Review Paper
Informatization Policy Vol. 30, No.4 (2023), pp.003-039
https://doi.org/10.22693/NIAIP.2023.30.4.003

문헌 분석을 통한 정보보안 감사 분야의 국내 및 국제 연구동향 분석

소 영 재* · 황 경 태**

요 약 정보/정보시스템의 중요성이 높아지면서, 정보보안에 대한 중요성이 강조되고 있고, 조직에 적합한 정보보안 수준을 유지하기 위한 도구로서 정보보안 감사의 중요성 또한 높아지고 있다. 본 연구의 목적은 정보보안 감사 분야의 국내외 학술 논문들을 분석하여 전반적인 연구 현황을 살펴보고 향후 연구 분야를 제시하는 것이다. 이를 위해 총 103편의 국내외 논문을 일반 기준과 연구 주제 관련 기준을 바탕으로 분석하였다. 주요한 분석 결과로는 연구 방법적인 측면에서 이 분야의 이론적인 발전을 위해 실증 연구의 비중을 높일 필요가 있다. 연구의 내용적인 측면에서 보면, 연구주제 '감사인/감사조직'의 경우, 연구의 누적적인 발전을 위해 역량과 같은 변수들에 대한 프레임워크를 제시하는 연구가 필요하다. 연구 주제 '감사 활동/절차'에 대해서는 감사의 세부 활동 과정/결과를 분석하는 연구를 수행할 필요가 있다. 연구 주제 '감사 대상'의 경우에는 해외 연구에서 분석한 신기술/특정 산업/특정 보안분야 등을 주목해 볼 가치가 있다. 연구 주제 '감사 목적/효과'의 경우, 현재 연구마다 서로 다르게 조작화되고 있는 성과/품질을 종합적이고 체계적으로 정의하는 연구가 필요하다. 연구 주제 '감사 기준/지침'의 경우, 국내에서는 2016년 이후로 지침/모델에 대한 연구가 없으므로, 지속적인 관심이 필요하다.

주제어 : 정보보안 감사, IT보안 감사, 정보보안 감리, 감사, 연구 동향

Analysis of Research Trends of the Information Security Audit Area Through Literature Review

So, Youngjae* · Hwang, Kyung Tae**

Abstract With the growing importance of information/information system, information security is emphasized, and the significance of information security audit as a tool for maintaining the proper security level is increasing as well. The objectives of the study are to identify the overall research trends and to propose future research areas by analyzing domestic and overseas research in the area. To achieve the objectives, 103 research papers were analyzed based on both general and subject-related criteria. The following are the major research results : In terms of research approach, more empirical studies are needed; For subject "Auditor," studies to develop a framework for related variables (e.g., capability) are needed; For subject "Audit Activities/Procedures," future research should focus on the process/results of detailed audit activities; Future domestic research for "Audit Areas" should look for the new technology/industry/security areas covered by foreign studies; For "Audit Objective/Impact," studies to define the variables (e.g., performance and quality) systematically and comprehensively are needed; For "Audit Standard/Guidelines," research on model/guideline needs to be continued..

Keywords : information security audit, IT security audit, information systems security audit, audit, research trends

Received Oct 31, 2023; Revised Nov 21, 2023; Accepted Nov 21, 2023

* Ph.D. Student, Dept. of MIS, Donnguk University-Seoul Campus (julianso@dongguk.edu, https://orcid.org/0009-0000-0257-4751)
** Corresponding Author, Professor, Dept. of MIS, Donnguk University-Seoul Campus(kthwang@dongguk.edu, https://orcid.org/0009-0000-7540-9458)

I. 서론

조직의 운영 및 관리에 있어서 보안은 전통적으로 그 중요성이 매우 높다. 보안의 대상 중에서도 정보 및 정보시스템이 조직 운영에 핵심적인 위치를 차지하게 되면서, 정보보안에 대한 관심과 중요성 또한 매우 높아지고 있다(Hwang & Kim, 2016). 조직에서 정보보안을 확보하기 위한 핵심 방안 중의 하나는 보안에 대한 정책과 가이드라인을 수립하는 것이다. 그러나 이러한 정책이 실효성을 발휘하기 위해서는, 수립된 정책이 잘 적용되고 실행되고 있는지, 조직의 전반적인 보안 상태는 어떠한지 등을 확인하고 검증하는 활동이 필요하고, 정보보안 감사가 바로 이러한 기능을 수행하는 중요한 활동이다.[1)]

정보보안 감사는 보안 사고로 인한 비용이나 기타 손실의 발생 없이 조직의 정보보안 상태를 파악할 수 있는 최선의 방안 중의 하나이다(Popescu, et al., 2008). 또한 정보보안 감사는 조직이 자신들에게 적합한 보안 수준이 무엇인지를 파악하고, 이를 달성하고 유지하기 위한 도구이다(Min & Lee, 2016; Tofan, 2011). 이러한 정보보안 감사는 조직 관리의 효과성을 체계적이고 일관성 있게 향상시킴으로써 조직이 목표를 달성하는 것을 지원한다(Grzyb & Kowalik, 2020). 따라서 민간 기업과 공공 기관, 더 나아가서 사회에 큰 영향을 미칠 수 있는 정보보안 감사에 관한 학술 연구의 동향을 살펴보는 것은 이론적으로나 실무적으로 의미있고 중요한 일이다.

특정 연구 분야의 상태를 주기적으로 검토하고 분석하여 전반적인 추세와 변화를 식별하는 것은 중요한 작업이다(Palvia, et al., 2017). 특정 분야의 연구에 대한 리뷰 논문은 해당 분야의 문헌들에서 제시하는 내용들을 분석하여 정리하고, 이 분야에서 향후 연구가 필요한 부분을 식별하는 역할을 수행한다. 이러한 리뷰 논문은 학술적으로 필요성을 인정받고 있는데, 경영정보학 분야의 예를 들면, 2000년~2014년 사이에 전세계 40개 상위 학술지 중에서 36개의 학술지에서 적어도 한 편 이상의 리뷰 논문을 게재하였고, 2000년 이후 200개 이상의 리뷰 논문이 상위 저널에 게재되었다(Schryen, et al., 2017).

본 연구의 목적은 정보보안 감사 분야에서 국내 및 해외에서 수행된 학술 논문들을 식별하고 분석하여 전반적인 연구 현황을 살펴보고 국내외의 연구 동향을 비교 분석하여, 향후 연구의 필요성 및 세부 분야를 식별하여 제시함으로써, 정보보안 감사 분야의 이론 발전에 기여하고, 이 분야의 실무적인 발전에 도움을 줄 수 있는 기반 정보를 제공하는 것이다.

이러한 연구 목적을 달성하기 위한 본 논문은 다음과 같이 구성된다. 다음의 제Ⅱ장에서는 본 연구의 수행 방법을 설명하는데, 여기에는 본 연구의 대상이 정보보안 감사의 의미/개념 정의, 관련 연구 문헌 수집 방법/결과, 분석 기준 등이 포함된다. 분석 기준에는 발간연도, 연구 방법 등과 같은 일반적인 기준과 정보보안 감사 분야의 주요한 연구 내용을 파악하기 위한 연구 주제에 관한 분류 기준이 포함된다. 제Ⅲ장에서는 위에서 수립한 기준을 바탕으로, 식별된 연구 문헌을 분석한 결과를 정리한다. 마지막으로 제Ⅳ장은 본 연구의 결론으로서, 연구의 주요 결과를 정리하고, 이 분야의 향후 연구 방향을 제시하고, 본 연구의 한계에 대해 설명한다.

II. 연구 방법

본 장에서는 먼저 본 연구의 대상인 정보보안 감사를 정의하고, 관련 용어들을 정리한다. 다음으로는 본 연구의 분석에 포함된 정보보안 감사에 관련된 연구 문헌을 식별하여 수집한 방법과 절차에 대해 설명한다, 마지막으로는 수집한 문헌의 분석 기준에 대해 설명한다.

1) 정보보안 감사의 정의에 대해서는 다음의 II장에서 자세하게 정리한다.

1. 정보보안 감사의 의미와 개념 정립

기본적으로 감사란 하나의 기준이나 일련의 가이드라인을 준수하고 있는지, 관련 기록이 정확한지, 효율성/효과성 등의 목표를 달성하고 있는지 등의 여부를 공식적으로 조사하고 검증하는 활동이다(OGC, 2007; Suduc, et al., 2010). 이러한 감사 활동 중에서 정보보안 감사는 다음과 같이 다양하게 정의되고 있다.

- 조직 정보의 기밀성/가용성/무결성을 보장하고 있는 방법을 감사(Popescu, et al., 2008).
- 조직의 정보 자산의 기밀성/무결성/가용성을 확보하기 위한 방법에 초점을 맞추고, 보안 정책의 준수 여부를 파악하기 위한 기술적인 평가(Dharmalingam & Smalov, 2016)
- 정보 인프라의 정량적/정성적 특성에 대한 정보를 수집하여, 정보시스템의 보안 수준을 평가하고, 그 결과를 바탕으로 정보보안 시스템에 대한 권고사항과 개발 프로그램을 개발(Gulzira, et al., 2020).
- 독립적인 정보보안 전문가들이 조직의 위험 통제가 위험 평가를 바탕으로 적절하게 수행되고 있는지의 여부를 평가하고 자문을 제공(Satoh & Komoda, 2005).
- 정보보안 시스템에서 취약점을 식별하고, 이를 바탕으로 정보보안 시스템의 보호 기능을 개선하는 활동(Raggad & Collar, 2006; Ivanova, et al., 2010).
- 정보시스템의 안정성과 신뢰성을 보장하기 위하여 정보시스템의 구축과 운영을 포함한 전 과정에 걸쳐 정보보안의 문제점을 식별하고 개선사항을 도출하여 시정토록 하는 것(Lee, et al., 2010)

위의 정의들을 종합해 보면, 정보보안 감사는 독립적인 감사인이 조직의 정보보안 시스템의 강약점을 평가하고, 이를 바탕으로 개선사항과 권고사항을 제시하고, 이를 이행하도록 하는 활동으로 정의할 수 있다. 이러한 정보보안 감사와 유사한 용어로는 IT 보안 감사(IT Security Audit), 정보시스템 보안 감사(Information System Security Audit) 등이 있고, 국내에서 많이 시행되고 있는 정보시스템 감리 영역 중에서 보안 감리가 여기에 속한다. 본 논문에서는 이러한 관련 용어 및 개념을 통합하여 정보보안 감사라는 용어를 채택하여 일관되게 사용하도록 한다.

2. 연구 방법

본 연구에서는 문헌고찰 연구 분야의 선행 연구를 바탕으로 연구 방법을 설정하였다(Kim & Cho, 2012; Lee & Myung, 2013). 먼저, 본 연구의 분석 범위와 그 범위에 포함된 연구문헌의 수집 방법을 결정하였다. 여기에 대해서는 다음의 '1) 관련 문헌 수집 방법 및 결과'에서 자세하게 설명한다. 다음으로는 정보보안 감사 분야에서 수행된 연구의 방법과 내용 두 가지 측면을 분석하기 위한 기준을 수립하였다. 분석 기준을 바탕으로 본격적인 분석을 하기에 앞서서 파일롯 테스트를 통해 기준을 수정 보완 후 최종 결정하였다. 이것은 다음의 '2) 분석 기준'에서 자세히 설명한다. 최종적으로 결정된 분석 기준을 바탕으로 수집된 문헌들을 분석하였고, 그 결과는 다음의 'III. 분석 결과'에 정리되어 있다.

1) 관련 문헌 수집 방법 및 결과

본 연구에서는 구글 학술검색엔진(Google Scholar)을 이용하여, 정보보안 감사에 관련된 국내외 문헌을 식별하고 수집하였다. 2022년 4월 5일에 검색을 수행하였는데, 외국 문헌의 경우에는 문헌 제목에 'Information Security Audit', 'IT Security Audit', 'Information System Security Audit' 등의 용어를 담고 있는 문헌들을 검색하였다. 검색 결과, 각 키워드 별로 163편, 8편, 9편 등 총 180편의 문헌이 식별되었다. 국내 문헌의 경우에는 '정보보안 감사', '정보보호 감사', '보안 감리' 등의 용어를 제목에 포함하고 있는 문헌을 검색하였고, 그 결과 각 키워드 별로 10편, 7편, 8편으로 총 25편의 문헌이 식별되었다.

식별된 문헌들 중에서 일차로 논문의 형식을 검토하여, 책, 보고서, 백서, 학위논문, 유관단체에서 발표한 원고, 언론 매체의 기사, 학술대표 발표논문 중 이후에 학술지에 출간된 논문, 영문 이외의 외국 언어(예: 중국어, 러시아어 등)로 작성된 문헌 등을 제외하였다. 그 다음으로 위의 기준을 통과한 논문들의 내용을 검토하여 정보보안 감사에 관련이 있는 논문인지를 재검토하였다. 논문의 초록을 읽어보고 내용을 명확하게 파악하기 어려운 경우에는 논문의 본문을 검토하였다. 내용 파악 후 논문 제목에는 Audit(또는 감사)이라는 용어가 포함되어 있으나, 정보보안 감사와 관련성이 없는 논문은 제외하였다.[2)]

이러한 과정을 거쳐 본 연구의 최종 분석 대상으로 식별된 논문의 수는 해외 논문 82편, 국내 논문 21편(합계 103편)으로 집계되었다.

2) 분석 기준

본 연구에서는 정보보안 감사에 관련된 연구 문헌들의 형식과 내용을 체계적으로 분석하기 위해 다음과 같은 분석 기준을 채택하였다. 먼저, 문헌들의 형식을 분석하기 위한 일반적인 기준으로서, 문헌 분석 연구에서 흔히 사용한 항목들을 차용하여 논문의 출간년도, 실증 연구 여부, 세부 연구방법 등을 채택하였다(Lee, et al., 2012; Lee, et al., 2014; Kim & Hwang, 2021). 이러한 일반 분석 기준은 다음의 〈표 1〉에 정리되어 있다.

출간년도는 해당 논문이 발표된 시기를 나타낸다. 연구 접근방법은 실증(Empirical) 연구와 비실증(non-Empirical) 연구를 구분한다. 실증 연구란 현상에 대한 데이터나 관찰을 기반으로 연구를 수행하는 것이고, 비실증 연구란 현상에 대한 관찰보다는 연구자의 아이디어나 개념에 의존하여 연구를 수행하는 것이다(Alavi & Carlson, 1992). 실증 연구와 비실증 연구의 세부 연구방법은 Alavi and Carlson(1992)의 분류 방법에 따라, 실증 연구의 세부 연구방법은 서베이(Survey), 사례연구(Case Study), 2차 데이터(Secondary Data) 분석 등으로, 비실증 연구는 개념(Conceptual) 모델, 수리/공학(Mathematical/Engineering) 모델, 튜토리얼/리뷰(Tutorial/Review) 등으로 분류한다.

다음으로 관련 연구 논문들의 구체적인 내용을 검토하기 위한 연구 주제에 관련된 기준은 Kim and Hwang(2021)의 기준을 차용한다. 이 기준은 정보보안 감사의 전체적인 상황과 맥락을 파악할 수 있는 항목들

〈표 1〉 일반 분석 기준
〈Table 1〉 General Analysis Criteria

Analysis criteria	Explanation	Analysis item
Publication year	Publication year of the research article	Year when the research article is published
Research approach	Empirical vs. non-empirical	Whether the research is empirical or non-empirical
Research method of the empirical study	Detailed research method of the empirical research article	Surveys, case study, secondary data analysis, etc.
Research method of the non-empirical study	Detailed research method of the non-empirical research article	Conceptual model, mathematical/engineering model, tutorial/review, etc.

