Journal of the Korea Academia-Industrial cooperation Society
Vol. 25, No. 3 pp. 609-614, 2024

https://doi.org/10.5762/KAIS.2024.25.3.609
ISSN 1975-4701 / eISSN 2288-4688

기업 모집단 기반 정보보호 최고책임자 신고의무 대상 선별 프로세스에 대한 연구

양형초[1], 이용준[1*], 강장묵[2]
[1]극동대학교 인공지능보안학과, [2]동국대학교 정보보호학과

A Study on The Selection Process for Those Subject to Reporting Obligation to The Chief Information Security Officer Based on The Corporate Population

Hyeong-Cho Yang[1], Yong-Joon Lee[1*], Jang-Mook Kang[2]
[1]Department of AI Security, Far East University
[2]Department of Computer and Information Security, Dongguk University

요 약 최근 경제·사회 전반의 디지털 대전환으로 인해 기업의 규모나 업종에 상관없이 인터넷 침해사고의 발생이 증가하고 있으며 이는 기업의 경제적 피해뿐 아니라 대외 신뢰도 저하로도 이어진다. 이에 따라 정보보호 관련 업무를 총괄하며 조직의 중요 정보와 자산을 보호하는 정보보호 최고책임자(CISO)에 대한 지위와 역할이 중요해지고 있다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서는 정보보호 최고책임자를 의무적으로 지정하여 신고하도록 하고 있으나, 기업이 의무대상임을 스스로 인지하여 신고하도록 되어 있어 일부 기업들의 신고율이 높지 않은 실정이다. 이에 본 연구에서는 정보보호 최고책임자 지정·신고 제도의 신고의무 제외 기준과 의무대상 기준 등을 반영하여 대상을 선별할 수 있는 프로세스에 대해 연구하였다. 본 연구를 통해 기업이 의무대상 여부를 직접 확인할 수 있게 함으로써 정보보호 최고책임자의 신고율을 높이고 기업의 정보보호를 강화하는데 도움이 되고자 하였다.

Abstract Owing to the recent digital transformation of the economy and society overall, the number of internet breaches is increasing regardless of the size or industry of the company, which causes economic damage and leads to a loss of external credibility. As a result, the position and role of the Chief Information Security Officer (CISO), who oversees information protection-related tasks and protects the organization's important information and assets, is becoming increasingly important. The "Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc." mandates the designation and reporting of a Chief Information Security Officer. On the other hand, the reporting rate of some companies is not high because companies are required to recognize and report that they are subject to this obligation. This study examined the process for selecting targets by reflecting the exclusion and obligation criteria of the Chief Information Protection Officer Designation and Reporting System. By enabling companies to check whether they are subject to the obligation, this study aims to help increase the reporting rate of information security officers and strengthen corporate information protection.

Keywords : CISO, Information Security, Network Communication Act, Mandatory Target, Selection Process

*Corresponding Author : Yong-Joon Lee(Far East Univ.)
email: hyoungcho79@gmail.com
Received February 6, 2024 Revised February 27, 2024
Accepted March 8, 2024 Published March 31, 2024

1. 서론

1.1 연구 배경 및 내용

1.1.1 연구 배경 및 목적

4차 산업혁명 기술 발전으로 경제·사회 전반의 디지털 전환(Digital Transformation) 속도가 빨라지고 있다. 또한, 코로나19 장기화 과정에서 생산, 소비, 유통 방식 등이 대면 중심에서 비대면 중심으로 변화함에 따라 글로벌 디지털 전환 흐름이 더욱 가속화되었다[1].

더불어 기업의 규모나 업종에 상관없이 인터넷 침해사고의 발생이 증가하고 있으며, 사이버 보안 위협도 급속도로 확대되고 있다. 이러한 침해사고는 기업의 경제적 피해와 함께 경영에 직·간접적인 영향을 끼치게 되며, 안전한 서비스 운영을 위해서는 정보보호가 중요하다는 것을 의미한다. 이에 따라 정보보호 업무를 총괄하는 정보보호 최고책임자(CISO : Chief Information Security Officer)에 대한 역할 및 지위의 중요성이 확대되고 있다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 “정보통신망법”)에 따르면 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 한다[2].

