논문 2004-41CI-6-2

정보시스템 보안관리를 위한 위험분석 방법론

(A Risk Analysis Methodology for Information Systems Security Management)

이 문 구*

(Lee, Moon-Ku)

요 약

본 연구는 기존의 위험분석 방법론들이 갖는 절차상의 복잡성을 최소한으로 줄이기 위하여, 정보시스템보안관리를 위한 위험분석방법론을 제안한다. 제안한 위험분석방법론은 사전처리단계, 대응책설정단계, 사후처리단계의 3단계로 구성된다. 사전처리단계에서는 기본위험분석단계와 상세위험분석 단계로 나누어 실행하도록 하였다. 기본위험분석단계에서는 정보보안 체계가 구축되지 않았거나 단기간에 최소한의 보안 제어를 위한 수단이 필요한 경우 설정된 항목들을 점검하도록 하는 기본적인 보안관리 단계이다. 상세위험분석단계에서는 자산, 취약성, 위협의 요소들을 분석하고 이를 기반으로 작성된 위험정도 산출표를 이용하여 위험의 정도를 13가지의 경우로 분류한다. 대응책설정단계에서는 위험의 정도에 따라 13가지의 위험정도를 수용, 무시, 감소, 또는 이양 등으로 대응방법을 설정한 후, 물리적, 관리적, 기술적으로 대응책을 실행하도록 하였다. 마지막으로 사후관리단계에서는 침투 테스트로 잔류위험을 평가하고, 보안정책수립과 감사 및 사고대응을 위한 대책이 이루어지도록 하였다.

Abstract

This study proposes a risk analysis methodology for information system security management in which the complexity on the procedure that the existing risk analysis methodology is reduced to the least. The proposed risk analysis methodology is composed of 3 phases as follows: beforehand processing phase, counter measure setting phase, post processing phase. The basic risk analysis phase is a basic security management phase in which fixed items are checked when the information security system is not yet established or a means for the minimum security control is necessary for a short period of time. In the detailed risk analysis phase, elements of asset, a vulnerability, and threat are analysed, and using a risk degree production table produced from these elements, the risk degree is classified into 13 cases. In regard to the risk, the 13 types of risk degree will execute physical, administrative, and technical measures through ways such as accepting, rejecting, reducing, and transferring. Also, an evaluation on a remaining risk of information system is performed through a penetration test, and security policy set up and post management phase is to be carried out.

Keywords : 취약성: vulnerability 위협: threat 수용: accepting 무시: rejecting 감소: reducing 이양: transferring 침투 테스트 : penetration test

I. 서 론

통신기술과 인터넷의 발달로 정보화가 더욱 진전됨에 따라, 정보시스템의 운영에 대한 비중이 높아지고, 의도적이든, 비의도적이든 해킹, 바이러스, 정보유출, 변조, 파괴, 사보타지 등의 보안사고들이 증가하고 있는 현실이다. 공공 인프라뿐만 아니라 업무수행을 정보시스템에 의존하는 개인이나 조직은 정보시스템 보안을 적절한 수준으로 관리하여야 하는 필요성에 대한 인식이 고조되고 있다. 보안관리는 기업의 컴퓨터와 정보보안의 핵심이라고 할 수 있으며, 위험분석은 보안관리를 수행하기위한 필수적인 과정이다. 그러나 보안관리를 위한 기존의 위험분석방법론은 실제 기업의 정보시스템의 보안대응책으로 적용하고자 할 때 위험분석 방법이 추상적이거나, 제시하는 예시가 극히 제한되어 실무자들이 적용하기에 너무나 많은 어려움을 갖는다. 그렇기

* 정회원, 김포대학 컴퓨터계열
(Department of Computer Science, Kimpo College)
※ 본 연구는 2004학년도 김포대학의 연구비 지원에 의하여 연구되었습니다.
접수일자: 2004년8월13일, 수정완료일: 2004년11월15일

때문에 본 논문에서 제안하는 위험분석 방법론은 위험분석을 위해 3단계의 프레임(사전처리단계, 대응책설정단계, 사후처리단계)으로 나누어 실행하도록 함으로써 업무의 효율성을 증대하도록 하였다. 또한 위험의 분류도 구체적으로 [표 6]의 위험정도 산출표를 근거로 1~13의 경우로 분류하여 구체적으로 그에 대한 대응책을 [표 7]에 예시함으로써, 기업이 실제 위험분석을 하고 보안정책을 수립하는데 도움이 되고자 방법론을 제안한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 정보시스템 보안관리의 개요와 보안관리의 기본원칙을 설명하고, Ⅲ장에서는 위험분석에 대한 개념과 일반적인 위험분석 단계와 위험분석모델에 대하여 간략히 기술하였다. 그리고 Ⅳ장에서는 제안하는 위험분석 방법론을 실행단계별로 자산, 취약성, 위협 요소의 분류와 위험정도 산출 및 대응책에 대하여 기술하였으며, 마지막으로 Ⅴ장에서는 결론을 맺도록 한다.

Ⅱ. 정보시스템 보안관리

1. 정보시스템 보안관리의 개요

정보시스템 보안관리는 정보와 정보기술 서비스로부터 적절한 수준의 비밀성, 무결성, 가용성을 달성하고 유지하기 위한 하나의 과정이다. 즉, 정보시스템 보안관리는 조직 내 정보보안 환경을 설계, 구축, 운영 및 감시하는 활동의 주기를 기획, 관리하여 이들 영향력간의 균형을 이루어 안전한 정보시스템 보안 환경을 달성하기 위한 활동이다. [그림 1]은 정보시스템 보안관리 과정의 주기를 도식화 한 것이다[2, 5, 6, 8].

정보시스템 보안관리 작업은 자원에 대하여 어느 정도의 권한부여를 가질 수 있는지를 규정해야 하며, 보안관리 작업의 관리적, 기술적, 그리고 물리적 통제는 기업의 자산을 보호하기 위해 공동 작업한다.

