

정보보호 텔러트 함양을 위한 역량 강화 로드맵

김 득 훈*, 꺾 진**

요 약

정보통신기술이 발전하면서 정보의 생성, 수집, 전송, 저장 및 삭제 등 정보주기를 갖는 업무처리가 네트워크 환경을 통해 이루어지고 있다. 이에 따라 정보 활용 시 고려할 사항 중 정보를 안전하게 보호하기 위한 정보보호가 중요한 학문으로 발전하고 있다. 최근에는 사물인터넷, 클라우드 컴퓨팅, 빅데이터 및 인공지능 등의 인터넷 기반 신기술과 다양한 정보통신기술이 융합되어 여러 산업에 적용되고 있다. 이는 신기술 적용 전의 개별 환경에서 존재하던 보안위협에 더불어, 적용 후의 융합환경에서 예상하기 어려운 보안위협까지 파생되어 발생할 수 있다. 따라서 앞으로 우리 삶의 질 향상을 위해, 다양한 환경에서 정보보호는 필연적으로 적용 및 발전될 것이다. 본 고에서는 인터넷 기반의 환경에서 발생하는 보안위협을 정보보호 관점으로 접근 및 대응할 수 있는 정보보호 텔러트를 함양하기 위한 역량 강화 로드맵을 분석하였다.

I. 서 론

인터넷 기반 신기술이 등장하고, 다양한 산업 분야에 적용됨에 따라 전 세계적으로 정보보호에 대한 중요성이 증가하고 있다. 이는 정보를 보호해야 하는 영역이 점차 많아지고 있음을 의미하며, 정보보호의 범주는 크게 물리적, 기술적, 관리적 보안으로 나뉘어지므로 해당 영역을 소수의 인원이 전부 보호하기에는 어려움이 따르기 때문이다. 이에 따라 정보보호 학문에서 세부 관심 연구에 따라 학·연·산을 인프라로 정보보호가 이루어지고 있다. 이때, 특정 분야를 선정하여 심도있게 연구하기 위한 로드맵으로 다양한 분야를 경험한 후 적합한 관심 분야로 나아가는 것이 중요하다.

우리 연구실의 연구분야는 사물인터넷, 클라우드, 핀테크 및 모바일 보안 등으로써 연구실명과 같이 다양한 분야에서의 정보보호응용및보증을 위해 노력하고 있다 [1]. 즉, 정보보호를 적용할 수 있는 모든 범주 내에 있는 분야에서의 정보보호 관점의 접근, 분석 및 결과 도출을 통해 경험을 축적해 나가는 정보보호 텔러트 역량을 중점으로 정보보호 연구를 수행하고 있다. 따라서, 정보보호 텔러트를 함양하기 위한 역량 강화 로드맵을 분석하려 한다. 본 고의 구성은 다음과 같다. 2장에서는 관심 연구로 선정하여 심도있게 연구하고 있는 분야에 관해 확인한다. 3장에서는 과거 및 현재 수행하는 프

젝트를 통해 정보보호 텔러트 역량을 강화한 로드맵에 대해 확인한다. 4장에서는 연구 성과를 확인하고, 5장에서 결론으로 본 고를 마무리한다.

II. 관심 연구

최근 관심을 갖고 연구하는 분야는 다양한 응용서비스 환경 중 의료 서비스 보안에 초점을 맞추고 있다. 의료 서비스 환경에서 발생 가능한 보안위협을 분석하고, 암호학 기반으로 상호 인증, 데이터 무결성 및 데이터 공유 등을 보증하기 위한 일련의 프로토콜을 설계한 후, 의료 서비스 환경에 맞춰 적용 및 안전성 검증을 수행한다. 이를 위해 다양한 의료 서비스 분야에서 두 가지 주제인 전자처방전 및 정밀의료 서비스 보안을 병렬적으로 연구하며, 거시적 관점에서 의료 서비스 통합 보안 프레임워크를 통해 안전성 향상을 최종목표로 연구 진행 중이다.

