보안관점의 전자폐기물 처리동향 분석 연구

[1] 이주노, [2] 한유나, [3] 최예지, [4] 최유림, [5*] 장항배

Analysis of E-Waste Disposal Trends in a Security Perspective

[1]Juno Lee, [2]Yuna Han, [3]Yeji Choi, [4]Yurim Choi and [5*]Hangbae Chang

요 약

제4차 산업혁명 흐름과 COVID-19 팬데믹으로 증가한 전자부품 수요는 인류의 삶을 편리하게 만들었지만, 전자폐기물의 발생량 또한 증가시켰다. 전자폐기물의 영향에 대한 논의는 환경, 건강, 사회문제 관점을 중심으로 이루어져 왔고, 전 세계의 법령도 이러한 문제들을 해결하는 데 초점을 맞추어 왔다. 하지만 일반적인 폐기물과 달리 전자폐기물에서는 기술 유출 및 개인정보 유출과 같은 보안 문제가 발생할 수 있다. 현재 전자폐기물 보안에 관한 논의는 다른 분야에 비해 매우 부족한 수준이다. 이에 본 연구는 상대적으로 덜 주목받았던 전자폐기물 보안 동향을 실증적으로 분석하고자 하였고 세 가지 접근법을 적용했다. 첫째, 연도별 문헌과 언론보도의 추세를 분석하여 전자폐기물에 관한 전반적인 논의 추이를 파악했다. 둘째, 전자폐기물 보안 위험을 다룬 문헌들을 분석하여 해당 분야의 키워드를 바탕으로 전자폐기물 보안 동향을 파악했다. 셋째, 각종 보안관련 국가지침 내 전자폐기물 처리 관련 규정을 검토하고, 이를 통해 전자폐기물 보안 대책 설계 필요성을 평가했다. 본 연구는 국내에서 거의 처음으로 전자폐기물을 보안 관점에서 다룬 연구라는 점과 전자폐기물 보안 동향을 다차원적으로 분석했다는 점에 의의가 있다. 전자폐기물 보안 동향 분석 결과는 전자폐기물과 전자폐기물 보안 문제에 대한 국내의 인식을 높이고 전자폐기물 보안 위험에 선제적으로 대응할 기회를 제공할 것으로 기대된다.

Abstract

The increased demand for electronic components, spurred by the Fourth Industrial Revolution and the COVID-19 pandemic, has facilitated human life but also escalated the production of e-waste. Discussions on the impact of e-waste have primarily revolved around environmental, health, and social issues, with global legislations focusing on addressing these concerns. However, e-waste poses unique security risks, such as potential technological and personal information leaks, unlike conventional waste. Current discourse on e-waste security is notably insufficient. This study aims to empirically analyze the relatively overlooked trends in e-waste security, employing three methodologies. Firstly, it assesses the general trend in discussions on e-waste by analyzing year-wise documents and media reports. Secondly, it identifies key trends in e-waste security by examining documents on the subject. Thirdly, the study reviews national security guidelines related to e-waste disposal to assess the necessity of designing security strategies for e-waste management. This research is significant as it is one of the first in korea to address e-waste from a security perspective and offers a multi-dimensional analysis of e-waste security trends. The findings are expected to enhance domestic awareness of e-waste and its security issues, providing an opportunity for proactive response to these security risks.

Keywords: *E-Waste, WEEE, Security, Data Security, Reverse Engineering*

[1] *중앙대학교 일반대학원 융합보안학과 석사과정 (iamjuno95@cau.ac.kr)*
[2] *중앙대학교 일반대학원 융합보안학과 박사과정 (juliahan094@cau.ac.kr)*
[3] *중앙대학교 일반대학원 융합보안학과 석사과정 (yjji9783@cau.ac.kr)*
[4] *중앙대학교 일반대학원 융합보안학과 박사과정 (julie330@cau.ac.kr)*
[5*] *교신저자 중앙대학교 경영경제대학 산업보안학과 교수 (hbchang@cau.ac.kr)*

Received: Nov. 14, 2023, Revised: Dec. 15, 2023, Accepted: Dec. 18, 2023

I. 서론

오늘날 제 4 차 산업혁명까지 이어지는 정보화 · 디지털화의 흐름과 COVID-19 로 인한 비대면의 일상화라는 특수한 시대적 상황은 전자부품에 대한 수요를 가파르게 촉진시켰다[1]. 이들 전자부품은 인류의 삶을 풍요롭게 하는 기반이 되었지만, 전자부품 수요의 증가는 곧 쓰레기로써 버려지는 전자폐기물의 급격한 증가라는 부정적 효과를 함께 초래했다. 유엔훈련조사연구소(UNITAR)의 보고서에 근거하면 2019 년 전 세계에서 5,360 만 톤의 전자폐기물이 발생하였으며, 연평균 약 200 만 톤씩 증가해 2030 년에는 7,470 만 톤, 2050 년에는 1 억 1,000 만 톤에 달할 것으로 예상된다[2].

전자폐기물의 증가로 인한 영향은 일반적인 폐기물과 마찬가지로 주로 환경, 건강, 사회적 문제 관점을 중심으로 논의되어 왔다. 전자폐기물에는 납, 니켈, 수은, 카드뮴과 같은 중금속과 독성 화학 물질이 포함돼 있어 적절하게 처리하지 않고 방치하거나 매립한다면 토양과 지하수를 오염시키는 등 환경 문제를 발생시킨다. 같은 맥락에서 오염된 환경은 식재료, 공기 질 저하 등 연쇄작용을 통해 인체 건강을 위협하는 요소로 작용한다. 이러한 영향으로 전자폐기물 처리는 기피 산업이 되었고, 선진국이 배출된 전자폐기물을 개발도상국으로 수출하며 전자폐기물 처리 과정에서 발생하는 부정적 외부효과를 떠넘긴다는 사회적 문제 또한 주목받고 있다.

