논문 02-27-11C-7 한국통신학회논문지 '02-11 Vol.27 No.11C

실용적인 위험분석 방법론 설계와 모듈 구현

정회원 정 윤 정*, 김 인 중*, 이 철 원*

The Design and Implementation for Practical Risk Analysis Method & Modules

Yoon-Jung Jung*, In-Jung Kim*, Cheol-Won Lee* *Regular Members*

요 약

현재 많은 조직은 정보시스템 환경의 급속한 변화로 인해 정보자산에 대한 위험을 인식하고, 이에 대한 적절한 관리를 필요로 한다. 또한 정보통신기반보호법의 시행으로 주요한 정보통신 인프라를 운영하는 조직은 주요 정보자산의 위협, 취약성 및 위험 분석·평가에 많은 관심이 고조되고 있다. 그러나 조직의 정보자산에 대한 위험을 분석하는 방법론과 도구들은 아직까지 외국에서 개발된 것이 대부분으로, 이 분야의 국내 연구가 미흡한 단계이다. 국내 주요 정보통신 인프라의 위험분석·평가를 수행함에 있어서 대부분 외국의 방법론이나 도구에 의존하는 것은 국내 현실을 반영하지 하지 못하기 때문에 위험 분석 수행과정에서 문제를 야기 시킬 수 있으므로 국내에서도 이 분야의 연구의 활성화가 필요한 시점이다. 본 논문은 국내 위험분석·평가 도구 개발의 한 단계 발전을 위하여 실제로 사용자 편의성을 고려하고, 국내 현실을 반영한 위험분석 방법론을 설계 및 프로토타입/모듈을 구현하였다.

ABSTRACT

In these days many Organizations recognize risk of information asset by rapid change of information system environments, and need suitable management for that. Also many organization which operate important information-communication infrastructure take interest in threat, vulnerability and risk analysis of important asset by enforcement of Act on protection of information and communication infrastructure. But, it is most that methodology and tools that analyze risk for organization's information asset are developed in abroad up to now, domestic research of this field is insufficient stage. An research of this field is necessary in domestic because it can't reflect domestic actuality by depending on most foreign methodology or a tool. In this paper we proposed design and implementation for the risk analysis methodology, a prototype and important modules that considers the user convenience. We expect that the result of this paper will for step improvement of domestic risk analysis methodology and tool development.

Ⅰ. 서 론

국내 대부분의 조직은 정보시스템을 안전하게 운영하기 위한 별도의 보안전담 조직이 없고, 네트워크 관리자나 시스템 관리자가 정보시스템의 보안을 담당하는 경우가 다수이므로 조직 내에 보안전문가는 거의 드물다. 이러한 국내 현실에서 위험분석이나 취약성 분석을 수행하기 위하여 외국의 현실을 반영한 위험분석·평가 방법론이나 도구들을 사용하면, 아직까지 보안 지식이 부족한 사용자가 사용하기에는 많은 어려움이 있다. 현재까지 국내 대부분의 조직은 정보자산에 내재되어 있는 위협, 취약성 및 위험을 측정하고, 그에 대한 보호대책을 세우기 위하여 외부의 전문기관이나 업체에 위험분석·평가를 의뢰를 한다.

그러나, 향후 국내 조직들도 보안전담 조직을 구

* 국가보안기술연구소

※ 본 논문은 2002년 4월 JCCI 학술대회에서 우수논문으로 선정되어 게재 추천된 논문입니다.

성하게 되면 자기 조직에 대한 위험분석·평가에 대한 자가수행을 위한 적용이 가능한 실용적인 위험분석 방법론이나 도구들이 필요하다.

그러므로 국내 위험분석 기술의 한 단계 진보를 위하여 현재까지 나온 위험분석·평가 방법론과 도구를 분석하고, 사용자들이 쉽게 사용이 가능한 실용적인 방법론을 개발이 필요하다.