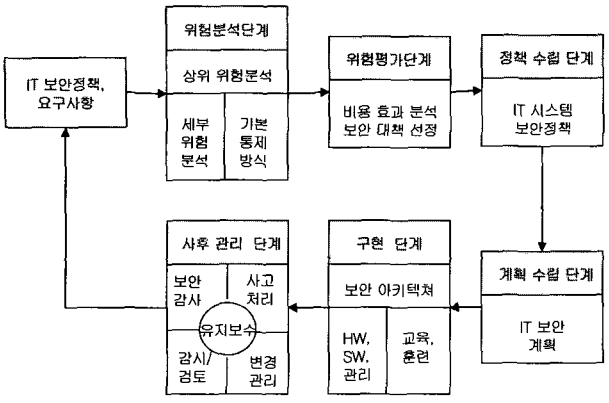

그림 1. 정보시스템 보안관리 과정
Fig. 1. Information System Security System Processing.

2. 보안관리의 기본원칙

보안관리를 수행하기 위한 주요 세 가지 기본 원칙은 기밀성, 무결성, 그리고 가용성이다[1].

기밀성은 데이터 처리와 권한이 없는 데이터 유출의 방지 사이의 교차점에서 필요한 수준의 비밀이 강요되도록 하는 능력을 제공한다. 이 수준의 기밀성은 데이터가 네트워크의 시스템과 장비에 보관되어 있는 동안, 데이터가 전송 될 때, 그리고 데이터가 목적지에 도달한 이후에도 잘 유지되어야 한다. 무결성은 정보와 시스템에 대한 정확성과 신뢰도에 대한 보장이 제공되고, 데이터에 대한 권한 없는 수정(modification)을 방지하는 경우에 유지된다. 가용성은 서비스 중단으로부터 안전하고 신속한 방법으로 복구함으로써 생산성에 부정적인 영향을 주지 않는 것이다.

Ⅲ. 일반적인 위험분석

1. 위험분석

위험분석은 정보시스템의 안전을 보장하기 위한 보안관리의 일환으로 수행하게 된다. 위험분석이란 자산의 취약성을 식별하고 존재하는 위협을 분석하여 이들의 발생 가능성 및 위협이 미칠 수 있는 영향을 파악해서 보안 위험의 내용과 정도를 결정하는 과정이다. 위험분석은 위험 식별, 잠재적 위협의 충격측정, 그리고 위험의 충격과 그 대책에 대한 비용-간의 경제적 균형 제공이라는 세 가지 주요 목표를 가진다[1].

2. 위험분석 단계

다음은 모든 위험분석과 평가에서 발생하는 기본 단계이다[1].

1) 정보와 자산에 가치 부여
- 해당 자산의 기업에 대한 가치는 무엇인가?
- 자산을 관리하기 위한 비용은 얼마인가?
- 기업에게 얼마만큼의 이윤을 가져다주는가?
- 경쟁사에게 있어서의 가치는 얼마인가?
- 다시 만들거나 복구하는데 드는 비용은 얼마인가?
- 획득하거나 개발하는데 지출한 비용은 얼마인가?

2) 위험에 대한 잠재적 손실 평가
- 어떤 물리적 피해발생 가능성과 손해는 얼마인가?
- 어느 정도의 생산성을 잃을 수 있으며 그 손해는 ?

- 기밀정보가 누설되었을 경우에 손해는 얼마인가?
- 바이러스 공격으로부터 복구하는데 드는 비용은?
- 해커공격으로부터 복구하는데 드는 비용은 얼마인가?
-중대한 장비가 고장 난 경우에 드는 비용은 얼마인가?
- 각 위험과 시나리오에 대한 SLE(Single Loss Expectancy)를 계산한다.

3) 위협분석 수행
- 발생하는 각 위험의 가능성에 관한 정보를 각 부서의 직원, 과거기록, 그리고 이러한 종류의 데이터를 제공하는 공식적인 보안 정보 자원을 통해 수집한다.
식별된 위험 발생의 확률을 계산한다. 각 위험이 1년에 몇 번이나 발생 할 수 있는 지를 나타내는 연간 예상 손실(ALE : Annualized Loss Expectancy)을 계산한다.

4) 위험에 대한 총체적인 잠재손실 추정
잠재적 손실과 확률을 결합하며, 처음의 세 가지 단계에서 계산된 정보를 이용하여 위험에 대한 연간 예상 손실을 계산한다. 각 위험을 분쇄하는 개선방법을 선택한다.

5) 위험을 줄이고 분담 혹은 수용
① 위험 감소 방법
보안 통제와 구성요소 설치, 절차 향상, 환경 변경.
위험이 발생하는 것을 조기에 탐지하는 방법을 제공하여 유발될 수 있는 피해를 줄인다. 특정한 위험이 발생하는 경우에 비즈니스를 지속시킬 수 있는 비상계획을 작성하여 위험으로 인한 확대 피해를 줄인다. 위험에 대한 방책을 세운다.
② 위험 분담
위험의 일부 · 전체를 이전하기 위해 보험에 가입한다.
③ 위험 수용
위험 방지 · 보호를 위해 전혀 비용을 지출하지 않는다.

3. 위험분석 모델

위험분석을 과학적인 기법으로 분석하기 위하여 여러 모델이 연구되었으며 그 시초는 1979년 미국 NIST (National Institude of Science & Technology)에서 발행한 "자동화된 데이터 처리에 관한 위험분석"으로 7단계의 과정을 거쳐 위험분석을 하도록 되어있다[9]. BLP (Bell-LaPadula) 위험분석 모델은 공식으로 표현되는 대표적인 위험분석 모델로서 비용(Burden)이 손실(Loss)이 일어날 확률(Probability)과 특정 사건사고에 대한 총체적 손실보다 작을 경우 보호대책을 수행한다는 의미이다. 또한 위험 분석은 결과성격에 따라 정량적 방법(Quantitative Approach), 정성적 방법(Qualitative Approach)으로 나눌 수 있고, 요구수준에 따라서 기본통제 접근방법(Baseline Approach), 위험분석 접근방법(Risk Analysis Approach)으로 나눌 수 있다. 정량적 방법은 위협의 영향, 빈도, 가능성을 화폐가치 또는 수치화 하여 연간기대손실(Annual Loss Expectance)을 척도로 하며, 정성적 접근방법은 화폐가치로 표현하기 어려운 경우 점수를 척도로 하여 사용하는 방법이다[7], [8].