현재 전자폐기물과 관련한 규제 또한 이러한 문제를 해결하는 데 초점을 맞추고 있다. EU WEEE 지침과 바젤 협약은 전자폐기물과 관련한 규정이 마련된 대표적인 국제 법령이다. 유럽연합 회원국에 적용되는 EU WEEE 지침은 전자폐기물 재활용에 관한 사항이 회원국의 국내법 형태로 구현되는데, 전자폐기물 처리에 대한 책임을 제조 및 유통업자에 부과한다. 바젤협약은 유해 폐기물 발생을 최소화하며 유해 폐기물이 발생할 때 발생지와 가까운 곳에서 처리할 수 있도록 하는 의무를 규정하며 전자폐기물을 포함한 유해 폐기물의 국가 간 이동 절차를 통제한다. 국내에는 전자폐기물 관련 법령으로 「폐기물관리법」, 「자원순환 기본법」, 「자원의 절약과 재활용촉진에 관한 법률」, 「전기 · 전자제품 및 자동차의 자원순환에 관한 법률」, 그리고 바젤 협약 준수를 위해 제정된 「폐기물의 국가 간 이동 및 그 처리에 관한 법률」 등이 존재한다. 일본은 2001 년부터 「순환형 사회형성 추진 기본법」을 시행하며 그 아래에 재활용 추진을 위한 「자원 유효 이용 촉진법」과 폐기물의 적절한 처리를 위한 「폐기물 처리법」을 추가로 제정하였다[3]. 특히 전자폐기물과 관련하여는 「가전 리사이클법」, 「소형가전 리사이클법」이 존재하나, 이들 역시 전자폐기물의 효과적 재활용을 목적으로 한다. 이처럼 지금까지 국내외 전자폐기물 처리 규제는 공통으로 환경, 건강, 사회적 문제 해결을 위해, 폐기물의 하위 분류로서 전자폐기물의 재활용 촉진과 국가 간 이동 통제에 초점을 맞추고 있다.

하지만 전자폐기물로 발생하는 문제는 기존 폐기물과 달리 환경, 건강, 사회적 문제에만 한정되지 않고 기술 유출이나 정보 유출과 같은 보안 위험을 포함한다. 전자폐기물에서 신용카드 정보나 개인식별정보 등 민감한 정보가 유출되는 문제는 과거부터 논의되었으나 대응책은 진전이 거의 없는 상황이다. 심지어 역공학을 통해 전자폐기물에서 첨단 반도체 기술과 영업비밀을 탈취하는 문제가 비교적 최근 확인되었으나 관련 논의는 연구뿐만 아니라 뉴스 기사로도 찾아보기 어렵다. 이처럼 현재 전자폐기물 보안에 관한 연구는 양적으로도 적고, 질적으로도 충분하지 못하다. 현재 보안 관점에서 전자폐기물 문제를 해결하기 위한 구체적인 관리 프로세스나 새로운 통찰력을 제공하는 연구는 거의 없으며, 기존 연구들은 대부분 위험을 식별하는 수준에 그치거나, 단편적인 기술 대책을 제시했다는 한계가 있다.

이에 본 연구는 전자폐기물 발생량이 지속해서 늘어가는 상황에서, 상대적으로 관심이 적었던 보안관점의 전자폐기물 처리동향을 실증적으로 파악하여 전자폐기물 보안 문제에 대한 국내 관심을 유도하고 향후 전자폐기물 보안 대책 설계를 위한 기반을 마련하고자 한다.

본 논문은 총 4 개 장으로 구성된다. 제 1 장은 서론이며 제 2 장은 전자폐기물 개념과 처리방법, 선행연구와 전문가 인터뷰를 통해 지금까지 식별된 전자폐기물 보안 위험을 정리하였다. 3 장에서는 다양한 분석방법을 사용하여 보안관점의 전자폐기물 처리동향을 파악한다. 4 장은 결론으로 본 연구의 의의 및 한계를 논하며 마무리한다.

II. 관련연구

2.1 전자폐기물 개념

전자폐기물은 광범위한 개념을 포함하는 용어로써 다양한 명칭과 정의가 혼용되어 사용되고 있다. 영어 명칭으로는 e-waste, electronic waste 또는 WEEE(Waste Electrical and Electronic Equipment) 등으로 표기되며 우리말로는 전자폐기물, 전자쓰레기, 폐전기전자제품이라는 명칭으로 사용되고 있다. 본 연구는 편의상 국내에서 일반적으로 사용되는 전자폐기물이라는 명칭을 사용한다.

유엔국제훈련조사연구소(UNITAR)는 전자폐기물(e-waste)을 '소유자가 다시 사용할 의도 없이 폐기한 모든 전기전자제품과 그 구성 부품'으로 정의한다[2]. EU WEEE 지침은 전자폐기물(WEEE)을 '폐기된 모든 전기전자제품 및 폐기 당시 제품의 일부였던 모든 구성요소 및 하위 조립품과 소모품'으로 정의[4]하며, 유사하게 바젤 협약은 전자폐기물(WEEE)을 '바젤 협약에 따라 장비가 폐기물이 되는 시점에 장비의 일부였던 모든 부품, 하위 조립품 및 소모품을 포함하여 폐기물인 전기 또는 전자 장비'로 정의한다. 정리하자면 전자폐기물은 '이전 소유자에게 가치가 다하여 폐기된 컴퓨터, 냉장고, 세탁기 등 다양한 형태의 전기전자제품 및 그 부품'을 의미한다고 볼 수 있다.

전자폐기물은 다양한 형태로 존재한다. 전자폐기물 분류체계로 가장 많이 활용되는 EU WEEE 지침은 전자폐기물을 ①온도교환장비, ②스크린 및 모니터 장비, ③램프 등 조명장비, ④대형장비, ⑤소형장비, ⑥소형 IT 및 통신장비 여섯 가지로 분류한다[4]. 온도교환장비에는 에어컨, 냉장고 등이 있고 램프류 형광등과 LED 등 다양한 조명 장비를 포함한다. 대형장비와 소형장비는 말 그대로 크기를 기준으로 분류되는데, 전자에는 세탁기, 광전지 패널 등이 포함되고 후자에는 청소기, 라디오, 비디오 카메라 등 다양한 소형 전기전자제품 등이 포함된다.

해당 분류체계는 완제품의 재활용 용이성을 중심으로 하여 설계되었지만, 보안관점에서는 자산이 보호가치가 있는지, 어떠한 위협이 발생하는지를 중심으로 전자폐기물을 바라볼 필요가 있다. 아직은 보안관점의 전자폐기물 분류체계는 존재하지 않지만, 일반적으로 보안 위험이 발생하는 전자폐기물은 첨단기술이 적용된 반도체, 중요정보가 저장된 저장매체와 같은 하위 구성부품에 해당한다. 따라서 본 연구는 첨단기술이 적용되었거나 중요한 정보를 담고 있어 보호가치가 있는 모든 유형의 하위 구성부품을 중심으로 논의를 진행하고자 한다. [그림 1]은 이러한 하위 구성부품과 이들이 포함되어 있는 완제품 형태의 전자폐기물 예시이다.