2.1. 안전한 전자처방전 관리 시스템 설계

전자처방전 시스템은 기존의 종이 처방전을 발급받고 약국에 방문하여 제시한 후 처방 약을 조제 받는 일련의 과정에서, 오프라인 종이 인쇄 없이 네트워크상에서 처방전을 교환하는 방식이다. 즉, 종이 처방전 방식

* 이주대학교 컴퓨터공학과 정보보호응용및보증연구실 (대학원생, kimdh1206@ajou.ac.kr)

** 이주대학교 사이버보안학과 (정교수, security@ajou.ac.kr)

은 처방전 불법 대리발급, 분실 및 관리 비용의 문제가 존재하였고, 이를 보완 및 대체하기 위해 전자처방전 시스템이 연구되고 있다. 그러나, 네트워크로 환경이 전환되면서 이에 수반되는 보안위협이 발생할 수 있다. 예시로 처방전에는 의료 서비스명 및 환자 관련 민감 정보가 포함되는데, 이와 같은 민감 정보를 네트워크를 통해 처리할 경우 해당 과정에서 정보유출, 변조 및 프라이버시 침해 등의 문제가 발생할 수 있다. 따라서, 전자처방전 시스템의 전주기적 관점에서 보안 취약지점을 분석하고 해당 구간에서 발생 가능한 보안위협에 대응하기 위한 안전한 전자처방전 관리 시스템을 설계 중이다. 해당 연구를 통해 전자처방전 시스템 및 데이터 공유에 대한 익명성, 안전성 등을 보장함에 따라 의료 서비스 보안 향상에 도움이 되고자 한다.

2.2. 정밀의료 시스템의 민감 정보 공유 스킴 설계

정밀의료 시스템은 개인의 유전정보, 질병정보, 생활 정보 등과 관련된 빅데이터가 여러 센서를 통해 수집 및 분석되고, 이를 통해 환자에게 적합한 최적의 치료 제공 및 질병 예방과 관리를 위한 의료 서비스를 제공한다 [2]. 이처럼 정밀의료 시스템은 기존의 의료 서비스와 다르게 인터넷 기반 신기술이 상호 연계된 집합체로 운영된다. 이때, 정밀의료에서 활용되는 개인의 민감 정보는 유출되거나 악용될 경우 파급 효과가 상대적으로 크다. 또한, 의료분야에서 생성되는 개인정보 및 의료정보의 경제적 가치와 의료기관을 대상으로 한 침해 위협이 지속적으로 증가하고, 민감 정보를 클라우드 환경에서 다룬다는 점에서 이용자들의 불안감이 증가하고 있다 [3]. 따라서, 정밀의료를 실현하기 위해 연구되는 다수의 분야 중 정보보호는 핵심 분야로 선정할 수 있으며, 정밀의료에 활용되는 민감 정보에 대한 안전한 공유 스킴이 필요하다는 것을 동기로 연구 수행 중이다 [4]. 해당 연구에서는 정밀의료 시스템에서 활용되는 민감 정보 [5]를 분석하고, 정밀의료 시스템에 참여하는 엔티티에 따라 민감 정보를 재구성하여 데이터 흐름을 도출하였다. 최종적으로 정밀의료 시스템에서 민감 정보를 안전하게 공유하기 위한 스킴을 암호학에 기반하여 설계하였고, 데이터 흐름에 따른 보안위협에 대응하기 위해 안전성을 분석하였다. 이를 통해 정밀의료 시스템에서의 엔티티 간 상호 인증, 민감 정보 무결성, 데이터 공유에 대한 안전성을 보장함에 따라 의료

서비스 보안 향상에 도움이 되고자 한다.

III. 연구 프로젝트

관심 연구와 함께 지도교수님의 총괄하에 다수의 정보보호 관련 프로젝트를 수행하였으며, 현재 수행하는 프로젝트도 존재한다. 이를 통해, 다양한 분야에서 정보보호를 위해 적용하는 접근방법, 기술 및 가이드 등의 넓은 시야를 확보하였고, 정보보호 텔러트에 대한 역량을 지속 강화하는 로드맵을 이어나갈 수 있다.

3.1. 현재 수행 프로젝트

2021년 3월 기준으로 정보보호 관련 수행 중인 프로젝트는 총 7건이며, 표 1과 같다.

