Journal of the Korea Academia-Industrial cooperation Society
Vol. 25, No. 4 pp. 427-432, 2024

https://doi.org/10.5762/KAIS.2024.25.4.427
ISSN 1975-4701 / eISSN 2288-4688

정보보호 및 개인정보보호 관리체계 인증심사에서 반복적으로 도출되는 주요 결함사항에 대한 분석

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

Analysis of major defects that are repeatedly derived from ISMS-P

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

요 약 오늘날 많은 기업과 기관들이 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증을 위한 노력을 하고 있고, 그 수는 꾸준히 늘어가고 있다. ISMS-P 인증심사 과정에서 최근 3개년간 도출된 전체 결함 사항을 확인하고, 연도별 주요 결함 내용과 도출되는 결함들의 구성을 살펴보았다. 또한 반복적으로 도출되는 결함의 내용과 결함의 원인 및 개선방안을 살펴본다. ISMS-P 인증심사에서 도출된 결함 사항들에 대한 분석을 통하여 연도별 결함 분포와 현황을 확인하고 연도별 주요 결함 사항들의 세부 통제항목별로 알아보았다. 또한 2020년부터 2022년까지 인증심사를 진행한 기업 및 기관을 대상으로 인증심사 시 도출된 결함의 내용 중 3년간 반복적으로 도출된 결함에 대하여 결함의 특성, 결함사례 등을 확인하고 특별히 관리체계 인증제도 관련자들의 의견을 통하여 주요 결함 사항의 원인을 다양한 시각을 확인하였다. 이를 통해 인증심사 시 많은 기업이나 기관에 인증심사시 주요 결함사례를 제시함으로써 기업과 기관들이 정보보호 및 개인정보보호 관리체계를 정교하게 구축하여 운영하고 진행하고, 나아가서 인증심사에 도움이 되고자 한다.

Abstract Today, an increasing number of companies and organizations are pursuing certification for their information security and privacy management system (ISMS-P). This report analyzes the total number of deficiencies identified during ISMS-P certification audits over the past three years, including main deficiency content and composition (by year), as well as recurring deficiency content, causes, and improvement measures. By analyzing the deficiencies identified in the ISMS-P certification audits, we reviewed their distribution and status by year, and examined the detailed control items of major deficiencies by year. Additionally, we analyzed the characteristics of deficiencies and identified cases of such deficiencies among companies and organizations that underwent certification audits between 2020 and 2022. We obtained diverse perspectives on the root causes of major deficiencies through the opinions of those involved in the management system certification process. Our aim is to provide companies and organizations with examples of major deficiencies during certification audits. This will help them establish and operate sophisticated information protection and privacy management systems, and prepare for certification audits.

Keywords : ISMS, ISMS-P, SecurityManagement, Defects, Audit

*Corresponding Author : Yong-Joon Lee(Far East Univ.)
email: yjlee@gmail.com
Received February 1, 2024 Revised February 26, 2024
Accepted April 5, 2024 Published April 30, 2024

1. 서론

현대 사회는 인공지능, 빅데이터, 클라우드, 모바일 등 4차 산업혁명 기술 환경의 구축과 정보통신 기술의 발전을 통한 사회 전 분야에서 정보통신 및 기반 인프라에 대한 의존도가 높아지고 있으며, 정보보호 또한 분야의 구분 없이 중요해지고 있다.

그러나 이러한 이면에는 해킹, 바이러스, 개인정보 유출 등의 역기능 또한 비약적으로 커지고 있다[1]. 그래서 기업이나 기관들은 과거의 직관적이고 경험적인 보안 관리 체계에서 벗어나 체계적인 정보보호 관리체계가 요구되고 있으며, 많은 기업들은 정보보호 활동이 단지 기업의 사업을 수행하기 위한 지원 요소가 아니라 기업의 사업 목표를 달성하기 위한 핵심적인 요소로 인식하기 시작했다[2]. 국내에서는 정보보호 및 개인정보보호 관리체계 인증제도를 마련하는 등 정보보호 정책 수립 및 제도 개선에 노력을 기울이고 있다.

해마다 많은 기업과 기관들이 ISMS-P 인증을 취득하기 위하여 노력하고 있다. 관리체계를 수립 운영하기 위한 컨설팅, 전문인력 확보 등을 통해 ISMS-P 인증을 획득하기 위한 준비를 하고 있으며, 인증 획득을 통한 객관적인 정보보호에 대한 증명을 하고자 하며 이는 사회 전반에 정보보호에 대한 인식변화와 함께 증가하는 추세이다.

