정보보호관리체계 통제사항 선정 모델 연구

정회원 장 호 익*, 한 호 현**, 이 남 용***, 조 창 희****°

A Model of Control Selection in Information Security Management System

Ho Ik Jang*, Ho Hyeorn Han**, Nam Yong Lee***, Chang Hee Cho****° *Regular Members*

요 약

해킹, 개인정보유출 등으로 인한 인터넷 침해가 크게 증가하면서 기업이나 국가기관의 정보시스템이 안전하고 신뢰성이 있음을 알리는 활동으로 정보보호관리체계를 도입하는 사례가 증가하고 있다. 그러나 정보보호관리체계에 사용되는 통제사항이 지나치게 일반화되어 있고, 통제사항 선정을 위한 방법이나 연구가 부족하여 정보보호관리체계의 수립 시 중요한 절차인 통제사항 선정에 많은 어려움을 주는 문제점이 있다.

본 논문은 이러한 정보보호관리체계의 통제사항 선정의 문제점을 해결하기 위하여 기존의 문헌 연구와 정보보호 실무 경험을 반영하여 통제사항을 효과적이고 객관적으로 선정할 수 있는 방법을 제시하였다.

이 방법을 통해 정보보호관리체계 통제사항을 선정할 경우 선정의 정확도를 높일 수 있으며 정보보호관리체계 도입 시 발생하는 시간과 비용을 크게 줄일 수 있는 이점을 제공한다.

Key Words : Information Security Management System, Control Selection, Risk Tree Model, Security

ABSTRACT

As internet threats arising from hacking, the cases are increasing to introduce information security management system as an activity to let them know that the information system and information assets which companies or governments have are secure and reliable. However, as controls used in the information security management system are too generalized excessively, and research or methods related to selecting controls are insufficient, there are many difficulties in selecting them, which is a important procedure when the information security management system is established.

This paper proposed the method to select controls effectively and objectively reflecting the existing literature review and the practical experience of information protection in order to figure out the problems of selecting controls of the information security management system.

Selecting the controls of the information security management system using the model provided in this paper can enhance the accuracy of selection, which provide the advantage to save a lot of time and costs to be spent when introducing the information security management system.

※ 본 연구는 숭실대학교 교내연구비 지원으로 수행되었습니다.
* 숭실대학교(hic1021@moleg.go.kr), ** (사)한국해킹보안협회(rhhan@paran.com)
*** 숭실대학교(nylee@ssu.ac.kr), **** 법제처(lawworld@korea.kr) (°:교신저자)
논문번호 : 10035-0724, 접수일자 : 2010년 7월 24일

Ⅰ. 서 론

기업과 공공기관의 정보시스템 의존도가 커지고, 해킹, 악성코드 등 인터넷 침해가 증가하면서 고객이나 국민들에게 시스템이 안전하고 신뢰성이 있음을 알리는 활동이 중요한 문제로 대두되고 있다. 이와 관련하여 정보시스템과 정보자산이 안전하고 신뢰성 있게 관리되고 있음을 객관적으로 인증해 주는 정보보호관리체계 인증 제도가 도입되어 운영되고 있다[1]-[3],[6],[13],[14].

정보보호관리체계 인증 제도의 대표적인 것으로 국제표준기구인 ISO (International Standard Organization)가 운영하는 ISO27000[13]이 있다. 또한 국내에서는 2001년 도입된 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 제47조에 의한 정보보호 관리체계 인증제도(방송통신위원회, KCC ISMS)[3] 인증제도가 운영되고 있다. 미국은 FISMA (Federal Information Security Management Act)법에 의한 FIPS(Federal Information Processing Standards) 199, FIPS 200 제도[10],[11]를 운영하고 있다.

정보보호관리체계를 수립하고 적용하여 운영하는데 있어서의 핵심 절차는 정보보호 통제사항의 선정이다. 그러나 정보보호관리체계에 사용되는 통제사항이 지나치게 일반화되어 있고, 통제사항 선정을 위한 방법이나 연구가 부족하여 통제사항 선정이 객관적인 절차나 방법에 의존하기 보다는 정보보호관리체계 수립을 담당하고 있는 담당자의 기술 수준이나 경험 등에 영향을 많이 받게 된다 [15],[18].

이러한 이유로 주요 통제사항이 누락되어 인증심사 과정에서 결함 사항으로 발견되거나 필요하지 않은 통제사항을 과다하게 선정하여 적용함으로써 불필요한 비용과 시간을 낭비하기도 한다[1],[5],[7],[18].

이와 같은 현상은 정보보호관리체계 수립 시 통제사항 선정 방법이 중요하다는 점과 이를 실질적으로 지원하기 위한 체계적인 수단이나 방안의 도입이 필요하다는 점을 시사하고 있다. 본 연구는 이러한 상황을 고려하여 정보보호관리체계 통제사항의 누락이나 과다 선정 오류를 최소화할 수 있는 모델을 제시하고 그 유용성을 규명 하고자 한다.

