KIPS Tr. Comp. and Comm. Sys.
Vol.3, No.8 pp.271~276 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2014.3.8.271

An Study on the Impact of N/A Check Item on the Security Level Result through Empirical Verification

Lee Jun ho[†] · Sung Kyung Sang[††] · Oh Hea Seok[†††]

ABSTRACT

This study analyzed that N/A check items affect the results of the security level degree, when performing vulnerability analysis · evaluation. For this, we were used vulnerability analysis · evaluation range, check items and quantitative calculation method. Furthermore, were applied grade and weight for the importance of the items. In addition, because technology develop rapidly, the institution is always exposed risk. therefore, this study was carried out empirical analysis by applying RAL(Risk Acceptabel Level). According to the analyzed result N/A check items factors affecting the level of security has been proven. In other words, this study found that we shall exclude inspection items irrelevant to the institution characteristics, when perform vulnerability analysis · evaluation. In this study suggested that security level evaluation shall performed, after that exclude items irrelevant to the institution characteristics based on empirical verification. And also, it proposed that model research is required for establish check items for which analysis-evaluate vulnerability based on empirical verification.

Keywords : Vulnerability Analysis · Evaluation, Empirical Verification, Security Level, Check Item, Quantitative Calculation Method

실증검증을 통한 N/A 점검항목이 보안 수준 결과에 미치는 영향에 관한 연구

이 준 호[†] · 성 경 상[††] · 오 해 석[†††]

요 약

본 연구는 취약점 분석 · 평가 수행 시 N/A 점검항목이 보안 수준 결과에 미치는 영향 정도를 분석하였다. 이를 위하여, 본 논문에서는 취약점 분석 · 평가 범위 및 점검항목과 정량적 산출 방식을 이용하였으며, 항목의 중요성에 따른 등급과 가중치를 부여하였다. 또한, 주위 환경과 IT 기술 발달로 기관은 항상 위험에 노출되어 있으므로 위험 허용 수준을 적용하여 실증적 분석을 수행하였다. 분석한 결과, N/A 점검항목이 보안 수준에 영향을 미치는 요인으로 증명되었다. 즉, 취약점 분석 · 평가 수행 시 기관 특성상 연계성이 없는 점검항목은 제외시켜야 하는 것을 알 수 있었다. 본 연구에서는 실증검증을 토대로 기관 특성과 연계성을 갖지 않는 항목을 제외한 후 보안 수준 평가를 수행해야 함을 시사하였으며, 기관 특성을 고려한 취약점 분석 · 평가 점검항목 정립 모델 연구가 필요함을 제시하였다.

키워드 : 취약점 분석 · 평가, 실증검증, 보안레벨, 점검항목, 정량적 산출방식

1. 서 론

2003년 1월의 1차 인터넷대란과 2009년 '7·7 DDoS' 공격 사건 그리고 2011년 '3·4 DDoS' 공격 사건 등 사이버 보안 침해사건이 발생하였다. 또한, 주요 방송사(KBS · MBC · YTN)와 금융회사(신한은행 · NH농협은행 · 제주은행) 전산망이 2013년 3월 20일 악성코드에 감염, 총 3만 2,000여 대에 달하는 컴퓨터가 일제히 마비되는 사상 초유의 정보보안 사고가 있었다.

사이버 보안 침해사건은 시간이 지날수록 침해유형 및 피해범위가 확대되고 있다. 특히 침해의 결과가 국민의 재산과 기본권뿐만 아니라 국가안보 전체에 영향을 미치는 것을 알 수 있다.

사이버 보안 침해는 그 빈도가 잦아지고 피해가 확대됨에

† 정 회 원 : ㈜코스콤 인프라본부 차장
†† 정 회 원 : Infosec 컨설팅 사업부 수석연구원
††† 종신회원 : 가천대학교 IT대학 교수
Manuscript Received : January 17, 2014
First Revision : March 11, 2014; Second Revision : July 31, 2014
Accepted : July 31, 2014
* Corresponding Author : Lee Jun ho(jhlee@koscom.co.kr)

도 불구하고 일련의 사이버 보안 침해사고의 대응과정은 국가와 기업이 사이버 환경에 적합한 보안 대응정책을 가지고 있는지 의구심을 갖게 만들었다[1].

