시스템 단위의 정량적 위험분석 도구 개발

박현우°, 방영환, 이강수
한남대학교 컴퓨터공학과
{tankboy°, bangyh, gslee}@se.hannam.ac.kr

A Development of Quantitative Risk Analysis Tool for System Unit

Hyunwoo Park° Younghawn Bang Gangsoo Lee
Department of Computer Engineering, Hannam University

요 약

정보시스템의 위험을 관리하기 위해서는 위험을 식별 및 측정하는 위험분석이 선행되어야 한다. 본 논문에서는 위험수준 평가, 보안대책에 의한 위험감소 및 잔여위험 분석이 가능한 정량적 위험분석 방법을 제안하며, 이를 적용한 위험분석 도구를 설계 및 구현하여 보인다.

1. 서 론

현대 사회가 정보화 사회로 일컬어 질만큼 정보시스템의 중요성이 강조된다. 이에 걸맞게 정보시스템의 구축은 획기적으로 증가하였다. 그러나 이에 대한 체계적인 보안관리가 제대로 이루어지지 않아서 많은 문제들이 발생하고 있다. 정보시스템의 보안관리를 위해서는 관리대상에 대한 정확한 파악과 평가가 이루어져야 한다. 이를 위해서, 다른 여러 분야와 마찬가지로 정보시스템 보안관리 분야에서도 위험을 파악하고 평가하여 관리하는 위험기반 관리방법이 주로 사용되고 있다.

일반적으로 위험관리는 위험분석단계와 보안대책 수행 단계로 이루어져 있다. 위험분석은 자산, 위협, 취약성 등의 엔티티로 위험을 형상화하여 파악하고 이를 평가척도에 매핑하고 조합하여 수준을 평가하는 과정이다. 보안대책 수행은 분석된 위험에 대하여 회피, 수용, 감소 등의 보안대책을 수행하는 단계이다.

정보시스템 위험분석의 성공요인으로써 ①합리적인 프로세스, ②분석자(평가자)의 재량, ③도구의 사용 등을 꼽을 수 있다. 위험분석은 많은 인력과 자원이 소요되는 대형 프로젝트의 개념이므로 합리적인 프로세스나 평가자를 지원하는 도구의 사용이 필수적이다.

시대적 요구에 따라, 국내외적으로 위험분석 방법론 및 도구들에 대한 연구가 다양하게 이루어지고 있다. 하지만 기존의 방법론들은 구현을 통해 실제 조직에 적용하여 평가하기에는 미흡한 면이 있으며, 도구들 또한 프로젝트 관리적인 측면과 여러 명의 평가자들이 다중으로 평가할 수 있는 부분이 미흡하다.

이에 따라, 본 논문에서는 평가대상 조직의 책임자가 이해할 수 있는 실제적인 평가결과를 도출해 낼 수 있는 시스템 기반의 정량적인 위험분석 방법론을 제안하였으며, 이를 효과적으로 지원하는 도구를 설계 및 구현하였다.

본 논문의 구성은 다음과 같다. 2장에서 기존의 위험분석 방법 및 도구를 비교분석한다. 3장에서 정보시스템을 위한 정량적 위험분석방법론을 제안한다. 4장에서는 이를 따르는 위험분석도구를 설계 및 구현해 보이고 5장에서 결론을 맺는다.

2. 기존의 위험분석 방법 및 도구 비교분석

위험분석 방법의 특징을 결정짓는 요인은 일반적으로 다음과 같은 3가지가 있다.

- 정량평가인가, 정성평가인가?
- 평가대상 단위는 어떠한가?
- 평가프로세스는 어떠한가?

본 장에서는 지금까지 연구된 위험분석 방법 및 도구들을 상기와 같은 요인을 기준으로 비교분석 한다.