본 연구에서는 정보보호 및 개인정보보호 관리체계 인증제도를 살펴보고, 기업이나 기관들이 정보보호 및 개인정보보호 관리체계 인증심사의 결함 사항을 토대로 결함의 내용을 확인한다. 특히 ISMS-P 제도로 통합된 이후인 2020년에서 2022년 총 최근 3개년간 도출된 결함 중에서, 연속적으로 도출되고 있는 주요 결함 사항을 분석한다. 그리고 제도 관계자인 ISMS-P 인증 기업 보안담당자, 인증을 희망하는 기업 보안담당자, 보안업체 ISMS-P 인증 컨설턴트, ISMS-P 인증 심사원의 설문을 통하여 원인에 대한 다양한 의견을 들어보고 향후 ISMS-P 인증을 획득하기를 희망하거나 이미 인증을 보유한 상태에서 사후, 갱신인증을 준비해야 하는 기업, 기관들이 관리체계 수립 및 인증 준비를 위해 반복되어 나타나는 결함을 미리 중점적으로 준비하여 이전보다 정교한 관리체계를 만들어 가는 데 도움이 되고자 한다.

2. 본론

2.1 ISMS-P 인증제도

2.1.1 인증의 개요

ISMS-P 인증은 “정보통신망 이용촉진 및 정보보호 등에 관한 법률”[6] 제47조와 제47조의 2, 동법 시행령 제 47조부터 제54조까지의 규정 및 같은 법 시행규칙 제 3조에 따른 정보보호 관리체계 인증과 “개인정보 보호법”[7] 제32조의2, 동법 시행령 제34조의2부터 제34조의8까지의 규정에 따른 개인정보보호 관리체계 인증을 법적 근거로 하고 있다. 또한 ISMS-P 인증은 “정보통신망 이용촉진 및 정보보호등에 관한 법률”[6]의 개정을 통하여 도입되었으며 2018년 기존 정보보호 관리체계와 개인정보 관리체계 인증이 하나로 통합되어 현재의 ISMS-P 인증이 되었다.

정보보호 및 개인정보보호 관리체계 인증은 크게 ‘ISMS 인증’과 ‘ISMS-P 인증’ 두 가지 종류로 구분된다. ‘ISMS 인증’은 정보보호 관리체계 인증으로 정보보호를 중심으로 관리체계를 인증하는 경우이다. ‘ISMS-P 인증’은 개인정보의 흐름을 포함한 정보보호 관리체계에 대해 인증하는 경우이다.

정보보호 및 개인정보보호 관리체계인증의 심사에는 3가지 종류가 있다.

‘최초심사’는 기업이나 기관이 정보보호 및 개인정보보호 관리체계인증을 최초로 취득하고자 할 때 수행하게 되는 심사이다.

‘사후심사’는 기업이나 기관이 인증을 최초심사를 통해 인증을 취득한 이후에도 정보보호 및 개인정보보호 관리체계가 잘 유지되고 있는지 점검하는 것을 확인하는 인증 심사이다.

‘갱신심사’는 최초심사의 유효기간(3년)을 갱신하기 위한 인증 심사이다[4].

Fig. 1. Information Security and Privacy Management System (ISMS-P) Audit Process[5]

2.1.2 인증심사기준

ISMS-P 인증기준을 살펴보면 관리체계 수립 및 운영과 보호 대책 요구사항과 개인정보 처리단계별 요구사항으로 구성되어 있다[4].

ISMS 인증의 기준항목은 16개의 관리체계 수립 및 운영 항목과 64개의 보호 대책 요구사항 항목 등 총 80개 항목에 대해서 심사를 통하여 관리체계가 수립되고 잘 운영되고 있다는 것이 확인되면 인증을 획득하게 된다.

ISMS-P 인증은 기존 ISMS 인증(관리체계 수립 및 운영과 보호 대책 요구사항)에 개인정보 처리단계별 요구사항 22개 항목을 추가로 심사를 통하여 확인되면 인증을 획득하게 된다[4].

Fig. 2. Information Security and Privacy Management System (ISMS-P) certification audit criteria[5]

2.2 인증심사 주요 결함 사항

Table 1은 3개년 간 심사를 통해 반복적이고 주기적으로 나타나고 있는 결함 수를 보여준다.