이와 같이 사이버 보안 침해사고로 국민들의 불안감이 확산됨에 따라 정부는 금융・통신・에너지 등 국민생활과 밀접한 정보통신기반시설을 안전하게 보호하기 위한 「정보통신기반시설 정보보호 강화방안」을 마련하였다. 정보통신기반시설(정보통신기반보호법 제2조)이란, 안보・행정・국방・치안・금융・통신・운송・에너지 등 관련 전자적 제어・관리시스템 및 정보통신망과 연관된 시설물을 통칭한다.

정부는 소관 주요 정보시스템에 대한 관리・운영 실태 현장점검을 실시하고 정보보호 관리실태 및 문제점을 분석하는 등 정보보호 강화방안을 위한 노력을 지속하고 있다[6][7].

이에 따라, 정부는 최근의 사이버침해 요인을 감안한 취약점 분석 및 평가기준(관리적, 물리적, 기술적)을 마련하고, 중앙행정기관 소관 기반시설에 대해 정보보호 대책 이행여부를 확인하도록 계획하는 등 기반시설에 대한 침해 예방 및 복구체계를 강화하고 있다.

정부는 핵심 시스템을 운영 중인 기관에 대해 전면 실태조사를 실시하여 유통, 물류, 석유・화학, 철강 등 신규 주요 정보통신기반시설 지정을 확대하고 있다[4][5].

현재, 미래창조과학부(미래부)와 안전행정부(안행부)는 동일한 점검 항목으로 정보통신기반시설 취약점 점검을 수행하고 있다. 즉, 수도시설, 철도, 교통, 행정 등 기관별 고유한 특성이 있음에도 불구하고 동일한 중요도 및 점검 기준을 적용하는 등 획일적인 점검 방식을 취하는 데 문제가 있다.

따라서, 본 연구에서는 정부에서 제시 및 적용하고 있는 취약점 평가기준과 점검항목을 분석하고, 기관 특성을 고려하지 않은 항목 및 평가기준을 적용함으로써 발생하는 보안 수준의 불합리함을 고찰하고자 한다.

2. 관련 연구

2.1 주요 정보통신기반시설 취약점 분석・평가 개요

취약점 분석・평가란, 악성코드 유포, 해킹 등 사이버 위협에 대한 주요 정보통신기반시설의 취약점을 종합적으로 분석 및 평가 개선하는 일련의 과정을 말하며, 매년 정기적으로 취약점 분석・평가를 실시하도록 의무화하고 있다. 취약점 분석・평가의 범위는 주요 정보통신기반시설의 세부시설로 정의된 정보시스템, 제어시스템, 의료시스템 등이다.

취약점 분석・평가는 ① 관리적, ② 물리적, ③ 기술적으로 구분하고 있으며, 기본 항목은 3단계(상・중・하)로 중요도를 분리하여 점검한다. 수행 절차는 Fig. 1에서 보는 바와 같이 4단계로 구성되어 있다.

4단계 취약점 평가 수행 시 취약점 분석 결과에 대해 세부내용을 서술하고, 발견된 취약점별 위험등급 표시 및 개선방향 수립을 원칙으로 하고 있다. 즉, 위험등급 '상'은 조기개선, '중', '하'는 중기 또는 장기개선으로 구분하여 개선방향을 수립하도록 권고하고 있다[2].

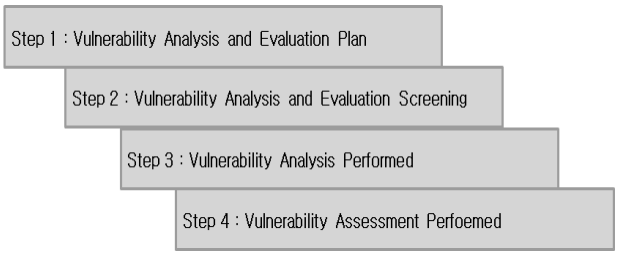

Fig. 1. Procedures Performed : Four Steps Configuration

2.2 취약점 분석・평가 범위 및 점검항목

미래부 및 안행부는 정보통신기반시설 취약점 분석・평가를 위해 Table 1과 같이 관리적・물리적・기술적(모의해킹 포함) 세부 점검항목표를 수립하고 있다. Table 1에서 보는 바