Ⅱ. 관련연구

2.1 정보보호관리체계

ISO27000은 영국의 표준인 BS7799를 근간으로 2005년도에 ISO 국제 표준으로 채택되었다. ISO27000은 그림 1과 같은 표준 문서 간 상호 밀접한 관계를 갖고 있다.

통제사항은 ISO27001에 11개 분야 133개의 통제사항으로 규정되어 있으며 이들은 정보보호관리체계를 운영하고자 하는 조직의 특성에 따라 선택하여 사용하게 되며 필요한 경우 새로운 통제사항을 추가할 수 있다.

미국의 FIPS(Federal Information Processing Standards) 200 규정은 2002년에 제정된 FISMA (Federal Information Security Management Act)법에 근거를 두고 있으며 미국 연방정부 정보시스템에 갖추어야 할 최소한의 보안 요구 사항을 규정한다 [10],[11]. FIPS 200은 미국 연방정부 정보시스템의 보안 분류 표준인 FIPS 199와 함께 사용된다. FIPS

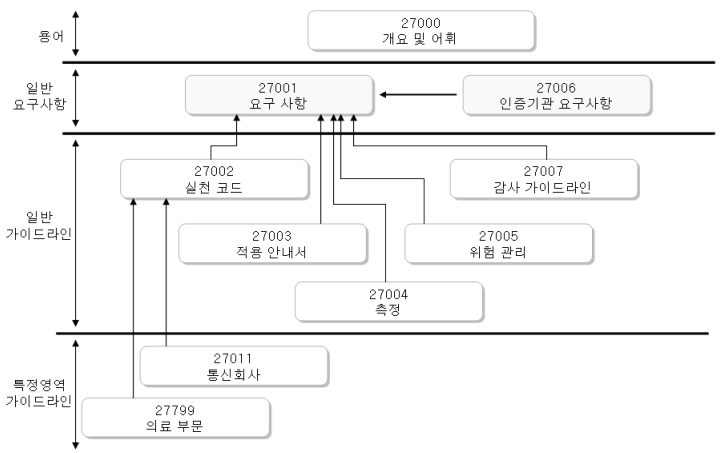


그림 1. ISO27000 표준 문서 관계도[13]

200의 목적은 최소한의 보안 요구 사항을 충족시키기 위해 통제사항을 선정하고 지정하는 방법을 제공함으로써 보다 향상된 보안 시스템을 개발, 적용, 운영하는데 있다. FIPS 200은 17개의 보안 분야를 설정하고 있는데, 이의 세부 통제사항은 NIST의 SP800-53 표준 문서[16]에서 다루고 있다.

우리나라 정보보호관리체계는 2001년 7월 정보통신망 이용촉진 및 정보보호 등에 관한 법률의 개정으로 인증 제도(방송통신위원회 정보보호관리체계, KCC ISMS)가 도입되었다.

2.2 기존의 통제사항 선정 방법

ISO27000의 통제사항 선정은 정보보호관리체계를 수립하는 과정에서 이뤄진다. 먼저 정보자산, 위협, 취약점 등을 식별하여 위험을 분석하고 평가한다. 이를 바탕으로 위험을 처리하기 위한 방안을 찾는다. 위험 처리 방안으로는 통제사항 적용, 위험 유지, 위험 회피, 위험 전가 등이 있다. 통제사항 선정은 위험 평가 및 위험 처리 절차에 따라 식별된 요구 사항에 따라 이뤄진다. ISO27000의 통제사항 선정을 위한 위험 관리 절차로 위험 평가(Risk Assessment) 부분은 위험의 크기를 산정(Risk Estimation) 분석하고, 그 위험 가치를 평가한다(Risk evaluation) [14].

FIPS 200의 통제사항은 NIST의 SP800-53에 언급된 내용에 따라 구성된다. FIPS 통제사항은 위험이 미치는 충격의 수준에 따라 낮음, 중간, 높음의 보안 체계를 기술한다. FIPS 200의 통제사항은 관리, 운영, 기술 등 3개 분류의 18개 통제 분야로 구분되는데, 각 통제사항은 통제, 보완 가이드, 통제 강화, 우선순위 등을 갖고 있다. 통제사항의 분류, 선정 등은 SP800-53의 가이드에 정의되어 있으며, FIPS 200은 통제사항 선정과 적용에 있어서 베이스라인 통제사항, 공통 통제사항, 통제사항 맞춤이라는 개념을 활용한다.

우리나라 정보보호관리체계의 통제사항 선정은 정보보호관리체계 과정 중 위험 관리 과정에서 이뤄진다. 위험 관리는 먼저 전략과 계획을 수립하고, 다음으로 위험을 구성하는 요소들을 분석한다. 그리고 이러한 분석 결과를 기초하여 위험을 평가한 다음 필요한 정보보호대책을 선정한다. 마지막으로 이들을 구현할 계획을 수립하는 다섯 단계의 과정으로 이루어진다.

