Journal of the KIMST, Vol. 20, No. 3, pp. 421-430, 2017
ISSN 1598-9127
DOI http://dx.doi.org/10.9766/KIMST.2017.20.3.421

Research Paper 정보 · 통신 부문

사회연결망분석 개념을 적용한 국방정보체계 취약점 분석·평가 모형 연구

장영천*,1) · 강경란1) · 최봉완2)

1) 아주대학교 NCW학과
2) 한남대학교 국방획득·M&S학과

A Study on the Vulnerability Assessment Model for National Defense Intelligence System Using SNA

Youngcheon Jang*,1) · Kyongran Kang1) · Bongwan Choi2)

1) *Department of NCW Engineering, Ajou University, Korea*
2) *Department of Defense Acquisition·M&S, Hannam University, Korea*

(Received 10 January 2017 / Revised 13 March 2017 / Accepted 12 May 2017)

ABSTRACT

In this research, we propose a methodology for assessing security vulnerability of the national defense intelligence system, considering not only target elements but also the interconnection relationship of the whole system. Existing approaches decide the security vulnerability of the whole system by assessing only target elements. However, those approaches have an issue with potentially showing the same outcome for the systems that have identical target elements but the different types of interconnection relationships. We propose a more practical assessment method which takes the interconnection relationship of a whole system into consideration based on the concept of SNA(Social Network Analysis).

Key Words : SNA(사회연결망분석), Vulnerability Assessment(취약점 분석), Natonal Defense Intelligence System(국방정보체계)

1. 서 론

오늘날 IT의 급속한 발전과 함께 국방의 거의 모든 분야에서 각종 정보체계를 사용하고 있으며, 이에 따라 우리 군은 '국방정보체계 취약점 분석·평가' 제도를 도입하여 발전시켜 나아가고 있다.

그러나 기존 '국방정보체계 취약점 분석·평가'는 정부의 '주요정보통신기반시설 취약점 분석·평가' 모형을 국방 분야에 적용하는 수준이다. 또한 평가지표 체계의 항목 분류 그리고 평가 대상체계를 제외한 평가항목에 대한 가중값에 관한 연구를 중심으로 진행

* Corresponding author, E-mail: cham357@gmail.com

되었으며, 평가 대상체계에 대한 연구가 부재하였다. 즉, 각종 무기체계에서 부터 M&S체계 등까지 다양한 국방정보체계에 적용이 가능한 '국방정보체계 취약점 분석·평가 모형'의 연구가 요구된다.

Table 1. Existing researches

연구자	평가지표체계 (평가항목)	가중치 방식	성숙도 평가방법
최광복[1]	9개 부분 22개 분야 120개 항목	분야별, 자산별 중요도 부여	100% 기준 (만점대비 분야별 평가값 총합)
김종혁[2]	3개 부분 13개 분야 41개 항목	적용하지 않음	5단계 등급
KIDA[3]	3개 부분 17개 분야 66개 항목	부분, 분야, 항목별 AHP	5단계 등급 (만점대비 분야별 평가값 총합)
원유환[4]	5개 부분 15개 분야 100여개 항목	평가 지표별 중요도	100% 기준 (만점대비 분야별 평가값 총합)

위의 Table 1은 국방정보체계분야 관련 기존 연구를 정리한 것이다. 이러한 연구들은 국방과 각종 산업 및 공공기관 등 각 분야별로 특성을 고려하여 정보보호 수준평가를 적용하기 위한 연구가 중심이 되어있다. 따라서 사이버위협과 국방정보체계의 자산(요소)을 중심으로 하는 취약점 분석·평가 모형 연구가 필요하며, 이는 사회연결망분석과 같이 정보체계를 대상으로 상대적 중요도를 반영할 수 있는 연구가 되어야 할 것이다.

본 연구에서는 기존 취약점 분석평가 모형을 재정리하고, 사회연결망분석 개념을 적용하여 평가의 대상인 정보체계를 중심으로 중요도를 고려하는 모형을 제안한다. 이를 통해 우리 군의 정보보호 수준측정 및 취약점을 개선시키고, 국방정보체계의 전반적인 정보보호 수준을 향상하는데 기여하고자 한다.

2. 취약점 분석·평가 개념과 방법

2.1 기존 취약점 분석·평가 개념

현재 국방정보체계 취약점 분석·평가는 국방정보보호 관리 업무의 하나이며 관련 업무활동은 Fig. 1과 같이 정리할 수 있다. 조직의 보호관리 측면에서 관리적·인적·물리적 보호/통제 업무 그리고 정보시스템의 구축/운영/관리와 직접적으로 관련된 정보보보시스템 보호 대책 및 보호계획 수립/관리, 사이버위협 탐지/대응, 취약점 분석·평가 업무 등이 해당된다[3].

