情報保護學會論文誌
第18卷 第4號, 2008. 8

사례기반 추론을 이용한 위험분석방법 연구

이 혁 로[1,2†], 안 성 진[2‡]
[1]한국과학기술정보연구원, [2]성균관대학교

A Study on Risk Analysis Methode Using Case-Based Reasoning

Hyeak-Ro Lee[1,2†], Seongjin Ahn[2‡]
[1]Korea Institute of Science and Technology Information, [2]Sungkyunkwan University

요 약

사이버 침해사고와 해킹의 위험성이 증대되고 있다. 이를 해결하기 위하여 정보보호기술중에서 보안위험분석 분야의 연구가 활발하게 이루어지고 있다. 하지만 평가를 위해서는 적지 않은 평가비용, 수개월의 평가기간, 평가 참여인원, 평가 후의 보안대책비용, 보안관리비용에 대한 부담이 클 수밖에 없다. 이에 따라, 본 논문에서는 정량평가 형태의 위험분석평가를 프로젝트단위로 관리하며, 평가기간 및 적정 평가자 선정을 위한 사례기반추론알고리즘을 이용한 위험분석방법론 제안한다.

ABSTRACT

The risk enlargement of cyber infringement and hacking is one of the latest hot issues. To solve the problem, the research for Security Risk Analysis, one of Information Security Technique, has been activating. However, the evaluation for Security Risk Analysis has many burdens; evaluation cost, long period of the performing time, participants' working delay, countermeasure cost, Security Management cost, etc. In addition, pre-existing methods have only treated Analyzing Standard and Analyzing Method, even though their scale is so large that seems like a project. the Analyzing Method have no option but to include assessors' projective opinion due to the mixture using that both qualitative and quantitative method are used for. Consequently, in this paper, we propose the Security Risk Analysis Methodology which manage the quantitative evaluation as a project and use Case-Based Reasoning Algorithm for define the period of the performing time and for select participants.

Keywords : Security Risk Analysis, Analyzing Method, Case-Based Reasoning Algorithm

Ⅰ. 서 론

정보통신 기술의 발달과 이에 따른 정보화의 추진으로, 정보시스템을 이용하는 금융, 무역, 의료, 에너지, 교육 등 사회 각 분야에서 정보화가 급속하게 진전되고 있다.

그러나 이러한 정보통신 시스템의 확대에 수반하여 지식과 정보에 대한 불법적인 침해, 불건전 정보의 유통, 사생활 침해 등의 역기능이 나타나고 있다. 따라서 이러한 역기능들에 수반될 폐해를 최소화 할 노력을 경주해야 하며, 이러한 노력을 소홀히 할 경우 바람직한 정보사회를 이룩할 수 없게 될 것이다. 정보시스템에 대한 보안관리는 위험분석평가가 선행 되어야하며, 보안위험분석은 요구되는 정보보호서비스의 취약점을 해결

접수일 : 2008년 4월 18일; 채택일 : 2008년 5월 19일
† 주저자, leehr@kisti.re.kr
‡ 교신저자, sjahn@songgang.skku.ac.kr

하고 위협으로부터 시스템을 안전하게 관리할 수 있는 최선의 방법이다[1].

하지만 기존의 위험분석에서는 수개월의 분석평가 기간과, 다수의 전문평가자가 참여하는 프로젝트 수준의 규모를 갖게 된다. 따라서 평가를 위해서는 적지 않은 평가비용, 수개월의 평가기간, 평가 참여인원, 평가 후의 보안대책비용, 보안관리비용에 대한 부담이 클 수 밖에 없다. 또한 기존의 위험분석 평가방법들의 대부분이 위험분석 평가의 규모가 프로젝트의 수준임에도 불구하고 분석기준 및 분석방법에 만을 다루고 있으며, 평가방법 또한 정성·정량 방법을 혼합하거나 분리해서 평가가 이루어지기 때문에 평가자의 주관적인 의견이 포함될 수밖에 없는 실정이다[2].