지금까지 살펴본 ISO27000, FIPS200, KCC ISMS의 정보보호관리체계의 통제사항 선정의 방법

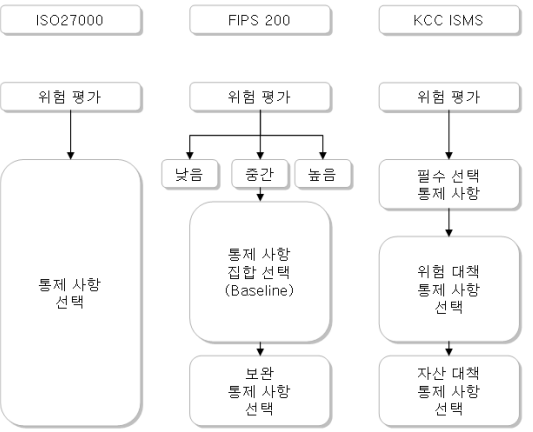


그림 2. 통제사항 선정 방법 비교

은 그림 2와 같이 요약할 수 있다.

ISO27000은 위험의 평가 결과에 따라 위험을 감소시키기 위한 통제사항을 통제 목록에서 선정한다는 특징을 갖는다. 반면에 FIPS 200은 위험의 평가 결과가 낮음, 중간, 높음에 따라 정해진 통제사항 집합을 일괄 선택한다. 통제사항을 일괄 선택한 후 특정한 위험 대책의 특성에 따라 추가적으로 보완하기 위한 통제사항을 추가로 선정한다는 특징을 갖는다. 우리나라 정보보호관리체계의 통제사항 선정 특징은 ISO27000과 FIPS 200의 혼합 형태를 갖는다. 필수 통제사항이 있고 여기에 자산 및 위험도에 따른 개별 통제사항을 선정한다.

ISO27000, FIPS 200, KCC ISMS의 통제사항 선정 방법의 특징과 문제점은 표 1과 같다. ISO27000의 방법은 위험평가에 따른 적절한 통제사항의 선정이 보장되는 반면에 통제사항 선정이 구체적이

표 1. 통제사항 선정 방법의 특징

구분	특징	문제점
ISO 27000	- 위험 평가에 따른 적절한 통제사항 선정권 보장 - 전문가의 도움이 필요 - 통제사항의 추가, 보완 용이	- 통제사항 선정 시 시간과 비용이 많이 듦 - 통제사항 선정의 구체적 방법이 제시되지 않음
FIPS 200	- 선정 방법 용이 - 시간과 비용이 적게 듦 - 전문가의 도움이 강하게 요구되지 않음	- 통제 상황 선정 시 과소 또는 과대 발생 - 환경 변화 등의 대처에 미흡
KCC ISMS	- 평가 기준 위주의 통제사항 제시 - 통제사항 선정의 용이성 - 선택 통제사항 선정 시 많은 노력 필요	- 통제사항 선정 방법이 구체적이지 않음 - 심사 시 통제사항에 대한 논란 발생 가능성이 큼

방법이 제시되지 않은 문제점이 있다. FIPS는 통제사항 선정 방법이 용이하게 되어 있으나 통제사항의 과다 또는 과소 선정의 가능성을 내포하고 있다. KCC ISMS는 통제사항의 선정이 용이하나 선택 통제사항의 선정에 많은 노력이 필요하다. 또한 통제사항 선정 방법이 구체적으로 제시되어 있지 않다. 즉 개별적인 통제사항 선택의 구체성 결여는 통제사항 선정의 한계라고 할 수 있으며 이는 누락이나 과다 선정 등 선정 오류로 이어져 위험 평가를 통한 통제의 목적 달성에 장애 요인이 된다.

2.3 공격 트리(Attack Trees)

공격 트리[8]는 1991년 Weiss가 제안한 모델로 시스템의 위협과 위험을 식별하는데 유용하다. 공격 트리 모델은 모든 공격 요소를 표현하고 공격이 성공하기 위하여 어떠한 특정 사건이 발생하여야 하는지를 결정하여 준다. 또한 위험을 결정하는데 시각적인 방법을 제공한다. 공격 트리는 공격의 길을 파악하여 대응하는 방안을 제공한다 [9]. 공격 트리의 활용은 가능한 공격 목적을 식별한 후 각각의 공격 목적에 대하여 개별 트리를 구성한다. 공격 트리가 완성되면 모든 노드에 가치를 부여하고 공격 가능성을 파악한다.

