https://doi.org/10.14400/JDC.2017.15.8.137

사이버 레질리언스 평가지표 개발에 관한 연구

김수진*, 김정덕**
중앙대학교 융합보안학과 석사과정*, 중앙대학교 산업보안학과 교수**

A Study on Developing Assessment indicators for Cyber Resilience

Sujin Kim*, Jungduk Kim**
Dept. of Security Convergence, The Graduate School of Chung-Ang Univ*
Dept. of Industrial Security, The College of Business & Economics of Chung-Ang Univ**

요 약 사이버 위협이 고도화 및 지능화됨에 따라 사이버 보안 사고를 사전에 완벽하게 예방하는 것은 한계가 있다. 따라서 보안사고 발생을 가정하고 이를 신속하게 탐지하고, 복구할 수 있는 역량이 필요해지고 있다. 이러한 필요성으로 인해 최근 사이버 레질리언스는 중요한 개념으로 부각되고 있으며, 이에 대한 수준을 평가하는 것은 중요하다. 그럼에도 불구하고, 현재 사이버 레질리언스와 관련 평가에 관한 연구는 미흡한 실정이다. 따라서 본 연구에서는 사이버 레질리언스에 대한 이론적 고찰과 전문가 회의를 통해 사이버 레질리언스를 평가할 수 있는 총 22개의 지표를 개발하였다. 개발된 지표는 포커스 그룹 인터뷰를 통해 제안된 지표의 중요도와 실현가능성을 평가하였다. 본 연구는 사이버 레질리언스를 평가함에 있어 의미 있고 유용한 지표를 도출하였다. 이는 향후 사이버 레질리언스 연구의 기반 자료로 활용될 것으로 기대되며, 향후 연구로는 실무적 활용 및 객관화를 위한 정량적 연구를 제안한다.

주제어 : 사이버 레질리언스, 사이버 보안, 보안 평가 지표, 보안 위험관리, 보안 대책

Abstract Recently, cyber resilience has emerged as an important concept, recognizing that there is no perfect security. However, domestic researches on cyber resilience are insufficient. In this study, the 22 indicators for cyber resilience assessment were initially developed by the literature survey and discussions with security experts. The developed indicators are reviewed using the Focus Group Interview method in terms of materiality and feasibility of the indicators. This study derived meaningful and useful indicators for the assessment of cyber resilience, and it is expected to be used as a foundation for the future cyber resilience studies. In order to generalize and apply the results of this study in practice, it is necessary to carry out quantitative researches in the future.

Key Words : Cyber Resilience, Cybersecurity, Security Indicator, Risk Management, Security Controls

1. 서론

오늘날 사회는 사물인터넷, 클라우드, 빅 데이터 및 모바일 등의 기술 발전으로 디지털 비즈니스 시대를 맞이하게 되었다. 이로 인해 네트워크 및 기업 등이 복잡하게 연계되어 있는 디지털 융·복합 환경이 등장하였다[1]. 복잡한 환경으로 인해 보안에 대한 위험은 점점 더 고도화되고 있으며, 특정 기업뿐만 아니라 환경 전체에 영향을

* This research was supported by the Chung-Ang University Research Scholarship Grants in 2017
Received 3 July 2017, Revised 3 August 2017
Accepted 20 August 2017, Published 28 August 2017
Corresponding Author: Jungduk Kim(Chung-Ang University)
Email: jdkimsac@cau.ac.kr

ISSN: 1738-1916

미치고 있다. 이와 관련하여 보안사고가 지속적으로 일어나고 있다. 우리나라의 경우, 13년 3.20 대란, 14년 카드사 개인정보 유출사고 등 매년 대형 보안사고가 발생하고 있다. 이것은 법률에서 요구하는 최소한의 보안 규정 준수, 예방 중심의 기술적 보안솔루션 운영만으로는 한계가 존재함을 의미한다. 급속하게 발전하는 디지털 융·복합 환경에서 지속적인 보안 수준을 제고하기 위해서는, 새로운 보안 요구사항에 맞는 평가 기준의 개선과 효율적인 평가방법이 필요한 시점이다.

