Information Systems Review
Vol. 21, No. 3 August 2019
http://dx.doi.org/10.14329/isr.2019.21.3.049

ICT기반 보안개념 정의와 범위에 관한 설계연구

The Design Research on ICT Security Concepts and Domains

전 민 서 (Minseo Jeon) 더존비즈온 포렌식센터
장 항 배 (Hangbae Chang) 중앙대학교 경영경제대학 산업보안학과, 교신저자

요 약

끊임없이 다양한 형태로 발생하는 보안사고와 이에 따른 피해의 규모가 증가함에 따라, 사회의 보안에 대한 관심과 함께 학문적 관심과 연구의 양도 지속적으로 증가하고 있다. 하지만 이러한 관심과 연구의 양적 증가에도 불구하고 보안과 안전에 대한 구분 없이 용어가 혼용되고 있으며, 다양한 보안개념용어들의 정의와 범위가 상호 공통성과 차별성을 보유하지 않은 채 연구가 진행되어 왔다. 실제로 현재 일반인을 대상으로 하는 뉴스 기사, 업무 문서 등에서 다양한 보안개념용어들이 오·남용되고 있는 관계로 보안의식과 이해수준을 낮추고 있으며, 궁극적으로는 보안학문이 고유영역을 확보하면서 지속적인 확장을 진행하는데 걸림돌이 되고 있다. 따라서 본 연구에서는 현재 학회 또는 산업현장 등에서 다양한 시각을 가지고 혼용되고 있는 보안개념용어들(정보보안, 사이버보안, 연구보안, 기업보안, 산업보안, 융합보안 등)에 대한 정의와 범위를 설계하고자, 학술중심의 문헌적 연구조사내용에 산업현장중심의 경험적 지식을 반영하는 과정(델파이 전문가 조사)을 통해 적정수준의 합의과정을 이끌어 내었다.

키워드 : 보안 개념과 범위, 사이버보안, 정보보안, 융합보안, 산업보안

Ⅰ. 서 론

ICT기술이 타 산업과 융합되어 새로운 가치를 생성함에 따라 경제와 산업발전에 많은 이익을 가져다주었지만, 동시에 보안관점에서는 새로운 형태의 위험요소들이 다가올 수 있다. 보안 사고에 활용되는 공격수법이 지능화되고 피해 규모 또한 큰 사건들이 발생하고 있다. 이러한 현재 또는 미래 보안위험들에 맞서 산업계에서는 보안이 더 이상 선택이 아닌 필수로 인지하고, 지속가능한 사업운용을 위해 전문성을 보유하고 있는 보안인력 채용을 통해 선제적인 보안대책을 수립하고 있다. 또한 학계에서는 보안을 독립된 학문영역으로서 연구하고, 전문 인력 양성을 목적으로 관련 학과를 신설되어 운영되고 있다.

하지만 보안의 중요성과 나날이 증가하는 사회의 관심에도 불구하고 보안과 안전에 대한 용어가 혼용되고 있을 뿐만 아니라, 새롭게 출현하는 다양한 보안용어들에 대한 개념적 정의와 범위 등에 대한 공통적 인식이 성립되지 않은 채 연구가 진

† 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음(IITP-2019-2014-1-00636).

행됨으로써 보안학문으로서의 정체성을 확보하지 못하고 있다.

아래와 같은 사례에서 보는 바와 같이 일반 국민들이 쉽게 접할 수 있는 신문기사의 경우(발췌 편집), 동일한 기사에서도 다양한 보안용어들이 오용 또는 혼용 되어 적용된 경우를 빈번히 찾아볼 수 있다. 세부적으로 정보보안과 사이버보안 사이에 개념을 동일하게 인식하여 용어를 혼용하여 사용하거나, 최근 산업 간 연결성이 확장되는 환경변화에 따라 새롭게 출현한 융합보안 개념이 다중적인 의미로 사용되는 것(박광민, 나원철, 2016)을 쉽게 접할 수 있다.

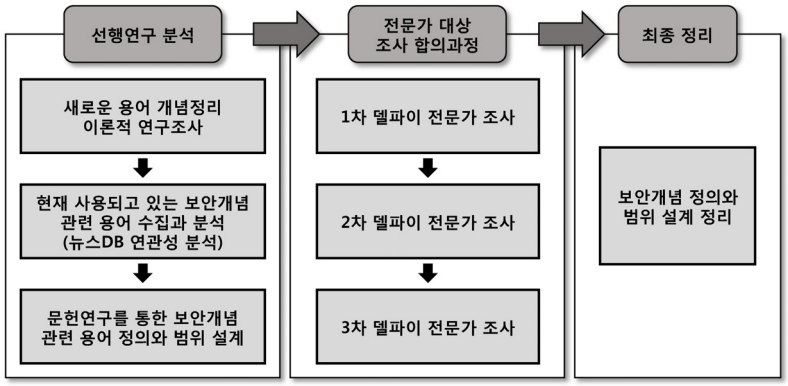
"이미 OOO는 XXX와 [사이버보안] 이 러닝 플랫폼을 구축하고, [정보보안] 분야의 직무능력 향상을 위한 교육을 제공하고 있다. 교육은 [정보보호] 일반과정과 심화과정 등으로 구성돼 있으며, 홈페이지를 통해 신청할 수 있다."

"미래의 보안산업은 기존 [물리보안]과 [정보보안] 영역에 New ICT 기술이 접목된 [융합보안] 서비스가 새롭게 등장할 것으로 예측된다."

