제조산업 클라우드 보안위험 식별 연구

[1] 오정훈, [2] 이주노, [3*]장항배

A Study on the Identification of Cloud Security Risks in the Manufacturing Industry

[1]Junghun Oh, [2]Juno Lee and [3*]Hangbae Chang

요 약

제4차 산업혁명으로 촉발된 디지털 전환과 비대면 서비스의 증가라는 흐름 속에서 클라우드 컴퓨팅 서비스에 대한 수요가 가파르게 촉진되고 있다. 현재 클라우드는 공공, IT, 금융 등 다양한 산업 분야에 도입되고 있으며, 제조산업 역시 미래 지속가능성 확보를 위하여 클라우드를 도입, 스마트 제조를 통한 혁신을 추진하고 있다. 하지만 제조기업이 클라우드를 도입하는 데는 보안 우려사항으로 인한 제약이 존재하는 것으로 나타났다. 클라우드 보안위험을 확인한 기존 연구는 제조산업을 고려했다기 보다는 일반적인 클라우드 보안위험이나 기술적 보안위험을 중심으로 클라우드 보안위험을 제시한 한계가 있었다. 이에 본 연구는 제조산업 현장에서 실제 우려하는 사항을 바탕으로 제조산업 클라우드 보안위험을 분석하고자 하였다. 이를 위해 전문가 인터뷰와 문헌조사를 시행해서 제조산업 클라우드 보안위험을 새롭게 식별하였으며, 선정된 보안위험에 대하여 설문조사를 통해 적합성과 시급성을 검증했다. 본 연구를 기반으로 향후 제조산업 클라우드 보안관리 체계가 설계된다면, 제조산업의 클라우드 도입이 보다 활성화될 것으로 기대한다.

Abstract

In the trend of digital transformation and the increase in non-face-to-face services triggered by the Fourth Industrial Revolution, the demand for cloud computing services is being sharply stimulated. Currently, the cloud is being introduced in various industrial sectors including public, IT, and finance, and the manufacturing industry is also adopting the cloud to secure future sustainability and is promoting innovation through smart manufacturing. However, it has been found that there are constraints in the adoption of cloud by manufacturing companies due to concerns about security. Existing studies that have identified cloud security risks have been limited to presenting general cloud security risks or technical security risks rather than focusing on the manufacturing industry. Therefore, this study aimed to identify cloud security risks in the manufacturing industry based on the actual concerns in the field. For this, expert interviews and literature research were conducted to newly identify cloud security risks in the manufacturing industry, and the adequacy and urgency of the selected security risks were verified through surveys. Based on this study, if a cloud security management system for the manufacturing industry is designed in the future, it is expected that the adoption of cloud in the manufacturing industry will be more activated.

Keywords: *Cloud Computing, Manufacturing Industry, Security, Digital Transformation, Industrial Security*

[1] *중앙대학교 융합보안학과 석사과정 (potter2040@cau.ac.kr)*
[2] *중앙대학교 융합보안학과 석사과정 (iamjuno95@cau.ac.kr)*
[3*] *교신저자 중앙대학교 산업보안학과 교수 (hbchang@cau.ac.kr)*

Received: Nov. 21, 2023, Revised: Dec. 22, 2023, Accepted: Jan. 10, 2024

I. 서론

제 4 차 산업혁명으로 인한 디지털 전환과 비대면 서비스의 증가 흐름 속에서 클라우드 컴퓨팅 서비스에 대한 수요가 계속해서 증가하고 있다. 클라우드 컴퓨팅 서비스는 '저장 및 컴퓨팅 시설, 소프트웨어, 데이터, 그리고 애플리케이션 등 공유 자원이 필요할 때, 사용량에 따라 지불하는 방식으로 자원에 액세스하고 사용하는 인터넷 기반 컴퓨팅 서비스'이다[1]. 초기의 클라우드 컴퓨팅 기술이 원격 저장 공간으로 주로 활용되었다면, 오늘날의 클라우드 컴퓨팅 기술은 대량의 데이터를 통합하고 AI 와 머신러닝 기술 등을 통해 분석하여 새로운 가치 창출을 가능하게 하는, 데이터 플랫폼 및 기술 플랫폼으로 진화하고 있다[2]. 이 같은 특징을 바탕으로 클라우드 컴퓨팅 기술은 디지털 전환을 가능하게 하는 제 4 차 산업혁명의 핵심 요소 기술로 자리잡고 있으며 IT, 금융, 공공 등 다양한 산업 분야에 도입이 활발하게 논의되고 있다. 제조산업 또한 클라우드 컴퓨팅 서비스가 큰 잠재력을 발휘할 수 있는 분야 중 하나이다. 클라우드 컴퓨팅 서비스가 제공하는 유연성 및 경제적 효율성이라는 가치는 제조기업이 미래 지속가능성을 확보하기 위해 추진하는 디지털 전환에 유리하게 작용할 수 있다.