본 논문에서 제안하고자 하는 실용적 위험분석 방법론은 사용자 편의성을 제공하는 것을 최우선적으로 고려한다. 본 방법론은 자동화 도구의 개발을 염두에 두고 고안되었으며, 정보보안 전문가가 아니더라도 활용할 수 있도록 위험분석의 수행 절차와 평가 기준을 가급적 간단명료하게 제시한다. 본 논문의 구성은 2장에서 현재까지 국내·외 위험분석 방법론에 대한 연구 동향을 소개하고, 3장은 위험분석의 자산평가부터 보안대책 제시까지 위험분석 방법의 절차를 설명한다. 그리고 4장은 제시한 위험분석 방법론에 대한 프로토타입과 모듈의 구현에 관하여 설명하고, 마지막으로 5장은 결론 및 향후 진행 과제를 기술한다.

Ⅱ. 위험분석 방법론의 연구 개발 동향

정보기술 위험분석이란 비즈니스 목표와 전략을 달성하기 위해 필요한 정보시스템과 관련된 정보자원에 대한 위험요소를 식별하고 평가하여 잠재적 위험을 통제하기 위한 제반수단을 연구하는 활동이라고 정의할 수 있다.

위험분석 방법론은 대상 조직의 정보시스템에 대해 관련 정보자산의 식별 및 평가, 위협 및 취약성 평가, 기존 정보보호 대응책의 효과성 평가 등으로 구성되는 위험분석 과정을 통해 위험을 상세하게 측정, 분석하는 절차와 방법을 의미한다.

위험분석을 수행함으로써 조직의 정보시스템에 대한 총체적 보안관리가 가능하게 되며 위험을 최소화시킬 수 있다. 또한 위험분석 결과를 토대로 비용 효과적인 정보보안 대책을 적용할 경우, 비용절감 효과를 기대할 수 있다.

외국의 위험분석 지침 및 방법론을 살펴보면 미국에서는 국립표준기술원(NIST) FIPS 65, GAO에서 정보보호관리지침 등을 통해 정부차원에서 표준이나 지침을 정부기관이나 민간에 공급함으로써 위험분석을 포함한 정보보호 컨설팅 사업이 활발히 이루어지고 있으며 백 개 이상의 위험분석 자동화 도구가 개발되어 사용 중이다.

영국에서는 정보보호관리 표준인 BS7799에 기초한 인증사업을 장려하고 있으며 정보보호관리시스템 구축을 위해서는 위험분석이 반드시 포함되어야 함을 규정화하고 있으며, CRAMM, RA 등의 위험분석 자동화 도구를 이용하여 정기적으로 수행하고 있다.

일본도 재단법인 일본정보처리개발협회에서 JRAM (1992)을 발표하여 위험분석을 장려하고 있다. 이러한 선진 각국의 노력들이 국제표준화 활동에도 반영되어 국제표준화기구(ISO)의 ISO/IEC, JTC1/SC27 WG1에서 정보기술 보안관리 지침(Guidelines for the Management of Information Technology Security)를 개발하여 Part 5를 제외하고 국제 표준화 되었다.

국내는 한국전산원에서 1996년 위험분석 방법론을 설계하고, 위험분석 자동화도구인 Hawk를 개발하였으나 대규모 네트워크에 적용하기에는 무리가 있는 실정이다. 국외의 위험분석 방법론에 대한 연구와 위험분석 자동화 도구에 대한 개발이 활발한데 비해서, 국내의 연구는 아직까지 위험분석 방법론 이론에 대한 기초연구 수준이다.

본 논문에서 제안한 실용적인 위험분석 방법론을 개발하기 위하여 캐나다의 CSE에서 발표한 위험관리방법론, 미국의 NIST에서 발표한 FIPS 65 정보보호관리지침에서의 위험분석 방법론, ISO/IEC JTC1 SC27에서 제정한 정보보호관리지침내의 위험분석 방법론, 그리고 취약성 평가 방법론인 VAF (Vulnerability Assessment Framework), OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) 등에 대한 분석을 선행하였다. 또한 국내 전산원에서 개발한 위험분석도구인 HAWK를 분석하였다.

Ⅲ. 실용적인 위험분석 방법론의 설계

실용적인 위험분석 방법론 및 도구를 설계하기 위하여 우선적으로 사용자가 이해하기 쉽고, 사용하기에 편리하기 위한 방법으로 본 방법론은 3가지를 제시한다.

