AHP-퍼지적분을 이용한 침입감내 시스템 도입 적절성 평가를 위한 정량적 평가방법 연구

(A Suitability Evaluation Method for Quantitative Assessment of Intrusion Tolerant System using AHP-Fuzzy Integral)

유 광 진 † 이 재 욱 † 배 성 재 † 조 재 익 † 문 종 섭 ††
(Kwangjin Yu) (Jaewook Lee) (Seongjae Bae) (Jaeik Cho) (Jongsub Moon)

요 약 침입감내 시스템은 오류에 의한 고장이나 악의적인 공격상황 하에서도 일정시간 필수적인 서비스를 지속시켜주는 정보보호체계로써, 국가 정보통신 기반구조·금융·국방분야 등에서 중요성이 증대되고 있다. 그러나 각 기관 및 조직에 적합한 시스템을 도입하기 위한 객관적인 평가 기준과 방법 연구가 미진한 실정이다. 이에 본 논문에서는 침입감내 시스템의 특성과 비용적 측면까지 고려한 평가항목을 정의하고, Analytic Hierarchy Process(AHP : 계층분석적 의사결정) 기법과 t-준노름 퍼지적분을 이용하여 평가자 주관성에 의한 평가오류를 감소시킬 수 있는 정량적 평가방법을 제안한다.

키워드 : 계층분석적 의사결정, 퍼지적분, 침입감내시스템

Abstract Intrusion tolerant system enables essential services to maintain for a period of time under system failure, malicious attacks and is gaining more importance in national defense, communication infrastructure, and financial sector. However, few objective evaluation criteria for companies and agencies to introduce an appropriate system are available. This paper proposes a suitability evaluation method, using Analytic hierarchy process and fuzzy integral, for intrusion tolerant system, along with evaluation criteria which considers the characteristics and costs of systems in addition to other factors.

Key words : AHP, Fuzzy integral, Intrusion tolerant system

1. 서 론

침입감내 시스템은 결함허용 기술과 침입차단, 탐지기술 등의 정보보호 기술들이 결합된 계층적 정보보호 개념으로, 물리적·시스템적 고장발생이나 공격자의 침입이 성공한 경우에도 시스템의 중요 서비스를 일정시간 지속시키는 것을 목표로 한다[1]. 최근 국내외에서는 다수의 침입감내 기술 관련 연구가 진행되고 있으며 미국과 유럽이 주도하고 있다. 미국 The Defense Advanced Research Projects Agency(DARPA)에서는 Hierarchical Adaptive Control of Quality of service for Intrusion Tolerance(HACQIT), Scalable Intrusion Tolerance Architecture(SITAR), Intrusion tolerance by Unpredictable Adaptation(ITUA) 등의 연구를 완료하였으며, 유럽 Information Society Technology(IST)에서는 Malicious and Accidental Fault Tolerance and Information Assurance(MAFTIA) 프로젝트를 완료하였다[2,3]. 그리고 국내에서는 한국정보보호진흥원(KISA) 주관의 DNS, DHCP 침입감내 시스템 연구가 완료되었다.

국가 정보통신 기반구조, 금융, 국방분야 등의 정보통신망은 어떠한 상황에서도 필수 서비스를 제공해야 하므로 침입감내 기술의 적용은 중요하다고 볼 수 있다.

· 이 연구에 참여한 연구자(의 일부)는 '2단계 BK21사업'의 지원비를 받았음

† 학생회원 : 고려대학교 정보경영공학전문대학원
remong2@korea.ac.kr
cakel@korea.ac.kr
baeseongjae@korea.ac.kr
chojaeik@korea.ac.kr
†† 정 회 원 : 고려대학교 정보경영공학전문대학원 교수
jsmoon@korea.ac.kr

논문접수 : 2008년 8월 7일
심사완료 : 2008년 12월 15일

정보과학회논문지: 시스템 및 이론 제36권 제2호(2009.4)

하지만 각 기관 및 조직에 요구되는 침입감내 시스템을 선택하는 것은 어려운 작업이며, 이를 지원할 객관적인 평가 기준과 평가 방법이 부족하다. 각국은 정보보호시스템의 신뢰성, 비밀성, 무결성을 보증하여 사용자가 보안요구수준에 부합하는 정보보호시스템을 선택할 수 있도록 보안성 평가·인증제도[4]를 시행하고 있으며, 국가 및 사설 테스트 전문기관을 중심으로 정보보호시스템의 성능수준을 평가하고 있다[5]. 그러나 정보보호시스템의 도입은 시스템의 보안성이나 성능뿐 아니라 관리적·비용적 측면까지 고려되어야 하지만 이에 대한 평가 방법 연구는 미흡한 실정이다.