Table 1. Vulnerability Analysis and Evaluation Inspection Items

Division		Check Item No.	Grading (High(Mid・Low))
Managerial Inspection Items	Privacy Policy	8	39(75)
	Information Security organization	4	
	Human Security	6	
	External Party Security	5	
	Asset Classification	5	
	Media Management	5	
	Education and Training	5	
	Access Control	21	
	Operations Management	33	
	Business Continuity	4	
	Incident Response	13	
	Audit	5	
Physical Inspection Items	Access Control	3	7(19)
	Surveillance and Control	8	
	Power Protection	4	
	Environmental Control	11	
Technical Inspection Items	Unix	73	43(30)
	Window	82	45(37)
	Security Equipment	26	16(10)
	Network Equipment	38	14(24)
	Control System	22	16(6)
	PC	20	14(6)
	DB	24	11(13)
	Web	28	28(0)
All		453	233(220)

와 같이 관리부문 114개, 물리 부문 26개 그리고 313개의 기술 부문으로 구성되어 있다. 특히, 기술 부문은 각 시스템의 특성을 고려하여 세부 항목으로 구체화하여 진단하고, 모의해킹을 통한 시스템 취약점을 심층적으로 분석하고 있다[2].

주요 정보통신기반시설 취약점 분석·평가 점검항목은 중요도에 따라 상·중·하로 등급화 하고 있다. 상(High)에 해당하는 점검항목이 미래부 및 안행부가 정한 평가 수준 이하의 평가를 받은 경우 위험 통제를 적용하고 즉시 조치할 수 있도록 권고하고 있다.

2.3 취약점 분석·평가 취약점 산출 개요

취약점 분석 결과에 대해 세부내용을 서술하고 발견된 취약점별 위험등급 표시 및 개선방향 수립을 원칙으로 한다[2][10][11].

취약점 분석·평가 결과에 대해 정량적 점수(백분율)로 산출·관리를 하고 있으며, 관리적·물리적·기술적 취약점 점검결과 점수를 합산하는 방식을 취한다[3].

취약점 점수 산출 방식은 식 (1)을 따른다.

$$\frac{A-B}{A}\times 100 \tag{1}$$

A : 모든 취약점이 식별되었을 경우의 점수합
B : 식별된 취약점들의 점수합

기술적 취약점 점수 산출 방식은 자산별로 취약점 점수를 계산한 후 전체 자산 점수의 평균을 계산하는 방식을 따른다. 기술적 취약점 점검항목에 따라 자산별로 취약점 점수를 계산하고, 자산별 점수를 합산하여 전체 자산 점수의 평균을 계산한다. 기술적 자산별 점수 합산 방식은 식 (2)와 같다.

$$\sum_{n=1}^{N} S_n \div N \tag{2}$$

식 (2)에서 N은 자산의 수를 나타내며, S_n은 자산별 점수를 표현한다. 즉, 자산별 점수의 평균치를 활용하기 위한 것이다. 미래부 및 안행부는 기관의 정보통신기반시설 보안 수준 평가를 위해 관리적·물리적·기술적 취약점 점검항목 수의 비율을 고려한 식 (3) 방식을 이용하고 있다.

$$\frac{A+B+C}{\text{전체취약점 점검항목수}} \tag{3}$$

A : (관리적 취약점 점수 × 관리적 취약점 점검항목수)
B : (물리적 취약점 점수 × 물리적 취약점 점검항목수)
C : (기술적 취약점 점수 × 기술적 취약점 점검항목수)

단, 망 분리의 경우 대다수의 기관에서 망 분리 비율을 적용하지 않는다는 조건이 있고, 기관 특성상 적용이 용이하지 않다. 따라서, 본 연구에서는 망 분리에 관한 취약점 평가 부분은 제외한다.

3. 취약점 점검 모형에 대한 연구

3.1 취약점 점검 모형

본 연구의 연구문제는 “기관의 특성에 따른 취약점 분석·평가 결과에 대한 신뢰도”이다. 연구문제를 검증하기 위해 앞서 살펴본 취약점 분석·평가 결과를 토대로 개념적 연구모형을 Fig. 2와 같이 정립할 수 있다.