"OOO학과는 미래 [자동차보안] 전문가 양성에 필요한 [융합보안] 교육과정을 개발해 운영하고 있다."

이러한 문제는 다양하고 복잡한 형태로 발생하는 보안 사고들에 대해 원인분석을 통한 새로운 관점의 거시적 보안대책을 수립하기 보다는 단편적인 보안문제 해결을 위한 미시적 보안대책들을 마련하는 데에만 집중해 온 것에 기인한다. 보안분야의 연구가 미래 지속가능 학문분야로 정체성을 확보하면서 발전하기 위해서는 무엇보다도 다양한 형태로 혼용되고 있는 보안용어들에 대한 개념과 범위에 대한 설계가 선행되어야 한다. 그러나 보안 분야 연구는 응용학문의 성격이며 보안이라는 용어자체가 다의적(多義的) 특성을 보유하고 있는 상태에서 제4차 산업혁명이라는 환경변화에 따라 ICT기술을 매개로 한 다양한 산업이 융합되어 보안대상과 위험요소가 복잡해지면서 보안용어들의 개념모호성은 더욱 확대되고 있다. 보안지식과 보안대책 사이에 밀접한 연관성이 있음 고려해 볼 때(한진영, 2016) 이러한 보안개념용어들 사이에 모호성은 보안 산업 현장에서 활동하는 전문가들 사이에 상호소통을 어렵게 만들고 있으며, 궁극적으로 보안 분야 내부는 물론 타 분야와의 학문적인 상호교류와 발전을 어렵게 만들고 있다.

따라서 본 연구에서는 문헌연구와 질적인 연구방법론을 활용하여, ICT 보안 분야에서 사용되고 있는 다양한 보안개념관련 용어들의 정의와 범위를 설계하고자 한다. 이를 위하여 먼저 새롭게 출현하는 용어에 대한 개념정의를 위해 필요한 이론적



〈그림 1〉 보안개념 관련 용어 정의와 범위설계 연구방법

선행연구를 살펴보고, 본 연구의 대상이 되는 보안개념 관련용어들을 수집하였다. 수집된 용어들은 빈도순위에 따라 우선순위를 부여하고, 보안개념 관련 문헌연구를 분석하여 선언적 문장형태로 정리하였다. 이후 보안 전문가들로 구성된 그룹을 대상으로 델파이 방법론을 적용하여 3차례의 합의과정을 통해 보안개념과 관련 용어들의 정의와 범위를 최종적으로 정리하였다.

Ⅱ. 보안 개념설계 선행연구

2.1 개념설계 선행 연구

본 연구의 가장 중요한 목표는 보안 개념을 정리함으로써 보안의 학문적 정체성 확립에 기여하는 것이다. 어떠한 분야가 학문으로 성립되기 위해서는 첫째, 고유한 분석의 단위가 존재하고 둘째, 인접 분야와는 구별되는 목표와 그에 따른 방법론이 정당하여야 한다고 하였다(Cabré Castellví, 2003). 이러한 이론의 연장선상에서 개념에 대한 연구를 용어 이론의 중심이자 출발점(Felber, 1987) 이라고 볼 수 있을 것이다. 이것의 연장선상에서 개념에 대한 체계적인 이론을 용어학에서 발견할 수 있었다. 용어학은 20세기 초 독일에서 시작된 학문으로 동일한 개념에 부여된 서로 다른 형태의 용어나 상징들을 의사소통에 사용함으로써 발생하는 잡음을 줄이기 위해 용어에 대한 연구가 시작되었다. 용어학은 어떤 개념과 그 개념들의 표현을 다루는 지식의 학제적 분야를 일컫는데 일반적으로 용어학으로 표현된다. 용어학에서 용어작업은 지식을 정리하는 활동과 그 지식을 전달할 수 있게 하는 기초를 제공한다. 지식 정리는 문헌의 초록작성과 내용요약, 분류와 같은 분석 활동을 통하여 개념을 표현하는 용어에 대한 연구이다(Felber, 1987; Nedobity, 1983). 용어작업은 용어학적 방법과 원칙 아래에 이루어지는데, 표준화기구인 ISO에서 제안하는 ISO 704: Terminology Work-Principles and methods에서 용어작업 기준을 명시하고 있었다.

〈표 1〉 ISO 704: 용어형성 원리(Terminology Work)-기준과 방법(Principles and methods)

기준(Principles)
투명성(Transparency)
일관성(Consistency)
적합성(Appropriateness)
언어의 경제성(Linguistic Economy)
파생력(Derivability)
언어학적 정확성(Linguistic Correctness)
모국어에 대한 선호도(Preference for Native Language)
용어 선택(Preferred term)

하지만 ISO 704에서 권장하는 원칙들은 상호모순적인 면이 있다. 예를 들어 한자로 된 용어가 투명성과 파생력에 있어서 뛰어날 수 있지만 모국어에 대한 선호도 면에서는 떨어질 수 있다. 따라서 위 원칙들을 모두 유지하면서 적용하는 것은 쉽지 않다. 위 ISO 704 원칙들에 기초하여 북한의 리수락 박사(리수락, 2006)는 다음과 같이 남북 용어 통일안 표준화 원칙을 제안하였다. 아래 제안된 원칙들은 ISO 704의 원칙을 세부 항목으로 나누어 정량화했다는데 큰 의의가 있다.