본 논문에서는 도입하고자 하는 정보보호시스템이 해당 조직의 정보보호 환경과 적합한지와 향후 운영에 따른 관리적, 비용적 부분을 고려한 종합평가를 '적절성 평가'로 정의한다[6]. 이에 침입감내 시스템 적절성 평가를 위해 침입감내 시스템의 특성을 고려한 평가항목을 도출하고, 정량적 평가를 위해 AHP를 통해 평가항목의 가중치를 측정한 후 퍼지적분을 적용한 평가 방법을 제시하고자 한다[7].

본 논문은 총 5장으로 구성된다. 2장에서는 국내외 정보보호시스템 평가방법 연구현황과 AHP, 퍼지적분에 대해 기술하고, 3장에서는 침입감내 시스템의 주요 특성을 반영한 평가항목 도출과 AHP를 이용한 평가항목 가중치 측정 및 퍼지이론을 적용한 평가방법을 제시한다. 4장에서는 단순 가중치를 적용한 평가방법과 제시된 평가방법을 비교하며, 5장에서는 결론을 서술하도록 하겠다.

2. 관련연구

2.1 국내외 정보보호시스템 평가 방법 연구현황

일반적으로 정보보호시스템 평가는 보안성 평가 또는 성능 평가를 의미하며, 적절성 평가에 대한 연구는 미진하다. 기관이나 기업들은 정보보호시스템 도입시 적절성 평가를 위해 임의의 평가항목을 작성하고 가중치를 부여하여 각 항목별 평가치에 가중치를 곱하여 더하는 가중치 평가방법을 주로 사용한다. n개의 평가항목에 대한 가중치를 ω, 평가치를 E라고 할 때 가중치 평가방법에 의한 평가결과 R은 식 (1)과 같으며, 평가 대상중 최대 결과치(R_{max})를 기록한 시스템을 도입대상으로 선택한다.

$$R = \sum_{i=1}^{n} w_i E_i \quad (1)$$

2.2 AHP

AHP는 1970년대 초반 T. L. Saaty에 의하여 개발된 것으로, 의사결정의 계층구조를 이루고 있는 요소간의 쌍대비교(pairwise comparison)를 통하여 평가자의 지식, 경험 및 직관을 포착하는 의사결정방법론이다[7]. AHP는 여러 주관적 요소와 객관적 요소에 대한 고려가 가능하고 평가항목간 우열 정량화가 편리한 이점이 있다. AHP는 다음의 네 단계에 따라 수행된다.

2.2.1 의사결정계층(decision hierarchy) 설정

첫 번째 단계로 상호 관련되어 있는 의사결정 사항들을 계층화하여, 최상층에 가장 포괄적인 의사결정 목적을 배치하고, 그 다음 계층에 의사결정에 영향을 미치는 요소들을 배치한다.

2.2.2 의사결정 요소들 간의 쌍대비교 수행

두 번째 단계에서는 평가자가 각 계층내 요소들에 대한 비교우위를 결정한다. 상위계층의 목표를 달성하기 위한 하위 요소들을 각 요소별 쌍대비교하여 표 1을 기준으로 행렬을 구성한다.

