이 더욱 중요 • 중요 데이터 유형: 운영 프로세스 데이터, OEM 정의 프로그램/설정 데이터, 사용자 정의 프로그램/설정 데이터, 보안 운영 데이터, OEM 정의 보안 프로그램/설정 데이터, 사용자 정의 보안 프로그램/설정 데이터

2.1.2. 공격 표면 특징화

다음으로 평가범위 내에서 표 2와 같은 정보들을 바탕으로 공격 표면에 영향을 미치거나 익스플로잇 시퀀스로 식별될 수 있는 자산의 모든 특징, 기능, 가능성을 분석하여 공격 표면을 특징화한다. 이때 본래 보안을 목적으로 하지 않았던 특징과 기능도 분석을 수행하여야 하며, 악용 가능성이 존재하는 경우 실제 사용 여부를 불문하고 반드시 분석해야 한다. 해당 과정을 통해 다양한 접근 방식을 기반으로 자산의 취약점이나 위협 요소를 식별할 수 있다.

해당 절차는 익스플로잇 시퀀스와 보안조치를 식별하기 위해 가장 밑바탕이 되는 절차이다. 이를 위해서는 수집 가능한 범위 내에서 자산 기능, 특징 등의 정보가 필요하며, 정보에 따라 다양한 공격 표면의 특징이 식별된다.

〔표 2〕 공격 표면 특징화를 위한 자산 정보

자산 정보
자산의 운영체제 및 펌웨어 업데이트 방법
자산의 운영체제 및 펌웨어 무결성 검증 방법
자산의 운영체제 및 펌웨어 암호화 또는 다른 보호 기능
자산의 운영체제 및 펌웨어 이름, 버전
응용 소프트웨어 이름, 버전, 무결성 검증 방법, 암호화 또는 다른 보호 기능
운영체제, 펌웨어, 응용 소프트웨어에 명시적으로 포함되지 않은 모든 데이터 파일 및 소프트웨어 객체
IP 주소 및 MAC 주소
현장에서의 물리적 및 논리적 위치와 주변 자산과의 관계
물리적 및 논리적 통신 포트, 터미널
자산이 제공하는 서비스(논리적 통신 포트 관련)
자산이 지원하는 통신 프로토콜
현장에서 사용하는 통신 프로토콜
설치된 구성 및 유지보수 방법
운영 및 유지보수 등에 사용되는 휴대용 장치
운영 및 유지보수 등에 사용되는 자산의 HMI (Human Machine Interface) 및 HMI 기능
타사 소프트웨어 및 외부 파일 등 설치 가능 여부 및 설치 방법과 데이터 흐름
동일한 특성을 가진 다른 모델 식별
현장에서의 사이버 보안 방어 수준
자산 스캔 유형, 사용 도구, 절차, 결과
취약점 여부 및 패치 빈도
자산에서 비활성화하거나 차단한 기능 및 차단 방법
자산에 적용한 보안조치

2.1.3. 익스플로잇 시퀀스 식별

특징화한 공격 표면을 참고하여 자산에 존재하는 익스플로잇 시퀀스를 도출한다. 익스플로잇 시퀀스는 공격 경로(attack pathway), 익스플로잇 목적(exploit objective), 익스플로잇 매커니즘(exploit mechanism)의 고유한 조합을 의미한다. 공격 경로는 공격 벡터, 물리적 인터페이스, 통신 프로토콜, 논리적 포트 번호, 인터페이스 커넥션(interface connection)으로 구성된다. 익스플로잇 목적은 표 3과 같이 자산에 직접적인 영향을 미치는 4가지 목적과 중요 데이터 유형 및 형태에 따라 데이터를 탈취하거나 변조하는 24가지 목적을 포함한 총 28가지의 고유 익스플로잇 목적으로 정의된다. 익스플로잇 매커니즘은 공격자가 익스플로잇 목적을 달성할 수 있도록 하는 자산의 특정 기능을 의미한다.