위험분석과정은 보호 대상이 되는 정보자산의 가치와 상호의존도를 파악하고 자산에 손해를 미칠 수 있는 위협의 유형을 파악하여 이의 강도와 빈도를 측정하는 위협분석을 수행하며 동시에 자산이 보유하고 있는 취약성을 평가하는 과정을 포함하고 있다. 이를 통해 자산의 가치와 위협 및 취약성 평가의 결과를 토대로 위험을 측정, 평가하는 과정으로 구성되어있다[9, 10].

Ⅳ. 제안하는 위험분석 방법론

1. 위험분석 방법론 개념

본 논문에서 제안하는 정보시스템 보안관리를 위한 위험분석 방법론은 3단계로 분류하여 사전처리단계, 대응책설정단계, 사후처리단계로 나누어 실행하도록 함으

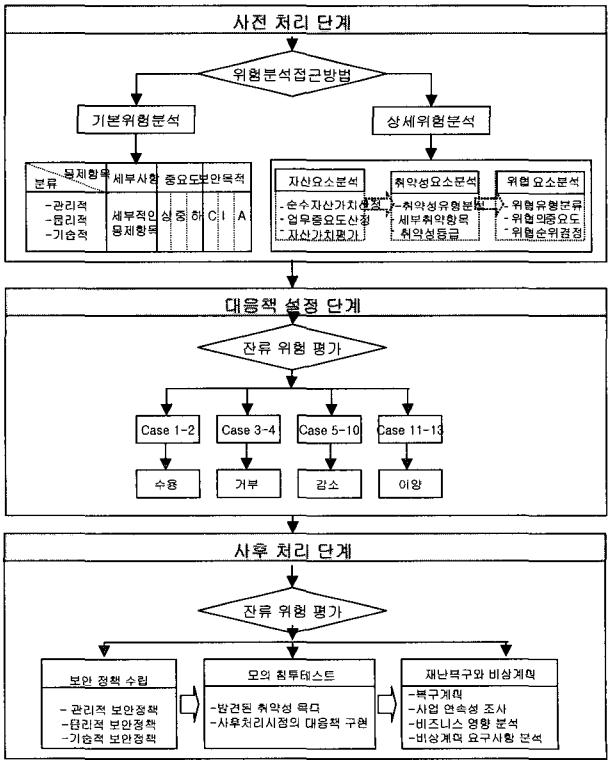

그림 2. 제안하는 위험분석 방법의 프레임
Fig. 2. Proposed Frame of Risk Analysis Method.

로써 기존의 일반적인 위험분석 방법보다 각 단계별로 계층적인 구조로 구성되어 보다 더 체계적으로 제안하였다.

사전처리단계에서 상세위험분석을 위하여 자산요소에 대한 분석, 취약성 요소에 대한 분석, 그리고 위협요소에 대한 분석 자료를 기반으로 위험정도를 산출할 수 있는 방법론을 제시하였다. 제시된 위험정도는 위험정도 산출표를 기반으로 13가지의 경우로 분류 하였다. 분류된 13가지의 경우는 수용, 거부, 감소, 그리고 이양 등의 대응책방법론에 따라 물리적, 관리적, 그리고 기술적인 대응방안을 제시하였다. 제안하는 정보시스템 보안관리를 위한 위험분석 방법론이 기존의 위험분석 방법과 비교하면 다음과 같은 특징 및 장점을 갖는다.

- 효율성 : 정보시스템의 수용 가능한 보안수준에 따라 위험분석이 실시 되도록 설계하였다. 즉, 기관의 정보시스템이 수용 가능한 보안수준에 따라 기본위험분석단계로만 시행하는 경우와 보다 높은 보안수준에 따라 상세 위험분석 단계에서 처리함으로써 위험분석 과정이 방법적, 절차적 그리고 사용자의 용이성 측면에서의 효율성을 높이도록 하였다.

- 확장성 : 제안하는 위험분석 방법론은 상세 위험분석 단계에서 자산, 취약성, 위협의 분석결과를 기반으로 산출된 위험의 정도에 따라 민감성의 수준을 13가지의 경우(case)로 분류하고, 위험수용, 위험무시, 위험감소, 그리고 위험이양의 4가지 대응책으로 분류하여 처리하도록 함으로써 위험의 정도를 좀더 세분화하고자 하는 경우 또는 정보시스템의 규모의 확장이 가능하도록 하였다.

- 안정성 : 상세위험분석단계는 세부적으로 자산분석, 취약성분석 그리고 위협분석을 구체적으로 실시하도록 하였으며, 위험정도를 13가지의 경우로 나누어 물리적, 관리적 그리고 기술적 관점에서 처리되도록 하였다. 그리고 사후처리단계에서는 잠재적인 위협 또는 미 발견된 취약성이나 이 시점에서 발견된 취약성을 찾기 위하여 모의 침투테스트과정을 실시함으로써, 보다 안정적인 정보시스템 보안관리가 가능하도록 하였다.

2. 위험분석 사전처리단계

위험분석 사전처리단계는 조직의 정보시스템 환경에 적합한 위험분석 수준을 결정하여 제안하는 위험분석 방법론의 효율성을 높이기 위함이다.

