情 報 保 護 學 會 誌
第 11 券 第 3 號, 2001. 6

정보기술 위험관리 과정과 기법

김 정 덕*, 이 성 일**

요 약

위험관리는 정보기술 보안관리의 초석이라고 할 정도로 매우 중요하고 비용효과적인 보안대책을 구현, 운영하기 위해서는 반드시 실행되어야 하는 과정이다. 특히 최근의 보안관리체계 인증에 대한 수요가 점증되면서 위험관리의 중요성이 대두되고 있다. 본 고에서는 위험관리 과정에 대한 표준문서의 내용을 요약 정리하였고 새로운 위험관리 기법의 발전방향인 시나리오 기반의 위험관리에 대해 소개하며 기존의 대표적인 위험분석 자동화 도구에 대한 비교분석을 수행하였다.

Ⅰ. 서 론

새로운 비즈니스 전략을 가능케 하는 enabler로서의 정보기술의 영향력이 점차 증대하고 있고 또한 인터넷을 통한 e-비즈니스의 활성화라는 새로운 경영 및 기술환경 변화에 정보기술이 차지하는 비중이 점차 높아지고 있다. 이에 따라 조직에서 사용하고 있는 정보기술에 대한 여러 위험 가능성도 점증하고 있어 보안관리의 필요성이 현안으로 대두되고 있다.

이중에서 보안관리의 핵심은 위험관리(Risk Management)로서 이는 정보자산에 대한 가치 평가와 정보자산의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 다양한 위협에 대해 시스템의 취약성을 인식하고, 이로 인해 예상되는 손실을 분석하는 위험(기대손실규모)분석 과정과 이에 기초하여 경영층이 허용할 수 있는 수준까지 위험을 감소시킬 수 있는 비용효과적인 대응책을 선정, 제시하는 일련의 과정이다.

이렇게 중요한 비중을 차지하는 위험분석 및 관리가 조직에서 회피되거나 무시된 이유는 첫째, 새로운 정보기술에 대한 위협요인을 파악하기가 어렵고, 둘째, 정보기술 관리자의 위험관리에 대한 인식 및 전문 지식이 결여되어 제대로 수행하기 어렵고, 셋째, 과거 적절치 못한 위험분석 방법 사용으로 인한 잘못된 경험으로 인한 오해 및 편견이 존재하며, 마지막으로 위험분석은 오랜 시간 및 많은 자금의 소요가 초래되고 있기 때문이라고 할 수 있다[16].

본 고에서는 위험관리의 보편적 활용을 위해 위험관리 방법론과 위험관리 기법의 발전 방향을 살펴본 후, 대표적 위험관리 자동화 도구에 대해 소개한다.

Ⅱ. 위험관리와 위험분석 과정 및 기법

위험관리는 정보기술 보안관리에서의 초석으로서 조직의 자산을 보호하기 위해 자산에 대한 위험을 분석하고, 비용 효과적인 측면에서 적절한 보호 대책을 선정하도록 지원하여 위험을 감수할 수 있는 수준으로 유지·관리하는 일련의 과정이라고 정의할 수 있다[4]. 위험분석은 위험관리의 주요 핵심 과정으로서 자산의 취약성을 식별하고 존재하는 위협을 분석하여 이들의 발생 가능성 및 위협이 미칠 수 있는 영향을 파악해서 보안 위험의 내용과 수준을 결정하는 과정이다. 위험관리의 과정을 도식화하면 그림 1과 같다.

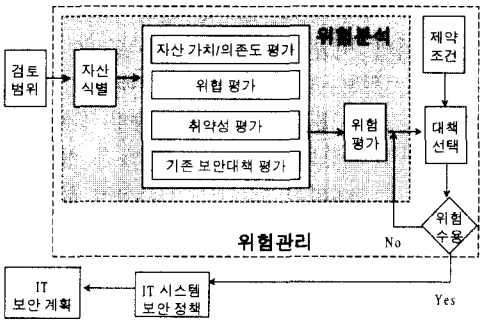
위험관리 과정은 다음과 같이 6 단계로 구분할 수 있다.

1) 자산분석 : 보호해야 할 전산 자원들의 체계적인 분류를 통해 소유하고 있는 자산들의 가치를 평가하고 이는 정량화 된 가치를 추출한다면 위험분석 과정을 통해 보호해야 할 기준이 마련되고

* 중앙대학교(jdkim@cau.ac.kr)
** 사이버패트롤(shooter@cyberpatrol.co.kr)

에에 대한 대책도 강구되므로 가장 중요한 기본적인 단계이다.