보안에 대한 많은 노력에도 불구하고 보안의 발전 속도는 급속한 환경변화를 따라가기 어려운 실정이다. 전 세계적으로 보안 산업은 지속적으로 상승하는 추세를 보이고 있지만, 여전히 기술적 솔루션에 대한 의존도가 높은 것으로 나타났다[2]. 기존의 기술과 예방 중심의 보안 대책으로는 더 이상 모든 위험을 통제하기에 한계가 존재하고 비효율적이다[3]. 이로 인해 보안 사고는 더 이상 완전히 예방할 수 없으며, 예방뿐만이 아닌 신속한 탐지 및 대응에 대한 중요성 등으로 사이버 레질리언스의 개념이 주요 이슈로 부각되고 있다. 현재 디지털 비즈니스 시대에서 가장 필수적인 사항으로 사이버 레질리언스를 보유하는 것이 가장 중요한 것으로 많은 연구들이 진행되고 있다[4].

현재 국내에는 사이버 레질리언스에 대한 필요성과 중요성에 대한 인식은 증가하고 있지만, 사이버 레질리언스에 대한 연구 및 평가 지표에 대한 연구는 미흡한 실정이다. 사이버 레질리언스가 중요하며 이를 구현해야 한다는 주장들은 많으나 실질적으로 이를 어떻게, 무엇을 통해 구현해야 한다는 연구 및 보고서는 찾아보기 어렵다. 따라서 본 연구에서는 사이버 레질리언스의 등장배경과 개념, 원칙 및 구성요소 등에 대해 조사·분석하고, 보안지표 개발 시 필요 속성을 고려한 전문가 회의를 통해 사이버 레질리언스 평가지표를 개발하였다. 개발된 지표는 전문가 그룹을 대상으로 구성된 포커스 그룹 인터뷰를 통해 지표에 대한 타당성을 검토하였다.

2. 관련 연구

본 장에서는 사이버 레질리언스의 등장배경과 개념, 사이버 레질리언스의 원칙 및 구성요소 등에 대한 조사·분석을 실시하였다. 또한 도출된 사이버 레질리언스의 주요영역들과 국내 정보보호 평가체계의 비교·분석을 통해, 기존 평가영역들이 사이버 레질리언스를 평가할 수 있는지에 대해 분석하였다.

2.1 사이버 레질리언스의 등장배경과 개념

현재까지 사이버 레질리언스를 정확하게 정의하고 사용하는 국제적인 표준은 존재하지 않지만, 사이버 레질리언스의 개념은 선행연구들에 의해 다양하게 연구되어 왔다. 하지만 대부분의 선행연구들은 다양한 분야에서 레질리언스의 개념에 초점을 맞추고 이를 각 분야에 적용시키는 것에 중점을 두었다. 따라서 우선 레질리언스 개념에 대한 선행연구들을 조사·분석할 필요가 있다.

메리엄-웹스터 사전(Merriam-Webster)에 따르면 레질리언스란 '스트레스로 인한 압박감을 회복하는 능력 또는, 불행한 사고 및 변화에 쉽게 적응하거나 회복하는 능력'으로 정의하고 있다. 국립방재연구원(현 재난안전연구원)의 레질리언스에 대한 선행연구 조사 및 분석에 따르면, 레질리언스란 '개인, 그룹 또는 조직이 위험에 직면하거나, 자원의 고갈 또는 물리적인 위협에서도 지속적으로 생존하고, 안정성을 유지하는 역량'으로 레질리언스의 공통된 개념을 정립하였다[5]. 이와 같이 기존 연구들은 레질리언스의 개념을 그동안 대부분 생태·생물학적 관점 또는 재난 연구 등에 집중적으로 적용하였다. 사이버 레질리언스의 개념은 사이버 공간 등장 이후로 이에 대한 위협을 주는 여러 요소들에 대한 대응으로 생겨난 개념이라고 할 수 있다[6].

본격적으로 사이버 레질리언스에 대한 개념은 2012년 다보스에서 개최된 세계경제포럼(WEF)에서 처음 사용한 이후 그 중요성이 크게 인식되고 있다. 포럼에서는 기술적 관점의 일시적 및 예방적 대응은 새로운 기술 발전과 위협에 취약하다고 평가하였다. 이로 인해 더 이상 보안에 대한 완벽한 예방이란 존재하지 않으며, 보안 사고의 발생을 인정하고 최대한 손실을 줄이기 위해, 사고 발생 이전 또는 그에 부합하는 상태로 신속하게 돌아가는 능력이 필요함을 의미한다[3].

