해외의 보안위험분석 방법론 현황 및 분석

이 성만* , 이 필중**

A study on Security Risk Analysis Methods in Overseas

Sung Man Lee and Pil Joong Lee

요 약

정보시스템에 대한 위험분석 (risk analysis) 은 정보시스템의 보안상태를 분석 및 평가하는 것으로 정보시스템의 보안상 취약부분을 보완하기 위한 보안대책을 수립하는데 안내자 역할을 하게 된다 [1][2][3]. 정보시스템의 보안대책 및 위험관리는 위험분석을 기초로 하므로 정보시스템은 합리적이고 정확한 위험분석을 수행해야 할 것이다. 위험분석기법은 수학적 기법과 다이어그램 기법이 있다. 수학적 접근방법 (mathematical approach) 은 실제상황을 적절히 표현하기 어려우며 증명하기가 어렵다 [4]. 다이어그램 기법 (diagraming techniques) 은 이러한 수학적 접근방식의 한계를 극복함에 있어 훨씬 더 유용하다. 본 논문에서는 외국의 위험분석 기법 (INFOSEC [4], SRAG [5], FIPS65 [6], JRAM [7]) 을 분석하였다.

Abstract

A security risk analysis provides an information system with the capability to investigate and estimate the status of its security, and gives a guideline for establishing a safeguard against any means of security threats [1][2][3]. The information system needs the judicious and accurate way for performing a risk analysis since security policy and risk analysis of the information system are based on risk analysis. The risk anaysis is composed of two methods : mathematical approach and diagramming technique. Mathematical approach cannot yield a precise description of the real world [4]. However, diagramming technique is more pragmatic since it overcomes this limitation. In this paper, we studied the security risk analysis methods proposed in overseas such as INFOSEC [4], SRAG [5], FIPS65[6], and JRAM[7].

* 포항공대 정보통신연구소

** 포항공대 전자전기공학과

1. 서론

하드웨어 및 정보자산으로 구성된 정보시스템 자산은 점점 고가화, 다양화, 복잡화되고 있으며 사회의 정보시스템 의존도는 계속 증가하고 있다. 정보시스템의 이러한 성격들은 공격, 특히 정보자산에 대한 공격동기를 증가시키며 갈수록 공격기법도 다양해지고 고도화되고 있다. 실제로 정보시스템은 자체적으로도 매우 복잡하게 구성되어 있으며 이들간의 연결을 통하여 하나의 거대한 정보망을 형성하고 있다. 이러한 부분들 또한 공격수단을 증가시키는 결과를 초래하고 있음은 물론 한번의 공격으로 막대한 피해를 입을 수도 있다. 어쨌든 정보시스템은 여러 위협에 대응해야 하며 효과적이고 체계적인 보안대책을 수립/구현해야 할 처지에 있음은 분명하다. 그러므로 보안대책을 수립함에 있어 어느부분을 어떻게 어느정도의 수준으로 할 것인가에 대한 결정들을 합리적으로 판단할 수 있는 기준이 요구된다.

위험분석 (risk analysis) 은 그 자체로서가 아니라 안전한 위험관리와 효과적인 보안대책 수립을 위해 요구되는 보안관리 과정이다 [1][2][3]. 위험분석은 시스템의 어느 부분이 어떠한 공격에 어느정도 취약한지 그리고 그로 인한 자산피해 규모는 어느정도인지를 분석하는 것이다. 따라서 위험분석의 결과가 신뢰할만해야 보안대책을 위한 의사결정에 이용될 수 있으며 위험분석의 결과가 정확할 수록 보안대책 구현으로 인한 비용이 절감되며 원하는 보안수준에 쉽게 도달할 수 있을 것이다.

위험분석 방법으론 수학적 접근방법과 다이어그램 기법이 있으나 수학적 접근방법은 실제상황을 적절히 표현하기 어려우며 정확성을 증명하기가 어렵다 [4]. 현재 대부분의 위험분석방법은 다이어그램 기법이라 할 수 있다. 본 논문에서 분석한 여러 위험분석 방법들은 모두 다이어그램 기법이라 하겠다. 그러나 여러 위험분석 기법들 중 어느것이 가장 우수한 것인지를 평가할 수 있는 기준이 없으므로 각 조직들은 각양각색의 위험분석모델을 사용하고 있다. 더우기 국내에서는 정보시스템에 대한 위험분석의 필요성이 이제 겨우 인식되고 있는 실정이며 국내 실정에 맞는 위험분석모델과 위험분석 tool을 선택함에 있어 고려해야할 기준들이 제시되어야할 상황에 있다. 본 논문에서는 미국, 유럽, 일본 등에서 수행된 위험분석방법들을 비교분석하여 위험분석에 관한 의식과 관심을 높이며 기술적으로 각종 정보시스템에서 실제로 적용될 수 있는 위험분석방법 개발을 돕고자 하였다.

2. INFOSEC project - risk analysis

이 과제는 INFOSEC '92 security Investigations Programme 의 여러 과제 중 하나로 위험분석에 관한 것이다 [4]. 이 과제의 궁극적인 목표는 기존의 그리고 개발중인 위험분석 기법들을 기초로 하여 전 유럽에 위험분석을 소개하고 이것이 널리 쓰이게 하기 위한 전략을 수립하고자 하는 것이다. 위험분석을 구성하는 요소 (components) 와 이들간의 상호관계 (relationships), 그리고 위험분석과정 (process flow)을 모델링하는 것은 이 과제의 기본적인 부분이다. 여기서는 이 과제의 위험분석모델을 설명하였다.