정보시스템 보안관리를 위하여 고려해야할 위험분석 사전처리단계의 요소로는 정보시스템의 사용목적과 정보시스템에 대한 업무의 의존도 및 시스템에서 처리하고자하는 정보의 비밀성, 무결성, 가용성에 대한 의존도 그리고 자산도입, 복구, 교체 등의 관점에서 시스템에 대한 투자정도 등의 요소에 따라 위험분석 접근방법을 기본위험분석단계 또는 상세위험분석단계로 분류하여 실행함으로써, 위험분석의 중복작업과정을 최대한 줄이도록 하였다.

가. 기본위험분석단계

정보시스템의 위험수준에 따라 위험분석 단계를 기본위험분석단계와 상세위험분석단계로 나누어 처리하도록 하였다.

기본위험분석단계는 정보시스템의 정보보안 체계가

표 1. 기본 위험분석을 위한 목록
Table 1. A list for basic risk analysis.

분류	통제항목	세부사항	중요도		보안목적		
			상	하	C	I	A
관리적	정책 및 절차	어떤 보안정책이 수립되어있는가?					
	직원통제	직무분리가 이루어지는가?					
		직무교대는 이루어지는가?					
		직원이해고, 정직 등에 대한 보안대책은 이루어지는가?					
	감독구조	경영진은 경영 및 감독구조를 구성하고 있는가?					
	보안의식훈련	보안의식 훈련이 정기적으로 이루어지고 있는가?					
	시험	모든 보안통제와 메커니즘을 정기적으로 시험하고 있는가?					
		침투시험을 하고 있는가?					
		절차와 기준들에 대한 재검토가 이루어지는가?					
물리적	네트워크분리	네트워크의 특별한 영역에 대한 보안카드를 사용하는가?					
	경계선보안	경비원, 경비견이 있는가?					
		CCTV, 조명, 담장, 동작 탐지기 센서, 경보, 등이 설치되어있는가?					
	컴퓨터통제	컴퓨터 커버의 자물쇠가 있는가?					
		컴퓨터 암호화를 실행하는가?					
		전기적 방출을 감소시키는 보호 장치를 실행하는가?					
	직업영역구분	특정한 직원들에 대한 작업영역이 분리되어 있는가?					
	데이터백업	데이터 백업은 어떤 장치로 어느 정도 주기를 갖고 실행되는가?					
	케이블링	케이블로 인한 혼선 혹은 도청을 방지하기위한 설비가 이루어져 있는가?					
기술적	시스템접근	안전한 패스워드를 사용하는가?					
		커버로스를 실행하는가?					
		특정한 인증기술을 사용하는가?					
	네트워크구조	일반사용자와 DMZ에의 접근 통제가 이루어지는가?					
	네트워크접근	여러 세그먼트로의 접근을 실행하는 기술적 통제가 이루어 지는가?					
	암호화, 프로토콜	어떤 암호화와 프로토콜이 구현되었는가?					
	통제구역	전자파 보안이 이루어지고 있는가?					
	감사	내, 외부적인 감사기능이 이루어지고 있는가?					

C : Confidentiality 비밀성 I : Integrity 무결성
A : Availability 가용성 DMZ : Demilitarized zone

구축되지 않았거나 단기간 내에 최소한의 보안 제어를 위한 수단이 필요한 경우 설정된 항목들을 체크 목록으로 이용하여 점검하도록 하였다. 기본위험분석단계의 목적은 정보시스템의 보안관리에 대한 최소한의 보안대책수립이다. 이 단계는 적은 비용으로 정보시스템의 기본적인 보안수준을 수립할 수 있다. [표 1]은 기본위험분석단계에서 시행될 항목별 위험수준과 보안목적을 위한 목록은 위험분석방법론[1]을 기반으로 보안의 중요도에 따라 도출하여 작성하였다. 이러한 기본위험분석 단계이서 수행될 "기본위험분석을 위한 목록"은 기업마다 요구되는 보안수준이 다르므로 관리적, 논리적, 기술적 보안통제에 대한 중요도와 보안목적에 점수를 부여하고, 합산하여 대응책을 고려하게 된다.

나. 상세위험분석단계

위험분석 대상이 되는 정보시스템 업무의 중요도, 의존도 그리고 투자정도와 자산의 가치가 높을 경우 보다 세부적인 상세위험분석과정을 실시하도록 하였다. 상세위험분석단계는 자산, 취약성, 그리고 위협요소들로 분석단계가 실행된 후 위험의 정도를 산출하도록 한다.

(1) 자산요소의 분석

정보시스템 보안관리를 위한 위험분석 방법론에서는 자산의 가치를 산정하기 위하여 3단계 과정을 실행한다.

[표 2]에서 제시한 것처럼 자산목록을 '자산 항목별로 분류하고, 다시 유형과 무형의 자산으로 분류한다. 자산 항목별로 분류된 자산은 기업의 정보시스템에 따라 순수자산가치 산정 기준표에 의하여 등급을 산정하도록 한다. 순수자산가치산정표는 조직 내에서 정보시스템에 대한 자산으로서 자체 가치산정 기준표 이므로 각 조직의 유형, 조직의 목표와 목적은 물론, 조직의 정보시스템의 중요도에 따라 다소 차이가 있을 수 있다. 순수자산의 가치산정 기준에 따라 등급을 1에서 5 로 분류하여 그 값을 할당하도록 한다. 조직자체에서 평가한 자산의 가치가 가장 높은 경우는 등급을 5로 하고, 자산의 가치가 높은 경우는 등급이 4, 자산의 가치가 보통이면 3, 자산 가치가 낮으면 2, 그리고 순수자산으로서의 가치가 가장 낮다고 평가되면 등급을 1로 산정한다[3],[7].

