https://doi.org/10.33778/kcsa.2020.20.2.003

조직의 능동적 보안문화 형성을 위한 활성화 요인에 관한 연구★

안 병 구*, 유 하 랑**, 장 항 배***

요 약

급속하게 변화하는 ICT 기반의 산업 환경이 조성되면서 조직은 새롭게 발생하는 보안위협에 당면하고 있다. 조직은 보안위협에 대한 대응방안의 일환으로 조직구성원 대상의 보안문화 내재화를 수립하고자 하고 있다. 그러나 보안활동 이행으로 인해 업무 프로세스에서 발생하는 불편사항이 존재하고 기존의 보안문화 정립 방안은 제어, 통제 등의 규범적 성격이 강조됨에 따라 조직구성원들의 보안 수용성이 낮은 실정이다. 본 논문에서는 능동적인 조직 보안문화의 활성화를 하나의 대응방안으로 구축하기 위해 기존의 수동적인 보안문화 정립 방안에서 벗어나 전사적 보안업무 효율을 높고 조직구성원의 자발적 참여를 유도할 수 있는 보안문화를 형성하고자 하였다. 이에 따라 관련 선행연구 간의 비교·분석을 진행하고 도출된 실행요소에 대해 통계적 검증을 수행하였다. 본 연구에서 도출된 보안문화 활성화 요인을 통해 향후 보안문화 수준측정을 위한 연구에 기여할 수 있을 것으로 기대된다.

A Research on Activating Factor for Cultivating a Proactive Organizational Security Culture

Byunggoo Ahn*, Harang Yu**, Hangbae Chang***

ABSTRACT

Organizations are facing a new, diverse security threat as ICT based industrial environment arises. As a way of effective countermeasure for security threat, organizations are making an effort to establish internalization of security culture, targeting a organizational members. However, members' awareness toward security receptiveness is low as inconvenience exists in business process and existing security culture focuses on controlling and regulating. Accordingly, this research desires to develop a participatory security culture which can higher the efficiency of security work process and induce members' voluntary participation. A comparative analysis on security culture related prior researches is conducted and based on a drawn components, statistical verification is accomplished. It is expected to contribute on future research on measuring a security culture level.

Key words : Security culture, Security Level, Trust, Activating Factor

접수일(2020년 2월 26일), 게재확정일(2020년 3월 16일)

★ 이 논문은 2020년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임 (P0008703, 2020년 산업혁신인재성장지원사업)

* 중앙대학교 일반대학원 융합보안학과 박사
** 중앙대학교 일반대학원 융합보안학과 박사과정
*** 중앙대학교 산업보안학과 교수(교신저자)

1. 연구배경 및 필요성

산업환경이 끊임없이 변화함에 따라 인프라 산업 패러다임의 변화를 주도할 수 있는 신기술 확보 및 이에 따른 맞춤형 서비스 개발이 주목받고 있다[1]. 4차 산업혁명을 대표하는 핵심기술인 빅데이터, 사물인터넷(IoT), 클라우드 기반으로 새로운 가치창출이 가능한 ICT 기반의 융합 환경이 조성되면서 사이버 공간과 물리적 공간이 하나의 네트워크로 연결됨에 따라 ICT와 물리적 시스템이 연결되는 사이버-물리 시스템(Cyber-Physical System)이 나타나게 되었다. 이렇듯 새로운 생산 공정이 점차 발전하면서 조직은 내부정보 유출의 증가뿐만 아니라 외부의 침해공격 등의 다양한 보안위협을 당면하게 되었고 그 범위 또한 기존의 전통적인 보안범위에서 점차 확대되고 있다[2].

조직은 시장 경쟁력 유지 및 강화를 위해 신속하고 정확한 의사결정, 내부조직 결속 및 업무효율 향상 등의 방향으로 조직문화를 발전시키고자 하고 있다. 동시에 새로운 형태의 보안위협이 계속해서 발생하게 됨에 따라 조직 내 보안인식 제고를 위한 노력을 가하고 있다. 그럼에도 불구하고 현재 국내 기업 등 다양한 조직에 속한 조직구성원들은 보안활동이 개방된 업무환경 활동을 제한한다는 부정적 인식을 지니고 있는 상황이다. 이에 따라 조직구성원들의 내부 요구사항을 기반으로 전사적인 조직 업무효율을 향상시킬 수 있도록 하는 능동적 참여에 의한 보안문화의 정착이 필요하다. 이러한 보안문화는 발생 가능한 업무적 어려움을 해결함으로써 보안활동 이행에 대한 조직구성원들의 인식변화와 적극적인 참여를 이끌어내고 불편사항 해소로 인해 발생 가능한 보안 리스크를 최소화하는 대응방안을 구축하는 방향으로 발전해나가야 한다. 이를 위해 본 연구에서는 능동적인 보안문화 활성화 요인 도출을 위해 관련 선행연구 분석을 통한 실행요소 도출 및 통계적 검증을 수행하고자 한다.

