www.calsec.or.kr
http://dx.doi.org/10.7838/jsebs.2014.19.2.109

지식 네트워크에 근거한 정보보호 점검기준 관계분석

Correlation Analysis in Information Security Checklist Based on Knowledge Network

진창영(Chang Young Jin)*, 김애찬(Ae Chan Kim)**, 임종인(Jong In Lim)***

초 록

정보보안 인식과 중요성이 시대적으로 고조됨에 따라 각 산업부문별로 조직의 정보자산을 보호하기 위해 정보보호 점검기준을 기반으로 한 정보보호 평가・인증 등의 제도가 마련되어 시행되고 있다. 본 논문은 정보보호 점검기준 간의 문맥적인 유사성과 차이점에 대해 규명하기 위하여 지식네트워크를 이용하여 분석한 결과로 ISMS와 PIMS, 금융 IT부문 경영실태평가, 금융 IT부문 보호업무 모범규준, 정보보안 관리실태 평가 상에 나타난 점검기준간의 관계는 다음과 같이 설명할 수 있다. 첫째, 본 논문에서 연구된 정보보호 점검기준은 공통적으로 정보시스템 및 정보통신망에서의 정보자산의 보호와 침해대응, 운영통제에 관한 부분을 다루고 있다. 둘째, 금융권에서는 앞선 공통부분 외에도 IT 경영 및 감사활동에 관한 적정성을 상대적으로 중요하게 다루고 있다. 셋째, ISMS의 점검기준은 PIMS, 금융 IT부문 경영실태평가, 금융 IT부문 보호업무 모범규준, 정보보안 관리실태 평가의 대부분의 내용을 포함하고 있는 것으로 확인된다.

ABSTRACT

As the emerged importance and awareness for information security, It is being implemented by each industrial sector to protect information assets. In this paper, we analyze the information security checklists or security ratings criteria to derive similarity and difference in context which used to knowledge network analysis method. The analyzed results of all checklists (ISMS, PIMS, 'FSS', 'FISS', 'G') are as follows : First, It is common factors that the protection of information systems and information assets, incident response, operations management. Second, It deals with relatively important factors that IT management, the adequacy of audit activities in the financial IT sector including common factors. Third, the criteria of ISMS contains the majority of the contents among PIMS, 'FSS', 'FISS'and 'G'.

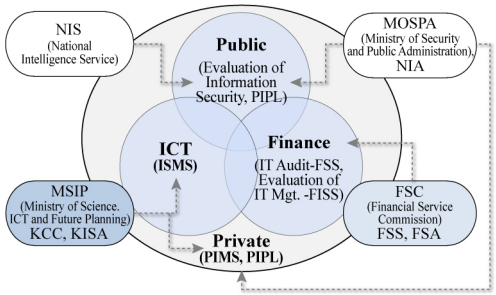
키워드 : 정보보호 점검기준, 지식 네트워크 분석
Information Security Checklist, Knowledge Network Analysis

* CIST(Center for Information Security and Technologies), Korea University, Seoul, Korea (cyjin1048@korea.ac.kr)
** CIST(Center for Information Security and Technologies), Korea University, Seoul, Korea (holytemple@korea.ac.kr)
*** Corresponding Author, CIST(Center for Information Security and Technologies), Korea University, Seoul, Korea(jilim@korea.ac.kr)
2014년 04월 05일 접수, 2014년 05월 01일 심사완료 후 2014년 05월 17일 게재확정.

1. 서 론

정보보호 인식 증대에 따른 시대적 요구와 흐름 속에 각종 정보보안 법규가 제·개정되고 있으며, 이를 근거로 한 정보보호평가 및 인증제도가 시행되고 있다. 국내 정보보안 및 관련 법규는 제정 목적 및 기능에 따라 정립되었으며, 국가기밀보호, 전자서명 및 인증, 정보통신망과 정보시스템의 보호, 침해행위의 처벌, 개인정보보호를 목적으로 정보보호 관련 법률을 분류할 수 있다. 특히 정보보안과 관련 주요 법률은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 정보통신망법), 「정보통신기반보호법」, 「개인정보보호법」, 「국가정보화기본법」, 「전자금융거래법」을 포함하며 이외에 각종 제도와 표준을 합하면 그 종류만 해도 10여 가지에 이른다. 이와 관련된 국내 대표적인 정보보호 인증제도는 정보통신망법에 근거하여 미래창조과학부·한국인터넷진흥원(KISA)이 시행하는 정보통신망에서의 정보자산의 보호를 위한 '정보보호관리체계(K-ISMS)'(미래부 고시 제2013-36호)와 개인정보의 보호를 위한 '개인정보보호관리체계(PIMS)'(방통위 고시 제2013-17호)인증이 대표적이다. 또한, 2014년부터는 「개인정보보호법」에 근거하여 안전행정부·한국정보화진흥원(NIA)의 '개인정보보호인증(PIPL)' 제도가 시행될 예정이다. 그 밖의 금융권은 정보보호 수준 평가제도의 일환으로 매년 「전자금융거래법」 제39조에 따른 금융감독원의 'IT 경영실태평가(IT검사)'를 의무적으로 받아야 하며, 「정보통신기반보호법」, 「전자금융감독규정」과 「금융회사 정보기술(IT)부문 보호업무 모범규준」 따른 취약점 점검·분석을 수행하여야 한다. 이 밖에 공공분야는 매년 국가정보원 지침에 따른 공공부문 '정보보안 관리실태평가'를 의무적으로 받아야 하는 상황이다. 현재 국내의 정보보호 관련 평가제도는 산업분야별로 시행기관이 다르며, 이에 따른 인증(certification)제도도 각각 상이한 모습을 보인다. 이처럼 정보보호 수준 및 성과 향상을 위한 각종 인증제도가 많아지는 추세에 따라 각 조직에서는 이에 상응하는 준법 대응을 위한 많은 시간과 노력이 소요되고 있다.