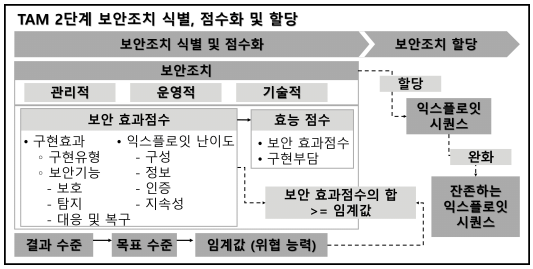
익스플로잇 시퀀스 식별은 앞서 수행한 공격 표면 특징에 따라 결과가 상이할 수 있으며, 평가자의 경험이나 보안 지식, 분석 깊이에 따라 결과물이 상이할 수 있다.

〔표 3〕 익스플로잇 목적 유형

구분	익스플로잇 목적		
자산에 직접적인 영향을 미치는 익스플로잇 목적	자산 활성화 및 비활성화 (즉시)		
	자산 비활성화 (지연)		
	서비스 거부 (DoS, Denial of Service)		
	멀웨어 (malware)		
중요 데이터 유형 및 형태별 익스플로잇 목적	운영 프로세스 데이터	전송 데이터	탈취
			변조
		저장 데이터	탈취
			변조
	OEM 정의 프로그램/설정 데이터	전송 데이터	탈취
			변조
		저장 데이터	탈취
			변조
	사용자 정의 프로그램/설정 데이터	전송 데이터	탈취
			변조
		저장 데이터	탈취
			변조
	보안 운영 데이터	전송 데이터	탈취
			변조
		저장 데이터	탈취
			변조
	OEM 정의 보안 프로그램/설정 데이터	전송 데이터	탈취
			변조
		저장 데이터	탈취
			변조
	사용자 정의 보안 프로그램/설정 데이터	전송 데이터	탈취
			변조
		저장 데이터	탈취
			변조

2.2. 2단계 보안조치 식별, 점수화 및 할당

2단계는 자산에 적용 가능한 보안조치를 식별 및 점수화하고, 보안조치 점수의 합이 목표 수준 이상이 될 때까지 보안조치를 익스플로잇 시퀀스에 할당하는 단계이다. 그림 3은 2단계를 도식화한 것으로, 보안조치 식별 및 점수화와 보안조치 할당과 같이 2가지 세부 절차로 구성된다.



〔그림 3〕 TAM 2단계: 보안조치 식별, 점수화 및 할당

2.2.1. 보안조치 식별 및 점수화

먼저 1단계에서 식별한 익스플로잇 시퀀스를 완화시키기 위하여, 자산에 적용할 수 있는 관리적, 운영적, 기술적 보안조치를 식별한다. 보안조치는 보호(protection), 탐지(detection), 대응 및 복구(respond & recover) 기능 중 하나 이상의 보안기능(security function)을 가지고 있으며, 자산에 직접적으로 구현되거나 다른 자산을 통해 구현될 수 있다. 보안조치를 식별한 후 보안 효과점수(security effectiveness score) 및 효능점수(efficacy score)를 산출한다. 두 점수는 보안조치를 서로 비교하고 익스플로잇 시퀀스에 보안조치를 할당하기 위한 기준으로 사용되며, 보안조치의 보안기능마다 따로 산출된다. 따라서 보안조치의 보호 기능, 탐지 기능, 대응 및 복구 기능에 대한 각각의 보안 효과점수 및 효능점수가 산출된다. 보안 효과점수는 익스플로잇 시퀀스를 완화시키는 정도를 판단할 때 사용되며, 구현효과(implementation effectiveness)와 익스플로잇 난이도(exploit difficulty) 평가 결과에 따라 점수가 산출된다. 구현효과는 구현유형(implementation type) 과 각 보안기능의 측정지표에 따라 평가되며, 익스플로잇 난이도는 구성(configuration), 정보(information), 인증(authentication), 지속성(persistence)의 측정지표에 따라 평가된다. 평가자는 TAM에서 제시하는 특정 기준에 따라 평가 요소를 None, Low, Medium, High 중 하나의 측정지표로 평가하며, 표 4와 같이 각 측정지표에 적합한 측정값이 할당된다.