Figure 1. E-waste that could pose a security risk
그림 1. 보안 위험이 발생하는 전자폐기물

2.2 전자폐기물 처리방법

전자폐기물 처리방법은 ①매립 및 소각을 통한 단순 폐기, ②재사용, 그리고 ③재활용 크게 세 가지로 정리할 수 있다[5]. 매립과 소각은 기존 단순한 일반쓰레기를 폐기할 때와 같이 전자폐기물을 땅에 묻거나 불에 태우는 것이다. 단순하고 간편한 폐기 방식이지만 전자폐기물 내에 함유된 중금속으로 인한 환경 오염 문제가 크기 때문에 전 세계적으로 해당 방법으로

전자폐기물을 처리하는 것을 지양하고 있다. 재사용은 다시 사용 가능한 전자폐기물의 전체 제품이나 부품을 분리하여 중고로 사용하는 방법이다. 엄밀히 분류한다면 최종적인 폐기 방법은 아니지만 일단 전자폐기물이 되었던 전기전자제품이 다시 공급망에 편입될 수 있기 때문에 결과적으로 전자폐기물의 양을 줄이는 데 도움이 된다. 하지만 그 과정에서 전자폐기물이 역외로 수출되는 경우가 많고, 재사용되는 전자폐기물은 다른 유형에 비해 보안 위험에 가장 취약하게 노출된다는 단점이 있다. 마지막으로 재활용은 전자폐기물의 부품에서 금속 등 다시 사용 가능한 소재를 분리하는 방법이다. 재활용은 전자폐기물을 역외로 옮기지 않고 국내에서 처리한 후 활용하며 부가가치를 창출할 수 있는 등 환경과 사회적 문제를 적절하게 해결할 수 있어 현재 많은 국가 및 국제 단체에서는 이를 권장하고 있다.

2.3 전자폐기물 보안 위험

전자폐기물은 중요 자산이 생애주기 중 생성, 활용 및 유통을 거쳐 폐기에 도달한 상태인데, 이미 활용 가치가 다한 자산에서 유의미한 정보를 획득한다는 특성상, 보안 위험은 역공학과 관련하여 발생한다. 역공학(Reverse Engineering)은 기존 제품을 분해하여 그 구성요소와 구조를 파악하고 궁극적으로 기술을 획득하는 방법으로 항공기와 같은 대형 구조물부터 작은 반도체, 소프트웨어까지 다양한 영역에서 다양한 형태로 발생 가능하다[6]. 용어의 원래 뜻을 고려하면 저장매체에 저장되었다가 삭제된 정보를 다시 복구하는 디지털 포렌식 또한 광의의 역공학으로 바라볼 수 있다. 이처럼 역공학은 다양한 방식으로 실시할 수 있는데, 이에 따라 전자폐기물 보안 위험도 다양한 형태로 발생하게 된다. 문헌연구와 전문가 인터뷰 결과, 전자폐기물 보안 위험은 다음과 같이 정리되었다.

2.3.1 전자폐기물 콘텐츠 역공학 위험

무형의 기술·정보를 포함하는 콘텐츠 측면의 역공학 위험은 '반도체 집적회로 콘텐츠 역공학 위험'과 '저장매체 중요 데이터 유출 위험' 두 가지의 하위 위험으로 분류된다.

먼저, 반도체 집적회로에 대한 역공학을 통해 첨단 기술에 해당하는 배치설계 기술이 유출될 수 있다. 집적회로(Integrated Circuit)는 설계에 막대한 시간과 비용의 투자가 필요함에도 [표 1]과 같이 다양한 역공학에 취약하기 때문에 완성된 집적회로는 역공학 방지를 위한 다양한 솔루션이 적용[7]되고 있으며 배치설계권이라는 신지식재산권을 통해 법적으로 보호받고 있다. 뿐만 아니라 특정 집적회로 배치설계 기술은 국가 경제안보에 미치는 영향이 크기 때문에 국가핵심기술로 지정받아 강력하게 보호되기도 한다. 하지만 연구개발 과정에서 폐기된 집적회로는 법적 보호가 미흡하거나 폐기물 특성상 존재하는 관리의 사각지대로 인해 역공학 시도가 쉽게 발생할 수 있다.

한편 반도체 집적회로 생산과정에서 합격하지 못하여 폐기된 불량품이 공격자에 의해 확보될 경우, 반도체 산업의 영업비밀이 유출될 가능성도 있다. 대표적으로 생산품 대비 합격품의 비율을 의미하는 수율은 채산성과 관련하여 반도체 제조 경쟁력을 의미하는 중요한 지표인데, 폐기된 집적회로 표본으로부터 공격자가 수율을 유추할 수 있다. 반도체 집적회로 콘텐츠 역공학 위험과 관련하여 반도체 산업 전문가에 따르면, 글로벌 반도체 기업들은 해외 법인에서 전자폐기물을 운송하는 도중 도난 사건을 경험하기도 했으며, 외국인이 국내에서 반도체 전자폐기물을 수집하기 위한 처리업체를 설립하는 경우도 있었다.

Table1. Types of reverse engineering for integrated circuit [6]
표 1. 집적회로 역공학 유형 [6]

Reverse Engineering Types	Description
Product teardowns	Identify the product, package, internal boards, and components
System level analysis	Analyze operations, signal paths, and interconnections
Process analysis	Examine the structure and materials to see how it is manufactured, and what it is made of
Circuit extraction	Delayer to transistor level, then extract interconnections and components to create schematics and netlists

다음으로 버려진 스마트폰, 태블릿 노트북, 컴퓨터 및 그들 내부의 저장 매체에 존재하는 개인정보, 신용카드 정보, 기업 및 국가의 중요 정보 등 민감한 정보가 유출될 수 있다. 저장매체가 존재하는 이들 제품이 폐기될 때에는 별다른 조치없이 그대로 버려지거나, 삭제 혹은 포맷 절차를 거쳐 버려지는 데, 이렇게 버려진 전자폐기물은 디지털 포렌식 기술로 내부에 저장된 정보가 복구되어 유출 당하는 위험에 노출된다. 이때 가나 등 제 3 국으로 수출된 전자폐기물에서 신용카드 정보, 계좌, 개인 사진 등이 확인되기도 하였으며[1], 이렇게 유출된 정보가 실제 사이버 범죄에 이용되는 연관성이 선행 연구에 의해 확인되었다[8]. 저장매체 중요 데이터 유출 위험은 다른 위험에 비해 비교적 빨리 식별되었지만, 해당 위험 완화를 위한 관리적 대책은 아직 진전이 거의 없는 상황이다.

