Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.6, Dec. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.6.1291

사이버공격 심각도 평가방법론 연구

배 선 하,[1†] 유 영 인,[1] 김 소 정[2‡]
[1,2]국가보안기술연구소 (선임연구원, 책임연구원)

A Study on the Cyber Attack Severity Assessment Methodology

Sunha Bae,[1†] Young-in You,[1] So Jeong KIM[2‡]
[1,2]National Security Research Institute (Senior Researcher, Principal Researcher)

요 약

국가 배후의 사이버공격 활동이 갈수록 증가하고 있으며, 국가 배후의 사이버공격은 개인 및 민간단체의 공격에 비해 규모와 영향이 커서 국가안보를 위협하고 있다. 이에 미국·영국을 비롯한 주요국과 EU·OECD 등 국제기구는 사이버공격에 대해 비례적 대응을 권고하고 있다. 우리나라도 2019년에 국가사이버안보전략을 발표하고, 사이버공격에 대한 억지력 확보를 위한 능동적 대응 의지를 밝혔다. 그러나 이후 관련된 정책이나 제도가 마련된 적이 없으며, 사이버공격 발생 시 비례적 대응을 위한 심각도 평가 및 대응방안이 미비한 상황이다.

본 논문에서는 국가 차원에서 사이버공격에 대한 대외 대응기준을 마련하고, 대응 시 비례적 대응이 가능하도록 피해의 규모와 영향을 측정할 수 있는 방법론을 제안한다. 또한, 제안하는 심각도 평가방법론을 이용해 한국 공격사례에 대해 심각도 평가를 수행하였으며, 평가결과를 기반으로 한국의 사이버위협 동향 및 심각도별 사이버공격 대응방안을 분석하였다.

ABSTRACT

State-sponsored cyberattacks have increased significantly and threaten national security in recent years. State-sponsored cyberattacks are often more sophisticated and destructive that attacks by individuals and private groups because of the concentration of manpower and resources. So major countries including the United States and the United Kingdom, as well as international organizations such as the EU and OECD, are recommending proportional response measures against cyberattacks. The Republic of Korea(ROK) is also trying to change its will to secure cyberattack deterrence and prepare active response through the 「National Cybersecurity Strategy 2019」. However, the ROK is not equipped with an adequate methodology to assess the severity of cyberattacks nor measures for proportional response to such attacks.

In this paper, we propose a Cyber Attack Severity Assessment(CASA) methodology that can assess the scale and impact of damage to prepare external response threshold for cyberattacks at the government-level and to enable proportional responses when responding.

Keywords: cyberattack severity, assessment, proportional response

I. 서 론

국가 및 국가배후조직의 선거공작, 기반시설공격, 사이버스파이(espionage) 활동을 통한 지식재산권 도용 등 정치적·경제적 이익을 위한 악의적인 사이버 활동이 증가하고, 사이버위협은 국가안보에 대한 위해를 가져오고 있다. 이로 인해 사이버공간의 정치적 중요성은 증가하고 있는데 반면, 사이버공간에 대한

Received(11. 08. 2021), Modified(11. 25. 2021), Accepted(11. 26. 2021)

† 주저자, sunhabae@nsr.re.kr
‡ 교신저자, sjkim@nsr.re.kr(Corresponding author)

책임 있는 국가 행동과 국제법, 규범에 대한 국제적 논의는 국가 간 이견으로 인해 합의를 이루지 못하고 교착 상태에 놓여있는 상황이다.

주요 국제기구 권고사항과 관련 연구에서는 각 국가 또는 지역협의체가 악의적인 사이버활동 발생 시 속성을 파악하고 정도를 평가하여, 이에 기반한 비례적 대응을 권장하고 있다. 탈린매뉴얼 저자인 마이클 슈미트는 평시의 악의적인 사이버 활동을 속성에 따라 분류하고, 이에 기반하여 대응수위를 결정하는 다이어그램을 제안하였다[1]. OECD는 중요활동(Critical Activities) 디지털 보안에 대한 권고사항에서 보안 속성 및 정도에 대해 신뢰할 수 있는 전달 메커니즘을 마련하고, 이에 기반하여 적절한 관리, 감사, 대응을 권장하고 있다[2]. 또한, EU도 사이버에 대한 EU 공동의 외교적 대응을 위한 프레임워크를 마련하고, 악의적인 사이버활동에 대한 비례적인 대응 원칙을 수립한 바 있다[3].

우리나라는 2019년에 국가사이버안보전략을 발표하고, 사이버공격에 대한 억지력 확보를 위한 능동적 대응 의지를 밝혔다[4]. 그러나 동(同) 수준의 대응을 위한 사이버공격 심각도 평가방법론, 대응안 등이 미비한 상태여서 사이버공격 발생 시 능동적 대응이 어려운 상황이다. 이에, 사이버공격 발생 시 심각도별 대응이 가능하도록 우리나라 환경을 고려한 사이버공격 심각도 평가방법론과 심각도 수준별로 국가 차원의 대응옵션을 마련하는 연구가 필요하다. 이를 통해 공공부문 사이버사고 발생 시 국가 차원의 대응수위 조정을 위한 기준과 민간부문 사이버사고 발생 시 정부개입 필요성 및 대응주체 구분을 위한 기준을 마련하고자 한다.

본 논문에서는 보편타당한 평가방법론 개발을 위해 국외 사이버공격 심각도 평가방법론의 평가항목과 평가결과 산출방안을 분석하였다. 그리고 국외 평가방법론 분석결과와 기반보호법에 따른 기반시설 부문 등 우리나라의 상황을 고려한 사이버공격 심각도 평가방법론을 제안한다. 평가주체는 사이버공격에 대한 정확한 조사결과를 취합 가능한 정부기관을 설정하였다. 그리고 제안하는 방법론을 이용하여 한국에서 발생한 사이버공격 사례 27건에 대한 심각도 평가를 수행하고 결과를 분석한다.

한국에서 발생한 사이버공격은 공격대상이 한국 기관·시설·사람 등인 경우를 말한다. 예를 들면, 2017년 전 세계적으로 발생한 워너크라이 공격은 러시아, 영국, 미국 등을 다른 국가를 대상으로 한 사이버공격임과 동시에 한국을 대상으로 한 사이버공격이다. 전 세계적으로 막대한 피해와 영향을 야기한 사이버공격인 경우에도 본 고에서는 한국의 비례적인 대외 대응기준을 마련하기 위해 심각도를 평가하기에 한국의 피해와 영향에 초점을 두고 심각도를 평가한다.

II. 국외 사이버공격 심각도 평가방법론 분석

국외 평가방법론은 IT, OT 분야에서의 사이버사고·공격에 대한 심각도 평가를 비롯하여 관련한 취약점 평가, 외교적 대응을 위한 평가 프레임워크 등 사이버공격의 심각도를 평가한 다양한 형태를 포괄적으로 살펴보았으며 각 평가방법론에서 사용하는 용어를 활용하여 비교·분석하였다.

분석 대상이 된 국외 사이버사고·공격 심각도 평가방법론은 다음 5가지이다. 먼저, 국가 차원에서 운용중인 평가방법론으로는 미국 국가사이버보안 및 통신통합센터(現 CISA, Cybersecurity & Infrastructure Security Agency)의 국가사이버사고평점시스템을 살펴본다.

또한, 소프트웨어·하드웨어·펌웨어 등 IT 사이버보안 위험을 관리하는 글로벌 보안업체인 파이어아이와 시만텍(現 노턴라이프록)의 평가방법론을 살펴본다.

마지막으로 사이버보안·안보 관련 국제조직 또는 이를 운영 중인 국제연합인 FIRST(Forum of Incident Response & Security Team)와 EU(European Union)의 평가방법론을 살펴본다.

2.1 국가사이버사고평점시스템(NCISS)

미국 국가사이버보안 및 통신통합센터(NCCIC, National Cybersecurity and Communications Integration Center)는 국가 차원에서 사이버사고 위험을 평가하여 점수화하고, 평점에 따라 공공자원배분 우선순위 결정을 위해 NCISS(National Cyber Incident Scoring System)를 개발하였다. 또한, 미국 산업제어시스템 사이버긴급대응팀(ICS-CERT, Industrial Control System Cyber Emergency Response Team)을 통해 2014년부터 주요기반시설 및 산업분야에 NCISS를 적용하고, 일관되게 사이버사고 위험을 평가하고 정보를 수집하고자 하였다[5].

