정보보안 예산 수립에서 퍼지 AHP의 적용을 통한 위험 비용 분석

류 시 욱* · 허 덕 규*
*한중대학교 공학부

Cost Risk Analysis for Preparing Budgets of Information Security using Fuzzy AHP

Si-Wook Ryu* · Duk-Gyu Her*
*School of Engineering, Hanzhong University

Abstract

Recently, the breakdown of online banking servers and the leakage of customer information give rise to much concern about the security of information systems in financial and banking companies in Korea. The enforcement of security for information system becomes much more important issue than earlier. However, the security reinforcement of information system is restricted by a budget. In addition, the activities' cost to secure information system from threatening are under uncertain circumstances and should be established by a human decision maker who is basically uncertain and vague. Thus, making the budget for information system is exposed to any extent of the risk for these reasons.

First, we introduce brief fuzzy set theory and fuzzy AHP (Analytic Hierarchy Process) methodology. Then, the cost elements that comprise yearly budget are presented and the priorities among the cost elements are calculated by fuzzy AHP. The cost elements that are exposed to risk are evaluated from the both perspectives of the risk impact and risk occurrence possibility which are expressed as linguistic terms. To get information on the risk profiles−pessimistic, most likely, and optimistic−for each cost element, the evaluation is accomplished and the result is presented. At last, the budget ranges−minimum, mode, maximum−for each cost element are estimated with the consideration of the risk profiles.

Keywords : Information Security System, Fuzzy AHP, Cost Risk Analysis

1. 서 론

최근 온라인 네트워크 혹은 인터넷 상에서 운영되는 다수의 기업이나 기관들이 해킹, 고객정보유출, 정전 등의 사고로 인한 정보시스템의 정지 등 정보보안에서 많은 어려움을 겪고 있다. 정보 유출의 경우 오프라인과 온라인의 모든 경우에 존재하며 이러한 경우는 양적 측면에서의 보안에 대비하는 장치가 있어야 할 것이다. 지난 해 일어난 사건들을 보면, 네이트온의 경우는 오프라인에서 내부직원에 의한 고객정보유출로 기업의 이미지 손상과 신뢰도 추락 등의 손실을 입었고, 싸이월드 온라인 해킹으로 3,500만 명의 개인정보 유출 사건, 넥슨의 경우는 게임 회원 1,320만 명의 개인 정보가 유출됨으로 인해 전화 금융사기와 같은 2차 피해의 심각한 우려를 낳기도 하였다.

† 교신저자: 류시욱, 강원도 동해시 한중대학교 공과대학 공학부
M · P: 010-8450-4852, E-mail: swkryu@hanzhong.ac.kr
2012년 7월 20일 접수; 2012년 9월 3일 수정본 접수; 2012년 9월 11일 게재확정

고객의 우려가 가장 큰 금융 기관에서도 해킹, 정전 등으로 인한 서버다운, 수시로 발생하는 뱅킹 서비스 장애 등은 정보시스템 보안에 심각한 수준의 문제점이 있음을 시사하고 있다.

이러한 문제점들이 발생하는 원인을 살펴보면 국내 기업들과 기관들의 정보 보호, 정보시스템 보안에 대한 투자가 턱없이 낮은 수준이기 때문인 것으로 보인다.

한국인터넷진흥원(KISA)이 작년 3월 발표한 '2010 국내 정보보안산업 실태조사'에 따르면 개인정보보호를 위해 보안장비 및 전담인력의 확충에 투자한 기관은 전체 6529개 사업자 중 36.5%에 불과한 것으로 나타났다.

작년 하반기 정부는 금융기관의 정보시스템 보안예산 확충비율을 기존의 5%에서 7%로 올리도록 권고했다. 그러나 기존의 5% 보안예산의 경우도 실제 책정 후 집행과정에서 이를 지키지 않는 경우도 많아 실효성에 대한 우려의 목소리가 높은 것도 사실이다[6]. 이는 기업이나 기관의 입장에서는 정보보안 활동이 불확실성이 높은 미래의 상황에 대비하는 비생산적인 것으로 인식되어 투자가 꺼려지기 때문이다. 그러나 오늘날 정보보안은 기업이나 기관 활동의 부차적인 것이 아니라 핵심선결 조건이라는 인식이 필요하다.

따라서 본 연구에서는 정보보안 활동의 예산을 수립해야 하는 기업이나 기관에서 의사결정자 판단의 불확실성과 향후 예상되는 미래의 불확실한 상황을 평가시에 반영할 수 있는 다기준의사결정(MCDM: Multi-Criteria Decision Making) 방법의 하나로 퍼지 AHP(Analytic Hierarchy Process)를 이용하여 정보보안 위험요소를 평가하고, 불확실한 상황에 기초한 예산의 범위를 추정하는 방안을 제시하고 사례를 보이는 것을 목표로 한다. 본 연구에서 제안하는 방법과 비용추정의 사례는 실제 기업이나 기관에서 의사결정자의 판단의 모호성, 불확실한 미래상황을 반영하여 예산의 범위를 알고자할 때 도움이 될 것으로 사료된다.