2.3.2 전자폐기물 부품 · 소재 역공학 위험

전자폐기물에서 역공학이 가능한 요소는 무형의 기술 · 정보와 같은 콘텐츠 외에도 눈으로 확인할 수 있는 부품 · 소재와 같은 요소도 존재한다. 전자부품을 제조할 때는 금과 구리와 같은 금속 소재를 비롯하여 각종 첨단 소재, 화학품 등이 사용된다. 이러한 소재의 구성 비율 등은 제품 기능의 효율성에 영향을 미칠 수 있는 요소로, 아직 출시되기 이전이라면 신소재 및 재료 공학 측면에서 기밀로 관리될 필요가 있다. 그런데 [표 1]의 프로세스 분석에 따르면, 구조 및 재료를 조사하여 제품이 어떻게, 무엇으로 만들어졌는지 역공학을 통한 확인이 가능하다. 만약 연구개발 과정 중에 폐기된 첨단 부품이 경쟁자에게 넘어간다면, 제품 상용화 이전부터 소재 관련 정보 등이 사전에 파악 당하여 큰 시간과 비용을 투자해서 확보한 경쟁우위를 빼앗길 수 있다.

III. 보안관점의 전자폐기물 처리동향 분석

3.1 연구 설계

본 연구는 보안관점의 전자폐기물 처리동향을 파악하기 위해 세 가지 방법을 활용했다. 먼저 전자폐기물과 관련된 전체 논의 흐름을 파악하기 위해 연도별 문헌, 언론보도 추이 분석을 시행하였다. 두 번째로 전자폐기물 보안 위험과 관련된 동향을 파악하기 위해 전자폐기물 보안 위험을 식별한 문헌에 대해 연관어 분석을 실시했다. 마지막으로 국가보안지침 관련 문헌의 검토를 통해 전자폐기물 보안 처리 관련 규정 존재 여부를 확인해서 전자폐기물 보안 대책 설계 필요 타당성 여부를 확인하고자 했다.

3.1.1 연도별 전자폐기물 관련 문헌 및 언론보도 추이 분석 연구 설계

연도별 흐름과 시대적 상황에 따른 전자폐기물 논의 동향을 파악하기 위해 전자폐기물 관련 국내 문헌과 해외 문헌, 그리고 국내 언론보도 건수를 양적으로 수집하여 정리하였다. 국내 문헌은 한국학술지인용색인(KCI)에서 2016 년 이후 발행된 학술지 논문과 학술대회 논문을 대상으로 수집하였다. 구체적으로 제목과 주제어를 대상으로 전자폐기물 및 유사어, 영문 명칭을 모두 수집할 수 있도록 '전자폐기물 OR 폐전기전자제품 OR 전자쓰레기 OR e-waste OR WEEE'와 같은 검색쿼리를 사용했다. 수집된 논문 중에는 실제 검색에 사용한 단어나 그 밖의 유사어가 제목 및 주제어에 존재하는 전자폐기물 관련 논문만을 선별하여 수집하였다. 학술 논문이 아니더라도 전자폐기물 '보안' 위험을 다룬 경우, 기관 발행물이나 백서 등 기타 문헌을 수집하려 했으나 관련 국내 문헌은 확인되지 않아 한국학술지인용색인 자료만을 분석하였다. 해외 문헌은 국제 학술 데이터 베이스인 WOS(Web of Science)에 제목과 주제어에 대하여'e-waste OR WEEE' 검색쿼리를 활용하여 2016 년 이후 발행된 논문, 리뷰 논문, 학술대회 논문 대상으로 수집하였으며, 그밖에 전자폐기물 보안 위험을 다루었을 경우 [표 2]의 문헌처럼 기관 보고서, 워킹페이퍼나 기타 학술대회 논문까지 수집했다. 마지막으로, 수집된 국내 문헌 표본이 작아 명확한 동향 파악에 한계가 있었기 때문에 추가적으로 언론보도에 대한 수집을 실시했으며 이를 위해 한국언론진흥재단에서 제공하는 뉴스 빅데이터 분석 서비스인 빅카인즈를 활용했다. 국내 학술논문과 마찬가지로 '전자폐기물 OR 폐전기전자제품 OR 전자쓰레기 OR e-waste OR WEEE' 검색 쿼리를 사용하였으며 2016 년 이후 발행된 11 개

전국일간지, 8 개 경제일간지, 28 개 지역 일간지, 5 개 방송사, 2 개 전문지의 관련 보도를 수집 대상으로 하였다.

3.1.2 전자폐기물 보안 관련 문헌 연관어 분석 연구 설계

연도별 전자폐기물 논의 흐름 파악 이후 전자폐기물 보안 위험에 관한 질적 수준 연구동향 파악을 위한 기법으로 연관어 분석을 선택하였다. 연관어 분석은 주어진 맥락에서 단어가 사용되는 방식을 파악하고 각 단어 간의 상호작용과 관계를 살펴보아 그 내용을 분석하는 방법이다[9]. 하지만 현재 국내에는 전자폐기물 보안 위험을 식별하거나 대책을 제시한 관련 문헌이 거의 확인되지 않으며, 해외 문헌 역시 다른 전자폐기물 주제에 비해 매우 부족한 수만이 존재하고 있다. 따라서 본 연구는 크롤링을 통해 다수 문헌을 수집하고 문헌 제목, 주제어, 초록의 텍스트를 분석하는 일반적인 연관어 분석방법 대신, 전자폐기물 보안 위험을 비교적 명확하게 식별한 문헌 4 종을 [표 2]와 같이 선정한 후, 파이썬을 통해 해당 문헌의 제목, 주제어, 초록 그리고 본문의 모든 단어까지 추출하여 연관어 분석을 시행하는 방법을 채택해서 전자폐기물 보안 위험 관련 통찰력을 도출하고자 시도했다.

Table 2. Documents to be analyzed
표 2. 분석 대상 문헌

Category	Format	Title	Author	Publication Year
Document A	Conference Paper	Security Threat Analysis and Prevention Techniques in Electronic Waste [7]	P. Roychowdhury et al.	2019
Document B	Review Article	E-waste forensics: An overview [1]	N. Kapoor et al.	2021
Document C	Working Paper	Digital Waste and Cyber Crime [8]	K. Hartwig	2016
Document D	Article	E-waste environmental and information security threat: GCC countries vulnerabilities [10]	J. Alghazo et al.	2018

문헌 내 데이터에 대한 전처리는 NLTK(Natural Language Toolkit)라이브러리를 활용하여 분석대상 단어를 토큰으로 분리한 뒤, 명사 추출 및 불용어 처리를 진행하였다. 명사는 일반명사, 복수형 일반명사, 고유명사, 복수형 고유명사를 추출하였으며, 복수형 명사에 대해서는 단수화를 진행했다. 전처리 이후에는 수집된 데이터셋을 바탕으로 빈도분석, 연결망 분석 등을 수행하여 단어 간 관계, 트렌드 등을 도출했다.

