Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.5, Oct. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.5.951

사이버 위협 지표 간 중요도 비교 분석 연구

이 로 운,[1†] 권 헌 영[2‡]
[1,2]고려대학교 정보보호대학원 (대학원생, 교수)

Priority Assessment of Cyber Threat Indicators

Ro-woon Lee,[1†] Hun-yeong Kwon[2‡]
[1,2]School of Cybersecurity, Korea University (Graduate student, Professor)

요 약

정보 자산에 대한 사이버 위협이 증가하면서 위협과 관련된 정보들을 빠르게 공유하는 것이 무엇보다 중요해졌다. 본 연구에서는 국내외 사이버 위협 정보의 공유 현황을 살펴보고 시장에서 공유되고 있는 위협 지표별 우선순위를 도출하여 위협 지표의 중요도를 평가하였다. 분석은 AHP 기법을 활용하였으며, 공격자 및 감염자 지표, 역할 지표, 악성 파일 지표, 기법 및 전파 지표의 네 가지 평가기준과 해당 기준별 세부항목에 대한 쌍대비교를 통해 이루어졌다. 분석 결과 상위 평가 기준 사이에서는 악성 파일 지표가 가장 중요한 것으로 확인되었으며, 각 기준별 세부 항목간 비교에 있어서는 공격자 및 감염자 지표의 경우 감염자 IP가, 역할 지표의 경우 C&C 정보가, 악성 파일 지표의 경우 악성코드 지표가, 기법 및 전파 지표의 경우 스미싱 관련 지표가 보다 중요한 요소로 확인되었다. 이와 같은 결과는 위협 정보에 대한 소비자의 선호도와 정보 제공자의 기여도를 판단하는 자료로서 정보 공유 활성화에 도움이 될 수 있을 것이다.

ABSTRACT

With the growing cyber threat to information assets, it has become important to share threat information quickly. This paper examines the sharing of cyber threat information and presents a method to determine the importance of threat indicators in the information sharing market by calculating weights. The analysis was conducted using AHP techniques, with a pairwise comparison of the four factors(attacker & infected system indicators, role indicators, malicious file indicators, technique & spread indicators) and the details of each factor. Analysis shows that malicious file indicators are the most important among the higher evaluation factors and infected system IP, C&C and Smishing are the most important factors in comparison between detailed items. These findings could be used to measure the preference of consumers and the contribution of information provider for facilitating information sharing.

Keywords: Cybersecurity Information, Information Sharing, Priority Analysis

I. 서 론

오늘날 정보 자산에 대한 위협은 더욱 지능적이고 다양화되고 있다. 취약점에 미처 대처하기 전에 이루어지는 제로데이 공격은 공격의 속도가 얼마나 빠르게 이루어지고 있는지를 보여주는 대표적인 사례이다. 이에 따라 정보보호 측면에서도 위협에 대한 정보를 보다 신속하게 획득하고 이에 대처하는 것이 중요해졌다. 나아가 빅데이터 기술의 발전과 더불어 개별 주체들이 보유한 위협 정보를 서로 공유하여 정보 획득 비용을 낮추고 신속한 대응을 추구하는 시도 또한 등장하였다. 국내의 경우에도 한국인터넷진흥원을

Received(06. 14. 2021), Modified(1st: 08. 06. 2021, 2nd: 09. 08. 2021), Accepted(09. 09. 2021)
† 주저자, leelowoon15@korea.ac.kr
‡ 교신저자, khy0@korea.ac.kr (Corresponding author)

비롯한 정부 기관을 중심으로 위협 정보 공유 시스템(C-TAS)과 ISAC(Information Sharing & Analysis Center) 등을 운영하여 사이버 위협 정보를 보다 효과적으로 공유하기 위해 노력하고 있다.

본 연구에서는 앞에서 설명한 사이버 위협 정보와 위협 정보 공유 시스템이 가지는 의의에 대해 살펴보고, 나아가 위협 정보 공유 시장을 활성화할 수 있는 방법에 대해 확인한다. 또한 정보보호 전문가를 대상으로 한 AHP(Analytic Hierarchy Process) 기법을 이용하여 위협 지표들 사이의 우선순위를 확인하고, 해당 분석 및 결과가 참여자들과 정보 공유 시장 활성화에 어떠한 의미를 가질 수 있는 지 살펴본다.