Table 1. Top 5 3-year recurring defects[8,9]

No.	Controls	2020	2021	2022	Total
1	2.10.1 Security system operations	44	526	582	1,152
2	2.6.2 Access to information systems	25	301	366	692
3	2.5.6 Review access permissions	34	290	295	619
4	2.10.8 Patch management	23	258	293	574
5	2.7.1 Enforcing a crypto policy	33	249	229	511

2.2.1 주요 결함 사항 발생 원인 분석

2020년부터 2022년까지 인증심사를 통해 도출된 주요 결함 사항 5가지에 대한 발생 원인과 보완 및 조치방안 제시를 통해 인증을 준비하는 신청기관이 중점적으로 준비해야 하는 사항을 확인하면 다음과 같다.

① 통제항목 2.10.1 보안시스템 운영의 결함

솔루션의 형태가 설치형, 클라우드 서비스형으로 늘어나고 확장됨에 따라서 각 솔루션의 특성과 특징을 고려한 운영정책이 필요하게 되었고, 또한 보안시스템별로 적용되어 운영되는 정책에 대한 공식적인 절차를 수립하고 승인 등의 절차를 통해 운영해야 하며 정책의 주기적인 검토가 타당한지 점검해야 한다.

해당 통제항목의 결함이 발생하는 예상 원인을 살펴보면 보안시스템의 특성을 고려한 운영에 대한 운영 절차가 없는 경우, 보안 솔루션 운영 시 정책 등의 절차가 없거나 이행되지 않을 경우, 운영하는 보안 솔루션의 정책 등이 주기적으로 검토되고 있지 않은 경우[3] 등이다.

② 통제항목 2.6.2 정보시스템 접근의 결함

시스템별 운영체제에 접근이 허용된 사용자, 접근 위치, 접근 방법, 접근 수단 등이 정책적으로 정의되고 이행되어야 한다. 보안이 강화된 통신수단을 이용해야 하고, 관리자 등 특수권한자에 대해 추가 인증 등 강화된 인증이 적용되어야 한다. 또한 정보시스템의 특성별로 네트워크 구분이 필요하며, 불필요한 서비스에 대한 통제가 필요하다.

해당 통제항목의 결함이 발생하는 예상 원인을 살펴보면 사용자의 제한이 이루어지고 있지 않은 경우, 서버 간의 불필요한 접근이 허용되고 있는 경우, 접근 시 안전한 접근 수단 및 안전한 인증수단이 적용되지 않은 경우[3], 관리자 등의 특수권한자의 제한 및 강화된 인증 미적용 등이다.

③ 통제항목 2.5.6 접근권한 검토의 결함

개인정보 처리 시스템 및 주요 정보 시스템에 접근하는 사용자 계정의 이력(생성 등)을 보관하고, 주기적으로 검토 및 적정성 여부를 확인해야 하며, 또한 사용자 계정 및 접근권한, 접근 이력에 대해서 책임 추적성이 확보되도록 해야 한다.

해당 통제항목의 결함이 발생하는 예상 원인을 살펴보면 사용자 계정의 관리 절차 등이 없는 경우, 퇴사한 직원의 계정 등 장기 미접속자의 계정이 활성화되어 있는

경우, 절차나 이행이 되지만 일부 누락된 부분이 발견되는 경우[3] 등이 있다.

④ 통제항목 2.10.8 패치 관리의 결함

소프트웨어, 네트워크, 보안시스템 등의 취약점으로 인한 사고 예방을 위해서 최신 패치를 적용해야 한다. 따라서 패치를 진행하는 절차 등이 필요하며 사전에 대상을 선별하고, 사전 서비스 영향도 분석 및 담당자, 관련 제조사 등의 절차를 마련해야 한다. 그러나 때로는 서비스의 영향 문제로 인해 적용이 어려운 경우가 있을 수도 있으나 위험도 분석을 통해 별도의 보완대책을 마련해야 한다. 하드웨어 또는 소프트웨어의 결함이나 체계 또는 설계상의 불완전함으로 인한 취약점 발생 시에 주기적인 패치를 통해 해당 취약점을 관리해야 한다. 또한 서비스 지원이 종료된 시스템에 대한 관리도 진행되어야 한다.

해당 통제항목의 결함이 발생하는 예상 원인을 살펴보면 서비스 지원이 종료된 취약한 운영체제를 사용하는 경우이나 이에 대한 대응계획이나 보완 대책이 없는 경우[3], 패치 절차가 없거나 패치 이력이 장기적으로 확인되지 않는 경우, 패치 업무를 위한 담당자가 지정되지 않고 자산 대장의 정보가 불일치하여 패치 대상에서 누락되는 경우 등이다.