이러한 배경에서 본 논문에서는 정량평가 형태의 위험분석 평가를 프로젝트단위로 관리하며, 평가기간 및 적정 평가자 선정을 위한 사례기반추론알고리즘을 이용한 위험분석방법론을 제안한다. 본 결과는 위험분석을 수행하는 초기단계 및 진행단계에서 기존의 평가결과를 추론규칙을 통해서 제공받음으로써 위험분석 평가프로젝트 수행에 대한 가이드를 제시하고, 평가기간 및 적정 평가자 선정, 보안대책비용의 추정 등을 통해 체계적인 평가프로젝트를 성공적으로 이룰 수 있을 것이다. 본 논문의 2장에서는 기존의 연구된 위험분석 방법 및 도구들을 비교분석하고, 3장에서는 위험분석 평가 프로세스 및 위험분석도구 개발을 위한 분석엔진 중 사례기반추론알고리즘 이용한 평가엔진을 제시하며 4장에서는 이를 이용한 평가 사례연구 통해 유용성을 입증하고, 끝으로 결론을 맺는다.

Ⅱ. 관련 연구

2.1 위험분석 평가방법비교

위험분석 방법의 특징을 결정짓는 요인은 일반적으로 평가방법이다. 평가 방법으로는 정량평가와 정성평가가 있으며, 정보인프라에 대한 분석과정을 통해 단위자산을 파악하고 위험분석 평가과정을 수행한다. 위험분석 방법론은 크게 정량평가와 정성평가로 나눌 수 있다. 정량평가는 자산의 가치(AV, Asset Value), 위협의 발생률(ARO, Annualized Rate of Occurrence), 노출지수(EF, Exposure Factor) 등을 계량적인 수치로 추정할 수 있다는 가정을 기반으로 하는 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 등급화 하는 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[2]. 국내외 정보보호분야의 조사연구로 평가방법 및 보안대책적용에 대한 의사결정방법에 대한 조사결과는 [표 1]과 같다.

[표 1] 기존의 위험분석방법에서의 평가방법 비교

구 분	평가 방법	의사 결정	구 분	평가 방법	의사 결정
ISO/IEC-13335-3부	정성	없음	CORA	정량/정성	없음
BS-7799	정성	없음	JANBER	정성	없음
카나다 CSE	정성	없음	RANK-IT	정량/정성	없음
TTAS.KO-12.007	정성/정량	없음	Risk Alert	정성	없음
OCTAVE	정성	없음	RiskCALC	정량	없음
CRAMM	정성	없음	RiskPAC	정량/정성	없음
auditMASTERPLAN	정성	없음	Risk Ranking Advisor	정성	없음
BDSS	정량/정성	없음	SecMOD	정성	없음
The Buddy System	정량/정성	없음	PRAM	정성	없음
CONTROL-IT	정성	없음	HAWK	정량	없음

정성평가만을 사용하는 위험분석방법 및 도구들은 ISO/IEC-13335-3부, BS-7799, 캐나다 CSE, OCTAVE, CRAMM, auditMASTERPLAN, JANBER, Risk Alert, RiskCALC, Risk Ranking Advisor, SecMOD, PRAM, HAWK가 있으며, 정성평가와 정량평가방법을 고려한 TTAS.KO-12.007, BDSS, The Buddy System, CORA, RANK-IT, RiskPAC 등이 있다[2].

기존의 정량적 위험분석 방법과 정량적 위험분석에서는 평가 기간 면에서 정량평가는 금전적 가치를 깊이 있게 분석해야하는 반면 정성평가는 평가기준에 대략적인 값을 사상하는 작업이므로 상대적으로 짧다[3]. 객관성 측면에서는 앞장에서 언급한 바와 같이, 정량평가는 통계자료나 지식 베이스를 기반으로 한 값을 이용하므로 정성평가보다 객관적이다[4,5].