디지털 융·복합 환경 내에서 위험을 효과·효율적으로 관리하기 위해서는, 조직 내부뿐만 아니라 외부 이해관계자를 포함한 전사적인 보안 생태계가 유지되어야 한다[7]. 이를 위해 기술적 및 예방적 차원의 대책 중심이 아

닌 지속적인 사후 대응 및 복구의 개념을 포함한 사이버 레질리언스의 개념이 등장하였다. 사이버 레질리언스에 대한 다양한 논의가 이어지고 있지만 가장 보편적인 정의는 '부정적인 사이버 이벤트에도 불구하고 의도한 성과 및 결과물을 지속적으로 전달할 수 있는 능력'으로 정의되고 있다[1].

2.2 사이버 레질리언스와 정보보호 개념 비교

사이버 레질리언스는 기존에 인식되고 활용되었던 정보보호의 개념과는 <Table 1>과 같이 다소 차이점이 존재한다. 정보보호는 일반적으로 네트워크화 된 IT 및 정보시스템을 보호하는 것을 목표로 하지만, 사이버 레질리언스의 경우 비즈니스 전달 보장을 목표로 한다[8]. 즉 사이버 레질리언스는 부정적 이벤트가 발생하였을 때 정보자산을 보호하는 것뿐만 아니라, 올바르게 비즈니스 가치를 제공하는 것을 목표로 한다. 결과적으로 정보기술보다 비즈니스가 우선이 되어야 한다.

또한 목표와 연계하여 기존 정보보호는 침입차단 등의 실패를 용납하지 않도록 시스템을 설계 및 보호하는 관점이지만, 사이버 레질리언스는 실패를 가정하고 목표를 달성할 수 있도록 신속히 반응하여, 실패를 극복할 수 있게 시스템을 설계하는 관점이다[9].

기존 정보보호는 정보보호의 범위를 단일 시스템 또는 단일 조직으로 선정하나, 사이버 레질리언스는 해당 조직뿐만 아니라 주위 환경에 대한 고려도 포함한다. 비즈니스와 정보자산, IT시스템을 주위 환경과 연결된 네트워크로 보고, 이를 위협의 원천으로만 판단하는 것이 아닌, 장점과 단점을 파악하는 다각적인 관점이다[10].

사이버 레질리언스는 보안이 시스템, 소프트웨어 IT 부서 혹은 보안부서만의 책임이 아님을 인식하는 것을 시작으로 이루어진다. 또한 사람을 중심에 두고 이들이 위험을 인식하고 역량과 도구를 활용하여, 예방조치와 회복 및 복구를 하는 것을 말한다[11].

즉 사이버 레질리언스는 사전적 예방 성격의 기존 정보보호 개념을 배제하는 것이 아니라 포함하는 개념이다. 뿐만 아니라, 신속한 탐지 및 사후적 복구 관점이 융합되어 보안 면역·회복체계를 구축하고, 이를 통해 조직의 미션을 유지하는 능력이다.

<Table 1> Comparing information security and cyber resilience

Aspect	Information Security	Cyber Resilience
Objective	Protect information system	Ensure business delivery
Intention	Fail-safe	Safe-to-fail
Approach	Add-on from outside	Built-in from within
Scope	Single organization	Network of organizations

2.3 사이버 레질리언스 구성요소 고찰

사이버 레질리언스 평가지표를 개발하기 위해서는, 사이버 레질리언스의 속성과 구성요소, 원칙 등에 대한 이론적 고찰이 필요하다. 이에 따라 본 절에서는 국내·외 사이버 레질리언스에 대한 연구들을 조사하여, 사이버 레질리언스의 공통된 주요 속성들을 분석하였다.

카네기 멜론 대학(CMU)에서 2010년 5월에 발표한 CERT-RMM(CERT-Resilience Management Model)[12]에서는 기업의 핵심 자산으로 인적자원, 정보(업무절차), 기술 및 시설을 포함하며, 이를 위한 레질리언스를 강조하고 있다. 또한 통합적 관점에서 핵심자산의 보호와 지속성 보장을 목표로 하며, 4개 분야(엔지니어링, 엔터프라이즈, 운영, 프로세스)의 26개 프로세스 영역으로 구성되어 있다. 이를 통해 사이버 레질리언스를 위해서 반드시 수행해야 하는 프로세스들을 확인할 수 있었다.

세계경제포럼(WEF)은 사이버 레질리언스의 가장 중요한 이슈로 리더십과 보안 책임의식을 강조하며, 이를 포함한 사이버 레질리언스 성숙도 모델을 제시하였다[13]. 이 모델은 증가하는 사이버 위험에 대항하기 위한 사이버 레질리언스 프로그램 가이드를 제공하는 목적으로 개발되었다. 이는 3개의 평가분야(거버넌스, 프로그램, 네트워크)와 19개의 평가항목으로 구성되어 있다. 이는 리더십과 보안 책임의식을 강조하여, 최고 책임자와 조직원의 보안 의무사항 이행, 책임 및 역할에 관한 항목이 주를 이루고 있다.

