*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.29, NO.5, Oct. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.5.1179

# 위험 평가 모델 기반의 정량적 사이버 보안 평가 체계*

김 인 경,[1†] 박 남 제[2‡]
[1]제주대학교 사이버보안인재교육원, [2]제주대학교 초등컴퓨터교육전공

# Quantitative Cyber Security Scoring System Based on Risk Assessment Model*

Inkyung Kim,[1†] Namje Park[2‡]
[1]Cyber security Human Resource Institute, Jeju National University,
[2]Dept. of Computer Edu., Teachers College, Jeju National University

## 요 약

사이버보안성 평가란 자산분석, 위협분석, 취약성 분석을 통하여 자산 및 시스템의 위험 수준을 평가하여 적절한 보안조치를 적용하는 일련의 과정으로 증가하는 사이버 공격에 대한 대비를 위해 체계적인 사이버보안성 평가가 요구된다. 이에 CWSS, CVSS 등 사이버 보안 수준 측정을 위한 다양한 지표가 개발되고 있으나 표준화된 보안성 평가 결과를 통해 위험 우선순위에 따라 적절한 보안조치를 적용하기 위한 정량적 방법은 미흡한 실정으로 대상자산이 가지는 특성, 적용되어 있는 환경, 자산에 미치는 영향 등을 고려한 평가 체계가 필요하다. 이에 본 논문에서는 기존의 사이버 보안 평가 방법 분석을 기반으로 정량적 위험 평가 모델을 정립하고 정립한 모델에 적용하기 위한 평가 요소들의 정량화를 위한 방법을 제시한다. 사이버 보안성 평가 시 필요한 정성적 속성 요소들의 수준을 AHP 기법을 통한 보안요건별 가중치, 위협 별 영향도, 취약점 요소 별 점수화를 통한 위협 성공 가능성에 대한 확률값 산출을 통해 통계적 데이터를 적용해야 하는 정량적 방법의 한계점을 보완하여 표준화된 사이버 보안 평가 체계를 확립할 것으로 기대된다.

## ABSTRACT

Cyber security evaluation is a series of processes that estimate the level of risk of assets and systems through asset analysis, threat analysis and vulnerability analysis and apply appropriate security measures. In order to prepare for increasing cyber attacks, systematic cyber security evaluation is required. Various indicators for measuring cyber security level such as CWSS and CVSS have been developed, but the quantitative method to apply appropriate security measures according to the risk priority through the standardized security evaluation result is insufficient. It is needed that an Scoring system taking into consideration the characteristics of the target assets, the applied environment, and the impact on the assets. In this paper, we propose a quantitative risk assessment model based on the analysis of existing cyber security scoring system and a method for quantification of assessment factors to apply to the established model. The level of qualitative attribute elements required for cyber security evaluation is expressed as a value through security requirement weight by AHP, threat influence, and vulnerability element applying probability. It is expected that the standardized cyber security evaluation system will be established by supplementing the limitations of the quantitative method of applying the statistical data through the proposed method.

**Keywords:** Risk Assessment, Cyber security Scoring System, Quantitative Risk Model

Received(07. 11. 2019), Modified(09. 02. 2019), Accepted(09. 20. 2019)

* 이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임[2019-0-00203,선제적 위험대응을 위한 예측적 영상보안 핵심기술 개발]. 그리고, 2019년도 정부(교육부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호:NRF-2019R1I1A3A01062789)

† 주저자, ikkim@jejunu.ac.kr
‡ 교신저자, namjepark@jejunu.ac.kr(Corresponding author)

## I. 서 론

사이버보안성 평가란 자산분석, 위협분석, 취약성 분석을 통하여 자산 및 시스템의 위험 수준을 평가하여 적절한 보안조치를 적용하는 일련의 과정으로 시스템의 사이버보안 상태를 판단하기 위해 필수적으로 수행되어야 한다. 사이버위협이 증가하면서 사이버 보안에 대한 주기적인 평가를 수행을 위해 ISO 27001, K-ISMS(KISA-Information Security Management Systems), PIMS(Personal Information Management System) 등 사이버보안 관리 수준의 평가 체계가 제공되고 있다. 표준화 기구인 국제전기통신연합(ITU), 세계경제포럼(WEF), 세계경제협력기구(OECD) 등에서는 사이버보안 평가를 위한 지표를 제시하고 지표를 기반으로 각국의 사이버보안 평가지수를 공개하고 있다. 미국의 NIST(National Institute of Standards and Technology), 영국의 BERR(Department for Business Enterprise & Regulatory Reform), 국내 KISA(Korea Information Security Agency)에서도 정보보호 수준 측정을 위한 지표를 자체적으로 개발하여 사용하고 있는 등 사이버 사고를 예방하기 위한 다양한 기술적 및 정책적 평가들이 이루어지고 있다[1].

또한 사이버보안 취약성에 대한 정량적 평가를 위해 대표적인 보안취약성 평가 체계로 CWSS(Common Weakness Scoring System) 및 CVSS(Common Vulnerability Scoing System)가 사용되고 있다. CWSS는 일반적인 보안 약점의 소프트웨어 내 출현빈도를 분석을 통해 다양한 약점에 대한 평가를 위해 정량적인 기준을 제시한다. 일부 평가 척도는 2011 SANS Top 25 선정 시에 활용이 되기도 하였다. 약점 제거의 우선순위를 줄 수 있는 기준으로 활용이 가능하나 특정 소프트웨어의 특성이나 용도를 고려한 평가 방안으로는 부족하다. CVSS는 실제 발생한 보안취약성의 분석을 통해 보안 취약성의 정량적 값에 대해 시간, 환경 요소를 반영할 수 있는 평가 척도를 제시하였다. 보안 위협의 심각성을 평가하기 위한 프레임워크를 제공하나 특정 사용 환경에 종속적임[2]에 다양한 시스템을 위한 평가 체계로는 한계가 있다.

