정보보호 거버넌스 구현을 위한 핵심성공요인에 관한 연구

김건우† · 김정덕††

요 약

최근 정보보호 거버넌스는 기업 거버넌스의 일부로서 기업의 가치 있는 비즈니스 정보자산을 보호하기 위한 중요한 이슈로 부각되고 있다. 현재 국내외에서 정보보호 거버넌스에 대한 활발한 연구가 진행되고 있지만, 그 개념이 추상적이기 때문에 실질적으로 정보보호 거버넌스를 구현한 조직은 드물다. 따라서 본 논문에서는 정보보호 거버넌스의 개념을 보다 구체화하기 위하여 ISO/IEC27014를 기반으로 최고 경영층 및 이사회가 수행 가능한 구체적인 활동을 식별하고, 조직의 목표 및 정보보호 거버넌스 목표를 달성하기 위한 핵심성공요인을 도출하였다.

키워드 : 정보보호 거버넌스, 핵심성공요인, 정보보호 관리

A Study on Critical Success Factors for Implementing Information Security Governance

Kun-Woo Kim† · Jung-Duk Kim††

ABSTRACT

Nowadays, information security governance which is an integral part of corporate governance has become an important issue in protecting valuable business information assets. However, there are few organizations which have implemented information security governance because of its abstract concept. The objective of this paper is to develop CSFs for implementing information security governance. Ten CSFs were developed based on the ISO/IEC 27014 Information Security Governance Framework.

Key Words : *Information Security Governance, Critical Success Factors*

† 중앙대학교 정보시스템학과 석사과정(제1저자)
†† 중앙대학교 정보시스템학과 교수(교신저자)
논문접수: 2010년 10월 5일, 1차수정을거쳐, 심사완료: 2010년 11월 15일
본 논문은 2008년도 중앙대학교 학술연구비 지원에 의한 것임

1. 서론

정보화 사회가 점차 고도화됨에 따라 대부분의 조직에서 정보를 핵심자산 중의 하나로 인식하고 있으며, 정보보호에 대한 관심 또한 증가하고 있다. 한국정보사회진흥원의 조사에 의하면, 우리나라의 정보화 수준은 전 세계 50개국 중 8위를 차지하고 있으며 정보에 대한 의존도가 점차 증가하고 있는 것으로 나타났다[2]. 반면, 2008년 정보보호 실태조사에 따르면, 정보화의 역기능 중의 하나인 보안사고 및 사건의 피해사례가 점진적으로 증가하고 있는 것으로 밝혀졌다[3]. 이러한 보안사고 및 사건의 피해를 최소화하기 위해서는 정보에 대한 의존성이 증가함에 따라 정보보호의 수준 역시 향상되어야 하며, 최근에는 조직의 보안 목표를 달성하기 위한 최고 경영층의 정보보호에 대한 방향제시 및 통제를 규정하는 정보보호 거버넌스가 중요한 이슈로 부각되고 있다.

Basie von Solms은 정보보호의 발전과정을 정보보호 기술 패러다임, 정보보호 관리 패러다임, 정보보호 조직화 패러다임, 정보보호 거버넌스 패러다임의 4가지 패러다임의 변화로 구분하고 있다[5]. 정보보호 기술 패러다임은 메인프레임에 대한 접근통제를 위한 보안기술을 중점적으로 연구하는 패러다임이고, 정보보호 관리 패러다임은 정보보호를 위한 기술적 솔루션의 한계를 인식하고, 이를 보완하기 위한 관리 활동에 초점을 맞춘 패러다임이다. 한편, 정보보호 조직화 패러다임은 효과적인 정보보호 구현을 위해 정보보호 표준 및 모범사례가 필요함을 인식하고, 정보보호 문화를 정착시켜 조직 구성원 전체의 정보보호 노력을 요구하는 패러다임이다. 끝으로, 정보보호에 대한 최고 경영층 및 이사회의 역할과 책임을 강조하는 정보보호 거버넌스 패러다임은 최고 경영층 및 이사회를 정보보호와 관련된 법, 규정에 대한 준수, 그리고 정보보호에 대한 계획 및 의사결정의 주체로 명시하고 있다.

현재 국내외에서 정보보호 거버넌스와 관련된 활발한 연구가 진행되고 있으며, 기존의 정보보호의 영역을 전통적인 기술적, 관리적 이슈에서 보다 전략적 차원으로 확대시키고 있다. 하지만 정보보호 거버넌스의 핵심인 최고 경영층 및 이사회의 역할과 책임을 업무에 반영하여 구체적인 활동으로 실체화시키기 어려운 것으로 나타났다. 즉, 기존의 정보보호 거버넌스에 대한 연구는 정보보호 거버넌스가 "왜" 필요하고, "무엇"을 대상으로 하는지에 초점이 맞추어져 있기 때문에 구체적으로 정보보호 거버넌스를 "어떻게" 구현해야 하는지에 대한 연구가 미흡하다고 할 수 있다. 따라서 정보보호 거버넌스 구현을 위한 핵심성공요인을 파악하여, 최고 경영층 및 이사회가 수행해야 하는 필수적인 활동들을 명시할 필요가 있다.

본 논문은 정보보호 거버넌스를 구현하기 위해 필요한 요인들을 도출하는 탐색적 연구로서, 정보보호 거버넌스의 목표를 달성하기 위한 최고 경영층 및 이사회의 필수적인 활동들을 구체화하기 위해 다음과 같은 질문들에 답할 것이다.

- 정보보호 거버넌스를 구현하기 위한 핵심성공요인은 무엇인가?
- 도출된 핵심성공요인은 정보보호 거버넌스 구현에 있어 어느 정도 중요하며, 실무에 적용 가능한가?