2) 예: 특정 기준(CobiT 또는 ISO/IEC 27001)을 바탕으로 특정 조직의 정보보안 수준을 분석한 논문

〈표 2〉 연구 주제에 관한 분석 기준
〈Table 2〉 Analysis Criteria for Research Topics

Analysis item	Explanation
A (Auditor/Audit Organization)	Subjects related to auditors (or audit organizations/entities) - Characteristics, capabilities, relationship with the auditee, time invested, etc.
Audits (Audit Activities/Procedures)	Subjects related to the performance of audit activities - Basic concepts, audit activities, audit procedures, etc.
B (Audit Area)	Subjects related to the area being audited - Overall areas, specific industry, specific technology/system, etc.
C (Audit Objective/Effect)	Subjects related to the objectives or effects (performance) of audit - Need for audit, objective, effect(performance), and quality of audit
D (Audit Standard/Guidelines)	Subjects related to guidance applicable to the audit process - Standard/Criteria, tools/techniques, models, guidelines, etc.

을 담고 있는데, 그것은 다음과 같은 명제로 구성된다.

A Audits B for C by D

이 명제에서 첫째 A(감사인/조직)는 정보보안 감사를 수행하는 감사인 또는 감사조직을 나타낸다. 여기에는 감사인의 특성에 관련된 요인(역량 등), 감사인과 피감사인과의 관계 요인, 감사인의 투입시간 등이 포함될 수 있다. 둘째 항목인 Audits(감사 활동/절차)는 정보보안 감사를 수행하는데 관련된 활동과 절차를 말한다. 이 항목에는 정보보안 감사의 기본 개념, 수행 활동, 수행 절차 등이 포함된다. 셋째 B(감사 대상)는 정보보안 감사의 대상 영역을 나타낸다. 대상 영역은 여러 가지 구분될 수 있는데, 예를 들면, 특정 세부 분야 없이 전반적 대상, 특정 산업, 특정 기술, 특정 시스템 등이 될 수 있다. 넷째, C(감사 목적/효과)는 정보보안 감사의 목적으로서, 여기에는 정보보안 감사가 필요한 이유/중요성, 정보보안 감사의 목적/효과/품질 등이 포함된다. 마지막 항목인 D(감사 기준/지침)는 정보보안 감사를 수행하는데 적용 및 활용되는 감사 기준/지침 등을 말한다. 이 명제의 각 구성요소의 의미와 세부 내용은 위의 〈표 2〉에 정리되어 있다.

Ⅲ. 분석 결과

분석 대상으로 결정된 103편의 논문을 대상으로 리뷰 논문에서 일반적으로 적용하는 절차에 따라 분석을 수행하였다. 먼저, 분석 기준의 명확성을 확인하고 필요시 기준을 정교화하기 위해, 103편의 논문 중에서 해외 논문 10편, 국내 논문 5편을 무작위로 선정하여, 본 논문의 저자인 2명의 연구자들이 각자 독립적으로 분석한 후, 그 결과를 검토하였다. 두 연구자의 분석 결과를 검토해보니, 해외 논문 2편, 국내 문헌 1편에서 일부 항목에 서로 차이가 있었고, 해당 항목의 분석 기준의 의미에 대해 서로 토의한 후에 분석 기준에 대한 상호간의 이해를 높이고, 이를 바탕으로 합리적인 분류 항목을 채택하였다. 그 이후 나머지 모든 연구 문헌에 대한 분석을 수행하였고, 해외 논문 6편, 국내 문헌 1편에 대해 일부 항목에 두 연구자의 분류 결과에 차이가 발생하였고, 사전 검토와 동일한 절차를 통해 합리적인 분류를 채택하였다.

분석은 국내외의 모든 문헌 전체에 대해 수행하고, 그 외에도 국내외의 연구 동향에 차이가 있는지를 파악하기 위해 국내외의 연구를 비교 분석하였다. 다음에서

는 분석 결과를 제시하는데, 먼저, 일반 기준을 바탕으로 수행된 분석 결과를 제시하고, 다음으로는 연구 주제에 대한 분석 결과를 정리한다.

1. 일반 기준에 의한 분석 결과

1) 논문 발간연도

논문 발간연도를 5년 단위로 구분하여 집계한 결과가 다음의 〈표 3〉에 정리되어 있다. 전체적으로 보면, 1990년대(해외의 경우 1998년, 국내의 경우 1993년)에 이 분야의 연구가 시작되어 역사가 30년이 안 된 비교적 새로운 연구 분야라는 것을 알 수 있다. 그러나 매년 꾸준히 연구되고 있으며 연구 편수가 증가하는 추세를 보이고 있다.

해외 연구와 국내 연구를 발간연도별로 비교해 보면, 해외의 경우, 1998년에 최초의 연구가 발표된 이후, 꾸준히 증가하고 있고, 비교적 최근인 2016~2020년의 기간 동안 가장 활발하게 수행된 것을 알 수 있다. 가장 최근 시기인 2021년 이후를 살펴보면, 2021년 한 해 동안 6편의 연구가 발표되어, 단순 추정하더라도 전기와 최소한 동일한 수준이거나 성장이 예상되므로, 최근까지 이 분야의 연구가 지속적으로 수행되고 있고, 증가 추세인 것으로 판단된다.

이에 비해 국내 최초의 연구는 1993년에 발간되어, 해외보다 5년이나 앞서 발표되었다. 그 이후 2006~2010년의 기간 동안에 가장 활발하게 수행된 이후 감소 추세를 나타내고 있고, 가장 최근에는 연구 실적이 없는 상황이다. 국내의 연구는 해외보다 먼저 시작되었고, 활발하게 수행된 기간도 해외에 비해 10년 이상 빨랐으나, 해외의 경우에는 아직까지 이 분야의 연구가 지속적으로 수행되고 있는데 반해, 국내의 경우에는 2016년부터 감소하여 최근에는 수행 실적이 없다.

국내의 연구가 최초로 수행된 시기나 가장 활동하게 수행된 시기가 해외에 비해 빨랐던 이유는 국내의 정보보안에 관련된 주요한 연혁에서 유추해 볼 수 있다. 우리나라의 경우, 연구가 가장 활발하게 수행되기 시작한 2006년 이전에 이미 정보보안에 관련된 제도나 법규가 상당히 정비되었다. 정보보안 관련 법률의 경우, 1995년에 제정된 '정보화촉진기본법'으로 정보보안에 관한 기본적인 규정이 마련되었고, 그 이후로 1999년에 「국가정보통신보안기본지침」이 제정되었고, 2001년에는 「정보통신망 이용촉진 등에 관한 법률」이 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」로 개정되었고, 정보보호 관리체계 인증제도(Information Security Management System: ISMS)가 도입되었다(Kim, 2014; NCSC, 2022). 정보보안 관련 조직 측면에서도 1996년에 한국정보보호센터(현재의 한국정보보호진흥원(KISA)), 1998년에 한국정보보호산업협회, 2000년

〈표 3〉 발간 기간별 연구편수(비율)
〈Table 3〉 Number (Ratio) of Papers by Period

Period	All	Overseas	Domestic
Before 2000	5 (4.9%)	2 (2.4%)	3 (14.3%)
2001~2005	8 (7.8%)	5 (6.1%)	3 (14.3%)
2006~2010	23 (22.3%)	16 (19.5%)	7 (33.3%)
2011~2015	27 (26.2%)	21 (25.6%)	6 (28.6%)
2016~2020	33 (32.0%)	31 (37.8%)	2 (9.5%)
After 2021	7 (6.8%)	7 (8.5%)	0 (0.0%)
Total	103 (100.0%)	82 (100.0%)	21 (100.0%)

에 국가보안기술연구소(NSRI), 2004년에 국가사이버안전센터(NCSC) 등의 정보보안 관련 기관들이 설립되었고, 1990년에 한국통신정보보호학회(현재의 한국정보보호학회), 2001년에 한국사이버테러정보전학회 등의 관련 학회들도 구성되었다. 이처럼 정보보안 분야의 기반이 구축되면서, 이를 바탕으로 학술 연구 또한 활발하게 수행된 것으로 풀이된다.

그 이후 시기의 주요한 연혁을 살펴보면, 2011년에 「개인정보보호법」이 제정되고, 개인정보보호위원회가 출범하고, 개인정보보호 관리체계 인증제도(PIMS) 도입되었다. 2013년에는 정보보호최고책임자협의회(Chief Information Security Officer: CISO)가 출범하였고, 2015년에는 「정보보호산업의진흥에관한법률」이 제정되었다. 그 후에는 새로운 법률/제도의 제정보다는 기존의 것을 보완하기 위한 개정 작업들이 주를 이루고 있는데, 예를 들면, 2016년의 정보보호 관리체계 인증 의무 대상을 교육·의료 분야로 확대, 2018년의 정보보호 및 개인정보보호 관리체계인증(ISMS-P) 통합, 2020년의 '데이터 3법(「개인정보 보호법」, 「정보통신망법」, 「신용정보법」)' 개정 등을 들 수 있다(NCSC, 2022).

이처럼 국내의 학술 연구 추세가 정보보안 분야의 현실과 유사한 패턴을 나타내는 것은 경영학 분야의 학술 연구는 선행적으로 실무를 주도하기 보다는 실무에서 나타나는 현상들을 후행적으로 분석한다는 일반적인 경향과 일치하는 결과이다(Alavi & Carlson, 1992; Gill & Bhattacherjee, 2009).

또한 국내의 연구가 해외에 비해 일찍 시작되어 빨리 감소하는 현상은 우리나라의 기업이나 조직들은 혁신적인 개념이나 기법들을 다른 나라들에 비해 더 빨리 도입하는 얼리 어답터(Early Adopter)이지만, 도입 이후 지속적인 개선과 내재화보다는 또 다른 혁신으로 신속히 전환하는 경향이 이 분야의 연구에서도 적용된 것으로 판단된다(Lee, et al., 2012).

국내의 연구 수행 건수는 해외의 1/4 수준에 머물고 있고, 여전히 조직과 기업에서 정보보안의 중요성이 감소하기보다는 증가하고 있는 현실을 감안한다면, 이 분야에 대한 학술적인 연구가 지속적으로 이루어져야 할 것이다.

2) 전반적 연구 접근방법

정보보안 감사 분야 연구의 전반적인 연구 접근방법을 전체, 해외, 국내로 구분하여 분석한 결과는 다음의 〈표 4〉에 정리되어 있다.

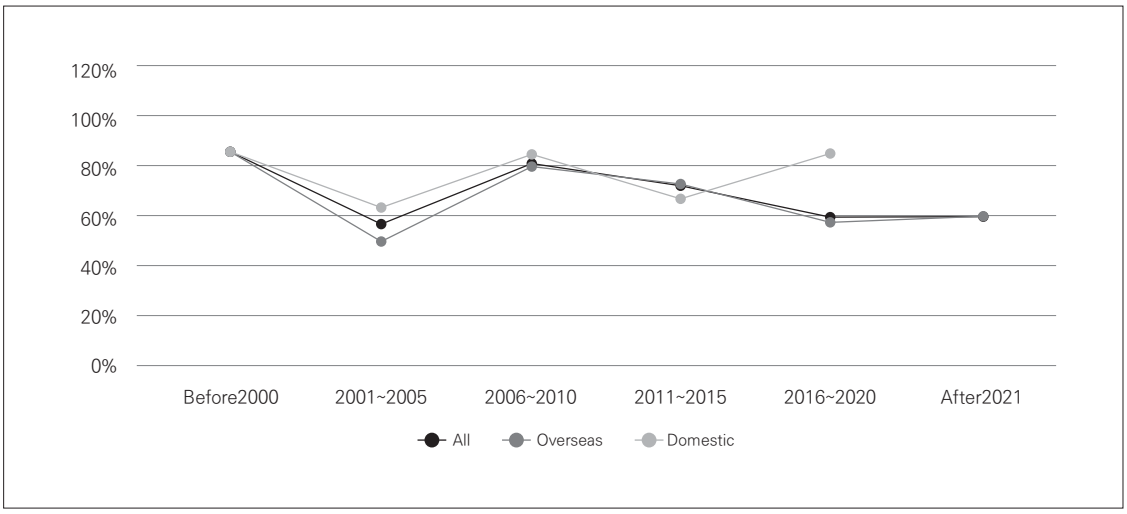
표에서 볼 수 있는 바와 같이, 정보보안 감사 분야의 연구는 비실증 연구의 비중이 80% 이상으로 절대적이고, 국내 연구의 경우에는 그 비중이 90% 이상으로 더욱 치중되어 있음을 볼 수 있다.

연구의 진화 과정은 비실증 연구로부터 출발하여 실증 연구로 발전해 가는 것이 일반적이다(Kim, et al.,

〈표 4〉 전반적인 연구 접근방법의 분포
〈Table 4〉 Distribution of Research Approach

Approach	All	Overseas	Domestic
Empirical	20 (19.2%)	18 (22.0%)	2 (9.1%)
Non-empirical	84 (80.8%)	64 (78.0%)	20 (90.9%)
Total	104 (100%)[3]	82 (100%)	22* (100%)

3) 표본의 전체 논문 편수는 103편이나, 한 국내 연구가 실증/비실증 방법을 병용한 관계로 104편이 됨 (따라서 국내 논문의 수도 21편이 아니라 22편이 됨)



〈그림 1〉 비실증 연구 비중의 변화 추이
〈Fig. 1〉 Patterns of Ratio of Non-empirical Research

2005; Shao, et al., 2010; Kim & Hwang, 2017). 즉, 이론 정립의 초기 과정에서는 해당 분야의 관련 개념을 설명하고 관련 변수를 식별하는 등의 비실증적인 탐색적(Exploratory) 연구가 많이 수행되고, 이를 바탕으로 해당 분야의 관련 변수들 간의 관계를 설명하는 서술적(Descriptive) 연구와 더 나아가서 변수들 간의 인과관계를 제시하는 설명적(Explanatory)인 실증 연구의 비중이 높아지는 것이 일반적이다.

〈그림 1〉에는 비실증 연구의 비중이 기간별로 변화한 모습이 나타나 있는데, 기간이 지남에 따라 비실증 연구의 비중이 작아진다는 증거를 찾기 어렵다. 이처럼 정보보안 감사 분야의 연구는 이론의 진화 과정을 반영하지 못하고 있는데, 그 이유 중의 하나로는 특정 산업/분야 또는 특정 신기술에 대한 정보보안 감사를 수행하는데 도움을 줄 수 있는 지침을 개발하는 연구들이 많이 수행되었고, 이러한 지침 개발 연구들은 대부분 비실증적인 연구방법으로 개발되었기 때문이다.[4)]

이 분야의 이론적인 발전을 위해서는 연구방법적인 측면에서 현재와 같이 비실증 연구들이 주로 수행되는 경향을 벗어나, 지금까지 수행된 비실증 연구에서 축적된 지식을 기반으로 보다 설명적인 결과를 제시할 수 있는 실증 연구의 비중을 높일 필요가 있다고 판단된다.

