사이버공격의 정량적 피해평가를 통한 공세적 대응규모 산정

홍 병 진*, 임 재 성*, 김 완 주*, 조 재 명*

요 약

우리사회와 정부에 대한 다양한 사이버 공격이 지속적으로 이루어지고 있으며 수시로 그 사례 및 피해가 발표되고 있다. 그리고 사이버공격의 영역 또한 사이버공간에 국한되는 것이 아니라 물리적 영역으로 확대되어 영향을 미치고 있다. 군사적 영역에서는 적의 물리적 공격에 대해 비례성을 갖고 대응한다는 원칙을 수립하고 시행하고 있다. 영역이 확대되고 있는 사이버전에서도 이러한 비례성 원칙이 필요할 것으로 판단되며, 실제 적용하기 위해서는 사이버공격에 대한 정량적, 정성적 대응 기준을 가지고 있어야 할 것이다. 그러나 사이버공격의 특성상 정확한 피해평가가 쉽지 않아 비례성이 모호하며 비례성 원칙으로 대응하는 것도 어려울 것이다. 이에 본 연구에서는 시나리오를 기반으로 사이버공격이 조직이나 시스템에 미치는 영향을 Gorden-Lobe 모델과 시큐리티 스코어링 기법을 이용하여, 사이버 공격 피해를 정량적·정성적으로 평가하여 피해규모를 산출하였다. 산출된 결과는 사이버공격에 대한 공세적으로 대응하기 위한 적절한 수준과 기준으로 제공할 것으로 기대한다.

Definition of aggressive response scale through quantitative evaluation of cyber attack

Byoungjin Hong*, Jaesung Lim *, Wanju Kim *, Jaemyoung Cho *

ABSTRACT

Various cyber attacks against our society and the government are continuing, and cases and damages are reported from time to time. And the area of cyber attack is not limited to cyberspace, but it is expanding into physical domain and affecting it. In the military arena, we have established and implemented the principle of responding proportionally to enemy physical attacks. This proportionality principle is also required in the version where the region is expanding. In order to apply it, it is necessary to have a quantitative and qualitative countermeasure against cyber attack. However, due to the nature of cyber attacks, it is not easy to assess the damage accurately and it is difficult to respond to the proportionality principle and the proportional nature. In this study, we calculated the damage scale by quantitatively and qualitatively evaluating the cyber attack damage using the Gorden-Lobe model and the security scoring technique based on the scenario. It is expected that the calculated results will be provided as appropriate level and criterion to counteract cyber attack.

Key words : Cyber attack damage evaluation, aggressive response, Gorden-Lobe model, security scoring technique, proportionality principle

접수일(2017년 9월 5일), 수정일(1차: 2017년 10월 25일), 게재확정일(2017년 10월 29일)

* 아주대학교 / NCW학과

1. 서 론

2017년 5월 13일 전 세계를 대상으로 '워너크라이' 또는 '워너크립트'로 명명된 툴을 사용한 무차별적 랜섬웨어 공격이 일어났다. 이후 공격에 사용된 툴과 인프라가 소니 픽처스 해킹과 방글라데시 중앙은행을 해킹한 라자루스 그룹이 사용한 기술과 상당히 유사해 동일 그룹의 소행으로 판단하였으며, '워너크라이' 랜섬웨어 공격이 북한의 해킹그룹인 '라자루스' 그룹과 관련 있다고 분석했다[1][2]. 이러한 사이버 공격은 이러한 민간 정보자산만을 대상으로 공격하는 것이 아니라 2014년 한수원 해킹, 2016년 국방망 해킹 등에서 살펴 볼 수 있듯이 국가안보의 핵심 시설과 국방기관을 직접 대상으로 하는 등 지속 확대되고 있다.

사이버 공격을 사전에 방지하는 것은 개인과, 사회, 국가에 이르기까지 모든 구성원의 안전을 보장하기 위해 중요한 문제이다. 그러나, 사이버 공격을 사전에 방지하기 위한 전략과 기술의 발전은 변화하는 과학기술의 발전속도를 따라가지 못하고 있어 전통적인 방어와 억제 모델로 해결할 수 없으며 사이버공격 행위자를 식별하고, 이러한 행위자에 대한 제제를 통해 사이버 공격 행위의 예방과 억제가 가능하다[3][4]. 이러한 사이버 공격 행위자를 식별하기 위해 공격무기인 악성코드를 이용하여 공격그룹을 식별하려는 시도[5]와

사이버 방어작전에 활용하는 프레임워크의 제안 등 다양한 연구가 진행되고 있다[6].

또한, 사이버 공격자의 공격 피해를 정확히 측정하여야만 공세적 대응활동 등 억제 전략 수립을 위한 적절한 활동이 가능하다. 즉, 전장에서 정확한 피해평가(BDA)를 통해 현행 작전의 성과를 측정하고 향후 작전을 계획하는 것과 같이 사이버 전장에서 적의 공격에 의한 피해를 정확히 평가할 수 있어야만 효과적인 대응이 가능하다.

그러나, 우리는 사이버공격에 대응하기 위한 명확한 기준이나 정량적 측정도구의 부재와 정확한 공격주체 식별의 어려움으로 인하여 실제적인 대응은 공격이후에 분석과 복구하는 수준에서 한정되어 이루어 질 수밖에 없다. 이러한 사이버공격에 대한 적극적인 대응을 위해 정량적, 정성적으로 피해효과를 평가하고 비례성원칙에 의하여 대응규모 산정이 절실히 필요하다.

따라서, 본 논문에서는 사이버 공격에 공세적으로 대응하기 위한 피해평가를 위해 시나리오 기반의 사이버공격에 따른 피해를 정량적, 정성적으로 산정하고, 결과를 바탕으로 적절한 대응규모를 산정하여 제시하였다. 연구의 결과가 실제 사이버 공격이 발생했을 때 공세적 대응을 위한 의사결정을 보다 신속하게 할 것이며, 이를 통해 사이버 공격을 효과적으로 억제할 수 있을 것이며, 물리전과 연계한 사이버전 수행체계 발전에 기여할 것으로 기대한다.

