공학석사 학위논문

중소기업에서 활용가능한 정보보호 관리체계 연구

2023년 8월

부 경 대 학 교 대 학 원

정보보호학과

백 낙 천

공학석사 학위논문

중소기업에서 활용가능한 정보보호 관리체계 연구

지도교수 이 경 현

이 논문을 공학석사 학위논문으로 제출함.

2023년 8월

부 경 대 학 교 대 학 원

정보보호학과

백 낙 천

백낙천의 공학석사 학위논문을 인준함.

2023년 8월 18일

위원장　　공학박사 김 창 수　　(인)

위　원　　이학박사 이 경 현　　(인)

위　원　　이학박사 신 상 욱　　(인)

목 차

<표 목 차>

<그 림 목 차>

A study on information security management system Available to SMEs

Baek Nak Cheon

Department of Information Security, The graduate School,
Pukyong National University

Abstract

Information security is increasingly important in today's world, but 90% of security incidents occur in small and medium sized businesses due to a lack of investment in information security. To help this situation, this study proposes a information security management system Available to SMEs. We hope that it can be used as a guide to help SMEs in their information protection activities.

To this end, we first examined the current state of information protection in SMEs and compared and analysed national and international information protection certification systems to determine their similarities. We derived 34 items by mapping cloud security certification Low Impact Level and ISMS. modified them based on previous studies and surveys. After dividing them into administrative and technical areas, the survey was used to derive the importance of the second layer and the difficulty of performing the third layer for SMEs.

This thesis Contribute to propose an information security management system of Available levels to SMEs. and to Enhance on information protection in SMEs. for further study, we need to have the expertes to evaluation Improve ISMS also we must do an in-depth survey of actual ISMS judges & practitioners who have experted on implemented of ISMS to derive & evaluate proper items.

Ⅰ. 서론

1. 연구의 배경 및 필요성

IT 기술의 발전은 기업 운영에 많은 도움이 주고 있지만, 의존도가 높아질수록 그에 비례하여 사이버 위협이 증가하고 있다. 데이터베이스의 발전으로 기업은 많은 정보를 저장하고 처리할 수 있게 되었지만 동시에 침해 사고가 발생할 경우 대량으로 정보가 노출된다. 또한 클라우드의 발전으로 기업은 유연하게 인프라를 관리할 수 있게 되었으며, 서비스를 운영함에 있어 많은 이점이 생겼지만 회사의 내부에 서버가 있는 것이 아니기 때문에 인증 및 접근 제어 문제가 있으며 더욱이 클라우드 서비스는 대부분 API 를 통해 제공되기 때문에 취약한 API 를 사용할 경우 악성 코드의 실행, 데이터 유출, 권한 상승 등의 위험을 초래할 수 있다.

코로나 사태로 인해 재택근무가 늘어나면서 회사 밖으로 내부 정보를 반출했다가 회사 내부보다 상대적으로 보안 수준이 낮은 외부의 사용자들에게서 정보가 노출되기도 하였으며, 반대로 재택 근무자가 회사 내부의 시스템에 접근하기 위한 VPN 을 이용하여 해킹 사고가 발생하기도 하였다. 최근에는 AI 와 관련하여 AI 의 도움을 받아 악성 코드나 좀 더 정교한 피싱 이메일을 작성하였거나, 사용자가 AI 를 이용하면서 개인정보를 입력하여 개인정보가 노출된 경우도 있으며 이와 같이 IT 기술이 발전함에 따라 사이버 위협도 같이 발전하고 있다.

이런 상황에서 기업의 정보보호 문제는 조직에게 중요한 관심사로 IBM 시큐리티의 “2022 데이터 유출 비용 보고서”[1]에 따르면 한국기업의 연간 평균 피해액은 43 억 3400 만원으로 2018 년부터 꾸준히 증가하고

있으며 피해 규모가 큰 산업은 금융, 서비스, IT 로 문제는 데이터 유출의 피해가 일회성으로 끝나는 것이 아니라 장기적으로 기업에 영향을 미쳤다고 밝혔다.

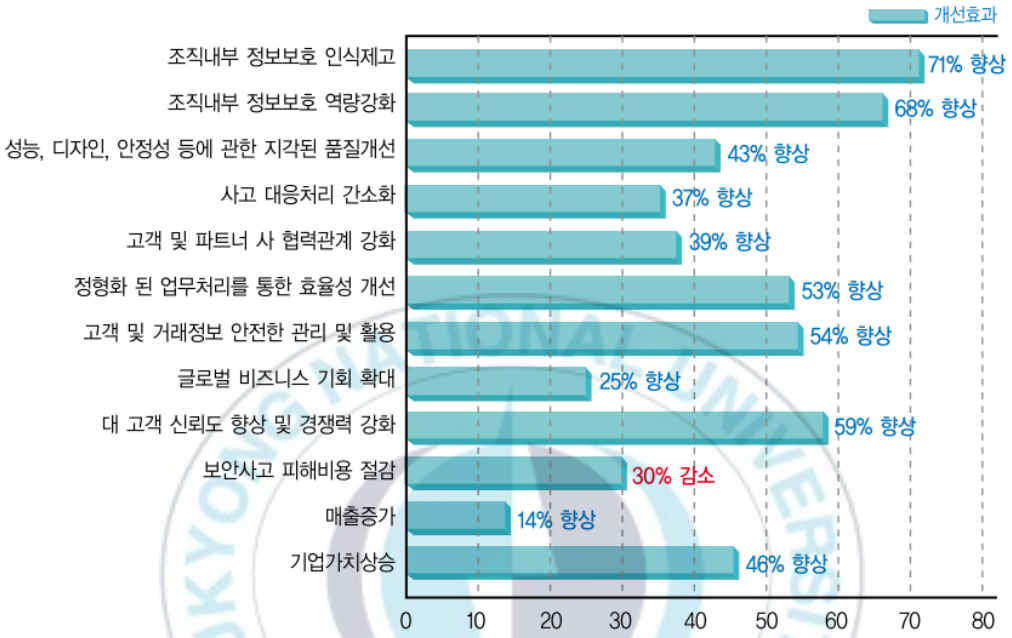
정부의 2021 년 “정보보호 실태조사”(한국 과학기술정보통신부, 2021, 응답 기관 7,500 개)[2]의 조사에 따르면 사업체의 88.9%가 정보보호의 중요성을 인식하고 있다고 응답하였다. 하지만 그에 비해서 정보보호 정책 보유율은 27%, 정보보호 조직 보유율은 11.6%이며 73%의 국내 사업체는 침해사고에 대응하기 위한 활동을 수행하지 않는다고 응답하였다.

이는 정보보호에 대한 인식에 비해 정보보호 조직과 인력에게 충분한 투자 및 지원을 하고 있지 않다는 것을 의미하고 있으며 이렇듯 기술적으로, 시대적으로 변화하고 복잡 해지며 진화하는 보안 위협 앞에 충분한 지원을 받지 못하는 기업 정보보호 조직의 실무자들은 어려움을 호소하고 있다.

이런 상황에서 기업의 정보보호에 효율적으로 도움을 줄 수 있는 것이 ISMS 인증이며 ISMS 의 긍정적인 효과에 대해서는 많은 사람들이 인정을 하고 있으며 많은 연구가 되었다. 그 중에 몇 가지를 뽑자면 최동권, 윤현식(2019)[3]은 ISMS 인증이 기업의 영업성과와 기업가치에 모두 긍정적인 영향을 미치는 것으로 나타난다고 하였으며 김동현, 이윤호(2020)[4]은 ISMS-P 인증의 도입이 기업의 규모와 실무자들의 경력에 관계없이 기업의 보안체계를 강화하는 데 긍정적인 영향을 미칠 것이라고 생각한다는 결과를 도출하였다.

ISMS 인증의 효과를 수치나 객관적인 지표로 표현한 자료가 있는지 찾아보았는데 2010 년에 KISA 가 ISMS 인증 취득 기업을 대상으로 한 설문조사[5]와 정보보호 관리체계 구축이 기업성과에 미치는 영향(장상수, 김상춘, 2015)[6]을 참고하면 ISMS 인증의 효과중에 조직내부 정보보호 인식제고, 역량강화의 향상이 컸다. 결론적으로 ISMS 인증을 도입해서

조직내부의 정보보호 인식제고 및 역량강화, 업무 효율성 등의 증가로 이어지고 그 결과 보안사고 예방에 도움이 된다고 추론할 수 있다.



<그림 1-1> ISMS 인증기업 대상 설문조사: ISMS 도입 후 개선효과[5]

ISMS 인증의 우수성에 대해서는 증명이 되었지만 ISMS 인증이 많은 기업들에게 활용되고 있는지를 묻는다면 그렇지 않다. 머니투데이의 기사 “'해커 먹잇감'된 중소기업들, 매년 수백번 털리지만..."돈도 사람도 없다” “[7]에 따르면 88%의 사이버 침해사고가 중소기업에서 발생하고 있다.

대기업에 비해 중소기업들이 더 많은 위협들에 노출되고 있지만 ISMS 인증을 획득하고 유지하고 있는 기업들 중에 중소기업의 비중은 적으며 중소기업이더라도 그 대부분이 사업의 특성 상 대량의 개인정보가 필요한 경우(전자상거래, 온라인 교육)와 사업적으로 높은 보안 수준이 요구되는 경우(호스팅 업체, 보안 업체, 암호화폐)가 대부분이었는데

한국기업의 99%가 중소기업이며 제조업 기반 회사들이 많은 걸 생각하면 이를 보완하기 위한 지원이 요구되는 실정이다.

이에 대해서는 오래전부터 지적이 있었으며 그 부분을 개선하기 위한 연구와 국가의 지원이 이루어지고 있지만 크게 해결되지 않고 있다. 선행 연구를 살펴보면 크게 두 분류로 나뉘는데 ISMS 의 효과와 개선방안이다. ISMS 의 효과와 중보보호의 중요성에 대해서는 이미 충분히 인식하고 있다고 생각하며 개선방안은 기업의 규모와 업종의 특성에 맞게 개선해야 한다는 연구가 많다.

기존의 연구들은 정보보호 관리체계의 항목에 대한 중요도를 측정하거나 중소기업에서 수행 가능성을 구하는 등 한가지의 방향으로 그 결과를 구하는 경향이 있는데 항목의 중요도와 수행 난이도는 한 쪽이 아닌 양쪽을 동시에 고려하여야 한다고 생각한다.

중소기업들이 ISMS 인증을 획득하기에는 힘들지만 ISMS 인증을 활용할 수 없는 것은 아니다. 그러기 위해서는 ISMS 인증의 모든 항목을 고려하는 것이 아닌 필요한 활동을 단계별로 나누어 우선순위와 수행가능성을 정하고 상황에 맞게 적용하는 방식으로 접근이 필요하다.

본 논문은 중소기업들이 ISMS 인증을 획득하고 활용함에 있어 구조적으로 어려운 점에 대하여 클라우드 보안 인증 하등급과 ISMS 를 매핑한 후 조정을 하여 기본적인 정보보호 관리체계의 틀을 잡고 통제분야들의 중요도와 통제항목들의 수행 난이도를 도출하여 중소기업에서 활용가능한 수준의 정보보호 관리체계를 제안하고 이를 가이드로 삼아 중소기업들의 정보보호 수준 향상을 도모하는 것을 목적으로 하고 있다.