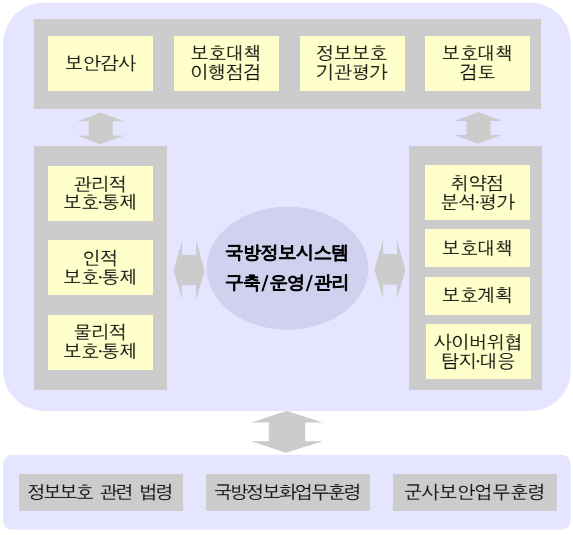

Fig. 1. Major activities of military intelligence security management

국방정보체계는 군에서 운영하고 있는 모든 정보관련 기기 및 체계를 말한다. 취약점 분석·평가는 정보체계의 안정성과 보안성을 약화 또는 훼손시키거나 전자적 침해행위에 악용될 수 있는 체계 구성요소(네트워크, 시스템 등)의 허점을 분석하고 평가하는 업무로, 주로 정보체계 운영단계에서 수행되는 주요 업무이다. 국방정보화업무훈령 제271조(주요기반체계 보호관리), 제304조(취약점 분석·평가)에서 취약점 분석·평가를 규정하고 있다[5].

국방정보체계의 취약점 분석·평가[6]의 점검 항목은 관리적/물리적 분야와 기술적 분야로 나누어지며, 기술적 분야는 네트워크, 서버, 데이터베이스, 웹/응용체계, 정보보호체계, 단말기로 구분되어있다. 총 118개의 세부 항목으로 이루어져 있으며, 중요도에 따라 상·중·

하 중요도(위험도)를 부여하고 있다.

아래 Table 2은 국방정보체계의 취약점 분석·평가 중요도별 점검항목과 점검내용을 정리한 것이다. 세부 항목은 항목별로 관련규정, 취약점 설명, 위험도, 취약점 점검방법, 보호대책 등으로 구성되어 있다.

Table 2. Assessment list

분 야		점검항목 및 중요도				주요 점검 내용
		상	중	하	계	
관리적 /물리적		6	12	0	18	정보보호 지침/조직, 보호구역 관리, 외부 인원 통제, 소방 및 설비 등
기술적	네트워크	9	8	0	17	비인가자에 의한 시스템 접근 취약점, 정보 유출 및 변조 취약점, 서비스 지연 및 마비 가능성 등의 기술적 측면
	서 버	12	17	3	32	
	DB	4	5	0	9	
	웹/응용체계	10	20	2	32	
	정보보호체계	15	5	0	20	
	단말기	7	1	0	8	
계		63	68	5	136	

또한 중요도(위험도)의 판단기준은 취약점으로 인한 침해의 정도에 따라 구분하고 있으며, Table 3와 같다.

Table 3. Importance level of assessment

구 분	내 용
중요도 '상'	해당 취약점 하나만으로 직접적인 침해 요인이 되면, 침해가 발생하면 심각한 피해가 예상되는 상태
중요도 '중'	타 취약점과 연계되거나 현재 상태의 작은 변화시 침해 발생이 가능하며, 침해 발생시 심각한 피해가 예상되는 상태
중요도 '하'	해당 취약점 하나만으로는 직접적인 침해 요인이 되지 않으나, 침해행위에 이용될 수 있는 상태

2.2 취약점 분석·평가 방법

취약점 분석·평가 방법론적 절차를 재구성하면 Fig. 2와 같으며, 기본적으로 평가항목을 기준으로 평가대상을 평가한 후 그 결과를 종합하여 보안수준 등급을 평가하는 과정이다. 보안수준 등급의 기준은 최우수(90점 이상), 우수(80~89점), 보통(70~79점), 미흡(60~69점), 저조(60점 미만) 등 5단계로 되어있다.

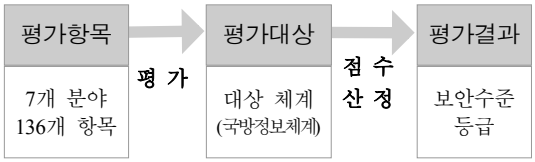

Fig. 2. Assessment process

첫 번째, 평가는 취약점 분석평가 점검항목을 기준으로 작성된 점검표의 「관리적/물리적 분야」 18개와 「기술적 분야」 118개 항목에 대한 평가를 한다. Table 4은 취약점 분석평가 점검표의 사례이다.

Table 4. Sample of assessment table

구분	평가 항목	점수	중요도
네트워크 구성	네트워크의 구성이 적절한가?		상

항목별 평가점수는 0~5점을 부여할 수 있으며, 그 기준은 다음과 같다.

