韓國 컴퓨터情報學會 論文誌
第10卷 第4號, 2005. 9.

2005-10-4-4-5

웹 기반 정보보안 수준 측정 도구 설계

성 경*

Web-Based Information Security Leveling Tool

Kyung Sung*

요 약

정보통신기술이 발달함에 따라 보안 사고가 증가로 조직의 효율적인 보안 관리를 위한 보안수준 측정에 대한 방법과 도구개발의 필요성이 요구되고 있다. 그러나 외국의 연구는 대부분 수준 측정을 위한 항목 구성이 우리 조직의 실정에 맞지 않고 또한 도구 역시 사용의 편이성이나 경제성을 제공하지 못하고 있으며, 국내의 연구 또한 보안수준 측정 시 조직의 특성을 적절히 감안하지 못하고 있다. 따라서 본 논문에서는 다중 가중치를 조직의 특성에 따라 가변적으로 적용하고 수준 측정자의 주관성을 감소시키기 위하여 퍼지기법과 비용 한계의 범위 안에서 보안 대책의 수립을 위해 유전 알고리즘을 적용한 효율적인 보안 수준측정 도구를 제안하고자 한다.

Abstract

As the development of information communication technology and thus the growth of security incidents, there has been increasing demand on developing methodologies and tools for measuring the information security level of organizations for the efficient security management. However, most works from foreign countries are not realistic in constructing the checklists, moreover their tools provide neither the ease of use nor the inexpensiveness, and most domestic works are not properly considering the characteristics of the organizations when measuring the information security level. In this study, an efficient information security levelling tool is suggested, which applies the multiple variable weights for security levelling according to the characteristics of organizations and the fuzzy technique to reduce the user's subjectivity and the genetic algorithm to establish the security countermeasure.

▸ Keyword : 정보보안수준(Information Security Leveling Simulator), 퍼지기법(Fuzzy), 위험관리(Risk Management)

• 제1저자 : 성경
• 접수일 : 2005.07.01, 심사완료일 : 2005.08.31
* 목원대학교 컴퓨터교육과 교수

Ⅰ. 서 론

인터넷과 정보통신 기술은 기업 활동 자체에도 근본적인 변화를 가져와 생산, 판매, 유통, 관리, 물류, 마케팅, 홍보 등 모든 기업 활동을 컴퓨터와 인터넷에 의존하여 실시간으로 이루어지고, 정보가 한 곳에 대량으로 저장되어 모든 사람이 네트워크를 통하여 이를 액세스 할 수 있는 기회를 갖게 된다. 이는 정보의 오남용·파괴 행위도 실시간에 대량으로 일어날 수 있음을 의미한다. 정보가 한 곳에 모임으로써 유용성이 커질 수도 있지만, 만일에 위해가 가해졌을 때 그 피해 또한 대단히 클 수밖에 없다. 다시 말해 정보화는 순기능과 함께 역기능을 동반하고 순기능이 클수록 역기능도 그에 비례해서 커질 수 있으며, 때로는 정보에 대한 무단유출 및 파괴, 변조 등과 인가 받지 않은 불법적인 사용자에 의한 정보시스템의 파괴, 개인정보의 유출, 불건전 정보의 유통 등의 역기능 때문에 순기능 자체가 크게 제약을 받을 소지가 있다. 따라서 위험에 노출된 정보자산을 보호할 필요성이 대두되고 있으며, 보안의 개념도 정보화가 진전됨에 따라 데이터보안(data security) 중심의 개념에서, 컴퓨터보안(computer security), 보안(information security)의 개념으로 달라지고 있는 것이다[1]. 이렇게 과거의 단순한 물리적 접근통제와 제도적 안전장치만으로 효과적인 정보보안의 수준을 달성하고자 하는 데에는 한계가 있어, 종합적이고 체계적인 정보보안을 위한 보안관리체계 구축이 요구된다.BS7799[1], BDSS(Bayesian Decision Support System)[2], CRAMM(CCTA Risk Analysis and Management Methodology)[4] 등의 기준과 소프트웨어가 국외 선진국에서 개발되었으나, 이러한 도구들은 사용이 어렵고 분석항목이 우리 실정과 다르기 때문에 널리 이용되지 못하고 있다. 이러한 실정을 감안해 볼 때, 전술한 외국의 방법 및 도구를 그대로 도입하여 사용하는 것은 현실적이지 못하다. 국내의 보안 수준측정 관련 연구로는 정보시스템 안전성 평가도구 개발[6] 및 정보보안수준 계량화[1] 등이 있으나 부족한 실정이다. 예를 들면, 항목별 보안요소에 대해 가용성, 무결성, 기밀성에 대한 가중치를 상, 중, 하 각각 10점, 7점, 4점으로 적용한 단순한 가중치 적용방법을 선택하였고, 또한 자산에 대한 가중치는 설정하였으나, 업무프로세스에 대한 가중치는 설정되어 있지 않다. 그러나 측정결과의 정확도를 높이기 위해서는 가중치를 단순 적용하기보다는 각 항목에 대하여 세부적으로 가중치를 적용할 필요가 있다.