사이버보안성에 대한 정량적 평가는 평가대상 자체에서 발견되는 취약성에 대한 본질적인 평가뿐 아니라 대상자산이 가지는 특성, 적용되어 있는 환경, 자산에 미치는 영향 등을 고려하여 설정된 평가 척도에 따라 수행되어야 위험요소에 대한 보안조치의 중요도를 객관적으로 판단할 수 있다. 이에 본 논문에서는 기존의 사이버보안 정량적 평가 방법론의 분석을 기반으로 사이버 보안성 평가를 위한 위험 평가 모델을 제시하고 모델에 적용하기 위한 평가 요소들의 평가 척도를 정립하여 표준화된 결과를 도출할 수 있는 방법을 제시하고자 한다.

## II. 분석 모델 관련 연구

일반적으로 사이버 보안성 평가는 자산, 위협, 취약성, 보안통제 등을 고려한 위험도 분석을 토대로 수행되며 평가 시 분석되는 요소들의 정성적 속성으로 인하여 수치로 표현하지 않고 기술변수로 나타내는 정성적 방법이 적용된다. 그러나 정성적 분석은 전문가의 주관적 판단이 개입될 우려가 높기에 객관적 결과를 생성하지 못하는 문제점이 있으며 자산의 특성 및 가치분석에 따라 가중치를 부여하지 못하여

Table. 1. Comparison of Risk Assessment Methodology

| | Conventional Methodology | Proposed Methodology |
|---|---|---|
| Formula | Risk = Impact × Probability(Likelihood) | |
| Process | - Risk data Collection<br>- Creation of occurrence distribution table or estimation of frequency<br>- Calculation of the value loss of risk occurrence | - Applicable Threat and Vulnerability Analysis<br>- Matching analysis of threats and vulnerabilities<br>- Establish standardized risk measures against risk tolerance |
| Charac teristic | - Historical risk data required<br>- Depends on mathematical formula to estimate occurrence frequency | - Calculation of weight by security requirement according to asset characteristics<br>- Possible objective criteria for risk level tolerance |

결과를 통한 보안 계획의 수립 및 조치 구현 시 우선순위 파악에 용이하지 않다는 단점이 있다[3]. 이러한 단점을 보완하는 정량적 방법은 위험수준과 대책 적용에 대한 효과를 객관적 수치를 통해 비교가 가능하기에 보안 대책 수립 시 의사결정에 도움을 주는 등 결과에 대한 활용가치가 높지만 통계적 데이터 또는 시스템 운영 및 관리 경험을 통한 정량화 작업이 요구되기에 과거 사이버 보안관련 사례에 대한 통계적 데이터가 존재하지 않는 경우는 어려움이 따른다.

이에 본 연구에서는 사이버 보안성 평가를 위해 정성적 속성 요소들의 수준을 통계적 데이터를 적용하지 않고 정량적 수치로 산출하여 Table 1에서의 정량적 방법의 한계점을 보완하고[3] 위험 평가 산술 모델을 통한 보안성 평가 방법론을 제시한다.

## 2.1 위험도 모델

사이버 보안성 평가는 시스템의 자산 분석을 통하여 구성요소 별 취약성을 파악하고 취약성을 이용한 위협의 발생 가능성과 위협 발생 시 시스템에 미치는 영향의 정도를 결정하는 과정인 위험분석을 통하여 사이버보안이 대상 시스템에 효과적으로 적용되고 있는지는 파악하는 과정을 포함해야 한다.

취약성이란 Fig.1에서와 같이 사이버 공격을 통한 위협의 수단으로 위협 시 시스템 자산에 악의적인 영향을 줄 수 있는 매개변수로 정의할 수 있으며 위협은 악영향을 줄 수 있는 공격을 의미하여 유형에 따라 시스템에 주는 피해 정도가 다르다. 즉, 정성적 사이버 보안성 평가는 사이버 위협의 정도와 취약성 정도의 조합을 통한 위험 분석을 토대로 평가 할 수 있으며 이는 자산 하나에 대한 위험(Risk), 위협(Threat), 취약성(Vulnerability)을 다음과 같은 식으로 표현한 평가 모델로 정립할 수 있다.

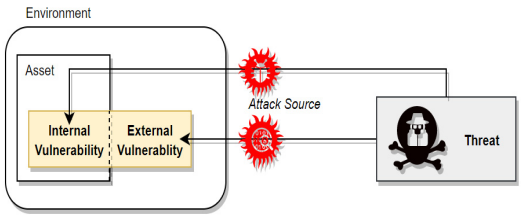


Fig. 1. Relationships Threats, Vulnerability, and Assets

$$R = T \times V$$

정량적 평가를 위한 위험 분석은 자산에 대한 하나의 위협을 기준으로 위협이 시스템에 미치는 영향성과 위협이 성공할 가능성의 정도를 결정하는 과정으로 상기 정립한 모델을 기본으로 위험 요소인 위협의 정도에 대한 정량적 정의가 필요하다. 위험분석 모델에서 $T$를 위협이 그 수준에 따라 시스템에 미치는 영향성을 수치화하여 정량적 계산이 가능하도록 표현할 수 있다. $V$는 취약성의 속성 및 개수에 따라 취약성 수준을 산출하여 위협의 성공 가능성으로 정량화 할 수 있다. 즉, 정량적 사이버 보안성 평가는 사이버 위협과 취약성의 조합을 통한 위험 분석을 위협의 요인인 취약성을 통한 위협의 성공 가능성과 그로 인한 위협 성공 시에 시스템에 미칠 영향성의 크기 정도를 수치화하여 결과를 도출하는 과정으로 수치화를 위한 모델은 다음과 같이 표현된다.