2. 연구의 내용 및 범위

본 논문에서는 자원이 부족한 중소기업에서 ISMS 인증의 항목들을 활용하여 효율적으로 정보보호 수준 향상에 도움이 될 수 있는 실질적인 방안을 고민하였다. 이에 전방위적 보안위협에 대응하는 것이 아닌 실효성 있는 정보보호 태세 구축을 위하여 ISMS 인증의 요구항목들을 분석하여 중요도만 아니라 기업들의 애로사항인 예산 부족, 인력 부족 등을 고려한 중소기업 수행 난이도를 같이 분석하여 중소기업에서 활용가능한 수준의 정보보호 관리체계를 도출하고 제안하고자 아래와 같은 실증분석을 기초로 하였다.

첫째, 중소기업의 정보보호에 대한 환경을 분석하고자 중소기업의 정보보호 실태를 조사하였다.

둘째, 정보보호 활동에 관한 선행연구 자료와 국내외 정보보호 관련 인증제도를 분석한 뒤 클라우드 보안인증과 ISMS 를 매핑하여 1 차적으로 임의의 정보보호 관리체계를 도출한다.

셋째, 선행 연구와 설문조사를 바탕으로 1 차적으로 도출된 임의의 정보보호 관리체계를 수정한다.

넷째, 도출된 정보보호 관리체계를 관리적 영역과 기술적 영역으로 구분한 뒤 설문조사를 통하여 통제 분야는 중요도를 통제 항목은 난이도를 구한 후 대입하여 중소기업에서 활용가능한 수준의 정보보호 관리체계를 제안한다.

Ⅱ. 이론적 배경

1. 중소기업 정보보호 실태

가. 중소기업의 정의

일반적으로 중소기업은 규모와 인원이 적은 기업을 뜻하지만 중소벤처기업부에서 2022 년 발간한 중소기업 범위해설[8]에 따르면 법적으로 보호와 육성을 위해 「중소기업기본법 시행령」 제 3 조 및 「조세특례제한법 시행」 제 2 조의 규정에 속하는 법인 기업을 뜻하며 요약하면 아래와 그림과 같다.

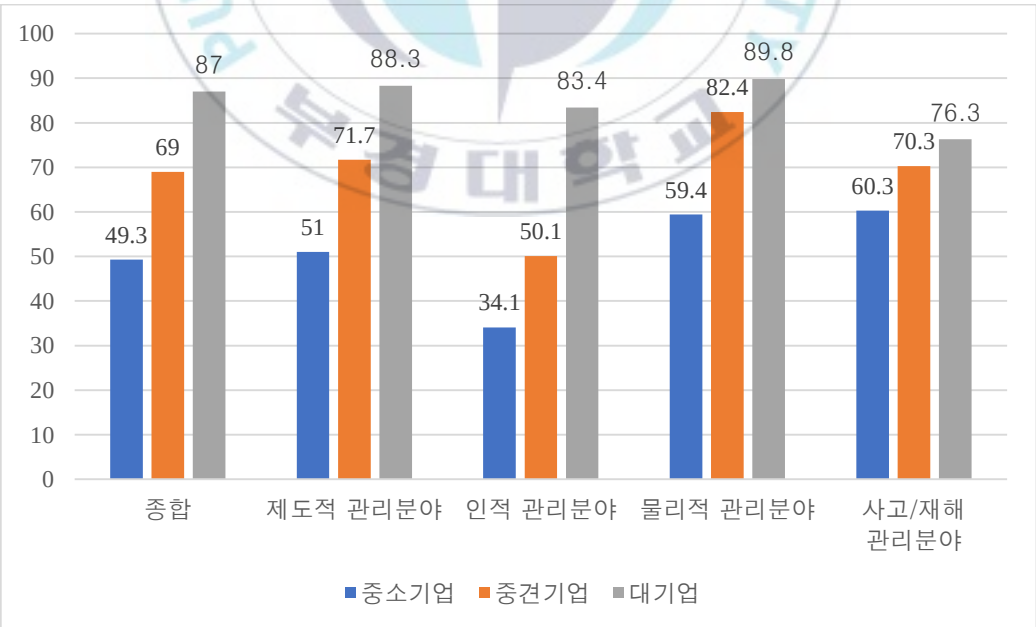
<표 2-1> 법률 상 중소기업의 정의

구 분	「중소기업기본법 시행령」 제3조	「조세특례제한법 시행령」 제2조
업 종	모든 업종	소비성 서비스업을 제외한 모든 업종
주업종	평균매출액이 큰 업종	사업별 사업수입금액이 큰 업종
규 모 기 준	「중소기업기본법 시행령」 [별표1]의 업종별 규모 기준에 따른 평균매출액·자산총액 5천억 원	「중소기업기본법 시행령」 [별표1]의 업종별 규모기준에 따른 매출액 · 자산총액 5천억 원
독립성 기 준	공시대상 기업제한 기업집단 제외	「중소기업기본법」과 같음 (「조세특례제한법 시행령」 제2조제1항제3호)
	5,000억 원 이상인 회사가 30% 이상의 지분을 직·간접적으로 소유하면서 최다출자자인 회사 제외	
	관계기업간에 합산한 평균매출액이 업종별 규모기준을 초과하면 제외	관계기업간에 합산한 매출액이 업종별 규모기준을 초과하면 제외

처음에는 규모로만 기준이 있었지만 중소기업의 보호와 육성을 위해서 혜택이 있는데 이를 규모 기준으로는 중소기업이지만 대기업의 자회사이거나 계열사들과 합한 규모가 중소기업 규모기준을 초과하는 기업도 중소기업으로 인정하는 것에 대한 불합리성이 꾸준히 제기되어 2011 년 1 월 1 일에 본격적으로 독립성 기준도 추가적으로 시행되었다.

나. 다른 규모의 기업 대비 중소기업 기술보호 역량

중소기업 기술보호 수준 실태조사 보고서(2022 중소벤처기업부)[9]에 따르면 기업 규모별로 기술보호 역량점수를 도출했는데 종합적으로 대기업은 87 점, 중견기업은 69 점, 중소기업은 49.3 점이며 그 중에 중소기업이 가장 취약한 부분은 인적 관리 분야로 34.1 점이 나왔으며 이 부분은 대기업에서는 83.4 점이 나왔다. 즉 대기업을 기준으로 중소기업의 인적 관리 수준은 절반에도 못 미치는 것이다.



<그림 2-1> 중소/중견/대기업 기술보호 역량점수 및 상대지수

위의 그림은 각 규모별 기업의 전체적인 평균을 나타낸 것이 같은 규모의 기업이라도 우수한 기업이 존재하며 이는 기업의 규모와 비례한다. 그에 관한 분포도는 아래의 표2-2와 같다.

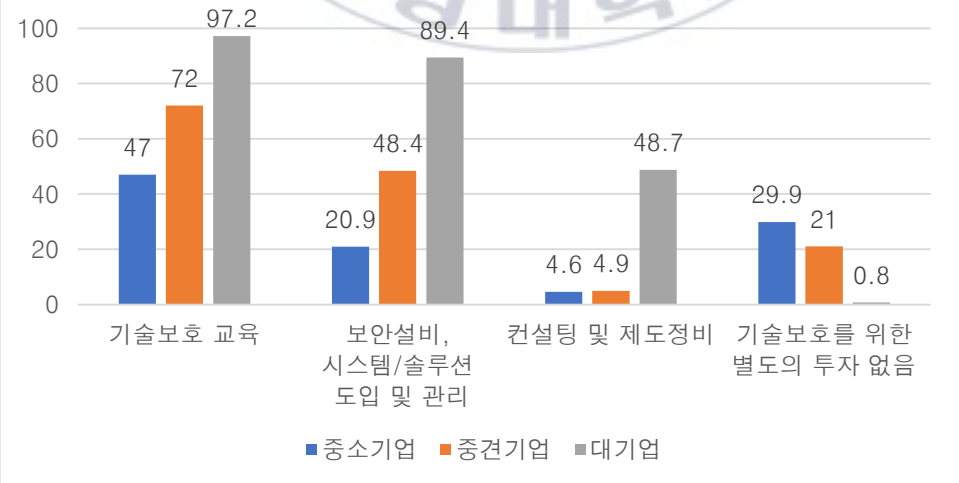
〈표 2-2〉 중소/중견/대기업 기술보호 역량수준 분포

구분	위험	취약	보통	양호	우수
중소기업	25	16.1	20.8	22	16.1
중견기업	4.5	6.7	13.1	30.1	45.6
대기업	0.8	0	1.7	3.9	93.6

위의 표에 따르면 중소기업의 41.1%가 기술보호 역량 수준이 위험하거나 취약한 것을 알 수 있다.

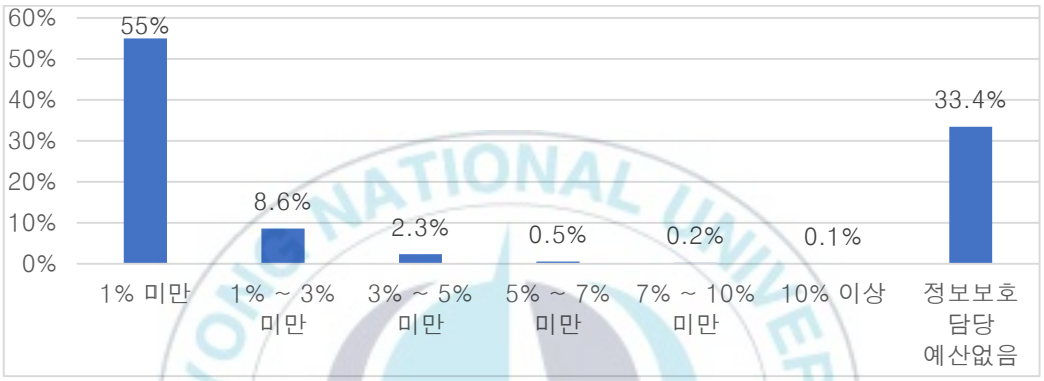
다. 다른 규모의 기업 대비 중소기업의 기술 보호 투자 상황

중소기업이 기술보호를 위해 투자하고 있는 분야 중 가장 높은 분야는 기술보호 교육(47%)이다. 제일 낮은 분야는 기술보호 컨설팅 및 제도정비(4.6%)로 나왔다. 자세한 내용은 아래의 2-2 그림으로 알 수 있다.



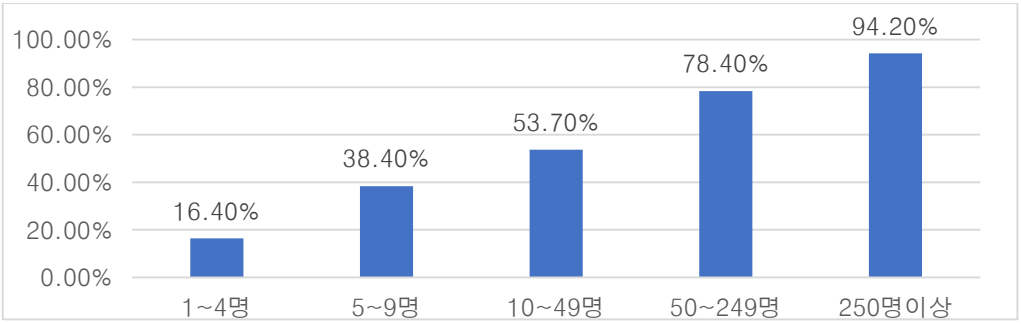
〈그림 2-2〉 기술보호를 위해 투자하고 있는 분야

또한 한국정보보호산업협회의 "2021 정보보호 실태조사"[10]에 따르면 정보보호 또는 개인정보보호에 예산을 편성한 기업은 66.6%으로 나왔으며 예산을 편성했어도 99% 이상이 IT 예산 중에 5% 이하로 정보보호 예산이 편성되었다. 이는 전체 기업에 대한 조사이므로 중소기업의 경우 더욱 낮아질 것으로 예상된다.