• **위험분석모델**

이 모델은 다이어그램 기법 (diagraming technique) 이며 12개의 다이어그램 (구성요소) 으로 구성되어 있다. 12개의 구성요소는 다음과 같다.

1.	0	위험관리 (Risk Management)
2.	3	위험분석 (Risk Analysis)
3.	3.2	자산간의 관련성 수립 및 평가 (Value and Estabilsh Dependences between Assets)
4.	3.3	위협평가 (Threat Assessment)
5.	3.3.1	사고로 인한 위협 정의 및 평가 (Identify and Assess Accidental Threats)
6.	3.3.2	의도적인 위협 정의 및 평가 (Identify and Assess Deliberate Threats)
7.	3.4	현존하는 보안기능 정의 및 시험, 취약성평가 (Identification and Examination of Existing Safeguards and Assessment of Vulnerabilities)
8.	3.4.2	취약성평가 (Vulnerability Assessment)
9.	3.5	강제요소 정의 (Identify Constraints)
10.	3.9	보안기능 규정 및 선정 (Identification and Seclection of Safeguards)
11.	3.9.3	보안기능 선정 (Selection of Safeguards)
12.	5	모니터링 및 적응시험 (Monitoring and Compliance Testing)

두 번째 열의 번호는 그림 1 과 2 에서 사용된 번호를 나타내며 3 으로 시작하는 번호는 위험분석에 직접적으로 속한 요소들이다. 위험관리 (Risk Management) 는 위험분석의 상위개념으로 보안정책과 위험분석 초기화단계, 위험분석, 보안기능 구현, 그리고 모니터링으로 구성된다. 그림 1 은 위험분석과 다른 보안요소와의 관계를 나타낸 것이며 그림 2는 위험분석의 제 요소들간의 관계와 위험분석의 흐름을 나타낸 것이다. 그림 3 은 위험분석의 기본요소들 간의 관계를 나타낸 것이다. 그림 3 에서 화살표가 사각형안으로 들어간 것은 항상 영향을 미침을 의미하고 화살표가 사각형 면에 접해 있는 경우는 영향을 미칠 수도 있음을 의미한다.

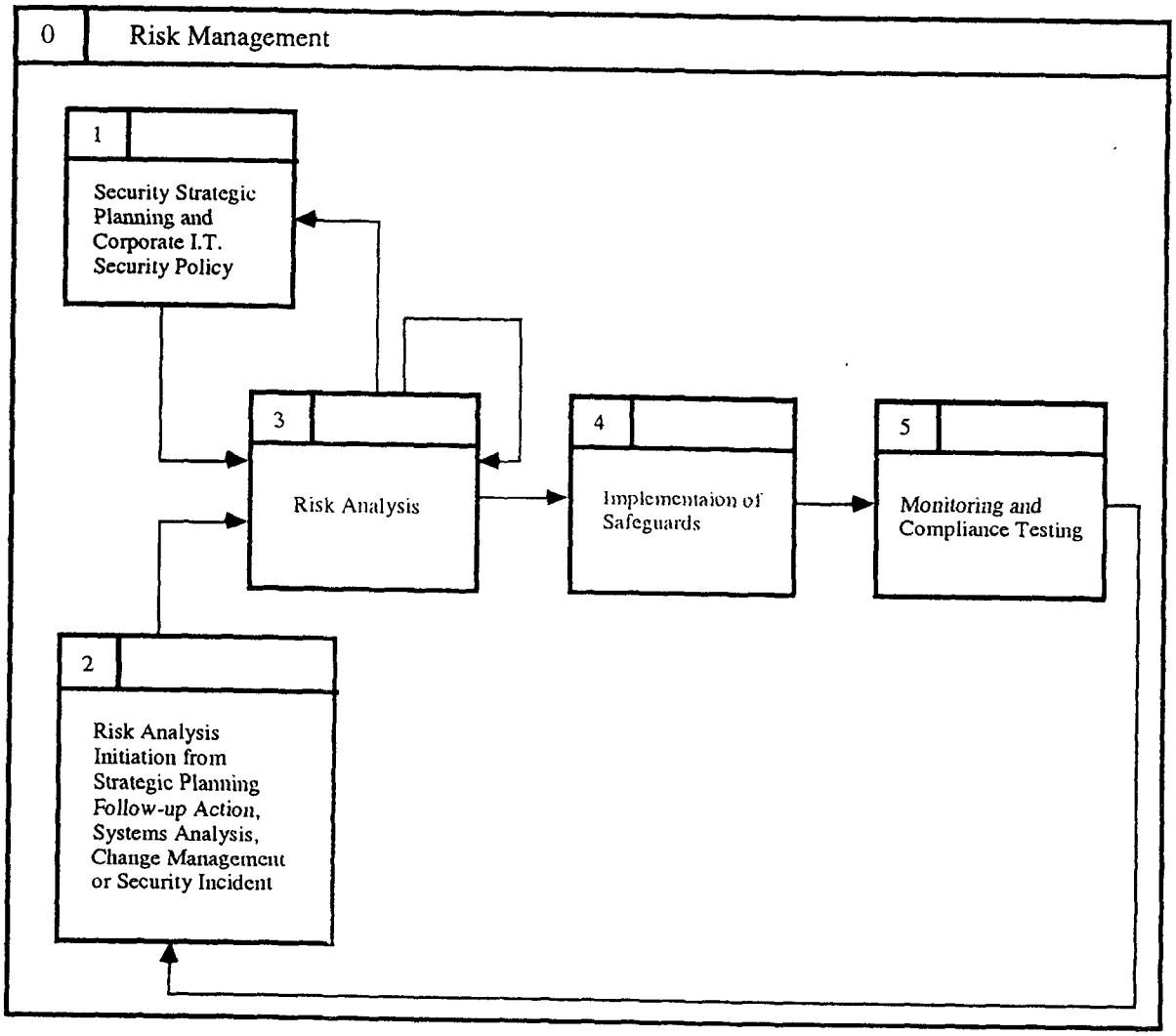
0
Risk Management
1
Security Strategic Planning and Corporate I.T. Security Policy
2
Risk Analysis Initiation from Strategic Planning Follow-up Action, Systems Analysis, Change Management or Security Incident
3
Risk Analysis
4
Implementaion of Safeguards
5
Monitoring and Compliance Testing