본 논문의 구성은 다음과 같다. 2장에서는 최근의 사이버 공격의 유형과 피해를 평가하는 기법들을 알아보고, 3장에서는 비례성 대응원칙을 적용하기 위한 고려요소들을 알아본다. 4장에서는 시나리오 기반 사이버공격에 대한 피해를 정량적, 정성적으로 산정하고 대응규모를 산정한다. 5장에서 사이버 공격에 대한 피해효과 및 대응규모 정량화에 따른 기대효과와 향후연구를 언급하며 결론을 맺는다.

2. 관련연구

사이버 공격에 대응을 하기 위해서는 공격의 유형을 알아야 하고 공격 유형과 공격주체가 원하는 효과가 무엇인지 예상하는 것이 중요하다. 따라서 다양한 공격의 유형을 정의하고 그러한 공격의 가능하게 하는 공격도구에 대한 분석이 필요하다. 이를 위해 첫째, 사이버 공격의 유형을 '기밀성 파괴, 가용성 파괴, 무결성 파괴'로 정의하여 사이버 공격 유형별 사례를 알아보고 공격 시나리오를 구성한다. 둘째, 공격을 위한 도구들의 종류와 기능 그리고 주된 피해 시스템 및 장비들을 정의하고 그에 따른 피해 정도를 정의한다. 셋째, 공격의 형태와 무기를 사용한 시나리오를 구성하고 시나리오에 의한 피해효과 규모를 피해액 산정모형인 Gordon 모형, Loeb모형 등을 통하여 금전적 형태로 산출하고 시큐리티 스코어링 기법을 통하여 위협수준을 정의한다. 넷째, 공격에 대한 피해규모에 상응하는

대응수준을 금액의 크기에 기준하여 정의한다.

2.1. 최근 사이버 공격의 유형

사이버 침해는 개인의 금전탈취, 기업의 경영자산 탈취·파괴, 국가안보 위협까지 광범위하게 발생하고 있다. 사이버공격의 목적은 과거 자기과시에서 금품갈취로 변하였으며 최근에는 사이버테러를 통한 사회혼란 및 정치적 목적으로 진화되어 국가안보를 위협하고 있다. 공격 기법은 수동공격에서 은닉, 자동화 되며 조직적이며 지능화하여 나타나고 있다. 공격대상은 개별시스템에서 대규모 네트워크를 이용하는 사회기반시설, 국가 기반시스템으로 변화되고 있다.

이와 같은 공격 양상의 변화를 고려해 볼 때 최근 사이버 공격 유형을 ①산업전반으로 번지는 한국 맞춤형 공격 ②자산관리 등 공용 소프트웨어를 통한 표적 공격 ③한국어 지원 등 다양한 형태의 랜섬웨어 대량 유포 ④사회기반시설 대상 사이버테러 발생 ⑤멀버타이징 공격 등 대규모 악성코드 감염기법의 지능화 ⑥악성앱 등 모바일 금융 서비스에 대한 위협 증가 ⑦좀비화된 사물인터넷(IoT) 기기의 무기화처럼 7가지로 정의할 수 있다[7].

2.2. 피해규모 산출을 위한 대상 선정

피해규모 산정을 위한 요소는 무수히 많겠지만 본 논문에서는 유형자산과 무형자산으로 구분하여 산정을 하고자 한다. 즉, 사이버 공격에 대하여 무형자산과 유형자산에 피해규모와 복구를 위한 투자내용을 고려하여 대응규모를 정의 한다.

<표 1> 공격대상별 자산 구분

공격대상에 따른 구분	
유형자산	ICT 장비 : 서버, 네트워크 장비, 클라이언트 장비
	기타 : 기반시설, 부동산, 교통수단, IoT 등
무형자산	소프트웨어 : 모든 상용 및 응용 SW
	기타 : 기업 이미지, 지적소유권, 기타 민감 정보

유형 자산에서의 피해효과 산정을 위한 공격자는 공격을 통하여 자산에 대하여 물리적 파괴를 시도한 경우를 가정하였다. 첫째, 유형 자산에 대한 비용의 산정은 시스템 복구를 위하여 물리적인 장비 교체를 위한 장비 구매비용이 적용된다. 또한 기반시설, 자동차, 항공기 등 운송수단, 그리고 다양한 IoT기기에 대한 파괴 시 그것을 복구하거나 구매하기 위한 비용을 고려한다.

둘째, 무형자산에 의한 피해평가 산출은 모든 상용 및 응용SW에 대한 복구 및 구매 비용을 고려할 수 있을 것이다. 기업의 경우에 사이버공격에 의해 어떠한 이슈가 발생되었다면 이것은 기업의 이미지와 직결되어 매출감소 및 주가하락 등 심각한 금전적 피해가 발생할 수 있다. 그 외에도 개인정보나 지적소유권을 가진 중요 정보 유출에 따른 비용도 상당히 발생한다고 볼 수 있다.

이러한 유형자산과 무형자산에 대한 피해효과 산출에 대한 대상을 구체화하고 Gorden-Loeb모델과 시큐리티 스코어링 기법을 연계하여 피해효과를 산정하고자 한다.

2.3. 피해평가를 위한 모델

Gorden-Lobe 모델[8]에서는 실제적인 위협에 대응하기 위한 보안투자와 그에 대한 손실함수를 통해 예상되는 피해를 산출한다. 즉 사이버공격에 대한 손실을 위협 및 공격이 발생 할 확률(t)과 보호해야할 정보 자산이 가지고 있는 취약점(v), 위협행위로 인하여 발생한 금전적 손실(λ)의 상관관계를 통하여 산출하였다. 그리고 보호를 위한 투자금액을 적용하였을 경우 그 보안투자금액의 효과에 대한 손실과의 상관관계를 정의하고 예상되는 이익(EBIS)을 수식화(1) 하여 실제 공격과 위협이 발생하였을 경우 다음과 같이 정량화 하였다.