수행 중인 프로젝트의 성향을 A,B 및 C로 구분하였다. A 성향의 프로젝트는 인터넷 기반 기술이 독립적이 아닌, 상호 연계적으로 다양한 기반시설 및 산업분야에 적용될 때, 기존의 환경보다 더욱 복잡하고 거대한 환경에서 발생하는 복합적 보안위협을 분석하고, 보안 오케스트레이션 제공 및 위협 대응 자동화를 목표로 수행 중이다. 이때 독립적으로 IT 자산 운용 시 발생하는 보

(표 1) 현재 수행 프로젝트 현황

구분	년도	프로젝트명 / 관리기관	성향
국연사	2021 ~	IoBE에서의 Blended Threat 대응을 위한 SOAR-CUBE 기술 개발 / 한국연구재단	A
	2019 ~	저작권 침해사이트의 생애주기 프로파일링 기술 개발 / 한국저작권위원회	B
용역	2021 ~	국내 발전소 환경에 적합한 SOAR 적용방안 연구 / 파이오링크	A
교내	2021 ~	SOAR를 활용한 IoBE 보안 기술 개발 / 아주대학교	A
	2020 ~	디지털 트랜스포메이션 사이버보안 기술 연구 / 아주대학교	C
	2019 ~	융합환경에 적용가능한 지능형 위협 대응 기술 / 아주대학교	A
	2018 ~	4차산업혁명 대비를 위한 사이버보안 기술 연구 / 아주대학교	A/C

안위협과 더불어, 융합된 환경의 사람-사물, 사물-사물 등이 상호 연결되어 발생하는 보안위협이 현재까지 분석 및 대응되고 있는 기존의 환경이라 정의할 수 있으며, 앞으로 다가오는 환경은 이러한 융합환경 간 연결에 의해 예상하기 어려운 복합적 보안위협까지 발생하는 거대한 환경까지 포함하고, 이를 IoBE (Internet of Blended Environment)로 정의하였다. 이와같이 IoBE에서는 기존의 환경에서 사용하는 정보보호 관점 및 기술을 무분별하게 적용할 경우 보안의 복잡성이 증대될 것이다. 따라서, IoBE에 적합하고 보안의 복잡성을 낮추기 위한 통합 보안 플랫폼을 연구함에 따라 IoBE에서 발생하는 복합적 보안위협에 선제적으로 대응하려 한다.

B 성향의 프로젝트는 정당한 저작권을 갖는 저작권자에게 합당한 이익을 보장하기 위해, 저작권법 및 저작물 유출방지 기술 등을 이용하여 불법 저작물 유통을 방지하고 있지만, 이를 회피하여 저작권 침해사이트가 지속적으로 생성 및 운영되고 있다. 이에 따라 발생하는 저작권 침해 피해를 감소시키기 위해 저작권 침해가 의심되는 다양한 사이트의 생애주기 및 특징을 프로파일링하여 이에 대한 탐지 및 대응 자동화를 목표로 수행 중이다. 데이터 사이언스 관점에서 정형 및 비정형 형태의 저작권 침해 의심 사이트에 대한 특징을 분석하고, 현재 저작권 침해 사이트에 수동으로 탐지 및 대응하고 있는 비효율적인 방식을 효율적으로 전환시키고자 한다. 특히, 데이터 사이언스는 정보보호를 위한 기초적인 이해 학문으로써 해당 성향의 프로젝트를 통해 정보보호를 위한 데이터의 범주 및 메커니즘에 대한 이해와 시야가 보다 넓어지는 계기가 되고 있다.

C 성향의 프로젝트는 4차산업혁명에 핵심 기술로 사용되는 사물인터넷, 클라우드 컴퓨팅, 빅데이터, 모바일, 블록체인 및 인공지능 기술 등에 대하여 정보보호 관점에서 활용 시 현재까지 나온 해당 기술의 문제를 보완하고, 효율적인 활용 및 기술의 발전 고도화를 목표로 수행 중이다. 특히, 비대면 환경으로 전환되고 있는 최근 이슈에 적합하게 다양하고 신속하게 파생되는 인터넷 기반 기술을 활용함에 있어 신뢰성을 향상하고자 한다.

이처럼 현재 수행 중인 프로젝트의 성향에 따라 접근 방법, 심도있는 기술 영역 분석 및 예상 결과가 서로 상이하므로, 이에 대한 정보보호 관점의 넓은 시야를 획득하여 정보보호 텔런트 역량을 높여 나아가고 있다.

3.2. 기 수행 프로젝트

2021년 3월 기준으로 정보보호 관련 기 수행한 프로젝트는 총 35건이며, 표 2와 같다.