- 국내 일반적인 조직에서 활용 가능한 평가기준 제시
- 정성적인 위험분석방법론에서 각 평가기준의 복잡한 판단수치를 간단하게 3단계로 제시
  (위험감소를 위한 보호대책 제시의 신뢰도를 보장하는 수준을 유지)

· 사용자가 사용하기 쉬운 인터페이스 제공

우선 위험분석을 적용하는 가장 기초적인 단위는 개별 자산이며, 여러 종류의 개별 자산들이 하나의 정보시스템을 구성한다. 한 조직에서 여러 정보시스템을 운영하고 있고, 시스템의 경계가 명확하게 분리되지 않는 것이 일반적이므로 단위 시스템을 어떻게 구분할 것인지에 대한 기준이 필요하다. 분류 기준은 업무 프로세스의 관점, 시스템의 물리적 구분, 해당 시스템에 대한 접근통제의 범위의 관점 등이 있다.

본 방법론은 시스템에 대한 기준을 업무 프로세스의 관점에서 구분을 하고 개발을 수행하였다.

그리고 전제적인 절차는 [그림 1]과 같이 계획수립, 자산평가, 위험평가 및 보안대책 제시 단계로 구성되고, 각 단계는 다수의 프로세스를, 각 프로세스는 여러 태스크로 구성되어 있다.

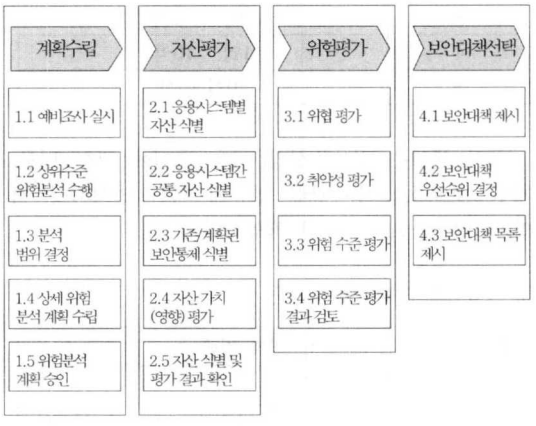


그림 1. 위험분석·평가 프로세스

자산평가와 위험평가는 합당한 평가결과를 위한 기준을 제시해야 한다. 본 논문에서는 자산평가는 데이터 자산에 기준을 두고 방법론을 전개하고, 위협, 취약성을 분석하여 위험도를 산정하는 기준을 제시한다. 마지막으로 위험을 줄이기 위하여 보호대책을 제시하는 방법과 보호대책 제시의 우선순위화에 대한 기준을 설명한다.

1. 자산 평가

자산평가 이전 단계에서 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. 자산의 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.

1.1 응용시스템별 자산 식별

각 분석 대상 시스템의 세부 자산을 식별한다. 자산을 식별할 때에는 보안통제(기술적 보안통제)를 포함한다. 이는 보안통제도 고의적 또는 우발적인 보안 위협에 의하여 손상될 가능성이 있기 때문이다. 예를 들어, 침입차단시스템도 화재에 의하여 물리적인 손상을 입을 수 있다.

○ 데이터 자산 식별

각 응용시스템에서 처리되는 데이터를 식별한다. 해당 시스템이 처리하는 데이터를 모두 하나의 논리적인 데이터 집합으로 본다.

○ 기타 자산 식별

데이터 자산 이외의 정보시스템을 구성하는 모든 요소들이 식별되며, 다음과 같이 구분된다.

- 소프트웨어 : 응용 프로그램, DBMS, 운영체제, 유틸리티 프로그램 등
- 하드웨어 : 워크스테이션, PC, 주전산기, 저장 장치 등
- 네트워크 : 허브, 라우터, 데이터통신망 등 각종 네트워크 장비
- 공조장치, 전원 등 기타 물리적 자산

1.2 응용시스템간 공통 자산 식별

해당 조직의 정보시스템 인프라를 구성하는 하드웨어, 통신 네트워크 및 기타 자산을 식별한다.

1.3 기존/계획된 보안통제 식별

자산 식별 단계에서 식별된 보안통제는 보안대책 선택 단계에서 제시된 보안대책과 비교하여 개선 또는 추가되어야 하는 보안대책을 확인하는데 활용된다. 이 단계에서 식별되는 보안통제에는 현재 구현되어 있는 보안통제뿐만 아니라 구현계획이 확정되어 있는 것도 포함한다.

