실용적인 위험분석 도구의 개발

이동호(동명정보대학교)
김종기(부산대학교)

초 록

기존의 정보기술 위험분석 방법론에 대한 연구는 캐나다의 CSE에서 발표한 위험관리 방법론, 미국의 NIST에서 발표한 FIPS 65 정보보호 관리지침에서의 위험분석 방법론, 그리고 ISO/IEC JTC1 SC27의 정보보호 관리지침 등이 있으며, 위험분석 자동화 도구는 크게 국외와 국내로 나뉘어 국외의 경우 영국의 정성적 위험분석 방법론의 대표적 도구인 CRAMM, 미국의 정량적 위험분석 방법론 도구인 BDSS, 그리고 네트워크 위험분석 중심의 Expert와 같은 어플리케이션이 개발/활용 되고 있다. 한편, 국내 위험분석 자동화 도구로는 한국전산원에서 국내 최초로 개발한 위험분석 자동화 도구인 HAWK와 KAIST/팬타 시스템이 있다. 연구에서는 기존의 국내외 위험분석 방법론들의 비교분석 결과를 바탕으로, 실용적인 위험분석 방법론을 제안하고 실용적으로 위험분석을 수행하기 위한 구체적인 도구를 개발하고 구현하였다. 세부적으로 위험분석 수행의 절차와 개념적 모형화에 대한 내용을 포함하여 표준적 틀을 유지하면서 현재 국내의 실무에 적합하며 간결한 위험분석 도구를 제시하였다.

I. 서론

1. 연구의 배경과 목적

현재 많은 조직은 정보시스템 환경의 급속한 변화로 인해 정보자산에 대한 위험을 인식하고 있으며 이에 대한 적절한 관리의 필요성을 느끼고 있다. 그러나 조직이 보유하고 있는 정보자산의 위험을 분석하는 방법론과 도구들은 주로 외국에서 개발된 것으로 국내 실정을 반영하지 못하고 있으며 특히 과거 통계자료의 미비와 사용상의 복잡성 등 많은 제약이 따른다. 따라서 정보보안의 체계적인 접근이나 분석을 위한 위험분석 방법론은 보안대책의 적절성과 효과성을 보장하기 위한 연구가 필요하다.

한편, 위험분석 과정의 수행은 그 효율성의 차원에서 자동화된 도구의 사용이 그 타당성을 가진다. 다수의 자동화도구가 국내외에서 개발되어 있으나 국외에서 개발된 도구는 상황적인 특성으로 인하여 국내에서의 적용 가능성 문제가 있으며, 국내에서 개발된 도구는 방법론상의 미비점과 도구 자체의 불완전성 내포하고 있다. 또한 위험분석 도구에 대한 개념적인 접근법에 대해서 상세한 논의도 그다지 많지 않은 것으로 나타나 실제 자동화된 도구를 개발하기 위한 연구에 지침이 될 수 있는 기반연구가 절실하다.

본 연구의 목적은 다음과 같다. 먼저, 현재 적용되고 있는 위험분석방법론의 적용 편의성과 분석 결과의 합리성을 염두에 둔 실용적인 위험분석 도구의 개발을 위한 제반 공정과 개념적인 모형을 제시한다. 이 과정은 기본적으로 국내외에서 논의되고 있는 위험분석 방법론에 대한 충분한 검토과정을 통해서 공통적이고 일반화된 수준에서의 개념적 모형을 제안하고자 한다. 또한 위험분석 알고리즘을 개발하고 실용적 위험분석을 위한 프로토타입을 제시한다.

2. 연구내용 및 범위

본 연구의 구성은 먼저 현재 개발/활용되고 있는 위험분석을 위한 자동화된 도구에 대해서 논의한

다. 자동화된 도구들 중에서 국내외에서 널리 활용되고 있는 CRAMM, Expert, BDSS, HAWK, KAIST/Penta 등의 기본적인 개념과 세부적인 위험분석 공정에 대한 내용을 살펴본다. 다음으로 현재의 정보기술 환경에 적합한 자동화된 도구의 개발을 위한 지침으로 활용될 수 있는 실용적인 위험분석 방법론의 적용을 위한 프로토타입을 개발하고 개념적인 모형에 대해서 논의한다. 자동화된 위험분석 도구의 개발을 위해서 일반적인 시스템 분석 및 설계의 모형화기법으로 사용되고 있는 자료흐름도와 개체관계도를 통해서 모형화를 수행하며, 마지막으로 위험분석 도구의 프로토타입에 대한 세부적인 내용을 포함하도록 한다.

II. 위험분석 도구의 분석

이론적인 측면에서 논의되는 위험분석 방법론과 함께 위험분석 도구들은 실무적으로 활용되고 있다. 본 장에서는 지금까지 개발되었거나 활용되고 있는 국내외의 다양한 위험분석을 위한 자동화된 도구에 대해서 살펴보도록 한다.

1. CRAMM

CRAMM(CCTA Risk Analysis and Management Method)은 1985년 영국의 CCTA(정부 중앙 컴퓨터, 및 전신통화 기관)와 BIS사에 의해서 개발된 정성적 위험분석 방법론이다. 이 방법론은 영국의 정보 정보시스템 보호 위원회와 국가 위원회인 정부 정보체계 보호 위원회가 요구하는 13가지 강제적 요구사항에 부응할 수 있도록 개발되었다. CRAMM에서 수행되는 공정은 크게 세 단계로 구분할 수 있으며 방법론의 구성에 대한 세부적인 내용은 다음에서 논의된다.

1.1 단계 1

CRAMM의 1 단계는 기본통제목록 수준의 보안만을 요구하는 시스템을 식별하여 상세한 분석을 수행하는데 시간과 자원을 낭비하지 않도록 하며, 중대한 위험의 가능성이 있는 자산에 대하여 더욱 상세한 검토를 수행하도록 하는 것을 그 목적으로 한다. 1 단계는 다음의 업무(task)들로 구성된다.

- 현재의 또는 계획된 시스템에 대한 기능적 명세를 서술하고, 분석의 범위와 일정을 결정
- 분석 범위 내의 데이터, 소프트웨어 및 물리적 자산을 식별하고 자산모델을 생성
- 데이터와 물리적 자산의 가치를 평가
- 물리적 자산에 대한 데이터 자산의 의존 관계를 확인
- 약식 위협 및 취약성 평가를 수행

자산의 가치는 비밀성, 무결성, 그리고 가용성의 측면에서 12개의 세부 평가 기준을 적용하여 1에서 10 사이의 척도로 부여된다. 모든 자산이 CRAMM 평가 척도로 2 이하로 평가된 경우에 해당 시스템은 기본통제목록 수준의 보안 요구사항을 갖는 것으로 간주한다. 즉, 기본통제목록 수준의 보안만을 요구하는 시스템을 식별하는 공정의 수행을 통해서 해당되는 시스템은 2 단계의 대부분을 생략하고 3 단계에서 적절한 보안대책을 생성하도록 한다.

1.2 단계 2

2 단계에서는 시스템의 위협과 취약성을 조사하며, 다음의 업무들로 구성된다.

- 식별된 자산에 대한 위협 파악
- 위협 및 취약성 평가 수행
- 위험 수준 계산

· 위험 분석 결과 검토회의 개최

각 자산에 대하여 적용 가능한 위협은 사전에 목록화되어 있으며, 그 중에서 분석에 포함시키고자 하는 위협만을 선택할 수도 있다. 각 자산에 대한 위협과 취약성은 각 세부 위협 및 취약성에 대한 일련의 설문들을 통하여 평가되며, 결과는 취합과정을 통하여 개별 위협과 취약성을 등급화한다. 등급화에 있어서 위협 5 단계로 취약성은 3 단계로 구분한다.