〔표 4〕 보안 효과점수 평가요소, 측정지표 및 측정값

평가요소			측정지표 (측정값)			
구현효과 (I)	구현유형		관리적 (1.0)	운영적 (1.05)	기술적 (1.25)	
	보안기능	보호	N (0.0)	L (0.927)	M (1.2)	H (1.7)
		탐지	N (0.0)	L (0.927)	M (1.2)	H (1.7)
		대응 및 복구	N (0.0)	L (0.927)	M (1.2)	H (1.7)
익스플로잇 난이도 (D)	구성		L (0.34)	M (0.67)	H (1.0)	
	정보		L (0.34)	M (0.5)	H (0.66)	
	인증		0 (0.0)	1 (0.5)	2+ (0.66)	
	지속성		L (0.34)	M (0.5)	H (0.66)	

평가자의 평가요소 평가 결과에 따라 수식 (1) 을 통해 0.10 ~ 3.00의 보안 효과점수가 산출된다. α는 효과점수를 0.10 ~ 3.00 내의 값으로 산출하기 위한 스케일링 계수로, 1.1339 값을 갖는다. D는 익스플로잇 난이도, I는 보안 기능에 따른 구현효과에 대한 값을 의미한다. 보안 효과점수가 높을수록 완화 효과가 더 높다는 의미를 갖는다.

$$E = \log_2(\alpha) + \log_{2_j}(D) + \log_2(I) \quad (1)$$

또한 효능점수는 보안조치 적합성 평가 시 사용되며, 보안 효과점수와 구현부담(implementation burden)에 따라 점수가 산출된다. 평가자는 특정 평가기준에 따라 평가요소를 평가하고, 표 5와 같이 결과에 따라 1 ~ 5의 효능점수가 산출된다. 충돌(conflict) 은 보안조치 적용 시 자산 또는 시스템 운영과 충돌 할 수 있어 보안조치 구현 금지를 권고한다는 의미이다.

보안조치 식별 및 점수화도 마찬가지로 평가자의 경험, 보안지식, 분석 깊이에 따라 결과물이 상이할 수 있다.

〔표 5〕 보안 효과점수 및 구현부담에 따른 효능점수

효능점수		구현부담 (B)			
		High	Medium	Low	Conflict
보안 효과 점수 (E)	None	None			구현 금지
	Low	1	2	3	
	Medium	2	3	4	
	High	3	4	5	

2.2.2. 보안조치 할당

TAM에서는 보안조치를 익스플로잇 시퀀스에 할당하여 익스플로잇 시퀀스를 완화시키고자 한다. 보안 효과점수와 효능점수 평가가 완료되면, 보안조치를 할당하기 이전에, 익스플로잇 시퀀스에 존재하는 목표 수준을 설정한다. 목표 수준은 익스플로잇 시퀀스에 따른 잠재적인 공격 결과 수준을 의미하며, 보안조치 할당 기준이 된다. 목표 수준은 보안기능마다 따로 설정하도록 구분되어 있어, 익스플로잇 시퀀스의 보호 목표 수준, 탐지 목표 수준, 대응 및 복구 목표 수준을 설정해야 한다. 평가자는 보안 효과점수 합이 목표 수준 이상이 되도록 익스플로잇 시퀀스에 보안조치를 할당하여 익스플로잇 시퀀스를 완화시킨다. 목표 수준은 잠재적인 공격 결과가 클수록 높아지기 때문에 표 6과 같이 요구되는 보안 효과점수의 합 또한 커지게 된다.