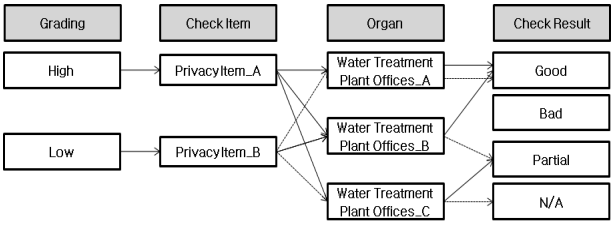

Fig. 2. Vulnerability Analysis Result

Fig. 2를 살펴보면, 중요도가 상(High), 하(Low)에 해당하는 항목의 경우, 동일한 업무를 수행하는 기관임에도 불구하고 상이한 결과를 보인다. 이러한 이유는 Fig. 3에서 보는 바와 같이 각 점검항목의 경우 관리 조직이 다르기 때문이다. 따라서, 관리 조직이 어디에 있느냐에 따라 항목에 따른 평가방식도 달라져야 함을 알 수 있다.

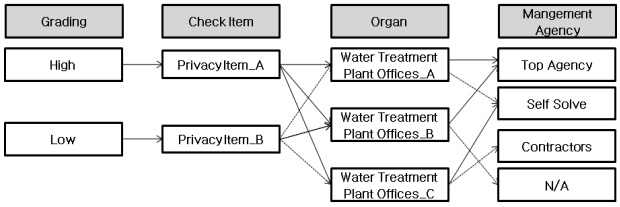

Fig. 3. Management Agency and the Correlation

즉, 상위기관에서 관리하는 점검항목의 경우 운영기관은 전혀 관여하지 않으므로 N/A(Not Applicable) 처리하는 방식을 취하는 것과 같다.

3.2 취약점 점검 모형의 문제점

일반적으로 미래부와 안행부에서 제시하는 취약점 점검 및 분석·평가에 따른 취약점 점검 모형은 Fig. 2와 Fig. 3과 같은 형태를 보인다. 그러나 Fig. 4에서 보는 바와 같이 전혀 다른 성격을 가지는 기관에게도 동일한 항목과 동일한 중요 등급으로 취약점 분석·평가에 적용하고 있다. 기관은

고유의 특성을 고려하여 기반시설물을 운영·관리하므로 점검항목이 적용되는 범위가 상이한 결과를 보이는 것은 당연하다.

그러나, 정수사업소와 도로교통공사, 행정기관의 역할과 임무가 확연히 다름에도 불구하고 중요 등급이 동일하게 적용되고 하다. 이러한 경우 점검 결과에 따른 보안수준에도 영향을 미치게 되므로 정확한 취약점 분석·평가를 수행하였다고 할 수 없다. 또한, Fig. 4에서 보는 바와 같이 중요등급이 상(High) 항목의 경우 도로교통공사에서는 모두 N/A 처리되고 있는데, 이것은 해당 항목이 도로교통공사 환경과는 무관하기 때문으로 해석할 수 있다.

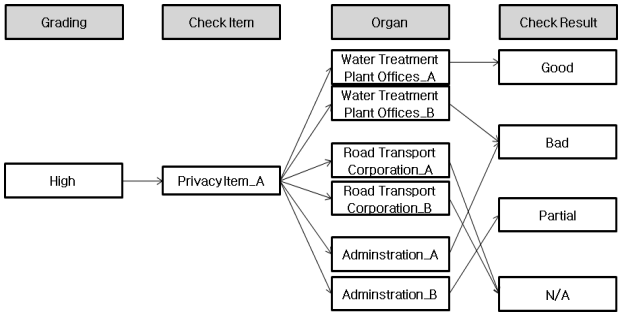

Fig. 4. The relationship between organ and Check Result

따라서, 이러한 환경적 요인이 취약점 분석·평가 결과에도 영향을 미칠 수 있기 때문에, N/A 처리되는 항목의 경우 기관 특성을 고려하여 점검 항목에서 제외하여 취약점 진단을 수행해야 한다.