① L(잠재적 손실) = t(위협확률) × v(취약점) × λ(위협행위에 따른 금전적 예상 손실)
② 조건 : $0 < t < 1$, $0 < v < 1$
③ S(z, v),
손실함수(S), 보안투자(z : dollar), 취약점(v)
④ 보안투자에 따른 예상되는 이익 :

$$EBIS^{1)}(z) = \lceil v - S(z, v) \rceil L \quad (1)$$

국방과학연구소가 개발한 CMT(Cyber Warfare Modelling Technology using LVC)[9]는 사이버전 효과분석을 위하여 기존에 개발한 네트워크 장비 모델에 사이버 공격 및 방어 속성, 피해평가 속성 등을 추가로 부여하여 각 장비 모델을 확장하고, 이러한 사이버 속성과 사이버 공격 및 방어 모델, 피해평가 모델 등을 연동해서 사용자가 원하는 효과분석 결과를 도출하는 사이버 피해평가 모델링 기법이다. 즉, CMT는 영향요소에 의한 공격을 시뮬레이션을 통하여 수행함으로써 그 영향을 분석하고 피해를 평가하는 모델링 기법이다. CMT에서 사용하는 용어는 IETF(Internet Engineering Task Force)에서 사이버 보안 사고에 대한 데이터를 공유할 때 정보 표현을 위해 사용하는 프레임워크인 IODEF(Incident Object Description Exchange Format)[10]를 사용하였다.

<표 2> IODEF Impact Type

Impact Type	설 명
admin	관리자 권한 획득 시도
dos	서비스 거부 시도
file	파일의 무결성 손상시도
info-leak	정보 노출 시도
misconfiguration	시스템의 형상 설정 변경시도
policy	보안 정책 위반 시도
recon	스캐닝 등의 정찰 시도
social engineering	사회 공학적 공격 시도
user	사용자 권한 획득 시도
unknown	알려져 있지 않은 행위 분류

사이버전의 피해평가는 공격에 대한 방어의 결과로서 산출하게 된다. 이러한 사이버전 방어 효과지표 (MOE : Measure of Effectiveness)는 방어 성공률과 호스트 감염 차단률로 정의한다[11]. 방어 성공률은 전체 공격 중 방어 시스템에 의해 차단된 공격의 비율이고, 호스트 감염 차단률은 공격 대상 호스트 중 방어 시스템에 의해 공격이 차단된 호스트의 비율이다. 사이버전 방어 성능지표(MOP : Measure of Performance)는 방어 시스템에 의해 치료 및 차단된 비율과 공격 및 호스트 미감염율, 공격 탐지 시각으로 구성된다. 백신 치료 성공률은 바이러스 백신에 의해 치료가 이루어진 호스트의 비율이다. 방화벽 차단 성공률은 방화벽에 의해 차단된 공격의 비율이다. IPS 차단 성공률은 IPS에 의해 차단된 공격의 비율이다. 접근 공격 미감염률은 호스트에 접근된 공격수 중 미감염된 공격의 비율이다. 호스트 미감염률은 공격이 접근한 호스트 중 미감염된 호스트의 비율이다. 공격 탐지 시각은 최초 공격을 탐지하고 차단한 시각이다.

<표 3>는 사이버전 방어 효과지표 및 성능지표를 정량적으로 계산하기 위해 수식으로 나타낸다. 방어 성공률을 산정할 수 있다면 역으로 공격 성공률을 산정할 수 있으며 이것은 피해효과를 정량적으로 산출 할 수 있게 해 준다.

<표 3> 사이버전 방어 MOE/MOP

구 분	항 목	정 의
MOE	방어 성공률	(차단 공격 수)/(전체공격수)×100
	호스트 감염 차단률	(1-(접근호스트 수)/(공격 대상 호스트 수))×100
MOP	백신치료 성공률	백신별, (치료공격수)/(전체공격수)×100
	방화벽 차단 성공률	방화벽 별, (차단 공격수)/(전체공격수)×100
	IPS 차단성공률	IPS별, (차단 공격 수)/(전체공격수)×100
	접근 공격 미감염률	(1-(감염공격 수)/(접근 공격 수))×100
	호스트미감염률	(1-(감염호스트 수)/(접근 호스트 수))×100
	공격 탐지 시각	최초 공격이 탐지하고 차단한 시각

방어적인 사이버전투 피해평가 연구도 활발히 이루어지고 있다. [12]에서는 공격자의 사이버공격 행위, 방법적인 측면과 디지털 포렌식 기법의 증거수집을 통하여 사이버 공격 방법론의 모든 경우를 고려한 완전한 목록(CAMEL : Cyber Attack

1) ※ EBIS : Expected benefits of an investment in information security

Methodology Exhaustive List)을 작성한다. 리스트를 와 영향을 이용하여 사이버공격방법에 의한 공격트리(CAMAT : Cyber Attack Methodology Attack Tree)를 구성하고 이것으로부터 방어적 사이버전투 피해평가를 가능하게 하는 모델(DCBDA : Defensive Cyber Battle damage Assessment)을 제안하였다. DCBDA 모델은 공격 가능성과 영향 수준에서 판단을 포함하지만 이러한 방법에도 불구하고 대응을 위한 구체적인 정량적 규모를 산정하기는 어렵다.

[13]에서는 사이버전투 평가에서 사이버전투피해 평가 와 공격자에 대한 사이버전투 능력의 강도 두 가지 측면에서 평가를 시도하여 위험을 평가하고 관리하고자 하였다. 즉 사이버 공격에 대한피해평가와 공격의 주체에 대한 방어자의 강도(CS : Cyber Strength)를 공격 이벤트, 치명성, 가능성, 영향 등 공격행위에 대한 13가지 요소들을 고려하여 위험을 평가하고 관리하고자 하였다.

사이버 공격에 대한 악의적인 행동을 나타내는 공격 그래프, 보안 메트릭 계산 및 위험 분석 절차를 제공하여 사이버 공격 모델링 및 영향 평가 프레임 워크를 제안하였다. 사이버 공격 모델링과 영향평가 구성 요소 (CAMIAC : Cyber Attack Modeling and Impact Assessment Component)를 이용하여 거의 실시간으로 대응수단의 결정에 기여하고자 하였다. 그러나 모델링과 악의적인 행위자를 탐지하더라도 적절한 대응 규모를 정량적으로 산정하기는 여전히 어려움이 있다[14][15].