하지만 기업이 클라우드 컴퓨팅 기술을 적극적으로 도입하는 데는 보안위험으로 인한 제약사항이 존재한다. 2023 년 국내 클라우드 현황을 조사한 자료에 따르면 기업의 클라우드 도입 및 활용 과정에서 가장 큰 어려움은 '클라우드 보안 기술 및 인력 부족'이 1 순위로 나타났다[3]. 제조산업 관점에서도 2022 년 한국산업보안한림원이 산업기술을 보유한 기업에 대해 시행한 설문조사에 의하면, 클라우드를 사용하지 않는 제조기업은 '법규의 모호성'과 '데이터 유출 우려' 등 보안 우려사항을 클라우드 미사용의 가장 큰 이유로 들었다[4].

클라우드 보안위험을 식별하고 대책을 제시한 선행연구들이 존재하지만, 기존 연구 대부분은 제조산업의 특수한 상황을 고려한 보안위험을 식별하지 않고 CSA(Cloud Security Alliance)가 제시하는 일반적인 클라우드 플랫폼 보안위험을 그대로 인용하거나, 사이버 보안위험 등 기존 기술적 측면 보안위험을 중심으로 클라우드 보안위험을 다루었다는 한계가 존재한다. 이 같은 문제로 인하여 실제 제조산업 현장에서 우려하는 보안위험과 기존 연구 사이에는 다소 차이가 발생하고 있다.

이에 본 연구는 제조산업 현장에서 실제 우려하고 있는 클라우드 보안위험을 식별하여 향후 관리체계 등 대책 설계를 위한 기반을 마련하고자 한다. 제 1 장 서론에 이어 제 2 장 관련연구에서는 제조산업 클라우드 컴퓨팅 서비스 도입 및 활용현황을 조사하고 기존 클라우드 보안 관련 선행 연구를 파악한다. 제 3 장에서는 다양한 분석방법을 통해 제조산업 클라우드 보안위험을 식별하고 타당성을 검증한다. 제 4 장은 결론으로 연구 결과와 의의, 그리고 한계를 논한다.

II. 관련 연구

2.1 제조산업 클라우드 도입 배경

클라우드 컴퓨팅은 제 4 차 산업혁명의 핵심 기술 중 하나로, 다른 기술과의 높은 연계성[5]을 바탕으로 디지털 전환(Digital Transformation)을 가능하게 한다. 디지털 전환은 디지털 기술을 통해 기존 비즈니스 경쟁력을 높이거나 새로운 비즈니스 모델을 창출하는 과정이다. IoT 기술을 통해 현실 데이터를 디지털화하여 빅데이터를 생성하고, 이를 인공지능과 머신러닝으로 분석하여 가치를 창출하는데, 일련의 과정에서 클라우드는 이들을 통합 관리하는 데이터 플랫폼 및 기술 플랫폼 역할을 수행한다[2]. 제조기업 또한 변화하는 환경에 민첩하게 대응하기 위해 제 4 차 산업혁명 기술을 제조 프로세스에 통합하고 있다. 이러한 디지털 전환 흐름은 스마트 팩토리로 진화하는 것을 목표로 하며, 현 제조산업이 클라우드를 도입하려는 주된 이유가 되고 있다.

클라우드 컴퓨팅 기술이 제조산업에 가져오는 효과는 유연성(Flexibility)과 경제적 효율성(Economic efficiency) 측면에서 바라볼 수 있다[4]. 유연성 측면에서 클라우드 컴퓨팅을 활용하면 변화하는 환경을 예측할 수 있을 뿐만 아니라, 비즈니스에 필요한 인프라를 신속하게

구축할 수 있고, 최신 기술이 적용된 소프트웨어도 거의 즉시 활용할 수 있어 환경변화에 민첩하게 대응할 수 있다. 또한 클라우드 컴퓨팅은 다양한 측면에서 경제적 효율성을 제고한다. 시공간적 요소에 방해를 받지 않고 업무 수행을 가능하게 하며, 데이터 공유와 협업을 촉진시키고, 지능화된 제조 프로세스를 통해 생산성을 향상시킨다. 그뿐만 아니라 온 프레미스 환경을 구축하는데 소요되는 초기 투자 비용과 시스템 관리 비용을 절약할 수 있고, 필요한 자원만을 그때그때 사용하기 때문에 낭비가 발생하지 않는다. 특히 경제적 측면에서 가장 큰 효과는 비즈니스 혁신을 가능하게 하는 것이다. 클라우드 컴퓨팅 플랫폼을 통해 축적된 데이터로부터 창출된 혁신 가치는, 결과적으로 새로운 수익모델의 탐색을 가능하게 함으로써 기업의 지속적인 경쟁력을 강화한다.