국제 증권 감독기구와 지급결제 및 시장 인프라 위원회(CPMI & IOSCO)는 국제적으로 사이버 레질리언스에 대한 논의를 이끌어온 조직들이다. IOSCO는 2016년 CPMI와의 협력을 통해 금융시장의 사이버 레질리언스 확보를 위한 가이던스를 발표하였다[14]. 이는 5개의 위험관리 범주(거버넌스, 식별, 보호, 탐지, 대응 및 복구)와 3개의 지원요소(테스트, 상황인지, 학습 및 진화)로 구성되어 있다. 본 가이던스는 금융시장의 사이버 레질리언

스를 구축하기 위해 제시되었지만, 다른 일반 조직에서도 공통적으로 활용할 수 있는 관리항목을 제시하고 이를 권고하고 있다.

대부분의 사이버 레질리언스에 대한 논문은 앞서 상술하였던 CMI의 CERT-RMM, WEF의 성숙도 모델, IOSCO의 가이던스를 기반으로 원칙과 구성요소에 대한 연구가 진행되었다. 따라서 추가 문헌연구에 대한 대상을 국제적으로 저명한 조직들의 보고서들을 포함하여 분석한 결과 <Table 2>와 같은 주요 공통 속성들을 도출할 수 있었다.

<Table 2> Key domain of cyber resilience

Domain of cyber resilience	Reference
Leadership of executive management	EY[8], CMU[12], WEF[13], IOSCO[14], Lyu[15], Hong[16], The Scottish Gov.[17]
Context analysis and establishing strategy	CMU[12], Gartner[17], PwC[19],
ICT service management	CMU[12], WEF[13], IOSCO[14], Hong[16], Gartner[17], PwC[19]
Composition of security organization	CMU[12], Lyu[15], The Scottish Gov.[18], Michal[20]
Risk-based security budget management	CMU[12], Lyu[15], Gartner[17], PwC[19]
Measurement and control of security effectiveness	CMU[12], WEF[13], Lyu[15], PwC[19]
Change management of security culture	EY[8], Hong[16], Gartner[17], PwC[19], Michal[20], The Scottish Gov.[18]
Security analysis and sharing	EY[8], WEF[13], IOSCO[14], Lyu[15], Hong[16], The Scottish Gov.[18], PwC[19], Michal[20]
Vulnerability Management	CMU[12], WEF[13], IOSCO[14], Michal[20]
Enterprise-wide incident response system	WEF[13], IOSCO[14], Lyu[15], Hong[16], PwC[19]

2.4 국내 정보보호 평가체계와의 비교

사이버 레질리언스에 대한 이론적 고찰을 통해 도출된 주요 도메인들을 국내 대표적인 정보보호 평가체계인 K-ISMS, 정보보호 준비도 평가와 비교분석 하였다. 이를 통해 국내 기존의 정보보호 평가 체계가 사이버 레질리언스를 평가할 수 있는지에 대해 <Table 3>과 같이 분석하였다. 의미가 같거나 비슷한 경우가 존재하였으나 사이버 레질리언스를 평가하기에는 부족한 영역들이 존재하였다. 또한 위험기반 예산관리, 보안 문화 변화관리, 보안 분석 및 공유 등의 사이버 레질리언스를 위한 새로운 분야들도 도출되었다.

<Table 3> Comparison with domestic information protection assessment system

Domain of cyber resilience	K-ISMS	SECU-STAR
Leadership of executive management	O	O
Context analysis and establishing strategy	O	X
ICT service management	O	X
Composition of security organization	O	O
Risk-based security budget management	X	X
Measurement and control of security effectiveness	O	X
Change management of security culture	X	X
Security analysis and sharing	X	X
Vulnerability Management	O	O
Enterprise-wide incident response system	O	X

3. 사이버 레질리언스 평가지표 개발

본 연구의 사이버 레질리언스 평가지표는 사이버 레질리언스에 대한 선행연구의 참고문헌과 전문가 토의를 통해 개발되었다. 전문가 토의는 사이버 레질리언스 관련 연구 및 프로젝트를 진행한 경험이 있거나, 지표를 활용하여 보안평가를 진행한 경험이 있는 보안 전문가들로 구성하였다. 또한 지표를 개발함에 있어, 차인환(2009)의 보안지표 개발 시 고려사항에 대한 연구결과에 따른, 보안지표의 주요 속성인 타당성, 용이성, 신뢰성을 기준으로 지표를 개발하였다[21]. 본 연구에서 개발한 평가지표는 10개의 분야, 22개의 지표로 구성되어 있으며 <Table 4>와 같다.