또한, 미국 국토안보부는 2016년에 발표한 국가사이버사고대응계획(NCIRP, National Cyber

Incident Response Plan)을 통해 NCISS 활용범위를 확대하고, NCISS를 사이버사고심각도단계(CISS, Cyber Incident Security Schema)와 연계하여 사용하도록 하였다[6]. CISS는 국가안보, 경제 등에 영향을 미치는 사이버사고 발생 시 연방정부에서 공통된 시각으로 사이버사고 심각도를 평가하도록 심각한 정도를 단계별로 정의한 것으로, 美 오바마 정부가 연방기관 전체의 사이버사고 평가기준으로 세웠다[7]. 이에 따라, NCISS 활용범위가 주요기반시설 및 산업분야에서 연방정부 전체로 확대되었으며, 민간부문에서도 활용하도록 권고되었다.

NCISS의 평가항목은 8가지 항목으로 Table 1과 같으며 각 항목은 중요도에 따라 가중치를 가진다. 기능에 미치는 영향은 조직 가용성 대한 영향으로서, 기능에 대한 실질적·지속적인 영향을 말한다. 관찰된 활동은 네트워크에서 위협 행위자의 활동, 관찰된 활동의 위치는 활동이 감지된 네트워크 위치를 말한다. 행위자의 특성은 행위자의 기술 수준 및 의도, 정보에 미치는 영향은 정보의 무결성과 기밀성에 대한 영향으로 정보의 손실·도용·손상을 말한다. 마지막으로 복구가능성은 복구를 위한 자원의 범위, 부처간 영향은 부처별 상호의존성, 잠재적 영향은 기업·기관의 피해가 국가에 미치는 영향(기관의 중요도)을 말한다.

Table 1. NCISS Assessment Domain Abb. w-weight / CS - Critical Service

Domain	w	Option
Functional Impact	6	No Impact
		No Impact to services
		Minimal Impact to Non-CS
		Minimal Impact to CS
		Significant Impact to Non-CS
		Denial of Non-CS
		Significant Impact to CS
		Denial of CS/Loss of Control
Observed Activity	5	None
		Prepare
		Engage
		Presence
		Effect
Location of Observed Activity	4	Level 1 - Business DMZ
		Level 2 - Business Network
		Unknown
		Level 3 - Business Network Mng.
		Level 4 - Critical System DMZ
Location of Observed Activity	4	Level 5 - Critical System Mng.
		Level 6 - Critical Systems
		Level 7 - Safety Systems
Actor Characterization	4	Hactivists
		Unwitting Insider
		Criminal
		Unknown
		Witting Insider
		APT
		APT-Targeted
Information Impact	2	No Impact
		Suspected but not identified
		Privacy Data Loss
		Proprietary Information Loss
		Destruction of Non-Critical System
		Critical Systems Data Breach
		Core Credential Compromise
		Core Credential Compromise, Destruction of Critical System
Recoverability	4	Regular
		Supplemented
		Extended
		Not Recoverable
Cross-Sector Dependency	3	Agriculture and Food
		Banking and Finance
		Chemical
		Commercial Facilities
		Communications
		Critical Manufacturing
		Dams
		Defense Industrial Base
		Emergency Services
		Energy
		Government Facilities
		Healthcare and Public Health
		Information Technology
		Nuclear Reactors, Materials and Waste
		Transportation Systems
		Water
Potential Impact	6	Minimal
		Low
		Moderate
		High
		Severe

평가점수는 항목별로 0~100 사이의 점수를 부여하고, 평가항목별 점수의 가중 합을 통해 종합적으로 0~100점 사이에서 사이버사고 심각도 평점을 산출한다.

평가결과는 점수와 단계로 나타내며, 단계는 평점 구간에 따라 CISS와 동일하게 아래 6단계로 구성하는데 정상(Baseline), 낮음(Low-Green), 중간(Medium-Yellow), 높음(High-Orange), 심각(Severe-Red), 비상(Emergency-Black)으로 이루어진다. 다수의 사고가 일련의 관계를 갖는 연결된 사고이거나, 조직적 활동으로 판단될 때에는 평가자의 의견을 반영하여 종합적인 사고 심각도 평가단계를 개별 사고의 평가단계에 비해 높은 우선순위를 갖도록 평가단계를 상향할 수 있다.

NCISS는 사이버사고가 미치는 영향을 다양한 측면에서 고려하여 평가항목을 선정하였다. 특히, 잠재적 영향 항목을 통해 사이버사고가 발생한 대상의 중요도와 파급력을 평가에 반영하도록 하였으며, 사고대상의 연간매출(예산), 서비스 인구 규모 등을 통계적 수치를 고려하여 사고대상의 잠재적 영향 및 가치를 계산하여 점수화하였다.

그러나 여러 부문에서 동시다발적으로 발생하는 사고 등 서로 상관관계를 갖는 사고를 고려할 수 있는 평가항목은 존재하지 않으며, 평가자의 주관적 분석을 통해 점수에 반영한다. NCISS는 검증 가능한 평가항목을 확대하고 평가자의 개별 분석 요인을 줄여 시스템의 전반적인 신뢰도를 향상하고자 하였으나, 일부 평가결과에 대해서는 평가자의 관점에 따라 다른 결과가 도출될 수 있다는 한계가 있다.

2.2 사이버보안사고분류법(OT-CSIO)

미국 사이버보안 업체인 파이어아이(FireEye)는 IT와 OT의 융합이 증가하고 OT에 대한 위협 또한 매우 증가한 상황에서 OT 공격에 대한 조직 경영진의 의사결정을 지원하고, 위험평가(Risk Assessment)를 위한 지침을 제공하고자 OT-CSIO(Operational Technology - Cyber Security Incident Ontology)를 개발하였다[8].

평가항목은 산업제어시스템 국제 표준인 ISA-99의 Purdue Model에 따라 산업제어시스템의 네트워크를 주요 구성요소 간 상호 연결성과 종속성 기반으로 구분하여 구성하였으며, 4가지로 이루어져 있고 Table 2와 같다.

항목별 배점이나 산술적 평가방법론은 포함하고 있지 않아 별도로 평가점수를 산출하지는 않으며, 평가결과를 Figure 1과 같이 점수 또는 등급이 아닌 매트릭스 형태로 나타낸다. 평가항목인 영향도, 정교성, 표적을 행·열로 배치하여 산업제어시스템의 사이버사고 결과를 시각화하고 과거 사고 사례 평가결과를 매트릭스에 함께 제공하여, 현재 발생한 사이버사고와 비교할 수 있도록 함으로써 경험적 지식을 활용할 수 있도록 하였다.

공격유형 분류 및 사례별 분석을 통해 유사 시나리오를 통한 공격을 방지하고, 조직에서 식별되지 않은 위협에 대한 고려가 가능하도록 하였다. 또한, 평가항목 중 피해장비에 계측제어안전시스템을 포함하는 안

Table 2. OT-CSIO Assessment Domain

Domain	Option
Target	ICS-targeted
	Non-targeted
Sophistication	Low
	Medium
	High
Impact	Data Compromise
	Data Theft
	Degradation
	Disruption
	Destruction
Impacted Equipment	Enterprise network(Zone 5)
	Site Business Planning and Logistics Network(Zone 4)
	Plant DMZ
	Site Operations and Control(Zone 3)
	Area Supervisory Control(Zone 2)
	Basic Control(Zone 1)
	Process(Zone 0)
	Safety System

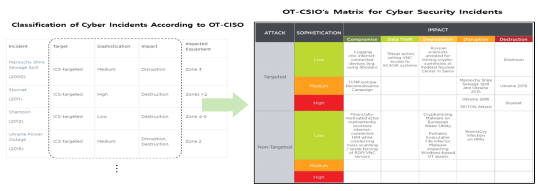

Fig. 1. Example of OT-CISO Cyber Incident Classification and Cyber Incident Matrix

전영역을 추가하는 등 산업제어시스템에 특화되어 안전개념을 강조하고 있다는 특징이 있다. 정보에 대한 영향과 시스템에 대한 영향을 통합하여 영향도 항목을 평가하고 있으며, 주로 가용성 관련한 항목으로 평가항목을 구성하고 있다.

