The Journal of the Convergence on Culture Technology (JCCT)
Vol. 10, No. 3, pp.279-288, May 31, 2024. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2024.10.3.279

JCCT 2024-5-33

국내기업 대상 SBOM (Software Bill Of Materials) 도입에 관한 연구 : 경영층의 지원과 제도적 지원의 조절 효과를 중심으로

Study on SBOM(Software Bill Of Materials) adoption in domestic companies :Focusing on the moderating effect of management support and institutional support

유한민*, 이신복**

Ryu Han Min*, Lee Sin-Bok**

요 약 ICT의 발달과 함께 기업에서는 정보교환 또는 운영관리를 위해 소프트웨어를 필수적으로 사용하게 되었다. 그러나 ICT의 발달과 함께 증가한 보안 및 소프트웨어 관리이슈는 지속해서 해결해나가야 할 문제이다. 2021년 미국에서는 이러한 소프트웨어 보안 대응책 중 하나로 SBOM을 정부주도하에 표준화 및 제도를 수립하였다. 본 연구는 이러한 SBOM이 국내에 도입되기 위한 초석을 마련하는 연구로서 시작되었다. SBOM의 대표적인 특징들이 도입 의도에 미치는 영향을 바탕으로 경영층 지원과 제도적 지원을 조절 변수로 검증하였다. 그 결과, 경영층 지원으로는 보안관리가 유의미한 조절 변수로 나타났으며, 정부의 제도적 지원에서는 투명성이 유의미한 조절 변수로 나타났다. SBOM을 도입하기 위해서는 기업과 정부의 노력이 함께 이루어져야 하는데, 각 관점에서 중요하게 여기는 변수가 다르다는 것을 검증한 것이다. 본 연구가 SBOM의 발전과 도입에 기여하길 바라는 바이다.

주요어 : Software Bill Of Materials, 소프트웨어, 경영층 지원, 제도적 지원

Abstract With the development of ICT, the use of software has become essential for organizations to exchange information or manage operations. However, security and software management issues that have increased with the development of ICT are issues that need to be continuously addressed. In 2021, the U.S. government has standardized and established SBOM as one of the countermeasures for software security. This research was initiated as a study to lay the groundwork for the introduction of SBOM in Korea. Based on the effects of SBOM characteristics on adoption intention, we tested management support and institutional support as moderating variables. As a result, security management was found to be a significant moderating variable for management support, and transparency was found to be a significant moderating variable for government institutional support. This study verified that SBOM adoption requires both corporate and government efforts, and the variables that are important from each perspective are different. We hope that this study will contribute to the development and adoption of SBOM.

Key words : Software Bill Of Materials, Software, Top Management Support, Institutional Support

*정회원, 한양대학교 대학원 경영학과 박사과정 (제1저자)
**정회원, 나사렛대학교 경영학과 조교수 (교신저자)
접수일: 2024년 3월 4일, 수정완료일: 2024년 4월 10일
게재확정일: 2024년 4월 20일

Received: March 4, 2024 / Revised: April 10, 2024
Accepted: April 20, 2024
*Corresponding Author: sblee@kornu.ac.kr
Dept. of Assistant Professor, Business Administration, Nazarene University, Korea

Ⅰ. 서 론

4차산업 기술로 비약적인 발전을 해온 ICT의 경우 이제는 ICT 소프트웨어를 사용하지 않는 기업을 볼 수 없을 정도가 되었다[1]. 특히나 4차산업의 발전을 비롯한 비약적인 ICT의 발전은 기업의 경영 및 운영관리를 위한 소프트웨어가 필수요소로 자리한 지 오래다[2]. 이러한 배경에 디지털상의 정보가 쉽게 공유되는 상황에서 기업에서는 자사의 자산과 기밀을 지키기 위해 보안에 큰 노력과 자본을 투자하고 있는 현실이다. 과학기술정보통신부와 한국정보보호산업협회(KISIA)에서 발표한 2023년 국내 정보보호산업 실태조사 보고서에 따르면 2022년 정보보호 시장규모는 전년도보다 16.7% 상승한 16조 원이 넘는 것으로 나타났다.

보안 시장규모의 이유를 보여주듯 2021년 국가사이버보안센터에서는 대대적인 보안패치 권고를 주도해서 나선 사건이 나타났다. 이는 2021년 발견된 Apache 'Log4j' 보안이슈 때문이었다[3]. Apache 'Log4j'는 관련 프로그램의 정보유출을 포함하여 사이버 공격의 피해까지 가능한 것으로 나타났다. 또한, Apache 'Log4j'라는 라이브러리는 대부분의 자바(JAVA) 웹프로그래밍 서버에서 사용되는 것으로 대표적인 사용처로는 애플의 주요 소프트웨어나 트위치를 포함하고 있다. 이러한 자바 웹프로그래밍 언어는 1995년 발표된 이래 대부분의 많은 프로그램이 사용한 프로그래밍 언어이기에 국내의 많은 소프트웨어에서도 사용하고 있어 큰 위협으로 다가온 사건이었다. 그 외에도 '랜섬웨어', 'DDoS' 등 다양한 바이러스와 해킹 프로그램들이 문제가 되었고, 2022년 조사에 따르면 ICT를 활용하는 기업이나 조직의 80% 이상이 랜섬웨어 피해를 봤다고 대답하였다[4]. 이뿐만이 아니라 2021년엔 애플의 하드웨어 공급업체 중 하나인 대만의 Quanta를 통해 애플의 기밀정보가 해킹된 사건도 발생 되었다[4][5].

소프트웨어의 문제는 비단 보안의 문제만 있는 것이 아니다. 조사에 따르면 2001년에도 프로그램 1대당 평균 35개 정도의 결함이 있으며, 연간 1,000억 라인의 결함을 보유한 채로 프로그램이 공개된다고 한다[4][6]. 이러한 문제를 방지하고자 2021년 미국에서는 정부주도하에 소프트웨어 보안 및 관리를 위한 대응책 중 하나로 SBOM(Software Bill Of Materials)이라는 방안을 내놓았다[4]. SBOM은 이름 그대로 소프트웨어의 자재명세서로 소프트웨어 내 필요한 부분마다 태그를 삽입하고 그 태그를 목록화하여 구조를 파악할 수 있게 하는 목록서라고 볼 수 있다[7][8]. 이 SBOM을 통해 소프트웨어의 구조를 투명하게 파악하여 보안 취약점이나 타 오픈소스 또는 라이브러리와 관계를 관리하고자 한 것이다. 예를 들어 SBOM이 있다면 Apache 'Log4j' 사건에서 피해 소프트웨어를 신속하게 파악하고 대응할 수 있었을 것이다.