또한 위와 같은 질문들에 답하기 위해 다음과 같은 사항에 대해 중점적으로 논하고자 한다. 우선, 기존에 연구된 정보보호 거버넌스의 개념 및 프레임워크를 분석하여, 최고 경영층 및 이사회가 수행해야할 필수적이고 구체적인 활동을 도출할 수 있는 프레임워크를 선별할 것이다. 그리고 선별된 정보보호 거버넌스 프레임워크에 핵심성공요인 이론을 적용하여, 정보보호 거버넌스 구현에 필요한 핵심성공요인을 파악하도록 한다. 끝으로, 도출된 핵심성공요인의 적합성 여부를 포커스 그룹 인터뷰를 통해 평가하고, 개선사항을 도출할 것이다.

2. 관련연구

2.1 정보보호 거버넌스

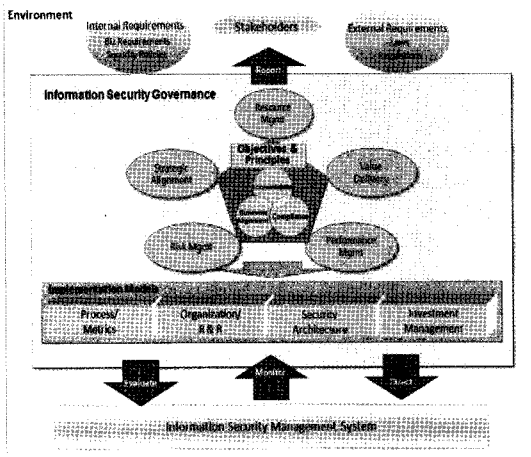
2.1.1 정보보호 거버넌스의 개념

조직의 정보시스템에 전자적으로 저장된 재무 데이터의 오남용 및 핵심 데이터의 취급에 대한 막강한 권한이 있는 최고 경영층의 사기 행위를 방지하기 위해 제정된 법, 규정의 준수를 강조하는 기업 거버넌스가 비즈니스 영역에서 점차 중요하게 인식되고 있다. 이러한 측면에서 정보보호 거버넌스는 최고 경영층의 비즈니스 관련 위험에 대한 관리를 지시하고, 통제하는 기업 거버넌스 측면의 정보보호 스 측면의인식되기 시작하였다[17]. 한편, Basie von Solms와 Rossouw von Solms은 정보보호 거버넌스는 기존의 정보보호 관리활동의 문제점을 극복하기 위한 방법으로써 그 필요성을 제시하였으며[4], 정보보호는 더 이상 중간 관리자의 책임이 아니고, 기술적인 이슈만이 아니라는 것을 알 수 있다. 또한, 다양한 비즈니스 환경을 고려한 최고 경영층의 정보보호 활동과 비즈니스 관련 법, 규정의 준수가 거버넌스 차원에서 수행되어야 함을 의미한다.

현재 정보보호 거버넌스는 국내외 학계 및 기관에서 연구되고 있으며, 국제 표준으로 제정되고 있는 중으로, 그 정의가 명확하게 정립되지 않고 다양하게 해석되고 있지만 기업 거버넌스의 일부이거나 최고 경영층에 의해 수행되어지는 정보보호 활동 및 프로세스로서 인식되고 있다[5][21][15][16]. 한편, 김정덕은 기존의 다양한 정보보호 거버넌스의 정의로부터 정보보호 거버넌스의 요구사항을 도출하여 통합적인 측면에서 정보보호 거버넌스의 개념을 정립하으며[11], 정보보호 거버넌스는 최고 경영층 및 이사회의 참여, 전사적 위험관리 노력, 비즈니스 목표 및 전략과의 연계, 관련 법규와 규정 준수, 적절한 책임의 할당, 사용자 참여 및 문화의 형성, 이해관계자에 대한 고려 등을 기본적으로 갖추어야 함을 알 수 있다.

2.1.2 정보보호 거버넌스 프레임워크

현재 정보보호 거버넌스의 국제 표준으로 개발 중인 ISO/IEC 27014에서는 정보보호 거버넌스의 구성요소를 목표, 원칙, 활동 분야, 구현모델로 제시하고 있으며, 정보보호 거버넌스는 정보보호 관리체계(Information Security Management System)의 보안 활동을 지시, 평가, 모니터링하는 개념으로 설명하고 있다[10]. 즉, 정보보호 거버넌스의 목표는 책임성(Accountability), 비즈니스 연계성(Business Alignment), 준거성(Compliance)으로, 각각의 목표를 달성하기 위한 실행 원칙들이 전략적 연계, 가치전달, 위험관리, 자원관리, 성과측정의 5가지 활동 분야에서 일관되게 적용된다고 할 수 있다.



[그림 1] ISO/IEC 27014의 정보보호 거버넌스 프레임워크

정보보호의 발달과정을 통해 정보보호 거버넌스의 중요성을 제시한 Shaun Posthumus와 Rossouw von Solms의 정보보호 거버넌스 프레임워크는 비즈니스 정보를 잠재적인 위험으로부터 보호하기 위하여 내적 정보보호 요구사항 및 외적 정보보호 요구사항을 충족시키는 동시에 비즈니스 정보 위험을 효과적으로 관리할 수 있는 전략을 거버넌스 측면과 관리 측면에서 수립할 것을 제안하고 있다[19].

한편, ITGI(IT Governance Institute)에서는 효과적이고 포괄적인 정보보호 프로그램을 개발하고 유지하기 위해 최고 경영층으로 하여금 정보보호 거버넌스 프레임워크를 수립할 것을 요구하고 있으며[21], 정보보호 위험관리 방법론, 비즈니스 및 IT와 연계된 포괄적인 정보보호 전략, 효과적인 정보보호 조직 구조 등 8가지 구성요소로 이루어져 있다.