- 5점 : 안전하며, 완벽한 보안통제
- 4점 : 안전한 편이며, 보안통제 보통
- 3점 : 안전도 보통이며, 보안통제 보통
- 2점 : 위험한 편이며, 보안통제 미흡
- 0~1점 : 매우 위험, 보안통제 없음
- N/A : 점검 항목 해당 없음(Not Applicable)

중요도별 점수는 상 : 5점, 중 : 4점, 하 : 3점이다.

두 번째, 취약점 분석평가 점검표에 의해 평가된 항목별 점수 및 중요도를 기준으로 「관리적/물리적 분야」와 「기술적 분야」의 점수를 각각 산정한다. 여기서 「기술적 분야」는 네트워크, 서버, 데이터베이스, 웹/응용체계, 정보보호체계, 단말기 분야의 총칭이다.

먼저 「관리적/물리적 분야」 점수산정은 항목별 평가점수에 중요도 가중치를 산정하여 더한 후 이 값을

백분율로 환산하여 점수를 산정한다.

$$V_M = \frac{\sum_{j=1}^{l}(R_{wj} \times A(j))}{\sum_{j=1}^{l}(R_{wj} \times Max_{credit})} \times 100 \quad (1)$$

V_M : 「관리적/물리적 분야」 평가점수
j : 「관리적/물리적 분야」 평가 항목
R_{wj} : 취약점 항목 j의 중요도 가중치
l : 「관리적/물리적 분야」 취약점 평가 항목 수
$A(j)$: 취약점항목 j에서 취약성 평가결과
Max_{credit} : 항목별 취약점 평가의 최고점수

그리고 「기술적 분야」 점수 산정은 항목별 '자산'의 점수를 산정한 후 이를 모두 합해 백분율로 환산하여 기술적 분야의 점수를 산정한다.

$$V_T = \frac{\sum_{k=1}^{m}\sum_{i=1}^{n}(R_{wk} \times A_k(i))}{\sum_{k=1}^{m}\sum_{i=1}^{n}(R_{wk} \times Max_{credit})} \times 100 \quad (2)$$

V_T : 「기술적 분야」 평가점수
k : 「기술적 분야」 평가 항목
i : 「기술적 분야」 평가 대상 자산
n : 「기술적 분야」 평가 대상 자산 수
m : 「기술적 분야」 취약점 평가 항목 수
$A_k(i)$: 취약점 항목 k의 자산 i에 대한 평가결과
Max_{credit} : 항목별 취약점 평가의 최고점수

최종적으로 「관리적/물리적 분야」 점수와 「기술적 분야」 점수를 합한 취약점 분석·평가 결과의 종합 결과 V는 다음과 같이 산정한다.

$$V = \frac{V_M \times l + V_T \times m}{l + m} \quad (3)$$

V : 취약점 분석·평가 결과
V_M : 「관리적/물리적 분야」 평가점수
V_T : 「기술적 분야」 평가점수
l : 「관리적/물리적 분야」 취약점 평가 항목 수
m : 「기술적 분야」 취약점 평가 항목 수

이렇게 산정된 최종 결과를 기준으로 정보보호수준 등급이 결정된다.

2.3 기존 취약점 분석·평가 방법의 한계

산정방법에 있어서 「관리적/물리적 분야」와 「기술적 분야」의 항목들 간의 동등한 관계로 계산하여 상호영향을 고려하지 못하였다. 그리고 대상 체계내의 구성 자산들 간의 중요도를 반영하지 못하는 단점이 있다.

3. 취약점 분석·평가 모형 제안

3.1 사회연결망분석의 취약점 분석·평가 적용 판단

최근 사회연결망분석(Social Network Analysis)이라는 비교적 새로운 접근과 방법론의 잠재적인 가능성에 대해 관심이 날로 높아지고 있다[7]. 특정한 관계의 패턴을 가지는 인간이나 집단의 집합을 사회적 네트워크(Social Network)라 한다. SNA는 이러한 사회적 네트워크의 구조 또는 형태의 특징을 도출하고, 네트워크를 구성하는 노드들의 관계를 수치화, 통계화 및 그래프화하여 노드들 간의 관계에 대한 계량적이고 과학적인 해석을 가능하게 하는 분석기법이다[8,9]. 여기서 노드(node)는 상호 고유한 속성을 가지는 행위자(actor, agent)를 나타낸다[10].

국방정보체계의 자산 간의 상호영향도를 고려할 때, 이러한 사회연결망분석 개념의 적용은 모든 구성요소(자산)를 동등한 대상으로 평가하는 것이 가능하고 정보체계내에서의 위치에 따른 중요도 반영이 가능하다.

사회연결망분석의 지표 중에서 가장 많이 사용되고 있는 지표는 중심성(centrality)이며, 이 중에서 가장 기본이 되는 지표는 프리만이 제안한 연결정도 중심성, 근접 중심성, 매개 중심성이다. 이러한 중심성을 사이버무기체계와 국방정보체계의 정보보호 측면에서 정리하면 다음과 같다[5].