본 연구는 국내기업에서도 많은 소프트웨어를 사용하는 만큼 보안과 관리를 위해 SBOM의 도입이 필요하다고 보고 이에 관한 연구를 진행하고자 한다.

Ⅱ. 이론적 배경

1. SBOM(Software Bill Of Materials)

SBOM(Software Bill Of Materials)은 제품의 자재명세서(BOM)에서 유래하여 소프트웨어 내 코드의 구성요소에 태그를 추가하고 태그를 '목록'으로 나타내어 소프트웨어의 구성 코드를 파악하는 방안이다[7][8]. SBOM이라는 명칭으로 소프트웨어에 자재명세서라는 개념을 도입한 것은 1990년대 후반부터 이다[9][10]. SBOM의 연구가 떠오른 이유는 하나의 소프트웨어를 개발할 때에도 무수히 많은 여러 코드와 타사의 오픈소스가 사용되기 때문이다[4][11]. 또한, 개발자마다 각자의 방식으로 개발을 진행하여 소프트웨어의 구조가 전부 다른 형태로 나오기 마련이다. 그리고 그 소프트웨어의 구조는 보통 수천억 라인의 코드로 구성되어 있다.

이러한 배경에서 미국에서는 SBOM을 보안이슈에 대응하는 하나의 방안으로 바라보고 2021년 발표한 The President's Executive Order (EO) 14028 (Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order)을 통해 정부의 모든 ICT 제품 조달 시 SBOM을 직접 제공하거나 공개 웹 사이트에 게시하여야 한다고 하였다[4]. 또한, 미국 정부는 SBOM의 표준화를 위해 2021년에 NTIA(National Telecommunications and Information Administration)를 통해 최소 요건을 지정하게 하였으며 Arora의 연구(2022)에서 이를 [그림1]과 같이 표로 제시하였다[11]. 그리고 SBOM을 Executive order (EO)는 SBOM을 소프트웨어 구축에 사용되는

그림 1. SBoM 요소의 가이드라인 리스트 (NTIA2021)
Figure 1. List of baseline SBoM Elements (NTIA 2021)

SBoM Element	Description
Author Name	Author of the SBoM entry
Supplier Name	Name or identity of supplier of the component in the SBoM entry
Component Name	One or more component name(s). May include the capability in case of multiple names or aliases
Version String	Version information which aids in identifying a component
Component Hash	Cryptographic hash of the component to uniquely and precisely identify a binary
Unique Identifier	A unique identifier of the component
Relationship	Relationship is inherent in the design of the SBoM. This could be *includes* (downstream) or *included in* (upstream). A *downstream* component is the one towards the consumer whereas an *upstream* component is towards the supplier.
Relationship Assertions	Refers to a component representing its immediate upstream relationships. Four categories cover these assertions— ▪ *Unknown*: This implies that immediate upstream (towards the supplier) components are not currently known and therefore not yet recorded. ▪ *Root*: This indicates that there are no immediate upstream relationships. ▪ *Partial*: There is at least one immediate upstream relationship and others may or may not be known. Known relationships are documented. ▪ *Known*: The entire set of immediate upstream relationships are known and documented.

출처: Arora, Wright, and Garman, Strengthening the Security of Operational Technology: Understanding Contemporary Bill of Materials (2022)

다양한 구성요소의 세부 정보 및 공급망 관계를 포함하는 공식 기록이라고 정의하였다[12]. 이러한 SBOM의 가장 큰 특징으로 세 가지를 꼽을 수 있는데 그 특징은 '투명성', '보안관리', '종속성'을 말한다.

먼저 투명성(Transparency)은 SBOM을 통해 소프트웨어의 구성요소를 투명하고 정확하게 파악 가능하다는 특징을 말한다[4][13]. 투명성을 통해 복잡한 소프트웨어 구조를 파악하고 잘못된 부분이나 개선이 필요한 부분을 쉽게 파악할 수 있다는 것이다.

두 번째로 보안관리(Security management)는 SBOM의 통해 소프트웨어 구조를 확인할 수 있으며, 이를 통해 보안 취약성 여부를 확인하고 관리할 수 있는 특징을 말한다[7]. SBOM의 보안관리 측면이 정부에서도 보안이슈 대응 방안으로 SBOM을 언급한 이유이기도 하다.

마지막으로 종속성(Dependency)은 SBOM의 내용으로 구성요소 간 하위 구성요소 또는 상위 구성요소를 파악할 수 있고, 오픈소스를 활용하더라도 그 출처와 소프트웨어 간의 관계를 파악할 수 있게 해주는 SBOM의 큰 특징이다[4][11][13]. 종속성이라는 특징으로 소프트웨어가 라이센스 규정의무를 지키는지, 문제가 발생시에 어디까지 영향을 미치는지를 파악하고 보증할 수 있게 된다[11].

미국에서는 2022년 정부의 주도하에 표준화 및 도입이 시작된 SBOM이 새로운 보안 대응의 하나로 떠오르고 있지만, 국내에서는 아직 그 시작이 미약하다. 특히나 여러 기업에서 사용하는 다양한 소프트웨어의 구조를 표준화된 기준을 가지고 파악하고 보안에 대응하려면 정부 차원의 지원은 물론 기업 차원에서도 투자와 관리가 필요하다. 이는 한 기업의 노력으로 도입이 어려운 방안이기에 보안에 대한 투자가 더욱 열악한 중소기업에는 더 먼 길이 될 수 있다. 따라서 본 연구에서는 SBOM의 특징을 가지고 자사의 소프트웨어 보안을 위해 기업에서 도입 할 의도를 가졌는지 살펴보고 SBOM의 도입을 위해 요구되는 정부의 제도적 지원과 경영층의 지원에 따라 그 영향이 달라지는지 보고자 한다.

