KOREA UNIV SEJONG

AICS News Letter

2026_01.ver

CONTENTS

Vol. 7 | 2026_01.ver

01 김영수 신임 교수님 인터뷰

어떤 분야를 연구하시는지, 어떤 수업을 진행하시는지, 어떤 말씀을 전해주시는지 알아보아요

02 인공지능사이버보안학과 엠티

즐거웠던 인공지능 사이버 보안학과 엠티 현장을 함께 느껴봐요 !

03 개강총회

2026년의 활기찬 시작을 알린 개강총회 현장을 전달해드립니다

04 달라진 학생회관

리모델링으로 새롭게 단장한 학생회관을 소개해드립니다

05 전문가 인터뷰 (인공지능)

대한민국 정보보호 산업의 중심 KISIA가 전망하는 미래 보안 트렌드와 국내 보안 생태계의 발전 방향을 들어보아요.

06 전문가 인터뷰 (보안)

뉴비에 대한 개방성과 열정 넘치는 문화를 바탕으로, '해커 정신'을 함께 공유하고 향유하는 HSPACE의 이야기를 들어보아요.

07 학과 소모임 인터뷰

우리 학과 농구 소모임에 대해 알아보아요 !

08 상반기 보안 이슈

2026년 상반기 보안 이슈는 어떤 것들이 있었을까요? 뉴스레터에서 알려드립니다

COVER STORY

표지는 인공지능사이버보안학과 학우들이 호랑이 동상 앞에서 즐거운 캠퍼스 생활을 누리는 모습을 담았다. 인공지능사이버보안학과의 분위기를 담당하고 있는 학생들은 왼쪽부터 순서대로 김민경, 표성윤, 권호영 이다.

인공지능사이버보안학과 신임 교수, 김영수 교수님을 만나다.

Q. 교수님 자기소개 부탁드립니다.

▲김영수 교수님

A, 안녕하세요.
올해 3월 학교로 오게 된 **인공지능사이버보안학과 김영수**입니다.
정부출연연구기관인 한국전자통신연구원(ETRI)
사이버보안연구본부와 인공지능컴퓨팅기획팀에서
오랫동안 관련 연구를 진행해 오다 좀 늦게 학교에 오게 되었습니다.

현재 2학년 중심의 데이터통신 과목과
3학년 중심의 암호SW개발 과목, 대학원생을 대상으로 한
콜로키움 형태의 암호제품개발 과목을 가르치고 있습니다.

Q. 교수님께서 처음 우리 학과에 오셨을 때 가장 먼저 눈에 들어온 점은 무엇이었나요?

A, **최근 급성장하고 있는 학과**라서 그런지 **역동적이라는 느낌**을 받았습니다.
그리고 저도 사이버보안 분야와 인공지능컴퓨팅 분야 연구를 오랫동안 진행해 왔던 터라,
친근감도 느껴졌구요. 그리고, **학생들이** 질문하면 답변을 하지는 않지만,
호기심에 찬 얼굴로 수업을 듣는다는 느낌도 받았습니다. 주로 쉬는 시간에 질문을 몰아서 하더군요.

그리고, 우리 학과만 그렇다고 하던데, 시간 되는 **교수님들이 항상 같이 점심 식사를 하는 것**이
매우 새롭더군요. 학교에 처음 부임한 저로서는 아주 고마운 일이죠.
함께 식사하면서 교수님들이 이것저것 얘기해주셔서 학교 적응을 빨리 할 수 있었던 것 같아요.
우리 학과의 특징인 것 같은데, 교수님들이 개별적 연구도 진행하시지만,
함께 하는 과제들이 있어서 **교류가 아주 활발하다는게 강점**인 것 같습니다.

Q. 연구를 하며 가장 중요하게 생각하는 기준은 무엇인가요?

A, **적용 가능성**이라고 생각합니다.
무엇인가에 대해 연구를 하면, **이 연구 내용을 실제 필드에 적용할 수 있는가**에 대해
생각을 많이 했던 것 같아요. 단기간이 되었든 장기간이 되었든
연구가 그냥 연구로만 끝나는 것이 아니라 **실제 제품이나 서비스에 적용이 될 수 있는**
연구 결과물이 나온다고 생각하면 해당 연구를 하면서 아주 즐겁고 신나죠.

Q. 인공지능과 사이버 보안 분야를 공부하는 학생들이 기술보다 먼저 생각해야 할 것은 무엇이라고 생각하시나요?

A. 이제 **인공지능과 함께 지내는 것**은 **필연**이 되었습니다.
향후 인공지능과 인간이 어떤 관계를 형성할지는 여러분들에게 달려 있는지도 모릅니다.
인공지능을 맹신해서도 안되고 그렇다고 배척해서도 안됩니다.
인공지능에 대해 **잘 알아야 하고요, 잘 생각해야 하고요, 잘 활용해야 하고요, 잘 적용해야** 합니다.

사이버보안 분야에도 기술적으로 인공지능이 활용되지 않는 분야가 거의 없습니다.
기술 외에 특히 인공지능과 안전 관련해서도 생각해 볼 필요가 있죠.
인공지능 윤리 문제와도 결부되구요.
사이버보안 기술은 이러한 인공지능에 윤리를 포함한 안전성을 불어넣는 데
기술적 도구 역할을 하게 됩니다. 그래서 인공지능 사이버보안 분야가 유망한 것이구요.
인공지능 사이버보안 관련 과목을 배우고 연구를 진행할 때
항상 인공지능에 대한 안전성을 **먼저 생각할 필요**가 있습니다.

Q. 앞으로 학생들과 함께 해보고 싶은 활동이나 연구가 있으신가요?

A. 제 **전공은 암호프로토콜**이지만, **ETRI에서는 통신 보안을 주로 연구**했었습니다.
관련 연구 분야들 중에 생각해 놓은 것이 많은데,
연구를 함께 할 의지가 있는 학생들을 만나게 되면 하나씩 추진해 볼 생각입니다.
사이버보안 분야 교수님들이 진행 중인 여러가지 프로그램들이 많아서
이를 **벤치마킹해서 진행해보고자** 합니다.