2.1 평가방법(정량 VS 정성)

위험분석 방법론 크게 정량평가와 정성평가로 나눌 수 있다. 정량평가는 자산의 가치(AV, Asset Value), 위협의 발생율(ARO, Annualized Rate of Occurrence), 노출지수(EF, Exposure Factor) 등을 계량적인 수치로 추정할 수 있다는 가정을 기반으로하는 평가방법이다.[1]

정량평가에서 어려운 문제는 위협의 ARO와 AV를 추정할 수 있는 데이터가 부족하다는 점이다. 특히 정보 자산의 가용성의 상실로 오는 손실에 대한 추정은 매우 어려운 문제이기 때문에 대규모 정보시스템의 정량적 위험분석은 상당한 기간이 소요된다.

이러한 문제를 해결하기 위하여 주관적인 평가척도를 사용하여 위험을 등급화하는 정성적 위험분석 방법이 등장하였다. 정성적 위험분석 방법은 자산, 위협, 취약성 등의 엔티티 들을 각각의 평가척도에 매핑하여 등급화한 후 이들을 조합하여 위험수준을 산정하는 방법이다. 하지만 정성적 위험분석 방법은 주관적 분석의 객관성 결여와 보안대책 예산에 관한 의사결정을 위한 계량적 분석의 결여라는 문제를 지니고 있다.

표 1은 기존의 위험분석 방법 및 도구들의 평가방법을 보인다.

[표 1] 기존의 위험분석방법에서의 평가방법 비교

구분	평가방법	구분	평가방법
ISO/IEC-13335-3부[2]	정성	CORA[12]	정량/정성
BS-7799[3]	정성	JANBER[13]	정성
카나다 CSE[4]	정성	RANK-IT[14]	정량/정성
TTAS.KO-12.007[5]	정성/정량	Risk Alert[15]	정성
OCTAVE[6]	정성	RiskCALC[16]	정량
CRAMM[7]	정성	RiskPAC[17]	정량/정성
auditMASTERPLAN[8]	정성	Risk Ranking Advisor[18]	정성
BDSS[9]	정량/정성	SecMOD[19]	정성
The Buddy System[10]	정량/정성	PRAM[20]	정성
CONTROL-IT[11]	정성	HAWK[21]	정량

[표 2] 평가방법의 장·단점 비교

구분	정량적	정성적
평가기간	길다	상대적으로 짧다
객관성	객관적	주관적
난이도	어렵다	쉽다
평가 근거	지식베이스	평가기준

표 2는 정량적 위험분석 방법과 정량적 위험분석을 비교하고 있다. 평가기간면에서 정량평가는 금전적 가치를 깊이있게 분석해야하는 반면 정성평가는 평가기준에 대략적인 값을 사상하는 작업이므로 상대적으로 짧다. 객관성 측면에서는 앞장에서 언급한 바와 같이, 정량평가는 통계자료나 지식 베이스를 기반으로한 값을 이용하므로 정성평가보다 객관적이다.

[표 3] 위험분석 방법 및 도구 비교

구분	평가단위	위험감소분석 여부	비고
ISO/IEC-13335-3부	개별자산	×	방법론
BS-7799	개별자산	×	방법론
카나다 CSE	개별자산	○	방법론
TTAS.KO-12.007	개별자산	○	방법론
OCTAVE	시스템	×	방법론
CRAMM	시스템	×	도구
auditMASTERPLAN	·	×	도구
BDSS	시스템	○	도구
The Buddy System	시스템	○	도구
CONTROL-IT	·	×	도구
CORA	개별자산	×	도구
JANBER	·	×	도구
RANK-IT	시스템	×	도구
Risk Alert	·	○	도구
RiskCALC	·	×	도구
RiskPAC	·	×	도구
Risk Ranking Advisor	·	×	도구
SecMOD	시스템	×	도구
PRAM	개별자산	×	도구
HAWK	시스템	×	도구

2.2 평가대상 단위자산

위험분석은 일반적으로 자산평가로부터 시작되므로 평가방법에서 평가단위의 설정은 매우 중요하다.

표 3에서 알 수 있듯이 위험분석 방법에서 평가단위는 크게 개별자산단위와 시스템단위로 나눌 수 있다. 평가대상 단위 설정방법에 따라 각각 표 4와 같은 장·단점을 갖는다.