2. 제도적 지원과 경영층 지원

기업이라는 조직에서 전반적인 정책이나 혁신을 시도하기 위해서는 경영층 지원, 조직구조, 적절한 보상이 필요하다고 한다[14], 조직의 혁신과 변화를 연구한 연구에서도 가장 중요한 영향을 주는 요인으로 경영층 지원, 직무 자율성, 지원적 조직, 시간적 여유, 보상을 제시하였다[15][16]. 그중 많은 연구자가 활동을 촉진하고 지원하며, 활성화 및 강화하기 위한 가장 중요한 요인으로 꼽는 부분은 경영층 지원이다[14][15][16][17][18]. 이에 본 연구에서는 SBOM을 새로 도입하고 활성화하여 실질적인 활용을 나타나게 하는 요인으로 경영층 지원을 바라보았다. 따라서 본 연구는 경영층 지원에 따라 기업이 SBOM 도입 의도가 달라지는지를 검토하여 경영층 지원에 대한 영향도를 살펴보고자 한다.

그러나 SBOM은 한 기업만의 노력으로 반영될 수 있는 것은 아니다. 여러 기업이 보유한 소프트웨어들의 종속성 및 보안관리와 투명성을 확보하기 위해서는 표준화된 기준이 필요하다. 이에 미국에서는 정부의 주도하에 NTIA에서 표준화된 초기 기준을 제시한 후 시행되었다[11]. 국내에서도 정부산하의 국가사이버보안센터, 한국인터넷진흥원(KISA) 등에서는 산업보안과 사이버 보안을 위해 보안 규정을 규정하며, 보안 인력을 양성하고 기업을 지원하는 활동을 하고 있다[3]. 또한, 정부는 기업의 기술에 대한 중요성을 인식하고 다양하고 많은 혁신 지원 방안 및 정책을 마련하고 있다[19].

2021년 발생한 대대적인 보안이슈 Apache 'Log4j' 사건에서도 보안 패치를 배포하기도 하였으며[3], 과학기술정보통신부(Ministry of Science and ICT) 정보보호 및 정보통신기술에 관한 법령을 관리하기도 한다. 따라서 국내에서도 미국의 정부주도하에 SBOM이 시행된 것처럼 정부의 지원과 노력이 필요하다. 이에 본 연구에서는 제도적 지원을 SBOM을 활성화하기 위한 정부의 지원으로 바라보고 이에 따른 SBOM의 도입 의도를 살펴보고자 한다.

III. 연구 방법

1. 표본설계와 측정 도구

본 연구는 기업 내 소프트웨어에 대한 보안 대응 방안 중 하나로 미국에서는 2021년부터 정부의 주도하에 시행되고 있지만, 국내에는 도입되지 않는 SBOM에 대하여 도입을 확산하고자 시작되었다. 따라서 조사 대상을 기업 내 시스템담당자를 대상으로 하였다. 다만 업무 숙련도와 이해를 위해 해당 직종의 최소 5년 이상의 경력자로 구성하였다. 또한, 국내에 아직 SBOM이 제대로 도입되지 않은 점을 고려하여 조사를 시작하기 전에 SBOM에 대한 설명을 덧붙여서 이해를 높였다. 본 연구는 시스템담당자에게 설문으로 진행되었으며 7점 리커드 척도로 측정하였다. 총 540개의 데이터를 수집하였으나, 결측값, 불성실 응답을 제외한 524개의 데이터가 연구에 활용되었다.

각 변수의 측정은 선행연구를 바탕으로 설문 형태의 질문으로 변형하였다. 각 측정 문항은 [Table 1]과 같다. 먼저 SBOM의 특징인 투명성은 SBOM을 통해서 소프트웨어의 구성요소와 정보를 투명하게 파악할 수 있는 정도를 기준으로 측정하였다[7][20][21]. 두 번째 SBOM의 특징인 보안관리는 SBOM을 통해 소프트웨어의 보안 취약성 여부를 파악하고 관리할 수 있는 정도를 측정하였다[7][20][21]. 마지막 SBOM의 특징인 종속성은 SBOM을 통해 소프트웨어의 출처와 종속 관계를 파악할 수 있으며, 관련된 업데이트나 관리 규정을 관리할 수 있는 정도로 측정하였다[7][20][21].

SBOM의 특징이 도입 의도에 미치는 영향을 조절할 것으로 예측한 경영층 지원은 경영층이 얼마나 SBOM 도입에 대한 의지와 필요성을 가졌는지를 살펴보았다[22][23][24][25]. 이에 대한 측정 도구는 빅데이터 도입에 대한 경영층의 의지를 조절 변수로 사용한 이선우와

표 1. 측정항목
Table 1. list of measurement

변수	측정 항목
투명성	SBOM으로 소프트웨어에 포함된 구성요소(오픈소스, 라이브러리 등)의 목록을 식별할 수 있다.
	SBOM은 소프트웨어 구성요소의 기본정보(이름, 고유번호, 업데이트 일시, 버전 등)를 확인할 수 있다.
	SBOM을 통해 소프트웨어 구성요소를 쉽게 관리할 수 있다.
	SBOM을 통해 소프트웨어 구성요소에서 원하는 부분을 쉽게 찾을 수 있다.
보안 관리	SBOM은 소프트웨어 생산 및 구매 시 알려진 보안에 취약한 구성요소를 회피할 수 있게 한다.
	SBOM은 소프트웨어 보안관리를 쉽게 할 수 있게 한다.
	SBOM은 소프트웨어 구성요소에서 보안에 문제가 되는 위치를 신속하게 파악할 수 있게 한다.
	SBOM은 소프트웨어 구성요소에 대한 보안 조치를 신속하게 취할 수 있게 한다.
종속성	SBOM은 소프트웨어 구성요소의 공급업체 정보를 알 수 있게 한다.
	SBOM은 여러 소프트웨어의 구성요소 간의 관계를 알 수 있게 한다.
	SBOM은 활용된 다른 오픈소스 또는 라이브러리의 업데이트나 서비스 종료를 식별하여 대비할 수 있게 한다.
	SBOM은 소프트웨어 구성요소와 관련된 규정 요구사항을 쉽게 식별하여 준수할 수 있게 한다.
경영층 지원	우리 기업의 경영층은 SBOM을 이해한다.
	우리 기업의 경영층은 SBOM을 긍정적으로 검토한다.
	우리 기업의 경영층은 SBOM의 필요성을 느끼고 있다.
	우리 기업의 경영층은 SBOM을 지원하고자 하는 의지를 가지고 있다.
제도적 지원	SBOM의 도입과 확산을 위한 국가 차원의 예산과 인력이 지원되어야 한다.
	기업이 SBOM 도입을 위한 세금우대 정책이나 정부보조금 지원이 있어야 한다.
	정부가 공공부문에 SBOM이 생성된 소프트웨어 제품의 사용을 적극적으로 권장해야 한다.
	SBOM 도입과 확산을 지원하는 법·제도가 마련되어야 한다.
	SBOM을 도입할 수 있는 인프라(국내표준, 국가의 인증 및 관리 등)가 충분히 지원되어야 한다.
도입 의도	SBOM 도입을 추천할 의향이 있다.
	SBOM을 도입할 것으로 예측할 수 있다.
	SBOM을 도입하여 사용할 의사가 있다.
	SBOM을 도입하여 사용법을 학습할 계획이 있다.