3) 세부 연구방법

다음으로는 이 분야 연구의 세부 연구방법을 살펴본다. 먼저, 실증 연구들의 세부 연구방법에 대한 분석 결과는 다음의 〈표 5〉에 정리되어 있다. 표에서 보는 바와 같이, 실증 연구들의 경우, 사례 연구가 절반을 차지하고 있고, 그 다음으로 서베이(35%), 2차 데이터 분석(15%)의 순으로 나타났다. 실증 연구의 세부 연구방법에 대해 국내외의 연구 경향을 비교해 보면, 국내 연구는 해외 경향과는 큰 차이를 타내고 있는데, 국내의 실증연구는 모두 서베이 방법만을 활용하고 있다는 것이다.

향후 국내 연구에서는 실증 연구를 수행할 때, 서베이뿐만 아니라 사례연구, 2차 데이터 활용 등과 같은 기

4) 이러한 연구의 비중 등의 자세한 수치는 연구 주제별 분석에서 제시한다.

〈표 5〉 실증연구 세부연구방법의 분포
〈Table 5〉 Distribution of Research Methods of Empirical Studies

Research method	All	Overseas	Domestic
Case study	10 (50.0%)	10 (55.6%)	0 (0%)
Survey	7 (35.0%)	5 (27.7%)	2 (100%)
Secondary data	3 (15.0%)	3 (16.7%)	0 (0%)
Total	20 (100.0%)	18 (100%)	2 (100%)

〈표 6〉 실증연구 세부연구방법별 연구주제 건수
〈Table 6〉 Number of Research Topics by Methods of Empirical Studies

Research topic	Case study	Survey	Secondary data
A (Auditor/Audit Organization)	1	1	2
Audits (Audit Activities/Procedures)	7	-	-
B (Audit Area)	2	1	-
C (Audit Objective/Effect)	5	6	2
D (Auditing Standard/Guidelines)	-	-	-

〈표 7〉 비실증연구 세부연구방법의 분포
〈Table 7〉 Distribution of Research Methods of Non-empirical Studies

Research method	All	Overseas	Domestic
Concept model	41 (48.8%)	26 (40.6%)	15 (75.0%)
Tutorial/Review	33 (39.3%)	29 (45.3%)	4 (20.0%)
Mathematical/Engineering Models	10 (11.9%)	9 (14.1%)	1 (5.0%)
Total	84 (100.0%)	64 (100.0%)	20 (100.0%)

타 연구방법들을 다양하게 채택하는 것이 바람직할 것으로 판단된다.

향후 연구자들이 연구주제에 적합한 연구방법을 선택할 때 참고할 수 있도록 각 연구방법에서 다룬 연구주제를 살펴보았다(〈표 6〉). 사례연구의 경우, 가장 많이 다룬 주제는 Audits와 C로서, 일반적으로 사례 조직에 대한 감사 과정(Audits)과 결과(C)를 분석하여 정리한 연구들이 대부분이었다. 서베이의 경우, 가장 많이 다루어진 주제는 C로서 정보보안의 품질과 성과를 분석하였다. 2차 데이터 분석의 경우에는 A와 C를 2차 데이터를 통해 분석하는 연구들이었다.

이러한 현황은 이 분야의 향후 연구에서 연구 주제에 대한 적절한 연구 방법을 선택할 때 참조가 될 것으로 판단된다.

다음으로 비실증 연구의 세부 연구방법에 대한 분석 결과는 〈표 7〉에 정리되어 있다. 전체적으로 개념적 모델을 제시하는 연구가 절반 정도(48.8%)를 차지하고 있고, 그 다음으로 기본 개념이나 기법 등을 소개하는 튜

〈표 8〉 비실증연구 세부연구방법별 연구주제 건수
〈Table 8〉 Number of Research Topics by Methods of Non-empirical Studies

Research topic	Conceptional model	Tutorial/ Review	Mathematical/ Engineering models
A (Auditor/Audit Organization)	0	2	0
Audits (Audit Activities/Procedures)	3	18	0
B (Audit Area)	19	13	0
C (Audit Objective/Effect)	5	5	2
D (Auditing Standard/Guidelines)	36	7	9

토리얼/리뷰 또한 많은 비중(39.3%)을 차지하고 있다. 나머지 11.9%의 연구는 수리/공학적 모델을 제시하고 있다. 해외 연구와 국내 연구를 비교해 보면, 국내 연구의 경우 개념 모델의 비중이 75%로 압도적이고, 수리/공학 모델의 활용이 저조한 것으로 나타났다.

향후 국내에서 비실증 연구를 수행할 때에는 개념 모델뿐만 아니라 수리/공학 모델의 활용도 고려해 볼 필요가 있을 것이다

비실증 연구에 대해서도 각 연구방법에서 다룬 연구 주제를 살펴보았고, 그 결과는 다음의 〈표 8〉에 정리되어 있다. 개념 모델 방법을 채택한 연구에서 가장 많이 다룬 주제는 D와 B로서, 특정 산업/기술 등 감사 대상 및 영역(B)에 대한 정보보안 감사의 모델(D)을 제시하는 연구가 대부분이었다. 튜토리얼/리뷰의 경우에는 모든 주제를 다루었으나, 특히 감사의 절차를 포함한 감사 활동(Audits)과 감사 대상(B)을 설명하는 연구들이 많았다. 마지막으로 수리/공학 모델에 관한 연구들의 경우에는 감사의 성과를 수리 모델을 통해 분석하거나, 공학적인 모델링을 통해 감사 도구나 모형을 제시하는 연구들이 주를 이루었고, 나머지 주제(A(감사인/조직), Audits, B)를 다룬 연구는 전혀 없었다. 향후에는 이러한 주제에 대해 수리/공학 모델을 적용해 보는 것도 이 분야 이론의 공백을 메우는데 기여할 수 있는 하나의 가능성이라고 생각된다.

2. 연구 주제에 대한 분석 결과

본 연구에서는 앞에서 설명한 바와 같이 일반 기준에 의한 분석 이외에도, 지금까지 이 분야에서 다루었던 연구의 내용을 살펴보고, 향후 연구에서 추가적인 연구가 필요하거나, 더 이상 고려할 필요성이 낮은 분야를 식별하기 위해 연구 주제를 중심으로 문헌들을 분석하였다. 이를 위해 첫째, 어떤 연구 주제가 많이/적게 연구되었는지를 파악하기 위해 연구 주제의 분포를 분석하였고, 둘째, 연구에서 단일 주제를 연구하였는지 그렇지 않으면 2개 이상의 주제를 복합적으로 연구하였는지를 살펴보기 위해 연구에 포함된 연구 주제의 수를 분석하였고, 마지막으로 각 연구 주제 하에서 분석한 세부 내용을 파악하기 위해 개별 연구 주제별 연구 내용을 분석하였다.

1) 연구 주제의 분포

정보보안 감사 연구에서 다루고 있는 연구 주제를 분석한 결과는 다음의 〈표 9〉에 정리되어 있다. 표에서 볼 수 있는 바와 같이, 연구 주제 D(감사 기준/지침)가 가장 많이 다루어졌고(36%), 그 다음으로 B(감사 대상) 24%, 그리고 Audits(감사 활동/절차)와 C(감사 목적/

5) Kim & Hwang(2021)의 분석 결과는 D(38%), B(26%), C(22%), Audits(10%), A(6%)의 순으로 나타났음.

〈표 9〉 연구주제별 연구건수(비율)
〈Table 9〉 Number (Ratio) of Papers by Research Topic

Research topic	All	Overseas	Domestic
A (Auditor/Audit Organization)	6 (4.1%)	6 (5.4%)	0 (0%)
Audits (Audit Activities/Procedures)	28 (19.2%)	26 (23.4%)	2 (5.7%)
B (Audit Area)	35 (24.0%)	22 (19.8%)	13 (37.1%)
C (Audit Objective/Effect)	25 (17.1%)	22 (19.8%)	3 (8.6%)
D (Auditing Standard/Guidelines)	52 (35.6%)	35 (31.5%)	17 (48.6%)
Total	146(100.0%)[6]	111 (100.0%)	35 (100.0%)

효과)가 비슷한 수준으로 연구되었다. 연구 주제 A(감사인/감사조직)는 4%의 비중으로 가장 적게 수행된 것으로 나타났다. 이러한 결과는 정보시스템 감사 분야의 연구를 분석한 결과와도 유사한 결과[5]인데, 정보보안 감사 분야의 연구에서도 감사의 수행 주체인 감사인이나 감사 조직에 대한 연구가 매우 미흡하게 수행되었다. 따라서 향후 이 분야의 연구에서는 정보보호 감사를 수행하는 감사인이나 감사 조직에 대한 분석이 보다 활발하고 심도있게 수행될 필요가 있다고 판단된다.

연구 주제에 대해 해외와 국내의 연구들을 비교해 보면, 국내의 연구는 해외 연구에 비해 연구 주제 D(감사 기준/지침)와 B(감사 대상)의 비중이 상당히 높고, Audits(감사 활동/절차)와 C(감사 목적/효과)에 대한 연구의 비중은 상대적으로 매우 낮고, A(감사인/조직)에 대한 연구는 전무한 상태이다.

이것은 우리나라의 경우, 정보보안 감사가 주로 공공 부문의 정보시스템 감리의 일부로 시행되고 있기 때문으로 판단된다. 우리나라에서 정보시스템 감리는 1999년에 '정보화촉진기본법'에 조항을 신설하여 정보시스템 감리의 시행 근거를 마련한 이후, 2005년에 '정보시스템의 효율적 도입 및 운영 등에 관한 법률'을 통해 공공 부문에 정보시스템 감리가 의무화되었고, 이에 따라 감리원의 자격 기준, 감리법인 등록 제도, 감리 기준 등이 규정화되었다. 이처럼 정보시스템 감리의 한 부분인 정보보안 감사가 선택이 아닌 의무사항이 되고, 감사인(감사 조직)의 자격 요건 등이 규정에 의해 정해짐에 따라 감사인/감사조직(A), 감사 활동/절차(Audits), 감사의 목적/효과(C) 등은 당연시 여겨짐으로써 추가적인 연구의 필요성이 낮아진 것으로 판단된다. 이에 따라 새로이 등장하는 신기술과 특정 산업과 같은 감사 대상(B)에 대한 감사 지침(D) 등을 개발하기 위한 연구가 주를 이루고 있는 것으로 판단된다.

따라서 향후 국내 연구에서는 정보보안 감사를 의무적으로 수행해야 하는 당연한 활동을 간주하기보다는 감사의 수행, 감사의 효과/성과/품질 등을 체계적이고 객관적으로 분석하여, 정보보안 감사를 더욱 개선하고 고도화하는데 기여할 수 있는 연구를 수행할 필요가 있다고 생각된다. 또한 정보스템 감리인의 자격 요건과 훈련 등은 공공 부문의 정보시스템 감리 기준 등에서 규정하고 있지만, 정보보안 감사에 특화된 감사인과 감사법인에 대한 연구 또한 정보보안 감사 분야의 발전에 기여할 수 있을 것으로 판단된다.

6) 분석 대상 논문의 수는 103편이지만, 2개 이상의 주제를 포함한 연구들이 있어 이러한 연구 주제들을 중복 집계한 결과 총합이 146편으로 표시되어 있음 (해외 논문의 수는 82년이나 111편으로, 국내 논문은 21편이나 35편으로 집계됨)

2) 포함된 연구 주제의 수

다음으로 논문에서 다룬 연구 주제의 개수에 대한 분포를 살펴보았는데(〈표 10〉), 전체적으로 봤을 때, 1개 주제만을 다룬 연구가 60% 정도를 차지하였고, 그 나머지는 대부분 2개의 주제를 다루었고, 3개의 주제를 다룬 연구가 1편 식별되었다. 국내외의 연구 경향을 비교해 보면, 우리나라의 연구는 해외와는 반대로 2개의 주제를 다룬 연구가 주를 이루고 있는 것으로 나타났다(67%). 이것은 우리 나라의 연구들이 한 가지 주제만을 살펴본 것이 아니라, 한번에 두 가지의 변수를 분석하고, 더 나아가 변수들 간의 상관관계까지 분석했다는 점에서 해외 연구에 비해 연구의 심도가 높은 고무적인 현상으로 보인다.

다음으로는 연구 주제의 수별로 다루어진 연구 내용을 분석하였다. 먼저 1가지 주제를 다룬 연구들의 경우, 전체적으로 절반 정도의 연구가 연구 주제 D(감사 기준/지침)를 분석하였고, 그 다음으로 Audit(감사 활동/절차), C(감사 목적/효과)의 순으로 연구가 이루어졌고, A(감사인/조직)와 B(감사 대상)에 대한 연구의 비중은 매우 낮게 나타났다(〈표 11〉). 국내외를 비교해 보면, 국내에서 1개 주제를 다룬 연구의 경우, 전체적으로 주제별 연구 비중은 해외 연구와 크게 다르지 않았지만, A(감사인)와 B(감사 대상)에 대한 연구가 전혀 이루어지지 않았는데, 앞서 지적한 바와 같이 A에 대한 연구를 향후 연구에서 주목할 필요가 있다고 판단된다.

다음으로 2개의 주제를 연구한 논문의 연구 내용의 분석 결과는 〈표 12〉에 정리되어 있다. 가장 지배적인 주제는 B(감사 대상)와 D(감사 기준/지침)를 같이 연구한 것이다(약 43%). 이러한 연구의 주된 내용은 특정 산업이나 기술에 적용할 수 있는 감사 지침을 제시하는 것

〈표 10〉 연구주제 수의 분포
〈Table 10〉 Distribution of Number of Research Topics

Number of Topics	All	Overseas	Domestic
1	61 (59.2%)	54 (65.9%)	7 (33.3%)
2	41 (39.8%)	27 (32.9%)	14 (66.7%)
3	1 (1.0%)	1 (1.2%)	0 (0%)
Total	103 (100%)	82 (100%)	21 (100%)

〈표 11〉 1개 주제연구의 연구주제 분포
〈Table 11〉 Distribution of Contents of 1-topic Research

Research topics	All	Overseas	Domestic
A (Auditor/Audit Organization)	4 (6.6%)	4 (7.4%)	0 (0.0%)
Audits (Audit Activities/Procedures)	13 (21.3%)	11 (20.4%)	2 (28.6%)
B (Audit Area)	2 (3.3%)	2 (3.7%)	0 (0.0%)
C (Audit Objective/Effect)	11 (18.0%)	10 (18.5%)	1 (14.3%)
D (Auditing Standard/Guidelines)	31 (50.8%)	27 (50.0%)	4 (57.1%)
Total	61 (100.0%)	54 (100.0%)	7 (100.0%)

〈표 12〉 2개 주제연구의 연구내용 분포
〈Table 12〉 Distribution of Contents of 2-topic Research

Research topics	All	Overseas	Domestic
A C	2 (4.9%)	2 (7.4%)	0 (0.0%)
Audits B	10 (24.4%)	10 (37.0%)	0 (0.0%)
Audits C	5 (12.2%)	5 (18.5%)	0 (0.0%)
B C	4 (9.8%)	3 (11.1%)	1 (7.1%)
B D	18 (43.9%)	6 (22.2%)	12 (85.7%)
C D	2 (4.9%)	1 (3.7%)	1 (7.1%)
Total	41 (100.0%)	27 (100.0%)	14 (100.0%)

A (감사인/조직); Audits (감사 활동/절차); B (감사 대상); C (감사 목적/효과); D (감사 기준/지침)

이다. 새로운 기술 분야나 지금까지 적용되지 않은 산업은 지속적으로 나타날 수밖에 없기 때문에 이 주제는 향후의 연구에서도 계속해서 다루어질 것으로 예상된다. 그 다음으로는 B(감사 대상)와 Audits(감사 활동/절차)를 같이 분석한 연구로서(24%), 특정 감사 대상에 대해 이루어진 감사 활동을 분석한 연구들이다. 이 부분 역시 감사 대상은 지속적으로 확대될 것이므로 향후에도 지속적으로 연구될 것이다.