3.2 연도별 전자폐기물 관련 문헌 및 언론보도 추이 분석

연도별 발행된 문헌 및 언론보도 추이 분석결과는 [표 3]과 같다. 조사기간 내 국내 문헌은 총 33 건, 해외 문헌은 총 2759 건 수집되어 국내 연구의 전자폐기물에 대한 주목도는 종합적으로 해외에 비해 크게 부족한 것으로 분석되었다. 또한 조사 기간 동안 수집된 국내 언론보도 건수는 569 건으로 같은 기간 발행된 국내 학술논문 건수 보다 크게 앞선 것으로 파악되었는데, 전자폐기물에 대한 국내 논의는 학술적 관점 보다는 사회적 관점에서 주목도가 높음을 확인할 수 있었다.

Table 3. Yearly trends in documents and newspaper articles
표 3. 연도별 학술논문 및 언론보도 추이

	2016	2017	2018	2019	2020	2021	2022	2023	Total
Domestic documents	6	2	4	3	4	5	5	4	33
International documents	239	260	328	341	382	470	445	294	2759
Domestic newspaper articles	4	21	30	24	14	60	259	157	569

연도별 통계를 살펴보면 국내 문헌은 표본 크기가 작아 특별한 흐름을 파악하기 어려웠다. 그에 반해 해외 문헌은 2016 년 이후 꾸준한 증가세를 보이다가 2021 년에 급증하여 최고치를 기록했으며, 2022 년에는 약간의 감소가 있었지만 여전히 높은 수준을 유지했다. 국내

언론보도는 2020 년까지 계속 하여 낮은 추세였으나, 그 이후에는 2021 년에 60 건, 2022 년에는 259 건으로 급증하는 추세를 보였다. 이러한 데이터를 통해, 해외 문헌과 국내 언론보도의 건수가 2021 년과 2022 년 사이에 급증하여, 일정한 경향성을 보이는 것을 알 수 있다. 이 기간은 COVID-19 팬데믹이 정점을 찍었던 시기이며, 비대면 생활 일상화로 인한 전자폐기물 발생량 증가가 관련 논의에 영향을 줄 수 있는 시기였을 것으로 보인다. 전반적으로 해외에서는 COVID-19 이전부터 전자폐기물에 대한 논의가 꾸준히 이루어지며 증가하는 추세를 보였지만, 국내에서는 COVID-19 이전에는 논의가 제한적이었으며 이후에는 사회적 관심이 증가했지만 학술적 관심은 여전히 부족한 것으로 나타났다.

3.3 전자폐기물 보안 관련 문헌 연관어 분석

[표 2]의 분석대상 문헌에서 추출한 키워드의 출현 빈도는 [표 4]와 같이 나타났다. 먼저 모든 문헌에 대해 ‘waste’ 및 ‘security’가 높은 빈도로 나타났는데, 문헌 선정 기준이 ‘전자폐기물 보안’이라는 점과 연결되어 해당 단어가 빈번하게 등장하였다.

Table 4. Results of Frequency Analysis
표 4. 빈도수 도출 결과

Document A		Document B		Document C		Document D	
Keywords	**Frequency**	**Keywords**	**Frequency**	**Keywords**	**Frequency**	**Keywords**	**Frequency**
data	52	waste	41	waste	104	country	69
component	29	device	38	drive	50	data	54
threat	26	crime	34	data	48	waste	42
technique	24	data	33	research	34	security	28
gadget	23	trade	22	country	34	production	27
waste	22	method	19	paper	32	management	26
memory	22	disposal	18	equipment	29	regulation	26
security	18	environment	18	information	27	disposal	20
system	18	health	17	study	26	ton	20
engineering	16	security	15	security	26	information	20
industry	16	metal	13	computer	23	device	17
country	16	management	13	number	21	year	15
protection	16	information	13	company	21	risk	15
device	15	impact	12	market	20	study	13
market	14	country	12	crime	19	privacy	12
level	13	use	11	category	19	issue	11
reverse	11	activity	11	source	18	metal	11
solution	11	effect	11	issue	18	lack	11
semiconductor	11	way	10	stream	18	system	10
method	11	component	10	value	18	government	10

문헌 A 는 'data,' 'component,' 'threat'이 가장 빈번하게 등장한 키워드로, 이를 연관시켜 보면 전자폐기물 부품 안에 있는 데이터에 대한 위협을 중점적으로 다룬 문헌임을 확인할 수 있다. 또한, 'reverse'와 'engineering', 그리고 ‘semiconductor’ 단어를 연결하면, 전자폐기물 반도체에 대한 역공학적 위협에 대해서도 다루었음을 알 수 있다. 문헌 B 는 'device,' 'crime,' 'data' 등이 빈번하게 등장하고 ‘information’이 확인되는데, 이를 통해 해당 문헌이 폐기된 장치에서 나오는 데이터 및 정보를 악용한 범죄에 관한 내용을 중심으로 다루고 있음을 알 수 있다. 문헌 C 는 'drive,' 'data,' 'research,' 'country' 등이 주요 키워드로, 앞의 두 단어로부터 문헌 B 와 유사한 보안 위협을 다루고 있음을 파악할 수 있다. 또한, 'research'와 'country' 키워드는 해당 문헌이 특정 국가적 관점에서 전자폐기물로 인한 보안 위협에 대한 다양한 사례를 조사하고 연구했음을 시사한다. 문헌 D 는 'country,' 'data,' 'production'이 주요 키워드로 나타나는데, 이 문헌 역시

데이터 보안을 중점적으로 다루었지만, 다른 문헌과 달리 'country'가 가장 높은 빈도수로 측정되었다. 이는 문헌 D 가 제목과 같이 특정 지역 국가에 연구 범위를 한정했기 때문인 것으로 보인다,

더 나아가, 깊이 있는 의미를 도출하기 위해 모든 문헌에 대해 공통어 분석을 시행했다. 먼저 각 문헌에서 상위 50 개의 키워드를 추출한 뒤, 각 문헌 별 빈도에 따라 키워드를 분류한 뒤 정렬했다. 일차적 분류 조건은 해당 키워드가 몇 개의 문헌에서 공통으로 나타나는지에 따라 결정했다. 해당 키워드가 더 많은 문헌에 등장할수록 공통어에 가까워진다. 분류이후에는 0 을 제외한 문헌 별 최소 빈도수가 가장 큰 순서대로 키워드를 정렬했다. [표 5]는 이러한 과정을 거쳐 가장 공통어에 가까운 20 개의 키워드를 정리한 것이다.