표 1 요소간 쌍대비교 척도

비교 기준	척도
A와 B가 비슷(equal importance)	1
A가 B보다 약간 중요(moderate importance)	3
A가 B보다 상당히 중요(strong importance)	5
A가 B보다 매우 중요(very strong importance)	7
A가 B보다 극히 중요(extreme importance)	9
2, 4, 6, 8은 위 값들의 중간값으로 적용	

2.2.3 각 요소의 상대적 중요도 계산

쌍대비교 행렬($mat_{(pairwise)}$)로부터 상대적 중요도를 계산하는 방법에는 산술평균법, 기하평균법, 최소자승법, 고유벡터법 등 여러 계산법이 있으며, 사용목적에 따라 적절한 계산법을 선택하여 상대적 중요도(ω)와 일치성 측도들의 평균값(λ)을 계산한다.

$$\lambda = mean(mat_{(pairwise)} \times mat_{(w)} / w_i) \quad (2)$$

2.2.4 쌍대비교 행렬의 일치성 확인

평가항목이 늘어나는 경우 쌍대비교 과정에서 모든 판단이 완벽하게 객관적 일치성을 유지하는 것은 불가능하다. 따라서 행렬의 일치성을 확인하는 것은 측정된 중요도의 사용가치를 판단하는 필수과정이다. Saaty는 일치성 지수(Consistency Index : CI)와, 일치성 비율(Consistency Ratio : CR)을 일치성 확인의 준거로 제시하였다. 일치성 비율 계산을 위한 임의지수(Random Index : RI)는 Oak Ridge 연구실에서 제시한 것을 이용하며, CI와 CR이 0.1 이하면 일치성이 있는 것으로

표 2 차수별 임의지수 표

n	2	3	4	5	6	7	8	9	10
RI	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.51

판단하고 그렇지 않을 경우 쌍대비교를 재실시하여 일치성을 재확인한다[7].

$$CI = \frac{\lambda - n}{n-1},\ CR = \frac{CI}{RI} \tag{3}$$

2.3 퍼지적분

2.3.1 $\varnothing_s$변환을 이용한 퍼지측도(fuzzy measure) 계산

어느 원소가 여러 개의 집합(crisp set)중에 임의의 집합에 소속될 때, 한 원소가 어느 집합에 속하는가에 대한 애매성(ambiguity)을 나타내는 척도를 퍼지측도라 한다. 퍼지측도는 애매한 대상을 주관적으로 계량할 때의 척도로써 유한의 전체집합 X, 임의의 A, B는 X의 부분집합, $P(X)$는 X의 멱집합이라고 할 때, 다음의 성질을 만족하여야 한다.

[공리 1] $g(\varnothing)=0, g(X)=1$ (경계조건)

[공리 2] $\forall A, B \in P(X)$

$A \subseteq B$이면, $g(A) \le g(B)$이다. (단조성)

본 논문에서는 퍼지측도 계산을 위해 평가자의 주관적 감성에 기초한 퍼지측도 할당방법인 $\varnothing_s$변환을 이용하도록 하겠다[8].

$$\varnothing_s : [0,1] \rightarrow s = [0, +\infty] \tag{4}$$

$$\varnothing_s(u) = \begin{cases} [u] & s=0 \\ u & s=1 \\ 1-[1-u] & s=+\infty \\ (s^u-1)/(s-1) & \text{기타} \end{cases} \tag{5}$$

$$\text{단, } [u] = \begin{cases} 1 & 0 < u \le 1 \\ 0 & u = 0 \end{cases} \tag{6}$$

$$s = ((1/\xi)-1)^2$$

따라서 퍼지측도는 다음과 같이 수식화 할 수 있다.

$$\mu(E) = \varnothing_s\left(\sum_{x \in E} w_x\right) \tag{7}$$

여기서 ω는 AHP법에서 구한 상대적 중요도와 동일하고, 상호작용계수 ξ의 값은 평가항목간의 결합관계가 비관적인가($\xi \le 0.5$), 낙관적인가($\xi \ge 0.5$)를 결정하는 [0,1] 사이의 상수이다. 예를 들어 평가자가 비관적인 평가를 하는 경우($\xi=0$) 식 (6)과 식 (7)에 의해 퍼지측도치는 모두 0으로 산출되어 종합평가치의 경우 평가치 중 가장 작은 값에 의해 결정되며, 낙관적인 평가를 하는 경우($\xi=1$) 퍼지측도치는 1로 산출되어 종합평가치는 평가치 중 가장 큰 값에 의해 결정되게 된다[9].

