집합이론을 적용한 위험분석 방법론 연구

방영환° 최승 장세진 이강수
(*) 한남대학교 컴퓨터공학과
{bangyhdar°, schoi, dar}@se.hannam.ac.kr, gslee@eve.hannam.ac.kr

A Study on Risk Analysis Method by Using The Theory of Sets

Younhwna Bang°, Seung Choi, Se-jin Chang, Gangsoo Lee
Dept. of Computer Engineering. Hannam University

요 약

정보통신 인프라를 운영하고 있는 조직은 주요 정보자산의 위협, 취약성 및 위험 분석·평가에 많은 관심이 고조되고 있다. 위험 분석·평가는 다수의 평가자(전문지식을 가진 평가자)의 주관적인 관점이 많이 작용하며 평가결과들 간에 평가 결과에 대한 문제를 야기 시킬 수 있다. 따라서 다수의 평가자들의 평가의견을 보다 효과적으로 결합(적용)할 수 있는 절차 및 방법이 요구된다.
본 논문에서는 분산 환경에서 다수의 평가자들의 평가의견을 집합개념 중 서로 다른 집합끼리의 합을 구하는 절차에서 착안 하여 이를 적용한 실용적인 위험분석 방법론을 제시한다.

1. 서 론

국내 대부분의 조직은 정보시스템의 환경의 급속한 변화로 인해서 정보자산에 대한 위험을 인식하고, 이에 대한 적절한 관리를 필요로 한다. 또한 정보통신 인프라를 운영하고 있는 조직은 주요 정보자산의 위협, 취약성 및 위험 분석·평가에 많은 관심이 고조되고 있다.
정보시스템은 정보보호관리 하에서 운용되어야 하며, 정보보호 관리는 위험관리를 포함하고 있다. 위험관리는 위험분석과 보안대책단계로 구성되며, 위험분석은 파악과 측정단계를 포함하고 있다. 최근의 위험분석 프로세스는 자산기반 모델이 주류를 이루고 있으며, 사실상의 표준 모델로 자리 잡고 있다.[1]

반면, 자산기반 위험분석에서의 평가활동들인 자산가액, 자산수준, 위협수준, 취약성수준, 대책비용 산정은 매우 주관적이며 평가자간의 편차가 심한 정성적인 방법에 의해 평가한다.[2, 3] 따라서, 다수의 평가자간의 서로 다른 의견을 하나로 조정하고 절충하는 절차가 필요하다. 집단의 합의가 필요한 문제를 해결하기 위하여, 기존의 위험분석 방법에서는 협의회(workshop)을 통하여 토의를 하고 있다. 하지만, 협의회와 같이 얼굴을 맞대고 토의하는 면대면 의견조정 과정에는 소수의 의견이 무시되는 다수의 횡포, 권위 있는 어느 한 사람의 발언의 영향, 사전조율에 의한 집단 역학의 약점, 한번 취한 입장의 고수 등 심리적으로 바람직하지 못한 효과가 작용하게 된다.[5] 또한 위험 분석·평가는 다수의 평가자가 많은 인터뷰 대상자를 만나고, 많은 자산들을 실사해야하는 시간관리가 중요한 프로젝트이다. 그런데 의견조정을 위해서 매 평가 때마다 시간을 정하여 평가시간을 할애하는 것은 시간낭비를 초래하여 이는 평가비용 증가와 직결된다.

본 논문은 2장에서 위험 분석·평가 시 다수의 평가자의 의견을 합리적으로 결합하는 메커니즘을 제시한다. 이는 기본적으로 집합개념을 이용한 것으로서 서로 다른 집합끼리의 합을 구하는 절차에서 착안한 것이다. 3장에서는 이를 적용한 위험분석 방법론을 제시하고, 마지막으로 4장은 결론 및 향후 진행과제를 기술한다.

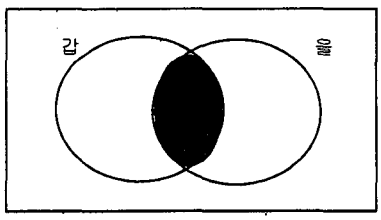
※ 본 연구는 과학기술부 지역협력연구사업
(과제번호 : R12-2003 -004-01001-0)지원으로 수행되었음

2. 위험 분석·평가 의견조정 방법

2.1 개요

위험 분석·평가는 다수의 평가자(전문지식을 가진 평가자)의 주관적인 관점이 많이 작용하며 평가결과들 간에 평가 결과에 대한 문제를 야기 시킬 수 있다. 따라서 다수의 평가자들의 평가의견을 보다 효과적으로 결합(적용)할 수 있는 절차 및 방법이 요구된다.

