https://doi.org/10.33778/kcsa.2024.24.3.187

대학 내 사이버 보안을 위한 제도·기술적 관점에서의 전략

이 기 호*, 이 용 준**

요 약

AI와 IoT의 발전으로 사이버 보안 위협은 급격히 증가하고 있다. 사이버 공격의 수단과 목적이 진화함에 따라 대학도 모든 주요 산업과 마찬가지로 심각한 사이버 보안 문제에 직면하고 있는 상황이다. 대학은 학생들의 개인정보, 연구 데이터, 지적 재산 등 방대한 양의 민감한 정보를 보유하고 있어 사이버 위협의 주요 대상이 된다. 이에 본 논문에서는 대학의 기관장과 정책 입안자들이 사이버 보안 태세를 강화하는데 도움이 되는 제도 및 기술적 관점에서의 사이버 보안 전략을 제시하고자 한다. 연구에서는 지금까지의 사이버 공격 흐름을 통해 동향을 검토하고, 랜섬웨어 및 AI 기반 맬웨어와 같은 고도화된 위협 증가에 대응하기 위해 거버넌스, 정책 개발, 위험 관리 및 FIDO와 AI 기반 기술적 보안 시스템 구축을 제시한다.

Strategies for Cybersecurity in Universities from Institutional and Technical Perspectives

Ki-Ho Lee*, Yong-Joon Lee**

ABSTRACT

With the advancement of AI and IoT, cybersecurity threats have increased dramatically. As the methods and objectives of cyber-attacks evolve, universities, like all major industries, are facing serious cybersecurity issues. Universities hold vast amounts of sensitive information such as students' personal data, research data, and intellectual property, making them prime targets for cyber threats. Therefore, this paper aims to present cybersecurity strategies from both institutional and technical perspectives to help university leaders and policymakers enhance their cybersecurity posture. The study reviews current trends through the flow of cyber-attacks and proposes governance, policy development, risk management, and the establishment of FIDO and AI-based security systems to respond to the increase in sophisticated threats such as ransomware and AI-based malware.

Key words : Cybersecurity, Cyber threats, Management strategies, University security

접수일(2024년 04월 03일), 게재확정일(2024년 05월 27)

* 극동대학교 인공지능보안학과 박사과정

** 극동대학교 해킹보안학과 교수

1. 서 론

인공지능과 사물인터넷 등 신기술의 발전과 함께 최근 사이버 보안 위협은 가파르게 증가하고 있다. 사이버 테러의 수단은 지속적으로 변화하고 있으며, 모든 주요 산업과 마찬가지로 대학의 사이버 보안 또한 도전에 직면하고 있다.

대학은 학생들의 개인정보와 연구 데이터, 특허와 같은 지적 재산 등 방대한 양의 정보를 소유하고 있으며, 이는 대학에 따라 다소 차이는 있을 수 있으나 규모가 작다고 해서 그 가치가 낮다고는 할 수 없다.

또한, 대학은 국가나 도시가 의존하는 중요한 인프라와 사용자 집약적인 시스템의 본거지로, 특히 지방대학이 타격을 받을 경우 대학이 소속된 지자체도 경제 및 사회적 악영향을 받을 수 있다.

대학의 전산 시스템은 공공기관의 성격을 띄면서도 다른 산업에서는 찾아볼 수 없는 개방성과 투명성의 독특한 학계 문화를 같이 갖추고 있어 보안 취약점을 스스로 만들기도 한다. 특히 2020년부터 시작된 팬데믹(Pendemic)으로 인한 원격 근무와 온라인 학습으로의 급격한 전환은 대학 네트워크와 IT시스템에 연결되는 개인용 스마트 기기가 폭발적으로 증가하는 계기가 되어 사이버 보안의 위험을 사상 최고치로 끌어올렸다. 사이버 침해 위협이 나날이 증가하는 지금, 대학 내 기관장과 정책 입안자들은 사이버 침해에 대응하기 위해 필요한 인재와 인프라에 투자를 해야할 것이며, 기관 전략을 우선순위에 두고 자원과 노력을 집중시켜야 할 것이다.

