http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.20, No.2, May 2015, pp.167-174
http://dx.doi.org/10.7838/jsebs.2015.20.2.167

# 정보보호 전담조직 편성모델에 관한 연구

## A Study on Information Security Departmentalization Model

강현식(Hyunsik Kang)*, 김정덕(Jungduk Kim)**

### 초 록

정보보호 전담조직은 IT 부서 산하에 편성되어있는 것이 일반적이었으나 정보보호의 중요성이 증대됨에 따라 전사적 보안을 위한 정보보호 전담조직의 편성이 중요한 이슈로 대두되고 있다. 국내 금융권에서도 전자금융거래법 개정안을 통해 CIO와 CISO를 분리하는 등 정보보호 전담조직의 분리에 대한 필요성이 증대되고 있다. 하지만 현재 정보보호 전담조직 하부구조에 대한 연구는 활발히 진행되고 있으나 편성방법에 대한 연구는 미흡하다. 따라서 본 논문에서는 효과적인 정보보호 전담조직의 편성을 위해, 상황적 접근방법을 통하여 기업의 비즈니스 위험도와 IT 의존도를 기준으로 정보보호 전담조직 편성모델을 제시하였다. 또한 정보보호 전담조직이 소속될 부서를 기획・조정 부서, 내부통제 부서, 내부관리 부서, IT 부서로 분류하고 각 부서에 편제되어있을 경우의 장단점을 분석하였다.

### ABSTRACT

Information security organization has normally been organized under the IT department. However, as the importance of information security has gradually increased, the way of information security organized for enterprise security management has become a noteworthy issue. The need for separation of Information security organization from IT department is growing, such as restriction on the concurrent positions in CIO and CISO. Nowadays there are many studies about Information security organization while relatively there has been minimal research regarding a departmentalization. For these reasons this study proposes a Information Security Departmentalization Model which is based on business risk and reliance on the IT for effectively organizing Information security organization, using Contingency theory. In addition, this study classified the position of Information security organization into Planning & Coordination, Internal Control, Management and IT and analyze the strengths and weaknesses of each case.

**키워드** : 정보보호 패러다임, 정보보호 전담조직, 조직 편성, 상황적 조직이론, 정보보호 기능
Information Security Paradigms, Information Security organization, Departmentalization, Contingency theory, Function of Information Security

---

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2015-H8501-15-1018).

* First Author, Dept. of Security Convergence, ChungAng University(hskang8911@gmail.com)
** Corresponding Author, Dept. of Industrial Security, ChungAng University(jdkimsac@cau.ac.kr)

Received: 2015-05-15, Review completed: 2015-05-21, Accepted: 2015-05-26

# 1. 서 론

전통적으로 정보보호 활동은 정보시스템 등 IT 인프라를 기반으로 수행되었기 때문에 일반적으로 정보보호 전담조직은 IT 부서 산하에 편성되는 경향이 있었다[6]. 그러나 현재 정보보호 전담조직은 IT 부서와 분리되는 현상을 보이고 있다[1]. 국내 금융권에서도 CISO의 임원 지정, 겸직 금지 등 전자금융거래법 개정안을 통해 정보보호 전담조직의 위상을 강화하고 IT 부서와의 분리를 요구하고 있다.

정보보호 전담조직과 IT 부서가 분리되는 현상의 이유는 다음과 같다. 첫째, 정보보호와 관련된 위험이 확장됨에 따라 정보보호의 중요성이 점차 증대되고 있다. 즉, 과거 정보보호 위험은 IT 영역에 국한되어 있었으나 기업 전사적으로 영향을 줄 수 있는 위험으로 확장되면서 정보보호를 단순 IT·기술적 문제로 인식하기에는 한계가 존재하며 전사적인 관점에서 정보보호 위험을 최소화하는 것이 필요해졌다. 둘째, 정보보호 전담조직과 IT 부서는 근본적으로 추구하는 목표가 다르기 때문에 갈등이 존재한다. IT 부서는 기업의 경영활동을 위한 IT 기술의 운영 효율성이 주된 목표지만 정보보호 전담조직은 정보의 기밀성, 무결성 및 가용성 보장을 위해 IT 운영을 통제함으로써, 두 조직간 갈등이 발생할 수 있다.