이러한 문제점을 해결 위해여 다수의 평가자들의 의견을 보다 효과적으로 결합할 수 있는 다음과 같은 알고리즘을 제시한다. 이는 기본적으로 집합개념을 이용한 것으로 원래의 기본아이디어는 서로 다른 집합끼리의 합을 구하는 절차에 착안한 것이다.[1]



<그림 1>두 평가자의 의견집합

즉 갑이라는 평가자와 을이라는 평가자가 있다고 했을 때 이들의 평가의견을 <그림 1>과 같이 집합으로 표현되어 있다고 이때 이들 두 평가자의 의견을 편견 없이 결합하는 방법은 다음과 같은 두 집합의 합을 구하는 식을 이용 할 수 있다.

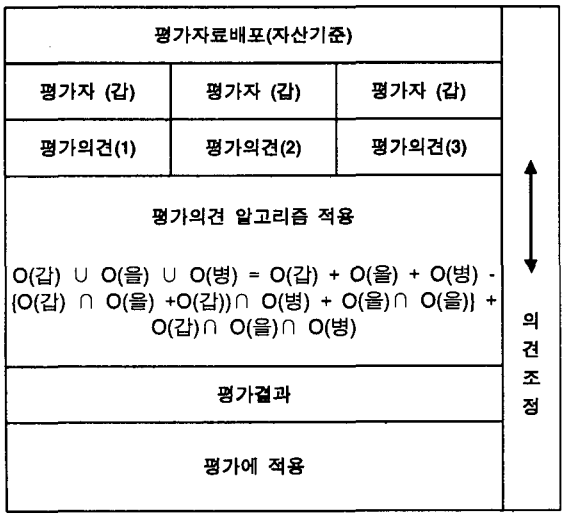
$$O(갑) \cup O(을) = O(갑) + O(을) - \{O(갑) \cap O(을)\}$$

여기서 O(갑)은 갑의 고유한 의견 (또는 평가 결과)
O(갑) ∩ O(을)은 갑과 을의 공통 평가의견을 의미한다.
이는 갑과 을의 의견을 결합하려면 각각의 의견을 더하되, 중복을 피하기 위하여 갑과 을의 공통의견을 빼준다는 것이다, 만약 평가자가 갑, 을, 병 세 사람이 있다면 이들의 평가의견의 합하기 위해서는 다음과 같은 식을 사용하면 될 것이다.

O(갑) ∪ O(을) ∪ O(병) = O(갑) + O(을) + O(병) - {O(갑) ∩ O(을) +O(갑))∩ O(병) + O(을)∩ O(을)} + O(갑)∩ O(을)∩ O(병)

따라서 이와 같은 집합의 합을 구하는 연산과정은 임의의 K명의 평가자의 의견을 결합할 때에도 일반화하여 적용될 수 있다.
우선 전체적인 의견조정 알고리즘의 흐름은 다음과 같다.

1단계 : 평가자료 배포(평가자 3명일 경우로 가정)
2단계 : 각 평가자가 작성한 평가의견(평가결과) 작성
3단계 : 의견조정 알고리즘 적용()
4단계 : 최종결과정리



<그림 2>의견조정 수행과정의 워크플로

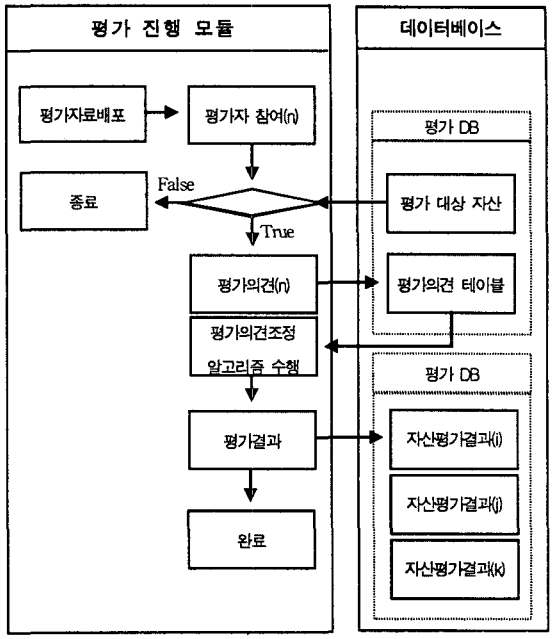
<그림 2>은 의견조정 수행과정의 워크플로를 보여주고 있다. 각 평가자들은 익명성을 유지하면서 다른 평가자의 평가결과를 참고할 수 있으며 추가적인 평가의견을 제시 할 수 있다.