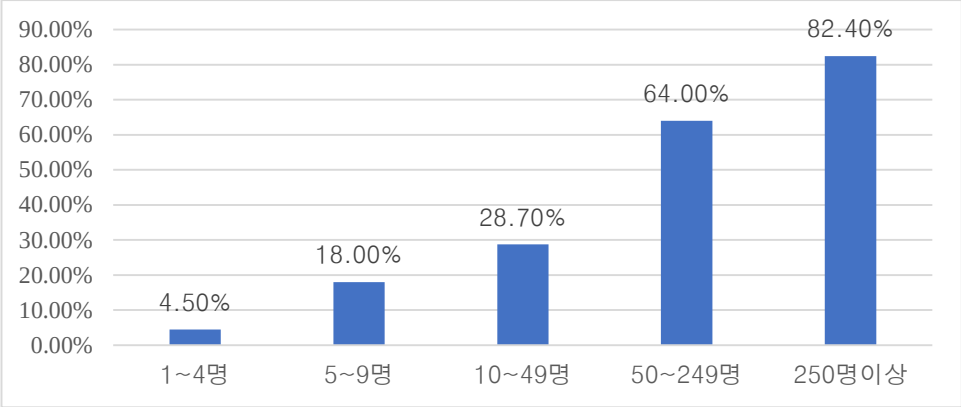


<그림 2-3> IT 예산 중 정보보호 예산 비중

기업 내 정보보호 정책과 조직의 유무 역시 간접적으로 정보보호 투자에 대한 상황을 알 수 있는 지표로 전체 기업의 27%는 정보보호 정책을 수립하는 것으로 조사되었으며 정보보호 조직을 운영하는 기업은 11.6%로 나왔다. 이 역시 기업의 규모와 비례하여 높게 나왔으며 아래의 그림 2-4 와 2-5 에 자세하게 나와있다.



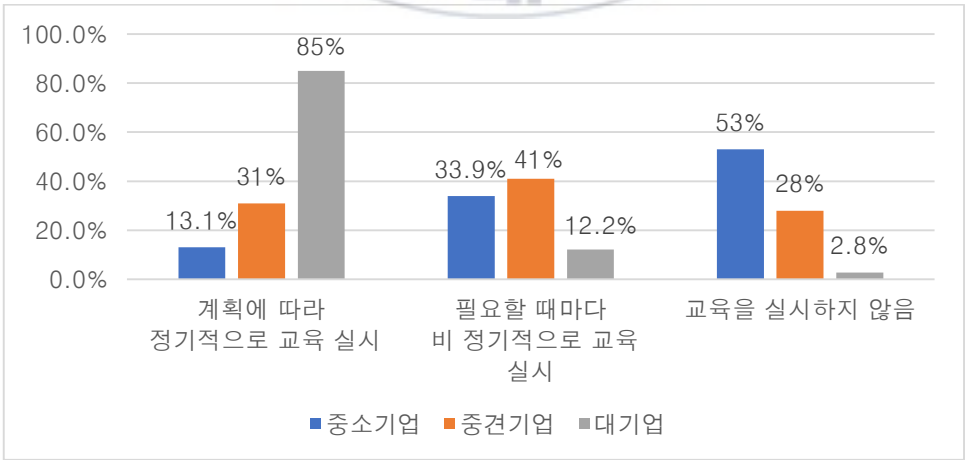
<그림 2-4> 규모별 정보보호(개인정보보호) 정책 수립 현황



〈그림 2-5〉 규모별 정보보호(개인정보보호) 조직 보유 현황

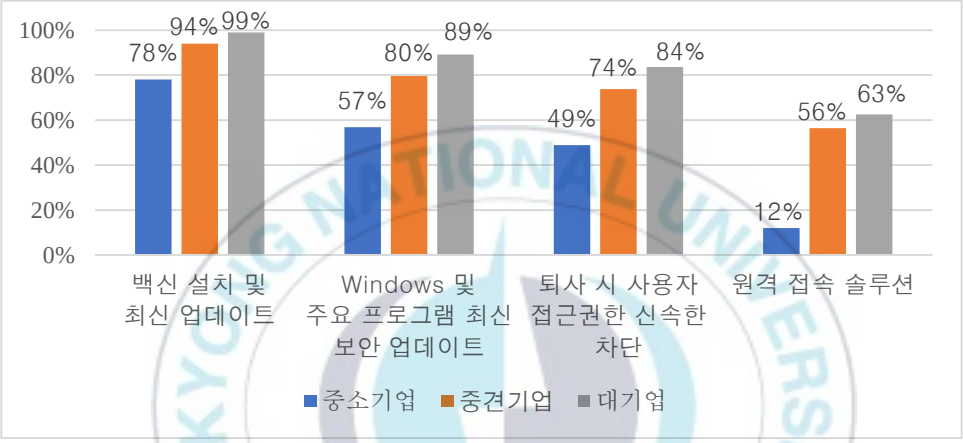
라. 중소기업의 보안사고 예방 활동 현황

중소기업은 53%가 기술보호 교육을 실시하지 않는 것으로 나타났으며 기술보호 교육을 실시하더라도 정기적보다는 필요할 때마다 비정기적으로 교육을 실시하는 것으로 조사되었다. 이는 아래의 그림 2-6 에 자세하게 나와있다.



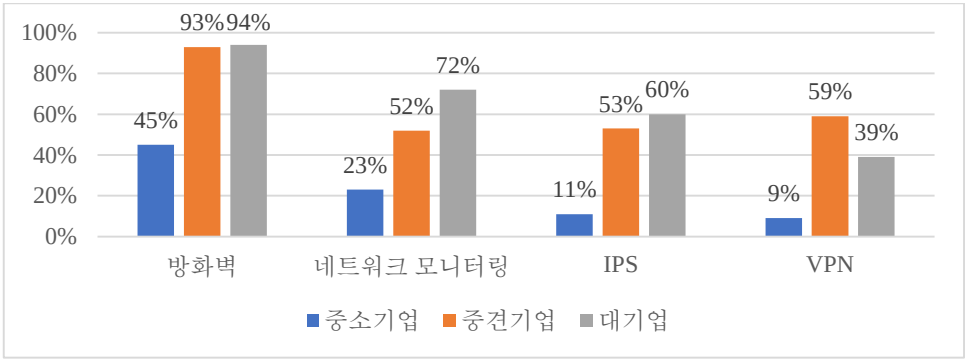
〈그림 2-6〉 기술보호 교육 실시 현황

중소기업의 사용자 계정 및 업무용 PC 보호에 대한 활동은 백신 설치 및 최신 업데이트가 78%로 가장 높았으며 재택/원격지에서 안전하게 회사 시스템에 접속하게 하는 원격 접속 솔루션의 도입 및 사용의 경우 11.9%로 다른 규모의 기업에 비해 현저하게 낮았다. 자세한 사항은 아래의 그림 2-7 에 나와있다.



<그림 2-7> 사용자 계정 및 업무용 PC 보호에 대한 활동

다음으로 네트워크 보안에 관련된 사항으로 중소기업의 방화벽 사용률은 45%로 대기업의 절반 정도이지만 IPS 와 VPN 의 사용률은 11%, 9%로 대기업의 5 분의 1 수준이다.



<그림 2-8> 기업 규모별 네트워크 보호를 위한 관리 방안

마. 중소 기업의 보안사고 현황

머니투데이의 기사 "'해커 먹잇감'된 중소기업들, 매년 수백번 털리지만..."돈도 사람도 없다"[7]에 따르면 2021 년 전체 보안사고를 당했다고 신고한 기업 중 640 건 중 580 건(93%), 2022 년 9 월 기준 852 건 중 756 건(88%)이 중소기업인 것으로 발표했다.

이 자료의 중소기업은 중견기업을 중소기업에 포함하여 대기업이 아닌 기업을 뜻하며 평균 90% 정도의 보안사고가 중소기업에서 발생하는 것을 알 수 있다. 2020 년부터 2022 년 9 월까지의 신고수를 보면 꾸준히 사고가 늘어나고 있으며 자세한 사항은 아래의 표 2-3 에 나와있다.

<표 2-3> 기업 규모별 보안사고 신고 현황

구분	2019	2020	2021	2022.9	합계	비율
대기업	10	23	20	29	82	3.26%
중소기업	386	522	580	756	2,244	89.3%
비영리	22	58	40	67	187	7.44%
합계	418	603	640	852	2,513	100%

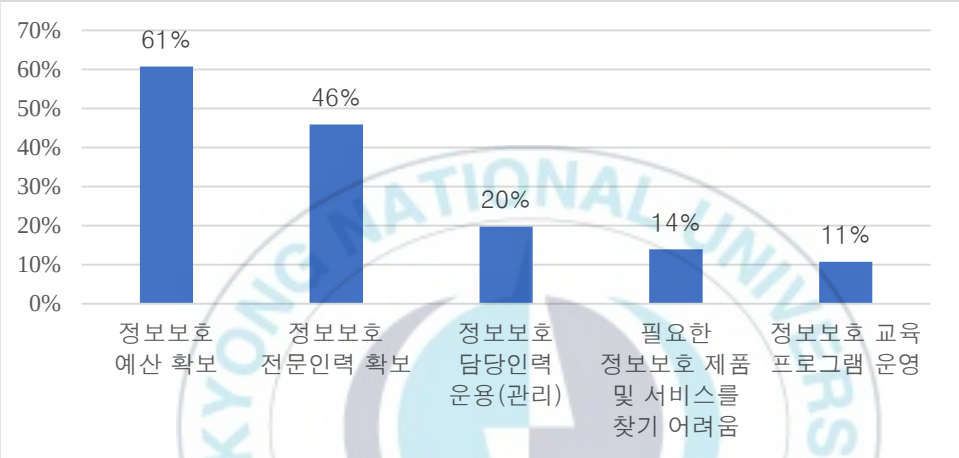
중소기업에서 기술 또는 경영상의 정보 침해 피해 유형을 살펴보면 인적 요인으로 인한 피해가 매우 높으며 중소기업의 기술보호 역량 중 인적 보호 관리 분야가 가장 낮았던 것과 같은 맥락으로 보인다. 중소기업의 정보 침해 피해 원인 유형에 대한 사항은 아래 표 2-4 과 같다.

<표 2-4> 중소기업의 정보 침해 피해 원인 유형 현황

구분	내부직원에 의한 유출	외부자에 의한 유출	해킹 등 외부 침입	기타
비율 (중복 가능)	68.4%	21.1%	10.5%	5.3%

바. 기업의 정보보호 애로사항 및 정부 지원 수요

사업체의 88.9%가 정보보호의 중요성을 인식하고 있다고 응답하였지만 그에 비해서 정보보호에 대해 투자를 못 하게하는 애로사항 중 가장 큰 비중은 정보보호를 위한 예산과 인력 문제였다.