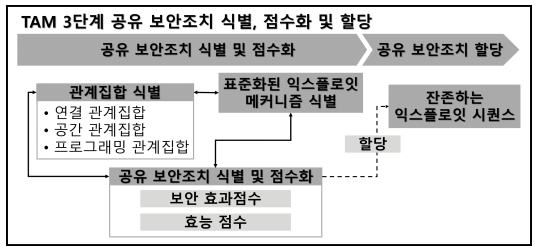
목표 수준을 설정한 후, 보안 효과점수와 효능점수를 고려하여 익스플로잇 시퀀스에 보안조치를 할당한다. 자산에 적용 가능한 모든 보안조치를 익스플로잇 시퀀스에 할당하였음에도 불구하고 보안 효과점수 합이 목표 수준 이상이 되지 못하였을 경우, 해당 익스플로잇 시퀀스는 잔존하는 익스플로잇 시퀀스로 불리며, 3단계에서 완화된다.

〔표 6〕 익스플로잇 시퀀스의 목표 수준에 따른 보안 효과점수 기준

목표 수준	보안 효과점수 임계값
A (높은 공격 결과 영향)	$3.30 \leq A$
B	$2.60 \leq B < 3.30$
C	$2.00 \leq C < 2.60$
D	$1.30 \leq D < 2.00$
E (낮은 공격 결과 영향)	$0.70 \leq E < 1.30$

2.3. 3단계 공유 보안조치 식별, 점수화 및 할당

3단계는 잔존하는 익스플로잇 시퀀스를 완화시키기 위해 자산 간의 관계를 관계집합으로 그룹화하고, 관계집합에 적용 가능한 공유 보안조치를 식별 및 점수화하여 익스플로잇 시퀀스에 할당하는 단계이다. 그림 4는 3단계를 도식화한 것으로, 공유 보안조치 식별 및 점수화와 공유 보안조치 할당과 같이 2가지 세부 절차로 구성된다.



〔그림 4〕 TAM 3단계: 공유 보안조치 식별, 점수화 및 할당

2.3.1. 공유 보안조치 식별 및 점수화

잔존하는 익스플로잇 시퀀스를 완화하기 위하여 공유 보안조치를 식별한다. 공유 보안조치를 식별하기 이전에, 자산의 관계집합과 표준화된 익스플로잇 메커니즘(NEM, Normalized Exploit Mechanism)을 식별한다. 관계집합은 표 7과 같이 자산 간의 연결 관계, 공간 관계, 프로그래밍 관계를 그룹화 한 것이다.

〔표 7〕 관계집합 유형

관계집합 유형	설명
연결 관계	• 논리적으로 연결된 자산의 중요 데이터 흐름으로 연결된 집합 • 방화벽 규칙, 네트워크 검색 규칙 등 통신 연결을 통해 자산 간 공유 • 공격 경로 제공
공간 관계	• 동일한 공간 구조에 위치한 자산의 집합 • 잠금 및 알림 캐비닛과 같은 공간 특성 장치나 카드 리더기와 같은 물리적 경계 접근 제어와 관련 • 공간 속성과 관련된 보안조치 할당 가능
프로그래밍 관계	• 구성 관리 또는 이동식 매체 및 모바일 장치 프로그램과 같은 보안조치 역할을 하는 프로그램 정책 및 절차에 의해 관리되는 자산

NEM은 1단계에서 식별한 익스플로잇 메커니즘 보다 더 넓은 개념으로, 표 8을 예시로 들 수 있다. 관계집합과 NEM을 바탕으로 관계집합에 적용할 수 있는 공유 보안조치를 식별 및 점수화 한다. 이 후 보안 효과점수의 합이 잔존하는 익스플로잇 시퀀스의 목표 수준 이상이 될 때까지 공유 보안조치를 할당한다.