Table 5. Co-occurring keywords analysis
표 5. 공통어 분석

Category	Keywords
Keywords in all documents	data(33), waste(22), device(15), security(15), country(12), information(10), privacy(8), drive(6), management(6), study(6)
Keywords in 3 documents	equipment(10), industry(5), material(5), method(7), system(7), year(5)
keyword in 2 documents	crime(19), disposal(18), market(14), risk(12),

[표 5]에 따르면 모든 문헌에 대하여 'data'가 가장 높은 빈도로 등장하는 공통 단어임을 파악할 수 있다. 그 밖에도 'device', 'information', 'privacy', 'drive'가 모든 문헌에 등장하고 있는데, 관련연구에서 확인한 저장매체 중요 데이터 유출 위험은 모든 문헌에서 보안 위험으로 인식하고 있음을 알 수 있다. 문헌 A, 문헌 B, 문헌 C, 그리고 문헌 D 를 검토한 결과 저장매체 중요 데이터 유출 위험이 실제로 모든 문헌에서 확인되었다. 세 개의 문헌에서 공통으로 등장한 키워드 중에는 보안과 관련한 키워드가 나타나지 않았다. 두 개의 문헌에서 나타난 키워드 중에는 'crime'과 'risk'가 있었는데, 이들은 비록 모든 문헌에 대해 등장하지는 않았지만 각각 19 번, 12 번의 빈도로 등장하여 일부 문헌에서 보안 위험을 범죄적 관점에서 중요하게 인식했음을 파악할 수 있다.

단어 연결망 그래프를 활용하면 이러한 도출 과정을 시각적으로 확인할 수 있다. 앞선 빈도수 분석에서 문헌 별로 추출한 단어 데이터셋 중 상위 20 개 키워드를 추출한 뒤, 빈도수에 가중치를 두어 [그림 2]와 같이 연결망 그래프를 생성했다. 가장 크기가 크고 노란색으로 표시된 A, B, C, D 노드는 각각 문헌 A, 문헌 B, 문헌 C, 문헌 D 를 의미한다. 사각형의 A, B, C, D 노드 안쪽으로 연결된 연두색 노드는 두 개 이상의 논문에 공통적으로 나타난 공통어로, 이는 곧 논문 간의 연결성을 의미한다. 사각형 밖에서 단일한 노란색 노드와 연결된 하늘색 노드는 각 문헌에서 서로 겹치지 않았던 특수어에 해당하는 단어로 특정 논문에 한정된 관심사를 나타낸다.

먼저 공통어를 나타내는 연두색 노드를 살펴보면, 'security', 'data', 'crime',' device', information'과 같은 보안 관련 키워드가 중앙에 위치하여 두 개 이상의 A, B, C, D 노드와 연결되는 모습이 확인된다. 이는 공통어 분석 결과와 마찬가지로 대부분 문헌이 각종 장치의 저장매체에서 중요 데이터가 유출되는 위험을 식별했음을 나타낸다. 이 유형의 위험은 다수 문헌을 통해 위험이 비교적 명확하게 드러났으므로 중요도가 높고 해결이 시급하다고 볼 수 있다. 문헌 A 와 관련된 특수어를 살펴보면 반도체를 뜻하는 'semiconductor'와 역공학(reverse engineering)이 실질 형태소로 분리된 형태인 'reverse'와 'engineering'을 확인할 수 있다. 이를 통해 문헌 A 는 반도체 집적회로 역공학 위험을 상당한 비중으로 다루었다는 사실을 가시적으로 확인할 수 있다. 다른 문헌에서는 해당 위험을 다루지 않았거나, 낮은 비중으로 다루었기 때문에, 반도체 집적회로 역공학 위험을 명확하게 식별하고 선제적으로 대응하기 위해서는 추가 연구가 필요함을 시사한다.