2) 위협분석 : 분류되고 가치가 평가된 자산들이 어떤 위협요소가 있는지 알아내는 단계인데, 여기에는 그 위협적인 요소가 얼마나 발생할 확률이 있는지를 분석하는 것도 포함된다.
3) 취약성분석 : 취약성은 정보 시스템이나 조직 목표에 손해를 끼치는 원인이 될 수 있는 조직, 절차, 인력관리, 행정, 하드웨어와 소프트웨어 등의 약점을 확인하고 분류하여 위협을 감소시키도록 하는 것이다.
4) 위험평가 : 자산분석과, 위협요소분석, 취약성분석을 거쳐 자산에 대한 손실을 평가 분석하는 과정으로서 위험분석의 정량적, 정성적, 혼합 등의 방법론으로 나누어진다.
5) 대책 분석 : 평가된 각각의 위협요소 및 취약요소에 대한 대책(Safeguard)을 선정하는 과정으로서 이를 구현하였을 때 드는 비용계산 등이 이 과정에서 필요하다.
6) 비용효과 분석 : 비용효과분석 과정은 위험분석 과정을 거쳐 대책 선정을 할 때 논리적 근거를 마련하는 과정으로서 이는 위험을 줄이기 위한 결과를 정량적으로 혹은 정성적으로 보이기도 한다.



〔그림 1〕 위험관리와 위험분석 과정

2.1 자산분석

위험분석 과정에서 자산을 정의하고 분류하는 것은 가장 중요한 일이다. 이러한 자산의 정의에 의하여 무엇을 보호해야 할 지와 보호되어야 할 자산의 가치를 결정할 수 있다. 과거에는 위험분석 작업이 물리적인 하드웨어에 한정되었으나, 요즈음은 전산망을 통하여 송수신되는 데이터가 가장 중요한 자산으로 취급되기도 할 만큼 전산망에서의 위험분석이 절 실히 요구되고 있다. 정보자산의 예로는 컴퓨터 하드웨어/소프트웨어, 네트워크, 데이터베이스, 정보, 직원, 시설, 응용프로그램, 주요 문서 등을 들 수 있다. 이러한 정보자산에 대해 자산의 가치, 다른 자원들과의 공유 여부, 조직이나 기능에 대한 민감성 여부, 소유권, 물리적 위치 등을 파악해야 한다.

〔표 1〕 정보자산 유형 분류 (BS7799의 경우)

[illegible]	[illegible]
정보자산	DB/Data File, 시스템문서, 사용자 지침서, 연수자료, 업무절차 등
문서자료 자산	계약서, 지침, 회사 서류 등
소프트웨어 자산	시스템,응용, 개발도구, 유틸리티 등
물리적 자산	컴퓨터 및 통신장비, 자기매체, 기타 지원장비, 가구, 주거시설 등
인적 자산(사람)	직원, 고객 등
이미지	회사이미지 / 평판
서비스	컴퓨터 및 통신 서비스, 기타 기술 서비스

정보자산의 가치를 산정 하는 것은 매우 어려운 작업이라고 할 수 있다. 정보자산의 가치는 조직 및 비즈니스에 미치는 영향력을 기반으로 산정하며 자산의 속성에 맞게 정성적/정량적 방법으로 가치를 평가할 수 있다. 즉 정량적 방법은 자산 도입 비용, 복구비용, 교체 비용을 기준으로 하고 있으며, 정성적 방법은 업무처리 기여도, 영향을 미치는 조직/사람의 수, 보안 속성(기밀성, 무결성, 가용성)에 대한 영향도 등을 기준으로 하여 평가한다[19].

〔표 2〕 정보자산 가치평가 방법

구분	기준	기준 내역
정량적 기준	자산 도입 비용	시스템 구축 시에는 그대로 적용 가능. 단, 운영 시에는 감가상각비용을 고려해야 함. 무형 자산(인력, 데이터, 보안 정책 등)에 적용이 어려움
	자산 복구 비용	무형자산은 기급적 정성분석이 적당하나 요구에 의해 정량분석을 할 경우는 다음을 따른다. -시스템관리자 : value = 시스템관리자수당/hr * 복구시간(보안 사고 발생 시 수동으로 업무를 대신하기까지 걸리는 시간) + 기회비용 -데이터 : value = 직접 비용(복구비용) + 간접비용(가치 중요도 기준 예상 영업 손실비용) = { 복구시간(hr)(복구나 재생에 걸리는 시간) * 복구 인력수당/hr + 기회비용 } + { 매출액 대비 downtime동안의 예상 영업 손실비용 * (정성 산출값(1~5)/5+1)}
	자산 교체 비용	유형 자산 가치산정에 이용. 하드웨어와 같이 성능 대비 가격 변화가 큰 자산에 대해 도입 비용 보다 교체 비용으로 가치산정함. -시설(Facilities) : Value = 해당 자원을 동작시키는데 필요한 인건비(시스템 관리자 비용) -장비(Equipment) : Value = 실제 구입 비용 + 유지보수 비용 -Software : •상업용 Value = 구매비용 + 장애사고 시에 무료 보상이 가능할 수 있으므로 보증 정보 •응용 Value = 재 개발비+기회비용 -Records and Files : Value = 자기적 장치 도입 비용 * 수(데이터가 갖는 정보가치 산정은 제외)

