The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 23, No. 2, pp.15-20, Apr. 30, 2023. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2023.23.2.15
JIIBC 2023-2-3

중소기업의 정보보호 관리체계 개선방안 연구

Improvement Research for Information Protection Management System of Small and Medium Enterprises

윤혜정*, 이용우*, 허희도*, 전삼현**

Hye-Joung Yun*, Yong-Woo Lee*, Hee-Doo Heo*, Sam-Hyun Chun**

요 약 최근 모든 산업에 있어서 디지털 전환이 가속되고 있고 그로 인해 생산되고 이용되는 정보 및 개인정보의 활용이 기업의 성패에 있어서 매우 중요하다. 그러나 이에 대한 역기능으로서 기업의 주요 정보 및 개인정보를 탈취하거나 유출하려는 시도는 계속 증가하고 있고, 이에 대한 적절한 방어 및 대응이 절대적으로 필요하다. 그러나, 중소기업의 경우 대기업에 비해 정보보호에 대한 우선순위나 전문인력 보유 면에서 매우 미흡한 상황이다. 본 논문에서는 국내에서 시행되고 있는 인증 및 진단에 대해 살펴보고, 개인정보보호법 고시 기준 확대 적용 및 지원 제도의 상시 운영을 통해서, 중소기업에 적합한 정보보호 인증 확대 적용 및 지원 제도의 실효성 제고 방안을 제시한다.

Abstract Recently, digitalization is accelerating in all industries, and the use of information and personal information produced and used in the process of it is very important for the success or failure of a company. However, malicious attempts to steal or leak major information and personal information of a company as an adverse effect continue to increase, and appropriate defense and response are absolutely necessary. However, in the case of small and medium-sized enterprises, the priority of information protection and the possession of professional manpower are very insufficient compared to large enterprises. This paper studies the certification and audit implemented in Korea, and suggests ways to expand the certification of the information protection system suitable for SMEs and improve the effectiveness of the support system through the expansion of the privacy law notification standard and operation of support system.

Key Words : information protection certification, information protection, ISMS-P, personal information protection certification, personal information protection, small and medium-sized enterprises

*정회원, 숭실대학교 IT정책경영학과 박사과정
**정회원, 숭실대학교 IT정책경영학과 교수(교신저자)
접수일자 2023년 1월 9일, 수정완료 2023년 3월 5일
게재확정일자 2023년 4월 7일

Received: 9 January, 2023 / Revised: 5 March, 2023 / Accepted: 7 April, 2023
**Corresponding Author: shchun@ssu.ac.kr
Graduate School of IT Policy and Management, Soongsil University, Korea

Ⅰ. 서 론

2022년 한국인터넷진흥원(KISA)이 공개한 '연도별 전체 침해사고 건수'에 의하면, 전체 신고 건수는 '21년 640건, '22년(1월~11월) 1045건으로 매년 증가 추세이며, 그 중, 연도별 랜섬웨어 신고 건수는 '21년 223건, '22년 303건을 차지하고 있으며, 규모별 랜섬웨어 신고 비율은 중소기업이 전체의 88.5%를 차지하고 있다[1]. 랜섬웨어에 일단 감염되면 해커에게 몸값을 지불해도 데이터 전체 복구 비율은 7분의 1에 불과하다고 하며[2], 신고되지 않은 경우까지 감안한다면 보안 침해사고로 인한 중소기업의 피해는 훨씬 더 심각할 것으로 추산된다.

국내에서는 개인정보보호 및 정보보호 수준 제고를 위해 관련 법률에 근거하여 의무대상에 대해 인증 및 진단이 시행되고 있다. 대표적으로 정보보호 관리체계 인증(Information Security Management System, 이하 'ISMS'라 한다) 및 정보보호 및 개인정보보호 관리 체계 인증(Personal information & Information Security Management System, 이하 'ISMS-P'라 한다), 개인정보 관리 수준 진단, 정보보안 관리실태 평가 등이 있다. 그러나, 일부 의무 대상을 제외한 대부분의 중소기업은 인증이나 진단 대상이 아니며, 법의 사각지대에서 안전하지 않은 환경에서 고객의 개인정보를 취급하거나 사업을 하는 경우가 일반적이다.