○ 기술적 보안통제 식별

자산 식별 단계에서 파악된 자산 중에서 보안 기능을 제공하는 자산을 식별하여 별도로 목록화 한다.

○ 관리적 보안통제 식별

소프트웨어 배포, 데이터 입출력 통제, 사용자 승인, 교육 및 훈련, 사고 처리 등 보안관리 지침과 절차를 파악한다.

○ 물리적 보안통제 식별

시설 접근 통제와 같은 물리적인 보안통제를 식별한다.

○ 자산 가치(영향) 평가

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 도구이다라는 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.

상기에 설명한 자산평가를 위하여 데이터 자산에 대한 평가기준을 제시한다. 자산 평가는 해당 자산의 소유자와 관리자에 대한 설문과 인터뷰를 통하여 수행된다. 데이터 자산은 위협이 현실화되었을 때 발생하는 영향에 의하여 평가한다. 세부 평가 기준은 조직의 규모, 조직의 유형의 보안 환경 등을 고려하여 조정 가능하다. 평가는 기밀성, 무결성 및 가용성의 관점에서 이루어지며, 세부 기준은 다음과 같다.

가용성은 최대 허용 가능 정지 시간(maximum allowable downtime; MADT)이 조직에 심각한 손실을 초래하는 경우를 고려하여 결정한다.

표 1. 가용성 평가 기준

척도	평가 기준
1	7일 이상
2	1일 - 7일
3	3시간 - 1일
4	15분 - 3시간
5	15분 미만

무결성과 기밀성의 세부 평가 기준은 다음과 같다. 직접적인 금전적 손실으로 수익의 감소와 비용의 발생을 나타낸다.

표 2. 직접적인 금전적 손실 평가 기준

척도	평가 기준
1	10만원 미만
2	10 - 100만원
3	100만원 - 1000만원
4	1000만원 - 1억
5	1억 이상

간접적인 금전적 손실은 업무 수행의 지장 초래로 인한 내부적/외부적 신뢰나 평판 훼손, 장기적인 금전적 손실을 말한다.

표 3. 간접적인 금전적 손실 평가 기준

척도	평가 기준
1	100만원 미만
2	100-1000만원
3	1000 - 1억
4	1억 - 10억
5	10억 이상

법적 책임은 정보통신망 이용 촉진에 관한 법률, 개인정보보호법 등 관련 법규에 의한 민형사상 책임, 인명 사상으로 인한 책임이다.

표 4. 법적 책임 평가 기준

척도	평가 기준
1	법적 책임이 없음
2	법적 책임은 없으나 언론에 보도되면 약간의 부정적인 이미지를 초래함
3	약간의 법적/행정적 책임(기관 및 책임자 경고)을 유발하거나, 언론에 보도되면 다소의 부정적인 이미지를 초래함
4	1년 이하의 징역 또는 1,000만원 이하의 벌금형/과태료가 부과됨
5	기관이나 보안 담당자가 민형사상 심각한 법적 책임(1년 이상 징역 또는 1,000만원 이상 벌금형)을 짐

이상의 기준들을 종합하면 다음의 표와 같다. 데이터 자산에 대한 평가는 각 자산에 대한 세부 평가 결과를 합산하여 평균값을 구하여 해당 자산의 가치를 구한다.

데이터 자산에 대한 평가 결과의 총 평균값은 항상 1이상 5이하이므로 자산의 가치는 아래 표의 총 평균값에 따라서 다음의 기준을 적용하여 데이터

자산 평가 값으로 환산한다.

표 5. 데이터 자산 평가 기준

평가 기준	직접적 손실	간접적 손실	법적 책임	MADT	평균
기밀성	○	○	○	-	A
무결성	○	○	○	-	B
가용성	-	-	-	○	C
총평균	(A+B+C)/3				

표 6. 데이터 자산 평가 환산 기준

총 평균 값	자산 평가
1 ~ 1.8	1
1.81 ~ 2.6	2
2.61 ~ 3.4	3
3.41 ~ 4.2	4
4.21 ~ 5	5

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(그러한 점은 이미 자산의 가치 평가에 반영되었음), 위협 인자 자체의 심각성을 고려하여야 한다.