따라서, 본 논문에서는 현재까지의 사이버 공격 흐름을 분석하여, 이를 토대로 대학의 기관장과 정책 입안자들이 참고할 수 있는 정책, 거버넌스 등 제도 중심의 개선 방향과 FIDO 인증 기술, AI 기반 관제 시스템 등의 기술 관점에서의 전략을 제공함으로써 보안의 완성도를 높이고자 한다.

2. 사이버 공격 개요

2.1 현재까지의 사이버 공격 흐름

1960년대, 사이버 보안은 주로 조직 자산을 보호하는데 중점을 두었다. 보안은 비밀번호, 다중 계층 보호 등 물리적 조치 위주로 구성되었다[1].

1970년대에는 컴퓨터가 중앙집중식에서 분산형 사용자 기반 시스템으로 전환되면서 사이버 보안 이슈가 주목받기 시작했다[2]. 인터넷의 등장으로 사이버 공격의 수와 형태가 급증했으며, 바이러스, 웜, 맬웨어와 같은 새로운 위협이 등장하기 시작했다. 이에 대응하기 위해 방화벽, 실시간 보호 프로그램 등이 개발되기도 하였다. 1990년대 말에는 인터넷의 대중화가 진행되었으며, 인터넷을 통해 전송되는 컴퓨터 바이러스가 대중 매체의 주목을 받기 시작했다[3]. 2010년대에는 소셜미디어가 새로운 공격 루트로 부상하였는데[4]. 사이버 공격의 형태가 더욱 복잡하게 진화함에 따라 2013년 스노든 사건과 3억 개의 야후 사용자 계정이 침해된 사건 등 심각한 대규모 데이터 유출 사건이 발생하기도 했다.

최근에는 랜섬웨어, 크립토재킹과 같은 새로운 유형의 맬웨어가 등장하여 사이버 범죄자들이 돈을 갈취하고자 한다. 이에 더불어 AI의 발전은 사이버 범죄자들의 테러 능력을 향상시킴과 동시에 사이버 보안에 대한 관행이나 고착화된 과거의 보안 방식을 개선하는 데에도 기여하고 있다[5].

2.2 교육부 사이버 테러 경로 분석

2023년 1월부터 8월까지 교육부 산하 기관 유형별 사이버 공격 탐지 및 대응 현황은 아래와 같다.

<표 1> 교육부 산하 공공기관 유형별 사이버 공격 탐지 및 대응 현황 (단위: 건)

구 분	침입시도	해킹메일	악성코드	웹해킹	경유지악용	서비스거부	총계
시·도 교육청	67	63	56	1	20	1	208
대학	35,636	334	2,225	23	1,591	4	39,813
공공기관	220	10	6	2	15	0	253
국립대학병원	88	2	8	0	36	0	134
소 계	36,011	409	2,295	26	1,662	5	40,408

교육부 산하 공공기관을 대상으로 한 사이버 침해 시도는 침입 시도가 가장 많았으며, 다음으로 악성코드, 해킹 메일, 경유지 악용, 웹 해킹, 서비스 거부 순서로 이어졌다[6].

대학의 경우에는 침입 시도, 악성코드, 경유지 악용, 해킹 메일, 웹 해킹, 서비스 거부 공격 순서로 많았고, 공격 시도를 받은 건수는 2018년부터 2013년 8월까지 21만 8,894건으로 교육부 산하 공공기관 전체 현황의 91.91% 달하였다.

2.3 잠재적 사이버 위협

세계경제포럼은 2020년 맬웨어와 랜섬웨어 공격이 각각 358%, 435% 증가했다고 발표하였다[7]. 사이버 테러 위협은 클라우드 컴퓨팅, 모바일 기술, 인공지능, 사물인터넷 등 신기술의 등장에 영향을 받아 사회 대응 능력을 뛰어넘는 속도로 발전하는 양상을 보였다.

특히나 AI 기술의 발전은 보안 능력을 강화했으나 동시에 새로운 위협도 만들어 냈다. 그중에서도 AI 기반 맬웨어는 랜섬웨어 공격 형태로 증가했으며, 모바일 기기의 보급 증가와 함께 사이버 공격의 전쟁터가 전통적 PC에서 모바일 플랫폼으로 옮겨가기도 하였다[6].