2.3.2 t-준노름 퍼지적분을 이용한 평가

Suarez와 Gill은 t-준노름(seminorm)과 t-준코노름(semiconorm) 두 작용소를 사용하여 두 개의 퍼지적분족을 정의하였다. 즉, 준노름 퍼지적분은 Sugeno 퍼지적분을 확장한 개념이기도 하다[10,11]. t-준노름에 의해 정의된 준노름 퍼지적분의 이론적 성질은 다음과 같다.

t-준노름은 다음의 두 가지 조건을 만족하는 함수

$\top : [0,1] \times [0,1] \rightarrow [0,1]$이다.

[공리 3] $x \in [0,1]$인 각각의 x값에 대하여,

$$\top(x,1) = \top(1,x) = x \quad \text{(경계조건)}$$

[공리 4] 만약 $x_1, x_2, x_3, x_4 \in [0,1]$인 경우

$x_1 \le x_3, x_2 \le x_4$일 때

$\top(x_1, x_2) \le \top(x_3, x_4)$이 성립한다.

(단조성)

t-준노름 함수는 다음과 같이 나타낼 수 있다.

$$\top_1(x,y) = x \wedge y \tag{8}$$

$$\top_2(x,y) = xy \tag{9}$$

$$\top_3(x,y) = 0 \vee (x+y-1) \tag{10}$$

위의 $\top$를 t-준노름이라고 가정하면 $L^0(X)$의 원소인 모든 h에 대하여, 집합 A상의 h의 준노름 퍼지적분은 다음과 같이 정의된다.

$$\int_A h \top g = \sup_{a \in [0,1]} \top(a, g(A \cap H_a)) \tag{11}$$

3. 제안하는 평가방법

3.1 침입감내 시스템 적절성 평가 수행절차

침입감내 시스템 적절성 평가는 다음의 5단계를 거쳐 수행된다.

Step 1 : 침입감내 시스템의 특성과 도입기관의 요구사항을 반영한 평가항목 도출

Step 2 : 쌍대비교를 통한 평가항목의 상대적 중요도(ω) 산출 및 일치성(CI, CR) 확인

Step 3 : 상대적 중요도(ω)와 상호작용계수(ξ)를 이용하여 퍼지측도($\mu(\cdot)$) 산출

Step 4 : 각 항목별 평가결과를 토대로 퍼지평가치 $h(\cdot)$를 산출

Step 5 : t-준노름 퍼지적분을 수행하여 종합평가 결과를 산출

3.2 평가항목 도출

적절성 평가를 위해서는 우선 도입기관의 요구사항이 반영된 평가항목을 작성하여야 한다. 그러나 각 기관별 요구사항과 도입조건들이 상이하고, 일반적인 정보보호 시스템 평가방법론에서 제시하는 평가항목은 본 요건들을 충족시키기에 부족하다.

이에 본 절에서는 침입감내시스템 적절성 평가를 위한 평가기준을 정의하고 해당기준을 바탕으로 침입감내 시스템의 특성과 각 도입기관의 공통 요구사항을 반영한 평가항목을 도출하도록 하겠다.

3.2.1 평가기준 .

침입감내시스템 적절성 평가기준 설정을 위해 기존 정보보호시스템 평가관련 연구[12]를 분석하여 평가분야를 크게 기술 분야, 관리 분야, 비용 분야로 구분하였다. 기술 분야에서는 시스템 자체의 필수 기능 구현여부와 성능수준, 안전성과 확장성에 관련된 사항을 포함하고,

관리 분야에서는 시스템의 구축 및 운영에 관련된 내용을 검토한다. 또한 비용 분야에서는 시스템 도입 및 유지·보수 비용에 대한 평가기준을 제시한다. 본 연구에서는 이를 바탕으로 8가지의 평가기준을 작성하여 표 3에 기술하였다.

3.2.2 평가항목

작성된 평가기준을 토대로 세부적인 평가항목을 도출하였다. 기술 분야에서는 침입감내시스템의 특성인 중복시스템(Redundant system), Security 보장, 결함회피 등을 반영하여 평가항목을 작성하였으며, 관리 분야에서는 설치와 관리·운용 및 교육에 관련된 내용을 평가항목으로 도출하였다. 마지막으로 비용 분야에서는 초기 도입비용을 포함하여 구축 및 유지·보수에 소요되는 비용을 평가항목에 포함하였다. 본 연구에서는 표 3의 평가항목을 기준으로 평가방법을 서술토록 하겠다.