또한, 2021년 6월 정보통신망법의 개정으로 정보보호 최고책임자에 대한 지위 기준이 구체화되었으며 정보보호 필요성이 큰 ‘중기업’ 이상으로 신고의무 대상자를 합리화하고 제외대상자를 확대하였다[3]. 그러나 기업이 스스로 의무대상임을 인지하여 정보보호 최고책임자를 지정하고 신고하도록 되어 있고, 이로 인해 중기업들의 신고율이 높지 않고 있다. 또한, 정보보호 최고책임자의 부재로 인해 일부 기업들은 보안위협에 취약한 상황으로 이를 개선할 수 있는 모델에 대한 연구가 필요하였다.

1.1.2 연구 내용 및 범위

본 연구는 정보보호 최고책임자 신고의무 대상을 선별할 수 있도록 기업 규모에 따른 모집단을 구축하고, 이 모집단을 통해 의무대상을 선별하는 프로세스에 대해 제안하는 연구이다. 이를 통해 경영진 및 정보보호 관련 임직원들이 의무대상 여부를 직접 확인할 수 있도록 하고자 하였다. 이로써 정보보호 최고책임자에 대한 신고율을 높이고, 기업이 스스로 정보보호를 강화할 수 있도록 수행된 연구이다.

본 연구에서는 정보보호 최고책임자를 신고한 기업들과 미신고한 기업들에게 설문조사를 수행하고, 그 결과를 분석하여 연구의 필요성과 기초 자료를 확보하고자 하였다. 또한, 모집단을 구축하기 위한 방법론을 제안하고 신뢰성이 검증된 기업 데이터 확보를 통하여 기업 모집단을 구축하고자 하였다.

이에 본 연구에서는 정보보호 최고책임자 신고의무 대상을 선별하는 프로세스를 구축하고, 이를 통해 신고제외 대상, 신고의무 대상의 선별이 가능하도록 하였다. 향후 연구로는 선별 프로세스를 통한 선정 모델을 설계 및 구현하여 개정 전의 의무대상 수와 비교 분석·검증하는 연구수행이 필요하다.

1.1.3 논문의 구성

본 논문은 총 4장으로 구성하였다. 1장은 연구 배경과 범위에 관하여 서술하였다. 2장에서는 관련연구로써 정보보호 최고책임자의 역할과 관련 제도에 대해 기술하고, 정보보호 최고책임자 신고 및 겸직 현황 등을 조사하였다. 3장에서는 설문결과를 수행한 결과를 분석하였고, 구축한 기업 모집단을 기반으로 한 의무대상 선별 프로세스에 관하여 기술하였다. 4장은 결론으로써 연구 결과를 정리하였고, 추가 연구 사항을 도출하였다.

2. 관련연구

2.1 정보보호 최고책임자의 역할과 관련 제도

2.1.1 정보보호 최고책임자의 역할

정보보호 최고책임자는 조직의 전반적인 정보보호를 총괄하고 책임지는 임원을 의미하며 조직의 정보보호 전략을 수립하고, 이를 조직의 전반적인 비즈니스 목표와 일치시킨다. 이를 위해 조직의 보안 위험을 식별하고 위험 평가, 위험관리 계획 수립, 위험 감소를 위한 통제를 이행한다. 정보보호 정책, 표준, 지침 및 절차 등을 개발하고 침해사고 발생을 대비한 대응 프로세스와 복구 절차를 수립한다.

최고경영진은 정보보호 최고책임자가 필요한 권한과 자원을 확보할 수 있도록 하여야 하고, 정보보호 관련 현황에 대한 직속 보고 체계를 마련하여야 한다. 또한, 위험을 효과적으로 관리하고, 보안 과제들을 극복하는 데 필요한 인력과 예산을 지원하여야 한다[4]. 전형적인 기업의 조직 구조와 정보보호 최고책임자의 주요 역할은 Fig. 1과 같다[5].

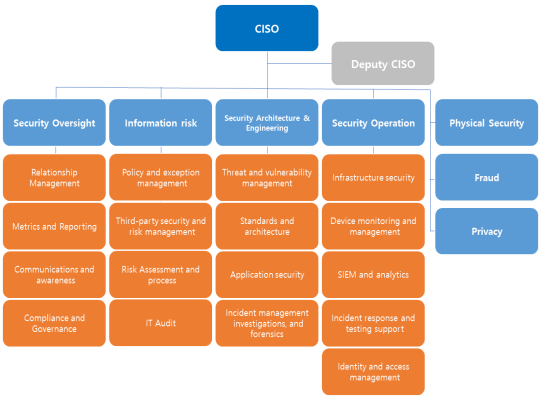

Fig. 1. Key roles of the Chief Information Security Officer

2.1.2 정보보호 최고책임자 지정·신고 제도

정보보호 최고책임자 지정·신고 제도는 최고경영자가 정보보호 최고책임자를 지정하여 공식적으로 임명하고 신고하는 제도이다. 정보통신망법 제45조3(정보보호 최고책침자의 지정 등)에 따라 정보보호 필요성이 큰 '중기업' 이상의 정보통신서비스 제공자는 정보보호 최고책임자 지정·신고를 의무적으로 수행해야 한다[3].