2.2 제조산업 클라우드 도입 및 활용 현황

현재 국내에도 제조기업이 클라우드를 도입하여 적극적으로 디지털 전환을 추진하는 사례가 존재한다. 글로벌 클라우드 서비스 사업자인 AWS 에 따르면 포스코는 2024 년까지 주요 사내 시스템을 퍼블릭 클라우드로 전환하는 로드맵을 세웠으며, 추진 계획의 일환으로 엔지니어링 가상 데스크톱 인프라 기술을 도입, 개인용 기기로 복잡한 3D 데이터 활용 업무를 간단히 처리할 수 있도록 하였다[6]. 두산 인프라코어는 클라우드 기반 빅데이터 플랫폼을 구축하여 협업 및 의사결정 구조를 혁신했으며, 드론 측량, 시공 계획 등에 필요한 데이터를 클라우드 플랫폼에 통합해서 현장 작업을 효율화하는 솔루션을 출시했다[2].

하지만 제조산업 전반적으로는 클라우드 컴퓨팅 기술의 도입이 원활하게 이루어지고 있다고 보기 어려운 상황이다. OECD 통계에 따르면 2018 년 국내 제조기업의 클라우드 활용률은 22.1%로, OECD 평균인 30.9%에 비해 낮은 것으로 드러났다[2]. 한국산업보안산림원은 2022 산업보안컨퍼런스에서 산업기술 보유 기업을 대상으로 조사한 클라우드 사용현황을 발표하였는데, 클라우드를 사용하지 않는다고 답한(22%) 모든 기업이 제조기업인 것으로 나타났다[4]. 클라우드를 사용하지 않는 이유는 법규의 모호성(50%), 데이터 유출 우려(25%), 초기 비용 부담이 (25%)인 것으로 응답되어 보안위험과 관련된 사유가 75%에 달하는 것으로 분석되었다. 그럼에도 이들 기업의 88.9%는 3 년 내 클라우드 사용 예정이 있다고 답하였는데, 클라우드 보안위험으로 인한 제약사항에도 여전히 클라우드에 대한 제조기업의 수요가 높은 상황을 확인할 수 있다.

2.3 클라우드 보안위험

클라우드 보안위험을 다룬 대부분의 국내 학술 논문은 클라우드 보안 협회, CSA 가 선정한 ‘클라우드 컴퓨팅 주요 위협(Top Threats to Cloud Computing)’을 주로 인용하고 있다. CSA 는 클라우드 컴퓨팅 환경을 안전하게 유지하기 위한 모범사례를 정의하고 클라우드 보안 인식을 제고하기 위한 활동을 수행하는 비영리조직으로, 주기적으로 클라우드 주요 위협을 식별한 보고서를 개정하여 내놓고 있다. 개정할 때마다 시의성에 따라 이전에 식별된 위협이 사라질 수도 있고, 새로운 위협이 추가되기도 하며, 주요 위협의 개수가 변하기도 한다. 2022 년 최신 개정판[7]은 여섯 번째 버전으로, ①불충분한 신원, 자격증명, 접근 및 키 관리, ②불완전한 인터페이스와 API, ③잘못된 설정 및 부적절한 변경관리, ④클라우드 보안 아키텍처 및 전략 부족, ⑤불안전한 소프트웨어 개발, ⑥안전성이 확보되지 않은 써드파티 자원, ⑦시스템 취약점, ⑧우발적 클라우드 데이터 노출, ⑨서버리스 및 컨테이너 워크로드의 잘못된 구성과 악용, ⑩조직 범죄, 해커, APT 위협, ⑪클라우드 저장소 데이터 유출 11 개의 주요 위험을 제시했다.

CSA 외에 클라우드 보안위험을 정의한 문헌은 주로 국내 정부기관이나 연구기관에서 발행한 백서를 통해 찾아볼 수 있다. 국가정보원과 국가보안기술연구소가 공동 발행한 ‘국가 클라우드 컴퓨팅 보안 가이드라인’ [8]은 클라우드 컴퓨팅 환경을 구성하는 ①가상환경, ②클라우드 인프라, ③정책, ④사고 및 장애 대응, ⑤인증 및 권한, 그리고 ⑥데이터 6 가지 요소 중심으로 각 구성요소의 보안 속성을 침해하는 다양한 보안 위협을 식별했다. 하지만 해당 연구는 위협이 발생하는 구체적 시나리오까지는 제시하지 못한 한계가 있다. 한국인터넷진흥원이 발행한 ‘2030 미래사회 변화 및 사이버 위협 전망 연구’ [9]는 클라우드 분야 사이버 위협을 공급자와 이용자라는 대분류로 나눈 뒤, 공급자의 중분류는 시스템,