[표 2] 기 수행 프로젝트 현황

구분	년도	프로젝트명 / 관리기관
국연사	2017 ~ 2020	신·변종의 모바일 위협 대응을 위한 지능형 악성코드 분석 기술 개발 / 한국연구재단
	2019	클라우드 기반 스마트기기 포렌식 연구 / 국가보안기술연구소
	2016 ~ 2019	지능정보기술을 활용한 금융서비스 보호 기술 연구 / 정보통신기술진흥센터
	2017 ~ 2018	IoT 보안기술연구 / 정보통신기술진흥센터
	2017	클라우드 자원 공동임차 위협 대응 및 사고대응 기술 연구 / 국가보안기술연구소
	2014 ~ 2017	IoT 환경에서의 통합 보안 프레임워크 기술 개발 / 한국연구재단
	2016	클라우드 가상머신 격리·분석 및 사고대응 기술 연구 / 국가보안기술연구소
	2015 ~ 2016	클라우드 보안 가시성 서비스 연구 / 국가보안기술연구소
	2013 ~ 2016	안드로이드 신규 취약점 탐지를 위한 모바일 소프트웨어보안 테스트 도구 개발 / 정보통신기술진흥센터
	2015	cPP 개발과 주요국 ICM/정보보호제품 도입정책 분석 / 국가보안기술연구소
	2012 ~ 2015	유무선 통합 환경에서의 안전한 클라우드 데이터센터 구축을 위한 지능정보안전관리 기술 개발 / 한국연구재단
	2013 ~ 2014	안전한 스마트워크 서비스 제공을 위한 보안 기술 개발 / 한국연구재단
	2013	홈페이지 점검 소요인력 산정방법 연구 / 국가보안기술연구소

구분	년도	프로젝트명 / 관리기관
국연사	2012 ~ 2013	제어시스템 보안설정 점검 방법 연구 / 국가보안기술연구소
	2012	모바일 환경 사이버공격 시나리오 및 대응 방안 연구 / 국가보안기술연구소
용역	2019	금융권 CISO 핸드북 발간 용역 / 금융보안포럼
	2017 ~ 2019	A Study on Intelligent Security Management Technology for Secure Workload Migration in Cloud Environment / Office of Naval Research
	2018	금융권 CISO 핸드북 발간 기초 조사 용역 / 금융보안포럼
	2018	기업의 클라우드 환경에서 가상화 환경 취약점 분석 기술 연구 / (주)윈스
	2017	기업 환경에서 IoT 센서 네트워크에 대한 인증 및 접근제어 기술 연구 / (주)윈스
	2017	Linux 암호처리 기능 안전성 분석용 역공학 도구 개발 / 한국전자통신연구원
	2016 ~ 2017	리눅스 기반 IoT 단말 응급 복구 솔루션 / (주)솔루세움
	2016 ~ 2017	차세대 ITS 보안 가이드 개발 / 한국인터넷진흥원
	2016	클라우드 가상화 환경에서 안전성 시험·이상행위 탐지 방안 연구 / 한국인터넷진흥원
	2016	MAC OSX 안전성 분석 도구 개발 / 한국전자통신연구원
	2015	전자정부 IoT 정보보호 전략 마련 관련 정책연구 / 행정자치부
	2015	Cloud UI 시스템에 대한 보안 취약점 및 보안성 평가 / 알티캐스트
	2014	빅데이터 기반 교육(행정)기관 보안관계 방안 연구
	2014	국내·외 CPS 보안정책 및 산업 실태조사 / 한국인터넷진흥원
	교내	2018 ~ 2019

구분	년도	프로젝트명 / 관리기관
교내	2018 ~ 2019	클라우드 서비스 인증 프로토콜 분석 및 위협 탐지 모델 연구 / 아주대학교
	2017 ~ 2018	모바일 위협 대응을 위한 악성코드 분석 모델 연구 / 아주대학교
	2016 ~ 2017	클라우드 환경에서 안전한 워크로드 마이그레이션을 위한 악성 가상머신 및 지능형 신변종 악성코드 탐지를 위한 연구 / 아주대학교
	2016 ~ 2017	클라우드 환경에서의 비인가 트래픽 차단 기술 연구 / 아주대학교
	2015 ~ 2016	IoT 환경에서의 디바이스(단말·센서) 보안 기술 연구 / 아주대학교

기 수행한 프로젝트는 성향에 따른 분석보다는 거시적 관점에서 특정 환경의 가이드라인, 도구 개발, 하드웨어 장치 포렌식, 정보보호제품 평가 방식, 다수의 정보보호인파 국내·외 공동 연구 및 해답을 도출하기 어려운 문제에 대한 접근 방법 등 일방향적 로드맵이 아닌 다방향적 로드맵에 따라 정보보호 텔러트 역량 강화를 수행하였다.

