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

The Journal of Society for e-Business Studies
Vol.25, No.1, February 2020, pp.45-64
https://doi.org/10.7838/jsebs.2020.25.1.045

# 인터넷기업에서 기업구성원 자율중심의 보안관리 방안 연구

## A Study on the Corporate Members' Autonomy-centric Security Management in the Context of Internet Companies

서현진(Hyunjin Seo)*, 김정덕(Jungduk Kim)**

### 초 록

급변하고 있는 비즈니스 환경에서 인터넷기업들은 비즈니스 특성상 유연하고 개방적이며 자율성을 강조하는 조직문화의 특징을 가지며, 시간과 장소에 구애받지 않는 유연한 스마트 업무환경으로 변화하고 있다. 이러한 인터넷 비즈니스 환경에도 불구하고 보안관리체계는 여전히 인터넷기업의 비즈니스 환경과 조직문화를 반영하지 못하고 있으며, 이로 인해 인터넷기업에서의 통제중심의 보안관리 방식은 한계에 부딪히고 있다. 따라서 본 연구에서는 인터넷기업의 비즈니스 환경과 조직문화의 특성을 고려한 보안관리의 연구를 위해 기업구성원 자율중심의 보안역할 항목을 설계하고 개발하였다. 본 연구결과는 민첩한 비즈니스 환경과 자율적인 조직문화의 인터넷기업에서 기업구성원 자율중심의 보안관리체계를 구현하고 운영하는데 활용될 것으로 기대된다.

### ABSTRACT

In the rapidly changing business environments, Internet companies have the characteristics of organizational culture that emphasize the flexible, open and autonomous nature of organizational culture, and are transforming into flexible smart working environment that is independent of time and place. Despite such an Internet business environment, the security management system still fails to reflect the business environment and organizational culture of the Internet company, and the control-focused security management system in the Internet company is facing limitations. Therefore, this study designed and developed Corporate members' autonomy-centered security items that considering the characteristics of the business environment and organizational culture of the Internet company. The results of this study are expected to be used to implement and operate corporate members' autonomy-centered security management system in internet companies with an agile business environment and an autonomous organizational culture.

**키워드** : 기업구성원 중심 보안, 자율 보안
Corporate Member-Centric Security, Autonomous Security

* First Author, MS, Department of Security Convergence, Graduate School, Chung-Ang University (cordias@naver.com)
** Corresponding Author, Professor, Department of Industrial Security, Chung-Ang University (jdkimcau@gmail.com)
Received: 2019-11-04, Review completed: 2019-12-30, Accepted: 2020-01-08

# 1. 서 론

4차 산업혁명의 등장으로 비즈니스 간의 영역이 파괴되고 있으며 산업 간, 기술 간의 융합화가 가속화되고 있다. 온・오프라인 경계가 해체되는 등 비즈니스의 패러다임이 빠르게 변화고 복잡해지고 있으며, 이에 따라 비즈니스의 불확실성이 증가하고 있다[23]. 이러한 급변하고 불확실성이 증가하는 비즈니스 환경에서 인터넷기업들이 생존하고 비즈니스를 연속적으로 유지하기 위해서는 비즈니스 환경의 변화와 기회를 파악하고 이를 통한 신속한 대응이 필요하다[5]. 이와 함께 기업 생존의 핵심 요인으로 기업의 창의성이 부각되고 있는데, 인터넷기업에서 창의적 성과를 내기 위해서 구성원들에 대한 자율성이 필수적인 요소이다[15]. 또한, 인터넷기업에서의 업무환경은 스마트폰, 태블릿PC, 노트북컴퓨터 등 각종 모바일 단말기와 슬랙(Slack), MS Teams 등 클라우드 기반의 협력 프로그램과 드롭박스, 구글드라이브, 원드라이브 등 파일 공유 서비스를 통해 언제 어디서나 장소에 구애받지 않고 유연하게 일을 할 수 있는 스마트워크 환경으로 변화하고 있다[24].

이러한 인터넷 비즈니스 환경의 변화에도 불구하고 전통적인 통제중심의 보안관리체계는 여전히 인터넷기업의 조직문화와 업무환경을 반영하지 못하고 기업구성원들의 창의성과 자율성을 제한하고 있는 실정이다. 이로 인해 인터넷기업에서 통제중심의 보안관리체계는 기업의 조직문화 및 업무환경에 상충되어 비즈니스에 더 이상 효과적이지 않고 방해가 된다고 생각되고 있다[3]. 또한, 불확실성이 크고 변화하는 인터넷 비즈니스 환경과 스마트워크 환경에서 통제중심의 보안관리 방식은 새로운 보안 위협 및 이슈를 예측하고 이를 대응하는데 어려움을 겪고 있다[9].

따라서 기존 보안관리체계의 한계를 극복하고 비즈니스 환경 변화에 신속히 대응하기 위해서는 법・규정 등에 대한 컴플라이언스 기반의 통제적인 보안활동이 아닌 근본적으로 새로운 접근 방식이 필요하며[10], 비즈니스와 연계된 보안 위험관리 기반의 자율적인 보안관리체계 수립이 필요하다. 이와 같은 자율적인 보안관리체계는 보안역할에 따른 기업구성원의 자기결정권과 자율성 보장을 통해 긍정적이고 자발적인 동기부여를 할 수 있도록 구현되어야 한다.

이러한 인터넷 비즈니스 환경에 따른 기존 보안 관리체제의 변화 요구에도 불구하고 지금까지 연구들은 대체로 아래와 같은 한계점을 지니고 있다. 첫째, 기업의 정보보호 관리체계의 적용 및 구현은 기업의 비즈니스 환경 및 조직문화에 따라 다르게 적용될 수 있음에도 이와 관련된 연구가 부족하였다. 최근에 들어서야 R&D 분야를 중심으로 R&D 환경 변화에 따른 연구자 중심의 보안관리 연구가 진행되고 있다[17]. 둘째, 자율을 중시하는 기업문화와 스마트워크 환경에서의 인터넷기업에서는 기업구성원의 보안역할이 필수적이다. 그러나 기업에서의 보안관리를 정보보안 전담 조직 및 인력의 전유물로 간주하여 정보보호위원회, CISO, 정보보호전담조직 등에 관련된 연구중심으로 이루어져 왔다[8, 11, 12]. 또한, 기업구성원은 보안위협 대응을 위한 공동 협의체가 아닌 통제 및 관리대상으로 인식해왔기 때문에 기업구성원이 기업의 보안활동에 참여하는 기업구성원의 보안역할에 관련된 연구는 매우 부족하였다. 셋째, 앞에서 설명한 내용들과 같이 불확실성이

크고 변화하는 새로운 인터넷 비즈니스 환경에서는 전통적인 통제중심의 보안관리와는 달리 인터넷기업의 비즈니스 환경 및 조직문화의 특성을 고려한 보안관리 연구가 필요하다. 그러나 인터넷기업의 특성을 고려한 기업구성원의 자율성을 보장하는 인터넷기업의 특성에 적합한 보안관리체계에 관련된 연구가 부족하였다.

본 연구에서는 인터넷기업에서 기업구성원들이 보안 이행주체로 참여해야 하는 보안 역할항목을 선정하고 선정된 보안 역할항목들 중에서 기업구성원에게 자율을 통해 이행할 수 있도록 함으로써, 인터넷 비즈니스 환경에서 기존의 보안조직 중심으로 하는 통제기반 보안관리체계의 한계 극복하고 기업구성원의 창의성과 자율성을 중요시하는 인터넷기업의 특성을 고려한 보안관리체계에 대한 연구를 진행하고자 한다.

