https://doi.org/10.33778/kcsa.2019.19.2.003

기술유출행위 군집화를 위한 탐색적 연구

김 재 수*, 김 자 원*, 김 정 욱*, 최 유 림*, 장 항 배**

요 약

지속적으로 발생하는 기술 유출 사고에 대응하기 위하여 다양한 보안대책이 시행되고 있으나, 대부분의 보안 대책은 내·외부 사이의 경계선을 보안하는데 초점이 맞추어져 있다. 이는 외부로부터 발생하는 공격을 탐지하고 대응하기에 효과적이지만, 내부에서 발생하는 보안 사고에 취약한 실정이다. 본 연구에서는 효과적인 내부유출방지를 위해 사용자 행위정보 중 기술유출 행위에 해당하는 행위를 식별하고 기술유출 행위 탐지 항목을 설계하였다. 설계 방법으로는 선행연구 기반의 기존 기술유출 탐지 방법들을 분석하고, 기술유출 사고·사례를 기술유출 행위 관점에서 분석하여 기술유출 행위로 식별 가능한 탐지 항목들을 도출하였다. 도출한 기술유출 행위 탐지 항목은 통계적 검증을 통해 적합·타당성, 신뢰성을 모두 확보하였으며, 항목 간 상관분석을 통해 항목 간 연관 정도를 확인하였다. 본 연구의 결과물을 통하여 향후 선행연구와 유출경험 사고·사례 기반의 기술유출 시나리오 설계에 기반이 될 수 있을 것으로 기대된다.

An Exploratory Study for Clustering of Technology Leakage Activities

Jaesoo Kim*, Jawon Kim*, Jeongwook Kim*, Yurim Choi*, Hangbae Chang**

ABSTRACT

Most of security countermeasures have been implemented to cope with continuous increase leakage of technology, but almost security countermeasures are focused on securing the boundary between inside and outside. This is effective for detecting and responding to attacks from the outside, but it is vulnerable to internal security incidents. In order to prevent internal leakage effectively, this study identifies activities corresponding to technology leakage activities and designes technology leakage activity detection items. As a design method, we analyzed the existing technology leakage detection methods based on the previous research and analyzed the technology leakage cases from the viewpoint of technology leakage activities. Through the statistical analysis, the items of detection of the technology leakage outcomes were verified to be appropriate, valid and reliable. Based on the results of this study, it is expected that it will be a basis for designing the technology leaking scenarios based on future research and leaking experiences.

Keywords : Insider Threat, Technology Leakage, Technology Leakage Detection

접수일(2019년 6월 19일), 게재확정일(2019년 6월 29일)

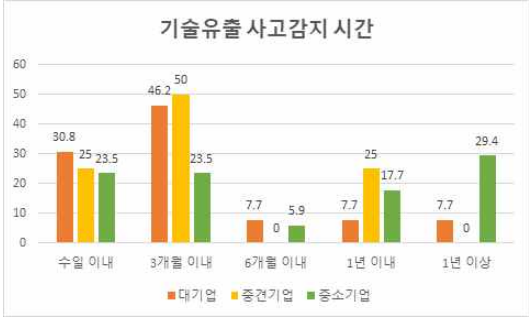
* 중앙대학교 일반대학원 융합보안학과
** 중앙대학교 산업보안학과(교신저자)

1. 서 론

오늘날 지속해서 발생하는 산업기술 유출 사고에 대응하기 위해 다양한 보안대책이 시행되고 있으나, 현재 대부분의 보안 대책은 내부와 외부 사이의 경계선을 보안하는 데에 초점이 맞춰져 있다. 이는 외부로부터 발생하는 보안 위험에 대응하기 위한 보안대책으로, 내부로부터 발생하는 보안 위험에 대응하는 데에 한계가 존재한다.