이에 본 논문에서는 현행 국내 정보보호 및 개인정보보호 인증 및 진단에 대해 살펴보고, 중소기업이 침해사고에 선제적인 대응체계를 갖출 수 있도록 실효성 있는 정보보호 및 개인정보보호 인증 및 진단이 시행될 수 있도록 방안을 제시하고자 한다.

Ⅱ. 정보보호 인증 및 평가

1. ISMS-P 인증제도

ISMS-P 인증제도는 융합화, 고도화되고 있는 침해 위협을 효과적으로 대응할 수 있도록 기업의 정보보호 및 개인정보보호 수준 제고를 위해 운영되고 있으며, 과학기술정보통신부와 개인정보보호위원회가 '정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시'를 공동으로 개정하여 시행하고 있다[3]. ISMS-P는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 및 동법 시행령, 시행규칙에 따른 정보보호 관리체계 인증과 '개인정보 보호법'과 시행령에 따른 개인정보보호 관리체계 인증을 법적근거로 하고 있다.

ISMS와 ISMS-P 인증영역은 [표1]과 같이 ISMS는 80개 항목, ISMS-P는 102개 항목으로 구성되어 있다. ISMS의 의무대상자는 [표2]에 해당되는 자이며, 일반 기업에 해당되는 기준은 이용자수 또는 매출액 기준으로, '정보통신서비스 부문 전년도 매출액이 100억원 이상인 자 또는 전년도 말 기준 직전 3개월간의 정보통신서비스 일일평균 이용자 수가 100만명 이상인 자'이다.

표 1. ISMS, ISMS-P 인증 영역
Table 1. ISMS, ISMS-P Certification Area

인증 영역	항목수	ISMS	ISMS-P
1. 관리체계수립 및 운영	16개	16개	16개
2. 보호대책 요구사항	64개	64개	64개
3. 개인정보 처리 단계별 요구사항	22개	-	22개
합계	**102개**	**80개**	**102개**

표 2. ISMS 의무대상자 기준
Table 2. Mandatory organizations of ISMS

구분	의무대상자 기준
정보통신망서비스 제공자(ISP)	「전기통신사업법」 제6조 제1항에 따른 등록을 한 자로서 서울특별시 및 모든 광역시에서 정보통신망 서비스를 제공하는 자
집적정보통신시설 사업자(IDC)	정보통신망법 제46조에 따른 집적정보통신시설 사업자
매출액 또는 이용자수 요건에 따른 대상자	정보통신서비스 부문 전년도 매출액이 100억원 이상인 자 전년도 말 기준 직전 3개월간 정보통신서비스 일일평균 이용자 수가 100만명 이상인 자 연간 매출액 또는 세입이 1,500억원 이상인 자 중에서 다음에 해당되는 경우 •「의료법」제3조의4에 따른 상급종합병원 • 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교

2. 개인정보 관리수준진단

개인정보 관리수준 진단은 공공기관의 개인정보 관리체계 및 유출 예방 활동 등을 진단하여 국민의 개인정보가 안전하게 관리될 수 있는 기반 조성을 유도하기 위한 제도로, 개인정보 보호법 제11조(자료제출 요구 등) 제2항을 법적근거로 하고 있다[4]. 개인정보 관리수준 진단은 연간 주기로 시행되며, 상황에 따라 일부 변동이 있을수 있으나, 그 전체적인 프로세스는 [그림1]과 같다.

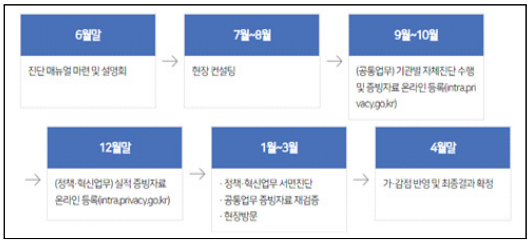

그림 1. 개인정보 관리수준 진단 연간 프로세스
Fig. 1. Annual process of diagnosis of personal information management level

대상기관은 800여개의 공공기관으로, 중앙부처, 지자체, 공공기관, 지방공기업이 그 대상이며, 평가 기준은 정량지표와 정성지표로 구성되어 있다. 정량지표는 자체진단으로 진행하고, 정성지표는 기관별 노력 정도를 평가하기 위한 목적으로 정책과 혁신지표로 구성되어 있다. 기관에서는 정량지표와 정성지표 진단 항목에 자체진단한 내용을 기입하고 실적자료를 제출하며, 개인정보보호위원회와 KISA에서는 작성을 위한 지원 및 1차 검증을 수행한다. 이어, 학계 · 법조계 · 산업계 등 각계 전문가로 구성된 수준진단 위원회에서 대상기관에 대한 현장검증 및 정성지표에 대한 진단을 수행한다.