## 2. 이론적 배경 및 선행 연구

### 2.1 인터넷기업에서의 보안관리 특징

인터넷기업은 인터넷을 매개로 가치를 창출하는 인터넷 비즈니스와 관련된 기업을 말하며, 인터넷 포털・뉴스・게임・쇼핑몰 등 인터넷을 통해 각종 정보를 제공하거나 인터넷 기반으로 서비스를 하는 기업들이 포함된다[16]. 인터넷기업의 비즈니스 환경은 정보와 지식의 연결 및 재구성을 통한 새로운 가치의 창출, 여러 산업 경계의 융합 등을 통해 새로운 비즈니스의 창출하는 등 빠르게 변화하고 있다[13]. 급격한 비즈니스 환경의 특성상 인터넷기업에서 기업문화의 변화는 매우 중요한 이슈이다. 이에 따라, 권위주의적이고 수직적인 위계질서 대신 개방적이며 수평적인 의사소통 그리고 복잡한 규정, 관료적 통제 대신 자율적인 조직문화가 인터넷기업의 특징이라고 할 수 있다.

한편, 2003년 1.25 인터넷 대란에서 2016년 온라인쇼핑몰의 개인정보 대규모 유출 사고 등 보안사고를 수습하고 정비하는 과정에서 정보보호 안전진단제도, 정보보호관리체계 인증 의무화 등 정부 규제들이 활성화되었다. 한편, 인터넷기업의 보안관리체계는 기업의 자발적인 요구에 따라 수립・운영되었다기보다 인터넷기업 대상의 이러한 보안 관련 규제들에 의해 수립되고 운영되어 온 경향이 있다.

따라서 인터넷기업의 통제중심 보안관리체제는 자율적인 조직문화 기반의 비즈니스기획, 개발, 지원부서 및 기업구성원들과 여러 분야에서 이해 충돌이 발생해왔으며 인터넷기업의 비즈니스 목적과 연계되지 않은 전략으로 인해 전반적인 관심과 협조를 이끌어내는데 어려움을 겪고 있다[14].

### 2.2 기업구성원 중심의 보안관리

기업 경영에서는 인간과 경영성과 사이의 연관성에 관련된 연구가 꾸준하게 진행되어 왔다. 이러한 연구들은 기업구성원은 존엄성을 가진 인격체이므로 구성원을 통해 기업의 경영성과를 최대로 이끌어 낼 수 있는 환경을 조성하는 것이 중요하며, 인간 중심적 경영이 기업의 지속적인 경쟁우위의 원천이라는 사실에 근거를 두고 있다[27]. 반면, 그동안 기업의 보안관리와 관련된 연구들은 기업 내 정보 유출의 상당 부분이 내부직원에 의해 진행되고 있다는 이유로 기업구성원을 보안 위협 대응을 위한 공동 협

의체가 아닌 통제 및 관리대상만으로 간주하여 진행되어 왔다[1, 28].

기업구성원 중심의 보안관리는 기업구성원을 잠재적 보안위반자가 아닌 존엄성을 가진 인격체로서의 인간 중심적 경영과 맥락을 같이 한다. 기업구성원 중심의 보안관리는 기업구성원에 대한 신뢰에서 시작하며, 신뢰와 독자적인 의사결정을 높여 구성원의 잠재력을 극대화하기 위한 목적을 가진다. 이러한 기업구성원 중심의 보안관리는 아래와 같은 특징을 갖는다[3]. 첫째, 기업구성원에게 보안에 대한 더 많은 역할과 책임을 부여하고, 그들의 행동에 대해 직접적인 책임을 지게 한다. 보안조직은 기업구성원이 부여된 보안역할을 원활하게 수행하도록 지원함으로써 새로운 가치를 만들어야 한다. 둘째, 기업구성원이 스스로에게 할당된 역할과 책임에 대해 적절한 행동을 수행할 수 있도록 보안에 대한 이해와 인식제고를 향상시키기 위한 활동을 지속해야 한다. 셋째, 구성원의 자율성을 보장하고 잠재력을 극대화하기 위해 예방적 통제를 최소화하고 모니터링 중심으로 전환해야 한다.

한편, 국내 R&D 분야에서도 연구자 중심의 R&D 환경 변화에 따라 연구자 중심의 창의적이고 자율적인 방식으로 연구를 지원하기 위해 연구과정에서 창출되는 연구 성과물 보호를 연구책임자가 스스로 이행하도록 하는 연구자 중심의 보안관리체계 연구가 진행되고 있다[17].

## 2.3 자율기반의 보안관리

자율성(autonomy)은 자신의 선택에 따라 결정하고 행동하며 외부로부터 구속되거나 얽매이지 않은 상태를 말하며, 자기 스스로의 원칙이나 규칙에 따라 결정하고 행동하고 그 결과에 대해 책임지는 것을 말한다[18]. 그리고 기업에서 자율성이란 업무 과정에서 업무 일정, 의사결정 권한과 유연성에 있어서 얼마나 많은 재량을 부여받고 있는지의 정도를 의미하며, 기업구성원에게 자율성 보장은 강한 동기유발 요인으로 직무성과에 긍정적인 영향을 주는 것을 알려져 있다[4]. 이러한 자율과 달리 통제는 외부 요인을 통해 일정한 목적에 따라 행위를 제한하거나 제약하는 것을 의미하며, 행위의 억제 및 결정을 통해 수립된 목표를 달성하거나 개선하고 조정하는 개념을 포함한다[2].

일반적으로 자율과 통제의 특성을 고정된 이분법적으로 이해하기 쉬운데, 자율과 통제는 고정된 특성이기보다는 정도의 문제라고 할 수 있다[19]. 또한, 자율과 통제에 있어 정도의 차이만 있을 뿐 행위에 제약이 따르며, 차이점으로 통제는 제약의 주체가 타인 또는 외부 요인이지만 자율은 제약을 주는 주체가 자기 스스로라는 것을 알 수 있다.

이러한 자율성의 개념에 근거하여 기업구성원 자율중심의 보안관리체계에 대한 개념을 살펴보면, 기업구성원 자율중심의 보안관리체계란 보안관리체계의 일부 항목에 대해 보안조직 및 조직장 등 기업 내·외부 요인이 아닌 기업구성원 자신의 결정을 통해 보안역할을 이행하는 것을 의미한다. 즉, 기업구성원 스스로가 보안역할 이행을 결정하고, 그 결과에 대해 책임을 지는 것이라고 볼 수 있다. 이러한 기업구성원의 자율을 통한 자기 결정은 자신의 행동이 바람직한 결과를 초래할 것이라는 대응효율을 통해 보안 준수 의도에 긍정적인 영향을 미치게 된다[7]. 따라서 기업구성원 자율중심의 보

안관리체계는 기업구성원들에게 자기 결정과 자기 책임의 보안 자율성을 부여하고 이를 통해 보안 준수에 대한 동기를 촉진함으로써 인터넷기업에서의 자율적인 업무환경과 스마트 워크 환경, 그리고 새로운 기술 발전으로 인한 기술적 솔루션 중심의 통제 한계를 극복할 수 있는 방안이라고 생각된다.