내·외부 경계선을 보안하는 기존의 단편적 보안 방법으로는 인력매수, 저작권 침해, 사회 공학적 공격 등 사람에 의해 발생하는 보안 위험에 자유로울 수 없으며, 발생한 보안 사고에 대응하는 것 또한 어려움을 겪고 있다.

내부로부터 발생하는 보안 위험은 조직구성원에 의해 발생하는 보안사고가 대부분으로 이는 사람에 의해 발생하는 특성으로, 보안사고 발생 자체에 대한 감지가 어려운 문제점이 있다. 실제로 중소벤처기업부[1]의 자료에 따르면 (그림 1)과 같이 기술 유출 사고감지 시간을 조사한 결과 중소기업의 경우 기술 유출 사고감지에 1년 이상의 시간이 걸리는 조직이 29.4%에 해당하는 높은 수치를 보임을 알 수 있다.



(그림 1) 기술유출 사고 감지 시간

내부로부터 발생하는 보안 위험은 조직구성원에 의해 발생하는 보안사고가 대부분으로 이는 사람에 의해 발생하는 특성으로,

내부에서 발생하는 융·복합적 보안 위험에 대비하기 위해서는 다차원적인 보안 활동이 필요하다. 더불어 보안사고 발생 이후 빠르게 복구 가능한 면역회복력을 지닌 보안대책을 수립해야 한다.

따라서, 본 연구에서는 기술 보호 관점의 기술 유출 행위 탐지 항목을 설계하기 위해 기술 유출 가능성이 높은 사용자 행위정보를 시간적 업무 흐름에 따라 재정리하고, 이를 기반으로 기술유출 탐지 항목을 설계하고자 한다.

이는 곧 기존의 기술 유출행위에 대한 잘못된 탐지 비율을 최소화하고, 확실히 위험도가 높은 기술 유출행위를 추출할 수 있는 긍정적 효과가 있을 것으로 기대되며 향후 빅데이터 기반의 기술 유출징후 탐지 연구 수행에 있어 활용 가능한 기술 유출 학습 데이터 마련이 가능할 것으로 기대된다.

2. 이론적 배경과 관련 연구

2.1 내부자 기술유출 행위 탐지 방법

전통적인 기술유출 방지 기술은 DLP(Data Loss Prevention), SCM(Secure Content Management), OCC(Outbound Content Compliance), ILD&P(Information Leakage Detection and Prevention) 등이 있으며, 조직 내에서 사용되어지는 다양한 중요 정보들을 관리하는 솔루션들이 해결책으로 제시되고 있다.

하지만, 기술유출 행위 탐지를 위해 사용되는 시나리오 및 항목들이 단편적으로 정해져있어 실제 탐지에 있어 오·과탐 비율이 굉장히 높은 수준을 차지한다. 이와 같이 발생하는 오·과탐은 조직 내 보안 담당자의 업무 가중을 불러올 뿐만 아니라, 솔루션의 신뢰성과도 직결되어 있는 문제점으로 오·과탐율을 줄이고자 다양한 연구가 활발히 진행되어 왔다.

하동욱[2]의 연구에서는 기계 학습 기반 내부자 위협 탐지 기술에 대해 언급하였으며, 세부적으로 업무 로그에 의한 RNN 기계 학습을 통하여 데이터를 수집하고 클러스터 군집분석을 활용하여 내부자 위협을 탐지하는 시스템을 개발하였다.

김현수[3]의 연구에서는 내부자 정보유출 탐지 방법을 도출하였으며, 널리 알려진 일련의 순차적 성질을 내포하고 있는 데이터를 다루는 문제에 적용 가능한 HMM 모델을 기반으로 비정상 절차에 대한 탐지 방안을 제안하였다. 조직에서 운영 중인 보안시스템(메일 보안시스템, 보안 USB, 문서 보안 시스템 등)을 활용하여 18가지 특징을 추출하고 비정상 행위에 대한 정형화를 수행하였다. 정의된 시스템 외 조직구성원의 활동에 대한 분석은 고려하지 않고 있으며, 보안시스템에만 한정된 행위 분석을 수행하였다.