2.3 보안대응 위협 심각도 평가

시만텍(Symantec)은 바이러스, 웜 등을 위협으로 정의하고, 위협 심각도 평가방법과 이에 대한 대응방안 매트릭스를 포함하는 보안대응 위협 심각도 평가(The Symantec Security Response Threat Severity Assessment)를 운용하였으며, 현재는 클라우드 호스팅 기반의 위협 인텔리전스인 시만텍 딥사이트(Symantec DeepSight) 서비스를 제공하고 있다[9]. 딥사이트는 시만텍의 위협 인텔리전스로, 사이버첩보·사이버범죄·핵티비스트 등 보안 위협 환경에 대한 통찰력을 확보하고, 인식을 강화하기 위한 모니터링 및 자동화된 취약점 관리 서비스 등을 제공하는 도구이다. 시만텍은 위협에 대한 정보 제공 시 각 위협에 영향을 받는 시스템, 발견 시기 등 기본적인 정보와 함께 본 평가방법론을 통한 심각도 평가결과를 함께 제공하였다.

평가항목은 3가지로 바이러스가 전파된 정도인 감염도, 감염이 미치는 영향인 피해정도, 감염의 확산속도 및 정도인 확산정도이다.

평가점수는 별도로 없으며 항목별 결과의 논리연산(and/or)을 통해 단계를 결정한다. 평가 결과지표는 심각도 단계로 CAT1 ~CAT5 까지 5단계로 구분하며, CAT 1로 분류된 사고가 가장 낮은 심각도를 갖고 CAT5가 가장 높은 심각도를 가진다. 또한, 심각도 단계별로 활용 가능한 대응방안을 매트릭스 형태로 제시한다[10].

Table 3. Symantec Assessment Domain

Domain	Option
Wild	High
	Medium
	Low
Damage	High
	Medium
	Low
Distribution	High
	Medium
	Low

2.4 공통취약점점수체계(CVSS) 3.1

CVSS(Common Vulnerability Scoring System)는 전 세계의 조직들이 활용하는 공개된 표준으로, 소프트웨어·하드웨어·펌웨어 등에 존재하는 취약점의 기술적 특징을 평가하여 점수화하는 체계이다[11]. FIRST의 특별분과회의(Special Interest Group, 은행·금융·기술산업·학계 등 다양한 부문의 대표자들로 구성된 그룹)에서 관리 및 개선하며 현재 3.1이 최신 버전이다. 시스템 요소에 존재하는 취약점 위주의 점수체계이기는 하나, 시스템 내·외부의 환

Table 4. CVSS Assessment Domain

Domain	Option		
Base Score	Vulnerability	AV, Access Vector	Network
			Adjacent
			Local
			Physical
		AC, Attack Complexity	Low
			High
		PR, Privileges Required	None
			Low
			High
		UI, User Interaction	None
			Required
	Scope		Unchanged
			Changed
	ISS	Confidentiality	High
		Integrity	Low
		Availability	None
Temporal Score	Exploit Code Maturity		Not Defined
			High
			Functional
			Proof of Concept
			Unproven
	Remediation Level		Not Defined
			Unavailable
			Workaround
			Temporary Fix
			Official Fix
	Report Confidence		Not Defined
			Confirmed
			Reasonable
			Unknown
Environmental Score	Modified Base Score		
	High	Confidentiality Requirement	Not Defined
		Integrity Requirement	High
			Medium
		Availability Requirement	Low

경과 관련 정보 현황 등을 반영한 종합적인 심각도를 확인할 수 있는 평가방법론이다. 따라서 특정 IT 제품 또는 플랫폼에 맞춰져 있지 않으며, 인력에 대한 피해, 금전적 손실 등 각 조직에 발생하는 고유 결과는 평가에 고려하지 않는다는 한계가 있다.

평가항목은 취약점의 기술적 특성에 집중하여 평가항목을 구성하고, 기본측정, 시간측정, 환경측정 3가지로 구분하였다. 기본측정 항목은 평가에 의무적으로 반영해야 하지만 시간측정, 환경측정 항목은 해당 조직과 시스템의 특성을 고려하여 필요 시 활용 가능하도록 하였다. 시간측정 항목은 시간에 따라 변화하는 특성이며, 환경측정 항목은 대상 조직의 IT 자산 중요도, 보안통제사항의 구현 여부 등을 포함한 사용자 환경에 따라 변화하는 특성이다.

평가점수는 기본적으로는 영향과 취약성의 합으로 이루어지고, 공격 범위에 따라 점수 산출을 위한 상수 및 계산방법에 차이가 있다. 항목별로 단계에 따라 점수를 배점하였으며, 취약성, 영향 등 연관이 있는 항목끼리 그룹화하고, 전체 점수와 별도로 그룹별로 점수 산출이 가능하다.

평가결과는 기본, 시간, 환경측정항목의 평가결과를 점수화하여 제공하며, 점수 구간에 따른 심각도를 위험없음, 저위험군, 중위험군, 고위험군, 치명적위험군 5단계로 구분한다. 또한, 점수 및 등급 외 추가적인 정보공유를 위해 기본측정항목의 평가결과를 문자열 형태로 제공한다.

2.5 사이버외교툴박스(CDT)

CDT(Cyber Diplomacy Toolbox)는 악의적 사이버 활동에 대한 EU의 외교적 공동대응을 위한 프레임워크로, EU 차원에서 악성 사이버 활동에 대한 회원국의 대응을 조정하는 방법을 제공한다[12]. 또한, EU의 사이버 외교 접근방식의 일부로써, 비례적 대응 원칙을 기반으로 사이버 분쟁 예방 및 사이버안보 위협완화에 목적을 두고 있다. 이는 EU가 기존 국제법이 사이버공간에 적용 가능하다는 합의(UNGGE 2015 등)를 강력히 지지함과 악의적 사이버 활동이 국제법에 위배 될 수 있음을 전제로 한다[13].

CDT는 항목별로 구체적인 내용이나 평가방법론은 제공되지 않아 사이버공격 심각도 평가방법론이라고 보기는 어려우나, 유럽의 사이버보안 정책 및 제도가 EU를 중심으로 추진되고 있기에 본 논문에서는 EU에서 악의적인 사이버활동에 대한 심각도 평가를 위해 선정한 평가항목을 국외 평가방법론의 하나로 살펴보았다.

평가항목은 범위(Scope), 규모(Scale), 지속시간(Duration), 강도(Intensity), 복잡성(Complexity), 정교성(Sophistication), 영향(Impact) 7가지이다. 별도의 평가 결과지표는 없으나 회원국에게 사이버공격 발생 시 평가항목을 종합적으로 고려한 평가결과에 기반하여 비례적 대응을 할 것을 제안하였다.

CDT는 주요 국제기구인 EU가 EU 회원국에 국가 및 시민을 대상으로 한 사이버공격 발생 시 심각도를 평가하고, 결과에 기반하여 비례적 대응을 권고하는 원칙을 수립했다는 점에서 의의가 있다. 그러나 평가항목과 평가방법론에 대한 구체적인 내용이 공개되지 않아 국가별로 다양하게 해석할 수 있을 것으로 판단되며, 상당주의 의무에 따라 악의적인 활동이 해당 국가의 영토(territory)에서 발생하는 경우 책임이 있음을 강조하기에 비례적 대응을 위한 대상의 범위가 확장될 가능성이 있다.

2.6 국외 사이버사고·공격 심각도 평가방법론 비교

앞서 살펴본 5가지 사이버공격 심각도 평가방법론의 세부적인 목적과 평가관점은 다소 차이가 있으나, 선정된 평가항목이 사이버공격에 대한 심각도 평가를 위한 항목이라는 점에서 공통점을 가진다. 이에 5가지 평가방법론에서 항목으로 선정된 평가항목을 포괄하도록 평가항목을 분류하였고, Table 5와 같다.