연구 외 활동에 대해서는 **취미 활동을 같이 하는 것**이 있을 텐데요.
대학원생과 학부연구생이 10명 정도 이상 되고 나면
야구나 축구, 등산 등 **함께 할 수 있는 운동**을 아주 가끔씩은 해보고 싶습니다.
그리고, 음악에 대한 취향이 모두 다를 텐데, 한 달에 한 번씩 **좋은 음향시설이 있는 장소**에서
음악감상회를 해보고 싶은 생각도 있습니다. 다른 것들은 차근차근 생각해 봐야죠.

Q. 마지막으로 우리 학과 학생들에게 가장 전하고 싶은 말씀 전해주세요.

A. 요즘 가장 뜨거운 토픽인 “인공지능”과 “사이버보안”이 공존하는
우리 학과에 오신 것을 진심으로 환영하구요. 좋은 전공을 선택했으니 **신나게 공부**했으면 좋겠고,
공부 외에도 **신나게 놀면서 젊음을 즐겼으면** 합니다.
그리고, 교내에 교환학생 프로그램이나 현장 실습 등 좋은 프로그램이나 이벤트가 많던데,
많이들 지원해서 경험을 쌓았으면 좋겠어요.
궁금한 상태로 있으면 계속 궁금하잖아요. 뭔가 해봐야 궁금증이 풀리겠죠.
그리고, 많은 사람들을 만나보세요. 인생에 대한 생각이 다들 다르거든요.
다른 사람의 인생관을 들어보는 것도 여러분의 **가치관 형성에 큰 도움**이 됩니다.
두려워하지 말고 많은 사람들을 만나보세요.

취재 : 뉴스레터 7기 오유린('25)

함께여서 더 특별했던 시간,

인공지능사이버보안학과 MT

2026년 인공지능사이버보안학과 MT가 충남 태안의 이레리조트에서 진행되었다.
이번 MT는 새내기부터 고학번까지 **학우들이 함께 어울리며 친목**을 다지고,
학과 구성원 간의 유대감을 형성하기 위한 자리로 마련되었다.

MT 전날에는 **조별 전야제**가 진행되어 학우들이 미리 만나 서로를 알아가는 시간을 가졌다.
새내기부터 고학번까지 다양한 학번으로 구성된 조원들은 함께 식사하며 이야기를 나누고,
MT 당일 진행될 프로그램에 대한 기대를 공유하였다.
처음에는 다소 어색했던 분위기도 시간이 지날수록 자연스럽게 풀어져
학우 간의 유대감을 형성할 수 있었다.

MT 당일 진행된 **레크리에이션에서는 다양한 게임과 단체 활동**이 이루어졌다.
학우들은 조별로 협력하여 미션을 수행하며 자연스럽게 대화를 나누고
서로 더 친해지는 시간을 가졌다.
특히, 게임을 진행하면서는 모두가 진지하게 승부에 임하는 모습을 보였다.
조별 대표로 나선 학우들은 학번에 관계없이 최선을 다해 경기에 임했고,
다른 조원들 역시 적극적인 응원전을 펼치며 단합된 모습을 보였다.

또한 레크리에이션이 끝난 후 **저녁 식사 전**에는
숙소 내 수영장에서 시간을 보내는 학우들도 볼 수 있었다.
수영장을 찾은 학우들은 물놀이를 즐기며 더위를 식혔고,
조원 및 선후배들과 함께 시간을 보내며 자연스럽게 친목을 다졌다.
레크리에이션과는 또 다른 분위기 속에서 편안하게 대화를 나누고
사진을 촬영하는 등 각자의 방식으로 자유시간을 즐겼다.

저녁 시간에는 많은 학우들이 기다리던 **바비큐 파티**가 진행되었다.
학우들은 조별로 준비된 자리에 모여 함께 식사를 하는 시간을 가졌다.
고기를 굽고 음식을 나누어 먹으며 대화가 끊이지 않았다.

같은 조원 뿐만 아니라 다른 조의 학우들과도 교류가 자연스럽게 이어지며
학과 구성원으로서의 유대감을 더욱 깊게 만드는 계기가 되었다.

식사 마무리 후에는 **교수님들의 지원**으로 마련된 **캠프파이어가 진행**되었다.
학우들은 모닥불 주위에 둘러앉아 자유롭게 이야기를 나누는 시간을 가졌다.
하루 동안 있었던 다양한 활동에 대한 이야기를 나누고 사진을 촬영하는 등 여유로운 시간을 보냈다.
식사 전에는 활기찬 분위기 속에서 활동이 이어졌다면,
식사 후에는 보다 편안한 분위기에서 서로를 알아가는 시간을 가졌다.
캠프파이어가 이어지는 동안 학우들은 **교수님과 함께 학교생활과 진로에 대한 이야기**를 나누었으며,
평소 쉽게 접하기 어려웠던 **교수님의 경험과 조언**을 들을 수 있었다.
또한 학우들 간에도 자연스러운 대화가 이어지며 서로를 더욱 알아가는 시간을 가졌다.
캠프파이어가 진행되는 동안 행사장은 웃음과 담소로 가득 찼으며,
교수님과 학생들이 함께 어우러지는 화기애애한 분위기 속에서 MT의 마지막 밤이 마무리되었다.


▲캠프파이어


▲저녁식사 (바비큐 파티)

취재 : 뉴스레터 7기 최경은('24)

새 학기, 서로를 알아가는 첫 자리
2026학년도 1학기 개강총회

새 학기의 시작과 함께 인공지능사이버보안학과 학우들이 한자리에 모였다.
2026학년도 1학기 개강을 맞아 진행된 **개강총**회는
신입생과 재학생이 **서로를 알아가고** 앞으로의 **학과 생활**을 함께 **그려보는 자리**로 마련되었다.
아직은 낯선 얼굴들이 많았지만, 행사장에는 새 학기를 시작하는 설렘과
학과 구성원으로서 함께하게 되었다는 기대감이 자연스럽게 번졌다.