지난 2021년 6월, 정보통신망법의 개정으로 정보보호 최고책임자의 지위를 기업 규모에 따라 낮추고, 의무대상의 규제를 완화하였다. Table 1과 같이 신고의무 제외 대상이 확대되어, 자본금 1억 원 이하인 자와 소기업 등은 정보보호 최고책임자를 신고하지 않아도 된다. 또한, 정보보호 최고책임자의 업무를 명확히 정의하고 유사업무와의 겸직이 가능하도록 개선하였다.

Table 1. Exemptions to the Chief Information Security Officer's reporting obligations

Before revision	After revision
· Additional telecommunication service provider with Capital of KRW 100 Million or Less · Small business · Some small businesses	· Persons with capital of 100 million won or less · Small business · Medium-sized enterprises that do not fall under the following: - Telecommunications business operator - ISMS mandatory - Personal information processor - Mail order seller

2.2 정보보호 최고책임자 관련 현황 분석

2.2.1 정보보호 최고책임자 임명 현황

국내 기업들의 정보보호 기반 및 환경, 침해사고 예방, 침해사고 경험 및 대응 등 정확한 정보보호 현황을 파악하기 위해 실시되는 정보보호 실태조사에 따르면 정보보호 관련 책임자가 임명된 국내 기업체의 비율은 Fig. 2와 같이 '정보관리 책임자' 28.9%, '정보보호 최고책임자' 19.2%로 나타났다[6]. 이처럼 정보보호 최고책임자의 임명 비율이 더 낮은 것은 기업들이 정보보호 최고책임자의 중요성에 대한 인식이 낮음을 보여준다.

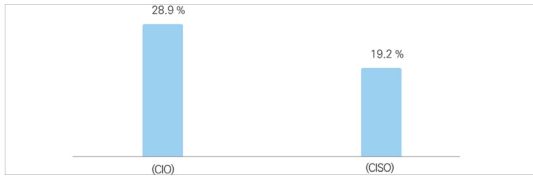

Fig. 2. Appointment of a person responsible for information protection[6]

Fig. 3은 종사자 수 규모별 정보보호 최고책임자 임명 비율을 나타내며 10~49명, 50~249명의 규모에서 임명 비율이 상대적으로 낮은 것을 볼 수 있다. 이는 중규모 기업들에게 제도에 대한 안내와 의무대상 여부를 인식시킬 필요가 있음을 보여준다.

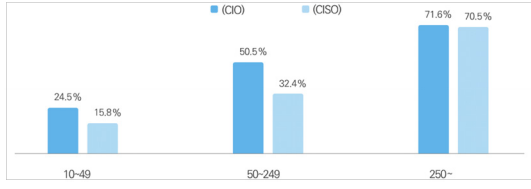

Fig. 3. Appointment of information protection-related managers by size[6]

2.2.2 정보보호 최고책임자 신고 현황

정보통신망법 시행령에 따라 중앙전파관리소는 정보보호 최고책임자 신고 업무를 과학기술정보통신부로부터 위임받아 수행하고 있으며, 정보보호 최고책임자 신고 업체현황 데이터를 매분기별로 공공데이터 포털에 공개하고 있다[7]. 이 데이터의 세부적인 분석을 통해 기존 의무대상 기준으로 일반기업 규모별 신고 현황을 파악하였다.