예를 들어, [표 2]에서 유형의 자산 중에 데이터가 재무정보, 프로젝트 상세정보, 또는 이윤 및 예측 정보 등과 같이 민감한 것은 순수자산가치의 등급이 5로 산정된다. 그러나 데이터가 특정프로젝트의 작업인원, 시작될 프로젝트 같은 공개 데이터인 경우는 등급이 1로 산정 된다. 자산 가치산정의 다음 단계는 [표 3]과 같이 조직의 업무처리에 따라서 분류된 자산을 정성적 그리고 정량적 방법을 이용하여 업무의 중요도 값을 산정한다. 물론, 업무중요도 자산가치는 조직의 정보시스템이 갖는 보안목적과 정책 그리고 자산가치산정에 따라 다르게 산정된다. 업무중요도의 등급이 5인 경우는 업무처리에서 중요도가 가장 높은 경우이고, 중요도가 비교적 높은 경우는 등급이 4, 중요도가 보통인 경우는 등급이 3, 그다지 중요하지 않은 경우는 등급이 2, 그리고 업무처리를 하는데 그다지 중요하지 않은 자산의 경우는 등급을 1로 나누어 평가하고 업무중요도 수치로 산정한다. 마지막 단계는 순수자산가치 산정값과 업무중

표 2. 순수자산가치 산정
Table 2. A production of pure asset values.

자산 목록		대분류	소분류	순수 자산가치
자산 항목별 분류	유형의 자산	S/W	OS	
			응용S/W	
			시스템S/W	
			보안 S/W	
			네트워크OS	
		H/W	서버	
			전산시스템	
			Firewall	
			IDS	
			PC	
		Network 장비	Gateway	
			Router	
			Hub	
			VPN	
		환경	UPS	
			화재통제시스템	
			항온항습기	
			차폐벽	
		DATA	민감	
			기밀	
			비밀	
			독점	
			공개	
	무형의 자산	사람	IT 관리자	
			DB 관리자	
			프로그래머	
			시스템운영자	
			운영책임자	

표 3. 업무중요도기반의 자산가치
Table 3. An asset value based on important of business process.

자산가치 산정 방법	업무처리별 분류	업무 중요도
정량적 방법	자산도입비용	
	자산복구비용	
	자산교체비용	
정성적 방법	B.P. 기여도	
	복구시간	
	조직과 작업 수	
	보안정책	

요도에서 산출된 값을 곱하고, 그 결과에 시간에 대한 상대적 가중치를 부여하도록 한다. 즉, 순수자산 중에서 유형의 자산은 시간이 경과된 자산에 대하여는 그 가치가 상쇄되는 것으로 한다. 그리고 무형의 자산, 예를 들면 사람의 지식정도, 업무능력 등은 시간의 경과와 직급에 따라 상대적인 가중치를 반영하도록 한다[1],[7].

(2) 취약성 요소 분석

취약성 요소에 대한 분석은 자산분석으로 도출된 자산의 속성과 중요도를 기반으로 자산이 근본적으로 갖고 있는 약점인 취약점을 찾아내고, 취약점이 전체적인 위험에 미칠 수 있는 영향을 분석하는 일련의 과정이다.

[표 4]는 취약성을 유형에 따라 운영, 행정, 인증, 보안정책, 비상계획, 재해대책, 교육, 그리고 감리/감사 등의 분야로 나누어 분류하고, 다시 세부 항목별로 분류하고 취약성 등급을 예시 하였다. 분류된 취약 항목들은 자산, 위협 등에 따라 위험을 초래하게 되고, 이에 대한 대응책이 강화되면 취약성은 감소하겠지만, 대응책 자체도 잠재적인 취약성을 갖고 있으므로, 취약성은

표 4. 취약성 유형과 등급의 예시
Table 4. An example of type & levels of Vulnerability.

취약성 유형	취약 항목	세부 취약 항목	취약성 등급
운영	시스템 운영	서버	3
		응용 시스템	4
		유선 시스템	4
		무선 시스템	5
	통신 운영	프로토콜	2
		네트워크장비	4
		전송매체	4
		통신 S/W	2
행정	자료 관리	기밀 자료	5
		보안자료	4
		일반자료	1
	건물 관리	CCTV	3
		담장	1
	인사 관리	입사	3
		퇴사	5
인증	접근 통제	임의적	3
		강제적	4
	권한부여	직접권한	5
		간접권한	4
보안정책	물리적 보안정책	컴퓨터 범죄	4
	관리적 보안정책	윤리	3
	기술적 보안정책	해킹	4
비상계획	백업	하드웨어 백업	4
		소프트웨어 백업	5
	재난 예측	비상사태 대응	3
재해대책	사업연속계획 (BCP)	잠재적인 계획	3
		전략 시나리오	3
	재해대책계획 (DRP)	점검표 시험	5
		시뮬레이션 시험	4
교육	교육정책	입사 전 교육	3
		입사 후 교육	4
감리/감사	감리/감사정책	감리정책	3
		감사정책	4

0이 될 수 없다. 그렇기 때문에 조직이 추구하고자하는 보안수준과 보안관리의 기본원칙인 기밀성, 무결성, 그리고 가용성 중에서 어디에 더 중요도를 두는가에 따라 취약성의 등급이 다르게 산정될 것이다. 그리고 조직에서 분석, 평가한 자산의 가치에 따라 취약성의 등급은 달라진다. 자산의 가치가 높을수록 취약성에 대한 가중치도 높아지게 된다. 취약성의 등급도 5단계로 설정한다[7]. 5등급은 취약성이 매우 높은 경우이고, 4단계는 취약성이 비교적 높은 단계, 3단계는 취약성이 보통, 2단계는 취약성이 낮은 단계, 그리고 1단계는 취약성이 거의 없는 경우로 산정한다. 예를 들어, [표 4]에서 취약성의 유형이 행정분야인 경우 취약항목에서 건물관리의 CCTV는 취약성이 3으로 책정하였다. 이는 CCTV가 갖고 있는 작동반경과 렌즈의 정확도 그리고 CCTV와 함께 경비원이 필요하다는 취약점 등을 고려하여 산정된 취약성 등급이다.