그림 1 : 위험관리의 흐름

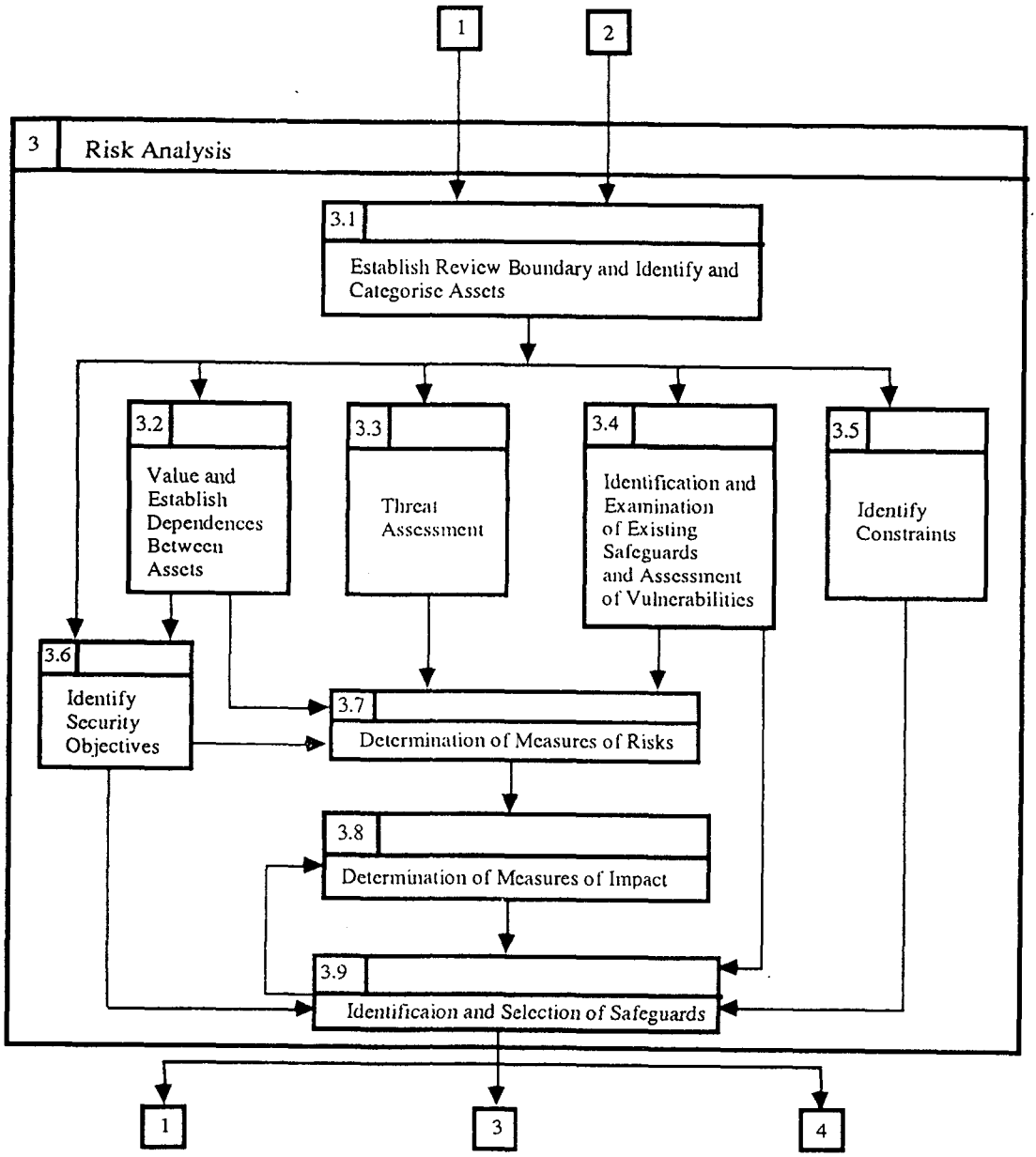
1
2
3
Risk Analysis
3.1
Establish Review Boundary and Identify and Categorise Assets
3.2
Value and Establish Dependences Between Assets
3.3
Threat Assessment
3.4
Identification and Examination of Existing Safeguards and Assessment of Vulnerabilities
3.5
Identify Constraints
3.6
Identify Security Objectives
3.7
Determination of Measures of Risks
3.8
Determination of Measures of Impact
3.9
Identificaion and Selection of Safeguards
1
3
4