2. 선행연구

2.1 이론적 개념

문화의 사전적인 개념은 '사회 전반의 생활양식'으로, 자연과 대립의 개념으로 자연적, 필연적으로 발생하는 자연을 소재를 기반으로 목적의식을 보유한 인간의 활동으로 실현되는 과정으로 정의되고 있다[3]. 또한 문화는 사회구성원에 의해 변화시켜온 물질적·정신적 과정의 산물로 조직 및 구성원들의 행동을 이루고 조직을 통해 학습 및 생성될 수 있다고 본다[4]. 사회의 생활양식으로써 문화는 한 조직의 구성원들로부터 공통적인 행동양식이 나타나는 공유성, 후천적 습득을 통한 학습성, 기존 문화에 새로운 문화가 더해지는 축적성, 시간의 흐름에 따라 끊임없이 변화하는 변동성, 문화 구성요소들이 서로 밀접한 관계를 갖는 총체성의 성격을 갖는다[5]. 이러한 문화적 성격을 기반으로 문화의 형성을 통해 조직구성원들의 행동양식이 수립될 수 있으며 이는 조직에 의해 후천적으로 학습될 수 있음을 알 수 있다.

정보보안문화의 형성은 컴퓨터와 네트워크가 지속적으로 발달함에 따라 정보보안 리스크에 대해 물리적, 기술적 성격의 대응만으로는 한계가 존재함을 인지함에 따라 정보보안에 문화적인 요소를 적용하며 시작되었다[6]. 정보보안문화 수립을 통한 정보보안 관리가 제시되면서 조직 내 정보보안문화가 효율적으로 형성되기 위해서는 정보보안 관련의 업무 프로세스의 목표, 구조와 조직구성원의 인식과 행동의 중요성이 강조되고 있다[7]. 또한 정보보안문화의 형성을 통해 조직구성원들로 하여금 정보보안 절차를 준수토록 함에 따라 정보시스템의 기밀성(confidentiality), 무결성(integrity), 가용성(availability)을 확보함으로써 조직 대상의 정보보안 위협 및 리스크를 사전적, 사후적으로 관리 및 조치할 수 있도록 한다[8]. 정보보안은 조직의 정책 수립, 업무 프로세스 등의 일상에서 문화적 변화를 전제한다고 봄에 따라 조직문화에 정보보안이 내포되어 있다고 보는 관점이 상당수를 이루고 있으며 문화적 관점에서의 정보보안에 대한 접근 동향은 점차 증가하고 있다[9].

조직문화는 조직의 관점에서 문화의 개념을 활용하고 있으며 조직 내에서 보유한 공유가치, 관습, 행동규범을 이른다[10]. 이는 특정 조직이 보유한 특성을 고유한 문화적 특성으로 하여 조직을 이해하고 평가하는 데에 있어 중요 요소가 된다. 기존의 사회학적 관점에서만 바라보던 문화의 개념을 조직의 관점에서

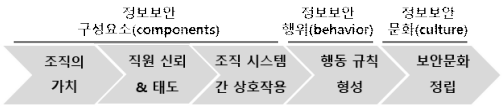
사용하면서 조직문화의 중요성이 강조되었고 조직 내 공유가치, 관습, 행동규범이 핵심 개념으로 제시되고 있다[11]. 조직문화의 기능은 업무 효과성을 증대시킨다는 점과 조직 결속력과 응집력의 강화를 통해 조직 공동의 목표 달성을 야기한다는 점을 가진다[12]. 이러한 조직문화 성격을 기반으로 조직문화의 강화를 위해 구성요소들의 일관성과 상호적으로 연결되는 관계 유지가 필요함을 확인하였다.

보안문화는 데이터, 정보, 지식의 보호에 기여하는 조직구성원의 행동으로 정의되고 있다[4]. 또한 보안문화는 조직구성원들의 활동과 의식에 보안인식이 내재화됨으로써 전사적 업무 과정에 있어 보안업무가 포함되어야 한다[12]. CPNI(Centre for the Protection of National Infrastructure)에 의하면 보안문화는 보안에 대해 조직구성원이 가지는 인식으로, 인간의 모든 이익에 위험이 되는 것을 줄이는 데에 집중화·활성화된 개방적이고 신뢰를 기반으로 한 환경을 구축하는 것이라고 정의하고 있다.

선행연구를 통해 살펴본 정의들을 바탕으로 본 연구에서는 문화는 조직이 가진 신념, 가치, 규범 등을 형성하며 조직구성원들의 행동양식을 이루는 것으로 파악한다. 정보보안문화는 효과적인 보안위협 대응방안과 정보보안 인식제고를 위해 사회심리학적 원리가 적용된 문화적 요소로 이루어진 문화 환경으로, 정보기술 위협에 대한 예방 및 조치의 문화적 접근을 의미한다. 조직문화에 대한 조작적 정의는 조직과 조직구성원들이 형성한 공유가치, 관습, 행동규범으로 한다. 보안문화는 조직이 지속성장하기 위해 조직구성원들이 채택한 보안에 대한 가치, 태도, 행동으로 정의하며, 자격제도 등의 연구가 포함되어야 한다.