3. 정보보안 관리실태 평가

정보보안 관리실태 평가는 국가정보원에서 사이버공격 및 위협에 예방 및 대응하기 위하여 중앙행정기관, 광역지자체, 공공기관 대상으로 매년 시행하고 있는 평가제도다. 그 추진 근거로는 국가정보원법, 사이버안보업무규정, 전자정부법, 공공기록물관리법 등이며, 평가지표는 해마다 정보보안 환경변화, 최신 사이버위협 등을 반영하여 수정 및 보완되며, 평가 절차는 [그림2]와 같이 5단계로 구성되어 있다[5].

우선 평가대상으로 선정된 기관은 평가지표를 참조하여 정해진 기간 내에 평가 항목별로 자체평가를 실시한다. 국가정보원은 기관 자체평가에 대한 확인을 위하여 해당 기관을 방문하며, 이때 객관성과 공정성을 위하여 현장 실사에 전문가를 참여시킬 수 있다. 이후 학·연 전문가로 구성된 '정보보안 관리실태 평가위원회'를 개최하여 평가결과에 대한 적정성을 검토·확인한다.

최종 평가 결과는 대상기관에 통보하며, 해당 기관은 평가결과를 자체 정보보안 정책 수립 시 반영하고, 미흡한 점을 개선·보완한다. 또한 평가결과는 국가·공공기관 정부업무평가에 반영하도록 행정안전부 및 기획재정부에 통보된다[4].

그림 2. 공공기관 정보보안 관리실태 평가 절차
Fig. 2. Evaluation procedure for Information security management status of public institutions

4. 중소기업 대상 정보보호 지원 제도

KISA에서는 중소기업·소상공인을 대상으로 개인정보의 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 위하여, 개인정보보호 기술상담 및 온라인 컨설팅, 현장방문 컨설팅 등을 지원하고 있다[6]. 또한, 중소기업의 침해사고 예방 및 대응을 위해 활용할 수 있는 서비스를 운영중이며, 그 내용으로는, '내PC 돌보미(PC 원격 보안점검)', '내서버돌보미(서버 원격 보안점검)', '중소기업 홈페이지 보안강화', '중소기업 보안 취약점 점검', '정보보호사전점검', '중소기업 SW 개발보안 진단' 등이 있다[7].

III. 인증 및 평가 제도의 문제점

1. 공공기관 평가 제도의 문제점 및 특이점

공공기관 대상으로 시행되는 정보보호, 개인정보보호 관련 진단 및 평가는 II에서 살펴본 바와 같이 있으며, 추가로 중앙행정 기관에서 산하기관 대상으로 수행하는 경우도 있다. 공공기관 대상으로 시행되고 있는 정보보호 및 개인정보보호 관련 평가 제도에 있어서 다음과 같은 문제점들이 있다.

가. 기관 간 점검 항목상의 문제

국가정보원에서 발간한 '2022 국가정보보호백서'에 의하면 조사 대상 공공기관 중 정보보호 전담부서를 운영하는 기관은 2020년 46%, 2021년 59%로 조사 되었다[8]. 2021년 조사 내용 중, 국가 전체적인 정보보호 우선순위에 대하여는 2020년과 동일하게 정보보호 담당인력 확충이 필요하다는 응답과 전문부서(관제센터 포함)

확대가 1, 2위를 차지했고, 이 두 응답은 전체의 60%를 차지했으며, 이는 해가 바뀌어도 공공기관 현장에서는 정보보호 인력 부족이 여전함을 보여준다. 그런데, 이에 반해 상당수의 공공기관들은 국가정보원의 정보보안 관리실태 평가와 개인정보보호위원회의 개인정보 관리수준 진단을 매년 받고 있고 그 평가와 진단에 있어서 중복되는 항목도 상당수 있다. 즉, 공공기관은 인력은 부족한데, 서로 다른 기관으로부터 유사한 항목 대응을 위한 인력이 소요되고 있는 것이다.