Ⅲ. 위험분석 평가방법

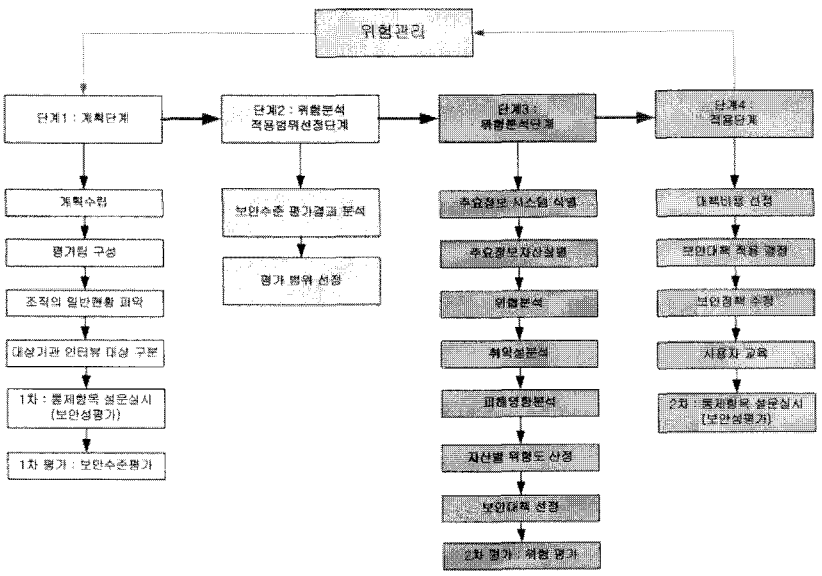
조사 연구된 표준이나 다른 많은 위험분석 방법론에서 제시하는 통제항목을 이용한 정보 보안 관리 및 보안 수준 평가, 자산식별, 위협분석, 취약성 분석, 피해영향 분석, 자산별 위험도 산정, 보안대책 구현 등을 기반으로 문제점을 분석하고 위험분석방법을 제안하고자 한다. 특히, 사례기반추론알고리즘을 통한 평과 결과의 활용 및 보안대책적용 측면, 전사적 위험분석 측면, 자산평가 측면, 프로세스 측면을 고려하였다.

3.1 위험분석 평가프로세스

평가프로세스는 평가 업무를 수행하기 위한 일련의 규칙이라 할 수 있다. 본 논문에서 제안한 평가 프로세스는 조직의 관리적, 환경적, 기술적 평가를 모두 수행할 수 있는 전사적 위험분석 평가가 가능하다. 또한 위험분석업무를 보다 효율적으로 처리하고 관리할 수 있도록 Top-down 방식으로 구성되었다. 위험분석 평가 업무에서 관리적, 환경적, 위험분석 평가는 BS7799의 일부를 이용하며, 기술적 평가 부분은 미국의 카네기멜론 대학의 OCTAVE 방법론 중 일부를 이용한다. 평가 프로세스는 전체 4단계로 진행되며, 각 단계별 평가 업무를 위한 프로세스로 구성되어 있다. 또한 평가 프로세스는 위험분석의 상위단계인 위험관리가 가능하도록 구성된 특징을 가진다.

3.2 평가프로세스의 특징

제안한 위험분석 평가프로세스는 다음과 같은 특성을 가진다. [그림 1]의 평가프로세스는 계획단계, 위험분석적용범위 선정단계, 위험분석단계, 적용단계의 4단계의 구분 된다. 1, 2단계를 상위수준평가 단계라고 하고 3, 4단계를 하위수준평가 단계로 분리하여 분석을 실시한다. 또한 평가 프로세서에 의해서 지속적인 보안관리를 할 수 있다. 상위수준에서는 상위수준 평가 프로