다만, 평가방법론별로 평가항목의 명칭은 다르나 유사한 의미를 갖는 경우가 있어 항목 간의 중복을 피하고자 유사한 평가항목을 그룹화하여 분류하였다. 유사항목 그룹화 시 그룹명은 분류된 항목을 통합하며 대표적 성격을 가지도록 정의하였다.

FIRST의 CVSS는 기술적 측면에 중점을 두고 기술 관련한 평가항목이 세분화되어 있어, 항목을 평가그룹 단위로 분류하고 기술적 항목은 공격의 복잡성·정교성으로 통합하여 분류하였다.

영향 관련 평가항목은 평가방법론에 따라 여러 가지 항목으로 구분되어 있거나 하나로 통합된 경우도 있었으나, 사이버공격으로 인한 주요 피해가 기능과 정보에서 발생하고 있어 기능에 대한 영향과 정보에 대한 영향 2가지로 구분하였다. 기능에 대한 영향은 해당 기관의 정보시스템에 대한 영향으로 시스템 손

상이나 서비스 중단 등을 말하며, 정보에 대한 영향은 해당 기관이 보유한 정보에 대한 영향으로 정보의 유출 또는 조작, 인증정보 도난 등을 말한다. FIRST는 영향 항목이 기밀성, 가용성, 무결성 3가지로 구분되어 있어, 기밀성과 데이터 무결성에 미치는 영향은 정보에 미치는 영향으로 분류하고, 가용성과 시스템 무결성에 미치는 영향은 기능에 미치는 영향으로 분류하였다. EU, 파이어아이, 시만텍은 영향 1가지로 통합되어 있어 기능에 대한 영향과 정보에 대한 영향을 모두 포함하는 것으로 나타냈다.

해당 그룹에 포함되는 평가항목이 있는 평가방법론의 수를 계로 산출했고, 계가 많을수록 더 많은 평가방법론에서 평가항목으로 활용되고 있음을 보여준다.

분류결과 대항목은 3가지로, 공격대상·공격역량·피해규모/영향도이며 3가지 대항목이 사이버공격 심각도를 평가하기 위한 주요요소임을 알 수 있다. 공격대상 대항목은 소항목을 공격부문과 피해시스템 중요도로 구분하고, 공격역량 대항목은 소항목을 공격의 복잡성·정교성과 공격단계로 구분하고, 피해규모/영향도 대항목은 피해규모, 기능에 미치는 영향, 정보에

Table 5. Domain Classification for Foreign Cyber Attack Severity Assessment

Dom.	Option	Detail	NCCIC	EU	FireEye	FIRST	Symantec	T.
Target of Attack	Area of attack	areas of attacked agencies and enterprises, significance of the facility, interdependency	cross-sector dependency	scope				2
			potential impact					
	Significance of damaged system	location where the attack took place and significance of damaged system	location of observed activity		impacted equipment	environment measurement (significance of IT assets)		4
Attack Capability	Complexity and sophistication of attack	complexity and sophistication of attack technologies and existence of targets	actor characterization (level of technology)	sophistication	targets	basic measurement (vulnerability) temporal measurement	distribution	5
				complexity	sophistication			
	Stage of attack	stage at time of attack detection (intrusion, stake-out or completion of attack, etc.)	observed activities					1
Extent of Damage/ Impact	Extent of damage	extent of damage (number of victims, number of infected PCs, amount of damage, etc.)		scale, intensity			wild	2
	Functional Impact	impact of attacks on system functions (system damage and service interruption)	functional Impact	Impact Duration	impact	basic measurement (impact)	damage	5
	Information Impact	impact of attacks on information	information Impact					5
	Recoverability	scope of resources needed for damage recovery	recover ability					1

미치는 영향, 복구가능성으로 구분하였다.

5가지 평가방법론에서 모두 공통으로 공격의 복잡성·정교성, 기능에 대한 영향, 정보에 대한 영향은 평가항목으로 활용하고 있기에, 해당 항목은 사이버공격 심각도 평가를 위해 필수항목인 것으로 판단된다.

평가방법론의 평가대상, 목적, 평가 결과지표는 Table 6과 같으며, 평가목적에 따라 평가 결과지표에 다소 차이가 있는 것으로 나타났다. 평가대상은 평가주체에 따라 국가기관, 주요기반시설 등의 정보시스템 및 산업제어시스템과 일반적인 IT 시스템으로 구분할 수 있다. 목적은 사이버사고 심각도 도출 및 공유를 위한 공통기준마련과 해당 사고의 대응방안 수립으로 구분할 수 있다. 평가 결과지표는 심각도 점수 및 등급과 평가결과 시각화를 위한 매트릭스가 활용되고 있었다.

정보공유 시 사고 심각도에 대한 공통된 기준을 제공하여 관련 업무 종사자의 이해를 돕고, 기준에 근거하여 대응 우선순위 도출하기 위해 점수 및 등급지표가 활용되었다. NCCIC는 사이버사고의 심각도를 공통된 기준으로 평가하고, 정보를 공유하며, 심각도 단계를 기반으로 대응 우선순위와 대응수위(정부의 개입 필요성 등)를 판단하였다. FIRST는 평가를 통해 전 세계에 일관된 취약점 점수와 심각도 수준을 배포하고, 각 조직·기관 등은 패치의 우선순위 결정에 이를 반영하도록 하였다.

평가결과를 시각화하고 대응방안 마련 시 의사결정을 지원하기 위해서는 매트릭스 지표와 기타 추가적인 결과지표가 활용되었다. 파이어아이는 의사소통과 분석이 쉽도록 복잡한 사고 결과를 시각화하여 매트릭스 형태로 표현하였으며, 해당 매트릭스에 과거 사례에 대한 평가결과를 함께 제공하여 대응방안 마련 시 과거의 사고 사례와 비교를 통해 경험적 지식을 활용할 수 있도록 하였다. 시만텍은 평가결과 등급별로 활용 가능한 대응방안을 매트릭스 형태로 제공하여 대응방안 마련 시 참고할 수 있도록 하였다. 또한, FIRST는 전체적인 평가결과 외에도 항목별 결과를 요약한 문자열을 제공하여 항목별 결과를 한눈에 확인할 수 있도록 하고, 각 기관에서 의사결정 시 활용하도록 하였다.

종합적으로 고려한 분석결과는 다음과 같다. 먼저, 사이버공격 심각도를 평가를 위해서는 국가 차원에서 고려가 필요한 사이버공격의 특징과 영향 등을 모두 포함하는 포괄적인 평가항목 도출이 필요하다. 조사한 평가방법론은 특정 부문 또는 시스템 등에 국한되

Table 6. Comparison of Assessment Agents, Targets, Objectives, Result Indicators

Classification		NCCIC	EU	FireEye	Symantec	FIRST
Assessment Agent		State	State	private security service provider	private security service provider	international organization
Target		all US systems in federal agencies /critical Infrastructure	national agencies and citizens	industrial control systems	general IT systems	general IT systems
Objective		identification of priority / distribution of resources for cyber incident response	proportionate response to malicious cyber activities	OT risk management and preparation of the basis for future incident response strategies	estimation of the severity of malware / provision of response options	sharing of information on the severity of vulnerabilities / identification of priority of patches
Result Indicator	Score	scores of the severity of cyber incidents	N/A			scores of the severity of vulnerabilities
	Level	levels of severity			levels of the severity of malware	levels of severity
	Matrix			matrix of cyber incident results	matrix of response	
	Etc.			assessment results of previous cases		string of the results by basic group

어 있다. 그러나 국가 차원의 사이버사고 심각도 평가를 위해서는 공격유형·기관·시스템 등 평가범위가 한정되지 않기에 종합적인 평가항목이 도출되어야 할 것이다.