이에 본 논문은 <Figure 1>과 같이 산업부문별로 시행되고 있는 정보보호 평가·인증제도 내 지표로 활용되는 점검기준에 대한 지식 네트워크 분석을 통하여 각 특성과 관계를 발견함으로써 평가기준별로 준법대응을 위한 전략을 수립하는 데 기초자료로 활용되는 데에 목적이 있다. 이와 관련된 지침과 관련된 문서들의 지식 네트워크 분석을 통하여 핵심어(구)와 유의한 보안통제영역을 식별하고, 각 평가기준의 영역의 공통부문을 특정하여 인증대상 분야별(정보통신, 금융, 공공)로 유의한 평가기준과 그 내용을 분석해본다. 또한, 이에 관한 분석결과를 시각화하여 직관적으로 표현하였다.



〈Figure 1〉 The Status of Information Security Certification in Each Industrial Field(In Korea)

본 논문의 제 2장에서는 지식 네트워크와 정보보호 평가·인증기준 분야에서의 최근 연구결과를 살펴본다. 제 3장에서는 본 논문의 연구방법과 과정을 설명하고, 제 4장에서는 수집한 데이터를 기초로 하여 구성한 지식 네트워크를 실증적으로 분석한 뒤 마지막 제 5장에서 본 논문의 결론을 기술하였다.

2. 관련 연구

2.1 지식 네트워크 분석에 관한 선행연구

과거에는 텍스트분석을 이용한 연구경향 분석은 주제별 내용 분석과 양적 분석이 주를 이루어왔으며, 주제별 내용 분석 방식은 특정 범주로 구분하고 해당 범주를 포함하는 논문의 수를 합산하는 방식인 계량정보학 관점의 분석이 주를 이루었다. 그러나 단순히 키워드나 논문수를 비교하여 시계열적으로 연구 경향을 분석하는 방식은 주제간 관계성을 설명하는 데에 어려움이 있었다[1, 16].

지식 네트워크(knowledge network)는 각종 정보자원을 구성하는 지식 개체의 유형과 패턴에 대해 공간적인 위치나 분포를 보여주는 그래프 또는 네트워크를 말하며, 이것은 지식지도(knowledge map) 또는 과학지도(science map)라 한다. 지식지도는 특정한 정보로부터 지식을 추출해내고자 하는 노력의 결과물 중의 하나이다[8]. 즉, 대량의 지식 정보 내에 숨겨져 있는 특정 유형을 찾아서 의미를 파악할 수 있도록 각종 연구자원에 대한 정보를 네트워크 형태로 구축한 것을 의미한다. 지식 네트워크는 주로 문헌정보학에서 문헌에 포함된 각종 지식개체들을 계량적으로 분석하기 위해 사용해 왔지만, 현재는 정보매체를 다루는 다양한 영역에서 활용되는 추세이다. 네트워크 분석기법(Network Analysis)에 해당하는 분석기법은 대표적으로 연결구조(connection)분석, 중심성(centrality) 분석, 응집구조(cohesion) 분석 등이 활용되고 있다[7, 8, 18].

지식 네트워크 분석방법의 하나로 여겨지는 연결망 분석은 텍스트 네트워크 분석(Text Network Analysis)이라고도 한다. 이는 텍스트 내용 분석을 통해 도출된 단어 간 공출현 행렬을 소셜 네트워크 분석(social network analysis, SNA)의 인접행렬(adjacency matrix)로 적용하여 현상의 구조적 특징을 분석하는 기법이다[3]. 언어 연결망 분석은 구성요소들 간의 관계를 찾아내 시스템의 구조를 파악하는 소셜 네트워크 분석을 공유된 의미를 통해 의사소통 구조를 파악하는데 유용한 방법이다. 텍스트 네트워크 분석은 요소들(nodes)의 상호 연계(link)로 구성된 연결망 구조를 분석하여 현상을 묘사하고 문제를 진단하는데 중점을 두고 있어 변수 간 인과관계를 검증하는 계량분석과는 다르다. 텍스트 네트워크 분석이 복잡하게 구성된 텍스트의 상호 연계 패턴에 초점을 두는 이유는 핵심 단어들의 결합이 단어들 사이의 의미론적 연관(semantic association)을 보여줄 수 있기 때문이다[11].

대표적인 정보학 분야 저자들의 동시인용 사례로는 White[14]의 연구가 있는데, 이 논문에서는 키워드를 나타내는 노드와 노드 사이의 유사성을 텍스트 분석을 통하여 도출한 뒤, 패스파인더(Pathfinder)의 방법으로 시각화하였다. 이에 한국어분석을 위하여 Park[10]은 KrKwic 프로그램을 고안하여, 문헌정보 및 사

〈Table 1〉 Related Work for Knowledge Network Analysis

Researcher	Objective	Data and Research Methodology
White, H. D.[14]	Trend analysis in Informatics	Text analysis in keyword of paper, Visualization by Pathfinder
Park, H. W.[10]	Text analysis in Korean	Introduction to 'KrKwic' Programs and Its application
Choi, Y. C.[1]	Trend analysis in public administration	Content analysis in korea journal public administration from 2005 to 2009, and then network analysis using Netminer
Shim, J. S.[12]	Change Analysis of residents conflict frame near a nuclear power plant	Content analysis using KrKwic, interview data(2005, 2008, 2010, 2011 yrs.) on residents of Go-ri nuclear power plant, network analysis using UCINET6
Wi, C. K.[15]	Detection of illegal anomaly loan	Network analysis using Netminer, in FSS DART(Data Analysis, Retrieval and Transfer) system data on the financial statements

회과학 분야에서의 한국어분석을 위한 기틀을 마련하였다. Choi[1]은 행정학보에 게재된 논문의 초록들의 언어관계를 네트워크 분석하였다. 또한, Shim[12]은 사회관계의 원인 규명을 위해 인터뷰자료를 기반으로 네트워크 분석을 하였다. 최근의 Wi[15]의 연구에서는 전자공시 데이터를 기반으로 불법 금융사기 대출의 이상 징후를 탐지하기 위한 방법으로써 네트워크 분석기법을 소개하였다. <Table 1>에서는 각 연구자의 연구결과를 정리하여 제시하였다.

2.2 정보보호 평가·인증기준에 관한 선행연구

정보보호 평가·인증과 관련한 평가기준과 체계는 미 국방성과 연방정부, NIST에서 고안, 도입하여 오늘날의 ISO27001 표준화 및 ISMS에 커다란 영향을 미쳤다. 대표적으로 미국의 NIACAP(National Information Assurance Certification and Accreditation Process)와 DITSCAP(Department of Defense Certification and Accreditation Process) 제도가 가장 유명하다[18].