첫 번째로, 연결정도 중심성(degree centrality)은 한 노드가 얼마나 많은 연결을 가지고 있는지를 측정하는 것으로 얼마나 많은 타 노드에게 영향을 끼칠 수 있는가를 나타낸다. 따라서 사이버무기체계의 공격을 고려할 때, 연결정도 중심성이 높은 노드일수록 높다고 판단할 수 있을 것이다.

두 번째로, 근접 중심성(closeness centrality)은 해당 노드가 얼마나 네트워크의 중앙에 있는지를 표현하는 것이다. 즉, 자신이 가진 자원(정보)을 가장 빠르게 전

체 네트워크에 배포 가능한 정도를 예측할 수 있다. 이것은 사이버무기체계의 공격을 받았을 때 핵심노드의 가치를 판단 가능할 것이다.

세 번째로, 매개 중심성(betweenness centrality)은 한 노드가 다른 노드 사이에 위치하는 정도를 측정하는 것이다. 즉, 이 위치는 정보의 흐름을 통제하는데 큰 영향을 가질 수 있다. 따라서 사이버무기체계의 공격에서 특정 노드를 마비시킬 때 피해가 더 클 수 있다.

이러한 중심성의 특성과 함께 산정 방법, 측정 대상 등을 고려하여 국방정보체계 취약점 분석평가 개선방안에 적용 가능성을 Table 5와 같이 제안한다.

Table 5. Applicability judgment of centrality

구분	연결정도 중심성(C_{Di})	근접 중심성(C_{Ci})	매개 중심성(C_{Bi})
근거	연결정도	연결거리	연결거리
방법	$\frac{\text{직접연결노드수}}{n-1}$	$\frac{n-1}{i\text{의 전체거리}}$	$\sum_{j,k}\frac{g_{jk}^{(i)}}{g_{jk}} \times (j \neq k \neq i, j, i \in N)$
	N : n개 노드의 집합 j,k : 전체 노드쌍에서 노드 i를 제외한 최단 연결거리를 가진 노드 쌍 g_{jk} : 노드 j와 k사이에 존재하는 최단 거리 경로의 수 $g_{jk}^{(i)}$: g_{jk}의 경로 중에서 노드 i를 경유(통과)하는 수		
측정 대상	한 노드가 얼마나 많은 연결을 가지고 있는 정도	한 노드가 네트워크의 중앙에 있는 정도	한 노드가 다른 노드 사이에 위치하는 정도
적용 판단	사이버무기체계가 침입한 노드로부터 확산을 고려할 때 다양한 노드 연결에 따른 중요도 반영 가능	사이버무기체계가 침입한 노드으로부터 목표한 노드까지 거리를 고려할 때 중요도 반영 가능	사이버무기체계가 침입한 노드으로부터 목표한 노드까지 최단거리를 고려할 때 중요도 반영 가능

3.2 SNA 개념을 적용한 모형 개발

SNA 개념 적용을 위한 첫 번째 단계가 SNA의 구성요소와 국방정보체계 취약점 분석·평가와의 관계를 설정하는 것이다.

국방정보체계 취약점 분석·평가 체계는 취약점 평가 목록을 기준으로 「관리적/물리적 분야」와 「기술적 분야」로 구성되어 있다. 이러한 평가 목록은 SNA의 구성요소인 노드와 링크를 구성하기 위해서 Fig. 3과 같이 가상체계와 실체계로 구분한다.

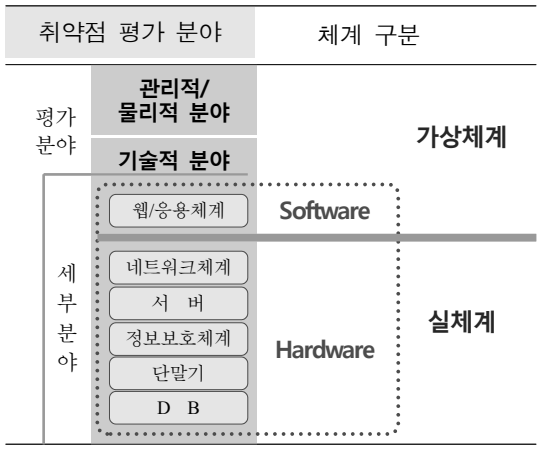

Fig. 3. Assessment list and system

SNA를 적용하기 위해서는 각 개체(자산)들은 링크에 대응되는 사회적 관계인 개체유사성과 영향유사성이라는 속성을 가져야 한다. 국방정보체계 취약점 분석·평가에서 가상체계의 유사성은 평가 항목, 논리적 요소, 평가질문의 흐름으로 정의하며, 실체계의 유사성은 정보체계 자산, 정보교환으로 정의한다.