본 연구에서는 4장 실증 분석을 통해 N/A 점검항목이 취약점 진단 결과에 미치는 영향 정도를 분석하였으며, 취약점 점검 항목과 평가 기준 적용 방안이 필요함을 제시하였다.

4. 실증 검증

본 장에서는 실제 데이터(real data)를 가지고 실증 분석하여 취약점 분석·평가에 대한 객관적 검증 결과를 구하고 본 연구에서 제시하는 내용을 검증하고자 한다.

Table 2는 본 연구 내용을 검증하기 위해 샘플링한 것으로, 실 데이터와 유사한 형태를 가진다[2][7].

다음은 Table 2에 대한 설명이며, 각 지수는 정성적 항목을 정량화하기 위해 부여한 것으로 점검 수행기관마다 상이할 수 있다.

최대 위험 수준의 경우, 항목의 중요성에 따라 상(High)은 9로 하였으며, 중(Mid)은 7, 하(Low)는 5를 적용하였다. 가중치의 경우, 해당 항목에 대해 기관이 잘 진행(Good)하는 경우는 1, 일부분만 진행(Partial)하는 경우 0.5, 안 되는 경우는 0을 적용하였다. 위험 수용 수준의 경우, 주위 환경과 IT 기술 발달로 기관은 항상 위험에 노출되어 있으므로 값을 3으로 고정하여 적용하였다.

Table 2. Sample Data for the Demonstrated Verification

Div.	Item_No.	Grade	Maximum Risk	Risk Exposure
Privacy_ Item	A-1	High	9	3
	A-2	High	N/A	N/A
	A-3	Low	9	9
	A-4	High	9	6
	A-5	Mid	7	5
	A-6	Mid	N/A	N/A
	A-7	Low	5	3
	A-8	Mid	N/A	N/A

Weight - Good : 1, Partial : 0.5, Bad : 0
Grade - High : 3, Mid :2, Low : 1
Acceptable Level of Risk(ALR) : 3

노출 위험도는 해당 항목의 위험 수준 정도를 나타내는 지표로서, 본 연구에서는 식 (4)를 정의하여 노출 위험도를 구하였다.

$$(((Grade-(Grade*Weigt))*2)+ALR \quad (4)$$

노출 위험도는 점검 및 평가 기관마다 달리 해석되어질 수 있으며, 본 연구에서는 앞서 정의한 내용을 토대로 실증 검증을 수행하였다.

Table 3은 현재 운용 중인 취약점 점검 방법과 본 연구에서 제시하는 방법을 비교 분석한 실증 검증 결과 내용이다.

Table 3. Result through the Demonstrate Verification

Div.	A	B
Privacy Policy	67%	56%
Information Security Organization	81%	77%
Human Security	100%	64%
External Party Security	N/A	45%
Asset Classification	81%	81%
Media Management	63%	62%
Education and Training	88%	88%
Access Control	66%	56%
Operations Management	70%	58%
Business Continuity	60%	60%
Incident Response	78%	63%
Audit	92%	92%
Risk Level	74%	62%

Table 3은 취약점 분석·평가를 위해 점검 기관이 사용하는 방식으로, A는 N/A 처리 항목을 포함하여 점검한 결과이며, B는 N/A 처리 항목을 제거하기 위해 보안 수준을 최적의 상태로 하여 위험 수준을 평가한 결과다. 평가 결과 각 위험 수준은 74%와 62%를 보였는데, 이와 같은 결과는 해당 기관의 보안 수준과 직결되어 해석할 수 있다. A 방식의 경우 보안 수준이 26%인 반면 B 방식으로 진단한 경우 38% 결과를 보였다. 즉, 새로운 솔루션이 도입되는 경우 보안 수준이 높아지고 있음을 나타낸다.

기관 특성과 IT 기술 발달로 상시 위험 수준에 노출되어 있다는 것을 적용한다면 새로운 솔루션이 도입되는 순간 위험 발생률은 높아져야 한다. 그러나, 현 상황에서는 오히려 위험 발생률은 낮아지고 보안 수준은 높아지고 있다. 즉, 정확한 보안 수준을 측정하기 위해서는 해당사항이 없는 점검항목의 N/A 처리 대신 기관의 특성을 고려한 취약점 점검항목의 최적화가 필요하다.