위의 피해평가 기법 중 Gorden-Lobe 모델은 공격에 대한 피해를 구체적인 금액으로 산출하고 대비를 위한 보안투자와 그 이익까지도 정량적으로 산출이 가능하다. 그러나 DCBDA모델, CMT모델, 사이버전 방어 효과지표는 사이버공격의 피해를 자산의 공격 성공률과 방어률 등 다양한 요소를 통하여 제시하였으나 구체적인 대응을 위한 규모를 산출하기는 어려웠다.

2.4. 시큐리티 스코어와 OWASP 위험 평가기법

시큐리티 스코어는 사이버공격 행위에 대한 가시화된 척도로서, 추적 가능하고 지속적으로 누적된 행위들에 의해 생성된 위험상태 표시이다. 시큐리티 스코어링을 효율적으로 활용한다면, 자산의 중요도에 따라 공격피해를 정량화하여 수치로 나타낼 수 있으며 가시화하여 지속적으로 관리해 나갈 수 있고 객관화된 지표를 통해 실시간으로 위협식별이 가능해져, 해당 공격에 대한 일시적이고 한정적인 대응에서 확장된 선제적이고 공세적인 대응을 가능하게 해주는 기준을 제시해 줄 수 있게 된다.

OWASP Risk Rating Methodology에서 위협에 대한 발생 가능성과 영향에 관련하여 다음과 같은 치명성 스코어를 정의하였다[16].

<표 5> Determining the Severity of the Risk

Likelihood and Impact Levels				
0 to < 3		LOW		
3 to < 6		MEDIUM		
6 to < 9		HIGH		
Overall Risk Severity				
Impact	HIGH	Med	High	Critical
	MED	Low	Med	High
	LOW	Note	Low	Med
		LOW	MED	HIGH
	Likelihood			

시큐리티 스코어링의 핵심은 사이버공격 행위에 대해 적절한 가중치를 부여하는 것이며, 가중치 부여를 위해서는 공격의 치명성, 자산의 중요도, 피해에 대한 복구능력 등 다양한 요소들을 고려해야한다. OWASP에서는 사이버공격의 발생 가능성과 그러한 공격이 미치는 영향을 3가지 수준(Low, Medium, High)으로 분류하였고, 전체적인 위협의 치명성을 발생가능성과 미치는 영향의 연계를 통하여 9가지 수준으로 세분화 하였다. 이러한 세분화된 기준을 고려하여 가중치를 부여 할 수 있다.

'FIRST'의 CVSS(Common Vulnerability Scoring System)은 보안취약점을 다양한 요소로 평가하여 정량화하는 시스템이다. CVSS는 이러한 취약점들을 기본적 척도(Base Metric) 8가지, 임시적 척도(Temporal Metric) 3가지, 환경적인 척도(Environmental Metric) 11가지 요소로 나누어 구

분하고 있으며 해당 사항을 선택하면 취약점 스코어가 산출되어 정량화 되는 계산기를 제공함으로써 사용자들로 하여금 보안취약점을 산출하여 볼 수 있도록 제공한다[17].

CVSS의 장점은 표준화된 취약점 점수를 제공하고 오픈 프레임 워크를 제공함으로써 점수를 추출하는 데 사용되는 개별적인 특성이 투명해지며, 위험의 우선순위를 정하는 데 도움이 된다. 환경 적 점수가 계산 될 때, 취약점은 각 조직에 맥락을 나타내기 때문에 조직에 대한 취약성으로 인한 위험을 보다 잘 이해할 수 있다. 하지만 기본적으로 가지고 있는 취약점을 관리할 수 있지만 공격에 대한 피해 평가를 정량화하기에는 한계를 가지고 있다.

3. 비례성의 원칙적용을 위한 고려요소

군은 적의 도발로부터 충분한 대응을 고려하고 있으며 이의 일환으로 비례성 대응원칙을 적용하여 왔다. 비례성 대응원칙을 위한 국가기반시설, 국가중요시설, 국방예상표적, 정보시스템 자산 중요도, 피해정도 등 다양한 요소들이 고려되어 정성적으로 판단되어야 할 것이다.

3.1. 국가기반시설 및 국가중요시설 보호등급

국가는 국가 주요기반시설<표 6> 및 국가중요시설들을 지정하고 적절한 수준으로 보호하여 국가안보와 국민생활을 적 위협으로부터 안전하게 보호하고자 한다[18].

“국가중요시설”이라 함은 공공기관, 공항, 항만, 주요산업시설 등 적에 의하여 점령 또는 파괴되거나 기능이 마비될 경우 국가안보 및 국민생활에 심대한 영향을 미치는 시설을 말한다[19]. 따라서 국가중요시설의 적절한 방호는 국가의 안보와 안전한 국민생활의 핵심요소라고 할 수 있으며, 시설의 기능・역할의 중요성과 가치의 정도에 따라 국가중요시설 “가”, “나”, “다”등급으로 분류하며 그 기준은<표 7>과 같다. 각 시설분야는 공공기관시설, 산업시설, 전력시설, 방송시설, 정보통신시설, 교통시설, 공항시설, 항만시설, 수원시설, 과학연구시설, 교정・정착지원시설, 지하공동구 시설 등이 해당하며 각 시설별 방호등급을 구분하여 적용한다.

<표 6> 국가기반시설 분야별 지정 현황

구분	산업분야	지정시설
에너지	전력	발전소
	가스	생산기지
	석유	생산시설, 비축시설
정보통신	통신망	통신국사, 망관리센터, 해저케이블육양국
	전산망	전산망, 정보센터
교통수송	철도	철도
	항공	항공교통센터, 공항
	화물	IDC
	도로	고속도로
	지하철	지하철
	항만	무역항
금융	금융	공공은행, 공공기관
보건의료	의료서비스	병원,응급의료정보센터
	혈액	혈액원, 혈액검사소
환경	환경	쓰레기 매립장, 소각장
식용수	댐	다목적 댐, 생공용수댐
	정수장	광역정수장,지방정수장

이러한 국가중요시설의 방호등급을 준용하여 각 구분 기준에 해당하는 시설들이 사이버공격을 당하여 시스템 파괴 및 기능마비 시 비례성의 원칙을 적용하여 2~4배의 대응을 적용하고자 한다. 즉 방호등급 “가”등급 = 4배, “나”등급 = 3배, “다”등급 = 2배의 대응 원칙을 적용하고자 한다.