2. 관련 연구

본 연구에서는 미래의 불확실한 보안 공격에 대비하기 위한 정보시스템의 보안업무 수행에 필요한 예산을 수립하는 데 있어 퍼지이론을 이용하여 위험요소를 평가하고 예상되는 위험수준에 따른 예산을 수립하는 방안을 마련하고 그 예제를 보이고자 한다. 다음으로 본 연구와 관련된 퍼지집합 이론, 퍼지 AHP 등에 대해 간략히 소개하고자 한다.

2.1 퍼지집합 이론

퍼지이론은 Zadeh[13]의 의해 완전정보의 부족에 따른 모호성, 부정확성을 반영할 수 있도록 기존의 집합이론을 확장한 개념이다. Bellman & Zadeh[7]는 퍼지집합 이론을 평가자의 의사결정 과정에서 발생하는 본질적인 부정확성, 모호성을 효과적으로 다루는 접근법으로 다기준 의사결정 분야에 처음 도입하였다. 먼저, 본 연구에서는 소속도 함수는 삼각 퍼지 수(TFN: triangular fuzzy number)를 따른다고 가정한다. 본 연구에서는 삼각 퍼지 수에 대한 퍼지집합 이론의 정의를 기존의 연구들(Buckley[8]; Dubios & Prade[12]; Zadeh[14])을 참조하여 다음과 같이 요약하였다.

정의 1. 어떤 양의 삼각 퍼지 수 $\tilde{n}$는 $\tilde{n}=(l, m, u)$로 정의할 수 있다. 퍼지 수 $\tilde{n}$의 소속도 함수 $\mu_{\tilde{n}}(x)$는 다음과 같이 정의할 수 있다.

$$\mu_{\tilde{n}}(x)=\begin{cases} 0, & x \le l \\ \dfrac{x-l}{m-l}, & l < x \le m \\ \dfrac{u-x}{u-m}, & m < x \le u \\ 0, & x > u \end{cases}$$

정의 2. 두 개의 삼각 퍼지 수 $\tilde{m}=(l_1, m_1, u_1)$와 $\tilde{n}=(l_2, m_2, u_2)$ 그리고 실수 r이 주어졌다면, 두 퍼지수의 산술 계산은 다음과 같이 수행한다.

$$\tilde{m} \oplus \tilde{n}=[m_1+n_1, m_2+n_2, m_3+n_3]$$
$$\tilde{m} \ominus \tilde{n}=[m_1-n_1, m_2-n_2, m_3-n_3]$$
$$\tilde{m} \otimes r=[m_1 r, m_2 r, m_3 r]$$
$$\tilde{m} \otimes \tilde{n}=[m_1 \times n_1, m_2 \times n_2, m_3 \times n_3]$$

정의 3. 위의 정의 2와 같이 두 삼각 퍼지 수 $\tilde{m}$와 $\tilde{n}$가 주어져 있다면 두 수 사이의 거리는 최단거리 방법에 의해 다음과 같이 정의된다.

$$d(\tilde{m}, \tilde{n})=\sqrt{\frac{1}{3}\left[(l_1-l_2)^2+(m_1-m_2)^2+(u_1-u_2)^2\right]}$$

2.2 AHP와 퍼지 AHP

AHP기법은 1970년대 중반 Saaty[13]가 개발한 계층적인 분석기법으로 평가자의 주관적인 판단을 정량적으로 분석하게 하여 의사결정을 수행하는데 도움을 주는 유용한 도구로 각광을 받아 왔으며 많은 분야에서 널리 활용되고 있다. Saaty는 평가에서 9점 척도를 기본으로 하고 평가과정의 일관성을 검증하기 위하여 일관성 비율(Consistency Ratio: CR)은 다음과 같은 식을 이용하여 검증하였다.

$$CR = \frac{CI}{RI} = \frac{\lambda_{\max} - N}{N-1} \bullet \frac{1}{RI} \quad (1)$$

(단, CI: 일관성 지수, RI: 확률 지수, $\lambda_{\max}$: 최대 고유행렬값, N: 행렬의 크기)

일관성 비율은 0.1 이하인 경우 일관성이 있는 것으로 판단한다. 한편, AHP 기법은 평가자의 주관을 정량적으로 다룰 수 있는 장점이 있지만, 평가자의 평가 논리에 내재된 모호한 가치판단 기준이나 인간이 사용하는 언어적 모호성을 갖는 경우에는 그 사용에 한계가 있다. Chang[9]은 삼각 퍼지 수를 사용하여 기존의 AHP를 퍼지 AHP로 확장하는 방법을 제안하였고, Zhu et al.[16]은 Chang[9]이 제안한 삼각 퍼지 수 이론에서 복합 퍼지값(fuzzy synthetic degree value)을 구하는 방법을 제안하였다.

본 연구에서는 기존의 AHP 기법에 퍼지집합론의 이론적 특성을 결합시킨 퍼지 AHP기법을 적용하였으며, 퍼지 AHP 수행절차는 다음과 같다.