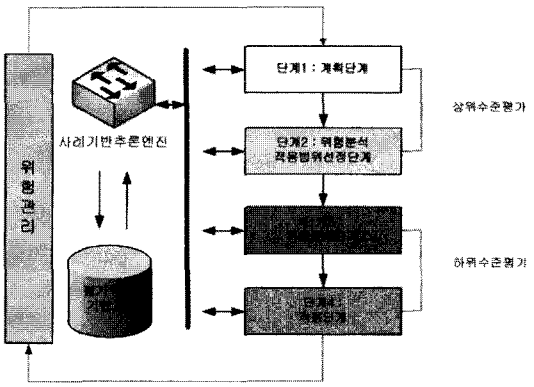
〔그림 1〕 위험분석 평가프로세스

젝트를 관리하고 BS-7799를 기반으로 한 보안관리에 관련된 설문과 인터뷰과정을 통해 평가대상기관의 보안관리에 대한 평가를 실시하고 하위수준평가는 핵심 업무를 통한 시스템을 분리하고 자산을 분석하는 방법을 이용한다. 하위분석평가 단계에서는 세부적인 평가를 실시 및 대책비용을 통한 보안대책이 결정되고 적용한다. 상위수준의 평가는 주로 통제항목을 통한 웹상에서 설문을 통해 이루어지므로, 전문적인 분석요원이 없이도 자체 분석 및 평가가 가능하다. 평가대상 조직은 정기적으로 상위수준의 평가를 실시하며 조직의 위험추이에 따라 하위평가를 실시할 수 있다. 상위수준의 평가는 평가계획을 위한 예비평가에 해당한다. 상위수준의 평가결과가 우수하다면, 노력이 많이 드는 하위수준의 평가는 유보할 수 있으므로, 조직의 보안관리 비용을 줄일 수 있을 것이다.

3.3 위험분석 프로세스와 추론엔진과의 관계

위험분석 방법 및 위험분석 도구의 대부분은 평가를 진행하는 초기 계획단계에서 다양한 평가대상기관 분석을 위한 평가사례를 제공하지 않고 있다. 하지만 본 논문의 위험분석 평가가 진행된 평가 사례를 기반으로 위험분석 계획 단계에서 평가의 범위 및 적정평가자의 구성 등과 같은 기초자료를 통한 위험분석을 진행할 수 있다. 또한 위험분석 및 보안대책 적용단계에서 평가에 대한 가이드를 제공하기 때문에 평가기간의 단축과, 객관적 평가를 유도 할 수 있다는 장점을 갖는다. [그림 2]는 시스템에 적용된 추론엔진의 역할을 개념화 하여 보여주고 있다.

특히 평가 계획단계에서 사례기반추론엔진을 이용한 평가사례를 제공은 최적의 평가 계획을 수립하여 평가결과 및 평가기간의 예측이 가능하다.



〔그림 2〕 추론엔진 적용 시스템개념도

〔표 2〕 위험분석 프로세스내용

단 계	중점사항	내 용
계획단계	관리적, 환경적 평가, 보안수준 평가	• 평가 업무를 위한 계획 및 전담반을 구성한다. • 조직의 일반현황을 파악하여 대상조직의 기관등급을 할당하고 기존의 사례기반추론 DB를 검색을 한다. • 검색된 결과를 기반으로 평가프로젝트에 대한 스케줄을 작성한다. • 대상기관의 참여자를 선별하고 인터뷰를 진행한다. • 통제항목 설문을 실시하며, 보안수준평가를 실시한다.
위험분석 적용범위 선정단계	중요 시스템 구분	• 계획단계에서 수준평가결과 및 인터뷰를 통한 보안점검 근거로 위험분석 단계의 진행 및 분석범위(중요 시스템 구분)를 결정한다. • 의견조정 시스템을 통해서 평가자의 의견을 결정 한다.
위험분석 단계	중요업무를 중심으로 시스템을 파악	• 계획단계의 분석범위를 기반으로 중요시스템을 식별한다. • 중요 정보시스템 식별 및 자산식별 • 위협 분석프로파일 작성 및 위협평가 • 취약성 프로파일 작성 및 취약성 평가 • 피해 영향 분석 • 자산별 위험도 산정 • 보안대책 생성
적용단계	보안 수준 점검 확인	• 대책비용을 기반으로 보안대책을 적용 • 사용자 교육을 실시 • 위험감소를 확인를 위한 통제항목을 통한 보안수준점검 확인 실시 • 보안관리 실시