Schneier, Edge 등은 공격 트리가 공격 가능성과 위협을 식별하는데 매우 유용하다는 점을 밝혔고, Bistarelli 는 공격 트리에 공격에 대응하는 대응책을 추가하여 보안 트리(Protection Tree) 모델을 제시하였다 [9]. 보안 트리 모델은 그림 3의 사례에서 보여 주듯이 각각의 공격 트리 노드에 상응하는 대책을 추가하여 공격을 효과적으로 통제 할 수 있는 방안을 제공하여 준다. 노트북을 훔쳐가는 과정은 문을 부수거나 열쇠로 열고 들키지 않는 행위가 필요하다. 이러한 행위에 대한 보안 대책은 보안문의 설치, 보안키의 설치가 있다. 또한 감시카메라 설치와 경비자 근무를 통한 감시를 하는 대책이 필요하다. 보안 트리의 장점은 시각적으로 보안 대책을 확인하여 공격에 대한 대비를 용이하게 한다는 점이다.

Ⅲ. 리스크 트리 모델

3.1 연구 모델의 전제 조건

통제사항은 정보시스템이나 정보에 대한 위험에 대한 보호 대책이다. 현재의 정보보호관리체계에서는 특정한 위험에 대하여 적절한 대책인 통제사항이 있다는 전제를 함의하고 있다. 예를 들어 인적 보안을 위하여 개인에게 구체적인 책임을 부여해야 한다는 통제를 하게 된다.

그러나 다수의 사례나 관련 문헌에서 나타난 바와 같이 특정 위험에 대하여 적용한 통제사항으로 당초의 모든 위험 제거를 달성하기 어렵다는 점을 기초로 다음과 같은 조건을 설정하였다.

조건 (1) : 통제사항의 내재 위험이 존재한다.
조건 (2) : 통제사항의 보완 통제사항이 존재한다.

ISO13335-1에서는 보호 수단이 위험을 감소시키는 효과가 있음을 그림 4와 같은 단순한 모델로 표현한다 [12]. 보호 수단을 적용함으로써 위험으로부터 보호를 해주고 궁극적으로는 취약점을 감소시킨다고 주장한다. 또한 잔여 위험을 일정한 수준 이하로 낮추기 위해서는 다수의 보호 수단이 필요하다고 밝히고 있다. 보호 수단을 적용하여 제거되고 남은 위험이 잔여위험이 된다.

통제사항의 적용에도 불구하고 잔여 위험이 존재하는 것은 통제사항자체의 모호성과 불완전성에 있다. 또한 대책의 원인이 되는 위험이라는 요소가 정성적으로 표현되는 데에도 그 원인이 있을 수 있다.

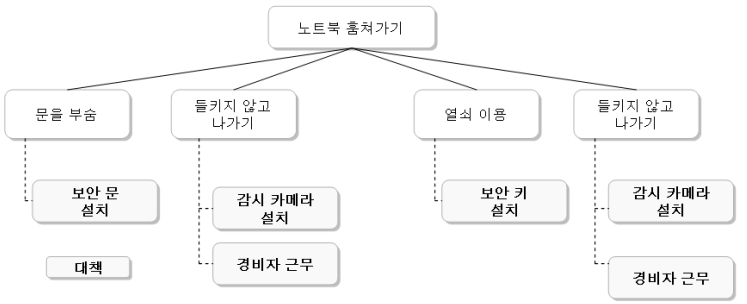


그림 3. 보안 트리 모델의 예[9]

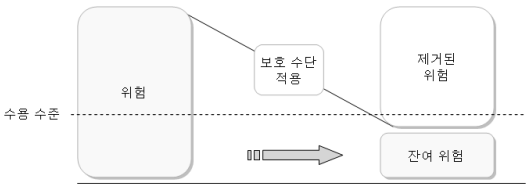


그림 4. 보호 수단과 위험 관계도[12]

ISO27000, FIPS 200에서는 위험을 일정 수준 이하로 감소시키기 위해서 다수의 통제가 필요함을 밝히고 있다. 하나의 통제사항으로 제거할 수 있는 위험은 한계가 있음을 의미한다 [16],[17].

3.2 리스크 트리 모델

본 논문에서 활용하는 리스크 트리 모델은 위험을 기반으로 최적의 통제사항을 누락 없이 선정하기 위한 모델이다. 이를 통하여 통제사항 선정의 효과성을 증진하기 위함이다. 이 모델은 공격 트리 모델에서 기본적인 개념을 도입하였다. 또한 특정 위험에 대응하는 다수의 통제사항이 필요하다는 문헌 연구 결과와 실제적으로 통제사항 선정 시 활용되는 통제사항의 일괄 선택이라는 실무적인 관점을 반영하였다.

3.2.1 리스크 트리의 정의

통제사항 선정을 위한 리스크 트리는 기본적으로 특정 위험 또는 통제 목적이 미치는 영향 경로에 따라 위험에 대비하기 위한 통제사항을 트리 구조로 배치하여 표현하는 것을 말한다. 그림 5는 리스크 트리 모델의 기본 구조이다. 특정 위험이나 통제 목적의 직접적인 목적을 달성하기 위한 주된 통제사항을 루트 노드에 배치하고 잔여 위험을 제거하기 위한 보완 통제사항을 루트 노드 하부에 리프 노드로 배치한다.