상기에서 설명한 세 가지 프레임워크를 포괄성(Comprehensiveness)과 유용성(Usefulness)을 기준으로 비교해 보았을 때[9], ISO/IEC 27014 정보보호 거버넌스 프레임워크는 앞서 설명한 두 프레임워크가 제시한 사항들을 포함하는 좀 더 포괄적이고 실무 적용이 용이한 프레임워크라 할 수 있겠다. 즉, 정보보호 거버넌스를 내/외부 환경 및 비즈니스 이슈 측면에서 다루고 있으며, 정보보로 활동에 대한 평가, 지시, 모니터링을 통해 정보보호 및 조직의 목표달성을 위한 지속적인 개선을 도모한다고 할 수 있다. 또한, 정보보호 거버넌스의 목표를 구체화함으로써, 정보보호 거버넌스를 수행하기 위해 필요한 이슈가 무엇인지 파악할 수 있으며, 이러한 목표를 달성하기 위해 지켜야할 원칙을 제시함으로써, 최고 경영층 및 이사회가 수행해야할 정보보호 활동을 도출하기 용이하다고 할 수 있다. 따라서 본 논문에서는 ISO/IEC 27014 정보보호 거버넌스 프레임워크를 활용하여 정보보호 거버넌스 구현을 위한 핵심성공요인을 도출하고자 한다.

2.2 핵심성공요인

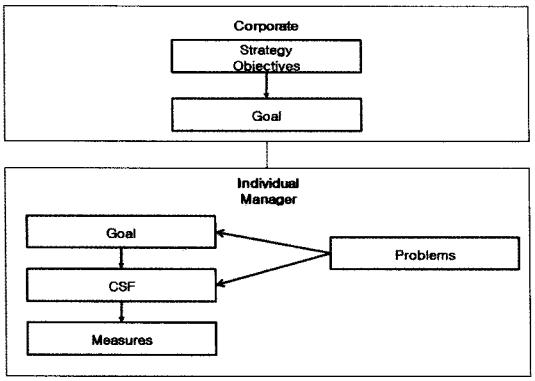
2.2.1 핵심성공요인의 개념

핵심성공요인(Critical Success Factors)이라는 개념은 1961년 D. Ronald Daniel에 의해 처음 소개되었으며, 조직의 목표 달성에 중요한 영향을 미치는 내적 또는 외적 요인으로 널리 사용되고 있다. D. Ronald Daniel에 의하면, 핵심성공요인은 조직의 목표를 달성하기 위한 최고 경영층의 의사결정을 지원하는 정보로서, 핵심성공요인을 통하여 조직의 목표를 효과적으로 달성할 수 있다고 한다. 또한, John F. Rockart는 핵심성공요인을 목표를 달성하기 위해 절대적으로 필요한 핵심 활동 영역으로 정의 내리고 있으며[7], 특히 Critical 이라는 단어는 조직의 목표달성을 위해 필수적인 것으로 이를 간과할 시 목표달성을 현실화 시킬 수 없다는 의미로 사용되고 있다.

D. Ronald Daniel과 John F. Rockart의 핵심성공요인에 대한 이론을 비교해보면, D. Ronald Daniel는 핵심성공요인을 단순히 최고 경영층이 효율적이고 효과적인 의사결정을 내릴 수 있게 도와주는 역할을 한다고 하였다. 반면, John F. Rockart의 이론은 이 보다 좀 더 범위를 넓혀 핵심성공요인을 조직의 IT 기술 및 비즈니스와 관련된 전략계획에 활용할 수 있음을 제시하였고, 현재 John F. Rockart의 이론처럼 핵심성공요인은 조직의 목표를 달성하기 위해 전략적인 차원에서 많이 사용되고 있다.

아래의 [그림 2]는 John F. Rockart와 Christine V. Bullen가 제시한 계층적 구조로, 조직의 미션이나 전략으로부터 목표가 도출되며 이러한 목표를 달성하는 데에는 다양한 문제들이 있으며 핵심성공요인을 통해 목표달성을 위한 핵심 활동을 식별하여 문제를 해결하며, 이를 평가하여 목표의 달성여부를 측정할

수 있다. 즉, 핵심성공요인은 아주 모호하고 구체적이지 않은 목표들로부터 시작하여, 매우 구체적이며 측정 가능한 것으로 이루어지는 하향식 접근법 또는 계층적 구조를 통하여 사용될 수 있다. 또한, 이러한 핵심성공요인을 도출하기 위한 계층적 구조는 확정적인 것이 아니며, 조직의 외적, 내적 환경에 따라 다양할 수 있다.



[그림 2] 핵심성공요인과 목표의 계층적 관계

2.2.2 정보보호 거버넌스와 핵심성공요인

정보보호 거버넌스는 이사회나 최고 경영층의 정보보호에 대한 방향제시와 통제 역할을 강조하는 개념이다[18]. 즉, 이사회나 최고 경영층은 전사적 정보보호 정책 및 계획을 수립함으로써 정보보호에 대한 책임과 의지를 보여주고, 조직의 임무, 목표, 전사적 정보보호 전략 수행을 지원해야 한다. 이러한 이사회와 최고 경영층의 노력은 정보보호와 경영 전략 및 조직 목표를 연계함으로써 정보보호 투자 효율성 확보에 따른 가치 창출을 가능하게 하며, 정보보호 위험과 업무에 미치는 영향을 수용 가능한 수준으로 감소시키게 된다. 이것은 정보보호의 목표를 달성하기 위해서는 정보보호 거버넌스를 고려해야 한다는 의미이다.