현재 정보보호 전담조직과 IT 부서가 분리되는 현상에 따라, 어느 부서 산하에 정보보호 전담조직을 편성해야 보안성과를 효율적·효과적으로 달성할 수 있는 지에 대한 이슈가 대두되고 있다[1]. 하지만 정보보호 전담조직의 하부구조에 대한 연구는 활발히 진행되고 있으나, 현재 정보보호 전담조직의 편성기준 및 방법에 대한 연구는 미약한 상태이다.

따라서 본 논문은 정보보호 기능 및 상황적 조직이론의 조사·분석을 통하여, 정보보호의 기능 정의 및 범위를 제시하고, 정보보호 기능과 상황적 접근방법에 따라 정보보호 전담조직 편성모델을 제시하였으며, 각 편제 별 장단점을 분석하였다. 본 논문에서 제시하는 정보보호 전담조직 편성모델은 포커스 그룹 인터뷰를 실시하여 상황변수 설정에 대한 적절성, 정보보호 기능에 따른 부서 편성 적합성 및 타당성을 검정하였다.

# 2. 관련 연구

본 장에서는 정보보호 기능 및 상황적 조직이론의 조사·분석을 통하여, 정보보호 기능의 정의 및 범위를 제시하고, 정보보호 기능과 상황적 접근방법에 따르는 정보보호 전담조직 편성모델의 기준을 설정하였다.

## 2.1 정보보호 기능

정보보호란 정보와 관련된 기업의 모든 자산을 보호하기 위하여 정보에 대한 기밀성, 무결성, 가용성을 보장하는 활동을 말한다[12]. 기업의 정보는 정보시스템 등 IT 자산을 기반으로 수집, 저장, 송·수신되었기 때문에 전통적으로 정보보호 전담조직은 IT 부서 산하에 편성되어서 IT 운영지원을 중점으로 정보보호 활동을 수행하였다. 하지만 정보보호의 중요성이 증대되고 정보보호 패러다임이 변화됨에 따라 정보보호 전담조직이 수행해야 할 책임의 범위가 넓어지게 되었다[8]. 이에 따라 정보

보호 기능도 단순 IT 영역에서의 운영 지원뿐만 아니라 비즈니스 전략 지원, 통제 및 내부관리 등으로 확장되었다[7].

정보보호의 비즈니스 전략 지원 기능은 정보보호를 전사적인 관점에서 비즈니스 프로세스를 보호 및 강화, 지원하고자 하는 정보보호 기능이다[11]. 최고경영층 지원, 전사적 협업체계 및 위험관리의 구축 등이 포함되며 이러한 과정을 통해서 비즈니스 위험에 대해 빠르게 대응하고, 비즈니스 측면에서의 보안성과를 극대화할 수 있는 전략을 설계하고 구축하는 것이 비즈니스 전략 지원 기능의 주된 목표이다.

통제는 정보보호의 가장 기본적인 기능으로, 기업의 정보보호 위험을 최소화하기 위해 기업의 인원, 자산 및 프로세스를 통제하는 역할을 수행한다[3]. 정보보호 위험관리, 보안감사, 내부통제, 규제 대응, 모니터링 등이 포함되며, 이러한 활동을 통해 정보보호 위험요소를 식별하고 조치 및 지속적으로 개선하는 것이 통제 기능의 주된 목표이다.

정보보호의 내부관리 기능은 인사・총무 등 전반적인 기업의 경영활동을 위한 지원을 의미하며, 이와 관련된 정보보호 기능으로 인원관리, 물리 보안 등이 포함된다. 이러한 정보보호 활동을 통해서, 관리적 보안업무를 지원하는 것이 내부관리 기능의 주된 목표라고 할 수 있다.

정보보호의 IT 운영지원 기능은 정보시스템, 서버, 네트워크 등 IT 자산을 보호하기 위해 수행하는 정보보호 기능으로 운영관리, 전산장비 관리, 시스템 도입・개발・유지보수 관리 등과 관련된 위험을 최소화하는 것이 IT 운영지원 기능의 주된 목표이다[10].