○ 자산별 위협 식별

각 자산에 대하여 적용 가능한 위협 항목을 식별한다. 자산 유형에 따라 적용되는 위협은 사전에 목록화된다.

○ 위협 수준 평가

위협 평가 기준은 위협의 심각성과 발생 확률을 동시에 고려한다. 발생 가능성(확률)은 다음의 표와 같이 5 단계로 평가한다.

표 7. 위협 발생 가능성 평가 기준

척도	평가 기준
1 (아주 높음)	1개월에 1회 이상 발생
2 (높음)	3개월에 1회
3 (보통)	1년에 1회
4 (낮음)	3년에 1회
5 (아주 낮음)	10년에 1회 미만

위협의 심각성은 위협 인자 자체에 따라 평가하며, 평가 기준은 다음과 같다.

표 8. 위협 심각성 평가 기준

척도	평가 기준
1 (낮음)	정보시스템의 운영에 약간의 장애를 초래하나 정상적인 업무 수행에는 지장이 없다.
2 (보통)	정보시스템의 운영에 상당한 피해를 초래하여 일시적인 장애를 유발할 잠재력을 가지고 있다.
3 (높음)	정보시스템의 운영에 치명적인 손상을 초래하여 업무 수행에 상당기간 막대한 지장을 초래할 잠재력을 가지고 있다.

위협의 발생 가능성과 심각성의 두 측면을 고려하여 위협의 수준을 평가하는 기준은 아래의 표와 같이 3 단계로 분류한다. 표의 위협 수준은 확률에 대한 비중이 심각성보다 높은 비대칭적인 구조를 가지는데, 이는 심각성이 낮더라도 빈도가 높은 위협에 더 주의를 기울여야 한다는 점에 근거하고 있다. 다음은 위협 수준의 계산을 나타내는 표이다.

표 9. 위협 수준 계산표

		확률				
		아주 낮음	낮음	보통	높음	아주 높음
심각성	낮음	1	1	2	2	3
	보통	1	1	2	3	3
	높음	1	2	2	3	3

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. 취약성의 평가 기준은 다음의 표와 같다.

표 10. 취약성 평가 기준

척도	평가 기준
1 (낮음)	추가적인 보안통제가 없이도 해당 자산이 관련된 위협에 노출될 가능성이 희박하다.
2 (보통)	해당 자산이 관련된 위협에 의해서 악용될 가능성이 다소 있어 보안통제가 추가/보완되어야 한다.
3 (높음)	해당 자산이 관련된 위협에 의해서 악용될 명백한 약점을 가지고 있다.

2.3 위험 수준 평가

위험 수준은 자산, 위협 및 취약성 평가에서 도출된 각각의 척도를 조합하여 도출한다. 위험 수준은 다음 단계에서 보안대책의 수준과 연계되어 보안대책의 선택에 하나의 기준으로 사용된다. 위험 수준은 아래의 표와 같이 7단계로 구분된다. 자산의 척도가 위협이나 취약성의 척도보다 범위가 크기 때문에 전체 위험 수준에 더 많은 영향력을 미치게 됨으로 자산 중심적인 평가 방법이다.

표 11. 위험 평가 기준

위협		낮음			보통			높음		
취약성		낮음	보통	높음	낮음	보통	높음	낮음	보통	높음
자산	아주 낮음	1	1	2	1	2	3	2	3	4
	낮음	1	2	3	2	3	4	3	4	5
	보통	2	3	4	3	4	5	4	5	6
	높음	3	4	5	4	5	6	5	6	7
	아주 높음	4	5	6	5	6	7	6	7	7

아래의 표는 상기의 표가 계산되는 과정을 보여주는 위험 수준 계산표이다. 자산, 위협 및 취약성의 척도 값을 합산하면 1에서 11사이에 분포하게 되는데, 값의 범위를 줄여서 7점 척도로 환산하고 척도 값의 분포를 고르게 하기 위하여 합계 값이 3과 4는 위험 수준을 1로 하고, 10과 11은 7로 변환한다.