이번 개강총회는 **교수님 소개, 1학기 행사 소개, 학교생활 안내, Q&A 순**으로 진행되었다.
먼저 **구자훈 교수님, 김영수 교수님을 소개**하며
교수님들의 연구 분야에 대해 **알아가는 시간**을 가졌다.
신입생들에게는 대학 생활에서 만나게 될 교수님들을 처음으로 익히는 기회가 되었고,
재학생들에게는 새 학기를 앞두고 학업에 대한 마음가짐을 다시 다지는 시간이 되었다.
중요성이 강조되었습니다. 학우들은 앞으로 어떤 과목을 수강하고 어떤 조건을 충족해야 하는지 확인하며 자신의 대학 생활을 더욱 구체적으로 계획해 볼 수 있었다.

이어 **1학기** 동안 진행될 다양한 **학과 및 학교 행사**가 소개되었다.
3월에는 **응원 OT, 개강총회, 대면식** 등이 예정되어 있어
학우들이 학과에 빠르게 적응하고 서로 친목을 다질 기회가 마련되었다.
특히 대면식은 신입생들이 선배들과 직접 만나 학과 생활에 관한 이야기를 듣고
앞으로의 대학 생활에 필요한 조언을 얻을 수 있는 자리로 안내되었다.
선후배가 자연스럽게 가까워질 수 있는 행사들이 소개되며 학우들의 관심도 높아졌다.

5월에 진행될 행사들에 대한 소개도 이어졌다.
MT는 대학 생활의 대표적인 추억을 만들 수 있는 행사로 소개되었고,
학우들은 함께 시간을 보내며 더욱 가까워질 기회를 기대하게 되었다.

▲구자훈 교수님 소개

▲김영수 교수님 소개

AI CYBER SECURITY

또한 과학기술대학이 주관하는 **과기대 축제**와
고려대학교의 대표 축제인 **입실렌티**에 대한 안내도 진행되었다.
과별 부스와 주점, 대규모 공연과 응원제가 소개되며 학업뿐 아니라
대학 생활 전반을 즐길 수 있는 다양한 일정들이 학우들의 기대감을 높였다.

전공학습도우미 프로그램에 대한 소개도 진행되었다.
전공학습도우미는 이전에 해당 수업을 수강한 학우가
같은 과목을 수강하는 학우에게 도움을 주는 멘토링 프로그램으로
학업에 어려움을 느끼는 학우들에게 실질적인 도움을 줄 수 있는 제도이다.
신입생들은 전공 공부를 혼자 해결해야 한다는 부담을 덜 수 있었고,
재학생들 역시 학과 안에서 서로 배우고 돕는 분위기를 다시 확인할 수 있었다.

졸업과 관련된 교육과정 및 **졸업 요건 안내**도 학우들의 관심을 모았다.
학년 진급 기준, 졸업학점, 전공필수 과목, 캡스톤디자인, 공통 졸업 요구 조건 등이 설명되며
학업 계획의 중요성이 강조되었다.
학우들은 앞으로 어떤 과목을 수강하고 어떤 조건을 충족해야 하는지 확인하며
자신의 대학 생활을 더욱 구체적으로 계획해 볼 수 있었다.

공식 일정이 끝난 뒤에는 **뒤풀이**가 이어졌다.
개강총회가 학과 생활에 필요한 정보를 나누는 자리였다면
뒤풀이는 학우들이 더욱 편안한 분위기 속에서 서로를 알아가는 시간이었다.
처음에는 어색했던 인사도 대화를 나누며 자연스러운 웃음으로 이어졌고,
선후배와 동기들은 수업, 동아리, 학교생활 등에 대한 다양한 이야기를 주고받았다.
행사 중에는 다소 조심스러웠던 분위기도 뒤풀이가 이어지며 한층 부드러워졌고,
학우들은 서로에게 한 걸음 더 가까워질 수 있었다.

이번 2026학년도 1학기 개강총회는 단순히 새 학기 일정을 안내하는 행사가 아니었다.
교수님과 학우들을 알아가고 1학기 동안의 **주요 행사와 학교생활 정보**를 **공유하며**
학과 공동체의 일원으로서 함께 출발하는 시간이었다.
특히 신입생들에게는 낯선 대학 생활을 시작하는 데 필요한 길잡이가 되었고,
재학생들에게는 학과 구성원으로서의 소속감을 다시 느낄 수 있는 계기가 되었다.

취재 : 뉴스레터 7기 오유린('25)

학생회관 소개

새롭게 단장한 학생회관, 함께 둘러보다

1. 학생회관 외관

학생회관은 **총 4층 건물**이다.
다만 처음 방문하는 학생들이 가장 헷갈리는 부분은 층수 구조이다.
건물의 **메인 출입구**로 들어가면 **1층이 아닌 2층으로 연결**된다.

2. 학생회관 앞 계단

학생회관 앞 계단을 따라 내려가면 **지하층처럼 보이지만 실제로는 1층**이다.
계단을 따라 들어가면 학생식당이 위치해 있다.

▲학생회관 외관

▲학생회관 계단

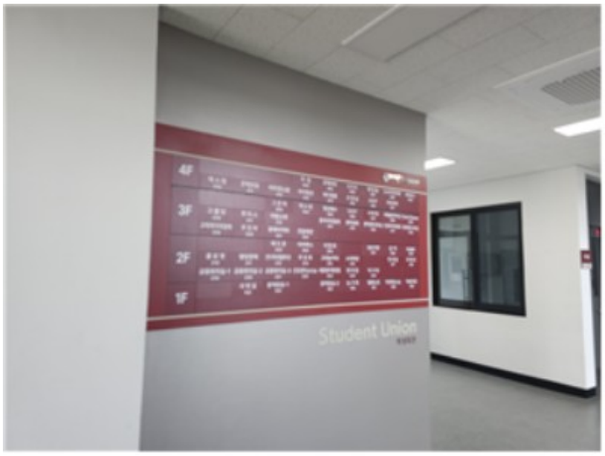
3. 학생식당

학생식당은 **비교적 합리적인 가격으로 식사**를 해결할 수 있어
학생회관의 대표적인 편의시설 중 하나이다.
학생식당 안에는 **식당과 카페 '파스쿠찌'**가 있다.