2.2 보안문화 형성과정

현재 실제 현장에서는 보안문화가 정보보안 성격 중심으로 형성되면서 수동적인 보안문화가 대다수를 이루고 있다. 수동적 보안문화는 아래 (그림 1)과 같이 조직 내 정보보안 구성요소들이 조직구성원들의 행동에 영향을 미치면서 형성된다[13]. 이때 조직구성원들은 보안 정책의 적용 대상으로 분류되어 보안 규범이 수립됨에 따라 통제 중심의 교육훈련을 통한 보안문화가 형성되면서 조직구성원들은 보안활동을 하나의 추가 규범으로 인식하게 된다. 또한 기존의 선행연구들에서 나타난 정보보안 기반의 보안문화 형성과정은 보안위협에 대한 예방 및 대응방안을 마련하는 것을 목적으로 함에 따라 조직구성원 대상의 일방향적(one-way) 문화 형성이라는 한계점을 지닌다.



(그림 1) 수동적 보안문화 형성과정

ICT 기술발달과 함께 보안의 범위가 확장됨에 따라 기술중심에서 나아가 인간중심으로 한 조직구성원 대상의 능동적 보안문화가 구축되어야 한다. 이에 따라 본 논문에서는 수동적인 보안문화에서 벗어나 조직문화 일환으로서의 보안문화 활성화를 위한 요인을 도출하고자 한다. 보안문화의 형성과정은 기존의 선행연구가 활성화되지 않음에 따라 조직문화와 정보보안문화 형성과정을 포함한 선행연구 분석을 통해 조직과 조직구성원의 보안행동에 영향을 미치는 구성항목 및 실행요소를 도출하고자 하였다.

2.3 보안문화 선행연구 분석

보안문화와 관련한 이론적 개념을 기반으로 <표 1>과 같이 나타난 총 9개의 관련 선행연구를 분석하고자 하였다[14-22]. 추가적으로 조직문화와 정보보안문화의 실행요소 간 비교·분석을 통해 확장된 보안문화의 구성항목과 실행요소를 도출하였다.

<표 1> 보안문화 선행연구

분류	선행연구
1	Security Culture(2015)
2	A Comprehensive Framework for Cultivating and Assessing Information Security Culture(2017)
3	A framework of information security culture change(2014)
4	A Conceptual Model for Cultivating an Information Security Culture(2015)

5	Design and Validation of Information Security Culture Framework(2015)
6	Creating, Maintaining and Managing an Information Security Culture(2013)
7	Security Cultures in Organizations : A Theoretical Model(2006)
8	Understanding and measuring information security culture in developing countries(2012)
9	Cultivating and assessing information security culture(2008)

Walton[14]은 조직의 장기적 성공에 있어 중요한 보안 인식을 향상시키기 위해 보안문화의 중요성을 강조하였으며 이를 위해 보안 관련 데이터의 조합 및 분석을 개선할 것을 주장하였다. 또한 경영진의 지원과 참여가 보안문화 수립에 있어 성공적인 수행과 추가적인 후속 조치 진행에 있어 중요함을 강조하였다. 이때 보안문화의 추가적인 기능으로 보안문화 및 인적 리스크 평가를 수행함으로써 전사적 조직 시스템과 통합해 자원의 중복을 예방할 수 있다고 주장하였다.

Tolah[15]의 연구에서는 조직행동의 요소로 조직구성원의 직무 만족, 개인적 특성을 꼽으며 정보보안문화에 영향을 주는 인자를 최고경영층, 보안정책, 정보보안 교육훈련 수행, 리스크 평가, 조직구성원들의 윤리적 행동을 주장한다. 이를 기반으로 보안문화가 수립될 시 조직에는 보안인식 제고, 보안 주인의식이 형성됨을 제시한다.

AlHogail[16]은 조직구성원들이 정보보안과 관련한 보안활동 수행에 있어 부정적 인식을 극복하기 위해서는 조직 변화관리가 중요함을 주장한다. 이를 위해 요구되는 보안문화 수립은 조직구성원 간 자유로운 소통, 동기부여, 조직구성원의 의사결정권 부여 등에 따라 긍정적 변화 및 구성원 참여를 유도할 수 있음을 주장한다. 또한 경영층 및 조력자에 의한 보안인식 및 이해를 향상시킴으로써 조직구성원의 조직만족도와 충성도를 향상시킬 수 있음을 주장한다. 이때 조직구성원의 보안 업무 프로세스 있어 요구사항을 수용 및 조정하는 작업을 수행하고 변경 필요 시 피드백과 이에 따른 조직구성원의 반응에 대한 관리 중요성을 강조하고 있다.

Sherif[17]의 연구에서는 정보보안문화 수립, 유지 및 발전을 위해 세 단계에 걸쳐 정보보안문화의 육성 모델을 제시하고 있다. 이와 함께 효과적인 보안문화의 수립은 조직구성원 개인의 의사결정을 어떻게 효율적으로 증진시킬 수 있는지에 의존된다고 주장한다. 이와 함께 보안 정책 및 규범 수립, 조직구성원의 보안활동 및 윤리적 행위, 조직 특성을 반영한 문화적 변화와 보안 프로세스의 중요성을 제시한다. 특히 조직구성원의 보안 인식 제고와 교육 프로세스에 있어 경영층의 적극적인 후원과 참여를 강조하고 있다.