⑤ 통제항목 2.7.1 암호정책의 결함

개인정보 및 주요 중요한 정보의 보호를 위해서 법적 요구사항을 반영하여 암호정책(암호화 대상, 암호 강도, 암호 사용 등)을 수립하여 이행해야 하며 개인정보 및 주요 중요정보의 저장, 전송, 전달 시 암호화를 적용해야 한다. 암호화 알고리즘은 법적인 요구사항 등을 고려한 안전한 암호화 알고리즘을 사용해야 한다. 또한 암호정책에 따라서 전송 및 저장 시 각각에 적합한 암호화를 수행해야 한다.

해당 통제항목의 결함이 발생하는 예상 원인을 살펴보면 법적 암호화 대상이나 누락되어 암호화되지 않고 평문 저장된 경우이거나 인증서의 미사용, 안전한 알고리즘의 미사용[3] 등의 경우이다.

기업 또는 기관이 상황에 맞는 암호화 정책을 적용하는 것이 중요하고, 안전한 알고리즘의 사용과 적용현황의 관리가 중요한 것으로 확인된다.

2.2.2 결함 원인에 대한 제도 관련자 의견

인증심사 시 3개년 동안 지속적 발생한 결함에 대해서 원인을 보다 객관적인 시각으로 확인하고자 ISMS-P 제도 관련자를 대상으로 설문조사를 진행하였는데, 응답 대상자 구성은 인증 희망 기업 보안담당자 12명, 인증유지기업 보안담당자 5명, ISMS-P 컨설턴트 9명, ISMS-P 인증심사원 5명 등 총 ISMS-P 인증제도와 관련된 전문가들 31명으로 되었다.

설문은 ISMS-P 인증심사 시 주요 결함 사항에 대한 원인을 파악하기 위해 진행했으며 중복된 원인을 고려하여 인당 최대 2개까지 응답할 수 있도록 구성했다.

통제항목 2.10.1 보안시스템 운영의 결함의 주요한 원인을 묻는 질문에 응답자 31명의 응답 중 '업무 편의상 절차를 무시한 운영'이 48.4%로 가장 많았고, 다음으로 '정책 등의 주기적 검토 절차 없음' 41.9%, '운영정책의 부재'는 38.7%, '담당자의 운영 미숙' 22.6%, '정책의 과다 허용' 16.1%인 것으로 파악되었다.

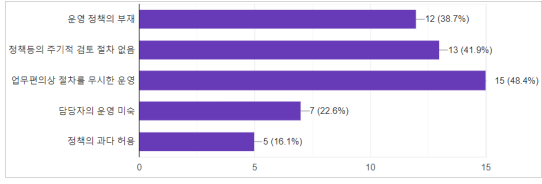

Fig. 3. Survey responses on the causes of deficiencies in security system operations(2.10.1)

제도 관련자들의 의견을 역할 기준으로 살펴보면 가장 주요한 결함 원인을 인증 희망 기업 보안담당자와 ISMS-P 인증 심사원의 경우는 전체 응답과 같은 '업무 편의상 절차를 무시한 운영'으로 응답했으며, 인증유지기업 보안담당자는 '정책의 과다 허용', ISMS-P 컨설턴트는 '정책 등의 주기적 검토 절차 없음'으로 응답하였다.

통제항목 2.6.3 정보시스템 접근 결함의 주요한 원인을 묻는 질문에 응답자 31명의 응답 중 '세션 타임 아웃 미적용 또는 장시간 적용' 48.4%, '서버 간 접속통제 미비' 45.2%, '예산 부족 등으로 인한 접근제어 솔루션 미운영' 41.9%, FTP나 TELNET 같은 '안전하지 않은 서비스 운영'이 22.6%, '불필요한 서비스 운영'이 9.7%로 파악되었다.

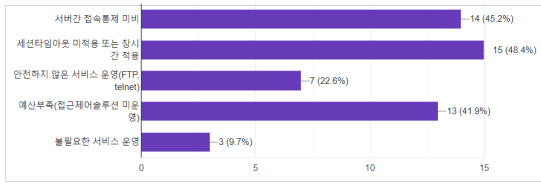

Fig. 4. Survey responses on the causes of deficiencies in access to information systems(2.6.3)

제도 관련자들의 의견을 역할 기준으로 살펴보면 가장 주요한 결함 원인을 전체 응답의 가장 높은 원인으로 지목된 '세션 타임아웃 미적용 또는 장시간 적용'이 ISMS-P 컨설턴트와 같은 의견으로 가장 많은 원인으로 응답되었다.