<table>
<tr><th>구분</th><th>기준</th><th>기준 내역</th></tr>
<tr><td>정성적 기준</td><td>•자산의 업무처리 기여도
•영향을 미치는 조직 및 직업 수
•복구 시간
•기타</td><td>무형 자산 가치산정에 이용. 각 고려사항 항목별로 1~5 까지의 등급을 주고 총 평균을 가치 등급으로 정함.
<table>
<tr><th>등급</th><th>설명</th></tr>
<tr><td>Very High (Scale : 5)</td><td>중요도가 가장 높은 경우</td></tr>
<tr><td>High (Scale : 4)</td><td>중요도가 비교적 높은 경우</td></tr>
<tr><td>Medium (Scale : 3)</td><td>중요도가 보통인 경우</td></tr>
<tr><td>Low (Scale :2)</td><td>그다지 중요하지 않은 경우</td></tr>
<tr><td>Negligible (Scale : 1)</td><td>중요하지 않은 경우</td></tr>
</table></td></tr>
</table>

2.2 위협분석

위험분석 및 관리의 최종목적은 자산을 여러 위협(threat)으로부터 안전하게 보호하고자 하는 것이므로 위험분석은 한 조직 또는 자산에 해를 끼칠 수 있는 가능한 모든 위협들을 찾아내고 그것의 발생확률 및 그것이 미칠 수 있는 피해정도를 평가하는 것, 즉 위협분석을 포함해야 한다. 위협이란 위험분석을 위해 고려하고 있는 자산(asset)에 해를 줄 수 있는 위험의 원천을 말하는 것으로 자산가치 평가 다음으로 수행해야 할 위험분석 요소이다. 각 위협들은 위협원천에 따라 크게 자연재해에 의한 것과 인간에 의한 것일 수 있으며 인간에 의한 위협은 다시 의도적인 위협과 비의도적인 위협으로 나눌 수 있다. 위협분석이란 자산에 해를 입힐 수 있는 가능한 모든 위협들을 규정하고 적절한 방법으로 분류하여 각 위협들의 성질을 파악하는 것이며 위협평가(threat assessment)는 이러한 위협들의 발생확률(probability of occurrence) 또는 발생빈도(frequence)와 자산에 해를 입히는 정도(severity)를 평가하는 것을 말한다[6][17].

〔표 3〕 일반적 위협유형 분류

<table>
<tr><th colspan="2">분류기준</th><th colspan="2">위협항목</th><th>위협내용</th><th>관련자산</th></tr>
<tr><td colspan="2">자연</td><td colspan="2">자연재해</td><td>시스템 전체에 대한 위협</td><td>물리, 정보자산</td></tr>
<tr><td colspan="2"></td><td colspan="2">정전</td><td>데이터 상실, 프로세싱 에러, 처리지연</td><td>소프트웨어 자산</td></tr>
<tr><td rowspan="6">사람</td><td rowspan="4">의도적 (빈도 점점 증가)</td><td rowspan="2">물리적 공격</td><td>하드웨어 파괴</td><td rowspan="2">물리적 접근이 가능할 때 발생. 접근제어로 차단 가능</td><td>모든 하드웨어(전산실, 단말기, 통신장비, 미디어 등)</td></tr>
<tr><td>절도</td><td></td></tr>
<tr><td colspan="2">기술적 공격</td><td>시스템 자원의 불법 사용, 불법 접근, 통신 선로 공격(도청, 데이터 변경/삽입/삭제), 시스템 사용방해(시스템 전체 down, 일부 프로그램 방해, 사용부인) 위조, 위장, 유해프로그램 삽입, 망분석</td><td>모든 하드웨어, 소프트웨어, 정보 자산</td></tr>
<tr><td rowspan="3">비의도적</td><td colspan="2">조작미숙</td><td>명령어 입력 오류, 잘못된 데이터 입력, 프로그램 작성 오류</td><td rowspan="3">OS, 소프트웨어 등 정보 자산</td></tr>
<tr><td colspan="2">조작실수</td><td>명령어 입력 실수, 부적절한 프로그램 실행</td></tr>
<tr><td colspan="2">데이터 누출</td><td>사용자 부주의로 비밀번호/기타 정보 누출</td></tr>
<tr><td rowspan="3">시스템 결함</td><td colspan="2">운영체제의 결함</td><td>백도어, 트랩도어</td><td rowspan="2">소프트웨어, 정보자산</td></tr>
<tr><td colspan="2">프로그램 결함</td><td></td></tr>
<tr><td colspan="2">과부하</td><td>동시 여러 사용자, Job 수행, 데이터 손상</td><td rowspan="2">HW,SW,정보자산</td></tr>
<tr><td colspan="2">하드웨어 고장</td><td></td></tr>
</table>