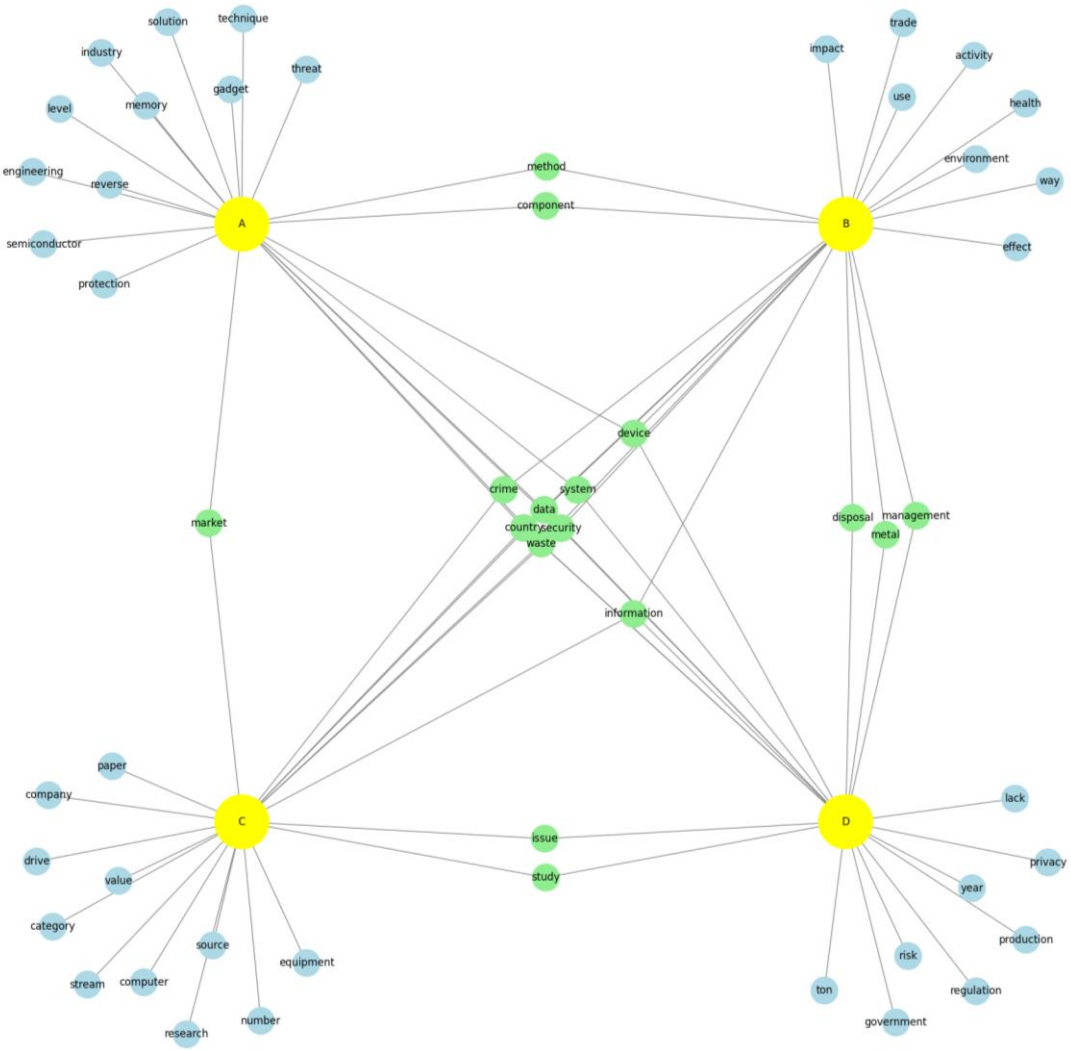

Figure 2. Keyword network graph
그림 2. 단어 연결망 그래프

3.4 국가보안지침 내 전자폐기물 처리 관련 규정 분석

마지막으로 전자폐기물 처리 관련 규정 분석을 위한 국가보안지침 관련 문헌은 「산업기술보호지침」, 「방위산업기술 보호지침」, 「국가 정보보안 기본지침」을 선정했다. 「산업기술보호지침」은 「산업기술의 유출방지 및 보호에 관한 법률」과 시행령에 따라 국가핵심기술 등 산업기술을 보호하기 위해 제정된 지침이며, 「방위산업기술 보호지침」은 「방위산업기술 보호법」과 시행령에 따라 방위산업기술 보호에 필요한 절차 등을 규정하기 위해 제정된 지침이다. 「국가 정보보안 기본지침」은 국가정보원이 관리하는 정부기관 등 각급 기관을 대상으로 정보보안 기본업무를 규정한 지침이다. 이들 지침에 대한 문헌 분석을 통해 전자폐기물 보안 처리 관련 규정의 존재 여부를 확인하고 그 문제점을 파악했다.

「산업기술보호지침」 제 3 장은 국가핵심기술의 보호조치를 규정하고 있다. 이에는 보호구역 설정, 인력관리, 접근통제 및 권한 관리, 보안관리 규정 제정, 통신수단 보안 등과 관련된 세부 조항이 포함되어 있다. 국가핵심기술에 해당하는 중요 자산 파기와 관련한 내용은 '제 13 조 국가핵심기술 관련정보 처리 과정 · 결과 자료 보호'에서 일부 확인된다. 하지만 국가핵심기술 정보의 생성부터 파기까지 보호등급에 따른 보안관리 의무를 규정할 뿐, 별도의 전자폐기물을 포함한 자산의 파기 절차와 방법을 규정한 구체적 요구사항은 확인되지 않는다.

그 밖에도 산업기술에 대한 침해신고와 대응, 복구에 관하여 규정한 「산업기술보호지침」 제 6 장에서 중요자산의 파기와 관련한 내용이 추가적으로 확인된다. 제 35 조제 2 항제 5 호는 국가핵심기술 백업매체를 폐기할 경우 폐기기준을 수립하고 기준에 부합한 절차를 준수하도록 하고 있다. 해당 조항은 자산의 파기와 관련한 관리적 요구사항을 제시하고 있지만, 구체적 범위가 백업매체에 한정되어 일반적인 전자폐기물 보안 관리를 요구하는 조항으로 보기에는 한계가 있다.

「방위산업기술 보호지침」 '제 5 장 정보보호'의 하위 항목인 '제 31 조 정보통신기기 및 저장매체 관리'를 전자폐기물 보안 유관 조문으로 볼 수 있다. 그 중 제 1 항제 4 호에는 '정보통신망에 접속하여 사용한 정보통신기기 및 저장매체는 외부에 반출되어서는 안 되며, 부득이한 경우 기술보호 전담부서 감독아래 완전포맷 등 전산자료를 삭제한 후 반출'이라는 규정이 존재한다. 해당 규정은 저장매체에서 중요정보가 유출되는 것을 방지할 수 있는 기술적 대책을 요구하나, 자산의 폐기가 아닌 반출 상황을 전제하므로 전자폐기물 보안과 직접적으로 관련된 조항으로 보기는 어렵다.

「국가 정보보안 기본지침」은 '제 61 조 저장매체 불용처리'를 통해 폐기물로 처리할 저장매체에 대해 다른 지침보다 세부적인 데이터 파기 통제를 요구하고 있다. 저장된 자료가 유출되지 않도록 자료 삭제 등 보안조치를 요구할 뿐만 아니라 비밀 및 대외비나 암호화키가 저장된 저장매체는 소각, 파쇄, 용해 등 물리적 방법으로 완전 파기하도록 요구한다. 그 밖의 불용처리 관련 사항은 국가정보원장이 배포하는 「정보시스템 저장매체 불용처리지침」을 준수하도록 하고 있다.

정리하자면 「산업기술보호지침」과 「방위산업기술 보호지침」은 전자폐기물 보안 처리 관련 규정이 다소 미흡한 것으로 확인된다. 그러나 국가핵심기술에는 반도체 기술이 다수 포함되어 있어 역공학을 통한 기술유출이 가능하고, 그 밖에 다른 국가핵심기술과 방위산업기술도 그들이 저장되었던 저장매체에 대한 포렌식으로 유출될 수 있다. 따라서 중요 산업기술과 관련된 전자폐기물은 보안 처리 필요성이 높아 관련 규정을 강화할 시급성이 있다고 볼 수 있다.