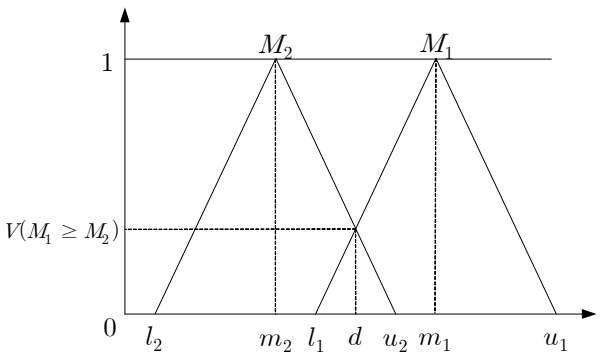
단계 1. 같은 계층의 요소들에 대해 쌍대 비교를 실시하며 퍼지 쌍대 비교 행렬 $A = (a_{ij})_{n \times n}$을 구한다. 쌍대비교는 퍼지한 사고를 반영하기 위하여 삼각퍼지함수 즉, $a_{ij} = (l_{ij}, m_{ij}, u_{ij})$를 이용한다. 이 때, l_{ij}는 삼각퍼지함수의 하한 값을 u_{ij}는 삼각 퍼지 함수의 상한 값을 m_{ij}는 1~9의 범위를 갖는 꼭지점에 해당하는 정수 값을 의미한다.

단계 2. 퍼지 확장원리(fuzzy extent principle)를 사용하여 복합 퍼지값(fuzzy synthetic degree value)은 다음 식으로 계산한다.

$$S_i = (\sum_{j=1}^{n} l_{ij}, \sum_{j=1}^{n} m_{ij}, \sum_{j=1}^{n} u_{ij}) \otimes (\sum_{j=1}^{n}\sum_{i=1}^{n} l_{ij}, \sum_{j=1}^{n}\sum_{i=1}^{n} m_{ij}, \sum_{j=1}^{n}\sum_{i=1}^{n} u_{ij})^{-1}$$
$$(i, j = 1, 2, \cdots\cdots, n) \quad (2)$$

퍼지 합성 확장값은 주어진 정보에 대한 가능성 정도(degree of possibility)를 구하는데 적용되며, 퍼지삼각함수 $M_1(l_1, m_1, u_1)$, $M_2(l_2, m_2, u_2)$가 볼록 퍼지함수(convex fuzzy function)일 때 가능성 정도는 다음 식(3)에 의하여 계산된다. 이 때, $\mu_{M_1}(d)$는 <Figure 1>과 같이 $\mu_{M_1}(x)$와 $\mu_{M_2}(x)$의 퍼지 교집합의 최대값을 나타낸다.

$$V(M_1 \geq M_2) = 1 \quad \text{iff } m_1 \geq m_2$$
$$V(M_2 \geq M_1) = hgt(M_1 \cap M_2) = \mu_{M_1}(d) = \frac{l_1 - u_2}{(m_2 - u_2) - (m_1 - l_1)}$$
$$\text{if } l_1 \leq u_2 \quad (3)$$



<Figure 1> Intersection of two triangular fuzzy numbers M_1 and M_2

단계 3. 퍼지 확장원리에 의한 가능성 정도는 다음 식(4)에 의하여 가중치 벡터로 주어지고 가중치의 합이 1이 되도록 정규화 시키면 최종 가중치를 구할 수 있다.

$$d'(A_i) = \min V(S_i \geq S_j)$$
단, $j = 1, 2, \cdots, n, \ j \neq i \quad (4)$
$$W' = (d'(A_1), d'(A_2), \cdots, d'(A_n))^T \quad (5)$$
$$W = (d(A_1), d(A_2), \cdots, d(A_n))^T \quad (6)$$

단계 4. 퍼지 AHP 기법에서 일관성 평가는 Saaty가 제안한 일관성 비율과 함께 Robert Csutora의 방법

($\lambda_{max} - 1 \leq 1$)을 많이 사용하고 있다. 본 연구에서는 이 두 방법에 대해 일관성을 평가하여 보았다. 이 때, 일관성 비율을 결정하기 위해 삼각 퍼지 수는 도심 비퍼지화 방법을 사용하여 하나의 비퍼지화(Defuzzy-fication)된 값으로 수치화하여 사용하였다.

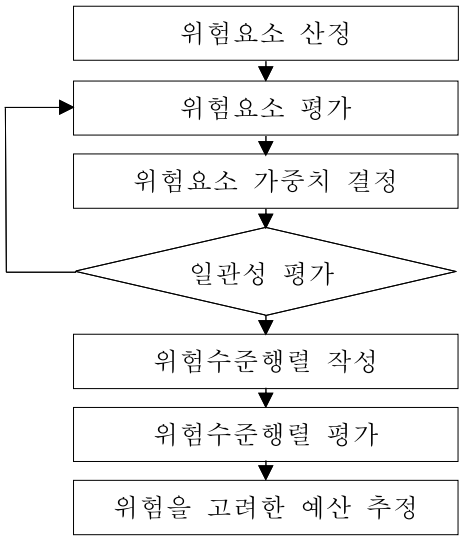
퍼지이론은 의사결정 분야에 적용되면서 여러 유형의 문제를 해결하는데 많이 활용되고 있다. 특히, 다기준 의사결정 분야에 적극적으로 도입되어 활용되고 있으며 퍼지 AHP는 그 중의 하나이다. 본 연구에서 다루고자 하는 정보시스템 보안에 대한 공격을 예상하는 일은 불확실성이 높은 영역에 해당한다. 본 연구에서는 두 가지 관점에서 정보의 부족, 모호성, 부정확성이 드러난다. 하나는 미래 해킹 공격에 대한 불확실성에 따른 정보의 모호성이나 부정확성이다. 그리고 나머지 하나는 이를 의사결정 과정에 이용하는 의사결정자의 판단과정에서 발생하는 모호성, 부정확성이다. 따라서 본 연구에서는 이러한 문제의 속성을 반영하여 퍼지개념을 이용한 문제해결의 과정을 제안하고 그 예를 다루고자 한다.