2.3 취약성 분석

취약성은 정보 시스템이나 조직 목표에 손해를 끼치는 원인이 될 수 있는 모든 정보자산 내의 약점을 의미한다. 취약성의 정의는 정확히 내리기 어려우며, 자산의 속성, 통제의 결여, 위협과의 상호관계 측면에서 고려될 수 있다. 취약성 분석은 자산, 위협, 위협에 따른 영향, 기존 보안 대책 등과의 연관관계를 고려해야 하며, 보호대책들이 적용되더라도 그대로 남아있거나 근본적으로 내재되어 있는 취약성에 대한 분석이 되어야 한다. 위협이 이용할 수 있는 취약성 항목을 관계 짓고, 그 연관 정도를 결정해야 한다. 연관 정도를 결정하기 위해서는 다음 항목들을 고려해야 한다. 취약점이 위협에 의해 사용된 경우 그 피해 규모는 어느 정도인가? 그리고 그 취약점은 얼마나 오래된 것인가?(위협에 노출될 확률)

취약성과 관련된 위협의 C(Confidentiality), I(Integrity), A(Availability) 영향력에 따라서 취약성을 기밀성, 무결성, 가용성에 따라 분류하여 평가할 수도 있다. 즉, 위험평가에서도 자산별 손실수준 측정 외에 시스템/어플리케이션에 대한 C, I, A를 파악할 수 있다.

취약성은 주로 3개의 유형으로 분류된다. 즉, 관리적, 물리적, 기술적 취약성이다. 관리적 취약성은 보안 관리, 인원 관리, 절차상 관리, 사고대책 관리를 포함하며 기술적 취약성은 H/W, O.S, 응용 S/W, 네트워크, 데이터 베이스 등에서의 취약성을 의미한다. 또한 물리적 취약성은 출입 통제나 환경관리 상의 취약성을 의미한다. 취약성은 일반적으로 다음과 같은 4-point scale에 기초하여 정성적으로 평가한다: 1) 매우 중요 : 많은 비용 또는 장기적 실시 기간을 필요로 하는 것, 행동을 개시하기 이전에 조직 경영자에 의한 충분한 분석이 필요하다, 2) 중요 : 기업 경영에 매우 중요한 영향을 미친다. 따라서 시급히 대책이 세워져야 한다, 3) 보통 : 기업 경영에 큰 압력을 가하는 것은 아니지만 심한 손실을 유발시킨다. 가능하면 1년 이내에 대책이 수립되어야 한다, 4) 경미 : 기업 경영에 영향을 미치는 것은 아니므로 교육, 경계심 등을 통하여 대처한다.

2.4 위험 평가

위험분석이란 정보시스템과 그 자산의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 다양한 위협에

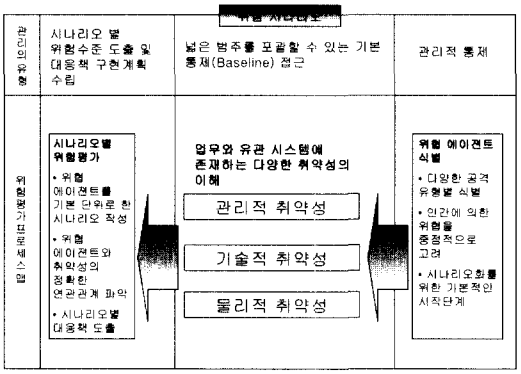
대해서 시스템의 취약성을 인식하고, 이로 인해서 예상되는 손실을 분석하는 것이다. 위험분석과정은 자산, 위협, 취약성, 보안대책, 그리고 손실을 계산하는 여러 요소들 간에 관계를 분석하는 것이다. 정보기술에 대한 위험분석에서 많이 사용되는 과거자료를 근거로 한 통계적 분석, 수학공식 접근법, 주관적 추정 접근법(3점 및 다점), 확률분포(추정법, 델파이법, 순위법), 시뮬레이션/시나리오 접근법 등이 있다[2][5][9][11][17].

III. 위험관리 기법의 발전방향

정보보호를 위해 기술적 능력이 요구되는 것은 분명한 사실이지만 정보보호 체계의 근간을 형성하고 있는 관리적 기반(전사적 차원에서의 조직적 지원)이 없을 경우 기술은 내재된 기능을 효과적으로 발휘할 수 없다. 즉, 정보보호 분야에서의 기술은 효과적이고 효율적인 관리를 위한 도구(Tool)의 역할을 수행한다고 볼 수 있다. 정보보호를 위한 대표적인 관리적 기반인 위험관리 역시 위험을 구성하고 있는 위협, 취약성, 자산, 대응책과 조직의 구조, 업무프로세스, 구성원, 문화, 구성원의 심리적 상태 등을 종합적으로 고려해야 한다. 기존의 위험관리 방식에서 현실과의 갭을 많이 느낄 수밖에 없었던 이유는 단일 시스템 기반으로 위험을 관리하는 방법을 이용하였기 때문에 업무시스템이 아닌 조직의 업무와 업무프로세스, 업무 문화와 항상 접하는 조직 구성원의 공감을 이끌어 내는데 어려움이 있었기 때문이다.