이희상(2014)의 연구[23]를 반영하여 SBOM에 맞게 조정하였다. 또 다른 조절 변수인 제도적 지원은 SBOM을 도입하기 위한 정부의 제도적 규정이나 지원의 필요성을 말한다[19][26][27][28][29]. 선행연구에서는 제도적 지원 부분을 자금지원, 세제지원, 판로지원, 인력지원, 정보지원으로 분류하기도 하였다[19]. 미국은 제도적으로 규정하고 사용을 권장하였다[11]. 이러한 부분들을 종합하여 본 연구는 선행연구들의 문항을 기반으로 제도적 지원에 SBOM을 반영하여 측정하였다.

마지막으로 본 연구의 종속변수로 SBOM을 도입하고 하는 의지가 어느 정도 인지 살펴보는 도입 의도를 측정하고자 하였다[29][30].

2. 분석방법

본 연구에서 활용된 변수의 요인은 선행연구의 이론을 바탕으로 질문형태로 변경하여 사용하였다. 따라서 문항이 요인으로서 구성이 되는지 살펴보기 위하여 탐색적 요인분석(Exploratory Factor Analysis)을 시행하였다. 이어서 변수 간 타당성을 확보하고자 상관관계 분석을 진행하였다. 변수의 인과관계를 확인하려는 방법으로는 구조방정식을 채택하였으며, 마지막으로 조절변수의 가설검증도 시행하였다. 본 연구에서 활용된 도구는 IBM의 SPSS 18.0과 Amos 18.0가 활용되었다.

3. 가설 설정

SBOM은 소프트웨어 개발에 사용되는 구성요소의 세부 정보 및 공급망 관계를 포함하는 공식 기록으로서 그 대표적인 특징으로 투명성, 보안관리, 종속성을 들 수 있다[4][7][11][13]. 이러한 SBOM을 미국에서는 정부주도하에 도입을 제도적으로 마련하고 권장하고 있다[4][11]. 그리고 SBOM의 특징이 가지는 장점이 기업에 정보보안에 긍정적 도움이 되기에 도입에 대한 부분도 긍정적으로 받아들일 것이다[4][11]. 이에 다음과 같이 가설을 수립하였다.

H1. 각 SBOM의 특징(투명성, 보안관리, 종속성)은 도입 의도에 긍정적인 영향을 미칠 것이다.

기업에서 혁신이나 새로운 기술의 도입 또는 새로운 프로세스의 도입을 하기 위해서는 여러 촉진요인이 필요하다. 그중 연구자들이 가장 중요한 요인으로 꼽는 것이 경영층 지원으로 경영층의 의지를 말한다[15][16][17][18][31]. 빅데이터와 같은 혁신적 기술을 도입할 때, 선행연구에서도 경영층의 의지를 조절 변수로 하여 새로운 혁신과 기술의 도입을 연구하였다[23]. 따라서 본 연구는 경영층 지원에 따라 도입 의도가 받는 영향이 달라질 것이라 여겨 다음과 같은 가설을 수립하였다.

H2. 경영층 지원은 각 SBOM의 특징(투명성, 보안관리, 종속성)이 도입 의도에 미치는 영향에 조절 효과가 있을 것이다.

SBOM은 한 기업의 노력으로 도입하기 어려운 특징들을 가지고 있다. 대표적으로 소프트웨어 간 종속성을 나타내는 것이나, 소프트웨어 구성요소를 표준화된 기준에 맞춰 목록을 작성하는 등이 있다. 이에 미국에서도 정부 주도로 표준화 작업이 이루어진 것을 확인할 수 있다[4]. 그리고 정부주도하에 제도적으로 규정하여 도입을 권장하고 있다[11]. 국내에서도 마찬가지로 정부는 기업의 기술과 혁신에 대한 지원을 위해 노력을 아끼지 않고 있다[19]. 이에 본 연구에서는 도입 의도가 정부의 제도적 지원에 따라 달라질 것으로 보고 다음과 같은 가설을 수립하였다.

H3. 제도적 지원은 각 SBOM의 특징(투명성, 보안관리, 종속성)이 도입 의도에 미치는 영향에 조절 효과가 있을 것이다.

Ⅳ. 분석 결과

1. 표본의 특성

조사된 대상의 인구통계학적 특징은 [표 2]와 같다. 성별은 남성이 403명, 여성이 121명으로 나타났으며, 직급은 선임급과 책임급이 84.2%로 대부분을 차지하였다. 대부분은 대졸자로 78.6%를 차지하였으며, 경력으로는 5년 이상부터 25년 미만에 고르게 분포되어 있었다.