또한, IoT 기기를 통해서도 다양한 공격 양상을 확인할 수 있는데, 실시간 데이터 수집이나 프라이버시 이슈 등 여러 취약점을 기반으로 공격이 진행되었다.

단독 기기를 인터넷에 연결해 스마트 기기로 전환하는 간단한 목표로 시작된 IoT는 일상과 기업 비즈니스 전반에 걸쳐 큰 영향을 미칠 수 있는 다음 산업혁명의 토대라고 할 수 있다. 다만, 안타깝게도 현재 IoT는 실시간 데이터 수집이나 프라이버시 이슈, 보안 표준화 및 요구사항이 완벽하게 다듬어진 상태는 아니며, 일례로 가정집 IoT 기기가 해킹당해 사생활이 노출되거나 스마트 공장이 해킹 위협을 받는 등 여러 취약한 모습을 보이는 사례가 존재한다.

지금까지의 양상을 토대로 분석해 보자면, 앞으로 10년간의 사이버 테러는 AI를 활용한 공격과 사물인터넷(IoT) 기기를 대상으로 한 침입 시도, 정보 유출 등 테러의 증가로 전개될 것으로 보인다.

3. 대학 사이버 보안 전략: 시스템에 대한 제도적 관점에서의 접근

모든 상황을 해결할 수 있는 사이버 보안 전략은 없다. 다만, 사이버 테러 양상을 분석해 보았을 때, 신속한 대처가 피해를 줄일 수 있음은 분명하다. 따라서, 도전 과제를 지속 가능한 방식으로 구성하여 조직 문화의 큰 흐름으로 만드는 것이 중요하며, 최대한 신속하게 사건을 해결할 수 있도록 전략을 구성해야 한다. 이를 위해 먼저, 제도적 관점에서 접근하는 것을 제안한다.

3.1 기관 거버넌스 강화 및 KPI 재검토

첫 번째로, 정보 자산 보호에 관련한 리더십과 조직 구조 및 프로세스의 거버넌스 접근 방식을 권장한다[8]. 사이버 보안에 대해 고위 경영진의 관심사를 가져오는 것이다. 기관장과 같은 고위 경영진의 참여를 필수로 보고 기관 전체의 노력이 되도록 하는 것이 핵심이다.

두 번째로, 새로운 기관 구조와 결재 방식이 도움이 될 수 있다. 기관장에게 사이버 보안에 대한 사항을 보고하는 고위 경영진, 구성원, 정보 책임자(CIO) 및 각 부서 대표로 구성된 운영 위원회를 구성하는 것이다. 운영 위원회는 대학 내 모든 사이버 보안 관련 행위를 감독할 책임을 가진다. 위원회를 통해 사이버 보안 이슈를 예방하고, 탐지 및 해결하기 위한 전략적 계획을 개발할 수 있다.

또한, 대학에는 교육부 정보보호 수준진단을 통해 공통적으로 진행하는 정보보안 인증 제도가 있으나 점수를 낮게 받거나 미실시 하더라도 어떠한 불이익이 없다. 이에 대학 내 사이버 보안 KPI는 점차 그 유효성을 잃어가고 있다. 따라서 대학 기관장들이 정확한 사이버 보안 성과 보고를 얻고 의미 있는 전략적 결정을 내릴 수 있도록 재검토되어야 한다.

유효한 KPI를 구축하는 기초 단계는 사이버 보안에 관련한 주요 요인과 영역을 이해하는 것이다. 최근 연구들은 조직이 물리적 보안, 취약성, 접근 제어, 인프라 등을 고려하여 KPI를 구성할 것을 제안한다[8]. 이러한 요소들은 사이버 보안 환경을 구성하는데 매

우 밀접한 관련이 있으나, 대학 기관장은 실제로 기관 요소, 사용 가능한 자원, 보안 목표, 지속 가능성을 고려해 전략을 형성해야 한다.

3.2 사이버 보안 정책 지침 명시

사이버 보안 정책은 조직 정보와 데이터 사용 및 보호에 대한 공식 선언이다. 대학에서 정책을 만든다는 것은 사이버 보안에 대한 약속을 나타내는 첫걸음이고, 기관 행동 양식을 지원하는 역할을 명확하게 설명할 수 있는 기회를 제공한다. 특히 보호해야 할 것과 집행이 어떻게 되는지 사이의 구분이 중요하고, 직원이 역할과 기여를 명확하게 이해할 수 있도록 작성해야 한다.