<표 7> 국가중요시설 보호등급 분류 및 기준

구 분	기 준
“가” 급	적에 의하여 점령 또는 파괴되거나, 기능 마비 시 광범위한 지역의 통합방위작전수행이 요구되고, 국민생활에 결정적인 영향을 미칠 수 있는 시설
“나” 급	적에 의하여 점령 또는 파괴되거나, 기능 마비 시 일부 지역의 통합방위작전수행이 요구되고, 국민생활에 중대한 영향을 미칠 수 있는 시설
“다” 급	적에 의하여 점령 또는 파괴되거나, 기능 마비 시 제한된 지역에서 단기간 통합방위작전수행이 요구되고, 국민생활에 상당한 영향을 미칠 수 있는 시설

3.2. 군 예상 표적에 대한 비례성원칙 적용

군 작전수행의 핵심역할을 하게 되는 군 자산 중 사이버공격의 주요 표적으로 예상 되는 자산을 정리해 보면 다음 <표 8>과 같으며 주요 자산은 전장정보관리체계, 자원관리정보체계, 타격체계, 방어체계, 감시자산, 전산/통신 인프라, 통신체계, 공개웹사이트, 개인소유정보체계 등으로 볼 수 있다. 그러나 예상표적 중 전쟁을 수행하는 핵심 의사결정지원체계인 지휘통제체계 및 감시체계(C4ISR)가 가장중요하다 할 수 있다.

<표 8> 군 영역의 주요 예상표적

분 야	대 상
전장관리정보체계	지휘통제체계, 중앙방공통제소 등
자원관리정보체계	국방인사정보체계, 국방물자정보체계 등
타격체계	지상, 해상, 공중 등 타격체계
방어체계	방공망, 미사일방어체계
감시자산	항공/위성 감시자산, 해상, 대공, 감시자산
전산/통신 인프라	유선망, 전장관리망, 전술통신망 등
공개웹사이트	홈페이지, SNS
개인소유정보체계	블로그 및 홈페이지, SNS

그리고, 다음으로 이러한 결심내용이 행위로 나타나게 되는 타격 및 방어 무기체계(W : Weapon system)가 중요하며, 그 외 전쟁수행이 가능하도록 중요체계들을 유기적으로 지원하게 되는 기타지원체계(S : Support system) 순으로 중요성을 재정의 할 수 있다. 따라서 주요 체계들의 중요성 또한 비례성 원칙을 적용하는데 큰 요소가 될 것이며, C4ISR표적 공격시 =4배, 타격 및 방어 무기체계 = 3배, 기타지원체계 = 2배의 비례성 원칙을 적용하여 대응규모를 산정한다.

3.3. 피해수준에 대한 비례성원칙 적용

사이버 공격이 조직이나 시스템에 미치는 영향의 수준에 따라 대응규모를 선정 시 비례성을 적용하려고 한다. 즉 어떠한 사이버 공격의 영향으로 인가되지 않은 노출, 임의적인 변경이나 파괴, 또는 사용자가 시스템 및 정보에 대한 접근차단 및 방해 등이 조직이나 자산, 대중이미지 등에 대한 제한적인, 중대한, 심각한 부정적 영향을 갖는 것으로 예측되는 경우에 이것을 영향수준으로 정의하고 비례성의 원칙을 <표 9>처럼 정의한다[20].

<표 9> 사이버 공격에 대한 영향수준 정의

영향 수준	정 의
LOW	①주요 유형 자산 또는 자원이 많이 손실, ②조직의 사명, 평판 또는 이익을 크게 위반하거나 해를 입히거나 방해, ③사람이 사망하거나 중상을 입을 수 있음.
MED	①값 비싼 자산 또는 자원의 손실을 초래 ②조직의 사명, 평판 또는 관심을 침해하거나 해를 입히거나 방해 할 수 있음. ③사람이 부상을 입을 수 있음.
HIGH	①일부 유형 자산 또는 자원의 손실을 초래 ②조직의 사명, 명성 또는 관심에 큰 영향을 미칠 수 있음.

즉 제한적인 부정적인 영향 = 2배, 중대한 부정적인 영향 = 3배, 심각한 부정적인 영향 = 4배의 대응규모를 비례성 원칙으로 대응규모를 적용하기로 한다.

3.4. 정보시스템의 중요도에 대한 비례성 적용

정보자산의 중요도를 기밀성, 무결성, 가용성 측면에서의 평가를 통하여 산정한다. 이렇게 산정된 중요도를 상, 중, 하 3단계의 수준으로 정의 한다. 기밀성, 무결성, 가용성의 세 가지 요소별 특성 훼손에 따른 정보자산 중요도 평가 기준을 표로 나타내 보면 다음<표 10>과 같다.

<표 10> 정보시스템 중요도 평가 기준

구분	기밀성훼손	무결성훼손	가용성훼손
“상” 평가	조직전체, 상당한 손실	조직전체, 상당한 손실	10분이내 복구필요
“중” 평가	부서나 팀, 상당한 손실	부서나 팀, 상당한 손실	1시간이내 복구필요
“하” 평가	피해 미비	피해 미비	24시간이내 복구필요

즉, 기밀성 측면에서는 자산에 대한 접근권한이 있는 자 만이 접근 및 열람이 가능한 자산으로 기밀성이 상실되었을 때 조직전체에 상당한 손실을 입히는 자산을 중요도 ‘상’으로 평가하고, 조직내부에 국한 하여 접근 및 열람이 가능한 자산으로 기밀성이 상실되었을 경우 부서나 팀에 상당한 손실을 입히는 자산을 중요도 ‘중’으로 판단하고 사외로 공개되어도 무방한 자산으로 기밀성의 상실이 있더라도 그 피해가 미비한 자산을 중요도 ‘하’로 평가한다.

무결성 측면에서 본다면 중요한 의사결정에 사용되는 데이터와 같이 무결성이 훼손 되었을 경우, 조직에 상당한 손실을 입히게 되는 자산을 중요도 ‘상’으로 평가하며, 부서나 팀에 상당한 영향을 미치는 수준은 중요도 ‘중’으로 평가한다. 무결성이 훼손되었을 경우, 그 피해가 미비한 자산을 중요도 ‘하’로 평가한다.