표 2. 인구 통계
Table 2. Demographics of the Survey Respondents

N: 524		N	%	N: 524		N	%
성별	남성	403	76.9	직급	사원	32	6.1
	여성	121	23.1		선임	263	50.2
나이	30~39세	196	37.4		책임	178	34.0
	40~49세	181	34.5		임원	51	9.7
	50~59세	101	19.3	경력	5~10년	103	19.7
	60세 이상	46	8.8		11~15년	142	27.1
학력	고졸	43	8.2		16~20년	133	25.4
	대졸	412	78.6		21~25년	104	19.8
	대학원졸	61	11.6		26~30년	40	7.6
	기타	8	1.5		31년 이상	2	0.4

2. 측정 항목의 신뢰성과 타당성

본 연구에서 활용된 변수의 질문들이 선행연구를 바탕으로 하였지만, 연구에 맞춰 내용 수정 및 변경이 있

표 3. 측정 항목의 신뢰성과 타당성
Table 3. Reliability and validity of measurement items

구분		요인 적재량						Cronbach's α	C.R	AVE
투명성	1	.818	.142	.173	.109	.242	.209	.937	.937	.788
	2	.817	.155	.162	.169	.263	.137			
	3	.808	.216	.237	.125	.232	.156			
	4	.801	.198	.221	.161	.269	.175			
보안관리	1	.179	.836	.197	.218	.172	.125	.932	.933	.777
	2	.152	.822	.239	.240	.177	.077			
	3	.152	.808	.237	.194	.177	.150			
	4	.221	.765	.225	.243	.183	.149			
종속성	1	.189	.243	.827	.180	.185	.081	.924	.924	.753
	2	.208	.179	.790	.142	.223	.164			
	3	.200	.242	.785	.172	.251	.145			
	4	.183	.239	.780	.156	.186	.178			
경영층지원	1	.141	.257	.149	.792	.222	.166	.913	.914	.726
	2	.137	.222	.191	.788	.214	.192			
	3	.160	.264	.128	.783	.237	.181			
	4	.137	.188	.216	.710	.281	.273			
제도적지원	1	.262	.187	.198	.231	.791	.203	.938	.926	.758
	2	.202	.223	.187	.154	.776	.196			
	3	.217	.117	.259	.221	.759	.160			
	4	.271	.177	.196	.223	.750	.187			
	5	.296	.175	.190	.318	.721	.191			
도입의도	1	.140	.129	.128	.180	.153	.861	.925	.938	.752
	2	.138	.092	.137	.163	.196	.849			
	3	.160	.119	.120	.122	.153	.847			
	4	.145	.098	.108	.189	.160	.824			
총계		3.395	3.378	3.296	3.141	3.789	3.477			
분산의 %		13.581	13.514	13.184	12.564	15.154	13.906			
Kaiser-Meyer-Olkin: .946, Bartlett: 12,156.375***, χ2: 567.347***, CMIN/DF: 2.182, RMR: 0.033, GFI: 0.921, AGFI: 0.901, NFI: 0.954, RFI: 0.947, IFI: 0.975, TLI: 0.971, CFI: 0.975, RMSEA: 0.048										

*p<=0.05, **p<=0.01, ***p<=0.001.

었기에 선행연구를 따르며 타당성을 검증하는 확인적 요인분석(Confirmatory Factor Analysis)보다는 구성요소의 집중 타당성을 볼 수 있는 탐색적 요인분석(Exploratory Factor Analysis)으로 진행하였다. [표 3]의 결과에서처럼 요인 적재량이 0.7을 넘으며, 다른 변수와 차이가 나타남으로 타당성을 확인할 수 있었다. 마찬가지로 변수 간의 상관관계가 다른 변수에 의해 얼마나 잘 설명되는지를 KMO(Kaiser-Meyer-Olkin)를 통해 확인하였는데 0.9 이상으로 아주 높은 적정값을 나타내었다. 탐색적 요인분석은 Bartlett 검정값의 유의성으로 모형 적합성을 판단하는데 이 부분 또한 0.001 미만의 값으로 나타났다.

또한, 함께 제시한 Cronbach's α 값은 내적 일관성인 신뢰성을 확보하는 수치로 0.7 이상을 기준으로 한다[32]. 본 검증 결과 모두 0.9 이상의 높은 수치로 신뢰성을 확인할 수 있었다.

그러나 요인설정의 타당성을 높이고자 모델 적합성 부분은 확인적 요인분석의 AMOS를 활용하여 추가 분석을 진행하였다. 요인의 모형 적합도 결과는 χ2값 567.347로 p<=0.001로 나타났으며, CMIN/DF 값이 2.182로 수용 가능 영역인 3 미만으로 나타났다. Root Mean-Square Residual인 RMR은 0.05 이하까지 보는데, 본 결과는 0.33로 적합하게 나타났다. Root Mean Square Error of Approximation인 RMSEA는 기준인 0.8 이하인 0.048로 적합함으로 나타났다. 이 외에도 모델 적합도를 검증하는 GFI(goodness of fit index) 0.921, NFI(normed fit index) 0.954, RFI(Relative fit index) 0.947, IFI(Incremental fit index) 0.975, TLI(Turker-Lewis index) 0.971, CFI(comparative fit index) 0.975로 모두 기준치인 0.9를 넘었으며 아주 높은 수치로 요인의 모델 적합성을 검증하였다.

다음으로 진행한 상관관계 분석(Correlation analysis) 결과와 AVE와 비교한 결과를 [표 4]로 제시하였다. 변수에 대한 판별 타당성은 각 변수에 대한 AVE를 상관계수의 제곱근과 비교하여 평가한다[33][34]. 상관계수 제곱근의 결과가 모두 1을 포함하지 않으며, AVE 결과도 상관계수 값을 초과하므로 타당성을 확보하였다.

표 4. 구성개념의 상관관계, 평균, 표준편차
Table 4. Correlations among Constructs

구분	요인 간 상관계수					
	1	2	3	4	5	6
투명화	(0.788)					
보안관리	.513	(.777)				
종속성	.551	.591	(.753)			
경영층지원	.484	.605	.523	(.726)		
제도적지원	.646	.542	.590	.636	(.758)	
도입의도	.446	.381	.408	.501	.498	(.752)
평균	4.974	4.228	5.013	6.222	5.085	5.343
표준편차	1.132	1.096	1.082	0.849	1.046	1.024

(): AVE 값

3. 측정모형의 적합도 검증

본 연구의 가설을 검증하기 위해 분석 도구로 AMOS를 활용하였으며, 구조방정식으로 인과관계를 분석하였다. 먼저 구조방정식 모형의 적합도를 살펴본 결과를 [표 5] 하단에 제시하였다. 모형 적합도 결과는 χ2 값 197.721로 p<=0.001로 나타났으며, CMIN/DF값이 2.018로 수용 가능 영역인 3 미만으로 나타났다. RMR

은 0.05 이하까지 수용으로, 결과값 0.34로 적합하게 나타났다. RMSEA는 0.044로 기준치인 0.8 이하로 적합함으로 나타났다. 다른 모형의 적합도를 검증하는 수치들인 GFI는 0.955로, NFI는 0.974로, RFI는 0.968로, IFI는 0.987로, TLI는 0.984로, CFI는 0.987로 나타나 모두 기준치인 0.9를 넘어 모델 적합성을 검증하였다.