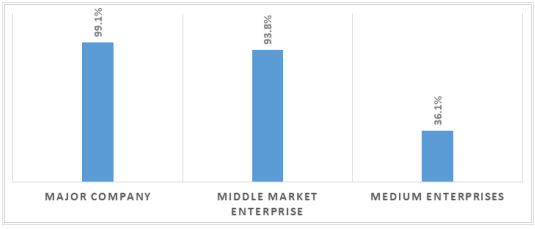

Fig. 4. Reporting rate to CISO by company size

위 Fig. 4는 일반기업에 대한 정보보호 최고책임자 신고 현황으로써, 대기업 99.1%, 중견기업 93.8%로 매우 높은 신고율을 보인 반면 중기업 36.1%로 상당히 낮은 신고율을 보이고 있다. 이는 중기업을 대상으로 의무대상을 선별할 수 있는 프로세스나 모델에 대한 연구가 필요함을 보여준다.

3. CISO 신고의무 대상 선별 프로세스

3.1 설문조사 결과 분석

3.1.1 설문조사 수행 목적 및 표본

정보통신망법 개정 전(2018년 6월) 기준으로 정보보호 최고책임자 신고기업과 미신고기업을 분류하여 설문조사를 실시하고, 이를 통해 연구의 필요성과 연구를 위한 기초 자료를 확보하고자 하였다. 이에 신고기업과 미신고기업 각각 설문 문항을 설계하여 조사 후 결과를 분석하였다.

설문조사를 위한 표본 설계는 정보보호 최고책임자 신고기업 대상 약 85%, 미신고기업 대상 약 15%로 1차 분류하고 대기업, 중견기업, 중소기업으로 나누어 규모별로 2차 분류하여 표본을 설계하였으며 총 표본 수는 약 2,000여개이다.

3.1.2 신고기업 설문조사 주요결과 분석

신고기업의 '정보보호 최고책임자 현재 직급'에 대한 조사 결과, 이사급 34.3%, 부장급 이하 29.8%, 대표이사 17.2% 순으로 파악하였다. 기업 규모별로 비교해보면 기업 규모가 작을수록 대표이사가 높았으며, 대기업과 중견기업에서도 부장급 이하 비율이 비교적 높음을 Fig. 5와 같이 확인하였다.

정보통신망법의 정보보호 최고책임자 지위 기준에 따르면 대규모 기업은 이사급, 중기업 이상은 부서의 장, 소기업은 사업주 또는 대표자를 지정하도록 되어 있다. 그러나 이를 준수하지 않는 비율이 높은 점으로 봤을 때 제도의 기준에 대한 준수 여부를 판단 할 수 있는 체계 마련이 필요해 보인다.

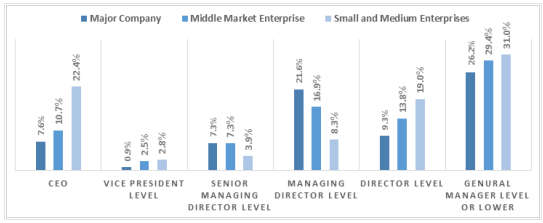

Fig. 5. CISO current position (by reporting company size)

3.1.3 미신고기업 설문조사 주요결과 분석

미신고기업의 '정보보호 최고책임자 지정·신고 제도에 대한 인지도'에 대한 조사 결과, '자세히 알고 있다'가 11.3%로 매우 낮았으며, '신고 의무대상임을 알고 있는가?'에 대한 조사 결과는 Fig. 6과 같이 '잘 모름'과 '아니오'의 합이 87.9%로 매우 높았음을 파악하였다.

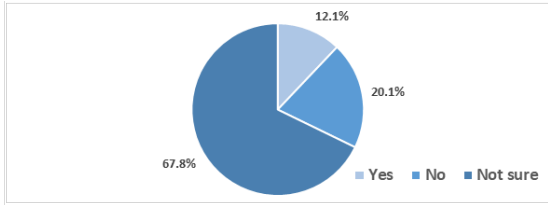

Fig. 6. Awareness of CISO reporting obligations

이처럼 신고의무 대상 여부조차 인지하지 못하고 향후 추진 계획도 없는 점을 봤을 때, 의무대상 기업들이 현 제도에 따른 대상임을 알 수 있도록 선별 프로세스에 대한 연구가 시급하다 할 수 있었다.

3.2 신고의무 대상 선별 프로세스 설계

3.2.1 기업 모집단 구축 방법론

3.1절의 설문조사 결과 분석을 통해 기업의 규모에 따른 정보보호 최고책임자 신고의무 대상에 대한 선별할 수 있는 연구가 시급한 것을 확인할 수 있었으며, 이는 본 연구의 필요성 및 방향성과 연결되었다. 신고의무 대상을 선별하는 프로세스 개발에 앞서, 규모별 기업 모집단을 구축하고 이를 활용하고자 하였다. 모집단 구축을 위한 방법론으로 다음 절차를 제안하였다[8].