즉, SNA 개념을 적용하기 위한 국방정보체계 취약점 분석·평가와 SNA 구성요소 정리는 Table 6와 같다.

Table 6. SNA and defense intelligence system

구 분		국방정보체계 취약점 분석평가	
		가상체계	실체계
노 드		평가 분야, 논리적 요소	국방정보체계 자산
링크	개체 유사성	평가 분야, 논리적 요소	정보체계 자산
	영향 유사성	논리적 흐름	정보교환

다음의 Fig. 4는 취약점 평가 분야와 대상에 가상체계와 실체계의 노드와 링크를 적용한 것을 개념적으로 나타낸 것이다.

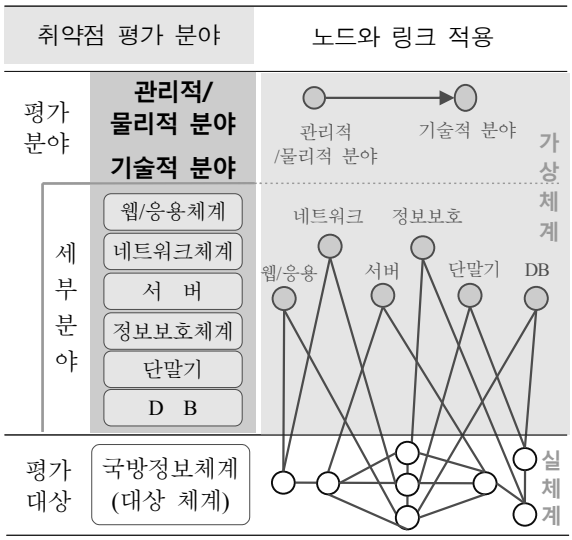

Fig. 4. Application of nods and links

SNA의 노드와 링크 그리고 중심성을 적용하여 수식을 정리하면, SNA 적용한 취약점 분석·평가 결과 (V_{SNA})는 수식 (4)로 정리된다. 여기서 평가점수는 백분율을 사용하기 위해 100을 곱하여 준다. 그리고 SNA 기법 중에서 연결정도 중심성, 근접 중심성, 매개 중심성 등 3가지 중심성들은 각각 특징을 가지고 있으며, 이 특징들을 국방정보체계 취약점 분석·평가에 균형적으로 적용하기 위해 중심성 평균값을 적용한다.

$$V_{SNA} = \frac{V_M \times l + V_{TSNA} \times m}{l + m} \quad (4)$$

V_{SNA} : SNA 적용 취약점 분석·평가 결과

$$V_M = \frac{\sum_{j=1}^{l}(R_{wj} \times A(j))}{\sum_{j=1}^{l}(R_{wj} \times Max_{credit})} \times 100$$

V_{TSNA} : SNA 적용「기술적 분야」평가점수

$$V_{TSNA} = \frac{V_M}{100} \times V_{TC}$$

V_{TC} : SNA 중앙성 적용「기술적 분야」평가점수

$$V_{TC} = \frac{\sum_{k=1}^{m}\sum_{i=1}^{n}(R_{wk} \times A_k(i) \times C_{AVk}(i))}{\sum_{k=1}^{m}\sum_{i=1}^{n}(R_{wk} \times Max_{credit} \times C_{AVk}(i))} \times 100$$

l : 「관리적/물리적 분야」취약점 점검 항목 수
m : 「기술적 분야」취약점 점검 항목 수
k : 「기술적 분야」평가 항목
i : 「기술적 분야」평가 대상 노드
R_{wk} : 취약점 평가 항목 k의 중요도 가중치
n : 「기술적 분야」평가 대상 노드 수
$A_k(i)$: 취약점 평가 항목 k의 노드 i에 대한 평가 결과
$C_{AVk}(i)$: 노드 i의 중심성 평균값

$$C_{AVi} = \frac{C_{Di} + C_{Ci} + C_{Bi}}{3}$$

C_{Di} : 노드 i의 연결정도 중심성
C_{Ci} : 노드 i의 근접 중심성
C_{Bi} : 노드 i의 매개 중심성
Max_{credit} : 항목별 취약점 평가의 최고점수

4. 사례 적용 및 분석

사회연결망분석(SNA) 개념을 적용한 국방정보체계 취약점 분석·평가 사례 적용과 분석을 통해 제안 모형의 효용성을 제시한다. 먼저 적용 사례는 해군00분석모델체계로서 Table 7과 같이 응용/운영체계로 구성되어 있다.

Table 7. Application/operation system

구 분	단말기	엔진서버	DB서버
응용체계	윈도우 7	모의엔진	오라클서버
운영체계	오라클운영	리눅스 5.4	리눅스 5.4

그리고 Fig. 5와 같이 구성되어 있으며, 평가결과 값은 랜덤함수의 임의 값을 사용하고 SNA 소프트웨어는 Pajek 4.0[11,12]을 사용하였다.