1.3 단계 3

CRAMM의 3 단계는 보안대책의 선택을 중심으로 한 위험관리이다. 이 단계에서 이루어지는 주요 활동은 다음과 같다.

· 단계에서 계산된 위험 수준에 대응할 수 있는 보안대책을 보안대책 목록에서 선택
· 이미 설치되어 있거나 설치 계획이 있는 보안대책을 식별
· CRAMM에 의해서 권고된 보안대책과 기존 또는 계획된 보안대책의 차이점을 조사
· 보안대책이 요구되거나 향상이 필요한 분야에 대한 권고안을 도출

2. BDSS

BDSS(Bayesian Decision Support System)는 미국의 OPA(Ozier, Perry & Associates)에서 개발한 위험분석 도구로 보안 영향을 심각성과 발생 확률로 구분하여 고려하고 설문 응답에 대한 타당성을 신뢰 수준으로 표시하는 정량적 방법론 도구로 What-if 기능을 담고 있다. BDSS는 크게 7단계로 구성되는 데, 먼저 준비(project sizing) 단계는 위험분석의 수행을 하나의 프로젝트로 간주하고, 프로젝트의 환경 및 배경 정보, 범위, 제약조건, 목적 및 목표, 책임, 그리고 BDSS의 방법론과 접근법에 대한 일반적인 사항들을 설명한다. 이 단계에서 또한 수용 가능한 위험의 기준을 설정한다.

두 번째 단계인 자산 목록화(asset inventory) 단계에서는 조직의 업무 및 임무 기능에 연관시켜 유형 자산과 무형 자산에 대한 자산 대체 가치와 손실 비용을 결정한다. 세 번째 단계인 위협/취약성 연계(threat/vulnerability mapping) 단계에서는 취약성을 식별하고, 식별된 취약성으로 인하여 빈번하게 발생하거나 영향이 많은 위협을 파악한다. 위험 평가 및 수정(evaluate/revise risk) 단계에서는 보안대책이 고려되기 전과 후의 개별 또는 결합된 위협의 손실 비용을 표와 그래프로 분석한다. 위협을 완화하기 위한 보안대책의 효과성에 대한 분석이 또한 수행된다.

보안대책 분석(safeguard analyzer) 단계에서는 위협/취약성 연계 단계에서 식별된 위협과 취약성을 완화하기 위한 보안대책을 선택한다. 보안대책 비용/효과(safeguard cost/benefit) 단계에서는 개별 보안대책의 개발/획득 비용, 보안대책의 가용 기간 동안 발생하는 연간 유지보수 비용, 그리고 비용 효과에 대한 현재가치 분석이 수행된다.

3. Expert

Expert는 네트워크의 보호 위험을 측정, 관리하고 이에 따른 영향을 분석할 수 있게 하는 네트워크 중심의 위험 평가 분석 도구이며, 네트워크 보호 위험과 재정적 영향을 연계하여 분석함으로써, 네트워크 보호 상황에 대한 적절한 의사결정과 네트워크에 대한 기업의 정보자산을 보호할 수 있도록 한다.

3.1 네트워크 위험평가 프로세스

Expert에서 적용되는 네트워크 위험평가 프로세스는 다음과 같다.

· 자산 검색 및 등록

· 네트워크 객체에 자산 부여
· 자산 평가 정리 보고서 작성
· 위협 등록
· 위협 평가 정리 보고서 작성
· 자산 보고서를 이용한 위험 평가 수행
· 취약성 및 보호대책(Safeguard) 보고서 작성
· 보호대책 할당
· 잔존 위험 보고 수행
· 위험 감소를 위한 작업 반복

3.2 Expert의 특징

Expert를 이용한 네트워크 위험 분석 공정의 진행은 관리하고자 하는 네트워크에 존재하는 자산에 대하여 자산 종류별, 대상별 자동 및 수동 검색과, 이에 대한 취약점을 평가한다. 그리고 기본 설정되거나 분석가에 의해 등록된 해당 자산에 대한 가치와 특성에 대한 정보를 통해 위험을 평가하고, 이에 대한 여러 가지 유형의 보고서를 생성하는 단계로 이루어진다. 이는 Expert를 사용하는 사용자에 대한 전문지식을 다른 도구와는 달리 비교적 적게 요구하기 때문에, 기본 설정만으로도 상당한 수준의 위험 분석 효과를 얻을 수 있다는 장점을 제공한다.

그러나 도구의 이용측면이 네트워크에 국한되어 있다는 특징 때문에, 주요 비즈니스와 연계된 전반적인 정보시스템에 대한 평가가 이루어지지 않는다는 단점이 존재하고, 데이터베이스에 대한 적절한 갱신이 이루어지지 않을 경우, 해당 자산에 대한 가치가 필요이상으로 높게 평가될 수 있을 뿐만 아니라, 새로 적용된 IT 장비 등에 대한 가치를 적절히 반영시킬 수 없는 문제가 있다. 이에 대해, 네트워크에 대한 도구 사용자의 전문적인 지식이 요구된다.

4. HAWK

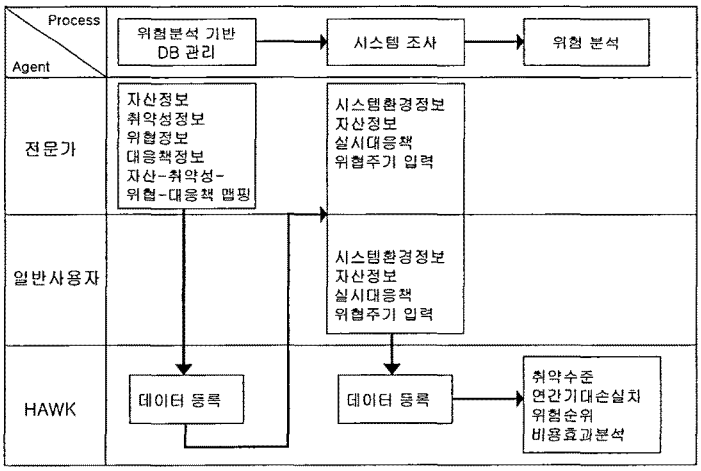
HAWK(Hankuk risk Analysis Watchout Kit)는 한국전산원 표준본부 보호기술표준팀에서 국내 최초로 개발한 위험분석 자동화 도구이다. HAWK 시스템은 크게 위험분석 기반 DB관리, 분석대상 시스템조사, 위험 분석의 절차를 수행해야 하며, 위험분석 기반 DB관리는 정보시스템에 대한 지식과 경험이 있는 전문가만이 사용할 수 있으며, 위험 분석을 위한 시스템 조사는 전문가와 일반사용자 모두 사용이 가능하다.

4.1 HAWK 공정

위험분석 기반 DB관리에서 자산, 취약성, 위협, 대응책의 정보가 입력되면, 이 데이터를 바탕으로 시스템 조사에서는 시스템환경, 자산조사, 실시대응책조사, 위협주기조사를 수행한다. HAWK는 조사된 데이터를 바탕으로 취약수준, 연간 기대 손실치, 위험순위 등을 산출하고, 비용효과 분석의 위험분석을 수행한다. 이러한 공정의 흐름은 [그림 1]과 같이 나타낼 수 있다.