다음에서는 AHP나 퍼지 AHP를 정보 보안 분야에 적용한 기존 연구들에 대해 살펴보고자 한다. 먼저 김수영&이승찬[2]은 정보시스템 솔루션을 선정하는데 있어 퍼지 AHP기법을 이용하였고 정량적인 데이터인 비용을 AHP의 정성적인 다른 요소들과 함께 고려하는 모델을 적용하는 방안을 소개하였다. 정철용&손동기[4]는 정보시스템 개발 프로젝트에서 위험요인을 평가하기 위한 계층모형을 개발하고 이를 AHP를 이용하여 평가하였다. 공희경 등[1]은 정보보호를 위한 보안제품들을 경제적 측면의 가격, 매출, 운영비용, 기업 이미지에 대해 그리고 기술적 측면의 기밀성, 무결성, 가용성 등에 대해 평가하는 연구를 수행하였다. 이경근&류시욱[3]은 정보보안 방안을 선택하는 문제에 대해 기존의 퍼지 AHP 방법인 복합 퍼지 값 방법과 Shannon entropy 방법에 추가하여 삼각 퍼지 수의 중간 값을 포함한 보완하는 새로운 방법인 U-uncertainty 방법을 제안하고 보안의 방안에 대해 평가하고 비교하는 연구를 수행하였다. Chen & Wang[10]은 세계 시장을 개척하는 정보시스템 산업에 있어 주요성공요인을 AHP를 이용하여 추출하는 방법을 보였다. 최철림&송영재[5]는 클라우딩 컴퓨팅의 보안성에 대한 ISO 7498-2표준의 관련 속성들이 전체 보안 품질에 미치는 상대적 영향도를 퍼지 AHP를 이용하여 평가하였다. 그리고 Zhang et al.(2012)은 e-커머스 보안 평가를 위한 AHP 계층모형을 수립하고 예제를 통해 그 과정을 소개하였다. 위의 연구들을 살펴보면 정보 보안 분야에 AHP를 적용한 연구는 어느 정도 있으나 퍼지 AHP를 적용한 연구는 그다지 많다고 보기는 어렵다. 특히나 퍼지 AHP 연구방법을 접목하고 퍼지집합 이론을 접목한 연구는 거의 없는 것으로 나타났다.

본 연구에서 다루는 문제에서는 퍼지이론은 두 과정에 응용된다. 하나는 보안 위험 요소를 평가하는 과정에 퍼지 AHP를 이용한다. 그리고 위험에 대한 발생빈도와 충격강도는 언어적 평가의 모호성을 반영할 수 있는 퍼지이론을 복합적으로 적용하며, 예산을 구성하는 비용요소들에 대해서는 위험 프로파일 즉, 미래의 불확실성을 낙관적, 정상적, 비관적 프로파일의 상황을 예상하여 이를 각 위험 수준에 대해 프로파일 별로 평가하는 방안을 소개하고 그 예제를 다루고자 한다.

3. 퍼지 AHP를 이용한 분석절차

위험 인자 간의 가중치를 위험 인자 간의 삼각 퍼지 멤버십 함수를 이용해서 비교하여 구하고 구한 위험 인자의 가중치를 비용적 측면에서 평가할 수 있는 통합 평가과정을 다음 절에서 제안하는 과정의 절차를 다음 <Figure 2>와 같이 수행한다. 이 과정은 퍼지 AHP를 이용한 위험 인자의 가중치를 결정하는 과정과 위험에 따른 비용을 산정하는 과정으로 구성된다.



<Figure 2> Analysis procedure using fuzzy AHP

3.1 퍼지 AHP를 이용한 위험 가중치 결정

정보시스템 보안을 위한 예산의 수립은 해당 기업이나 조직마다 그 규모가 다를 수 있다. 본 연구의 도메인은 이와 같이 다른 규모의 기업이나 조직에 대한 어떤 일반적인 연구결과를 얻고자 하는 것이 아니라 본

연구 방법을 구체적인 사례에 적용하여 의사결정에 도움을 주고자 하는데 맞추어져 있다. 본 연구 방법의 적용 과정을 보이기 위하여 하나의 예제를 도입하여 소개하고자 한다. 데이터 범위의 적절성은 실제 정보시스템 예산계획을 수립하는 책임자를 통하여 실시하였고 연구를 진행하였다. 정보시스템의 보안 위험 요소로 보안정책 위험, 보안시스템 위험, 물리적 통제 위험의 3가지 항목을 도출하였으며 일관성 검증을 동시에 수행하며 쌍대비교한 결과는 <Table 1>과 같이 요약하였다.