'최고경영진의 리더십'을 위해서는 우선 최고경영진으로 구성된 위원회, 최고경영진 수준의 보안책임자의 역할 및 책임에 대한 정의가 선행되어야 한다. 최고경영자는 경영목표 달성을 보증할 수 있도록 필요한 제반 환경 구축을 지원해야 한다. 또한 보안 활동에 대한 거버넌스 활동을 수행해야 하며, 보안에 대한 명확한 의사소통 채널을 보유하고 있어야 한다.

<Table 4> Assessment indicators for cyber resilience

Domain of cyber resilience	Assessment indicators for cyber resilience
Leadership of executive management	Chief executive officer support (CEO)
	Approval and coordination of the executive management(EXE)
	Clear security communication channel(CHN)
	Appointed security officer as a top-level (CSO)
Context analysis and establish strategy	Security environment analysis(ENV)
	Establishment of security range (SCP)
	Security strategy and business performance alignment (STR)
ICT service management	ICT service asset management(SAM)
	ICT service risk assessment(SRM)
Composition of security organization	Composition of security dedicated unit and security workforce(COM)
	Definition of security dedicated organization task(TSK)
Risk-based security budget management	Independent budgeting based on risk management(BUD)
Measure and control effectiveness of security	Implement security level measurement program(MSM)
	Evaluating and improving the effectiveness of security measures(EVA)
Change management of security culture	Policy of security culture change(CUL)
	Role-based education according to roles, responsibilities and requirements(EDU)
Security analysis and sharing	security cooperation system with suppliers and partners(COP)
	Sharing security status(SHR)
Vulnerability Management	Systematic Vulnerability Management(VUL)
	The periodic identification of potential threats(THR)
Enterprise-wide incident response system	enterprise-wide incident planning and training(INC)
	Establishment of the security control system for agile response(SCS)

‘환경 분석 및 전략 수립’에서는 조직의 전사적인 보안 환경을 면밀히 분석하는 것이 중요하다. 조직의 환경과 연계된 보안 환경 분석 없이는, 점차 고도화·지능화되는 보안위협에 대한 신속하고 효율적인 보호대책 수립이 어려울 수 있다. 보안환경 분석을 통하여 변화하는 대내외 환경 및 이해관계자들의 요구사항을 식별할 수 있으며, 조직의 적합한 보안 관리범위 설정 및 전략 수립이 가능하다.

‘ICT 자산 및 서비스 위험관리’를 위해서는 조직의 핵심 업무를 파악하고 이와 관련된 ICT 서비스와 정보자산을 식별해야 한다. 단순히 네트워크, DB, 서버 등 ICT 인프라에 대한 위험관리만 수행할 경우, 비즈니스 업무 프로세스 및 서비스와 이와 관련된 실질적인 정보의 흐름을 파악하는데 한계가 있다. 또한 주기적으로 ICT 서비스와 업무별 정보자산을 식별 및 현행화해야 한다. 핵심 업무 프로세스와 관련된 정보의 흐름을 파악하여 중요도 분석을 수행하고, 시나리오 분석 등 조직에 적합한 방법론에 따라 위험평가를 수행하는 것이 중요하다.

‘보안 전담조직 구성’을 위해서는 자율적 보안활동 및 지속적인 역량강화를 위해, 보안조직의 역할 및 책임을 정의하고, 역량을 지닌 전담 인력이 필요하다. 또한 보안 전담조직은 이해당사자로부터 독립적으로 업무수행이 가능한 전담 인력이 필요하며, 공식적으로 이를 규정화하는 것이 필요하다.

‘위험기반 예산관리’는 컴플라이언스 기반 보안활동이 융·복합적인 환경에서 모든 위험을 반영하기 어렵기 때문에, 전사적 위험관리에 기반을 둔 보안활동이 필요하며, 이에 따라 보안 예산도 위험관리 결과에 따라 수립되어야 한다는 내용이다. 대부분의 조직이 IT예산에 대한 편중 및 기술적인 보호대책 위주의 예산을 수립하고 있다. 사이버 레질리언스를 위해서는 IT예산과 분리된 독립적인 보안 예산이 편성될 필요가 있다.