(1) 규모와 운영 방식에 따라 분류 후 그룹을 만든다.

(2) 중기업의 신고의무 제외 여부를 판단하는 기준에 해당하는 그룹을 추가한다.
(3) 각 그룹별 데이터 출처를 조사하고 출처가 없는 경우 데이터 발굴 기법을 수립한다.
(4) 각 그룹의 기업리스트 내용에 포함될 기업 정보(의무대상 판단을 위한 필수정보)를 정의한다.
(5) 각 그룹에 해당되는 기업들을 조사하여 기업 모집단의 구축을 완료한다.

3.2.2 기업 모집단 구축 결과

앞서 정의한 모집단 구축 방법론에 따라 수행된 결과는 다음과 같다[8].

(1) 기업의 규모와 운영 방식에 따라 '기업집단(동일 기업집단 소속 국내회사들의 직전연도 자산총액이 5조원 이상인 경우[9])', '중견기업(자산총액이 5천억 원 이상인 경우[10])', '중기업', '공기업', '병원(「의료법」 제3조의4에 따른 상급종합병원)'으로 그룹을 생성하였다.
(2) 중기업 중 '전기통신사업자', '정보보호 관리체계 의무대상자' 그룹을 추가하였다.
(3) 각 그룹에 대한 데이터 출처를 조사한 결과, '기업집단' 그룹은 기업집단포털의 기업집단공시자료[11], '중견기업' 그룹은 중견기업 정보마당의 중견기업 목록[12], '중기업' 그룹은 중소기업 현황정보시스템의 중기업 목록[13], '공기업' 그룹은 공공기관 경영정보 공개시스템의 공공기관 현황[14], '병원' 그룹은 공공보건의료지원센터의 공공보건의료기관정보[15], '전기통신사업자' 그룹은 과학기술정보통신부 및 중앙전파관리소 신고 현황[16,17], '정보보호 관리체계 인증 의무대상자' 그룹은 한국인터넷진흥원의 인증서 발급 현황[18]을 통해 확보하고자 하였다.
(4) 의무대상을 판단하기 위해 필요한 기업 정보로는 기업명, 사업자 등록번호, 법인 등록번호, 표준산업분류, 자산총액 등을 정의하였다.
(5) 위 단계를 통해 전체 7개 그룹의 모집단을 구축 완료하였다.

3.3 신고의무 대상 선별 프로세스

3.3.1 대상 선별 프로세스 설계

앞서 구축된 7개 그룹의 모집단을 기반으로 신고의무 제외 요건인 '개인정보처리자', '통신판매업자', '전자금융거래법 대상'을 추가로 반영하여, 의무대상을 선별할 수 있는 프로세스를 Fig. 7과 같이 설계하였다. 이 프로세스를 통해 의무대상 제외자와 기업의 규모에 따른 신고의무 대상자를 분류할 수 있다.

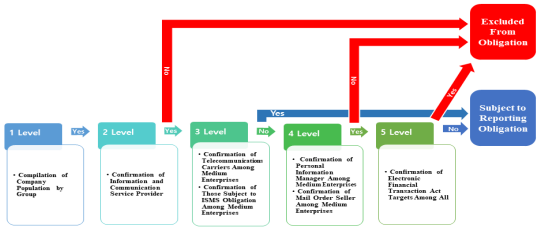

Fig. 7. CISO reporting obligation selection process

3.3.2 대상 선별 프로세스 세부절차

선별 프로세스를 통해 '의무대상 제외', '신고의무 대상'을 판단하는 단계별 세부 수행 내용은 아래와 같다.

(1) 7개 그룹에 대한 기업 모집단을 전체 취합한다.
(2) 전체 기업 모집단에서 홈페이지 운영여부 등을 통해 정보통신서비스 제공자를 확인한다. 이에 해당되지 않으면 의무대상 제외로 분류한다.
(3) 중기업 모집단과 전기통신사업자, 정보보호 관리체계 인증 의무대상자 모집단을 비교한다. 이에 해당되는 중기업은 신고의무 대상으로 분류한다.
(4) 남은 중기업 모집단 중 홈페이지 개인정보처리방침 등을 통해 개인정보처리자를 확인하고, 공정거래위원회의 통신판매업자를 비교한다. 이에 해당되지 않으면 의무대상 제외로 분류한다.
(5) 남은 기업 모집단 중 「전자금융거래법」을 우선 적용 받는 대상인지를 확인한 후 의무대상 제외 및 신고 의무대상으로 최종 분류한다.