Kim[6]은 한국의 IT서비스 환경에서 적용 가능한 클라우드 서비스의 정보보호 관리체계 평가기준에 관한 연구를 수행하였다. NIST 등의 보안연구기관에서 제시한 보안위협 및 통제항목 들의 공통적 요인을 매핑한 후 신규 평가항목을 도출함으로써 국내 클라우드 서비스 제공을 위한 정보보호 관리체계 평가기준을 제안하였다. Kim[4]은 컴플라이언스 위험평가 관점에서 ISO 27001, K-ISMS, 국내 금융회사 정보기술(IT)부문 보호업무 모범규준간의 평가 및 통제항목의 공통요인을 시스템 다이내믹스 기법으로 인과관계를 매핑하며 금융회사에 유의한 정보보호영역의 핵심 평가항목을 산정하고, 의사결정에 따른 정책 평가모형을 제안하였다. 또한, 다음 <Table 2>에서는 나머지 연구자의 연구결과를 정리하여 제시하였다. 또한, Jang[2]의 연구에서는 정보보호 평가기준 간 상관분석의 결과를 후보성과지표로 결정한 뒤, 요인분석과 회귀분석의 통계적 방법으로 금융IT 정보보호 활동의 핵심성과지표를 도출하였다.

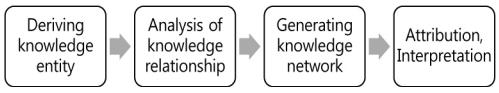
〈Table 2〉 Recent Work for Information Security Ratings Criteria in Korea

Researcher	Objective	Data and Research Methodology
Kim, K. C.[5]	Propose on Smart Grid ISMS ratings Criteria	Propose new security ratings criteria of each industrial field that are analyzed by the standard
Kim, K. C.[6]	Propose on Cloud Service ISMS ratings Criteria	
Kim, A. C.[6]	Propose financial IT ISMS policy assessment model	Correlation analysis using system dynamics for financial information security policies and K-ISMS
Jang, S. O.[4]	Development of Financial IT information security KPI	Regression, factor analysis for deriving KPIregarding financial IT information security regulations

3. 연구 설계

3.1 분석과정 및 사용도구

지식 네트워크는 <Figure 2>와 같은 과정을 통해 분석된다. 먼저 정보자원으로부터 지식개체(knowledge entity)를 추출한다. 지식개체의 예로는 저자, 키워드, 인용, 하이퍼링크 등이 있다. 다음으로는 지식개체들 간의 지식 관계를 파악한다. 공저 관계, 인용 관계, 동시단어 관계, 링크 관계 등이 이에 해당되며, 관계분석이 완료된 뒤에는 지식개체를 노드로, 지식관계를 링크로 하는 지식 네트워크를 생성한다. 생성된 네트워크의 특성을 설명하고 해석함으로써 분석을 완료한다.



〈Figure 2〉 Process in Knowledge Network

본 논문은 텍스트 분석을 위한 도구와 지식 네트워크 분석을 위한 도구를 연계하는 방식을 따른다. 텍스트 분석을 위한 단어 빈도 분석도구로 Park[11]이 공개한 KrKwic을 활용하였다. KrKwic 프로그램은 KrKwic, KrTitle, KrText 등 3개의 하위 프로그램으로 구성되어 있다. 최근에는 64비트 컴퓨터 환경에서 프로그램 기능을 지원하기 위해 Krwords라는 이름으로도 배포되고 있다. 텍스트 분석과정에서 여러 번의 데이터 정제작업이 필요하다. 데이터 정제과정에서는 어간, 조사, 어미 등의 불필요한 수식어구 등은 생략하여 데이터 전처리 과정의 분석대상에서 항목을 제외하였다.

KrKwic을 이용하면 핵심어를 파악할 수 있는데, 핵심어는 선택된 메시지에서 자주 출현하는 단어로 정의할 수 있다. 핵심어는 통상 4~7회 이상으로 다른 핵심어보다 많이 빈출된(more frequent) 것으로 선정하였다. 핵심어가 추출된 후에는 KrTitle을 이용하여 동시출현(co-occurrence) 대칭행렬을 도출한다. 공출현 빈도 행렬이 생성되면 지식관계를 분석한 뒤, 범용 소셜 네트워크 분석(Social Network Analysis : SNA) 도구인 Netminer의 패키지 내의 다양한 함수를 이용하여 연결구조 및 중심성 분석, 구조적 분석을 통하여 핵심어의 특징을 도출한 뒤, 통계적 예측기법을 통하여 연구결과에 대한 해석과 특정을 통하여 결론을 내린다.

3.2 분석대상

본 논문에서는 보안관리의 수행 및 구현도구로 제정된 정보보호정책, 표준, 지침, 절차 중에서 '지침'이나 '절차'에 준용하는 점검기준과 평가・인증 기준에 대해 기술된 문서를 분석대상으로 한다. 법률이나 규정은 정책과 표준에 해당한다고 할 수 있으며, 지침이나 절차는 조직의 상황이나 환경에 따라 변용이 가능하나 원칙적으로 상위의 목표인 정책이나 표준에 위배되어서는 안 된다[9, 13].

이에 분석대상은 정보통신서비스(시스템)에서 국내 정보보호 관리체계인 ISMS(2013. 05. 15)의 기준과 개인정보보호 관리체계의 PIMS 점검기준(2013. 09. 11), 금융권 IT감독 기준인 IT부문 경영실태평가(FSS, 2013. 08. 30)와 금융 IT 보호업무 모범규준(FISS)의 점검기준(2012. 10) 공공부분 정보보안 관리실태 평가의 점검기준(2013)을 지식 네트워크로 분석한다.

4. 지식 네트워크 분석

4.1 점검기준별 분석

본 절에서는 정보보호 관리체계(ISMS)와 개인정보 관리체계(PIMS), 금융 IT부문 경영실태평가 내 항목별 점검기준(FSS), 금융 IT부문 보호업무 모범규준(FISS), 공공부문 정보보안 관리실태 평가(G)의 점검기준에 대한 지식 네트워크의 구조적 분석을 수행한다. 다만, 본 논문에서는 공공부문의 정보보안 관리실태 평가는 분석결과만을 소개한다.