〈표 2〉 남북 용어 통일안 표준화 원칙

용어 표준화 원칙
개념표현의 정확성
학술적 체계성 및 원어와의 대응관계
우리말 다듬기 정도
언어적인 완성도
문화적인 측면

보안 분야뿐만 아니라 다양한 학문 분야에서 개념 정립을 통하여 학문의 정체성을 확립하고자 하는 시도가 이루어지고 있었다. 건축학, 체육학, 법학, 행정학 등 여러 분야의 혼용 사례 분석과 개념 정립 연구를 분석한 결과 혼용하고 있는 용어의 개념을 정립하기에 앞서 명확한 정의를 내리기 위하여 기준이 선행되어야 함을 알 수 있었다.

위에서 살펴본 바와 같이 ISO 704 표준화 원칙과 같은 지침이 용어작업에 있어 절대적으로 따라야 하는 원칙은 아니다. 하지만 전문가의 용어 작업에 있어 충분히 고려되어야 하는 사항일 것이다(최기선, 2007). 따라서 본 연구 목표에 부합하는 결과를 도출하기 위하여 용어학의 용어작업 기준과 보안 개념 관련 선행연구 분석을 참고하였다.

2.2 보안 개념설계 선행연구

앞서 언급한 바와 같이 본 연구에서는 혼용하고 있는 보안 용어를 선정하고 그 개념을 정리하고자 한다. 이를 수행하기 전 먼저 보안과 안전의 의미를 검토하기 위해 국립국어원 표준국어대사전과 옥스퍼드 사전에서 정의하고 있는 보안과 안전의 사전적 정의를 다음과 같이 정리하였다.

〈표 3〉 보안과 안전에 대한 사전적 정의

구분	정의
안전 (安佺)	위험이 생기거나 사고가 날 염려가 없음(또는 그런 상태)
Safety	① the state of being safe and protected from danger or harm ② the state of not being dangerous ③ a place where you are safe
보안 (保安)	① 안전을 유지함 ② 사회의 안녕과 질서를 유지함
Security	① the activities involved in protecting a country, building or person against attack, danger, etc. ② the department of a large company or organization that deals with the protection of its buildings, equipment and staff ③ a place at an airport where to go after your passport has been checked so that officials can find out if you are carrying illegal drugs or weapons ④ protection against something bad that might happen in the future

국립국어원의 표준국어대사전과 옥스퍼드 사전에서 정의하고 있는 안전(Safety)과 보안(Security)의 의미를 살펴본 바, 두 단어 모두 공통적으로 '위험'과 '보호'라는 단어를 내포하고 있었다. 하지만 안전(Safety)은 단순히 상태를 말하고 있는 반면에 보안(Safety)은 보호하는 활동이라 정의하며 좀 더 적극적인 의미를 내포하고 있었다. 또한 주체로 둘의 차이가 나타났는데, 안전(Safety)은 위험과 사고가 나지 않는 상태로 만들 주체가 명시되지 않았다. 하지만 보안(Security)은 사회의 안녕, 국가, 건물 등 보호대상을 명시함으로써 보호하는 활동에 중점을 두며 책임의 주체를 유추해 볼 수 있었다. 정필운(2011)은 그의 연구에서 사이버보안, 정보보안, 정보보호, 사이버안전 등의 개념이 어떻게 정의될 수 있으며 서로 어떤 상관성이 있는지 정리하고, 정보통신기술로 모든 것이 연결되는 세상에서 정보통신에 대한 침해행위에 대응하는 것을 지시하는 개념으로 어떠한 개념을 사용하는 것이 가장 적합한지 탐색하고자 하였다. 김정덕 등(2009)은 융합보안에 대한 국외의 연구를 참고하여 국내에서 혼용되고 있는 융합보안의 개념을 재정립하고 융합보안을 통합보안과 복합보안 측면에서 분석함으로써 향후 융합보안 적용 시 고려해야할 접근 방법을 제시하였다. 융합보안에 대한 정의를 위해 국외의 다양한 연구기관에서 제시된 융합보안 개념을 참고하였다. 또한 이창무(2017)는 보안이라는 개념의 모호성이라는 문제점을 파악하고 산업보안을 제목으로 설정한 모든 학술지 논문을 대상으로 조사를 했다는 점에서 의미가 있다. 또한 국내외 문헌과 표준문서에서 제시한 개념을 종합한 다른 연구와 달리 이론화와 개념화에 대해 깊은 고민을 하였던 연구였다.

Ⅲ. 보안개념 설계과정과 결과

3.1 보안개념 설계기준 선정

용어작업 기준으로 제시된 ISO 704 및 남북통일 표준화 원칙은 절대적인 원칙은 아니지만 용어작업에 있어 중요한 정보를 제공하고 있으므로 용

어작업 기준 선정에 충분히 고려되어야 한다. 따라서 위 원칙들을 존중하면서 현재 실정에 맞게 수정하여 기준을 명료성, 배타성, 포괄성으로 선정하였다.

명료성의 경우 ISO 704와 남북통일 표준화 원칙에서 가장 첫 번째로 꼽는 투명성(Transparency)과 개념표현의 정확성을 참고하였다. 개념의 가장 주된 특징을 반영하고 애매 혹은 모호한 표현 없이 개념을 표현하고 있다면 명료성이 높은 점수로 나올 것이라 예상하였다. 배타성은 전통적 용어 이론의 원리 중 제4원칙 일의성 원칙이 이론적 배경이 되었다. 전통적 용어 이론의 원칙은 다음 표와 같이 크게 5가지로 볼 수 있다. 배타성의 이론적 배경이 된 '제4원칙'은 인지 용어론자들로부터 용어의 자율적인 발전과 변화를 규제한다는 비판을 받는다. 하지만 대표적인 사회 인지 용어론자인 Temmerman(2000)은 제4원칙이 전문용어에 효과적이라 관찰하였다. 포괄성의 경우 현재 보안 개념이 혼용되는 원인 중 하나인 외국어로 된 개념을 국내로 받아들이면서 번역의 오류로 인한 개념상의 혼란이 야기하는 점을 새로 제시하는 개념에서 바로잡고자 하였다. 따라서 적합성(Appropriateness), 학술적 체계성 및 원어와의 대응관계 등을 고려하여 본 기준을 선정하였다.