본 연구의 구성 체계는 다음과 같다. 제 1장에서는 연구의 목적과 배경, 방향에 대해 제시하였으며, 제 2장에서는 사이버 위협 정보의 개념을 정의하고 정보 공유의 필요성을 살펴본다. 제 3장에서는 국내외에서 운영되고 있는 위협 정보 공유 시장의 현황 및 한계점에 대해 살펴보았다. 제 4장에서는 AHP 기법을 적용하여 위협 지표간 중요도 분석과 결과를 제시하였다. 마지막으로 제 5장에서는 본 연구의 결과를 분석하고 한계점 및 시사점에 대해 서술하였다.

II. 이론적 배경

2.1 사이버 위협 정보의 개념

미국 위험성 평가 가이드라인인 NIST SP 800-30에 따르면 사이버 위협이란 "무허가 접근, 파괴, 공개 또는 정보 수정을 통해 조직 운영(사명, 기능, 이미지 또는 평판 포함), 조직 자산, 개인, 기타 조직 또는 국가에 악영향을 미칠 수 있는 모든 상황 또는 사건"을 말한다[1]. 때문에 사이버 위협은 그 주체와 대상에 따라 다양하게 나타날 수 있으며. 이에 대응하기 위한 정보 역시 다양한 종류와 형식을 가지게 된다. 미국 위협 정보 공유 가이드라인인 NIST SP 800-150에 따르면 사이버 위협 정보는 ①지표(Indicator), ②기술, 기법 및 절차(Tactics, Techniques, and Procedures), ③보안 경고(Security Alerts), ④위협 인텔리전스 보고서(Threat Intelligence Reports), ⑤도구 설정(Tool Configurations)으로 구분되어 진다[2]. 첫째, 지표는 임박하거나 진행된 공격에 대한 기술적 산출물 또는 관측 결과를 의미한다. C&C 서버의 IP 주소, URL, 파일의 해시 정보 등이 위협 지표의 예에 해당한다. 다음으로 기술, 기법 및 절차(TTPs)는 위협에서 확인되어지는 공격자의 행위 정보를 의미한다. 기술에서 기법, 절차로 내려갈수록 행위에 대한 보다 세부적인 내용을 의미하며, 공격 메커니즘과 도구 등이 어떻게 활용되었는지를 보여준다. 보안 경고는 권장사항, 게시판, 취약점 노트 등으로도 알려져 있으며, 취약점과 악용 및 기타 보안 이슈에 대해 읽을 수 있는 기술적 알림을 제공한다. 위협 인텔리전스 보고서는 TTPs, 공격자, 대상 시스템 및 정보 유형, 더 나은 상황 인식을 제공하는 기타 위협 관련 정보를 기술한 문서이다. 또한 이는 조직의 의사결정 과정에 이용하기 위해 수집, 분석, 변환된 정보를 의미한다. 마지막으로 도구 설정은 위협 정보의 수집과 교환, 처리를 위해 사용되는 도구를 위한 권장 사항이다. 예를 들어 루트킷을 설치하고 사용하는 방법에 대한 지침이 이에 속한다.

앞에서 살펴본 정보 유형 중 사이버 위협 지표의 경우 기초적인 정보이자 실제로 관측되고 공유된 결과로서, 공격 메커니즘에 대한 복잡한 분석 없이도 참여자들에 의한 공유가 가능하다. 그러나 한국인터넷진흥원의 2020년 4분기 사이버위협동향보고서에 따르면 위협 지표를 통한 공유 활동이 상대적으로 저조한 것으로 조사되었으며, 다수의 정보를 선별적으로 반영하기에 어려움이 있다는 점을 보여주고 있다[3]. 따라서 위협 지표들의 선별과 관련된 분석이 우선적으로 필요할 것으로 보이며, 본 연구에서는 다양한 위협정보 유형 중 지표(Indicator)를 그 대상으로 하여 논의한다.