2.4 위험 수준 평가 결과 검토

보안대책의 선택 단계를 수행하기 전에 자산, 위협 및 취약성 평가 과정에서 오류/누락이 없는지 확인하여 위험 수준의 평가 결과의 적절성을 확인한다.

표 12. 위험 수준 계산 자료

위협		1			2			3		
취약성		1	2	3	1	2	3	1	2	3
자산	1	3	4	5	4	5	6	5	6	7
	2	4	5	6	5	6	7	6	7	8
	3	5	6	7	6	7	8	7	8	9
	4	6	7	8	7	8	9	8	9	10
	5	7	8	9	8	9	10	9	10	11

3. 보안대책 선택

이전 단계에서 평가된 위험 수준에 대응할 수 있는 적절한 보안대책이 제시된다.

3.1 보안대책 제시

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, 구현 및 운영비용 등이 포함된다. 이 중에서 해당 자산의 위험 수준에 대응되는 보안 수준을 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.

3.2 보안대책 우선 순위 결정

열거된 보안대책들의 우선 순위를 부여한다. 우선 순위 부여의 기준이 되는 항목은 대응되는 위협의 수, 보안대책의 강도, 구현 및 운영비용이다. 구체적인 우선 순위 평가 기준은 다음의 표와 같다.

3.3 보안대책 목록 제시

분석 대상 시스템에 요구되는 보안대책을 앞 단계에서 결정된 우선 순위에 따라 열거한다.

표 13. 보안대책 우선순위 결정 기준

요인	척도	가중치
비용	낮음 (100만원 이하)	5
	중간 (100 ~1,000만원)	3
	높음 (1,000만원 이상)	1
효과성 등급	낮음	1
	중간	3
	높음	5
보안대책이 대응하는 위협의 수		대응되는 위협당 1점

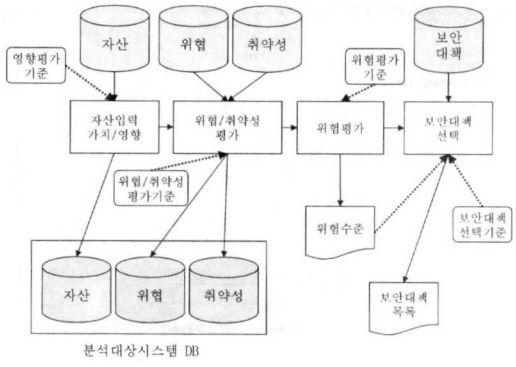


그림 2. 프로토타입 개발을 위한 시스템 구성도

Ⅳ. 제시한 방법론의 프로토타입 및 모듈 구현

본 프로토타입은 상위 위험분석을 통하여 분석 대상 시스템을 이미 선택한 후 해당 시스템에 대한 상세 위험분석의 수행하는 절차와 평가 알고리즘이 구현되어 있다. 개발 플랫폼은 Windows 시스템이고, 개발에 사용한 프로그램은 Visual Basic 6.0과 Microsoft Access 2000이다.

위험분석·평가를 위한 자동화 도구의 주요 구성요소는 다음과 같다.

- 자산, 위협, 취약성 및 보안대책이 저장된 DB
- 분석 대상 시스템에 대하여 식별된 자산, 위협 및 취약성 목록과 평가 결과가 저장되는 DB
- 자산 가치, 위협 및 취약성의 심각성, 위험 수준, 그리고 보안대책 선택을 위한 평가 기준
- 분석 대상 시스템의 자산, 위협 및 취약성 평가 결과를 기록하기 위한 입력 모듈
- 위험 수준 평가 결과와 제안하는 보안대책 목록을 보여주는 출력 모듈
- 자산 가치, 위협 및 취약성 평가, 위험 수준, 그리고 보안대책 우선 순위를 결정하기 위한 알고리즘

모듈 개발을 위한 프로토타입의 전체적인 구성은 다음의 그림과 같다. 모듈은 자산평가, 위협평가, 취약성 평가, 보호대책 제시 모듈로 구성되어 있다. DB는 자산, 위협, 취약성, 보호대책에 대한 데이터들로 구성되어 있고, 각 DB는 서로 상관관계를 가지고 있다.