기기/인프라, 데이터, 네트워크로 구성했고 이용자의 중분류는 서비스 이용 보안 이슈로 구성했다. 소분류에 해당하는 14 개 위협 중 이용자 측면 위협은 2 개 존재하는데, 현재 발생하는 대부분 클라우드 보안 사고가 고객사의 책임임을 고려하면, 식별한 위협이 지나치게 공급자의 기술적 위협에 치중된 측면이 있다고 볼 수 있다. 한편 소프트웨어정책연구소는 '클라우드 보안의 핵심이슈와 대응책' [10]에서 기술적 측면의 위협과 기술 외적 측면의 위협을 제시했다. 기술적 측면의 위협은 공통 IT 인프라에서 발생하는 위협 보다는 가상화라는 특성에서 발생하는 하이퍼바이저 감염 위험, 가상머신 공격 경로 다양성, 공격자의 익명성, 가상머신의 이동성으로 인한 확산 문제를 다루어 다른 연구와는 차별성을 보였다. 기술외적 측면에는 관리 측면의 문제, 내부자 문제, 해커들의 타겟, 피해 규모의 확산, 법 · 제도적 문제 다섯 가지 위협을 다루었다, 해당 연구의 위협 분류 기준은 기존 클라우드 보안 관련 연구와 차별화되는 측면이 있으며, 현재 클라우드 보안에 관한 논의가 기술 보다는 기술 외적인 측면에서 주로 이루어지는 점을 고려할 때 이전 연구들의 한계를 일부 극복한 점에 의의가 있다고 볼 수 있다.

클라우드 보안 관련 선행연구를 살펴보면 제조, IT, 공공 등 특정 산업분야에 따른 보안위험 보다는 일반적인 클라우드 플랫폼에 관한 보안위험을 다루고 있다는 점을 파악할 수 있다. 또한 이들 연구 다수는 공통 IT 인프라를 사용하는 데서 발생하는 기술적 위험을 주로 다루고, 법 · 제도적 문제나 사고 발생 시 책임 소재 문제, 데이터 통제권 문제, 정책 부재 등 기술 외적 문제는 다소 적은 비중으로 다루고 있었다. 하지만 제조산업에서 클라우드를 도입하는 데 있어서 주된 제약으로 작용하는 사항은 기술적 보안 우려사항 보다는 데이터의 통제권과 클라우드 서비스 사업자에 대한 신뢰 문제가 중심이된다는 점에서, 클라우드 보안위험을 식별한 기존 연구는 실제 제조산업 현장에서 우려하는 보안위험과 다소 차이가 있었다. 따라서 본 연구는 제 3 장에서 제조산업 클라우드 보안위험을 새롭게 확인하고자 시도하였다.

III. 제조산업 클라우드 보안위험 식별 및 타당성 분석

3.1 연구설계

본 연구는 제조산업 클라우드 보안위험을 분석하기 위해 전문가 인터뷰, 문헌 분석, 설문조사 기법을 활용하였다. 먼저, 제조산업에 종사하는 전문가를 대상으로 인터뷰를 진행하여 클라우드 도입 및 활용 과정에서 우려되는 보안위험을 파악하여 정리했다. 다음으로는 제조산업에서 우려하는 보안위험 외에 [표 1]과 같이 클라우드 보안위험 관련 문헌을 분석하여 추가적으로 중요한 보안위험을 확인했다. 국내 학술논문은 CSA 가 과거에 선정했던 보안위험을 그대로 인용한 경우가 많기에 관련 문헌은 백서를 중심으로 선정하였다. 그밖에 다양한 참고문헌을 바탕으로 클라우드 보안위험을 통합하여 정리하거나 분석한 학술 논문도 분석 대상 문헌으로 선정하였다.

Table 1. Documents related to Cloud Security Risks for Analysis
표 1. 분석대상 클라우드 보안위험 관련 문헌

	Title	Format	Author	Publication year
1	National Cloud Computing Security Guidelines [8]	White paper	National Intelligence Service et al.	2023
2	Top Threats to Cloud Computing [7]	White paper	Cloud Security Alliance	2022
3	2030 Future Society Changes and Cyber Threat Forecast Study [9]	White paper	Korea Internet & Security Agency	2021
4	Key Issues and Countermeasures in Cloud Security [10]	White paper	S. W. Ahn et al.	2017
5	Vulnerability and Security Management System from the Perspective of the Cloud Service Users [11]	Article	Y. J. Choi et al.	2012
6	Study on Security Considerations in the Cloud Computing [12]	Article	C. S. Park	2011

마지막으로 법률가, 보안 담당자, 보안업계 종사자 등 보안 전문가 등을 대상으로 설문조사를 시행하여 식별된 제조산업 클라우드 보안위험에 대한 타당성을 검증했다. 타당성 검증을 위한 설문은 리커트 5 점 척도를 사용하여 각 보안위험에 대해 적합성과 시급성을 평가하도록 하였으며 설문은 총 16 부가 회수되었다. 적합성은 식별된 보안위험이 제조산업에서 실제로