표 5. 가설검증 결과
Table 5. Result of Research Model

가설		Estimate	S.E.	C.R.	P	결과
1.1	투명화 → 도입의도	0.270	0.05	5.448	***	채택
1.2	보안관리 → 도입의도	0.120	0.053	2.276	0.023	채택
1.3	종속성 → 도입의도	0.153	0.054	2.824	0.005	채택
χ2: 197.721***, CMIN/DF: 2.018, RMR: 0.034, GFI: 0.955, AGFI: 0.938, NFI: 0.974, RFI: 0.968, IFI: 0.987, TLI: 0.984, CFI: 0.987, RMSEA: 0.044						

*p<=0.05, **p<=0.01, ***p<=0.001.

4. 연구가설 검증 결과

먼저 본 연구의 가설1에 대한 검증을 위해 구조방정식으로 본 분석 결과를 [표 5]와 같이 제시하였다. 가설1은 SBOM의 특징인 투명성, 보안관리, 종속성이 도입의도에 미치는 영향을 본 결과이다. 투명성은 0.270(P<0.001)로, 보안관리는 0.120(P<0.05)로, 종속성은 0.153(P<0.01)로 나타나 모두 채택되었다. SBOM의 각 특징은 SBOM의 도입 의도에 긍정적인 영향을 미칠 만큼 모두 중요한 변수들로 나타난 것이다.

표 6. 조절효과 검증 결과
Table 6. Results of Moderating Effect Analysis

가설. 2		종속변수: 도입 의도					
		1단계		2단계		3단계	
독립	투명화(1)	.281	***	.223	***	.223	***
	보안관리(2)	.134	.007	-.003	.960	-.033	.514
	종속성(3)	.174	.001	.110	.025	.111	.023
조절	경영층지원(4)			.336	***	.457	***
상호작용	(1)*(4)					.023	.658
	(2)*(4)					.188	.001
	(3)*(4)					-.015	.785
$R^2(\Delta R^2)$		0.247		0.312(0.065)		0.338(0.026)	
F(ΔF)		56.895***		58.812***(48.854)		37.641***(6.789)	
가설. 3		종속변수: 도입 의도					
		1단계		2단계		3단계	
독립	투명화(1)	.281	***	.162	.002	.192	***
	보안관리(2)	.134	.007	.082	.094	.072	.138
	종속성(3)	.174	.001	.099	.054	.085	.105
조절	제도적지원(5)			.291	***	.329	***
상호작용	(1)*(5)					.125	.035
	(2)*(5)					.071	.193
	(3)*(5)					-.070	.232
$R^2(\Delta R^2)$		0.247		0.288(0.041)		0.304(0.016)	
F(ΔF)		56.895***		52.53***(29.937)		32.198**(3.91)	

*p<=0.05, **p<=0.01, ***p<=0.001.

가설2와 가설3은 앞서 가설1에서 증명된 SBOM 도입에 긍정적 영향을 미치는 SBOM 특징들이 각 경영층 지원과 제도적 지원이라는 조절 변수에 따라 그 영향이 달라지는 본 결과이다.

[표 6]에서 제시된 가설2의 결과를 보면 경영층 지원을 조절 변수로 하였을 때 투명화(P=0.658)와 종속성(P=0.735)은 기각되었지만, 보안관리(P=0.001)는 유의한 결과로 나타났다. 경영층에 시점에서 소프트웨어의 구조나 업데이트 및 관리보다는 보안의 측면을 중요시하고 SBOM을 고려한다는 것을 알 수 있는 결과이다.

가설3의 결과를 보면 제도적 지원을 조절 변수로 하였을 때 보안관리(P=0.193)와 종속성(P=0.232)은 기각되었지만, 투명화(P=0.035)는 유의한 결과로 나타났다. 이 결과로 정부의 제도적 지원 필요성에는 소프트웨어의 보안관리와 종속적 관계 파악보다는 투명한 관리에 더 초점을 맞추고 있다는 것을 알 수 있었다.

V. 결 론

ICT의 발달과 함께 대부분 기업에서는 정보공유를 위해 경영 및 운영과 관리 소프트웨어를 사용하고 있다. 그러나 이러한 소프트웨어는 구조적으로 많은 라이브러리 또는 오픈소스 등 복잡하게 구성되어 변형이나 관리 또는 보안에 취약하기도 하다. 이에 미국에서는 보안에 대한 새로운 대응으로 SBOM의 표준화 및 도입에 노력을 시작하였다. 따라서 본 연구는 국내에서도 SBOM의 도입에 관한 연구로 시작되었다.

먼저 본 연구의 결과로 SBOM이 가지는 특징이 도입 의도에 미치는 결과에서 모두 채택되었다. 기업의 관점에서도 SBOM의 필요성을 증명한 것이라 하겠다. 그러나 SBOM을 새로 도입하기 위해서는 경영층의 의지와 지원이 필요하다. 그리고 SBOM이 여러 시스템 간 종속 관계를 나타내며, 표준화된 목록으로 여러 시스템이 일관된 명칭과 관리가 필요하기에 정부의 제도적 지원이 필요한 방안이다. 따라서 SBOM의 필요성을 증명한 1차 연구 결과를 바탕으로 경영층 지원과 제도적 지원을 조절 변수로 추가 분석을 진행하였다.

두 번째로 SBOM의 특징이 도입 의도에 미치는 영향에서 경영층의 지원은 보안관리에서만 유의미한 결과를 나타내었다. 이는 경영자라는 관점에서 기업의 자산인 정보를 보호하기 위한 보안관리 측면에서 SBOM

의 가치를 바라본다는 것을 나타낸 결과이다. 투명성과 종속성이 기각된 사유로는 SBOM의 투명한 구조파악과 업데이트 및 관리를 위한 종속성은 실무자들에게 중요한 요인이 될 수 있겠지만, 경영자의 측면에서 유의미하게 나타나지 않다는 결과이다. 따라서 경영자와 실무자가 바라보는 SBOM의 가치가 다르기에 도입을 위한 설득에서도 다른 관점으로 접근해야 한다는 것을 알 수 있다.