쌍대비교는 삼각퍼지함수로서 최소, 최적, 최대의 범위 값으로 구성하였다. 예를 들어, 쌍대비교 행렬의 a_{23}의 첫째 항은 행기준(보안 시스템 위험)이 열기준(물리적 통제 위험)보다 언어적 표현으로서 "약 4배 정도" 중요하다는 것을 반영한다. 이 때, 2의 멤버십 함수 값은 1이고, 2와 6의 멤버십 함수 값은 0이 된다. 즉 보안시스템 위험이 물리적 통제 위험보다 2이하로 중요하거나 6이상으로 중요할 가능성은 0이라는 것을 의미한다.

<Table 1> Pairwise comparison between risk elements

위험 요소	보안정책 위험	보안시스템 위험	물리적 통제 위험
보안정책 위험	$(1, 1, 1)$	$(\frac{1}{3}, \frac{1}{2}, 1)$	$(1, 3, 5)$
보안시스템 위험	$(1, 2, 3)$	$(1, 1, 1)$	$(2, 4, 6)$
물리적통제 위험	$(\frac{1}{5}, \frac{1}{3}, 1)$	$(\frac{1}{6}, \frac{1}{4}, \frac{1}{2})$	$(1, 1, 1)$

<Table 1>의 삼각 퍼지 함수 값으로부터 퍼지 합성 확장 값으로 변환시키면 다음과 같다.

$$S_1 = (2.33, 4.50, 7.00) \otimes (\frac{1}{19.50}, \frac{1}{13.08}, \frac{1}{7.70}) = (0.12, 0.34, 0.91)$$

$$S_2 = (4.00, 7.00, 10.00) \otimes (\frac{1}{19.50}, \frac{1}{13.08}, \frac{1}{7.70}) = (0.21, 0.54, 1.30)$$

$$S_3 = (1.37, 1.58, 2.50) \otimes (\frac{1}{19.50}, \frac{1}{13.08}, \frac{1}{7.70}) = (0.07, 0.12, 0.32)$$

퍼지 확장 원리에 의한 가능성 정도는 식 (4)~(6)에 의해서 가중치 벡터(W')로 변환된다. 따라서 위의 퍼지 합성 확장 값으로부터 다음의 결과를 얻을 수 있다.

$$V(S_1 \geq S_2) = \frac{0.21 - 0.91}{(0.34 - 0.91) - (0.54 - 0.21)} = 0.77$$

$$V(S_1 \geq S_3) = 1,\ V(S_2 \geq S_1) = 1,\ V(S_2 \geq S_3) = 1$$

$$V(S_3 \geq S_1) = 0.48,\ V(S_3 \geq S_2) = 0.21$$

$$d' = (\text{보안정책}) = \min(V(S_1 \geq S_2),\ V(S_1 \geq S_3)) = \min(0.77, 1.0) = 0.77$$

$$d' = (\text{보안시스템}) = 1$$

$$d'(\text{물리적 통제}) = 0.21$$

위의 값으로부터 가중치는 다음과 같다.

$$W' = (0.77, 1.0, 0.21)^T$$

따라서 가중치의 합이 1이 되도록 정규화 시키면 보안정책, 보안시스템, 물리적 통제관련 위험의 상대적 가중치를 의미하는 최종가중치(W)를 구할 수 있다.

$$W' = (0.39, 0.50, 0.11)^T$$

일관성측정을 위해 삼각퍼지함수를 비퍼지화하여 AHP 절차에 맞게 스프레드시트 프로그램을 작성하였으며, 그 결과는 <Table 2>와 같이 Saaty의 일관성 비율과 Robert Csutora의 일관성 평가지수 모두 만족하는 것으로 나타났다.

<Table 2> Results of consistency index

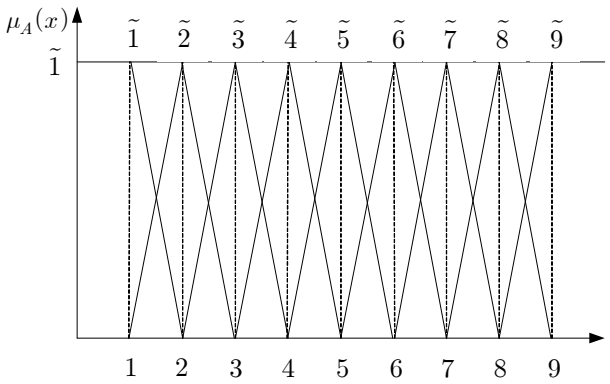
측정방법	계산	결과
Saaty의 방법	$CR = \frac{CI}{RI} = \frac{\lambda_{max} - N}{N-1} \cdot \frac{1}{RI} = \frac{3.001-3}{3-1} \cdot \frac{1}{0.58} = 0.0007 < 0.1$	O.K.
Robert Csutora 방법	$\lambda_{max} - n = 3.001 - 3 = 0.001 < 1.0$	O.K.