향후의 위험관리 방식은 이전 단락에서 언급하였던 공감의 문제를 해결하는데 초점을 두어야 하고 공감의 문제를 해결하기 위해 본 논문에서 제시하는 방법론이 바로 시나리오 기반의 위험관리 방법인 것이다[13]. 시나리오 기반 위험관리 방법론의 중심적인 고려대상은 기존의 많은 통계 자료들과 문헌에서 확인할 수 있는 가장 대표적 위협 에이전트인 인간이다. 시나리오 기반의 위험관리 방법론은 인간에 의해 발생될 수 있는 가장 현실적인 위험을 시나리오로써 정리하고 단일 시나리오가 나타내는 위험수준을 결정하는 위험평가 과정과 시나리오 상의 위험에 대응할 수 있는 기술적, 관리적, 심리적, 문화적 대응책 도출, 구현계획 수립, 조직적 차원의 구현으로 이끌어 내는 대응책 구현과정으로 구성된다.

그림 2는 시나리오 기반의 위험관리 방법을 도식화한 내용이다.



〔그림 2〕 시나리오 기반의 위험관리 모델

본 고에서는 시나리오 기반 위험관리 실행을 위한 조직 구성원의 기본 요건과 위험관리 담당자의 고려사항, 그리고 시나리오 작성의 기본 자료인 위협 에이전트에 대해 간략히 기술하고자 한다.

3.1 조직 구성원의 기본요건

조직에 새로운 위험관리 방법을 도입하기 이전에 중간관리자들은 누군가에 의해 조직 내 시스템에 부적절한 행위가 이루어진다는 가정 하에서 조직 구성원들을 대상으로 다음의 3가지 부분에 대한 자체적인 정보보호 관점의 반응형태를 파악해야 한다.

- 행위 자체의 옳고 그름을 판단할 수 있는 인식 부분
- 부적절한 행위를 문제/사고라는 관점에서 인식하고 실질적/적극적으로 대응하는 수준
- 부적절한 행위를 처리/보고하는 정형화된 사고대응 체계의 이해 정도

위의 세 가지 부분의 평가 결과에 대해 중간관리자가 만족할 수 있다면 문제가 발생하지 않겠지만 만족할 수 없다면 새로운 위험관리 방법의 도입 이전에 정보보호 인식 훈련 및 정보보호 정책 수립, 등 위험관리 이전에 구축되어야 하는 정보보호 기반 체계 구축이 선행되어야 한다.

3.2 시나리오 기반 위험관리를 위한 담당자 고려사항

효과적인 시나리오 기반의 위험관리를 위해서는

다음의 세 가지 요인이 고려되어야 한다.

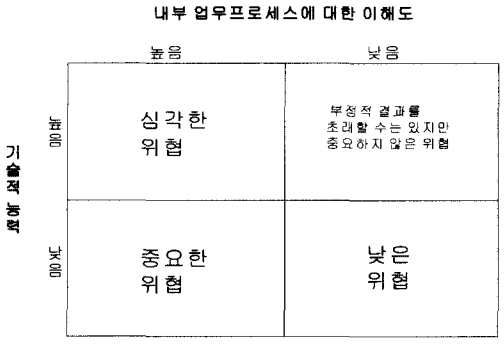
첫째, 조직의 업무목표 달성 관점에서 조직 내 정보자산의 가치를 파악해야 하고 만약 정보자산이 손상, 노출되어 위험으로 발전될 경우를 가정하여 위험을 평가하고 관리해야 한다.

둘째, 조직 차원의 정보자산 관리 방식이 기존 정보보호 정책의 준거 범위 내에서 계층화, 레이블화(Label)되어야 한다. 시나리오 상에서 위협에이전트의 능력은 다양하게 나타날 수 있지만 공격대상인 정보자산의 관리방식은 일관성을 나타내야 한다.

셋째, 위험을 발생시키는 가장 큰 원인은 인간이라는 사실에 항상 주목해야 한다. 인간에 의해 나타날 수 있는 다양한 형태와 능력의 위협을 고려해야 한다.

3.3 시나리오 작성을 위한 위협 에이전트의 식별 - 인간에 의한 위협

위험 시나리오 작성을 위해서는 두 가지 축으로 잠재적인 위협 에이전트를 분류해야 한다. 두 가지 축은 위협 에이전트의 기술적인 능력(성숙도)을 나타내는 수직 축과 내부 업무 프로세스에 대한 이해 정도를 나타내는 수평축으로 구성된다. 두 가지 축 중 어느 한가지라도 능력이 부재할 경우 시나리오적 접근 자체가 불필요한 단순 시스템 절도 정도 수준의 위협으로 볼 수 있다. 즉, 가시적인 금전적 피해 외의 무형의 피해를 창출할 수 있는 능력은 없는 것으로 간주한다.