4.2 HAWK의 특징

위험분석 순서는 HAWK에 의해 제공되는 기본 모듈인 Expert 모듈, Preview 모듈, Survey 모듈, Analysis 모듈의 순으로 진행되나, 분석중 이들 모듈들에 수시로 접근하여 분석이 진행될 수 있기 때문에, 상위 임의의 모듈로 접근이 가능하다. 그러나 데이터의 무결성을 위해 임의의 이전 모듈을 수행할 경우 다시 이후의 모듈을 재실행해야 하는 단점이 있다. 뿐만 아니라, HAWK를 이용한 위험분석 중 초기단계인 Expert 모듈은 일반 사용자가 사용하기는 어렵기 때문에 실제 위험분석 전문가 없이는 전체 위험분석을 실행하기 어렵다는 단점이 존재한다.



[그림 1] HAWK의 작업 흐름도

5. KAIST/Penta

KAIST/펜타 전문가시스템은 위험분석 방법론에 사례기반 추론기법(Case Based Reasoning)을 접목하고 취약성 분석도구와 연계한 위험 분석 주 프로그램 및 자료 수집을 위한 프로그램으로 이원화한 것으로, 자산 분류에 있어서 업무 프로세스(Business Process)의 고려를 시도하였다는 점을 특징으로 들 수 있다.

5.1 KAIST/Penta의 개요

KAIST/펜타 전문가시스템 역시 고려 대상 위협과 취약성이 매우 한정적이나, 여기서는 위험분석 절차의 논리적 타당성과 위험평가 기준의 객관성 측면에서 살펴본다. 전반적인 방법론의 구성은 [그림 2]와 같다.

5.2 KAIST/Penta의 특징

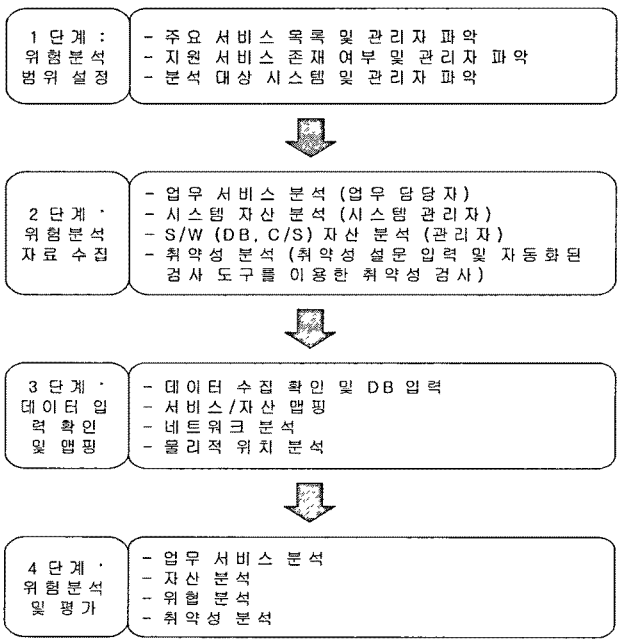
KAIST/펜타 위험분석 방법론에서는 취약성을 소프트웨어, 운영체제, 시스템(네트워크), 환경, 그리고 전체 사이트로 분류하고 각 분야마다 다수의 취약성 항목들을 식별하고 있다. 160여 개의 기술적 분야의 취약성과 200여 개의 관리적인 분야의 취약성이 열거되어 있는데, 기술적 분야의 취약성은 취약성 스캐닝 도구를 이용하여 수집함으로써 자동화를 도모하고 있다.

특정한 위협에 대한 취약성을 사전에 연계한 데이터베이스를 구축하여 취약성과 위협을 연계하고 있는데, 위협의 발생 빈도에 대한 신뢰할 만한 데이터가 존재한다면 위의 설명이 설득력이 있겠으나, 그런 자료가 존재하지 않는다는 점에서 위협의 빈도를 확률적으로 추정하는 방법이 무리가 있으며, 또한 자동으로 수집할 수 있는 취약성 데이터는 아주 제한적이므로 그런 통계적 데이터가 존재한다 하더라도 전체 위험분석 과정에서 정량적인 위협 빈도의 추정이 가지는 의미는 미미할 것이다.

자산의 가치 평가에 있어서 사례기반추론(CBR)을 이용하여 자산의 피해 금액을 정량적으로 추정한다. 여기에서 자산의 피해 금액은 운영체제, 시스템, 네트워크에 적용되고 소프트웨어와 데이터에 대하여는 비밀성, 무결성 및 가용성의 각 측면에서 가치를 추정한다. 업무 프로세스를 업무재설계(BPR)의 관점에서 정확하게 분석한다는 것은 그 자체로도 방대한 작업이므로 정보 서비스 중심으로 업무 프로세스를 분석한다. 즉, 자산의 평가 단위를 주요 서비스와 지원 서비스로 구분하고 가치의 선정 방식도 달리 한다.

위협의 평가에 있어서는 위협의 강도와 빈도를 구분하여 분석한다. 위협의 강도에 대한 일반적인 기준이 설정되어 있지 않는데, 이는 위협이 발생하는 대상 자산에 대하여 피해 규모가 동일하지 않다고 보기 때문이다. 즉, 동일한 위협이라도 대상 자산에 대하여 상이한 손실을 가져온다는 것이다. 소프트웨어의 경우에 최대 피해액의 몇 %에 해당하는가를 위협의 강도로 보며, 하드웨어의 경우에는 시스템 교체, 부품 교체 및 부품 수리로 구분하여 각각이 발생할 비율로 위협의 강도를 측정한다. 그러나 구체적인 방법과 기준은 제시되어 있지 않다.

위험 수준의 평가에 있어서는 특정한 위협이 특정한 자산에 발생하였을 때 발생하는 피해 가치를 정량적으로 평가하며, 자산의 유형에 따라 평가 방법이 달라진다. 자산을 논리적인 자산과 물리적인 자산으로 구분하고, 논리적인 자산의 경우에는 자산 가치와 위협 강도를 곱하고, 물리적인 자산의 경우에는 위협의 강도 평가에서 사용된 세 가지 경우에 발생하는 복구비용과 복구 소요 시간을 구하여 이를 평균하여 피해액을 계산한다. 정량적으로 계산된 위험 수준에 추가하여, 개별 위협과 자산의 쌍에 대하여 위협 빈도와 취약성 수준을 이용하여 정성적인 위험 수준을 평가하는데, 정량적인 위험 수준과 정성적인 위험 수준이 어떻게 결합되어 종합적인 위험 수준이 평가되는지에 대해서는 보고서에 자세히 언급되어 있지 않다.



[그림 2] KAIST/Penta 위험분석 방법론 절차

III. 실용적인 위험분석 방법론

본 연구에서 제안하는 위험분석 방법론은 사용 편의성을 우선적으로 고려하고 있으며, 자동화된 도구의 개발을 위한 지침으로 활용할 수 있는 내용을 포함하고 있다. 따라서 정보보안에 대한 어느 정도의 기초적인 지식과 위험분석의 개념에 대한 기본적인 이해가 있는 경우, 정보보안 전문가가 아니더라도 활용할 수 있도록 위험분석의 수행 절차와 평가 기준을 가급적 간단명료하게 구성하였다.

위험분석이 적용되는 가장 기초적인 단위는 개별 자산이며, 여러 종류의 개별 자산들이 하나의 정보시스템을 구성한다. 한 조직에서 운영되는 정보시스템은 다수이며, 이러한 시스템들 간의 경계가 명확하게 분리되지 않는 것이 일반적인 현상이다. 즉 단위 시스템을 어떻게 구분할 것인지에 대한 기준이

필요하다. 연구에서 논의되는 분류 기준은 업무 프로세스의 관점, 시스템의 물리적 구분, 해당 시스템에 대한 접근통제의 범위의 관점 등으로 설명된다. 다음으로 해당 시스템의 위험평가와 보안대책의 선택과정이 수행되며 세부적인 내용은 이후 설명된다.