국내외의 연구를 비교해 보면, 매우 큰 차이가 있는데, 국내 연구의 경우, B(감사 대상)와 D(감사 기준/지침)를 함께 분석한 연구가 절대적인 비중(86%)을 차지하고 있다. 그 이유는 앞서 언급한 바와 같이 우리나라의 경우 정보보안 감사가 정보시스템 감리의 일부로 의무화되어 감사의 필요성과 효과 등은 크게 따질 필요가 없고, 감사인의 자격, 감사 기준 등은 정해져 있는 것이기 때문에 새로이 등장하는 신기술과 특정 산업과 같은 감사 대상(B)에 대한 감사 지침(D) 등을 개발하기 위한 연구가 주를 이루고 있는 것으로 판단된다.

3) 연구 주제의 세부 내용

다음에서는 각 연구 주제별로 다루어진 세부 내용에 대한 분석 결과를 제시한다.

(1) 연구주제 A(감사인/감사조직)

정보보안 감사를 수행하는 주체인 감사인과 감사 조직에 관련된 연구에서 다루어진 세부 내용은 다음의 〈표 13〉과 같다. 표에서 볼 수 있는 바와 같이, A (감사인/조직)에 관련된 세부 내용에는 감사인의 투입 시간, 감사인/감사조직의 자격 요건 및 역량, 감사인(감사조직)과 비감사인(조직)과의 관계 등이 포함된다. 연구 주제 A를 포함하여 2개 이상의 연구 주제를 분석한 연구들은 모두 A와 C[7] 간의 관계를 분석한 연구였다.

연구 주제 A(감사인/조직)의 세부 내용을 발표 기간별로 분석한 결과는 다음의 〈표 14〉에 정리되어 있다. 표에서 볼 수 있는 바와 같이, 이 주제는 많이 연구되지 않은 분야이고, 비교적 최근 들어 연구되고 있는 분야라는 것을 알 수 있다. 또한 국내에서는 이 분야에 대해 이루어진 연구가 없다는 사실을 확인할 수 있다. 이것은 앞서 설명한 바와 같이 정보보안 감사인의 자격 요건과 훈련 등이 공공 부문의 정보시스템 감리 기준 등에서 규정되어 있는 관계로 추가적인 연구의 필요성이 낮은 때문으로 추측된다. 그러나 정보보안 감사에 특화된 감사

7) 여기에는 감사의 효과(기업 내외부 위협의 식별)와 감사의 성과(정보보안 성과)가 포함됨

〈표 13〉 연구주제 A(감사인)의 세부 내용
〈Table 13〉 Contents of Research Topic A

Content	Topic	Detailed contents	Related literature
Audit man-hours	A	Proposes a labor time estimation method for the information security audit	Satoh & Komoda, 2005
Qualifications/ Competencies of auditor/audit organization	A	Auditor qualifications, code of ethics, and training requirements	Drastich, 2013
	A, C	Analyze the relationship between the audit organization's industry expertise, size, experience, etc. and identification of internal/external threats facing the client	Yen, et al., 2018
Relationships with non-audit personnel/ organizations	A	Describe the relationship between the audit department and the information security department	Steinbart, et al., 2013
		Explain the role played by accounting societies/professional associations in relation to information security audits	Stafford, 2018
	A, C	Analyze the impact of the relationship between the audit department and the information security department on information security performance	Steinbart, et al., 2013

A (감사인/조직); Audits (감사 활동/절차); B (감사 대상); C (감사 목적/효과); D (감사 기준/지침)

〈표 14〉 연구주제 A(감사인)의 기간별 분석 결과
〈Table 14〉 Analysis Results for Research Topic A by Period

Content	2001~2005	2006~2010	2011~2015	2016~2020	Total
Audit man-hours	Satoh & Komoda, 2005	-	-	-	1(0)
Qualification/ Competencies	-	-	Drastich, 2013	Yen, et al., 2018	2(0)
Relationship with non-audit	-	-	Steinbart, et al., 2013	Stafford, et al., 2018; Steinbart, et al., 2018	3(0)
Total	1(0)	0(0)	2(0)	3(0)	6(0)

Numbers in ( ) are the numbers of domestic research articles

인/감사법인 등에 대한 연구는 이 분야의 발전에 기여할 수 있을 것이다.

세부 내용을 살펴보면, 첫째, 감사인/감사조직의 자격요건/역량과 감사인/감사조직과 기타 관련자(관련조직) 간의 관계가 많이 연구되었는데, 역량이나 기타 관련자들의 조작화가 종합적이고 일관성 있게 이루어지지 않고 있다. 예를 들면, Drastich(2013)은 감사인의 자질로 분석능력, 정직성, 외교력, 윤리적인 행동, 의사소통 능력, 객관성, 공정성, 전문성, 유용성, 협동심, 양심, 인내심, 친절성 등을 나열하고 있다. Yen,

et. al(2018)은 감사조직의 역량을 규모, 산업에 대한 전문성, 경력 등으로 측정하고 있다. 정보보안 감사에 이해 관계를 가진 엔티티로는 회계학회와 전문협회(Stafford, et. al., 2018), 정보보안 부서(Steinbart, et. al., 2018) 등이 분석되었다. 이것은 이 분야 연구의 누적적인(Cumulative) 발전에 걸림돌이 될 수 있으므로, 향후 감사인의 역량과 정보보안 감사에 관련된 이해관계자들을 종합적이고 체계적으로 나타낼 수 있는 프레임워크를 수립하는 연구가 필요하다고 판단된다.

둘째, 연구 주제 A(감사인/조직)만을 살펴보는 것보다는 A(감사인/조직)와 다른 주제들과의 상관관계를 분석하는 것이 보다 고도화된 연구인데, 감사인(조직)이 감사의 효과/성과/품질 등에 미치는 영향을 분석하는 연구가 지금까지 2편만 수행되었는데, 여기에 대한 보다 적극적인 연구가 필요하다고 판단된다.

(2) 연구주제 Audits(감사 활동/절차)

연구 주제 Audits(감사 활동/절차)에 관련하여 수행된 연구에서 다룬 세부 내용은 다음의 〈표 15〉에 정리되어 있다. 세부 내용은 크게 정보보안 감사의 개념, 감사 수행 절차, 감사 수행 활동 과정/결과 등으로 구분해 볼 수 있다. 연구 주제 Audits(감사 활동/절차)를 포함하여 2개 이상의 주제를 함께 분석한 연구는 개념, 절차, 활동 전반에 걸쳐서 Audits(감사 활동/절차)와 B(감사 대상)를 함께 분석하였다. 이것은 특정 감사 대상(B)[8]에 대한 개념, 절차, 감사 수행의 과정과 결과를 설명하는 연구들이다.

발표 기간별로 분석한 결과는 다음의 〈표 16〉에 정리되어 있다. 이 주제는 양적으로 그다지 많지는 않지만, 2006년~2020년까지 꾸준히 연구가 수행되었고, 최근까지 이어지고 있다. 세부 내용을 살펴보면, 정보보안 감사의 개념이나 기본적인 수행 절차와 같은 기본적인 사항에 대한 연구는 최근에는 없고, 정보보안 감사의 구체적인 활동 과정과 성과를 분석하는 연구들이 진행되고 있는 것을 알 수 있다.

이처럼 개념이나 기본적인 절차 등에 대한 연구는 이제 더 이상 학술적으로나 실무적으로 기여하는 바가 크지 않기 때문에 향후 연구는 정보보안 감사의 세부 활동 과정에집중할 필요가 있을 것으로 보인다. 예를 들면, 주요한 감사 활동(감사 계획 수립, 감사 시행, 감사 보고서 작성/전달, 감사 사후관리)의 수행 과정과 그 결과 등을 체계적으로 분석하는 연구를 들 수 있다.

(3) 연구주제 B(감사 대상)

연구 주제 B(감사 대상)를 주제로 수행된 연구에서 다룬 세부 내용은 신기술, 특정 보안 분야, 특정 산업 등으로 구분해 볼 수 있다(〈표 17〉 참조), 정보보안 감사의 대상으로 분석된 신기술로는 EDI 시스템, 전자화폐, 웹기반 시스템, 산업제어 시스템, RFID, SCADA 시스템, 클라우드 컴퓨팅, 전자상거래, ERP/CRM 시스템, 빅데이터, 모바일 기기 등 다양한 기술이 포함된다. 연구에 포함된 특정 보안 분야는 네트워크, 개인정보, 데이터/데이터베이스, 사이버 범죄, 재무 웹 애플리케이션 등으로 나타났다. 분석된 특정 산업에는 국방, 공공 기관, 교육기관, 의료기관, 은행, 전력 산업 등이 포함된다. 그 외에도 사용자 인식(데이터 보안에 대한 사용자 인식), 법규(SOX법) 등이 식별되었다.

특기할 사항은 국내 연구와 해외 연구에서 분석한 신기술/특정 산업/특정 보안분야 등이 대체로 중복되지 않는다는 사실이다. 예를 들면, 웹기반 시스템, RFID, SCADA, 산업 제어시스템 등의 기술은 국내 연구에서만, 클라우드, 가상 환경, ERP/CRM, 빅데이터, 모바일 기기 등은 해외 연구에서만 식별되었다. 산업에서도 국방, 공공 등은 국내 연구에서만, 교육, 금융, 전력 산업은 해외 연구에서만 연구되었다. 또한 특정 보안 분야 측면에서도 개인정보 보호는 국내에서만, 네트워크 보안은 해외에서만 연구된 것으로 나타났다.

이것은 물론 국내와 해외의 기술 환경과 문화 등을

8) 분석에 포함된 감사 대상 영역들은 다음의 연구주제 B(감사 대상)에서 자세하게 설명한다.

〈표 15〉 연구주제 Audits(감사 수행)의 세부 내용
〈Table 15〉 Contents of Research Topic Audits

Content	Topic	Detailed contents	Related literature
Concepts	Audits	Describe the need and procedures for information security audits	Pathak, 2006; Popescu, et al., 2008
		Explain the basic concept of information security audit	Surcel & Amancei, 2007; Tofan, 2011; Min & Lee, 2016; Lu, et al., 2018
	Audits, B	Describe the need for and audit areas of e-business security audits	F. Nastase & P. Nastase, 2007
Procedures	Audits	Describe information security audit procedures	Suduc, et al., 2010; Azubike, 2011; Grzyb & Kowalik, 2020
		Describe the procedures for information security audits	Kim, et al., 2013
	Audits, B	Describe the ERP Security Audit Procedure	Yu & Gao, 2013
		Describe information security audit procedures in the electric power industry	Radu & Isai, 2014
		Describe the procedures for network security audits	Cohen, 1998; Quanxiu & Guangying, 2011; Afifi, 2020; Zhou, 2020
		Provide a method for auditors to identify/correct when organizational insiders inadvertently pose a threat to the company's information security	Stafford, et al., 2018
Activities	Audits	Summarize the process/results of an information security audit for a case organization	Lo & Marchand, 2004; Goel, et al., 2006; Candiwan & Priyadi, 2016
	Audits, B	Present security audit procedures/results for an organization's financial web applications	Vieira & Serrão, 2016
		Present a cybercrime security audit plan	Alviana, 2020
		Explain the applicability of auditing for mobile device security	Othman, et al., 2021
	Audits, C	For lecture purposes, explain the audit procedures/results, etc. for a hypothetical organization.	Tanriverdi, et al., 2006
		Present the audit process/results based on CISSP CBK for XYZ school	Arionadi, et al., 2016
		Present the purpose/process/results of information security audit	Barankova, et al., 2019
		Presenting the importance of and procedures for risk identification/assessment in information security audits	Beldiman, 2021

A (감사인/조직); Audits (감사 활동/절차); B (감사 대상); C (감사 목적/효과); D (감사 기준/지침)

〈표 16〉 연구주제 Audits(감사 수행)의 기간별 분석 결과

〈Table 16〉 Analysis Results for Research Topic Audits by Period

Content	Before 2000	2001~2005	2006~2010	2011~2015	2016~2020	After 2021	Total
Concepts	-	-	Pathak, 2006; Surcel & Amancei, 2007; F. Nastase & P. Nastase, 2007; Popescu, et al., 2008	Tofan, 2011	Min & Lee, 2016; Lu, et al., 2018	-	7(1)
Procedures	Cohen, 1998	-	Suduc, et al., 2010	Azubike, 2011; Quanxiu & Guangying, 2011; Kim, et al., 2013; Yu & Gao, 2013; Radu & Isai, 2014	Stafford, et al., 2018; Grzyb & Kowalik, 2020; Afifi, 2020; Zhou, 2020	-	11(1)
Activities	-	Lo & Marchand, 2004	Goel, et al., 2006; Tanriverdi, et al., 2006	-	Arionadi, et al., 2016; Candiwan & Priyadi, 2016; Vieira & Serrão, 2016; Barankova, et al., 2019; Alviana, 2020	Beldiman, 2021; Othman, et al., 2021	10(0)
Total	1(0)	1(0)	7(0)	6(1)	11(1)	2(0)	28(2)

Numbers in ( ) are the numbers of domestic research articles

반영한 결과이겠지만, 향후 국내 연구에서는 지금까지 해외 연구에서만 다루어졌고 아직까지 국내에서는 다루어지지 않은 기술/산업/보안 분야를 주목해 볼 가치가 있다고 생각된다.

연구 주제 B(감사 대상)는 국내에서도 연구가 비교적 활발하게 수행되었기 때문에, 해외 연구 동향과 비교해 보았다(〈표 18〉). 표에서 볼 수 있는 바와 같이, 국내의 연구에서 신기술을 다룬 연구의 비중이 해외에 비해 상당히 높게 나타났다. 이것은 앞서 언급한 바와 같이 우리나라의 조직들이 신기술의 얼리 어답터(Early Adopter)로서, 많은 신기술들을 도입하는 경향을 반영하는 결과라고 생각된다.

연구 주제 B(감사 대상)를 발표 기간별로 분석한 결과는 다음의 〈표 19〉와 같다. 표에서 볼 수 있듯이, 모든 세부 내용들이 초기부터 지금까지 꾸준히 연구되고 있다는 것을 알 수 있다. 특히 신기술에 대한 연구는 초기부터 지금까지 상대적으로 많은 수의 연구가 지속적으로 수행되고 있다. 정보보안 감사의 대상이 되는 신기술은 앞으로도 지속적으로 출현할 것이고, 감사가 적용될 산업과 보안 분야 또한 지속적으로 확대될 수밖에 없기 때문에 이 주제에 대한 연구는 앞으로도 계속해서 진행될 것으로 예상된다.