IV. 연구 성과

정보보호 학문을 시작한 이후 국내의 저널 5편, 학술대회 31편, 지식재산권 24건, 수상 10건의 연구 성과를 얻었다.

관심 연구 주제를 Q1에 속한 저널에 출판하였으며, 창의연구학회 주관 하에 Best Paper Award를 수상하였다. 또한, 금융보안연구원 주관 하에 진행된 금융정보보호 공모전, 국가보안기술연구소 주관 하에 진행된 경량·고속 블록암호 LEA 구현 및 고속해시함수 LSH 구현 경진대회 등 다양한 분야의 공모전과 우수신진연구자 한국인터넷진흥원 원장상 및 한국정보보호학회 젊은 정보보호인 30인의 수상 성과를 얻었으며, 향후에도 계속 정보보호 텔러트 역량을 강화하여 성과를 도출하려 한다.

V. 결 론

학사 및 석사 학위는 인터넷 기반 특정 기술을 주 관

심 연구로 수행하였고, 박사과정을 진행하면서 응용서비스 환경 중 의료 서비스 보안을 주 관심 연구로 수행하고 있다. 향후 지도교수님 지도 하에 박사 학위 취득 후 응용서비스 통합 보안 프레임워크에 대한 연구를 지속해나갈 것이다. 최근에는 비대면 이슈로 폐쇄적인 성향을 갖는 기반시설도 다소 개방적으로 변화하고 있다. 즉, 우리 삶의 편리함은 증가할 수 있지만, 이에 대한 정보보호 방안이 적절하게 적용되어야 실현 가능하므로, 트렌드에 맞춰 정보보호 관점으로 대응할 수 있는 역량을 갖추어나가기 위해 노력할 것이다.

본 고에서는 정보보호인으로서 갖추어나간 정보보호 텔런트 역량 강화를 위한 로드맵을 분석하였다. 그러나, 정보보호라는 학문에 있어 본인이 그려가는 로드맵에 정해진 방향은 없을 것이다. 즉, 정보보호를 선구하신 분의 가르침에 따라 정보보호라는 매력적인 학문을 전공하고 있는 모든 정보보호인이 한 가지 또는 그 이상의 정보보호 텔런트를 함양하고 나아간다면 정보보호의 발전에 도움이 되는 인재가 될 것이다.

참 고 문 헌

- [1] 정보보호응용및보증연구실, “<http://isaa.re.kr/>”
- [2] 문세영, 장기정, 김한해, “정밀의료의 성공 전략”, *Korea Institute of S&T Evaluation and Planning(KISTEP)*, 15, pp. 14-32, Aug 2016.
- [3] 한근희, “의료 데이터의 개인정보보호 이슈 및 전망”, *한국인터넷진흥원*, 11, 2018.
- [4] D.H Kim, H.J Kim, J. Kwak, “Secure Sharing Scheme of Sensitive Data in the Precision Medicine System,” *CMC-computers Materials & Continua*, 64(3), pp. 1527-1553, June 2020.
- [5] *The Precision Medicine Initiative Cohort Program - Building a Research Foundation for 21st Century Medicine*, NIH, Sep 2015.

<저자 소개>



김 득 훈 (Deuk-Hun Kim)

증신회원

2013년 8월 : 순천향대학교 정보보호학과 학사

2015년 8월 : 순천향대학교 정보보호학과 석사

2015년 9월~현재 : 아주대학교 컴퓨터공학과 박사과정

2021년 3월~현재 : 아주대학교 사이버보안학과 특임교원 <관심분야> 응용서비스 보안, 클라우드 컴퓨팅 보안, 암호 프로토콜



곽 진 (Jin Kwak)

증신회원

2000년 8월 : 성균관대학교 학사

2003년 2월 : 성균관대학교 석사

2006년 2월 : 성균관대학교 박사

2006년 4월~2006년 11월 : 일본 큐슈대학교 방문연구원

2006년 8월~2006년 11월 : 일본 큐슈시스템정보기술연구소 특별연구원

2006년 11월~2007년 2월 : 정보통신부 정보보호기획단 개인정보보호팀 통신사무관

2007년 3월~2015년 2월 : 순천향대학교 정보보호학과 교수

2008년 1월~현재 : 한국정보보호학회 상임이사

2015년 3월~현재 : 아주대학교 사이버보안학과 교수 <관심분야> 응용시스템보안, 클라우드 컴퓨팅 보안, 암호 프로토콜, 개인정보보호, 정보보호제품평가