2.2 사이버 위협 정보 공유의 의의

Anthony Rutkowski(2010)에 따르면 사이버 보안정보교환(Cybersecurity Information Exchange)은 위협 정보의 공급자와 수요자인 조직 또는 사람, 디바이스와 프로세스 사이에서 이루어지는 활동으로 사이버 공격에서 자신의 자산을 보호하고 보다 신속하게 대응하기 위한 협력체계를 구성하는 것이 목적이다[4]. 이와 같은 정보 공유 활동과 관련해 고유미(2012)는 정보공유 활동은 개별 조직의 정보 수준을 전체적인 수준으로 확장시켜 조직 사이의 연결과 경제적 가치를 창출한다고 주장하였다[5]. Gordon(2003)의 경우에도 보안 정보 공유가 가지는 경제적인 이득에 주목하였으며[6], Cavelty(2007), Hausken (2007)은 지속적인 정

보 공유 활동이 경제적인 효과를 가지기 때문에 범정부 차원의 노력이 필요하다고 보았다[7][8]. 실제로 2011년 3월 발간된 국회 입법조사처의 보고서에 따르면 2011년 3.4 DDoS 공격의 경우 2009년 발생한 7.7 DDoS 공격보다 약 37,000여 대의 컴퓨터가 더 많이 악성코드에 감염되었지만 신속한 공격 차단으로 인해 피해 규모는 더욱 적었던 것으로 확인되었다. 이는 7.7 DDoS 공격 때 확보된 정보에 기반하여 네트워크 간 공유와 협력을 이뤄냈기 때문이라고 보고 있다[9].

사이버 위협 정보 공유에 영향을 미치는 요인에 대한 선행 연구들을 살펴보면 김하영(2017)은 사이버 위협 정보 공유에 영향을 미치는 요인을 TOE 프레임 워크에 기반하여 법적책임, 자율화, 품질평가, 익명성, 최고경영자의 지원으로 나누어 분석하였다. 이에 따르면 정보 공유 시에 발생하는 법적 위반 사항에 대한 면책, 민간 주도의 정보 공유 시스템 운영, 공유되는 정보에 대한 평가 등이 영향을 미친다고 보았다[10]. 박지백(2018)은 사이버 위협 정보의 공유 활성화 방안과 관련하여 표준화, 공유 체계 장벽 제거, 정보 공유에 대한 보상 체계, 정보 평가 시스템의 구축 등이 영향을 미친다고 보았다[11]. 김애찬(2016)은 사이버 위협 정보 공유 체계 수립 시 확인되는 정책적 요구사항과 기술적 요구사항에 대해 AHP 분석 방법을 이용하여 우선순위를 도출하였다. 연구에 따르면 정책적 요구사항이 기술적 정책 사항에 비해 중요한 것으로 확인되었으며, 정책적 요구사항에서는 법적 근거의 마련과 정보 관리체계 마련이 중요한 요인으로 나타났다. 반면 기술적 요구사항의 경우 정보의 표현방식, 전송규격 표준화와 정보 수집 방법, 신뢰성 개선이 중요한 요인인 것으로 나타났다[12].

본 연구에서는 사이버 위협 정보 공유에 영향을 미치는 다양한 요인들 중에서도 '공유되는 정보'의 역할에 초점을 맞추어, 실제로 공유되고 있는 위협 지표들 간 우선순위에 대해 도출하고 그 결과가 사이버 위협 정보 공유 활성화에 있어 어떠한 의미를 가지고 있는지에 대해 살펴본다.

III. 국내외 위협 정보 공유 현황 및 한계점

3.1 C-TAS와 ISAC

C-TAS(Cyber Threat Analysis & Sharing)는 여러 산업 분야에 걸쳐 광범위하게 발생하고 있는 침해사고에 대응하기 위한 사이버 위협 정보 수집•분석•공유 시스템이다[13]. 2013년 7월에 발표된 '국가 사이버 안보 종합대책'에 기반하여 설립된 C-TAS는 사이버 위협 정보의 공유 및 신속한 대응 체계를 마련하기 위해 한국인터넷진흥원(KISA)의 관리 하에 운영되고 있다. C-TAS에 공유되는 위협 정보들은 API 및 홈페이지를 통한 다운로드 방식을 이용하여 제공되고 있으며, 정보 공유 대상 및 범위에 차등을 둔 양방향 정보공유 체계로 이루어져 있다. 제공되는 정보의 경우 단일 지표, 분석 보고 등을 포함한 총 8개 항목, 40여 종의 정보로 정보 수집 및 분석, 검증 단계를 거쳐 공유되어진다.

ISAC(Information Sharing & Analysis Center)은 유사 업무 분야별로 전자적 침해 행위 및 사이버 위협에 대해 공동으로 대응하기 위한 정보공유분석센터이다[14]. 지난 1998년 미국에서 금융 ISAC을 비롯한 8개 분야의 ISAC을 운영한 이래로 세계 각 국에서 도입하여 시행하고 있다. 우리나라의 경우에도 '정보통신기반보호법(2001.1)'에 근거하여 지난 2002년 12월 금융감독원 주도의 금융 ISAC을 시초로, 통신과 지자체, 의료 ISAC을 함께 운영중에 있다.