1. 자산 평가

자산 평가 단계에서는 수집된 자료를 기초로 각 정보시스템을 구성하는 자산을 구체적으로 식별하고 자산의 가치를 평가한다. 설문지에 의하여 기본 자료를 수집하고, 수집된 자료에 대하여 미흡하거나, 의심스러운 부분 또는 상충되는 내용에 대하여 인터뷰를 통하여 확인한다. 일반적으로 자산에 대한 가치 평가는 자산의 유형에 따라서 다른 방법을 사용한다. 자산은 크게 데이터와 그 이외의 자산으로 구분되는데, 데이터 자산은 자산 자체의 내재적인 가치, 즉 데이터를 생성하고 유지하는데 투입된 비용보다는 해당 데이터가 조직의 업무 수행에 어떤 영향을 미치는지를 분석하는 방법으로 이루어진다.

자산 평가에 있어서 위협 인자가 작용하는 자산이 물리적인 자산인 경우도 있으나, 최종적으로 영향을 미치는 것은 데이터 자산이다. 즉, 데이터 이외의 모든 자산은 데이터를 처리하기 위한 도구라는 관점에서 데이터 자산을 중심으로 해당 시스템의 가치를 평가한다. 자산 가치 평가는 어떠한 보안대책이 강구되어 있든지 간에 보안상의 문제가 발생하였을 때 자산 그 자체와 조직에 미치는 영향을 판단하는 과정이다. 따라서 특정 자산의 가치(영향)를 평가할 때 이미 구현된 보안통제를 고려한다. 즉, 기존의 보안통제가 실행되고 있음에도 불구하고 위협이 현실화되었을 때 나타나는 영향을 정도를 평가하는 것이다. 크게 자산의 가치 평가는 데이터 자산과 기타 자산에 대해서 이루어지며 세부적인 내용은 다음과 같다.

1.1 데이터 자산 평가

평가는 해당 자산의 소유자(관리자)와 관리자에 대한 설문과 인터뷰를 통하여 수행된다. 데이터 자산은 위협이 현실화되었을 때 발생하는 영향에 의하여 평가한다. 세부 평가 기준은 조직의 규모, 조직의 유형(정부기관, 금융기관, 민간기업 등) 보안 환경 등을 고려하여 조정 가능하다. 평가는 비밀성, 무결성 및 가용성의 관점에서 이루어진다. 데이터 자산에 대한 평가는 각 자산에 대한 세부 평가 결과를 합산하여 평균값을 구하여 해당 자산의 가치를 구한다.

1.2 기타 자산 평가

데이터 자산 이외의 모든 자산은 대체비용 또는 재구축비용으로 평가하며, 평가 기준은 화폐가치를 기준으로 수행된다. 한 시스템 내의 자산들 사이의 연관성을 부여하기 위하여 데이터 자산 이외의 각 자산의 가치가 해당 시스템의 데이터 자산의 가치보다 낮은 경우에는 데이터 자산의 평가 값을 해당 자산의 가치로 본다.

2. 위험 평가

자산 식별 및 평가 단계에서 식별된 각 자산 항목에 대하여 위험 평가가 수행된다.

2.1 위협 평가

위협의 평가에 있어서 유의할 점은 위협의 발생으로 인한 영향의 측면을 고려하는 것이 아니라, 위협 인자 자체의 심각성을 고려하여야 한다. 위협의 발생 가능성과 심각성의 두 측면을 고려하여 위협의 수준을 평가하며, 위협 수준은 심각성이 낮더라도 빈도가 높은 위협에 더 주의를 기울여야 한다는 기준을 적용한다.

2.2 취약성 평가

취약성은 특정 자산 항목이 특정 위협의 공격에 대해 얼마나 많이 노출되어 있는지, 즉 위협에 의해

얼마나 쉽게 이용될 수 있는지에 의해서 평가한다. 이는 특정 자산이 위협에 대한 대항력 수준으로 이해될 수 있다. 취약성의 평가에서도 취약성 자체의 심각성과 취약성이 위협에 의하여 현실화되었을 때 나타나는 영향의 두 측면을 동시에 고려하여야 하나, 취약성이 현실화되어 나타나는 피해의 정도는 자산의 평가에서 이미 반영됨으로 취약성 자체의 심각성, 즉 위협 인자에 얼마나 많이 노출되어 있는가를 평가한다. 취약성은 자산에 내재한 속성으로서 또는 이미 구현된 보안통제를 통하여 위협에 대한 대항력의 정도를 나타낸다. 또한 취약성은 특정한 자산이 특정한 위협에 얼마나 노출되어 있는가에 의해서 평가되며, 이는 취약성을 위협/자산의 쌍의 관점에서 바라본다.

2.3 위험 수준 평가

위험 수준은 자산, 위협 및 취약성 평가에서 도출된 각각의 평가를 조합하여 도출한다. 위험 수준은 다음 단계에서 보안대책의 수준과 연계되어 보안대책의 선택에 하나의 기준으로 사용된다. 보안대책의 선택 단계를 수행하기 전에 자산, 위협 및 취약성 평가 과정에서 오류/누락이 없는지 확인하여 위험 수준의 평가 결과의 적절성을 확인한다.

3. 보안대책 선택

앞 단계에서 평가된 위험 수준에 대응할 수 있는 적절한 보안대책이 제시된다. 하나의 위협에 대응하기 위하여 복수의 보안대책이 존재할 수 있으며, 또한 하나의 보안대책이 복수의 위협에 대응할 수 있다. 서로 대응되는 위협과 보안대책은 사전에 목록화되어 제공되는 것이 편리하다. 특정 자산에 대한 특정 위협에 대응하기 위한 보안대책이 제시된다. 보안대책도 사전에 목록화되어 있어야 하며, 목록화되는 세부 내용은 적용되는 자산, 보안대책에 대응되는 위협, 보안대책의 강도(효과성), 구현 및 운영비용 등이 포함된다. 이 중에서 해당 자산의 위험 수준에 대응되는 보안 수준(효과성)을 가진 보안대책이 선택된다.

제안된 보안대책들 중에서 자산 식별 단계에서 파악된 기존의 또는 계획된 보안대책은 제외한다. 경우에 따라서는 해당 위험 수준에 대응하는 보안대책이 존재하지 않을 수도 있다. 위험을 감소시키기 위한 적절한 보안대책이 존재하지 않는 경우에는 위험을 회피하거나 전이하기 위한 방안을 모색하여야 한다. 다음으로 해당 시스템과 관련된 위험의 수준에 따라서 분석 대상 시스템에 요구되는 보안대책을 앞 단계에서 결정된 우선순위에 따라 열거하고 제시한다.

4. 실용적 위험분석 방법론의 개념적 모형화

앞서 논의된 위험분석 방법론의 기본적인 공정에 근거하여 제안된 방법론의 자동화된 도구로 개발하기 위해서는 시스템 설계에 사용되는 보편화된 모형으로 제안될 필요가 있다. 연구에서는 일반적으로 시스템 분석과 설계에 적용되는 자료흐름도와 개체관계도를 를 통해서 검증한다. 이러한 자료흐름도와 개체관계도의 모형화과정은 다음과 같은 내용이 포함된다.