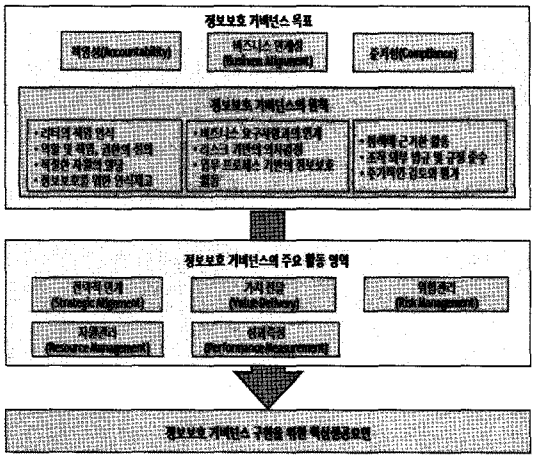
하지만, 이러한 기대효과에도 불구하고 지금까지 수행된 정보보호 거버넌스에 대한 연구는 구체적으로 최고 경영층이 어떠한 방법으로 정보보호에 참여할 것인지에 대한 실질적인 활동을 명시하지 못하여 현실상 실무에 적용하기 어려운 수준이다. 따라서 정보보호 거버넌스를 구현하기 위해서는 핵심성공요인을 도출하여, 우선적으로 최고 경영층 및 이사회가 정보보호 활동에 참여하기 위해 필요한 핵심적인 활동들을 명시할 필요가 있다. 즉, 최고 경영층 및 이사회는 자신들이 수행해야할 정보보호 활동들을 인식하고, 시간 및 자원의 낭비 없이 이에 집중할 수 있을 것이다.

Paul Williams는 이사회 및 최고 경영진의 관점에서 정보보호 거버넌스의 핵심성공요인을 제시하였지만[14], 일부 기존의 정보보호 관리 수준에서의 요인들이 존재하며, 정보보호 거버넌스 목표와의 연계성에 대한 설명이 부족하다고 할 수 있다. 따라서 다음 장에서는 ISO/IEC 27014의 정보보호 거버넌스 프레임워크에 핵심성요인과 목표의 계층적 관계를 고려하여 정보보호 거버넌스 구현을 위한 핵심성공요인을 도출하도록 하겠다.

3. 정보보호 거버넌스 구현을 위한 핵심성공요인 도출

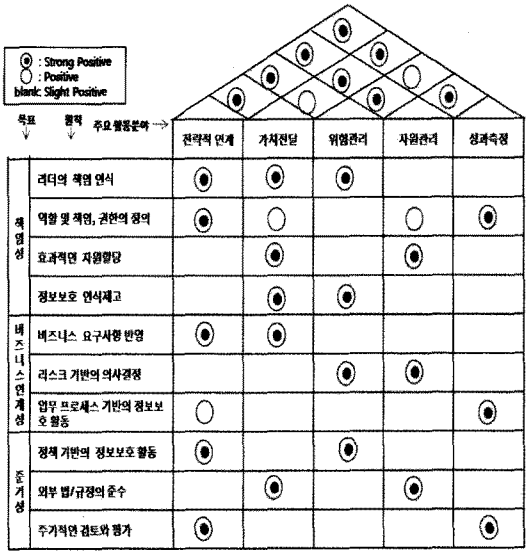
3.1 핵심성공요인 도출 방법

핵심성공요인을 도출하기 위해서는 성공 사례를 조사하여 성공요인을 도출하는 것이 일반적인 방법이지만 정보보호 거버넌스의 경우, 아직 실무 도입이 초기 단계이며 인식수준이 낮기 때문에 일반적인 접근이 불가능하다. 따라서 아래의 그림과 같이 ISO/IEC 27014에서 제시한 정보보호 거버넌스의 목표 및 원칙과 주요 활동 분야에 기반하여 핵심성공요인을 도출하기 위한 모델을 수립하였다.



[그림 3] 정보보호 거버넌스 구현을 위한 핵심성공요인 도출 모델

[그림 3]의 의미를 살펴보면, 정보보호 거버넌스의 목표가 달성되기 위해서는 목표에서부터 도출된 10가지 원칙이 지켜져야 하며, 정보보호 거버넌스의 구현을 위한 핵심성공요인을 도출하기 위해서는 정보보호 거버넌스의 10가지 원칙이 정보보호 거버넌스의 5가지 주요 활동 분야에 투영되어 구체적인 활동 기반의 요인들이 도출되어야 한다는 것이다. 또한, 정보보호 거버넌스의 원칙을 주요 활동분야에 상호 관련성을 고려하여 적용시키기 위해 HOQ(House of Quality)를 이용하였다. HOQ는 소비자의 요구사항과 기술적 반응, 상호관련성, 기술적 상관관계 등을 고려하여 우선순위를 부여하는 방법론이다[13]. 즉, [그림 4]와 같이, 소비자의 요구사항을 대신하여 정보보호 거버넌스의 목표를 달성하기 위해 요구되어지는 10 가지 원칙을 적용하였으며, 기술적 반응을 대신하여 10 가지 원칙이 적용될 수 있고, 이 때 사용될 수 있는 방법론을 제시하는 5 가지 주요 활동분야를 적용하여 정보보호 거버넌스 구현을 위한 핵심성공요인을 도출하였다. 또한, 주요 활동분야 간의 상호 관련성을 파악하여, 관련성이 매우 높은 분야를 ◉ 기호로, 어느 정도 관련성 존재하는 분야를 ○ 기호로 표시하였다. 마찬가지로 정보보호 거버넌스의 10 가지 원칙과 5 가지 주요 활동분야 간의 상호 관련성을 고려하여 구체적인 활동이나 방법론을 도출할 수 있을 경우 ◉ 기호로, 구체적이지는 않지만 관련된 활동 및 방법론을 제시할 수 있을 경우 ○ 기호로 표시하였으며, 이때 정보보호 거버넌스의 원칙이 관련성이 높은 활동분야에 적용되었을 경우, 정보보호 거버넌스 구현을 위한 구체적인 활동들이 도출된다고 할 수 있다.