그림 2 : 위험분석의 흐름

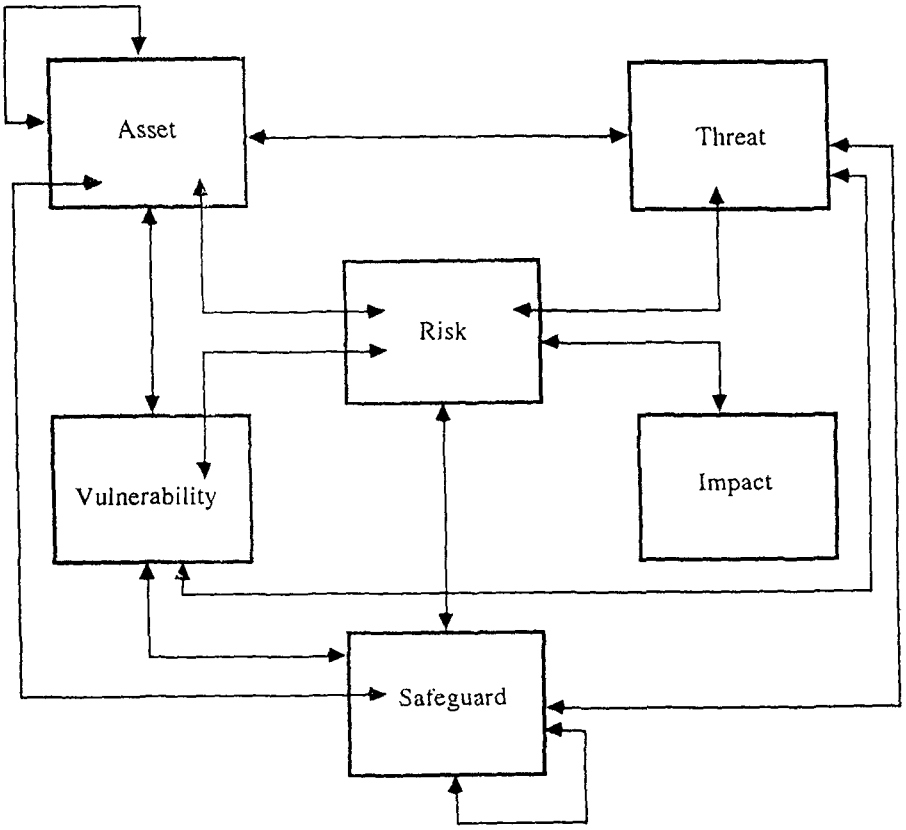

그림 3 : 위험분석의 기본적인 요소들간의 관계모델

3. SRAG (Simplified Risk Analysis Guidelines)

정보시스템을 사용하는 미국 정부기관의 위험분석에 관한 요구들은 1970년대 후반부터 자체적인 위험분석 지침들을 만들게 하였으며 이러한 지침들은 정부기관과 대학의 여러 학자들에 의해 수정 보완되어 왔다. 그러나 위험분석을 완벽하게 수행하는 것은 너무 많은 시간과 노력을 요하며 또 그 자체가 바로 시스템의 보안수준을 향상시키는 것이 아니므로 위험분석을 간단히 수행할 수 있는 단순화된 위험분석지침의 필요성이 생기게 되었다. 미국 법무성은 (U.S Department of Justice) 은 이를 위해 단순화된 위험분석을 위한 지침 (SRAG) 을 만들었다 [5]. 이것은 특정한 위험분석 기법 (정량적 분석기법, 정성적 분석기법 등) 을 요구하지 않으며 추가적인 위험분석 지침이 없이도 위험분석을 수행할 수 있도록 한 것이다.

• 위험분석모델

SRAG 위험분석의 특징은 세가지로 요약할 수 있다. 첫째로 위험분석을 요구하는 시스템을 세가지 범주로, 즉 PC, 메인프레임 및 원거리 접근 정보시스템 (Automated Information System : AIS), 그리고 기타 응용 시스템으로 나누었으며 각각을 더 세분화하여 적용하였다. 둘째로 SRAG 위험분석은 7 단계로 구성된다. 처음 두단계는 정보시스템 환경과 보안고려사항, 그리고 현재 존재하는 보안기능을 설명하는데 사용되며 단계 3 은 AIS 환경이 최소한의 보안요구사항들을 얼마나 만족하는지가 평가된다. 나머지 단계들은 위협 및 손실분석을 통해 추가적인 보안기능이 필요한지 여부를 결정, 보안기능의 선택, 보안기능을 위한 비용/효과분석, 그리고 현존하는 위험을 수용할 것인지 또는 보안기능을 구현할 것인지에 대한 의사결정 등을 위해 수행되는 과정이다. 그림 4 는 SRAG 의 위험분석 과정을 나타낸 것이다.

단계 1. 시스템 설명 (SYSTEM DESCRIPTION)

단계 1 의 목적은 시스템에 대한 일반적인 설명이다. 여기서는 하드웨어의 구성, 소프트웨어의 종류, 그 정보시스템에 의해 처리되는 데이타에 대한 일반적인 설명, 시스템의 목적, 그리고 각 시스템 구성요소의 비용평가 등이 포함된다. 시스템 취약점을 효과적으로 찾기 위해서는 모든 시스템 구성요소와 정보의 흐름을 잘 검토해야 한다.