3.2.2 리스크 트리 작성

리스크 트리의 작성은 위험 평가에서 시작된다. 평가된 위험을 감당 가능한 위험 수준으로 낮추기 위하여 직접적이고 가장 핵심이 되는 통제사항을 선정한다. 다음으로 잔여 위험을 분리 도출한다. 잔여 위험이 분리 도출 되면 잔여 위험을 낮추기 위해 필요한 통제사항을 선정한다. 분리된 잔여 위험은 위험의 특성이나 충격 정도, 통제 목적에 따라 2개 이상으로 나누어 통제사항을 선정할 수 있다 (‘AND’ 트리 노드). 통제사항은 경우에 따라 두 개 이상의 대안이 나타날 수 있다(‘OR’ 트리 노드). 이러한 과정을 위험이 위험 수용 수준 이하로 낮추어 질 때 까지 반복한다. 각 단계에서 얻어진 통제사항을 트리 구조의 리프 노드에 배치함으로써 리스크 트리를 완성한다. 다음 그림 6은 리스크 트리를 작성하는 절차를 보여 준다.

잔여 위험에 대처하기 위하여 주어진 위험을 분리하여 대처하거나 하나 이상의 대안을 적용할 수 있다. 위험을 분리하여 대처하는 경우 ‘AND’ 노드가 만들어 진다. 두개 이상의 대안이 있는 경우 ‘OR’ 노드가 생성된다. 향후 ‘OR’ 노드는 대안의 선택에 활용할 수 있다. ‘AND’ 노드는 반드시 동시에 선정되어야 함을 의미한다. 리스크 트리 모델에서는 ‘OR’ 노드만을 구분 표기하여 ‘AND’ 노드와 구별하기로 한다. 다음의 그림 7은 ‘AND’ 노드와 ‘OR’ 노드를 표현한 리스크 트리 구조이다.

그림 7에서 통제사항 2.4, 통제사항 5.2는 대안 선정이 가능하다. 통제사항의 적용 환경, 적용 가능

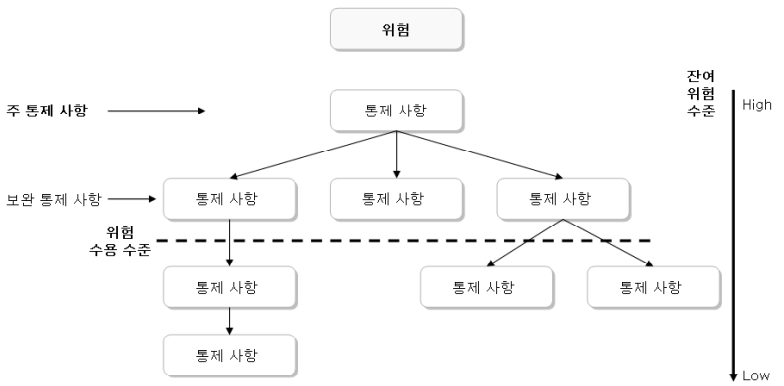


그림 5. 리스크 트리 모델 기본 구조

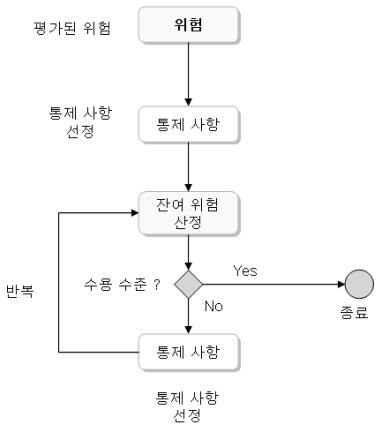


그림 6. 리스크 트리 작성 절차

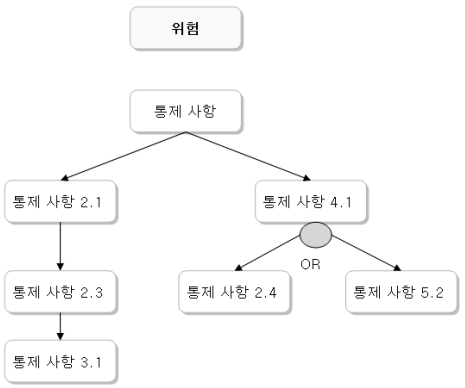


그림 7. 'OR' 노드 표시의 예

성, 비용 등을 고려하여 최적의 조건에 따라 선정을 가능하게 해준다. 다수의 위험에 대하여 리스크 트리를 구성할 경우에 동일한 리스크 트리 노드가 발생한다. 그림 8은 동일한 구성의 리스크 트리 노드 구조가 발생한 예이다. 이러한 현상은 평가된 위험이 동일하거나 유사한 위협에서 비롯된 특정한 위험이 있는 경우 등에서 나타날 수 있다. 이러한 결과를 통하여 서로 다른 위험에 대한 리스크 트리의 유사성을 직접적으로 확인할 수 있다.