[그림 4] 정보보호 거버넌스 원칙과 주요 활동분야의 상호 관련성

우선, 주요 활동분야 간의 상호 관련성을 살펴보면, 전략적 연계의 경우 다른 주요활동 분야와 매우 밀접한 관계가 있다고 할 수 있다. 즉, 비즈니스와 정보보호를 연계하기 위해서는 우선 정보보호가 어떠한 가치를 창출할 수 있는지 인식하는 것이 중요하며, 조직의 내/외부 위험을 어느 정도의 자원을 사용하여 감소시킬 수 있고, 이러한 정보보호 활동이 비즈니스 성과에 어느 정도 기여하였는지 측정하는 것이 중요하다. 가치 전달의 경우, 정보보호 투자 의사결정 시 가용한 자원이 어느 정도 인지 파악하는 것이 중요하며, 이는 곧 정보보호의 투자 성과에 직결된다고 할 수 있다. 위험관리의 경우, 조직의 위험허용한도 내에서 업무 수행이 이루어지고 있는지 측정하는 것이 중요하며, 정

보보호 투자 의사결정 시 기술적 측면뿐만 아니라, 비즈니스 위험을 고려하여야 하며, 적절한 위험관리 활동을 위해서는 효과적으로 자원할당되어야 한다. 성과측정의 경우, 어느 정도의 정보보호 자산을 사용하여 어느 정도의 성과를 이루었는지 평가하는 것이 중요하다고 할 수 있으며, 이는 곧 정보보호 투자 성과와 직결된다고 할 수 있다.

따라서 정보보호 거버넌스의 5 가지 주요 활동분야들은 서로간의 높은 관련성을 지니며, 하나의 원칙을 달성하기 위해 다수의 활동분야가 동시에 고려되어질 수 있다. 그리고 이러한 주요 활동분야에서 수행되는 활동 및 사용가능한 방법론들을 통하여 정보보호 거버넌스의 원칙을 달성할 수 있는 구체적인 활동들을 도출할 수 있다.

3.2 정보보호 거버넌스 구현을 위한 핵심 성공요인

본 논문에서는 정보보호 거버넌스의 원칙을 주요 활동분야에 적용시키기 위해 기존의 정보보호 거버넌스 관련 선행연구를 참고하여 그 관련성을 판단하였다. 또한, ISO/IEC 27014 정보보호 거버넌스 프레임워크의 주요 활동분야에 대한 설명을 참고하여 최고 경영층 및 이사회가 수행해야할 구체적인 활동을 도출하여, 이를 핵심성공요인으로 표현하였다. 아래의 <표 1>은 정보보호 거버넌스의 원칙과 도출된 핵심성공요인을 정리한 내용이다.

또한, 본 논문에서 제시하고자 하는 정보보호 거버넌스 구현을 위한 핵심성공요인과 관련된 구체적인 활동들은 다음과 같다.

- 정보보호를 비즈니스 이슈로 인식전환: 조직의 정보보호 관련 위험이 기술적인 이슈가 아닌 비즈니스 이슈임을 인식하여 비즈니스 전략 수립 시 정보보호가 논의되도록 하고, 적절한 투자가 이루어지도록 한다.
- 정보보호 주요 의사결정 유형에 따라 권한 및 책임을 명확히 정의: 정보보호 투자 및 아웃소싱과 같은 정보보호 관련 중요 의사결정 시 실행 증적이 확보될 수 있도록 책임을 명확히 정의하고 적절한 권한 및 역할을 할당한다.
- 준수여부의 지속적인 모니터링 및 경영성과 관리체계에 반영: 정보보호 정책 및 외부 법/규정에 대한 준수여부를 지속적으로 모니터링할 수 있도록 보고체계를 수립하고, 준수여부를 경영 성과관리체계에 반영하여 포상 및 처벌한다.
- 정보보호 거버넌스 반영을 위한 규정체계 재구성: 기존의 규정체계를 재구성하여 정보보호 정책에 정보보호 거버넌스를 반영하고, 전사적인 차원에서의 준수여부를 확인을 위
  해 감사위원회를 설립한다.
- 비즈니스 전략 및 계획 수립 시 정보보호 반영: 정보보호 프로세스와 자산계획 및 투

〈표 1〉 정보보호 거버넌스의 원칙과 핵심성공요인

정보보호 거버넌스의 원칙	정보보호 거버넌스 구현을 위한 핵심성공요인
리더의 책임 인식	정보보호를 비즈니스 이슈로 인식전환
역할 및 책임, 권한의 정의	정보보호 주요 의사결정 유형에 따라 권한 및 책임을 명확히 정의
효과적인 자원할당	정보보호 투자 최적화를 위한 자원의 할당 승인
정보보호를 위한 인식제고	조직의 위험성향을 고려한 정보보호 문화형성
비즈니스 요구사항 반영	비즈니스 전략 및 계획 수립 시 정보보호 반영
리스크 기반 의사결정	정보자산을 포함하는 비즈니스 단위로 위험을 고려
업무 프로세스 기반 정보보호 활동	비즈니스 측면에서의 정보보호 성과평가
정책 기반의 정보보호 활동	정보보호 거버넌스 반영을 위한 규정체계 재구성
외부 법/규정의 준수	효율적인 규제준수를 위한 준수관리체계 수립
주기적인 검토와 평가	준수여부의 지속적인 모니터링 및 경영성과관리체계에 반영

자 프로세스를 통합하여 비즈니스 전략 및 계획 수립 시 반영한다.