다만 한국인터넷진흥원에서 한국침해사고대응팀협의회 회원인 73개사에 대해 조사한 2020년 4분기 사이버위협동향보고서에 따르면 수집되는 위협 정보에 대한 만족도는 매우만족(9.5%), 만족(20.55%), 보통(53.24%), 부족(16.44%)으로 나타나 수집되는 위협 정보에 대한 만족도는 크지 않은 것으로 나타났다. 수집하는 위협 정보 유형에 대한 설문에서는 취약점 정보(87.67%), 사고대응 보고서(63.01%), 보안 트렌드(61.64%), 위협 지표(41.10%)로 확인되었으며, 상대적으로 위협 지표를 활용한 정보 공유의 효과가 낮은 것으로 조사되었다. 위협 정보와 보안 트렌드를 활용하는데 겪는 어려움에 대해서는 정보의 양이 너무 많아 선별적으로 반영하는데 어려움이 있다는 의견과 최신 및 맞춤형 정보를 구하기 어렵다는 의견이 있었다[3].

3.2 美 정보 공유법(CISA)

미국 사이버안보 정보공유법 (CISA: Cyber Information Sharing Act)은 사이버 위협 정보의 공유를 장려하고 자발적인 위협 정보 공유 체계의

설립을 위해 지난 2016년에 제정된 법이다. 주요 내용으로 정부와 민간 사이의 자유로운 정보 공유, 공유에 따른 민·형사상의 책임 면제 등을 다루고 있다.

안정민(2018)에 따르면 CISA를 통해 민간 기업들은 보유한 위협정보를 자발적으로 공유할 수 있으며, 또한 이렇게 수집된 정보는 신체 및 경제적 피해를 유발하는 심각한 위협에 대처하고 이를 예방 또는 완화시키기 위해 사용될 수 있다. 정보 공유에 따른 기업들의 법적 책임에 대해서도 특정 조건을 만족할 경우 면제하는 규정을 두고 있다. 다만 공유되는 위협 정보에 특별히 지정된 개인정보가 포함된 경우, 기업은 해당 정보를 기술적으로 삭제한 뒤 제공해야 한다. 마지막으로 연방정부는 사이버 위협지표들과 방어적 조치들을 공유하기 위한 구체적인 절차를 마련하여야 한다고 명시하여 위협 정보 공유에 있어 연방정부의 역할도 강조하고 있다[15].

위와 같이 효과적인 정보 공유 체계를 설립하기 위해 제정된 법임에도 불구하고, CISA에 기반한 위협 정보 공유 체계는 다음과 같은 한계점을 가진다. 우선 위협 정보 공유 시 노출된 개인정보가 다양하게 이용될 소지가 있다. 신체 및 경제적 피해를 유발하는 심각한 위협이 발생한 경우에만 이용할 수 있다고 규정하고 있지만, 이와 같은 기준의 내용이 구체적이지 않고 모호하다는 지적이 존재한다[15]. 나아가 정보 공유자에 대한 인센티브 역시 한정적이다. 동법 Section 106(b)에서는 민간 기업이 다른 민간기업 또는 연방정부와 정보를 공유할 때 발생하는 법적 책임을 면제하는 내용을 담고 있다. 이는 정보 공유 시 발생할 수 있는 법적 책임을 인지하고 이러한 책임을 어느 정도 경감시켜 주었다는데 의의가 있으나, 위협 정보 제공에 대한 기여도 판단이나 보상 체계에 대해서는 다루고 있지 않다는 한계점이 있다.