(4) 연구주제 C(감사 목적/효과)

연구 주제 C(감사 목적/효과) 부분에서 수행된 연구의 세부 내용은 정보보안 감사의 필요성, 목적, 성과(효

〈표 17〉 연구주제 B(감사대상)의 세부 내용
〈Table 17〉 Contents of Research Topic B

Content	Topic	Detailed contents	Related literature
New Tech	B	Ripple effect of electronic money on information security audits (B)	Warigon, 1999
	B, C	Network security audit in the big data era	Lin & Huang, 2020
	Audits, B	Describe the ERP Security Audit Procedure	Radu & Isai, 2014
		Describe the need for and audit areas of e-business security audits	Lee, et al., 2018; F. Nastase & P. Nastase, 2007
		Applicability of auditing for mobile device security	Othman, et al., 2021
	Audits, D	Propose an audit trail system for EDI system security	Jeong, et al., 1997
		Propose an audit model for web-based systems/applications	Yun, et al., 2003; Jeon, et al., 2007
		Propose an audit model for Industrial Control Systems	Lee, 2008
		Propose an audit model for RFID-based information system	Lim, et al., 2008; Jeon, et al., 2012
		Propose an information security audit model for SCADA systems	Lee, et al., 2009
		Propose audit standards/models for the cloud computing field	Bendovschi & Ionescu, 2015; Gupta & Shakya, 2015
		Propose the audit process/framework in a virtual environment	Dharmalingam & Smalov, 2016
		Propose an audit system for e-commerce personal information protection	Lee, et al., 2018
		Explain the audit methodology for ERP/CRM systems	Voevodin, et al., 2020
Security areas	Audit, B	Network Security Audit	Cohen, 1998; Quanxiu & Guangying, 2011; Afifi, 2020 Zhou, 2020
		Financial web application	Vieira & Serrão, 2016
		Security plan against cybercrime	Alviana, 2020
	B, C	Explain the need for auditing network security in the era of big data	Lin & Huang, 2020
		Explain the need to introduce an audit system for personal information protection	Jeong, et al., 2013
		Data/Database security audit	Almadhoob & Valverde, 2014
	B, D	Audit model for privacy protection	Lee & Park, 2010; Lee, et al., 2018
	B, C, D	Identify factors affecting the quality of database security audits and present a conceptual framework for audits.	Muneeb-ul-Hasan & Arshad, 2019
Industry	Audits, B	Audit procedures in the power industry	Yu & Gao, 2013
	B, C	Survey on the IT security audit status of medical institutions	Hermann & Tanguy, 2022
	B, D	Propose the audit system of public institutions	Jeon, et al., 2006
		Propose an audit model for defense information systems	Choi & Nam, 2001
		Propose an audit process model for educational institutions	Billones & Ona, 2011
		Propose an audit model for the hospital information system	Yu, et al., 2014
		Propose a meta-model for bank audits	Wen, et al., 2018
Others	B, C	User awareness (user awareness of data security)	Almadhoob & Valverde, 2014
	B	SOX (Identify risks to SOX and IT resources)	Smith, 2007

A (감사인/조직); Audits (감사 활동/절차); B (감사 대상); C (감사 목적/효과); D (감사 기준/지침)

〈표 18〉 연구주제 B(감사대상)의 세부 내용
〈Table 18〉 Contents of Research Topic B

Content	All	Overseas	Domestic
New Technology	17 (44.7%)	9 (37.5%)	8 (57.2%)
Specific Security Areas	12 (31.6%)	9 (37.5%)	3 (21.4%)
Specific Industry	7 (18.4%)	4 (16.7%)	3 (21.4%)
Others	2 (5.3%)	2 (8.3%)	0 (0%)
Total	38[9] (100.0%)	24 (100.0%)	14 (100.0%)

〈표 19〉 연구주제 B(감사대상) 연구의 기간별 분석 결과
〈Table 19〉 Analysis Results for Research Topic B by Period

Content	Before 2000	2001~2005	2006~2010	2011~2015	2016~2020	After 2021	Total
New Tech	Jeong, et al., 1997; Warigon, 1999	Yun, et al., 2003	F. Nastase & P. Nastase, 2007; Jeon, et al., 2007; Lee, 2008; Lim, et al., 2008; Lee, et al., 2009	Jeon, et al., 2012; Radu & Isai, 2014; Bendovschi & Ionescu, 2015; Gupta & Shakya, 2015	Dharmalingam & Smalov, 2016; Lee, et al., 2018; Lin & Huang, 2020; Voevodin, et al., 2020	Othman, et al., 2021	17(8)
Security areas	Cohen, 1998	-	Lee & Park, 2010	Quanxiu & Guangying, 2011; Jeong, 2013; Almadhoob & Valverde, 2014	Vieira & Serrão, 2016; Muneeb-ul-Hasan & Arshad, 2019; Lee, et al., 2018; Lin & Huang, 2020; Afifi, 2020; Zhou, 2020; Alviana, 2020	-	12(3)
Industry	-	Choi & Nam, 2001	Jeon, et al., 2006	Billones & Ona, 2011; Yu & Gao, 2013; Yu, et al., 2014	Wen, et al., 2018	Hermann & Tanguy, 2022	7(3)
Others	-	-	Smith, 2007	Jeong, 2013; Almadhoob & Valverde, 2014	-	-	3(1)
Total	2(1)	2(2)	7(6)	9(4)	7(1)	1(0)	28(14)

Numbers in () are the numbers of domestic research article

9) 주제 B를 다룬 분석 대상 논문의 수는 35편이지만, 2개 이상의 세부 주제를 포함한 연구들이 있어 이러한 연구 주제들을 중복 집계한 결과 총합이 38편으로 표시되어 있음

〈표 20〉 연구주제 C(감사 목적/효과)의 세부 내용
〈Table 20〉 Contents of Research Topic C

Content	Topic	Detailed contents	Related literature
Need	B, C	Present the need to introduce an audit system for personal information protection	Jeong, 2013
		Analyze user perception of data security	Almadhoob & Valverde, 2014
		Necessity of network security audit in the era of big data	Lin & Huang, 2020
		Survey on the IT security audit status of medical institutions	Hermann & Tanguy, 2022
Objective	C	Present the 5C objectives of information security	Chandra, 2008
		Explain the relationship between financial audits and information security audits	Singleton & Singleton, 2008
	Audits, C	Present audit process/results based on CISSP CBK for XYZ school	Arionadi, et al., 2016
		Present the purpose/process/results of information security audit	Barankova, et al., 2019
		Describe the audit procedures/results, etc. for a hypothetical organization	Tanriverdi, et al., 2006
Performance	C	Present metrics to measure the process/results of information security audits	Popa, 2010
		Analyze the relationship between information security audit and bank performance for four banks in Ghana	Hatsu, et al., 2015
		Analyze the impact of audits (awareness of audits) on information security performance	Jeon, et al., 2015
		Analyze the impact of IT governance and knowledge management on the audit results	Au & Fung, 2019
		Analyze the relationship between the implementation of audit recommendations and reduction of security incidents	Salihu & Berisha-Hoti, 2019
		Analyze the relationship between audits and number of accidents based on the fuzzy theory	Dias, 2021
		Analyze the relationship between audit data/audit scope/cost submitted to SEC and number of audit violations	Westland, 2021
	A, C	Analysis of impact of the relationship between the audit department and the information security department on information security performance	Steinbart, et al., 2018
		Analyze the relationship between the audit organization's industry expertise/size/experience, etc. and identification of internal and external threats facing the client company	Yen, et al., 2018
	Audits, C	Provide a method for auditors to identify/correct when organizational insiders inadvertently pose a threat to the company's information security	Stafford, et al., 2018
		Present the importance of/procedures for risk identification/assessment in information security audits	Beldiman, 2021
Quality	C	Analyze the relationship between network security policies and documentation of audit evidence	Hamdan, 2017
		Describe the security concerns that should be carefully considered in an audit	Shakya & Gupta, 2017
	C, D	Present a quantitative model for auditing and analyze the impact on audit quality	D. Kim & H. Kim, 2004
		Present audit work breakdown diagram and budget model for audit cost control	Surcel & Amancei, 2011
	B, C, D	Identify factors affecting the quality of DB security audits and present a conceptual framework for auditing	Muneeb-ul-Hasan & Arshad, 2019

A (감사인/조직); Audits (감사 활동/절차); B (감사 대상); C (감사 목적/효과); D (감사 기준/지침)

과), 품질 등으로 구분해 볼 수 있고, 이와 관련된 연구 문헌은 다음의 〈표 21〉에 정리되어 있다. 정보보안 감사의 필요성에 관한 연구는 모두 특정 감사 대상(예: 개인정보보호, 데이터 보안, 네트워크 보안, 의료기관)에 정보보안 감사를 수행할 필요성이 있는지를 분석하였다. 정보보안 감사의 목적에 관한 연구는 정보보안 감사의 목적(C)만을 다룬 연구도 있었지만,[10] 대부분 감사 활동 수행(B)의 목적(C)을 분석한 연구들이었다. 정보보안 감사의 성과에 관련된 연구에는 정보보안 감사의 성과(C)만을 다룬 연구[11] 감사인(A)과 성과(C) 간의 관계를 분석한 연구, 감사수행 활동(B)의 성과(C)를 분석한 연구 등이 포함된다. 마지막으로 정보보안 감사의 품질을 분석한 연구에는 품질(C)만을 다룬 연구, 기준/지침(D)의 품질(C)을 다룬 연구 등이 있다.

감사의 목적/효과를 주제로 한 연구의 세부 내용을 기간별로 분석한 결과는 〈표 21〉과 같다.

정보보안 감사의 필요성과 목적에 대한 연구는 비교적 적은 수의 연구들이 간헐적으로 이루어진 것으로 나타났다. 정보보안 감사의 성과/효과에 대한 연구는 초기부터 현재까지 이 주제에 대해서 가장 활발하게 수행되고 있다는 것을 알 수 있다. 그런데, 이 부분에 대한 국내 연구는 지금까지 1편밖에 식별되지 않고 있다. 정

〈표 21〉 연구주제 C(감사목적)의 기간별 분석 결과
〈Table 21〉 Analysis Results for Research Topic C by Period

Content	2001~2005	2006~2010	2011~2015	2016~2020	After 2021	Total
Need			Jeong, 2013; Almadhoob & Valverde, 2014	Lin & Huang, 2020	Hermann & Tanguy, 2022	4(1)
Objective	-	Tanriverdi, et al., 2006; Chandra, 2008; Singleton & Singleton, 2008	-	Arionadi, et al., 2016; Barankova, et al., 2019	-	5(0)
Performance	-	Popa, 2010	Hatsu, et al., 2015; Jeon, et al., 2015	Steinbart, et al., 2018; Yen, et al., 2018; Stafford, et al., 2018; Au & Fung, 2019; Salihu & Berisha-Hoti, 2019	Beldiman, 2021; Dias, 2021; Westland, 2021	11(1)
Quality	D. Kim & H. Kim, 2004	-	Surcel & Amancei, 2011	Hamdan, 2017; Shakya & Gupta, 2017; Muneeb-ul-Hasan & Arshad, 2019	-	5(1)
Total	1(1)	4(0)	5(1)	11(0)	4(0)	25(2)

Numbers in () are the numbers of domestic research article

10) Chandra(2008)은 정보보안 감사의 목적을 다음과 같은 5가지 특성을 바탕으로 정보보안 정책의 효과성을 평가하는 것으로 정의함. comprehensive, current, communicated, compliant, convertible.

11) 정보보안 감사의 성과로는 조직의 성과(Hatsu, 2015), 정보보안 성과(Jeon, et al., 2015), 감사 결과(Au & Fung, 2019)), 보안사고 건수(Dias, 2021; Salihu & Berisha-Hoti, 2019), 감사위반 건수(Beldiman, 2021) 등이 포함된다.

보보안 감사의 품질에 대한 연구는 2011년 이후 시작되어 2016년~2020년의 시기에 비교적 활발하게 수행된 것을 알 수 있고, 국내 연구는 매우 초기에 1편의 연구만이 식별되었다.

위와 같은 현황을 통해서 이 분야의 향후 연구 분야를 다음과 같이 정리해 볼 수 있다. 첫째, 정보보안 감사의 필요성/목적 등에 대한 연구는 이 분야의 연구가 시작된지 이미 30년 정도의 역사를 가지고 있는 상황이므로, 정보보안 감사의 필요성에 대한 정당성을 부여하기 위한 연구는 이제 더 이상 크게 필요하지 않을 것으로 판단된다.

둘째, 정보보안 감사의 성과/효과와 품질에 대한 연구의 향후 연구 방향으로는 현재 연구마다 서로 다르게 조작화되고 있는 성과와 품질을 체계적이고 일관성 있게 정의할 수 있는 프레임워크를 제시하는 연구가 매우 필요하다고 생각된다.

셋째, 정보보안 감사의 성과와 품질은 국내 연구에서 거의 다루지 않고 있는 것은 앞서 지적한 바와 같이 우리나라의 정보보안 감사는 대부분 공공 부문에서 의무화되어 있는 정보시스템 감리의 일환으로 수행되고 있기 때문에 어쨌든 의무적으로 해야 하므로 구태여 성과나 효과, 품질을 분석하고 측정할 필요성이 낮기 때문인 것으로 판단된다. 그러나, 의무적으로 해야 하는 상황이라도, 이를 통해 어떤 효과가 있고, 어떤 성과를 거두고 있으며, 감사의 품질이 어떠한지를 측정하고 분석하지 않는다면 개선이 이루어질 수 없기 때문에 여기에 대한 연구는 반드시 수행될 필요가 있다고 생각된다.

(5) 연구주제 D(감사 기준/지침)

연구 주제 D(감사 기준/지침)에 관해 수행된 연구의 세부 내용을 살펴보면, 정보안 감사 기준/표준, 감사 도구/기법, 감사 지침/모델 등으로 구분해 볼 수 있다(〈표 22〉 참조).

기준/표준에 관한 연구의 경우, 일반적인 정보보안 감사 전반에 대한 기준과 표준을 제시한 연구가 있고, 클라우드 컴퓨팅과 같은 특정 분야(B)를 위한 기준(D)을 제시한 연구(Bendovschi & Ionescu, 2015)가 있다. 도구/기법의 경우에도, 정보보안 감사 전반에 적용될 수 있는 도구/기법을 제안한 연구들이 대다수이지만, ERP/CRM, EDI, 공공 기관 등과 같은 특정 감사 대상(B)과 감사 비용 통제라는 특정 목적(C)을 위한 기법(D)을 제안한 연구들도 있다. 모델/지침의 경우에도 일반적인 정보보안 감사에 적용 가능한 모델을 제시한 연구들이 있지만, 특정 감사 대상(B)이나 특정 목적(C)을 위한 지침을 제시한 연구들이 다수를 차지하고 있다.

연구 주제 D(감사 기준/지침)에 대해 수행된 연구들을 국내외로 비교해 보았다(〈표 23〉). 국내 연구의 경우, 정보보안 감사의 기반 또는 인프라의 역할을 수행하는 감사 기준/표준, 도구/기법에 대한 연구보다는 즉시 현장에서 적용 가능한 지침/모델 등을 제시하는데 집중하고 있다는 것을 알 수 있다.

이것은 우리나라가 시간과 노력은 많이 들지만 당장 적용은 어려운 기초 과학이나 기초 학문에 대한 연구보다는 응용 분야에 집중하는 경향과 유사한 현상이라고 생각된다. 기초 연구는 응용 연구의 기반이 되고, 이에 따라 기초 연구의 기반이 없이 수행되는 응용 연구는 사상누각일 수 있으므로 정보보안 감사 수행의 근간이 되는 기준/표준, 도구/기법에 관한 연구를 활성화할 필요가 있다고 판단된다.