〔표 8〕 NEM과 익스플로잇 매커니즘 관계 (예시)

NEM	익스플로잇 메커니즘
자산에 대한 물리적 비인가 접근	전원 공급장치 또는 루프 케이블 분리
	JTAG 인터페이스를 통한 펌웨어 수정
공급망을 통한 자산 비인가 접근	전면판을 통해 공정 변수 읽음
	공급망을 통해 수정된 펌웨어 파일 전송

공유 보안조치는 관계집합을 어떻게 식별하는지에 따라 다르게 식별될 수 있다. 공유 보안조치를 식별한 후, 2단계에서 보안조치를 점수화한 것과 마찬가지로 공유 보안조치의 보안 효과점수와 효능점수를 산출한다.

2.3.2. 공유 보안조치 할당

잔존하는 익스플로잇 시퀀스를 완화시키기 위해 보안 효과점수가 목표 수준 이상이 될 때까지 공유 보안조치를 익스플로잇 시퀀스에 할당하여, 잔존하는 익스플로잇 시퀀스를 완화시킨다.

		Combined Security Effectiveness Score			Target Levels			Security Control Method Quantity		
Exploit Sequence	Attack Pathway	Protect	Detect	R/R	Protect	Detect	R/R	Protect	Detect	R/R
E01.A01.X1	A01	1.44	3.69	5.12	A	A	A	1	3	4
E03.A02.X2	A02	3.58	4.48	5.59	A	A	A	3	4	6
E05.A04.X3	A04	3.96	3.14	3.46	A	A	A	4	3	3
E12.A05.X4	A05	3.58	4.48	5.59	A	A	A	3	4	6
E13.A04.X3	A04	3.96	3.14	3.46	A	A	A	4	3	3
E16.A03.X5	A03	0.00	1.50	2.99	A	A	A	0	1	2
E17.A02.X6	A02	2.85	2.95	2.95	A	A	A	2	2	2

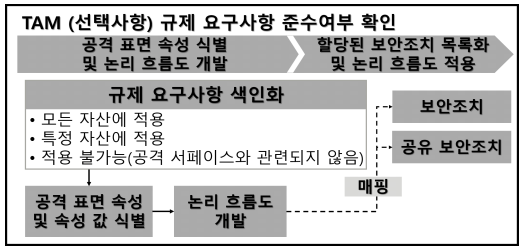
		Combined Sec... Effectiveness Sc...			...get Levels			Security Control Method Quantity		
Exploit Sequence	Attack Pathway	Protect	Detect	R/R	Protect	Detect	R/R	Protect	Detect	R/R
E01.A01.N1	A01	3.44	3.69	5.12				3	3	4
E03.A02.N3	A02	3.58	5.47	5.59				3	5	6
E05.A04.N2	A04	3.96	4.58	3.46				4	4	3
E12.A05.N4	A05	3.58	4.48	5.59				3	4	6
E13.A04.N2	A04	3.96	4.58	3.46				4	4	3
E16.A03.N3	A03	4.15	3.49	3.86				2	2	3
E17.A02.N4	A02	4.39	4.46	4.46				3	3	3

〔그림 5〕 TAM 적용 결과: 2단계 보안조치 할당 (상), 3단계 공유 보안조치 할당 (하)

자산을 대상으로 TAM을 적용하여, 그림 5와 같은 결과를 확인할 수 있다. 2단계 보안조치를 할당한 결과 7개의 익스플로잇 시퀀스 중 2개의 익스플로잇 시퀀스가 완화되는 것을 확인할 수 있으며, 3단계 공유 보안조치를 할당한 결과 잔존하는 익스플로잇 시퀀스가 모두 완화된 것을 확인할 수 있다[7,8,9,10,11,12].

