

웹 기반 정보 보안 수준 측정 도구 설계 및 구현

성 경*

*동해대학교 컴퓨터공학과

Design and Implementation of a Web-Based Tool for Information Security Levelling

Kyung Sung*

*Dept. of Computer Engineering, Donghae University

요 약

정보가 진전되고 보안사고가 증가됨에 따라 과거의 단순한 통제수단으로는 전체적인 정보보안의 목표를 달성하기가 어려워 종합적인 정보보안 관리체계 구축이 요구되고 있으며, 이에 보다 효율적인 보안 관리를 위한 보안수준 측정에 대한 방법 및 도구개발이 높이 요구되고 있다. 그러나 외국의 연구는 대부분 수준 측정을 위한 항목 구성이 우리 조직의 실정에 맞지 않고 또한 도구 역시 사용의 편의성이나 경제성을 제공하지 못하고 있다. 따라서 본 연구에서는 웹 상에서 조직의 특성을 반영한 4가지의 다중 가중치를 적용하고, 국내 표준을 기초로 보안수준 측정 도구를 제안하고자 한다.

1. 서론

정보화가 진전됨에 따라 종합적인 정보보안 관리체계 구축을 원하는 조직은 적절한 보안수준 측정 과정을 통하여 현재의 보안상태를 파악하고 보안상 취약한 부분과 보강해야 할 부분 등을 식별하여 체계적이고 비용 효과적인 보안 관리체계를 구축이 필수적인 요구 사항이 되었다. 그러나 최근 대부분의 연구는 보안수준 측정 프로세스를 위험관리모델, 위험분석 모델 등에 포함하여 인식하여 왔다. 이로 인해 다음과 같은 문제점이 발생한다. 첫째, 보안 수준측정이 조직의 현재의 종합적인 보안수준을 측정하는 것이 아니라 단순히 대응책 구현상황을 점검하는데 그치고 있다. 둘째, 보안 관리체계구축을 위한 비용 문제이다. 보안 수준측정을 위해서는 보안 수준측정 단계가 포함된 고가의 위험관리

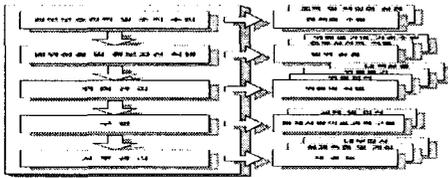
또는 위험분석을 위한 도구를 도입해야하기 때문에 소수의 대규모 조직을 제외한 대다수의 투자비용이 부족한 중소기업 조직에서는 도입에 어려움이 있으며, 전문적인 지식 없이는 수행할 수 없는 것이 현 실정이다.

본 연구를 통한 기대성과는, 첫 번째. 다중가중치 방식을 적용하여 측정자의 주관성을 감소 시킴으로 정확성을 높이고, 두 번째는 측정결과를 관리자가 직관적으로 조직이 처한 상황을 판단할 수 있고, 마지막으로 웹 기반 구현으로 소프트웨어의 구입이 없이 조직의 보안수준을 측정할 수 있다.

2. 관련연구

2.1 보안 관리과정

정보란 정보시스템에 의해 가공, 처리, 저장되는 데이터뿐만 아니라 이들 데이터로부터 유추해 낸 자료로 정의할 수 있으며, 보안은 이러한 유형, 무형의 정보들을 내부 또는 외부의 위협으로부터 보호하는 것[8]으로서 정보시스템의 자료와 이에 관련된 모든 자산에 대해 이들 정보와 자산의 무결성, 기밀성, 가용성을 관리하기 위해 수립되는 통제구조라고 볼 수 있다[그림1].



[그림 1] 보안 관리과정

2.2. 보안수준 측정 관련연구

이 절에서는 보안 수준측정에 관한 기존의 국내의 관련연구를 분석하면, 첫 번째로 ‘정보시스템 안전성 평가도구[5]’는 보안관리체계와 위험분석 방법을 적용한 안전성 평가도구로서 평가를 위한 항목을 작성하는 범위설정, 자산의 가치평가, 취약성평가, 위협평가, 발생 빈도에 따른 가치평가, 자산정보 등을 포함하는 자산평가, 5개 항목의 ISMS 요구사항평가 및 11개 항목의 세부통제사항과 취약성평가방법을 이용한 보안 평가, 자산의 근본적인 약점을 파악하고 취약성과의 관계를 분석하는 취약성 분석, 그리고 기관별로 가중치를 차등 적용하였다.