- 효율적인 규제준수를 위한 준수관리체계 수립: 정보보호 정책 및 외부 법/규정 준수를 위한 충분한 자원이 할당되었는지 평가하고, 중복투자를 방지하기 위한 준수관리체계를 수립한다.
- 정보자산을 포함하는 비즈니스 단위로 위험을 고려: 위험분석 및 평가, 위험관리 전략 수립 등 위험관리 활동의 실행 시 정보자산에 존재하는 위험이 아닌 정보자산을 활용하여 업무를 수행하는 비즈니스에 존재하는 위험을 고려할 수 있는 방안을 수립 및 실행하도록 한다.
- 조직의 위험성향을 고려한 정보보호 문화형성: 정보보호 관련 국제 표준 및 Best Practices에서 제시하는 적절한 위험관리 방법론을 선택하여 조직의 위험성향에 적합하고 위험허용수준 내에서 업무를 수행하도록 문화를 형성한다.
- 비즈니스 측면에서의 정보보호 성과평가: 비즈니스 전략 달성 시 정보보호의 기여도를 측정할 수 있도록 BSC 등 비즈니스 성과평가 기법을 활용한다.
- 정보보호 투자 최적화를 위한 자원의 할당 승인: ROSI를 이용한 정확한 정보보호 투자 수익률 계산을 통해 정보보호 자산이 효율적으로 할당되도록 한다.

4. 실증분석

4.1 분석방법

본 논문에서는 정보보호 거버넌스 및 핵심성공요인에 대한 기존 연구를 기반으로 정보보호 거버넌스 구현을 위한 핵심성공요인을 도출하였고, 도출된 핵심성공요인의 타당성을 검증하기 위해 포커스 그룹인터뷰 방법을 채택하였다. 왜냐하면, 현재 국내에 정보보호 거버넌스를 구현한 조직의 사례가 드물기 때문에 도출된 핵심성공요인이 반영되었을 때 실제로 정보보호 거버넌스 구현에 어떠한 영향을 주는지 객관적으로 파악하기 어렵기 때문이다. 따라서 본 논문에서는 학계 및 연구소, 정보보호 분야의 전문가로 구성된 포커스 그룹을 구성하여 심층면접을 수행하였으며, 상호의견을 수렴하였다.

연구단계는 차례로 기존 연구에서 핵심성공요인을 도출, 측정 항목 선정, 포커스 그룹인터뷰 수행, 핵심성공요인의 타당성 검증, 자료 분석의 순서로 진행하였다. 정보보호 거버넌스에 대한 기존 연구들은 아직 초기 단계이기 때문에 일관성이나 체계성을 찾기가 쉽지 않아 본 논문에서는 정보보호 거버넌스 구현을 위한 핵심성공요인을 평가하기 위해, 경영정보학 분야에서 사용되는 평가 기준 및 우선순위 결정 방법을 참고하였다[6][8][20]. 핵심성공요인이란 결국 조직의 목표달성을 위해 필요한 요인들 중 가장 우선순위가 높은 요인이기 때문에 본 논문에서 도출된 정보보호 거버넌스 구현을 위한 핵심성공요인의 타당성을 평가하기에 적합하다고 판단하였다.

본 논문에서는 중요성(Importance)과 실현가능성(Feasibility)을 검증 항목으로 사용하여 중요성과 실현가능성이 높은 요인을 핵심성공요인으로 결정하였다. 또한, 중요성이 높은 반면 실현가능성이 낮은 경우, 중요성이 낮은 반면 실현가능성이 높은 경우에는 포커스 그룹의 의견을 수렴하여 채택 및 기각 여부를 판단하였다. 한편, 이러한 항목들은 각각 다른 분야에서 적용되었기 때문에 본 논문에 적용하기 위해서는 항목에 대한 조작적 정의가 필요하며, 아래의 <표 2>와 같다.

〈표 2〉 검증 항목의 도출

항목	조작적 정의	측정	출처
중요성	정보보호 거버넌스 구현시 도출된 핵심성공요인의 중요성 여부	책임성 관련 핵심성공요인의 중요성 비즈니스 연계성 관련 핵심성공요인의 중요성 준거성 관련 핵심성공요인의 중요성	[6] [8] [20]
실현 가능성	도출된 핵심성공요인이 실제로 수행 가능한지의 여부	책임성 관련 핵심성공요인의 실무적용 가능성 비즈니스 연계성 관련 핵심성공요인의 실무적용 가능성 준거성 관련 핵심성공요인의 실무적용 가능성	[6] [8] [20]

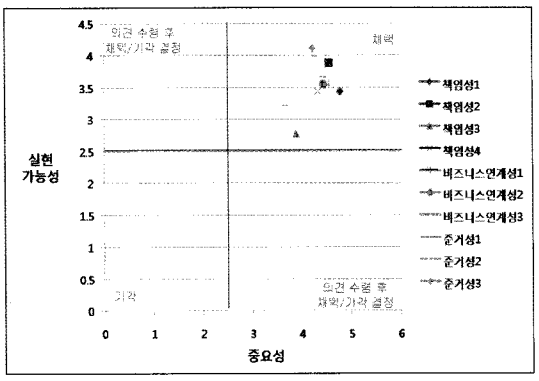
또한 본 논문에서는 대표적인 정성적 연구방법 중의 하나인 포커스 그룹 인터뷰(FGI: Focus Group Interview)를 사용하였다. 왜냐하면, 정량적 연구의 목적은 연구결과의 일반화에 있지만, 정성적 연구는 연구주제에 대한 인터뷰 참여자의 이해와 통찰을 얻는데 목적이 있으므로, 현재 국내의 정보보호 거버넌스에 대한 인식 수준이 낮은 상태에서 정량적 연구를 수행하였을 경우 일반화가 어렵고, 깊이 있는 결과를 도출하기 힘들다고 판단하였기 때문이다.