AlHogail[18]의 연구에서는 조직 내 보안문화 형성을 위해 요구되는 다양한 실행항목을 제시하고 있다. 먼저 조직구성원의 보안 행동 및 활동에 영향을 주는 법률 및 규정 등과 같은 외부적 요인에 대해 고려가 되어야 하며 조직구성원은 윤리적 행위에 대해 인지하고 있어야함을 주장한다. 더불어 조직구성원 대상의 보안 교육을 통해 효율적인 보안 행동을 수립해야 하며 보안 자체에 대한 불만·불편의 완화를 통해 향후 발생 가능한 변화사항에 대해 조직구성원이 긍정적인 태도를 유지할 수 있도록 해야 함을 강조하였다. 또한 보안전략은 보안 정책, 목적 등의 보안 요소 시행과 관련되고 조직구성원 대상으로 접근하는 정책이 명확하고 명료하게 수립됨에 따라 보안 업무 프로세스에 있어 불편을 완화할 수 있음을 주장한다. 이러한 사항에 대해 보안가이드라인을 활용함으로써 조직구성원들의 신뢰를 향상시킬 수 있으며 경영층을 포함한 전체 조직구성원 간의 소통채널(communication channel)을 구축함으로써 보안 인식에 대한 긍정적 향상과 거부감 완화가 가능함을 주장한다.

Fagerström[19]은 정보보안문화 수립, 유지 및 관리에 있어 조직구성원이 공유하는 신념과 가치로 이루어진 특정문화 유형에 따라 정보보안문화의 수준을 네 단계로 구분하고 있다. 또한 정보보안문화 구축에 있어 보안정책과 가이드라인, 교육 및 훈련과 데이터 프로세싱 보호, 재난 대응 및 복구 등의 중요성을 강조하고 있다. 이때 인간중심의 조직구성원 관리를 위한 규정준수에 대해서는 보안정책, 보안 업무 프로세스, 운영, 모니터링 및 피드백 관리, 유지보수 및 향상의 PDCA 순환모델의 활용을 제안하면서 체계적으로 구조화된 정보보안문화 관리를 위해서는 인간중심의

행위가 고려되어야함을 강조하고 있다.

Ramachandran[20]의 연구에서는 조직 내 보안문화가 형성되기 위한 이론적 모델과 함께 관련 구성항목을 제시하고 있다. 효과적인 보안문화가 형성되기 위해서는 조직구성원의 행동이 보안과 관련한 신념 및 행동으로 인해 발생하는 보상과 보안활동을 수행함으로써 얻는 실제 조직 생산성으로부터 비롯됨을 주장한다. 나아가 보안에 대한 신뢰도는 조직구성원의 보안 인식제고 정도와 준수 정도에 따라 영향을 받는다고 주장한다. 이때 조직에서 수립된 보안정책 및 규범, 교육은 조직구성원들에게 보안의 필요성에 대한 긍정적 인식과 호의적인 신념을 갖게 하며 이러한 신념은 선순환으로 보안 정책, 보안 표준, 보안 교육 및 훈련 등에 긍정적 영향을 미쳐 보안 준수 정도를 향상시킬 수 있음을 주장한다.

Alnatheer[21]는 보안문화를 이루는 요인으로 보안 인식과 보안 주인의식(Ownership)을 제안하고 있다. 또한 보안문화는 조직구성원의 보안 인식 단계에서 한 단계 향상된 상태로, 보안 인식 제고, 지식 및 능력은 체계적인 보안문화 형성을 위한 기반을 이룬다고 주장하며 특히 보안 교육을 통해 윤리적 행동 제고와 보안 인식 수준을 향상시켜 보안문화 형성에 일조할 수 있음을 강조하였다. 또한 보안 주인의식을 보유함으로써 보안 활동에 대한 중요성과 책임을 인지하고 개인의 어떠한 행위가 보안 리스크를 야기할 수 있는지 이해할 수 있음에 따라 조직구성원의 보안 주인의식의 중요성을 강조하고 있다.

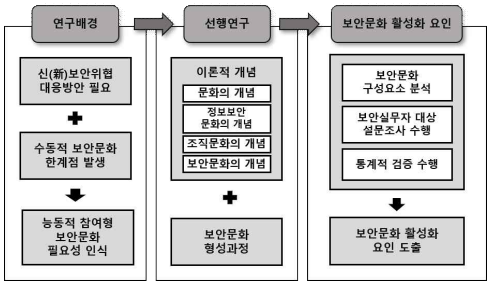
Veiga[22]는 경영진의 후원과 조직구성원들의 역할 및 책임을 명확히 구분함으로써 조직 내 보안문화 수준을 향상시킬 수 있다고 주장하였다. 이에 따라 경영층의 지원이 가능한 보안 정책, 규범, 표준이 요구되며 조직구성원 대상의 보안 인식, 교육 프로그램 진행을 통해 보안 환경에 대한 신뢰를 향상할 것을 주장한다. 또한 조직구성원 대상의 보안 프로그램이 효율적으로 운영되고 있는지에 대한 피드백 및 관리를 위해 보안 준수 정도 측정 및 지속적인 모니터링과 감사의 필요성을 강조하고 있다.

3. 보안문화 활성화 요인 도출

3.1 연구방법론

본 연구에서는 변화하는 산업환경 속성에 발맞추어 조직의 지속성장을 이끌 수 있는 보안문화 설립을 목적으로 한다. 현재 조직이 가지는 수동적 보안문화의 한계점을 수동적 보안문화 한계점을 인식하여 조직구성원들이 능동적으로 참여할 수 있는 조직문화 일환으로써의 보안문화 형성에 대한 필요성을 인지하였다.