감사 기준/지침을 주제로 한 연구의 세부 내용을 발간 기간별로 분석한 결과는 다음과 같다(〈표 24〉).

감사 기준/표준에 대한 연구는 2001년부터 기간별로 1~2편 정도의 적은 수의 연구가 수행되었고, 도구/기법에 대한 연구는 이보다 늦은 2006년부터 매기간 상당 수의 연구가 수행되었고, 지침/모델에 대한 연구는 초창기부터 상당수의 연구가 지속적으로 활발하게 수행된 것을 파악할 수 있다. 지침/모델 부문에서는 국내 연구도 해외 연구와 동수로 매우 활발하게 이루어졌으나, 전체적인 연구 동향에서 살펴본 바와 같이 연구가 왕성하게 이루어진 시기는 해외보다 빨랐다.

감사 기준/표준은 한번 수립되면 일부 유지보수 차원의 수정은 있지만, 크게 변경되는 경우는 많지 않으므

〈표 22〉 연구주제 D(감사기준)의 세부 내용
〈Table 22〉 Contents of Research Topic D

Content	Topic	Detailed contents	Related literature
Standards/ Criteria	B, D	Propose auditing standards for cloud computing	Bendovschi & Ionescu, 2015
	D	Explain ISO 27001, which may aid in information security audits	Capuder, 2004; Cefaratti, et al., 2011
		Describe standards related to information security audits	Popa & Doinea, 2007
		Describe the IT Baseline Protection Manual	Bhaskara, et al., 2018
Tools/ Techniques	B, D	Present an audit methodology for ERP/CRM systems	Voevodin, et al., 2020
		Develop an audit trail system for EDI system security	Jeong, et al., 1997
		Analyze and design an audit system for the information protection management of public institutions	Jeon, 2008
	C, D	Present the audit work breakdown diagram and budget model for audit cost control	Surcel & Amancei, 2011
	D	Comparative analysis of the concept of an audit trail mechanism that provides the information necessary for security audits and various mechanisms	Kim & Nam, 1993; Roratto & Dias, 2014
		Design a network monitoring system that provides an audit trail	Ryu, et al., 1997; Rudowski & Tarnowska, 2016
		Propose an expert system for information security audit	Popescu, et al., 2007; Kanatov, et al., 2014; Atymtayeva & Kozhakhmet, 2015
		SWOT analysis of three methods of information security audit	Ivanova, et al., 2010
		Present a methodology to increase the efficiency of information security audits	Shultz, et al., 2014
		Propose an open source security information management system that supports information security audits	Hermanowski, 2015
		Present the Security Requirements Elicitation from the Business Processes (SREBP) approach to support information security audits	Kozlovs, et al., 2016
		Propose an audit methodology based on semantic web ontology	Li, 2016
		Present an instantaneous information security audit methodology	Livshitz, et al., 2016
		Propose a matrix methodology	Markina & Diachkov, 2019
		Propse a methodology for auditors to predict risk using Bayesian inference techniques	Satoh & Samejima, 2019
		Present an audit methodology based on the Neuro-Fuzzy System to support information security audits	Lakhno, et al., 2021
		Propose a remote information security audit methodology	Lontsikh, et al., 2021

〈Table 22〉 Continued

Content	Topic	Detailed contents	Related literature
Models/ Guidelines	B, D	Propose an audit model for personal information protection	Lee & Park, 2010
		Present an information security audit model for RFID-based information systems	Jeon, et al., 2012
		Propse an IT security audit system for e-commerce personal information protection	Lee, et al., 2018
		Propose an audit process model for educational institutions	Billones & Ona, 2011
		Present an audit model for cloud computing	Gupta & Shakya, 2015
		Present audit process/framework in a virtual environment	Dharmalingam & Smalov, 2016
		Propose a meta model for bank information security audits	Wen, et al., 2018
		Propose an information security audit model for defense information systems	Choi & Nam, 2001
		Present an audit model for web-based systems	Yun, et al., 2003
		Propose an information security audit model for web applications	Jeon, et al., 2007
		Present an information security audit model for industrial control systems	Lee, 2008
		Propose an information security audit model for RFID-based information systems	Lim, et al., 2008
		Present an information security audit model for the SCADA system	Lee, et al., 2009
		Propose an audit model for the hospital information system	Yu, et al., 2014
	C, D	Present a quantitative model for auditing and analyze the impact on audit quality	D. Kim & H. Kim, 2004
	B, C, D	Identify factors affecting the quality of DB security audits and present a conceptual framework for auditing	Muneeb-ul-Hasan & Arshad, 2019
	D	Propose a security and privacy audit model	Zorkadis & Siougle, 2001
		Present the SISAP (Simple Information Security Audit Process) methodology	Raggad & Collar, 2006
		Propose a conceptual framework for international standards-based auditing	Pereira & Santos, 2010
		Propose an information security audit model	von Roessing, 2005; Lee, et al., 2010; Gulzira, et al., 2020; Pereira & Santos, 2011
		Present an audit model using XML concepts	Golyash, et al., 2011
		Present a maturity-based audit model	Lee & Park, 2015
		Presenting a fuzzy-based audit model	Rytov, et al., 2017

A (감사인/조직); Audits (감사 활동/절차); B (감사 대상); C (감사 목적/효과); D (감사 기준/지침)

〈표 23〉 연구주제 D(감사 기준/지침)의 세부 내용
〈Table 23〉 Contents of Research Topic D

Content	All	Overseas	Domestic
Standard/Criteria	5 (9.6%)	5 (14.3%)	0 (0%)
Tools/Techniques	21 (40.4%)	17 (48.6%)	4 (23.5%)
Model/Guidelines	26 (50.0%)	13 (37.1%)	13 (76.5%)
Total	52 (100%)	35 (100%)	17 (100%)

〈표 24〉 연구주제 D(감사 기준/지침) 연구의 기간별 분석 결과
〈Table 24〉 Analysis Results for Research Topic D by Period

Content	Before 2000	2001~2005	2006~2010	2011~2015	2016~2020	After 2021	Sum
Reference/ Standard	-	Capuder, 2004	Popa & Doinea, 2007	Cefaratti, et al., 2011; Bendovschi & Ionescu, 2015	Bhaskara, et al., 2018	-	5(0)
Tools/ Techniques	-	-	Popescu, et al., 2007; Ivanova, et al., 2010; Lee & Park, 2010; Lee, et al., 2010	Surcel & Amancei, 2011; Jeon, et al., 2012; Kanatov, et al., 2014; Shultz, et al., 2014; Atymtayeva & Kozhakhmet, 2015; Hermanowski, 2015; Rudowski & Tarnowska, 2016	Kozlovs, et al., 2016; Li, 2016; Livshitz, et al., 2016; Rudowski & Tarnowska, 2016; Lee, et al., 2018; Markina & Diachkov, 2019; Satoh & Samejima, 2019; Voevodin, et al., 2020	Lakhno, et al., 2021; Lontsikh, et al., 2021	21(4)
Model/ Instructions	Kim & Nam, 1993; Jeong, et al., 1997; Ryu, et al., 1997	Zorkadis & Siougle, 2001; Choi & Nam, 2001; Yun, et al., 2003; D. Kim & H. Kim, 2004; von Roessing, 2005	Raggad & Collar, 2006; Jeon, et al., 2006; Jeon, et al., 2007; Lee, 2008; Lim, et al., 2008; Lee, et al., 2009; Pereira & Santos, 2011	Billones & Ona, 2011; Golyash, et al., 2011; Pereira & Santos, 2011; Yu, et al., 2014; Lee & Park, 2015; Gupta & Shakya, 2015	Dharmalingam & Smalov, 2016; Rytov, et al., 2017; Wen, et al., 2018; Muneeb-ul-Hasan & Arshad, 2019; Gulzira, et al., 2020	-	26(13)
합계	3(3)	6(3)	12(7)	15(3)	14(1)	2(0)	52(17)

Numbers in () are the numbers of domestic research articles

로, 향후 활발한 연구가 필요한 분야는 아니라고 판단된다. 이에 비해서 도구/기법, 지침/모델 부분은 향후 새로운 기술, 연구되지 않은 산업 등과 같은 감사의 대상은 지속적으로 확대 발전할 것이므로 이러한 변화를 반영한 도구/기법, 지침/모델에 대한 연구는 계속 추진될 것으로 예상된다. 한 가지 우려되는 사항은 지침/모델의 경우, 국내의 연구는 2016년 이후로 찾아볼 수 없다는 점이다. 향후 국내에서도 이 분야에 지속적인 관심을 가질 필요가 있다고 판단된다.

Ⅳ. 결론

본 연구에서는 정보보안 감사 분야에서 수행된 국내외의 문헌 103개를 식별하여, 이러한 문헌의 일반적인 연구 동향과 세부 내용을 분석하고, 국내외 문헌들의 내용을 비교 분석하였다. 다음에서는 이러한 분석 결과를 토대로 본 연구의 주요한 발견 사항을 재정리하고, 이를 바탕으로 정보보안 감사 분야의 향후 연구에서 고려해야 할 사항들을 제시하도록 한다.

정보보안 감사 분야의 학술 연구는 1990년대에 시작된 비교적 새로운 연구 분야인데, 그 이후 지속적으로 연구되어 매년 연구 편수가 증가하고 있다. 국내 연구는 해외에 비해 5년 정도 앞서 시작되었고, 연구가 활발하게 수행된 시기도 10년 정도 빨랐다. 그러나 해외에서는 이 분야의 연구가 지속적으로 수행되고 있으나, 우리나라의 경우에는 2018년 이후에는 발표된 연구 논문이 없는 것으로 나타났다. 민간과 공공을 막론하고 조직에서 정보보안의 중요성이 점점 더 높아지고 있는 현실을 감안한다면, 이 분야에 대한 학술적인 연구가 다시 한번 활성화될 필요가 있다고 판단된다.

연구 방법적인 측면에서 보면, 이 분야의 연구는 비실증 연구의 비중이 절대적이고(80%), 국내의 경우에는 그 비중이 90% 이상으로 더욱 치중되어 있다. 실증 연구의 세부 연구방법을 살펴보면, 해외 연구는 여러 가지 방법이 활용되고 있으나, 국내 연구는 모두 서베이 방법만을 사용하고 있다. 비실증 연구의 세부 연구방법 또한 해외 연구는 여러 가지 방법을 비교적 균형 있게 적용하는데 반해서, 국내 연구의 경우에는 개념 모델의 비중이 압도적이고(75%), 수리/공학 모델이 활용이 매우 저조한 것으로 나타났다.

이 분야의 이론적인 발전을 위해서는 비실증 연구에서 축적된 연구 결과들을 기반으로 보다 설명적인 결과를 제시할 수 있는 실증 연구의 비중을 높일 필요가 있다. 또한 국내 연구에서는 실증 연구나 비실증 연구를 수행할 때, 현재 많이 사용하고 있는 서베이, 개념 모델 등의 방법뿐만 아니라 기타 연구방법들의 활용을 고려할 필요가 있다.

연구의 내용적인 측면에서 보면, 첫째, 연구주제 A(감사인/감사조직)는 주제들 중에서 가장 적게 연구되었고, 비교적 최근 들어 연구되고 있는 분야이지만, 본 연구에서 검색한 바로는 국내에서는 수행된 연구를 찾을 수 없었다. 우리나라에는 정보보안 감사인의 자격 요건과 훈련 등을 규정하는 공공 부문의 정보시스템 감리 기준 등이 존재하기 때문에 이 분야의 연구가 없는 것으로 생각되지만, 정보보안 감사 분야에 특화된 감사인/감사법인 등을 연구하는 것은 이 분야 발전에 기여할 수 있을 것이다.

또한 연구에 사용된 감사인의 역량과 같은 변수가 종합적이고 일관성 있게 정의되지 않고 있다. 정보보안 감사 분야 연구의 누적적인 발전을 위해서는 이러한 변수들에 대한 전체적인 프레임워크를 수립하는 연구가 필요하다. 또한 연구 주제 A(감사인/조직)만을 살펴보는 것보다는 다른 주제들과의 상관관계를 분석하는 것이 보다 고도화된 연구이므로 감사인(A)이 감사의 효과/성과/품질(C) 등에 미치는 영향을 미치는 연구 등은 이론적으로나 실무적으로 유용한 연구가 될 수 있다.

둘째, 연구 주제 Audits(감사 활동/절차)의 경우, 양적으로 많은 것은 아니지만, 지속적으로 연구되고 있는 주제이다. 그런데 정보보안 감사의 개념/절차 등과 같은 기본적인 사항에 대한 연구는 이미 많이 수행되었으므로, 감사의 주요한 활동(감사 계획 수립, 감사 시행, 감사 보고서 작성/전달, 감사 사후관리)의 수행 과정/결

과를 체계적으로 분석하는 연구와 같이, 감사의 세부 활동 과정과 결과를 분석하는 연구를 수행할 필요가 있다.

셋째, 연구 주제 B(감사 대상)에 대한 연구에서는 다양한 신기술, 보안 분야, 산업 등을 분석하였는데, 정보보안 감사의 대상이 되는 신기술과 감사가 적용될 산업/보안 분야는 지속적으로 확대될 것이므로 이 주제에 대한 연구는 앞으로도 계속해서 진행될 것이다. 그런데 흥미로운 사실은 국내 연구와 해외 연구에서 분석한 신기술/특정 산업/특정 보안분야 등이 대체로 중복되지 않는다는 것이다. 따라서 향후의 국내 연구에서는 지금까지 해외 연구에서만 다루어졌으나 국내에서는 다루어지지 않은 분야를 주목해 볼 가치가 있다.

넷째, 연구 주제 C(감사 목적/효과)의 경우, 정보보안 감사의 필요성/목적 등에 대한 정당성을 부여하기 위한 연구는 이 분야의 역사를 고려할 때 이제 더 이상 크게 필요하지 않을 것으로 판단된다. 정보보안 감사의 성과/효과와 품질에 대해 향후에 필요한 연구로는 현재 연구마다 서로 다르게 조작화되고 있는 성과/품질을 종합적이고 체계적으로 정의하는 연구가 매우 필요하다. 특히 국내 연구에서는 정보보안 감사의 성과/품질을 거의 다루고 있지 않은데, 국내의 정보보안 감사를 개선하고 향상시키는데 기여할 수 있는 학술 연구가 꼭 필요한 실정이다.

연구 주제 D(감사 기준/지침) 분야의 경우, 감사 기준/표준, 도구/기법, 지침/모델 등에 대한 연구가 이루어졌는데, 이 중에서 지침/모델에 대한 연구들이 가장 활발하게 수행되었고, 특히 국내 연구는 이 부분에 집중되어 있다. 감사 기준/표준은 한번 수립되면 크게 변경되는 경우는 많지 않으므로, 향후 활발한 연구가 필요한 분야는 아니라고 판단된다. 이에 비해서 도구/기법, 지침/모델 부분은 향후 감사의 대상이 확대 발전됨에 따라 이러한 변화를 반영한 연구는 계속 추진될 것으로 예상된다. 한 가지 우려되는 사항은 지침/모델의 경우, 국내의 연구는 2016년 이후로 찾아볼 수 없다는 점이다. 향후 국내에서도 이 분야에 지속적인 관심을 가질 필요가 있다고 판단된다.

