Journal of the Korea Academia-Industrial cooperation Society
Vol. 25, No. 3 pp. 461-466, 2024

https://doi.org/10.5762/KAIS.2024.25.3.461
ISSN 1975-4701 / eISSN 2288-4688

대학 정보보호 강화 방안 연구: 교육부 정보보안 수준진단을 기준으로

이기호[1], 이용준[2*], 강장묵[2]
[1]극동대학교 인공지능보안학과, [2]극동대학교 해킹보안학과

A Study on Measures to Strengthen University Information Protection: Based on the Ministry of Education's information security level diagnosis

Ki-Ho Lee[1], Yong-Jun Lee[2*], Jang-Mook Kang[2]
[1]Department of Artificial Intelligence Security, Far East University
[2]Department of Hacking Security, Far East University

요 약 디지털 환경의 발전에 따라 대학에 대한 사이버 위협도 증가하고 있다. 이에 대하여 교육부는 ISMS 업무중복 해소를 위해 대학이 교육부 정보보호 수준진단에서 우수 등급을 획득할 경우 ISMS 의무를 이행한 것으로 협의하였다. 다만, 정보보호 수준진단 지표가 ISMS의 요구에 맞추기 위해서는 그 수준 또한 상향평준화될 수밖에 없어 일부 대학교에서는 적용하기 어려운 부분이 발생하였다. 대형 종합 대학과 중소 규모 대학의 보안 수준은 차이가 벌어지기 시작했고, 간극을 좁히기 위한 연구가 필요해 졌다. 따라서 본 연구에서는 정보보안 수준진단 대상인 213개 대학을 그룹 별로 분석하였고 재학생 5천 명 미만의 중소 규모 대학에서 점수를 받기 어려운 문항을 분류하여 원인을 파악해 지원 방안을 제시하고자 한다.

Abstract As the digital environment develops, cyber threats to universities are increasing. In response, the Ministry of Education has agreed that if a university achieves an excellent grade in the Ministry of Education's information security level diagnosis to eliminate ISMS work duplication, it will be considered to have fulfilled its ISMS obligation. On the other hand, the level had to be standardized upward for the information security level diagnosis index to meet the requirements of ISMS, making it difficult to apply at some universities. The security levels of large universities and small and medium-sized universities began to differ, necessitating research to narrow the gap. Therefore, in this study, 213 universities subject to information security level diagnosis were analyzed according to the group. The questions were classified to make scoring difficult at small and medium-sized universities with less than 5,000 students to identify the cause and suggest support measures could be identified.

Keywords : Information-Security, University-Security, Isms, Information-security Level Diagnosis, Small and medium-sized University Security

*Corresponding Author : Yong-Jun Lee(Fareast Univ.)
email: yjlee@gmail.com
Received January 30, 2024 Revised February 22, 2024
Accepted March 8, 2024 Published March 31, 2024

1. 서론

1.1 연구 배경 및 필요성

네트릭스(Netwrix)의 '2023년 하이브리드 보안 동향 보고서: 교육분야'에 따르면 교육 기관의 69%는 지난 12개월 이내 사이버 공격을 1회 이상 받은 것으로 확인되었다[1]. 또한, JISC(Joint Information Systems Committee)는 2019년 보고서를 통해 영국 대학을 대상으로 실시한 침투 테스트에서 스피어 피싱을 이용해 2시간 이내 고등 교육 기관의 가장 중요한 데이터에 접근할 수 있었다고 밝혔다[2].

이러한 침해 위협은 국내 대학가에도 나날이 증가하는 추세이며, 교육부 및 교육부 산하기관 대상 사이버 공격 시도는 2021년 4만 2,564건으로 2015년 이후 매년 4만 건 이상에 달하고 있다[3].

우리나라는 정보보호 수준 향상을 위해 교육부 정보보호 수준진단 제도를 시행하고 있다. 다만, 정보보호 수준진단 지표가 ISMS의 요구에 맞추기 위해 수준이 상향평준화되어 일부 대학에서는 적용하기 어려운 부분이 발생하기도 하였다. 특히나 국내 대학에서는 예산 등 현실적인 문제로 인하여 정보보안 전문가나 전담 조직을 갖추지 못하고 겸직을 수행하는 경우가 빈번하고, 정보보호 수준 진단 평가에서 보통 단계의 인증조차 받지 못하는 경우가 대다수 존재한다.