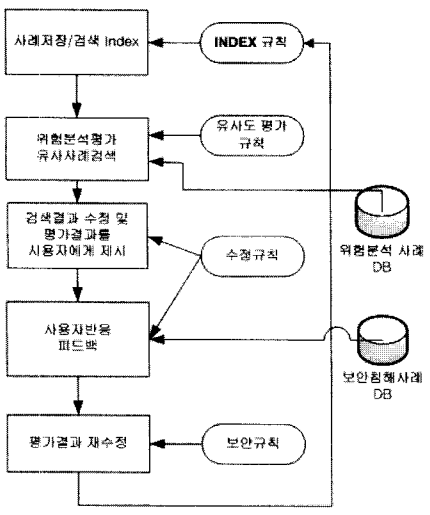
3.4 위험분석방법을 위한 사례기반추론 적용방법

3.4.1 사례에 대한 저장 및 수행 절차

평가사례 기반 추론은 위험분석 계획단계에서 기존의 평가결과를 검색규칙을 통해서 가장 검색규칙 값에 가까운 평가결과를 검색한다. 검색된 평가결과는 평가기간, 적정 평가자수, 보안점검분야, 평가결과를 사전에 예측, 할 수 있다. [그림 3]은 위험분석 평가결과에 대한 사례 저장 및 검색에 대한 수행 과정이다.

사례기반추론 알고리즘의 기능 및 처리는 대한 설명은 다음과 같다.

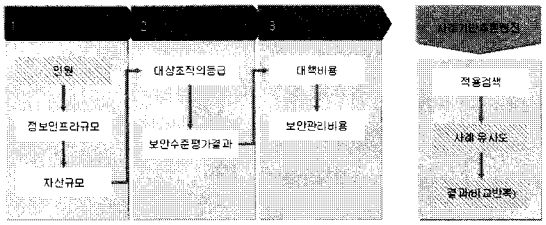
- 사용자로부터 특정조직에 대한 속성정보를 입력받으며, 입력받은 속성정보를 위험분석 대상이 되는 입력사례로 간주한다.
- 저장되어 있는 기존의 평가결과 사례 중에서, 상기 입력사례(Case)와 가장 유사도가 높은 위험분석 사례를 검색 한다.
- 검색된 가장 유사한 위험분석 사례에 대한 평가 결과를 이용하여 입력사례에 대해 정보보안수준, 평가기간, 평가자수, 핵심 업무 및 시스템, 자산 가치, 위협수준, 취약점 수준, 보안대책 적용리스트, 위험도 등을 사전에 파악 할 수 있다.
- 평가결과를 종합하여 상기 특정 조직에 대한 위험을 분석하고, 상기 정보보안 위험 분석 결과를 평가자에게 제공함으로써 평가프로젝트의 성공률을 높일 수 있다.



〔그림 3〕 사례 저장 및 검색 수행과정

3.4.2 평가사례 적용 규칙

평가사례기반추론을 위해서는 추론 규칙이 필요하며, 추론 규칙은 평가결과 검색 또는 평가 결과를 저장할 때 이용된다. 추론규칙은 대상조직의 규모, 보안수준평가결과, 상위 관리자의 보안수준 인식정도 등을 규칙별 점수로 계산하고 가장 유사한 값을 검색 결과로 사용한다.