$$R = I \times P$$

즉, 정량적 위험도 모델을 통한 자산에 대한 위험은 위협을 매개변수로 가지는 함수로 위협 하나 당 자산에 미치는 영향에 확률을 적용한 확률적 기대값으로 산출되어 위협 변수 하나에 대한 공격 성공의 가능성이 높을수록 또는 영향성이 높을수록 높은 위험도의 값이 도출됨에 따라 위협의 정도를 기술화하는 정성적 해석과도 일치한다.

Table 2. Notation

| Abbreviation | Content |
|---|---|
| $R$ | Risk |
| $I$ | Impact Factor |
| $P$ | Probability Factor |

## 2.2 평가 모델

Fig.2는 상기에서 정립한 모델을 기본으로 위험을 정량화할 수 있는 체계를 수립하기 위해 Fig.1을 일반화시킨 다이어그램으로 하나의 자산을 기준으로 자산에 가할 수 있는 위협 변수를 $\{t_i\}$, 하나의 위협 시 악용될 수 있는 취약성의 집합을 $\{v_{ij}\}$의 형태로 표현하고 위협의 개수를 $m$개, 하나의 위협에

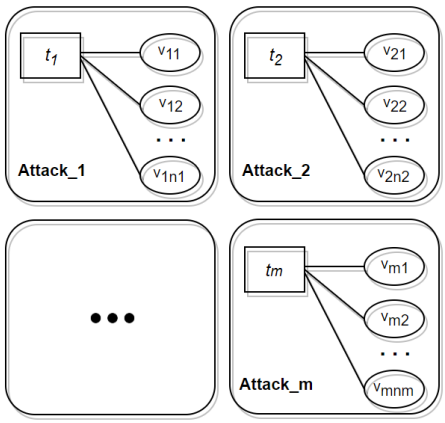


Fig. 2. A general Diagram of the Threat and Vulnerability

대응되는 취약점 개수는 $n_i$개라 하며 위협과 취약성은 모두 정성적 속성을 띄기에 모두 셀 수 있는 유한개의 범위로 간주한다.

일반적으로 하나의 위협을 가할 시 두 개 이상의 취약성이 이용될 수 있지만 본 연구에서는 하나의 위협 시 한 개의 취약성만 이용된다는 가정과 하나의 취약성은 두 개 이상의 위협에 이용될 수 있다는 가정으로 포함하여 위협과 취약성의 관계를 구성하였다. 또한 하나의 위협이나 취약성이 다른 위협이나 취약성을 야기 시킬 수 있어 위협과 위협 간의 관계, 취약성과 취약성 간의 관계의 연관성 규명을 통한 파급성에 대한 분석이 필요하지만 본 연구에서는 하나의 위협이 다른 위협에 영향을 주거나 하나의 취약성이 다른 취약성에 영향을 주지 않는 서로 독립적인 사건으로 가정한다. 즉, 위협 $t_i$을 가할 시에는 자산의 취약성 중 $\{v_{i_1}, v_{i_2}, v_{i_3}, \cdots, v_{i_{n_i}}\}$이 위협의 수단으로 작용될 수 있으며 본 연구에서의 가정을 적용한 위험 평가 모델을 위한 환경의 구성을 수식으로 표현하면 Fig.3와 같다.

상기에서의 가정과 표현방법을 정량적 위험도 모델에 적용하면 Impact factor는 위협 $t_i$을 변수로 하는 함수 $I(t_i)$로 구체화시킬 수 있으며 위협의 가능성은 Probability factor는 $t_i$와 맵핑되는 $v_{ij}$의 취약한 수준 $V(v_{ij})$에 따라 위협의 성공 가능성을 확률값으로 가지는 함수 $P(t_i;v_{ij})$로 구체화시킬 수 있다. 자산 $X$에 대한 정량적 위험도 모델은 다음과 같이 표현할 수 있다.

Configuration : Risk Assessment Model

*Let*

Threat set
$= \{t_i \mid i = 1,2,3...m\}$
Vulnerability set
$= \{v_{ij} \mid i = 1,2,...,m,\ j = 1,2,...,n_i\}$

*Assumption*

① $t_i$ : *independent*
$v_{ij}$ : *independent*

② $\exists\ v_{ij} = v_{i'j}$

③ $\{v_{ij} \cap v_{ij'}\} = \varnothing$ for $i = 1,2,...,m$
$j = 1,2,...,n_i$

Fig. 3. Concept of Environment for Risk Assessment Model

$$\Rightarrow R(t_i) = I(t_i)\sum_{j=1}^{n_i} P(t_i;v_{ij})$$

$$\Rightarrow R(X) = \sum_{i=1}^{m} R(t_i)$$

**Risk of Asset per one asset($X$)**

$$R(X) = \sum_{i=1}^{m} I(t_i)\sum_{j=1}^{n_i} P(t_i;v_{ij})$$

## III. 제안된 평가 요소와 분석

정량적 위험도 모델을 적용하면 각 자산에 대한 위험도를 수치화시킬 수 있으며 이를 확장시키면 시스템 단위의 위험도 측정도 가능하다. 그러나 정량적 위험도 값의 신뢰성을 위해서는 위험도 함수의 변수 Impact factor와 Probability factor에 대한 객관적 수치가 필요하며, 많은 통계적 자료 및 모의 침투와 같은 실험적 자료를 통해 정량적 값을 제시하고 그 객관성을 보장하기에 어려움이 있다. 일부 시스템은 특성상 보안 관련한 데이터가 잘 공개 되지 않으며 가동 중인 시스템에 대한 모의 해킹 및 침투 테스트를 통한 실험적 데이터 축적이 힘들다. 또한 사이