가용성 측면에서 본 중요도는 원래대로 복구되어 정상적인 서비스가 되어야만 하는 필요시간을 기준으로 산정하여 10분이내 가용성 보장이 필요한 경우 중요도 ‘상’으로 평가하고, 1시간이내는 중요도 ‘중’, 24시간이내는 중요도 ‘하’로 평가한다.

3.5. 고려요소 별 비례성원칙 적용 방법

위의 다양한 요소들을 고려하여 공격에 대한 비례성 대응원칙을 적용하기 위해 <표 11>에서 고려요소별 비례성 대응 규모를 정의 한다. 즉, ① 국가중요시설 보호등급 수준, ② 사이버공격으로 초래되는 부정적 영향수준, ③ 정보시스템 자산의 중요도, ④ 군사적 영역에서 예상표적 중 중요도를 고려하여 비례성 대응원칙의 규모를 다음과 같이 정의 하고자 한다.

<표 11> 비례성 대응원칙에 대한 관계 정의

구분	국가중요시설 방호등급	공격영향수준	정보자산중요도	군사영역의 예상표적	비례성 대응규모 적용
수준	“가”급	HIGH	상	C4ISR	**4배**
	“나”급	MED	중	W	**3배**
	“다”급	LOW	하	S	**2배**

적의 공격에 대한 <표 11>의 관계에서 비례성 대응규모는 정성적 평가의 기준이 되며 네 개의 요소들이 모두 해당되어야만 그 수준의 대응규모가 적용되는 것이 아니라, 어느 하나라도 해당이 된다면 그 요소가 평가된 수준에서의 대응규모를 적용한다. 그리고 낮의 수준의 요소로 평가가 되더라도 추가적인 요소가 반복되어 평가된다면 대응규모의 상향적용이 고려될 것이다. 또한 두 가지 이상의 요소가 중복되어 나타난다면 그 중 상위수준의 대응 규모를 적용한다.

4. 피해규모 정량화를 위한 모델적용 및 고려요소 적용

사이버공격의 피해평가를 위해 Gorden-Lobe 모델을 이용하여 실제적인 위협에 대한 대응을 위한 투자와 그에 대한 손실함수를 통해 예상되는 피해를 산출한다. 그리고 그 결과에 대하여 OWASP Risk Rating Methodology, 비례성 대응원칙을 위한 고려요소와 관계를 활용하여 정성적인 평가 및 대응규모를 산정한다.

4.1. 사이버공격 시나리오에 대한 피해사례

유형자산과 무형자산별 피해에 따른 규모산정을 위해 다음과 같은 시나리오를 적용한다. 즉 사이버 공격에 의해 물리적인 손상 및 무형자산에 대한 피해가 발생하여 금전적 비용 없이 회복이 불가능 한 상태를 가정하였다.

항공 서비스를 제공하는 A항공사는 사이버 공격이 발생하여 운항통제시스템과 고객에 대한 항공편 예약 서비스를 제공하는 시스템의 WAS 및 DB서버가 파괴되었다. 이로 인해 고객의 DB를 재구축하여야 하고 WAS 및 DB 서버(IBM S824)를 구매하여야 한다. 관련 장비를 재 구매해야 하며 서버구동을 위한 상용SW 및 응용SW도 구매해야 하는 상황이다. 또한 관련내용이 언론에 보도되어 고객들에게 개인정보유출에 대한 소송이 제기되었고 현재 주가는 총 발행 주식 2,000만주에서 1주당 10,000원에 거래되던 주식이 사이버공격 발생이후 3일간 20% 가 하락하여 현재 8,000원에 거래되고 있으며 큰 변동 폭 없이 횡보하고 있다. 결국 시가총액 대비 사건발생 이전 2,000억 원에서 1,600억원으로 400억원의 시가 총액이 손실을 보게 되었다. 또한 이미지의 쇄신을 위해 마케팅 광고를 계획하고 있으며, 그 비용으로 10억원이 지출될 예정이다. A그룹에서는 향후 이러한 사고를 방지하기 위해 단계적으로 20억원 규모의 투자를 통하여 보안시스템을 구축하고 인력을 확보할 계획이다. 위의 시나리오를 통해 산정한 피해 금액<표 12> 및 보안투자 금액<표 13>을 정리하면 다음과 같다.

<표 12> 시나리오 기반 피해금액 및 복구비용

단위(백만원)

피해자산(TAV, IAV)			복구 내용	비용
유형 (TAV)	서버	DB, WAS	구매	200
무형 (IAV)	상용 응용 SW	Weblogic, Oracle 등	구매	200
	주가 하락	시가총액 대비 20%하락	-	40,000
피해금액합계(TAV+IAV)				40,400

<표 13> 위협 예방을 위한 투자 내용

단위(백만원)

투자금액		내용	비용
정보 보호 투자	보호시스템 구축	IDS, IPS, ESM	1,600
	정보보증 전문 인력채용	고급기술자 중급기술자 초급기술자	연간 200
마케팅 투자	정보보증 팀 신설	사무실 및 업무환경구축	200
	이미지 회복을 위한 마케팅	광고 및 프로모션	1,000
계			3,000

위와 같은 계산을 통하여 발생한 피해발생금액은 유형자산 복구비용 4억원과 무형자산(주식가치 하락 금액) 600억원 등 총 604억원의 피해에 대한 비용이 발생하였다. 또한 이후 이에 대한 능동적 대응과 예방을 위한 보안투자 금액 30억원이 발생하였다. 이것을 정리해보면 위협행위에 대한 대응 총액을 산출 할 수 있을 것이다.