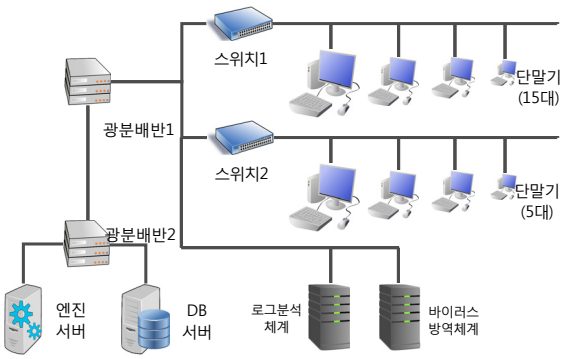

Fig. 5. Concept of 00 analysis M&S system

4.1 해군00분석모델체계 사례 적용

첫 번째 단계로 대상체계의 노드와 링크를 구성한 후 가상체계와 실체계의 노드와 링크로 구성하면 Fig. 6과 같다.

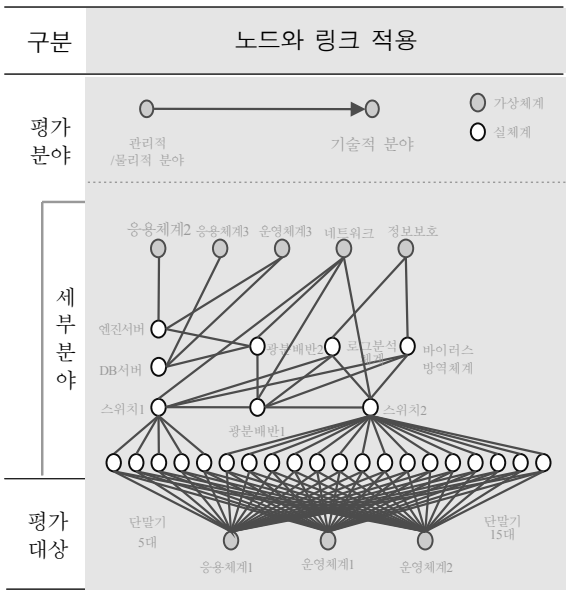

Fig. 6. Nodes and links of 00 M&S system

이렇게 구성된 36개 노드와 101개 링크를 SNA 소프트웨어 Pajek 4.0을 이용하여 가시화 하면 Fig. 7과 같다.

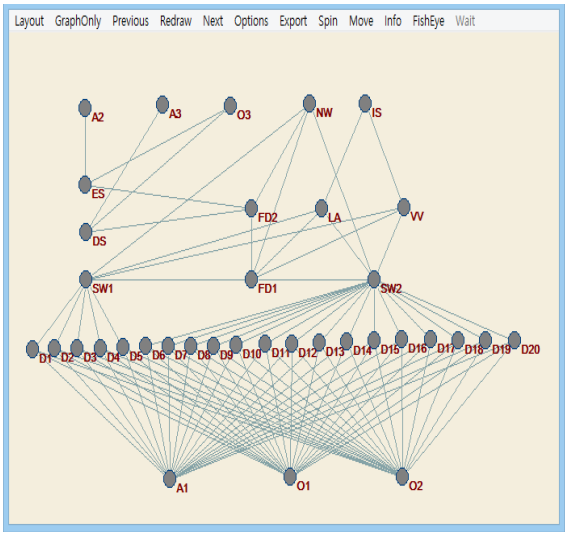

Fig. 7. Visualized nodes and links

먼저「관리적/물리적 분야」취약점 평가 결과는 1~5의 값을 이용하여 Table 8과 같이 생성하였고, 평가결과의 산정은 기존 방식과 동일하다.

Table 8. Results of assessment for the management/physical part

분 야	항 목	중요도	평가결과
관리적/물리적	정보보호시스템 운용	중	4
	… 중 략 …		
	정보시스템 이중화	중	4
	중요도 × 평가 결과 합		286

이러한 기술적 분야의 가상체계 웹/응용체계와 실체계의 노드를 평가한다. 그리고 각 노드별 SNA 중심성의 산정은 SNA 소프트웨어인 Pajek에 입력된 노드와 링크 관계를 각각 연결정도 중심성, 근접 중심성, 매개 중심성 값으로 도출한 후 평균값을 구한다. 이렇게 중심성 평균값을 평가 세부 분야별로 계산의 분자 값이 되는 중요도 × 평가결과 × 중심성 평균값($R_{wk} \times A_k(i) \times C_{AVk}(i)$)과 분모 값인 중요도 × 평가 최고점 × 중심성 평균값($R_{wk} \times Max_{credit} \times C_{AVk}(i)$)을 정리하면 Table 9과 같다.