따라서, 본 연구에서는 각 조직의 보안 수준측정을 위한 가중치를 조직의 특성을 감안한 조직별 가중치, 업무프로세스별 가중치, 프로세스 소속자산에 대한 가중치 및 점검항목별 가중치의 4가지 다중 가중치를 부여하고, 수준 측정 시 나타나는 수준측정자의 주관성을 감소시키기 위해 1972년 일본 동경공업대학의 Sugeno 교수[7]에 의해 제안된 퍼지척도를 적용하여 보다 정확하게 조직의 보안 수준을 측정할 수 있는 도구를 제안하고자 한다.

본 논문의 구성은, 2장에서는 시스템 설계에 필요한 관련연구를 살펴본 후 3장에서는 정보보안 수준 측정 도구 설계 및 구현에 대하여 논의한 후 4장에서는 실제 구현된 측정 도구에 대한 실험결과를 분석하고, 끝으로 5장에서 결론 및 향후 연구방향을 제시한다.

Ⅱ. 관련 연구

2.1. 정보보호 관리과정

한국정보보호진흥원에서 발표한 '정보보호 관리기준 해설서[8]'에 따르면 정보보호관리과정은 (그림 1)과 같이 5과정 14개 항목으로 이루어져 있으며, 각 과정에서 세부지침을 작성하여 조직이 정보보호관리의 목표에 도달할 수 있도록 계획한다.

효율적인 정보보호정책을 위해서 조직의 각 단계 및 사업 단위 또는 부서별로 정의하여 각각의 조직 수준과 사업 단위별로 다양한 목표, 전략, 정책을 수립하여야 한다. 정보보호조직은 적합한 정보보호정책을 계획, 구현, 승인, 감독할 수 있는 조직 체계를 수립하여 구성원의 역할과 책임 및 권한을 명확히 규정하여 모든 직원이 이를 이해하도록 한다. 정보보안 관리체계의 범위 설정은 한 조직에서 중요하다고 판단되는 요소를 포함해야 하며, 조직은 자산식별을 통하여 자산을 파악하고, 자산의 가치 및 중요도를 산출하며, 정보자산과 업무처리와의 관계도 알아낼 수 있다. 자산평가 과정은 크게 자산 조사와 자산가치 산정의 2가지로 나눌 수

있으며, 자산조사 과정에서는 조사할 자산의 범위를 설정하고, 자산목록을 작성한다. 자산가치 산정 과정에서는 자산을 정량적 또는 정성적으로 산출하는 기준과 절차를 정의한다.

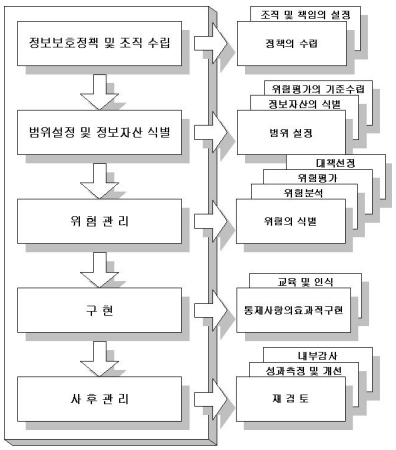

그림 1. 정보보호 관리과정
Fig 1. Information Security Management Process

위험관리는 크게 위험분석, 위험평가, 대책설정 3가지의 과정으로 구분되며, 위험관리 절차는 (그림 2)와 같다.

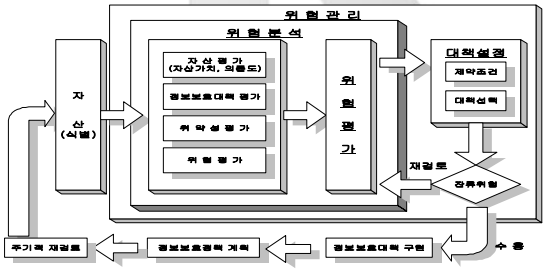

그림 2. 위험관리 절차
Fig 2. Risk Management Process

정보보호에 대한 위험으로부터 정보자산을 보호하기 위해 선택된 통제사항은 적절한 관리 조치와 우선순위에 따라 구현되어야 한다. IT 보안 계획이 일단 완료되면 대책 실행 및 시험을 하여 보안 준수를 점검하고 사후관리를 하여야 한다. 사후관리에는 정보보호관리체계의 재검토, 정보보호관리체계의 모니터링 및 개선, 내부감사가 포함된다.

2.2. BS7799

BS7799[2]는 영국에서 상무성을 주관으로 "정보보안관리 실무규범(A Code of Practice for Informarmation Security Management)"이라는 제목 하에 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용하도록 1995년에 처음 제정되었고, 1999년 10월에 ISO표준으로 제안되어 ISO/IEC DIS 17799-1로 제정된 정보보안 관리체계 구축을 위한 지침서이다. BS7799는 두 부분으로 구성되는데, 제1부는 표준적인 실무지침으로 조직이 정보보안 통제를 구현하는데 기반이 되는 10개의 주요 분야로 나누어진 127개의 통제항목으로 구성되어, 종합적인 보안통제 목록을 제시하고, 제2부는 6단계로 구성된 정보보안 관리시스템(Information Security Management System : ISMS)을 어떻게 구성하는지를 보여주는가에 대한 표준적인 명세이다.