3.2 위험비용 산정 모델

정보시스템의 안전에 끊임없이 위협하는 보안의 문제는 정보시스템의 보안을 수행하는데 필요한 예산의 범위를 추정하기 위하여 향후 예측되는 위험을 고려하여 정량적인 평가를 수행할 필요가 있다. 각 위험 인자에 대한 정량적인 평가를 위해서 위험에 따른 발생빈도와 충격강도를 동시에 고려하는 복합 위험 수준(composite risk level)을 결정하여야 한다. 본 연구에서는 복합 위험 수준을 퍼지집합론을 이용하여 <Table 3>과 같이 퍼지 멤버십 함수를 선정하였다.

<Table 3> Membership function for composite risk levels

퍼지수	멤버십 함수
$\tilde{1}$	(1, 1, 2)
$\tilde{2} \sim \tilde{8}$	$(x-1,\ x,\ x+1)$ for $x = 2 \sim 8$
$\tilde{9}$	(8, 9, 9)



<Figure 2> Fuzzy membership function to evaluate composite risk levels

그리고 식 (7)은 여러 단계의 언어적 변수로 표현되는 위험의 발생빈도와 충격강도를 결합하여 퍼지 위험을 평가하며 그 평가된 위험 수준의 결과는 매트릭스 형태로 <Table 4>와 같이 구성된다.

$$RL_{ij} = RI_{ij} \oplus RP_{ij} \tag{7}$$

(단, RL: 위험 수준, RI: 위험 충격강도, RP: 위험 발생확률, $\oplus$: RI와 RP 각각에 대한 매트릭스 대응)

<Table 4> Composite risk level matrix

위험충격 강도(RI)	위험 발생빈도 (RP)				
	VH	H	M	L	VL
VS	$\tilde{9}$	$\tilde{8}$	$\tilde{7}$	$\tilde{6}$	$\tilde{5}$
S	$\tilde{8}$	$\tilde{7}$	$\tilde{6}$	$\tilde{5}$	$\tilde{4}$
MO	$\tilde{7}$	$\tilde{6}$	$\tilde{5}$	$\tilde{4}$	$\tilde{3}$
L	$\tilde{6}$	$\tilde{5}$	$\tilde{4}$	$\tilde{3}$	$\tilde{2}$
VL	$\tilde{5}$	$\tilde{4}$	$\tilde{3}$	$\tilde{2}$	$\tilde{1}$

(단, VH: Very High, H: High, M: Medium, L: Low, VL: Very Low, VS: Very Serious, S: Serious, MO: Moderate)

각각의 비용요소에 대한 위험 인자들의 발생빈도와 충격강도에 따른 복합 위험 수준은 관련 전문가의 주관적 판단으로 퍼지하게 결정된다. 예를 들어, 위험 충격강도가 낮고(Low) 위험 발생빈도가 높다(High)면 위험 충격강도와 위험 발생빈도의 상관관계를 통한 복합 위험 수준은 "약 5"의 값($\tilde{5}$)을 가지게 된다.

복합 위험 수준은 낙관적(Optimistic), 정상적(Most Likely), 비관적(Pessimistic)인 프로파일들의 경우에 대하여 각각 평가된다. 이 때, 퍼지 AHP 기법을 통하여 산출되어진 위험 인자들의 가중치를 곱하여 합산하면 각각의 위험 프로파일에 대한 합계 점수를 도출할 수 있다. 위험 점수에 대한 산출 식은 식(8)와 같고 그 결과는 <Table 5>와 같이 제시하였다. 이 때, 위험 프로파일의 작성은 앞에서 위험 요소 간의 쌍대비교를 수행한 정보시스템 예산계획을 수립하는 책임자를 통하여 실시하였다.

$$\underset{k=o.p.}{\overset{p.p.}{(+)}} RS_{ij} = \bigvee_{i=1}^{n} \left[\underset{k=o.p.}{\overset{p.p.}{(+)}} RV_{ij} \times \sum_{j=1}^{m} W_j \right] \tag{8}$$

(단, k: 위험 프로파일 $k \in (o.p.,\ m.p.,\ p.p.)$, RS_{ij}: i 요소, j요소에 대한 위험 점수, RV_{ij}: i요소, j요소의 위험 프로파일 값)

각 위험 프로파일에 대한 위험 점수들이 도출되면 비관적, 낙관적인 경우의 위험 점수를 정상적인 경우의 위험 점수로 나누어 위험 프로파일 간 상대비율을 구하고 이 비율을 이용하여 비용 위험을 고려한 요소업무에 대한 예산의 위험을 반영한 최소값, 최빈값, 최대값을 추정할 수 있다. <Table 5>은 정보시스템의 보안업무에 대한 예비 견적과 위험 간 상대비율, 예상 업무비용의 추정 범위를 정리하여 나타내었다. 이 추정 값들은 정보보안 예산을 수립하는데 있어 불확실성에 대비한 유연하고 신뢰성 있는 예산의 추정을 가능하게 할 것이다.

