https://doi.org/10.33778/kcsa.2020.20.1.049

공개출처정보를 활용한 사이버위협 평가요소의 중요도 분석 연구★

강 성 록*, 문 미 남**, 신 규 용***, 이 종 관***

요 약

우리는 일상생활 가운데 사이버위협에 노출된 채 살아가고 있다. 그럼에도 불구하고 많은 사이버위협 및 공격은 공격자, 공격목적, 피해규모 등을 명확히 식별하기 어렵고, 단일출처의 정보에 의존하게 되어 객관성 있는 정보를 획득하는 것이 제한된다. 이에 본 연구의 선행연구[1]에서는 공개출처정보(Open Source Intelligence, OSINT)를 활용한 사이버공격 데이터베이스(Database, DB)를 구축하기 위한 새로운 방법론을 제시하였다. 본 연구는 사이버 위협을 정량화할 수 있도록 사이버공격 DB 중 사이버 위협 평가요소를 선정하고 그 평가요소에 대한 중요도를 분석하고자 한다. 사이버공격 DB 중 사이버위협의 상대적 중요도에 영향을 미치는 평가요소로 공격목적, 공격범주, 공격대상, 공격 용이성, 공격 지속성, 공개출처정보의 빈도를 선별하고, 각 평가요소들에 대한 하위 계층의 요소들을 선정한 후 각 요소들의 중요도를 계층분석적 의사결정방법(Analytic Hierarchy Process, AHP)을 활용하여 분석하였다.

A Study on Priority Analysis of Evaluation Factors for Cyber Threats using Open Source Intelligence (OSINT)

Sungrok Kang*, Minam Moon**, Kyuyong Shin***, Jongkwan Lee***

ABSTRACT

It is no exaggeration to say that we live with cyber threats every day. Nevertheless, it is difficult for us to obtain objective information about cyber threats and attacks because it is difficult to clearly identify the attacker, the purpose of attack, and the range of damage, and rely on information from a single source. In the preceding research of this study, we proposed the new approach for establishing Database (DB) for cyber attacks using Open Source Intelligence(OSINT). In this research, we present the evaluation factors for cyber threats among cyber attack DB and analyze the priority of those factors in oder to quantify cyber threats. We select the purpose of attack, attack category, target, ease of attack, attack persistence, frequency of OSINT DB, and factors of the lower layer for each factor as the evaluation factors for cyber threats. After selection, the priority of each factor is analyzed using the Analytic Hierarchy Process(AHP).

Key words : Open Source Intelligence, OSINT, Cyber Threats, AHP

접수일(2020년 03월 02일), 수정일(1차: 2020년 3월 17일), (2차: 2020년 03월 26일), 게재확정일(2020년 3월 28일)

★ 본 논문은 2018년 국군사이버사령부(11-1290000-000742-01)의 지원에 의해 연구되었음

* 육군사관학교 심리경영학과(주저자)
** 육군사관학교 수학과(교신저자)
*** 육군사관학교 컴퓨터학과

1. 서 론

IoT, 클라우드 등 새로운 IT 기술들의 발전과 이의 매우 빠른 확산은 사람들로 하여금 일상의 편의성과 효율성의 극대화를 가능하게 하고 있다. 그러나 이와 함께 악성코드, 지능형 지속 공격(Advanced Persistent Threat, APT) 등 사이버 위협도 매우 빠르게 증가하고 있고, 증가하는 사이버 위협에 대처하기 위해서 많은 연구들이 진행되고 있다. 특히 사이버 위협을 사전에 예측하기 위한 모델 개발을 위하여 공격 그래프(Atach graph)[]2, 베이지안 네트워크[], 딥러닝[4], 데이터마이닝[5] 등 다양한 방법들이 활용하고 있다.