5. 결 론

본 연구에서는 실제 데이터 기반의 실증검증을 통해 기관의 취약점 점검 항목 최적화에 대한 중요성을 살펴보았다.

기관의 특성과 업무 역량이 상이함에도 불구하고 점검항목과 중요도를 동일하게 적용하는 것은 기관의 보안 수준을 정확히 평가하는 데 어려움이 따른다.

본 연구에서는 취약점 분석·평가 대상 기관의 특성을 고려하여 연계성을 갖지 않는 항목과 점검항목의 중요도를 바탕으로 보안 수준 평가를 수행해야 함을 시사하였고 추후 정밀한 취약점 분석·평가를 수행하기 위한 점검항목의 최적화에 대한 모델 연구가 필요하다.

Reference

[1] Korea Communication Commission, “A Study on Solutions for the Advancement of Security Legislation”, Dec., 2011.

[2] Ministry of Science, ICT and Future Planning, “The main information and communication infrastructure, vulnerability analysis and ratings”, 2013.

[3] Ministry of Security and Public Administration(MOSPA), “Vulnerability Analysis Score Equation”, 2013.

[4] ICT News, “Cyber Security level improving for National critical infrastructure”, 2008.

[5] Ajunews.com, “Information and communication infrastructure, expanding into 400 to 2017”, 2013.

[6] Kang. J. M. etc. 5, “A Study on National Cyber Capability Assessment Methodology”, The Journal of KIISC, Vol.22, No.5, pp.1039-1055, 2012.

[7] Kim H. G., “A study on National Information Policies”, KISA, 2010.

[8] Kim, Y. J., Lee, J. H., Lim, J. I., “A Study on the Secure Plan of Security in SCADA Systems”, The Journal of KIISC, Vol.19, No.6, pp.145-152, 2009.

[9] Park, J. S., Kim, K. K., Lee, K. J., Jung, J. H., “The main information and communication infrastructure, sophisticated research on information security level evaluation”, The Journal of The NIPA, 2009.

[10] Lee, Y. R., Jo, J. W., “A Study on the Evaluation Consulting Methodology of Important Information Communication Base Facility”, The Journal of the SDPM, Vol.5, No.1, pp.55-68, 2007.

[11] Kang, D.J., Lee, J.J., Lee, Y., Lee, I.S., Kim, H.K., “Quantitative Methodology to Assess Cyber Security Risks of SCADA system in Electric Power Industry”, The Journal of the KIISC, Vol.23, No.3, pp.53-58, 2013.

이 준 호

e-mail : jhlee@koscom.co.kr
1994년 광운대학교 수학과(학사)
1997년 광운대학교 수학과(석사)
1996년~1999년 백두정보기술 선임연구원
2013년 가천대학교 전자계산학과(박사수료)
1999년~현 재 ㈜코스콤 인프라본부 차장
관심분야 : 정보보호, 정보통신, 경영정보

성 경 상

e-mail : actofgod@naver.com
2001년 호원대학교 전자계산학과(공학사)
2003년 숭실대학교 컴퓨터공학과(공학석사)
2009년 경원대학교 컴퓨터공학과(공학박사)
2009년~2011년 CST 컨설팅 사업본부 선임연구원
2011년~2012년 Inzent 전략기획실 과장
2013년~현 재 Infosec 컨설팅 사업부 수석연구원
관심분야 : 전자문서 암호화 알고리즘, 유비쿼터스 정보보안, 인터넷 보안, 센서 네트워크 보안, 사용자 인증 및 프라이버시

오 해 석

e-mail : oh@gachon.ac.kr

1975년 서울대학교 계산통계학과(학사)

1981년 서울대학교 계산통계학과(공학석사)

1989년 서울대학교 계산통계학과(공학박사)

1982년~2003년 숭실대학교 컴퓨터학부 교수/부총장(역임)

2009년~2013년 대통령 IT 특별보좌관 역임

2003년~현 재 가천대학교 IT대학 교수

관심분야 : 멀티미디어, 데이터베이스, 지식경영, 정보통신