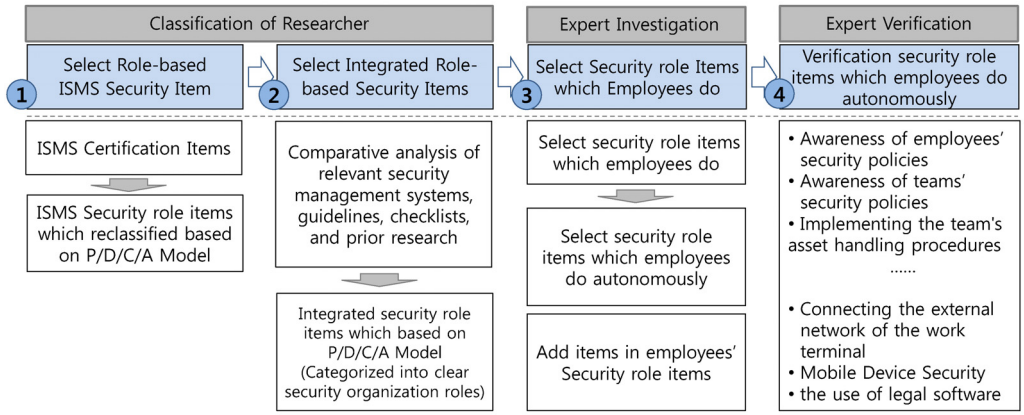
새로운 기술과 경쟁자, 새로운 비즈니스 모델이 수시로 생성되는 급변하는 인터넷 비즈니스 환경에서 정해진 규율과 외부 요인에 얽매인 통제정책은 기업구성원의 자율적이고 창의적인 활동의 저하를 초래하며 이러한 비즈니스 환경에 적응하기 어렵다[25]. 이에 따라, 인터넷기업을 중심으로 창의성과 강한 동기부여를 위해 직무 자율성을 보장하는 기업 문화가 활성화되고 있으나 보안관리에서는 통제 형태를 벗어나 보안 자율성을 부여하는데 어려움을 겪고 있다. 따라서 새로운 비즈니스 환경 변화에 신속히 대응하기 위해서는 컴플라이언스 기반의 통제중심 보안관리보다는 기업구성원의 보안 역할에 대한 자기 결정권을 높이고 이에 따른 책임을 부여하는 자율적인 보안관리체계 수립이 필요하다. 그리고 인터넷기업에서 기업구성원의 통제를 최소화하고 자율적이고 자기 결정권을 통한 창의적 업무활동을 보장하기 위한 자율적인 보안관리체계 수립을 위해서는 기업구성원에게 관련된 보안항목에 대한 역할과 이에 따른 책임에 대한 정리가 선행되어야 하겠다. 다만, 자율중심의 보안관리체계는 기업의 핵심인력, 주요 규제대상 업무취급자, 퇴직예정자 등을 포함한 모든 범위에 걸쳐 구현하기는 적합하지 않으므로 비즈니스와 연계된 위험관리 기반으로 기존 통제중심의 보안관리체계와 병행하여 수립될 필요가 있다.

# 3. 기업구성원 자율중심의 보안관리 체계 개발

## 3.1 기업구성원 자율중심의 보안관리 연구방법

본 연구에서는 인터넷기업의 비즈니스 환경에서의 민첩성과 창의성을 확보하기 위해 보안관리에 대한 기업구성원의 통제를 최소화하고 자율을 부여하는 기업구성원 자율중심의 보안관리체계를 개발하고자 한다. 이를 위해 ISMS 정보보호관리체계 인증기준을 바탕으로 하였는데, ISMS(정보보호관리체계) 인증기준이 통제중심의 보안항목으로 구성되어 있지만, 자율과 통제는 정도의 차이이며 제약을 가하는 주체에 따라 자율과 통제의 방향이 달라진다는 선행연구 결과와 ISMS 정보보호관리체계가 기업의 정보보호관리체계의 효과성을 객관적으로 보증하는데 가장 널리 활용되고 있다는 점에 근거하고 있다[21].

본 연구는 인터넷기업에서의 기업구성원 자율중심의 보안관리 설계 및 검증을 아래 <Figure 1>과 같이 4단계에 걸쳐 진행하였다[17]. 1단계에서는 연구자가 ISMS(정보보호관리체계) 보안 인증기준을 PDCA 순환모델을 기반으로 이행 주체의 보안 역할항목으로 재분류하였다[6]. 2단계에서는 연구자가 ISMS 보안 역할항목을 다른 보안관리체계 지침, 점검항목 등의 보안항목을 반영한 통합 보안 역할항목으로 구성하였다. 3단계에서는 전문가조사를 통해 역할 중심의 보안항목 중에서 기업구성원에게 역할을 부여해야 하는 기업구성원 보안역할 항목을 선정하고, 선정된 보안역할 항목에 대해 기업구




〈Figure 1〉 Process of the Security Role Items which Employees do Autonomously

성원이 역할항목을 이행할 때 자율과 통제, 어느 방식으로 이행하도록 할지에 대해 분류하였다. 마지막 4단계에서는 인터넷기업에 근무하고 있는 인터넷기업 전문가조사를 통해 인터넷기업에서 기업구성원이 보안역할 항목 이행 시 자율측면에서 이행해야 하는 기업구성원 자율보안항목에 대한 검증을 진행하였다.

## 3.2 기업구성원 자율중심의 보안관리체계 설계

본 연구에서 인터넷기업의 기업구성원 자율중심의 보안관리 체계 개발을 위해 인터넷기업을 포함한 기업・기관이 수립・관리・운영하는 정보보호 관리체계의 적합성에 대해 인증을 부여하는 제도인 「ISMS(정보보호관리체계)인증 기준」의 관리체계 수립 및 운영 16항목, 보호대책 요구사항 64개의 80항목을 기반으로 진행하였다[21]. ISMS 정보보호관리체계 인증기준에서는 '관리체계 수립 및 운영영역'과 '보호대책 요구사항'으로 분리되어 있었으나, '관리체계 수립 및 운영영역'은 주로 정보보호 조직의 보안역할에 해당하므로 '보호대책 요구사항'을 기반으로 개발하게 되었다. 한편, ISMS 정보보호관리체계 인증기준은 정보보호에 대한 인증 및 점검 등의 목적으로 개발된 보안항목이기 때문에 보안이행 주체별로 구분하기에 적합하지 않다. 따라서 연구자는 PDCA 순환모델을 기반으로 해당 보안항목을 이행해야 하는 주체 또는 조직 중심의 보안역할 항목으로 재분류하였으며[6], 108개의 보안역할 항목을 도출하였다.

그리고 ISMS 기반의 보안역할 항목을 보완하기 위해 연구자는 추가적으로 「ISO/IEC 27001:2013」, 「NIST-SP 500-53 R4」, 「주요정보통신기반시설 취약점 분석・평가 점검항목」, 「중소기업기술보호지침」의 각 항목에서 기업구성원에 관련된 보안항목을 추가 및 재구성하였다[6, 20, 22, 26]. 구체적으로는 첫째, ISMS 기반 보안역할 항목을 이행 주체별 보안역할을 상세화하기 위한 목적으로 기업구성원의 보안정책 인지, 부서별 보안정책 인지, 직무기술서 작성, 기업구성원 보안서약서 징구 및 보관, 방문객 및 외부인의 출입관리, 출입증 패용 등의 보안항목을 추가 반영하였다. 둘째, ISMS 기반

보안역할 항목에 포함되지 않은 항목을 보완하기 위한 목적으로 보안관련 기관 및 전문가 연계, 주요지식 및 기술 정보관리, 핵심기술관리, 기술거래관리, 개발환경 보안, 외주개발 보안, 시스템 보안 테스트, 시스템 인수 테스트 등의 보안항목을 추가하였다. 셋째, 기업구성원 역할을 상세화하기 위한 목적으로 업무단말기기에 프로그램 다운로드 및 설치 주의, 스팸메일 열람 주의, 모바일기기 보안, 업무단말기 분실 대책 등을 추가하였다. 이와 같은 보안항목 추가 및 재구성을 통해 총 31개 보안 역할항목이 증가하였으며, 전체 139개의 통합 보안 역할항목을 <Table 1>과 같이 정리하였다.