이를 위해 먼저 보안문화 관련 문헌에 대한 수집 및 분석을 통해 실행요소 문항을 도출하고 이에 대한 통계적 검증을 수행하였다. 해당 연구추진 방법을 도식화하면 아래 (그림 2)와 같다.



(그림 2) 보안문화 활성화 요인 도출을 위한 연구방법론

3.2 구성요소

조직구성원의 자발적 참여형 보안문화를 정립하기 위해 관련 선행연구들을 기반으로 실행요소들을 도출하고자 하였다. 앞서 수행한 선행연구 분석을 기반으로 도출한 총 7개의 구성항목과 31개의 실행요소를 구성하여 조직문화의 인적 실행요소와 정보보안문화 실행요소를 추가하여 조직 전체를 대상으로 하는 확장된 보안문화 구성항목과 실행요소를 도출하였다. 아래 <표 2>에서는 총 9개의 선행연구를 기반으로 조직문화와 정보보안문화 형성 과정에서 발생하는 구성항목 및 실행요소를 도출한 것을 보여준다. 이를 기반으로 각 구성항목과 실행요소에 대한 통계적 검증 수행을 위해 설문조사를 수행하였다. 설문조사는 국내 기업 보안담당자를 대상으로 진행하였으며 특정 분야에 한정되지 않도록 근무 경력, 업종, 연령대의 범위를 제한하지 않고 설문조사를 진행하였다.

<표 2> 자발적 조직 보안문화 활성화 요소 도출을 위한 선행연구 분석 결과

구성항목	실행요소
사용자 보안 관리	고객관리와 피드백
	개인정보와 사생활 보호
	교육 훈련
	윤리 행위
	직원 인식
직원참여와 주인의식	직무 만족
	성격 특성
	신뢰
	보안 불편 해소
	소통
리더쉽과 거버넌스	리스크 관리
	투자 회수율
	거버넌스
	후원(sponsorship)
	전략
보안정책	정책
	절차
	표준
	모범사례
	인증(certification)
	지침(guideline)
보안관리와 운영	프로그램 조직
	법률과 규정
보안프로그램 관리	준수(compliance)
	모니터링과 감사
기술 보호와 운영	보안 자산 관리
	보안 시스템 개발
	기술적 운영
	물리적 환경적
	보안사고 관리
	비즈니스 지속성 관리(BCP)

3.3 통계적 검증

선행연구에서 도출된 31개의 실행요소에 적합타당성 검증에 있어서는 3.5 ~ 3.9의 평균값(타당성)을 'Weak level'로, 평균값 4.0 이상의 값을 'Good ~ Excellent level'를 구분함에 따라[19] 아래 <표 3>과 같이 4.0 미만의 값을 도출한 11개의 실행요소는 탈락되었으며 20개의 실행요소가 도출되었다.

<표 3> 보안문화 실행요소별 적합타당성 검증 결과

기술통계량		
실행요소	평균	표준편차
고객관리와 피드백	4.64	.486
개인정보와 사생활 보호	4.13	.711
교육 훈련	4.45	.503
윤리 행위	4.32	.594
직원 인식	4.45	.544
직무 만족	3.77	.937
성격 특성	3.81	.770
신뢰	4.11	.787
보안 불편 해소	4.02	.821
소통	4.04	.833
리스크 관리	4.06	.845
투자 회수율(ROI)	3.53	1.080
거버넌스	4.17	.702
후원	4.68	.663
전략	4.15	.780
정책	4.06	.845
절차	3.87	.741
표준	4.02	.847
모범사례	3.77	.960
인증	3.60	.970
지침	3.87	.850
프로그램 조직	4.23	.813
법률과 규정	4.17	.732
준수	4.45	.717
모니터링과 감사	4.53	.546
보안 자산 관리	3.74	.943
보안 시스템 개발	3.98	.897
기술적 운영	3.91	.855
물리적 환경적	4.09	.717
보안사고 관리	4.17	.816
비즈니스 지속성 관리(BCP)	3.81	.924

본 연구에서 도출한 20개의 보안문화 활성화 실행요소에 대해 요인분석을 수행하였다. 이때 실행요소인 '소통(communication)'의 요인적재량이 0.35로 도출

되어 기준 0.4 이상을 충족하지 못해 실행요소는 19개로 최종 도출되었다. 이를 기반으로 요인분석을 한 결과 아래 <표 4>와 같이 7개의 요인으로 형성됨을 볼 수 있다.