통제항목 2.5.6 접근권한 검토의 결함의 주요한 원인을 묻는 질문에 응답자 31명의 응답 중 '접근권한 검토 정책/기준 미비' 45.2%, '접근권한 부여 시 권한 과다부여, 45.2%로 두 항목이 가장 많은 응답이 있었고, '접근권한 검토 수행 이력 확인 불가' 35.5%, '정책과 맞지 않는 장기 미사용 계정 활성화' 29%, 접근권한 의심 사례에 대한 후속 조치 미비' 16.1%로 파악되었다.

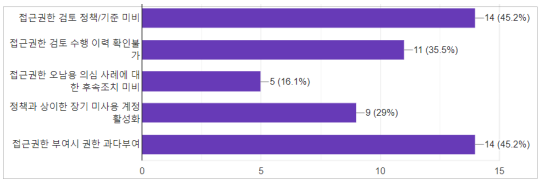

Fig. 5. Survey responses on causes of defects in access review(2.5.6)

제도 관련자들의 의견을 역할 기준으로 살펴보면 가장 주요한 결함 원인을 '접근권한 검토 정책/기준 미비'의 경우 인증 희망 기업 보안담당자와 인증유지기업 보안담당자가 주요 결함 원인으로 응답했으며, ISMS-P 컨설턴트와 ISMS-P 인증심사원의 경우는 '접근권한 검토 수행 이력 확인 불가'를 주요 결함 원인으로 응답했다. 또한 '접근권한 부여 시 권한 과다부여'의 경우는 인증유지기업 보안담당자와 ISMS-P 인증심사원의 의견이 동일했다.

통제항목 2.10.8 패치 관리의 결함의 주요한 원인을 묻는 질문에 응답자 31명의 응답 중 '예산 부족으로 서비스지원 종료 버전 사용' 58.1%로 가장 많은 응답을 보였고, '패치 적용 정책/절차 미비' 48.4%, '내부망 단말기의 인터넷을 통한 패치 업데이트' 25.8%, '담당자 지정 안됨' 19.4%, '패치이력 확인 안됨' 12.9% 로 파악되었다.

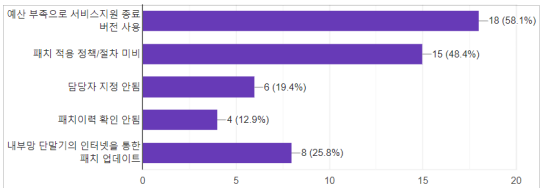

Fig. 6. Survey responses on causes of deficiencies in patch management(2.10.8)

제도 관련자들의 의견을 역할 기준으로 살펴보면 가장 주요한 결함 원인을 '예산 부족으로 서비스 지원 종료 버전 사용'이 주요 결함 원인으로 지목되었으며 인증 희망 기업 보안담당자와 ISMS-P 심사원의 의견이 같은 것으로 나타났다.

통제항목 2.7.1 암호정책 적용의 결함의 주요한 원인을 묻는 질문에 응답자 31명의 응답 중 '암호화 관련 내부정책 미비' 54.8%로 가장 많은 결함 원인으로 응답되었고, '저장·전송구간 암호화 미비' 45.2%, 안전하지 않은 알고리즘 사용' 38.7%, '개인정보의 암호화 법적 기준 미비' 19.4%, '패스워드의 일방향 암호화 미적용' 9.7%로 파악되었다.

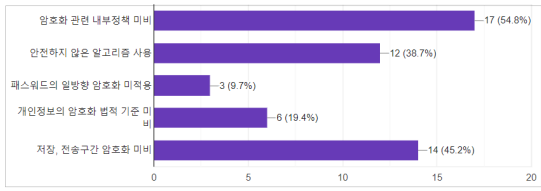

Fig. 7. Survey responses on causes of deficiencies in encryption policy enforcement(2.7.1)

제도 관련자들의 의견을 역할 기준으로 살펴보면 가장 주요한 결함 원인을 인증 희망 기업 보안담당자는 '암호화 관련 내부 정책 미비'를 결함 원인으로 응답했고, 인증유지기업 보안담당자는 '안전하지 않은 알고리즘 사용'으로 응답했으며, ISMS-P 컨설턴트와 ISMS-P 인증심사원의 경우는 '저장, 전송구간 암호화 미비'를 주요 결함 사항으로 응답하였다.