[표 4] 평가단위에 따른 위험분석 방법 비교

구분	개별자산 단위	시스템 단위
손실가치 산정(AV)	어려움	상대적으로 쉬움
위협분석	어려움	상대적으로 쉬움
취약성분석	기술적 취약성분석이 상대적으로 쉬움	관리적 취약성분석이 상대적으로 쉬움
보안대책분석	기술적 보안대책이 상대적으로 쉬움	관리적 보안대책이 상대적으로 쉬움

자산가치 산정에서 개별자산 단위로 평가하는 경우 개별자산이 업무에 미치는 영향을 판단하기가 쉽지 않으므로, 상대적으로 업무 프로세스와 매핑이 쉬운 시스템 단위의 평가보다 어려운 점이 있다. 위협분석은 위협 도메인의 설정에 따라 차이가 있지만 업무와 관련된 위협을 설정할 때에는 개별자산 단위보다 시스템 단위 평가가 상대적으로 쉽다. 취약성분석에서는 기술적 취약성은 개별자산 단위 평가가 쉬운 반면 관리적/물리적 취약성 분석은 시스템 단위의 평가가 상대적으로 쉽다. 보안대책분석은 취약성분석과 맥을 같이한다.

2.3 평가프로세스

평가프로세스는 ①위협과 취약성의 처리 차원, ②보안대책분석 처리 차원 등의 2가지 측면에서 살펴 볼 필요가 있다. ①은 위협분석시에 다루어야할 개념인 자산(A), 위협(T), 취약성(V)중에서 위협과 취약성의 구분이 애매하여, 이들을 처리하는 관점을 기준으로 구분하는 방법이다. ②는 보안대책 선택시 비용효과 분석부분의 처리를 기준으로 구분하는 방법이다.

2.3.1 위협과 취약성 관점

AVR, AVTR, ATVR 및 ATR타입은 "자산기반" 위험분석 방법이라 할 수 있으며, AVR과 ATR은 위협과 취약성간의 애매성을 배제하기 위해 한가지만을 택하고 있다. 특히, 위험분석 방법중 지명도가 높은 카나다의 CSE와 SEI의 OCTAVE는 이 부류에 속한다. 또한, AVTR과 ATVR타입의 경우에도 위협과 취약성중 한가지만을 집중적으로 분석하고있다.[22]

[표 5] 위협과 취약성의 처리 차원에서 프로세스 비교

모델 형태	해당 방법
AVR 형태 (자산→취약성→위험)	ISO/IEC TR 13335-3부, OCTAVE
AVTR 형태 (자산→취약성→위협→위험)	BDSS, HWAK
ATVR 형태 (자산→위협→취약성→위험)	FIPP-65, FIPS-191, CRAMM, 팬타, PRAM, CISSP, Buddy System
ATR 형태 (자산→위협→위험)	CSE
TVR 형태 (위협→취약성→위험)	SP-800-30, SSE-CMM, GAO1, GAO3, 에너지성-SRAG
TR 형태 (위협→위험)	법무성-SRAG
자료 없음	ISO/IEC TR 13335-1부, BS-7799, Open Framework

2.3.2 보안대책분석 관점

위험관리는 위험분석과 보안대책 부분으로 구성되어 있다. 보안대책을 선정하기 위해서는 보안대책에 의한 위험감소분석이 선행되어야 한다. 또한 정성평가에서는 보안대책분석시 위협척도의 감소와 대책비용간에 서로 다른 단위를 가지고 있기 때문에 어려운점이 있다. 표 3은 기존의 위험분석 방법 및 도구에서 위험감소분석 지원 여부를 보인다. 방법론에서는 구체적인 위험감소 산정에 대해서는 다루고 있지 않으며 BDSS, The Buddy System, Risk Alert 등의 도구에서 위험감소분석 기능을 제공하고 있다.