또한, 사이버공격 심각도 평가의 활용 목적에 따라 점수 및 등급 외에도 다양한 결과지표 활용이 필요하다. 조사된 국외 사이버사고·공격 심각도 평가방법론은 활용 목적에 따라 점수 및 등급, 매트릭스, 항목별 결과 제공을 위한 문자열 등 다양한 결과지표를 사용하고 있다. 따라서 사이버공격 심각도 평가방법론 설계 시 심각도 기준 마련, 정보공유, 기준별 대응방안 마련 등의 목적에 따라 이를 효과적으로 달성하기 위해 적합한 결과지표를 활용해야 할 것이다.

III. 사이버공격 심각도 평가방법론

제안하는 사이버공격 심각도 평가방법론(Cyber Attack Severity Assessment, 이하 CASA)은 사이버공격 발생 시 공격의 피해규모와 영향을 중심으로 공격의 심각도를 평가하기 위한 것으로, 평가결과에 기반하여 국가 차원의 대응 필요 여부와 대외 대응수위를 조정하기 위한 기준 마련이 목적이다. 따라서 CASA의 평가주체는 발생한 사이버공격에 대한 정확한 조사결과를 취합할 수 있고 이를 기반으로 대응방안을 결정할 수 있는 정부기관으로 설정하였다.

기존에 국가정보원의 사이버위기경보는 현재의 사이버위협 수준을 평가 및 공개함으로써 공공 및 민간부문과 위협수준을 사전에 공유하고, 인식을 제고하기 위한 예방적 성격의 지표이다[13]. 반면 제안하는 CASA는 귀속을 기반으로 공격 배후 대상에 대한 사후 대응에 초점을 두고 있어 차이가 있다.

평가항목은 국외 사이버공격 심각도 평가항목을 분류한 결과 하나 이상의 국외 사이버공격 심각도 평가방법론에서 평가항목으로 선정된 항목을 CASA의 평가항목으로 선정하였다. Table 5에서 식별한 공격대상/공격역량/피해규모·영향도를 대항목으로 두고, 대항목 아래 7개의 세부항목을 평가항목으로 도출하였으며 Table 7과 같다. 다만, 공격단계는 제외하였는데 CASA는 공격이 진행 중이거나 공격 가능성이 있는 경우가 아닌 이미 공격이 발생한 사이버공격에 대한 사후 대응을 목적으로 하기 때문이다.

평가항목별 세부항목 및 배점은 국외 사이버공격 심각도 평가방법론을 융복합하고, 이를 한국의 상황에 맞게 수정하였다.

3.1 평가항목

3.1.1 공격대상 - 공격부문

공격부문은 사이버공격이 발생한 부문을 말하며 대상의 중요도와 상호의존성, 즉, 다른 시설에 미치는 영향을 고려하여 세부항목을 나누고 배점하였다. 세부항목은 기반시설과 이에 포함되지 않는 기타 민간시설로 하며 기반시설은 주요정보통신기반보호법에 근거하여 행정, 국방, 치안, 금융, 통신, 운송, 에너지로 정의하였다. 기반시설에 해당하지 않는 민간기관과 기업은 기타 민간시설에 해당한다. 세부항목별 배점은 NCCIC의 부처간 영향(상호의존성) 점수와 우리나라 행정안전부의 주요기반시설 상호의존성 매트릭스 점수를 참고하였다. NCCIC의 부처간 영향(상호의존성) 점수는 미국 기반시설자문위원회(NIAC, National Infrastructure Advisory Council)의 부처간 상호의존성과 위험평가 가이드(2004)를 기반으로 한다. 이는 부처별 전문가를 대상으로 설문조사를 통해 기반시설 16개에 대해서 부처별로 가장 높은 의존도를 갖는 우선순위를 1~3까지 선정하였다[14]. 그 결과 전력계통의 기능장애가 타 기반시설에 미치는 영향이 가장 큰 것으로 나타났으며, 다음은 통신 운송 순으로 나타났다. 그리고 우리나라 행정안전부도 우리나라 기반시설 관리자를 대상으로 한 설문조사를 기반으로 주요기반시설 상호의존도 매트릭스를 도출하였는데, 그 결과 전력은 상대적으로 영향력 및 의존도가 모두 높게 나타났으며 통신·전산 분야 시설은 영향력이 높고 화물·철도 분야 시설은 의존도가 높은 것으로 분석되었다[15]. 따라서 공격부문 점수는 에너지(전력)가 가장 높고, 국방, 통신, 운송, 행정, 치안, 기타 민간시설의 순으로 점수를 부여하였다.

또한, 공격이 하나의 부문이 아닌 다수의 부문에 동시다발적으로 발생한 경우 이를 평가에 반영하기 위해 공격부문의 개수별 가중치를 두었다. 공격이 발생한 부문 중 가장 높은 부문의 점수와 개수별 가중치의 곱으로 공격부문 점수를 산출한다.

3.1.2 공격대상 - 피해시스템 중요도

피해시스템 중요도는 공격자의 행위가 발견된 피해시스템의 중요도를 말하며, 세부항목은 행정안전부의 정보보호등급제에 근거하였다. 정보보호등급제는 행

정안전부가 시스템의 중요도·보안성 정도에 따라 차등적 보안관리 기준을 적용하여 체계적인 보안관리를 하기 위한 것으로, 중앙부처 및 지방자치단체 등에서 운영 중인 정보시스템들을 시스템이 관리하는 정보 또는 서비스의 중요도(기밀성, 무결성) 및 가용성(사용자 수, 연계기관 수) 등에 따라 1~5등급인 공개시스템, 기관단순정보시스템, 중요정보시스템, 유사제어시스템, 국가존립시스템으로 분류하였다[16]. NCCIC의 관찰된 활동 및 위치 항목과 파이어아이의 피해장비 항목은 산업제어시스템의 특성을 고려하여 시스템 종류와 네트워크 위치를 분류한 바 있다.
CASA는 산업제어시스템 외에 일반 정보시스템까지 포함하여 피해시스템의 정보 및 서비스의 중요도를 고려하기 위해 우리나라 행정안전부의 정보보호등급제를 근거로 하였다.

3.1.3 공격역량 - 공격의 복잡성・정교성

공격의 복잡성·정교성은 공격자의 기술 수준을 말하며, 공격이 낮은 기술 수준으로 불특정 대상에게 이루어졌는지 또는 표적을 겨냥하여 지속적으로 정보를 수집하고, 표적에 최적화하여 공격이 수행했는지 등을 고려하여 세부항목을 나누고 배점하였다. 세부항목은 NCCIC의 공격자 특성과 파이어아이의 정교성 항목, FIRST의 기본측정 취약성 항목 및 시간측정 항목을 융합하여 아래와 같이 3가지로 나눠 상/중/하로 정의하였다.

상은 표적에 대해 세부정보를 가지고 대체로 오랜 기간 공격을 준비하며, 공격을 위해 특별히 요구되는 권한이나 조건이 없이 공격자가 원하는 대로 이용이 가능한 높은 기술 수준이 요구되는 경우이다. 중은 알려진 취약점을 표적에 맞게 수정·변형하였거나 물리적인 접근 없이도 네트워크 상에서 가능한 공격인 경우이다. 하는 일반적으로 알려진 취약점과 맬웨어 등을 사용한 낮은 기술 수준이 요구되는 경우이다. 공격의 복잡성과 정교성이 높을수록 높은 점수를 배점한다.

3.1.4 피해규모/영향도 - 피해규모

피해규모는 공격으로 인한 정량적인 피해의 규모를 말하며, 감염 PC 수/감염사이트 수/감염국가 수/피해자 수/피해 금액을 고려하여 세부항목을 나누고 배점한다. 세부항목은 시만텍의 감염도 항목을 참고하여 상/중/하로 정의하였으며, 평가기준을 다양화하여 개인정보유출 또는 자금유출 공격 발생 시 피해규모 산정을 위한 피해자 수와 피해 금액을 추가하였다.

피해자 수와 피해 금액을 기준으로 피해규모 평가 시 상/중/하로 나눴으나, 이를 구분하는 기준에 관한 연구가 활발하지 않아 명확한 근거는 충분하지 않은 상황이다. 따라서 추후 유사 연구결과를 통해 개선할 필요가 있다. 다만, 본 평가방법론에서는 피해자 수와 피해 금액을 기준으로 활용 가능하다는 관점에서 공개된 한국에서 발생한 사이버공격 사례 목록을 분석한 결과 상/중/하 세부항목이 각각 유사한 비율을 갖도록 기준을 정의하였으며, 피해규모가 클수록 높은 점수를 배점하였다.