본 연구에서는 정보보안 감사 분야에서 출간된 모든 연구 논문을 분석 대상을 하다보니, 학술대회 발표 논문들도 포함되었고, 분석에 포함된 논문의 질을 평가하지는 못한 한계를 가지고 있다.[12] 향후 이 분야의 문헌고찰 연구에서는 논문의 품질도 고려한 연구가 바람직할 것으로 판단된다.

■ References

Afifi, M. A. (2020). "Assessing Information Security Vulnerabilities and Threats to Implementing Security Mechanism and Security Policy Audit." *Journal of Computer Science, 16*(3), 321-329.

Alavi, M. & Carlson, P.(1992). "A Review of MIS Research and Disciplinary Development." *Journal of MIS, 8*(4), 45-62.

Almadhoob, A. & Valverde, R. (2014). "Cybercrime prevention in the Kingdom of Bahrain via IT security audit plans." *Journal of Theoretical and Applied Information Technology, 65*(1), 274-292.

Alviana, S. (2020). "User Care Level Audit of Information Data Security at PT XYZ Using Guttman Scale." *IOP Conference Series: Materials Science and Engineering, 879*(1), 1-7.

Arionadi, K., Dharma, S. A. & Partha, C. G. I. (2016). "IT security audit based on CISSP PMBOK framework." *International Journal of Engineering and Emerging Technology, 1*(1).

Atymtayeva, L. & Kozhakhmet, K. (2015). "Development of expert system for information security audit."

12) 본 연구의 분석에 포함된 논문들이 게재된 학술지의 목록은 부록에 첨부되어 있다.

International Journal of Computer Research, 22(4), 399.

Au, C. & Fung, W. (2019). "Integrating knowledge management into information security: From audit to practice." *International Journal of Knowledge Management(IJKM), 15*(1), 37-52.

Azubike, J. (2011). "Computer information security audit: Procedures for policy design and implementation." *Nigeria Journal of Education, Health and Technology Reserch(NJEHETR), 1*(2), 164-168.

Barankova, I. & Mikhailova, U. & Kalugina, O. (2019). *Analysis of the Problems of Industrial Enterprises Information Security Audit.* Paper presented at the International Russian Automation Conference, 976-985.

Beldiman, C. (2021). "Risks' Identification and Assessment in a Public Entity Regarding the IT Security Audit." *Annals of the University Dunarea de Jos of Galati: Fascicle: I, Economics & Applied Informatics, 27*(1).

Bendovschi, A. & Ionescu, B. (2015). "The Gap between Cloud Computing Technology and the Audit and Information Security." *Audit Financiar, 13*(125).

Bhaskara, I. M. A., Suardani, L. G. P. & Wijaya, W. A. (2018). "Data and Information Security Audit Using IT Baseline Protection Manual at PT." *XYZ. International Journal of Engineering and Emerging Technology, 2*(2), 78-82.

Billones, M. O. M. & Ona, S. E. (2011). *Formulation of an Information Security Audit Process Model Applicable to Educational Institutions*. Paper presented at the International Conference on Information Theory and Applications, I29.

Candiwan, M. Y. D. & Priyadi, Y. (2016). "Analysis of Information Security Audit Using ISO 27001: 2013; ISO 27002; 2013 at IT Division-X Company, In Bandung, Indonesia." *International Journal of Basic and Applied Science, 4*(4), 77-88.

Capuder, L. (2004). "ISO-17799-Standard for Information Security: A Welcome Boon for Security Management and Audit." *EDPACS, 31*(11), 1-10.

Cefaratti, M. A., Lin, H. & Wallace, L. (2011). "The information security control environment: chief audit executives responding to a survey identify the most and least common controls their organizations deploy to protect IT resources." *Internal Auditor, 68*(2), 55-59.

Chandra, I. (2008). "The five C's of IT policy: reviewing the effectiveness of information security policies is a key part of IT audit plans." *Internal Auditor, 65*(6), 23-25.

Choi, J. & Nam, K. (2001) "A Study on an Audit Model for the Defense Information System security using BS7799." *Journal of the Military Operations Research Society of Korea, 27*(1), 89-100.

{최장욱·남길현 (2001). BS7799 (정보보안관리 표준)를 적용한 국방정보체계 보안감사모델에 관한 연구. 〈한국국방경영분석학회지〉, 27권 1호, 89-100.}

Cohen, F. (1998). "Managing Network Security: How does a typical IT audit work?" *Network Security, 1998*(7), 8-11.

Dharmalingam, R. & Smalov, L. (2016). "Information Security Audit in Virtual Environment." *The Research Bulletin of Jordan ACM, 2*, 132-136.

Dias, B. (2021). "Big data information security audit" *Earth Sciences*, 19, 51-53.

Drastich, M. (2013). "Audit of information security management system." *Global Journal on Technology, 3*, 1051-1056.

Gill, G. & Bhattacherjee, A., (2009). "Whom Are We Informing? Issues and Recommendations for MIS Research From an Informing Sciences Perspective." *MIS Quarterly, 33*(2), 217-235.

Goel, S., Pon, D. & Menzies, J. (2006). "Managing information security: Demystifying the audit process for security officers." *Journal of Information System Security, 2*(2), 25-45.

Golyash, I. & Sachenko, S. & Rippa, S. (2011). *Improving the information security audit of enterprise using XML technologies*. Paper presented at the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems, 2, 795-798.

Grzyb, M. & Kowalik, D. (2020). "Information security management–audit of the IT system." *Information management in the era of the Internet*, 83-104.

Gulzira, M., Gulmira, B., Altynbek, S. & Assel, O. (2020). *The audit method of enterprise's Information security*. Paper presented at the 6th International Conference on Engineering & MIS 2020, 1-5.

Gupta, A. & Shakya, S. (2015). "Information System Audit: Cloud Computing Security and Challenges." *International Journal of Computer Science and Mobile Computing (IJCSMC), 4*(11), 48-56.

Hamdan, M. N. M. (2017). "The Relationship between Network Security Policies and Audit Evidence Documentation: The Accounting Information Security Culture as a Mediator." *International Journal of Business and Management, 12*(12), 168-180.

Hatsu, S., Ujapka, M. B. & Mpimwood, E. D. (2015). "An examination of the extent of implementation of the information security system and IT audit system in Ghananian Banks [J]." *Journal of Mass Spectrometry, 11*(11), 375-382.

Hermann, Y. K. J. & Tanguy, K. B. (2022). "Study on the Audit of IT Security in Health Structures: Case of Health Structures in Burkina Faso." *American Journal of Science, Engineering and Technology, 7*(2), 39-43.

Hermanowski. D. (2015). *Open source security information management system supporting IT security audit.* Paper presented at 2015 IEEE 2nd international conference on cybernetics, 336-341.

Hwang, I. & Kim, D. (2016) "The Effect of Organizational Information Security Environment on the Compliance Intention of Employee." *Journal of information systems, 25*(2), 51-77.

{황인호·김대진 (2016). 조직의 정보보안 환경이 조직구성원의 보안 준수의도에 미치는 영향. 〈정보시스템연구〉, 25권 2호, 51-77.}

Ivanova, N., Korobulina, O. & Burak, P. (2010). "Methods of analysis for the information security audit." *New Trends in Information Technologies. ITHEA, Sofia*, 152-161.

Jeon, K., Jang, J. & Noh, H. (2007) "Security Auditing Check List for Web Applications." *Institute for Basic Science(IBS), 18*, 153-166.

{전계현·장주현·노희영 (2007). 웹 애플리케이션을 위한 보안감리 점검항목. 〈기초과학연구〉, 18권, 153-166.}

Jeon, S., Lim, J., Lee, K. & Han, K. (2012) "A Study on Security Audit Checking Items for the RFID-Based Information System." *Korea Society of IT Services, 11*(4), 107-121.

{전상덕·임지영·이기영·한기준 (2012). RFID 기반 정보시스템을 위한 보안감리 점검항목 연구. 〈한국IT서비스학회지〉, 11권 4호, 107-121.}

Jeon, S., Zeelim-Hovav, A. & Lee, H (2015). "Impact of Psychological Ownership, Job Position and

Awareness of Audit on Information Security Policy Compliance Intention." *The Journal of Internet Electronic Commerce Research, 15*(6), 39-55.

{전수현·아낫 호바브·이해원 (2015). 심리적 임파워먼트, 직급, 감사에 대한 인식이 정보보안정책 준수의도에 미치는 영향. 〈인터넷전자상거래연구〉. 15권 6호, 39-55.}

Jeon, Y., Cho, K. & Kim, W. (2006) "A Design and Implementation of Information Security Management and Audit System for Government Agencies." *Journal of Internet Computing and Services (JICS), 7*(5), 81-93.

{전용준·조기환·김원규 (2006). 공공기관의 정보보호관리체계 감사시스템의 설계 및 구현. 〈한국인터넷정보학회〉, 7권 5호, 81-93.}

Jeong, K., Kim, K., Seo, K., Ryu, K. & Kang, C. (1997) "Implementation of Audit Trail Service System for EDI Security." *The KIPS Transactionsty, 4*(3), 754-766.

{정경자·김기중·서경란·류근호·강창구 (1997). 정보보안 EDI 보안 감사 추적 서비스 시스템 구현. 〈정보처리학회논문지〉, 4권 3호, 754-766.}

Jeong, C. (2013) "Review of Privacy Policies of Personal Data Processors and Audit of Privacy Protection: Lessons from the EU, the UK and the US Experiences." *Chosun law journal, 20*(1), 3-29.

{정찬모 (2013). 개인정보취급방침 심사와 개인정보보호 감사제도 도입방안: EU, 영국, 미국의 사례와 시사점. 〈법학논총〉, 20권 1호, 3-29.}

Kanatov, M., Atymtayeva, L. & Yagaliyeva, B. (2014). *Expert systems for information security management and audit.* Implementation phase issues. Paper presented at the 2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS), 896-900.

Kim, D. & Kim, H. (2004). "Research on application of quantification model to security audit evaluation to improve information system audit quality." *Journal of Information Technology Applications & Management, 11*(2), 45-64.

{김동수·김현수 (2004). 정보시스템 감리품질향상을 위한 보안 감리평가에의 정량화 모델 적용 연구. 〈Journal of Information Technology Applications & Management〉, 11권 2호, 45-64.}

Kim, J. & Hwang, K. (2022). "Analysis of domestic research trends in the field of information system auditing." *Public Audit and Inspection Review, 37*, 95-121.

{김지영·황경태 (2022). 정보시스템 감사 분야의 국내 연구 동향 분석. 〈감사논집〉, 37권, 95-121.}

Kim, M., Park, S. & Kwon, H. (2013). *Research on IT audit process for information security.* Paper presented at the Korean IT Service Society Conference Proceedings, 639- 642.

{김민전·박성갑·권호열 (2013). 정보보호를 위한 IT 감사 프로세스에 관한 연구. 〈한국 IT 서비스학회 학술대회 논문집〉, 639-642.}

Kim, T. (2014). "A review of domestic information protection-related laws and systems." *Boannews*, 2022

{김태형 (2014). 국내 정보보호관련 법·제도 되짚어보기. 〈보안뉴스〉. (검색일 2022.03.15}

Kim, Y. & Nam, K. (1993). "Information system security and audit trail mechanisms." *Journal of Communications and Information Security, 3*(3), 67-79.

{김영철·남길현 (1993). 정보시스템 보안과 감사증적 메카니즘. 〈통신정보보호학회지〉, 3권 3호, 67-79.}

Kim, Y. & Cho, S. (2012). "Analysis of social network

service research trends in the media area." *informatization policy, 19*(4), 3-26.

{김유정·조수선 (2012). 미디어 영역에서의 소셜네트워크서비스 연구동향 분석. 〈정보화정책〉, 19권 4호, 3-26.}

Kozlovs, D., Cjaputa, K. & Kirikova, M. (2016). "Towards Continuous Information Security Audit. REFSQ Workshops."

Lakhno, V., Akhmetov, B., Chubaievskyi, V., Desiatko, A., Palaguta, K., Blozva, A. & Chasnovskyi, Y. (2021). "Information Security Audit Method Based on the Use of a Neuro-Fuzzy System." *Proceedings of the Computational Methods in Systems and Software.* 171-184.

Li, Z. (2016). "Research on Information Security Audit Base on Semantic Web Ontology and Improve Vector Space Model." *International Journal of Security and Its Applications, 10*(12), 141-152.

Lee, C. (2008) "A Study on industrial control system information security Auditing framework." *Journal of The Korea Institute of Information Security and Cryptology (JKIISC), 18*(1), 139-148.

{이철수 (2008). 산업제어시스템 정보보안 감리 프레임워크 연구. 〈정보보호학회논문지〉, 18권 1호, 139-148.}

Lee, C., Hong, S., Kang, S. & Kim, J. (2009). "The Study on the Information Security Audit Guideline for SCADA System." *Informational International Interdisciplinary Journal, 12*, 147-162.

Lee, D. & Park, J. (2010) "A Study on the Information System Security Audit Method for Personal Information Protection." *Journal of Korea Safety Management & Science, 12*(4), 107-116.

{이동녁·박정선 (2010). 개인정보보호를 위한 정보시스템 보안감사 방법에 관한 연구. 〈대한안전경영과학회지〉, 12권 4호, 107-116.}

Lee, E., Park, B., Jang, S. & Lee, S. (2018) "Study on IT security audit system for e-commerce private information protection." *The Korea Society of Computer and Information, 26*(1), 179-182.

{이은경·박병우·장석은·이상준 (2018). 전자상거래 개인정보 보호를 위한 IT 보안감사체계 연구. 〈한국컴퓨터정보학회 학술발표논문집〉, 26권 1호, 179-182.}

Lee, H. & Myung, S. (2013) "Analysis of Research Trends in domestic informatization and e-government since 2000." *Informatization Policy, 20*(4), 3-22.

{이혜원·명승환 (2013). 국내의 정보화 및 전자정부 연구동향 분석. 〈정보화정책〉, 20권 4호, 3-22.}

Lee, J., Shin, S., Kim, H. & Hwang, K. (2012) "A Study on Research Framework and Research Trends in IT Service Management (ITSM) Area." *Informatization Policy, 19*(1), 3-24.

{이종옥·신성희·김홍근·황경태 (2012). IT 서비스 관리(ITSM) 분야의 연구 프레임워크 및 연구동향 분석. 〈정보화정책〉, 19권 1호, 3-24.}

Lee, J., Kim, D. & Kim H. (2010) "A Design on the Information Security Auditing Framework of the Information System Audit." *Journal of the Korea Society of Digital Industry and Information Management, 6*(2), 233-245.

{이지용·김동수·김희완 (2010). 정보시스템 감리에서의 정보보호 감리모형 설계. 〈디지털산업정보학회 논문지〉, 6권 2호, 233-245.}

Lee, N., Lee, J. & Hwang, K. (2014) "Research framework and research trends in the field of healthcare information technology." *informatization policy, 21*(3), 3-32.

{이난경·이종옥·황경태 (2014). 헬스케어 정보기술 분야의 연구 프레임워크 및 연구동향. 〈정보화정책〉, 21권 3호, 3-32.}

Lee, S. & Park, D. (2015) "A Study on Maturity Model for Improving Security Check in Information

System Audit." *Journal of Security Engineering, 12*(2), 151-168.