그리고 연구자가 진행했던 통합 보안 역할항목에 대한 중복과 누락 등의 문제점을 확인하고 기업구성원에 의해 이행되어야 할 보안역할 항목 선정을 위해, 보안 관련 실무 경력 10년 이상인 10명의 전문가 대상으로 이메일과 현장 인터뷰를 통한 전문가조사를 2차례에 걸쳐 진행하였다.

1차 전문가조사에서는 139개의 통합 보안역할 항목 중에서 보안 계획수립, 보안 점검, 보안 개선활동 등 명백하게 기업구성원의 보안 역할 항목이 아닌 65개 항목을 제외한 74개의 보안역할 항목 중에서, 기업구성원의 보안역할 항목에 해당하는 항목에 'O'로 표시하게 하였다. 그리고 기업구성원의 보안 역할항목으로 선정한 항목에 대해서 추가적으로 기업구성원이 보안 역할을 이행할 때 해당 보안역할 수행을 자율적으로 이행하도록 할지 또는 통제적으로 이행하도록 할지를 선정하도록 하였다. 마지막으로, 조사지의 통합 보안 역할항목 중에서 역할항목

〈Table 1〉 Standard for Certification of Information Security Management System & Integrated Security Management Items Based Security Role

| Area | ISMS-Items | Integrated-Items |
|---|---|---|
| 1. Policy, Organization | 3 | 6 |
| 2. Asset Management | 4 | 7 |
| 3. Personnel Security | 15 | 21 |
| 4. External Security | 5 | 5 |
| 5. Physical Security | 10 | 15 |
| 6. Management of Authentication and Rights | 9 | 9 |
| 7. Access Control | 11 | 11 |
| 8. Cryptography | 3 | 3 |
| 9. Information System Introduction and Development Security | 6 | 10 |
| 10. System and Service Operations Management | 8 | 9 |
| 11. System and Service Security Management | 7 | 7 |
| 12. Personal Device Management | 16 | 21 |
| 13. Accident Prevention and Response | 5 | 8 |
| 14. Business Continuity Plan | 2 | 3 |
| 15. Compliance | 4 | 4 |
| Total | 108 | 139 |

〈Table 2〉 The Result of Experts Investigation about Employee's Security Role Item

| | | 1st Step | | 2nd Step | |
|---|---|---|---|---|---|
| Total of Security Item | | 74 | - | 89 | - |
| Employees Security Role Item | | 35 | 47.3% | 40 | 48.3% |
| | Autonomous Security Role Item | 12 | 34.3% | 21 | 41.9% |
| | Control Security Role Item | 3 | 8.6% | 4 | 11.6% |
| | Other Security Role Item | 20 | 57.1% | 15 | 46.5% |

이 중복되거나 누락된 항목이 있는 경우 기타 의견에 기술하도록 하였다. 이와 같이 진행된 1차 전문가조사에서 <Table 2>와 같이 35개의 기업구성원 보안 역할항목을 선정하였고, 그중에서 기업구성원 자율을 통해 이행할 수 있는 보안역할 항목 12개, 보안통제가 반드시 필요한 보안역할 항목 3개를 선정하였다. 또한, 보안역할항목 중복 및 누락에 대한 의견 반영은 2명 이상의 전문가가 동일한 항목에 대해 수정 의견을 제시한 경우 진행하였는데, <Table 3>과 같이 15개(기존항목 분리, 추가항목)항목이 확인되었으며 이를 2차 전문가조사를 위한 조사지에 반영하였다.

2차 전문가조사에서는 <Table 2>와 같이 1차 전문가조사보다 15개 보안 역할항목이 증가한 89개 보안역할 항목에 대해 기업구성원 보안역할 항목 선정을 다시 진행하였다. 그 결과 <Table 2>과 같이 40개의 기업구성원 보안역할 항목과 기업구성원 보안역할 항목 중에서 기업구성원 자율을 통해 이행할 수 있는 보안역할 항목이 21개, 보안통제가 반드시 필요한 보안역할 항목 4개를 도출하였다. 1차 전문가조사보다 2차 전문가조사 결과를 비교해보면, 기업구성원 보안역할 항목 중 자율중심의 보안역할 항목 비중이 약 7.6% 증가하였다.

## 4. 기업구성원 자율중심의 보안관리체계 검증

연구 설계에서 확인된 기업구성원 자율중심의 보안역할 항목에 대한 검증을 위해 인터넷기업에서 근무하고 있는 보안경력 10년 이상 전문가 15명을 대상으로 인터넷기업 보안 전문가조사를 진행하였다.

인터넷기업 전문가조사는 사전에 참여한 전문가에게 대면이나 전화를 통해 보안역할 자율성 수준의 점수가 높을수록 이행에 대한 행위금지나 모니터링 등의 관여 등의 외적 요인의 개입이 적음을 설명하였다. 또한, 인터넷기업 전문가조사의 조사지 작성은 기업구성원의 보안 역할항목에 대해 어느 정도의 자율을 부여할지를 리커트 5점 척도로 표시하도록 하였다. 그 결과 <Table 3>의 Degree of Autonomy: Verification 컬럼과 같이 정리되었으며, 기업구성원 자율중심 보안역할 항목의 채택은 인터넷기업 전문가 15명의 평균점수 3.5 이상 항목으로 하였다.

그 결과, <Table 3>과 같이 보안정책 영역 2개 항목, 자산관리 영역 1개 항목, 인적보안 영역 6개 항목, 물리보안 영역 3개 항목, 접근통제 영역 2개 항목, 업무단말기 보안관리 영역

10개 항목, 보안사고 예방 및 대응 영역 1개, 준거성 영역 1개 총 26개의 기업구성원 보안 자율역할 항목이 확인되었다.

보안정책 영역에서는 보안정책에 대한 인지, 자산관리 영역에서는 '기업구성원에게 지급된 자산에 대한 취급 절차 이행', 인적보안 영역에서는 '직무기술서 및 보안 서약서 작성', '인식제고 및 교육훈련 참여', '외부 커뮤니케이션 및 공공장소 보안관리' 항목이 확인되었고, 물리보안 영역에서는 '방문객 및 외부인 출입관리', '출입증 패용', '오피스 업무환경에서의 보안 이행'에 대해 기업구성원에게 자율역할 부여가 필요하다고 확인되었다. 그리고 접근통제 영역에서 '오피스환경으로의 원격접속', '안전한 인터넷 접속 연결 이행', 업무 단말기 보안관리 영역에서는 '프로그램 다운로드 및 설치', '스팸메일 열람 주의', '업무 단말기기에서 정보전송 관리', '업무 협업프로그램 사용', '업무 단말기기 정보저장 이행', '출력 및 출력물 정책 이행', '업무단말기기 반·출입 관리', '업무단말기기의 외부 네트워크 연결', '모바일기기 보안', '업무단말기기 및 매체 분실 대응', 보안사고 예방 및 대응영역에서 '구성원 보안 이벤트 보고', 준거성 영역에서 '정품 소프트웨어 사용'에 대해 기업구성원에게 자율역할 부여가 필요하다고 확인되었다. 반면, '퇴직보안 관리', '외부 계약자의 계약 변경 및 만료에 따른 보안', '장비 운영공간에서의 반·출입 정책 이행', '개인소유 기기의 사내 유선·무선 네트워크의 보안' 항목은 기업구성원에게 자율을 부여하기 어려운 항목으로 확인되었다.