ISMS의 지식 네트워크 노드는 134개로 구성되어 있으며, 중심성 분석으로 도출된 1차 핵심어는 "수립", "보호", "절차", "관리", "시스템"으로 확인된다. 1차 핵심어의 중심성은 0.735 이상을 보인다. 2차 핵심어는 중심성이 0.656 이상으로 "사용", "대책", "검토", "이행"으로 확인된다. 또한, 하위 네트워크 집단 간 분할강도에 따른 Modularity를 이용한 Community 응집구조를 분석한 결과로 3개의 하위 네트워크 그룹(접근통제 및 정보보호정책, 정보시스템 운영 및 침해대응, 위험관리)으로 분류된다.

PIMS의 지식 네트워크 노드는 148개로 구성되어 있으며, 중심성 분석으로 도출된 1차 핵심어는 "관리"와 "보호"이다. 2차 핵심어는 "절차", "사용", "처리", "정책", "접근", "취급", "시스템"인 것으로 확인된다. 또한, 각각의 중심성은 0.684, 0.590으로 ISMS와 비교하였을 때 다소 중심성이 떨어지며, 응집구조의 분석결과로는 3개의 하위 네트워크 그룹(개인정보처리시스템 통제, 개인정보보호정책, 개인정보 수집 및 이용)으로 분류된다.

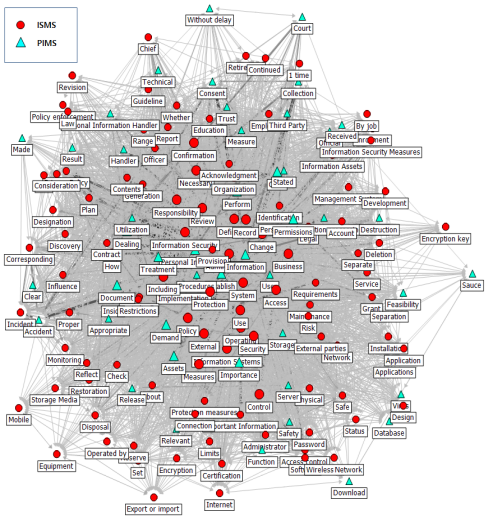
금융 IT부문 경영실태평가에 나타난 점검항목의 지식 네트워크 노드는 165개로 구성되어 있으며, 중심성 분석을 도출된 1차 핵심어는 중심성이 0.757 이상으로 "시스템", "운영", "업무"로 확인된다. 2차 핵심어는 중심성이 0.673 이상으로 "절차", "통제", "내용", "관리", "사용"으로 확인된다. 응집구조 분석결과로 3개의 하위 네트워크 그룹(IT 감사관리, 전자금융 내부통제, 운영관리)으로 분류되었다. 또한, 금융 IT부문 모범규준에 의한 네트워크 노드는 37개로 구성되며, 핵심어는 중심성이 0.556 이상인 "방지", "이상", "조치", "업무", "이용자", "대책"으로 확인된다. 응집구조 분석으로 2개의 하위 네트워크 그룹(침해대응, 접근통제)으로 분류된다. 이에 네트워크 구조 분석의 요약된 결과는 <Table 3>과 같다.

〈Table 3〉 Network Structural Analysis of which Criteria on each Industrial field

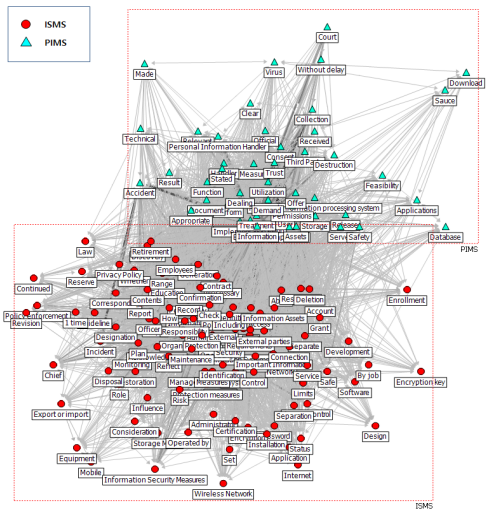
Industrial fields	Criteria	Number of Node(n)	1st keyword	2nd keyword	Number of sub-network(N)	Characteristic of network groups
			Centrality Value			
ICT	ISMS	134	establish, protect, process, management, system	use, measures, review, implement	3	access control/ information system operation and Incident response/ risk management
			0.735	0.656		
ICT/ private	PIMS	148	management, protection	procedures, use, processing, policy, access, treatment, system	3	personal information processing systems control/ privacy policy/ personal information collection and use
			0.684	0.590		
Finance	Evaluation of IT management (FSS)	165	systems, operations, business	procedures, control, information, management, use	3	IT audit management/ electronic financial internal control/ operationsmanagement
			0.757	0.673		
	Financial IT Security Standards (FISS)	37	prevent, anomaly, actions, tasks, users, and measures		2	Incident reponse/ access control
			0.556			

정보통신서비스 및 민간부문에 해당하는 ISMS, PIMS에 대한 2개의 지식 네트워크를 혼합하여 구조를 분석한 결과로 중심성 0.620 이상인 핵심어는 “사용”, “접근”, “정책”, “수행”, “절차”, “관리”, “시스템”, “변경”, “검토”, “업무”, “운영”, “외부”, “책임”, “취급”으로 확인된다. 구성된 네트워크를 시각화 하면 <Figure 3>과 같이 나타나며, 중심성이 큰 노드는 크게 표현된다. 이는 평가기준이 공통적으로 정보시스템의 안전한 사용과 보호 절차의 수립에 중점을 두고 있음을 알 수 있다. 반면에 <Figure 4>는 평가기준에 따른 네트워크의 분류를 나타낸다. 이에 ISMS는 정보통신망에서의 정보보호 및 침해대응에 중점을 두고 있으며, PIMS는 개인정보의 흐름에 따른 관리, 통제, 보호에 초점을 두고 있는 것으로 확인된다.