사이버 공격 예측 모델은 예측의 목적에 따라 다음과 같이 세 가지 경우로 분류할 수 있다. 먼저, 가장 전통적인 경우로 공격투영(Attack projection) 및 공격의도 인지(Attack intention recognition)이다[6]. 이는 공격자(해커)가 다음 단계에서 어떤 공격을 할 것인지, 공격자의 궁극적인 목적이 무엇인지를 예측하는 것이다. 실제 상황에서 공격투영 및 공격의도 인지는 매우 유사한 특성을 지니고 있으며 효과적인 예측을 위해 이를 통합할 필요가 있다. 이에 공격투영 및 공격의도 인지를 보다 일반화하여 사이버 공격을 예측하는 방법이 침입 예측(intrusion prediction)이다[7]. 이는 어떤 종류의 공격이 언제 어디서 일어날지를 예측하는 것이다. 마지막으로 공격자의 공격이 아닌 네트워크의 전체 상황을 예측하는 네트워크 보안 상황 예측(Network Security Situation Forecasting)이다[8]. 이는 발생한 전체 네트워크에서의 상황을 예측하는 것이다.

위와 같이 사이버 공격을 예측하기 위해서는 비밀정보 및 공개정보 같이 많은 정보들이 요구된다. 하지만 비밀정보의 수집은 과도한 비용, 윤리문제, 정보의 적시성 및 공유 등의 제한사항이 있다[9]. 반면 공개정보는 공공에서 접근할 수 있는 모든 공개출처(신문, 방송, 간행물, 온라인 매체 등)를 통해 획득하는 정보로서, 쉽게 공유 및 접근할 수 있고 즉시적으로 활용할 수 있어 사이버 위협 예측을 위한 정보수집의 최적의 대안이 될 수 있다.

그럼에도 불구하고 지금까지 공개출처정보는 주로 테러리즘과 범죄분야에 국한되어 활용되어 왔으며 사이버 위협을 예측하기 위해 공개출처정보의 활용은 매우 미진한 상태이다. 이에 본 연구의 선행연구[1]에서는 데이터마이닝(Data Mining) 기법을 활용하여 공개출처정보로부터 사이버공격 데이터베이스를 구축하는 방법론을 제안하였다. 구축된 공개출처정보를 활용하여 사이버 위협을 예측할 수 있는 모델을 개발하기 위해서는 사이버 위협을 나타내는 데이터베이스 변수로부터 평가요소를 식별하고, 이를 정량화하는 작업이 필요하다. 즉, 특정 사이버 위협이 얼마나 위협적인지를 판단하기 위해서는 사이버 위협의 각 평가요소들에 대한 중요도를 계산할 수 있어야 한다.

많은 연구에서 사이버 위협의 각 평가요소들에 대한 중요도를 계산하기 위해 계층분석적 의사결정방법(Analytic Hierarchy Process, AHP)을 활용하였다. Badie의 연구에서는 사이버 위협에 대한 인식부족과 컴퓨터 보안 위험사이의 관계를 찾기 위해 계층분석적 의사결정방법(AHP)을 사용하여 상대적 중요도를 분석하였고[10], Bodin의 연구진은 감지된 복합위험(PCR, Perceived Composite Risk)에 대한 평가 척도들의 가중치 결정을 위해 계층분석적 의사결정방법(AHP)을 이용하였다[11].

따라서 본 연구에서는 선행연구[1]를 통해 구축된 사이버 공격 데이터베이스로부터 (1) 사이버 위협 예측을 위한 평가요소를 식별하고, (2) 계층분석적 의사결정방법(AHP)을 활용해 해당 평가요소들에 대한 중요도를 결정하는 방법론을 제시한 뒤, (3) 마지막으로 향후 활용방안을 모색한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 사이버 위협평가 요소의 중요도 분석을 위한 방법인 계층분석적 의사결정방법(AHP)을 소개한다. 3장에서는 계층분석적 의사결정방법(AHP) 모형 설계 및 데이터 수집방법을 설명한다. 4장에서는 사이버 위협 평가요소의 중요도 분석결과를 제시한다. 마지막으로, 5장에서는 본 연구의 결론 및 향후 연구방향을 제시한다.

2. 계층분석적 의사결정방법(AHP) 소개

계층분석적 의사결정방법(AHP)은 토마스 사티(Thomas L. saaty)에 의해 제창되고 종합적으로 정립되었다. 계층분석적 의사결정방법(AHP)은 여러 개의 평가기준으로부터 의사결정을 해야 할 때, 해당 분야 전문가의 지식, 경험, 직관을 바탕으로 평가기준들을 계층화하고, 계층에 따라 그 중요도를 결정하는 다기준 의사결정 방법이다. 계층분석적 의사결정방법(AHP)은 평가기준이 다수이고, 상호배반적인 대안들이 존재할 때 효과적으로 의사결정을 지원할 수 있다[12].