버 사고 시 시스템마다 다양한 경우와 맥락을 가질 수 있기에 정량화하기가 쉽지 않다. 이에 본 절에서는 상기 정립한 정략적 위험도 평가 모델에서 자산에 대한 위험성을 결정하는 요소인 Impact factor와 Probability factor를 정량화 할 수 있는 체계를 수립하고자 Impact factor와 Probability factor를 결정짓는 요소인 자산, 위협, 취약성 별 평가 척도를 제시하고 평가 척도에 따른 정량적 값 산출 방법을 제시하고자 한다.

### 3.1 자산 요소

시스템 내의 세부적인 자산을 기준으로 보면 자산의 유형, 특성, 속성 등에 따라 우선순위를 갖는 보안요소가 달라진다. 예를 들어 시스템 소프트웨어 내 통신 프로토콜은 정확하고 완전한 값을 가져야 하며 조작 및 변경 등이 없음을 보장하기 위해 높은 무결성이 요구된다. 이는 통신 프로토콜의 취약성을 이용한 조작의 위협이 가해지면 기밀성, 무결성, 가용성 측면에서 모두 영향을 받을 수 있지만 자산의 특성으로 인하여 무결성의 보안 요건이 가장 중요시 되므로 위협에 따른 영향도 산출 시 무결성에 대한 가중치를 부여해야 정확한 위험도 평가 값을 도출 할 수 있다. 즉, 자산에 대한 위협의 영향도 값인 Impact factor 산출 시 자산에 요구되는 기밀성, 무결성 및 가용성의 수준을 고려하여야 하고 우선순위에 따른 가중치 값을 부여하여야 한다. 부여하는 가중치는 자산의 성격에 따라 특정한 보안요건만이 가장 중요하다고 할 수 없는 경우도 있을 수 있기에 등급 별 정량적 값을 주는 방식보다는 자산을 기준으로 보안 요건의 상대적인 비교를 통해 정량화하는 방식이 필요하다. 이에 본 연구에서는 객관적 데이터가 없을 때 다속성을 고려한 정량적 평가 방법 중의 하나인 AHP(analytic hierarchy process)에 기반한 보안 요건의 가중치 값 산출을 제안한다. AHP는 행렬을 이용한 가중치 산정법으로 AHP 과정의 일부 중 이원비교 행렬을 통해 상호 중요도를 수치적으로 도출할 수 있다.

따라서 AHP 기법을 적용한 보안 요건 별 가중치 값을 이용한 위협의 영향도 값 산출은 자산의 특성 및 속성에 따른 위험분석 결과의 정확도를 높여준다. 자산의 보안요건 별 가중치 값 산출의 일반화 방법은 다음과 같다.

*step 1.* 보안요건의 이원비교 행렬화

Table. 3. Example of Ration scale

| Scale | Standard |
|---|---|
| 1 | *Equal* importance |
| 3 | *Weak* importance of one over another (A>B) |
| 5 | *Moderately* importance of one over another (A>B) |
| 7 | *Strong* importance of one over another (A>B) |
| 9 | *Extremely* importance of one over another (A>B) |

자산의 속성 및 특성을 고려하여 기밀성, 무결성, 가용성을 상대비교 비율척도를 정의하여 행의 수와 열의 수가 같은 정방행렬인 이원비교 행렬화 수행

*step 2.* 쌍대비교 행렬의 정규화

쌍대비교행렬 각 열의 원소들을 합하고 각 열의 요소를 해당 열의 합으로 나눈 정규화 행렬 도출(정규화 행렬 각 열의 합

Normalized Matrix :

$$w^N = \begin{pmatrix} w_{11}/\sum_{i=1}^{3} w_{i1} & w_{12}/\sum_{i=1}^{3} w_{i2} & w_{13}/\sum_{i=1}^{3} w_{i3} \\ w_{21}/\sum_{i=1}^{3} w_{i1} & w_{22}/\sum_{i=1}^{3} w_{i2} & w_{23}/\sum_{i=1}^{3} w_{i3} \\ w_{31}/\sum_{i=1}^{3} w_{i1} & w_{23}/\sum_{i=1}^{3} w_{i3} & w_{33}/\sum_{i=1}^{3} w_{i3} \end{pmatrix}$$

Configuration : Pairwise Comparison Matrix

*Let*

$$w = \begin{pmatrix} w_{11} w_{12} w_{13} \\ w_{21} w_{22} w_{23} \\ w_{31} w_{32} w_{33} \end{pmatrix}$$

where

① $w_{ij} = \begin{cases} 1 & if \quad i = j \\ 1/w_{ji} & if \quad i \neq j \end{cases}$