<표 4> 보안문화 실행요소 요인분석 결과

실행요소	1	2	3	4
신뢰	0.843	-0.088	-0.057	-0.02
보안 불편 해소	0.665	0.084	0.015	0.282
후원	0.623	0.341	0.295	0.182
거버넌스	0.595	-0.113	0.344	0.04
상시 모니터링과 감사	-0.088	0.77	0.012	-0.028
프로그램 조직	-0.131	0.632	0.127	0.439
고객관리와 피드백	0.187	0.626	0.001	0.044
교육 훈련	0.123	-0.103	0.813	0.197
윤리 행위	0.021	0.37	0.651	0.077
개인정보와 사생활 보호	-0.054	0.05	0.603	0.006
직원 인식	0.31	0.104	0.486	0.103
법률과 규정	0.108	0.07	0.157	0.857
표준	0.142	0.094	0.067	0.635
법규 준수	0.363	0.388	0.309	0.475
리스크 관리	0.213	0.149	0.128	0.124
전략	0.111	0.222	0.146	0.091
정책	0.373	0.479	0.151	0.121
보안사고 관리	0.15	0.143	-0.056	0.073
물리· 환경적	-0.016	-0.023	0.173	0.211

실행요소	5	6	7
신뢰	0.081	0.056	0.173
보안 불편 해소	0.352	-0.072	-0.245
후원	-0.303	-0.079	0.147
거버넌스	0.216	0.287	0.094
상시 모니터링과 감사	-0.126	0.04	0.225
프로그램 조직	0.104	0.034	0.023
고객관리와 피드백	0.283	0.161	-0.138
교육 훈련	-0.033	-0.007	-0.047
윤리 행위	0.217	-0.063	0.039
개인정보와 사생활 보호	0.335	0.43	0.093
직원 인식	-0.208	0.384	0.147
법률과 규정	-0.047	0.137	0.081
표준	0.408	0.047	0.387
법규 준수	0.275	0.164	0.034
리스크 관리	0.827	0.008	0.191
전략	0.089	0.773	0.052
정책	0.18	0.513	0.204
보안사고 관리	-0.02	-0.009	0.877
물리· 환경적	0.387	0.069	0.657

요인분석을 통해 도출된 7개의 요인에 따른 19개의 보안문화 활성화 요인과 관련해 신뢰도 계수(Cronbach Alpha)를 활용해 신뢰도를 분석하였다. 신뢰도 값은 아래 <표 5>와 같이 도출되었다. 분석결과 '보안사고 관리', '물리·환경적'으로 구성된 요인은 0.588의 값으로 0.6미만(Cronbach Alpha 0.6 이상 수용)으로 탈락되어, 최종적으로 보안문화 활성화 요인은 6개의 요인과 17개의 실행요소를 가지는 것으로 도출되었다.

<표 5> 보안문화 실행요소 신뢰도 분석 결과

실행요소	신뢰도 계수
신뢰	0.716
보안 불편 해소	
후원	
거버넌스	
상시 모니터링과 감사	0.606
프로그램 조직	
고객관리와 피드백	
교육 훈련	0.673
윤리 행위	
개인정보와 사생활 보호	
직원 인식	
법률과 규정	0.74
표준	
법규 준수	
리스크 관리	-
전략	0.732
정책	
보안사고 관리	0.588
물리· 환경적	

신뢰도 분석을 통해 수용 가능한 것으로 도출된 17개의 실행요소 명칭과 세부 설명은 선행연구를 기반

으로 아래의 <표 6>과 같이 정리하였다. ‘상호 신뢰’란 조직구성원들의 조직 및 조직 내 보안문화에 대한 신뢰로, 조직의 경영층은 보안 정책 준수를 위해 조직구성원들을 신뢰하고 조직구성원들은 보안 활동에 대한 책인 인식 및 경영진에 대한 신뢰를 보유해야 한다.

‘보안 불편 해소’는 조직 내 업무 효율 향상을 위한 보안 관련의 불편사항 해소 및 수용을 뜻한다.

‘후원’은 보안문화에 대한 경영층의 지원 및 후원을 의미하며 이때 후원자(sponsor)는 보안을 의제 항목으로 제시하도록 한다. ‘거버넌스’란 보안 불편사항 해소 및 리스크 대응방안에 대한 경영층의 수용체계이며 ‘상시 모니터링과 감사’는 보안 관련 규정 준수에 대한 모니터링 및 감사를 의미한다. 이때 조직은 자체 규정 준수 여부, 사용자 준수여부를 모니터링 해야 한다.

‘프로그램 조직’이란 보안 조직 설계, 구성 및 보고 등의 보안 프로그램을 수행하는 조직 활동을 의미한다. ‘고객관리와 피드백’은 보안에 대한 홍보와 보안 위반 모니터링 사례 및 결과를 통해 피드백을 수행하여 미래에 발생 가능한 문제 재발을 방지하는 것을 의미한다.

‘교육 훈련’은 조직구성원 대상의 보안 교육 및 훈련을 통한 보안 향상을 의미하며 이때 모든 조직구성원을 대상으로 보안 정책, 절차 등에 대한 인식 제고 및 교육을 정기적으로 진행해야 한다.

‘윤리적 행위’란 조직 구성원들의 윤리적 행동을 통해 옳거나 잘못된 것을 구별하는 가치와 규칙을 의미한다. ‘개인정보와 사생활 보호’란 보안의 대상이 되어야 하는 고객 및 조직구성원들의 개인정보 및 사생활에 대한 보호로, 조직에서는 대상의 보호를 위해 적절한 통제가 마련되어 있는지 확인해야 한다.

‘직원 인식’은 조직구성원들의 보안 생활화 등을 통한 보안 인식(awareness)을 의미한다. ‘법률과 규정’은 조직이 보안 업무를 수행하기 위해 필요한 보안 관련 법률과 규정으로, 다양한 국내 및 국제법을 포함해야 한다.