김송영[4]의 연구에서는 빅 데이터를 이용한 보안정책 개선을 제안하였으며, 네트워크 보안, 서버 보안, 응용 보안, PC 보안시스템 등으로부터 원시데이터를 수집하여, 기하급수적으로 증가하는 대용량 로그를 통합하고 조직 구성원의 행위를 분석하여 클러스터링을 통한 패턴을 군집화함으로써 보안 모니터링에 활용할 수 있는 방안을 제시하였다. 실증 데이터나 기술유출 사례에 대한 직접적인 적용이 아닌 제안자가 설정한 Rule 기반의 가상 유출 시나리오를 설계하고 특징을 분석하였다.

대부분의 선행연구에서는 조직 구성원의 사용자 행위정보를 기반으로 이상징후를 추출하여 기술유출 행위 탐지를 수행하고자 하였으며, 빅데이터 기반의 사용자 행위 분석 내용이 주를 이루었다. 하지만, 사용자 행위를 분석함에 있어 체계적인 기술유출 탐지 항목, 시나리오를 설계하지 못한 한계점이 존재하였다.

따라서, 본 연구에서는 선행연구 분석과 기술유출 사고·사례를 기반으로 체계적인 기술유출 행위 탐지 항목을 설계하고자 한다.

2.2 기술유출 사고·사례 선행연구

기술유출 행위 사고·사례는 크게 이론적 지식과 유출경험 사례로 나누어 분석할 수 있다. 이론적 지식의 경우, 범죄심리학을 기반으로 한 기술유출 행위, 징후에 대한 연구 내용이 주를 이루고 있고, 유출경험 사례의 경우, 보안 학문이 응용학문인 특성 상 다양한 사례를 기반으로 한 기술유출 행위 및 징후를 확인할 수 있다. 따라서, 본 연구에서는 한국산업보안연구학회[5]의 자료를 통해 산업기술유출 주요 사건과 판례를 기술유출 행위 관점에서 분석하였다. 총 25건의 기술유출 사고·사례를 참고하였으며, 주요 내용으로는 “중요문서(파일)을 대상으로 이메일 유출, 출력 유출, USB 등 외부저장매체를 통한 유출”이 가장 중복적으로 발생하는 유출 행위로 나타났으며, “핵심인력을 통한 유출”의 경우, 이직, 퇴사 이후, M&A 등을 통한 유출 행위가 가장 중복적으로 발생하는 유출 행위로 분석되었다. 또한 판례에서는 24건의 기술유출 판례를 참고하였으며, 주요 내용으로는 “조직 사내망에 불법접속을 통한 기술유출”이 이루어진 점과 “타인의 계정정보로 불법접근”을 통한 기술유출 판례가 특징적이었다고 할 수 있다.

노재철[6]의 연구에서는 기술유출의 일반적 형태를 조사하고, 기술유출 방법에 대해 조사 분석을 진행하였다. 기술유출의 주된 형태를 4가지로 분류하였으며, 기술유출 방법에 대해 분류하고, 조사를 통해 빈번하게 발생되는 기술유출 방법의 비율을 확인하였다. 기술유출 방법은 ‘복사 및 절취’(42.1%)와 ‘핵심인력 스카우트 또는 매수’(36.0%)가 높게 나타나고 있으며, 다음으로 휴대용저장장치(USB, 외장하드 등), E-mail(26.4%), 위장거래, 위수탁거래(합작사업, 공동연구 등)(25.2%), 컴퓨터 해킹(11.7%), 관계자 매수(10.7%) 등의 순으로 나타났다. 조호대[7]의 연구에서는 기술유출 사례 분석을 통한 효과적 산업보호 방안에 대해 제언하였으며, 세부적으로 기술유출의 경로 및 특징을 5가지로 분류하고 대표적인 기술유출 사례를 심도있게 분석하였다. 분석한 선행연구 내용을 기반으로 본 연구에서는 발생가능한는 주요 기술유출 행위를 업무 시간별로 나누어 정리하고, 이론적 지식으로 검증된 기술유출 탐지 항목과 유출경험 사례를 통해 분석된 기술유출 탐지 항목의 공유정도가 높은 항목들을 재정리하고, 통계적 검증을 통해 이론적 지식과 유출경험 사례가 반영된 체계적인 기술유출 행위 탐지 항목을 설계하고자 한다.