(3) 위협 요소 분석

위협 요소 분석단계는 위협의 주체(예를 들면, 절도, 화재, 해킹 등)가 취약성을 활용하여 조직의 자산에 피해를 가할 수 있는 잠재적인 요소인 위협의 요소를 파악하는 단계이다. 그리고 알려진 위협 혹은 그렇지 않은 위협들이 자산에 미치는 영향의 정도에 따라서 그 중요도를 산정하고 산정된 위협의 중요도와 자산의 가치산정 결과 값을 합한 결과를 순위별로 정리하여 위협 순위를 결정한다.

예를 들면, 위협의 요소가 사람의 '조작미숙 혹은 실수'에 의한 것(위협의 중요도는 4)이라고 할 때, 자산이 되는 '인사정보 데이터'의 자산가치는 3등급으로 산정되어 있으므로 산출된 위협 점수는 7이고 이에 대한 위협 순위는 다른 위협순위와 상호 비교하여 결정될 것이며,

표 5. 위협의 유형
Table 5. A type of threats.

위협 유형	대 분류	소 분류	위협의 중요도	위협 순위	위협 결과 값
의도적 위협	물리적	절도			
		테러			
	기술적	유해프로그램 삽입			
		해킹			
비의도적 위협	사람	조작실수/미숙			
		데이터 유출			
	천재지변	화재			
		수해			
		지진			
	시스템	OS 결함			
		시스템 결함			

표 6. 위험정도 산출표
Table 6. risk degree production table.

VL : Very Low : 매우 낮음, L : Low : 낮음
M : Medium : 보통, H : High : 비교적 높음
VH : Very High : 매우 높음

위협		매우 낮음					낮음					보통					높음					매우 높음				
취약성		VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH	VL	L	M	H	VH
자산가치	1	1	2	3	4	5	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9
	2	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10
	3	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11
	4	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12
	5	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13

이에 따른 위협의 결과 값을 1~5의 범위에서 산정한다.

3. 대응책 설정단계

가. 위험정도산출

자산과 취약성 그리고 위협에 대한 분석 자료를 기반으로 [표 6]과 같이 위험정도를 산출한다[11]. 자산의 가치 산정값은 1~5의 범위로 설정하고, 취약성은 VL(Very Low) 매우 낮음, L(Low) 낮음, M(Medium) 보통, H(High) 비교적 높음, VH (Very High) 매우 높음의 5등급으로 범위를 설정하고, 위협은 매우낮음, 낮음, 보통, 높음, 그리고 매우높음의 5개 등급으로 설정한다[5]. 자산의 가치가 1이고, 취약성은 매우 낮음(Very Low) 그리고 위협이 매우 낮음인 경우 위험정도 산출표의 값은 1을 기준으로 시작되며, 위협이 낮음, 보통, 높음, 매우높음에 따라 위험정도는 1등급씩 증가되도록 설정되어서 전체 위험정도는 1에서 13까지의 경우를 갖게 된다. 예를 들어, 자산가치가 3이고, 위협은 낮음, 취약성은 보통(M)인 경우 위험정도는 6인 경우로 산출된다.

나. 대응책 설정

자산, 취약성, 위협의 요소에 대한 분석결과를 기반으로 [표 6]과 같이 위험정도가 1에서 13가지의 경우로 산출되면 이에 대한 대응책을 설정한다.

[표 7]은 대응책 설정을 위하여 위험에 대응하여 어떻게 대처할 것인가를 위험 수용(accepting), 위험 무시(rejecting), 위험 감소(reducing), 그리고 위험 이양(transfe-rring)의 방법으로 물리적, 관리적, 기술적인 관점에서 실행하도록 한다.

위험을 수용하는 경우는 자산의 가치에 비하여 비용효과적인 측면에서 위험에 대한 대응책 비용이 위험비용을 초과하는 경우로서 이 경우는 위험을 수용하는 대응책을 실행하도록 한다. 위험무시의 경우는 정보시스템이 위험에 대한 기본 물리적, 관리적, 기술적 보안대응책으로 보안이 가능하다고 판단되며, 그 이상의 대응책에 대한 비용효율문제를 고려하여, 새로운 대응책에 대하여는 무시해버리는 경우이다.

그러나 정보시스템이 보안대응책을 설치하여 가능한 위험을 감소시키는 대응책은 일반적인 보안 대응책으로

표 7. 대응책 설정단계
Table 7. counter measure setting phase.

위험정도	대응책	관리적	물리적	기술적
1 2	위험 수용	수용		
3 4	위험 무시	시설접근통제	식별메커니즘	잠금, 패스워드 IC 카드
		인적접근통제	인증메커니즘 울타리(fencing) 조명, 감시장치 경비원, 경비견 시각적녹화장치 탐지장치	마그테틱카드 무선근접판독기 CCTV,파장형태 근접탐지장치 광전자사진캐커니즘 수동식적외선시스템
		건설 관리	벽, 문, 천장, 창	차폐벽, 경보 가연성, 화재등급 접근성
		대피절차 시스템종료절차 화재진압기술 사회불안정의 올바른처리방법 고장,사고대응책	설비 구성요소 전원공급 정전기예방 온도,습도,통풍	전력보호 -UPS -전력선조절기 -백업전원 -화재탐지기 -소화기
		보안의무사항 인력관리	업무분담 수동작업훈련 업무교대 보안교육	사전고용심사 직원관리 고용종결후 지속적인보안교육
5 6 7 8 9 10	위험 감소	네트워크관리	네트워크설계 토플로지 프로토콜	보안테트워크장비 (라우터, 브리지, 스위치, 게이트웨이) 매체접근기술 보안프로토콜구축
		통신관리	LAN, MAN VAN, WAN ISDN	전화통신보안 S/LAN, S/WAN XDSL, VPN
		무선통신관리	무선사설지역네트워크	블루투스 무선보안기술
		시스템접근통제	특권통제 임의적, 강제적	스마트카드 생체인식기술
		Firewall 관리	시스템보안 네트워크보안	패킷필터링 프록시, 하니팟
		침입탐지 복구	침입탐지시스템	맨 트랩 네트워크IDS 호스트 IDS
		감사	감사,감시,감독	감사시스템 모니터링
		보안정책 사업연속계획 재해복구계획	재난복구 비상계획 백업대안 문서화 시험과 훈련 비상사태대응	바이러스제거, 복구 하드웨어백업 -핫, 웜, 콜드사이트 소프트웨어백업 -중분,차별,완전백업
		법률, 조사 윤리규정	윤리강령 법 명령 규제	해킹대응 식별,보호,기소 폐기논점(장비,S/W) 수출입법, 사적보호
11 12 13	위험 이양	보험관리	보험	