포커스 그룹 인터뷰는 주제와 관련하여 공통된 특성을 가지고 있는 구성원들의 상호작용을 통하여 연구자가 정한 주제에 대한 자료를 수집하는 연구방법으로, 연구자가 특수한 목적을 가지고 면담을 진행하여 단기간에 참여자들로부터 주제에 초점을 맞추어 많은 양의 집중적인 대화를 유도해내는 것이며 그룹 내의 상호작용을 통해 그들의 경험, 감정 및 신념을 이끌어낼 수 있는 유용한 방법이다[1]. 특히 포커스 그룹인터뷰는 어떤 현상에 대한 생각이나 감정의 범위를 알아보고자 할 때, 집단 간의 시각 차이를 파악할 때, 의견, 행동, 동기에 영향을 미치는 요인들을 조사할 때, 아이디어, 소재, 계획, 또는 정책을 미리 시험해보고자 할 때, 대규모 설문조사를 하기 전 내용을 파악하고자 할 때, 이미 정량적 연구방법으로 얻어진 연구결과를 뒷받침할 때 사용된다는 점에서 탐색적 연구를 수행하기에 적합한 방법론이라고 할 수 있다[12].

포커스 그룹 인터뷰를 수행하기 위해 연구소 및 정보보호 분야의 전문가가 참여한 포커스 그룹을 구성하여 설문지 작성과 심층면접을 동시에 수행하였다. 우선, 설문지는 도출된 핵심성공요인의 중요성과 실현가능성을 측정하기 위해 리커드 5점 척도를 사용하였으며, 도출된 핵심성공요인 이외에 추가적으로 필요한 요인이나 개선사항에 대하여 작성하도록 하였다. 그리고 설문이 끝난 후 30분에 걸쳐 참여자들 간 의견을 교류하고, 연구자의 주도하에 도출된 핵심성공요인이 중요한 이유를 토론하고, 실무에 적용이 어려운 요인에 대해서는 그 이유를 규명하기 위해 대화 형식으로 토론을 이끌었다.

4.2 분석결과

포커스 그룹 인터뷰의 결과를 종합해보면, 정보보호 거버넌스 구현을 위한 10 가지 핵심성공요인이 모두 필수적으로 고려해야 할 사항으로 도출 되었다. 또한, 중요성과 실현가능성 측면에서 핵심성공요인에 대한 전문가의 의견과 중요성이 높은 반면 실현가능성이 낮은 경우, 혹은 중요성이 낮은 반면 실현가능성이 높은 경우, 이에 대한 개선사항을 분석하였다.



[그림 5] 핵심성공요인의 분포

〈표 3〉 핵심성공요인의 우선순위

핵심성공요인	중요도	실현가능성	구분
정보보호를 비즈니스 이슈로 인식전환	4.78	3.44	책임성1
정보보호 주요 의사결정 유형에 따라 권한 및 책임을 명확히 정의	4.56	3.89	책임성2
준수여부의 지속적인 모니터링 및 경영성과관리체계에 반영	4.22	4.11	준거성3
정보보호 거버넌스 반영을 위한 규정체계 재구성	4.22	4.00	준거성1
비즈니스 전략 및 계획 수립 시 정보보호 반영	4.56	3.56	비즈니스 연계성1
효율적인 규제준수를 위한 준수관리체계 수립	4.44	3.67	준거성2
정보자산을 포함하는 비즈니스 단위로 위험을 고려	4.44	3.56	비즈니스 연계성2
조직의 위험성향을 고려한 정보보호 문화형성	4.33	3.44	책임성4
비즈니스 측면에서의 정보보호 성과 평가	3.67	3.22	비즈니스 연계성3
정보보호 투자 최적화를 통한 자원의 할당	3.89	2.78	책임성3

본 논문에서 제시한 핵심성공요인은 중요성에 대해서는 어느 정도 높게 측정된 반면, 몇몇 핵심성공요인들은 실무에 직접 반영하기 어려운 것으로 나타났다. 즉, 비즈니스 연계성 관련 핵심성공요인의 경우, 정보보호가 비즈니스에 어떠한 가치를 제공하는지 정량적으로 측정 가능한 지표 없이는 정보보호와 비즈니스를 연계하기 힘든 것으로 나타났다. 또한 준거성 관련 핵심성공요인의 경우, 준수여부의 지속적인 평가 및 모니터링과 효율적인 준수관리체계를 수립하고 운영하기 위한 평가 지표 없이는 기존의 정보보호 관리 차원에서의 문제점을 해결하기 힘든 것으로 나타났다. 따라서 본 논문에서 제시한 핵심성공요인을 적용하여 성공적으로 정보보호 거버넌스를 구현하기 위해서는 다음과 같은 연구가 추가적으로 수행되어야 할 것이다.