- 자산, 위협, 취약성 및 보안대책이 저장된 데이터베이스
- 분석대상 시스템에 대해 식별된 자산, 위협 및 취약성목록과 평가결과가 저장되는 데이터베이스
- 자산가치, 위협 및 취약성의 심각성, 위험 수준, 그리고 보안대책 선택을 위한 평가 기준
- 분석대상 시스템의 자산, 위협 및 취약성 평가 결과를 기록하기 위한 입력 모듈
- 위험 수준 평가 결과와 제안하는 보안대책 목록을 보여주는 출력 모듈
- 자산가치, 위협 및 취약성 평가, 위험 수준, 그리고 보안대책 우선순위를 결정하기 위한 알고리즘

연구에서 제시하는 실용적 위험분석 방법론을 실제 어플리케이션으로 구현하기 위한 모형화를 위해서 정보시스템 모형화에 일반적으로 적용되고 있는 자료흐름도(DFD)와 개체관계도(ERD)는 이후에서

세부적으로 논의된다. 기본적인 개체의 구성은 위험분석방법론에서 논의되고 있는 자산, 위협, 보안통제간의 관계를 통해서 위험을 평가하는 방법론을 적용하고 있으며 전체관계의 이해와 입출력 설계의 용이성을 위해서 일부 테이블에 대해서는 정규화를 엄격하게 적용하지 않았다.

4.1 자료흐름도

실용적 위험분석 방법론의 구체적인 프로토타입의 구현을 위한 자료흐름도는 일반적으로 요구되는 수준인 제 2수준까지 제안하고 있다.

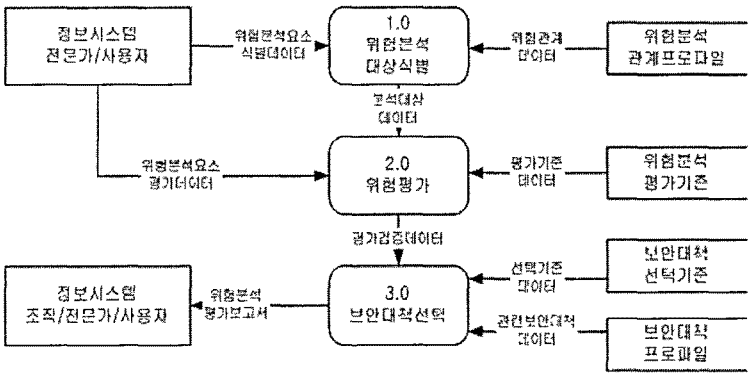
1) 배경도

실용적 위험분석 방법론의 기본적인 배경도(context diagram)는 [그림 3]과 같이 나타낼 수 있다. 그림에서 간략하게 나타나 있듯이 주요 외부개체로는 정보시스템을 사용하는 사용자와 전문가 혹은 위험분석을 수행하는 조직 구성원으로 나타낼 수 있다.

[그림 3] 실용적 위험분석 방법론의 배경도

2) 제 1수준의 자료흐름도

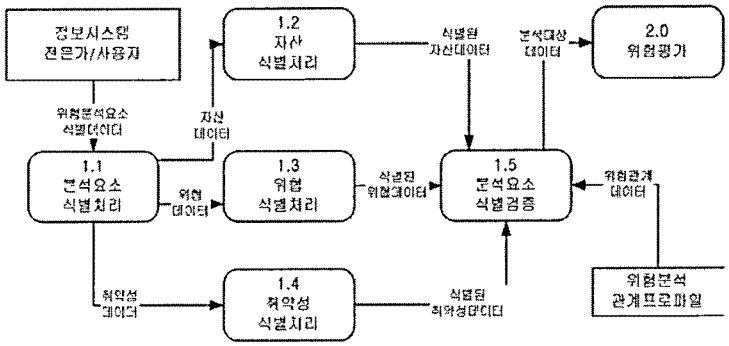
1수준의 자료흐름도는 [그림 4]로 제시한다. 그림에 나타나 있듯이 기본적인 구조는 위험분석대상 식별, 위험평가, 보안대책선택의 세 개의 프로세스로 구성되고 실제 시스템의 개발을 위해서는 2수준까지 확장하여 표현할 수 있다. 실제 프로세스의 수행을 위해서 관련 평가기준과 프로파일이 사전에 작성되며 사용자가 입력하는 자산, 위협, 취약성을 해당 프로파일과 기준에 의해서 평가하여 위험수준이 도출되고 이에 따라 보안대책을 제안하고 선택하도록 구성되어 있다.



[그림 4] Level 1의 자료흐름도

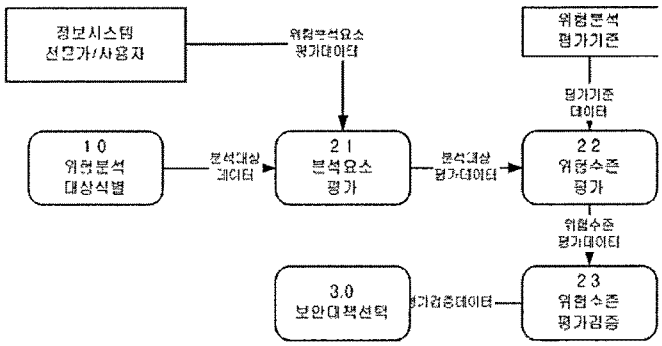
3) 제 2수준의 자료흐름도

제 1수준의 자료흐름도에 나타난 세 프로세스를 다시 분해하여 제안할 수 있다. 먼저 [그림 5]는 프로세스 1.0의 제 2수준을 모형화하고 있다. 앞서 논의된 자산, 취약성, 위협에 대한 식별과 평가의 프로세스를 통해서 위험분석 프로세스의 수행을 위한 해당시스템의 자료를 처리하는 형태로 제안된다.



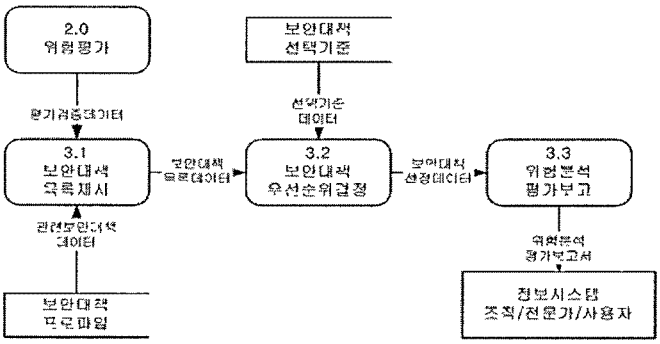
[그림 5] 프로세스 1.0의 Level 2 자료흐름도

[그림 6]은 프로세스 2.0의 제 2수준 자료흐름도를 나타낸 것으로 분석요소평가, 위험수준평가, 위험수준평가검증의 세 프로세스로 구성된다.



[그림 6] 프로세스 2.0의 Level 2 자료흐름도

마지막으로 보안대책 선택 프로세스의 제 2수준 자료흐름도는 보안대책 목록제시, 보안대책 우선순위 결정, 위험분석 평가보고의 세 프로세스로 다음의 [그림 7]과 같이 나타낼 수 있다.