{이수현·박대하 (2015). 정보시스템 감리 보안점검 성숙도 모델. 〈보안공학연구논문지〉, 12권 2호, 151-168.}

Lim, J., Kim, D. & Han, K. (2008) "Securiry Audit Checking Items for the RFID-Based Information Systems." *Korea Society of IT Services*, 419-422.

{임지영·김동오·한기준 (2008). RFID 기반 정보시스템을 위한 보안감리 점검항목. 〈한국 IT 서비스학회: 학술대회 논문집〉, 419-422.}

Lin, R. & Huang, Y. (2020). *Enterprise Internal Audit Data Network Security System in the Information Age.* Paper presented at the International Conference on Cyber Security Intelligence and Analytics, 98-103.

Livshitz, I. I., Nikiforova, K. A., Lontsikh, P. A. & Karasev, S. N. (2016). *The new aspects for the instantaneous information security audit*. Paper presented at the 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS), 125-127.

Lo, E. C. & Marchand, M. (2004). *Security audit: a case study information systems*. Paper presented at the Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No. 04CH37513), 1, 193-196.

Lontsikh, P. A., Safonova, O. M., Koksharov, A. V., Lontsikh, N. P. & Golovina, E. Y. (2021). *Remote Audit Improvement Methods in the System-oriented Information and Security Analysis.* Paper presented at the 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 178-182.

Lu, H., Cui, X., Wang, L., Jiang, Y. & Cui, M. (2018). *The Research on Security Audit for Information System Classified Protection*. Paper presented at the International Conference on Cloud Computing and Security, 300-308.

Markina, I. & Diachkov, D. (2019). "Information security audit specificity." *Moderní věda,* 1, 13-20.

Min, H. & Lee, H. (2016). *The need to redefine the concept of information security auditing.* Paper presented at the Korea Society of IT Services Conference Proceedings, 293-294.

{민현우·이희조 (2016). "정보보호 감사의 개념 재정립 필요성." 〈한국 IT 서비스학회 학술대회 논문집〉, 293-294.}

Muneeb-ul-Hasan, S. H. O. & Arshad, M. M. (2019). "A Conceptual Framework of Information Security Database Audit and Assessment." *International Journal of Innovative Computing, 9*(1), 7-13.

Nastase, F. & Nastase, P. (2007). "Information Security Audit in e-business applications." *Informatica Economica, 11*(1), 79-87.

NIA (2022). *National informatization white paper*.

{한국지능정보사회진흥원 (2022). 〈2022 국가지능정보화백서〉.}

NCSC (2022). *National Cyber Security Center Guideline 2022.*

{국가사이버안전센터 (2022). 〈2022년 국가 정보보안지침〉.}

Office of Government Commerce(OGC). (2007). ITIL V3. Service Design.

Othman, N. A. A., Norman, A. A. & Kiah, M. L. M. (2021). "Information System Audit for Mobile Device Security Assessment." 2021 3rd International Cyber Resilience Conference(CRC), 1-6.

Palvia, P., Chau, P., Kakhki, M.D., Ghoshal, T., Uppala, V. & Wang, W. (2017). "A Decade Plus Long Introspection Of Research Published In Information & Management." *Information & Management, 54*(2), 218-227.

Pathak, J. (2006). "Internal audit and corporate

governance: A program for information security review audit." *The EDP Audit, Control, and Security Newsletter, 31*, 1-13.

Pereira, T. & Santos, H. (2010). "An audit framework to support information system security management." *International Journal of Electronic Security and Digital Forensics, 3*(3), 265-277.

Pereira, T. & Santos, H. (2011). "Description of a Practical Application of an Information Security Audit Framework." *Paper presented at the European Conference on Cyber Warfare and Security,* 315.

Popa, M. (2010). "Requirements for Development of an Assessment System for IT&C Security Audit." *Journal of Mobile, Embedded and Distributed Systems, 2*(2), 56-64.

Popa, M. & Doinea, M. (2007). "Audit Characteristics for Information System Security." *Informatica Economică, 11*(4), 103-106.

Popescu, G., Popescu, V. A. & Popescu, C. R. (2007). "Information systems security audit." *Manager Journal, 6*(1), 81-88.

Popescu, G., Popescu, V. A. & Popescu, C. R. (2008). "Conducting an information security audit." *Manager Journal, 7*(1), 76-82.

Quanxiu, H. & Guangying, C. (2011). "Research of security audit of enterprise group accounting information system under internet environment." *Paper presented at the 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC),* 516-519.

Radu, R. I. & Isai, V. (2014). "Determination of the Effectiveness of Information Security and Audit Accounting IT Informational Program." *Annals of the University Dunarea de Jos of Galati: Fascicle: I, Economics & Applied Informatics, 20*(2), 93-98.

Raggad, B. G. & Collar, E. J. (2006). "The Simple Information Security Audit Process: SISAP." *International Journal of Computer Science and Network Security, 6*(6), 189-198.

von Roessing, R. (2005). *Improving the IT Security Audit Framework: Standards, Common Ground, and Strategic Alignment.* Proceedings of Security and Protection of Information 2005, 25-32.

Roratto, R. & Dias, E. D. (2014). "Security information in production and operations: a study on audit trails in database systems." *JISTEM-Journal of Information Systems and Technology Management, 11*, 717-734.

Rudowski, M. & Tarnowska, K. (2016). "Decision support system for information systems security audit (WABSI) as a component of IT infrastructure management." *Information Systems in Management, 5*(3), 389-400.

Rytov, M. Y., Leksikov, E. V., Sakalo, V. I. & Kovalev, P. A. (2017). "The Use of Fuzzy Cognitive Modelling to Manage Information Security Audit of Information Portals of Regional Executive Authorities." *Journal of Physics: Conference Series, 803*, 1-5.

Ryu, K., Kim, K., Yoon, S. & Lee, Y. (1997) "Design of intrusion detection and audit tracking system using information security computer network events." *Information Processing Society Journal, 4*(9), 2342-2353.

{류근호·김기중·윤상훈·이용준 (1997). 정보보안 전산망 사건을 이용한 침입 감지 및 감사 추적 시스템 설계. 〈정보처리학회논문지〉, 4권 9호, 2342-2353.}

Salihu, A. & Berisha-Hoti, X. (2019). "The Effect of IT

Audit on Security Incidents." *International Journal of Scientific & Technology Research, 8*(8), 1342-1347.

Satoh, N. & Komoda, N. (2005). *A labor time estimation model for the information security audit by quantitative analysis I and regression analysis.* Paper presented at the 4th WSEAS International Conference on E-Activities, 136-141.

Satoh, N. & Samejima, M. (2019). "Risk words suggestion for information security audit by Bayesian inference." *Electronics and Communications in Japan, 102*(1), 42-48.

Schryen, G., Benlian, A., Rowe, F., Gregor, S., Larsen, K., Petter, S. & Yasasin, E. (2017). "Literature reviews in IS research: What can be learnt from the past and other fields?" *Communications of the Association for Information Systems, 41*(30), 759-774.

Shakya, S. & Gupta, A. (2017). "Concerns on Information System and Security Audit". *Journal of Advanced College of Engineering and Management, 3*, 127-135.

Schultz, V., Kulba, V. & Shelkov, A. (2014). "Information security audit of automated control systems." *Trends and management, 4*, 319-334.

Singleton, T. W. & Singleton, A. J. (2008). "The potential for a synergistic relationship between information security and a financial audit." *Information Security Journal: A Global Perspective, 17*(2), 80-86.

Smith, G. (2007). "Greatest IT audit and security risks of 2006." *Journal of Corporate Accounting & Finance, 18*(4), 43-48.

Stafford, T., Deitz, G. & Li, Y. (2018). "The role of internal audit and user training in information security policy compliance." *Managerial Auditing Journal, 33*(4), 410-424.

Stafford, T., Gal, G., Poston, R., Crossler, R. E., Jiang, R. & Lyons, R. (2018). "The role of accounting and professional associations in it security auditing: An AMCIS panel report." *Communications of the Association for Information Systems, 43*(1), 482-493.

Steinbart, P. J., Raschke, R. L., Gal, G. & Dilla, W. N. (2013). "Information security professionals' perceptions about the relationship between the information security and internal audit functions." *Journal of Information Systems, 27*(2), 65-86.

Steinbart, P. J., Raschke, R. L., Gal, G. & Dilla, W. N. (2018). "The influence of a good relationship between the internal audit and information security functions on information security outcomes." *Accounting, Organizations and Society, 71*, 15-29.

Suduc, A. M., Bîzoi, M. & Filip, F. G. (2010). "Audit for information systems security." *Informatica Economica, 14*(1), 43.

Surcel, T. & Amancei, C. (2007). "The Information Security Management System, Development and Audit." *Informatica Economica, 11*(4), 111-114.

Surcel, T. & Amancei, C. (2011). "A Progressive Improvement of the Integrated System for Academic Management through Information Security Management System Audit and Metrics." *Academy of Economic Studies. Economy Informatics, 11*(1), 132-141.

Tanriverdi, H., Bertsch, J., Harrison, J., Hsiao, P. L., Mesuria, K. S. & Hendrawirawan, D. (2006). "AlphaCo: A Teaching Case on Information Technology Audit and Security." *Journal of Digital Forensics, Security and Law, 1*(1), 45-68.

Tofan, D. C. (2011). "The Security Audit Within Information Systems." *Paper presented at the 6th International Conference on Knowledge Management: Projects, Systems and Technologies, 18.*

Vieira, T. & Serrão, C. (2016). "Web applications security and vulnerability analysis financial web applications security audit a case study." *International Journal of Innovative Business Strategies (IJIBS), 2*(2), 86-94.

Voevodin, V. A., Markina, M. S. & Markin, P. V. (2020). "Determination of the weight of audit evidence by the method of point ratings in the information security audit." *Computational Nanotechnology, 1*, 57-62.

Warigon, S. (1999). "Information Security and Audit Implications of Electronic Money." *EDPACS, 26*(7), 12-15.

Wen, C. C. K., Othman, S. H. & Sirat, M. M. (2018). "Development of Metamodel on Information Security Risk Audit and Assessment for IT Assets in Commercial Bank." *International Journal of Innovative Computing, 8*(2), 23-32.

Westland, J. (2021). "Assessing Privacy and Security of Information Systems from Audit Data." *Information Systems Frontiers,* 1-18.

Yen, J., Lim, J., Wang, T. & Hsu, C. (2018). "The impact of audit firms' characteristics on audit fees following information security breaches." *Journal of Accounting and Public Policy, 37*(6), 489-507.

Yoon, S., Jang, E. & Kwon, H. (2003) *A study on security audit process model of web-based system.* Paper presented at the Korea Society of IT Services Conference Proceedings, 407-412.

{윤상현·장은정·권호열. (2003). 웹기반 시스템의 보안감리프로세스 모델에 관한 연구. 〈한국 IT 서비스학회 학술대회〉, 407-412.}

Yu, G. & Gao, P. (2013). *Risk-Based Information Security Audit Applied Research in the Power Industry.* Paper presented at the 2013 International Conference on Control Engineering and Communication Technology. 176-179.

Yu, W., Han, K., Kim, D. & Kim, H. (2014) "Audit model for information protection in hospital information systems." *Digital convergence, 12*(7), 133-145.

{유완희·한기준·김동수·김희완 (2014). 병원정보시스템에서의 정보보호를 위한 감리모형. 〈디지털융복합〉, 12권 7호, 133-145.}

Zhou, X. (2020). *Improvement of information System Audit to Deal With Network Information Security.* Paper presented at the 2020 International Conference on Communications, Information System and Computer Engineering (CISCE). 93-96.

Zorkadis, V. & Siougle, E. (2001). *Information Security and Privacy Audit Modeling*. Paper presented at the 5th world multiconference on Circuits, Systems, Communications and Computers.

[부록] 본 연구의 분석에 포함된 논문이 발간된 학술지명

국문 학술지 (가나다 순)

- 감사논집
- 기초과학연구
- 대한안전경영과학회지
- 디지털산업정보학회 논문지
- 디지털융복합
- 법학논총
- 보안공학연구논문지
- 인터넷전자상거래연구
- 정보보호학회논문지
- 정보시스템연구
- 정보처리학회논문지
- 정보화정책
- 통신정보보호학회지
- 한국국방경영분석학회지
- 한국인터넷정보학회
- 한국IT서비스학회지
- Journal of Information Technology Applications & Management

국문 학술대회 논문지 (가나다 순)

- 한국컴퓨터정보학회 학술발표논문집
- 한국IT서비스학회 학술대회 논문집

영문 학술지 (알파벳 순)

- Accounting, Organizations and Society
- American Journal of Science, Engineering and Technology
- Audit Financiar
- Communications of the Association for Information Systems
- Computational Nanotechnology
- Earth Sciences
- Economics & Applied Informatics
- Economy Informatics
- EDPACS
- Electronics and Communications in Japan
- Global Journal on Technology
- Informatica Economica
- Information-An International Interdisciplinary Journal
- Information management in the era of the Internet
- Information Security Journal: A Global Perspective
- Information Systems Frontiers
- Information Systems in Management
- Internal Auditor
- International Journal of Basic and Applied Science
- International Journal of Business and Management
- International Journal of Computer Research
- International Journal of Computer Science and Mobile Computing
- International Journal of Computer Science and Network Security
- International Journal of Electronic Security and Digital Forensics
- International Journal of Engineering and Emerging Technology
- International Journal of Innovative Business Strategies
- International Journal of Innovative Computing
- International Journal of Knowledge Management
- International Journal of Scientific & Technology Research
- International Journal of Security and Its Applications
- International Russian Automation Conference
- IOP Conference Series: Materials Science and Engineering
- Journal of Accounting and Public Policy
- Journal of Advanced College of Engineering and Management
- Journal of Computer Science
- Journal of Corporate Accounting & Finance
- Journal of Digital Forensics, Security and Law
- Journal of Information System Security
- Journal of Information Systems
- Journal of Information Systems and Technology Management
- Journal of Mass Spectrometry
- Journal of Mobile, Embedded and Distributed System

- Journal of Physics
- Journal of Theoretical and Applied Information Technology
- Manager Journal
- Managerial Auditing Journal
- Moderní věda
- Nigeria Journal of Education, Health and Technology Reserch
- Network Security
- New Trends in Information Technologies. ITHEA, Sofia
- Security Audit
- The EDP Audit, Control, and Security Newsletter
- The Research Bulletin of Jordan ACM
- Trends and management

| 영문 학술대회 논문지 (알파벳 순)

- Canadian Conference on Electrical and Computer Engineering 2004
- Computational Methods in Systems and Software
- International Conference on Cloud Computing and Security
- International Conference on Information Theory and Applications
- The International Conference on Cyber Security Intelligence and Analytics
- Security and Protection of Information 2005
- 4th WSEAS International Conference on E-Activities
- 5th World Multiconference on Circuits, Systems, Communications and Computers
- 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems
- 6th International Conference on Engineering & MIS 2020
- 6th International Conference on Knowledge Management: Projects, Systems and Technologies
- 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce
- 2013 International Conference on Control Engineering and Communication Technology
- 2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS)
- 2015 IEEE 2nd international conference on cybernetics
- 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies
- 2020 International Conference on Communications, Information System and Computer Engineering
- 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies
- 2021 3rd International Cyber Resilience Conference