- 정보보호 가치의 측정을 위한 지표 개발: 정보보호 투자 정당성 및 비즈니스 기여도를 측정하기 위한 지표에 관한 연구가 필요함
- 정보보호 관련 법/규정의 준수 여부를 측정하기 위한 지표 개발: 효율적인 준수관리체계를 수립하고 준수여부를 경영성과체계에 반영하기 위한 지표에 관한 연구가 필요함

5. 결론

본 논문에서는 정보보호 거버넌스의 개념을 보다 구체화하기 위해 정보보호 거버넌스를 구현하기 위한 최고 경영층 및 이사회의 필수적인 활동을 핵심성공요인으로서 도출하였다. 즉, 정보보호 거버넌스는 도출된 핵심성공요인에 초점을 두어 최고 경영층 및 이사회가 적절한 정보보호 활동을 수행하였을 때 비로소 성공적으로 구현될 수 있다는 의미이다. 또한 본 논문에서 도출한 정보보호 거버넌스 구현을 위한 핵심성공요인은 ISO/IEC 27014 Information Security Governance Framework를 기반으로 작성되었으며, 정성적 분석방법인 포커스 그룹 인터뷰를 사용하여 중요성 및 실현가능성 측면에서 타당성을 검증하였고, 우선순위를 결정하였다.

한편, 본 연구의 한계는 정성적 분석방법에 의존하여 도출된 핵심성공요인의 객관성 확보 및 일반화가 어렵다는 것이다. 즉, 학계, 연구소, 정보보호 분야의전문가의 의견을 수렴하는 데 초점을 두어 실질적으로 정보보호 거버넌스를 구현해야 하는 실무의 의견을 반영하지 못하였다. 또한, 본 논문에서 제안한 핵심성공요인은 이론을 기반으로 작성되었기 때문에 전문가의 의견을 수렴하였더라도 실무차원에서는 그 중요성 및 적용 가능성이 상이할 수 있다. 따라서 향후에는 국내 정보보호 전문가뿐만 아니라 최고경영층 및 이사회를 대상으로 정량적 분석을 실시할 필요가 있으며, 현실과 이론사이의 차이를 규명할 필요가 있다.

끝으로 본 논문에서 제시한 정보보호 거버넌스 구현을 위한 핵심성공요인을 실무에 적용하기 위해서는 비즈니스에 대한 정보보호의 기여

도 및 정보보호 투자 정당성을 확보하기 위한 평가 지표, 정보보호 활동 및 법/규정의 준수 여부를 지속적으로 평가, 모니터링하여 경영성과체계에 반영할 수 있는 지표에 대한 연구가 추가적으로 이루어져야 할 것이다.

참 고 문 헌

[1] 김성재 외 4명역(Morgan, D.L. 저, 2007). 질적 연구로서의 포커스 그룹. 군자출판사.

[2] 한국정보사회진흥원 (2008). 국가 정보화 백서.

[3] 한국정보보호진흥원 (2008). 정보보호 실태조사.

[4] Basie von Solms, Rossouw von Solms. (2004). The 10 Deadly Sins of Information Security Management. Computers & Security. Vol.23 pp.371-376.

[5] Basie von Solms. (2006). Information Security: The Fourth Wave. Computers and Science. Vol.25 pp.165-168.

[6] Bogie Ozdemir, Peter Miu. (2009). Basel II Implementation: A Guide to Developing and Validating a Compliant, Internal Risk Rating System. McGRAW-HILL.

[7] Christine V. Bullen, John F. Rockart. (1981). A Primer on Critiacl Success Factors. Center for Information Systems Research No.69 pp.16-19.

[8] Derek Cabrera, James T. Mandel, Jason P. Andras, Marie L. Nydam. (2008). What is the crisis? Defining and prioritizing the world's most pressing problems. Front Ecol Environ pp.469 - 475.

[9] Douglas R. Vogel, James C. Wetherbe. (1984). MIS Research: A Profile of Leading Journals and Universities. DATA BASE.

[10] ISO/IEC 27014: Information Security Governance Framework. 1st WD. (2008).

[11] Jungduk Kim, Seongil Lee. (2008). A Framework of Business Security Governance. Joint Workshop on Information Security.

[12] Krueger, R. & Casey. (2000). M. Focus Groups: A Practical Guide for Applied Research. Thousand Oak, CA: Sage Publications, Inc. 2000.

[13] Lou Cohen. (1995). Quailty Function Deployment: How to Make QFD Work for You. Engineering Process Improvement Series.

[14] Paul Williams. (2001). Information Security Governance. Information Security Technical Report, Vol.6 No.3 60-70.

[15] Pauline Bowen, Joan Hash, Mark Wilson. (2006). Information Security Handbook: A Guide for Managers. NIST Special Publication 800-100.

[16] Rolf Moulton, Robert S. Coles. (2006). Applying Information Security Governance. Computers & Security Vol.22 No.7 pp.580-584.

[17] Rossouw von Solms, Basie von Solms. (2004). From Policies to Culture. Computers & Security. Vol.23 pp.275-279.

[18] Rossouw von Solms, S.H. (Basie) von Solms. (2005). Information Security Governance: A model based on the Direct - Control Cycle. Computers and Security Vol.25 pp.408-412.

[19] Shaun Posthumus, Rossouw von Solms. (2004). A framework for the governance of information security. Computers and Security. Vol.23 pp.638-646.

[20] Sork, T. J. (1982). Determining Priorities. Vancouver, Canada, University of British Columbia.

[21] W. Krag Brotby et. al. (2006). Information Security Governance Guidance for Boards of Directors and Executive Management 2nd Edition. IT Governance Institute.

김 건 우

중앙대학교 정보시스템학과
(학사)
중앙대학교 정보시스템학과
(석사과정)
관심분야: 정보보호 관리, 정보보호 거버넌스, 시스템 감사

김 정 덕

연세대학교 정치외교학과
(학사)
연세대학교 경제학과대학원
(석사)
University of S. Carolina, MBA
Texas A&M University, Ph.D. in MIS
전 한국전산원, 선임연구원
현재: 중앙대학교, 교수
관심분야: 정보보호 거버넌스, 정보보호 관리, IT 감사, 정보시스템의 전략적 응용 등