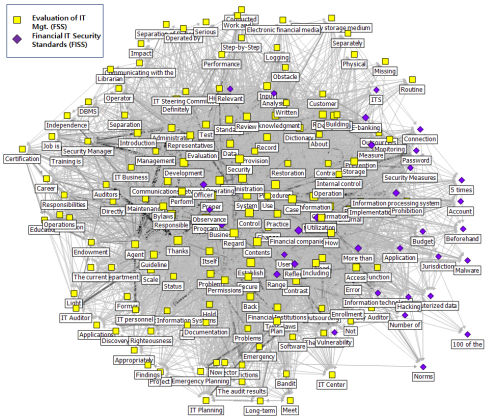
다음, 금융부문에 해당하는 금융 IT부문 경영실태평가 점검기준 및 모범규준에 대한 2개의 지식 네트워크를 혼합하여 구조를 분석한 결과로 중심성이 0.516 이상인 핵심어는 <Figure 5>와 같이 “시스템”, “업무”, “운영”, “통제”, “개발”, “사용”, “수립”, “내용”, “프로그램”, “변경”, “감사”로 확인된다. 이를 토대로 현행 금융권에서의 정보보호 업무 관련 평가기준들은 전자금융 및 시스템에 대한 안전한 개발과 운영, 감사 및 경영 활동의 적정성을 평가하는 것으로 나타난다. <Figure 6>은 평가기준에 따른 지식 네트워크의 분류를 나타낸다. 금융감독원의 점검기준은 IT경영 및 감사활동에 대한 적정성을 검증하는 부분이 나타나며, 이에 수반하는 정보시스템 개발 및 운영 활동을 겸하여 평가하고 있음을 알 수 있다. 또한, 금융IT 보호업무 모범규준에서는 정보시스템 개발 및 운영통제를 보다 중요시하고 있으며, 이는 중심성 지표를 고려할 때 금융감독원의 점검기준과 근접거리에 정보시스템 개발 및 운영통제와 관련된 노드와 밀접히 연결되어 있음을 알 수 있다.



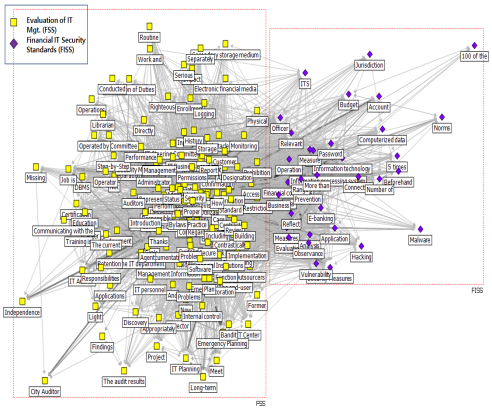
〈Figure 3〉 Knowledge Network of mixed ISMS-PIMS



〈Figure 4〉 Knowledge Network of Classified ISMS-PIMS



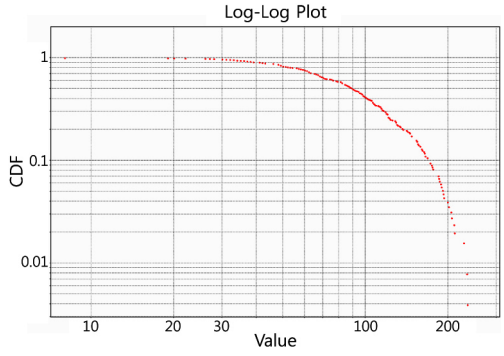
〈Figure 5〉 Knowledge Network of Mixed FSS-FISS



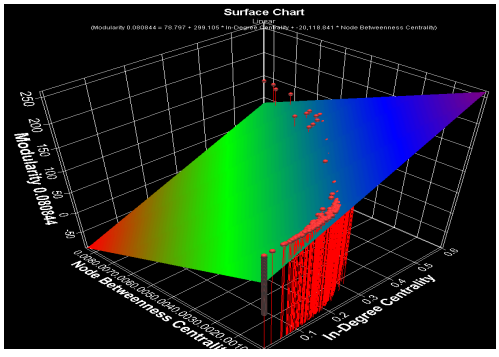
〈Figure 6〉 Knowledge Network of Classified FSS-FISS

4.2 구조적 · 관계적 분석

현실에서 관찰되는 대부분의 네트워크 연결구조는 상위의 20%의 노드가 80%의 연결관계에 있는 불평등한 구조를 갖는 것으로 알려져 있다. 즉, 이러한 불평등의 네트워크를 구성하는 연결 관계가 멱함수 분포(power law)에 근접하면 보다 현실에 가까운 네트워크의 구조에 따르고 있는 것이다[17]. 이에 본 논문은 지식 네트워크가 멱함수의 분포를 따르는 것을 보이고 있으며, <Figure 7>에서 Kolmogorov-smirnov statistic 값은 0.112로 이 값이 작을수록 멱함수의 분포를 따를 확률이 보다 높다. 또한 <Figure 8>에서 응집구조의 정도를 나타내는 Modularity와 인접 중심성(Node Betweenness Centrality)이 선형의 비례관계에 있음을 보이며, 노드의 중심성(Degree Centrality)은 멱함수의 분포를 따르고 있다.



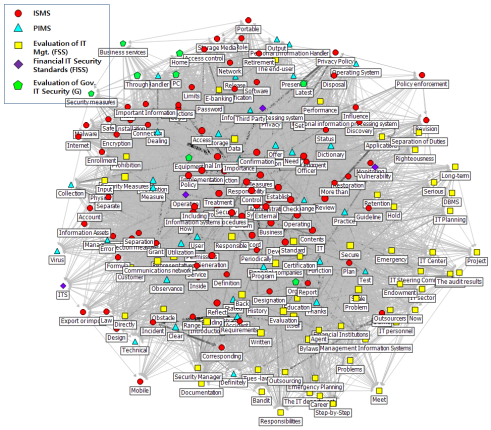
〈Figure 7〉 Verification of Power-Law Distribution



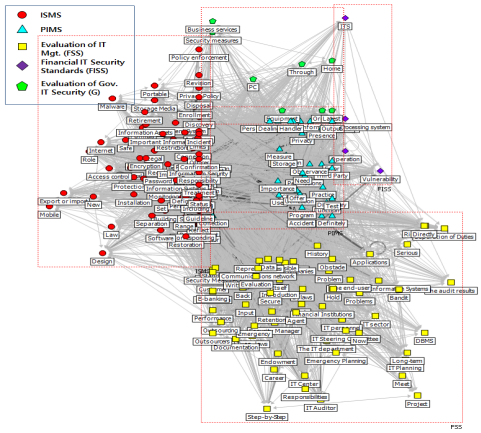
〈Figure 8〉 Surface Chart : Network Connection Indicators by Three-Dimensions