3.1.5 피해규모/영향도 - 기능에 대한 영향

기능에 대한 영향은 공격이 대상의 기능, 즉, 시스템에 미치는 영향을 말하며, 시스템의 기능 저하, 시스템 혼란, 시스템 파괴 등을 고려하여 세부항목을 나누고 배점한다. 세부항목은 NCCIC의 기능에 미치는 영향, 파이어아이의 가용성, 무결성 영향 항목을 융합하여 영향없음/의심스러우나 발견되지 않음/중요하지 않은 시스템 기능 저하/중요한 시스템 기능 저하/중요하지 않은 시스템의 파괴/중요한 시스템 파괴 6가지로 정의하였다. 기능에 대한 영향은 발생한 시스템의 중요도에 따라 중요도가 높은 경우에 그리고 시스템의 기능 저하보다는 파괴의 경우에 보다 높은 점수를 배점한다.

3.1.6 피해규모/영향도 - 정보에 대한 영향

정보에 대한 영향은 공격이 대상의 정보에 미치는 영향을 말하며, 정보의 손실, 파괴 등을 고려하여 세부항목을 나누고 배점한다. 세부항목은 NCCIC의 정보에 미치는 영향, 파이어아이의 기밀성, 무결성 영향 항목으로 융합하여 영향없음/의심스러우나 발견되지 않음/개인정보 유출/독점정보 유출/핵심 자격증명 침해/중요한 시스템 정보 파괴 6가지로 정의하였다. 영향이 발생한 정보의 중요도에 따라 중요도가 높은 경우에, 그리고 정보의 손실보다는 파괴의 경우에 보다 높은 점수를 배점한다.

Table 7. CASA Assessment Domain and Scoring

No.	Domain	Sub-Domain	Option		
			Name	Details	Value
C1	Target of Attack	Area of attack (w1=6)	administration	Government agencies and public institutions related to administration	40
			national defense	Agencies and institutions related to national defense including the military	80
			public safety	Government agencies and public institutions related to public safety such as the police	40
			finance	Public and private institutions related to finance such as banks	35
			communications	Public and private institutions related to communications such as major internet service providers	75
			transportation	Public and private institutions related to transportation such as roads, rail, ports, aviation, etc.	75
			energy	Public and private institutions related to electricity	100
			other private facilities	Other private institutions that do not fall into the category of infrastructure	25
C2		Significance of damaged system (w2=3)	open system	Open systems that offer open services with insignificant impact on citizens	40
			simple institutional information system	Simple institutional information systems for carrying out tasks	50
			critical information system	Critical information systems related to public health such as personal information and health promotion, etc.	70
			emergency control system	Emergency control systems related to the lives of citizens such as earthquakes, aviation, natural disasters, etc.	80
			system for national existence	Systems for national existence in areas such as national defense, diplomacy, and unification.	100
C3	Attack Capability	Complexity & Sophistication of attack (w3=4)	high	Attacks that require long periods for preparation and reconnaissance and uses various IT tools and ICS vulnerabilities to achieve goal through the use of the target's assets or specific information on the network	100
			medium	Attacks using malware or wireless access modified and optimized to targets for IT-based targeted reconnaissance or information from an insider or known vulnerabilities	80
			low	Attacks using commercial malware or known vulnerabilities, etc.	50
C4	Extent of Damage/Impact	Extent of Damage (w4=4)	high	1,000 computers / 10 infected sites / 5 countries / 20 million victims / damage of 100B or more	100
			medium	50-999 computers / 2 infected sites / 2 countries / 10 million victims / damage of 50B or more	80
			low	49 computers or less / 1 infected site or less / 1 country or less / less than 10 million victims / less than damage of 50B	50

No.	Domain	Sub-Domain	Option		
			Name	Details	Value
C5	Extent of Damage/Impact	Functional impact (w5=5)	no impact		0
			suspected but not identified		40
			degradation of non-critical systems		50
			degradation on critical systems		60
			destruction of and loss of control on non-critical systems		80
			destruction of and loss of control on critical systems		100
C6.		Information impact (w6=3)	no impact		0
			suspected but not identified		40
			leakage of personal information		50
			leakage of exclusive information		60
			infringement of core credentials		80
			destruction of critical system information		100
C7		Recoverability (w7=4)	regular	An enterprise's internal staff can handle an incident without external support	20
			supplemented	Time to recovery is predictable but additional resource is required	40
			extended	Time to recovery is unpredictable and additional resources and external assistance is required. (e.g. formation of multiple project teams across multiple institutions or organizations to handle incident)	60
			not recoverable	Recovery from the incident is not possible. (e.g. leakage and disclosure of sensitive data)	100

3.1.7 피해규모/영향도 - 복구가능성

복구가능성은 피해에 대해 복구가 가능한지 여부와 복구를 위해 필요한 자원의 범위를 말한다. 세부항목은 NCCIC의 복구가능성 항목을 참고하여 대상기관이 자체적으로 피해복구가 가능한지, 아니면 복구를 위해 추가적인 자원 또는 다른 기관의 도움이 필요한지, 또는 복구가 불가능한지로 정의하였다. 복구가 어려울수록 높은 점수가 배점한다.

3.2 평가점수 산출방안

평가는 항목별 점수는 세부항목의 값에 따라 0~100점 사이의 점수를 부여한다. 그리고 항목별 점수와 항목별 가중치 곱을 합산하여 종합적인 점수는 0~100점으로 부여한다. 또한, 공격부문 항목은 항목별 가중치 외에도 개수별 가중치를 함께 고려하여 평가점수를 산출한다.

$$Assessment\ Score = \sum_{n=1}^{7} w_n \times C_n$$

$$C_1 = Max[C_1(i)]/2 \times b_i,$$

where i represents the number of the area of the attack

개수별 가중치는 다수의 부문에 공격 발생 시 심각도가 가중될 수 있기에 이를 반영하기 위한 것으로, 대상 1개부터 8개까지 고려하여 가중치는 정의하였다. 개수별 가중치는 Table 8과 같다. 공격이 1개의 부문에 발생한 경우에는 해당 공격부문의 세부항목 값과 개수별 가중치를 곱하고, 다수의 부문에 동시 발생한 경우 공격이 발생한 공격부문 중 가장 높은 세부항목 값을 갖는 공격부문의 세부항목 값으로 점수와 개수별 가중치를 곱하여 산출한다.

종합적인 평가점수 산출은 예를 들면 다음과 같다. 공격부문은 행정, 금융, 통신이고, 피해시스템은 공개시스템, 공격의 복잡성·정교성은 중, 피해규모는 상, 기능에 대한 영향은 중요한 시스템 파괴 및 통제력 상실, 정보에 대한 영향은 없음, 복구가능성은 확장적

Table 8. Weighted Value for the Number of the Targets

No. of the Targets	Weight	No. of the Targets	Weight
b_1	1.7	b_5	1.9
b_2	1.75	b_6	1.95
b_3	1.8	b_7	2.0
b_4	1.85	b_8	2.0

인 복구인 경우이다. 평가항목별로 점수를 0~100점으로 부여하였으나, 종합점수를 0~100점으로 환산하기 위해 가중치를 Table 9와 같이 환산하였다.

공격부문은 행정, 금융, 통신이 각각 40, 35, 75점이기에 최댓값($Max[C_1(i)]$)은 통신으로 75점이다. 개수별 가중치는 Table 8에서 3개부문에서 발생한 경우 가중치(b_3)가 1.8이고, 항목점수(C_1)는 75/2×1.8=67.5점이다. 공격부문 환산가중치는 0.207이기에 점수는 67.5×0.207=13.97이다.