<그림 2-9> 정보보호 애로사항

기업에서 원하는 정부의 지원에 대해서는 보안 시스템 및 장비 구축 지원의 수요가 가장 높았다.

<표 2-5> 기업규모 별 정부 지원 수요

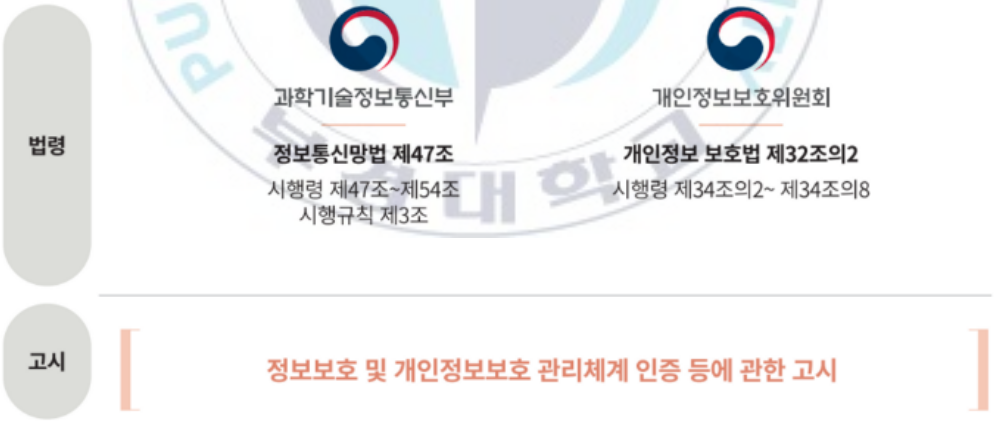
구분	보안 시스템/장비 구축 지원	기술보호 교육 (온라인 교육 등)	기술보호 컨설팅	보안관제 지원
중소기업	62.9%	36.0%	29.2%	23.6%
중견기업	57.1%	28.7%	22.7%	25.9%
대기업	63.2%	51.8%	40.4%	21.4%

2. 국내·국제 정보보호 인증제도 분석

가. 국내 정보보호 인증제도 현황

1) 정보보호 및 개인정보보호 관리체계(ISMS-P)

ISMS-P 분석은 KISA ISMS-P 인증제도 안내서(2021.7)[11]과 ISMS-P 인증기준 안내서(2022.4.22)[12]를 참고하여 분석하였다. 정보보호 및 개인정보보호 관리체계는 다음의 법령「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 「개인정보 보호법」 및 해당 고시「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」를 법적 근거로 삼고 있다.



<그림 2-10> ISMS-P 의 법적 근거 조항

의무 인증 대상자가 존재하며 그 외 별도로 자율 신청 기업을 위한 인센티브도 존재한지만 자율 신청의 경우 기업의 이미지 상승, 정보보호 업무 효율성 증가 등 인증으로 얻는 효과를 위하여 신청하는 경우가 많으며 인증대상에 관한 자세한 설명은 표 2-6 과 같다.

<표 2-6> ISMS-P 의 의무인증 대상

구분	대상
ISP	「전기통신사업법」 제 6 조제 1 항에 따른 등록을 한 자로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
IDC	「정보통신망법」 제 46 조에 따른 집적정보통신 시설 사업자
병원/학교	연간 매출액 또는 세입이 1,500 억원 이상인 자 중에서 다음에 해당되는 경우 -「의료법」 제 3 조의 4 에 따른 상급종합병원 - 직전연도 12 월 31 일 기준으로 재학생 수가 1 만명 이상인 「고등교육법」 제 2 조에 따른 학교
정보통신 서비스 제공자	- 정보통신서비스 부문 전년도 매출액이 100 억원 이상인 자 - 전년도 말 기준 직전 3 개월간의 일일평균 이용자 수가 100 만명 이상인 자

정보보호 관리체계 및 개인정보보호 관리체계는(ISMS-P)는 정보보호 관리체계(ISMS)와 전자정부 정보보호 관리체계(G-ISMS), 개인정보 관련 인증인 개인정보보호 관리체계(PIMS)와 개인정보 보호 인증(PIPL)이 통합되어 만들어진 인증이다.

제일 먼저 2001 년에 시행된 정보보호 관리체계(ISMS)는 국제표준 정보보안경영시스템(ISO 27001)을 기준으로 모방하여 개발하였고 「정보통신망법」 개정을 통하여 도입하게 되었다. 2009 년에는 전자정부 정보보호 관리체계(G-ISMS)를 만들어 공공기관을 대상으로 인증을 시행하였으며, 2013 년 「정보통신망법」을 개정하여 정보통신망 서비스제공자(ISP), 집적정보통신 시설 (IDC) 사업자, 정보통신 서비스제공자 중 기준에 해당하는 기업들을 의무대상자로 지정하였다.

2014 년에 ISMS 와 G-ISMS 를 구분하는 것에 대한 효율성이 부족하여 통합되었으며 2016 년에는 민감성 높은 정보를 취급하는 상급종합병원, 많은 개인정보를 취급하는 재학생 수 1 만 명 이상의 학교 등을 신규 의무대상자로 포함하도록 「정보통신망법」을 개정하였다.

개인정보보호 관리체계(PIMS)는 SK 브로드밴드, 옥션 등의 대규모 개인정보 유출 사태 등으로 개인정보보호에 대한 사회적 공감대가 형성되어 2010 년에 시행되었으며 2011 년에 개인정보보호법이 제정된 후 인증제 도입에 대한 필요성이 대두되며 2013 년에 개인정보보호 인증제(PIPL)이 시행되었으며 PIPL 은 민간부문(소상공인, 중소기업, 대기업)과 공공부문으로 나뉘어져 있는 게 특징이다. 기업의 혼란 해소를 위해 각 인증을 주관하던 행정자치부와 방송통신위원회가 공동고시를 마련하여 PIPL 인증 제도와 PIMS 인증 제도가 2016 년에 통합되었다.

2018 년에 ISMS 와 PIMS 가 통합이 되었으며 그 이유는 행안부, 과기정통부, 방통위 ISMS-PIMS 통합 추진팀에서 설명하길 아래와 같다

「이번 개정안은 양 인증의 내용이 일정 부분 **동일, 유사**함에도 각각 인증을 받아야 하는 **기업의 중복 부담을 완화**하기 위해 인증체계, 인증기준, 인증, 심사기관 등 **인증제도 전반의 실질적인 통합**을 이루는데 중점을 두었다. 」[13]

ISMS-P 의 인증 기준 구성은 1. 관리체계 수립 및 운영 16 개 항목, 2. 보호 대책 요구사항 64 개 항목, 3. 개인정보 처리단계별 요구사항 22 개 항목으로 구성되어 있으며 ISMS 인증만 받을 경우 1,2 의 80 개 항목만 받으면 된다. ISMS-P 인증 세부항목을 요약하면 아래 표 2-7 과 같다.

<표 2-7> ISMS-P 의 세부항목 요약

인증영역	인증기준	항목 수	적용 여부	
			ISMS	ISMS-P
1. 관리체계 수립 및 운영(16 개)	1.1 관리체계 기반 마련	6	●	●
	1.2 위험 관리	4	●	●
	1.3 관리체계 운영	3	●	●
	1.4 관리체계 점검 및 개선	3	●	●
	2.1 정책, 조직, 자산 관리	3	●	●
	2.2 인적 보안	6	●	●

2. 보호대책 요구사항 (64 개)	2.3 외부자 보안	4	●	●
	2.4 물리 보안	7	●	●
	2.5 인증 및 권한관리	6	●	●
	2.6 접근통제	7	●	●
	2.7 암호화 적용	2	●	●
	2.8 정보시스템 도입 및 개발 보안	6	●	●
	2.9 시스템 및 서비스 운영관리	7	●	●
	2.10 시스템 및 서비스 보안관리	9	●	●
	2.11 사고 예방 및 대응	5	●	●
	2.12 재해 복구	2	●	●
3.개인정보 처리단계별요 구사항 (22 개)	3.1 개인정보 수집 시 보호조치	7	–	●
	3.2 개인정보 보유 및 이용 시 보호조치	5	–	●
	3.3 개인정보 제공 시 보호조치	4	–	●
	3.4 개인정보 파기 시 보호조치	3	–	●
	3.5 정보주체 권리보호	3	–	●
합계		102	80	102

2) 클라우드 보안 인증제

클라우드 보안 인증 분석은 KISA 의 클라우드서비스 보안인증제도 안내서[14] 참고하여 분석하였다. 클라우드 보안 인증제는 다음의 법령「클라우드컴퓨팅 발전 및 이용자 보호에 대한 관한 법률」 제 5 조에 의한 「제 1 차 클라우드컴퓨팅 기본계획」과 다음의 고시「클라우드 컴퓨팅 서비스 정보보호에 관한 기준 고시」 제 7 조에 따른 정보보호 기준의 준수여부 확인을 법적 근거로 삼고 있다. 인증대상은 공공기관에 업무를 위하여 클라우드 서비스를 제공하려는 자이며 클라우드 서비스를 제공하기 위해선 반드시 클라우드 보안 인증을 받아야 하는 건 아니며 우선적으로 고려하여야 한다고 명시되어 있다.

좀더 자세하게 인증 대상을 구분하자면 클라우드 서비스에 포함되었거나 관련 있는 모든 자산, 조직, 지원서비스 등 모든 것이 포함되며 그 예시는 아래의 표 2-8 과 같다.

〈표 2-8〉 클라우드 서비스의 세부항목 요약

구분	설명
서버	각종 프로그램이 운영되는 서버(Windows, Linux) 등
네트워크	라우터, 스위치, 허브 등
정보보호시스템	침입차단시스템, 침입방지시스템, 웹방화벽, 가상사설망 제품 등
소프트웨어	패키지 소프트웨어, 시스템 소프트웨어, 오픈소스 SW 등
응용프로그램	관리, 모니터링, 빌링, 분석 프로그램 등
데이터베이스	MS-SQL, MySQL, 오라클 등
홈페이지	서비스 정보 안내, 신청 및 관리 등을 위한 홈페이지 등
단말기	PC, 노트북, 모바일 디바이스 등
매체	USB, 외장형 메모리, 디스크, 테이프 등
문서	정보보호 정책 지침, 절차, 매뉴얼 등
설비	출입보안, 전기 · 공조 · 소방 설비, 부대설비 등
가상자원 운영 S/W	하이퍼바이저, 클라우드 플랫폼 등
가상자원	가상서버, 가상 PC, 가상 스토리지, 가상 네트워크, 배포이미지 등
지원서비스	Auto Scaling, Load Balancer, DNS, 모니터링, 로그 분석 등

클라우드 보안 인증제는 미국의 FedRAMP 를 기반으로 2016 년 공공기관에 안정성 및 신뢰성이 검증된 민간 클라우드서비스를 공급하기 위하여 시행되었다. 이 둘의 가장 큰 차이점은 클라우드 보안인증의 경우 인프라 운영조직의 업무 분야를 기반으로 구성했으며 FedRAMP 의 경우 보안 목표인 기밀성, 무결성, 가용성과 같은 주제들을 기반으로 구성되어 있다.