두 번째로 ‘정보보안수준 계량화[6]’는 정보보안 수준을 효과적이고 효율적으로 측정할 수 있는 간편한 지표를 개발하여 계량화하였으며, 전통적인 보안요소인 물리적 보안, 기술적 보안, 관리적 보안과 정보보안 의식/투자/환경 등 4가지 범주를 설정하였다.

세 번째로 영국의 상무성을 주관으로 제정된 ‘BS7799[1]’은 10개의 주요 분야로 나뉘어진 127개의 통제 항목으로 구성되어 현재 사용되고 있는 최선의 정보보안 실무들로 구성된 종합적

인 보안 통제 목록을 제공하고, 또한 ISMS 구축방안을 제시하며, 정보보안 정책의 ISMS범위 정의, 위협평가 수행, 위협관리, 통제목적과 구현되는 통제 선택, 정보보안 정책의 문서화 등 여섯 단계로 구성된다.

네 번째로, ‘CRAMM(CCTA Risk Analysis and Management Model)[3]’은 영국의 표준화 기관(CCTA)에서 정부기관의 정보시스템 위험관리를 위한 전통적 위험관리 모형을 기초로 개발된 소프트웨어로, 1단계는 위험가능성이 있는 자산에 대하여 더욱 상세한 검토를 수행하는데 목적을 두고 있고, 2단계는 시스템의 위협과 취약성을 조사하며, 3단계는 보안대책의 선택을 중심으로 위험관리 과정을 구성하고 있다.

2.3. 퍼지척도의 개념

퍼지이론은 1965년 미국 버클리 대학의 Lofti, A. Zadeh[11]에 의해 처음 소개되었으며 일본 및 유럽에서 활발하게 연구되고 응용하고 있는 학문으로 퍼지정도를 측정하는 함수를 퍼지정도 척도(measure of fuzziness)라고 한다.

퍼지정도 척도를 나타내는 함수 f 는 다음과 같이 표현된다[7].

$$f: P(X) \rightarrow R$$

퍼지정도 척도가 가져야할 세 개의 공리는 다음과 같다.

공리1 :

$$f(A) = 0 \text{ if } fA \text{가 보통집합(crispset)이다}$$

공리2 : 단조성(monotonicity)

$$A < B \text{ 이면 } f(A) \leq f(B)$$

공리3 : 퍼지정도(불확실한 정도)가 최대이면, 퍼지정도 척도 $f(A)$ 가 최대가 되어야 한다.

이상의 공리를 바탕으로 퍼지집합 A 의 퍼지정도를 측정할 수 있는 척도 $f(A)$ 를 정의해 보면 다음과 같다.

$$f(A) = - \sum_{x \in X} (\mu_A(x) \log_2 \mu_A(x) + [1 - \mu_A(x)] \log_2 [1 - \mu_A(x)])$$

이 척도 $f(A)$ 값을 다음과 같이 정규화(normalize)하여 $F(A)$ 를 얻을 수 있다.

$$F(A) = \frac{f(A)}{|X|}, \quad |X|: \text{cardinality}$$

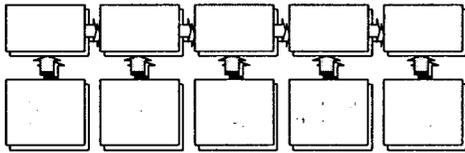
정규화된 척도는 다음과 같은 관계를 갖는다.

$$0 \leq F(A) \leq 1$$

이 척도는 퍼지정도 척도의 공리 1과 공리 2를 만족한다[7].

3. 보안수준 측정 도구 설계

본 연구에서는 기본적으로 보안 관리기준에서 제시된 프레임워크를 따르면서 다중 가중치(조직 특성별, 업무프로세스별, 자산별, 항목별)를 부여하여 세밀하고 정확한 보안 수준을 측정할 수 있는 도구를 설계하였다[그림 2].