이 프로세스에서는 1단계에서는 모든 정보 자산과 조직의 가치를 분석하고, 정책을 고안하도록 한다. 2단계에서는 관리 대상의 범위를 정의한다. 3단계에서는 가치를 상실하는데 따른 위험을 분석하며, 그 위험을 어떻게 관리할지를 결정한다. 4단계에서는 보안대책을 선정한다. 그러나 BS7799의 목록은 완전한 것이 아니기에, 필요에 따라 추가적인 보안대책이 포함될 수 있다. BS7799가 국내의 실정에 맞지 않기 때문[5]에 2002년 5월 한국정보통신기술협회에서 '정보보호 관리표준[8]'을 제정하였으며, 국내 실정에 맞게 12개의 분야에 119개의 세부통제항목으로 구성하였다. 따라서 본 연구는 '정보보호 관리표준'의 119개의 세부통제 항목과 정보보안수준 계량화 연구에서 중요한 지표로 측정된[1] 'CEO의 의지 및 마인드', '임원·부서장의 의지 및 마인드', '직원의 의지 및 마인드', '정보보안 관련투자' 등의 세부점검사항 8개 항목을 종합하여 총 127항목으로 설정하였다.

2.3 퍼지 기법

퍼지이론은 1965년 미국 버클리 대학의 Lofti, A. Zadeh [9]에 의해 처음 소개되었으며 일본 및 유럽에서 활발하게 연구되고 응용하고 있는 학문이다. 퍼지집합으로 나타난 불확실성의 정도를 퍼지정도(fuzziness)라고 하고, 이 퍼지정도를 측정하는 함수를 퍼지정도 척도(measure of fuzziness)라고 한다. 퍼지정도 척도를 나타내는 함수 f는 다음과 같이 표현된다[10]

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

이 때, P(x)는 전체집합 X의 모든 부분집합을 모은 멱집합(power set)이다.

퍼지정도 척도가 가져야할 세 개의 공리는 다음과 같다.

[공리 1]

$f(A) = 0$ if fA가보통집합($crispset$)이다

[공리 2] 단조성(monotonicity)

$$A < B\text{이면} f(A) \leq f(B)$$

두 개의 퍼지집합 A,B에서 A가 B보다 불확실성이 적다면, f(A)가 f(B)보다 작아야 한다.

[공리 3] 퍼지정도(불확실한 정도)가 최대이면, 퍼지정도 척도 f(A)가 최대가 되어야 한다.

이상의 공리를 바탕으로 퍼지집합 A의 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.

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

정규화된 척도는 다음과 같은 관계를 갖는다.

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

이 척도는 퍼지정도 척도의 공리 1과 공리 2를 만족한다[7].

본 연구에서는 이러한 퍼지정도의 척도를 적용하여 불확실한 판단자의 주관성을 줄이고자 시도하였다. 전체집합 X를 각각의 자산에 대한 가중치 또는 프로세스에 대한 가중치의 집합으로 보고, 사용자가 부여한 가중치를 집합X 내의 퍼지집합 A로 보기로 한다. 그러면, 부여 가능한 가중치의 집합 X에 대해, 자산에 대한 가중치집합 A는 집합 X 의 멱집합이 되고, 집합 A의 원소들을 살펴보면, 0.1 ~ 0.9까지의 값들을 갖는다. 이 값들은 절대적인 값이 아닌, 사용자의 주관에 의해 판단된 값이므로 퍼지집합이고, 일반적으로 조직에 속한 어떠한 자산, 프로세스는 그것의 중요도가 아주 큰 경우와 아주 작은 경우는 직관적으로 판단할 수 있다.

따라서 0.1이나 0.9의 경우에는 불확실성이 0.3, 0.5, 0.7의 경우에 비해 상대적으로 적다고 볼 수 있다. 따라서 이 집합은 퍼지정도 척도의 공리2를 만족한다. 공리 1에 대해 만약 집합 A를 보통집합으로 본다면, 집합 A의 원소들은 두 가지의 상태로 나타낼 수 있다. 즉, 중요하다(1)와 중요하지 않다(0)로 구분할 수 있는데, 이 경우 퍼지정도 척도를 도출해 보면 0이 된다.

또한 공리 3에 대해, 집합 A에서 가중치가 0.5인 경우 퍼지정도가 최대라 말할 수 있고, 가중치가 0.1 또는 0.9인 경우 퍼지정도가 최소라고 말할 수 있다. 이 두 경우에 f(A)를 계산해 보면, 0.5인 경우 1이 도출되고, 0.1 또는 0.9인 경우 0에 가까운 값이 도출된다. 따라서 공리 3도 만족한다. 결과적으로, 집합 A에 대한 퍼지정도 척도는 퍼지정도 척도가 가져야할 세 개의 공리를 만족하므로 이러한 이론을 수준측정시에 수준측정 결과의 정확성을 보다 더 높이기 위해 사용할 수 있다.