클라우드 보안인증의 기존의 유형은 클라우드 서비스 분류에 따라 서비스형 인프라(IaaS, 2016 년), 서비스형 플랫폼(PaaS, 2018 년), 서비스형 데스크탑(DaaS, 2020)이 있었다. 하지만 공공기관에 서비스를 제공하기 위해서는 사실상 클라우드 인증이 필수이기에 공공시장

진입장벽을 낮추기 위한 목적으로 기존의 서비스별 인증 유형에서 FedRAMP 와 같이 등급으로 변경(2023 년)되어 상, 중, 하로 나뉘지만 상, 중 등급의 인증 항목의 수는 아직 정해지지 않았다. 자세한 인증 유형과 등급은 아래 표 2-9 과 같다.

〈표 2-9〉 클라우드 보안 인증 기준 항목 수

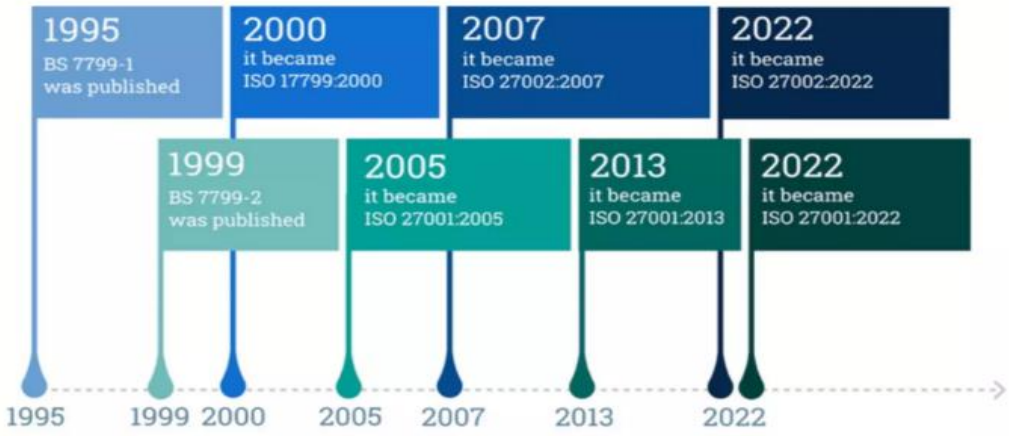
통제분야	통제항목	통제항목 수				
		IaaS	SaaS	DaaS	하 등급	하 등급 Saas
1. 정보보호 정책 및 조직	1.1. 정보보호 정책	3	3	3	1	
	1.2. 정보보호 조직	2	2	2	1	1
2. 인적보안	2.1. 내부인력 보안	5	4	4	1	1
	2.2. 외부인력 보안	3	–	3	–	–
	2.3. 정보보호 교육	3	1	1	1	1
3. 자산관리	3.1. 자산 식별 및 분류	3	1	3	2	–
	3.2. 자산 변경관리	3	1	3	–	–
	3.3. 위험관리	4	1	4	1	–
4. 서비스 공급망 관리	4.1. 공급망 관리정책	2	2	2	1	–
	4.2. 공급망 변경관리	2	1	2	1	–
5. 침해사고관리	5.1. 침해사고 대응 절차 및 체계	3	3	3	3	1
	5.2. 침해사고 대응	2	2	2	2	1
	5.3. 사후관리	2	2	2	1	–
6. 서비스 연속성 관리	6.1. 장애대응	4	4	4	4	1
	6.2. 서비스 가용성	3	2	3	1	1
7. 준거성	7.1. 법 및 정책 준수	2	1	2	1	1
	7.2. 보안 감사	2	2	2	1	–
8. 물리적 보안	8.1. 물리적 보호구역	5	–	5	2	–
	8.2. 정보처리 시설 및 장비보호	6	–	6	–	–
9. 가상화 보안	9.1. 가상화 인프라	6	2	5	5	1
	9.2. 가상 환경	4	4	2	1	–
10. 접근통제	10.1. 접근통제 정책	2	2	2	2	1
	10.2. 접근권한 관리	3	3	3	3	–
	10.3. 사용자 식별 및 인증	4	4	4	4	3
11. 네트워크 보안	11.1. 네트워크 보안	6	5	6	5	2

12. 데이터 보호 및 암호화	12.1. 데이터 보호	6	6	6	2	1
	12.2. 매체 보안	2	–	2	–	–
	12.3. 암호화	2	2	2	1	1
13. 시스템 개발 및 도입 보안	13.1. 시스템 분석 및 설계	5	5	5	3	1
	13.2. 구현 및 시험	4	4	4	3	1
	13.3. 외주 개발 보안	2	2	2	–	–
	13.4. 시스템 도입 보안	4	3	4	–	–
14. 국가기관등의 보안요구사항	14.1. 관리적 보호조치	4	4	4	4	4
	14.2. 물리적 보호조치	2	2	2	2	2
	14.3. 기술적 보호조치	4	3	4	5	5
합계		119	83	113	64	30

나. 국제 정보보안 인증제도 현황

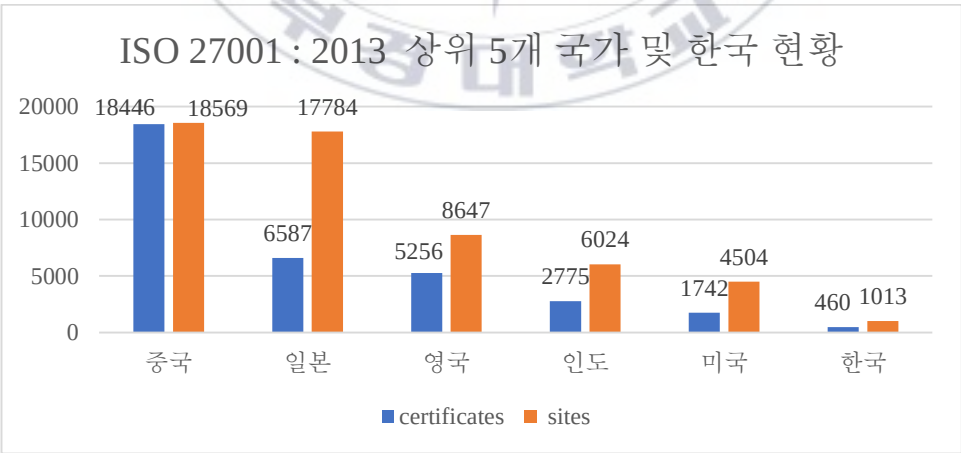
국제 정보보안 인증제도에서는 가장 대표적인 인증제도인 ISO-27001 에 대해서만 알아볼 것이며 ISO 27001 은 영국의 정보보호 관리체계 인증 규격인 BS 7799-1(British Standard Part 1 정보보안 관리에 대한 실행지침, 1995) 과 BS 7799-2(British Standard Part 2 정보보안 관리시스템에 관한 규격, 1999)를 기반으로 2000 년에 국제표준화기구에 채택되어 ISO 17999 로 발간되어 사용되었다가 2005 년에 ISO 27001 로 제정되어 현재까지 공식적인 국제표준 인증제도로 널리 활용되고 있다.

2013년에 1차 개정, 2022년 10월에 2차 개정되었고 현재는 전환작업이 이루어지고 있기에 기존의 인증조직들은 유예기간인 3 년안에 전환을 완료하여야 한다. ISO 27001 의 역사에 대한 자세한 사항은 아래의 그림 2-11 과 같다.



<그림 2-11> ISO 27001,2 history [14]

2021 년 ISO 에서 조사한 결과[15]에 따르면 ISO/IEC 27001: 2013 의 경우 유효한 인증서의 총 수는 58,687 개이며 총 사이트 수는 101,794 개로 조사되었다. 제일 많은 국가순은 중국, 일본, 영국이었으며 한국의 경우 460 개의 유효한 인증서와 1,013 개의 사이트가 있었다. 자세한 사항은 아래 그림 2-12 와 같다.



<그림 2-12> ISO 27001: 2013 현황, 2021 년 기준

ISO 27001 은 ISO 에서 위험관리 프레임워크(Risk Management Framework: RMF)기반으로 기업 활동에서 생산 및 품질 등을 관리하는 범용적인 기법인 PDCA(plan – do – check – act)를 적용하여 Life-Cycle 을 만들었다. ISO 27001 은 크게 관리과정과 통제과정으로 나뉘는데 정보보호 관리과정에서 조직의 상황, 리더십, 계획, 지원, 운영, 성과 평가, 개선 등의 7 개 HLS(High Level Structure) Framework 로 요구사항을 정의하며, 정보보호 통제과정은 Annex A 로 구성되어 있다. Annex A 의 항목은 2013 년판의 경우 14 개 영역, 114 개의 통제 항목이었지만 2022 년에 4 개 영역, 93 개의 통제항목으로 개정되었다.

ISO 27001:2022 의 상세한 항목은 아래의 표 2-5 와 같으며 ISO 27001 문서[16]와 advisera.com 의 Overview of new security controls in ISO 27002:2022[17]를 참고하여 분석하였다.

<표 2-10> ISO 27001:2022 상세 항목

ISO/IEC 27001: 2022					
정보보호 관리과정	요구 영역	요구사항	정보보호 통제과정	통제 영역	통제항목
	4. 조직의 상황	4		A.5 조직 통제	37
	5. 리더쉽	3			
	6. 계획	5		A.6 인적 통제	8
	7. 지원	7			
	8. 운영	3		A.7 물리적 통제	14
	9. 성과 평가	6			
	10. 개선	2		A.8 기술적 통제	34
	7 개 영역	30		4 개 영역	93

2022 년 개정판에서 통제항목의 수가 줄었지만 실제로 삭제된 항목은 없으며 11 개의 신규 통제항목이 생겼으며 23 개의 통제항목은 이름이 변경, 57 개의 통제항목은 24 개의 항목으로 통합되었고 1 개의 통제항목이 2 개로 분할되었다. 이후 분석을 위해 이 부분들을 자세하게 살펴보도록 하겠다.

먼저 57 개에서 24 개로 통합된 통제항목은 아래의 표 2-11 과 같다.