연구설계의 항목과 비교해보면, 기업구성원 자율중심 보안 역할항목이 21개 항목에서 26개 항목으로 5개 보안항목이 증가하였다. 설계 단계에서보다 '직무기술서 작성', '보안서약서 서약,' '방문객 및 외부인 출입관리', '오피스로의 원격접속 항목', '업무단말기기 및 매체 분실 대응', '구성원의 보안 이벤트 보고'의 6개 항목이 추가되었으며, '구성원의 보조 저장 매체 정책 이행' 항목이 제외되었다. 그러한 이유는 아직까지 인터넷기업에서는 정보보호 관리체계 인증 등의 외부기관의 인증 유지 때문에 구성원의 보조 저장 매체 정책 이행에 대한 증적이 필요하고, 인터넷기업들의 대부분 인터넷 서비스 이용자 개인정보를 취급하고 있어 구성원의 보조 저장 매체 정책에 대해 민감하게 생각하고 있어 해당 항목을 자율로 맡기기 어렵다고 추정된다. 또한, 자율항목으로 추가된 '오피스로의 원격접속항목', '업무단말기기 및 매체 분실 대응', '구성원의 보안 이벤트 보고'의 보안항목은 보안조직에서 보안시스템 등을 통제가 어려워 부득이하게 자율항목으로 선택했을 것으로 추정된다.

이렇게 선정된 기업구성원 자율 보안역할 항목은 통제중심 보안관리체계에서의 획일적인 방식에서 벗어나 기업마다 기업의 비즈니스 환경 및 조직환경에 따라 다양한 방식으로 적용될 수 있을 것이다. 예를 들면, 보안 인식제고 및 교육훈련에 대한 보안활동의 경우 기존에는 구성원의 강제적인 보안역할로 간주되어 참여하지 않았을 경우 해당 구성원은 인사적인 불이익을 받기도 했었다. 그러나 자율중심 보안관리체계에서는 보안 인식제고 및 교육훈련의 참여가 강제가 아닌 자율이며, 다만 보안 인식제고 및 교육훈련의 불참여로 발생되는 결과와 그에 따른 불이익은 기업구성원 스스로 책임질 수 방식으로 운영될 수 있을 것이다.

〈Table 3〉 Degree of Autonomy for the Employee's Security Role Items in Integrated Security Role Items

| Area | Security Role Items | [1] | [2] | [3] | [4] | [5] | R/A | Add Items by Expert Investigation | Employee Role Items | Degree of Autonomy | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | Design | Verifica-tion |
| 1. Security Policy, Organization (6) | | | | | | | | | | | |
| 1.1 | Establishing and Reviewing Security Policy | ● | ● | ● | ● | ● | 100% | | | | |
| 1.2 | Approving and Sharing Security Policy | ● | ● | | ● | ● | 80% | | | | |
| **1.3** | **Recognizing member security policies** | ● | ● | | ● | ● | **80%** | | O | 8 | 3.93 |
| **1.4** | **Recognizing security policies by department** | ● | ● | | ● | ● | **80%** | | O | 7 | 4.00 |
| 1.5 | Assigning roles and responsibilities for security organizations | ● | ● | ● | ● | ● | 100% | | | | |
| 1.6 | Contact with relevant Security agencies and experts | | ● | | ● | ● | 60% | | | | |
| 2. Asset Management (8) | | | | | | | | | | | |
| 2.1 | Establish Asset Management Procedures and Protection Measures | ● | ● | | ● | ● | 80% | | | | |
| 2.2 | Asset Identification Management | ● | ● | | ● | ● | 80% | | | | |
| 2.3 | Establish Asset Classification and Marking Procedures | ● | ● | ● | ● | ● | 100% | | | | |
| **2.4** | **Implementing procedures for handling organizational asset** | ● | ● | ● | ● | ● | 100% | Separation | O | 4 | 3.40 |
| **2.5** | **Implementing procedures for handling personal assets** | ● | ● | ● | ● | ● | 100% | Separation | O | 7 | 3.67 |
| 2.6 | Key Knowledge/Technical Information Management | | | | | ● | 20% | | | | |
| 2.7 | Critical Technology Management | | | | | ● | 20% | | | | |
| 2.8 | Technical Transaction Management | | | ● | | ● | 40% | | | | |
| 3. Personal Security (23) | | | | | | | | | | | |
| 3.1 | Establishing key job-based management policies | ● | | ● | | | 40% | Separation | | | |
| 3.2 | Designate and manage key people | | | | | | | Separation | | | |
| 3.3 | Writing job description | | | | ● | | 20% | | O | 3 | 3.67 |
| 3.4 | Establishing standards for division of duties | ● | ● | ● | ● | | 80% | | | | |
| 3.5 | Job separation fulfillment | ● | ● | | ● | | 60% | | | | |
| 3.6 | Specify Security Compliance for member | ● | ● | ● | | | 60% | | | | |
| 3.7 | Commitment member security | ● | ● | ● | ● | ● | 100% | | O | 3 | 3.67 |

〈Table 3〉 Degree of Autonomy for the Employee's Security Role Items in Integrated Security Role Items(Continued)

| Area | Security Role Items | [1] | [2] | [3] | [4] | [5] | R/A | Add Items by Expert Investigation | Employee Role Items | Degree of Autonomy | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | Design | Verifica-tion |
| 3.8 | Managing member security documents | ● | ● | ● | ● | ● | 100% | | | | |
| 3.9 | Establishment of Planning for Awareness, Education and Training | ● | ● | ● | ● | | 80% | | | | |
| 3.10 | Implementing of Awareness, Education and Training | ● | ● | ● | ● | ● | 100% | | | | |
| 3.11 | Participate in awareness | ● | ● | ● | | | 60% | Separation | O | 7 | 4.27 |
| 3.12 | Participate in Education and Training | ● | ● | ● | | | 60% | Separation | O | 7 | 4.07 |
| 3.13 | 5) Applying the results of Awareness, Education and Training | ● | ● | | ● | | 60% | | | | |
| 3.14 | 1) Establishing a security management procedure for job change | ● | ● | ● | | ● | 80% | | | | |
| 3.15 | 2) Implementing job change security management | ● | ● | ● | | ● | 80% | | O | 2 | 3.13 |
| 3.16 | 1) Establishment of retirement management procedures | ● | ● | ● | ● | ● | 100% | | | | |
| 3.17 | 2) Implementing of Retirement Management | ● | ● | ● | | ● | 80% | | O | 2 | 2.93 |
| 3.18 | 3) Checking results of retirement management | ● | ● | ● | | ● | 80% | | | | |
| 3.19 | 1) Establishing external communication security measures | | | ● | | | 20% | | | | |
| 3.20 | 2) Implementing external communications security | | | ● | | | 20% | | O | 9 | 4.07 |
| 3.21 | 1) Establishing security measures for public places | | ● | | | | 20% | | | | |
| 3.22 | 2) Implementing security in public places | | ● | | | | 20% | | O | 9 | 4.40 |
| 3.23 | Action in case of security breach | ● | ● | ● | | ● | 80% | | | | |
| 4. External Security (7) | | | | | | | | | | | |
| 4.1 | 1) Identifying the status of outsiders | ● | ● | | | ● | 60% | Separation | | | |
| 4.2 | 2) Outsider status protection management | | | | | | | Separation | | | |
| 4.3 | Security Management at External Contracts | ● | ● | | ● | | 60% | | | | |
| 4.4 | 1) External Security Implementation Check | ● | ● | ● | ● | | 80% | Separation | | | |
| 4.5 | 2) Managing and supervising the implementation of external security | | | | | | | Separation | | | |
| 4.6 | Security on External Contract Changes and Expires | ● | ● | | | | 40% | | O | 3 | 2.80 |
| 4.7 | Checking for implementing External Security Management | ● | ● | ● | ● | | 80% | | | | |