3.3 CTA

CTA(Cyber Threat Alliance)는 글로벌 보안 기업들을 주축으로 사이버 위협에 공동으로 대응하는 민간 위협 대응 플랫폼이다. 현재 비영리기관으로 운영되고 있으며, 산재되어 있는 다양한 위협 정보들을 통합하여 사이버 위협에 신속하게 대응하기 위한 목적으로 마련되었다. CTA에 참여하기 위해서는 일정량의 위협 정보를 클라우드 협업 플랫폼인 CTA 플랫폼에 제공해야 하며, 이러한 정보에 대한 심사과정 역시 뒤따른다. 또한 의심 파일 정보 공유 사이트인 VirusTotal에서 조회되지 않는 1000여 개의 신종 악성코드 샘플들을 제공할 수 있어야 참가 자격이 주어진다[16]. 2021년 5월 현재 총 33개의 보안 벤더사들이 정보 공유에 참여하고 있으며, 각 기업들은 자신들이 제공한 정보의 가치와 양에 따라 서로 다른 접근 권한을 가지게 된다[17]. 다만 이러한 CTA의 운영과 관련하여 지나치게 폐쇄적이어서 모든 이해관계자들이 정보 공유의 혜택을 누리기 어렵다는 비판 역시 존재한다[16].

IV. 사이버 위협 지표 간 우선순위 비교

4.1 연구모형

4.1.1 계층분석기법(AHP)

AHP(Analytic Hierarchy Process)는 미국 피츠버그 대학의 T. L. Saaty 교수에 의해 처음 개발된 계층분석기법이다. AHP 기법은 수량화하기 어려운 복잡한 문제를 단순화하여 두 가지 항목씩 쌍대비교함으로써 가중치를 도출하며, 이러한 과정은 항목의 계층적인 구성과 단계적인 실행을 통하여 이루어진다[18][19]. 계층의 가장 상위 항목은 평가의 목적을 설정하고, 그 하위 항목에는 목적에 부합하는지를 판단하기 위한 평가기준을 설정한다. 추가로 가장 아래에 하위 항목을 만들어 각각의 평가기준들을 더욱 세분화하여 세부적인 평가기준들을 설정하기도 한다. AHP 기법의 장점은 수량화하거나 모델화하기 어려운 복잡한 문제를 보다 단순화시켜 계량화하는 것에 있다[20]. 특히 자연과학적 분석을 진행하기 어려운 인간의 주관적인 판단에 대한 연구에서도 합리적인 총합화 과정을 이용해 의사결정을 도출할 수 있다[21].

4.1.2 조사대상 및 평가기준

AHP 기법에서는 의사결정을 위한 계층적인 구조를 설정하고, 평가 기준들 사이의 쌍대비교를 진행하기 위한 매트릭스를 구성한다. 본 연구에서는 상대적으로 공유 효과가 적은 것으로 나타난 위협 지표(Indicator)에 대해 분석을 진행하였으며, 이를 통해 지표별 중요도를 평가하여 정보의 선별적 반영에 기여하고자 하였다. 대상 지표로는 한국인터넷진흥원의 C-TAS를 통해 실제로 공유되고 있는 주요 단일

Table 1. Research Hierarchy

Overall Objective	Criteria	Sub-criteria
Prioritization of Cyber Threat Information	Attacker & Infected System Indicators	Attacker IP
		Infected System IP
	Role Indicators	Malware Distribution Sites
		Identity Theft Sites
		Command & Control Servers
	Malicious File Indicators	Malware
		Ransomware
	Technique & Spread Indicators	Phising
		Pharming
		Smishing
		Malicious Emails

지표 항목 11개를 분석 대상으로 선정하였다. 11개의 지표는 각각 공격시도 IP, 감염자 IP, 유포지, 정보유출지, C&C, 악성코드, 랜섬웨어, 피싱, 파밍, 스미싱, 악성이메일로 구성되며, 지표별 성격과 특징에 따라 공격자 및 감염자 지표, 역할 지표, 악성 파일 지표, 기법 및 전파 지표로 상위 계층을 분류하였다. AHP 분석에 있어서의 세부 계층 구성은 Table.1과 같다.

4.2 표본추출 및 분석절차

본 연구에서는 사이버 보안과 관련된 업무를 수행하고 있는 전문가 총 9명을 대상으로 설문을 진행하였으며 각 설문의 일관성 비율(Consistency Ratio)은 0.2 이하가 되도록 설정하였다. 일반적으로 AHP 분석의 일관성 비율은 0.1 이하일 경우 합리적인 일관성을 가진다고 판단하나, 김영문·채수원(1996)은 AHP 분석에 익숙하지 않은 대상자에 대해 0.2까지 허용 가능한 일관도 기준으로 판단하고 있다[22]. Saaty & Kearms(1985) 역시 0.2 이하의 기준에서 일관성이 유지될 수 있다고 보고 있다[23].