Table 9. Application of centrality average

구 분		적용 결과	
		$R_{wk} \times A_k(i) \times C_{AVk}(i)$	$R_{wk} \times Max_{credit} \times C_{AVk}(i)$
네트워크	SW1	35.28	59.85
	… 중 략 …		
	FD2	29.90	65.55
… 중 략 …			
D B	DS	19.76	26.00
총 합계	$\sum_{k=1}^{m}\sum_{i=1}^{n}(R_{wk} \times A_k(i) \times C_{AVk}(i))$ = 1,194.39		
	$\sum_{k=1}^{m}\sum_{i=1}^{n}(R_{wk} \times Max_{credit} \times C_{AVk}(i))$ = 1,968.42		

4.2 해군00분석모델체계 사례 적용 결과

Table 10은 기존 취약점분석·평가 모형과 제안 모형을 적용한 결과에 대한 비교이다.

Table 10. Results of the current model and the proposal model

구 분		기존 모형	제안 모형
제한 사항	평가 분야 상호영향 반영	-	$V_{TSNA} = \frac{V_M}{100} \times V_{TC}$
	세부 분야 평가 반영	-	네트워크(4개), 정보보호(6개)
	동종 자산 간의 중요도 반영	-	$C_{AVi} = \frac{C_{Di} + C_{Ci} + C_{Bi}}{3}$ (SNA 중심성)
	체계내 자산별 상대적 중요도 반영	-	
평가 결과	「관리적/물리적 분야」	V_M = 73.30	V_M = 73.30
	「기술적 분야」	V_T = 64.30	V_{TSNA} = 44.48 (V_{TC} = 60.68)
	평가 종합	V = 65.29	V_{SNA} = 47.66

제안 모형은 기존의 모형에서 반영하지 못한 평가 분야 간 상호영향, 세부 분야 평가, 동종 자산 간의 중요도, 체계내 자산별 상대적 중요도 등의 제한 사항들을 반영할 수 있었고, 각 분야별 중요도를 반영한 결과를 도출할 수 있었다.

특히, 평가분야 및 항목 상호영향 관련 세부 평가 결과는 다음과 같았다. 첫 번째, 「관리적/물리적 분야」와 「기술적 분야」의 상호영향 반영은 「기술적 분야」의 평가의 결과(V_{TC})에 「관리적/물리적 분야」의 평가 결과(V_M) 비율을 곱하여 결과를 반영하였다. 즉, 「관리적/물리적 분야」의 평가 결과 73.30 % 수준이므로 「기술적 분야」 평가점수(V_{TSNA}) 60.68의 평가 결과에 반영되어 SNA 적용 「기술적 분야」 평가점수(V_{TSNA})는 44.48로 재산정 되었다. 이것은 「관리적/물리적 분야」의 평가 결과(V_M)가 「기술적 분야」 평가점수(V_{TSNA})에 약 27.7 %(16.20)의 감소영향을 주었다는 것이다. 두 번째, 「기술적 분야」 세부 분야 평가 반영은 총 136개 평가 항목 중에서 네트워크 4개, 정보보호 6개를 식별하여 가상 노드로 별도 구성하고, 중심성 평균값을 반영하여 「기술적 분야」 평가점수(V_{TSNA})를 산정하였다. 현 사례로 제시된 대상 체계가 구성 자산(요소)들이 단순하여 효과성 검증은 어려우나 복잡한 체계에서는 가능할 것이다.

그리고 정보체계 자산(구성요소) 중요도 관련 사항은 다음과 같았다. 첫 번째, 동일한 종류의 자산(체계요소)들이지만 체계내의 역할과 위치가 다른 자산들에 대해 다른 중요도를 반영하였다. 즉, 사례의 세부 분야 중 각각 2개의 자산들로 구성된 네트워크 분야의 스위치와 광분배반에 중심성 평균값을 적용함으로써 각각의 역할과 위치에 따른 중요도를 반영하였다. Table 11은 이러한 스위치와 광분배반의 평과결과를 정리한 것이다.

여기서 「기술적 분야」의 평가 결과가 기존 모형(V_T = 64.30) 보다 제안 모형(V_{TC} = 60.68)이 낮지만, Table 10에서와 같이 스위치와 광분배반의 평가 결과는 기존 모형(V_T)보다 제안 모형(V_{TC})이 스위치는 0.96, 광분배반은 0.25가 높다. 이것은 대상체계 내에서 스위치와 광분배반의 역할과 중요도가 반영되었다고 할 수 있다.

특히, Fig. 8과 같이 중심성 평균값(C_{AVi})의 차등적 반영으로 단말기보다 더 중요하게 고려된 네트워크는 기존 모형보다 높은 결과 값이 나왔다. 그러나 대상체

계 내에서 상대적으로 중요도(중심성)가 낮은 단말기는 제안 모형에서 더 낮은 결과 값이 나왔다.