〈Table 3〉 Degree of Autonomy for the Employee's Security Role Items in Integrated Security Role Items(Continued)

| Area | Security Role Items | [1] | [2] | [3] | [4] | [5] | R/A | Add Items by Expert Investigation | Employee Role Items | Degree of Autonomy | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | Design | Verifica-tion |
| 5. Physical and Environment Security (18) | | | | | | | | | | | |
| 5.1 | Specify a security zone | ● | ● | ● | ● | ● | 100% | | | | |
| 5.2 | Establishment and Implement Physical access control Policy | ● | ● | ● | ● | ● | 100% | | | | |
| 5.3 | Visitor and outsider access control | | | ● | ● | ● | 60% | | O | 6 | 4.00 |
| 5.4 | Wearing an ID Card | | | | ● | ● | 40% | | O | 7 | 4.33 |
| 5.5 | System protection | ● | ● | ● | ● | | 80% | | | | |
| 5.6 | Operating of Protection Facility | ● | ● | ● | ● | ● | 100% | | | | |
| 5.7 | Establishing Job management procedure in security area. | ● | ● | | | | 40% | | | | |
| 5.8 | Implementing job procedure in security area. | ● | ● | ● | ● | | 80% | Separation | | | |
| 5.9 | Reviewing of work results in security area. | ● | ● | ● | ● | | 80% | Separation | | | |
| 5.10 | Security Management in Shipping and unloading area | | ● | ● | | | 40% | | | | |
| 5.11 | Equipment Layout and Protection | | ● | ● | | | 40% | | | | |
| 5.12 | Establishing and reviewing the policy of equipment into and out | | ● | ● | | ● | 60% | Separation | | | |
| 5.13 | Implementing policy of equipment into and out | | ● | ● | | ● | 60% | Separation | O | 1 | 2.80 |
| 5.14 | Reuse and Disposal of Equipment | | | | | | | | | | |
| 5.15 | Establishing a Office Environment Security measures | ● | ● | | | ● | 60% | | | | |
| 5.16 | Implementing Office Environment Security | ● | ● | | | ● | 60% | | O | 8 | 4.33 |
| 5.17 | Establishing measures to protect public facilities and devices | ● | ● | | | ● | 60% | | | | |
| 5.18 | Implementing public facilities and device protection measures | ● | ● | | | ● | 60% | | | | |
| 6. Authority and Authentication (9) | | | | | | | | | | | |
| 6.1 | Implement policy of member Account Management for members | ● | ● | ● | | ● | 80% | | | | |
| 6.2 | Complies with Policy of Account management for members | ● | ● | | ● | ● | 80% | | O | 2 | 3.33 |
| 6.3 | Granting minimum work permissions | | | | | | | Add item | O | 2 | 3.40 |
| 6.4 | Member Identification | ● | ● | ● | ● | | 80% | | | | |

〈Table 3〉 Degree of Autonomy for the Employee's Security Role Items in Integrated Security Role Items(Continued)

| Area | Security Role Items | [1] | [2] | [3] | [4] | [5] | R/A | Add Items by Expert Investigation | Employee Role Items | Degree of Autonomy | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | Design | Verifica-tion |
| 6.5 | Membership authentication | ● | ● | ● | ● | | 80% | | | | |
| 6.6 | Establishing policy of password management procedure | ● | ● | | ● | ● | 80% | | | | |
| 6.7 | Complies with Policy of password management procedure | ● | ● | | ● | ● | 80% | | O | 2 | 3.27 |
| 6.8 | Performing policy of password management procedure | ● | ● | | ● | | 60% | | | | |
| 6.9 | Managing of Privileged account and access rights | ● | ● | ● | | ● | 80% | | | | |
| 6.10 | Reviewing access authority | ● | ● | | | ● | 60% | | | | |
| 7. Access Control (12) | | | | | | | | | | | |
| 7.1 | Implementing of Access Control Policy for Network | ● | ● | ● | ● | ● | 100% | | | | |
| 7.2 | Access Control for Network on Personal devices | ● | ● | | ● | | 60% | | O | 3 | 2.73 |
| 7.3 | Access Control to Information System | ● | ● | ● | ● | | 80% | | | | |
| 7.4 | Access Control for Application | ● | ● | | | | 40% | | | | |
| 7.5 | Access Control for Database | ● | ● | | | | 40% | | | | |
| 7.6 | Implementing Access Control Policy for Wireless Network | ● | ● | ● | ● | | 80% | | | | |
| 7.7 | Access Control for Network on Wireless Personal devices | ● | ● | ● | ● | | 80% | | O | 2 | 2.80 |
| 7.8 | Establishing and Implementing Remote access control Policy | ● | ● | ● | ● | | 80% | | | | |
| 7.9 | Comply with Remote access control Policies to Information System | ● | ● | | ● | | 60% | Separation | | | |
| 7.10 | Comply with Remote access control Policies to Office Network | ● | ● | | ● | | 60% | Separation | O | 2 | **3.53** |
| 7.11 | Establishing Internet Access Control Policies | ● | ● | | | | 40% | | | | |
| 7.12 | Complies with secure Internet access policies | ● | ● | | | | 40% | | O | **8** | **4.00** |
| 8. Cryptography (3) | | | | | | | | | | | |
| 8.1 | Establishing Cryptography Policy | ● | ● | ● | | | 60% | | | | |
| 8.2 | Implementing Cryptography Policy | ● | ● | ● | | | 60% | | | | |
| 8.3 | Cryptography key Management | ● | ● | ● | ● | | 80% | | | | |
| 9. System acquisition, development Security (10) | | | | | | | | | | | |
| 9.1 | Defining Security Requirements | ● | ● | ● | | | 60% | | | | |

〈Table 3〉 Degree of Autonomy for the Employee's Security Role Items in Integrated Security Role Items(Continued)

| Area | Security Role Items | [1] | [2] | [3] | [4] | [5] | R/A | Add Items by Expert Investigation | Employee Role Items | Degree of Autonomy | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | Design | Verifica-tion |
| 9.2 | Review and test security requirements | ● | ● | ● | | | 60% | | | | |
| 9.3 | Isolating operating and testing environment | ● | ● | | ● | | 60% | | | | |
| 9.4 | Test Data Security | ● | ● | | | | 40% | | | | |
| 9.5 | Source program Management | ● | | ● | ● | | 60% | | | | |
| 9.6 | Transfer operation environment | ● | ● | | | | 40% | | | | |
| 9.7 | Development Environment Security | | ● | | | | 20% | | | | |
| 9.8 | Outsourcing Development Security | | ● | ● | | | 40% | | | | |
| 9.9 | System security Test | | ● | ● | ● | | 60% | | | | |
| 9.10 | System Acceptance Test | | ● | ● | ● | | 60% | | | | |
| 10. System and Services Operation Management (9) | | | | | | | | | | | |
| 10.1 | Change Management | ● | ● | ● | | | 60% | | | | |
| 10.2 | Performance and Capacity Management | ● | ● | ● | | | 60% | | | | |
| 10.3 | Incident Management | | ● | | ● | ● | 60% | | | | |
| 10.4 | Backup and Recovery Management | ● | ● | | ● | ● | 80% | | | | |
| 10.5 | Log and Connection record Management | ● | ● | ● | | | 60% | | | | |
| 10.6 | Log and Connection Record Check | ● | ● | ● | | | 60% | | | | |
| 10.7 | Time synchronization | ● | ● | ● | | | 60% | | | | |
| 10.8 | Establishing and Establishing Reuse and Disposal of Information Assets | ● | ● | | ● | | 60% | | | | |
| 10.9 | Checking Reuse and Disposal of Information Assets | ● | ● | | | | 40% | | | | |
| 11. System and Services Security (7) | | | | | | | | | | | |
| 11.1 | Security System Operation | ● | ● | | ● | ● | 80% | | | | |
| 11.2 | Cloud Security | ● | | | ● | ● | 60% | | | | |
| 11.3 | Public Server Security | ● | ● | | | | 40% | | | | |
| 11.4 | Electronic Trade and Fintech Security | ● | | | | | 20% | | | | |
| 11.5 | Information Transfer Security | ● | ● | ● | | | 60% | | | | |