② $w_{12}$ : Relative comparison value of Confidentiality and Integrity

$w_{22}$ : Relative comparison value of Confidentiality and Availability

$w_{23}$ : Relative comparison value of Integrity and Availability

Fig. 4. Concept of Pairwise comparison matrix applying AHP technique

*step 3.* 가중치 행렬 도출
step1에서의 정규화 행렬에서 각 행의 원소들을 합하고 원소의 개수인 3으로 나누어 각 행의 평균을 도출하여 가중치 행렬 도출(가중치 행렬 각 행의 합

Weight Matrix :

$$W=\begin{pmatrix} \sum_{j=1}^{3} w_{1j}^{N} \div 3 \\ \sum_{j=1}^{3} w_{2j}^{N} \div 3 \\ \sum_{j=1}^{3} w_{3j}^{N} \div 3 \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{3} [w_{1j}/\sum_{i=1}^{3} w_{i1}]/3 \\ \sum_{j=1}^{3} [w_{2j}/\sum_{i=1}^{3} w_{i2}]/3 \\ \sum_{j=1}^{3} [w_{3j}/\sum_{i=1}^{3} w_{i3}]/3 \end{pmatrix}$$

Weight Matrix의 각 행의 값은 자산에 대한 보안 요건 별 가중치 값을 의미하고 기밀성의 가중치를 $w_C$, 무결성의 가중치를 $w_I$, 가용성의 가중치를 $w_A$라 하면 다음과 같이 표현할 수 있다.

**Weight of Security Requirements**

$$w_C = \sum_{j=1}^{3} [w_{1j}/\sum_{i=1}^{3} w_{i1}]$$
$$w_I = \sum_{j=1}^{3} [w_{2j}/\sum_{i=1}^{3} w_{i2}]$$
$$w_A = \sum_{j=1}^{3} [w_{3j}/\sum_{i=1}^{3} w_{i3}]$$

### 3.2 위협 요소

사이버 위협은 자산의 손실을 발생시키거나 보안에 해를 끼치는 원인이나 행위, 사건으로 사이버 공격보다 상위단으로 정의하며 행위자에 따라 의도적 위협과 비의도적 위협으로 구분할 수 있다. 비의도적 위협은 지진, 태풍과 같은 자연재해와 기술적 결함, 정전과 같은 환경적 요소를 통해 자연적으로 발생하거나 사람의 조작 미숙, 실수와 같은 내부자의 부적절한 행위로 전파될 수 있으며 의도적 위협은 테러리스트, 산업스파이 및 내부자의 악의적인 공격으로 인해 발생할 수 있다.

정성적 속성의 위협 요소는 정량적 위험도 모델의 Impact factor를 결정짓는 변수로 정량적 값으로 산정하면 위협으로 인한 자산에 미치는 악영향의 정도를 의미하고 악영향의 정도는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)에 미치는 영향의 정도를 다음과 같이 등급으로 나누어 각 등급 별 정량적 값을 통해 산출하고자 한다.

사이버 보안에 대한 많은 데이터를 통한 통계적 수치를 기반으로 등급 별 정량적 값을 도출할 수 없는 경우 평가자의 주관적 판단에 따라 값이 임의로 배분되기에 객관적 수치로 활용하기에 현실적이 어려움이 있다. 이에 본 연구에서는 등급 별 정량적 값에 대한 신뢰성을 높이기 위해 CVSS에서 공격 영향인 Base Score를 산출할 때의 값을 적용하였다[3]. CVSS는 NVD(National vulnerability Database)에서 제공하는 Vulnerability Metrics로 MITRE에서 제공하는 정보를 기반으로 알려진 취약성에 대한 보안 취약성의 중요성, 영향성 등을 평가하여 보안 취약성의 중요성을 평가하는 프레임워크를 제공하며 기본 평가 항목에서 기밀성, 무결성, 가용성에 대한 영향도 수준을 High, Low, None으로 등급화하고 등급 별 정량적 값을 제공하고 있다. CVSS는 방대한 데이터베이스와 오랜 연구를 기반으로한 정량적 값을 제시하고 있으며 취약성 평가 표준으로 활용되기에 주관적으로 임의로 적용한 정량값보다 객관적 신뢰도가 높다고 판단된다. CVSS의 등급 별 정량적 값을 적용한 기밀성, 무결성, 가용성에 미치는 영향을 산출하기 위한 등급 별 기준을 다음 Table 4, 5, 6과 같이 제시한다.

Table 4. Criteria and quantitative values by level of Confidentiality requirement

| Level | Standard | Value |
|---|---|---|
| High | The level to which an information leak directly affects the performance of a critical system or an attacker can read all information | 0.56 |
| Low | Although information leakage does not have a direct impact on the performance of critical functions, it may affect the ability to support critical systems or the level of readability of critical information | 0.22 |
| None | The level at which information leakage does not affect the performance of critical functions and supporting functions | 0 |

Table 5. Criteria and quantitative values by level of Integrity requirement

| Level | Standard | Value |
|---|---|---|
| High | The degree to which information that directly affects the performance of a major system is altered or an attacker can tamper with all information | 0.56 |
| Low | It does not have a direct impact on the performance of critical system functions, but it can affect critical system support functions due to information tampering, or the level at which an attacker can tamper with sensitive information | 0.22 |
| None | The level of information tampering does not affect the performance of the critical system functions and support functions | 0 |

Table 6. Criteria and quantitative values by level of Availability requirement

| Level | Standard | Value |
|---|---|---|
| High | The level of disruption that could directly interfere with the performance of critical system functions or stop the use of all resources affected by the attacker | 0.56 |
| Low | It does not directly interfere with the performance of key system functions, but it can interfere with the support functions of the critical system or prevent attackers from using critical resources | 0.22 |
| None | Levels that do not affect the performance of critical system functions and support functions | 0 |

상기 표를 통해 기밀성, 무결성, 가용성에 미치는 영향성 정도를 수치화하고 정립한 자산의 보안요건별 가중치 값을 적용하면 정량적 위험도 모델에 적용하기 위한 산출식은 다음 그림 5의 과정을 통하여 산출할 수 있다.