2.4 유전 알고리즘

유전 알고리즘은 1975년 Holland의 논문 'Adaptation in Natural and Artficial System'에서 처음 소개되었으며, 그 후 20여년 동안 그 이론과 응용에 관하여 활발한 연구가 이루어져 오고 있다.[12-14]

유전 알고리즘은 유전학과 자연 진화를 흉내낸 적응 탐색법으로 복잡한 최적화 문제를 해결하기 위해서 집단을 사용하고, 모의 진화를 일으켜 이를 점진적으로 개선해 나간다. 집단은 다수의 염색체로 구성되고 염색체는 문제 공간상의 한 점을 대표하게 된다. 최적화하고자 하는 파라미터들을 염색체로 표현하여 주어진 함수의 적합 정도에 따라 적합도를 할당하고, 적합도가 높은 인자의 유전자를 추출하여 교배와 돌연변이 등을 통해 새로운 염색체를 생성해 낸다. 이렇게 만들어진 염색체는 세대를 거치면서 최적화가 이루어지게 된다.

유전 알고리즘의 순서를 간단히 살펴보면, 탐색 공간에서의 임의 점 n개를 선택하여 초기 개체 집단으로 형성한다. 이 개체 집단에서 주어진 문제에 적합한 개체를 확률적으로 선택하여 교차(Crossover)와 돌연변이(Mutation) 등의 유전 연산자(Genetic Operator)를 통해 다음 세대를 만들고 적합도

를 판별하여 그 개체 집단에 찾고자 하는 개체가 있거나 미리 정해 놓은 세대수를 넘으면 탐색을 종료하게 된다.[13].

유전 알고리즘의 기본 연산자는 재생산, 교차, 돌연변이이다. 첫째, 재생산은 주어진 한 세대의 개체 집단에서 다음 세대의 개체 집단을 만들기 위해 중간 단계의 집단을 선정하는 작업이다. 이 중간 단계의 집단을 선정하는 방법에는 적합도가 큰 개체를 선택하게 된다. 이것은 적합도가 큰 개체로부터 더 큰 적합도의 개체가 발생할 가능성이 크다는 가정에 따른다. 재생산을 식으로 나타내면

$$fsum(K) = \sum_{i=0}^{n} fi(K)$$

단$fi(K) = f(Si(K))$는i번째개체의적합도이다. 개체들의 적합도의 합을 계산하고 각 개체의 선택확율을 계산한다.

$$Ps(Si(k)) = Si(k)\text{의적합도/개체들의적합도합} = fi(k)/fsum(k)$$
$$(1 \le i \le N)$$

둘째, 교차는 재생산에 선택된 개체 집단 중 임의의 또는 특정 규칙에 의해 선택된 두개의 개체로부터 서로 정보 교환이 이루어져 새로운 두 개의 개체를 생성하는 것이다. 셋째, 돌연변이는 원치 않는 해로부터 벗어나기 위한 메카니즘이다. 이는 재생산과 교차는 지역해나 사점(dead corner)을 벗어나기 위한 메카니즘이 없는 관계로 유전자의 다양성이 결핍되고 준 최적해(suboptimal solution)나 사점(dead corner)에 빠지게 되는 요인이 되기 때문이다.

III. 정보보안 수준 측정 도구 설계 및 구현

정보보안 수준 측정 도구는 비전문가도 쉽고 간단하게 조직의 정보보안 수준을 측정하고, 정보보안 수준 향상을 위한 의사결정에 도움을 주기 위한 목적으로 설계되었다. 이 도구의 프로세스 구성은 (그림 3)과 같이, 조직의 현 정보보안 수준 측정, 취약한 부분에 대한 세부적인 위험분석, 정보보호 수준을 향상시킬 수 있는 선택 가능한 대응책 제시, 제시된 대응책 목록 중 사용자 선택, 대응책 구현 후 정보보호 수준 측정, 시뮬레이션을 통한 대응책 구현 후의 정보보안 수준 비교 등의 과정으로 구성되어 있다.

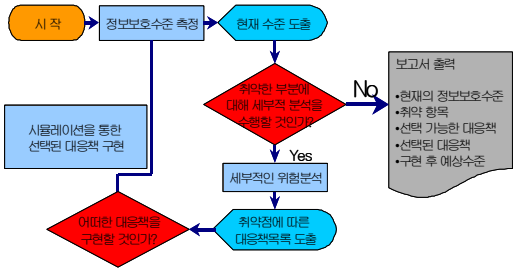

그림 3. ISLS 프로세스 구성
Fig 3. Construction Process of ISLS

본 연구에서는 정보보안 수준 측정 도구의 설계 및 구현을 기본적으로 정보보호 관리 기준에서 제시된 프레임워크를 따르면서 4가지의 다중 가중치를 부여하여 좀더 세밀하고 정확한 정보보안 수준을 측정할 수 있는 도구를 (그림 4)와 같이 설계하였다.