<Table 6> Budget ranges considering risk

비용 요소	예상 비용 (단위: 만원)	프로파일 간 상대비율			위험을 고려한 예산의 범위		
		$o.p./m.p.$	$m.p./m.p.$	$p.p./m.p.$	최소값	최빈값	최대값
조직관리	120	0.51	1	1.49	61.2	120	178.8
인적자원	8,000	0.68	1	1.32	5,440	8,000	10,560
HW관리	1,000	0.62	1	1.38	620	1,000	1,380
SW관리	1,200	0.67	1	1.33	804	1,200	1,596
DB관리	700	0.60	1	1.40	420	700	980
구역관리	360	0.42	1	1.58	151.2	360	568.8
재해대비	200	0.53	1	1.47	106	200	294
접근제어	100	0.53	1	1.47	53	100	147

<Table 5> Risk profile evaluation with different risk levels

비용 요소	위험 프로파일	보안정책위험			보안시스템위험			물리적 통제위험			합계
		0.39			0.50			0.11			
		RI	*RP*	결과	*RI*	*RP*	결과	*RI*	*RP*	결과	
조직 관리	PP	VS	M	$\tilde{7}$	MO	M	$\tilde{5}$	VS	H	$\tilde{8}$	6.11
	MP	S	L	$\tilde{5}$	L	L	$\tilde{3}$	S	M	$\tilde{6}$	4.11
	OP	MO	VL	$\tilde{3}$	VL	VL	$\tilde{1}$	MO	L	$\tilde{4}$	2.11
인적 자원	PP	S	H	$\tilde{7}$	VS	VH	$\tilde{9}$	VS	VH	$\tilde{9}$	8.22
	MP	MO	M	$\tilde{5}$	S	H	$\tilde{7}$	S	H	$\tilde{7}$	6.22
	OP	L	L	$\tilde{3}$	MO	M	$\tilde{5}$	MO	VH	$\tilde{5}$	4.22
HW 관리	PP	MO	M	$\tilde{5}$	VS	VH	$\tilde{9}$	S	H	$\tilde{7}$	7.22
	MP	L	L	$\tilde{3}$	S	H	$\tilde{7}$	MO	M	$\tilde{5}$	5.22
	OP	VL	VL	$\tilde{1}$	MO	M	$\tilde{5}$	L	L	$\tilde{3}$	3.22
SW 관리	PP	S	H	$\tilde{7}$	VS	VH	$\tilde{9}$	S	H	$\tilde{7}$	8.00
	MP	MO	M	$\tilde{5}$	S	H	$\tilde{7}$	MO	M	$\tilde{5}$	6.00
	OP	L	L	$\tilde{3}$	MO	M	$\tilde{5}$	L	L	$\tilde{3}$	4.00
DB 관리	PP	MO	M	$\tilde{5}$	VS	VH	$\tilde{9}$	MO	M	$\tilde{5}$	7.00
	MP	L	L	$\tilde{3}$	S	H	$\tilde{7}$	L	L	$\tilde{3}$	5.00
	OP	VL	VL	$\tilde{1}$	MO	M	$\tilde{5}$	VL	VL	$\tilde{1}$	3.00
구역 관리	PP	MO	M	$\tilde{5}$	MO	M	$\tilde{5}$	VS	VH	$\tilde{9}$	5.44
	MP	L	L	$\tilde{3}$	L	L	$\tilde{3}$	S	H	$\tilde{7}$	3.44
	OP	VL	VL	$\tilde{1}$	VL	VL	$\tilde{1}$	MO	M	$\tilde{5}$	1.44
재해 대비	PP	S	H	$\tilde{7}$	MO	M	$\tilde{5}$	VS	VH	$\tilde{9}$	6.22
	MP	MO	M	$\tilde{5}$	L	L	$\tilde{3}$	S	H	$\tilde{7}$	4.22
	OP	L	L	$\tilde{3}$	VL	VL	$\tilde{1}$	MO	M	$\tilde{5}$	2.22
접근 제어	PP	S	H	$\tilde{7}$	MO	M	$\tilde{5}$	VS	VH	$\tilde{9}$	6.22
	MP	MO	M	$\tilde{5}$	L	L	$\tilde{3}$	S	H	$\tilde{7}$	4.22
	OP	L	L	$\tilde{3}$	VL	VL	$\tilde{1}$	MO	M	$\tilde{5}$	2.22

4. 결 론

본 연구는 AHP기법에서 퍼지이론을 접목한 기존의 연구들의 결과를 이용하여 정보시스템 보안업무를 수행하는데 예상되는 예산의 비용을 낙관적, 정상적, 비관적 상황을 고려하여 추정할 수 있는 방법과 함께 이를 적용한 예제를 소개하였다.

위험 인자 간의 가중치를 위험 인자 간의 삼각 퍼지 멤버십 함수를 이용해서 비교하여 구하였고 위험 인자의 가중치는 퍼지 AHP를 이용하여 결정하였다. 그리고 각 위험 인자에 대한 정량적인 평가를 위해서 위험에 따른 발생빈도와 충격강도를 동시에 고려하는 복합 위험 수준은 퍼지집합론을 이용하는 방법을 제시하였다.