3. 시스템 단위의 정량적 위험분석 방법

3.1 위험분석 프로세스

표 6은 본 논문에서 제안하는 시스템 기반의 정량적 위험분석 방법의 프로세스를 보여주고 있다.

[표 6] 위험분석 프로세스

단계	활동
시스템 분석	시스템 프로파일 작성
	자산 프로파일 작성
	위협 프로파일 작성
취약점 분석	취약점 프로파일 작성
	취약점수준 평가
위험 분석	위험수준 평가
보안대책 분석	보안대책 프로파일 작성
	위험감소 평가
	보안대책 선택
	잔여위험 분석

- **시스템 분석**

비즈니스 프로세스와 관련된 핵심 시스템을 파악하고 하위의 노드들인 개별자산을 파악한다. 또한 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**

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 보안대책후 잔여위험을 분석한다.

3.2 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 델파이 의견조정방법을 사용하여 전문평가자들의 의견을 조율한다. 마지막으로 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 있는 그림 1와 같은 방법을 사용하였다.

P_i(i = 1, 2, 3, ... n)을 위협에 속한 취약점수준이라 하고,

P_i를 내림차순 정렬한 수열을 $\{P_i'\}$라 할 때,

$$EF = \sum_{i=1}^{n} \frac{P_i' - 3}{8}$$ 이다.

[그림 1] 노출수준 산정 공식

3.3 특징

본 논문에서 제안하는 방법론의 특징은 시스템 단위의 정량적인 평가를 하는 것이며, 프로세스 타입은 자산기반의 ATVR타입이다. 또한 위협감소분석을 통한 보안대책분석이 가능하다.

4. 위험분석도구의 설계 및 구현

4.1 개발환경

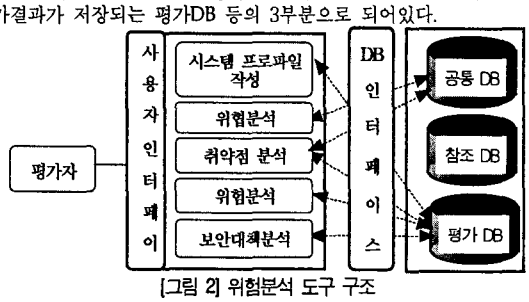
표 7은 본 논문에서 제안한 위험분석 방법을 따르는 도구의 개발환경을 보이고 있다.

[표 7] 개발환경

구분	환경
운영체제	Windows 2000 Server
개발언어(도구)	Power Script(Power Builder 9.0)
데이터베이스	MySql-3.23.52
기타	phpMyAdmin-2.4.0(웹 DB 관리 도구)

4.2 도구의 구조

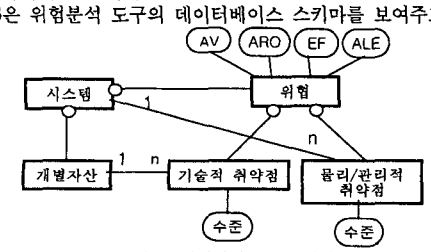
그림 2는 위험분석도구의 전체 구조를 보여주고 있다. 도구는 방법론의 프로세스를 따라 기능들이 제공되며, 데이터베이스는 보안대책목록 등을 제공하는 공통DB, 평가 프로세스 등을 제공하는 참조DB 및 평가결과가 저장되는 평가DB 등의 3부분으로 되어있다.



[그림 2] 위험분석 도구 구조

4.3 데이터베이스 스키마

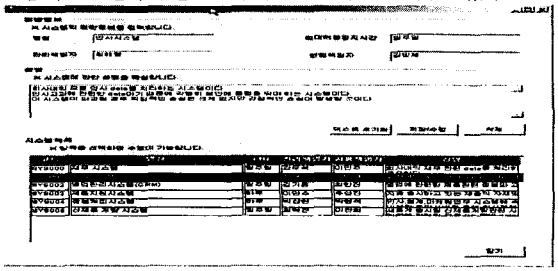
그림 3은 위험분석 도구의 데이터베이스 스키마를 보여주고 있다.