〔그림 3〕 인간에 의한 위협의 분류

그림 3에서 나타난 위협의 4가지 수준에 대한 설명은 다음과 같다.

- 심각한 위협: 내부 업무프로세스에 대한 높은 이해도를 가진 숙련된 기술 인력이 악의를 품었을 경우에 나타낼 수 있는 가장 심각한 위협
- 중요한 위협: 가장 빈번하게 나타나는 위협으로 중점적으로 시나리오가 작성되어야 하는 부분이며 일반적으로 컴퓨터 범죄에서 가장 높은 부분을 차지하고 있는 내부인의 위협을 의미한다.
- 부정적 결과를 초래할 수 있지만 중요하지 않은 위협: 일반적으로 외부의 침입자나 신입 직원의 실수로 인해 나타날 수 있는 위협
- 낮은 위협: 기술적 능력과 내부 업무프로세스에 대한 이해도가 모두 낮기 때문에 중요하지 않은 낮은 위협으로 분류되며 시나리오 작성 대상에서 제외된다.

IV. 위험관리 방법론 및 자동화 도구

위험관리 방법론이란 위험관리 수행을 위한 절차 및 기법과 관련 산출물을 규정한 하나의 체계라고 정의할 수 있다. 1979년 미국 NIST (National Institute for Science and Technology)에서 발행한 자동화된 데이터 처리에 관한 위험분석[2]이 최초로 많은 작업이 이루어졌으며 ISO에서도 보안관리 표준화 작업 일환으로 위험관리 모델 및 위험분석 절차[4]를 규정하고 있다. 또한, 미국, 영국, 캐나다, 일본 등 여러 국가에서 자체적인 위험관리 모델을 개발하였다. 미국의 표준기구인 NIST에서는 FIPS 966 위험관리 표준을 개발하여 사용을 권장하였고 미 법무성에서는 기존의 방법론이 매우 복잡하고 어렵다는 단점을 완화하기 위해 위협과 손실부분을 제거한 매우 단순화된 방법론인 SRAG (Simplified Risk Analysis Guideline)[12]를 제시하였다. 영국에서는 공공기관에의 위험분석을 의무화하고 있으며 CRAMM[7]을 표준기법으로 제정하여 사용을 권고하고 있다. 또한 영국 표준인 BS7799중 1부를 국제 표준화하여 ISO17799로 제정하고 있고, 보안관리체계 인증을 위한 문서인 2부에서는 위험분석 수행을 필수조건으로 하고 있다. 캐나다에서는 위험분석 지침(A Guide to Risk Assessment and Safeguard select for ITS)을 개발하여 사용을 권장하고 있다. 일본에서는 1992년에 일본정보처리개발협회에서 JRAM(일본위험분석기법)을 발표하여 나름대로 실용적인 방법론을 개발하여 사용을 권고하고 있다.

현재 50여 개의 상용 위험분석 자동화 도구들도

나름의 방법론과 모델을 따라 구현되어 있다. 자동화 도구는 위험분석에 걸리는 시간과 비용을 단축시킬 수 있다는 장점이 있으나 입력되는 자료에 대한 실질적인 검증절차 기능이 약하고 분석결과에 대한 분석 담당자의 검증 및 해석이 필요하다는 단점이 있다.

이중에서 대표적인 위험분석 도구인 BDSS, Buddy System, Control-IT, CRAMM, AnalyZ를 소개한다. BDSS는 위험분석 기법에 통계 알고리즘을 최초로 적용한 위험분석 소프트웨어로서 기존의 문제점을 고려한 정량분석 및 정성분석 허용하고 있으며 다단계 이벤트 트리의 계층적 구조로 구성된 질문들을 데이터베이스화한 특징이 있다. 그러나 무형자산 분석 능력이 미흡하고 수학적 통계 모델을 적용하기 어려운 단점이 있다.

Buddy System은 취약성, 대응책, 위협, 자산, 정보분석을 위한 위험분석 소프트웨어로서 ISO 정의에 상충하는 5가지 명제를 바탕으로 알고리듬 구성하고 있으며, 보다 정확한 분석을 위해 분석 대상 시스템 환경의 특성을 반영할 수 있도록 커스터마이징 요소를 포함하고 있다. Riskpac, BDSS, CRAMM 등 타 위험분석도구에 비해 비용효과 비율이 상대적으로 우수하고 유지보수비용이 저렴하다는 장점이 있으나, 정보보안 전문가에 의해 적절한 시나리오를 공급하는 Dynamic Approach가 요구된다.