정보보호 전담조직이 모든 정보보호 활동을 완벽하게 수행하는 것이 가장 좋으나 비용 대비 성과측면에서 비효율적이기 때문에, 기업은 어떠한 정보보호 기능을 우선할 것인지에 대한 결정이 필요하다. 때문에 기업은 경영활동에 미치는 정보보호의 영향, 기업의 IT 의존도 등, 기업이 직면한 상황을 고려하여 정보보호 기능의 우선순위를 설정하고 이에 따른 정보보호 전략을 수립할 필요가 있다. 일반적으로 전략 수립의 방향은 조직구조 설계에 영향을 주며[13], Gartner[9]의 설문조사 결과를 살펴보면, 실제 정보보호 전담조직은 기업이 설정한 정보보호 전략 방향에 따라 기획・조정 부서, 경영지원 부서, 내부통제 부서, IT 부서 등에 편성되어있는 것으로 분석되었다.

## 2.2 상황적 조직이론

상황적 조직이론이란 모든 상황에 적합한 최적의 조직구조는 존재하지 않으며, 조직구조 및 설계는 조직이 직면한 상황에 따라 다르다는 이론이다[2, 17]. 조직구조는 상황변수에 의해 영향을 받으며 상황변수와 조직구조가 적합할 때, 최종적으로 조직의 효율성이 높아질 수 있다[8]. 상황변수란 조직을 둘러싼 상황의 특성을 나타내는 변수로서 조직구조에 영향을 미치는 결정요소이며 일반적으로 환경, 기술, 조직의 규모를 상황변수로 설정한다.

환경은 조직성과에 영향을 줄 수 있는 외부요소이며, 환경적인 불확실성이 조직구조에 영향을 준다. 환경적인 불확실성은 조직 효과성에 위협요소가 될 수 있기 때문에 환경적인 불확실성을 최소화 할 수 있는, 즉 환경에 적합한 조직구조를 설계하는 것이 필요하다[18]. 기술이란 조직이 투입물을 산출물로 전환시키는

방법을 말하며 투입물을 조직이 원하는 산출물로 변환시키는데 이용되는 지식, 도구, 활동 등이 기술에 포함된다[2]. Hall[16]의 기술과 조직구조간 관계에 대한 연구에 의하면, 기술이 계급의 강조, 분업 등 조직구조에 영향에 주는 것으로 분석되었다. 조직규모는 일반적으로 종업원의 총수로 정의하며[4]. 조직의 규모에 따라 조직구조에 영향을 미치지만, 앞서 설명한 환경 및 기술에 비하여 상대적으로 미치는 영향이 적다고 할 수 있다. 추가적으로, 조직 편성방법은 조직구조를 구성하는 하나의 영역으로, 조직 편성 시 기업마다 중요시하는 정보보호 기능에 차이가 있기 때문에 상황적 접근방법을 고려할 필요가 있다.

본 논문에서는 일정규모 이상의 기업을 대상으로, 상황적 접근방법에 기반하여 정보보호 전담조직의 편성방법을 결정하기 위해 환경과 기술을 상황변수로 고려하였다. 환경변수는 보안 사고 발생 시 비즈니스에 악영향을 주는 비즈니스 위험도로 설명할 수 있으며, 기술변수는 기업의 경영활동을 위해 정보시스템 등 IT 자산이 활용되는 정도를 의미하며, IT 의존도로 설명할 수 있다.

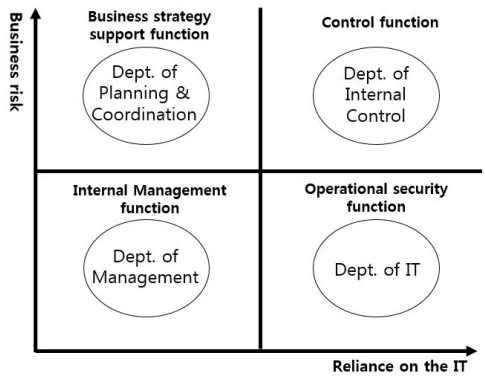
## 3. 정보보호 전담조직 편성

본 장에서는 상황적 접근방법을 통해 정보보호 전담조직의 편성모델을 제시하고, 편제별 장단점을 분석하고자 한다.