Table 11. SNA conditions and the results of assessment of the SW and the FDF

구 분			스위치		광분배반	
			SW1	SW2	FD1	FD2
SNA 조건	직접 연결노드 수		9개	19개	6개	4개
	중심성값	연결정도	0.09	0.19	0.06	0.04
		근접 중심성	0.42	0.55	0.50	0.38
		매개 중심성	0.11	0.37	0.16	0.26
		평균값(C_{AVi})	0.21	0.37	0.24	0.23
평가 결과	∑(중요도×평가값)		168	188	197	130
	기존 모형(V_T)		62.46		57.37	
	제안 모형(V_{TC})		63.42		57.62	

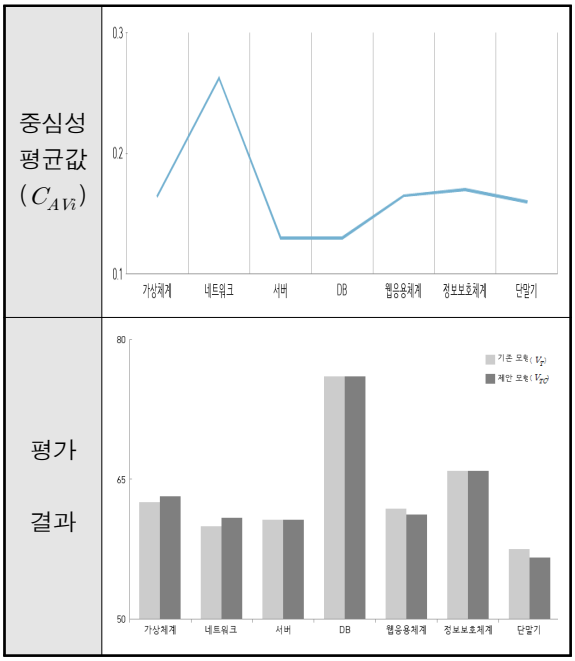

Fig. 8. Centrality averages and assessment results

5. 결 론

본 연구에서는 국내·외 정보보호관리·평가체계와 관련된 기존 연구들을 정리하고, 기존의 국방 분야의 국방정보체계 취약점 분석·평가에 대한 제한 사항을 도출하여 개선된 수행 절차 모형을 제시하였다. 그리고 기존 모형과 본 연구에서 제시한 모형을 국방 M&S체계의 해군00분석모델체계 사례에 적용을 통해 기존 모형의 제한 사항 개선 가능성을 확인하였다.

본 연구에서 제시한 국방정보체계 취약점 분석·평가 모형은 다음과 같은 장점 및 특징들을 가진다. 첫 번째, 평가 분야인 「관리적/물리적 분야」와 「기술적 분야」 사이의 상호영향을 반영하였다. 두 번째, 「기술적 분야」의 세부 분야 평가에서 대상을 중심으로 구분하였다. 세 번째, 「기술적 분야」의 평가 대상 자산 중에서 동종의 자산에 대한 실질적 중요도를 반영하였다. 네 번째, 사이버위협의 특성을 고려하여 대상체계의 상대적 중요성을 반영하였다.

앞으로 본 연구에서 제안한 모형을 기반으로, 각 종 국방정보체계별로 세부 분야 평가 내용을 지속적으로 분류하여야 한다. 그리고 사이버위협의 특성을 고려하여 양방향 링크를 이용한 중요도를 도출하였으나, 대상체계내 자산(요소) 사이의 상호영향까지 고려한 링크에 대한 연구가 필요할 것이다. 즉, 단방향 링크에 대한 추가 연구를 통해서 군의 모든 국방정보체계에 대한 취약점 분석·평가가 가능할 수 있도록 발전시켜 나아가야할 것이다.

References

[1] Choi Kwangbok, “Research on the Defense Information Security Management System in Preparation for Cyber Warfare,” Suwon University, 2012.

[2] Kim Jonghyuok, “A Study on the Development of the Method of Defense Information Security Management System and Assessment,” Chungnam National Unoversity, 2013.

[3] Korea Institute for Defense Analyses, “A Study for Standard Assessment System of Defense Information Security,” 2012.

[4] Won youhwan, “A Study on Evaluation Criteria of Defense Information Security Management System,”

Konkuk Univesity, 2017.
[5] Ministry of National Defense, “Instruction of Informationalization Of National Defense,” 2015.
[6] Ministry of National Defense, Practice Guidelines for Vulnerability Assessment of Defense Intelligence Systems, 2015.
[7] John Scott, “Social Network Analysis A Handbook,” SAGE Publications of London, 2000.
[8] Jung Chiyoung, A Study on Synergy Effectiveness Measurement Model for NCW using SNA, Korea National Defense University Press, 2012.
[9] Jang Seonhi, Jang Seikhyen, “A Framework for Visualizing Social Network Influence,” Journal of Multimedia Information System, Vol. 12, No. 1, 2009.
[10] Lee Susang, “Network Analysis Methodology,” Pusan National University of Institute for Social Science Research, 2012.
[11] de Nooy, Wouter, Mrvar, Andrej Batagelj, Vladimir, “Exploratory Social Network Analysis with Pajek,” Cambridge University Press, 2011.
[12] http://mrvar.fdv.uni-lj.si/pajek/