또한 보안위협에 대한 대응과 예방을 위해 시스템 구축 및 인력채용에 대한 투자와 보호활동을 한 결과 최초 공격과 유사한 공격이 추가적으로 발생 하였으나 시스템 이중화 구축을 통하여 메인 서버의 하드웨어 파괴와 DB 일부분이 파괴되었지만 데이터 분산 및 이중화로 인하여 신속히 복구가 되었다. 이에 대한 복구비용은 서버구매비용 2억원, DB복구비용 등 2,000만원이 발생하였으며 일시적인 서비스 제한으로 인하여 해당기간 내 매출액이 전년대비 4,000만원이 줄었다. 따라서 시스템 구축 및 보안에 대한 투자로 인하여 손실액은 2.6억 원이 발생하였다. 또한 신속한 대응 및 복구로 인하여 언론보도에도 불구하고 주가는 5%하락한 9,500원에 거래되고 안정되었다. 따라서 주가총액 대비 100억원의 하락이 발생하였다. 따라서 투자이후 총 손실액은 102.6억 원이 발생하였다. 이는 전년 동일한 사고 발생(414억) 대비 75%가 감소함을 보였다.

위협행위 발생에 따른 총 대응을 위한 비용발

생(TRV)은 유형자산 복구금액(TAV) + 무형자산 피해액(IAV) - 투자액에 따른 이익(EBIS) 추정 액으로 다음 수식(2)와 같이 정리 할 수 있다.

$$TRV = TAV + IAV - EBIS(z) \quad (2)$$
$$EBIS(z) = \lceil v - S(z, v) \rceil L$$

① TRV(Total Response Value) :
위협행위 발생에 대응해야 할 총 금액 규모

② TAV(Tangible Asset Value) :
유형자산에 대한 피해규모

③ IAV(Intangible Asset Value) :
무형자산에 대한 피해규모

위의 시나리오에 대하여 대응을 위한 금액을 위의 식으로 산정해 보면 다음과 같이 정량적 규모 102.6억이 산출된다.

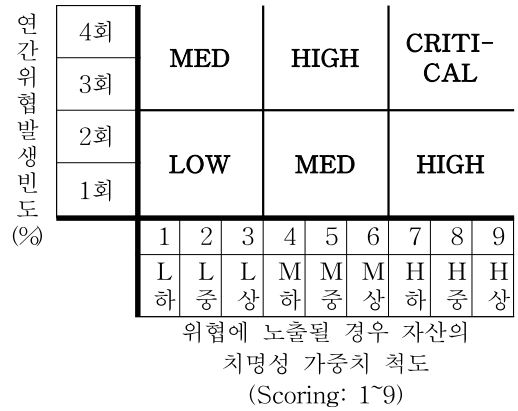
TRV = 2억원 + 402억원 - 301.4억원
= 102.6억원

4.2. 자산의 가치와 치명성 가중치에 따른 비례성 원칙의 적용

이러한 결과를 군사적 상황에 대비하여 적용하기 위해 OWASP Risk Rating Methodology를 활용하여 물리적 비례성의 원칙 대응을 적용하려고 한다. 공격행위의 위험도에 따라 기본적으로 부여되는 가중치를 설정하고, 그러한 공격행위가 군 조직과 국가에 미치는 영향, 즉 사이버공격 행위에 대응하기 위해 조직이 기울여야만 하는 노력의 정도에 따라 가중치는 차등 적용되어야 한다. 여기에서는 자산에 대한 중요도 및 치명성에 따라 가중치를 1~9까지 부여하도록 한다. 이러한 가중치를 위협에 노출되었을 경우 발생하는 피해규모에 적용한다. 연간 위협행위 발생에 따른 위험비용 산정은 아래와 같이 정의 할 수 있다.

① 연간위험발생비용 = 자산가치 × 위험발생확률

이러한 상관관계를 바탕으로 자산의 가치와 연간위협발생 빈도에 따른 대응규모를 다음 (그림 1)과 같이 표현 한다.



(그림 1) 위협에 대한 자산의 가치와 연간위협발생 빈도에 따른 대응규모

사이버 공격에 대한 비례성에 원칙에 의한 대응규모를 2~4배 규모로 적용한다고 가정할 경우 대응을 위한 공격 예상피해효과를 산정하는 수식(3)은 다음과 같게 된다. 즉 공격에 노출되었을 때 자산의 중요도와 치명성의 정도에 따라 스코어링 가치척도 1~3까지는 저 위협 공격에 대한 대응으로 2배의 비례성 원칙을 적용하여 대응 규모를 정하고 스코어링 가치척도 4~6까지는 중간 위협공격에 대한 대응규모로 3배의 비례성 원칙을 적용하며 마지막으로 스코어링 가치척도 7~9는 고 위협 공격에 대한 대응규모로 4배의 비례성원칙을 적용, 또는 그 이상의 최대 역량으로 대응한다. 하지만 치명성이 낮다 하더라도 발생빈도가 높아지면 영향과 손실이 커질 수 있다. 따라서 기본적으로 자산의 치명성과 중요도를 판단하고 사이버 위협행위의 발생빈도에 따라 총체적인 피해수준을 판단하여 (그림1) 에서처럼 대응규모를 LOW=2배, MEDIUM=3배, HIGH4배, CRITICAL=4배를 초과하여 적용한다.

$$LTAR = TRV \times 2 \text{ (LOW)}$$
$$MTAR = TRV \times 3 \text{ (MEDIUM)} \quad (3)$$
$$HTAR = TRV \times 4 \text{ (HIGH)}$$
$$C\text{-}TAR = TRV \times 4 \text{ 초과 (CRITICAL)}$$

① LTAR(Low Threat Attack Response)
자산의 가치척도에 사이버 공격 발생빈도에

따른 저 위협 대응규모

② MTAR(Medium Threat Attack Response)
자산의 가치척도와 사이버 공격 발생빈도에 따른 중간 위협 대응규모

③ HTAR(High Threat Attack Response)
자산의 가치척도와 사이버 공격 발생빈도에 따른 고 위협 대응규모

④ C-TAR((Critical Threat Attack Response)
자산의 가치척도와 사이버 공격 발생빈도에 따른 치명적 위협 대응규모

시나리오에 대하여 자산의 가치와 발생빈도를 고려하였을 경우 국가기반시설(국가중요시설)에 대한 공격이며, 시스템에 대한 직접적인 파괴행위가 있었으므로 시설의 중요도와 가치측면을 고려할 때 상당한 영향을 미칠 수는 있지만 국가적인 수준에서의 치명적인 영향은 없었으므로 공격행위의 수준을 중간위협공격(MEDIUM)으로 판단하였다. 따라서 대응규모는 3배의 비례성 원칙을 적용한다. 구체적인 대응규모를 산정하기 위하여 TRV에 3배를 곱하면 아래와 같이 307.8억원의 정량적/정성적 대응 규모가 산출된다. 이러한 결과를 사이버 공격에 대한 선제적 대응 및 공세적 대응의 기준으로 사용할 수 있다.