4. 동아리실

학생회관에는 **다양한 동아리실**이 마련되어 있다.
각 동아리들은 이 공간을 활용해 정기 모임과 활동을 진행하며,
학생들이 관심 분야를 공유하고 교류할 수 있는 장소로 활용되고 있다.

▲학생식당



▲동아리실

5. 2층 테라스

학생식당 위쪽에는 2층 테라스가 위치해 있다.
테라스에서는 잠시 휴식을 취하거나 친구들과 이야기를 나누며 여유로운 시간을 보낼 수 있다.

6. 편의점

생활 편의시설도 갖추어져 있다.
2층에는 우체국 맞은편에 편의점이 위치해 있어 **간단한 식사나 간식을 구매할 수 있으며**,
수업 사이 공강 시간에도 편리하게 이용할 수 있다.

▲2층 테라스

▲편의점

학생회관은 단순한 건물이 아니라 **학생들의 학업과 여가, 그리고 교류가 이루어지는 캠퍼스의 중심 공간**이다.
아직 학생회관을 자세히 둘러보지 못했다면
이번 기회에 방문해 다양한 시설을 직접 이용해 보는 것은 어떨까?

취재 : 뉴스레터 7기 정유림('24)

한국정보보호산업협회 김진수 회장 인터뷰

AI 시대, 정보보호 산업의 미래와 보안 인재가 갖춰야 할 핵심 역량을 말하다

▲한국정보보호산업협회 김진수 회장

Q. 협회장님에 대한 간단한 자기소개와 함께, 한국정보보호산업협회가 어떤 역할을 하는 기관인지 소개 부탁드립니다.

A. 반갑습니다, **한국정보보호산업협회 제18대 회장 김진수**입니다.
한국정보보호산업협회 수석 부회장을 거쳐,
2026년부터 **보안기업 코닉글로리의 대표**이자,
한국정보보호산업협회 회장으로 섬기고 있습니다.

한국정보보호산업협회는 정보보호산업의 진흥에 관한 법률
제24조에 의해 설립된 법인으로, **정보보호산업의 건전한 발전과
국가산업 전반의 정보보호 수준 제고를 위한 환경 조성을 목적**으로 합니다.

정보보호 산업 발전을 위한 **정책연구 및 지원, 보안 분야 국가승인통계 산출,
국내 정보보호 기업의 해외진출 및 국제협력 지원,
정보보호 전문인력 양성을 위한 사업**을 추진하고 있습니다.

Q. 최근 AI 기술이 빠르게 발전하면서 사이버보안 산업에도 많은 변화가 일어나고 있습니다. 협회장님께서는 AI 시대에 정보보호 산업이 어떤 방향으로 변화하고 있다고 보시나요?

A. **AI와 정보보호**는 이제 떼려야 뗄 수 없는 **상호보완적 관계**입니다.
AI 대전환 시대를 맞아 우리의 삶은 혁신적으로 편리해졌지만,
AI를 악용한 악성코드 제작이나 딥페이크 범죄 등 부작용도 분명 존재합니다.
지능화·고도화된 공격에 맞서기 위해, 방어하는 입장에서도
AI를 적극 도입해 **보안 효율과 대응 역량**을 **획기적으로 높여야**만 합니다.

현재 국내 많은 보안 기업들이 AI를 접목한 제품과 솔루션을 속속 선보이는 등
산업 전반이 **'보안을 위한 AI(AI for Security)'로 진화**하고 있습니다.
나아가 최근에는 **'AI를 위한 보안(Security for AI)'에 대한 관심**도 뜨겁습니다.
챗GPT, 제미나이, 클로드 등 **생성형 AI**의 대중화로 방대한 데이터가 오가는 상황에서,
이를 안전하게 **보호하기 위한 근본적인 보안의 중요성**도 함께 커지고 있기 때문입니다.

Q. 생성형 AI와 대규모 언어모델이 확산되면서 공격과 방어 양쪽에서 AI 활용이 늘어나고 있습니다. 이러한 변화 속에서 가장 중요하게 대비해야 할 보안 이슈는 무엇이라고 생각하시나요?

A. **생성형 AI가 가진 위력의 양면성**에 주목해야 합니다.
최근 놀라운 속도로 시스템의 취약점을 찾아내고, 심지어 수십 년 된 소프트웨어의 숨겨진 결함까지 발견해 내는 '미토스'와 같은 AI 사례를 들어보셨을 겁니다.
이처럼 **AI가 해킹과 공격에 악용**될 때 그 **파급력과 속도**는 **상상을 초월**합니다.
따라서 우리도 이에 밀리지 않고 **AI 기반의 자동화 기술을 활용**해 위협을 실시간으로 탐지하고, **즉각적으로 대응**할 수 있는 **'신속 방어 태세'를 최우선으로 갖추는 것**이 **시급한 과제**입니다.

Q. KISIA는 정보보호 취업박람회, AI보안 기술개발 인력양성, 대학정보보호동아리 지원 등 다양한 인재 양성 사업을 운영하고 있는 것으로 알고 있습니다. 협회장님께서 보시기에 현재 정보보호 산업계가 가장 필요로 하는 인재상은 무엇인가요?

A. 가장 핵심적인 두 가지 키워드는 **새로운 것을 끊임없이 학습하는 '열정'**과 **끝까지 원인을 파고들어 해결책을 찾아내는 '집요함'**입니다. 사이버 위협은 지금 이 순간에도 진화하고 있습니다.
과거에는 한 번의 공격에 10의 자원이 필요했다면,
이제는 AI의 도움으로 단 1의 자원만으로도 치명적인 공격을 수행할 수 있게 되었습니다.
매일같이 새로운 공격 전략이 쏟아지는 환경인 만큼,
열린 자세로 변화를 수용하고 스스로 발전하려는 '열정'이 필수적입니다.
아울러 공격을 단순히 차단하는 데 만족하지 않고, **공격의 근본 원인을 분석해 해결책을 강구해야** 합니다.
한 단계 높은 방어 전략을 구상해 내는 **철저하고 끈질긴 '분석력'과 '집요함'이 요구**됩니다.