발생할 수 있는 클라우드 보안위험이 맞는지를 평가하는 지표이며, 시급성은 보안위험이 실제 발생할 경우 예상되는 위험의 영향도의 크기, 즉 보안위험의 중요도를 평가하는 지표이다. 적합성은 "클라우드 서비스에 저장된 정보에 대해 클라우드 서비스 사업자의 임의 접근 가능 항목은 보안위험으로 어느 정도 적합하다고 생각하십니까?"와 같은 형식으로 설문이 진행되었으며, 응답은 ①전혀 적합하지 않음 ②적합하지 않음 ③보통임 ④적합함 ⑤매우 적합함의 5 점 척도로 구성되도록 하였다. 시급성의 경우 "클라우드 서비스에 저장된 정보에 대해 클라우드 서비스 사업자의 임의 접근 가능 보안위험이 실제 발생했을 때, 위험성의 크기에 따른 중요성이 어느 정도라고 생각하십니까?"와 같은 형식으로 설문이 진행되었으며, 응답은 ①전혀 중요하지 않음 ②중요하지 않음 ③보통임 ④중요함 ⑤매우 중요함의 5 점 척도로 구성되었다. 각 보안위험 항목의 적합성과 시급성에 대한 평가기준은 보안 관련 연구에서 일반적으로 활용되는, 보통(평균 3.0) 이상 수준인 평균 3.5 로 설정하였다[13].

3.2 연구결과

제조산업에 종사하는 전문가 인터뷰를 기반으로, 보충적 문헌조사를 통해 최종적으로 식별한 제조산업 클라우드 보안위험은 15 가지로 확인되었다. 확인된 각 위험은 한국산업보안한림원이 조사한 제조기업의 클라우드 도입 우려사항[4]을 참고하여 세 가지로 분류하였다. 그 결과 데이터 통제권 관련 위험 7 개, 고객사 관련 위험 3 개 그리고 클라우드 서비스 사업자 자체 보안위험 5 개가 확인되었다. 고객사 관련 위험과 클라우드 서비스 사업자 자체 보안위험은 책임공유모델에 따라 위험관리 주체와 사고 발생 시 책임 등이 비교적 명확하게 구분되고, 선행연구에서도 비교적 자주 확인되는 유형의 위험이다. 또한, 이러한 유형의 위험은 기술적 취약점과 고객의 권한 관리 실수와 같은 관리적 취약점으로 인하여 주로 발생한다. 하지만 데이터 통제권 관련 위험은 기존 문헌보다는 주로 제조산업 현장의 전문가 인터뷰를 통하여 새롭게 확인된 유형의 위험이다. 이러한 유형의 위험은 주로 기업 외부에 데이터를 저장하는 특성으로 인한 신뢰의 문제와 함께, 해외 클라우드 서비스를 이용하는 데서 발생하는 다소 복잡한 법적 문제를 포함한다.

Table 2. Results of Adequacy Assessment
표 2. 적합성 평가 결과

Type	Security Risks	Average
Data Control Associated Risks	1. Inability to verify the physical location and form of storage of critical information such as trade secrets owned by manufacturing companies	4.50
	2. Potential for arbitrary access by cloud service providers to information stored in cloud services	4.00
	3. Possibility of cloud service operators dispersing backup content abroad or in remote locations without clear accountability	4.00
	4. Risk of exposure of critical information stored in cloud services by foreign government agencies through court warrants or other means	3.50
	5. Issues with complete data destruction upon termination of cloud services	4.19
	6. Data loss in the event of the cloud service provider's business withdrawal or closure	4.06
	7. Disputes related to the legitimacy of the current shared responsibility model in the event of a data security incident, where the user bears 100% responsibility	3.50
Customer Related Security Risks	8. Potential for insider (or account hijacker) leakage due to the absence of proper authority management such as authentication and access control	4.31
	9. Risk of information exposure and leakage due to mistakes such as setting failures by the cloud responsible manager at the manufacturing company	4.13
	10. Lack of cloud security architecture and strategies due to low understanding of the cloud computing service environment	3.94
Cloud Service Providers Inherent Security Risks	11. Presence of security vulnerabilities in the virtualized environment of cloud computing services such as risk of hacking	3.75
	12. Need to ensure availability from operational disturbances of cloud services due to disasters and calamities	4.13
	13. Availability impairment of cloud services due to DDoS attacks	4.25
	14. Interoperability and portability issues between legacy systems or other cloud services	3.25
	15. Necessity for audit activities to monitor legal compliance and verify adherence to SLAs by cloud service providers	3.75

확인된 제조산업 클라우드 보안위험에 대해 설문조사를 실시한 결과, 각 보안위험의 적합성은 [표 2]와 같이 나타났다. 검증 결과 클라우드 서비스 사업자 자체 보안위험 중 '14.

레거시 시스템, 또는 타사 클라우드 간 이식성 및 상호 운용성'은 적합성 평균이 보통이상 수준인 3.5 미만에 해당하는 3.25 로, 제조산업 클라우드 보안 위험으로서 부적합하다는 결과가 도출되었으며, 이외의 모든 항목은 평균 3.5 이상으로 제조산업 클라우드 보안위험으로 적합한 것으로 확인되었다.