MTAR = TRV(102.6억원) × 3(MEDIUM)
= 307.8억원

5. 결론 및 향후연구

본 논문을 통하여 우리는 공격 형태와 유형에 대하여 피해규모를 정의함으로써 실제적인 대응 수준에 대한 규모와 기준을 산출하는 방법을 제시하였다. 이는 상황발생시 대응을 위한 의사결정을 더욱 신속하게 할 것이며 대응의 수준과 규모에 대한 모호성을 배제시켜 대응활동을 하는 주체들 에게 명확한 기준을 제공하게 될 것이다. 또 사이버 위협이나 공격에 대한 실제적이고 입체적인 대응을 보완하여 사이버킬체인의 완성도를 높이게 될 것으로 생각한다. 특히, 사이버전과 입체적인 물리전 연계를 위해 정성적/정량적 피해평가 분석기술, 사이버전 피해평가 자동화 기술의 발전을 위한 방향을 제시하게 될 것이다. 그러므로 일시적인 방어위주의 대응개념에서 탈피하여 공세적이며 입체적인 대응체계를 구축하게 되는 기반을 제공 할 것이다.

향후 연구할 분야는 정량화되어 산출된 피해규모와 기준을 가지고 선제적이고 공세적인 대응을 위해 어떻게 적용하고 활용할 것인가에 대해 기준별, 규모별 세분화하여 연구할 필요가 있다.

참고문헌

[1] KISA, “Special Report of WannaCry Analysis”, pp80-85, 2017.

[2] Sysmantec, “WannaCry : Ransomware attacks show strong links to Lazarus group”, https://www.symantec.com/, 2017.

[3] Richard B. Andres, “The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence,” in Derek S. Reveron (ed.) Cyberspace and National Security : Threats, Opportunities, and Power in a Virtual World, Washington DC : Georgetown University Press, 2012.

[4] Jeffrey Hunker, Bob Hutchinson, and Jonathan Margulies, “Role and Challenges for Sufficient Cyber-Attack Attribution,” Dartmouth College : Institute for Information Infrastructure Protection, January 2008.

[5] Hyo-young Lim, Wan-ju Kim, Hong-jun Noh, Jae-sung Lim. “Research on Malware Classification with Network Activity for Classification and Attack Prediction of Attack Groups”. Journal of KICS, 42(1), 193-204. 2017

[6] Wanju Kim, Changwook Park, Soojin Lee, Jaesung Lim, “Methods for Classification and Attack Prediction of Attack Groups based on Framework of Cyber Defense Operations”, Journal of KIISE : Computing Practices and Letters 20(6), pp. 317-328, Jun. 2014.

[7] KISA, “Cyber Threat Trend in 2016 and 7 Cyber Threat Forecasts in 2017”, 2017.

[8] Gordon, Lawrence A, and Martin P. Loeb. “The

economics of information security investment.", ACM Transactions on Information and System Security (TISSEC) 5.4, pp438-457, 2002.

[9] Wansoo Cho, Taekyu Kim, Yonghyun Kim. "Modeling and Simulation of Cyber Damage Assessment for Cyber Warfare Effectiveness Analysis", Proceedings of Spring Conference of KIIE, pp 3119-3125. 2016.

[10] Yoon Jong-Sung et al., "Influence Indicator Research and Development Trend Analysis Report", ADD, ADDR-525-150921, 2015.

[11] Kim Tae-Kyu et al.. "Research on Matrix of Measurement of Effectiveness(MOEs) and Measurement of Performance(MOPs) for Cyber Threat and Defense Behavior on Cyberwarfare Simulation", Proceedings of Spring Conference of KIIE, pp3114-3118. 2016.

[12] Danyliw, Roman, Jan Meijer, and Yuri Demchenko. "The incident object description exchange format." 2007.

[13] Ostler, Ryan. "Defensive cyber battle damage assessment through attack methodology modeling", Air Force Inst of Tech Wright-patterson AFB of Graduate School of Engineering and Management, 2011.

[14] Denning, D. "Assessing Cyber War. Assessing War: The Challenge of Measuring Success and Failure", Blanken, L., Ed, 266-284. 2015

[15] Kotenko, Igor, and Andrey Chechulin. "A cyber attack modeling and impact assessment framework.", Cyber Conflict (CyCon), 2013 5th International Conference on. IEEE, 2013.

[16] OWASP, "The OWASP Risk Rating Methodology", https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology, 2017

[17] FIRST, "Common Vulnerability Scoring System Version 3.0 Calculator", https://www.first.org/cvss/calculator/3.0, 2017

[18] Jong-in Lim et al., Korea Univ., "Research on development of cyber threat scenarios and countermeasures", 2014.

[19] 국방부, 국방부훈령 제1057호(국가 중요시설 지정 및 방호 훈령), 2009.

[20] NIST, "Special Publication 800-30, Risk Management Guide for Information Technology Systems", July 2002.

〔저자소개〕

홍 병 진 (Byoung-jin Hong)
2001년 2월 동아대학교 경영학 학사
2016년 1월 국방대학교 컴퓨터공학 석사
2017년 3월 아주대학교 NCW학과
박사과정
email : ancjsdldi77@naver.com

임 재 성 (Jaesung Lim)
1983년 2월 아주대학교 전자공학 학사
1985년 2월 한국과학기술원 전자공학 석사
1994년 8월 한국과학기술원 전자공학 박사
email : jaslim@ajou.ac.kr

김 완 주 (Wanju Kim)
1998년 2월 서울과기대 전자공학 학사
2008년 1월 국방대학교 전산정보학 석사
2017년 2월 아주대학교 NCW공학 박사
email : sizipus1@gmail.com

조 재 명 (Jaemyung Cho)
1995년 2월 육군사관학교 전산학 학사
2004년 2월 한국과학기술원 전산학 석사
2017년 3월 아주대학교 NCW학과
박사과정
email : chojm@ajou.ac.kr