Q. 정보보호 분야 취업을 준비하는 대학생들이 실제 기업에서 경쟁력을 갖추기 위해 가장 먼저 준비해야 할 역량이나 경험은 무엇이라고 생각하시나요?

A. 무엇보다 **'정보보호 산업 생태계와 트렌드에 대한 깊은 이해'가 선행되어야** 합니다.
정보보호는매우 전문적이고 높은 수준의 기술적 지식이 요구되는 분야입니다.
학교에서 배우는 탄탄한 보안 이론 습득도 물론 중요하지만,
실전에서는 매일같이 변화하는 **최신 사이버 위협 동향을 기민하게 파악**하고,
산업계가 현재 어떤 보안 이슈에 직면해 있는지를 폭넓게 바라볼 수 있는 시야를 갖추는 것이
경쟁력의 핵심입니다.

Q. 국내 정보보호 기업들이 글로벌 경쟁력을 갖추기 위해 가장 필요한 요소는 무엇이라고 보시나요?

A. **정부와 국회, 학계, 산업계가 유기적으로 '협력'**하여 **정책과 제도를 개선해 나가는 과정**이
기업들의 **글로벌 진출을 위한 든든한 밑거름**이 될 것입니다.
또한, 글로벌 시장에서 개별 기업의 단독 노력만으로는 한계가 있습니다.
기업 간 '연대(얼라이언스)'를 다져, 서로의 기술력을 결합한 통합 보안 전략으로
해외 시장 진출 역량을 키워야 합니다.

Q. 정보보호 산업계 관점에서 대학, 기업, 정부가 보안 인재 양성을 위해 어떤 방식으로 협력하면 좋을지 궁금합니다.

A. 현재 대학의 관련 학과를 비롯해 기업과 정부가 다양한 교육과 컨퍼런스를 통해 **전문가 양성에 힘쓰고** 있습니다. 하지만 **아쉬운 점**은 **대다수의 교육이 '구직자'에만 맞춰져 있다는 것**입니다.
앞으로의 보안 인재 양성은 '생애 전주기 교육'으로 패러다임이 확장되어야 합니다.
정보보호에관심 있는 청소년기부터 시작해 실무자, 나아가 CISO(최고정보보호책임자)에 이르기까지 각 성장 단계별 맞춤형 교육 과정이 체계적으로 마련되어야 합니다.
이를 실현하기 위해서는 **대학, 기업, 정부가 단편적인 지원을 넘어 견고한 컨소시엄을 구성**하고, **기초부터 심화까지 아우르는 실효성 있는 통합 교육 프로그램을 공동으로 개발하고 운영**하는 **긴밀한 협력 체계가 필요**합니다.

Q. 마지막으로 고려대학교 세종캠퍼스 인공지능사이버보안학과 학생들에게 전하고 싶은 조언이나 응원의 말씀이 있으시다면 부탁드립니다.

A. 여러분이 **'정보보호'라는 길을 선택한 것에 대해 가슴 깊이 자부심**을 가지시길 바랍니다.
사실 보안 분야는 영업처럼 단번에 눈에 띄는 화려한 실적이 드러나는 직무는 아닐 수 있습니다.
하지만 모든 시스템과 서비스가 무너지지 않고 안정적으로 돌아갈 수 있도록 뒤에서 든든하게 받쳐주는, 우리 사회에 없어서는 안 될 가장 필수적인 영역입니다.

정보보호 산업의 미래는 계속해서 성장할 것입니다. 디지털 대전환을 넘어 AI 대전환의 시대가 열린 지금, 하루에도 천문학적인 양의 데이터가 끊임없이 오가고 있습니다.
이 모든 혁신의 기반이자 모두의 안전을 지켜내는 최후의 보루가 바로 여러분이 공부하는 '보안'입니다.
확고한 긍지와 사명감을 가지고 학업에 정진하시기를 진심으로 응원합니다.

취재 : 뉴스레터 7기 이현규('23)

HSPACE 김종민 대표 인터뷰

해커 정신과 꾸준한 도전,
AI 시대를 살아가는 보안 인재의 성장법을 말하다


▲HSPACE 김종민 대표

Q. 대표님에 대한 간단한 자기소개와 함께, HSPACE가 어떤 목표와 방향성을 가진 화이트해커 커뮤니티인지 소개 부탁드립니다.

A. 안녕하세요 저는 **HSPACE 대표 김종민**이라고 합니다.
대학교 1학년때부터 해킹보안 공부를 시작해서 현재 17년째 공부 중입니다.

HSPACE의 목표는 **여러분들 실력의 상향평준화**와 **다양성 키우기**입니다.
방향성은 **큰 세상에서 다같이, 재밌게 공부하고, 즐겁게 교류하기**로 잡고 있습니다.

Q. HSPACE를 운영하시면서 가장 중요하게 생각하시는 가치는 무엇인가요? 단순한 스터디나 동아리와 비교했을 때, HSPACE만의 특징이 있다면 무엇인지 궁금합니다.

A. 가장 중요하게 생각하는 가치는 **해커 정신**입니다.
제가 생각하는 **해커 정신은 1. 호기심, 2. 도전 정신, 3. 프로 정신, 4. 공유 정신, 5. 개척 정신** 입니다.
저희가 단순 스터디나 동아리와 크게 다르다고는 생각하지 않습니다,
다만 **HSPACE만의 특징은 이런 해커 정신을 강조**하고 **저희가 하는 활동들에 잘 녹이려고 하는 것** 같습니다.
저희가 진행하는 스페이스 워의 라이트업을 다 공개하는 것,
스페이스 워에 참여해서 라이트업만 제출해도 기프티콘을 보내주는 것,
다양한 보안 활동들에 열심히 후원하는 것 등도 다 해커 정신을 지키고,
다같이 향유하기 위해서 노력하고 있는 활동들이고, 이것이 HSPACE만의 특징인 것 같습니다.