3.3 AHP를 이용한 평가항목의 상대적 중요도 측정

적절성 평가를 위한 평가항목을 결정한 후에 항목간 쌍대비교를 수행한다. 쌍대비교 행렬을 바탕으로 고유벡터법이나 산술평균법 등의 계산법을 이용하여 상대적 중요도를 계산한다. 쌍대비교 결과 검증을 위해 식 (3)을 통해 일치성 지수를 확인하고, 일치성 지수와 일치성 비율이 0.1 이하면 다음 단계로 진행한다.

3.4 퍼지적분을 이용한 침입감내 시스템 평가

상대적 중요도 산출 후 식 (5), (6), (7)을 이용하여 퍼지측도를 계산하고, 퍼지측도치와 퍼지평가치를 t-준노름 퍼지적분으로 계산하여 종합결과를 도출한다.

4. 실험을 통한 평가방법 비교

본 장에서는 제안된 평가방법과 가중치 평가방법을 비교하여, 침입감내 시스템 적절성 평가방법과 평가결과간 상관관계를 살펴보도록 하겠다. 평가방법 비교를 위해 각 항목의 평가치를 0(미흡)에서 10(우수) 구간에서 부여하였고 본 연구에서는 표 4를 A, B, C 회사의 침입감내 시스템의 기능적 측면 평가치로 가정하였다.

4.1 AHP-퍼지적분을 이용한 침입감내 시스템 평가

4.1.1 평가항목 도출

조직이나 기관에 적절한 침입감내 시스템을 도입하기 위해서는 본 논문에서 제시한 평가항목과 각 조직특성에 따른 항목들을 추가하여 평가항목을 구성한다. 본 연구에서는 평가방법 비교를 위해 평가항목의 일부인 기능적 측면의 침입예방 기능, 침입탐지 기능, 서비스 보장 기능을 평가항목으로 가정한다.

4.1.2 평가항목의 상대적 중요도(ω) 산출 및 일치성 (CI, CR) 확인

표 3 침입감내 시스템 평가 항목

평가기준	목적	평가항목
기능적 측면 (Capability)	중심 기능에 대한 기능의 다양성과 깊이 평가	침입예방(Prevention) 기능
		침입탐지(Detection) 기능
		서비스 보장(Availability) 기능
성능적 측면 (Performance)	기능 수행시의 정확성, 속도, 자원 사용량 등의 성능 평가	결함(Fault), 오류(Error), 고장(Failure) 식별 기능
		침입감내 시스템 신뢰도(중복성)
		고장 발생시 서비스 지속 가능시간
		결함, 오류, 고장 발생시 성능 저하율
		시스템 오류 처리(대치 또는 복구) 시간
		시스템 결함 치료 시간
안전성 측면 (Robustness)	시스템 자체 안전성에 대한 평가	취약성 부분
		오용성 부분
		보안성 부분(인증, 접근제어, 감사, 암호화)
관리적 측면 (Manageability)	대규모 환경에서 침입감내 시스템 설치, 설정, 제어 기능 등의 평가	설치 및 제거
		시스템 관리
		시스템 지원
연동성 측면 (Interoperability)	표준 파일 포맷이나 네트워크 연결 등을 통한 다른 시스템 구성 요소와의 연동 기능 평가	표준 파일 포맷 적용 여부
		표준 프로토콜 적용 여부
		연동시 데이터 누락(loss)율
확장성 측면 (Scalability)	대규모 환경으로 확장될 수 있도록 제공하는 기능 평가	확장시 시스템 변경요소
편이성 측면 (Usability)	중심 기능에 대해 배우고, 사용하고, 수정함에 있어서의 평가	사용자 인터페이스
		교육 및 기술자문
비용적 측면 (Cost)	가용한 예산범위내에서 요구수준의 시스템 도입·운영 가능여부 평가	초기 도입비용
		유지·보수 비용

표 4 A, B, C사의 침입감내 시스템 기능적 측면 평가치

회사	침입예방 기능(x_1)	침입탐지 기능(x_2)	서비스 보장 기능(x_3)
A사	8.700	2.600	3.400
B사	5.300	5.500	6.000
C사	2.500	8.200	9.100

평가자는 표 3을 기준으로 평가항목간 상대적 중요도를 쌍대비교표로 작성한 후 산술평균법을 이용하여 상대적 중요도(ω)와 일치성 측도들의 평균치(λ)를 계산한다.