계층분석적 의사결정방법(AHP)에 대한 이론적 배경은 다음의 4가지의 공리에 의해 토대를 두고 있다. 첫째, 상호비교(reciprocal)이다. 연구에 참여하는 해당 분야의 전문가와 의사결정자는 비교 대상에 대하여 상대적 중요도를 짝지어 비교할 수 있는 전문지식과 경험을 구비해야 한다. 둘째, 동질성(homogeneity)이다. 비교대상 간의 차이가 너무 크게 되면 오류의 가능성도 증가하므로, 비교가능한 일정한 범위를 갖는 기준들이 필요하다. 셋째, 독립성(independence)이다. 동일 수준의 요인들은 특성이나 내용 측면에서 상호 독립성을 가지고 있어야 한다. 넷째, 기대성(expectations)이다. 의사결정자들의 합리적 기대에 부응하는 완전한 구조를 갖추고 있어야 한다. 수준의 수가 너무 많으면 계산상의 복잡성 문제가 발생하게 된다[13].

계층분석적 의사결정방법(AHP)은 정성적인 기법 등을 활용하여 처리하기 곤란한 의사결정에 적용될 수 있는 장점이 있다. 이 기법은 사람이 가지고 있는 주관이나 감(勘)이 반영될 수 있으며, 다수의 목적을 동시에 고려할 수 있고, 불확실한 상황을 명확하게 설명하는 것이 가능하며, 의사결정자가 간단하게 사용할 수 있는 특징을 가지고 있다[14]. 즉 계층분석적 의사결정방법(AHP)은 정량적인 정보뿐만 아니라 정성적인 평가요인도 포함할 수 있는 장점이 있으며, 복잡한 수학적 이론보다 해당 분야 전문가의 직관을 바탕으로 분석하기 때문에 그 논리가 비교적 쉽다고 볼 수 있다. 이와 같은 단순성, 간편성, 명확성 등으로 인해 계층분석적 의사결정방법(AHP)은 그 활용도가 증가하고 있다.

계층분석적 의사결정방법(AHP)은 위와 같은 많은 장점을 가지고 있는 반면, 다음과 같은 단점이 있다. 첫째, 의사결정 문제를 계층화할 때 이론적 틀이 존재하지 않는다. 만약 전문가들과 의사결정자의 해박한 지식과 경험이 선행되지 않는다면, 계층의 수준을 잘못 설정하거나 요인들 간의 독립성을 확보하지 못하는 경우가 발생할 수 있다. 둘째, 의사결정 대안들의 수가 제한적이며 수준의 수는 3~7개가 적절하다. 만약 계층의 구조와 수준의 수가 증가한다면 계산이 매우 복잡해지며 의사결정자의 판단에 혼란을 초래하게 된다. 셋째, 분석 결과를 의사결정자의 의도대로 조작할 수 있으므로 의사결정자의 진실성과 윤리가 매우 중요하다. 마지막으로, 일관성 지수가 낮은 경우 다시 설문을 실시하기 어려울 뿐만 아니라 여러 쌍대비교 중 어떤 쌍대비교가 일관적이지 않은지를 찾기가 쉽지 않다[13].