〈Table 3〉 Degree of Autonomy for the Employee's Security Role Items in Integrated Security Role Items(Continued)

| Area | Security Role Items | [1] | [2] | [3] | [4] | [5] | R/A | Add Items by Expert Investigation | Employee Role Items | Degree of Autonomy | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | Design | Verifica-tion |
| 11.6 | System Patch Management | ● | ● | ● | | | 60% | | | | |
| 11.7 | System Malicious Code Control | ● | ● | ● | ● | | 80% | | | | |
| 12. Work Terminal Security (25) | | | | | | | | | | | |
| 12.1 | Work Terminal Security Management | ● | | | | | 20% | | | | |
| 12.2 | Implementing Work Terminal Security Settings | ● | | | | | 20% | | | | |
| 12.3 | Operating Work Terminal Security Settings | ● | | | ● | | 40% | | O | 6 | 3.20 |
| 12.4 | Implementing Work Terminal Patch Policy | ● | ● | ● | | | 60% | | | | |
| 12.5 | Complies with Work Terminal Patch Policy | ● | ● | ● | ● | | 80% | | O | 5 | 3.20 |
| 12.6 | Malicious code control for Work terminal devices | ● | ● | ● | ● | | 80% | | | | |
| 12.7 | Caution Program Download and Install in Work terminal devices | | | | ● | | 20% | | O | 8 | 3.80 |
| 12.8 | Caution of Reading Spam mail | | | ● | ● | | 40% | | O | 8 | 3.93 |
| 12.9 | Protection measures for Information transmission in Work terminal | ● | | | | | 20% | Separation | | | |
| 12.10 | Information transmission Management in Work terminal | ● | | | | | 20% | Separation | O | 7 | 3.80 |
| 12.11 | Protection measures Work collaboration program usage | ● | | | ● | ● | 60% | Separation | | | |
| 12.12 | Usage for Work collaboration program | ● | | | ● | ● | 60% | Separation | O | 7 | 3.93 |
| 12.13 | Protection Measures Data Transmission for External Network | ● | | | | | 20% | Separation | | | |
| 12.14 | Data Transmission Management for External Network | ● | | | | | 20% | Separation | O | 6 | 3.33 |
| 12.15 | Protection Measures for Information Storage at Work terminals | ● | | | | | 20% | Separation | | | |
| 12.16 | Implementing Information Storage at Work terminal information | ● | | | | | 20% | Separation | O | 8 | 3.73 |
| 12.17 | Establishing Auxiliary Storage Media Control Policy | ● | ● | ● | ● | ● | 100% | | | | |
| 12.18 | Complies with Auxiliary Storage Media Control Policy | ● | | | | | 20% | | O | 8 | 3.47 |
| 12.19 | Management of Printing Critical Document | ● | | | | | 20% | | | | |
| 12.20 | Complies with Printing Management Policy | ● | | | | | 20% | | O | 8 | 3.93 |
| 12.21 | Management of Removal Asset | ● | | | | | 20% | | O | 8 | 4.07 |
| 12.22 | Connection Work Terminal from External Network | ● | | | | | 20% | | O | 7 | 3.93 |

〈Table 3〉 Degree of Autonomy for the Employee's Security Role Items in Integrated Security Role Items(Continued)

| Area | Security Role Items | [1] | [2] | [3] | [4] | [5] | R/A | Add Items by Expert Investigation | Employee Role Items | Degree of Autonomy | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | Design | Verifica-tion |
| 12.23 | Mobile Device Security | ● | | | | | 20% | | O | 7 | 3.93 |
| 12.24 | Measures to protect the loss of work terminals and media | ● | | | ● | | 40% | | | | |
| 12.25 | Response to protect the loss of work terminals and media | | | | ● | | 20% | | O | 6 | 3.87 |
| 13. Prevention and Response Security Incident (10) | | | | | | | | | | | |
| 13.1 | Prevention Security Incident and Establishment Countermeasures System | ● | ● | ● | ● | ● | 100% | | | | |
| 13.2 | Check and Action for security vulnerabilities | ● | ● | ● | ● | ● | 100% | | | | |
| 13.3 | Monitoring and Analysis of Abnormal Activities | ● | ● | ● | ● | | 80% | | | | |
| 13.4 | Reporting Security Event by Security Management System | | ● | ● | ● | | 60% | Separation | | | |
| 13.5 | Reporting Security Event by Information System | | ● | ● | ● | | 60% | Separation | | | |
| 13.6 | Reporting Security Event by member | | ● | ● | ● | | 60% | Separation | O | 5 | 4.13 |
| 13.7 | Training and Improvement to Information Security Incident | ● | | ● | ● | | 60% | | | | |
| 13.8 | Response and Recovery to Information Security Incident | ● | ● | ● | ● | | 80% | | | | |
| 13.9 | Learning from Information Security Incident | | ● | ● | ● | | 60% | | | | |
| 13.10 | Collection of evidence | | ● | | | | 20% | | | | |
| 14. Business Continuity Security Management (3) | | | | | | | | | | | |
| 14.1 | Disaster Identification and Impact Analysis | | ● | ● | ● | | 60% | | | | |
| 14.2 | Establishment of Disaster Recovery System | ● | ● | ● | ● | | 80% | | | | |
| 14.3 | Test and Improvement of Disaster Recovery | ● | ● | ● | ● | | 80% | | | | |
| 15. Compliance (4) | | | | | | | | | | | |
| 15.1 | Complies with applicable legislation and contractual requirements | ● | ● | | ● | | 60% | | | | |
| 15.2 | Intellectual property rights | ● | ● | | ● | | 60% | | | | |
| 15.3 | Using of proprietary Software Products | ● | ● | | ● | | 60% | | O | 7 | 3.93 |
| 15.4 | Privacy and Personal Security | ● | ● | | | | 40% | | | | |

Note: [1] K-ISMS Certification Standard, [2] ISO/IEC 27001:2013, [3] NIST-SP 500-53 R4, [4] Critical Information Infrastructure Protection Technical Vulnerability & Analysis assessment Detailed guides, [5] SMEs Technical Protection Guide

## 5. 결 론

비즈니스의 패러다임이 빠르게 변화하고 복잡해지는 인터넷 비즈니스 환경에서 기업들은 생존하고 비즈니스 연속성을 유지하기 위해 민첩하고 기업구성원의 창의성과 자율성을 중요하게 여기는 조직문화로 개편하고 있다. 이에 따라 인터넷기업의 보안관리체계도 비즈니스의 환경과 조직문화 변화에 따라 새로운 보안관리체계로의 변화에 대한 필요성이 제기되고 있다.

따라서 본 연구는 인터넷기업에서 기존 보안조직 주도의 통제중심 보안관리체계의 한계를 극복하고 인터넷 비즈니스 환경과 조직문화에 적합한 기업구성원 자율중심의 보안관리체계에 관한 연구를 아래와 같이 진행하였다.