3. 연구방법론과 설계

3.1 연구추진 체계

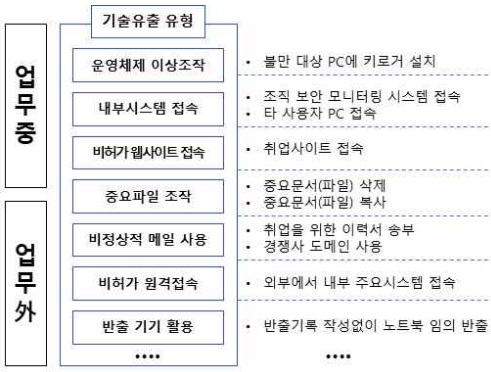
이론적 지식과 유출경험 사례가 반영된 체계적인 기술유출 탐지 항목 설계를 위한 연구방법론은 다음 (그림 2)와 같다.

먼저, 선행연구 조사 및 분석을 통하여 기술유출 행위 탐지 방법을 분석하였다. 또한, 기술유출 행위 사고 사례를 조사하여 유출 위험 행위를 식별 및 구분하였다. 기술유출행위는 크게 출근 이전, 퇴근 이후에 해당하는 업무 외 시간과 업무 수행 시간으로 나누어 구분하였으며, 선행연구에 부합하는 공유 정도를 확인하였다.

다음으로, 선행연구 분석내용을 기반으로 기술유출 행위의 유형을 분류하여 기술유출 행위 항목을 설계하였다. 설계한 기술유출 행위 항목에 대해 타당성을 검증하고자, 업무 행위와 정보유출사고의 연관성에 대해 설문 조사를 시행하여 통계적 타당성을 검증하였다. 설문 조사는 기술유출 사고 경험이 있는 보안 담당자를 대상으로 진행하였고, 76명의 설문 유효 결과를 보였다. 통계적 타당성 검증을 위해 항목에 대한 적합·타당성, 크론바흐 알파 값을 통한 신뢰성 확보, 피어슨 상관계수 분석을 순차적으로 수행하여 통계적 타당성을 확보한 기술유출 행위 항목을 도출하였다.

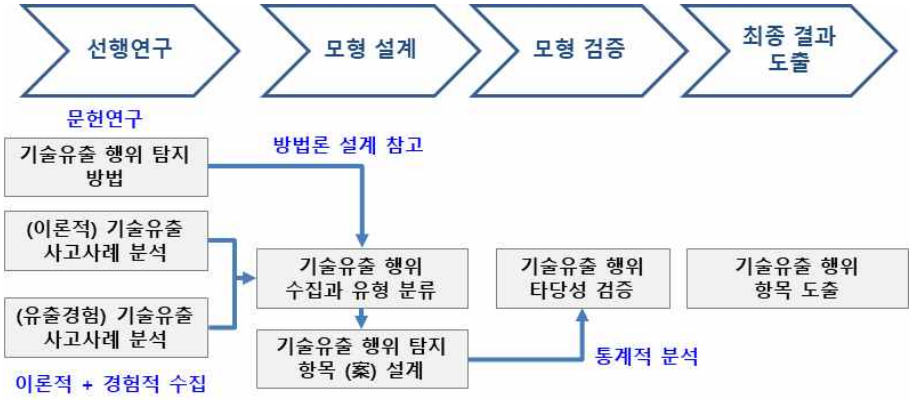
3.2 기술유출 행위 탐지 항목 설계

앞서 분석한 선행연구 내용을 중심으로 발생할 수 있는 주요 기술유출 행위를 아래 (그림 3)과 같이 정리하였다.