Configuration : Impact Factor Function

Impact Value by weight
$= w_C I_C(t_i),\ w_I I_I(t_i),\ w_A I_A(t_i)$

since $0 < w_\mu < 1,\ 0 < I_\mu(t_i) < 1$ ,

Product for Comprehensive impact value
$= (1-w_C I_C(t_i)) \cdot (1-w_I I_I(t_i)) \cdot (1-w_A I_A(t_i))$

The larger the value in the evaluation index, the larger the influence is. Therefore, we have to set Impact Factor Function as

$\Rightarrow 1-(1-w_C I_C(t_i))(1-w_I I_I(t_i))(1-w_A I_A(t_i))$

Fig. 5. Solving Process for Impact Factor Function

Impact Factor per one Threat

$$I(t_i) = 1 - \prod_{\mu}^{C,I,A} (1 - w_\mu I_\mu(t_i))$$

### 3.3 취약성 요소

취약성은 자산에 악영향을 주는 위협의 수단으로 사용되는 자산의 약점으로 정의할 수 있으며 자산의 기술적 결함뿐만 아니라 관리적, 물리적, 구조적인 문제점들도 위협이 유입될 수 있는 통로를 제공하여 취약성으로 분석될 수 있다. 공격행위자 입장에서는 취약성이 많을수록, 자산에 대한 취약한 수준이 높을수록 취약성을 이용한 위협을 가했을 시 성공률은 높아질 것이며 이를 통해 취약성 수준에 대한 정량적 값은 위협 가능성의 확률값과 매칭시킬 수 있다.

정성적 속성의 취약성 요소는 정량적 위험도 모델의 Probability factor를 결정짓는 변수로 정량적 값으로 산정하면 취약성의 그 심각성에 따라 위협의

성공 가능성인 확률적 성공률을 의미하기에 취약성 요소의 정량화는 이를 고려한 취약한 정도를 평가하기 위한 평가 요소와 평가 척도가 필요하다. 또한, 취약성의 고유하고 근본적인 특징, 대응 수준, 부수적 피해 잠재성 등 다양한 각도에서 본 평가 값을 도출하기에 본 연구에서 정립한 정량적 위험도 모델에서 취약성의 정량적 값이 의미하는 위협의 성공 가능성에 대한 값으로는 적절하지 않기에 위협의 성공 가능성에 초점을 둔 취약점 평가 체계 구축이 필요하다. 이에 본 연구에서는 CVSS, CWSS에서의 평가 요소 및 평가 척도를 참조하여 정량적 위험도 모델 산출에 필요한 평가 요소와 평가 척도를 제시한다.

• 접근벡터(Attack Vector : AV)

취약성에 접근할 수 있는 침해 통로에 대한 평가 요소로 취약성 접근 방법이 원거리 일수록 공격자가 취약성에 접근할 수 있는 가능성이 높기에 높은 값을 적용한다.

• 권한 요구도(Privileges Require: PR)

취약성에 접근하기 위한 권한의 요구도에 대한 평가 요소로 접근에 필요한 권한이 높을수록 권한 획득이 어렵기에 높은 값을 적용한다.

• 기술적 난이도(Technical Complexity : TC)

취약성을 이용하는 공격 기법의 난이도에 대한 평가 요소로 공격 기법 개발이 어렵거나 숙련된 공격자에 의해 공격이 가능할수록 높은 값을 적용한다.

• 인증(Authentication : AU)

취약성에 접근하기 위해 필요한 인증의 횟수에 대한 평가 요소로 인증의 강도, 복잡도 등 기술적 요소는 배제하고 필요한 인증의 횟수가 적을수록 높은 값을 적용한다.

Table 7. Criteria and quantitative values by level of Attack Vector

| Level | Standard | Value |
|---|---|---|
| S | Wireless Accessible | 0.9 |
| C | Accessible via an open network | 0.7 |
| H | Accessible through physical or logically separated internal network | 0.5 |
| M | Only accessible directly to the system with the target asset | 0.3 |
| L | Accessible through physical access using specific devices | 0.1 |

Table 8. Criteria and quantitative values by level of Privileges Require

| Level | Standard | Value |
|---|---|---|
| S | No privileges required | 0.9 |
| C | Guest-level privileges required | 0.7 |
| H | User-level privileges required | 0.5 |
| M | Administrator-level privileges required | 0.3 |
| L | developer-level privileges required | 0.1 |

• 사용자 상호작용(User Interaction : UI)

취약성에 접근하거나 이용한 공격을 가할 때 필요한 피공격자의 추가적인 활동 여부에 대한 평가 요소로 예를 들어 이메일 열람, 웹페에지 방문 등 공격 성공을 위해 필요한 행위가 통상적이거나 간단할수록 높은 값을 적용한다.

Table 7, 8, 9, 10, 11에서의 평가척도 별 정량값은 확률값 환산을 고려하여 확률적 해석을 위해 1보다 작은 값 내에서 0부터 0.9까지를 균등하게 배분하여 부여하였다[7] 제시한 평가 요소 별 평가 척도에 따라 취약성 요소의 정량적 값의 산출방법은 다음과 같다.