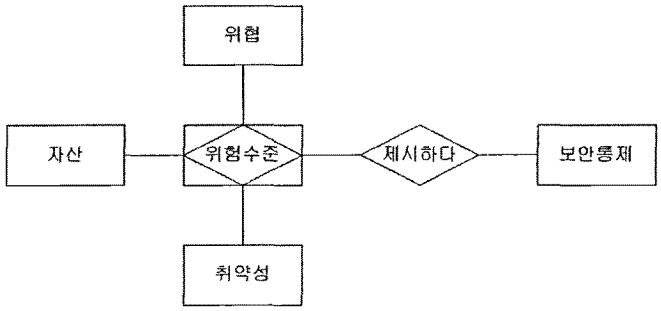


[그림 7] 프로세스 3.0의 Level 2 자료흐름도

4.2 개체관계도

위험분석시스템의 개발에 있어서 관련된 개체와 관계를 나타내기 위해서 연구에서는 개체관계도를 이용하였다. 기본적으로 위험수준 혹은 위험은 자산과 위협 그리고 취약성의 관계로 논의가 되는데, [그림 8]에 나타나 있듯이 위험수준을 결합개체(associative entity)로 표시하였다. 위험수준과 보안통제

간에는 해당되는 조건을 만족하는 값을 제시하도록 관계가 설정되어 있다.



[그림 8] 실용적 위험분석 시스템의 개체관계도

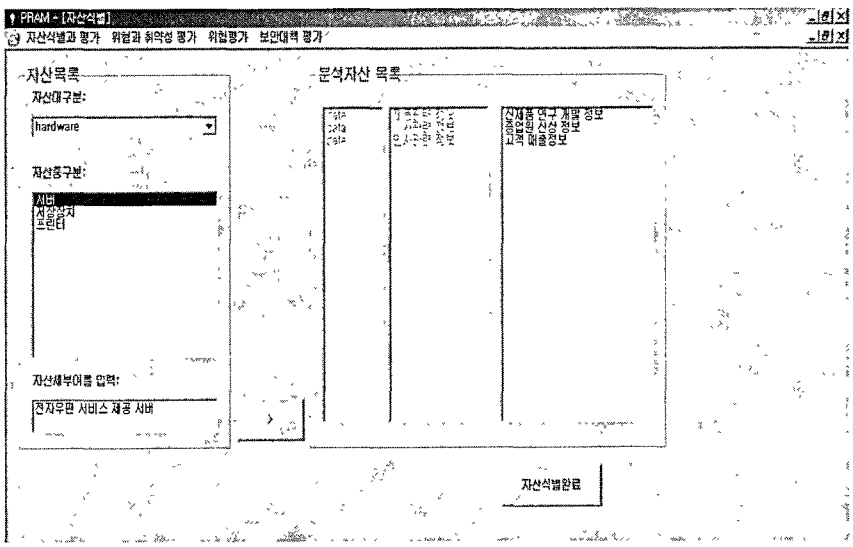
4.3 입출력화면 설계와 프로토타이핑

1) 초기화면

프로토타입을 실행하면 전체 4개의 명령구조로 구성된다. 자산식별과 평가는 다시 두 개의 하부 메뉴로 구성이 되어 있으며, 나머지의 프로세스는 하나의 메뉴로 구성되어 있다. 전체 진행의 과정은 앞서 기술한 위험분석 및 관리의 형태를 그대로 준수하고 있다.

2) 자산 식별 및 평가

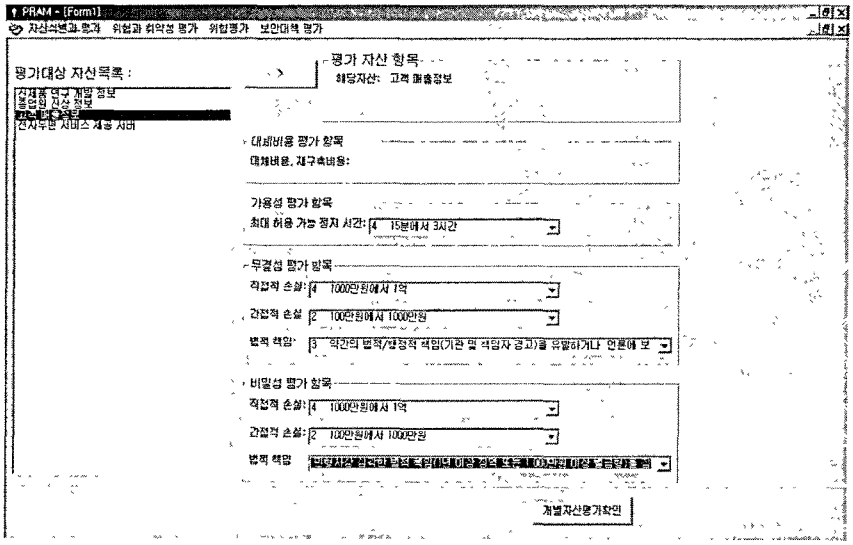
자산 식별 메뉴를 선택하면 [그림 9]와 같은 화면이 출력된다. 좌측의 프레임의 콤보 박스와 리스트 박스는 기존의 목록에서 사용자가 분석 대상 자산을 선정하도록 하고 있으며, 하단의 텍스트 박스에서 개별자산에 대한 이름을 입력하도록 하고 있다. 입력이 완료되면 우측의 프레임의 분석 대상 목록에 추가되며, 모든 분석 대상에 대한 추가가 끝나면 자산식별 완료 버튼을 클릭함으로써 다음 단계로 진행하게 된다.



[그림 9] 자산 식별 입력 화면

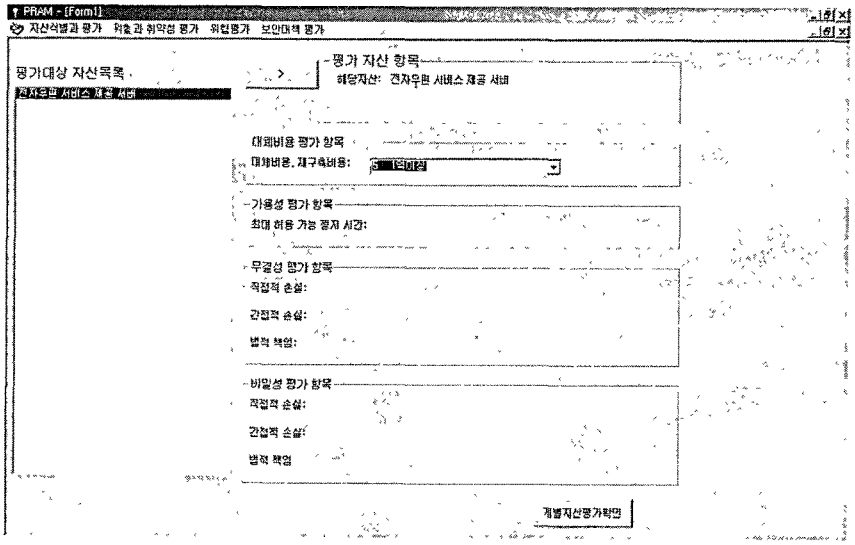
자산 식별의 다음 단계로 분석 대상 자산에 대한 평가가 이루어지는데, [그림 10]과 같은 화면으로 구성된다. 좌측의 프레임에는 이전의 단계에서 수행한 평가대상 자산의 항목이 출력되고, 각 항목을 더블클릭 하게 되면 좌측의 평가 자산 항목의 난에 해당 내용이 표시되면서 해당 자산에 대한 평가 기준

이 하단의 콤보 상자에 표시되게 된다.



[그림 10] 자산 평가 화면

평가기준의 출력은 해당자산이 [그림 10]과 같이 고객매출정보와 같은 데이터 자산인 경우에는 가용성, 무결성, 기밀성의 정성적인 척도로 평가하도록 하고, 비데이터 자산인 전자우편 서비스 제공 서버와 같은 하드웨어 자산인 경우에는 [그림 11]과 같이 대체비용의 항목만 표시하도록 함으로써 구별된 평가를 수행하도록 하고 있다. 평가된 개별 자산은 자동으로 분석 목록에서 제거되어 분석할 자산이 더 이상 없는 경우 자동으로 창이 닫히고 다음의 과정으로 진행한다.