〔그림 4〕 사례기반추론 검색 및 저장 규칙

3.4.3 사례기반 알고리즘

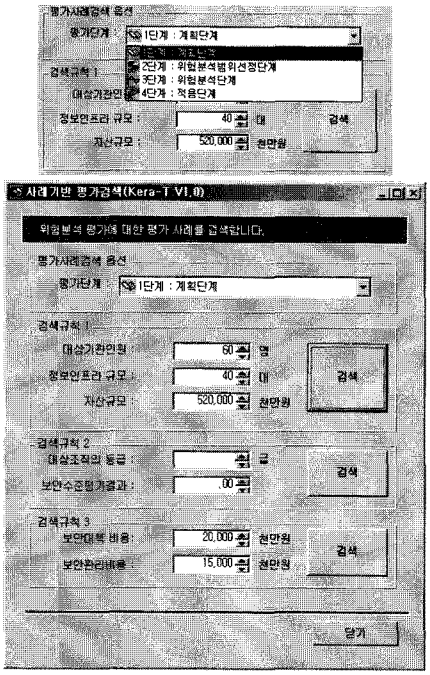
위험분석평가에 적용한 평가사례기반추론 알고리즘은 대상조직 파악을 통한 사례기반 DB로부터 규칙 값에 가장 근접한 유사사례를 확인하고, 근사 값이 존재하지 않으며 그 외의 값 중에서 근사치가 높은 것을 검색결과로 사용한다. 위험분석에 대한 평가가 종료하면, 평가결과에 대한 기존사례기반과 분석사례를 비교하여 분석사례의 변형을 위해서 도출과 검증을 통해서 새로운 사례로 저장한다.

Case Retrievel
input : 새로운 평가 *project* $F_n = \{\alpha_n, I_n, O_n, T_n\}$;
output: *select case* $C_s = \{F_n, B_s, M_s\}$;
begin
for *each case IN Case Base*
새로운 평가 대상기관 정보와 유사도를 계산.
최대 유사도를 갖는 평가사례를 선택.
선택된 평가 *case*는 $C_s = \{F_n, B_s, M_s\}$;
평가사례 F를 선택된 F_s에 대체하고
F_s를 저장한다.
end

C_i : 사례 , F_i = 보안기능, α_i = 자산평가방법,
l_i = 자산리스트, O_i = 자산수준리스트,
T_i = 기술적 제약요인, B_i = 세부평가단계도,
M_i = 세부평가(평가 설계의 결과로 설계된,
M_α={자산평가 A_α, 위협평가 T_α, 취약성평가 V_α,
가상평가결과모델 CV_α

Ⅳ. 적용 사례연구

위험분석평가 프로세스 및 사례기반추론 알고리즘을 적용한 국내실정을 고려한 위험분석도구를 설계 구현하였다. 위험분석도구는 사례기반추론엔진을 중심으로 3개의 서브시스템으로 구성된다. 평가와 관리를 담당하는 사용자를 위한 도구, 평가에 필요한 자료와 평가결과를 관리하는 데이터베이스, 웹을 통한 설문을 하고 설문결과를 관리하는 웹 설문 등의 3부분이다. 기본적으로 위험분석 수행을 위한 기능을 제공하며, 사용자들을 통제하는 RBAC기반의 사용자관리 기능, 평가자들 간의 의견을 조정할 수 있는 의견조정 기능 및 시스템관리 기능 등을 가진다. 또한 평가대상조직의 사용자들이 가진 정보를 획득하기 위한 인터뷰기능을 가진다. 데이터베이스는 평가에 사용되는 취약점목록, 보안대책 목록 등을 담당하는 공통DB, 평가결과를 관리하는 평가DB, 평가자들의 의견조정이 이루어지기 전에 평가결과를 임시로 저장하는 임시DB, 시스템관리와 관련된 데이터를 관리하는 관리DB, 평가척도 등의 참조자료를 관리하는 참조DB 등의 5부분으로 구성된다. Web Survey부분은 평가대상 조직의 정보를 수집할 때 임의의 응답자를 대상으로 웹기반 설문을 하고 설문결과를 자동으로 분석할 수 있는 기능을 제공한다. 위험분석은 많은 인력과 자원이 소요되는 대형프로젝트 단위이므로 평가프로젝트를 관리할 수 있는 기능을 지원된다. [그림 5]는 위험분석 평가 계획단계에서의 사례기반추론기능을 이용한 사용자 화면을 보여준다.