3.2 개념설계 대상 보안용어 추출

용어정의와 범위설계 대상이 되는 보안관련 개

〈표 4〉 전통적 용어이론 원리

원칙	내용
제1원칙 명칭적 관점	언어를 배제한 개념으로부터 시작되어야 함
제2원칙 개념 단절성	개념은 명확히 구별가능하고, 논리 및 존재론적으로 구조화된 개념체계 내에 설계되어야 함
제3원칙 분석 및 내포적 정의 방식	내포적 정의방식으로 이상적으로 정의되어야 함
제4원칙 일의성 원칙	하나의 용어에 의해 지칭되고, 하나의 용어는 단 하나의 개념을 지시하여야 함
제5원칙 공시태 원칙	개념과 용어간의 대응은 영속적이어야 함

〈표 5〉 문헌연구를 통한 보안개념용어 선언적 정의와 범위설계

용어	개념	
보안	환경에 놓인 보호대상을 위험요소(Risk)로부터 보호하여 질서와 안녕을 유지하는 활동	보호대상(Object) / 환경(Environment)
정보보안	정보 생애주기(생성, 유통, 파기)과정에서 정보를 가지고 있는 자산을 보호하는 활동	정보자산(Information) / 환경(Environment)
사이버보안	사이버공간에서의 보호대상을 위험으로부터 보호하는 활동	보호대상(Object) / 사이버 공간(Cyber Space)
기업보안	조직의 안정적인 비즈니스 활동을 위해 보유자산을 위험으로부터 보호하는 활동	자산(Asset) / 조직(Organization)
연구보안	국가연구개발사업 전체수행과정에서 발생하는 주요 연구개발성과를 유출 또는 침해당하지 않도록 방지하기 위한 활동	연구내용(Research Contents) / 연구조직(Research Organization) + 수행과정(Time Dimension)
산업보안	① (협의적 개념) 조직이 보유한 기술을 보호 ② (광의적 개념) 산업의 비즈니스 특징을 반영한 산업의 보안	① 기술(Technology) / 조직(Organization) + ② 비즈니스 특징(Value Chain)
융합보안	① (협의적 개념) 보안수단 통합(물리보안+정보보안) ② (광의적 개념) 보안기술과 타 산업과의 융합을 통한 새로운 가치 창출	

념들을 추출하기 위해, 2016년 9월 1일부터 2017년 8월 31일까지 총 2,193건의 보안뉴스기사에서 키워드를 수집하였다. 그 다음 관계데이터 분석도구인 'Net Miner'를 사용하여 '보안'키워드와의 연관성 분석을 진행하였다. 연관성 분석을 통해 본 연구의 대상과 거리가 있는 보안관련 인물, 기관, 장소, 기술 등은 제외하고, '보안'분야에서 가장 많이 사용되고 있는 보안관련 개념들을 추출한 결과, '정보보호', '사이버보안', '기업보안', '산업보안', '융합보안', '연구보안' 등이 최다빈도 노출 키워드로 추출되었다. 따라서 본 연구에서는 이들을 개념설계를 위한 우선순위 대상으로 설정하고, 국내외 문헌연구 분석을 통하여 <표 5>와 같이 선언적인 문장형태로 정리하였다.

3.3 1차 전문가 대상 델파이 분석

앞서 추출된 보안 용어들에 대한 개념과 범위 설정에 대해 전문가들이 어떻게 평가하는지를 확인하기 위해 델파이조사를 실시하였다. 델파이 조사방법은 전문가 그룹의 의견을 체계적으로 도출하고 수렴하기 위하여 고안된 기법(Gordon, 1992)으로서, 혼용하고 있는 보안 개념들을 정리하고 합의된 의견을 이끌어 내는데 적절하다고 판단되어 본 연구에 적용하였다. 참여한 전문가는 보안 관련 대학, 연구소, 기업체 등에서 10년 이상의 경험을 보유하고 있는 전문가 15명을 대상으로 하였다. 1차 전문가 대상 델파이 조사지에서는 전문가 의견을 종합적으로 수집하는 차원에서 폐쇄형 및 개방형 형태로 질문지를 설계하였다. 예를 들어 "제시된 개념 외에 더욱 적절하다고 생각하는 개념과 그에 대한 이유를 적어주시기 바랍니다."와 같이 선정된 각각의 용어와 제시한 개념에 대해 개방형의 질문 형태를 제시함으로써 전문가들의 대표적 견해를 자유로운 분위기에서 수집하고자 하였다. 또한 필요시 전문가의 이해와 응답의 용이성을 위하여 개념을 도식화한 그림을 함께 제시하였다.