세 번째로 제도적 지원의 필요성에 대한 변수로 본 조절 효과는 투명화가 유의미한 결과로 채택되었다. 정부의 관점으로는 기업들이 사용하는 소프트웨어의 표준화 및 제도적 지원을 통해 소프트웨어들을 투명하게 관리하는 것이 무엇보다 중요하기에 나타난 결과로 보인다. 보안관리도 유의성이 높지 않은 값(P=0.193)으로 나타났지만, 통계적으로 기각되었다. 이는 보안관리 측면으로도 고려가 될 수 있지만 투명한 관리가 더 중요한 것임을 나타낸 것이다. 종속성의 이점이 기업 내 관리 측면에서 가지는 이점으로 정부의 관리에는 큰 의미가 있다고 보기 어렵기 때문으로 종속성이 도입 의도에 미치는 영향에서 제도적 지원의 조절 효과가 기각된 것으로 보인다. 따라서 표준화 및 투명한 관리를 위해 정부는 제도적 지원 필요성을 가지고 앞장서야 할 것이다.

본 연구는 실무적인 관점에서 소프트웨어의 보안을 강화하고 관리를 더 용이하게 하는 대응책으로 새로이 제시되고 있는 SBOM의 도입을 연구했다는 측면에서 그 시사점을 가진다. 특히나 SBOM은 최근 미국에서도 정보 주도하에 시행해온 만큼 효과를 기대할 방안이라고 볼 수 있다. 또한, 기업의 소프트웨어 구조는 글로벌 오픈소스와 라이브러리 등이 활용되는 만큼 국내에서도 제대로 도입된다면 타 국가의 SBOM과 정보교환과 호환을 기대할 수 있을 것이다.

미국의 정보주도하에 시행된 SBOM이지만 국내에서는 그 연구를 발견하기 어렵다. SBOM이 소프트웨어의 보안과 관리 방안으로 제시된 지 오래지 않을뿐더러 기업 자체의 노력으로 시행될 수 없는 방안이다 보니 연구사례가 더 부족한 것이 사실이다. 이에 본 연구는 국내기업을 대상으로 한 SBOM 연구의 초석으로서 학문적 가치를 보유하고 있다.

그러나 연구의 한계점으로 아직 국내사례를 찾기 힘든 만큼 국내에서 SBOM의 효과성을 입증할 수 없다는 부분이다. 또한, 도입을 위해 기업의 경영층과 정부의 제도를 언급하였지만, 실질적인 도입에 더 많은 연구와 표준화 및 제도적 규범이 필요할 것이다.

향후 국내의 도입된 사례를 대상으로 연구가 이루어지거나 국내 SBOM의 표준화에 관한 연구가 이루어진다면 SBOM 도입을 더욱 앞당길 수 있는 연구가 될 것이다.

본 연구가 SBOM 도입을 위한 초석으로 기업의 발전에 기여할 것이라고 기대한다.

References

[1] J.M. Kim, S.S. Wee, N.I. Kim, and N.I. Kim, “A Study on Cyber Security Policy for S/W Supply Chain Security in Korea”, *The Journal of Society for e-Business Studies*, Vol. 28, No. 1, pp. 29-53, February 2023. DOI:10.7838/jsebs.2023.28.1.029

[2] Y.P. Rhee, “A Study on the Relationships among ICT Capability, Global Orientation and Export Marketing in Korean SMEs”, *Korea Trade Review*, Vol. 42, No. 2, pp. 251-276, April 2017

[3] National Cyber Security Center, *Security patch recommended for Apache 'Log4j' vulnerability*, Available from https://www.ncsc.go.kr:4018/main/PageLink.do (accessed February 10, 2024)

[4] S. Kumar, and R.R. Mallipeddi, “Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions”, *Production and Operations Management*, Vol. 31, No. 12, pp. 4488-4500, September 2022. DOI:10.1111/poms.13859

[5] L.H. Newman, *Apple's ransomware mess is the future of online extortion*, Available from https://www.wired.com/story/apple-mac-lockbit-ransomware-samples/ (accessed May 1, 2023)

[6] R. Anderson, *Why information security is hard - an economic perspective, Seventeenth Annual Computer Security Applications Conference, New Orleans, LA, USA*, pp. 358-365, December 2001. DOI:10.1109/ACSAC.2001.991552

[7] S. Carmody, A. Coravos, G. Fahs, G. Fahs, A. Hatch, J. Medina, B. Woods, and J. Corman, “Building resilient medical technology supply chains with a software bill of materials”, *npj Digital Medicine*, Vol. 4, No. 1, pp. 34, February 2021

[8] H.Y. Noh, and S.B. Lee, “The Effects of

information security perceptions of collaborative system managers on intention to use SBOM(Software Bill Of Materials) : Focusing on the Theory of Planned Behavior", *The International Promotion Agency of Culture Technology*, Vol. 9, No. 5, pp. 463-474, July 2023. DOI:10.17703/JCCT.2023.9.5.463

[9] R. Schmidt and T. Duffy, *Non-interfering software distribution, Paris: Data Systems in Aerospace-DASIA*, Vol. 97, No. 409, PP. 351 - 358, May 1997.