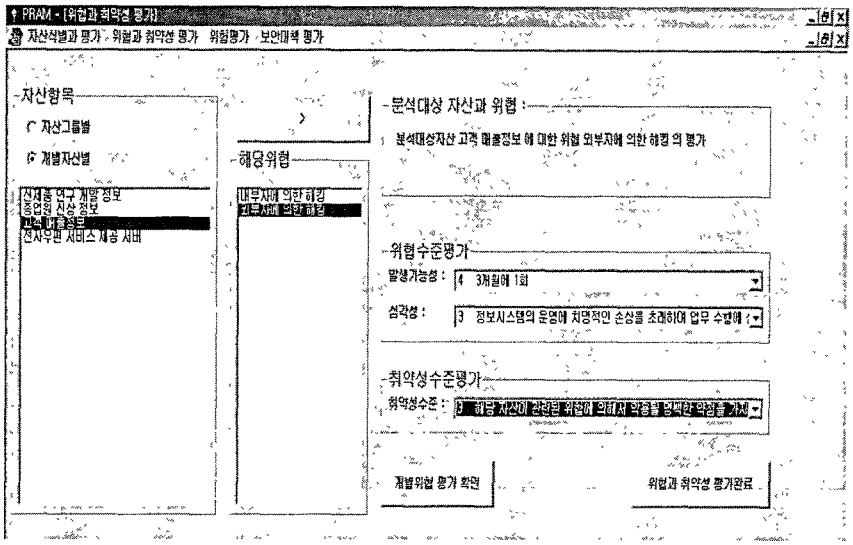


[그림 11] 데이터 이외의 자산 평가 화면

3) 위협 및 취약성 평가

자산의 식별과 평가의 과정이 완료되면, 개별 자산과 관련된 위협과 해당 자산의 위협에 대한 취약성의 평가가 이루어진다. 이러한 평가는 데이터베이스의 스키마에서도 나타나 있듯이 그 관계는 사전

에 결정된 테이블의 값을 참조하도록 한다.



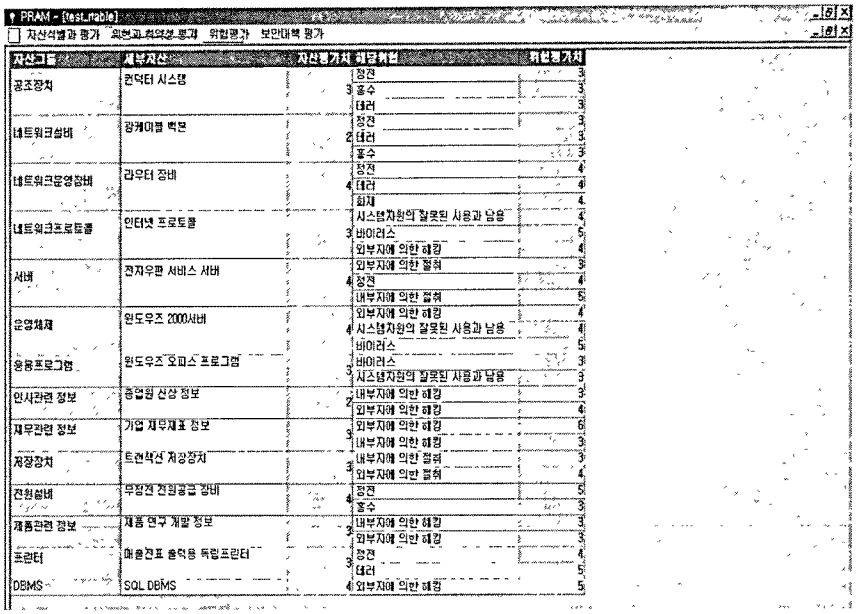
[그림 12] 위협 평가 화면

위협과 취약성 평가 메뉴를 클릭하게 되면 [그림 12]과 같은 화면이 출력된다. 그림에 나타나 있듯이 좌측의 프레임에는 해당 자산의 항목들이 출력되게 되어 있으며, 각 항목을 클릭하면 그 해당자산과 관련된 위협만 그 우측의 목록 상자에 출력되도록 하고 있다. 해당 자산과 해당 위협을 클릭으로 선택하고 나면, 그 다음으로 우측의 콤보 상자에 위협수준과 취약성 수준을 평가하게 한다.

하나의 개별 자산에 대한 위협의 평가가 완료되면 개별위협 평가 확인 버튼을 눌러서 한번의 평가를 완료하고 모든 개별자산과 개별위협에 대한 평가가 완료되면 위협과 취약성 평가완료 버튼을 클릭함으로써 이 과정을 종료하게 된다. 이 과정으로 분석대상 자산에 대한 위험 분석 테이블의 구조가 확정되게 되고 이렇게 확정된 내용은 다음 단계에서 화면으로 출력된다.

4) 위험평가

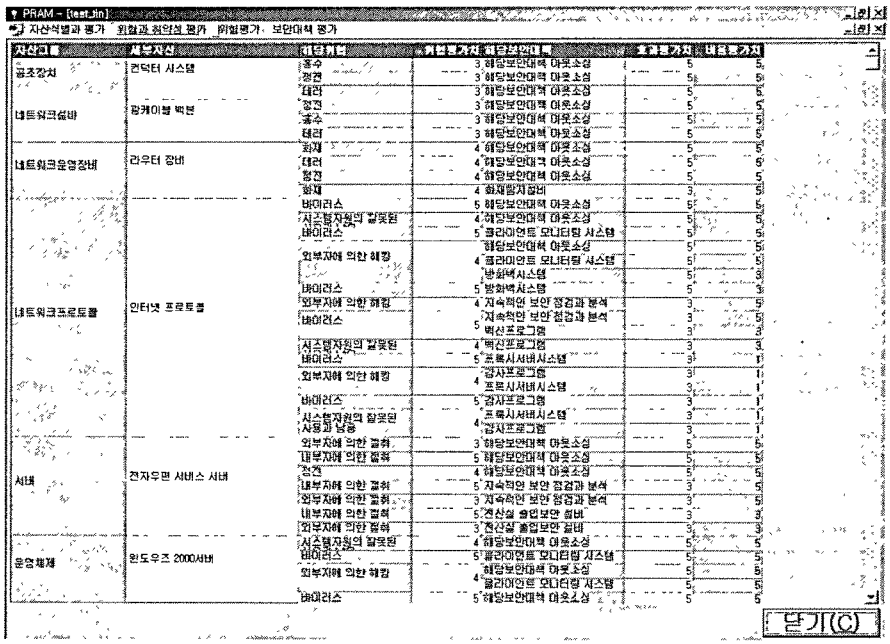
위험평가 항목을 선택하게 되면 위험 평가 결과 화면이 나타나게 된다. [그림 13]에 나타나 있듯이 개별 자산의 자산 그룹과 세부 자산별로 그룹핑(grouping)을 한 형태로 요약한 테이블로 제시가 된다. 이러한 표를 통해서 전반적인 자산과 위협간의 관계와 그 평가치를 요약하여 확인할 수 있게 되고 이러한 위험에 대한 분석이 완료되면 다음의 단계인 보안대책에 대한 평가의 과정이 수행되게 된다.