단계 2. 정보시스템의 보안정보 (AIS SECURITY INFORMATION)

단계 2 에서는 보안관련 정보를 수집하고 이를 문서화한다. 이러한 정보로는 현재 존재하는 보안기능의 효율성평가, 시스템에서 처리되는 데이타의 유형에 관한 정보, 보안정책, 보안절차, 현존하는 보안기능의 명확한 문서화, 데이타가 노출, 변경, 파괴로 인해 입을 수 있는 충격평가 등이 있으며 추가적으로 시스템의 사용횟수와 시스템 접근방법 등을 포함할 수 있다.

단계 3. 최소한의 보안요구사항 (MINIMUM SECURITY REQUIREMENTS)

이 단계에서는 앞에서 분류한 세가지 시스템에 각각에 대하여 최소한의 보안요구사항을 규정한다. SRAG 은 각 시스템에 대한 보안요구사항을 세등급으로 분류하여 제시하고 있다. 또한 현재 존재하는 보안기능이 보안요구사항을 어느정도 만족하는지를 평가한다.

단계 4. 위협 및 손실 분석 (ANALYSIS OF THREATS AND LOSSES)

단계 4 의 목적은 위협과 그로인한 자산손실을 평가하는 것이다. 이것은 손실을 줄이기 위해 보안기능이 더 필요한지 여부를 결정하기 위해 사용된다. 그리고 위협의 가능성과 그로인한 손실을 정성적인 방법 (매우 낮음, 낮음, 보통, 높음, 매우 높음) 으로 평가한다.

단계 5. 보안기능 선택 (SELECTION OF SECURITY MEASURES)

단계 5 에서는 단계 3, 4 의 결과를 기초로 하여 보안기능을 선택한다. 이 선택은 충족시키지 못한 최소한의 보안요구사항을 만족시키며 심각한 위험을 초래하는 위협을 감소시키는 보안기능을 포함한다.

단계 6. 비용-이윤분석 (COST BENEFIT ANALYSIS)

이 단계는 단계 4 에서 심각하다고 판단된 위협에 대처하기 위해 선정된 보안기능의 비용-이윤분석을 수행한다. 비용-이윤분석에서 비효과적으로 판명된 보안기능은 더이상 고려되지 않는다. 비용은 하드웨어 또는 소프트웨어, 인력, AIS 작동에 드는 비용 등에 기초하여 달러로 계산될 수 있으며 비용과 이윤은 일년 단위로 평가한다. 비용 산출은 정성적으로 할 수도 있다. 이윤은 위협이나 손실의 감소와 보안수준의 향상으로 인해 파생된 이윤으로 구성되며 비용과 같이 일년 단위로 정량적 또는 정성적으로 평가될 수 있다. 위험분석자는 비용-이윤분석에 기초하여 어느 보안기능이 합리적인 것인지를 결정하게된다.

단계 7. 의사결정을 위한 권고 (RECOMMENDATIONS FOR MANAGEMENT DECISION)

이 마지막 단계에서는 각 권고된 보안기능을 구현해야할지 여부를 결정할 수 있도록 비용-효과적인 측면의 분석결과를 제시한다. 보안관리는 이러한 권고사항을 구현하기 위해 소요되는 사항들을 고려하여 현존하는 위험을 그대로 방치할지 아니면 권고된 보안기능을 구현할지를 결정하게 된다.