위에서 구한 λ를 식 (3)에 대입하여 CI와 CR을 구한다.

$$CI = \frac{\lambda - n}{n-1} = \frac{3.101-3}{3-1} = 0.051$$

$$CR = \frac{CI}{RI} = \frac{0.051}{0.58} = 0.087$$

계산결과 CI = 0.051, CR = 0.087 < 0.1로 일치성을 보이므로 쌍대비교는 적절히 수행된 것으로 판단한다.

4.1.3 상대적 중요도(ω)와 상호작용계수(ξ)를 이용하여 퍼지측도($\mu(\cdot)$) 산출

상호작용계수는 평가항목간 상관관계의 결합관계를 [0, 1] 공간의 수치로 표현한 것으로, 상관관계가 적을수록 '0'으로, 반대의 경우는 '1'로 결정한다. 상호작용계수는 평가자가 각 항목간 상관관계를 판단한 것의 평균치를 사용하며, 본 연구에서는 ξ = 0.3으로 가정한다. 이제 AHP를 통해 산출한 표 5의 상대적 중요도와 상호작용계수를 식 (4), (5), (6), (7)에 대입하여 계산하면 표 6의 퍼지측도를 산출할 수 있다.

4.1.4 항목별 퍼지평가치 h(·) 산출

표 4의 평가치를 기준으로 각 항목의 가장 높은 값을 1.000으로 하여 [0, 1] 공간의 상대값으로 치환하면 표 7의 퍼지평가치가 얻어진다.

4.1.5 t-준노름 퍼지적분을 이용하여 종합평가 결과를 산출

표 7 기능적 측면의 퍼지평가치

회사	h(x_1)	h(x_2)	h(x_3)
A사	1.000	0.317	0.374
B사	0.609	0.671	0.659
C사	0.287	1.000	1.000

표 7의 퍼지평가치를 통해 A회사의 $\top_1$, $\top_2$, $\top_3$ 퍼지적분을 수행하면 다음과 같다.

$$\int h_A \top_1 g = \top_1[h_A(\{x_2\}),\ g(\{x_1, x_2, x_3\})] \vee \top_1[h_A(\{x_3\}),\ g(\{x_1, x_3\})] \vee \top_1[h_A(\{x_1\}),\ g(\{x_1\})] = 0.374$$

$$\int h_A \top_2 g = \top_2[h_A(\{x_2\}),\ g(\{x_1, x_2, x_3\})] \vee \top_2[h_A(\{x_3\}),\ g(\{x_1, x_3\})] \vee \top_2[h_A(\{x_1\}),\ g(\{x_1\})] = 0.371$$

$$\int h_A \top_3 g = \top_3[h_A(\{x_2\}),\ g(\{x_1, x_2, x_3\})] \vee \top_3[h_A(\{x_3\}),\ g(\{x_1, x_3\})] \vee \top_3[h_A(\{x_1\}),\ g(\{x_1\})] = 0.371$$

같은 방법으로 B, C사의 퍼지적분을 수행하면 표 8과 같은 종합평가 결과가 도출된다.

4.2 가중치에 의한 침입감내 시스템 평가

표 4의 기능적 측면 평가치와 표 5의 상대적 중요도를 식 (1)에 대입하여 계산하면 표 9의 A, B, C사의 침입감내 시스템을 평가결과를 얻을 수 있다.