[그림 13] 위험 평가 결과 화면

5) 보안대책평가

보안 대책에 대한 평가도 앞서의 자산과 위협간의 관계와 마찬가지로 이미 정해진 보안대책 목록으로부터 해당되는 분석 자산의 집합만을 선별적으로 조인(join)하여 하나의 테이블로 요약하여 제시하고 있다. 보안대책평가 항목을 클릭한 결과의 화면은 다음의 [그림 14]와 같이 나타나게 된다.



[그림 14] PRAM의 보안대책 목록 화면

위의 화면은 프로토타이핑 프로그램으로 생성되는 최종의 위험분석 보고서로써, 화면에 나타나 있듯이 자산그룹과 세부자산에 대해서 그룹핑된 요약 표를 제시하고 있다. 제시된 표에서 가장 우측의 컬럼은 해당 자산에 대한 적절한 보안대책을 선택하는데 유용한 기준으로 작용한다. 즉, 그림에 나타나 있듯이 네트워크 운영장비인 라우터에 관련된 위협은 화재, 테러, 정전 등으로 관련되어 있으며 이에 대응된 보안대책은 아웃소싱을 하거나 화재 탐지 설비를 설치하는 것이다. 이러한 가능한 대안 중에서 효과성의 컬럼은 이 프로세서의 이전에 특정의 위협수준을 완화하지 못하는, 즉 예를 들면 위험 수준이 7로 아주 높은 경우 보안대책 수준이 1로써 매우 미약한 경우에는 처음부터 그러한 보안대책에 대한 고려는 배제된 것만 출력된다.

따라서, 효과성 컬럼은 현재의 위험 수준을 충분히 완화할 수 있는 것 중에서 산출이 되며, 이러한 보안대책은 해당 비용평가치의 비교를 통해서 선정할 수 있는 제안을 하고 있다. 즉, 앞서 설명한 사례에서 화재에 대한 대응책으로 아웃소싱을 하는 것과 화재 탐지 설비를 구현하는 것이 나와 있는데, 두 대응책간의 비용은 동일한 수준이므로 효과성이 높은 아웃소싱이 선택되게 되는 것이다. 그와 반대로 동일한 효과성이라면 보다 비용수준이 높은 항목을 선정하면 되는 것이다.

IV. 결론

연구에서는 현재 이론적으로나 실무적으로 적용되고 있는 다양한 위험분석 방법론들에 대해서 논의하였으며, 이를 통해서 실용적으로 위험분석을 수행하기 위한 위험분석 방법론 제안하고 있다. 제안된 방법론은 자동화된 도구로 개발할 수 있으며, 제시된 개체관계도와 평가기준 그리고 평가 알고리즘을 통해서 가능하다.

한편 연구에서 제안하는 방법론의 한계점으로는 자산과 위협간의 관계, 위협과 보안대책과의 관계에 대한 방대한 프로파일이 아직 현실적으로 완전하게 구축되지 못하고 있다는 점을 들 수 있다. 실무적으로 활용되는 CRAMM의 경우에 있어서도 그 방대한 양의 프로파일 데이터베이스가 수년에 걸쳐서 구축되었으며 이러한 것을 국내에 적용하여 축적된 자료로 사용하는데 있어서는 상당한 시간이 필요할 것으로 판단된다.

향후 연구에서는 제안된 방법론과 평가알고리즘 그리고 개체관계도를 바탕으로 실제 실용적인 위험분석도구를 개발하여 구현하는 것과 관련된 논의가 이루어질 것이며, 구체적인 어플리케이션의 개발에 대한 연구가 수행될 것이다. 또한, 개별 어플리케이션의 수준을 넘어서 실용성을 보다 높이기 위한 방법으로 ASP나 PHP를 이용한 웹기반의 위험분석 방법 도구로 확장 개발될 수 있을 것으로 판단된다.

참 고 문 헌

김기윤, 김정덕, "정보보호를 위한 위험분석 방법: 분류와 선택기준", *한국경영정보학회*, 1994

김정덕, "정보보안관리와 위험관리", *정보통신망정보보호워크숍(NETSEC-KR '98)*, pp. 173-206, 1998. 6.

한국전산원, *전산망 보안을 위한 위험관리 기술지원서*, 1994

한국전산원, *위험분석 방법론 및 자동화 도구 기술 이전 교육 교재*, 1998.

정창덕, 사례기반추론을 이용한 전자상거래 위험분석, *한국과학기술원 박사학위논문*, 2001.

펜타/KAIST, 전산망 위험분석 전문가시스템 개발, *펜타시큐리티시스템/한국과학기술원*, 1999.

Barnard, L. and Solms, R. "A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls", *Computer & Security*, Vol. 19, No. 2, 2000, pp.185-194.

BSI, BS7799 - Code of Practice for Information Security Management, *British Standards Institute*, 1999.

CMU/SEI, Operationally Critical Threat, Asset, Vulnerability Evaluation (OCTAVE) Framework, Verion 1.0, *CMU/SEI-99-TR-017*, June 1999.

CSE, Threat and Risk Assessment Working Guide, Government of Canada, *Communications Security Establishment*, 1999.

Eloff, M. and S. H. Solms, "Information Security Management: A Hierarchical Framework for Various Approaches," *Computers & Security*, Vol. 19, 2000, pp.243-256.

Fitzgerald, K., "Information security baselines," *Information Management & Computer Security*, Vol. 3, No. 2, 1995, pp 8-12.

GAO, Information Security Risk Assessment - Practices of Leading Organizations, Exposure Draft, *U.S. General Accounting Office*, August 1999.

Halliday, S., K. Badenhorst and R. Solms, "A business approach to effective information technology risk analysis and management," *Information Management & Computer Security*, Vol. 4, No. 1, 1996, pp.19-31.

Humphreys, E.J., Moses, R.H., and Plate, A.E., Guide to Risk Assessment and Risk Management, *British Standard Institute*, 1999.

Insight Consulting, CRAMM User Guide, Issue 2.0, *U.K. Security Service and CESG*, January 2001.

ISO/IEC JTC 1/SC27, Information technology - Security technique - Guidelines for the management of IT security (GMITS) - Part 3: Techniques for the management of IT security, *ISO/IEC JTC1/SC27 N1845*, 1997. 12. 1.

KPMG Peat Marwick LLP, Vulnerability Assessment Framework 1.1, *Critical Infrastructure Assurance Office*, October 1998.

NIST, An Introduction to Computer Security: *The NIST Handbook, Special Publication 800-12*, Oct. 1995.

NIST, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), *NIST Special Publication 800-27*, June 2001.

NIST, Generally Accepted Principles and Practices for Securing Information Technology Systems, *NIST Special Publication 800-14*, Sept 1996.

NIST, Security Self-Assessment Guide for Information Technology Systems, *NIST Special Publication 800-26*, Aug. 2001.

OGC, Draft Guidelines on Managing Risk, *Office of Government Commerce, U.K.*, 2001.

Peltier, T., Information Security Risk Analysis, *Auerbach*, 2001.

Solm, R., "Information Security Management(1): Why Information Security Is So Important", *Information Management & Computer Security*, Vol. 6, No. 4, 1998, pp.174-177.

Solm, R., "Information Security Management(2): Guidelines to The Management of Information Technology Security (GMITS)", *Information Management & Computer Security*, Vol. 6, No. 5, 1998, pp.221-223.

Solms, B. "Information Security - The Third Wave?" *Computers & Security*, Vol. 19, No. 7, pp.615-620, 2000.

White, K. B., "National(UK) Computer Security Survey 1996," *Information Management & Computer Security*, Vol. 4, No. 3, 1996, pp.3-17.