‘보안 대책의 효과성 측정 및 통제’에서는 조직의 고유한 보안위험을 식별하여 적합한 보호대책을 수립하였는지, 보안활동이 과연 효과가 있는지 평가가 필요하다. 이는 지속적인 개선과 역량 강화를 위해 반드시 필요한 활동이다. 효과성 측정은 일회성 활동이 아닌 프로그램 차원에서 지속적으로 관리하여야 한다. 보안효과성을 측정하기 위한 지표가 없을 경우, 객관적이고 포괄적인 평가가 어려우며, 장기적인 개선 방향 수립에 제한이 있을 수 있다.

‘보안 문화 변화관리’를 위해서는 보안 전담조직뿐만 아니라, 모든 임직원이 보안을 일상 업무의 일환으로 수행할 수 있도록 역할과 책임을 할당해야 한다. 또한 조직의 긍정적인 보안 문화를 정착하기 위한 변화관리 차원에서의 전략과 제도적 지원이 필요하다. 또한 보안 교육 및 인식제고 프로그램은 각 책임과 역할, 요구사항에 따른 직급 별 교육이 이루어져야 한다.

‘보안 분석 및 공유’를 위해서는 혁신적 기술 등장과 비즈니스 환경의 다변화로 인해, 보안 관련 위험이 고도화되고 예측하기 어려워졌기 때문에, 다양한 이해관계자들과의 소통과 공유가 반드시 필요하다. 새로운 보안 위

협은 단일 조직 자체적으로 대응하는데 한계가 있기 때문에, 조직 외부의 주요 비즈니스 파트너, 보안 전문기관과 최신의 정보를 공유하고 협업하여 새로운 위험에 체계적이고 효율적으로 대응할 수 있다.

'취약점 관리체계'는 침해시도를 효과적으로 대응하고 사전에 예방할 수 있으며, 보안시스템의 취약점을 개선하는데 매우 중요하다. 취약점 정보 수집을 취약점 분석 도구 또는 일부 벤더에서 제공되는 단편화된 정보에 의존한다면, 보안 위협에 적극적으로 대응하기 어려울 수 있다. 취약점 정보를 다양한 채널에서 폭넓고 체계적으로 수집하여 관리해야 하고, 취약점이 미치는 영향을 종합적으로 분석하여야 한다.

'전사적 위기대응 체계'는 보안사고 등으로 인한 서비스 장애가 비즈니스 위기로 확산되지 않도록, 관련된 모든 조직이 참여하는 위기 상황의 시나리오에 따라 훈련을 실시해야 한다는 내용이다. 전사적 위기대응 체계를 수립하여 대응하면 위기를 신속히 복구하고 비즈니스를 지속할 수 있다.

4. 타당성 검토

본 연구는 사이버 레질리언스의 이론적 고찰과 전문가 회의를 통해 총 10개의 영역과 22개의 지표를 개발하였다. 사이버 레질리언스에 대한 국내 연구 현황을 고려해 보았을 때, 정량적인 방법으로는 깊이 있는 결과를 도출하기 어렵다고 판단하였다. 따라서 개발된 지표들에 대한 타당성 검토를 위해 포커스 그룹 인터뷰(FGI) 방법을 선정하였다. 포커스 그룹은 <Table 5>와 같이, 보안 지표를 활용한 평가 경험이 있는 참여자, 사이버 레질리언스 관련 연구 및 프로젝트를 진행한 경험이 있는 참여자, 일반 기업의 보안 전문가로 구성하였으며, 참여 대상자는 모두 최소 10년 이상의 경력을 보유하였다.

<Table 5> Focus group interview members

Group Members	Member's Speciality
Consultant	Risk management
ISMS Auditor	ISO 27001 Audit
Senior researcher 1	Governance, Risk and Compliance
Senior researcher 2	Cyber security
Security manager 1	Security governance
Security manager 2	Security management

포커스 그룹 인터뷰는 설문지 작성 및 심층면접을 진행하였다. 우선 설문지는 개발된 평가지표의 중요성(materiality)과 실현가능성(feasibility)을 리커드 5점 척도를 사용하여 조사하였으며, 추가적으로 개발된 지표에 대한 개선사항 또는 개발된 지표 이외에 필요사항에 대하여 작성하도록 하였다. 설문이 끝난 후 60분에 걸쳐 참여자 간 의견 교환 및 토론을 진행하여 개발된 지표의 타당성을 검토하였다.