따라서 본 연구에서는 첫 번째, 대학 정보보호 수준진단 중 개인정보보호를 제외한 정보보안 수준진단 그룹별 결과를 분석하고자 한다.

두 번째, 실제 평가 사례를 확인하여 '매우 높은 노력이 필요'하다고 평가 받은 지표를 확인하고자 한다.

세 번째, 해당 지표가 다른 그룹이나 중소 규모의 대학에서도 낮은 점수를 받는 경향을 보인다면, 그에 대한 원인을 파악하고 지원 방향을 제안하고자 한다[4].

2. 본론

2.1 정보보안 수준진단 분석

2022학년도 정보보안 수준 진단은 213교를 대상으로 시행되었다[5].

시행 결과 재학생 1만 명 이상 대학은 75개 대학으로 그 중 69개 대학이 우수(92%), 3개 대학이 보통(4%), 3개 대학이 미흡(4%)평가를 받았다.

재학생 1천 명 이상 1만 명 미만 그룹은 105개 대학으로 49개 대학이 우수(46.67%), 38개 대학이 보통(36.20%), 17개 대학이 미흡(16.20%) 평가를 받았으며 1개 대학이 미 실시로 확인 되었다.

재학생 5천 명 미만의 중소 대학에서 정보보안 수준진단을 '미흡', '미실시'로 평가 받은 대학은 총 37개교로 전체 대학에서 '미흡', '미실시'평가를 받은 경우의 80.44%에 해당하는 것으로 확인되었다.

또한, 설립 구분에 따라 국립대학인 경우 40개 대학 중 35개 대학이 우수(87.5%), 4개 대학이 보통(10%), 1개 대학이 미흡(2.5%) 평가를 받은 반면, 사립대학은 173개 대학 중 85개 대학이 우수(49.14%), 43개 대학이 보통(24.86), 43개 대학이 미흡(24.86%)평가를 받고 2개 대학이 진단을 받지 않았다.

2.2 정보보안 수준진단 사례 분석

중소 대학 중, 재적 학생 수 약 3천 명, 2022학년도 정보보안 수준진단 결과 '미흡'평가를 받은 충북의 A대학교 세부 결과를 토대로 취약 지표를 확인하고자 하였다. 평가 결과 중에서도 '매우 높은 노력이 필요'하다고 평가 받은 부분만을 간추려 보았으며 도출된 항목은 Table 1에서 보는 바와 같다.

Table 1. 'A' University information security supplements

'A' University Information Security Supplements
1. Information security organization and budget areas
2. User authentication and authority management area
3. PC Security area
4. Logs and backups area
5. Establishment of cyber crisis management system area

도출된 취약 지표는 첫 번째, 정보보안 조직 및 예산 영역에서 전담 인력 보유 여부, 두 번째, 사용자 인증 및 권한 관리 영역에서 패스워드 규칙 및 2차 인증 등 권한 관리 여부, 세 번째, PC 보안 영역에서 업무용과 인터넷용 PC 분리 여부, 네 번째, 로그 및 백업 영역에서 로그 기록 보존 및 관리 여부, 마지막으로 사이버위기 관리체계 구축 영역으로 확인되었다.

2.3 정보보안 수준진단 그룹별 지표 분석

충북의 A대학교 사례를 통해 확인된 취약 지표를 토대로 그룹별 분석을 시행하였다.

그룹 분류는 대학 정보보호 수준진단 그룹 분류를 따랐으며, 기존 '가'그룹은 A, '나'그룹은 B, '다'그룹은 C로 구분하였다.

첫 번째는, 정보보안 조직 및 예산 지표 중 진단항목 '1.2.1 기관의 정보보안 업무를 전담하는 조직이 있는가?' 항목이다.

지표는 정보보안 전담조직이 있으면 3점, 전담조직 없이 조직 구성 계획만 있으면 A그룹 1.2점, B그룹 2.1점이 부여된다.

Table 2. 1.2.1 Score status by group

Group	Score	National and public universities		Private university	
		Number	Rate	Number	Rate
A	3.0	8	53%	13	35%
	2.1	2	13%	6	16%
	1.2	2	13%	8	22%
	0.0	3	20%	10	27%
	Total	15	100%	37	100%
B	3.0	9	30%	26	28%
	2.1	2	7%	12	13%
	1.2		0%		0%
	0.0	19	63%	56	60%
	Total	30	100%	94	100%
C	3.0	1	25%	10	40%
	2.1	1	25%	2	8%
	1.2		0%		
	0.0	2	50%	13	52%
	Total	4	100%	25	100%

분석 결과 Table 2와 같이 국립대는 A그룹 10개 대학(66%), B그룹 9개 대학(30%), C그룹 1개 대학(25%)만이 전담 조직을 보유한 것으로 확인되었고, 사립대의 경우 A그룹 19개 대학(51%), B그룹 26개 대학(28%), C그룹 10개 대학(40%)이 전담 조직을 보유한 것으로 확인되었다.