위험분석 수행을 위한 기본 자료가 수록되어 있는 자산 데이터베이스 테이블에서 분석 대상 시스템에 해당되는 항목을 위협과 취약성 테이블에서 선택하고 각 자산의 가치를 평가하여 새로운 테이블에 저장한다. 그 다음 각 자산 항목에 대한 위협과 취약성을 평가하고, 이를 기반으로 위험 수준을 평가하며, 평가된 위험 수준에 대응하는 보안대책을 선택하여 목록화하여 제시한다.

프로토타입 개발 절차는 다음과 같이 진행되었다.

- 위험분석에 필요한 데이터베이스의 스키마 분석
- 입출력 화면 설계
- 평가 알고리즘 설계
- 데이터베이스 테이블, 입출력 화면 및 알고리즘 코딩
- 샘플 데이터를 이용한 알고리즘 검증

프로토타입에 구현된 위험분석 절차는 자산 평가, 위협 및 취약성 평가, 위험 평가, 그리고 보안대책 선택의 네 가지 주요 단계로 되어 있으며, 각 단계는 위험분석의 진행 절차와 동일하다.

프로그램을 실행하면 전체 4개의 명령구조로 구성된 화면이 출력된다. 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.

○ 자산 식별 및 평가

자산 식별 메뉴를 선택하여 자산을 입력하고, 자산식별의 다음 단계로 분석 대상 자산에 대한 평가가 이루어지는데, 다음의 그림과 같은 화면으로 구성된다.

평가기준의 출력은 해당자산이 그림과 같이 고객 매출정보와 같은 데이터 자산인 경우에는 가용성, 무결성, 기밀성의 정성적인 척도로 평가하도록 하고,

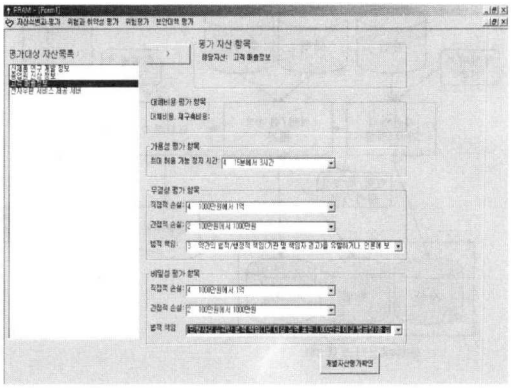


그림 3. 자산식별 및 평가 화면

비데이터 자산인 전자우편 서비스 제공 서버와 같은 하드웨어 자산인 경우에는 아래의 그림과 같이 대체비용의 항목만 표시하도록 함으로써 구별된 평가를 수행하도록 하고 있다.

○ 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 사전에 결정된 테이블의 값을 참조하도록 한다.

위험평가 항목을 선택하게 되면 위험 평가 결과 화면이 나타나게 된다. 아래의 그림에 나타나 있듯이 개별 자산의 자산 그룹과 세부 자산별로 그룹핑을 한 형태로 요약한 테이블로 제시가 된다.

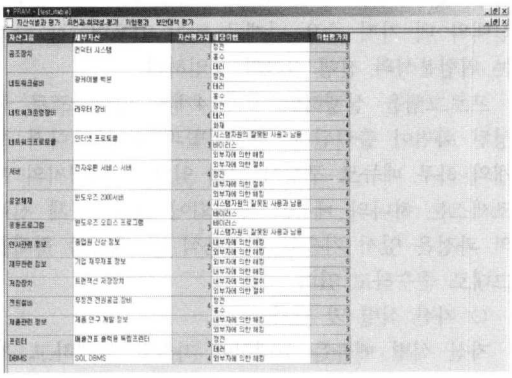


그림 4. 위협 및 취약성 평가 화면

이러한 표를 통해서 전반적인 자산과 위협간의 관계와 그 평가치를 요약하여 확인 가능하고, 이러한 위험에 대한 분석이 완료되면 다음의 단계인 보안대책에 대한 평가의 과정이 수행되게 된다.

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 그림과 같이 나타나게 된다.