### 3.1 정보보호 전담조직 편성모델

정보보호 전담조직의 편성방법이 중요한 이유는 편성방법이 보안성과에 영향을 줄 수 있기 때문이다. Pennings[15]는 조직이 직면한 상황과 조직구조의 적합도가 조직 효과성에 영향을 준다고 주장하였으며, 이러한 관점에서 기업의 상황과 정보보호 조직의 편성방법의 적합도가 보안성과에 영향을 준다고 볼 수 있다.

본 논문에서는 효과적으로 보안성과를 달성하기 위해, 상황적 접근방법을 통한 정보보호 전담조직 편성모델을 제시하였으며 <Figure 1>과 같다. 정보보호 전담조직 편성 모델은 관련 연구를 통해 비즈니스위험도와 IT 의존도로 구성된 상황변수를 기준으로 활용하였으며 상황변수에 따라 우선되어야 할 정보보호 기능을 제시하였다.




〈Figure 1〉 Information Security Departmentalization Model

### 3.2 정보보호 전담조직 편성모델 분석

비즈니스 위험도가 높고 IT 의존도가 낮은 경우, 비즈니스 전략 지원 기능을 우선할 수 있다. 왜냐하면, 빠르게 변화하는 비즈니스 환경에 신속히 대응하고, 발생 가능한 위험을 사전에 조치하기 위해서는 정보보호 기능이 전략 단

계에서부터 고려되어야하기 때문이다. 따라서 비즈니스와의 전략적 연계 및 낮은 IT 의존도를 고려하면, 정보보호 전담조직은 기획·조정 부서 산하에 편성되는 것이 효율적일 것이다. 하지만 기획·조정 부서는 일반적인 운영업무와는 거리가 있기 때문에 IT 보안 운영 및 보안 사고 대응에 한계가 있을 수 있다.

비즈니스 위험도와 IT 의존도가 모두 높을 때에는 통제 기능을 우선할 수 있다. 왜냐하면, 엔론 사태나 최근의 금융 보안 사고에서 알 수 있듯이 IT와 관련된 보안 사고는 비즈니스에 큰 위협으로 작용되며, 내부통제의 관점에서 다루어져야하기 때문이다. 감사 부서, 위험관리 부서 및 준법준수 부서 등이 내부통제 부서에 포함되며[5], 정보보호 전담조직이 내부통제 부서 산하에 편성될 경우, 전사적인 통제활동에 협업이 잘 이루어질 수 있으나, IT 운영 효율성을 목표로 하는 IT 부서와는 심한 이해상충이 발생 할 수 있다.

비즈니스 위험도가 낮고 IT 의존도가 높을 경우, IT 운영 지원 기능을 우선할 수 있다. 왜냐하면 IT 의존도가 높은 경우, 신규 시스템 구축 및 개발 등 빈번한 정보화 사업이 추진되며, IT와 관련된 보안위험에 신속히 대응하기 위해서는 정보보호의 기능을 IT 운영 보안에 초점을 맞출 수 있기 때문이다. 따라서 이러한 경우, 정보보호 전담조직은 IT 부서 산하에 편성될 수 있으며, IT 인프라에 대한 공유가 용이하기 때문에 서버, 네트워크 등 IT와 관련된 보안 업무를 효율적으로 처리할 수 있을 것이다. 반면, 정보보호와 IT의 목표가 상이함에 따라 정보보호 관련 업무의 우선순위가 낮아질 수 있으며, 기술적 측면이 강조되어 비즈니스 요구사항을 반영하기 어려울 수 있다.

비즈니스 위험도와 IT 의존도 모두가 낮을 때에는 정보보호의 내부관리 지원 기능이 우선될 수 있다. 왜냐하면, 기본적인 IT 접근통제 및 인원보안, 물리보안 등 최소한의 정보보호 요구사항을 충족하는 것이 기업 입장에서 효과적일 수 있기 때문이다. 이러한 경우, 정보보호 전담조직은 인사, 총무 등 경영지원 부서 산하에 편성될 수 있으며, 임직원 보안교육 및 출입통제 시스템 운영 등 예방활동을 효율적으로 수행할 수 있으나, 보안 사고 발생 시 전문적인 대응이 어려울 수 있다.