4.3 평가결과 비교

표 8의 퍼지적분을 적용한 평가결과에서는 B사, A사, C사 순으로 평가된 반면 표 9의 가중치를 적용한 가법적 종합평가 결과에서는 A사, B사, C사 순으로 각 1, 2위의 순위가 역전되었다. 이는 평가과정 중 개입된 평가자의 주관적 판단의 보정유무에 따른 결과로, 그림 1의 a, b 영역에 해당한다. 예를 들면, 평가자에 따라 a 구

표 5 기능적 측면 평가항목의 쌍대비교 행렬 및 상대적 중요도

	x_1	x_2	x_3	중요도	일치성 측도
x_1	1	3	4	0.575	3.417
x_2	1/3	1	3	0.311	2.712
x_3	1/4	1/3	1	0.114	3.175
					λ=3.101

표 6 기능적 측면의 퍼지측도

$\mu(\cdot)$	퍼지측도치	$\mu(\cdot)$	퍼지측도치	$\mu(\cdot)$	퍼지측도치
$\mu(x_1)$	0.371	$\mu(x_1, x_2)$	0.785	$\mu(x_1, x_2, x_3)$	1.000
$\mu(x_2)$	0.156	$\mu(x_2, x_3)$	0.237	-	-
$\mu(x_3)$	0.048	$\mu(x_3, x_1)$	0.498	-	-

표 8 기능적 측면의 t-준노름 퍼지적분 결과

회사	$\int h \top_1 g$	$\int h \top_2 g$	$\int h \top_3 g$	순위
A사	0.374	0.371	0.371	2
B사	0.609	0.609	0.609	1
C사	0.287	0.287	0.287	3

표 9 기능적 측면의 가중치 평가 결과

평가항목 / 가중치 / 회사	x_1	x_2	x_3	평가결과	순위
	0.575	0.311	0.114		
A사	8.700	2.600	3.400	6.198	1
B사	5.300	5.500	6.000	5.442	2
C사	2.500	8.200	9.100	5.026	3

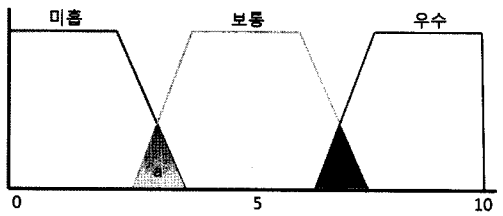

그림 1 평가자의 주관적 판단 개입 영역

간에서 긍정적인 평가자는 미흡하다고 판단하면서 높은 평가치를 부여하고, 반대로 부정적인 평가자는 보통이라고 판단하면서도 긍정적 평가자보다 낮은 평가치를 부여할 수 있다. 평가치가 정량적으로 산출되는 경우 즉 a, b 영역이 최소화 되는 경우에는 가중치를 적용한 가법적 평가방법으로 평가가 가능하다. 그러나 대부분의 평가는 평가항목간 상호연계성을 지니고 있으며, 평가자체도 평가자의 주관이 개입되는 경우가 많다. 이러한 경우 평가항목간 상호관계와 평가자의 주관적 견해를 반영하여 평가하는 본 연구의 제안방법이 보다 정확한 판단을 내려준다고 볼 수 있다.

5. 결 론

정보통신망에 대한 의존도가 심화되면서, 역기능에 의한 피해도 확대되고 있다. 이에 각 기관과 업체들은 각종 정보보호 시스템을 도입하였고 이를 위한, 성능평가 방법이 다수 제시되었다. 그러나 도입 기관별 환경적, 재무적, 업무적 특성을 고려한 평가방법에 대한 제안은 미흡하였다.

본 논문은 도입대상 정보보호시스템이 해당 조직의 정보보호 환경에 적합한지와 향후 운영에 따른 관리적, 비용적 부분 등을 고려한 종합평가를 '적절성 평가'로 정의한 후, 침입감내 시스템 도입기관의 특성을 고려한 기술적·관리적·비용적 측면의 평가항목을 도출하였다. 그리고 AHP를 이용하여 각 평가항목의 상대적 중요도를 산출하고 t-준노름 퍼지적분을 통해 퍼지측도와 퍼지평가치를 계산하여 정량적 평가를 수행하였다.