[그림 5] 평가사례 검색인터페이스

본 논문에서 제시한 사례기반추론 적용 위험분석 시스템은 위험분석 평가계획부터 보안대책 선정 및 적용까지의 기간 동안을 기존분석방법과 사례기반추론을 적용한 방법의 모의실험을 통한 성능평가를 실시하였다. 기존의 평가에 대비 평가기간 및 평가자의 적절한 선택으로 평가비용의 감소를 가질 수 있으며, 초기 사례기반추론에 대한 평가결과가 존재하지 않기 때문에 평가에 대한 참조데이터의 증가됨으로 본 결과보다 성능이 향상될 것으로 기대되며, 실제 위험분석을 위한 검증이 필요할 것으로 보인다.

Ⅴ. 결 론

본 논문에서는 기존의 위험분석평가 방법을 조사·연구하여 평가프로세스를 개발하였고, 사례기반 추론을 이용하여 사례의 재사용 및 사례적용과정 제시를 통한 위험분석 평가에 최적을 평가 프로젝트의 설계를 수립하고 위험관리를 고려한 위험분석 방법을 제안하였으며, 이를 지원하고 향상된 기능을 제공하는 위험분석도구를 설계 구현하였다. 복잡한 평가 프로젝트이나 새로운 평가대상기관의 의뢰가 있을 경우 평가계획에 대한 최적화된 설계를 통한 성공적인 평가계획을 수립할 수 있다. 위험분석 평가에 대한 성능관점에서는 평가에 대한 관리, 평가자의 평가행동에 대한 가이드, 평가기간 단축으로 인한 비용절감, 적정 평가가 선택을 통한 평가일력 최적 활용을 들 수 있다. 본 결과는 위험분석을 수행하는 초기단계 및 진행단계에서 기존의 평가결과를 추론규칙을 통해서 제공받음으로써 위험분석 평가프로젝트 수행에 대한 가이드를 제시하고, 평가기간 및 적정평가자 선정, 보안대책비용의 추정 등을 통해 체계적인 평가프로젝트를 성공적으로 이룰 수 있을 것이라 기대된다.

참고문헌

[1] Young-hwan Bang, Yoon-jung Jung, In-jung Kim, "*The Design and Development for Risk Anlysis Automaitc Tool*", LNCS 3043, Part 1,

pp.491-499, May. 2004.

[2] Hoh Peter In, Young-Gab Kim, Taek Lee, Chang-Joo Moon, Yoonjung Jung, Injung Kim, "*Security Risk Analysis Model for Information Systems*," LNCS 3398, Systems Modeling and Simulation : Theory and Applications : Third Asian Simulation Conference, AsianSim 2004.

[3] 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

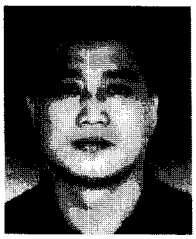
[4] CSE, "A Guide to Security Risk Management for IT Systems", Government of Canada, Communications Security Establishment(CSE)", 1996.

[5] British Standards Institution(BSI), "BS-7799", 1999.

[6] Bundesamt fur Sicherheit in der Informationstechnik, "IT Baseline Protect Manual", - Standard security safeguards, http://www.bsi.bund.de/gshb/english/menue.htm

[7] SSE-CMM, "Project, Systems Security Engineering Capability Maturity Model (SSE-CMM) - Model Description Document", V.2, http://www.sse-cmm.org, 1999. 4. 1.

〈著者紹介〉



이 혁 로 (Hyeak Ro Lee) 학생회원

1996년 : 대전산업대학교 정보통신공학과 졸업(학사)
2004년 : 공주대학교 교육정보대학원 영상매체학과 졸업(석사)
2007년 : 성균관대학교 일반대학원 교과교육학과(박사 수료)
1990~현재 : 한국과학기술정보연구원 선임연구원
<관심분야> Security Risk Analysis, Network Measurement, IPv6 Technology

안 성 진 (Seong jin Ahn) 정회원

1988년 : 성균관대학교 정보공학과(학사)
1990년 : 성균관대학교 정보공학과(석사)
1998년 : 성균관대학교 정보공학과(박사)
2000년~현재 : 성균관대학교 컴퓨터교육학과 교수
<관심분야> Network Measurement, Network Security, IPv6