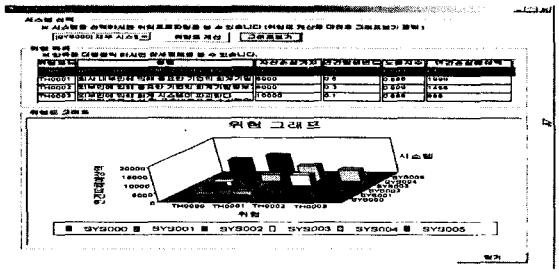
[그림 3] 데이터베이스 스키마

4.4 개발된 도구의 GUI 예

그림 4, 5는 실제 구현된 도구의 GUI 일부를 보여주고 있다.



[그림 4] 시스템 프로파일 작성 GUI



[그림 5] 위험수준 그래프 출력 GUI

5. 결론

본 논문에서는 기존의 위험분석 방법 및 도구들을 평가대상 단위자산의 범위, 평가프로세스, 보안대책분석 관점 등에서 비교분석하여 비즈니스 프로세스와 매핑이 쉬운 시스템 단위의 정량적 위험분석 방법을 제안하고 이를 지원하는 도구를 설계 및 구현하여 보였다. 본 논문에서 제안한 위험분석 방법은 ①시스템 단위의 정량적 위험분석, ②물리적/관리적 관점과 기술적 관점으로 구분하여 취약점 분석, ③ 위험감소 분석, ④보안대책의 비용대비 효과 분석 등의 특징을 가진다. 차후에는 이를 지원하는 도구의 필드 테스트를 통하여 방법론과 도구의 문제점을 보완하여 나가겠다.

참고문헌

[1] 김세헌, 정보보호 관리 및 정책, 생능출판사, 2002.
[2] ISO/IEC TR 13335, "IT 보안관리 지침", 1998.
[3] British Standards Institution(BSI), BS7799, 1999.
[4] CSE, "A Guide to Security Risk Management for IT Systems", Government of Canada, Communications Security Establishment(CSE)", 1996.
[5] TTA, "공공정보시스템 보안을 위한 위험분석 표준 - 개념과 모델", TTAS.KO-12.007, 1998. 11.
[6] OCTAVE, "OCATVE Criteria, Version 2.0", Carnegie Mellon Software Engineering Institute(2001. 12), OCATVE Method Implementation Guide Version 2.0, OCTAVE, 2001. 6, http://www.sei.cmu.edu/publications/pubweb.html.
[7] "A Practitioner's View of CRAMM", http://www.gammassl.co.uk/.
[8] auditMASTERPLAN, http://www.jebcl.com
[9] 김기윤, 나관식, 김종석, "보안관리를 위한 위협, 자산, 취약성의 분류 체계", 정보보호학회지, 6권 1호, 1995. 6.
[10] The Buddy System, http://www.buddysystem.net.
[11] CONTROL-IT, http://ourworld.compuserve.com/homepages/jerardra.
[12] CORA, http://www.ist-usa.com.
[13] JANBER, http://www.emainc.com.
[14] RANK-IT, http://ourworld.compuserve.com/homepages/jerardra.
[15] Risk Alert, http://www.jebcl.com.
[16] RiskCALC, "List of Risk Analysis, Assessment and Management Tools", http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=207.
[17] RiskPAC, http://www.csciweb.com.
[18] Risk Ranking Advisor, http://www.methodware.com.
[19] SecMOD, http://www.m-tech.ab.ca/products/secmod.
[20] 김정덕 (외), "위협 분석 도구 기초기술 개발에 관한 연구", ETRI 연구보고서, 2001.
[21] 송관호(외), "정보시스템 보안을 위한 위험분석 소프트웨어 개발" 한국전산원 연구보고서, 1997. 12.
[22] 박현우 외 5명, "정보시스템을 위한 범용 웹기반 위험분석 프로세스", 한국디지털컨텐츠학회지, 3권 1호, 2002.12