〔표 3〕 자동화 위험분석 도구

명칭	방법론	명칭	방법론
ARES	정량적	JANBER	정성적
@RISK	정량적	LAVA	정량/정성적
BDSS	정량/정성적	LRAM	정성적
The Buddy System	정성적	MARION	정량/정성적
Control Matrix Methodology for Microcomputers	정성적	Micro Secure Self Assessment	정성적
COSSAC	정량적	MINIRISK	정성적
CRITI-CALC	정량/정성적	Predictor	정량적
CRAMM	정성적	PRISM	정량적
GRA/SYS	정량적	QuickRisk	정량적
IST/RAMP	정량적	RA/SYS	정량적
RANK-IT	정량적	RISKPAC	정량/정성적
RISKCALC	정량적	RISKWATCH	정량/정성적

Control-IT은 조직 내 보안 담당자들의 의견을 수렴하는 델파이 기법을 이용한 전반적 위험측정용 위험분석 소프트웨어로서, 위험요소의 정도가 수치나 통계에 의해 분석되지 않고 상대적 순위로 나타나며 따라서 조직내의 보안담당자나 전문가의 확보가 필수적이라 할 수 있다. 조직 내 보안 담당자나 전문가들이 식별하는 위험요소에 주관적 판단이 개입될 가능성이 있으며, 기대 손실치나 취약성 산출 등의 기능이 없으므로 정확한 위험분석은 불가한 단점을 가지고 있다. 따라서 전반적인 수준의 위험분석을 수행할 시에 Control-It를 활용하고, 이후 세밀한 위험분석 작업을 추가적으로 하는 것이 보다 효과적이라고 할 수 있다.

CRAMM은 구조화된 정성적 방법을 사용하고 있으며 대규모의 데이터베이스를 보유하고 있으며 약 3000여 개의 계층적인 보안대응책을 보유하고 있는 영국에서의 공공기관에서 사용되는 소프트웨어이다. 그러나 너무 많은 산출물을 표준으로 하고 있으며 포맷 수정/변경이 불가능하며 또한 사용이 난해하여 많은 경험을 요구하고 있다.

AnalyZ는 조직의 중앙 보안 부서에서 정보시스템의 Project분석에 주로 사용되며 위험분석 과정이 비교적 간단하며 암호화, 접근제어 등 자체적인 보안기능을 보유하고 있다. 그러나 위험관련 질문 유형이 외국 전산환경/상업 조직에 편중되어 있으며 단순히 정해진 사지선다형 질문을 통해 자료 입력이 가능해 조직 정보시스템의 특성을 반영하기 힘들며 또한 질문 내용의 공정성이 모호한 경우도 발견할 수 있다.

〔표 4〕 미국, 영국의 대표적 위험분석도구 비교

제품명	BDSS	BUDDY	Riskpac	Control-It	CRAMM	AnalyZ
개발자	Dr.Ozier	Dr.Buddy	Chemical Bank	Jerry Fitzgerald	CCTA(UK)	Zergo(UK)
가격	$ 14,900/copy	$ 2,500 /copy ($250/yr)	$ 9,000 /copy $ 2,500/yr)	$ 900 /copy	약 1천만 원	약 3천만 원
방법론	정량/정성	정성	정량/정성	정성	정성	정량/가능
알고리즘	Baysian	Risk Ranking	Risk Ranking	Control Matrix	Level Identification	
공급	O.P.A	Countermeasure Inc.	CSCI	Fitzgerald Associates	BIS Ltd.	Zergo Ltd.

현재, 국내에는 상용화된 개발 자동화 도구는 없으나 1996년 한국전산원에서 개발한 HAWK(Hankuk risk Analysis Watch-out Kit)이라는 일종의 프로토타입[15]이 있고, 1997년 Penta Security社에서 개발한 e-rat이라는 소프트웨어를 1999년 국정원 주관으로 e-rat 기반의 공공기관용 SW 개발하고 있는 상황이다.

V. 결 론

정보통신기반보호법의 제정과 더불어 국가 공공기관에서의 정보보호에 대한 위험분석 및 취약성 점검이 의무화되고 있으며 이와 관련하여 보다 적극적인 차원에서의 정보보호관리체계에 대한 인증의 필요성이 점차 대두되고 있다. 이에 본 고에서는 정보보안을 위한 위험분석 과정에 대한 표준 문서의 내용을 소개하였고 향후 위험관리 방법의 발전방향에 대해 소개하였으며 대표적인 위험분석 자동화 도구에 대한 간단한 비교분석을 하였다.