이어 같은 지표 중 진단항목 '1.2.2 기관의 정보보안 업무를 전담하는 인력이 있는가?'에 대한 항목 분석 결과는 다음 Table 3과 같다.

지표는 3인 이상 전담인력이 있는 경우 A그룹 3점이 부여되고, 2인 이상 전담 인력이 있는 경우 A그룹 2.4점, B그룹 3점이 부여된다. 그 이하는 담당인력 수에 따른 점수가 부여된다.

분석 결과 국립대는 A그룹 4개 대학(27%)이 전담 인력을 2인 이상 갖추고 있었으며, B그룹에서는 2개 대학(7%), C그룹에서는 2개 대학(50%)이 전담 인력을 2인 이상 보유했음을 알 수 있다.

Table 3. 1.2.2 Score status by group

Group	Score	National and public universities		Private university	
		Number	Rate	Number	Rate
A	3	3	20%	3	8%
	2.4	1	7%	2	5%
	1.8	6	40%	17	46%
	1.2	4	27%	10	27%
	0.6	1	7%	5	14%
	0		0%		0%
	Total	15	100%	37	100%
B	3	2	7%	1	1%
	2.4	7	23%	30	32%
	1.8	11	37%	31	33%
	1.2	10	33%	31	33%
	0.6		0%		0%
	0		0%	1	1%
	Total	30	100%	94	100%
C	3	2	50%	1	4%
	2.4		0%	10	40%
	1.8	2	50%	14	56%
	1.2		0%		0%
	0.6		0%		0%
	0		0%		0%
	Total	4	100%	25	100%

사립대의 경우 A그룹 5개 대학(13%), B그룹 1개 대학, C그룹 1개 대학(4%)이 전담 인력을 2인 이상 갖추고 있었다.

두 번째로, 사용자 인증 및 권한관리 영역 중 진단항목 '5.4.1 행정업무 정보시스템 로그인에 따른 보안조치를 수행하는가?' 항목이다.

지표는 동시 로그인 차단, 로그인 시 접속 기록 표시, 일정 횟수 로그인 실패 시 차단 여부, 자동 로그아웃 기능, 사용자 비밀번호 규칙 준수, 총 5개 항목에 대해 점검하였으며, 모두 포함해 조치할 경우 2점, 2개 이상 실시할 경우 1.4점, 1개만 수행할 경우 0.8점, 아무것도 수행하지 않을 경우 0점이었다.

분석 결과 Table 4와 같이 사립대의 경우 A, B그룹 87%이상 대학이 2개 이상 보안 조치를 시행하였고, C그룹은 9개 대학이 1개 이하로 정보시스템 로그인 보안 조치를 시행함을 알 수 있었다.

세 번째, PC보안 영역 중 진단항목 '6.4.2 사용자 PC를 업무용과 인터넷용으로 분리하여 운영하는가?'이다.

지표는 모든 사용자 PC를 분리한 경우 A그룹 1점, 1/2이상 분리한 경우 A그룹 1.6점, B그룹 2점, 1/2미만 분리한 경우 A그룹 1.2점, B그룹 1.6점, C그룹 2점, 망분리 계획만 수립한 경우 A그룹 0.8점, B그룹 1.2점, C그룹 1.6점을 부여하였다.

Table 4. 5.4.1 Score status by group

Group	Score	National and public universities		Private university	
		Number	Rate	Number	Rate
A	2	9	60%	10	27%
	1.4	5	33%	26	70%
	0.8		0%		0%
	0	1	7%	1	3%
	Total	15	100%	37	100%
B	2	11	37%	31	33%
	1.4	17	57%	53	56%
	0.8	1	3%	3	3%
	0	1	3%	7	7%
	Total	30	100%	94	100%
C	2	2	50%	3	12%
	1.4	2	50%	13	52%
	0.8		0%	4	16%
	0		0%	5	20%
	Total	4	100%	25	100%