[10] P.M. Fangman, L.H. Gerhardstein and B.J. Homer, *Federal Emergency Management Information System (FEMIS): Bill of Materials (BOM) for FEMIS (version 1.4.5. No. PNL10689-Ver. 1.4.5), Richland*, WA: Pacific Northwest National Laboratory, June 1998. DOI:10.2172/663230

[11] A. Arora, V. Wright, and C. Garman, "Strengthening the Security of Operational Technology: Understanding Contemporary Bill of Materials", *JCIP The Journal of Critical Infrastructure Policy*, Vol. 3, No. 1, pp. 111, Spring/Summer 2022. DOI:10.18278/jcip.3.1.8

[12] Federal Register, *Improving the Nation's Cybersecurity A Presidential Document by the Executive Office of the President on 05/17/2021*, Available from https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity (accessed February 10, 2024)

[13] N. Zahan, E. Lin, M. Tamanna, and M. Tamanna, "Software Bills of Materials Are Required. Are We There Yet?", *IEEE Security & Privacy*, Vol. 21, No. 2, pp. 81-88, April 2023. DOI:10.1109/MSEC. 2023.3237100

[14] D.F. Kuratko, R. V. Montagno, and J.S. Hornsby, "Developing an Intrapreneurial Assessment Instrument for an Effective Corporate Entrepreneurial Environment", *Strategic Management Journal*, Vol. 11, No. Special Issue, pp. 49-58, Summer 1990

[15] J.S. Hornsby, D.F. Kuratko, and S.A. Zahra, "Middle managers' perception of the internal environment for corporate entrepreneurship: assessing a measurement scale", *Journal of Business Venturing*, Vol. 17, No. 3, pp. 253-273, May 2002. DOI:10.1016/S0883-9026(00)00059-8

[16] S.A. Zahra, H.J. Sapienza, and P. Davidsson, "Entrepreneurship and Dynamic Capabilities: A Review, Model and Research Agenda", *Journal of Management studies*, Vol. 43, No. 4, pp. 917-955, May 2006. DOI:10.1111/j.1467-6486.2006.00616.x

[17] I.C. Macmillan, Z. Block, and P.N. Narasimha, "Corporate venturing: alternatives, obstacles encountered, and experience effects", *Journal of Business Venturing*, Vol. 1, No. 2, pp. 177-191, April 1986. DOI:10.1016/0883-9026(86)90013-3

[18] J.A. Pearce II, T.R. Kramer, and D.K. Robbins, "Effects of managers' entrepreneurial behavior on subordinates", *Journal of Business Venturing*, Vol. 12, No. 2, pp. 147-160, June 1998. DOI:10.1016/S0883-9026(96)00066-3

[19] H.J. Yoon, A.R. Hong, and S.D. Jung, "The effects of R&Ds, technology innovation capability and the innovation support system of small- and medium-sized businesses on the company performance", *Innovation studies*, Vol. 13, No. 2, pp. 209-238, May 2018. DOI: 10.46251/INNOS.2018.05.13.2.209

[20] S.W. Kim, and K.H. Son , "SBOM trends for OSS traceability", Review of KIISC, Vol. 32, No. 5, pp. 53-66, October 2022

[21] Y.S. Choi, "U.S. software supply chain security policy trends: Focusing on the SBOM case", *Review of KIISC*, Vol. 32, No. 5, pp. 7-14, October 2022

[22] J.W. Lian, D.C. Yen, and Y.T. Wang, "An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital", *International Journal of Information Management*, Vol. 34, No. 1, pp. 28-36, November 2014. DOI:10.1016/j.ijinfomgt.2013.09.004

[23] S.W. Lee, and H.S. Lee, "A Study on an Integrative Model for Big Data System Adoption : Based on TOE, DOI and UTAUT", *Journal of Information Technology Applications and Management*, Vol. 21, No. 4_Special Issue, pp. 463-483, December 2014. DOI:10.21219/jitam.2014.21.4_spc.463

[24] D.H. Kim, S.D. Park, S.J. Kim, and S.J. Kim, "A Study on Establishment of Cyber Threat Information Sharing System Focusing on U.S. Case", *Convergence Security Journal*, Vol. 17, No. 2, pp. 53-68, June 2017

[25] D.J. Yoon, Y.S. Jee, Y.S. Lee, and Y.S. Lee, "A Study on the Low Meaning and Improvement of Personal Information ADR(Alternative Dispute Resolution)", *Journal of The Korea Society of Information Technology Policy & Management*, Vol. 12, No. 1, pp. 1567-1574, November 2020

[26] W.H. DeLone, and E.R. McLean, "Information systems success revisited", *Proceedings of the*

35th annual Hawaii international conference on system sciences, IEEE, pp. 2966-2976, August 2022. DOI:10.1109/HICSS.2002.994345

[27] G. Premkumar, and M. Roberts, "Adoption of new information technologies in rural small businesses", *Omega*, Vol. 27, No. 4, pp. 467-484, June 1999. DOI:10.1016/S0305-0483(98)00071-1

[28] K. Zhu, S. Dong, S.X. Xu, and S.X. Xu, "Innovation diffusion in global contexts: determinants of post-adoption digital transformation of European companies", *European journal of information systems*, Vol. 15, pp. 601-616, December 2006

[29] S.H. Jang, W.S. Lee, D.H. Jun, and D.H. Jun, "A Study on Cloud-based Non-identification Processing Data Provision Platform(Focusing on Agriculture Bigdata)", *Journal of The Korea Society of Information Technology Policy & Management*, Vol. 12, No. 4, pp. 1883-1892, June 2020

[30] J.R. Bettman, and C.W. Park, "Effects of prior knowledge and experience and phase of the choice process on consumer decision processes: A protocol analysis", *Journal of consumer research*, Vol. 7, No. 3, pp. 234-248, December 1980. DOI:10.1086/208812

[31] S.B. Choi, and S.D. Chang, "Middle-Level Managers' Perception of Corporate Entrepreneurship and Their Innovative Work Behaviors in SMEs", *Journal of Human Resource Management Research*, Vol. 20, No. 2, pp. 27-54, June 2013

[32] C.E. Lance, M.M. Butts, and L.C. Michels, "The sources of four commonly reported cutoff criteria: What did they really say?", *Organizational research methods*, Vol. 9, No. 2, pp. 202-220, April 2006. DOI:0.1177/1094428105284919

[33] J. Hulland, "Use of partial least squares (PLS) in strategic management research: A review of four recent studies", *Strategic management journal*, Vol. 20, No. 2, pp. 195-204, February 1999. DOI:10.1002/(SICI)1097-0266(199902)20:2<195::AID-SMJ13>3.0.CO;2-7

[34] C. Fornell, and D.F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error", *Journal of marketing research*, Vol. 18, No. 1, pp. 39-50, February 1981. DOI:10.1177/002224378101800104

[35] Y.M. Oh, H.Y. Noh, "A study on the adoption of smart work for ICT companies : Focusing on the innovation resistance model", The Journal of the Convergence on Culture Technology (JCCT), Vol. 9, No. 5, pp. 649-659, September 2023