<표 2-11> ISO 27001:2013 -> ISO 27001:2022 통합 항목

ISO 27001: 2013	ISO 27001: 2022
5.1.1 정보보안을 위한 정책	5.1 정보보안를 위한 정책
5.1.2 정보보안 정책의 검토	
6.1.5 프로젝트 관리에서의 정보보호	5.8 프로젝트 관리에서의 정보보안
14.1.1 정보보호 요구사항 분석 및 명세	
6.2.1 모바일 기기 정책	8.1 사용자 엔드포인트 디바이스
11.2.8 방치된 사용자 장비	
8.1.1 자산 목록	5.9 정보 자산 및 기타 자산 목록
8.1.2 자산 소유권	
8.1.3 자산 이용	5.10 정보 자산 및 기타 자산 이용
8.2.3 자산 반환	
8.3.1 이동식 매체 관리	7.10 저장 매체
8.3.2 매체 폐기	
8.3.3 물리적 매체 이송	
11.2.5 자산 반출	
9.1.1 접근통제 정책	5.15 접근 통제
9.1.2 네트워크 및 네트워크 서비스 접근통제	
9.2.2 사용자 권한 설정	5.18 접근 권한
9.2.5 사용자 접근권한 검토	
9.2.6 접근권한 제거 또는 조정	
9.2.4 사용자 비밀 인증번호 관리	5.17 인증 정보
9.3.1 기밀 인증정보 사용	
9.4.3 패스워드 관리시스템	
10.1.1 암호 통제사용 정책	8.24 암호 사용
10.1.2 키 관리	
11.1.2 물리적 출입 통제	7.2 물리적 출입
11.1.6 배송 및 하역 구역	
12.1.2 변경 관리	8.32 변경 관리
14.2.2 시스템 변경 통제 절차	
14.2.3 운영 플랫폼 변경 후 어플리케이션 기술적 검토	
14.2.4 소프트웨어 패키지 변경 제한	
12.1.4 개발, 시험, 운영, 환경 분리	8.31 개발, 시험 및 생산 환경 분리
14.2.6 개발 환경 보안	
12.4.1 이벤트 로그 기록	8.15 로깅
12.4.2 로그 정보 보호	
12.4.3 관리자 및 운영자 로그	
12.5.1 운영 시스템 소프트웨어 설치	8.19 운영 시스템 소프트웨어 설치
12.6.2 소프트웨어 설치 제한	

12.6.1 기술적 취약점 관리	8.8 기술적 취약점 관리
18.2.3 기술 준거성 검토	
13.2.1 정보 전송 정책 및 절차	5.14 정보 전송
13.2.2 정보 전송 협약	
13.2.3 전자 메시지 교환	
14.1.2 공중망 응용 서비스 보안	8.26 애플리케이션 보안 요구 사항
14.1.3 응용, 서비스 거래 보호	
14.2.8 시스템 보안 시험	8.29 개발 및 인수 보안시험
14.2.9 시스템 인수 시험	
15.2.1 공급자 서비스 모니터링 검토	5.22 공급자 서비스 모니터링 검토
15.2.2 공급자 서비스 변경 관리	
16.1.2 정보보안 이벤트 보고	6.8 정보보안 이벤트 보고
16.1.3 정보보안 이벤트 평가 및 의사결정	
17.1.1 정보보안 연속성 계획	5.29 장애 중 정보보안
17.1.2 정보보안 연속성 구현	
17.1.3 정보보안 연속성 검증, 검토, 평가	
18.1.1 적용 법규 및 계약 요구사항 식별	5.31 법률, 법규, 규제의 계약 요구사항
18.1.5 암호 통제 규제	
18.2.2 보안 정책 및 표준 준수	5.36 정보보안 정책, 규칙 및 표준 준수
18.2.3 기술 준거성 검토	

다음으로 신규 생성된 11 개의 통제항목은 아래의 표 2-12 과 같다

<표 2-12> ISO 27001:2022 신규 통제항목

통제영역	통제항목
조직 통제	5.7 위협 인텔리전스
	5.23 클라우드 서비스 이용을 위한 정보보안
	5.30 비즈니스 연속성을 위한 ICT 준비
물리적 통제	7.4 물리적 보안 모니터링
기술적 통제	8.9 구성 관리
	8.10 정보 삭제
	8.11 데이터 마스킹
	8.12 데이터 유출 방지
	8.16 모니터링 활동
	8.23 웹 필터링
	8.28 보안 코딩

다음으로 이름이 변경된 통제항목은 23 개이며 변경된 의도가 제대로 표현되지 않을 수도 있기에 영어로 표기했으며 아래의 표 2-13 과 같다

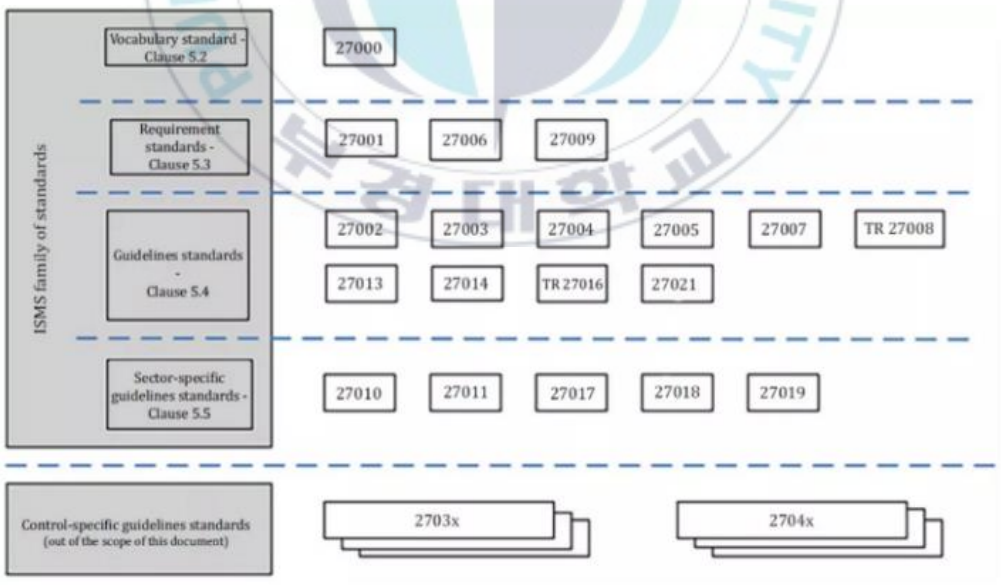
<표 2-13> ISO 27001:2013 -> ISO 27001:2022 이름 변경 항목

ISO 27001 : 2013	ISO 27001 : 2022
6.2.2 Teleworking	6.7 Remote working
7.3.1 Termination or change of employment responsibilities	6.5 Responsibilities after termination or change of employment
9.2.1 User registration and de-registration	5.16 Identity management
9.2.3 Management of privileged access rights	8.2 Privileged access rights
9.4.2 Secure log-on procedures	8.5 Secure authentication
9.4.5 Access control to program source code	8.4 Access to source code
11.1.1 Physical security perimeter	7.1 Physical security perimeters
11.2.6 Security of equipment and assets off-premises	7.9 Security of assets off-premises
11.2.9 Clear desk and clear screen policy	7.7 Clear desk and clear screen
12.2.1 Controls against malware	8.7 Protection against malware
12.7.1 Information systems audit controls	8.34 Protection of information systems during audit testing
13.1.1 Network controls	8.20 Networks security
13.1.3 Segregation in networks	8.22 Segregation of networks
14.2.1 Secure development policy	8.25 Secure development life cycle
14.2.5 Secure system engineering principles	8.27 Secure system architecture and engineering principles
14.3.1 Protection of test data	8.33 Test information
15.1.1 Information security policy for supplier relationships	5.19 Information security in supplier relationships
15.1.2 Addressing security within supplier agreements	5.20 Addressing information security within supplier agreements
15.1.3 Information and communication technology supply chain	5.21 Managing information security in the ICT supply chain
6.1.1 Responsibilities and procedures	5.24 Information security incident management planning and preparation
16.1.4 Assessment of and decision on information security events	5.25 Assessment and decision on information security events

17.2.1 Availability of information processing facilities	8.14 Redundancy of information processing facilities
18.1.4 Privacy and protection of personally identifiable information	5.34 Privacy and protection of PII

마지막으로 2013 버전의 18.2.3 기술 준거성 검토 항목이 2022 버전의 5.36 정보보안 정책, 규칙 및 표준 준수와 8.8 기술적 취약점 관리로 나뉘어졌다.

ISO 27001 의 강점은 다른 경영시스템(QMS, EMS, BCMS, MDMS, PSMS 등)과 연계가 가능하며 추가적으로 ISMS family of standard 들을 자신의 기업에 맞게 선택하여 확장성이 용이하다는 점이다. ISMS family of standards 의 구성을 살펴보면 상단부터 1 단에 원칙/매커니즘, 2 단에 인증기준, 3 단에 가이던스, 4 단에 섹터(분야별)가이던스, 5 단에 정보보호 통제 가이던스로 나뉜다. 자세항 사항은 아래의 그림 2-13 과 같다.



<그림 2-13> ISMS family of standards [18]

27000 부터 27010 까지 11 개의 표준이 ISMS 의 가장 기본적인 표준이며 그 이후는 부가적으로 추가 구현 통제, 확장 통제 등으로 사용되는 표준이다. 내용은 아래 표 2-14 과 같다

<표 2-14> ISO 27000 표준과 설명 [19]

Standard	Publish	Title
27000	2018	ISMS 수립 및 인증에 관한 원칙과 용어를 규정하는 표준
27001	2022	ISMS 계획, 운영, 지원, 평가 및 개선을 위한 요구사항을 규정
27002	2022	ISMS 운영 및 유지하기 위한 실무적인 지침 및 원칙
27003	2017	ISMS 구현을 위한 구체적인 구현 가이드라인을 규정
27004	2016	ISMS 유효성 측정 프로그램과 프로세스를 규정
27005	2022	ISMS 위험평가 과정 구분 및 세부 활동을 규정
27006	2015	ISMS 수립 및 인증에 관한 원칙과 용어를 규정하는 표준
27007	2020	ISMS 감사 가이드라인
27008	2019	정보보안 통제의 평가를 위한 가이드라인
27009	2020	ISO/IEC 27001 의 섹터별 적용 요구사항
27010	2015	정보보안 관리를 위한 내부 업무 및 조직 간 조정
27011	2016	통신섹터를 위한 정보보안 제어
27013	2021	ISO/IEC 27001 및 ISO/IEC 20000-1 의 통합 구현
27014	2020	조직의 정보 보안 관리 거버넌스
27016	2014	정보보안 조직 경제학
27017	2015	클라우드 보안
27018	2019	클라우드 개인정보보호
27019	2013	에너지섹터를 위한 정보보안 제어
27021	2017	정보보안 관리 시스템 전문가를 위한 역량 요구 사항
27032	2012	사이버보안 지침
27036	2021	공급망 관련 지침
27041	2015	보안사고 조사 지침

필요에 따라 위의 표준들을 부가적으로 사용할 수 있는 게 ISO 27001 의 장점이라고 판단되며 한국의 ISMS-P 도 분야별로 부가적으로 적용할 수 있는 지침들을 추가하는 게 바람직하다고 생각된다.

3. 국내・외 정보보호 인증 유사성 및 비교분석

가. 국내 클라우드 보안 인증과 K-ISMS 비교

ISO-27001 도 약자가 ISMS 이기에 한국의 ISMS 와 구별하기 위하여 유사성 비교에서는 한국의 ISMS 를 K-ISMS 라고 부르겠으며 K-ISMS 와 국내의 클라우드 보안 인증을 비교를 위하여 한국인터넷진흥원(KISA) "ISMS-P 인증기준 안내서"(2022.04.22)와 "클라우드서비스(IaaS) 보안인증기준 해설서"(2023.03)[20]를 기준으로 분석하였다.