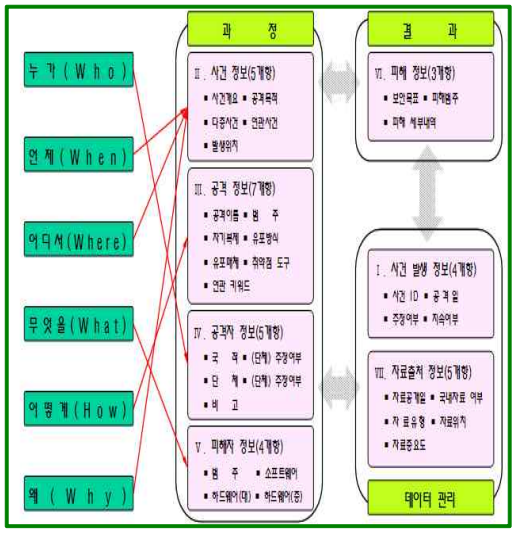
계층분석적 의사결정방법(AHP)을 이용하여 의사결정과 관련된 문제를 해결하기 위해서는 다음의 4단계의 작업을 거치게 된다. 1단계에서는 의사결정 문제를 계층 구조화한다. 우선 상위개념을 규정하고, 계층 구조에서 하위 수준을 다시 나누게 된다. 이 때 각 계층에 포함되는 비교대상은 최대 9개로 제한하는 것이 바람직하다. 2단계에서는 의사결정 요소들 간의 쌍대비교로 판단자료를 수집한다. 일반적으로 전문가의 설문을 통해 자료를 수집하며 쌍대비교는 보통 9점 척도를 이용한다. 3단계에서는 의사결정 요소들의 상대적 가중치를 추정하고, 연구에 참여한 전문가가 내린 판단의 논리적 모순이 존재하는지 여부를 알아보기 위하여 일관성 비율(Consistency Ratio)을 검증하고, 설문결과가 일관성 비율이 요구되는 수준 보다 낮을 경우 설문결과를 제외하는 등 일관성을 높이기 위한 방법을 강구한다. 마지막 4단계에서는 각 수준들의 전반적인 우선순위를 산출하게 된다. 평가대상이 되는 여러 대안들에 대한 우선순위를 도출하기 위하여 의사결정 요소들의 상대적 가중치를 종합한다.

3. 계층분석적 의사결정방법(AHP) 모형 설계 및 데이터 수집

이 장에서는 계층분석적 의사결정방법(AHP)을 적용하기 위한 계층적 구조를 설계하고, 각 평가요소들의 중요도를 분석하기 위한 데이터 수집 방법을 설명한다.

3.1 사이버공격 데이터베이스 구조

(그림 3-1)에서 보듯이 본 연구의 선행연구로부터 구축된 사이버공격 데이터베이스는 사건발생 정보, 사건 정보, 공격 정보, 공격자 정보, 피해자 정보, 피해 정보, 그리고 자료출처 정보 등 7가지 범주 33개 변수로 구성되어 있다[1].



(그림 3-1) 사이버공격 데이터베이스 구성[1]

계층분석적 의사결정방법(AHP)을 적용하기 위해서는 (그림 3-1)의 33개 데이터베이스 변수로부터 사이버공격의 위협을 직접적으로 묘사할 수 있는 변수를 평가요소로 선정하여야 한다.

3.2 계층분석적 의사결정방법(AHP) 모형 설계

사이버 위협 평가요소 선정을 위해서는 사이버공격 데이터베이스로부터 특정 사이버 위협의 중요도에 영향을 미치는 변수를 식별하는 것에서 출발한다. 이때 사이버 위협은 누가 공격하는지, 언제 공격하는지, 무엇을 공격하는지, 어떻게 공격하는지, 왜 공격하는지, 공격의 방법이 얼마나 쉬운지, 단발성 공격인지 지속적 공격인지에 따라 그 위협도가 달라진다. 또한 공개출처정보를 활용해 데이터베이스를 구축하고 있기 때문에 공개출처의 빈도 또한 사이버 위협의 정도를 판단하는 중요한 근거가 된다. 이러한 의미에서 본 연구에서는 사이버 위협에 직접적으로 영향을 미치는 ① 공격목적, ② 공격범주, ③ 공격대상, ④ 공격 용이성, ⑤ 공격 지속성, ⑥ 공개출처정보의 빈도 등 총 6개 요소를 사이버 위협 평가요소(계층 2)로 선정하였다.

<표 3-1> 공격목적에 대한 기술통계분석 결과

구 분	빈 도	비 율 (%)
1. 정치적 목적	6	4.80
2. 경제적 목적	57	46.00
3. 업무방해 목적	9	7.30
4. 데이터 탈취 목적	46	37.10
5. 시스템 파괴	3	2.40
6. 기타	2	2.40
Total	124	100.00

다음으로는 이미 구축된 사이버공격 데이터베이스를 활용해 계층 2의 각 평가요소에 대한 기술통계분석을 통해 세부 평가요소(계층 3)를 식별하였다. 예를 들어 공격목적에 대한 기술통계분석 결과는 <표 3-1>에서 보는 바와 같이 경제적 목적, 데이터 탈취 목적, 업무방해 목적, 정치적 목적, 시스템 파괴 목적, 기타 순으로 나타났기 때문에 계층 3의 평가요소로 각각 선정하였다.