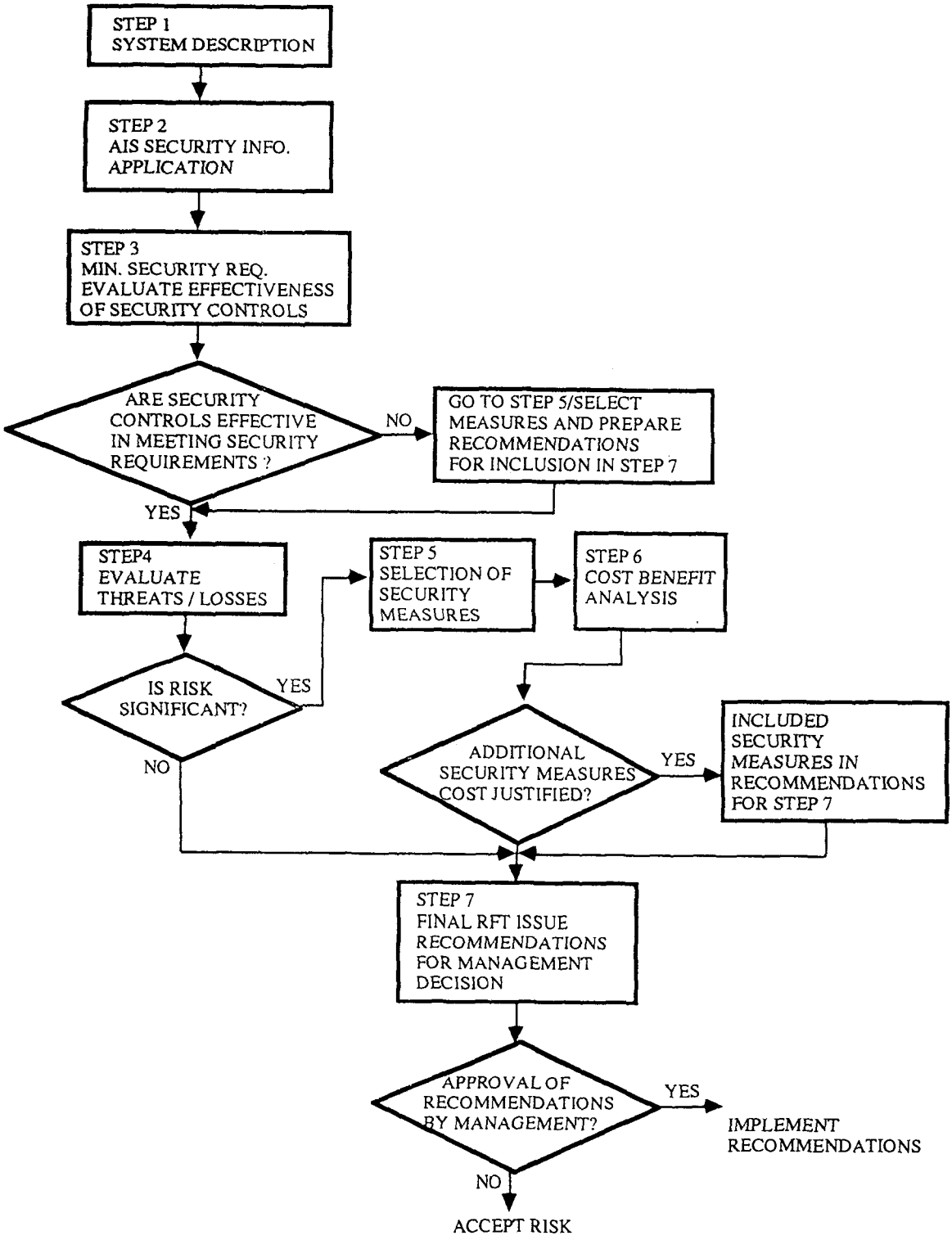

그림 4: SRAG 위험분석 흐름도

4. FIPS65

FIPS65 (Federal Information Processing Standards Publication 65)는 미국 상무성 (U.S. Department of Commerce)에 의해 수행된 것으로 자동 데이타처리 시스템 (Automatic Data Processing : ADP)의 위험분석을 위한 지침서이다 [6]. 이 지침서에서는 위험분석을 해야하는 이유와 위험분석 절차 및 이를 위해 사용되는 형태, 그리고 보안대책을 비용-효과적 측면에서 평가하는 방법을 설명하고자 하였다.

• 위험분석모델

이 위험분석모델은 위험분석의 본질적인 요소로 위협으로 인한 자산손실과 그 위협의 발생가능성을 들고 있다. 이 모델에서는 위험분석에 있어 관리의 역할을 강조하였고 위험분석과정을 예비조사단계와 위험분석단계로 나누었다.

관리의 역할 (The Role of Management)

위험분석의 성공여부는 최고 관리권이 수행하는 역할에 의존하며 관리가 위험분석을 위해 지원해야 하는 사항들은 다음과 같다.

1) 과제가 조직의 모든 수준에 표현될 수 있도록 관리적 지원이 있어야 한다.
2) 위험분석의 목적과 범위에 대한 관리적 측면의 설명이 있어야 한다.
3) 우수한 위험분석팀의 선정과 공식적인 책임과 권한을 부여받은 대표를 선임해야 한다.
4) 위험분석팀의 분석결과에 대한 관지적 측면에서 검토가 있어야 한다.

위험분석팀은 관리자에 의해 선정되는데 위험분석결과는 위험분석팀에 의해 민감하게 영향을 받으므로 위험분석팀을 위험분석에서 요구되는 정보를 정확히 알고 그것에 대한 책임있는 사람들로 구성하거나 위험분석을 위한 정보를 얻고자 할 경우에 그와같이 책임있는 사람에 의한 답변을 들어야 할 것이다.

예비조사단계 (Preliminary Security Examination)

위험분석을 수행하기 위한 예비작업으로 위험분석팀은 ADP 시스템의 보안과 자산대체비용, 그리고 ADP 시스템이 취약한 위협들을 조사한다. 이 예비조사에서 얻게 되는 세가지 사항은 자산대체비용목록, 시스템의 취약부분에 대한 위협목록, 현재 존재하는 보안기능 목록 등이다.

위험분석단계 (Risk Analysis)

위험분석의 본질적인 요소는 위협으로 인한 자산의 손실평가와 그 위협이 일정기간동안 발생할 가능성 (횟수)을 평가하는 것이다. 자산이 입을 수 있는 피해의 유형은 데이타 무결성, 데이타 기밀성, ADP 시스템의 가용성이며 위협은 이 세가지 유형의 하나 또는 그 이상의 피해를 초래한다. 자산손실평가는 이러한 유형의 손실로 인한 피해액을 산출하는 것으로 일정기간 동안의 자산손실은 다음의 식으로 계산된다.

*손실 (Loss) = 충격 (Impact) * 위협의 발생횟수 (Frequency of Occurrence)*

이러한 손실액은 일년을 단위로 산출하며 위협으로 인한 충격과 위협의 발생횟수를 정확하게 아는 것이 불가능하므로 손실액과 발생횟수를 적당히 등급화하여 평가한다.

5. JRAM

JRAM (JIPDEC Risk Analysis Method)은 일본정보처리 개발협회 (JIPDEC)에서 지금까지의 위험분석에 관한 검토 및 실제적인 경우에 이용가능한 분석방법으로 제시한 위험분석방법이다 [7]. JRAM은 JRAM 질문표를 통하여 조직의 취약성을 확인하고 손실의 실태에 기초한 분석결과에서 위험의 경제적 영향을 경영 관리자에게 제시할 것을 목적으로 하고 있다.