Table 9. Criteria and quantitative values by level of Technical Complexity

| Level | Standard | Value |
|---|---|---|
| S | Known attack techniques for vulnerabilities | 0.9 |
| C | Vulnerability attack techniques can be developed and easily executed without being an experienced attacker | 0.7 |
| H | Vulnerability attack techniques can be developed and executed by skilled attackers | 0.5 |
| M | It is possible to develop an attack technique against the vulnerability but it is difficult to carry out the attack in practice | 0.3 |
| L | Attack techniques for vulnerabilities can only be developed theoretically | 0.1 |

Table 10. Criteria and quantitative values by level of Authentication

| Level | Standard | Value |
|---|---|---|
| S | No authentication required | 0.9 |
| C | One authentication request | 0.7 |
| H | Require more than one authentication | 0.5 |
| M | Require authentication every time and every time you try | 0.3 |
| L | Require two or more authentication methods | 0.1 |

Table 11. Criteria and quantitative values by level of User Interaction

| Level | Standard | Value |
|---|---|---|
| S | No victim's action is required for successful attack (passive attack) | 0.9 |
| C | In order to succeed in the attack, victims need frequent normal actions (e-mail reading, file viewing, web page visits, etc.) | 0.7 |
| H | To succeed in the attack, the victim's normal behavior (update and upgrade, patch management, etc.) is required. | 0.5 |
| M | For the attack to succeed, the victim needs to be uncommon (such as ignoring security warnings). | 0.3 |
| L | In order to succeed in the attack, the victim must induce or actively cooperate with the attack. | 0.1 |

$$V(v_{ij}) = \text{Value}(AV) + \text{Value}(PR) + \text{Value}(TC) + \text{Value}(AU) + \text{Value}(UI)$$

산출된 취약성 요소의 정량적 값은 값이 낮을수록 취약한 정도의 그 심각성이 높으며 산출된 취약성 값이 최하점일지라도 취약성으로 인한 위협 발생 가능성은 0%라 단정할 수 없음을 고려하면 일반적으로 확률변수의 값이 증가할수록 확률이 감소하는 확률분포에 따라 취약성 값의 확률값 환산을 적용할 수 있다. 본 연구에서는 제시한 평가 척도에 대한 등급별 정량적 값은 취약한 정도가 높을수록 높은 값이 도출됨을 고려하여 적절한 확률분포 모델로 다음의 함수를 제안한다.

$$P(V) = 1 - e^{-\lambda V} \quad (1)$$

일반적으로 알려진 취약성을 이용한 위협의 빈도수가 알려지지 않은 취약성을 이용한 위협보다 더 높을 것이고 정량적 값 도출 시 이에 대한 반영이 필요하다. (1)에서의 $\lambda$는 그래프의 기울기를 결정하는 변수로, $\lambda$값이 높아질수록 확률값이 높아짐에 따라 위협의 성공 가능성을 보다 상세하게 조절할 수 있다. 즉, 알려진 취약성과 알려지지 않은 취약성에 따라 다음과 같이 $\lambda$값을 다르게 적용하면 위협의 빈도수를 반영한 취약성에 대한 위협의 성공률을 도출할 수 있다.

그래프를 통해 확인할 수 있듯이 위협의 성공률은 취약성의 취약한 정도, 위협의 발생빈도를 적용하여 $0 \le P(t_i;v_{ij}) \le 1$의 값을 가지는 확률적 성질의 값으로 도출된다. 예를 들어 알려진 $v_{ij}$의 산출된 값 $V(v_{ij})$이 0이면 위협 성공률 $P(V)$은 0으로 환산되어 이 취약성을 이용한 위협 성공 가능성은 0%로 취약성이 있더라도 위협의 가능성이 없으므로 자산에 영향을 미치지 않기에 취약성에 대한 보안조치를 적용의 필요성 여부를 판단하는 근거 자료로 활용할 수 있다. 본 연구에서의 각 위협과 취약성에 대한 독립성

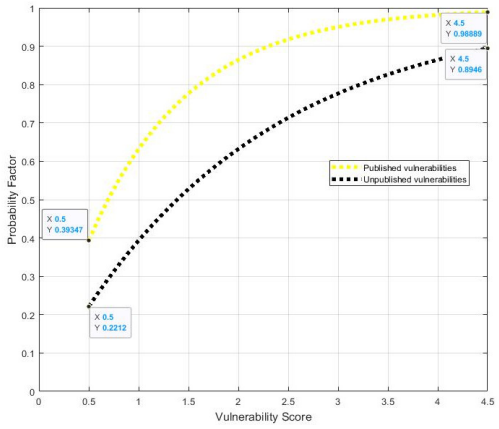


Fig. 6. Graph of Probability Factor according to Vulnerability Score

Table 12. Lambda value according to case

| Case | Value of $\lambda$ |
|---|---|
| **Published vulnerabilities** | 1 |
| **Unpublished vulnerability** | 0.5 |

과 취약성들의 배반적 성격에 의하여 앞선 정량적 위험도 모델에 적용하기 위한 산출 방법은 수학적으로 모델링하여 정리하면 다음과 같이 표현할 수 있다.