[그림 2] 보안수준 측정 프로세스

3.1 기본정보 입력

해당 조직이 속한 업종을 입력하고, 조직의 가용성, 무결성, 기밀성에 대한 가중치를 선택할 수 있게 하였으며, 또한 사용자의 판단에 따라 가중치를 입력하거나 생략할 수도 있게 설계하였다

3.2 업무 프로세스 분류

일반적으로 IT 위험분석 수행 시 자산을 중심으로 분석해 왔으나 이는 대상조직에 잠재하고 있는 위험의 실체를 파악하는데 부족하다 [12]. 위험의 피해는 각각의 IT 자산뿐만 아니라 궁극적으로는 IT자산이 조합되어 수행되는 업무처리에 대해 가해진다[8].

3.3 자산분류 및 평가

자산의 분류는 자산의 유형과 성질을 바탕으로 크게 7개의 대분류로 나누고, 이를 다시 세

분화해서 분류한 뒤 목록을 작성한다[8][12].

3.4 보안수준 측정

전술된 127개의 각 항목마다 보안을 위한 대책 구현을 상, 중상, 중, 중하, 하, 해당 안됨의 6단계로 구분하여 조직의 특성에 따른 가중치를 부여하기 위해 세부통계사항 12가지 항목을 무결성, 기밀성, 가용성에 대해 분류하였다[5].

3.5 퍼지기법을 적용한 측정결과 종합

먼저, 자산 항목별 취득할 수 있는 가용성, 무결성, 기밀성에 대한 최대점수(MVAL: Maximum Value of Asset List)를 구해보면 다음의 식으로 표현할 수 있다.

$$MVAL_{(j)a} = \frac{(TVA_{(j)a} \times (TVL \times (Adda/100)))}{TVa}$$

$TVA_{(j)a}$: j번째 자산의 가용성에 해당하는 항목의 미리 정의된 값
(TVA_j : 무결성, TVA_j : 기밀성)

TVL : 체크리스트에서 기본항목을 제외한 가중치 적용 항목 점수의 합
 $Adda$: 가용성의 가중치 (Add_j : 무결성, Add_j : 기밀성)

→ 상: 50, 중: 30, 하: 10 적용 안함: 각각 33.3

TVa : 체크리스트 전체에 대한 가용성에 해당하는 항목 점수의 합
(TV_j : 무결성, TV_j : 기밀성)

같은 방법으로

$$MVAL_{(j)i} = \frac{(TVA_{(j)i} \times (TVL \times (Addi/100)))}{TVi}$$

$$MVAL_{(j)c} = \frac{(TVA_{(j)c} \times (TVL \times (Addc/100)))}{TVc}$$

를 도출할 수 있다. 또한 자산에 공통적으로 해당하는 점검항목의 기밀성, 무결성, 가용성에 대한 최대값 또한 이러한 공식으로 도출해 낼 수 있다.

$$MVBLa = \frac{(TVBa \times (TVL \times (Adda/100)))}{TVa}$$

$$MVBLi = \frac{(TVBi \times (TVL \times (Addi/100)))}{TVi}$$

$$MVBLc = \frac{(TVBc \times (TVL \times (Addc/100)))}{TVc}$$

가중치가 적용된 각 항목별 점수(VL: Value of Check List apply weight)는 다음의 공식에 의해 구해질 수 있다.

$$VL_{(i)a(i)} = \frac{DVL_{(i)a(i)} \times MVALa}{TVA_{(i)a}}$$

$DVL_{(i)a(i)}$: i번째자산의가용성에해당하는i번째항목의정의된(가중치표)점수

$VLc_{(i)}, VLi_{(i)}, VBa_{(i)}, VBC_{(i)}, VBi_{(i)}$ 또한 같은 방법으로 도출해 낼 수 있다.