3. 결론

현재도 많은 기업 또는 기관들이 정보보호 및 개인정보보호 관리체계 인증을 취득하기 위해서 지속적인 노력을 진행하고 있다. 또한 인증제도의 개선을 위한 논의도 많이 이루어지고 있으며 양질의 심사원 양성을 위한 노력도 함께 진행되어 전체적으로 정보보호 및 개인정보보호 관리체계 인증제도는 바람직한 방향으로 진행되어가고 있다고 볼 수 있다.

3년 동안 반복적인 양상으로 도출되는 결함에 대해서 특징과 결함사례, 제도 관련자 설문조사를 통하여 결함 원인에 대한 응답자의 의견도 함께 살펴보았고, 특히 제도 관련자들의 경험이나 지식, 현재 수행하고 있는 역할

에 따라서 의견이 다를 수 있음을 확인하였다.

인증심사 시 자주 도출되는 결함사례를 통하여 인증심사를 최초로 준비하는 기업 또는 기관들이나 이미 인증을 보유하고 있는 기업 또는 기관들도 인증심사 준비 시 중점적으로 준비해야 하는 주요 결함 사항 및 조치방안, 예상되는 결함 원인을 다양한 시각에서 제시함으로 준비하는 기업 또는 기관들에 도움이 되고자 하였다.

나타나는 모든 결함의 형태는 결국 예산과 인력 등 경영자의 지원 부족, 정책 절차 등 관리체계의 수립의 미흡, 환경이나 구조의 문제로 인한 관리체계 이행의 어려움에 있는 것으로 확인되었다. 또한 인증심사를 위한 관리체계의 운영이 형식적인 수준에서 그치는 것도 비슷한 결함이 계속 발생하고 있는 것으로 보여, 의무대상자의 기준, 인증기준도 기업의 규모별, 산업별로 달라져야 할 필요가 있어 보인다.

References

[1] Jang, Sang-Soo, and Lee, Hoseop, "A Study on the Analysis of Deficiencies in Information Security Management System (ISMS) Certification Audit", *Journal of the Korean Information Protection Society of Information Protection*, v.20 no.1, pp.31-38, 2010.02

[2] Kyuman Ko, Jae-Sung Kim, and Sang-Soo Jang, "An Analysis of Common Defects in Information Security Management System (ISMS) Implementation", *Journal of the Korean Society of Information Protection*, v.17 no. 4, pp. 34-41 2007.08

[3] KISA, "Information Security and Privacy Management System (ISMS-P) Certification Standards Guide", 2019.01, 2022.04

[4] KISA, "Information Security and Privacy Management System (ISMS-P) Certification System Guide", 2021.07

[5] Ministry of Science and ICT, Act On Promotion Of Information And Communications Network Utilization And Information Protection and Enforcement Decree Of The Act On Promotion Of Information And Communications Network Utilization And Information Protection

[6] Personal Information Protection Commission, Personal Information Protection Act and Enforcement Decree Of The Personal Information Protection Act

[7] KISA, https://isms.kisa.or.kr

[8] Ministry of Interior and Safety, https://www.data.go.kr, ISMS certification audit annual defect data(2020, 2022)

[9] Ministry of Interior and Safety https://www.open.go.kr, ISMS certification audit annual defect data(2021)

송 호 열(Ho-Yeol Song) [정회원]

- 2024년 2월 : 극동대학교 대학원 인공지능보안학과 (공학석사)
- 2022년 5월 ~ 2023년 10월 : 에프원시큐리티 보안컨설턴트
- 2023년 5월 ~ 현재 : 테크빌교육 정보보안팀 팀장

〈관심분야〉
정보보안, 정보보호 관리체계

이 용 준(Yong-Joon Lee) [종신회원]

- 2005년 2월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2010년 2월 ~ 2016년 3월 : 한국인터넷진흥원 수석연구위원
- 2016년 4월 ~ 2020년 3월 : 국방보안연구소 연구관
- 2021년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수

〈관심분야〉
인공지능보안, 국방보안, 해킹보안

강 장 묵(Jang-Mook Kaong) [정회원]

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

〈관심분야〉
인공지능, 블록체인, 인공지능보안