피해시스템의 중요도는 공개시스템이기에 40점, 환산가중치는 0.103이기에 40×0.103=4.12이다. 공격의 복잡성·정교성은 중이면 80점, 환산가중치는 0.138이기에 80×0.138=11.04이다. 피해규모가 상이면 100점, 환산가중치는 0.138이기에 100×0.138=13.8이다. 기능에 대한 영향은 시스템 파괴 및 통제력 상실 100점, 환산가중치는 0.172이기에 100×0.172= 17.2이다. 정보에 대한 영향은 영향 없음 0점, 환산가중치는 0.103이기에 0×0.103=0이다. 복구가능성은 확장적인 복구 60점, 환산가중치는 0.138이기에 60×0.138=8.28이다. 이 경우 종합점수는 68점으로 심각도는 높음에 해당한다.

Table 9. Weight Conversion

No.	Weight	Weight conversion	No.	Weight	Weight conversion
w_1	6	0.207	w_5	5	0.172
w_2	3	0.103	w_6	3	0.103
w_3	4	0.138	w_7	4	0.138
w_4	4	0.138			

3.3 평가 결과지표

심각도 평가결과는 심각도 단계와 점수로 나타내며, 심각도 단계는 평가점수에 따라 분류하였으며, 단계별 점수 구간은 Table 10과 같다. 심각도 단계는 정상(Baseline) 상황인 0단계를 포함하여 낮음(Low), 중간(Medium), 높음(High), 심각(Severe), 긴급(Emergency) 6가지로 정의한다.

Table 10. Severity Level

Level	Category	Score
0	Baseline	0 - 35
1	Low	36 - 50
2	Medium	51 - 65
3	High	66 - 75
4	Severe	76 - 90
5	Emergency	91 - 100

IV. 한국 사이버공격 사례 심각도 평가결과 분석

4.1 한국 사이버공격 사례 목록

한국에서 발생한 사이버공격을 제안하는 CASA를 이용해 심각도를 평가해보았다. 공격사례는 2000년 이후로 발생한 공격 중 기반시설에 발생한 사이버공격과 민간시설에서 발생한 대규모 사이버공격을 중심으로 27건의 목록을 구성하였다. 공격사례 정보는 언론에 공개된 내용을 기반으로 평가하였으며, 귀속 정보는 추정사항까지 포함하였고, Table 11과 같다. 귀속은 북한(NK), 중국(CN), 한국(KOR), 러시아(RU), 알수없음(Unknown)으로 나타내었으며, 국가인 경우(S), 국가지원그룹인 경우 (SG), 민간그룹인 경우(PG)로 표기하였다.

4.2 심각도 평가결과

27건의 사례 중 심각도 단계가 중간인 경우가 14건으로 전체의 51%, 높음인 경우가 8건으로 전체의 29를 차지하였으며, 중간과 높음 단계의 공격이 가장 많은 것으로 나타났다. 높음과 심각 단계 사이버공격 8건 중 1건은 러시아, 나머지 7건은 북한의 소행으로 추정되며, 한국 사이버공격 사례 목록 중 북한 소행으로 추정되는 공격이 64%로 우리나라에서 일어나는 대규모 사이버공격의 절반 이상이 배후가 북한인 것으로 드러났다.

다만, 평가에 활용된 공격사례 정보가 언론에 보도된 내용만을 기반으로 하였기에 평가결과의 객관성에 한계가 있을 수 있으며, 보다 객관성 있는 평가결과 도출을 위해서는 사고 조사기관에서 수집한 정확한 정보를 기반으로 해야 할 것이다.

4.3 한국의 사이버위협 및 대응 동향 분석

공격사례 분석결과 우리나라에서는 에너지, 국방 분야 등 국가기밀과 첨단 산업·기술 정보를 획득하기 위한 국가 또는 국가의 지원을 받는 단체의 것으로 의심되는 스파이 행위가 꾸준히 발생하는 경향을 보였다.

한수원 해킹(2014), 한국 평창올림픽 해킹(2018) 등 국가 또는 국가의 지원을 받는 단체가 정치적 영향력 행사, 사회적 혼란 야기를 목적으로 공공 정보통신망을 침투하여 파괴·마비시키는 공격이 증가하였다. 또한, 불특정 다수를 노린 국내·외 동시다발적인 공격이 감소하고, 하나의 대상을 목표로 정한 뒤 침입에 성공할 때까지 지속적으로 다양한 방법을 사용하여 공격하는 APT가 증가하였다.

한국 코인레일 해킹(2018), 한국 빗썸 해킹(2018), 한국 업비트 해킹(2018) 등 최근 가상화폐 거래소에 대한 금전적 이익을 노리는 사이버공격이 증가하였으며, 이는 북한이 사이버공격을 통해 자금 확보에 집중하고 있는 것과 무관하지 않다. 유엔 대북제재위 전문가패널 보고서에 따르면 북한이 은행이나 가상화폐거래소에 대한 해킹으로 20억 달로 규모의 자금을 탈취했다고 평가되고 있으며, 한국은 최대 피해국이고, 빗썸 해킹을 비롯하여 피해사례가 10건에 이른다고 밝혔다[17].

지하철 해킹(2015), 인터파크 개인정보 유출(2016), 한국 사이버사령부 해킹(2016), 한국 방사청 해킹(2018) 등 공격 피해가 공격 발생 시 즉각적으로 드러나기보다는 장기간 공격대상 시스템에 남아 있다가 공격자의 금전적 요구 시나 우연한 계기로 밝혀져 피해규모와 영향을 정확하게 파악하기 어려워지고 있다는 특징이 있다.

Table 11. List and Severity Levels of Cyberattacks in the ROK

No.	Month/Year	Cyberattack	Severity	Score	Attribution
1	JAN 2003	JAN 25 Internet crisis	High	68.45	NK(S)
2	FEB 2008	personal data Leak, Auction, 18.63M users	Medium	52.67	CN(PG)
3	JUL 2009	JUL 7 DDoS attack	High	72.83	NK(S)
4	MAR 2011	MAR 4 DDoS attack	Medium	60.90	NK(S)
5	APR 2011	paralyzint the computer network, NongHyup (National Agricultural Cooperative Federation)	Medium	63.40	NK(S)
6	JUL 2011	personal data leak, Nate, 35M users	Medium	58.19	CN(PG)
7	OCT 2011	hacking, National Election Commission	Low	45.66	CN(PG)
8	JUN 2012	hacking, JoongAng Ilbo	Medium	60.60	NK(S)
9	MAR 2013	MAR 20 computer system Crisis	High	73.92	NK(S
10	JUN 2013	JUN 25 cyber terror	High	70.48	NK(S)
11	JAN 2014	KB Card, Lotte Card, etc., 20M customers	Medium	53.05	KOR(PG)
12	MAR 2014	SKT, LGU+, 12.3M customers,	Medium	61.47	KOR(PG)
13	MAR 2014	personal data leak, KT	Low	48.28	KOR(PG)
14	DEC 2014	hacking, Korea Hydro & Nuclear Power	Severe	79.31	NK(S)
15	OCT 2015	hacking, subway lines 1-4	Medium	62.84	NK(S)
16	JAN 2016	emails impersonating the Blue House	Low	42.55	NK(S)
17	JUN 2016	hacking, Cyber Command	High	72.00	NK(S)
18	JUL 2016	personal data leak, Interpark	Medium	58.19	NK(S)
19	MAR 2017	retaliatory attack for Korea's stance towards China's THAAD	Baseline	29.31	CN(SG)
20	JUL 2017	20 companies including Eugene Futures, DBpia, etc.	Medium	57.37	CN(SG)
21	OCT 2017	hacking, Daewoo Shipbuilding's drawings, etc. of Aegis Vessels	High	67.86	NK(S)
22	DEC 2017	hacking, Youbit	Medium	64.74	NK(S)
23	FEB 2018	hacking, ROK Pyeongchang Olympics	High	71.72	RU(S)
24	JUN 2018	hacking, Coinrail Korea, damage worth 40B KRW	Medium	59.22	Unknown
25	JUN 2018	hacking, Bithumb Korea, damage worth 35B KRW	Medium	59.22	NK(S)
26	NOV 2018	hacking, Korean Military Defense Acquisition Program Administration	High	72.34	NK(S)
27	NOV 2019	hacking, UPbit, damage worth 58B KRW	Medium	63.36	NK(S)

그러나 한국은 사이버공격 발생 시 피해를 복구하고, 재발 방지를 위해 국가 정책과 제도를 수정하는 형태로 대내 방어적 대응이 대부분이다. 사이버공격에 대한 대응방안은 27건의 사례 중 전체 27건의 사례에서 방어적인 대응방안을 취하고 있다.