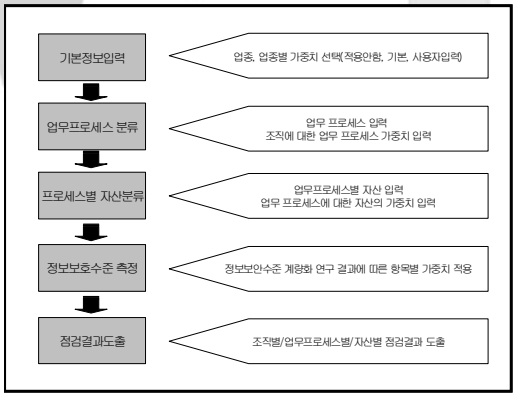

그림 4. 정보보호 수준 측정 프로세스
Fig 4. Process of Information Security Level Measurement

3.1 기본정보 입력

이 단계에서는 조직이 속한 업종을 입력하고, 조직의 가용성, 무결성, 기밀성에 대한 가중치를 선택할수 있게 하였다. 사용자의 판단에 따라 가중치를 입력하지 않을 수도 있고, 입력을 할 수도 있게 설계하였다

3.2 업무프로세스 분류

일반적으로 IT 위험분석 수행 시 자산을 중심으로 분석해 왔으나, 이는 대상조직에 잠재하고 있는 위험의 실체를 파악하는데 부족하다[11]. 위험의 피해는 단위 IT 자산뿐만 아니라 IT 자산이 조합으로 수행되는 업무처리에 가해지는 것이다[8]. 서로 다른 조직의 같은 부분의 업무프로세스라 하더라도 조직의 특성상 중요도가 다를 수가 있다. 이에 각 프로세스가 조직에 차지하는 비중을 상, 중상, 중, 중하, 하와 같이 5개의 등급으로 입력하게 되고, 이러한 등급에 대해 각각 1, 0.7, 0.5, 0.3, 0.1의 가중치가 적용되어 중요한 프로세스에 구현된 대응책은 (그림 5)와 같이 더 높은 가치를 가지게 된다.

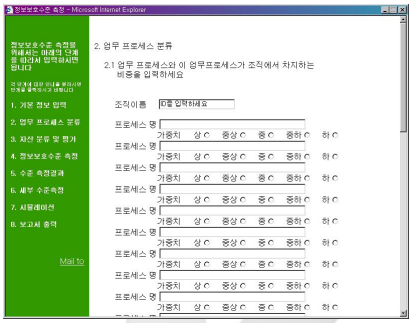

그림 5. 업무 프로세스 입력
Fig 5. Input Screen of Work Process

3.3 자산분류 및 평가

조직의 운영/경영에 있어서 다양한 IT 자산을 식별하고, 분류하는 작업으로, IT 자산에 관한 적절한 관리는 조직의 자산을 적절하게 보호하는데 있어서 필수적인 과정이다. 자산의 분류는 자산의 유형과 성질을 바탕으로 크게 7개의 대분류로 나누고, 이를 다시 세분화해서 분류한 뒤 목록을 (그림 6)과 같다[8][11].

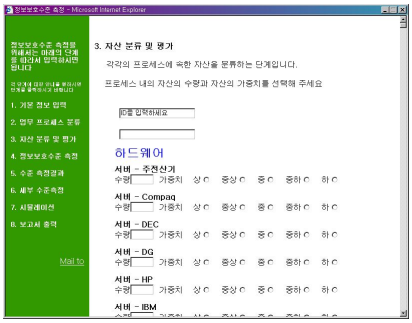

그림 6. 자산 분류 및 가중치 입력
Fig 6. Asset Classfication and Input of Asset Weight

3.4 정보보안 수준 측정

이 단계에서는 '정보보호 관리표준'에 따른 요구사항 평가 및 세부통제 사항과 '정보보안 수준 계량화 연구'를 이용한 체크리스트를 이용하여 평가하게 된다. 각 항목마다 정보보안를 위한 대책 구현을 상, 중상, 중, 중하, 하, 해당 안됨의 6단계로 구분하였다.

- 상: 문항의 조건을 90%이상 만족함
- 중상: 문항의 조건을 70~90% 만족함
- 중: 문항의 조건을 50~70% 만족함
- 중하: 문항의 조건을 30~50% 만족함
- 하: 문항의 조건을 30%이하 만족함
- 해당 안됨: 현 조직에서 해당되지 않음

이와 같이 구분하였고, 각 단계에 대해서 1~0.1까지의 가중치를 실제 계산에서 적용하게 된다.

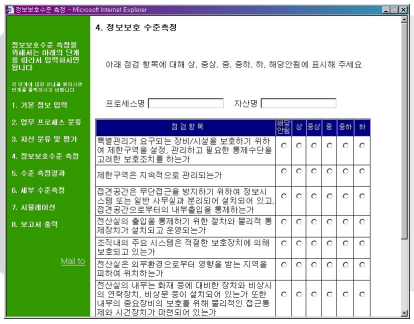

그림 7. 업무 프로세스 입력
Fig 7. Input of Affairs Process

각 항목에 관련된 가중치에 대해서는 '정보보안 수준 계량화 연구[1]' 결과에 따른 가중치를 적용하여 입력자에 의한 상대적 가중치와 항목별 절대 가중치를 모두 고려하여 측정하게 된다.