• 위험분석모델

JRAM의 특징은 JRAM 질문표와 사고분석을 통하여 위험분석을 수행하는데 있다. JRAM 질문표는 시스템의 취약성을 파악하기 위한 것으로 응답자의 주관적 측면을 나타낸다. 사고분석은 실제 발생한 사고에 관한 것을 기록/분석하는 것으로 사고의 발생 및 원인 분석, 장해복구보고, 손실분석 등을 수행한다. 그림 5는 JRAM의 구조를 나타낸 것으로 취약성분석 (질문표)과 실태분석 (사고분석), 두 분석결과를 토대로 위험분석보고서가 작성된다.

JRAM 질문표

질문표는 조직의 취약성을 파악하기 위한 것으로 질문항목, 질문서의 구성, 회답자, 사용방법 등을 나타내고 있다.

1) 질문항목 : 일본 통산성이 책정한 "전자계산기 시스템 안전 대책 기준"과 IBM 사의 "Security 종합평가 질문서"를 고려하여 작성하였다.
2) 질문표의 구성 : 이 질문표는 다음과 같이 7개의 큰 항목으로 구성되어 있다.

- 관리통제
- 신뢰성
- 사용업무의 보전성
- 데이타전송의 보호
- 물리적 보안
- 비상사태 대응계획
- 접근 관리

3) 질문표 사용법 : 질문표 사용법에는 회답자 결정, 회답시 주의사항, 회답방법 등이 나타나 있다.

JRAM 사고분석

JRAM 사고분석은 상기의 질문표에 따라 조직의 취약성을 파악한 후에 처리하는 경우도 있고 독자적으로 처리하는 경우도 있다. 사고분석은 업무방해 요인, 사고현상, 원인, 손실평가 등을 수행하기 위하여 업무일지, 장해보고, 장해복구완료보고, 손실보고, 위험분석작업표를 사용한다. 특히 사고분석에서는 사고현상과 원인과의 인과관계를 명확히하고 그 결과인 손실이 조직에 어느정도의 충격을 초래하는가를 판단하게 된다. JRAM 사고분석 단계는 다음과 같다.

1) 업무일지, 장해보고, 장해복구완료보고, 손실보고 작성
2) 사고현상의 문제점 조사
3) 손실타입의 확정
4) 손실의 발생확률(빈도) : 잠재적 손실의 크기(강도) 파악
5) 손실강도의 평가(손실에 있어서의 상대적 여향도 평가)
6) 위험 처리를 위한 우선순위의 결정
7) 위험 처리 방법의 비용대효과의 분석