기존의 위험분석에 대한 불신과 현실과의 갭을 상쇄시키기 위해서는 향후의 전망을 수용한 표준화, 정형화된 위험분석 및 위험관리 방법론의 개발이 필수적인 요소이다. 향후 위험관리 방법론은 위협 에이전트의 성향에 기반한 시나리오적 접근법이 요구되고 있으며 위험분석 부문에서는 기존의 정형적인 절차인, 자산평가, 위협분석, 취약성분석, 기존 대응책분석, 위험분석을 국내의 현실에 부합하도록 자동화 모듈로 구현함으로써 대규모 업무와 정보자산에 대한 위험수준을 효율적, 객관적으로 산출할 수 있는 위험분석 자동화 도구의 개발이 요구되고 있다. 현재 약 50개의 분석도구가 상용화되어 시판 및 사용되고 있으나 국내 제품으로 상용화되고 있는 제품은 전무한 실정이며, 단지 프로토타입 정도가 개발된 실정이다. 2001년도에 접어들면서 위험분석에 대한 수요는 급증하고 있으나 자동화 도구 개발을 위해 준비작업을 수행하고 있는 업체는 소수에 불과하다. 향후 개발될 위험분석 도구가 국내 실정에 적합하면서 또한 나름대로의 효과성을 보이기 위해서는 이론적 배경, 실제 데이터 및 경험을 토대로 보다 심도 깊은 연구와 개발이 요구된다.

참 고 문 헌

[1] Commission of the European, Final and Strategy Report, Project S2014 - Risk Analysis, ReportNo. 9744 (S2014/WP08), Feb. 1993.

[2] FIPS PUB 65, Guidelines for Automatic Data Processing Risk Analysis, U.S. Department of Commerce/National Bureau of Standards, Aug. 1979.

[3] FIPS PUB 73, Guidelines for Security of Computer Applications, U.S. Department of Commerce/National Bureau of Standards, Jun. 1980.

[4] ISO/IEC JTC1/SC27 TR 13335-3, Guidelines for the Management of IT System Security: Part3-Techniques for the Management of IT Security, 1999.

[5] Keefer, Donald L. & Bodily, Samuel E., "Three-Point Approximations For Continuous Random Variables," Management Science, Vol.29, No.5, May 1983, pp.595-609.

[6] Moses, Robin., "Risk Analysis and Management," Computer Security Reference Book edited by Jackson, K. M. & Hruska, J. & Parker, Donn B., CRC Press, Inc., 1992, pp.227-263.

[7] CCTA, "CCTA Risk Analysis and Management Methodology(CRAMM)," Datapro Reports on Information Security, December 1992, pp. 101-110.

[8] DOT, Departmental Guide to Risk Assessment Planning, 1999.

[9] Ozier, Will., "Issues in Quantitative Versus Qualitative Risk Analysis," Datapro Reports on Information Security, March 1992, pp. 101-107.

[10] Perry, William E. & Kuong, Javier F., EDP Risk Analysis and Control Justification, Management Advisory Publications 1981.

[11] Rainer, Rex Kelly, Jr. & Snyder, Charles A. & Carr, Houston H., "Risk Analysis for Information Technology," Journal of Management Information Systems, 1991, Vol.8, No.1, pp.129-147.

[12] Department of Justice, Simplified Risk Analysis Guidelines(SRAG), 1990.

[13] Gartner Group, "2000~2001 Information Security Trend", 2001.

[14] TTA, 공공정보시스템 보안을 위한 위험분석 표준 - 위험분석 방법론 모델, 2000.

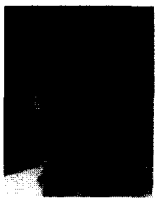
[15] 이재우 외 2인, 전산망 보안을 위한 위험분석 프로그램에 관한 연구, NCA, 1995.

[16] 김정덕, 김기윤, "정보시스템 위험분석과 관

리", 경영정보학회 학술대회, 1994.
[17] 김정덕, "정보보호를 위한 위험분석 방법: 분류와 선택기준", 한국정보보호학회학술대회, 1995.
[18] GAO, Information Security Risk Assessment, 1999. 8.
[19] CIAO, Practices For Securing Critical Information Asset, 2000

〈著者紹介〉

김 정 덕 (Jungduk Kim)
1979년 : 연세대학교 정치외교학과, 학사
1981년 : 연세대학교 경제학과 대학원, 석사
1986년 : University of S. Carolina, MBA
1990년 : Texas A&M University, Ph.D. in MIS
1991년 ~ 1993년 : 한국전산원, 선임연구원
1993년 ~ 1995년 : 원광대학교, 조교수
1995년 ~ 현재 : 중앙대학교, 부교수
관심분야 : 정보보호관리, 시스템감사, 전자상거래



이 성 일 (Seongil Lee)
1998년 : 중앙대학교 정보시스템학과, 학사
2000년 : 중앙대학교 대학원 정보시스템학과, 석사
2000년 : (주)사이버패트롤 보안사업본부 컨설팅서비스팀, 컨설턴트
관심분야 : 정보시스템 위험관리 및 업무지속성계획