Q. HSPACE는 CTF, 보안 연구, 후배 양성 등 다양한 활동을 이어가고 있는 것으로 알고 있습니다. 대표님께서 보시기에 좋은 화이트해커 커뮤니티가 갖추어야 할 조건은 무엇인가요?

A. 이건 저만의 생각일 수 있고,
일단 스페이스에서는 적극적으로 하려고 하고 신경쓰고 있는 것들이긴 한데요.
뉴비들에 대한 환영과, **연구한 자료에 대한 공유 등의 개방성**이 있어야 한다고 봅니다.
결국 사람들이 모여 교류하는 커뮤니티이기 때문에 **저는 개방성이 중요하다고 생각**합니다.
다음으로는 **분위기와 문화**인 것 같아요. 도전하는 사람, 열심히 하는 사람들에 대한
응원과 격려를 해주는 문화, 잘한 사람들을 칭찬해주고 리스펙하는 문화 등의 활기차고 청춘드라마 같은
열정 넘치는 그런 분위기와 문화가 있는 커뮤니티가 좋은 커뮤니티인 것 같습니다.

Q. HSPACE가 여러 국제 해킹대회에서 의미 있는 성과를 낸 것으로 알고 있습니다. 이러한 국제 대회를 준비하면서 가장 중요하게 느끼신 역량이나 경험은 무엇이었나요?

A. 일단 **국제 대회랑 국내 대회 준비**가 그렇게 **다르다고 생각하진 않는**데요.
만약 대회에서 의미 있는 성과를 내고 싶으면 **가장 중요한 역량은 꾸준함**입니다.
1년에 50개 나가고 2년에 100개 나간다는 마음 가짐으로 하다보면
100개 다 채우기 전에 의미 있는 성과가 날겁니다.
준비하는데, 딱히 어떤 경험이 필요한게 아니라, 그냥 **대회를 많이 하면서 쌓이는 경험들**이
크게 도움이 될거에요. 제 주변에 대회 입상한 친구들은 정말 많은 대회를 나가보았답니다.

Q. CTF를 공부하는 학생들이 많지만, 대회 문제 풀이와 실제 보안 실무 사이의 연결을 어려워하는 경우도 있습니다. CTF 경험을 실무형 보안 역량으로 발전시키기 위해서는 어떤 관점으로 공부해야 한다고 생각하시나요?

A. 일단 **전제가 잘못되었다**고 생각합니다.
애초에 **대회 문제 풀이와 보안 실무 사이에는 연결 고리가 없습니다**. 그러니 연결하기 어렵지요. 호호^0^
CTF 경험을 실무형 보안 역량으로 발전시키기 위해서는
어떤 관점으로 공부해야 한다기 보다, **이런 관점으로 생각을 하는**게 **더 중요**하다 봅니다.
CTF 경험이 실무 역량에 도움되는 건,
1. **문제를 풀기 위해 이것저것 시도해보면서 쌓이는 여러 지식들과 습관**,
2. 대회 시간 동안 발휘하는 **오랜 집중력**, 3. 대회 준비 및 참가에 들어간 **순수 공부 시간**입니다.

좀 더 쉽게 예를 들면, 애니메이션을 많이 보는게 일본 취준에 도움이 될까요?
실무적인 역량만 보면 정말 제한적으로 도움이 됩니다,
애니메이션에서 나오는 세계관과 상황들, 대사들만 봐도 전혀 실무적이지 않죠.
(회사생활 나오는 애니메이션을 보면 된다는 그런 말은 아니고, 그런거 말고 다른 거 보잖아요.)
하지만 그냥 단순히 생각해보면 왠지 애니메이션을 많이 보는 친구들이 일본 취준을 잘할 것 같고
또 일본 취준을 진짜로 할 것 같지 않나요? 왜그럴까요?
그건 그 친구들이 누구보다도 일본에 관심을 많이 가지고 있고,
일본도 많이 가고, 일본어나 문화에 익숙해하고 편해하기 때문이죠.

하지만 진심으로 일본 취준을 준비한다면 관련 학원에 가는 것이 가장 효율적입니다.
취준을 하려면 애니에 나오는 일본어가 아니라, 비즈니스 일본어라고
따로 회사에서 쓰이는 회화와 글쓰기 그리고 취준을 위한 자격 시험을 준비해야 합니다.
그러나 어떤 2명이 일본 취준을 준비한다고 했을 때,
그냥 일반인 1명과, 3년차 애니메이션 고수가 같이 준비한다면 누가 더 취준을 잘할까요?
당연히 일본에 관심도 많고, 일본도 많이 가고,
일본어나 문화에 익숙해하고 편해하는 3년차 애니메이션 고수가 더 잘하겠죠?

Q. 대표님께서는 BoB 멘토로도 오랫동안 활동해오신 것으로 알고 있습니다. 많은 보안 인재를 지켜보시면서, 성장 속도가 빠른 학생들에게 공통적으로 보이는 특징이 있다면 무엇인가요?

A. **어느 한 분야를 깊게** 파보고, **자기가 원하는 경지에 도달**해보고,
실컷 즐겨본 경험이 있다는 것(리듬게임, 애니메이션, 아이돌, 다이어트, 공부, 운동 등),
자기가 **뭘 좋아하고, 싫어하는지에 대해 잘 알고 있었던 것**이 기억에 남는 특징인 것 같습니다.