이와 같은 단계를 거쳐 6개의 계층2의 평가요소별 계층 3의 평가요소를 선정하였고, 완성된 사이버 위협 평가요소의 계층 구조는 (그림 3-2)에서 보는 바와 같다. 공격의 범주 또는 공격의 목적 등의 하위 계층의 평가요소는 선행연구[1]에서의 데이터베이스 구축 방법론에서 제시한 방법에 따라 선정하였으며 각 평가요소별 구체적 내용은 <표 3-2>에서 보는 바와 같다.

(그림 3-2) 사이버 위협 평가요소의 계층 구조

3.3 데이터 수집 방법

평가항목의 중요도를 선정하기 위한 데이터 수집은 설문을 통해 실시하였다. 설문 대상자는 사이버 위협 및 사이버 공격과 관련된 업무를 수행 중인 전문가 집단으로 구성하였다. 설문조사는 2018년 11월에 관련 전문가 36명을 대상으로 설문의 목적과 설문 작성요령을 구체적으로 설명한 후 1시간 정도 실시하였다.

A	A가 더 중요하다								동등	B가 더 중요하다								B
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
경제적 목적																		데이터 탈취
경제적 목적																		업 무 방 해
경제적 목적																		시스템 파괴
경제적 목적																		정치적 목적
경제적 목적																		기 타
데이터 탈취																		업 무 방 해
데이터 탈취																		시스템 파괴
데이터 탈취																		정치적 목적
데이터 탈취																		기 타
업 무 방 해																		시스템 파괴
업 무 방 해																		정치적 목적
업 무 방 해																		기 타
시스템 파괴																		정치적 목적
시스템 파괴																		기 타
정치적 목적																		기 타

(그림 3-3) 계층 2 평가요소에 대한 설문(예)

설문은 (그림 3-3)에서 보는 바와 같이 계층 2의 평가요소에 대한 쌍대비교 후, 계층 3 평가요소들에 대한 쌍대비교 순으로 진행되었다. 계층 3 평가요소들에 대한 설문지는 지면관계상 생략한다.

<표 3-2> 계층 3의 구체적 내용

계층 2	계층 3(계층 2의 세부 항목)
공격의 목 적	경제적 목적 : 경제적인 이득을 취하기 위한 공격(ex. 랜섬웨어)
	데이터 탈취 : 개인정보 등의 데이터를 탈취하기 위한 공격(ex. 스파이웨어)
	업무방해 : 정상적인 업무를 수행하지 못하게 하는 공격(ex. DDoS)
	시스템 파괴 : 시스템이 정상적으로 동작하지 못하도록 하는 공격(ex. 스턱스 넷)
	정치적 목적 : 자신들의 정치적인 목적을 달성하기 위한 공격(ex. 핵티비즘)
	기타 : 위 목적을 제외한 다른 목적의 공격(ex. 자기 과시 등)
공격의 범 주	스파이웨어 : 비밀번호, 금융정보, 주민번호와 같은 각종 정보를 수집
	랜섬웨어 : 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구
	봇넷(botnet) : 악성 소프트웨어를 이용해 빼앗은 다수의 좀비 컴퓨터
	백도어 : 정상적인 인증 과정을 거치지 않고 운영 체제나 프로그램 등에 접근
	와이퍼 : 공격자가 피해 시스템의 정보나 자신의 활동 흔적을 삭제
	기타 : 애드웨어, 다운로더, 드로퍼, 루트킷, 익스플로잇 등
공격의 대 상	불특정 다수 :특정한 대상이 아닌 모든 사람을 공격 대상으로 하는 경우
	일반업체(IT업체 포함) : 특정 업체나 업체에 속한 인원을 대상으로 하는 경우
	금융권(가상화폐 포함) : 금융권 혹은 금융권 종사자를 대상으로 하는 경우
	정부기관(군/경찰 포함) : 정부기관 혹은 정부기관 종사자를 대상으로 하는 경우
	사회기반시설 : 철도, 항만, 항공, 가스 등 사회기반시설을 대상으로 하는 경우
	기타 : 탈북자 혹은 북한연구자 등
공 격 용이성	어려움 : 고급 기술이 필요해서 전문적인 지식을 가진 사람만이 공격 가능
	쉬움 : 자동화 도구나 익스플로잇 키트가 존재해서 누구나 쉽게 공격 가능
공 격 지속성	지속 : 해당 공격이 지속적인 피해를 입히고 있는 경우
	비지속 : 해당 공격이 이미 종료되어 더 이상 피해를 입히지 않는 경우
공개출처 정보의 빈도	높음 : 단위 시간 동안 공개출처정보가 다수 생산된 경우
	낮음 : 단위 시간 동안 공개출처정보가 소수 생산된 경우