그림 5. 보안대책 평가 화면

V. 결 론

본 논문에서는 국내 적용이 가능한 실용적인 위험분석·평가 방법론을 설계하기 위하여 캐나다의 CSE에서 발표한 위험관리 방법론, 미국의 NIST에서 발표한 FIPS 65 정보보호관리지침에서의 위험분석 방법론, 그리고 영국 BS7799 위험분석 방법론과 ISO/IEC JTC1 SC27 GMITS의 위험분석 방법론을 분석하였다. 또한 기존의 다양한 방법들을 모두 근거로 한 통합적인 취약점 분석 방법론인 VAF, 미국 카네기멜런 대학에서 개발한 정보보호 위험평가 방법론인 OCTAVE, CSI에서 제공하는 IPAK 등 대표적인 취약점 분석 방법론들에 대해서 살펴보았다.

이러한 분석들을 통하여 위험분석을 수행하는 절차와 각 절차를 수행하기 위한 평가기준의 관점에서 방법론을 제시하고, 각 평가절차에 대한 모듈을 개발하여 위험분석 수행 알고리즘을 구현하였다.

본 논문을 통하여 국내의 위험분석에 대한 연구로 활용이 가능하고, 이를 활용하여 위험분석에 관한 연구의 한 단계 진보가 가능하리라 판단된다.

향후 자산, 취약성, 위협, 그리고 보안대책의 세부적인 분류와 구성요소들간의 상호관련성에 대해서는 좀 더 추가적인 연구가 필요하다. 또한 제시한 방법론에 대한 프로토타입의 구현을 자동화 위험분석

도구의 개발로 확장할 예정이다.

참 고 문 헌

[1] FIPS-65, "Guidelines for Automatic Data Processing Risk Analysis", NIST, 1975

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

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

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

[5] http://www.bsi-global.com/Products+Services/Standards+Kits/insec.xalter

[6] JIPDEC Risk Analysis Method(KRAM), 1992

[7] 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.

[8] 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.

[9] 한국전산원, 전산망 보안을 위한 위험관리 기술지원서, 1994

[10] 한국전산원, 위험분석 방법론 및 자동화 도구 기술 이전 교육 교재, 1998.

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

[12] OCATVE Method Implementation Guide Version 2.0, OCTAVE, 2001. 6,

[13] OCTAVE, "OCATVE Criteria, Version 2.0", Carnegie Mellon Software Engineering Institute, 2001.12

정 윤 정(Yoon-Jung Jung) 정회원

1997년 : 성균관대학교 정보공학과 (공학사)

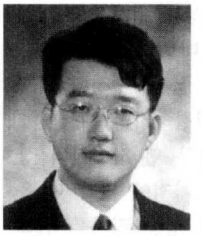
1999년 : 성균관대학교 전기전자 및 컴퓨터 공학부 석사 (공학석사)

1999년~2000년 : 하나로통신

2000년 11월~현재 : 국가보안기술연구소 연구원

<주관심 분야> 컴퓨터 및 네트워크 보안, 정보이론, 위험분석

김 인 중(Injung Kim) 정회원



1990년 : 충남대학교 전자공학과 (공학사)

1992년 : 충남대학교 전자공학과 (공학석사)

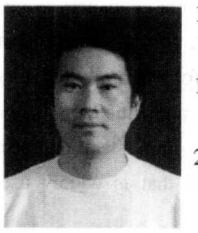
2001년~현재 : 성균관대학교 전기전자및컴퓨터공학부 박사과정

1992년~2000년 : 국방과학연구소 선임연구원

2000년~현재 : 국가보안기술연구소 선임연구원

<주관심 분야> 응용 보안 기술, 보안 소프트웨어, 위험분석

이 철 원(Cheol-won Lee) 정회원



1987년 : 충남대학교 수학과 (이학사)

1989년 : 중앙대학교 전자계산학과(이학석사)

2001년 : 아주대학교 컴퓨터공학과 박사과정 수료

1989년~1996년 : 한국전자통신연구원 선임연구원

1996년~2000년 : 한국정보보호센터 선임연구원/통신 모델링 과제책임자

2000년~현재 : ETRI부설 국가보안기술연구소 팀장

<주관심 분야> 컴퓨터 및 네트워크 보안, 정보통신 기반보호, 정보보호시스템 평가기준