이러한 경우는 위험감소 방법이다. 마지막으로, 정보시스템 보안관리를 위해서 총체적 혹은 잔류 위험이 운에 맡기기에는 너무 위험하다면 자산을 보호하기 위해 보험회사에 위험을 이양하도록 하는 대응책을 시행한다.

위험정도가 1~2이면 자산의 가치가 1~2정도로서, 자산의 가치가 매우 적다. 그리고 취약성과 위협 역시 "매우낮음"으로서 정보시스템이 기본적으로 대응이 가능한 경우로 고려되며, 비용효과적인 측면을 고려할 때 위험을 그냥 받아들이는 위험수용의 방법으로 설정하였다. 위험의 정도가 3~4이면 자산의 가치와 보안대응책을 위한 비용효율문제를 고려할 때, 보안교육, 차폐벽, 부서에 대한 개인 접근통제, 시스템 잠금장치 등과 같은 기본적인 시설물관리 등으로 대응하도록 하며, 위험에 대하여는 위험무시 대응책을 시행하도록 하였다. 위험정도가 5~10이면 자산으로서의 가치도 있으며, 위협과 취약성에 대한 적절한 보안 대응책으로 가능한 위험을 감소시키기 위한 대응책 구현이 절절하다고 고려되어 위험감소 대응책으로 설정하였다. 위험정도가 11~13이면 자산의 가치도 "매우높음" 이지만 그에 대한 위협과 취약성 또한 매우높음인 경우로 위험에 대한 대응책을 보험회사에 이양하는 대응책이 필요한 것으로 설정하였다. 조직의 대응책 실행은 "대응책의 가치 = 대응책 설치전의 ALE -대응책 설치후의 ALE - 대응책의 연간비용"과 같이 실행이전 그리고 이후와 비교하여, 비용 대 효과의 관계를 고려하여 각 단계별로 실행하도록 한다.

보안 대응책은 관리적, 물리적, 그리고 기술적인 관점에서 통제가 이루어지도록 한다. 관리적 통제는 보안정책, 표준, 그리고 절차의 개발과 공표, 지침, 개인에 대한 심사, 보안의식 교육, 시스템 활동 감시, 그리고 변화통제 절차를 포함한다. 기술적 통제는 논리적 접근통제 메커니즘. 패스워드와 자원관리, 식별과 인증방법, 보안장비, 그리고 네트워크 설정 등으로 구성된다. 물리적 통제는 시설물과 다른 부서에 대한 개인들의 접근을 통제하고, 시스템을 잠그고 불필요한 플로피와 CD-ROM 드라이브를 제거하며, 시설물의 경계를 보호하고, 침입에 대한 감시와 환경의 통제를 수반한다.

3. 사후관리단계

사후관리는 보안 정책 수립에서 위험관리에 이르기까지 수행된 보안관리 단계가 조직의 보안성 향상에 실질적으로 도움이 되었는지 점검하고 관리하는 분야로서, 감사(audit), 점검(monitoring), 사고대응(incident respond), 대책의 유지보수 등이 이루어진다.

표 8. 보안 정책
Table 8. Security Policy.

특성	내용
규제적	특정한 산업에 의한 표준을 따르고 법에 의해 규제되는 것을 보증하기위해 작성
권고적	조직 내에서 이루어져야 하는 특정한 종류의 행동과 활동들을 강력하게 제의하기 위한 것
정보적	특정한 주제를 조직의 일원들에게 알리기 위해 작성하며 기업목표와 사명 등을 보고하는 체계 등

가. 보안정책 수립

보안정책은 조직 안에서 어떤 종류의 역할을 보안이 수행하는지를 규정하기위한 선언 작업이다. 보안정책에는 그 특성에 따라 [표 8]처럼 규제적(regulatory), 권고적(advisory), 그리고 정보적(informative)인 정책으로 수립할 수 있다. 대응책은 기술적인 구현 후에도 시스템 보안정책과 수행계획에 맞게 구현되었는지를 검증하고 승인했을 경우에만 대응책이 운영에 들어갈 수 있도록 지속적으로 관리, 운영해야 한다.

나. 모의 침투테스트

대응책의 설정과 실행 이후에도 잔재 위협과 취약성으로 인한 잔류 위협은 항상 존재 가능성이 있으므로 잔류위험 요소에 대한 평가단계를 실행하기 위하여 정보시스템에 침투테스트를 실행하도록 한다. 침투테스트를 실행하기 위해서는 정보시스템의 동작 전체를 일시 중단하거나, 모의실험으로 하거나, 부분실험 등의 방법으로 실행한다. 침투테스트 결과 발견된 취약성 목록을 정리하고, 사후처리시점에서 적절한 대응책을 구현하도록 한다.

다. 재난복구와 비상계획

이미 손실, 혹은 침해를 당한 경우라면 복구계획으로 손실을 최소화하고, 중요한 시스템과 인력의 가용성을 보장하기 위해서 계획의 수립과 재난에 대한 사전준비 작업을 시행한다. 이를 위한 기반자료로는 재난이후에도 사업이 최대한 연속적으로 수행될 수 있도록 하며, 이에 대한 비즈니스의 영향을 분석하고, 비상계획을 위한 요구사항들을 분석하도록 한다.