1차 조사를 실시한 결과 <표 6>과 같은 조정된 결과 값을 얻을 수 있었으며 다음 표는 그 중 보안에 대한 결과를 정리한 것이다. 첫 번째 문항인 보안에 대한 명료성의 경우 평균 4.73(표준편차 044), 배타성의 경우 평균 4.13(표준편차 0.81), 포괄성의 경우 평균 4.40(표준편차 0.71)로 나타났다. 두 번째 문항인 정보보안의 경우 명료성 평균 4.20(표준편차 0.65), 배타성 평균 4.20(표준편차 0.83), 포괄성 평균 4.27(표준편차 0.68)로 나타났다. 세 번째 문항은 사이버보안이었는데 명료성의 경우 평균 4.73(표준편차 0.44), 배타성 평균 4.00(표준편차 1.10), 포괄성 평균 4.53(표준편차 0.62)로 나타났다. 다음으로 기업보안의 평가 기준 중 명료성의 평균은 4.60(표준편차 0.49), 배타성의

〈표 6〉 보안개념용어 정의와 범위 전문가 평가

용어		응답자(n = 15)	
		전문가평가 평균	전문가평가 표준편차
보안	명료성	4.73	0.44
	배타성	4.13	0.81
	포괄성	4.40	0.71
정보보안	명료성	4.20	0.65
	배타성	4.20	0.83
	포괄성	4.27	0.68
사이버보안	명료성	4.73	0.44
	배타성	4.00	1.10
	포괄성	4.53	0.62
기업보안	명료성	4.60	0.49
	배타성	3.93	1.18
	포괄성	4.33	0.87
산업보안	명료성	3.93	0.77
	배타성	3.53	1.15
	포괄성	3.87	0.96
연구보안	명료성	4.27	1.06
	배타성	4.00	1.10
	포괄성	4.07	0.93
융합보안	명료성	4.13	0.88
	배타성	3.87	0.88
	포괄성	3.87	1.02

평균은 3.93(표준편차 1.18), 포괄성의 평균은 4.33(표준편차 0.87)로 나타났다. 산업보안의 개념의 경우 명료성 평균은 3.93(표준편차 0.77), 배타성 평균 3.53(표준편차 1.15), 포괄성 평균 3.87(표준편차 0.96)로 나타났다. 다음의 문항인 연구보안 명료성 평균은 4.27(표준편차 1.06), 배타성 평균 4.00(표준편차 1.10), 포괄성 평균 4.07(표준편차 0.93)로 나타났다. 마지막으로 융합보안의 경우 명료성 평균 4.13(표준편차 0.88), 배타성 평균 3.87(표준편차 0.88), 포괄성 평균 3.87(표준편차 1.02)로 나타났다.

3.4 2차 전문가 대상 델파이 분석

2차 전문가 조사는 라운드테이블 회의방식으로 진행되었는데, 참가자 간 상하 구별 없이 자유롭게 의견을 나누며 수평적인 자유토론을 거쳐 합의에 이르고자 하였다. 2차 전문가 조사는 1차 조사에 응답한 인원 중 전문성과 경력을 감안하여 6명을 별도 선정하여 심층논의가 이루어졌다. 1차 조사결과에 자신의 의견을 서면으로 작성하고 상호 확인을 거친 후 토론 형식으로 진행되었다.

2차 조사과정에서는 '보안'용어에서 파생된 보안개념관련 용어들이 많기 때문에 '보안'자체에 대한 의 미를 명확하게 정리하는 것이 무엇보다 선행되어야 한다는 점에 의견이 모아졌다. 세부적으로 보안과 안전 사이에 경계선을 손실행위의 주체와 범죄 연관성에 두고, 보호대상의 피해여부와 상관없이 실수에 의한 오용과 의도적 남용 등의 모두가 보안활동의 범위 안에 속한다고 정리하였다. 이후 정보보안과 사이버보안, 기업보안과 산업보안 사이에 개념정의와 범위설계 차별화에 관한 상호조정회의가 진행되었으며, 연구보안의 경우 국가의 연구개발 사업만을 보호대상으로 한정하지 않고, 자체 연구개발 사업을 진행하는 조직(기업)에도 확대적용이 필요함이 제시되었다.

"보안과 안전의 사전적 의미는 서로 확연하게 구별되는데도 불구하고 여전히 모호하게 사용되고 있다. 보안과 안전은 피해의 인위성 여부에 따라 차이를 갖는다. 인간의 행위로 인한 피해냐 아니냐에 따라 보안과 안전의 차이가 구별되는 만큼 보안의 개념에 인위성 여부가 포함되어야 한다고 생각한다."

"인간의 불법적인 요소가 중요한 구분점이라고 생각하기 때문에, 제시된 개념에서 불법적인 위험요소를 추가해야 한다고 생각한다. 환경에 놓인 보호대상을 불법적인 위험요소로부터 보호하여 질서와 안녕을 유지하는 활동이라고 정의하는 것이 적절하다고 생각한다."

"정보보안의 개념 중 정보의 생애주기라는 표현은 보안이나 IT 쪽 전문가가 아닌 이상 정확한 뜻을 알기 힘들기 때문에 다소 부적절하다고 생각한다. 정보보안은 가장 흔하게 사용되는 개념이지만, 보호해야 할 정보가 무엇인지에 대한 명확한 개념 없이 사용하는 경우가 많다." "현재 정보보안은 주로 IT보안으로 개념이 정립된 것 같다."

"사이버보안은 정보보안과 달리 외부 공격을 방어하는 것에 대해 중점을 둔다는 의견이 있다. 사이버보안 개념에 사이버 해킹이나 사이버 범죄행위(왕따, 사기, 가짜뉴스 등)를 포함시키면 정보보안과 차별성이 생긴다."