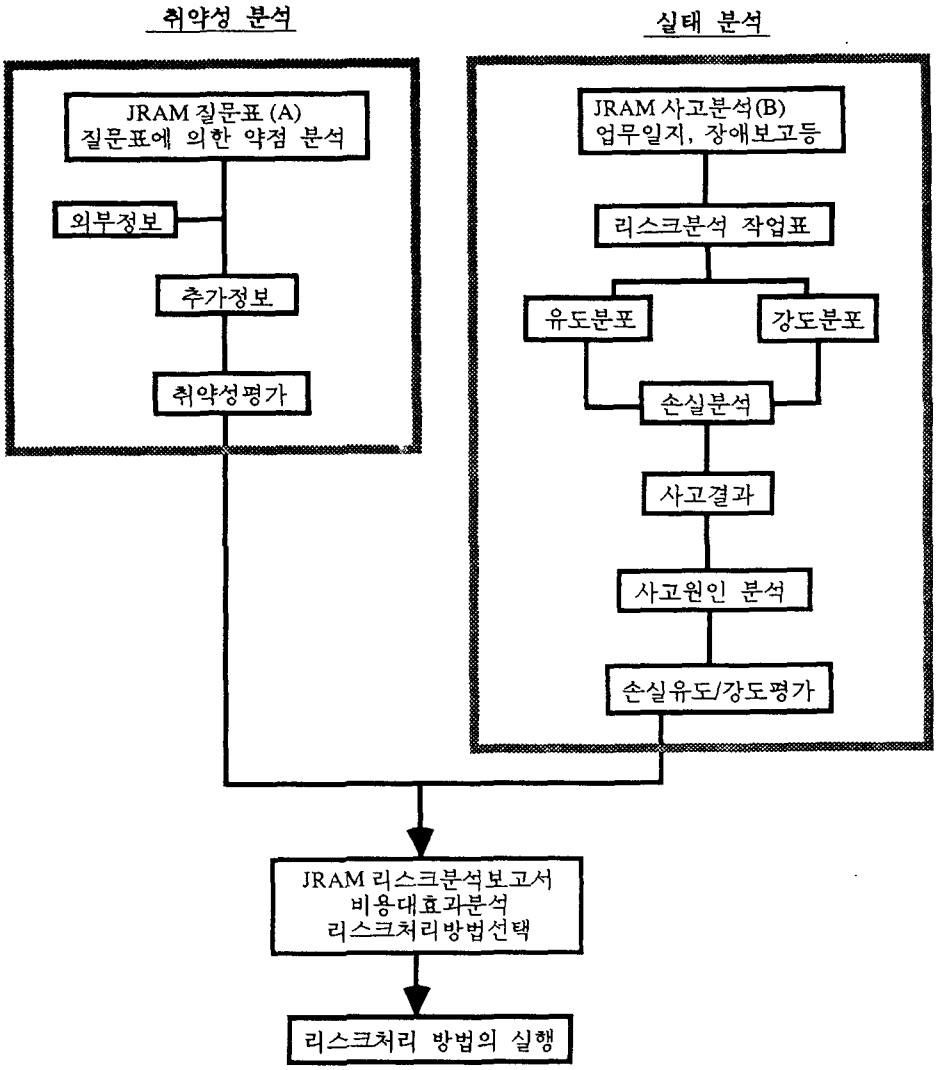

그림 5 : JRAM의 구조, 주관적 측면과 실태적 측면

6. 위험분석 방법 비교분석

위 네개의 위험분석방법들은 모두 정보시스템이 실제로 위험분석을 수행할 수 있도록 돕기 위한 지침들이다. 위험분석이란 정보시스템이 받을 수 있는 자산손실을 예상/평가하고 경영자가 이를 막기위한 보안대책을 결정할 때 필요한 기준 및 관련정보를 제공하는 것이다. 그러나 조직 실무자가 위험분석을 수행하고자 할 때 올바른 위험분석(이것은 자산손실이 얼마나 정확하게 예측/평가되었는가와 보안대책에 대한 비용-효과분석의 정확성에 의존한다)을 위해서 무엇을 해야 할 지 결정하는 것은 쉬운 일이 아니며 실제로 위험분석을 통해 얻어진 결과들에 대한 신뢰도를 평가하는 것도 역시 쉬운 일이 아니다. 결국 위험분석은 그 성격상 평가가 주관적일 수 밖에 없으나 위험분석자는 위험분석이 요구하는 필수적인 요소와 그들간의 관계, 그리고 일반적인 평가 방법을 따름으로써 분석결과의 객관성을 유지할 수 있을 것이다. 위험분석에 대한 지침들은 이러한 관점에서 연구/작성되어야 하며 지나치게 개연적이거나 반대로 지나치게 구체적(적용할 시스템 환경이 다를 수 있으므로)으로 흐르지 않도록 해야 할 것이다. 본 장에서는 지침적 성격으로 위험분석모델이 갖추어야 할 요건들을 제시하고 이를 바탕으로 앞에서 설명한 네개의 위험분석방법들을 비교분석하였다.

1) 위험분석을 명확히 정의하고 있는가
2) 위험분석의 필수요소를 충분히 반영하고 있는가
3) 위험분석요소들간의 관련성을 잘 묘사하였는가
4) 위험분석의 전체흐름을 제시하고 있는가
5) 위험평가방법이 타당한가
6) 구체적 적용이 용이한가

INFOSEC 은 요건 1), 2), 3), 4)을 잘 충족시키나 요건 5)에 대해서는 설명하고 있지 않으며 요건 6)의 관점에서는 매우 약하다.
SRAG 은 세가지의 정보시스템에 따라 각 단계에서 필요한 사항들을 제시하여 위의 요건 4)과 6)를 만족시킨다고 하겠으나 여건 3)과 5)를 충분히 설명하고 있지 못하다.
FIPS65 는 위험분석의 기본적인 사항은 포함하고 있으나 위의 요건들을 대부분 만족시키지 못하고 있다.
JRAM 은 위험분석에 대한 체계적인 설명보다는 오히려 실무에서 바로 사용될 수 있도록 하는 것에 초점이 맞춰져 있기 때문에 요건 4), 5), 6) 은 잘 만족시키나 요건 1), 2), 3)의 측면에서는 충분치 않다고 할 수 있다.

7. 결론

정보시스템에 대한 공격방법의 다양화와 그로 인한 피해의 심각성이 증가함에 따라 시스템에

대한 안전한 보안대책이 요구되게 되었다. 위험분석은 조직의 관리자가 안전하고 경제적인 보안대책을 수립할 수 있도록 보안관리와 관련된 의사결정기준을 제공해주기 위한 것이다 [1][2][3]. 현재 많은 위험분석방법들이 있으나 어느것이 가장 우수한지에 대한 평가기준은 없으며 위험분석은 성격상 많은 주관적 요소을 포함하고 있다. 이러한 이유로 여러 국가기관에서는 조직의 위험분석을 돕기 위해 위험분석을 위한 지침들을 연구/개발하게 되었다. 그러나 이러한 지침들에 대하여도 신뢰성과 타당성을 평가하기 쉬운 일이 아니므로 위험분석을 하고자 하는 조직은 제시된 지침들의 도움을 받아 주관적으로 위험분석작업을 수행할 수 밖에 없는 형편이다. 본 논문에서는 네개의 위험분석모델들의 내용과 특징을 설명하고 위험분석모델(또는 지침)이 갖추어야 하는 요건들을 제시하였으며 이것을 기준으로 위 네개의 위험분석모델들을 비교분석하였다.

외국의 경우와 마찬가지로 국내에서도 국내 정보시스템 환경에 쉽게 적용할 수 있고 평가방법 및 결과의 객관성을 높일 수 있는 위험분석모델의 제시가 필요하며 이에 대한 연구가 꾸준히 지속되어야 할 것이다.

참조문헌

[1] Deborah J. Bodeau, "A Conceptual Model for Computer Security Risk Analysis," in *Computer Security Applications Conference*, 1992

[2] David J. Stang, Sylvia, *Network Security SECRETS*

[3] ISO/IEC JTC1/SC27/WG1 N423, Guidelines for the Management of IT Security - Part 3, March 18th, 1994

[4] Robin Moses, *INFOSEC Project S2014 : Risk Analysis, Final and Strategy Report*, 1993

[5] Edward Roback, *NISTIR 4387, Simplified Risk Analysis Guidelines*, 1990

[6] NIST, FIPS PUB 65, *Guidelines for ADP Risk Analysis*, 1979

[7] JIPDEC, *JIPDEC Risk Analysis Method*, 1992