<표 2-15> 국내 클라우드 보안 인증과 K-ISMS 유사성 비교

클라우드 보안인증	K-ISMS
1.1. 정보보호 정책	1.1 관리체계 기반 마련
1.2. 정보보호 조직	
2.1. 내부인력 보안	2.2 인적 보안
2.2. 외부인력 보안	2.3 외부자 보안
2.3. 정보보호 교육	2.2 인적 보안
3.1. 자산 식별 및 분류	1.2 위험 관리
3.2. 자산 변경관리	2.1 정책, 조직, 자산 관리
3.3. 위험관리	1.2 위험 관리
4.1. 공급망 관리 정책	-
4.2. 공급망 변경관리	
5.1. 침해사고 대응 절차 수립 및 체계	2.11 사고 예방 및 대응
5.2. 침해사고 대응	
5.3. 사후관리	
6.1. 장애대응	2.12 재해 복구
6.2. 서비스 가용성	
7.1. 법 및 정책 준수	1.4 관리체계 점검 및 개선
7.2. 보안 감사	
8.1. 물리적 보호구역	2.4 물리 보안
8.2. 정보처리 시설 및 장비보호	
9.1. 가상화 인프라	-
9.2. 가상 환경	
10.1. 접근통제 정책	2.6 접근통제

10.2. 접근 권한 관리	2.5 인증 및 권한관리
10.3. 사용자 식별 및 인증	
11.1. 네트워크 보안	2.6 접근통제
12.1. 데이터 보호	
12.2. 매체 보안	2.10 시스템 및 서비스 보안관리
12.3. 암호화	2.7 암호화 적용
13.1. 시스템 분석 및 설계	2.8 정보시스템 도입 및 개발 보안
13.2. 구현 및 시험	

매핑 비교 결과, 클라우드 보안 인증 중 특수한 분야인 국가기관 등의 보안 요구사항을 제외한 32 개 통제 분야 중 K-ISMS 와 유사성을 가진 통제 분야는 28 개로 도출됐으며 이는 87.5%의 유사성을 가진 것으로 비교 분석되었다.

유사성이 없는 통제 분야는 가상, 공급망 관련 분야로 공급망 관련 이슈는 비교적 최근에 문제가 되어 K-ISMS 의 모태인 ISO 27001 에서도 2022 년 개정판에 추가되었다. 그렇기에 향후에 K-ISMS 에서도 추가될 것으로 예상되며 가상 관련 분야는 K-ISMS 의 범위에 포함되어 있다고도 할 수 있지만 클라우드 보안인증처럼 따로 구별은 하지 않기에 제외하였다.

K-ISMS 와 클라우드 보안인증의 가장 큰 차이점은 2 개가 있는데 K-ISMS 는 의무대상이 존재하고 클라우드 보안인증은 상, 중, 하로 등급을 나눌 수 있다는 것이다. 한국 산업계의 전체적인 정보보호 수준을 올리기 위해서는 K-ISMS 의 의무대상을 확대하고 기업의 규모에 따라 등급을 나눠서 인증을 하고 그에 필요한 지원이 필요하다고 생각되며 클라우드 보안인증의 경우 공공기관에 품질이 검증된 클라우드 서비스를 제공하기 위하여 만든 보안인증이라 K-ISMS 와 취득 의도가 다르지만 결국 두 개의 인증은 상당히 유사하기에 클라우드 보안인증도 K-ISMS 에 편입시키는 게 효율적이라고 판단된다.

나. K-ISMS 와 ISO27001 비교

K-ISMS 와 ISO27001 를 위하여 ISO 27001: 2022 의 경우 기존의 항목들은 KS X ISO 27001:2014, 신규 항목들은 ISO 에서 발행한 ISO/IEC 27001: 2022 를 기준으로 분석하였다.

먼저 K-ISMS 의 정보보호 관리과정이라 할 수 있는 1. 관리체계 수립 및 운영과 ISO 27001: 2022 의 정보보호 관리과정을 비교하였다.

<표 2-16> K-ISMS 와 ISO-27001:2002 관리과정 유사성 비교

K-ISMS (1. 관리체계 수립 및 운영)		ISO-27001:2022 (정보보호 관리과정)
1.1 관리체계 기반 마련	1.1.1 경영진의 참여	5.1 리더십과 의지
	1.1.2 최고책임자의 지정	5.3 조직의 역할, 책임, 권한
	1.1.3 조직 구성	
	1.1.4 범위 설정	4.3 정보보호 경영시스템의 범위 결정
	1.1.5 정책 수립	5.2 정책
	1.1.6 자원 할당	7.1 자원
1.2 위험 관리	1.2.1 정보자산 식별	5.10 정보 자산 및 기타 자산 이용 (통제과정)
	1.2.2 현황 및 흐름분석	-
	1.2.3 위험 평가	6.1 위험과 기회에 따른 조치
	1.2.4 보호대책 선정	
1.3 관리체계 운영	1.3.1 보호대책 구현	9.1 모니터링, 측정, 분석, 평가
	1.3.2 보호대책 공유	7.4 의사소통
	1.3.3 운영현황 관리	6.2 정보보호 목표 및 달성 계획
1.4 관리체계 점검 및 개선	1.4.1 법적 요구사항 준수 검토	5.31 법률, 법규, 규제의 계약 요구사항 (통제과정)
	1.4.2 관리체계 점검	9.2 내부 감사
	1.4.3 관리체계 개선	10.1 지속적 개선

관리체계 수립 및 운영 경우 16 개 항목 중 15 개가 유사성이 있는 항목으로 93.75%의 유사성이 있는 것으로 비교 분석되었다.

다음으로 K-ISMS 물리적 요구사항과 ISO 27001: 2022 통제과정과의 매핑은 아래 표 2-17 과 같다.

<표 2-17> K-ISMS 와 ISO-27001:2002 관리적 분야 유사성 비교

K - ISMS (2. 보호대책 요구사항 / 관리적 분야)		ISO 27001: 2022 (정보보호 통제과정)
2.1 정책, 조직, 자산 관리	2.1.1 정책의 유지관리	5.1 정보보호를 위한 정책
	2.1.2 조직의 유지관리	5.3 조직의 역할, 책임 및 권한 (관리과정)
	2.1.3 정보자산 관리	5.10 정보 자산 및 기타 자산 이용
2.2 인적 보안	2.2.1 주요 직무자 지정 및 관리	-
	2.2.2 직무 분리	5.3 직무 분리
	2.2.3 보안 서약	6.2 고용 계약조건
	2.2.4 인식제고 및 교육훈련	6.3 정보 보안 인식, 교육 및 훈련
	2.2.5 퇴직 및 직무변경 관리	6.5 퇴직 또는 직무변경의 사후 관리
	2.2.6 보안 위반 시 조치	6.4 징계 절차
2.3 외부자 보안	2.3.1 외부자 현황 관리	5.19 공급자 관계의 정보보호
	2.3.2 외부자 계약 시 보안	5.20 공급자 협약 내 보안 명시
	2.3.3 외부자 보안 이행 관리	5.22 공급자 서비스 모니터링, 검토 및 변경 관리
	2.3.4 외부자 계약 변경 및 만료 시 보안	6.5 퇴직 또는 직무변경의 사후 관리
2.11 사고 예방 및 대응	2.11.1 사고 예방 및 대응체계 구축	5.24 정보보호 사고 관리 계획 및 사전 준비
	2.11.2 취약점 점검 및 조치	8.8 기술적 취약점 관리
	2.11.3 이상행위 분석 및 모니터링	5.25 정보보호 이벤트 평가 및 의사결정
	2.11.4 사고 대응 훈련 및 개선	-
	2.11.5 사고 대응 및 복구	6.1 위험과 기회에 따른 조치
2.12 재해 복구	2.12.1 재해 · 재난 대비 안전조치	5.29 장애 중 정보보호
	2.12.2 재해 복구 시험 및 개선	

매핑 결과 K-ISMS 의 2. 보호대책 요구사항(관리적 분야) 경우 20 개 항목 중 18 개가 유사성이 있는 항목으로 도출되었으며 이는 90%의 유사성이 있는 것으로 비교 분석되었다.

다음으로 K-ISMS 물리적 요구사항과 ISO 27001: 2022 통제과정과의 매핑은 아래 표 2-18 과 같다.

<표 2-18> K-ISMS 와 ISO-27001:2002 물리적 분야 유사성 비교

K - ISMS (2. 보호대책 요구사항 / 물리적 분야)		ISO 27001: 2022 (정보보호 통제과정)
2.4 물리 보안	2.4.1 보호구역 지정	7.1 물리적 보안 경계
	2.4.2 출입통제	7.2 물리적 통제
	2.4.3 정보시스템 보호	7.8 장비 배치 및 보호
	2.4.4 보호설비 운영	7.11 지원 설비
	2.4.5 보호구역 내 작업	7.6 보호구역 내 작업
	2.4.6 반출입 기기 통제	-
	2.4.7 업무환경 보안	7.9 책상 및 화면 정리

마지막으로 K-ISMS 기술적 요구사항과 ISO 27001: 2022 통제과정과의 매핑은 아래 표 2-19 과 같다.

<표 2-19> K-ISMS 와 ISO-27001:2002 기술적 분야 유사성 비교

K - ISMS (2. 보호대책 요구사항 / 기술적 분야)		ISO 27001: 2022 (정보보호 통제과정)
2.5 인증 및 권한관리	2.5.1 사용자 계정 관리	5.16 신원 관리
	2.5.2 사용자 식별	
	2.5.3 사용자 인증	5.17 인증 정보
	2.5.4 비밀번호 관리	
	2.5.5 특수 계정 및 권한관리	8.2 특수 접근 권한
	2.5.6 접근권한 검토	5.18 접근 권한
2.6 접근통제	2.6.1 네트워크 접근	8.20 네트워크 보안
	2.6.2 정보시스템 접근	5.15 접근 통제
	2.6.3 응용프로그램 접근	8.3 정보 접근 제한

	2.6.4 데이터베이스 접근	–
	2.6.5 무선 네트워크 접근	8.1 사용자 엔드포인트 디바이스
	2.6.6 원격접근 통제	6.7 원격 근무
	2.6.7 인터넷 접속 통제	5.14 정보 전송
2.7 암호화 적용	2.7.1 암호정책 적용	8.24 암호 사용
	2.7.2 암호키 관리	
2.8 정보시스템 도입 및 개발 보안	2.8.1 보안 요구사항 정의	5.8 프로젝트 관리에서의 정보보안
	2.8.2 보안 요구사항 검토 및 시험	8.29 개발 및 인수 보안시험
	2.8.3 시험과 운영 환경 분리	8.31 개발, 시험 및 생산 환경 분리
	2.8.4 시험 데이터 보안	8.33 정보 시험
	2.8.5 소스 프로그램 관리	–
	2.8.6 운영환경 이관	8.29 개발 및 인수 보안시험
2.9 시스템 및 서비스 운영관리	2.9.1 변경관리	8.32 변경 관리
	2.9.2 성능 및 장애관리	8.6 용량 관리
	2.9.3 백업 및 복구관리	8.13 정보 백업
	2.9.4 로그 및 접속기록 관리	8.15 로깅
	2.9.5 로그 및 접속기록 점검	
	2.9.6 시간 동기화	8.17 시각 동기화
	2.9.7 정보자산의 재사용 및 폐기	7.14 장비의 안전한 폐기 또는 재사용
2.10 시스템 및 서비스 보안관리	2.10.1 보안시스템 운영	
	2.10.2 클라우드 보안	5.23 클라우드 서비스 이용을 위한 정보보안
	2.10.3 공개서버 보안	–
	2.10.4 전자거래 및 핀테크 보안	–
	2.10.5 정보전송 보안	5.14 정보 전송
	2.10.6 업무용 단말기기 보안	8.1 사용자 엔드포인트 디바이스

	2.10.7 보조저장매체 관리	7.10 저장 매체
	2.10.8 패치관리	-
	2.10.9 악성코드 통제	8.7 악성코드로부터 보호

매핑 결과 K-ISMS 의 2. 보호대책 요구사항(기술적 분야) 경우 37 개 항목 중 31 개가 유사성이 있는 항목으로 도출되었으며 이는 83.78%의 유사성이 있는 것으로 비교 분석되었다.