V. 결 론

본 연구는 기존의 위험분석 방법론들은 위험분석방법을 위한 단계가 비체계적이고 위험분석 방법도 추상

적인 표현이거나, 제시하는 예시가 극히 제한되어 있어서, 실무자들이 위험분석의 범주를 결정하고 대응하는 보안대책을 설정하는데 많은 어려움을 갖고 있다. 그렇기 때문에 본 논문에서 제안하는 위험분석 방법론은 절차상의 복잡성을 최소한으로 줄이기 위하여 3단계의 프레임(사전처리단계, 대응책설정단계, 사후처리단계)으로 나누어 실행하도록 함으로써 업무의 효율성을 향상시키도록 하였다. 사전처리단계는 기본위험분석단계와 상세위험분석단계로 나누어 처리하도록 하였다. 기본위험분석단계에서는 정보보안 체계가 구축되지 않았거나 단기간에 최소한의 보안 제어를 위한 수단이 필요한 경우 설정된 항목들을 점검하도록 하는 기본적인 보안관리 단계이며, 상세위험분석단계에서는 자산, 취약성, 위협의 요소들을 분석하고 분류하여 그에 대한 위험의 정도를 분류하는 단계이다. 제안하는 위험분석방법론은 자산, 취약성, 위협에 따라 위험의 정도를 산출하기위하여 자산, 취약성, 위협을 5등급으로 나눈 후 그에 대한 위험정도 산출표를 [표 6]으로 작성한 결과 위험의 정도는 1~13(취약성, 위협 이 0인 경우는 없음)종류로 분류·산출 되었다. 이렇게 산출된 위험의 종류에 대하여 자산의 가치와 취약성의 정도, 위협의 정도 그리고 이들에 대한 보안대응정책의 비용문제를 고려하여 위험수용, 위험거부, 위험감소, 위험이양 등의 보안 대응정책을 실행하도록 하였다.

자산의 가치수준이 1~2정도이면 Case 1-2 로 분류한다. 이 경우는 자산의 가치가 매우 적으므로 위험을 기업에서 "수용"하는 대응책을 실행한다. 자산의 가치수준이 3~4정도인 경우인 Case 3-4는 자산의 가치에 비하여 보안을 위한 대응정책비용이 너무 높은 경우이므로 비용 대 효율성을 고려하여 위험을 "거부"하는 대응책을 실행한다. Case 5-10인 경우는 자산의 가치와 위협, 취약성 등을 고려할 때 위험을 "감소"하기 위한 보안 대응책을 실시한다. Case 11-13인 경우는 자산의 가치도 높지만 그에 대한 보안 대응책의 비용을 기업이 감수하기에는 너무 과한경우로써 위험을 보험회사 등에 "이양"하는 보안대응책을 실시한다. [표 7]은 이러한 대응책 설정에 대하여 관리적, 물리적, 기술적으로 예시한다. 마지막으로 사후관리단계에서는 모의 침투테스트 등으로 지금까지는 드러나지 않았지만 잠재적인 취약성 혹은 정책수립이후 시점에서 발견된 위협 등에 대한 대응책 설정을 이행하는 단계이다. 또한, 위험 혹은 재난을 겪게 된 경우에도 사업은 연속적으로 수행되어야 하는데, 그에 대한 대책과 개선 및 유지보수 등의 수행도 사후관리단계에서 수행되어야 할 업무이다. 이상으로 제안한 위험분석방법론은 위험을 분석하고 보안대응책을 위한 방법론을 제시함으로써, 위험분석 절차상의 중복성을 없애고 효율성을 높이도록 하였다.

참 고 문 헌

[1] All in one *"CISSP Certification"* Mc Graw Hill, 2000.

[2] B. D. Jenkins, *"Security Risk Analysis and management"*, Countermeasures, Inc., 1998.

[3] Gray Stonebumer, Alice Goguen, and Alexis Feringa *"Risk Management Guide for Informa-tion Technology Systems"*, NIST, Oct., 2001.

[4] Harold F. Tipton and Micki Krause, *"Information Security Management Volume 3"*, 4th Edition, Auerbach Publications, pp. 417-430, 2002.

[5] ISO 7497-2, Information Processing Systems -Open Systems Interconnection-Basic Reference Model - Part 2 : Security Architecture

[6] ISO/IEC TR 13335, Guidelines for the Manage-ment of IT Security, 1997.

[7] *"Risk Analysis and Management Standards for Public Information Systems Security- Risk Analysis Methodology Model"*, 한국정보통신 기술 협회(TTA), 2000.

[8] 김정덕 *"ISO 정보기술 보안관리 지침 표준화동향"* 한국정보보호진흥원 2000.11.

[9] 박순태 *"보호프로파일개발을 위한 위험분석"* 한국정보보호진흥원, 2001.6.

[10] 엄정호 *"정보시스템의 체계적인 위험관리를 위한 실용적인 위험감소 방법론에 관한 연구"* 정보처리학회 논문지 C 제10-C권, 2003. 4

[11] 주영지, 이문구 *"업무프로세스기반의 위험분석평가 모델 설계 및 구현사례"* 이화여자대학교, 정보과학대학원 석사학위논문. 2003.

저 자 소 개

이 문 구(정회원)
1984년 숭실대학교 전자계산학 (학사)
1993년 이화여자대학교 대학원 전산교육학 (석사)
2000년 숭실대학교 대학원 컴퓨터시스템 (공학 박사)
2000년 3월~현재 김포대학컴퓨터계열 조교수
<주관심분야: 인터넷 보안, 시스템 보안, 암호화 알고리즘, 전자상거래 보안, 침입탐지 및 차단시스템, 정보관리>