"기업보안은 주로 가치사슬에서 보조적 활동(개발과 생산을 간접적으로 지원)에 관계되는 자산에 대한 보호를 의미하며, 산업보안은 본원적 활동(개발과 생산을 직접적으로 지원)에 관계되는 자산에 대한 집중적인 보호활동을 의미하는 것으로 판단된다. 범위에 있어 기업보다 산업이 상대적으로 크기 때문에 이들 사이에 공통적 보호활동과 차별적 보호활동이 존재한다."

"지금까지 많이 인용되고 있는 산업보안의 개념은 첨단기술과 산업 활동에 유용한 기술정보를 산업스파이에 의해 유출당하지

않도록 하는 보호와 관리의 활동이다. 이에 반해 현재 제시된 개념에서는 조직이 보유한 기술에만 한정하였기 때문에 협의적이라고 생각한다. 따라서 조직이 보유한 경영정보도 보호대상에 포함되어야 한다.”

“연구보안을 국가연구개발 사업에 한정하지 않고, 연구소와 기업 등에서 개별적으로 수행하는 연구개발 사업에도 적용이 되도록 광의의 개념을 도입하는 것이 좋겠다.”

“융합보안의 정의가 학문적인 개념과 실무적 개념의 차이가 있었다는 점은 대부분 인지하지 못하고 있었던 것 같다. 이 부분에 대한 명확한 구분과 설명이 필요하다.”

3.5 3차 전문가 대상 델파이 분석

2차 조사 때 수렴된 전문가들의 의견을 반영하여 수정된 개념을 제시하고, 2차 조사와 같은 방식으로 3차 라운드테이블 회의가 진행되었다. 회의가 진행되면서 제시된 보안개념관련 용어들 사이에 배타성에 대한 문제점이 지속적으로 언급되었으나, 각각 보안개념관련 용어들이 보안자체 개념에서 파생된 용어들임에 따라 보호환경과 위험요소가 융·복합적인 형태로 진화하기 때문에 각각의 개념이 완벽하게 배타적일 수 없다는 결론을 도출하였다.

따라서 사이버보안과 정보보안 사이에 개념설계에 있어 보호대상이 정보이고, 보호환경이 사이버공간이라는 공통성을 가지고 있으나, 사이버보안은 정보뿐만 아니라 사이버 객체를 추가적인 보호대상으로 포함하고 있으며, 정보보안은 사이버공간 내 정보뿐만 아니라 물리적인 공간 내 정보에 대해서도 보호대상으로 설정하고 있음을 확인할 수 있었다. 기업보안은 조직의 공통자산이 보호대상(개발과 생산을 간접적으로 지원하는 관리자산)으로 설정되나, 협의의 산업보안은 기업의 특성(업종)을 결정짓는 핵심요인인 기술을 대상으로 하는 보호활동이며, 광의의 산업보안은 기술을 포함한 추가적인 고유자산(개발 및 생산 등과 직접적으로 관계되는 고유자산) 포함여부에 따라 이들 사이에 개념적 범위가 구분되어 진다. 이중 조직의 제품(서비스)을 개발하는 과정에서 관계되는 보호대상(연구원, 연구 산출물, 연구시설과 공간 등)에 대한 보안활동은 연구보안 범위로 한정하여 설명할 수 있었다. 마지막으로 융합보안은 다양한 보안방법들의 연계 또는 통합의 의미로 사용되었으나, 최근에는 복합적인 보호대책이 ICT 기술이 내재화된 융합제품(서비스)에 부합됨에 따라 의미가 확장되어 광의의 산업보안 개념범위와 일부 공통성을 가지게 되었다. 참고로 광의의 산업보안은 ICT기술뿐만 아니라 산업의 특성을 결정짓는 고유기술이 내재화된 제품(서비스)을 대상으로 보안대책을 수립하는 과정으로 설계된다(자동차 산업보안, 이동통신서비스 산업보안, 의료서비스 보안, 물류서비스 보안, 관광산업 보안 등).

“지난 2차 회의에서 부족 한 점으로 언급되었던 보안과 안전의 차별성에 대한 내용이 반영된 것 같다. 각각의 개념마다 보호 대상도 명확해졌다. 열거된 보안의 개념들을 처음으로 정리하려 시도한 것만으로도 의미 있는 결과라고 생각한다.”

“보안에서 파생된 용어들이기 때문에 보안을 제외한 개념들이 전반적으로 상호 배타성은 낮은 편이나, 보안의 공통적 개념이 내재화 되어 있음을 배제할 수 없다. 정보보안과 사이버보안의 경우 보호대상과 환경의 차이로서 명확하게 구분하니 이들에 대한 차별성 확보에 성공한 것 같다.”

“기업보안은 모든 산업의 기업이 업종에 관계없이 공통적으로 보유하고 있는 자산에 대한 보호활동이고, 산업의 고유한 특성이 반영된 제품(서비스) 개발 과정과 생산 공정 등에 연계된 자산에 대한 보호활동과 고유기술이 내재화된 제품(서비스)에 대한 보안을

산업보안으로 정리하는 것이 적절한 것으로 의견이 모아진다. 또한 이를 세분화하여 자산보호와 손실방지 관점에서 협의적 기술보호와 광의적 산업의 보안으로 구분하여 정리하는 것이 필요하다."

"연구보안의 개념은 중요성에 비하여 아직 정립되지 않은 것 같다. 특히 연 20조 규모의 국가연구개발 사업이 진행되는 현 시점에서 연구관리 전문기관, 연구과제 수행기관(정부출연연구소, 기업부설연구소 등), 연구과제 수행자(연구 책임자, 참여연구원) 등을 대상으로 동일한 보안관점(개념과 범위)에서 다양한 보안활동이 진행될 필요가 있다."