여기에서 한가지의 가중치를 더 적용하게 되는데, 그것은 조직의 특성에 따른 가중치이다. 조직의 특성에 따른 가중치를 부여하기 위해, 세부통제 사항 11가지 항목을 무결성, 기밀성, 가용성에 대해 분류해 보면 다음과 같다[6].

- 가용성: 인적보안, 물리 및 환경적 보안, 통신 및 운영관리, 시스템 개발보안, 업무 연속성 관리, 침해사고 대응 및 복구

- 무결성 : 정보자산 분류와 통제, 접근통제
- 기밀성 : 아웃소싱 및 제3자 접근, 인적보안, 물리 및 환경적 보호, 접근통제, 요구사항 준수

'정보보안 수준 계량화 연구'의 결과인 가중치 표 또한 가용성, 무결성, 기밀성에 따라 분류해 보면 다음과 같다.

- 가용성 : 물리적 접근통제, 환경위험에 대한 대책, 업무연속성 계획, 감사추적, 응용프로그램보안, 하드웨어 보안, 네트워크 보안, 위험분석, 인사보안, 유지보수 점검
- 무결성 : 물리적 접근통제, 시스템 접근통제, 데이터베이스 보안, 바이러스 보안, 자산파악
- 기밀성 : 물리적 접근통제, 환경위험에 대한 대책, 시스템접근 통제, 데이터베이스 보안, 인사 보안, 정보보안 법/제도/표준

3.5 점검항목 측정치 종합

자산 항목별 취득할 수 있는 가용성, 무결성, 기밀성에 대한 최대 점수(MVAL: Maximum Value of Asset List)를 구해보면,

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

$TVA_{(i)}a$: i번째자산의가용성에해당하는항목의미리정의된값(가중치표)의합

(TVA_i:무결성, TVA_c:기밀성)

TVL:체크리스트에서기본항목을제외한가중치적용항목(가중치표)의 점수의합

$Adda$:가용성의가중치($Addi$:무결성, $Addc$:기밀성)

TVa:체크리스트전체에대한가용성에해당하는항목(가중치표)의점수의합

(TVi:무결성, TVc:기밀성)

같은 방법으로

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

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

를 도출할 수 있다. 또한, 자산에 공통적으로 해당하는 점검 항목의 기밀성, 무결성, 가용성에 대한 최대값 또한 이러한 식으로 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 식에 의해 구해질 수 있다.

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

$DVL_{(j)a_{(i)}}$: j번째자산의가용성에해당하는i번째항목의정의된(가중치표)점수

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

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

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

$CVL_{(j)a_{(i)}}$: j번째자산에대한점검항목중가용성에속하는 i번째항목의점검점수

같은 방법으로

$CTVALi, CTVALc, CTVBLi, CTVBLc, CTVBLa$

를 계산해 낼 수 있다.

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

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

이 되고, 자산별 적용된 가중치에 대해 퍼지기법을 적용하기 위해 분류된 프로세스에 속한 자산의 가중치 집합 A는 n개의 자산에 대해,

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

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. 여기에서 F(A)는 수준 측정자가 측정한 측정값의 불확실한 정도를 나타내므로, 부여된 가중치에서 이 값을 제외시킴으로써 측정값의 불확실성을 줄일 수 있다. 즉, 실제적으로 적용되는 가중치는 각각의 자산에 대한 가중치 Ai에 대해

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

가 되고, 공통 항목에 대한 정보보호 수준(SLB : Security Level for Base List)을 측정해 보면,

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

이 되고,

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

$AddA$: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 정보보호 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

이렇게 도출된 값을 이용하여 본 정보보안 수준 측정 도구는 전체조직의 정보보안 수준, 업무프로세스별 정보보안 수준, 자산별 정보보안 수준 등 3가지의 결과를 (그림 8)과 같이 보여주게 된다.

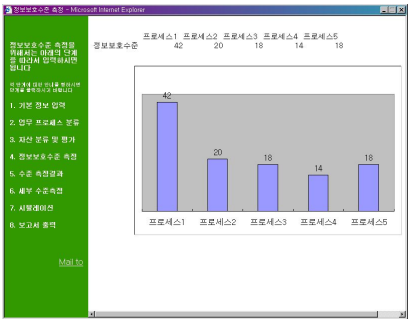

그림 8. 수준측정 결과
Fig 8. Result of Leveling Measurement

3.6 세부 위험 분석

정보보안 수준 측정을 통해 도출된 3가지 결과, 즉, 자산별 정보보호 수준, 프로세스별 정보보호 수준, 조직 전체의 정보보호 수준 가운데, 취약하다고 판단되는 프로세스에 대해, 프로세스에 속한 자산에 대한 세부적인 위험분석을 수행하는데, 먼저 자산에 대해 알려진 취약성 목록을 도출하고, 취약성 목록에 대해 정보보호 수준 측정 시 각 자산에 대해 점검항목에 체크한 값을 기준으로 자산이 취약한 정도를 파악한다. 자산이 취약한 정도를 파악한 다음 각각의 취약성에 대해 위협분석을 수행하게 되는데, 각각의 취약성이 악용되어 침해가 일어났을 경우, 피해의 영향에 따라 위협을 분석하게 된다.