(그림 3) 기술유출 행위 탐지 항목 도출 과정

선행연구를 기반으로 기술유출 행위를 유형화하고 업무 시간에 따라 발생하는 기술유출 행위의 형태를 분석하였으며, 각각의 공유정도 또한 확인하였다. 선행연구와 공유 정도를 가장 많이 차지하는 항목은 “사외 메일을 통한 내부 직원에게 악의적 메일 발송” 세부항목과 “취업 사이트 접속” 세부항목이 참고한 10개의 선행연구 중 6개를 공유하고 있음을 확인하였다.



(그림 2) 연구추진체계

정리한 기술유출 행위의 선행연구 공유정도와 발생빈도 등을 고려해 <표 1>과 같이 6개 영역 25개 세부항목으로 정리하였다. 설계한 탐지 항목(案)에 대해 통계적 검증을 수행하고자 한다.

<표 1> 기술유출 행위 탐지 항목(案) 설계

기술유출 가능 행위	
조직 내 PC단말 조작(설치)를 통한 유출징후	운영체제 설정환경 변경(재설치)
	2. 내부IP주소 변경
	3. 보안프로그램 강제종료
	4. 불법 SW 설치(Key Logger)
중요문서의 조작을 통한 유출징후	5. 중요문서 암호화 해제
	6. 중요문서 워터마크 해제
	7. 중요문서 복사
	8. 중요문서 출력
	9. 중요문서 파일명 변경
	10. 중요문서 확장자 변경
	11. 중요문서 삭제
외부로부터 접속을 통한 유출징후	12. 허가되지 않은 외부에서 내부서버 접속(VPN/FTP)
전자메일을 통한 유출징후	13. 외부(상용) 메신저 사용
	14. 다른 사용자 컴퓨터에서 전자메일 송부
	15. 메일내용 중 중요단어 사용
	16. 중요파일 첨부
	17. 기준크기 이상의 파일전송
	18. 파일을 분할하여 첨부
	19. 외부메일을 통해 내부직원에게 악의적 메일 발송
불법접속을 통한 유출징후	20. 비허가 사이트 (정보교환 사이트 등) 접속
	21. 외부 저장공간(사이트) 접속
	22. 외부 취업사이트 접속
저장매체를 통한 유출징후	23. 허가되지 않은 이동형 저장장치(USB/HDD) 연결
	24. 스마트폰을 저장장치로 연결
	25. 기기(노트북/저장장치)임의 반출

4. 통계적 검증

4.1 적합·타당성 및 신뢰도 검증

선행연구를 분석한 내용을 바탕으로 도출한 기술유출 행위 탐지 항목에 대한 설문 조사를 기술유출 사고 경험이 있는 보안 전문가 76명을 대상으로 실시하였다. <표 2>는 설문 조사로 얻은 결과를 가지고 각 세부 항목에 대하여 적합·타당성을 검증한 결과 및 평균을 기준으로 각 항목에 대한 우선순위를 정하였다.