<Figure 9>의 생성된 지식 네트워크는 4개의 영역과 정보보안 관리실태 평가의 점검부문을 혼합하여 총 5개 영역에 대해 혼합한 것으로, 네트워크를 구성하는 391개의 핵심어 노드와 핵심어와 점검기준 간 동시출현 관계 매트릭스를 기반으로 총 24,682개의 링크를 구성되어 있다. 중심성이 0.5 이상인 핵심어는 주로 ISMS 평가기준에서 제안된 것으로 찾아볼 수 있는데, ISMS에서 제시된 평가기준이 타 산업부문의 평가기준과 혼합된 지식 네트워크에서도 중심성이 높은 지표로서 해석된다. 상대적으로 금융감독원의 IT부문 경영실태평가 점검기준은 상대적으로 중심성이 떨어지는 지표로서 나타나지만, 이는 금융권에 업무프로세스 고유의 특성을 반영하여 검사에 적정성 검증에 평가기준이 설계되었기에 발생하는 차이점으로 판단된다.

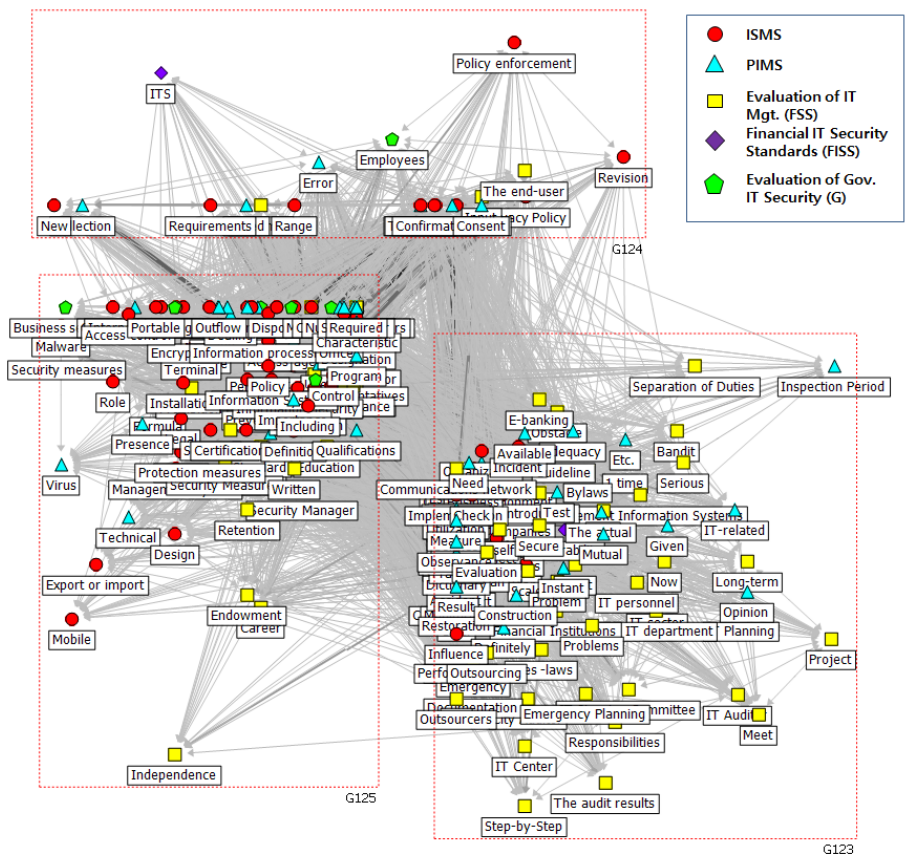
<Figure 10>은 각 평가기준에서 다루는 핵심어를 분류한 내용을 보여준다. 각 평가기준과 핵심어는 각 산업부문별로 중복하여 인용하는 네트워크의 관계에 있으며, 특히 ISMS와 정보보안 관리실태 평가, PIMS, 금융IT 보호업무 모범규준 간에 강한 연결 관계가 있음을 알 수 있다. 이러한 지식 네트워크 내 핵심어의 연결 관계와 분류로 볼 때 ISMS, 정보보안 관리실태 평가, 금융IT 보호업무 모범규준은 정보시스템의 안전성 확보, 침해대응에 관한 점검을 핵심요소로 보고 있다. 또한, PIMS는 개인정보처리시스템의 보호뿐만 아니라 수집-처리-보관-파기 단계에 이르는 프로세스 중심의 절차수립 및 이행여부에 점검요소를 두고 있다. 이와는 상이한 금융감독원의 IT부문 경영실태평가 점검기준은 내부감사 활동의 적정성과 경영전략과의 연계성, 전자금융거래 관련 정보시스템 보호와 업무의 연속성 확보 측면에 보다 중점을 두고 있다. <Figure 11>의 군집화된 지식 네트워크에서 유의한 군집으로 분류된 G123, G124, G135중에서 G123와 G124는 IT 경영 및 감사, 정보시스템 운영통제의 관점으로 군집되고, G124와 G125는 개인정보의 흐름과 절차 및 관리에 관한 관점으로 각각 군집된다. 또한,



〈Figure 9〉 Mixed Knowledge Network



〈Figure 10〉 Knowledge Network Based on Each Criteria



〈Figure 11〉 Clustered Knowledge Network

G123는 금융감독원의 점검기준이 보다 많이 분포하였으며, G125은 ISMS-PIMS로 많은 분포를 보이고 있다(<부록 1> 참조). <Figure 10>, <Figure 11>에서 도출된 핵심어와 분포는 볼 때 금융권에서 현재까지 시행해온 IT부문 경영실태평가는 개인정보보호와 관련된 점검기준의 연결정도나 핵심어의 분포로 볼 때 고객정보보호에 관한 수집-이용-보관-파기 등에 관한 점검부분이 상대적으로 부족하였음을 판단해볼 수 있다. 2014년 1월에 발생한 카드사 개인정보 유출 사태 등은 기존의 전자금융서비스 및 금융 정보시스템 침해가 아닌 금융소비자의 개인정보보호 활동으로도 확장되어야 함을 역설함으로, 이를 위해서는 ISMS와 PIMS의 점검기준을 금융권으로 차용하여 금융권 특성에 맞도록 점검기준을 개발할 필요성이 있다.