첫째, 정보보호에 대한 인증 및 점검 등의 목적으로 개발된 ISMS 정보보호관리체계 인증기준을 이행 주체별 역할에 따른 보안항목으로 분류하고, 이를 여러 보안관리체계의 지침 및 점검항목 등의 보안항목을 반영하여 통합 보안 역할항목으로 재구성하였다. 둘째, 전문가조사를 통해 통합 보안 역할항목 중에서 기업구성원이 이행해야 하는 기업구성원 보안 역할항목을 선정하였다. 셋째, 기업구성원 보안 역할항목 중에서 기업구성원의 자율을 통해 이행할 수 있는 기업구성원 자율 보안역할 항목을 선정하였다. 마지막으로, 선정된 기업구성원 자율 보안역할 항목에 대해 인터넷기업에 근무하는 보안전문가를 통해 기업구성원이 담당해야 하는 보안 역할항목 40개를 도출하고, 그중에서 기업구성원이 자율적으로 보안역할을 수행할 수 있는 26개 항목을 도출하여 기업구성원 자율중심의 보안관리 항목으로 개발하였다.

본 연구는 기존의 획일적인 통제중심의 보안관리체계에서 탈피하여 불확실성이 크고 급변하는 인터넷 비즈니스 환경을 고려한 기업구성원의 자율 개념을 도입하여 보안관리체계에 대한 학문적 연구영역을 확대했다는 점에서 의의가 있다. 또한, 인터넷기업을 비롯한 국내 여러 글로벌 기업 등에서 추진하고 있는 자율 기업문화에 적합한 보안관리체계 수립 및 운영을 위한 기초 자료를 제공한다는 점에서 실무적 활용도가 높다고 생각된다.

다만, 본 연구는 전문가조사 특성상 일반화하기 어려웠다는 한계를 지니고 있으며, 향후 양적 연구를 통한 연구 결과에 대한 보완이 필요하다. 또한, 기업구성원 자율중심의 보안관리체계 수립 및 적용을 위한 비즈니스 및 조직환경의 특성 등에 관한 연구가 필요한데 이와 같은 내용이 병행되지 못했으며, 이러한 환경에서 통제중심의 보안관리체계보다 기업구성원 자율중심의 보안관리체계가 어떤 측면에서 우위인지 확인하기 어려웠다.

이에 향후 연구에서는 인터넷기업에서 효과적인 자율 보안관리체계 수립 및 운영을 위한 기업의 환경적, 문화적 요인에 관한 연구가 필요하며, 추가적으로 자율중심의 보안관리체계의 효과성을 확인하기 위해 보안 자율성이 직무성과 및 보안 준수에 미치는 영향에 대한 실증적 연구가 필요하다고 하겠다.

## References

[1] Cha, I. H., “A study on the development of personnel security management for

protection against insider threat," The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 3, No. 4, pp. 210-220, 2008.

[2] Education Research Institute Seoul National University, Dictionary of the Terms of Education, 1994.

[3] Gartner, "Maverick research: Kill off security controls to reduce risk," Sep. 2012.

[4] Hackman, J. R. and Oldham, G. R., "Development of the job diagnostic survey," Journal of Applied Psychology, Vol. 60, No. 2, pp. 159-170, 1975.

[5] Huumonen, J., "Conceptualizing agility of enterprises," Human Factors and Ergonomics in Manufacturing & Service Industries, Vol. 21, No. 2, pp. 132-149, 2011.

[6] ISO/IEC 27001:2013, Information security -Security techniques-Information Security Management Systems-Requirements, ISO, 2013

[7] Jeffrey, D. W. and Paul, B. L., "Control-related motivations and information security policy compliance: The role of autonomy and efficacy," Journal of Information Privacy and Security, Vol. 9, No. 4, 2013.

[8] Kang, H. S. and Kim, J. D., "A study on information security departmentalization model," The Journal of Society for e-Business Studies, Vol. 20, No. 2, pp. 167-174, 2015.

[9] Kim, J. D., "Major issues and future strategies for information protection management paradigm shift," Review of KIISC, Vol. 23, No. 5, pp. 5-8, 2013.

[10] Kim, J. D., Kim, B. K., Park, S. H., and Kim, K. W., "Considerations for information protection innovation in a self-regulated environment," Review of KIISC, Vol. 25, No. 4, pp. 63-68, 2015.

[11] Kim, J. S., Kim, J. B., and Shin, Y. T., "A study on the effect of CISO's recognition of the role to the information security performance," Korean Management Consulting Review, Vol. 12, No. 4, pp. 21-34, 2012.

[12] Kim, K. W. and Kim, J. D., "A study on effects of implementing information security governance by information security committee activities," Journal of the Korea Institute of Information Security & Cryptology, Vol. 25, No. 4, pp. 915-920, 2015.

[13] Kim, S., "Internet business environment," e-Business Review, Vol. 3, No. 1, pp. 247-272, 2002.

[14] KISA, A Research on ISMS Maturity Level and Evaluation Methodology, 2010.

[15] Ko, E. J., Lee, S. J., and Kim, S. S., "Effects of job autonomy and self-efficacy on creative behavior: Focusing on the mediation effect of knowledge sharing in smart work environment," Knowledge Management Research, Vol. 19, No. 2, pp. 163-185, 2018.

[16] Lee, C. S., "A research on the revenue structure model for internet business," The Journal of Internet Electronic Com-

merce Research, Vol. 9, No. 3, pp. 93-113, 2009.

[17] Lee, J. K., Na, O. K., and Chang, H. B., "A study on the research security system of the researcher-centric," The Journal of Society for e-Business Studies, Vol. 23, No. 3, pp. 65-84, 2018.

[18] Lee, M. R. and Ju, S. H., "Policy suggestions for autonomy of university," CNU Journal of Educational Studies, Vol. 27, No. 1, pp. 69-93, 2006.

[19] McClure, M. L., "Managing the professional nurse: Part II. Applying management theory to the challenges," JONA: The Journal of Nursing Administration, Vol. 14, No. 3, 1984.

[20] Ministry of Science and ICT, Korea Internet & Security Agency, "Critical information infrastructure protection technical vulnerability & analysis assessment detailed guides," 2017.

[21] Ministry of Science and ICT, Ministry of the Interior and Safety, Korea Communications Commission and Korea Internet & Security Agency, Information & Personal Information management System Guidebook, 2019.

[22] Ministry of SMEs and startup and Korea Foundation for Corporation of Large Small Business, Rural Affairs, "SMEs Technical Protection Guide," 2018.

[23] Ministry of Trade, Industry and Energy, "White paper of trade, industry and energy(part of industry)," 2018.

[24] National Information Society Agency, "2017 Smart work survey report," 2017.

[25] Netflix Culture, Https://jobs.netflix.com/culture.

[26] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 R4)," 2013.

[27] Pfeffer, J., "The human equation: Building profits by putting people first," Harvard Business School Press, 1998.

[28] Rha, H. D., "A theoretical comparative study of human resource security based on Korean and int'l information security management systems," Journal of Convergence for Information Technology, Vol. 6, No. 3, pp. 13-19, 2016.

## 저 자 소 개

서현진 (E-mail: cordias@naver.com)
1999년 한림대학교 컴퓨터공학과 졸업
2001년 한림대학교 대학원 컴퓨터공학과 졸업
2018년 중앙대학교 융합보안학과 수료
2020년 네이버(주) Security Policy
관심분야 자율중심 보안, 보안 인식제고, 보안관리체계, 중소기업보안

김정덕 (E-mail: jdkimcau@gmail.com)
1979년 연세대학교 정치외교학과 (학사)
1981년 연세대학교 정치외교학과 (석사)
1986년 Univ. of S. Carolina, MBA
1990년 Texas A&M Univ., Ph. D. in MIS
1995년~ 중앙대학교 정보시스템학과 교수
2015년~현재 중앙대학교 산업보안학과 교수
관심분야 정보보호 거버넌스, 정보보호 관리, 디지털 비즈니스 보안