「국가 정보보안 기본지침」의 경우 저장매체에 대한 기술적 보안 처리를 요구하는 규정이 확인되고 있다. 하지만 실질적으로 이러한 매체가 파기되었다는 것을 검증하는 방법은 현재 보안 서약서와 증명서의 발급을 통해 이루어지고 있다. 이러한 규정의 존재만으로는 실제 보안 폐기가 이루어 지지 않아 보안 위험이 발생하는 것을 제대로 통제하기 어렵다. 전자폐기물이 물리적 · 화학적 방법을 통해 파괴되는 것을 실질적으로 검증하기 위한 모니터링과 같은 절차가 포함된 관리체계를 설계해야 하며, 이를 「산업기술보호지침」을 포함한 각종 국가보안 관련 지침에 반영할 필요가 있다.

IV. 결론

전자폐기물 발생량이 계속해서 증가함에도 전자폐기물 보안에 관한 논의가 여전히 제대로 이루어지지 못하고 있다는 문제의식 속에서, 본 연구는 보안관점의 전자폐기물 처리동향을 실증적으로 분석하고자 하였다. 먼저 연도별 전자폐기물 관련 문헌 및 언론보도 추이 분석결과, 전자폐기물에 대한 국내의 학술적 관심도가 매해 증가추세를 보이는 해외와 달리 상당히 부족하며 절대적 기준으로도 매우 낮은 것으로 밝혀졌다. 다음으로 전자폐기물 보안 관련 문헌 연관어 분석결과, 저장매체 중요 데이터 유출 위험이 모든 문헌에서 공통적으로 식별한 주요 위험으로 분석되어 빠른 대책마련이 필요할 것으로 파악되었다. 그 밖에 문헌 A 에서 확인된 반도체 집적회로 역공학 위험은 다른 문헌에서 잘 파악되지 않아 추가 연구가 필요한 위험으로 확인되었다. 마지막으로 국가보안지침 내 전자폐기물 처리 관련 규정 분석결과 전자폐기물 보안 처리와 관련한 규정이 명확하게는 존재하지 않거나 존재하더라도 실효성을 담보하기 어려운 수준으로 확인되어 관련 대책을 마련할 필요가 있을 것으로 보인다.

본 연구의 의의는 국내에서 거의 처음으로 전자폐기물을 보안관점에서 다루었다는 점과 다차원적인 분석을 통해 전자폐기물 보안 동향에 관한 다양한 통찰을 제공했다는 점에 있다.

하지만 전자폐기물 보안 관련 문헌 연관어 분석 과정에서 전자폐기물 보안 위험을 식별한 문헌이 적었던 나머지, 주제에 맞도록 수집이 가능했던 네 개의 문헌만을 분석한 결과로 충분한 타당성을 확보하지 못한 한계가 있다. 향후 전자폐기물 보안에 관한 관심도가 높아져 관련 연구가 다수 진행된다면, 더 다양한 문헌을 분석하여 이 같은 한계를 극복할 수 있을 것으로 보인다. 보안관점의 전자폐기물 처리동향을 파악하고 문제점을 식별했음으로, 이후에는 전자폐기물 보안 위험을 통제하기 위한 실효성 있는 관리적 보안 대책을 설계하는 후속 연구를 진행하고자 한다.

V. 감사의 글

이 논문은 2021 년도 중앙대학교 CAU GRS 지원에 의하여 작성되었음.

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

VI. 참고문헌

[1] N. Kapoor, P. Sulke, A. Badiye, “E-waste forensics: An overview,” Forensic Sci. Int.: Animals and Environments, Vol. 1, 2021.

[2] C. P. Baldé, E. D’Angelo, V. Luda, O. Deubzer, R. Kuehr, “Global Transboundary E-waste Flows Monitor - 2022,” United Nations Institute for Training and Research (UNITAR), 2022.

[3] S. Seo, "Policy Tasks for Transition to a Resource-Circulating Society: Focusing on the Implications of the Japanese Case," Journal of Budget and Policy, Vol. 4, No. 1, pp. 181-213, May 2015.

[4] European Parliament and Council, “Directive 2012/19/EU on waste electrical and electronic equipment (WEEE),” Official Journal of the European Union, July, 2012.

[5] S. A. Patil, N. M. Sharma, “Electronic waste – a literature review,” Int. J. Sci. Res., Vol. 4, No. 4, pp. 1622–1624, 2015.

[6] R. Torrance and D. James, "The State-of-the-Art in IC Reverse Engineering," in Proc. of the International Workshop on Cryptographic Hardware and Embedded Systems, 2009, pp. 363–381.

[7] P. Roychowdhury, J. M. Alghazo, B. Debnath, S. Chatterjee, and O. K. M. Ouda, "Security Threat Analysis and Prevention Techniques in Electronic Waste," in Proc. of the Sixth International Conference on Solid Waste Management 2016(6th IconSWM 2016), Kolkata, 2019, pp. 853–866.

[8] K. Hartwig, "Digital Waste and Cyber Crime," 2016.

[9] Y. J. Choi, J. W. Byun, J. W. Moon, H. B. Chang, "Exploratory Study on the Application of Blockchain for ESG Management in the Distribution Industry," Knowledge Management Research, Vol. 24, No. 3, pp. 217-237, Sep. 2023.

[10] J. Alghazo, O. K. M. Ouda, A. E. Hassan, "E-waste environmental and information security threat: GCC countries vulnerabilities," Euro-Mediterranean Journal for Environmental Integration, Vol. 3, Article No. 13, January, 2018.

Authors

이주노 (*Juno Lee*)

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

관심분야 : 산업보안, 국가핵심기술, 보안관리체계, 전자폐기물

한유나 (*Yuna Han*)

2014 년~2019 년 8 월 숙명여자대학교 한국어문학부 (학사, 복: 컴퓨터과학부)
2019 년~2021 년 8 월 중앙대학교 일반대학원 컴퓨터공학과 (석사)
2022 년~현재 중앙대학교 일반대학원 융합보안학과 산업보안기술전공 (박사과정)

관심분야 : 인공지능, 산업보안기술, 내부자 위협, 프라이버시, 정보 등급화

최예지 (*Yeji Choi*)

2018 년~2022 년 중앙대학교 사회과학대학 사회학과 (학사)
2022 년~현재 중앙대학교 일반대학원 융합보안학과 산업보안기술전공 (석사과정)

관심분야 : 산업보안기술, 데이터사이언스, 개인정보보호, 전자폐기물

최유림 (*Yurim Choi*)

2015 년~2019 년 성신여자대학교 사회과학대학 융합보안학과 (학사)
2019 년~2021 년 중앙대학교 일반대학원 융합보안학과 산업보안전공 (석사)
2021 년~현재 중앙대학교 일반대학원 융합보안학과 산업보안전공 (박사과정)

관심분야 : 산업보안, 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, 전자폐기물