정보보호 전담조직 편성모델은 상황적 접근방법에서 개발되었기 때문에 기업마다 다를 수 있다. 따라서 기업이 직면한 상황에 따라 우선되는 정보보호 기능이 설정되어야 하며, 이에 따라 정보보호 전략이 수립되고 이를 기반으로 정보보호 전담조직 편성이 결정되어야 할 것이다.

## 4. 정보보호 전담조직 편성모델 검정

현재 정보보호 전담조직 편성 관련 선행연구가 많지 않으며, 상황적 접근방법을 기반으로 개발된 편성모델은 일반화가 어렵기 때문에, 본 연구에서는 정보보호 전담조직 편성모델을 검정하기 위하여 포커스 그룹 인터뷰를 실시하였다. 포커스 그룹 인터뷰는 전문가들의 집단 토의, 정보 교환 등의 과정을 통해 설문지보다 훨씬 다양한 범위의 의견들을 수렴할 수 있으며, 문헌연구에서 얻을 수 없는 심층적인 정보를 습득할 수 있다[14].

포커스 그룹은 정보보호 전담조직의 설계 및 편성과 관련이 있는 이해관계자들로 구성

하였으며, 중견기업의 CEO 2명 및 대기업, 회계법인, IT 기업 등의 CIO 3명, CISO 8명 및 정보보호 분야의 교수 2명으로 총 15명의 전문가들로 구성하였다. 포커스 그룹을 통해 논문의 상황변수에 대한 적절성, 상황 및 정보보호 기능에 따른 부서 편성의 적합성을 검정하였다.

상황변수에 대한 적절성은 환경과 기술변수 CEO, CIO 및 CISO 그룹 모두 적절하다고 논의되었으나, CEO 그룹 중 1명이 추가적으로 기업의 규모가 고려되어야 한다는 의견을 제시하였다. 또한 CISO 그룹에서 비즈니스 위험도와 IT의존도에 대해 정량적으로 측정할 수 있는 척도가 개발되어야 한다는 의견이 제시되었다. 이에 대해 비즈니스 위험도에 대한 척도로 민・형사적인 판결에 따른 손실, 서비스의 손실 등이 제시되었고, IT 의존도에 대한 척도로는 경영활동에 IT 자산이 활동되는 정도 등이 활용될 수 있다는 의견이 제시되었다.

한편, 비즈니스 위험도가 낮을 때 IT 부서 및 내부관리 부서 산하에 정보보호 전담조직이 편성되는 것은 CEO, CIO 및 CISO 그룹의 대부분이 적합하다고 논의되었다. 하지만, 비즈니스 위험도가 높고 IT 의존도가 높을 경우, CEO 그룹 중 1명, CISO 그룹 중 2명이 전사적인 보안활동. 비즈니스 및 IT와의 연계, 효율적인 예산 및 자원 할당이 가능하기 때문에 내부통제 부서 산하보다 기획조정 부서 산하가 적합할 수 있다는 의견을 제시하였다. 하지만 대부분의 전문가들은 비즈니스 위험도와 IT 의존도가 높을 경우, 전사적인 관점에서 통제 기능을 우선하는 것이 중요하기 때문에 내부통제 산하에 정보보호 전담조직이 편성되어 있는 것이 적합하다는 의견을 제시하였다. 끝으로, CISO의 그룹 중 대부분이 정보보호 전담조직이 CEO 직속의 별도 조직으로 개편되는 경우, 최고 경영층의 정보보호 활동 참여, 효율적인 의사결정 및 보고체계 수립 등 거버넌스 차원에서 다양한 장점이 존재한다는 의견을 제시하였다. 즉 기업의 정보보호 수준을 향상하기 위해서는 무엇보다 최고경영층의 리더십이 아주 중요하기 때문에[19], CEO 직속으로 정보보호 전담조직이 개설될 필요가 있다는 의견이 제시되었다. 하지만 이에 대해 CEO 및 CIO 그룹은 다소 회의적인 의견을 제시하였다. 현재 기업의 CISO의 위상이 낮아 현실적으로 한계가 존재하고, 조직 규모적인 측면에서 정보보호 조직의 규모가 너무 작기 때문이다.

## 5. 결 론

현재 정보보호 전담조직과 IT 부서의 분리가 이슈화되고 있는 상황에서, 효율적인 정보보호 전담조직 편제에 대한 관심이 증가하고 있다. 본 연구에서는 정보보호의 기능과 상황적 접근방법을 기반으로 정보보호 전담조직 편성 모델을 제시하였으며, 이는 다음과 같은 의의를 갖는다.