2.2 기존 위험분석시 평가 의견조정의 문제점

위험분석에서의 기존 방법은 다음과 같은 해결해야할 문제점들을 가지고 있다.
① 위험분석은 여러명의 평가자가 많은 인터뷰 대상자를 만나고, 많은 자산들을 실사해야하는 시간관리가 중요한 프로젝트이다. 그런데 의견조정을 위해서 매 평가 때마다 시간을 정하여 평가시간을 할애하는 것은 시간낭비를 초래하며 이는 평가비용 증가와 직결된다.
② 또한, 의견조정관리를 위한 인력 및 자원이 추가로 소요된다.
③ 평가자들의 의견조정과정은 차후 분쟁의 소지가 있기 때문에 평가내역이 관리되어야한다.
④ 평가관리를 사람이 직접 하게 되면 평가내용의 기밀성 보장에 어려움이 있다.

본 논문에서는 집합이론을 이용한 평가의견에 대한 합의점을 쉽게 제시할 수 있다. 평가의견조정 모듈은 위험분석 도구의 각 평가 모듈에서 평가자들 간의 의견을 조정하기 위하여 공통적으로 사용할 수 있는 모듈이다.

<그림 3>는 평가 의견조정 알고리즘을 UML(Unified Modeling Language)의 활동다이어그램으로 표현하였으며 사용 데이터베이스를 추가설명하고 있다.



<그림 3>의견조정알고리즘 모듈

3. 위험분석 방법론

위험분석 방법론을 설계하기 위해서는 우선적으로 사용자가 이해하기 쉽고, 사용하기에 편리하기 위한 방법으로 다음과 같이 제시한다.

- 국내 일반적인 조직에서 활용 가능한 평가기준제시
- 위험분석 방법론에서 각 평가기준의 복잡한 판단수치를 3단계로 제시
- 사용자가 사용하기 쉬운 인터페이스제공

우선 위험분석을 적용하는 가장 기초적인 단위는 개별자산이며, 여러 종류의 개별 자산들이 하나의 정보시스템을 구성한다. 한 조직에서 여러 정보시스템을 운영하고 있고, 시스템의 경계가 명확하게 분리되지 않는 것이 일반적 이므로, 단위 시스템을 어떻게 구분할 것인지에 대한 기준이 필요하다. 분류기준은 업무 프로세스의 관점, 시스템의 물리적 구분, 해당 시스템에 대한 접근통제의 범위의관점등 있다.
본 방법론은 시스템에 대한 기준을 업무 프로세스의 관점에서 구분을 하고 개발을 수행하였다. 전체적인 절차는 계획수립, 자산평가, 위험평가, 및 보안대책 제시 단계로 구성되고, 각 단계는 다수의 프로세스를 , 각 프로세스는 여러 개의 타스크로 구성되었다.

3.1 위험분석 프로세스

표 1은 본 논문에서 제안하는 시스템 기반의 위험분석 방법의 프로세스를 보여주고 있다.

[표 1] 위험분석 프로세스

단계	활동	의견조정 방법적용
계획단계	- 예비조사 및 실사 - 상위 위험분석 수행(자료조사, 설문) - 분석범위 설정 및 평가팀 구성	
자산평가	- 시스템 프로파일 작성(응용시스템별 자산식별) - 자산 프로파일 작성 및 평가 - 기존 계획된 보안통제 식별	○
위험평가	- 위협 프로파일 작성 - 취약점 프로파일 작성 - 취약점수준 평가 - 위험수준 평가	○
보안대책 분석	- 보안대책 프로파일 작성 - 위험감소 평가 - 보안대책 선택 - 잔여위험 분석	○

■ 계획단계

예비조사 및 실사 및 상위 위험분석 수행(자료조사, 설문)활동을 하며, 분석범위 설정 및 평가팀 구성 한다.

■ 자산평가

시스템 프로파일 작성(응용시스템별 자산식별), 자산 프로파일 작성 및 평가, 기존 계획된 보안통제 식별들을 수행한다.

- 시스템 분석 : 비즈니스 프로세스와 관련된 핵심 시스템을 파악하고 하위의 노드들인 개별자산을 파악한다.