**Probability Factor per one Threat**

$$P(t_i;v_{ij}) = 1 - e^{-\lambda V(v_{ij})}$$

where

① $\lambda = \begin{cases} 1 & if \;\; v_{ij} : published \;\; vul. \\ 0.5 & if \;\; v_{ij} : unpublished \;\; vul. \end{cases}$

② $V(v_{ij}) = V(AV) + V(PR) + V(TC) + V(AU) + V(UI)$

## IV. 결 론

정량적 위험도 산출은 표준화된 보안성 평가 결과를 통해 위험 우선순위에 따라 적절한 보안조치를 적용하기 위해 필요한 사이버 보안성 평가 방법으로 원전 특성 및 환경을 고려한 위험도 산출 방법론이 요구되고 있다. 이에 본 논문에서는 기존의 IT 및 ICS 환경에서 제안된 평가 방법 분석을 기반으로 사이버 보안성 평가를 위한 위험도 산출 모델을 제시하고 모델에 적용하기 위한 평가 요소들의 평가 척도를 정립하여 표준화된 평가 결과를 도출할 수 있는 방법을 제시하였다. 사이버 보안성 평가 시 필요한 정성적 속성 요소들의 수준을 AHP 기법을 통한 보안요건 별 가중치, 위협 별 영향도, 취약점 요소 별 점수화를 통한 위협 성공 가능성에 대한 확률값을 산출하여 통계적 데이터를 적용해야 하는 기존 정량적 방법의 한계점을 보완하고 제시한 방법을 통해 자산 별 표준화된 위험도 산출값 비교가 가능하다. 본 연구에서 제시한 위험도 산출 모델은 위험 및 보안조치 우선순위에 판단에 유용할 것으로 기대되나 위협 간의 관계, 취약성 간의 관계 등의 연관성 및 파급성, 보안조치 현황 등 본 논문에서 제한한 조건들을 고려한 고도화된 위험도 산출 모델이 필요하다. 이에 본 연구의 방법론은 사이버 보안성 평가를 정량화하는 프레임워크의 기반으로 활용될 것으로 기대된다.

## References


〔1〕 Korea Communications Commission, "A Study on Development and Methodology of Globally Standardized Cybersecurity Index", Nov, 2010

〔2〕 Joonseon Ahn, Byeong-Mo Chang, Eunyoung Lee, "Quantitative Scoring System on the Importance of Software Vulnerabilities", Journal of The Korea Institute of information Security & Cryptology, 25(4), pp. 921-932, Aug. 2015

〔3〕 Korea Information Security Agency, "Guide for Selecting Automated Risk Analysis Tools", Sep, 2002

〔4〕 Common Vulnerabilities and Exposures (CVE), http://cve.mitre.org

〔5〕 CWE, Common Weakness Scoring System (CWSS), http://cwe.mitre.org/cwss/

〔6〕 FIRST, A Complete Guide to the Common Vulnerability Scoring System Version 3.0 specification(v1.7)

〔7〕 2011 CWE/SANS Top 25 Most Dangerous Software Errors, http://cwe.mitre.org/top25/

〔8〕 Woomyo Lee, Manhyun Chung, Byung-Gil Min, Jungtaek Seo, "Risk Rating Process of Cyber Security Threats in NPP I&C", Journal of The Korea Institute of information Security & Cryptology, 25(3), pp. 639-648, Jun. 2015

〔9〕 Dong-joo Kang, Jong-joo Lee, Young Lee, Im-sop Lee, Huy-kang Kim, "Quantitative Methodology to Assess Cyber Security Risks of SCADA system in Electric Power Industry", Journal of The Korea Institute of information Security & Cryptology, 23(3), pp. 445-457, Jun. 2013

〔10〕 Joong Gil Park. "Information Security : Methodology of Analyze

the Risk Using Method of Determinated Quantity". The KIPS Transactions : Part C, 13(7), pp. 851-858. 2006
〔11〕 Sang Sik Shin, Kil Soo Lee, Heung Gi Cho. "An Objective Method of Risk Assessment Based on Stochastic Modelling". Journal of the Korean society for Quality Management, 41(3), pp. 465-472, 2013
〔12〕 Nam-Kyun Baik, Sung-Min Jung, Tae-Kyung Kim. "A Study on the Risk Evaluation Scheme based on the Probabilistic Analysis". Journal of Security Engineering, 10(2), pp. 141-150, 2013
〔13〕 Donghyeok Lee, Namje Park, 'A Study on Metering Data De-identification Method for Smart Grid Privacy Protection', Journal of the Korea Institute of Information Security & Cryptology 26(6), pp. 1593-1603, Dec, 2016
〔14〕 Namje Park and Namhi Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle", Journal of Sensors (Basel), VOL.16, NO.1, pp. 1-16, Dec. 2015
〔15〕 Donghyeok Lee, Namje Park, Geonwoo Kim, Seunghun Jin, "De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment", Journal of Peer-to-Peer Networking and Applications, Vol.11, No.6, pp. 1299-1308, Nov. 2018

## 〈저자소개〉

김 인 경 (Inkyung Kim) 정회원
2015년 2월: 고려대학교 수학과 석사
2017년 5월~2019년 4월: 한국원자력통제기술원 사이버보안실 전문연구원
2019년 5월~ 현재: 제주대학교 사이버보안인재교육원 책임연구원
〈관심분야〉 사이버보안 평가, 기반시설 보안, 융합기술 보안 등

박 남 제 (Namje Park) 종신회원
2008년 2월: 성균관대학교 컴퓨터공학과 박사
2003년 4월~2008년: 12월:한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월~2009년: 12월:미국 UCLA대학교 공과대학 Post-Doc,WINMEC 연구센터 Staff Researcher
2010년 1월~2010년 8월: 미국 아리조나(ASU) 주립대학교 컴퓨터공학과 연구원
2010년 9월~현재: 제주대학교 초등컴퓨터교육전공,융합정보보안학과 주임교수
〈관심분야〉 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드 등