나. 검증절차의 문제

공공기관 평가 및 점검의 특장점 중의 하나는 해당 제도를 주관하고 있는 기관 뿐만 아니라, 산업계, 학계 등의 민간 전문가 풀을 구성하고, 해당 전문가들을 통해 검증 절차를 거친다는 것이다. 이를 통해, 해당 기관에서 단독 추진하는 경우 대비 다양한 전문가 의견을 청취할 수 있고, 객관적인 점검 결과를 얻을 수 있다. 또한, 점검 결과 하위 그룹에 해당하는 기관에 대해서는 후속으로 전문가 컨설팅 등을 통해 수준을 제고할 수 있는 방안이 제공되고 있으며, 기관들은 점검 결과가 기관 평가에 반영되기 때문에 대체로 이 일련의 과정에 적극적으로 동참한다. 즉, 공공기관은 정보보호 수준제고를 위해 준비된 전문 인력을 활용하는 절차와 기관의 참여를 강제할 수 있는 제도적 장치가 마련되어 있다. 상대적으로 민간기업에는 지원되지 않는 좋은 여건이 공공기관에는 편중되게 제공되고 있는 것이다.

2. 민간기업의 정보보호 제도적인 문제점

금융업계 등 특수한 산업을 제외한 일반 민간기업에 있어서는 ISMS 인증 의무대상자 이외에는 진단이나 평가 등에 대해 법적인 의무나 강제사항이 거의 없다. 즉, 정보보호 및 개인정보보호에 있어서 민간은 기본적으로 자율적으로 준비하고 대응해야 하며, 그로 인해 다음과 같은 이슈들이 발생하고 있다.

가. 중소기업 대상 제도적 미비

ISMS 및 ISMS-P 제도는 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 공식적인 증명을 위하여, 인증 의무대상자 및 자율신청자 대상으로 시행되고 있다. 2022년 12월 현재 ISMS 및 ISMS-P 인증 유지 건수는 1018건임을 확인할 수 있으며[9], 이는 의무대상 ISMS 인증 뿐만 아니라, ISMS-P 인증, 금융기관 수검 ISMS까지 포함한 수치다.

정보통신업에서 2021년 신생 중소기업은 25,000개 이상이며, 활동중인 중소기업은 12만개를 훌쩍 넘는다 [표5][10]. 중소기업수와 인증취득 현황에서 알 수 있듯이, ISMS 인증을 취득한 중소기업은 미미하다. 또한, ISMS 의무대상 요건에 해당되지 않는 경우, 추진의 우선순위 및 정보보호 체계 부재로 실질적인 정보보호 수준은 상당히 미흡할 수 밖에 없다.

표 3. 통계청 2021년 정보통신업 기업 규모별 통계
Table 3. Statistics by size of companies in the information and communication industry in 2021 by Statistics Korea

정보통신업 기업규모별	2021년 (단위:개)	
	활동	신생
계	123,518	25,408
대기업	771	32
- 중견기업	407	7
중소기업	122,747	25,376
- 소기업	119,794	25,283
.소상공인	102,191	24,049

나. 현실적 한계

국가정보원의 '2022 국가정보보호백서'에 의하면 민간부문에서 공식적인 정보보호(개인정보보호) 조직을 보유한 국내 사업체의 비율은 11.6%에 불과하다[8].

KISA나 중소기업부에서는 중소기업에서 정보보호 관련 컨설팅이나 지원이 필요한 경우 요청할 수 있도록 안내를 하고 있다. 해당 서비스들은 중소기업기본법 등에 근거한 중소기업이 대상이며, 활용을 원하는 기업이 요청하는 경우, 확인과정을 거쳐 지원이 되도록 하고 있다. 그러나, 정보보호 및 개인정보보호 진단 등에 대한 법적 의무사항이 없고, 전문 인력도 부재한 상황에서 다른 업무에 우선하여, 기관의 지원 서비스를 자발적으로 확인하고 절차를 통해 반영하는 일련의 활동을 한다는 것은 현실적으로 쉽지 않다.