Table 5. 6.4.2 Score status by group

Group	Score	National and public universities		Private university	
		Number	Rate	Number	Rate
A	2		0%	2	5%
	1.6		0%		0%
	1.2	6	40%	24	65%
	0.8	5	33%	4	11%
	0	4	27%	7	19%
	Total	15	100%	37	100%
B	2	1	3%	1	1%
	1.6	3	10%	5	5%
	1.2	5	17%	13	14%
	0.8		0%		0%
	0	21	70%	75	80%
	Total	30	100%	94	100%
C	2	2	50%	5	20%
	1.6	1	25%	5	20%
	1.2		0%		0%
	0.8		0%		0%
	0	1	25%	15	60%
	Total	4	100%	25	100%

분석 결과 Table 5와 같이 국립대는 A그룹 6개 대학(40%)이 절반 미만의 사용자 PC를 업무용과 인터넷용으로 분리하였으며, 사립대는 24개 대학(65%)이 절반 미만의 사용자 PC를 분리하였다.

B그룹은 국립대 21개 대학(70%), 사립대 75개 대학(80%)이 사용자 PC를 물리적으로 분리하지 않았다.

네 번째는, 로그 및 백업 영역 중 진단항목 '6.5.1 정보시스템에 대한 사용자 및 관리자의 접속기록을 안전하게 보존 관리하는가?'이다. 지표는 정보시스템 로그 1년 이상 보관 여부, 정보시스템 로그 정기적인 점검 여부, 로그기록을 별도 저장장치를 통해 백업 여부 등 3개로 구성되어 모두 실시할 경우 1점을 부여하였다.

Table 6. 6.5.1 Score status by group

Group	Score	National and public universities		Private university	
		Number	Rate	Number	Rate
A	1		0%	2	5%
	0.7	6	40%	24	65%
	0.4	5	33%	4	11%
	0	4	27%	7	19%
	Total	15	100%	37	100%
B	1	1	3%	1	1%
	0.7	3	10%	5	5%
	0.4	5	17%	13	14%
	0	21	70%	75	80%
	Total	30	100%	94	100%
C	1	2	50%	5	20%
	0.7	1	25%	5	20%
	0.4		0%		0%
	0	1	25%	15	60%
	Total	4	100%	25	100%

분석 결과 Table 6과 같이 정보시스템 접속기록 진단문항에 대해 국립대 A그룹에서는 4개 대학(27%)이, B그룹에서는 21개 대학(70%)이, C그룹에서는 1개 대학(25%)이 아무것도 조치하지 않았으며, 사립대 A그룹은 7개 대학(19%), B그룹은 75개 대학(80%), C그룹은 15개 대학(60%)이 아무것도 조치하지 않고 있음을 알 수 있었다.

다섯 번째, 사이버위기 관리체계 구축 영역 중 진단항목 '4.1.2 침해사고 대응 절차를 숙지하고 모의훈련을 연 1회 이상 실시 및 결과를 반영하여 대응 매뉴얼을 개선하는가?'이다.

지표는 도상훈련 실시, 해킹메일훈련 실시, DDoS 대응 훈련 실시, 전산망 침투훈련 실시, 모의훈련 결과 설명회 및 강평회 실시, 위기대응 매뉴얼 반영 등 총 6개로 구성되어 있었다.

지표 중 5개 이상 포함해 실시한 경우 A그룹 1점, 4개 이상 실시한 경우 A그룹 0.8점, B그룹 1점, 3개 이상 실시할 경우 A그룹 0.6점, B그룹 0.8점, C그룹 1점, 1개 또는 2개 실시할 경우 A그룹 0.4점, B그룹 0.6점, C그룹 0.8점, 모두 실시하지 않을 경우 A그룹 0점, B그룹 0.4점, C그룹 0.6점이 부여된다.

분석 결과 Table 7과 같이 국립대의 경우 A그룹 7개 대학(47%), B그룹 21개 대학(70%)이 4개 항목 이상을 모두 실시하는 것으로 확인되었다.

반면, 사립대의 경우 B그룹 77개 대학(82%), C그룹 23개 대학(92%)이 모두 실시하지 않음을 알 수 있었다.