3.2.3 리스크 트리의 노드 구조

리스크 트리의 핵심 내용은 정보보호관리체계에서 정의하고 있는 통제사항을 위험의 전이에 따라 그 관련성을 구성하는 것이라고 할 수 있다. 개별 정보보호관리체계의 통제사항 구성은 정보보호관리체계 별로 다른 구성을 갖는다. 리스크 트리 모델은 이러한 다양한 통제사항의 구성과 관계없이 적용이 가능하다. 리스크 트리 노드의 논리적 구조는 그림 9와 같다. 통제사항, 위험 통제 수준, 적용 비용, 통제의 복잡도 등을 표현하여 정보보호관리체계 구축 시 활용할 수 있도록 한다.

리스크 트리 노드는 정보보호관리체계의 통제사항을 기본적으로 표현한다. 또한 해당 통제가 위험을 제거할 수 있는 수준인 위험 통제 수준을 정의한다. 위험 통제 수준은 잔여 위험을 계산하는데 활용된다. 위험 통제 수준은 점 척도로도 표시가 가능하다. 적용 비용은 해당 통제 목적을 달성하기 위하여 통제사항을 적용하는데 드는 비용을 표시한다. 통제의 복잡도는 통제사항의 구현 또는 운영과 관련하여 발생하는 복잡성이나 난이도를 표시한다.

통제사항의 선정은 리스크 트리를 추적해 가면서 위험 통제 수준이나 적용 비용 등을 반영하여 결정된다. 여기서 위험 통제 수단과 적용 비용은 통제사항 선정의 가장 중요한 역할을 하며 신속하고 용이

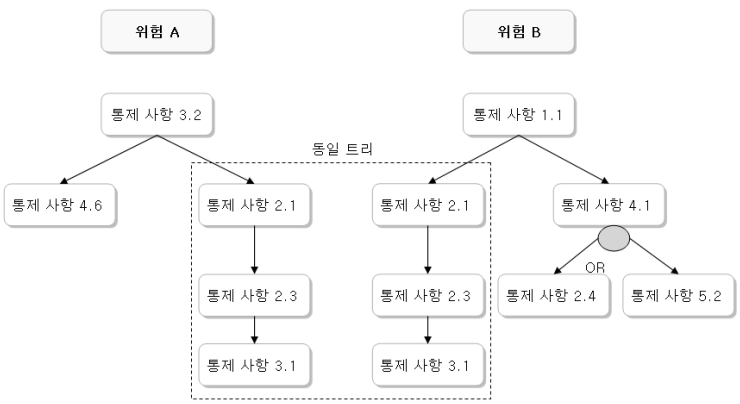


그림 8. 동일 리스크 트리 출현의 예

그림 9. 리스크 트리 노드의 논리적 구조

한 의사 결정의 틀을 제공한다.

Ⅳ. 리스크 트리를 이용한 통제사항 선정 실험

4.1 통제사항 선정 실험 방법

리스크 트리 모델의 유용성 확인을 위하여 통제사항 선정 실험을 하였다. 통제사항 선정 실험은 위험 평가의 결과를 특정 수준으로 가정하고 제시된 통제사항 중에서 통제사항을 적절하게 선정하는지에 대하여 실험 평가 집단을 4개의 집단으로 나누어 시행하였다. 실험을 위한 실험 조건은 위험 정의, 위험 평가, 운영시스템 구성, 통제사항, 위험 수용 수준 등 다섯 개의 조건을 설정하였다.

4.1.1 실험 조건

통제사항 선정 실험을 위한 환경 및 제반 제약 조건은 다음의 표 2와 같이 구성하였다.

위와 같은 실험 조건을 기준으로 선정된 통제사항 목록은 다음의 표 3과 같다. 선정된 통제사항은 실제 적용되어야 할 통제사항 6개와 실험을 목적으로 추가된 통제사항(오 선정 대상) 4개 등 모드 10개의 통제사항으로 구성하였다. 통제사항은 KCC

표 2. 통제사항 실험 조건

조건	내용
위협 정의	조직의 개인정보 DB를 해커가 해킹으로 탈취하여 개인 정보침해사고 우려
위험의 평가	위험의 평가 결과 적절한 통제사항을 선정하여 위험을 감소시켜야 함
운영 시스템 구성	해커가 해킹을 하는데 필수적으로 필요한 최소의 시스템이 운영되고 있는 것으로 가정
통제사항	위협이나 위험 감소와 관련하여 필요한 최소 통제사항과 선정 실험의 목적으로 추가된 통제사항만을 사용
위험 수용 수준	모든 위험을 수용하는 수준으로 가정

표 3. 실험에 사용된 통제사항 목록

구분	통제사항	분야	번호
적용 대상 통제사항	데이터베이스 접근	접근 통제	1
	네트워크 접근	접근 통제	2
	인터넷 접속 관리	운영 관리	3
	사용자 패스워드 관리	접근 통제	4
	사용자 등록	접근 통제	5
	보안 사고 관리	사고 관리	6
오 선정 대상 통제사항	주요 시스템 보호	운영 관리	7
	백업 및 복구 관리	운영 관리	8
	원격 운영관리	운영 관리	9
	원격 작업	운영 관리	10

ISMS의 통제사항을 기준으로 제시되었다.