이 때 취약성의 수준은 초기 정보보안 수준 측정 시 각 항목에 대해 선택되었던 자산의 정보보안 수준과 자산의 가중치를 기준으로 평가한다. 위협의 수준은 침해 발생시 피해의 정도가 조직 전체의 업무에 충격이 가해지는 정도에 따라 5등급으로 나누게 된다.

대응책의 우선순위는 대응책 구현비용과 대응책 복구비용에 따라 등급을 나누게 되는데 도출된 대응책 목록에 따라 정보보안 수준 시뮬레이션을 하게 된다.

3.7 시뮬레이션

정보보안 수준 시뮬레이션은 대응책 구현 후의 정보보안 수준을 가시적으로 나타내어, 대응책 구현 전과 후의 정보보안 수준의 향상을 쉽게 판단할 수 있어 대응책 구현을 위한 우선순위 의사결정에 도움을 준다.

취약한 자산에 대한 대응책 우선순위 표에 따라 '구현', '이미 구현되어 있음'으로 선택된 값들을 초기 정보보호 수준 측정단계에서의 사용자 입력치 대신에 입력하게 된다. 이때, '이미 구현되어 있음'에 해당하는 값들은 초기 정보보호 수준 측정 단계에서 사용자가 선택하였던 자산에 대한 세부통제 항목의 점검상태라 볼 수 있고, '구현'으로 선택한 값들은 사용자가 정보보호 수준 향상을 위해 선택한 대응책 수준이라고 볼 수 있다. 이렇게 입력된 값과 취약하지 않은 부분에 대한 초기 사용자 입력치를 종합하여 대응책 구현 후의 향상된 정보보호 수준을 측정하게 된다.

3.8 보고서 출력

도출된 정보보안 수준의 측정값, 취약한 프로세스의 자산에 대한 취약성/위협 목록, 선택 가능한 대응책 목록, 선택된 대응책 목록, 시뮬레이션 후의 향상된 정보보호 수준 측정값 등을 도출하고, 전체 과정을 마치게 된다.

IV. 실험 결과 분석

4.1 실험환경

가중치를 주지 않고, 전체 항목의 측정값을 '상', '중', '하'로 가정했을 때의 결과를 보면, 모든 값이 '상'일 때는 100% 정보보안 수준을 만족하고, 값이 '중'일 때에는 정보보호 수준이 50%로 측정되었고, 값이 '하' 일 때는 10%의 정보보안 수준을 만족하는 결과가 도출되었다. 이러한 결과로 볼 때, 프로세스와 자산, 조직의 가중치를 부여하지 않고 측정했을 때, 결과는 구현된 대책의 상황에 따라 도출된다고 볼 수 있다. 이제 각각의 항목에 대해서는 같은 값을 넣고, 가중치를 부여했을 때와 부여하지 않았을 때, 가중치를 부여하고 퍼지기법을 적용하였을 때의 결과를 비교분석 함으로써, 본 도구의 타당성과 적절성을 보이도록 하겠다. 이 테스트에서의 입력값은 다음과 같다.

- 프로세스 수 : 5개
- 프로세스 당 자산 수 : 17개
- 자산의 가중치 : 1, 0.7, 0.5, 0.3, 0.1
  5가지의 경우
- 프로세스의 가중치 : 0.9. 0.5, 0.1
  3가지의 경우
- 업종별 가중치 : 기밀성 > 무결성 > 가용성의 순서
- 항목별 대책 구현 사항 : 같은 자산에 대하는 가중치를 주었을 때와 주지 않았을 때, 퍼지기법을 도입하였을 때 모두 같은 값

4.2 실험 결과 분석

실질적인 정보보호 수준 측정 도구의 실행결과, 가중치를 주지 않은 경우 모든 항목에 대해 '상' 수준의 구현이 이루어진 조직에서는 정보보호의 수준 또한 높게 나오고, 반대의 경우에는 낮게 나왔다. 그러나, 가중치의 개념을 도입하게 됨으로써, 조직에서의 프로세스, 자산 등이 차지하는 비중을 정보보안 수준 측정에 반영할 수 있게 되었고, 퍼지기법을 적용함으로써 판단자의 주관성을 줄일 수 있는 방안을 제시하였다.

표 1. 가중치와 퍼지기법 도입에 따른 결과
Tab 1. Result According to Weight, Fuzzy

	프로세스 1	프로세스 2	프로세스 3	프로세스 4	프로세스 5
가중치 부여않음	45	45	45	45	45
가중치 부여	43	36	30	24	18
퍼지기법 도입	42	20	18	14	18

본 연구의 실험 결과, 다중가중치와 퍼지기법을 도입함으로써 조직의 정보보안 수준을 좀 더 정확하게 측정하고, 분석할 수 있다는 것을 볼 수 있다.