4. 분석결과

4.1 일관성 지수 및 일관성 비율 검증

일관성 검증의 주된 목적은 각 전문가별 설문결과에 대한 일관성을 검증하여 신뢰성 있는 데이터를 선별하여 중요도 지수 산출을 위한 가중치로 활용하는데 있다. 이를 위해 쌍별비교 행렬(matrix)로부터 일관성 지수(CI; Consistency Index)와 일관성 비율(CR; Consistency Ratio)을 산출하고, CR < 0.1의 조건을 충족하면 쌍별비교가 합리적인 일관성을 갖는 것으로 판단하였다.

이에 대한 계산식은 다음과 같다.

$$-\quad I \quad \frac{\lambda_{\max}-n}{n-1},\ CR=\frac{CI}{RI}$$

이 때, n은 평가요소의 수를 의미하며, $_{\max}$는 $n\times n$ 행렬에서 최대고유치이고 항상 n 이상이다. 그리고 무작위 지수(RI; Random Index)는 다음의 <표 4-1>의 n값에 따른 RI 값을 사용한다. $n=2$인 경우 RI값은 0이므로 일관성 검증이 불가하다. 예를 들어 <표 4-4>에서 계층 2는 5개의 하위 평가요소들로 구성되어 있으므로 $RI=1.12$로 설정하였고, 공격 목적은 6개의 하위 평가요소들로 구성되어 있으므로 $RI=1.24$로 설정하였다.

<표 4-1> n값에 따른 RI 값

n	3	4	5	6	7	8
RI	0.58	0.9	1.12	1.24	1.32	1.41

<표 4-2>는 공격목적의 일관성 지수 CI와 일관성 비율 CR을 계산하기 위한 다양한 값의 일부이다. 이러한 절차에 따라 사이버 위협 관련 전문가 36명의 설문결과 중 $CR<0.1$인 신뢰성 있는 데이터를 분류한 후 그 설문결과를 이용하여 중요도 분석을 실시하였다. 계층 2에서는 36개의 설문 중 21개, 계층 3의 공격목적, 공격범주, 공격대상은 각각 20개, 21개, 26개의 설문결과로 중요도 분석을 실시하였다.

<표 4-2> 공격목적의 CI와 CR값 계산의 예

설문	n	$\lambda_{\max}$	CI	RI	CR
1	6	6.14	0.03	1.24	0.02
2	6	6.78	0.16	1.24	0.13
3	6	7.42	0.28	1.24	0.23
4	6	6.18	0.04	1.24	0.03
5	6	6.11	0.02	1.24	0.02

4.2 계층별 중요도 분석결과

사이버 위협 평가요소의 상대적 중요도에 대한 계층별 분석 결과는 <표 4-3>와 같다. <표 4-3>에서 제시된 바와 같이, 공격 용이성의 세부항목에 대한 중요도는 어려움(0.516)과 쉬움(0.484)이 거의 유사한 것으로 나타났다. 이에 사이버 위협 평가항목에서 공격 용이성 요소를 제외시키는 것이 사이버 위협 모델의 간결성을 향상시킬 것으로 판단된다. 이에 앞에서 제시한 절차와 동일한 과정으로 <표 4-4>과 같은 평가요소별 상대적 중요도를 구할 수 있다.