4.1.2 실험 방법

리스크 트리 모델의 유용성 확인하기 위한 통제사항 선정 실험은 앞에서 제시한 실험 조건을 이용하여 솔로몬 4집단 실험설계(Solomon four-group design) 방법을 사용하였다. 이 실험 방법은 모든 외생 변수의 영향을 제거해 내적 타당성을 높일 수 있어 본 논문의 효과를 검증하는데 유용한 실험 방법으로 선정하였다 [4].

표 4. 실험 집단 구성

구분	집단	인원	리스크트리 모델 적용	실험 결과	
				사전 실험	사후 실험
실험 집단	실험집단 1	15	적용	O1	O2
	실험집단 2	15	적용	-	O5
통제 집단	통제집단 1	15	적용하지 않음	O3	O4
	통제집단 2	15	적용하지 않음	-	O6

표 5. 실험 결과

구분	1	2	3	4	5	6	소계	7	8	9	10	소계	계
O1	15	10	7	10	10	9	61	12	9	5	8	34	95
O2	15	14	14	15	14	11	83	5	3	4	6	18	101
O3	14	13	7	6	7	7	54	12	8	6	7	33	87
O4	15	13	8	12	9	5	62	7	5	5	6	23	85
O5	14	14	14	14	10	13	79	7	3	4	6	20	99
O6	14	14	6	11	5	7	57	10	8	6	7	31	88

4.2 선정 실험 결과 분석

선정 실험의 결과는 집단별로 선정 결과의 정확성을 비교 분석하였다. 또한 전제 조건과 관련한 설문에 대하여는 집단별 전체 결과를 종합하여 하나의 결과로 분석하였다.

4.2.1 선정 정확성 비율 및 과다 선정 개수

각 집단별 통제사항의 선정의 정확성 비율은 다음의 표 6과 같다.

솔로몬 4집단 실험 설계의 실험 효과는 다음과 같은 수식으로 산정된다.

실험 효과 = [O5 - 1/2(O1 + O3)]
- [O6 - 1/2(O1 + O3)]

위의 결과를 토대로 실험 효과를 계산하면

실험 효과 = [87.8% - 1/2(67.8% + 60.0%)]
- [63.3% - 1/2((67.8% + 60.0%)]
= 24.5%포인트가 된다.

이는 리스크 트리 모델을 적용하여 통제사항을 선정할 경우 기존의 선정 방법에 비하여 24.5%포인트의 개선 효과가 있음을 보여준다.

표 6. 통제사항 선정 정확성 비율

구분	사전 실험결과	사후 실험결과	비고
실험집단 1	67.8% (O1)	92.2% (O2)	리스크 트리 적용
통제집단 1	60.0% (O3)	68.9% (O4)	-
실험집단 2	-	87.8% (O5)	리스크 트리 적용
통제집단 2	-	63.3% (O6)	-

4.2.2 개별 통제사항 선정

개별 통제사항 선정의 변화를 분석하기 위하여 실험집단2와 통제집단2의 결과를 비교 분석해 본다.

과다 선정 대상 영역에서는 통제집단2가 실험집단2에 비하여 다소 많이 선정되었다.

두 집단간 선정의 정확성 비율과 과다 선정 개수의 분포는 다음의 그림 10과 같다.

표 7. 통제사항별 선정 결과

구분	선정 대상 영역					과다 선정 대상 영역				
	1	2	3	4	5	6	7	8	9	10
실험 집단2	14	14	14	14	10	13	7	3	4	6
통제 집단2	14	14	6	11	5	7	10	8	6	7

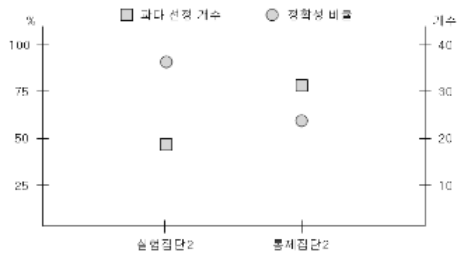


그림 10. 정확성 비율 및 과다 선정 개수 분포도

V. 결 론

정보보호관리체계의 통제사항 선정 과정에서의 오류를 방지하기 위한 방법으로 리스크 트리 모델을 제시하고 선정 실험을 통하여 리스크 트리 모델의 유용성을 보여주었다. 선정 실험의 결과 기존의 통제사항 선정 방법에 비하여 통제사항의 선정 정확도가 높아지고 과다 선정하는 오류를 크게 개선할 수 있음을 증명하였다.