효과적인 사이버 보안 정책 수립을 위해서는 아래와 같은 내용이 포함되어야 한다.

첫 번째, 잠재적인 취약점을 이해하기 위해 위험 관리 및 평가를 수행해야 한다. 위험 관리는 대학 사이버 보안 전략의 핵심 요소로, 모든 잠재적 위협을 식별, 분석, 평가하고 위협 요소를 완화하기 위한 적절한 대책을 구현하여야 한다. 위험 관리의 주요 목표는 조직이 수용할 수 있는 위험 수준을 정의하고 그 한계를 초과하는 위험을 감소시키는 것이다.

위험 관리 프로세스는 다음과 같다. 위험 식별, 위험 평가, 위험 대응 전략 결정, 위험 완화 조치 구현, 위험 모니터링 및 검토, 위험 식별 단계에서는 가능한 모든 사이버 보안 위협을 찾아내야 하며, 위험 평가 단계에서는 각 위협의 가능성과 결과를 평가해야 한다. 이러한 정보를 바탕으로 대학은 위험을 피하거나 수용하거나 완화하는 등 대응 전략을 결정할 수 있다.

위험 관리 프로세스는 정적인 것이 아니라 지속적인 과정이다. 기술의 발전, 새로운 위협의 등장, 조직 내부의 변화 등에 따라 정기적으로 위험 관리 프로세스를 검토하고 업데이트하는 것이 중요하다. 이를 통해 대학에서는 사이버 보안 위협 환경의 변화에 능동적으로 대응할 수 있다.

두 번째, 측정 가능한 결과를 위해 명확한 목표를 정의하는 것이다. 예를 들어 1년 이내 피싱 공격을 50% 이상 감소시키거나 6개월 이내 조직의 50% 이상에 2단계 인증을 구현하는 등 진행 상황을 추적할 수 있는 측정 가능한 목표를 포함하여야 한다. 또한, 사이버 보안 목표가 전반적인 비즈니스 목표와 일치하는지 확인하여 운영 효율성을 방해하지 않는지 분석해야 한다.

세 번째, 직원의 역할과 책임을 명확하게 정의하여야 한다. 사이버 보안과 관련해서는 모든 직원이 중추적인 역할을 하게 된다. 따라서 모든 사람의 책임을 명확하게 정의하고 전달하는 것이 중요하다. 특히 인력 위주로 구성된 대학 조직에서는 네트워크 보안 담당자나 데이터 보호 책임자와 같은 직무를 정의하는 것이 좋다. 또한, 사소하게는 의심스러운 이메일을 즉각적으로 보고하는 것을 포함하여 직원들의 역할 이해도를 확인하는 것이 필요하다. 이를 통해 사이버 보안 규정 및 제도를 준수하는 문화를 조성할 수 있어야 한다.

네 번째는 정기적인 정책 업데이트와 직원 교육이다. 사이버 보안 분야는 끊임없이 진화하는 과제이므로, 정기적인 정책 업데이트와 지속적인 교육이 필요하다. 새로운 위협과 기술 발전을 반영할 수 있는 정기적인 정책 업데이트와 최신 사이버 위협 및 예방 기술에 대한 교육이 필요하다.

3.3 모바일 기기 관리 조치 도입

현재 대학은 출결 관리나 전자결재 시스템, 학사 시스템 등 업무 및 학업 관리에 있어, 모바일 앱 구축이 활발하게 진행되고 있다. 그러나 정보보호 수준진단에서는 모바일을 포함한 업무용 단말기에 대한 보안만 존재하고, 모바일 앱 관련한 정보보호 지표는 반영되어 있지 않다.

모바일 기기의 사용은 대학 비즈니스 및 학생 커뮤니케이션 등 일상 활동에 필수적이며, 교육 및 연구, 행정 관리에 있어서도 유용한 도구이다. 그러나 이러한 기기의 편의성에도 불구하고 사이버 보안 위협에 특히 취약하다.