"융합보안 개념은 일정수준의 합의과정 없이 관련된 정부정책에 따라 일방적으로 발표되어 혼용되는 사례가 많았던 것 같다(물리보안 기술과 정보보호 기술의 결합, 예를 들어 지능형 CCTV 등). 이번 기회를 바탕으로 ICT융합제품(서비스)에 대한 보안개념으로 어느 정도의 합의과정이 진행된 것 같다."

Ⅳ. 연구결과 정리와 향후연구

새로운 형태의 보안대상과 보안위험 등이 지속적으로 출현하는 현 시점에서, 보안학문에 대한 관심과 연구 성과물의 증가추세와 부합하여 보안개념들에 대한 시각을 정련화하기 위한 목적의 용어정의와 범위설계 과정은 학문의 지속가능성을 위해 필수조건이라고 판단된다. 따라서 본 연구에서는 혼용되고 있는 다양한 보안개념들에 대해 노출빈도에 따라 우선순위를 부여한 다음, 이들에 대해 개념을 정리하고 그 결과에 대한 전문가들의 합의를 도출하였다. 세부적으로 본 연구는 용어개념정리와 설계에 관한 선행 연구, 보안개념관련 용어 도출, 용어개념 정의와 설계, 수차례 전문가 조사와 합의과정 진행 등을 통해 연구가 진행하였다.

개념정리대상 용어는 '보안'자체용어와 함께 '정보보호', '사이버보안', '기업보안', '산업보안', '융합보안', '연구보안' 등으로 추출되었으며, 이들에 대한 선언적인 개념정의와 범위를 문헌연구를 기초로 정리하였다. 정리된 개념의 적절성을 평가하기 위하여 보안 분야의 10년 이상 전문가를 선정하여 델파이 방법론을 활용하여 조정 작업을 진행하였다. 먼저 적절성 평가는 기준은 용어관련 학문분야의 이론적 배경을 참고하여 명료성, 배타성, 포괄성 등으로 설정하고, 1차 전문가회의에서 양적인 평가를 진행하였다. 이후 2, 3차 전문가회의에서 질적인 평가를 진행하면서 개념 정의와 범위를 조정하였다. 조정회의가 진행되면서 제시된 보안개념관련 용어들 사이에 배타성에 대한 의견이 지속적으로 언급되었으나, 각각 보안개념관련 용어들이 보안자체 개념에서 파생된 용어들이기 때문에 보호환경과 위험요소 등이 융·복합적인 형태로 진화하기 때문에 각각의 개념들 사이에 상호 공통점과 차별성을 동시에 존재함을 확인할 수 있었다. 최종적으로 정리된 보안개념관련 정의와 범위는 <표 7>과 같다.

현재까지의 보안연구는 주로 보안기술, 보안관리, 보안법제도 등 다양한 분야로 확산되고 있으나 그 기초가 되는 이론적 연구는 아직 한계에 머물러 있다. 특히 다양한 의미로 사용되고 있는 보안개념용어들에 대한 정의와 범위에 대한 연구가 아직까지 진행되지 못한 부분은 보안학문이 고유영역을 확보하면서 지속적인 확장을 진행하는데 걸림돌이 될 수 있다. 실제로 현재 일반인을 대상으로 하는 뉴스 기사, 연구 논문과 보고서, 업무문서 등에서 다양한 보안개념용어들이 오·남용되고 있는 관계로 보안의식과 이해수준을 낮추고 있다.

본 연구는 현재 학회 또는 산업현장 등에서 다양한 시각을 가지고 혼용되고 있는 보안개념용어들에 대한 정의와 범위를 설계하고자, 학술중심의 문헌적 연구조사내용을 대상으로 산업현장 중심의 경험적 지식을 반영함으로써 처음으로 적정수준의 합의과정을 이끌어 냈다는 점에서 의의(기여도)를 찾을 수 있다. 이러한 점은 조직의 안정적

〈표 7〉 최종적으로 조정된 보안개념 정의와 범위설정 결과

보안용어	보안개념 정의와 범위
보안	[보안대상] 다양한 환경에 존재하는 가치대상을 [보안위험] 우연적 또는 의도적 범죄행위(위조·변조·탈취·파손 등)로부터 보호하여 [보안목적] 질서와 안녕을 유지하는 활동(지속가능성 확보)
정보보안	(물리적 공간 + 사이버 공간 內) 정보자산에 대한 보호활동 ※ 보호자산 = (컴퓨팅 환경 內) 전자정보 + 일반문서
사이버보안	사이버공간에서 보호대상에 대한 보호활동 ※ 보호자산 = 디지털 신원 + 디지털 정보 + 디지털 경제자산
기업보안	조직의 공통자산(개발과 생산을 간접적으로 지원하는 관리자산) 대한 보호활동 ※ 보호자산 = 경영정보 + 직원 + 시설 + 공간
연구보안	기술개발 과정(연구기획 + 연구수행+ 연구 성과활용)에 대한 보호활동 ※ 보호자산 = 연구원 + 연구내용 + 연구시설과 공간(환경)
산업보안	① (협의적 개념) 핵심기술개발 과정과 산출물에 대한 보호활동(= 기술정보 보호활동) ② (광의적 개념) 핵심기술이 내재화되는 과정과 함께 내재화된 제품(서비스)에 대한 보호활동 (= 조직의 고유자산에 대한 보호활동)
융합보안	① 보안수단들을 연계한(또는 통합한) 보호활동(물리적 보안장치 + IT 보안시스템 + 보안지침) ② ICT기술이 내재된 제품(서비스)에 대한 보호활동

인 보안체계 구축을 지원함으로써, 궁극적으로는 조직의 성과에도 기여할 수 있을 것으로 예상된다 (구자면 등, 2013).