<표 4-3> 평가요소별 상대적 중요도

계층 2		계층 3		종합 평가치 $=\omega\quad\omega_2$
요소	가중치 ω_1	요소	가중치 ω_2	
공격 목적	0.339	경제적 목적	0.148	0.050
		데이터 탈취	0.198	0.067
		업무 방해	0.108	0.037
		시스템 파괴	0.289	0.098
		정치적 목적	0.197	0.067
		기 타	0.060	0.020
공격 범주	0.116	스파이웨어	0.194	0.023
		랜섬웨어	0.172	0.020
		봇 넷	0.196	0.023
		백도어	0.270	0.031

		와이퍼	0.108	0.013
		기 타	0.060	0.007
공격 대상	0.271	불특정 다수	0.080	0.022
		일반업체	0.087	0.024
		금융권	0.173	0.047
		정부기관	0.237	0.064
		사회기반 시설	0.356	0.096
		기 타	0.066	0.018
공격 용이성	0.090	어려움	0.516	0.046
		쉬 움	0.484	0.044
공격 지속성	0.117	지 속	0.810	0.095
		비지속	0.190	0.022
OSINT 빈도	0.066	높 음	0.663	0.044
		낮 음	0.337	0.022

<표 4-4>에서 계층 2의 평가요소를 <표 4-3>와 비교하면 공격 범주와 공격 지속성의 상대적 중요도가 역전되었음을 알 수 있고, 계층 3의 평가요소의 가중치 값은 변화가 없으나, 종합 평가치에서는 사회기반시설과 시스템 파괴의 순서가 역전되었음을 확인할 수 있다.

<표 4-4> 평가요소별 상대적 중요도

계층 2		계층 3		종합 평가치 $=\omega \quad \omega_2$
요소	가중치 ω_1	요소	가중치 ω_2	
공격 목적	0.367	경제적 목적	0.148	0.054
		데이터 탈취	0.198	0.073
		업무 방해	0.108	0.040
		시스템 파괴	0.289	0.106
		정치적 목적	0.197	0.072
		기 타	0.060	0.022
공격 범주	0.131	스파이 웨어	0.194	0.025
		랜섬웨어	0.172	0.023
		봇 넷	0.196	0.026
		백도어	0.270	0.035
		와이퍼	0.108	0.014
		기 타	0.060	0.008
공격 대상	0.304	불특정 다수	0.080	0.024
		일반업체	0.087	0.026
		금융권	0.173	0.053
		정부기관	0.237	0.072
		사회기반 시설	0.356	0.108
		기 타	0.066	0.020
공격 지속성	0.123	지 속	0.810	0.100
		비지속	0.190	0.023
OSINT 빈도	0.075	높 음	0.663	0.050
		낮 음	0.337	0.025

5. 결론 및 향후 연구방향

본 논문에서는 공개출처정보로부터 구축된 데이터베이스에서 사이버위협 평가요소를 선정하고, 그 중요도를 분석하였다. 이를 위해서 데이터베이스의 주요 변수 중 사이버 위협을 평가할 수 있는 6가지 요소를 선정하였고, 사이버 위협 및 사이버 공격과 관련된 업무에 종사 중인 전문가 집단 36명의 설문 후 계층분석적 의사결정방법(AHP)을 활용하여 사이버 위협을 정량화하기 위한 평가요소들의 중요도를 분석하였다. 분석결과 최초 선정했던 6가지 평가요소 중 공격의 용이성은 계층 3에서 요소들의 상대적 중요도가 거의 유사하게 분석되었고, 이를 보완하기 위해 공격 용이성을 제외한 5가지 평가요소들 간의 상대적 중요도 분석을 제시하였다.

향후 구축된 사이버공격 데이터베이스와 본 연구에서 제시한 평가요소별 상대적 중요도를 활용하여 사이버위협을 정량화할 것이다. 나아가 일자별 또는 사건별 사이버 위협도를 계산하여 제시

하고, 나아가 시계열 분석, 의사결정나무, 인공신경망 등의 다양한 기법을 활용하여 사이버 위협을 가장 잘 예측할 수 있는 모델을 개발할 것이다.