2.4. 규제 요구사항 준수여부 확인

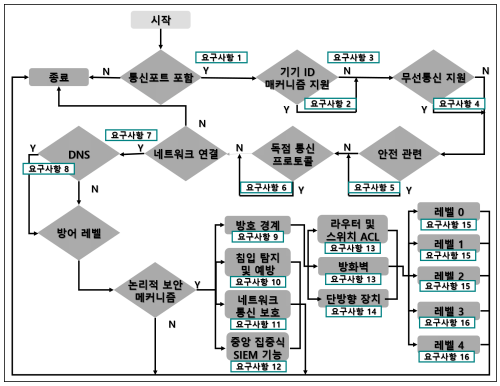
해당 단계는 선택사항으로, 자산에 적용 가능한 규제 요구사항을 식별하고 자산에 적용된 보안조치를 매핑하여, 규제 요구사항 준수 여부를 확인하는 단계이다. 그림 6은 해당 단계의 세부 절차를 도식화한 것으로, 공격 표면 속성 식별 및 논리 흐름도 개발과 할당된 보안조치 목록화 및 논리 흐름도 적용과 같이 2가지 세부 절차로 구성된다.



〔그림 6〕 TAM 선택사항: 규제요구사항 준수여부 확인

2.4.1. 공격 표면 속성 식별 및 논리 흐름도 개발

규제 요구사항을 색인화하기 위해 공격 표면 속성과 논리 흐름도를 개발한다. 규제 요구사항은 글머리 기호 또는 문장 단위로 동일한 공격 표면 속성을 나타내고 있으며, 상위 수준으로 색인화된 요구사항의 경우 다수의 하위 요구사항을 포함한다는 특징을 바탕으로 규제 요구사항을 색인화한다. 그 후 이와 동일한 의미를 가진 공격 표면 속성값을 식별한다. 공격 표면 속성은 설치된 구성과 데이터 흐름에 따른 자산의 특징으로, 서로 종속적이거나 계층적일 수 있기 때문에 이를 반영한 논리 흐름도를 개발한다. 그림 7과 같은 논리 흐름도를 예로 들 수 있다.



〔그림 7〕 논리 흐름도 (예시)

2.4.2. 할당된 보안조치 목록화 및 논리 흐름도 적용

보안조치를 규제 요구사항에 매핑하기 위해 보안조치를 목록화시킨 후, 사전에 개발한 논리 흐름도에 보안조치를 적용하여 어떤 규제 요구사항에 해당하는지 확인한다. TAM에서는 규제 요구사항을 모든 자산에 적용 가능한 규제 요구사항, 특정 자산에 적용 가능한 규제 요구사항, 공격 표면과 관련이 없어 적용 불가능한 규제 요구사항으로 구분하여, 규제 요구사항 유형에 따라 보안조치를 매핑하는 방법을 제시하고 있다.

Ⅲ. TAM의 특징 및 활용 방안

발전시설 사이버보안 평가 방법론인 TAM을 분석한 결과 2가지 특징이 존재한다. 첫째, 발전시설에 적용된 보안조치의 효과성과 적합성을 근거로 발전시설의 사이버보안 평가를 수행할 수 있다. 보안조치의 보안 효과점수와 효능점수를 통해 정량적인 수치로 효과와 효능을 확인할 수 있기 때문이다. 보안 효과점수는 보안조치가 구현된 유형과 보안기능을 통해 보안조치의 성능을 파악하고 공격자가 보안조치를 우회(overcome) 할 수 있는 정도를 고려하여 보안조치가 사이버 공격을 얼마나 차단할 수 있는지에 대해 평가할 수 있으며, 효능점수는 보안조치의 효과와 보안조치 구현 시 소모되는 자원을 고려하여 보안조치 적합성에 대해 평가할 수 있다. 둘째, 효과적인 보안조치를 선별하여 적용할 수 있다. 자산의 기능 및 특성을 분석하여 발생 가능한 익스플로잇 시퀀스를 식별하고 익스플로잇 시퀀스를 완화할 수 있는 보안조치를 식별한 후, 보안조치 점수화를 통해 익스플로잇 시퀀스를 완화하는데 더욱 효과적인 보안조치를 선별하여 적용할 수 있다.