다음으로 적합성이 검증된 14 가지 보안위험에 대해서 시급성을 평가하였다. 적합성이 검증된 모든 보안위험은 시급성 평균이 3.5 이상으로 대책 마련이 필요한 것으로 파악되었다. 특히 [그림 1]과 같이 각 보안위험의 시급성은 적합성이 높을 수록 높게 나타나, 적합성과 시급성은 비례하는 경향을 보였다. 따라서 식별된 클라우드 보안위험이 제조산업에서 발생 가능한 것으로 인식되는 보안위험일수록, 실제 발생하였을 경우 위험성의 크기도 클 것으로 예상된다.

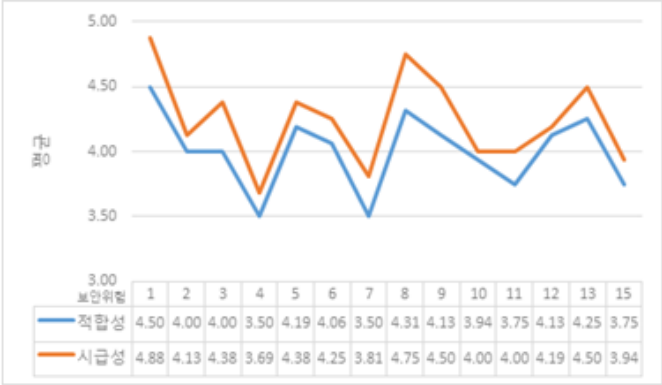

Figure 1. Relationship between the Adequacy and Urgency of Cloud Security Risks in the Manufacturing Industry
그림 1. 제조산업 클라우드 보안위험 적합성 및 시급성 관계

적합성이 검증된 제조산업 클라우드 보안위험을 시급성이 큰 순서대로 정리하면 [표 3]과 같다.

Table 3. Results of Urgency Assessment
표 3. 시급성 평가 결과

Rank	Security Risks	Average
1	1. Inability to verify the physical location and form of storage of critical information such as trade secrets owned by manufacturing companies	4.88
2	8. Potential for insider (or account hijacker) leakage due to the absence of proper authority management such as authentication and access control	4.75
3	9. Risk of information exposure and leakage due to mistakes such as setting failures by the cloud responsible manager at the manufacturing company	4.50
3	13. Availability impairment of cloud services due to DDoS attacks	4.50
5	3. Possibility of cloud service operators dispersing backup content abroad or in remote locations without clear accountability	4.38
5	5. Issues with complete data destruction upon termination of cloud services	4.38
7	6. Data loss in the event of the cloud service provider's business withdrawal or closure	4.25
8	12. Need to ensure availability from operational disturbances of cloud services due to disasters and calamities	4.19
9	2. Potential for arbitrary access by cloud service providers to information stored in cloud services	4.13
10	10. Lack of cloud security architecture and strategies due to low understanding of the cloud computing service environment	4.00
10	11. Presence of security vulnerabilities in the virtualized environment of cloud computing services such as risk of hacking	4.00
12	15. Necessity for audit activities to monitor legal compliance and verify adherence to SLAs by cloud service providers	3.94
13	7. Disputes related to the legitimacy of the current shared responsibility model in the event of a data security incident, where the user bears 100% responsibility	3.81
14	4. Risk of exposure of critical information stored in cloud services by foreign government agencies through court warrants or other means	3.69

시급성이 1 순위로 높은 위험은 ‘1. 제조기업이 보유한 영업비밀 등 중요정보가 물리적으로 어느 장소에 어떠한 형태로 저장되어 있는지 확인 불가(4.88)’로 나타났다. 2 순위는 ‘8. 인증 및 접근통제 등 적절한 권한관리 부재로 인한 내부자(혹은 계정 탈취자) 유출 가능성(4.75)’으로 확인되었다. ‘9. 제조기업 클라우드 담당 관리자의 설정 실패 등 실수로 인한 정보 노출 및 유출(4.50)’과 ‘13. DDoS 공격으로 인한 클라우드 서비스 가용성 훼손(4.50)’은 공동으로 3 순위로 나타났다. ‘3. 현재 운영되는 클라우드 서비스에 대한 백업 내용을 클라우드 서비스 기업이 해외 등 원격지에 임의 소산 가능성(4.38)’과 ‘5. 클라우드 서비스 이용 종료 시 데이터 완전 파기 문제(4.38)’ 또한 공동으로 5 순위로 나타났다. 7 순위는 ‘6. 클라우드 서비스 사업자의 사업 철수 및 폐업 시 데이터 손실(4.25)’으로 나타났다. 8 순위는 ‘12. 재해 및 재난 등에 의한 클라우드 서비스 운영 장애로부터 가용성 확보 필요(4.19)’로 확인되었다. 9 순위는 ‘2. 클라우드 서비스에 저장된 정보에 대해 클라우드 서비스 사업자의 임의 접근 가능(4.13)’으로 나타났다. 10 순위는 ‘10. 클라우드 컴퓨팅 서비스 환경 낮은 이해도로 인한 클라우드 보안 아키텍처 및 전략 등 정책의 부재(4.00)’와 ‘11. 해킹 위험 등 클라우드 컴퓨팅 서비스 가상화 환경에 대한 보안 취약점 존재(4.00)’가 공동으로 나타났다. 12 순위는 ‘15. 클라우드 서비스 사업자 대상 준법 감시 및 SLA 준수 확인 등을 위한 감사 활동 필요성(3.94)’으로 나타났다. 13 순위는 ‘7. 현 책임공유 모델에 의한, 데이터 보안 사고 발생 시 사용자의 100% 책임 타당성 관련 분쟁(3.81)’으로 나타났다. 14 순위는 ‘4. 법원 영장 등 해외 정부기관에 의해 클라우드 서비스에 저장된 중요정보의 노출 가능성(3.69)’으로 나타났다.