V. 결론 및 향후과제

정보보호 수준을 도출한 결과 자산에 대한 정보보안 수준이 독립적으로는 완벽하게 도출되었을지라도 그 자산이 프로세스에서 차지하는 비중과 그 자산이 소속된 프로세스가 조직에서 차지하는 비중과 또한 업종의 성격(기밀성, 무

결성, 가용성)에 따라 종합적인 결과에서는 낮은 비중을 차지할 수 있다는 것을 확인할 수 있었다. 이와 같이 업종별 가중치, 프로세스에 대한 가중치, 프로세스에 속한 자산에 대한 가중치, 체크 항목에 대한 가중치 등 4가지의 다중가중치를 적용하고, 퍼지기법을 이용하여 판단자의 주관성을 최소화함으로써, 정보보호 수준 측정의 정확성 및 신뢰성을 높일 수 있었다.

도출된 결과에 따라 취약한 부분에 대해서는 세부적인 위험분석을 이용한 시뮬레이션으로 선택된 대응책 구현 후의 예상 정보보호 수준을 비교 평가할 수 있다. 또한, 결과를 가시적인 그래프로 나타냄으로써, 관리자에게 정보보호 수준 향상을 위한 대응책을 선택하기 위한 의사결정에 도움을 준다. 또한, 웹을 기반으로 구현함으로써 사용자가 더 쉽고 간단하게 조직의 정보보호 수준을 측정할 수 있으며, 구현된 도구는 비전문가도 자산의 목록을 입력하고 비교적 간단한 체크리스트에 표시함으로써 쉽게 사용할 수 있다.

본 연구의 활용 방안을 몇 가지로 요약해보면, 첫째, 정보보안 관리체계를 구축하기에 앞서, 현재의 정보보안 수준을 점검하고자 하는 조직이 활용할 수 있고, 둘째, 정보보안 수준 향상을 위한 대응책 선택 시 의사결정에 도움을 줄 수 있으며, 셋째, 기존의 위험관리/위험분석 도구들과는 달리 정보보안에 대한 기본적인 지식만으로도 조직의 소유자나 경영자 또는 관리자 등이 쉽게 사용할 수 있다.

향후 연구과제로는, 첫째, 점검항목을 기업의 경영자, 또는 운영자 등이 수행함에 따른 주관성의 문제를 최소화 할 수 있는 방법이 개발되어야 할 것이며, 둘째, 웹상에서 운영되기 때문에 조직의 중요 정보에 대한 보안문제 등이 앞으로 해결되어야할 것이며, 셋째, 본 연구의 결과를 기초로 하여 조직의 특성별로 정보보안 수준의 차이를 분석하기 위한 지표항목 개발과 적용방법이 개발될 경우 종합적인 정보보호 관리체계 연구에 유용할 것이다.

참고문헌

[1] 김현수, "정보보안수준 계량화 연구", 1999. 12., 경영정보학 연구 제9권 제4호

[2] "BS7799 Part 1 : The Code of Practice", British Standard Institution. Part 2 : The Management S tandard".

[3] "위험분석 도구 기초기술 개발에 관한 연구", 2001, 한국 전자통신 연구원 부설 국가보안기술연구소.

[4] "CRAMM User Guide", Issue 2.0., U.K. Security Service and CESG, 2001.2.

[5] 박진섭 외1 "베이스라인 보안정책을 위한 위험분석 체크리스트" 1997, Journal of the Institute of Industrial Technology(Taejon Univ.) Vol. 8. No. 2 : 23-40

[6] 홍승구 외2, "정보시스템 안전성 평가 도구 설계 및 구현" 2002. 05. 한국멀티미디어학회

[7] "정보시스템 보안을 위한 위험분석 소프트웨어 개발", 1997., 한국전산원

[8] "정보보호 관리표준" 2002. 5., 한국정보통신기술협회

[9] 이광형, 오길록 "퍼지이론 및 응용", 홍릉과학출판사, 1991. 3

[10] L.A.Zadeh, "Fuzzy Sets", Information and Control 8, 1965.

[11] "취약점 분석, 평가를 위한 자산분석 지침(안) - 위험산정 및 분석 방법 이론 소개", 2001. 9., 한국정보보호진흥원

[12] 이진환 외2, 유전 알고리즘을 이용한 퍼지 규칙 기반 표적 추적 시스템설계, 한국 퍼지 및 지능시스템 학회, Vol.9, No3. 1999.

[13] William F.Punch, et al., "Design Using Genetic Algorithms-Some Results for Laminated Composite Structures," IEEE Expert, Jan 1995.

[14] NIST, Dictionary of Algorithma and Data Structures,http://www.nist.dads/HTML/knapsackProblem.html

[15] 박성진, 정보보안 침해 위험신호의 조직학습 실패에 관한 시스템 다이나믹스적 연구, 한국컴퓨터정보학회 제 8권 3호, pp180-181

저 자 소 개

성 경

1998년~1990년국제종합기계(주)

1993년 경희대학교 대학원 공학석사

2003년 한남대학교 대학원 공학박사

1994년~2004년 동해대학교 컴퓨터공학과 교수

2004년~현재 목원대학교 컴퓨터교육과 교수

<관심분야> 정보관리(정보보호), 신경망, 컴퓨터교육