설문 자료를 직업별로 구분해보면 보안 관제 4명, 보안 솔루션 운영 2명, 정보보호 컨설팅 2명, 보안 담당자 1명으로 구성되었다. 참여 인원들은 사이버 위협 지표를 활용하여 정보보호 업무를 수행하는 5~10년 경력의 실무자들로서, 위협 지표에 기반한 보안 경보 발송, 솔루션 내 지표 반영, 위협 인텔리전스 관련 컨설팅 및 조직 내 보안 이슈 전파 등의 업무를 담당하고 있다.

설문은 먼저 상위 평가 기준들(공격자 및 감염자 지표, 역할 지표, 악성 파일 지표, 기법 및 전파 지표)에 대해 쌍대비교를 진행한 뒤, 각 기준별 세부항목들 사이의 항목들에 대하여 쌍대비교를 다시 한 번 진행하였다. 점수 산정에 대해서는 9점 척도 방식을 이용하였으며, 설문지 별로 각 평가 기준 별 가중치를 측정한 뒤 기하평균법을 적용하여 전체 설문에서 각 항목이 차지하는 가중치를 도출하였다.

4.3 분석 결과

분석 결과 항목별 신뢰도에 있어서 평가 목표에 대한 일관성 비율은 0.0169로 나타났다. 각 기준에 대한 일관성 비율은 각각 공격자 및 감염자 지표의 경우 0.0, 역할 지표의 경우 0.00040, 악성 파일 지표의 경우 0.0, 기법 및 전파 지표의 경우 0.00655로 확인되었다. 이는 김영문·채수원(1996) 등이 제시한 0.2 보다 작은 값으로 수용할 수 있는 결과임을 의미한다.

Table 2는 사이버 위협 지표의 상위 평가 기준과 세부 평가 기준에 대해 우선순위를 도출한 표이다. 상위 평가 기준에 대한 쌍대비교에 있어서는 악성 파일 지표, 기법 및 전파 지표, 역할 지표, 공격자 및 감염자 지표가 각각 순서대로 40.2%, 25.4%, 19.2%, 15.2%의 가중치를 가지는 것으로 확인되어 악성 파일 지표가 가장 높은 수치를 기록하였다. 하위 기준별 쌍대비교에서는 공격자 및 감염자 지표의 경우 감염자 IP가 55.9%로 공격시도 IP에 비해 높게 나타났다. 역할 지표의 세부 기준별 쌍대비교에서는 C&C가 52.7%를 차지하여 31.4%와 15.9%를 차지한 유포지와 정보유출지보다 높은 수치를 기록하였다. 악성 파일 지표의 세부 기준별 쌍대비교에 있어서는 악성코드가 56.7%로 43.3%로 나타난 랜섬웨어에 비해 중요한 항목으로 평가되었다. 마지막으로 기법 및 전파 지표에 있어서는 스미싱이 36.2%로 가장 높은 비중을 차지하였으며, 파밍은 27.6%,

Table 2. The priority analysis of cyber threat information

Criteria	Relative importance	Sub-criteria	Relative importance of Sub-criteria
Attacker & Infected System Indicators	0.15233	Attacker IP	0.44116
		Infected System IP	0.55884
Role Indicators	0.19168	Malware Distribution Sites	0.31438
		Identity Theft Sites	0.15850
		Command & Control Servers	0.52712
Malicious File Indicators	0.40180	Malware	0.56671
		Ransomware	0.43329
Technique & Spread Indicators	0.25419	Phising	0.15031
		Pharming	0.27575
		Smishing	0.36192
		Malicious Emails	0.21203

악성 이메일은 21.6%, 피싱은 15.0%를 차지하였다.