4. 결론

본 연구에서는 기업의 규모에 따라 모집단을 구축하고, 이 모집단을 이용하여 정보보호 최고책임자 신고의무 대상을 선별하기 위한 프로세스를 연구하였다. 프로세스의 각 단계를 거치며 기업 규모별 신고의무 대상을 선정하는 모델을 개발하였다.

제안된 모델은 운영 중인 제도의 의무대상 기준과 신고의무 제외 기준을 반영하였으며 신고의무 대상을 명확하게 선별할 수 있는 연구라 평가할 수 있다. 향후 추가 연구로는 선별 프로세스를 통한 모델을 설계하고 구현하여 개정 전 의무대상 수와 결과값을 비교 및 검증하는 연구의 수행이 필요하다.

References

[1] Gyeongwan Noh, Chunggi Baek, Digital Transformation and the State of the ICT Industry in Southeast Asia, BNK Institute of Economics, NO.2022-06, 2022.6.

[2] Act on Promotion of Information and Communications Network Utilization and Information Protection, Article 45-3, 2021.6.8.

[3] Ministry of Science and ICT, Korea Internet & Security Agency, Designating and Reporting a Chief Information Security Officer Guide, 2021.12.

[4] Erastus Karanja, Mark A. Rosso, The Chief Information Security Officer: An Exploratory Study, Journal of International Technology and Information Management, Vol. 26 Issue 2, 2017.
DOI: https://doi.org/10.58729/1941-6679.1299

[5] Gijeong Song, Directions for Risk Management of Customer Information Assets in Financial Institutions, Deloitte Anjin Review 2014 APRIL NO.1, pp.42-43, 2014.

[6] Ministry of Science and ICT, Korea Information Security Industry Association, 2022 Information Security Survey, 2023.

[7] Public data portal, Ministry of Science and ICT, Central Radio Management Service, Status of companies reported to Chief Information Protection Officer, 2022.

[8] Hyeongcho Yang, A Study on the Selection Model for Reporting Obligation to the Chief Information Security Officer by Company Size, Doctoral Dissertation, Far East University Graduate School, 2024.

[9] Enforcement Decree Of The Monopoly Regulation And Fair Trade Act, Article 38, 2023.5.30.

[10] Ministry of Trade, Industry and Energy, Federation of Middle Market Enterprises of Korea, Explanation of scope for mid-sized companies in an easy-to-understand format, 2021.2.

[11] Fair Trade Commission, Corporate group portal, 2023.

[12] Ministry of Trade, Industry and Energy, Medium-sized company information center, 2022.

[13] Ministry of SMEs and Startups, Small and Medium Business Status Information System, 2022.

[14] Ministry of Economy and Finance, Public institution management information disclosure system, 2023.

[15] National Medical Center, Public Health Medical Support Center, 2023.

[16] Public data portal, Ministry of Science and ICT, Basic telecommunication business operator with line facilities, 2023.

[17] Central Radio Management Service, Additional/main business registration status, 2023.

[18] Korea Internet & Security Agency, ISMS-P Certificate issuance status by year, 2023.

양 형 초(Hyeong-Cho Yang) [정회원]

- 2008년 2월 : 전남대학교 정보보호협동과정 석사
- 2024년 2월 : 극동대학교 인공지능보안학과 박사
- 2010년 2월 ~ 현재 : 한국인터넷진흥원 수석연구원

〈관심분야〉
정보보호, 인공지능보안

이 용 준(Yong-Joon Lee) [종신회원]

- 2005년 2월 : 숭실대학교 컴퓨터학과 박사
- 2010년 2월 ~ 2016년 3월 : 한국인터넷진흥원 수석연구원
- 2016년 4월 ~ 2020년 3월 : 국방보안연구소 연구관
- 2021년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수

〈관심분야〉
해킹보안, 국방보안, 인공지능보안

강 장 묵(Jang-Mook Kang) [정회원]

- 2005년 8월 : 고려대학교 정보보호대학원 공학박사
- 2010년 3월 ~ 2017년 8월 : 고려대학교 컴퓨터공학과 연구교수
- 2021년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수

〈관심분야〉
인공지능, 블록체인, 인공지능보안