<표 2> 적합·타당성 검증 결과

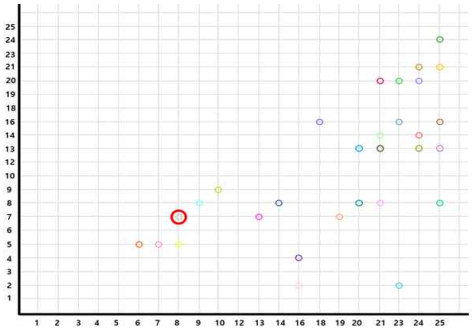
기술유출 가능 행위	평균(점)	우선순위
1. 운영체제 설정환경 변경(재설치)	4.00	15
2. 내부IP주소 변경	3.70	19
3. 보안프로그램 강제종료	4.53	4
4. 불법 SW 설치(Key Logger)	4.59	3
5. 중요문서 암호화 해제	4.21	10
6. 중요문서 워터마크 해제	3.71	18
7. 중요문서 복사	4.03	14
8. 중요문서 출력	3.88	16
9. 중요문서 파일명 변경	3.76	17
10. 중요문서 확장자 변경	4.30	8
11. 중요문서 삭제	3.09	-(기각)
12. 허가되지 않은 외부에서 내부서버 접속(VPN/FTP)	4.68	1
13. 외부(상용) 메신저 사용	4.39	7
14. 다른 사용자 컴퓨터에서 전자메일 송부	3.70	19
15. 메일내용 중 중요단어 사용	3.49	-(기각)
16. 중요파일 첨부	4.14	11
17. 기준크기 이상의 파일전송	3.43	-(기각)
18. 파일을 분할하여 첨부	3.59	21
19. 외부메일을 통해 내부직원에게 악의적 메일 발송	4.63	2
20. 비허가 사이트 (정보교환 사이트 등) 접속	4.12	12
21. 외부 저장공간(사이트) 접속	4.47	6
22. 외부 취업사이트 접속	3.07	-(기각)
23. 허가되지 않은 이동형 저장장치(USB/HDD) 연결	4.49	5
24. 스마트폰을 저장장치로 연결	4.09	13
25. 기기(노트북/저장장치)임의 반출	4.22	9

각 세부항목의 평균값(기준 타당성)은 3.5를 기준으로 하여 항목의 적합함을 구분하였다. 이에 따라 4가지 항목이 제외되고, 적합·타당성 검증 기준을 만족한 세부항목은 총 21개로 도출하였다. 또한, 신뢰도 확인을 위한 크론바흐 알파 값을 구한 결과 0.893으로 신뢰도가 높게 나타난 것을 확인하였다.

4.2 상관분석을 통한 항목 간 연관관계 분석

적합·타당성과 신뢰성을 확보한 항목에 한하여, 상관분석을 수행하고 변수 간에 어떠한 선형적 관계를 갖고 있는지 분석하였다. 피어슨 상관계수 분석 방법을 통해 분석을 진행하였으며, 통상적으로 분석 결과 값이 0.4이상이면 상관관계가 다소 높다고 판단되어진다.

일반적으로 상관분석은 독립변수와 종속변수 간의 연관성을 분석하지만, 본 연구에서는 기술유출 행위 항목 간의 연관성을 분석하기 위해 사용하였다.



X-Y(항목 번호)	표시	값	X-Y(항목 번호)	표시	값
9-8		.4	25-21		.476
16-2		.4	21-20		.482
20-13		.404	25-8		.485
21-14		.409	24-14		.486
19-7		.411	14-8		.488
18-16		.412	24-13		.492
25-16		.412	21-8		.5
20-8		.419	24-20		.503
13-7		.429	8-5		.506
23-20		.429	7-5		.521
23-2		.446	23-16		.537
24-21		.447	6-5		.578
21-13		.457	10-9		.593
16-4		.458	25-13		.599
25-14		.473	8-7		.746

(그림 4) 상관분석 결과

따라서, (그림 4)에서 나타내는 상관관계의 선형 그래프 X, Y축 모두 기술유출 행위 항목을 나타내며, 각 항목 간 0.4 이상의 상관계수와 0.01 수준의 유의확률을 모두 충족하는 상관계수를 나타낸다.

분석결과 “7. 중요문서 복사” 항목과 “8. 중요문서 출력 항목” 간의 연관성이 .746으로 가장 높게 나타남을 확인하였으며, 이러한 상관분석 결과를 기반으로 향후 기술유출 행위 항목을 기반으로 한 시나리오 설계에 큰 도움이 될 수 있을 것으로 기대된다.