가중치가 적용된, 각 자산리스트에 대한 측정 점수(CTVAL: Checked Total Value for each Asset List)는 다음의 공식에 의해 구해질 수 있다.

$$CTVALa = \sum(CVL_{(i)a(i)} \times VL_{(i)a(i)})$$

$CVL_{(i)a(i)}$: i번째자산에대한점검항목중가용성에속하는

i번째항목의점검점수

(상:1, 중상:0.7, 중:0.5, 중하:0.3, 하:0.1)

같은 방법으로

$$CTVALi, CTVALc, CTVBLi, CTVBLc, CTVBLa$$

를 계산해 낼 수 있다.

각 자산에 대한 보안 수준(SLA : Security Level for each Asset)을 측정해 보면,

$$SLA_{(i)} = \left(\frac{CTVAL_{(i)a} + CTVAL_{(i)i} + CTVAL_{(i)c}}{MVAL_{(i)a} + MVAL_{(i)i} + MVAL_{(i)c}} \right) \times 100$$

이 된다. 자산별 적용된 가중치에 대해 퍼지 기법을 적용하기 위해 분류된 프로세스에 속한 자산의 가중치 집합 A는 n개의 자산에 대해,

$$A = \{A_1, A_2, A_3, \dots, A_n\}$$

가 되고, 이 집합에 대해 f(A)는

$$f(A) = - \sum_{A_i \in X} (A_i \log_2 A_i + [1 - A_i] \log_2 [1 - A_i])$$

가 된다. 이 값을 정규화 시키면,

$$F(A) = \frac{f(A)}{n}$$

이 된다. 즉, 실제적으로 적용되는 가중치는 각각의 자산에 대한 가중치 Ai에 대해

$$ADDA_i = A_i - [A_i \times F(A)]$$

가 되고, 프로세스 각각에 대한 보안 수준(SLBP : Security Level for Business Process)을 측정하기 위해 먼저, 공통항목에 대한 보안 수준(SLB : Security Level for Base List)을 측정해 보면,

$$SLB = \left(\frac{CTVBLa + CTVBLi + CTVBLc}{MVBLa + MVBLi + MVBLc} \right) \times 100$$

이 되고,

$$SLBP_{(i)} = \frac{\sum_{j=1}^n (SLA_{(i)} \times ADDA_{(i)}) + (SLB \times ADDB) + \left(-\frac{CBLV}{BLV} \times 100 \right)}{n+2}$$

AddA: 자산에대한가중치(상:1, 중상:0.7, 중:0.5, 중하:0.3, 하:0.1)

AddB: 공통항목에대한가중치(상:1, 중상:0.7, 중:0.5, 중하:0.3, 하:0.1)

CBLV: 기본점검사항의점검값 BLV: 기본점검사항의값의총합

이 된다.

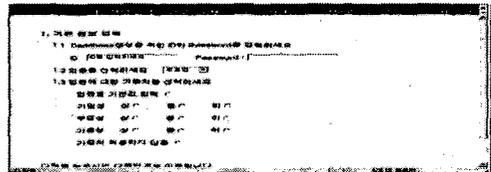
조직 전체에 대한 보안 수준(SLO : Security Level of Organization)은 다음의 식으로 얻을 수 있다.

$$SLO = \frac{\sum_{i=1}^n (SLBP_{(i)} * Add_{BP(i)})}{n}$$

Add_{BP(i)}: i번째업무프로세스의가중치

4. 보안수준 측정 도구 구현

보안수준 측정 도구는 ASP(Active Server Page)와 MS-SQL을 이용하여 Internet Explorer 6.0에서 작동하도록 구현되었다[그림 3].



[그림 3] 보안수준 측정도구

5. 실험 및 결과 분석

5.1 실험환경 및 결과

가중치를 적용하지 않고 전체 항목의 측정값을 '상'으로 가정했을 때와, '중', '하'로 가정했을 때의 결과를 보면 모든 값이 '상'일 때는 90%보안 수준을 만족하고, 모든 값이 '하'일 때는 10%의 보안 수준을 만족하는 결과가 도출되었다. 그리고 모든 값이 '중'일 때에는 보안 수준이 50%로 측정되었다. 이러한 결과로 볼 때, 프로세스와, 자산, 조직의 가중치를 부여하지 않고

측정했을 때의 결과는 구현된 대책의 구현상태에 따라 도출된다고 볼 수 있다.