본 연구에서 제안한 사이버 위협 평가요소들은 제한된 데이터베이스의 기술통계분석을 통해 도출되었기 때문에, 만약 사이버공격 데이터베이스를 축적하여 이를 활용한다면, 보다 적합한 위협 평가요소를 선정하고 정확한 사이버 위협을 예측하는 것이 가능해질 것으로 예상된다. 따라서 추후에 기업, 정부, 연구소, 대학 등이 연계하여 공개형 사이버 공격 데이터베이스를 구축하여 공동으로 대응한다면 이를 기초로 다양한 사이버 위협을 예측하고 이를 예방할 수 있으리라 생각한다.

참고문헌

[1] Kuyoung Shin, Jinchel Yoo, Changhee Han, et al., "A study on building a cyber attack database using Open Source Intelligence(OSINT)", Convergence Security Journal 19(2), pp. 113-133, 2019.

[2] N. Polatidis, E. Pimenidis, M. Pavlidis, S. Papastergiou, and H. Mouratidis,"From product recommendation to cyber-attack prediction: generating attack graphs and predicting future attacks," Evolving Systems, 2018.

[3] K. Huang, C. Zhou, Y. C. Tian, S. Yang, and Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems", IEEE Transactions on Industrial Electronics, 2018.

[4] Torres, J.M.; Comesaña, C.I.; García-Nieto, P.J. "Machine learning techniques applied to cyber security", Int. J. Mach. Learn. Cybern. 2019

[5] M. Husak and J. Kaspar, "owards Predicting Cyber Attacks Using Information Exchange and Data Mining," in 2018 14th International Wireless Communications Mobile Computing Conference (IWCMC), 2018.

[6] A. A. Ahmed and N. A. K. Zaman, "Attack intention recognition: A review," IJ Network Security, 2017.

[7] M. Abdlhamed, K. Kifayat, Q. Shi, and W. Hurst, "Intrusion Prediction Systems". Cham: Springer International Publishing, 2017.

[8] Y.-B. Leau and S. Manickam, "Network Security Situation Prediction: A Review and Discussion". Springer Berlin Heidelberg, 2015.

[9] Eyungchul Cho, "A System for National Intelligence Activity Based on All Kinds of OSINT(Open Source INTelligence) on the Internet", Journal of Information and Security, Vol. 3, No. 2, pp. 41-55, June 2003.

[10] Nasrin Badie and Habibi Lashkari, "A new evaluation criteria for effective security awareness in computer risk management based on AHP", Journal of Basic and Applied Scientific research, Vol. 2, No. 9, pp. 9931-9947, 2012.

[11] Lawrence D. Bodin, Lawrence A. Gordon and Martin P. Loeb, "Information Security and Risk Management", Communications of the ACM, Vol. 51, No. 4, pp. 64-68, 2008.

[12] Saaty T. L., "The Analytic Hierarchy Process", New York, USA : McGraw-Hill, 1980.

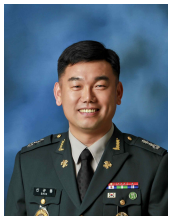
[13] 권박현, 고길곤, 송지영, 신경식. "예비타당성조사 수행을 위한 다기준분석 방안 연구", 한국개발연구원, 2000.

[14] 木下榮藏 and 大屋隆生. "전략적 의사결정기법 AHP(역자 권재현), 도서출판 청람, 2012.

〔저자소개〕

강 성 록 (Sungrok Kang)
1996년 3월 육군사관학교 학사
2001년 2월 연세대학교 석사
2010년 8월 (美)오리건주립대(OSU) 박사
email : ksr6452@mnd.go.kr

문 미 남 (Minam Moon)
2001년 3월 육군사관학교 학사
2006년 2월 고려대학교 수학석사
2015년 8월 텍사스 A&M 대학교 수학박사
email : hereandnow@kma.ac.kr



신 규 용 (Kyuyong Shin)
1996년 3월 육군사관학교 학사
2000년 2월 한국과학기술원 석사
2009년 12월 (美)노스캐롤라이나 주립대학교(NCSU) 박사
email : kyshin@kma.ac.kr

이 종 관 (Jongkwan Lee)
2000년 3월 육군사관학교 학사
2004년 3월 한국과학기술원 석사
2011년 3월 아주대학교 박사
email : jklee64@kma.ac.kr