특히, 공격 발생 시에 대한 대응체계가 명확하지 않아 사후적 대응을 위해 국민 정서와 여론을 의식하여 정책 및 제도를 급하게 마련하는 경우가 많았다. 2009년 7.7 DDoS 공격 발생 시에는 국가사이버위기종합대책을 발표하였고, 2011년 3.4 DDoS와 농협전산망 공격에서는 국가사이버안보마스터플랜을 수립하였다. 2013년 6.25 사이버테러 발생 시에는 사이버안보종합대책을 수립했고, 2015년 한수원 해킹사고 시에는 국가사이버안보태세 종합대책을 수립했다[18]. 정책 및 제도가 근본적인 법적 기반 개선이나 체질 개선이 아닌 시급한 상황에 대한 복구 및 방어에만 초점을 맞추고 있으며, 국가사이버안보기본법 등 관련 법안 마련도 추진은 하였으나 반대에 부딪히고 대책 수립에 그쳤다.

정부 주도로 조사를 통해 공격의 원인과 배후를 밝히고 배후가 북한이면 공개적으로 지명하고 있으나, 러시아·중국 등 그 외 국가의 공격에 대해서는 공개적인 귀속 사례가 많지 않으며 공격자에 대해서도 기소나 별도의 제재를 가한 바가 없다. 특히, 한국 평창올림픽 사례의 경우 러시아 사이버공격에 대해서도 정부의 공개적인 귀속은 없었다.

V. 결 론

사이버공격의 주체와 수단이 다양해지고, 국가안보에 위협적인 사이버공격이 증가하고 있어 사이버공격에 대하여 대내 방어적 대응 외에 대외 비례적 대응을 통한 억지력 확보가 필요하다. 이에 본 논문에서는 사이버공격 발생 시 공격의 속성에 따라 심각도를 평가할 수 있는 방법론을 개발하였다. 제안하는 CASA의 목적은 사이버공격 발생 시 공격의 심각도를 평가하여 국가 차원의 대응 필요 여부와 대응수위 조정을 위한 기준을 마련하는 것이며, CASA가 우리나라의 소극적인 사이버공격 대응체계를 강화하고 정부의 비례적 대외 대응 수행 마련의 기반이 되기를 기대한다.

평가방법론 개발을 위해서는 국외 사이버공격 심각도 평가방법론의 연구 동향을 분석하고, 이를 기반으로 CASA의 평가항목을 도출하였다. 또한, 항목별 가중치 및 평가점수 산출방안을 마련하고, 평가점수에 따라 사이버공격 심각도를 6단계로 분류하였다. 그리고 한국에서 발생한 사이버공격 사례 27건을 CASA를 이용해 심각도를 평가하고, 한국의 사이버위협과 한국 정부의 사이버공격에 대한 대응 동향을 분석하였다. 그 결과 심각도 단계가 중간인 공격이 가장 많은 것으로 나타났으며, 심각도가 높은 사이버공격은 북한이 배후인 경우가 많았다. 그러나 한국의 사이버공격 대응방안은 대부분 소극적인 대내 역량강화 방안 마련에 국한되어 있었다.

추후 CASA의 실제적인 활용을 위해서는 평가항목 및 가중치에 대한 전문가 검증을 통해 객관성을 확보할 필요가 있다. 또한, 정부의 능동적인 대외 대응 유도를 위해 활용되기 위해서는 사이버공격의 심각도에 따라 국가가 어떤 대응방안을 활용 가능한지에 대한 연구가 수행될 필요가 있으며, 심각도 외에 국가 대응방안 수립을 위해 필요한 추가적인 고려사항에 대한 검토가 필요하다.

References

[1] Michael N. Schmitt, "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law," Harvard National Security Journal, vol. 8, pp. 239-282, May. 2017, .

[2] OECD Legal Instruments, "Recommendation of the Council on Digital Security of Critical Activities," pp. 1-19, Dec. 2019.

[3] Council of the EU, "Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities," pp. 1-16, Oct, 2017.

[4] National Security Office of Cheong Wa Dae, "National Cybersecurity Strategy," pp. 16-17, Apr. 2019.

[5] US-CERT, "NCISS Incident Scoring Demo" https://www.us-cert.gov/nciss/demo, Accessed Oct. 21, 2021.

[6] Department Homeland Security, "National Cyber Incident Response Plan", pp. 38-39, Dec. 2016.

〔7〕 The U.S. Whitehouse, "FactSheet:President Policy Directive on United States Cyber Incident Coordination" https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/fact-sheet-presidential-policy-directive-united-states-cyber-incident-1, Accessed Oct. 21, 2021.
〔8〕 Mandiant, "The FireEye OT-CSIO" https://mandiant.com/resources/ontology-understand-assess-operational-technology-cyber-incidents, Accessed Oct. 21, 2021.
〔9〕 Petraq Papajorgji, Automated Enterprise Systems for Maximizing Business Performance, 1st Ed., IGI Global, pp. 233-234, 2015.
〔10〕 Joseph Boyce, Daniel Jennings, Information Assurance:Managing Organizational IT Security Risks, 1st Ed., Butterworth-Heinemann, pp. 253-254. 2002.
〔11〕 FIRST, "Common Vulnerability Scoring System version 3.1" https://www.first.org/cvss/v3.1/specification-document, Accessed Oct. 21, 2021.
〔12〕 Council of EU, "Draft Council Conclusions on a Framework for a joint EU Diplomatic Response to Malicious Cyber Activities(Cyber Diplomacy Toolbox)," pp. 1-5. June 2017.
〔13〕 NIS, "Cyber crisis Alarm" https://www.nis.go.kr:4016/AF/1_7_1_2.do, Accessed Oct. 28. 2021.
〔14〕 Martin G. McGuinn, "Cross Sector Interdependencies and Risk Assessment Guidance," National Infrastructure Advisory Council, pp. 94, Jan. 2004.
〔15〕 Jindong Shin, Analysis of Interdependencies and Cascading Failure Effects on Critical Infrastructure", National Disaster Management Institute, pp 89-103, Dec. 2013.
〔16〕 Ministry of the Interior and Safety, "Security Management by Information System Level" https://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bsId=BBSMSTR_000000000008&nttId=71455,Accessed Oct. 28. 2021.
〔17〕 UN Security Council, "Midterm report of the Panel of Experts submitted pursuant to resolution 2464(2019)," pp. 26, Aug. 30, 2019.
〔18〕 NIS et al., "White Paper on Information Security 2020," pp. 6-7, May. 31, 2020.

〈저자소개〉

배 선 하 (Sunha Bae) 정회원
2007년 2월: 한양대학교 미디어통신공학과(학사)
2009년 1월: 한국과학기술원 전기 및 전자공학과(석사)
2009년 1월~2013년 2월: LIG 넥스원 주임연구원
2013년 4월~2014년 1월: 두산중공업 기술연구원 주임연구원
2015년 2월~현재: 국가보안기술연구소 선임연구원
〈관심분야〉 정보보호, 정책평가, 기반보호정책

유 영 인 (Young-in You) 정회원
2013년 8월: 서울시립대학교 수학과 졸업
2015년 8월: 고려대학교 정보보호대학원 석사
2019년 2월: 고려대학교 정보보호대학원 박사
2018년 12월~현재: 국가보안기술연구소 선임연구원
〈관심분야〉 정보보호, 위험관리, 안보정책

김 소 정 (So Jeong KIM) 종신회원
1998년 2월: 부산대학교 사학과(학사)
2001년 2월: 경희대학교 평화복지대학원 동북아학과(석사)
2005년 2월: 고려대학교 정보보호대학원 정보보호정책학과(박사)
2001년~2002년: 한국전파진흥협회 ITU-WRC 담당 연구원
2004년~현재 국가보안기술연구소 정책연구실장, 책임연구원
〈관심분야〉 사이버안보 전략, 정보보호정책, 기반보호정책