Table 7. 4.1.2 Score status by group

Group	Score	National and public universities		Private university	
		Number	Rate	Number	Rate
A	1	7	47%	11	30%
	0.8	4	27%	3	8%
	0.6	1	7%	11	30%
	0.4	1	7%	5	14%
	0.2	2	13%	7	19%
	0		0%		0%
	Total	15	100%	37	100%
B	1	21	70%	9	10%
	0.8	6	20%	3	3%
	0.6	2	7%	3	3%
	0.4	1	3%	77	82%
	0.2		0%	1	1%
	0		0%	1	1%
	Total	30	100%	94	100%
C	1	1	25%	1	4%
	0.8		0%	1	4%
	0.6	3	75%	23	92%
	0.4		0%		0%
	0.2		0%		0%
	0		0%		0%
	Total	4	100%	20	100%

3. 결론

3.1 대학 정보보호 강화 방안

앞선 정보보안 수준진단 지표 분석 결과 대학 내에서 정보보호 강화를 위해 필요한 요소는 인력, 보안 시스템 확충, 정보보호 활동으로 구분할 수 있다. 이를 위해 가장 먼저 대학 내 최고책임자의 정보보호 관심도와 투자를 유도할 필요가 있다. 교육부 등 기관에서 시행하는 대학 지원 사업의 기준 중 하나로 보안 수준을 적용시키거나 혹은 교육부 대학 평가에 정보보호 수준진단 점수를 반영하는 것이다[6,7].

그 다음으로, 대학이 수행하기 어려운 지표에 대한 비중을 낮추고, 시대 변화에 대한 반영이 이뤄져야 한다고 보았다. 아래는 정보보안 수준진단 지표 개선 및 지원 방안에 대한 제안이다.

첫 번째, 정보보안 수준진단 지표 4.1.2 침해사고 대응 절차 숙지 및 모의훈련을 연 1회 이상 실시, 결과를 반영한 대응 매뉴얼 개선 부분이다. 이에 대해 국립대는 A그룹 47%, B그룹 70%대학이 수행한 반면 사립대 B그룹은 82%에 해당하는 대학이 모두 실시하지 않는다고 답하였다.

이러한 차이는 전문가의 부재, 그리고 모두 실시하지 않아도 절반에 가까운 점수를 부여하는 상황으로 인하여 교육부에서 주관하는 사이버공격 대응 훈련 등 보안 지원 체계가 존재함에도 참여할 필요를 느끼지 못하기 때문이다. 따라서 각 침해 상황에 맞는 매뉴얼만이라도 구비할 수 있도록 하는 등 일부에 한해서라도 실질적 참여를 장려할 수 있는 대안이 필요하다.

두 번째, 정보보안 수준진단 지표 6.4.2 사용자 PC를 업무용과 인터넷용으로 분리 항목이다. 망 분리는 가상화 기술을 통한 논리적 망 분리와 PC를 2대로 사용하는 물리적 망 분리가 존재한다. 국가정보원 및 정보보안 기본지침 제40조(내부망 · 인터넷망 분리)는 둘다 허용하고 있으나, 동 지표는 물리적 망 분리만 허용하고 있어 논리적인 망 분리를 한 대학은 점수 획득에 제한이 존재한다. 물리적 망 분리 환경이 더 안전한 PC환경일 수 있으나, 대학에서는 여러 SW나 인터넷을 활용한 교수법 등 다양한 방식으로 교육을 진행하므로 업무용 PC와 인터넷용 PC의 완벽한 분리 운영이 어렵다.

따라서 대학에서도 주요 정보를 취급하는 산학협력단이나 연구소, 대학원 등 부서나 유관 기관을 중심으로망 분리를 반영할 수 있는 방안이 필요하다. 또한, 내부적 지침에 따라 핵심 자원을 구분하고 중요 부서에 대해 우선적으로 망 분리를 시행한 대학에 대해 이점을 줄 수 있는 지표나 제도 개선이 필요하다.

마지막으로 현재 대학의 전자결재나 학사시스템 등 행정망에 관한 제안이다. 현재 대학은 모바일 앱을 통한 출결 관리나 전자결재 시스템, 학사시스템 등 구축이 활발히 진행되고 있다. 그러나 정보보호 수준진단에서는 모바일을 포함한 업무용 단말기에 대한 보안만 존재하고, 모바일 애플리케이션 관련한 정보보호 지표는 반영되어 있지 않다. 따라서 모바일 애플리케이션 취약점 분석 등 관련 지표를 반영할 필요가 있다[8,9].

3.2 시사점

연구 결과 사립 대학교의 경우 국립 대학교보다 수준진단 점수가 대체로 낮았고, 대학 규모에 따라서도 보안 수준의 차이가 존재함을 알 수 있었다. 다만, 대학은 규모가 작다고 해서 보유한 연구 기술이나 데이터의 값어치도 낮다고 할 수 없다.