연구의 분석 결과는 다음과 같이 요약할 수 있다.

첫째, 선정 실험을 통하여 리스크 트리 모델의 유용성과 효과성을 확인하였다. 선정 실험 결과 리스크 트리 모델을 이용한 통제사항 선정 집단이 기존의 방법을 이용한 집단에 비하여 현저하게 높은 선정 정확도를 보였으며 과다 선정의 개수도 크게 줄어듦을 보였다.

둘째, 통제사항간 위험 전이 관계를 활용할 수 있음을 입증하였다. 통제사항간 위험의 전이를 활용하여 리스크 트리 모델을 구성함으로써 위험을 체계적으로 분리하고 이를 활용하여 대책을 세울 수 있다는 점을 밝혔다.

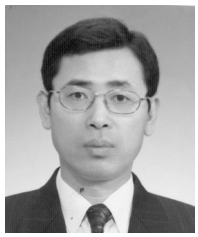
셋째, 통제사항 선정 과정을 객관화하고 자동화할 수 있는 가능성을 제공하였다.

참 고 문 헌

[1] 고규만, 김재성, 장상수, "정보보호관리체계 구축

시 일반적으로 나타나는 결함사례에 관한 분석," 정보보호학회지, 제17권, 제4호, 2007. 8.
[2] 김정덕, 이경석, "ISO/IEC JTC1 SC27의 정보보호관리 국제표준화 동향," 정보보호학회지, 제18권, 제4호, 2008. 8.
[3] 방송통신위원회 고시 제2010-3호, 정보보호관리체계 인증 등에 관한 고시, 방송통신위원회, 2010
[4] 정우석, 손일권, SPSS활용 과학적 조사방법론, 두양사, 2010.
[5] 최인수, 박지훈, 국방정보체계 수준별 정보보호 적용방안 연구, 한국국방연구원, 2007.
[6] 행정안전부 훈령 제164호, 전자정부 정보보호관리체계 인증지침, 행정안전부, 2009.
[7] KISA, "정보보호관리체계 위험관리 가이드", KISA, 2005.
[8] Bruce Schneier, "Attack Trees," Dr. Dobb's Journal, 1999.
[9] Edge K, A Framework for Analyzing and Mitigating the Vulnerabilities of Complex System via Attack and Protection Trees, 박사학위논문, AFIT, 2007.
[10] FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, NIST, 2006.
[11] FIPS PUB 200, Minimum Security Requirements for Federal Information Systems and Organizations, NIST, 2006.
[12] ISO/IEC 13335-1, Information technology - Security techniques - Management of Information and Communications Technology Security - Part 1, ISO, 2004.
[13] ISO/IEC 27000, Information technology - Security techniques - Information security management systems - Overview and Vocabulary, ISO, 2009.
[14] ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements, ISO, 2005.
[15] Richard T., Allison S., "An Autocorrelation Methodology for the Assessment of Security Assurance," Cyber Security Information and Global Information Assurance, Information Science Reference, 2009.
[16] SP800-53, Recommended Security Controls for Federal Information Systems and Organizations, NIST, 2009.
[17] SP800-53A, Guide for Assessing Security Controls in Federal Information System, NIST, 2008.
[18] Yves Barlette, Vladislav, "The Adoption of Information Security Management Standards," Cyber Security Information and Global Information Assurance, Information Science Reference, 2009.

장 호 익 (Ho Ik Jang) 정회원



2010년 8월 숭실대학교 박사과정
2010년 8월 현재 법제처 경제법제국장
<관심분야> 정보보호, 개인정보, 법령정보 시스템

한 호 현 (Ho Hyeorn Han) 정회원

1985년 서울대학교 해양학과 학사
1999년 서강대학교 경영대학원 석사
2010년 숭실대학교 컴퓨터학과 박사
2009년~현재 한국해킹보안협회 전무
<관심분야> 정보통신, 통신보안, 무선통신

이 남 용 (Nam Yong Lee) 정회원

1980년~1983년 고려대학교 경영대학원 경영정보학(MIS)(경영학석사)
1990년~1993년 미국 미시시피 주립대학교(MSU) 경영정보학(MIS)(경영학박사)
1999년 숭실대학교 컴퓨터학부 교수
<관심분야> 소프트웨어 테스팅, 품질보증, MIS, 정보보호

조 창 희 (Chang Hee Cho) 정회원

2007년 2월 숭실대학교 컴퓨터학과 박사

2010년 8월 현재 법제처 국가입법지원센터장

<관심분야> SW발주체계, 법령정보DB, 법정보학, 정보화관계법령 등