IV. 중소기업 정보보호 개선 방안

1. 인증 의무대상 확대 및 사전 지원 제도 필요성

빈번하게 발생되고 있는 중소기업의 정보보안 사고 대응을 위해서는, 기존 ISMS 의무 대상을 확대하여 중소기업들이 법제도 안에서 의무를 자각하는 것이 먼저 필요

하다고 본다. 즉, 사업 추진 못지 않게 중요한 서비스 안전성에 대한 자발적인 대응 체계를 갖추기 위해서는 중소기업에게도 정보보안 체계 수립 및 이행에 대한 법적인 의무를 부여할 필요가 있다. 아울러, 중소기업 내에 직면하고 있는 전문인력 부족 문제의 실효성있는 지원을 위해, 인증시행시 사전 무료 컨설팅 의무 이용제도의 시행이 필요하다고 생각한다. 현재는 기관의 제도를 알고 요청하는 중소기업에 한해서만 지원이 되기 때문에 서비스 지원 효과가 제한적일 수 밖에 없다. 따라서, 중소기업을 위한 ISMS 인증 제도 확장과 더불어서 인력이 부족한 대상 중소기업이 연간 일정기간 이상 이용해야 하는 필수 지원 서비스로 재정의할 필요가 있다.

2. 안전성 확보조치 기준 유형 분류를 반영한 대상 규모별 인증 기준 시행

성격과 규모가 상이한 인증 대상기관의 동일한 결함사항을 ISMS에서 동일한 인증기준으로 결함을 받도록 하는 것이 적절한가에 대한 연구[11], ISMS-P의 보안 요소에 대한 효과성 연구[12] 등 ISMS 관련 다양한 연구들이 있지만, 이미 의무 대상에 편입된 기업의 경우는 인증체계 하에서 전반적인 점검이 이루어지므로, 공정성 면에서는 다툴 여지가 있지만, 서비스 안전성 면에서는 인증의무 비대상 기업 대비 좋은 환경이라 할 수 있다.

중소기업을 위한 정보보호 인증제도는 실효성 제고를 위해 기존 ISMS 대비 중소기업 규모별로 달리 평가 항목이 적용될 수 있도록 항목 구성이 필요하며, 그 기준은 개인정보보호법 하위 고시인 '개인정보의 안전성 확보조치 기준'과 유사한 방식의 도입을 적극 고려해 볼 수 있다. 개인정보의 안전성 확보조치 기준에서는 개인정보처리자 유형을 [표4]와 같이 분류하고 [표5]에서와 같이 유형에 따라 준수해야 하는 안전조치 기준을 달리 정의하고 있다. 즉, 개인정보처리자 유형 및 다루는 개인정보 규모에 따라 대응 인력 규모 및 서비스 복잡도가 달라질 수 밖에 없기 때문에 유형별 안전조치 기준을 달리함은 상당히 합리적이라 할 수 있다.

중소기업을 위한 인증기준도 개인정보의 안전성 확보조치 기준 유형기준과 유사하게 의무대상에 따른 인증유형을 달리하는 방안을 고려해볼 수 있다. 예를들어, 서비스 규모나 복잡도가 큰 유형3의 경우는 102개 항목 전체를, 평균적인 규모인 유형2의 경우 80개 항목, 작은 규모인 유형1의 경우 60개 항목 정도의 항목으로 구성하는 것이다. 이를 통해, 불필요한 인증항목에 대한 부담은 경감하되, 필수적인 항목에 대해서는 반드시 보안성을 갖추고 서비스가 일상적으로 운영되도록 할 수 있다.

표 4. 개인정보 안전성 확보조치 기준 상의 개인정보처리자 유형 분류
Table 4. Classification of types of personal information processors under the standards for measures to ensure personal information safety

유형	적용 대상
유형1 (완화)	·1만명 미만의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인
유형2 (표준)	·100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업 · 10만명 미만의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 1만명 이상의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인
유형3 (강화)	·10만명 이상의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 100만명 이상의 정보주체에 관한 개인정보를 보유한 중소기업, 단체

표 5. 개인정보처리자 유형별 안전조치 기준
Table 5. Standards for safety measures by type of personal information processors

안전조치 기준			
조	유형1 (완화)	유형2 (표준)	유형3 (강화)
제4조		·제4조:제1항제1호부터제11호까지 및 제15호, 제3항부터 제4항까지	제4조
제5조	·제5조:제2항부터 제5항까지	· 제5조	제5조
제6조	·제6조:제1항, 제3항, 제6항 및 제7항	·제6조:제1항부터 제7항까지	제6조
제7조	·제7조:제1항부터 제5항까지,제7항	·제7조:제1항부터 제5항까지, 제7항	제7조
제8조	· 제8조	· 제8조	제8조
제9조	· 제9조	· 제9조	제9조
제10조	· 제10조	· 제10조	제10조
제11조	· 제11조	· 제11조	제11조
제12조			제12조
제13조	· 제13조	· 제13조	제13조