공동 5 순위까지 해당하는 상위 6 개 보안위험을 살펴보면, 데이터 통제권 관련 위험 유형에 속하는 보안위험이 3 개로 가장 많이 확인되고 있다. 그 중에는 가장 시급성이 높은 것으로 드러난 ‘1. 제조기업이 보유한 영업비밀 등 중요정보가 물리적으로 어느 장소에 어떠한 형태로 저장되어 있는지 확인 불가’가 포함된다. 이는 주로 클라우드 서비스 사업자에 대한 신뢰가 문제가 되어 발생하며 데이터가 저장되는 서버의 물리적 위치를 국내로 한정하고 대략적인 지역을 안내하며, 이를 추적 및 보증할 수 있는 조치를 적용하는 방향으로 통제가 필요할 것으로 보인다. 다음으로는 공동 5 위였던 ‘3. 현재 운영되는 클라우드 서비스에 대한 백업 내용을 클라우드 서비스 기업이 해외 등 원격지에 임의 소산 가능성’과 ‘5. 클라우드 서비스 이용 종료 시 데이터 완전 파기 문제’가 있다. 이들 역시 제조기업 관점에서 클라우드 서비스 사업자에 대한 신뢰 문제가 중점이 되는 보안위험으로, 클라우드 서비스 사업자에게 특정 통제 조치와 로그 등을 요구할 수도 있지만, 후자의 경우는 서비스 이용종료 시 고객사가 정보를 암호화하고 키를 파기하는 방향으로 직접 통제 또한 가능할 것으로 보인다. 정리하자면 다수의 데이터 통제권 관련 위험이 새로 식별되었고 그 중 약 절반은 시급성이 높은 위험으로 나타났다.

고객사 관련 위험 유형은 시급성 상위 6 개 보안위험 중 2 개가 확인되었는데, 이에는 2 순위인 ‘8. 인증 및 접근통제 등 적절한 권한관리 부재로 인한 내부자(혹은 계정 탈취자) 유출 가능성’과 함께 3 순위인 ‘9. 제조기업 클라우드 담당 관리자의 설정 실패 등 실수로 인한 정보 노출 및 유출’이 포함된다. 이러한 유형의 위험은 주로 고객사 내부에서 잘 정리된 클라우드 보안 정책과 교육 등을 통해 통제가 필요할 것으로 보인다. 정리하면 3 개가 식별된 고객사 관련 위험 중 2 개의 시급성이 높은 것으로 나타났는데, 이는 데이터 통제권 관련 위험이라는 새로운 위험 유형이 확인되었음에도, 고객사 관련 위험은 여전히 대책 마련이 시급한 보안위험 유형이라는 점을 시사한다.

마지막으로 클라우드 서비스 사업자 자체 보안위험 유형은 시급성 상위 6 개 중 1 개만이 확인되었으며, 3 순위인 ‘DDoS 공격으로 인한 클라우드 서비스 가용성 훼손’이 해당된다. 외부 서비스를 이용하는 특성상 가용성이 중요했던 이슈였던 것으로 보이며, 제조산업에서도 클라우드 서비스 사업자 측면의 보안위험 보다는 고객사 측면의 보안위험이 중요도가 높다고 해석할 수 있다.

IV. 결론

연구결과, 전문가 인터뷰와 문헌조사에 기반한 제조산업 클라우드 보안위험은 데이터 통제권

관련 위험 7 개, 고객사 관련 보안위험 3 개, 클라우드 서비스 사업자 자체 보안위험 5 개로 확인되었다. 특히 기존 클라우드 보안 관련 문헌이 주로 고객사 관련 보안위험과 클라우드 서비스 사업자 자체 보안위험을 다루었던 것과 달리, 제조산업 현장에서는 주로 데이터 통제권과 관련한 보안위험이 새롭게 식별된 것으로 나타났다. 식별된 제조산업 클라우드 보안위험 중 클라우드 사업자 자체 보안위험 유형에 해당하는 1 개 보안위험 항목을 제외한 14 개 보안위험의 적합성이 검증되었으며, 적합성이 검증된 모든 보안위험에 대한 시급성이 보통 이상 수준인 것으로 분석되었다. 또한, 보안위험의 시급성은 적합성과 비례 관계에 있어, 제조산업에서 발생 가능한 것으로 예상되는 보안위험일수록, 이러한 위험이 실제 발생하였을 경우 위험의 영향도 클 것으로 보인다.