특정용어에 대한 개념정의와 범위설계는 정해진 기준에 따라 임의로 설정되는 것이 아니라, 해당 분야에서 종사하는 좀 더 깊고 넓은 범위에 걸친 전문가들로부터의 사회적 합의과정이 필요하기 때문에 향후에는 본 연구결과로 정리된 보안개념용어들에 대한 추가적인 조정 작업이 필요하다. 또한 환경이 진화함에 따라(예를 들어 컴퓨팅 환경) 가치수준도 변화하고 위험요소도 다양해지기 때문에, 기존에 정리된 보안개념용어들에 대한 지속적인 보정작업과 함께 새롭게 출현한 보안개념용어들에 대한 정의와 범위설계 작업도 추가적으로 요청된다.

참 고 문 헌

[1] 구자면, 박주석, 박재형, “정보보안체계 수립이 Multibusiness 기업성과에 미치는 영향에 관한 연구: IT Relatedness 이론 관점에서”, *Asia Pacific Journal of Information Systems*, 제23권, 제4호, 2013, pp.129-149.

[2] 김정덕, 김건우, 이용덕, “융합보안의 개념 정립과 접근방법”, *정보보호학회지*, 제19권, 제6호, 2009, pp. 68-74.

[3] 리수락, “남북 IT 교류 ; 전문용어 표준화의 원칙과 평가기준”, *정보처리학회지*, 제13권, 제5호, 2006, pp. 54-66.

[4] 박광민, 나원철, “보안에 대한 개념 정립에 관한 연구”, *한국산업보안연구*, 제6권, 제1호, 2016, pp. 123-142.

[5] 이창무, “산업보안 개념의 비판적 고찰”, *한국경호경비학회지*, 제50권, 2017, pp. 285-303.

[6] 정필운, “사이버 보안 특집: 사이버보안이란 개념사용의 유용성 및 한계”, *연세 의료·과학 기술과 법*, 제2권, 제2호, 2011, pp. 1-25.

[7] 최기선, “전문 용어의 표준화-남북 표준에서 시맨틱 웹까지”, *새국어생활*, 제17권, 제1호, 2007, pp. 11-24.

[8] 한진영, 유현선, “경영진의 정보보안 지능이 조직원의 보안대책 인식에 미치는 영향”,

Information Systems Review, 제18권, 제3호, 2016, pp. 137-153.

[9] Cabré Castellví, M. T., "Theories of terminology: Their description, prescription and explanation", *Terminology*, Vol.9, No.2, 2003, pp. 163-199.

[10] Felber, H., "Manuel de terminologie", Organisation des Nations Unies pour l'Education, la Science et la Culture, 1987.

[11] Gordon, T. J.. "The methods of futures research", The Annals of the American Academy of Political and Social Science, Vol.522, No.1, 1992, pp. 25-35.

[12] Nedobity, W., "The general theory of terminology: A basis for the preparation of classified defining dictionaries", *Journal of the Dictionary Society of North America*, Vol.5, 1983, pp. 69-75.

[13] Temmerman, M., *Towards new ways of terminology description: The sociocognitive-approach*, John Benjamins Publishing Company, Philadelphia, PA, 2000.

Information Systems Review
Volume 21 Number 3
August 2019

The Design Research on ICT Security Concepts and Domains

Minseo Jeon* · Hangbae Chang**

Abstract

As the number of security incidents and damages increase steadily, interest in the security of society is growing, and the amount of academic interest and research is steadily increasing. However, despite these concerns and the quantitative increase in research, the terms ‘security’ and ‘safety’ have been mixed and studies have been conducted without the conceptual definition of various security terms being clearly defined. As a result, various forms of security concepts based on ICT environments have been misused. Therefore, we tried to derive the consensus of experts among the various security terms which are mixed in this study, and to summarize the concepts based on the analysis of domestic and foreign documents based on the concept of the terms. Through this research, we intend to contribute to the establishment of the academic identity of security by preventing related mistakes caused by the mixed use of terminology.

Keywords: ***Security Concepts, Security Domains, Cyber Security, Information Security, Convergence Security, Industrial Security***

* Forensic Center, Douzone ICT Group
** Corresponding Author, Department of Industrial Security, Chung-Ang University

◐ 저 자 소 개 ◑

전 민 서 (jms2381@douzone.com)

중앙대학교 일반대학원 산업융합보안 전공으로 석사학위를 취득하였으며, 현재 더존비즈온 포렌식센터 연구원으로 재직 중이다. 주요 관심분야는 Convergence Security, Industrial Security, Digital Forensics 등이다.

장 항 배 (hbchang@cau.ac.kr)

중앙대학교 경영경제대학 산업보안학과 정교수로 재직 중이다. 현재 과학기술정보통신부 블록체인서비스연구센터(ITRC) 센터장을 맡으면서, 보안데이터분석과 서비스, 보안관리체계 연구 등을 진행하고 있다. 관련연구들은 Future Generation Computer Systems, ACM Transactions On Embedded Computing Systems, Electronic Commerce Research, Enterprise Information Systems, Security Journal 등에 논문을 게재하였다.

논문접수일 : 2019년 04월 20일 **게재확정일 : 2019년 06월 18일**
1차 수정일 : 2019년 06월 14일