V. 결 론

본 연구는 사이버 위협 정보 공유 시장에서 공유되고 있는 위협 지표들 사이의 중요도 비교 분석을 통하여 소비자의 정보 선호도 측정과 정보 제공자의 기여도 판단에 도움을 주고자 하였다. 분석을 통하여 알 수 있는 특징들은 다음과 같다. 첫째, 상위 평가 기준별 비교에서는 악성 파일 지표가 다른 상위 기준들보다 중요한 요소인 것으로 나타났다. 이는 APT 공격의 도구로 악성코드 및 랜섬웨어가 주로 이용되고 있으며, 다양한 루트를 통해 유포되는 악성 파일들에 대한 탐지가 중요하기 때문으로 추측된다. 해당 결과는 강성록, 문미남, 신규용 및 이종관(2020)의 연구에서 악성코드를 이용한 시스템 파괴 공격이 가장 중요한 공격 목적으로 조사된 것에서도 확인된다[24]. 둘째, 역할 지표에서 C&C가 유포지나 정보 유출지에 비해 중요한 지표로 조사되었다. C&C의 경우 감염 여부를 확인할 수 있는 지표이며, 해커의 명령을 받아 추가적인 공격으로 이어질 수 있기 때문에 상대적으로 중요한 지표로 판단된 것으로 보인다. 셋째, 기법 및 전파 지표에서 스미싱 관련 지표가 가장 중요한 항목으로 확인되었다. 이는 최근 모바일 기기의 업무 활용도가 높아지고 있으며, 사회 공학적 기법 등을 이용한 모바일 대상 사이버 공격이 증가함에 따라 관심이 높아졌기 때문으로 보인다. 민병길, 안우근 및 서정택(2014)의 연구에서도 모바일 기기의 업무 활용도가 증가함에 따라 취약점 등의 보안 위협 평가 시 모바일 환경에 대한 고려가 필수적으로 이루어져야 한다고 판단하고 있다[25].

반면 본 연구는 다음과 같은 한계점을 가지고 있어 주의가 요구된다. 첫째, 정보 공유 시스템을 통해 공유되고 있는 단일 지표 항목들을 대상으로 분석을 진행하였으며, 이러한 평가 항목들은 시스템과 분석가에 의해 달라질 수 있다. 둘째, 단일 지표를 구성하는 항목들 간의 비교에 초점을 맞추고 있으며, 공유되는 정보의 양적 측면에 대한 비교는 포함되어 있지 않다. 이는 향후 정보 공유 시스템의 통계에 대한 분석과 연구가 병행되어질 필요가 있을 것으로 보인다.

그럼에도 불구하고 본 연구는 실제로 공유되고 있는 주요 위협 지표들의 상대적 중요도를 도출하여 소비자의 항목별 선호도를 파악하였음에 그 의의가 있다. 이는 국내외 보안 솔루션 개발 업체 및 위협 인텔리전스 서비스 제공 업체 등에서 소비자의 관심사를 측정하는 하나의 기준으로 사용할 수 있을 것이다. 또한 정보보호 관련 교육 기관에서는 사이버 공격에 대한 대응 및 중요성을 인지시키는 목적으로 해당 결과를 활용할 수 있다. 나아가 정보보호 관련 투자를 고민하고 있는 기업의 입장에서는 대량의 데이터 앞에서 한정적인 시간과 자원을 효율적으로 투입하기 위한 가이드의 역할을 수행할 것이다. 정보 공유 서비스 제공자의 경우 해당 분석 및 결과를 바탕으로 정보 공유에 따른 유용성과 트랜드를 확인하고 이를 공유 활성화에 이용할 수 있다. 마지막으로 향후 징벌적 손해배상제도와 같은 유관 제도 도입 시, 개별 정보 제공자의 사회적 정보보호 기여도를 산정할 수 있는 하나의 지표로서 활용될 수 있기를 기대한다.

References

[1] Joint Task Force Transformation Initiative Interagency Working Group, "Guide for conducting risk assessments," NIST SP 800-30 Rev. 1, National Institute of Standards and Technology, Sep. 2012.

[2] C. Johnson, L. Badger , D. Waltermire, J. Snyder and C. Skorupka, "Guide to cyber threat information sharing," NIST SP 800-150, National Institute of Standards and Technology, Oct. 2016.

[3] Korea Internet & Security Agency, "Threat information and security trend collector survey results," KISA cyber security issue report Q4 2020, Korea Internet & Security Agency, pp. 38-44, Dec. 2020.

[4] A. Rutkowski, "Public international law of the international telecommunication instruments: cyber security treaty provisions since 1850," info, vol. 13 no. 1, pp. 13-31, Jan 2011.

[5] Yu-mi Ko, Jae-won Choi and Beom-soo Kim, "Protecting individuals from secondary privacy loss using breached personal data information center," Review of KIISC, 22(2), pp. 391-400, Apr. 2012.

[6] L.A. Gordon, M.P. Loeb, and W. Lucyshyn. "Sharing information on computer systems security: An economic analysis," Journal of Accounting and Public Policy, vol. 22, no. 6, pp. 461-485, Dec. 2003.