■ 위험평가

- 위협 : 위협을 설정하여 위협에 의한 손실가치(AV)와 통계적인 연간발생빈도(ARO)를 파악한다.
- 취약점 분석 : 취약점분석은 물리적/관리적 측면과 기술적 측면으로 나누어 분석한다. 물리적/관리적 측면은 시스템 수준에서 통제 절차와 이행수준을 분석하고 기술적 측면은 취약점 도구 및 CVE 기반의 취약점 데이터베이스를 이용하여 평가자가 분석한다. 취약점은 각각 3등급의 스케일을 가지는 평가척도를 이용하여 분석한다. 취약점분석을 통해 시스템의 위협에 대한 노출지수(EF)를 산정한다.
- 위험 분석 : 위험분석에서는 앞서의 프로세스에서 산정한 AV, ARO 및 EF를 곱하여 ALE를 산출한다.

■ 보안대책 분석

- 보안대책 : 보안대책은 취약점과 1:1로 평가자가 분석하여 제시한다. 제시된 보안대책이 모두 수행되었다는 전제하에 노출지수를 다시 산정하여 감소된 위험을 평가한다. 평가자는 위험감소 분석 결과를 조직의 관리자에게 제공하여, 실제 적용할 보안대책을 비용대비 효과분석을 통하여 선택한다. 마지막으로 보안대책 후 잔여위험을 분석한다.

■ 위험수준 산정 방법

정량적인 평가방법을 위험수준을 다음과 같은 공식을 사용한다.

$$ALE = AV \times ARO \times EF$$

- 손실가치(AV)와 연간발생빈도(ARO)의 산정은 객관적인 결과를 도출하기 위해 지식베이스를 사용하거나 전문평가자들의 재량에 많이 의존하게 된다.(본 방법론에서는 지식베이스의 부재시 평가결과의 객관성을 위해 의견조정방법을 사용하여 전문평가자들의 의견을 조율한다.)
- 노출수준(EF) : 노출수준(EF) 은 위협에 속해있는 취약점의 수준을 조합하여 산정한다. 여러 취약점의 수준을 조합하여 하나의 노출수준을 도출할 때 어려운 점은 취약점 전체개수의 무제한성으로 인해 총합이나 평균값으로 노출수준을 계상할 때 현실적이지 않은 결과가 도출된다는 것이다.

본 논문에서는 이러한 문제점들의 제약을 적게 받으면서 합리적인 결과를 도출해 낼 수 있다

3.2 특징

본 논문에서 제안하는 방법론의 특징은 다음과 같다.

- 의견조정방법를 적용한 시스템 단위의 정량적인 평가
- 프로세스 타입은 자산기반의 ATVR타입
- 위험감소분석을 통한 보안대책분석이 가능하다.

4. 결론

본 논문은 다수의 위험분석 평가자들에 의해 수행되는 위험분석에서 평가자들 간의 의견조정방법을 적용하여 평가자들의 평가의견을 보다 효과적으로 결합(적용)할 수 있는 절차 및 방법을 제시하였다. 의견조정방법은 면대면 의견조정 방법의 단점인 다수의 횡포, 권위 있는 어느 한 사람의 발언의 영향, 사전조율에 의한 집단 역학의 약점, 한번 취한 입장의 고수 등 심리적으로 바람직하지 못한 효과를 지양하는 장점이 있다.

향후 자산, 취약성, 위협, 그리고 보안대책의 세부적인 분류와 구성요소들 간의 상호 관련성에 대해서는 좀 더 추가적인 연구가 필요하다 또한 제시된 방법론에 대한 자동화도구의 구현에 대한 연구를 향후 과제로 남긴다.

참고문헌

[1] 박현우 외 5명 "정보시스템을 위한 범용 웹기반 위험분석 프로세스", 한국디지털컨텐츠학회지, 3권 1호, 2002.12
[2] British Standards Institution(BSI), BS-7799, 1999
[3] TTAS, "공공정보시스템 보안을 위한 위험분석 표준 - 개념과 모델", TTAS.KO-12.007, 1998
[4] 이건창, 퍼지인식도를 이용한 웹기반 조직지식 획득에 관련 연구, 한국지능정보시스템학회지, 제2권 2호,1999.12
[5]이종성, 델파이 방법, 한국학술정보(주), 2001.
[6] Custer, et al., "The Modified Delphi Technique - A rotational Modification", Journal of Vocational and Technical Education, Vol. 15, No.2, 1998
[7] B. Ludwig and W. Ohio, "Predicting the Future: Have you considered using the Delphi Methodology", Journal of Extension, Vol. 35, No.5, Oct. 1997
[8] B. Boehm, "Software Engineering Economics", Prentice-Hall, 1981.
[9] Will Ozier, "Risk Analysis and Assessment", Information Security Management Handbook(4'th Ed.), CRC Press, 2000.