첫째, 정보보호 전담조직의 편성에 대한 이론적인 방법론을 제공할 수 있다. 둘째, 전체적인 기업 구조에 대한 선행연구는 활발히 진행되어 왔으나 조직 편성을 중점으로 하는 연구는 아직까지 미흡하기 때문에 향후 조직 편성에 관한 선행연구로서 사용될 수 있다. 셋째, 편성은 조직 구조의 한 영역으로, 향후 정보보호 전담조직구조 설계 시 이에 대해 근간이 되는 자료를 제공할 수 있다.

하지만 본 연구는 정보보호 전문가를 대상

으로 편성모델에 대한 적합성과 실현가능성을 검토하였으나, 일반화가 어렵다는 단점이 있다. 따라서 향후 연구에서는 케이스 스터디, 실증연구 등을 통해 본 연구에서 제시한 편성모델을 검정할 필요가 있다.

## References


[1] BoanNews, “The CISO should manage Security Organization,” 2014.

[2] Oh, S. H., “Organization Theory,” Pakyoungsa, 2011.

[3] Bob, B., “Information Security is Information Risk Management,” The 2001 workshop on New security paradigms, pp. 97-104, 2001.

[4] Bruns, W. J., “Budgetary Control and Organization Structure,” Journal of Accounting Research, Vol. 13, No. 2, pp. 177-203, 1975.

[5] COSO, “Enterprise Risk Management: Integrated Framework: Executive Summary,” 2004.

[6] Dr. Gerald, K., “Establishing an Information Systems Security Organization (ISSO),” Computers and Security, Vol. 17, No. 7, pp. 600-612, 1998.

[7] Evan Wheeler, “Organizational Stricture What Works,” 2011.

[8] Forrester, “Security Organization 2.0: Building a Robust Security Organization,” 2010.

[9] Gartner, “Determining Whether the CISO Should Report Outside of IT,” 2014.

[10] Gartner, “Difference between governance, management, operation,” 2011.

[11] IBM, “Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security,” 2009.

[12] ISO/IEC, ISO/IEX 27000: Information security management systems: Overview and vocabulary, 2013.

[13] Jay, R. Galbraith, Designing Organizations, Pfeiffer, 2001.

[14] Kang, M. A., Son, J. Y., and Kim, H. J., “A Study on applicability of Mixed-methodology,” “Korean Public Administration Review,” Vol. 41, No. 4, pp. 415-437. 2007.

[15] Pennings, J. M., “Structural contingency theory: A reappraisal,” Research In Organizational Behavior, Vol. 14, pp. 267-309, 1992.

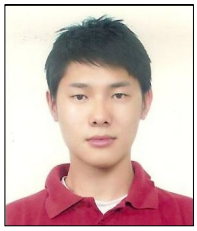
[16] Richard, H. H., “Intraorganizational Structural Variation: Application of the Bureaucratic Model,” Sage Publications, Inc., Vol. 7, No. 3, pp. 295-308, 1962.

[17] Richard, L., Organization Theory and Design, Cengage Learning, 2012.

[18] Stephen, P., Robbins, Organizational Behavior, Prentice Hall, 2014.

[19] Yoo, J. H., “Comparison of Information Security Controls by Leadership of Top Management,” The Journal of Society for e-Business Studies, Vol. 19, No. 1, pp. 63-78, 2014.

## 저 자 소 개



강현식 (E-mail: hskang8911@gmail.com)
2015년 중앙대학교 정보시스템학과 (학사)
2015년~현재 중앙대학교 융합보안학과 석사과정
관심분야 정보보호조직 설계, 정보보호 관리체계

김정덕 (E-mail: jdkimsac@cau.ac.kr)
1979년 연세대학교 정치외교학과 (학사)
1981년 연세대학교 경제학과 (석사)
1986년 Univ. of S. Carolina (MBA)
1990년 Texas A&M Univ. (Ph. D. in MS)
1995년~현재 중앙대학교 산업보안학과 교수
관심분야 정보보호 거버넌스, 정보보호 관리, IT 감사