따라서 본 연구의 결론과 같이 대학이 능동적으로 여러 보안 행동을 할 수 있도록 유도하는 지원 체계나 정보보안 수준진단 지표 수정이 필요하다.

다만, 수준진단을 위한 지표라는 것은 무엇보다 객관성이 중요한 요소이므로 섣불리 수정할 경우 특정 요소

에만 유리하게 변질될 가능성이 존재한다.

따라서, 특정 그룹에서만 성취도가 현저하게 낮거나, 최신 트렌드를 반영하지 못한 부분에 변화를 가져오는 것이 중요하다.

또한, 매년 급변하는 정보보호 환경에 대비할 수 있는 전문가의 확보가 우선되어야 할 것이며, 전담 인력이 없더라도 완전히 정보보호 업무에 일임할 수 있는 환경을 조성하여 국가기관에서 제공하는 정보보호 가이드를 업무에 충분히 적용할 수 있는 시간과 기회를 주어야 할 것이다.

References

[1] Netwrix, 2023 Hybrid Security Trends Report Additional Findings for the Education Sector, Analysis Report, Netwrix, USA, pp.1-2.

[2] Dr. J. Chapman, Cyber-security in Higher Education, Analysis Report, Jisc, England, pp.3.

[3] I. S. Lee, A Study on Reinforcement Measures for Information Protection of SMEs : Focusing on training security personnel, Master's thesis, Dongguk University, pp.1-3.

[4] H. C. Kwon, Y. J. Lee, W. H. Park, "Comparative Analysis of Cyber Attacks of Korea Government and Policy Countermeasures", *Convergence security journal*, Vol.20, No.5, pp.19-26, 2020.
DOI: https://doi.org/10.33778/kcsa.2020.20.5.019

[5] E. H. Lim, University Information Security Diagnosis Results, Analysis Report, University Education Research Institute, Korea, pp.1-3.

[6] J. W. Kim, Y. J. Lee, S. D. Lee, "Design and implementation of control support intelligence for the enhancement of efficiency in the Security Operations Center (SOC)", *Korean Society of Industrial-Academic Technology*, Vol.24, No.8, 607-614, Aug 2023.
DOI: https://doi.org/10.5762/KAIS.2023.24.8.607

[7] J. D. Yu, Y. J. Lee, "Advancing Defense Cyber Security through the Development of International Multilateral Conferences", *Korean Society of Industrial-Academic Technology,* Vol.24, No.8, pp. 461-467, Aug 2023.
DOI: https://doi.org/10.5762/KAIS.2023.24.8.461

[8] H. G. Lee, Research and Analysis Report on Ways to Improve Information Security Level Diagnosis, Korea Education Network Operation Headquarters, Korea, pp.170-171.

[9] T. Y. Kim, T. S. Kim, H. J. Jun, "Impact of Organizational Security Awareness and Activities on the Level of SMEs Technology Protection", *Korea Industrial Security Research*, Vol.12, No.1, pp.79-109, Apr.2022.
DOI: https://doi.org/10.33388/kais.2022.12.1.079

이 기 호(Ki-Ho Lee) [정회원]

- 2018년 2월 : 동국대학교 국어국문학과 (문학사)
- 2024년 2월 : 극동대학교 인공지능 보안학과 (공학석사)
- 2020년 10월 ~ 현재 : 극동대학교 개인정보보호 및 정보보호 담당 직원

〈관심분야〉
사이버보안, 융합보안, 산업보안

이 용 준(Yong-Jun Lee) [종신회원]

- 1999년 2월 : 강남대학교 전자계산학과 (공학사)
- 2001년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2005년 2월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2010년 2월 ~ 2016년 3월 : KISA 사이버침해대응본부 수석연구위원
- 2010년 2월 ~ 2016년 3월 : 군사안보지원사 국방보안연구소 연구권
- 2016년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수

〈관심분야〉
사이버보안, 융합보안, 산업보안

강 장 묵(Jang-Mook Kang) [정회원]

- 1999년 2월 : 고려대학교 일반대학원 석사
- 2005년 8월 : 고려대학교 정보보호대학원 (공학박사)
- 2020년 8월 ~ 현재 : 동국대학교 국제정보보호대학원 AI융합 보안 교수
- 2021년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수

〈관심분야〉
인공지능, 블록체인, 융합보안, 산업보안