대학은 위협에 대응하기 위한 모바일 기기 관리 정책(Mobile Device Management, MDM)을 개발하고 실행하여 기기에 저장된 데이터와 전송 중인 데이터 보안을 보장해야 한다. 정책은 기기 설정, 앱 설치 및 사용, 데이터 암호화, 도난 기기의 원격 삭제 기능 등을 포함해야 한다.

4. 대학 사이버 보안 전략: 시스템에 대한 기술적 관점에서의 접근

최근 한국 장학재단은 국가 근로 관리자 등 대학 내에서 개인정보를 취급하는 직무 담당자에게 로그인 시 공동인증서나 금융인증서 2차 인증을 진행하도록 요구하였다.

이처럼 2차 인증 도입은 사용자의 계정이 유출되더라도 공격자에게 기회를 주지 않는다는 점에서 필수적인 보안 요소로 채택되고 있는데, 아직 대학 행정망에서는 아이디와 패스워드만으로 로그인하는 경우가 많다. 따라서, 여러 방식의 보안 조치를 검토하여 도입할 필요가 있다.

4.1 정교한 보안 조치 도입 : FIDO(Fast IDentity Online)

FIDO는 온라인에서 ID, 패스워드 없이 지문, 홍채, 얼굴인식, 목소리, 정맥 등 생체 인식 정보나 보안 키 등을 활용해 보다 편리하고 안전하게 사용자 인증을 수행하는 기술 표준이다. 사용자들이 여러 개의 계정과 패스워드를 생성하고 기억해야 하는 문제를 해결하기 위한 목적으로 설립되었으며, 인증 프로토콜과 인증 수단을 분리하여 생체 정보 전송의 위협과 저장된 생체정보가 해킹될 가능성을 원천 차단하는 구조로 프레임워크를 제안하였다.

FIDO 1.0은 2014년도 12월 개발 표준이 공개되었으며, 다음과 같이 크게 두 가지 구성 요소로 이루어져 있다.

첫 번째는, UAF(Universal Authentication Framework)로 사용자가 비밀번호 없이도 생체 인식(지문, 안면 인식, 홍채 등)이나 핀 번호 등을 이용해 인증할 수 있게 해주는 프레임워크이다.

두 번째는, U2F(Universal 2nd Factor)로 기존 패스워드 기반 인증에 두 번째 요소로서 USB나 NFC를 통해 연결되는 보안 키를 사용하는 인증 프로토콜이다.

FIDO 1.0 이후 모바일에 더불어 PC를 포함한 모든 온라인 환경에서 생체인증을 사용할 수 있게 해주는 FIDO 2.0이 등장하였는데, 단말기에 종속되지 않는다는 장점이 존재한다. FIDO 2.0의 인증 프로토콜은 UAF, U2F, CTAP(Client to Authenticator Protocol)로 나뉜다. UAF는 FIDO 1.0에서 고안된 기술로 2.0 버전에서도 동일하게 사용된다.

CTAP는 외부장치를 이용한 인증 방식에 사용하는 프로토콜로 모바일 단말기, USB, NFC, BT와 같은 외부 장치를 이용하여 운영체제나 웹 브라우저 등과 인증자 연동을 구성한다. 해당 프로토콜이 표준 연동 방식으로 자리 잡은 후 단말기 자체에서만 생체인증이 가능했던 UAF와 간편한 2차 인증을 제공하는 U2F가 하나의 플랫폼으로 구성되었다.

FIDO는 공개 키 암호방식을 사용을 통해 대학 내 산업 기술의 근간이 되는 연구 실적 및 특허 기술, 개인정보 등 정보보호의 기반이 될 수 있으며, 패스워드의 분실 위험 없이 교직원의 빠르고 간편한 인증 절차 효율성을 제공할 수 있다. 또한, 관리적 이점을 제공하고, 국제적인 정보보호 규정을 준수하여 글로벌 보안 제도를 선진적으로 적용할 수 있다는 장점이 있다.

실제로 FIDO 기술은 Google의 사례 연구를 통해 효용성이 증명된 바 있다. Google은 FIDO U2F 보안 키의 내부 구현 후 물리적 보안 키 사용을 요구한 이후로 85,000명 이상의 직원에 대한 피싱 공격을 막아내었다고 밝혔다[9]. 이러한, 높은 보안성이 증명된 기술을 토대로 도입을 고려해야 한다.