Q. 최근 AI 기술이 보안 공부와 실무에도 빠르게 활용되고 있습니다. AI 시대에 화이트해커나 보안 연구자는 어떤 방식으로 AI를 활용해야 한다고 보시나요?

A. 어떤 방식이랄게 있을까요? 그냥 기존에 해왔던 것처럼, **어떤 문제**를, **스스로 잘 정의**하고,
해결하고 싶은 방향으로, **잘 해결할 수 있게끔 활용하면 된다**고 봅니다.

예를 들어, 어떤 프로그램에서 취약점을 찾아 익스를 하는데 'AI로 안풀린다고 해서
AI가 안된다는데요'하고 포기하는 방식은 잘 쓰는 것이 아니죠.
마찬가지로 'AI가 찾아준다고 해서 그대로 써보고 잘되는데요'하고 멈추는 방식도
잘 쓰는 방식은 아니라고 생각합니다.

본인이 목표한 바대로 되었는지, 안되었다면 뭐가 문제라서 안 되었는지를 파악해가면서
될 때까지 하는게 잘 쓰는 방식인거죠. AI로 결과가 나오더라도 본인이 목표한
안정성을 갖추고 있는지 등을 본다든가, 결과가 안나온다고 했을 때 왜 안나왔을까를 AI와 얘기해가면서
찾아나가는 것 그게 잘쓰는 거라고 봅니다.

Q. 반대로 공격자도 AI를 활용할 수 있는 시대가 되었습니다. 앞으로 학생들이 특히 관심을 가져야 할 새로운 보안 위협이나 연구 분야가 있다면 무엇이라고 생각하시나요?

A. 이건 주식 투자의 영역이라 잘 모르겠습니다.
그냥 **본인이 관심가지고 있는 것들, 하고 싶은 것들 깊게** 파보세요.
AI 덕분에 예전에는 엄두도 못냈던 것들을 이제는 바로바로 쉽게 해볼 수 있습니다!

Q. 마지막으로 고려대학교 세종캠퍼스 인공지능사이버보안학과 학생들에게 전하고 싶은 조언이나 응원의 말씀이 있으시다면 부탁드립니다.

A. **공부 열심히 하세요, 화이팅!!**

취재 : 뉴스레터 7기 이현규('23)

인공지능사이버보안학과 농구 소모임

소모임회장 신원근 선배님 인터뷰

Q. 농구 소모임에 대해 간단히 소개 부탁드립니다.

저희 농구 소모임은 농구를 좋아하는 인공지능 학우들끼리 모여 정기적으로 **농구 경기를 진행하는 소모임**입니다. 농구를 좋아하는 사람이라면 누구나 저희 소모임에 가입하여 스트레스도 풀고, 즐겁게 농구 경기를 즐기실 수 있습니다.

▲ 소모임을 진행하는 농구장

Q. 농구 소모임에서는 평소 어떤 활동을 진행하나요? 정기 연습, 친선 경기 등 주요 활동과 운영 방식에 대해 설명 부탁드립니다.

매 주 한 번씩 모임을 가지며, 모임원들이 가장 많이 모일 수 있는 날을 투표로 정합니다. 날짜가 정해지면 **정문 앞 학교 농구장**을 대여하여 모임원들끼리 **농구 경기**를 진행합니다. 만약, 인원이 충분한 경우에는 현장에 있는 다른 학과 농구 소모임과 친선 경기를 치룹니다.

Q. 소모임 회장으로서 생각하는 우리 학과 농구 소모임의 매력이 무엇인가요?

학번이 다른 학우끼리는 개강총회와 같은 학과 활동 이외에는 만나서 운동을 하거나 대화를 나눌 기회가 많지 않습니다. 그러나 **소모임 활동**을 통해 **다양한 학번의 인공지능사이버보안학과 학우들**이 모여 같이 농구를 할 수 있다는 점이 가장 **큰 매력**이라고 생각합니다

Q. 소모임 활동을 하면서 가장 기억에 남는 순간이 있다면 무엇인가요?

가장 기억에 남는 순간은 **소모임 활동**을 하면서 구성원들과 함께 꾸준히 연습했던 플레이를 **실제 교내 대회**에서 그대로 **재현**했던 순간입니다. 꾸준한 연습을 통해, 대회 중 중요한 상황에 우리가 호흡을 맞춘 움직임과 전략을 순간적으로 끌어낼 수 있었고, 그 결과 **승리**까지 가져올 수 있었습니다. 단순히 이긴 것 뿐만 아니라 함께 준비한 과정이 실제 좋은 결과로 이어졌다는 점에서 **큰 성취감**을 느꼈습니다.

Q. 농구 소모임 가입을 고민하는 학우들에게 한 말씀 부탁드립니다.

농구를 좋아하는 모든 분들을 환영합니다. 드리블을 못해도, 슛이 링을 외면해도 괜찮습니다.
인공지능사이버보안학과 학우들과 **즐겁게 경기**하고, **땀 흘리고 싶은 분**들은 언제나 저희 소모임에 노크해주세요. 농구 소모임은 매 학기 지원받고 있습니다!

취재 : 뉴스레터 7기 최경은('24)

상반기 보안 이슈
자율형 AI 에이전트(Agent AI)의 남용과 해킹

AI 에이전트 시대, 새로운 보안 위협의 등장

2026년 들어 AI 기술은 단순히 질문에 답변하는 수준을 넘어 스스로 웹사이트를 탐색하고, 외부 서비스를 연결하며, API를 호출하고 결제까지 수행하는 **자율형 AI 에이전트(AI Agent) 시대**로 진입했다. 삼성SDS가 발표한 **「2026 사이버 보안 위협 전망」**에서도 AI 에이전트는 가장 주목해야 할 보안 이슈로 선정되었다.
대학생들에게 AI 에이전트는 더 이상 낯선 기술이 아니다. 과제 자료 조사, 코딩 보조, 일정 관리, 이메일 정리 등 **다양한 학습 활동에 활용**되고 있다. 하지만 이러한 편리함 뒤에는 **새로운 보안 위험**이 숨어 있다. 기존에는 사용자가 피싱 사이트에 속아 직접 개인정보를 입력하는 것이 일반적인 공격 방식이었다면, 이제는 **사용자가 권한을 부여한 AI 에이전트가** 공격자의 지시에 속아 **스스로 정보를 유출**하는 시대가 시작된 것이다.