4.3 통계적 분류 및 예측

본 절에서는 앞서 생성된 지식 네트워크를 이루는 391개의 핵심어 노드와 24,682개의 링크 정보를 기반으로 데이터마이닝 기법을 적용하여 분석된 결과로 핵심어와 평가기준이

〈Table 4〉 Keyword Reclassification Based on Data Mining Techniques

(Unit : Number of, %)

Techniques \ Criteria	ISMS	PIMS	'FSS'	'FISS'	'G'	Reclassification rate (Total)
Number of original counts	138	84	110	18	41	(391)
k-NN	351	14	26	0	0	59.7%
SVM	109	0	114	168	0	68.4%
Naive Bayes	158	0	66	31	136	65.1%

어떠한 관계를 갖는지 살펴본다. 적용된 데이터마이닝 분류기법은 학술적으로 인정받아 가장 많이 활용되는 k-NN, SVM(Support Vector Machine), 나이브 베이즈(Naive Bayes)의 3가지 분류기법을 이용한다. 분석은 주어진 데이터의 학습과정(machine learning)을 거쳐 일반적인 규칙이나 생성된 지식을 토대로 데이터를 분류한다.

<Table 4>는 데이터마이닝 기법으로 분류된 결과로 3가지 분류기법을 적용하여 도출된 결과를 보여준다. 전체 391개의 핵심어 중에서 ISMS는 138개에 해당하며, PIMS는 84개, FSS는 110개의 분포를 보인다. 재분류 비율(Reclassification rate)은 전체 391개의 핵심어가 갖고 있는 본래의 기준(ISMS, PIMS, FSS, FISS, G)과 데이터마이닝 기법으로 재분류된 속성이 일치하지 않는 핵심어의 개수를 전체의 개수로 나눈 비율을 계산한 것이다. 재분류 비율이 높을수록 본래의 기준에서 재분류로 변경된 비율이 높다는 것을 의미하며, 비율이 낮을수록 본래의 기준과 재분류된 기준이 변하지 않았음을 의미한다.

k-NN 기법으로 분류하였을 때에는 351개로 재분류되어 높은 비율로 ISMS의 평가기준에 매핑되고 있음을 알 수 있으나, SVM의 기법의 경우에는 다소 FISS와 FSS로 재분류되는 경향을 보인다. 그러나 Naive Bayes 기법을 사용한 경우에는 다시 158개로 ISMS에 분류되어 높은 비율로 매핑되고 있음을 확인할 수 있다. 특히, k-NN 기법의 경우에 ISMS의 점검기준이 FSS의 점검기준의 대부분을 포함하는 것으로 볼 수 있으며, Naive Bayes 기법의 경우에도 대부분의 FSS 점검기준이 ISMS와 G로 재분류되는 경향을 보이므로 ISMS와 G의 점검기준 기준이 FSS의 점검기준을 포함하는 것으로 간주된다. 또한, 분석결과로 PIMS의 점검기준은 재분류되는 개수가 매우 적고, ISMS와 FISS의 기준으로 높은 상관관계를 보여 해당 기준으로 재분류되고 있다. 즉, PIMS는 ISMS와 FISS의 점검기준과 높은 상관관계를 보여 그 내용이 유사함을 보인다.

4.4 연구결과 요약 및 시사점

지식 네트워크의 구조적 분석결과로 ISMS는 정보통신망에서의 정보보호 및 침해대응에 중점을 두고 있으며, PIMS는 개인정보의 흐름에 따른 관리, 통제, 보호에 초점을 두고 있는 것으로 확인된다. 금융감독원의 점검기준은 IT경영 및 감사활동에 대한 적정성을 검증하는 부분이 나타나며, 이에 수반하는 정

보시스템 개발 및 운영 활동을 겸하여 평가하고 있음을 알 수 있다. 또한, 금융IT 보호업무 모범규준에서는 정보시스템 개발 및 운영 통제를 보다 중요시하고 있으며, 이는 중심성 지표를 고려할 때 금융감독원의 점검기준과 근접거리에 정보시스템 개발 및 운영 통제와 관련된 노드와 보다 밀접히 연결되어 있음을 나타난다. 각 평가기준과 핵심어는 각 산업부문별로 중복하여 인용하는 네트워크의 관계에 있으며, 특히 ISMS와 정보보안 관리실태 평가, PIMS, 금융IT 보호업무 모범규준 간에 강한 연결 관계가 있음을 알 수 있다.

ISMS, 정보보안 관리실태 평가, 금융IT 보호업무 모범규준은 정보시스템의 안전성 확보, 침해대응에 관한 점검을 핵심요소로 보고 있다. 또한, PIMS는 개인정보처리시스템의 보호뿐만 아니라 수집-처리-보관-파기 단계에 이르는 프로세스 중심의 절차수립 및 이행여부에 점검요소를 두고 있다. 이와는 상이한 금융감독원의 IT부문 경영실태평가 점검기준은 내부감사 활동의 적정성과 경영전략과의 연계성, 전자금융거래 관련 정보시스템 보호와 업무의 연속성 확보 측면에 보다 중점을 두고 있다.

현재까지 시행해온 금융 IT부문 경영실태평가(2013. 08. 30)에는 개인정보보호와 관련된 점검기준의 연결 정도나 핵심어의 분포로 볼 때 고객정보보호에 관한 수집-이용-보관-파기 등에 관한 점검부분이 상대적으로 부족하였음을 판단해볼 수 있다. 또한, 데이터마이닝 기법에 따른 핵심어의 재분류 결과로 ISMS의 점검기준이 FSS의 점검기준들을 대부분 포함하고 있는 것으로 확인된다.