4.2 정교한 보안 조치 도입 : AI 기반 관제 시스템

<표 2> 인력·AI 중심 보안관제 시스템 구성 비교

구분	인력 중심	AI 중심	SOC
초기 비용	2~2.5억 원	1~1.5억 원	0.5~2억 원
운영 비용	1.5~2억 원	0.5~1억 원	1~2.5억 원
총 비용	첫 해 최대 4.5억 원 이후 최대 2억 원	첫 해 최대 2.5억 원 이후 최대 1억 원	첫 해 최대 4.5억 원 이후 최대 3.5억 원

현재 보안관제 시스템은 인력 중심에서 AI 기반으로 변화하는 추세이다. 인력·AI 중심, 그리고 SOC 관

제시스템 도입 및 운영 비용은 다음 표와 같다[10][11][12].

먼저 인력 중심으로 보안관제 시스템을 구축하고자 할 때, 초기비용으로는 초기 설치 및 구성 비용 외에도 인력 고용과 교육에 대한 비용이 발생한다. 일반적으로 보안관제 직무의 연봉은 현재 신입 기준 3천만 원, 경력직 5천만 원까지 책정된다[13][14]. 이에 따라 최소 3교대 기준으로 3명 이상의 인력을 고용하고, 초기 SW·HW 설치 비용을 포함할 경우 첫 해 최대 약 4.5억 원, 매년 유지보수와 인건비 약 2억 원이 소요된다.

다음, AI 기반의 보안관제 시스템을 구축하고자 할 때, 초기비용으로는 SW·HW 설치 비용이 소요되어 첫 해 최대 약 1.5억 원이 소요 된다. 시스템의 특성상 한 명의 담당자만 보유해도 되므로 첫 해에는 최대 2.5억 원, 매년 유지보수와 인건비로 약 1억 원이 소요 된다.

마지막으로 보안운영센터(SOC)를 외주로 구축할 때에는 SOC를 설계하고 구축하는데 필요한 컨설팅 비용과 SW·HW 설치 비용이 소요되며 최대 2억 원 정도 비용이 발생한다[15]. SOC의 경우 보통 연간 계약으로 이루어지고, 24/7 모니터링과 위협탐지, 인시던트 대응을 포함하면 연간 1~2억 정도 비용이 발생할 수 있다. 또한, 위협 인텔리전스나 맞춤형 보고서 작성 등 추가 서비스에 따라 2~5천만 원의 추가 비용이 발생할 수 있다. 따라서, 초기 구축 비용은 최대 약 4.5억 원, 이후 매년 연간 계약 비용으로 최대 2억 원이 소요된다.

공공기관의 경우 보안에 투자되는 예산이 많지 않다. 따라서 소요 비용과 성능을 비교한 합리적 보안 방안을 강구해야 하는데, 대형 종합 대학에서는 SOC나 자체적인 보안관제를 통해 이상징후 모니터링 및 사이버 공격 분석, 대응이 가능한 반면, 중소 규모 대학에서는 대규모 예산을 투자하기 쉽지 않으므로 AI의 고려가 필수적이다.

또한, 국가정보자원관리원은 최근 AI 보안관제를 통해 하루 1,000만 건 이상 사이버 공격 대응이 가능하다고 밝혔다. 신·변종 사이버 공격에 대응할 수 있으며, 수동 작업 시 10분이 소요된다면 AI 자동화의 경우 30초 이내로 단축할 수 있다. 이는 앞으로의 보안 방향에 있어 AI 도입을 고려해야 하는 이유이다[16].

5. 결 론

디지털 혁명은 취약성을 수반한다. 새로운 형태의 사이버 공격은 지속적으로 대학의 사이버 보안 역량을 시험할 것이다. 이러한 맥락에서 본 연구는 우선, 기존 사이버 침해 현황과 흐름을 분석하였고, 국내 대학의 특수성에 알맞은 제도적·기술적 관점에서의 보안 전략을 제시하였다.