5. 결론 및 향후연구

본 연구에서는 기술유출 행위 탐지 항목 설계를 위해 선행 문헌에 근거하여 시간적 흐름에 따른 기술유출 가능 행위를 식별하고 수집하였다. 또한, 선행연구 및 주요 기술유출 사고·사례 및 판례 등을 통하여 기술유출 행위의 유형을 식별하고 기술유출 행위 유형을 체계화 하였다. 도출한 기술유출 행위 항목을 기반으로 기술유출 사고 경험이 있는 보안 전문가를 대상으로 설문을 진행하였으며, 설문조사 결과에 대하여 적합·타당성, 신뢰계수, 상관분석을 수행하였다.

본 논문의 결과를 통하여 향후 기술유출 행위 탐지 항목 기반의 시나리오 설계 연구를 통해 오·과탐율을 최소화 할 수 있는 체계적인 시나리오 설계가 가능할 것으로 기대된다.

감사의 글

이 논문은 2019년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임(P000873, 2019년 산업전문인력역량강화사업)

참고문헌

[1] 중소벤처기업부, 대중소기업농어업협력재단, '2017년도 중소기업 기술보호 수준 실태조사 보고서', 2018

[2] 하동욱, 강기태, 류연승, "기계학습 기반 내부자 위협 탐지기술: RNN Autoencoder를 이용한 비정상행위 탐지", 정보보호학회논문지, 제27권, 제4호, pp. 763-773, 2017

[3] 김현수, "내부자 정보 유출 탐지 방법에 관한 연구", 한국인터넷방송통신학회논문지, 제17권, 제4호, pp. 11-17, 2017

[4] 김송영, 김요셉, 임종인, 이경호, "빅데이터를 이용한 보안정책 개선에 관한 연구", 정보보호학회논문지, 제23권, 제5호, pp. 969-976, 2013

[5] 한국산업보안연구학회, "산업보안백서", 2015

[6] 노재철, 고준기, "기술유출방지 및 보호지원에 관한 법률 제정에 관한 연구", 한국콘텐츠학회논문지, 제17권 7호 pp. 487-497, 2017

[7] 조호대, "기술유출 사례 분석을 통한 효과적 산업보호 방안", 한국경찰학회보, 제37권 pp. 335-354, 2012

[8] 이창훈, 하옥현, "기밀유출방지를 위한 융합보안 관리 체계", 융합보안논문지, 제10권 4호 pp. 61-67, 2010

[9] 공효순, 송은지, "빅 데이터를 이용한 호텔기업 CRM 및 보안에 관한 연구", 융합보안논문지, 제13권 4호 pp. 69-75, 2013

[10] 김석훈, 김은수, 송정길, "통합보안관리 시스템에서의 침입탐지 및 대응을 위한 보안 정책 모델에 관한 연구", 융합보안논문지, 제5권 2호 pp. 9-17, 2005

〔저자소개〕

김 재 수 (Jaesoo Kim)

2015년 3월 ~ 현재 중앙대학교
일반대학원 융합보안학 박사과정
email : sdkjs@cau.ac.kr

김 자 원 (Jawon Kim)

2018년 3월 ~ 현재 중앙대학교
일반대학원 융합보안학 박사과정
email : jjawon@cau.ac.kr

김 정 욱 (Jeongwook Kim)

2018년 9월 ~ 현재 중앙대학교
일반대학원 융합보안학 석사과정
email : seed@cau.ac.kr

최 유 림 (Yurim Choi)

2019년 3월 ~ 현재 중앙대학교
일반대학원 융합보안학 석사과정
email : julie330@cau.ac.kr

장 항 배 (Hangbae Chang)

2006년 2월 연세대학교
정보시스템관리 박사
2014년 3월 ~ 현재
중앙대학교 경영경제대학
산업보안학과 교수
email : hbchang@cau.ac.kr