포커스 그룹 인터뷰 결과, <Table 6>과 같이 22개의 지표 모두 사이버 레질리언스를 평가함에 있어 중요성이 높게 검토되었다. 실현가능성의 경우는 상대적으로 점수가 낮은 3.5 이하의 지표가 3개로, 이에 해당하는 일부 지표의 실현가능성에 대한 재검토 또는 추가적인 요구사항이 필요하다는 의견이 제시되었다.

'최고경영진의 승인 및 조정'의 경우, 국내 조직의 현실을 고려하였을 때, 보안 안건에 대한 승인은 대다수 보안 최고책임자 주관의 정보보호 위원회에서 보안이슈에 대한 논의가 이루어지며, 이에 따라 경영위원회에서 모든 보안 이슈를 다루기에는 어렵다는 의견이 제시되었다. 추가적인 의견으로, 현실적 여건을 고려하여 정보보호 위원회에서 비즈니스에 영향을 미치는 보안 안건들을 검토하고, 이를 상정하는지에 대해 평가해야 된다는 의견이 제시되었다.

'경영성과와 연계한 보안전략 수립'은 비즈니스 관점에서는 현실적으로 보안 활동에 대한 가치를 투자 수익률 등의 재무적인 가치에 중점을 두기 때문에 실현가능성이 다소 낮을 것으로 검토되었다. 또한 보안성과를 비즈니스 관점에서 평가 할 수 있는 지표가 현실적으로 미흡하기에 한계점을 지닌다는 의견도 제시되었다.

'위험관리 기반 독립적 예산 편성'은 아직 국내에서는 ICT와 보안이 명확하게 분리되어있지 않으며, 이로 인해 예산 또한 분리되기 쉽지 않을 것이라는 의견이 제시되었다. 추가 의견으로는 최근 동향을 살펴보았을 때, 보안 전담 조직이 IT조직과 분리되고 있는 상황이기에 향후에는 별도의 보안 예산 항목이 편성될 수 있을 것이라는 의견이 제시되었다.

<Table 6> Review of Assessment indicators for cyber resilience using FGI

Assessment indicators for cyber resilience	Materiality	Feasibility
CEO	4.7	4.0
EXE	4.1	3.5
CHN	4.5	4.2
CSO	4.43	4.0
ENV	4.1	3.8
SCP	4.4	4.1
STR	4.2	2.8
SAM	4.1	4.0
SRM	4.1	3.8
COM	4.4	4.2
TSK	4.2	3.8
BUD	4.0	3.4
MSM	4.2	3.7
EVA	4.7	4.2
CUL	4.5	4.4
EDU	4.5	4.1
COP	4.1	3.8
SHR	4.4	3.8
VUL	4.1	4.0
THR	4.4	3.8
INC	4.2	4.0
SCS	4.3	4.0

5. 결론 및 향후 연구 과제

본 연구는 디지털 융·복합적인 환경에서 필수적인 사이버 레질리언스에 대한 10개의 영역과 22개 평가 지표를 개발하였다. 기존의 정보보호 관점을 반영하고 의미가 수정된 평가지표도 개발되었지만, 기존에 존재하지 않던 '위험기반 예산관리', '보안 문화 변화관리', '보안 분석 및 공유' 영역이 도출되었으며, 이에 따른 새로운 지표들도 개발되었다. 이는 기존 정보보호 평가체계와는 차별화 된 사이버 레질리언스의 속성을 반영함에 있어 중요한 의미를 지닐 것으로 사료된다. 개발된 지표들은 모두 사이버 레질리언스의 속성과 원칙 등에 대한 이론적 고찰을 통해 개발되었다. 이에 향후 사이버 레질리언스 연구의 기반이 될 수 있을 것으로 기대된다.

본 연구의 한계점은 다음과 같다. 첫째, 본 연구는 국내 사이버 레질리언스의 연구가 미흡한 실정임에 따라, 포커스 그룹 인터뷰로 타당성을 검토하여 일반화에 어려움이 존재한다. 따라서 향후 더 많은 표본을 통해 다변량 분석 등을 포함한 정량적인 연구가 필요하다. 둘째, 개발된 지표는 대부분이 정성적 지표이며, 이에 대한 구체적인 데이터 수집 종류와 수집 방법이 필요할 것으로 보인다. 이에 따라 향후 연구에서는 정성적 지표에 대한 데이터를 객관화하여 이를 평가할 수 있는 구체적인 방법이 필요할 것으로 보인다.