당연하게도 제시한 방법은 모든 사이버 공격을 방어하지 못할 수도 있다. 다만, 시스템 전체적인 관점에서 보았을 때, 대학의 사이버 위협에 대항하는 것에 있어 기본적이며, 비교적 가성비가 높고, 단순한 수단을 대표한다고 볼 수 있다. 또한, 제시한 전략을 바탕으로 국내 대학 전반은 규모에 관계 없이 공통적으로 반영할 수 있는 보안 대책을 마련할 수 있으며, 이를 통해 사이버 보안에 대한 문화를 형성할 수 있을 것이다.

참고문헌

[1] https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/, “A History of Information Security”, 2022, Feb.

[2] In Lee, “Cybersecurity: Risk management framework and investment cost analysis”, Business Horizons, Vol. 64, No. 5, pp. 659-671, 2021.

[3] William Easttom, “Computer Security Fundamentals, 4th Edition” Pearson IT, 2019.

[4] Rakesh Singh Kunwar, Priyanka Sharma, “Social Media: A new Vector for Cyber Attack”, Conference: International Conference on Advances in Computing, Communication & Automation (ICACCA 2016), pp. 1-5, 2016.

[5] Nektaria Kaloudi, Jingyue Li, “The AI-Based Cyber Threat Landscape: A Survey”, ACM Journ

als; ACM Computing Surveys, Vol. 53, No. 1, pp. 1-34, 2020.
[6] https://www.medicalworldnews.co.kr/news/view.php?idx=1510957663, “2018년~2023년 8월 현재까지 교육부 산하 기관 유형별 사이버 침해 탐지·대응 현황 외, 2023, Oct.
[7] World Economic Forum. ”The Global Risks Report 2022“, 17th ed.;World Economic Forum: Cologny, Switzerland, 2022.
[8] Richard Baskerville, Mikko Siponen, “An Information Security Meta-Policy for Emergent Organizations”, Logistics Information Management, Vol. 15, No. 5/6, pp. 337-346, 2002.
[9] https://fidoalliance.org/google-case-study/?lang=ko, “FIDO Case Studies Google 사례연구”, FIDO ALLIANCE, 2019, Jan.
[10] https://www.s1.co.kr/info-security/network-security/security-control, “네트워크 보안 및 보안 관제” 에스원, 2024, June.
[11] https://www.gartner.com/reviews/market/security-information-event-management, “Security Information and Evert Management Reviews and Ratings“, Gartner.
[12] https://shinsegae-inc.com/business/itService/security.do, “Security Service”, Shinsegae I&C.
[13] https://www.saramin.co.kr/zf_user/company-info/view-inner-salary/csn/WTZqYityZFcrMHJCYVFtOFJZQzc3UT09/company_nm/%EC%97%90%EC%8A%A4%EC%BC%80%EC%9D%B4%EC%89%B4%EB%8D%94%EC%8A%A4, “SK 쉴더스 연봉정보”, Saramin.
[14] https://www.teamblind.com/kr/post/%EC%95%88%EB%9E%A9-%EB%B3%B4%EC%95%88%EA%B4%80%EC%A0%9C-%EC%8B%A0%EC%9E%85-%EC%B4%88%EB%B4%89%EC%97%B0%EB%B4%89-7QSgw2NR, “안랩 보안관제 신입 초봉”, Team Blind.
[15] https://www.samsungsds.com/kr/security-operation-center-consulting/security-operation-center-consulting.html, “Security Operation Center Consulting”, Samsung SDS.
[16] https://www.datanet.co.kr/news/articleView.html?idxno=185705, “Security Managed Service Provider Market Growth”, DataNet. 2023. Jul.

〔저자소개〕

이 기 호 (Ki-Ho Lee)
2018년 2월 : 동국대학교 국어국문학과 학사
2020년 10월 ~ 2024년 3월 : 극동대학교 정보보호 담당자
2024년 2월 : 극동대학교 인공지능보안학과 석사
2024년 3월 ~ 현재 : 극동대학교 인공지능보안학과 박사과정
email : lkheio92@gmail.com

이 용 준 (Yong-Joon Lee)
2005년 2월 : 숭실대학교 컴퓨터학과 박사
2010년 2월 ~ 2016년 3월 : 한국 인터넷진흥원 수석연구위원
2016년 4월 ~ 2020년 3월 : 국방보안연구소 연구관
2021년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수
email : 2020032@kdu.ac.kr