5.2 실험결과 분석

실질적인 보안수준 측정 도구 실험결과 가중치를 주지 않은 경우 모든 항목에 대해 '상' 수준의 구현이 이루어진 조직에서는 보안의 수준 또한 높게 나오고, 반대의 경우에는 낮게 나왔다. 그러나, 가중치의 개념을 도입함으로써 조직에서의 프로세스 및 자산 등이 차지하는 비중을 보안수준 측정에 반영할 수 있게 되었고, 조직 전체의 보안 수준은 자산별 가중치, 프로세스 가중치, 업종별 가중치 모두에 따라 영향을 받을 수 있다.

6. 결론 및 향후과제

본 연구는 최근 개발된 보안 관리표준의 119가지 항목에 정보보안수준 계량화에서 보안수준 측정지표로 도출된 8가지의 항목을 추가하여 128가지 항목을 자산 및 업종별 가중치 순으로 분류하여 점검항목을 작성하였다. 또한, 웹을 기반으로 구현함으로써 조직관리자가 간단한 체크리스트에 표시함으로써 쉽게 사용할 수 있다.

본 연구의 활용방안으로, 첫째, 보안 관리체계를 구축하기 전에 현 보안수준을 점검하고자 할 때, 둘째, 측정결과를 바탕으로 위험분석 또는 위험관리 방법론을 선택하는데 활용될 수 있으며, 셋째, 보안관련 투자를 위한 우선순위 결정에 활용할 수 있으며, 마지막으로, 보안에 대한 기본적인 지식만으로도 사용할 수 있다.

향후 연구과제로는 첫째, 주관성의 문제를 최소화 할 수 있는 방법이 개발되어야 할 것이며, 둘째, 웹 상에서 운영되기에 조직의 중요 정보의 보안문제 등이 해결되어야 하며, 또한 본 연구의 결과를 기초로 하여 업종별 또는 조직의 특성별로 보안 수준의 차이를 분석하기 위한 지표항목 개발과 적용방법이 개발될 경우 종합적인 보안 관리 체계 연구에 유용할 것이다.

참고문헌

- [1] "BS7799 Part 1 : The Code of Practice", British Standard Institution. Part 2 : The Management Standard".
- [2] "위험분석 도구 기초기술 개발에 관한 연구", 한국 전자통신 연구원 부설 국가보안기술연구소, 2001,
- [3] "CRAMM User Guide", Issue 2.0., U.K. Security Service and CESG, 2001.2.
- [4] 박진섭, 김봉희 "베이스라인 보안정책을 위한 위험분석 체크리스트", Journal of the Institute of Industrial Technology(Taejon Univ.) Vol. 8. No. 2 : 23-40, 1997.
- [5] 홍승구, 김 강, 박진섭, "정보시스템 안전성 평가 도구 설계 및 구현" '2002년 한국멀티미디어학회 추계학술발표논문집' 2002. 05. pp.959-964
- [6] 김현수, "보안수준 계량화 연구", 경영정보학 연구 제9권 제4호, p182-201, 1999. 12.
- [7] 이광형, 오길록 "퍼지이론 및 응용 제1권 : 이론" 홍릉과학출판사, 1991.
- [8] "정보보호 관리기준 해설서", 한국 보안 진흥원, 2001. 11.
- [9] "정보보호 관리표준", 한국정보통신기술협회, 2002. 5.
- [10] 김기윤, 김용겸 '정보시스템의 위험관리 - 외국의 위험관리방법과 한국전산원의 위험관리 방법의 비교', 한국 리스크 관리연구 Vol.5, No.0, pp.27-63., 1995,
- [11] L.A Zadeh, "Fuzzy Sets." Information and Control 8, pp. 338-353, 1965
- [12] "취약점 분석, 평가를 위한 자산분석 지침 (안) - 위험산정 및 분석 방법 이론 소개", 한국 보안 진흥원, 2001. 9.
- [13] "전산망 위험분석 전문가시스템 개발", 팬타시큐리티시스템/한국과학기술원.1999