‘법규 준수’는 보안 정책을 준수(compliance)하고 시의적절한 대응 구축을 위해 보안 규정의 준수 및 시행이 고려된다. ‘리스크 관리’란 보안 리스크 발생에 따른 대응방안 관리로 리스크 관리 평가 및 통제가 포함된다.

‘전략’이란 보안문화에 대한 조직의 전사적 전략 수립을 의미하며 이때 전략은 조직의 경영목표의 달성을 위해 조직 전체의 전략과 연관되어야 한다.

마지막으로 ‘정책’이란 보안문화 전략을 기반으로 조직의 전사적 정책을 수립하는 것으로 조직의 보안에 대한 의도와 방향을 의미한다.

<표 6> 보안문화 활성화를 위한 실행요소 정리

실행요소	개념정리
상호 간 신뢰	조직과 보안문화 정책에 대한 조직구성원들의 신뢰
보안 불편 해소	조직구성원들의 보안 관련 불편사항 해소 및 수용
후원	경영층의 보안문화 지원 및 후원
거버넌스	수렴된 보안 불편사항 해소 및 리스크 대응방안 등에 대한 경영층의 수용체계
상시 모니터링과 감사	보안 규정 준수에 대한 모니터링 및 감사
프로그램 조직	보안 프로그램을 수행하는 조직 활동
고객관리와 피드백	보안에 대한 조직구성원의 홍보 및 보안 위반 사항에 대한 모니터링수행
교육 훈련	지속적인 보안 교육 및 훈련을 통한 조직 보안 향상 효과
윤리적 행위	윤리적 행동 수행을 통해 옳고 그름을 구별하도록 하는 가치와 규칙
개인정보와 사생활 보호	보안 업무 과정 중 보호 대상이 되어야 하는 고객 및 조직구성원의 개인정보 및 사생활 보호
직원 인식	보안 생활화 등을 통한 조직구성원들의 보안 인식
법률과 규정	보안 업무 수행을 위한 보안 관련 법률 및 규정
표준	보안 정책 수립을 위한 보안 표준화
법규 준수	보안문화 정책 수립을 위한 관련 규제 및 법률 준수
리스크 관리	보안 리스크 대응방안에 따른 관리
전략	보안문화에 대한 전사적 전략 수립
정책	보안문화 전략 기반의 전사적 정책 수립

통계적 검증 수행에 의해 재구성된 첫 번째 요인은 조직구성원 간 신뢰를 바탕으로 업무 프로세스 등에서 발생 가능한 보안 불편사항 해소를 위해 경영층과의 소통이 영향을 주는 것을 의미함에 따라 요인의 명칭을 '참여와 주인의식'으로 정의하였다. 해당 요인은 '상호 간 신뢰', '보안 불편 해소', '후원', '거버넌스'의 총 네 개의 실행요소를 포함한다.

두 번째 요인은 '상시 모니터링과 감사', '프로그램 조직', '고객관리와 피드백'의 총 세 개 실행요소로 구성된다. 해당 요인은 조직구성원의 보안 불편사항 해소에 따른 자율성 및 개방성 확대에 따라 조직에서 보완 조치의 일환으로 수행하는 상시 감사 및 모니터링을 위한 시스템, 운영부서와 모니터링 결과 및 이에 따른 피드백을 내포함에 따라 요인의 명칭을 '상시 감사 및 피드백'으로 나타내었다.

세 번째 요인은 '교육훈련', '윤리 행위', '개인정보와 사생활 보호', '직원 인식'의 네 가지 실행요소를 포함한다. 이는 조직구성원을 대상으로 수행한 보안 교육훈련을 통해 개인정보 및 사생활 보호, 윤리적 행동 수행 등에 기반한 조직구성원의 인식 제고를 의미함에 따라 '보안 인식 제고'로 명명하였다.

'법률과 규정', '표준', '법규 준수'의 실행요소로 묶인 요인은 보안문화를 뒷받침하는 법률과 규정을 인지하고 보안 표준 및 준수의 의미를 가짐에 따라 '보안 법규와 준수'로 나타내었다.

'보안 리스크 관리'로 명명된 다섯 번째 요인은 조직구성원이 겪는 보안 불편의 해소와 업무 프로세스 향상 등에 의한 사내외 보안 위협에 의한 리스크 대응 방안 수립 및 관리를 위한 단일 실행요소로 구성되어 있다.

마지막 요인은 '전략'과 '정책'의 실행요소를 포함하며 조직의 장기적이고 지속가능한 경영과 기술변화에 의한 조직 전략 및 정책 수립의 보안문화 방향 설정을 의미함에 따라 해당 요인의 명칭을 '보안 전략과 정책'으로 정하였다.

최종 도출된 6개의 요인과 17개의 실행요소는 아래 <표 7>과 같이 정리할 수 있다.