ACKNOWLEDGMENTS

This research was supported by the Chung-Ang University Research Scholarship Grants in 2017.

REFERENCES

[1] J. D. Kim and C. G. Jin, "International Standardization Trends and Issues of Cyber Resilience", Review of KIISC, Vol. 26, No. 4, pp. 11-15, 2016.

[2] Gartner, "Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware", 2014.

[3] World Economy Forum, "Collaboration with Deloitte, Risk and Responsibility in a Hyper connected World: Pathways to Global Cyber Resilience", Geneva: World Economic Forum, 2012.

[4] Gartner, "Prevention is Futile in 2020: Protect Information via Pervasive Monitoring and Collective Intelligence", 2013.

[5] Korea National Disaster Management Institute, "Development of Community Resilience Framework", 2013.

[6] H. S. Lyu, "A Study on Cyber Security Policy and Governance in the ICT Convergence Environment: Focused on "Authentication", Korea Institute of Public Administration, pp.58-89, 2015.

[7] Ernst&Young, "Achieving Resilience in the cyber ecosystem", 2014.

[8] S. A. Merrell, A. P. Moore and J. F. Stevens, "Goal-based assessment for the cyber security of critical infrastructure", IEEE International Conference on

Technologies for Homeland Security, pp.84-88, 2010.
[9] Deborah B. and Graubart R. “Cyber Resiliency Engineering Framework”, MITRE Report, 2011.
[10] Fredrik Björck, Martin Henkel, Janis Stirna and Jelena Zdravkovic, “Advances in Intelligent Systems and Computing”, Springer, Vol.353, pp.311-317, 2015.
[11] Symantec, “The Cyber Resilience Blueprint-A New Perspective on Security”, 2014.
[12] Carnegie Mellon University, “CERT® Resilience Management Model. 1.0”, 2010.
[13] World Economic Forum, “Advancing Cyber Resilience principles tool”, 2017.
[14] Bank for International Settlements and International Organization of Securities Commission, “2016 Guidance on cyber resilience for financial market infrastructures”, 2016.
[15] H. S. Lyu, H. J. Cho and H. A. Lee, “A Study on Priorities of Cyber Security Policy and Governance”, Crisisnomy, Vol. 12, No. 8, pp.86-103, 2016.
[16] S. K Hong, “Megatrend: Digital Future and Cyber Security Service of Accounting Corporation”, Ernst&Young Eyesight, Vol. 13, pp.37-42, 2017.
[17] Gartner, “Use Six Principles of Resilience to Address Digital Business Risk and Security”, 2015.
[18] The Scottish Government, “Consultation on proposal for a Cyber Resilience Strategy for Scotland. Glasgow: Cyber Resilience Policy Team”, 2015.
[19] PricewaterhouseCoopers, “Insurance 2020 & beyond: Reaping the dividends of cyber resilience. New york: PricewaterhouseCoopers LLP”, 2015.
[20] M. Choras, M. P. T. Bruna, A. Churchill, I. Eguinoa, R. Kozik, A. Yautsikhin, I. Maciejewska and A. Jomni, “Comprehensive Approach to Increase Cyber Security and Resilience: CAMINO Roadmap and Research Agenda”, Availability, Reliability and Security 2015 10th International Conference on, pp. 686-692, 2015.
[21] I. H. Cha, “An Empirical Research on Developing Personnel Security Management Indicators in Information Security”, Ph.D. dissertation, p.123, Quarterly Resource, Kwangwoon University, 2009.

김 수 진(Kim, Sujin)

・2010년 2월 : 덕성여자대학교 컴퓨터공학과(학사)
・2015년 8월 ~ 현재 : 중앙대학교 융합보안학과(석사과정)
・관심분야 : 사이버 레질리언스, 보안투자, 정보보호 거버넌스
・E-Mail : top44313@gmail.com

김 정 덕(Kim, Jungduk)

・1979년 2월 : 연세대학교 정치외교학과(학사)
・1981년 8월 : 연세대학교 경제학과 대학원(석사)
・1986년 8월 : Univ. of S. Carolina, MBA
・1990년 12월 : Texas A&M Univ., Ph. D. in MIS
・1995년 3월 ~ 현재 : 중앙대학교 산업보안학과 교수
・관심분야 : 디지털 비즈니스 보안, 산업보안 거버넌스 및, 보안관리
・E-Mail : jdkimsac@cau.ac.kr