본 논문에서는 자산에 TAM을 적용함으로써, 자산에 존재하는 사이버보안 위험도가 감소하였음을 확인할 수 있다. TAM은 자산의 취약점이나 위협 요소를 통해 발생 가능한 사이버 공격을 식별하고, 이에 대응할 수 있는 보안조치를 선별할 수 있다. 또한 보안 효과점수와, 효능점수를 활용하여 사이버 공격을 완화할 수 있는 다수의 보안조치를 비교하고, 더 높은 점수가 산출된 보안조치를 우선적으로 적용할 수 있다. 목표 수준이라는 보안조치 할당 기준은 사이버 공격을 완화시키는데 필요한 최소한의 보안조치 적용 기준으로 참고할 수 있으며, 최종적으로 도출된 TAM의 결과물을 통해 발전시설의 사이버보안 평가를 할 수 있다고 판단된다.

Ⅳ. 결 론

미국 EPRI에서 개발한 발전시설 대상 사이버 보안조치 평가 방법론인 TAM은 발전시설의 잠재적인 위협요소를 고려하여 익스플로잇 시퀀스를 식별하고, 익스플로잇 시퀀스를 완화할 수 있는 사이버 보안조치를 식별한다. 식별한 사이버 보안조치의 효과성과 적합성을 점수화하여 정량적으로 사이버 보안조치의 성능을 평가한다. 본 논문에서 TAM을 분석한 결과, TAM은 평가자의 경험, 보안지식, 분석 깊이에 따라 결과가 상이하게 나타날 수 있다. 그러나 평가자의 전문성을 확보하고 면밀히 평가 대상을 분석할 수 있다면, 정량화된 보안조치의 성능과 사이버 공격을 완화하기 위한 최소한의 보안 수준을 바탕으로 발전시설의 사이버보안을 평가할 수 있다. 또한 사이버보안 평가뿐만 아니라, 발전시설에 사이버 보안조치를 적용하고자 할 경우, 보안조치의 점수를 비교하여 더 높은 점수가 산출된 보안조치를 우선적으로 적용할 수 있다. TAM은 발전시설의 사이버보안 평가하는 데 적합하다고 판단되며 발전시설뿐만 아니라 다양한 주요정보통신기반시설 대상의 사이버보안 평가에 활용 가능할 것으로 판단된다.

참 고 문 헌

[1] IBM X-Force Incident Response and Intelligence Services (IRIS), “X-Force Threat Intelligence

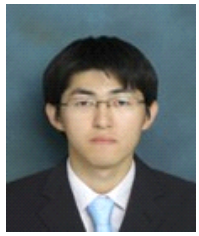
Index", IBM, pp. 5-6, 2020.
[2] Paul Martyak, "Risk-Informed Digital Engineering Update: Nuclear I&C Program", NEI Cyber Security Implementation Workshop, pp. 23-37, 2019.
[3] Michael Thow, "Cyber Security Technical Assessment Methodology (TAM): OT Assessment First Principles", Electric Power Research Institute (EPRI), pp. 1-23, 2019.
[4] EPRI, "Cyber Security Roadmap", EPRI, pp. 2-30, 2018.
[5] Lubos Mlcoch, "Security and Hardening of Your PI System", PI World Gothenburg 2019, pp. 27-44, 2019, https://www.osisoft.kr/presentations/security-and-hardening-of-your-pi-system/
[6] EPRI, "Cyber Security Technical Assessment Methodology: Risk Informed Exploit Squence Identification and Mitigation, Revision 1", EPRI, 2018, https://www.epri.com/research/products/3002008023
[7] Korea Electric Power Corporation and Korea Hydro & Nuclear Power CO., LTD, "APR1400 DESIGN CONTROL DOCUMENT TIRE 2: CHAPTER 7 INSTRUMENTATION AND CONTROL", Korea Electric Power Corporation and Korea Hydro & Nuclear Power CO., LTD, 2014, https://www.nrc.gov/docs/ML1500/ML15006A042.pdf
[8] 이철권, "원전 I&C 사이버보안 테스트베드 구축 및 활용", 원자력안전규제정보회의, 2017.
[9] 한국원자력연구원, "시스템 통합 및 기기/계통 기술성 평가: 비안전계통 구조 계발 및 기기/계통 평가 (KAERI/RR-2870/2007), 한국원자력연구원, 2017, https://inis.iaea.org/collection/NCLCollectionStore/_Public/39/121/39121486.pdf?r=1&r=1
[10] 한국원자력통제기술원, "원자력시설의 컴퓨터 및 정보시스템 보안", 한국원자력통제기술원, 2016.
[11] 손광섭, 김동훈, 손철웅, "고신뢰도 안전등급 제어기기 개발", 전기학회논문지, 62(1), pp.109-119, 2013.
[12] 최윤혁, 이상진, "원자력시설의 필수디지털자산에 대한 기술적 보안조치항목에 대한 연구", 한국정보보호학회논문지, 29(4), pp. 877-884, 2019.