<표 7> 최종적으로 도출된
보안문화 활성화 요인과 실행요소

요인	실행요소
참여와 주인의식	상호 간 신뢰
	보안 불편 해소
	후원
	거버넌스
상시 감사 및 피드백	상시 모니터링과 감사
	프로그램 조직
	고객관리와 피드백
보안 인식 제고	교육 훈련
	윤리 행위
	개인정보와 사생활 보호
	직원 인식
보안 법규 및 준수	법률과 규정
	표준
	법규 준수
보안 리스크 관리	리스크 관리
보안 전략 및 정책	전략
	정책

4. 결론

융·복합 환경에서 끊임없이 변화하는 산업 패러다임과 새롭게 발생하는 다(多)차원의 보안 위협은 조직으로 하여금 신속한 대응방안을 마련하도록 촉진함에 따라 조직 내 경영층은 보안활동 수행에 상당한 노력을 가하고 있다. 그러나 실무 현장에서는 보안활동 이행에 대해 조직구성원이 불만을 표출하거나 인식 자체가 결여되는 상황이 지속적으로 나타나고 있음에 따라 조직구성원의 자발적 참여를 위한 효율적 보안문화 정립을 위한 보안문화 활성화 요인을 도출하고자 하였다. 이를 위해 보안문화와 관련한 선행연구의 수집 및 분석을 통해 보안문화 정립을 위한 실행요소를 도출하여 설문조사를 수행하였다. 설문조사 결과를 바탕으로 적합타당성 검증과 요인분석을 수행하였다.

본 연구는 조직별로 형성되는 다양한 조직문화를 고려하지 못했다는 한계점을 지닌다. 향후 연구에서는 설문조사 표본 수 및 근무 분야의 수를 늘리고 조직 보안문화의 수준측정에 대한 연구가 진행되어야 할

것이다.

참 고 문 헌

[1] 삼정KPMG 경제연구원, “4차 산업혁명과 패러다임”, 삼정 인사이트, 2018.

[2] 장항배, “미래산업융합 환경과 보안과제”, 한국IT서비스학회 춘계학술대회, pp. 339-343, 2016.

[3] Kroeber, A. L., & Kluckhohn, C, “Culture: a critical review of concepts and definitions.” Peabody Museum of Archaeology & Ethnology, Harvard University, Vol. 47, No. 1, 1952.

[4] Dhillon, G, “Managing Information System Security”, 1997.

[5] 정철현, ‘문화정책록’, 서울경제경영, 2004.

[6] Thomson, M, E, Solms, R, V, “Information security awareness: educating your users effectively”, Information Management & Computer Security, Vol. 6, No. 4, pp. 167-173, 1998.

[7] Niekerk, J, F, Solms, R, “Information Security Culture: a management perspective”, Computers and Security, Vol. 29, No. 4, pp. 476-486, 2010.

[8] 정해철, 김현수, “조직구성원의 정보보안 의식과 조직의 정보보안 수준간의 관계 연구”, 정보기술과 데이터베이스 저널, Vol. 7, No. 2, pp. 117-134, 2000.

[9] 이미정, 이선중. “지방공무원의 정보보호 인식 및 행태에 관한 연구”, 한국사회와 행정연구, Vol. 20, No. 4, pp. 453-478, 2010.

[10] Pettegrew, A, M, “On studying organizational culture”, Administrative Science Quarterly, Vol. 24, pp. 570-581, 1979.

[11] Schultz, M, Hatch, M, J, “Living with Multiple Paradigms the Case of Paradigm Interplay in Organizational Culture Studies”, Academy of Management Review, Vol. 21, No. 2, pp. 529-557, 1996.

[12] Thomson, K, L, Solms, R, von, Louw, L, “Cultivating an organizational information security culture”, Computer Fraud & Security, Vol. 6, No. 4, pp. 7-11, 2006.

[13] Veiga, A, D, Eloff, J, H, P, “A framework and assessment instrument for information security culture”, Computers & Security, Vol. 29, pp. 196-207, 2010.

[14] Walton, H, “Security Culture”, Routledge, 2015.

[15] Tolah, A, Furnell, S, S, Papadaki, M, “A Comprehensive Framework for Cultivating and Assessing Information Security Culture”, HAISA, pp. 52-64, 2017.

[16] Alhogail, A, Mirza, A, “A framework of information security culture change”, Journal of Theoretical and Applied Information Technology, Vol. 64, No. 2, pp. 540-549, 2014.

[17] Sherif, “A Conceptual Model for Cultivating an Information Security Culture”, 2015.

[18] AlHogail, “Design and Validation of Information Security Culture Framework”, 2015.

[19] Fagerström, A, “Creating, Maintaining and Managing an Information Security Culture”, KPMG Finland, 2013.

[20] Ramachandran, S, Rao, S, “Security Cultures in Organizations: A Theoretical Model”, AMCIS 2006 Proceedings, pp. 3460-3464, 2006.

[21] Alnatheer, M, A, “Understanding and measuring information security culture in developing countries: case of Saudi Arabia”, Queensland University of Technology, 2012.

[22] Veiga, A, D, “Cultivating and assessing information security culture”, University of Pretoria, 2008.

〔저자소개〕

안 병 구 (Byunggoo Ahn)

2019년 2월 중앙대학교
융합보안학과 박사

email : bgahn0405@naver.com

유 하 랑 (Harang Yu)

2020년 3월 중앙대학교
융합보안학과 박사과정

email : hryu356@cau.ac.kr

장 항 배 (Hangbae Chang)

2006년 2월 연세대학교
정보시스템관리 박사
2014년 3월~ 현재
중앙대학교 산업보안학과 교수

email : hbchang@cau.ac.kr