본 연구는 제조산업이 클라우드를 도입하며 발생할 수 있는 보안위험을 현장의 보안 우려사항을 중심으로 파악했다는 점에 의의가 있다. 하지만 제조산업을 이해하고 있는 보안 전문가 확보의 어려움으로 충분한 설문조사 응답을 확보하지 못했기에, 제한된 수준의 적합성 및 시급성 검증이 이루어진 한계가 있었다. 향후 본 연구를 바탕으로 제조산업 클라우드 보안 관리체계 등이 설계되어 안전한 클라우드 활용을 위한 기반이 마련된다면, 제조산업의 클라우드 도입을 통한 디지털 전환이 보다 활성화 될 것으로 기대한다.

V. 감사의 글

이 논문은 2023 년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임(P0008703, 2023 년 산업혁신인재성장지원사업).

VI. 참고문헌

[1] Q. Qi, F. Tao, "A Smart Manufacturing Service System Based on Edge Computing, Fog Computing, and Cloud Computing," IEEE Access, Vol. 7, pp. 86769-86777, Jun. 2019.
[2] J. Lee, "Data(D.A.T.A.): A Strategy for Digital Transformation in Manufacturing Industry Using Cloud," Trade Focus, No. 27, Korea International Trade Association (KITA), Aug. 2021.
[3] "2023 Domestic Cloud Computing Status and Prospects: Market Pulse," IDG Korea, Feb. 2023.
[4] Korea Academy of Industrial Security, "Protection Measures for Industrial Technology in Response to the Spread of Cloud Computing," in Proc. of the 2022 Industrial Security Conference, Seoul, Nov, 2022.
[5] Y. Oh, T. Kang, "Analysis of New Technology Adoption Strategies in Manufacturing Companies: Focusing on Domestic Smart Production Cases," Innovation Studies, Vol. 18, No. 1, pp. 97-117, Feb. 2023.
[6] S. J. Jung. (2022, Dec), [Focus] AWS, Introduction of the Role of Cloud and Examples for Digital Transformation in Manufacturing Industry. CAD&Graphics [Online]. Available: https://www.cadgraphics.co.kr/newsview.php?pages=news&sub=news01&catecode=2&num=71901#
[7] "Top Threats to Cloud Computing," Cloud Security Alliance, 2022.
[8] "National Cloud Computing Security Guidelines," National Intelligence Service and National Security Technology Research Institute, Jan. 2023.
[9] "2030 Future Society Changes and Cyber Threats Outlook Research," Korea Internet & Security Agency, Dec. 2021.
[10] S. W. Ahn, H. S. Yoo, D. H. Kim, "Key Issues and Countermeasures in Cloud Security," Software Policy Research Institute, Dec. 2017.
[11] Y. J. Choi, J. H. Ra, P. K. Hong, S. H. Lee, "Vulnerability and Security Management System from the Perspective of Cloud Service Users," Journal of Information Technology and Architecture, Vol. 9, No. 4, pp. 401-411, Dec. 2012
[12] C. S. Park, "Study on Security Considerations in the Cloud Computing," Journal of Korea Academia-Industrial Cooperation Society, Vol. 12, No. 3, pp. 1408-1416, Mar. 2011.
[13] O. C. Na, H. B. Chang, "Design of National R&D Project Security Rating Evaluation Model," Journal of Korea Technology Innovation Society, Vol. 23, No. 4, pp. 841-862, Aug. 2020.

저자소개

오정훈(*Junghun Oh*)

2018 년~현재 소프트캠프㈜ 전략기획실장, 마케팅본부장
2019 년~현재 중앙대학교 일반대학원 융합보안학과 산업보안전공 (석사과정)

관심분야 : 산업보안, 연구보안, 클라우드 보안, 제로 트러스트 보안, 공급망 보안

이주노(*Juno Lee*)

2015 년~2021 년 중앙대학교 경영경제대학 산업보안학과 (학사)
2022 년~현재 중앙대학교 일반대학원 융합보안학과 산업보안관리전공 (석사과정)

관심분야 : 산업보안, 국가핵심기술, 클라우드 보안, 보안관리체계, 전자폐기물

장항배 (*Hangbae Chang*)

2007 년~2012 년 대진대학교 경영학과 조교수
2012 년~2013 년 상명대학교 경영학과 조교수
2014 년~현재 중앙대학교 산업보안학과 교수

관심분야 : 산업보안, 정보등급화, 보안데이터분석, 연구보안, 클라우드 보안