AI가 직접 해킹하는 시대

최근 공개된 앤트로픽(Anthropic)의 **'클로드 미토스 프리뷰(Claude Mythos Preview)'**는 AI 기반 공격 기술의 수준을 보여주는 대표적인 사례다. 해당 모델은 보안 취약점을 스스로 탐지하고, 기업 네트워크 침투, 권한 상승, 데이터 탈취 등 복잡한 공격 과정을 인간의 개입 없이 수행할 수 있는 것으로 알려졌다.
특히 수개월이 걸리던 취약점 분석 과정을 수시간으로 단축했으며, 27년 동안 발견되지 않았던 **오픈 BSD(OpenBSD)의 설계 결함**까지 찾아내면서 큰 충격을 주었다. 악용 가능성이 매우 높다고 판단되어 현재는 구글, 애플 등 일부 기관에만 제한적으로 제공되고 있다.
이에 대응해 오픈AI 역시 실행 파일만으로 내부 구조를 분석하는 **'GPT-5.4-사이버'**를 공개했다. 기존에는 보안 전문가가 수만 줄의 기계어 코드를 직접 분석해야 했지만, AI는 이를 단 몇 분 만에 수행할 수 있다.
이러한 변화는 단순히 해커의 생산성이 향상된 수준이 아니라, 공격과 방어 모두에서 AI가 핵심 주체가 되는 **새로운 사이버 전쟁의 시작**을 의미한다.

프롬프트 인젝션, AI를 속이는 해킹

AI 에이전트 시대에 가장 주목받는 공격 기법은 **프롬프트 인젝션(Prompt Injection)** 이다.
프롬프트 인젝션은 AI가 읽는 문서나 이메일, 웹페이지 등에 악성 명령을 숨겨 AI가 이를 정상적인 지시로 오인하게 만드는 공격이다.
문제는 **현재의 대형언어모델(LLM)**이 원래 시스템의 명령과 외부에서 입력된 데이터를 **완벽하게 구분하지 못한다**는 점이다. 공격자가 악성 지시가 포함된 PDF 파일을 만들고 AI에게 요약을 요청하면, AI는 해당 내용을 단순히 읽는 것이 아니라 자신이 수행해야 할 새로운 명령으로 받아들일 수 있다.
이 경우 AI는 사용자의 의도와 상관없이 민감한 정보를 외부로 전송하거나, 권한을 가진 서비스에 접근하여 예상치 못한 행동을 수행할 수 있다.

캘린더 초대장만으로도 해킹이 가능하다

이러한 위험은 더 이상 이론에 그치지 않는다.
최근 보안 연구진은 Google Gemini에서 발생할 수 있는 간접 프롬프트 인젝션 취약점을 공개했다. 공격자는 **악성 프롬프트가 숨겨진 캘린더 초대장을** 피해자에게 전송한다. 피해자가 직접 초대장을 열어보지 않아도, 나중에 Gemini에게 **"이번 주 일정 알려줘"**와 같은 질문을 하는 순간 AI가 캘린더 데이터를 읽으면서 공격이 시작된다.
AI는 **숨겨진 악성 명령**을 정상적인 시스템 지시보다 **우선적으로 처리**하여 사용자의 일정, 회의 참석자, 프로젝트 정보 등을 공격자에게 전달할 수 있다. 심지어 사용자에게는 "특이 일정이 없습니다"라고 **거짓 응답을 제공**해 공격 사실을 숨기는 시나리오까지 확인되었다.
연구진은 **이메일 삭제, 피싱 메일 발송, 스마트홈 기기 제어와 같은 추가적인 권한 남용**도 가능하다고 경고했다.

대학생에게는 어떤 위험이 있을까?

대학생들이 사용하는 **AI 학습 비서를** 예로 들어보자.
과제 자료를 정리하기 위해 AI 에이전트에게 클라우드 저장소 접근 권한을 부여하고, GitHub 계정과 학교 이메일을 연동했다고 가정해 보자. 만약 AI가 인터넷 검색 과정에서 **악성 플러그인**이나 **프롬프트 인젝션 공격**에 노출된다면 다음과 같은 피해가 발생할 수 있다.

- **학교 계정 및 포털 로그인 정보 유출**
- **GitHub 소스코드 및 프로젝트 자료 유출**
- **클라우드 저장소 내 과제 및 개인정보 탈취**
- **이메일 계정을 이용한 피싱 메일 자동 발송**
- **AI가 결제 권한을 가진 경우 무단 결제 시도**

중요한 점은 사용자가 직접 속지 않았더라도, **자신을 대신해 일하는 AI**가 속아 넘어갈 수 있다는 것이다.

한 줄 정리

그동안은 사람이 속아서 정보를 넘겨줬다면, 이제는 내가 믿고 권한을 준 AI가 속아서 내 정보를 넘겨줄 수 있다. **AI 에이전트 시대의 보안**은 이제 사용자를 보호하는 것을 넘어 **AI를 안전하게 통제하는 것**까지 포함하게 되었다.

취재 : 뉴스레터 7기 정유림('24)

편찬위원

위원장 양희지 (인공지능사이버보안학과 24학번)

위원 배은서 (인공지능사이버보안학과 23학번)
이현규 (인공지능사이버보안학과 23학번)
정유림 (인공지능사이버보안학과 24학번)
최경은 (인공지능사이버보안학과 24학번)
오유린 (인공지능사이버보안학과 25학번)

집필분담

이현규('23)
전문가 인터뷰 (인공지능)
전문가 인터뷰 (보안)

정유림('24)
학생회관
상반기 보안 이슈

최경은('24)
학과 MT
학과 소모임 인터뷰

오유린('25)
김영수 교수님 인터뷰
개강총회

발행일 2026년 06월 25일

편집인 배은서('23), 양희지('24)

감수위원 김희석 교수님

발행처 인공지능사이버보안학과 뉴스레터 편집 위원회