각 위험 프로파일에 대한 위험 점수들은 낙관적, 정상적, 비관적인 프로파일의 위험 점수를 정상적인 프로파일의 위험 점수로 나누어 위험 프로파일 간 상대비율을 구하고 이 비율을 이용하여 비용 위험을 고려하고 예산을 구성하는 비용요소에 대해 최소값, 최빈값, 최대값으로 그 범위를 추정하였다.

그러나 본 연구는 다음과 같은 한계점도 있다. 먼저, 정보보안 예산을 수립하는 과정으로 제시한 방법에 대한 객관적인 효과성을 검증하지 못하였다는 점이다. 둘째, 정보보안 예산을 수립하는 연구의 도메인에 대한 타당성을 연구하지 못한 점도 꼽을 수 있다. 따라서 연구 방법 및 연구 도메인에 대한 효과성을 객관적으로 비교분석하는 연구를 추후 과제로 삼고자 한다.

마지막으로 본 연구를 통해 정보보안에 필요한 예산의 범위를 추정해 봄으로써 실제 정보 보안에 대한 연간계획을 수립할 때 불확실한 상황을 반영한 예산을 수립하는데 도움이 될 것으로 사료된다.

참 고 문 헌

[1] 공희경, 전효정, 김태성, “AHP를 이용한 정보보호 투자 의사결정에 대한 연구,” Journal of Information Technology Application & Management, 제15권, 제1호, 2008, pp. 139-152.

[2] 김수영, 이승찬, “퍼지 AHP를 이용한 정보시스템 솔루션 선정 모델에 관한 연구,” Entrue Journal of Information Technology, 제4권, 제1호, 2005, pp. 79-89.

[3] 이경근, 류시욱, “정보 보안 방안 선택을 위한 퍼지 AHP 방법의 비교 검토,” 정보시스템연구, 제19권, 제3호, 2010, pp. 59-73.

[4] 정철용, 손동기, “AHP 기법을 활용한 정보시스템 개발 프로젝트 위험요인 평가에 관한 탐색적 연구,” 정보시스템연구, 제15권, 제2호, 2006, pp. 77-93.

[5] 최철림, 송영재, “Fuzzy AHP를 적용한 클라우드 컴퓨팅 환경에서 보안 속성의 상대적 중요도 평가,” 한국항행학회 논문지, 제15권, 제6호, 2011, pp. 1098-1103.

[6] 한국인터넷진흥원, “2010 국내 정보보안산업 실태조사,” 2010.

[7] Bellman, R.E. and Zadeh, L.A., "Decision-Making in a Fuzzy Environment", Management Science, Vol.17, No.4, 1970, pp. 21-31.

[8] Buckley, J.J. (1985). "Ranking Alternatives using Fuzzy Numbers," Fuzzy Sets Systems, Vol.15, No.1, pp. 21-31.

[9] Chang, D.Y., "Application of the Extent Analysis Method on Fuzzy AHP," European Journal of Operational Research, Vol.95, 1996, pp. 649-655.

[10] Chen, M.K. and Wang, S.C., (2010). "The Critical Factors of Success for Information Service Industry in Developing Interantional Market: Using Analytic Hierarchy Process (AHP) Approach," Expert Systems with Applications, Vol.37, pp. 694-704.

[11] Cheng, C.H., "Evaluating Naval Tactical Missile Systems by Fuzzy AHP based on the Grade Value of Membership Function," European Journal of Operational Research, Vol.96, 1996, pp. 343-350.

[12] Dubios, D. and Prade, H. (1982). "A Class of Fuzzy Measures based on Triangular Norms," International Journal of General Systems, Vol.8, pp. 43-61.

[13] Saaty, T.L., The Analytic Hierarchy Process. New York, McGraw-Hill, 1980.

[14] Zadeh, L.A., (1965). "Fuzzy set," Information and Control, Vol.8, No.3, pp. 338-353.

[15] Zhang, Y., Deng, X., Wei, D. and Deng, Y. (2012). "Assessment of E-Commerce Security using AHP and Evidential Reasoning," Expert Systems with Applications, Vol.39, pp. 3611-3623.

[16] Zhu, K.J., Jing, Y. and Chang, D.Y. (1999). "A Discussion on Extent Analysis Method and Application of Fuzzy AHP," European Journal of Operational Research, Vol.116, pp. 450-456.

저 자 소 개

류 시 욱

부산대학교 산업공학과 학사, 석사, 박사 취득. 현재 한중대학교 공과대학 공학부 교수로 재직.
관심분야 : 퍼지 의사결정, SCM, TRIZ, TOC, 식스 시그마, 철도 안전 등

주소: 강원도 동해시 지양길 200, 한중대학교 공학부

허 덕 규

한남대학교 대학원 컴퓨터공학과 석사, 박사학위 취득. 현재 한중대학교 공과대학 공학부 교수로 재직.
관심분야 : 시스템 시뮬레이션, 디지털 워터마킹, 퍼지 시스템, DEVe'S 등

주소: 강원도 동해시 지양길 200, 한중대학교 공학부