5. 결 론

현재 국내에서 산업분야별로 시행되고 있거나 향후 도입 예정인 정보보호 평가·인증 제도는 국내 정보보호 산업과 특성, 법률과의 관계를 이해할 때 제도의 시행목적을 보다 정확히 이해할 수 있다. 본 논문은 이러한 관점에서 조금 벗어나 평가·인증제도에 나타나는 점검기준간의 문맥적인 유사성과 차이점에 대해 보다 이론적으로 접근하고자 하였다.

지식 네트워크 분석기법으로 도출된 결과로 ISMS의 점검기준 기준이 타 영역의 평가기준인 PIMS, 금융 IT부문 경영실태평가, 금융 IT보호업무 모범규준, 정보보안 관리실태 평가의 대부분의 내용을 포함하고 있는 것으로 확인된다. 이에 전체적으로 재분류되는 비율이 높은 ISMS의 점검기준은 정보보호 수준 측정 및 관리활동에 가장 적합한 평가·인증 기준이라는 점이 확인되고 있다. 그러나 ISMS의 점검기준이 타 영역의 평가기준의 점검기준을 전부 대체하는 것은 아니며, 기준별로 시행되는 인증제도와 점검기준의 중점사항이 상이하였음이 앞선 '연구결과 요약' 부분에 나타난다. 이러한 점을 고려할 때 향후 발전 가능한 한국형 정보보호 관리체계는 산업별 정보보호 평가기준 간 공통영역으로 간주되는 '정보시스템의 보호 및 침해대응'과 '운영통제'에 관하여서는 공통의 영역으로 항목을 개발·관리하고, 금융 및 민간, 공공 등 산업부문별로 특징에 따라 상이하게 고려해야할 보안통제영역에 대해서는 시행기관별로 명시하여 점검기준을 개발·관리하는 것이 보다 효율적일 것이라 판단된다.

References

[1] Choi, Y. C. and Park, S. J., "Trend Analysis on Public Administration Research : Applications of Network Text Analysis methods," The Journal of Korea Public Administration, Vol. 45, No. 1, pp. 123-139, 2011.

[2] Jang, S. O. and Lim, J. I., "Developing key Performance Indicators for Financial IT Security," The Journal of Society for e-Business Studies, Vol. 18, No. 3, pp. 125-142, 2013.

[3] Jeong, J. H. and Kim, D. W., "A research on the methods and target of privacy risk in smart social," Korea Journal of Local Information Society, Vol. 16, No. 3, pp. 113-136, 2013.

[4] Kim, A. C., Lee, S. M., and Lee, D. H., "Compliance Risk Assessment Measures of Financial Information Security using System Dynamics," IJSIA(International Journal of Security and Its Applications), Vol. 6, No. 4, pp. 191-200, 2012.

[5] Kim, K. C. and Kim, S. J., "Evaluation Criteria for Korean Smart Grid based on K-ISMS," Journal of The Korea Institute of Information Security and Cryptology, Vol. 22, No. 6, pp. 1375-1391, 2012.

[6] Kim, K. C., Heo, O., and Kim, S. J., "A Security Evaluation Criteria for Korean Cloud Computing Service," Journal of The Korea Institute of Information Security and Cryptology, Vol. 23, No. 2, pp. 251-265, 2013.

[7] Kim, Y. H., Yoon, J. R., Cho, H. S., and Kim, Y. J., "Structure of Collaboration Network among Korean Scientists-'Small World' and Position Effect," Korea Journal of Sociology, Vol. 41, No. 4, pp. 68-103, 2007.

[8] Lee, S. S., Network Analysis Methodology. Social Science Research Institute, Pusan National University Studies series, Vol. 2, Seoul, 2012.

[9] NIST, SP 800-53, Recommended Security Controls for Federal Information Systems, Oct 2003.

[10] Park, H. W. and Loet Leydesdorff., "Kr-Kwic for Korean content analysis and understanding of the applicable program," Journal of the Korean Data Analysis Society, Vol. 6, No. 5, pp. 1377-1387, 2004.

[11] Popping, R., Computer-assisted Text Analysis. London, Sage Publications, 2000.

[12] Shim, J. S. and Kim, J. S., "Understanding Conflict Frames about a Nuclear Power Plant : Focusing on the Effect of the Fukushima Nuclear Accident," The Journal of Korea Public Administration, Vol. 45, No. 3, pp. 173-202, 2011.

[13] TTA, TTAK.KO-12.0093, A Guide to Establishing Information Security Policies of Organization, Dec 2008.

[14] White, H. D., "Pathfinder networks and author cocitation analysis : A remap-

ping of paradigmatic information scientists," Journal of the American Society for Information Science and Technology, Vol. 54, No. 5, pp. 423-434, 2003.

[15] Wi, C. K., Kim, H. J., and Lee, S. J., "A Study on Detection Technique of Anomaly Signal for Financial Loan Fraud Based on Social Network Analysis," Journal of The Korea Institute of Information Security and Cryptology, Vol. 22, No. 4, pp. 851-868, 2012.

[16] Won, D. K. et al., Development and implementation of knowledge Map in academic social science research area, Korea Institute of Science and Technology Information Research Report, 2009.

[17] Wikipedia, "Power law," http://en.wikipedia.org/wiki/Power_law.

[18] Wikipedia, "NIACAP," http://en.wikipedia.org/wiki/NIACAP.

저 자 소 개

진창영 (E-mail : cyjin1048@korea.ac.kr)
2000년~현재 한국거래소 차장
2013년~현재 고려대학교 정보보호대학원 석사과정
관심분야 금융보안, 정보보호정책

김애찬 (E-mail : holytemple@korea.ac.kr)
2005년~2009년 서울과학기술대학교 산업정보시스템공학과 (학사)
2009년~2011년 육군 정보체계. 망관리장교
2012년~2014년 고려대학교 정보보호대학원 (석사)
2014년~현재 현재 고려대학교 정보보호대학원 박사과정
관심분야 금융보안, 네트워크 보안, 패턴인식

임종인 (E-mail : jilim@korea.ac.kr)
1980년 고려대학교 수학과 (학사)
1982년 고려대학교 수학과 (이학석사)
1986년 고려대학교 수학과 (이학박사)
1986년~2001년 고려대학교 자연과학대학 정교수
2001년~현재 고려대학교 정보보호대학원 원장, 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 안전행정부 정책자문위원회 위원, 방송통신위원회 인터넷협의회 운영위원 등
관심분야 정보법학, 디지털포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등