V. 결 론

중소기업은 공공기관에서 연간 수검하고 있는 진단이나 평가와 같은 체계적인 점검을 받고 있지 못하며, 대기업처럼 정보보안 전문 조직이나 전문 인력을 보유하고 있지 못한 경우가 대다수다. 이에 본 논문에서는 개인정보의 안전성 확보조치 기준에 근거한 유형에 따라 ISMS 인증을 달리 시행하고, 자체 전문 인력 부족 문제를 해소

하기 위한 방안으로 컨설팅 제도 의무 시행을 통한 지원 제도 개선에 대해 연구하고 방안을 제시했다.

이후, 개인정보 안전성 확보조치 기준의 유형을 ISMS 항목에 매칭하여 유형별 인증 기준 수립 및 중소기업 지원 서비스의 활용 증대를 통한 실효성 있는 지원체계 확립을 위한 연구가 후속으로 필요하다.

References

[1] KISA, "Cyber Security Forecast 2023", KISA, https://www.boho.or.kr

[2] Dell Technologies, "The Long Road Ahead to Ransomware Preparedness", Dell Technologies, https://www.dell.com

[3] KISA, "ISMS-P Introduction of KISA ISMS-P Certification System(2021.7)", KISA, https://isms.kisa.or.kr

[4] Personal Information Protection Commission(PIPC), "Assessment of Public Institutions' Management Level", PIPC, https://www.pipc.go.kr

[5] NCSC, "Security Diagnosis and Management Status Assessment", NCSC, https://www.ncsc.go.kr

[6] KISA, "Technical support for personal information protection", KISA, https://www.privacy.go.kr

[7] KISA, "Information security check for SMEs", KISA, https://www.boho.or.kr

[8] NIS, "Appendix. Ch1. The Statiscics for Information Security", 2022 National Security White Paper, pp. 239-273, May 2022

[9] KISA, "Certificate Issuance Status", KISA, https://isms.kisa.or.kr

[10] Statics Korea, "Number of companies by industry and company size", Statics Korea,, https://kosis.kr

[11] Sung Wook Hong, Jae-Pyo Park, , "Effective Management of Personal Information & Information Security Management System(ISMS-P) Authentication systems", Journal of the Korea Academia-Industrial cooperation Society, Vol. 21, No. 1 pp. 634-640, 2020.
DOI: https://doi.org/10.5762/KAIS.2020.21.1.634

[12] Dong Hyun Kim, Younho Lee, "A Study on the ISMS-P Accreditation Effect Using the Seven Threats of Security - Focused on Enterprise Size and Career", Journal of KIIT, Vol. 18, No. 4, pp. 109-119, Apr. 30, 2020.
DOI : 10.14801/jkiit.2020.18.4.109

저 자 소 개

윤 혜 정(정회원)

- 숙명여대 전산학 학사, 숙명여대 전산학석사를 취득하였으며, 현재 숭실대학교 IT정책경영학과 박사과정 재학중이다.
- 한국투자신탁, 인터파크를 거쳐, 그래디언트에 재직중이다
- 관심분야 : 정보보안, 개인정보보호, ISMS-P, 정보보호 인증

이 용 우(정회원)

- 고려대 농업경제학과 학사, 미국 일리노이주립대 정책경제학 석사, 연세대 법무대학원 법학석사를 취득했고, 숭실대학교 IT정책경영학과 박사과정 재학중이다.
- 전경련 상무와 GS리테일 상무를 역임했고 대구 테크노파크 재직중이다.
- 관심분야 : IT정책경영, DAO

허 희 도(정회원)

- 국제대학교 컴퓨터공학 학사, 숭실대학교 IT정책경영학과 석사학위를 취득했으고, 숭실대학교 IT정책경영학과 박사과정 재학중이다.
- 티맥스 OS 대표이사를 역임했다.
- 관심분야 : 공개SW 활성화 방안 및 국산 SW 발전 방안

전 삼 현(정회원)

- 숭실대학교 법학학사, 숭실대학교 대학원 상법석사, 프랑크푸르트대학교 대학원 상법박사를 취득하였으며, 현재 숭실대학교 IT정책경영학과 교수로 재직중이다.
- 주요 관심분야 : IT정책경영, 자본시장법, 회사법 등