[7] M.D. Cavelty, Cyber-security and threat politics: US efforts to secure the information age, Routledge, Nov. 2009.

[8] K. Hausken. "Information sharing among firms and cyber attacks," Journal of Accounting and Public Policy, vol 26, no. 6, pp. 639-688, Oct. 2007.

[9] Hee-jung Cho, "3·4 DDoS attacks and network security," 31-9735032-0006 28-14, National Assembly Research Service, Mar. 2011.

[10] Ha-young Kim and Tae-sung Kim, "Factors to affect sharing cyber threat information in South Korea," Review of KIISC, 27(5), pp. 1167-1188, Oct. 2017.

[11] Ji-baek Park, Byung-hwan Choi and Hak-su Cho, "Measures to enable sharing of cyber threat information," The Journal of Korean Institute of Communication Sciences, 35(7), pp. 41-48, Jun. 2018.

[12] Ae-chan Kim and Dong-Hoon Lee, "A study on the priorities of requirements for establishing effective cyber threat information sharing system," Review of KIISC, 26(1), pp. 61-67, Feb. 2016.

[13] KISA Internet Bohonara & KrCERT, "Cyber Threat Information Analysis Sharing (C-TAS) System," https://www.boho.or.kr/webprotect/ctas.do, 2021. 06. 13.

[14] Korea Financial Telecommunications & Clearings Institute, "Korea Financial Information Sharing and Analysis Center," http://www.kftc.or.kr/kftc/business/EgovIsacInfo.do, 2021. 06. 13.

[15] Jung-mihn Ahn, "Issues presented by cybersecurity information sharing act 2015," Yonsei Law Review, 28(4), pp. 259-282, Dec. 2018.

[16] ITworld, "Spreading ransomware, serviceability is the main reason," http://www.itworld.co.kr/news/102463, 2016. 12. 07.

[17] Bodnara, "Cyber Threat Alliance (CTA), establishing official non-profit

corporation, adding new members, and appointing the first new representative," https://www.bodnara.co.kr/bbs/article.html?num=138671, 2017. 02. 23.
[18] W. Yoram, and T.L. Saaty. "Marketing applications of the analytic hierarchy process." Management Science, vol. 26, no. 7, pp. 641-658. Jul. 1980.
[19] T.L. Saaty, "Transport planning with multiple criteria: The analytic hierarchy process applications and progress review," Journal of Advanced Transportaion, vol. 29, no. 1, pp. 81-126, Apr. 1995.
[20] Jin-kyu Kang and Byung-chan Min, Theory and practice of AHP, Inter-Vision, Oct. 2008.
[21] Yong-sung Park, Decision Making by AHP, Kyowoo, Aug. 2009.
[22] Young-moon Kim and Su-won Chae, "The application of the analytical Hierarchy Process (AHP) to the travel destination choice," Journal of Tourism Sciences, 20(1), pp. 63-81, Jan. 1996.
[23] T.L. Saaty and K.P. Keams, Analytical Planning: The Organization of Systems. Pergamon Press, Inc., New York, p.32, Oct. 1985.
[24] Sung-rok Kang, Mi-nam Moon, Kyu-yong Shin and Jong-kwan Lee, "A study on priority analysis of evaluation factors for cyber threats using open source intelligence (OSINT)," Convergence security journal, 20(1), pp. 49-57, Mar. 2020.
[25] Byung-gil Min, Woo-geun Ahn, and Jung-taek Seo. "Vulnerability assessment by cybersecurity threat changes," Review of KIISC, 24(1), pp. 7-12, Feb. 2014.

〈저자소개〉

이 로 운 (Ro-woon Lee) 정회원
2015년 2월: 경희대학교 경제학과 졸업
2017년 9월~현재: 고려대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, 침입탐지, 인증·권한관리

권 헌 영 (Hun-yeong Kwon) 종신회원
1992년 2월: 연세대학교 법학과 학사
1998년 2월: 연세대학교 법학과 석사
2005년 2월: 연세대학교 법학과 박사
2008년 3월~2015년 8월: 광운대학교 법과대학 교수
2015년 9월~현재: 고려대학교 정보보호대학원 교수/사이버보안정책센터 센터장
〈관심분야〉 정보보호, 사이버보안, 사이버안보, 정보화, 전자정부, ICT 관련 법 및 정책, 개인정보보호법 및 정책, 데이터법과 정책