기존의 단순 가중치를 이용한 평가방법이 가중치 설정 단계부터 평가수행시까지 평가자 주관 개입에 의한 평가오류의 한계를 지니고 있는 반면 AHP-퍼지적분을 이용한 평가방법은 수학적 연산을 통해 상대적 중요도를 산출하고, 일치도를 확인하여 평가오류를 방지하였다. 또한 퍼지적분을 통해 평가치에 내재된 주관적 견해를 보정하여 일반적인 가법적 평가에 비해 합리적인 평가결과를 얻었다. 이에 AHP-퍼지적분을 이용한 적절성 평가방법은 정성적 평가항목이 포함된 의사결정 과정에서 도입기관의 요구사항에 최적화된 효과적이고 정량적 평가결과를 도출해낸다고 할 수 있다.

참 고 문 헌

[1] 최중섭, 이경구, 김홍근, "침입감내기술 연구 동향", 정보보호학회지, 제13권, 제1호, pp. 56-63, 2003.
[2] 박현도, 김수, 이희조, 임채태, 원유재, "BcN에서의 침입감내를 위한 네트워크 디자인 연구", 정보과학회논문지, 제34권, 제5호, pp. 305-315, 2007.
[3] James Reynolds, James Just, Ed Lawson, Larry Clough, Ryan Maglich, "The Design and Implementation of an Intrusion Tolerant System," Proc. IEEE DSN, 2002.
[4] ISO/IEC 15408, "Information technology - Security techniques - Evaluation criteria for IT security," 1999.
[5] 정태인, 김진호, 신용녀, 박희운, "정보보호제품 성능시험 동향 분석", 정보보호학회지, 제12권, 제5호, pp. 62-69, 2002.
[6] 최상수, 김소연, 이강수, "정보보호시스템 적절성 평가 방법론", 보안공학연구논문지, 제2권, 제1호, 2005.
[7] T. L. Saaty, The AHP: Planning, Priority Setting, Resource Allocation, McGraw-Hill, 1980.

[8] Eiichiro TAKAHAGI, "On Identification Methods of λ-Fuzzy Measures using Weights and λ," 日本ファジィ學會誌, Vol.12, No.5, pp. 73-84, 2000.
[9] Eiichiro TAKAHAGI, "Fuzzy Measure Choquet Integral Model as an Aggregation Operator," 日本經營數學會誌, Vol.22, No.2, pp. 85-98, 2000.
[10] 김미혜, 이순석, "Fuzzy Measures Defined by the Semi - Normed Fuzzy Integrals", 한국콘텐츠학회논문지, 제2권, 제4호, pp. 99-103, 2002.
[11] 김미혜, "퍼지적분을 이용한 침입탐지시스템 평가방법", 정보보호학회논문지, 제14권, 제2호, pp. 113-121, 2004.
[12] 유신근, 이남훈, 심영철, 김홍근, 김기현, "침입탐지시스템 평가 기준에 관한 연구", 한국정보과학회 학술발표논문집, 제26권, 제2호, pp. 300-302, 1999.

유 광 진
2001년 3월 공군사관학교 산업공학과 졸업. 2008년 3월~현재 고려대학교 정보경영공학전문대학원 석사과정. 관심분야는 시스템 보안, 네트워크 보안, 데이터 마이닝

이 재 욱
2008년 2월 고려대학교 전자 및 정보공학부 졸업. 2008년 8월~현재 고려대학교 정보경영공학과 석사과정. 관심분야는 악성 코드, VoIP

배 성 재
2005년 8월 서울시립대학교 컴퓨터통계학과 졸업. 2007년 9월~현재 고려대학교 정보경영공학과 석사과정. 관심분야는 침입탐지, 악성 코드, 데이터 마이닝

조 재 익
2005년 2월 동국대학교 컴퓨터학과 졸업. 2008년 2월 고려대학교 정보경영공학전문대학원 석사 졸업. 2008년 3월~현재 고려대학교 정보경영공학전문대학원 박사과정. 관심분야는 네트워크 모델링, 패턴인식

문 종 섭
1981년~1985년 금성 통신 연구소 연구원. 1991년 Illinois Institute of technology 졸업(전산학 박사). 1993년~현재 고려대학교 전자 및 정보공학부 교수
관심분야는 생체인식, 침입탐지, 운영체제