〈저자소개〉

정 다 운 (Daun Jung)
학생회원
2020년 2월 : 순천향대학교 정보보호학과 졸업
2020년 3월~현재 : 순천향대학교 정보보호학과 석사과정
<관심분야> 정보보호, 사이버보안 평가

신 지 호 (Jiho Shin)
종신회원
2007년 8월 : 한국교육개발원 컴퓨터공학과 졸업
2015년 2월 : 고려대학교 정보보호대학원 디지털포렌식 석사
2019년 3월~현재 : 순천향대학교 정보보호학과 박사과정
<관심분야> 정보보호, 디지털포렌식, 제어시스템 보안

이 채 창 (Chaechang Lee)
정회원
2007년 2월 : 고려대학교 정보수학과 졸업
2014년 2월 : 고려대학교 정보보호대학원 금융보안학과 석사
2016년 5월~현재 : 한국원자력통제기술원 사이버보안실 선임연구원
<관심분야> 정보보호, 제어보안



권 국 희 (Kookheui Kwon)
정회원
2007년 2월 : 경북대학교 컴퓨터공학과 졸업
2013년 2월 : 아주대학교 정보시스템공학과 석사
2018년 2월 : 충남대학교 컴퓨터통신 및 보안학과 박사 수료
2011년 3월~현재 : 한국원자력통제기술원 사이버보안실 실장
<관심분야> 정보보호, 제어보안

서 정 택 (Jung Taek Seo)

종신회원

1999년 2월 : 한국교통대학교 컴퓨터공학과 졸업
2001년 2월 : 아주대학교 컴퓨터공학과 석사
2006년 2월 : 고려대학교 정보보호대학원 정보보호공학과 박사
2000년 11월~2016년 2월 : 국가보안기술연구소 책임연구원/연구부장
2014년 6월~2015년 6월 : University of Florida 초빙연구원
2016년 3월~현재 : 순천향대학교 정보보호학과 부교수
2009년 12월~2013년 5월 : 제주 스마트그리드 실증단지 보안센터 센터장
2013년, 2018년 : 한국철도공사 정보화자문단 자문위원
2016년 1월~2016년 12월 : ㈜ SR 철도안전자문단 자문위원
2017년 1월~현재 : 한국정보보호학회 CPS보안연구회 위원장
2017년 2월~현재 : 한국남동발전 사이버보안자문단 자문위원
2017년 11월~현재 : 인천국제공항공사 사이버보안 자문위원회 위원
2018년 12월~현재 : 한국서부발전 사이버보안 자문위원
2020년 6월~현재 : 한국전력공사 보안위원회 자문위원
<관심분야> CPS보안, 제어시스템 보안, 스마트그리드 보안, 원자력 발전 사이버보안, 스마트팩토리 보안, 스마트시티 보안, 자율주행인프라 보안