이를 종합하여 K-ISMS 의 2. 보호대책 요구사항의 64 개 항목 중 55 개가 유사성이 있는 항목으로 도출되었으며 이는 85.93%의 유사성이 있는 것으로 비교 분석되었으며 1. 관리체계 수립 및 운영을 항목도 포함하면 K-ISMS 와 ISO 27001: 2022 는 80 개의 항목 중 70 개가 유사성이 있는 항목으로 도출되었으며 이는 87.50%의 유사성이 있는 것으로 비교 분석되었다.

ISO 27001 이 2022 년에 개편되면서 신규로 추가된 항목으로 인하여 유사성은 더 올라갔을 것으로 판단되며 이렇게 높은 유사성이라면 ISO 27001 인증을 받은 기업은 K-ISMS 받은 것과 동등 혹은 그 이상의 정보보호태세를 갖추고 있다고 인정할 수 있을 것이다.

앞서 언급했듯이 ISO-27001 의 강점은 확장성이 높다는 것인데 예를 들어 ISO-27001 에 더해서 추가 구현 통제, 확장 통제 등으로 ISMS-P 처럼 개인정보보호와 관련된 표준도 추가할 수 있으며 ISO-27001 의 이런 유연성도 받아들이면 K-ISMS 은 더욱 더 발전할 여지가 있다고 판단된다.

4. 국내의 기존 선행연구

선행연구에서도 분야나 통제항목에 대해서 중요도나 우선순위를 구하는 연구는 많았지만 객관적인 데이터로 중요도나 우선순위를 구하지는 못하였으며 대부분 설문조사를 통한 전문가집단-AHP 방식으로 중요도 및 우선순위를 산출하였다. 참고한 선행연구는 아래의 표 2-20 과 같다.

<표 2-20> 참고한 국내의 선행연구

발행 년도	연구 제목	산출 방식	연구자
2014	정보보호 항목의 중요도 및 정보보호투자와의 우선순위 차이에 관한 연구 [21]	AHP	김진
2018	콜센터 정보보호관리체계(ISMS) 인증항목의 우선순위 선정에 관한 연구 [22]	AHP	조경재
2022	정보보안 효과성 측정 모델에 관한 연구 [23]	AHP	공우진
2021	중소기업의 특성을 고려한 정보보호 관리체계 평가 모델 개선 [24]	설문조사 분석	김이헌
2022	중소기업을 위한 정보보호관리체계 연구 [25]	AHP	박재성

김진(2014)의 연구[21]는 한정된 자원으로 정보보호 위협에 대처할 수 있도록 정보보호 항목에 중요도에 따른 우선순위를 도출하고 실제 투자 우선순위와 비교하여 정보보호 활동에 이용할 수 있는 자료를 제공하는 것으로 ISMS 를 기반으로 정보보호 활동의 항목을 정하고 이해도가 높은 15 명의 인원을 대상으로 ISMS 의 영역과 분야를 AHP 기법을 통하여 우선순위를 도출하였다. 내용은 아래 표 2-21 과 같다.

<표 2-21> 김진(2014)[21] 상대적 중요도 표

구분	상대적 중요도				
1 계층 통제영역 구분	1 계층 상대적 중요도	2 계층 정보보호 대책	2 계층 상대적 중요도	최종 상대적 중요도	순위
기술적/물리적 통제영역	0.360	시스템 개발 보안	0.184	0.066	8
		암호 통제	0.137	0.049	13
		접근 통제	0.293	0.105	2
		운영보안	0.183	0.066	9
		물리적보안	0.202	0.073	6
사전 관리적 통제영역	0.425	정보보호 정책	0.157	0.067	7
		정보보호 조직	0.153	0.065	10
		외부자 보안	0.128	0.054	11
		정보자산 분류	0.117	0.050	12
		정보보호 교육	0.212	0.090	5
		인적보안	0.233	0.099	3
사후 관리적 통제영역	0.215	침해사고 관리	0.541	0.117	1
		IT 재해복구	0.459	0.099	4

이 연구에서는 1 계층 영역적으로는 사전 관리적 통제영역, 기술적/물리적 통제영역 그리고 2 계층 정보보호 대책적으로는 기술적침해사고 관리, 접근통제, 인적보안, 재해복구, 정보보호 교육순으로 중요도가 도출되었다.

다음으로 조경재(2018)의 연구[22]는 콜센터 시스템의 경우 ISMS 인증대상 및 범위에서 제외되어 있기에 정보보호의 사각지대가 발생하였으며 이를 해결하기 위하여 정보보호 관리체계 인증을 기반한 콜센터에 특화한 가이드라인을 제안하는 것을 목적으로 하고 있다. 중요도를 콜센터 실무자의 관점과 정보보호 전문가의 관점에서 콜센터에 필요한 ISMS 의 항목을 필요성, 시급성, 효과성, 콜센터 적합성을 기준으로 우순순위를 구하였으며 자세한 내용은 아래 표 2-22 와 같다.

〈표 2-22〉 조경재(2018)[22] 정보보호 전문가(기술적 관점)의 가중치 합

구분	가중치 합	RANK
정보보호 정책	1.000	1
정보보호 조직	0.702	4
외부자 보안	0.430	10
정보자산 분류	0.314	11
정보보호 교육	0.596	7
인적 보안	0.742	3
물리적 보안	0.579	8
시스템 개발 보안	0.531	9
암호통제	0.651	6
접근통제	0.977	2
운영 보안	0.656	5
침해사고 관리	0.248	12
IT 재해복구	0.000	13

이 연구에서는 실무자 관점에서는 접근통제, 정보보호 정책, 암호통제 순으로 우선순위가 도출되었으며 정보보호 전문가의 관점에서는 정보보호 정책, 접근통제, 인적 보안, 정보보호 조직, 운영 보안 순으로 중요도가 도출되었다.

공우진(2021)의 연구[23]는 정보보호 인증제도의 효과성 측정 목표와 측정지표 및 세부 측정항목에 대한 수행 항목 간의 중요도 구분과 조직 집단의 특징을 반영할 수 있는 의사 과정 모델에 관하여 연구하였다. 공공기관 보안 담당자, 교육기관 보안담당자, 보안산업 전문가별로 구한 중요도로 기술적 분야는 없으며 관리적, 물리적 분야에 대한 중요도를 구하였다. 분야별 중요도인 2계층에 대해서 구하였으며 자세한 내용은 아래의 표2-23와 같다.

<표 2-23> 공우진(2021) [23] 분야별 최종 중요도

요소	최종 중요도				순위			
	통합 결과	산업	공공 기관	교육 기관	통합 결과	산업	공공 기관	교육 기관
내부자 보안	0.1848	0.1742	0.1958	0.1926	1	1	1	1
정책, 조직, 자산보안	0.1620	0.1679	0.1405	0.1634	2	2	4	2
정보보안 사고대응	0.1429	0.1511	0.1256	0.1418	3	4	5	4
정보보안 업무연속성	0.1349	0.1291	0.1723	0.1135	4	5	2	6
외부자 보안	0.1323	0.1074	0.1690	0.1485	5	7	3	3
정보보안 감사	0.1270	0.1521	0.1105	0.1003	6	3	6	7
시설 보안	0.1162	0.1880	0.0863	0.1398	7	6	7	5

이 연구에서는 분야별로는 내부자 보안, 정책-조직-자산 보안, 정보보안 감사 순으로 도출되었다.

위의 연구들은 정보보호 관리체계의 항목들에 대하여 중요도에 기반한 우선순위를 연구한 것으로 박재성(2022)의 연구[25]는 분야나 항목들의 중요도를 분석하는 게 아닌 중소기업에서의 수행가능성을 분석한 연구이다.

중소기업의 정보보호 애로사항인 예산과 인력 부족에 근거하여 단순 중요도가 아닌 투자가 부족한 중소기업의 특성을 고려하여 주요정보통신기반 취약점 분석평가와 ISMS 를 비교 분석하여 중복되거나 유사한 항목 97 개를 추출하여 중소기업에게 해당 항목의 수행가능성 여부를 설문 조사한 뒤 수행가능성을 기반으로 유형 1(완화), 유형 2(표준), 유형 3(강화)의 중소기업 유형별 점검항목을 만들었다.

마지막으로 김이헌(2021)의 연구[24]는 중소기업 정보보호 컨설팅 지원사업의 결과를 바탕으로 중소기업의 정보보호가 잘 이루어 지지 않는

이유를 중소기업 정보보호 컨설팅 경력이 있는 10 년 이상 경력의 컨설턴트 3 명과 기업 정보보호 관리체계(ISMS) 관련 부서와 중소기업 정보보호 지원부서의 관리자로 역임한 제도 관계자 1 명의 의견도 인터뷰하여 조사하였으며 이를 바탕으로 점검항목의 중소기업 적용여부에 대해서 분석하였다.

〈표 2-24〉 김이헌(2021)[24] 전문가 집단 점검항목 적용여부

점검항목	중소기업 적용여부			
정보보호 정책을 정기적으로 검토하고 제·개정하고 있는가?	C1	C2	C3	S1
식별된 정보자산에 대해 중요도와 보안등급을 부여하고 있는가?	×	×	×	○
주기적·상시적으로 수행하여야 할 정보보호 활동을 식별하고 있는가?	△	△	○	○
네트워크 이상행위 분석 및 모니터링을 수행하고 있는가?	×	×	×	△
정보시스템 세션 타임아웃을 적용하고 있는가?	×	×	×	×
사용자 PC 단말에서의 네트워크를 통한 정보유출 대책을 마련하고 있는가?	×	×	×	×
내부자료 유출방지를 위한 대책을 마련하고 있는가?	×	△	×	×
보조저장매체를 통한 정보유출방지를 위한 대책을 마련하고 있는가?	○	×	×	△
보조저장매체를 통한 정보유출 방지를 위한 대책을 마련하고 있는가?	○	×	×	△
정보시스템의 알려진 취약점에 대한 정기적 분석 및 점검을 수행하고 있는가?	○	○	△	△
침해사고 및 개인정보 유출사고에 대한 예방·대응 체계와 절차를 마련하고 있는가?	○	△	△	○
- C1: 정보보호 컨설턴트 1 - C2: 정보보호 컨설턴트 2 - C3: 정보보호 컨설턴트 3 - S1: 제도 관계자	- ○ : 중소기업이 이행하여야 함 - △ : 필요성은 인정되나 기준을 완화하거나 내용을 대체하여 이행 - × : 필요성이 낮거나 중소기업에서 이행할 수 없음			

전문가들의 답변을 보면 지속적인 관리가 힘들며 세션 타임아웃, PC 단말의 네트워크를 통한 정보유출 대책 같은 높은 기술력이 요구되는 부분도 어려운 경향이 있다.

Ⅲ. 연구 모형 및 연구 방법론

1. 연구 모형

ISO 27001: 2022 에 따르면 정보보호 관리체계는 정보보호 관리과정과 정보보호 통제과정은 나뉘며 통제과정은 조직적 영역, 인적 영역, 물리적 영역, 기술적 영역 4 가지로 나뉜다. 조직적 영역에는 정책, 자산, 정보보호 조직에 관련된 사항부터 인증 및 권한 관리, 공급망, 보안 사고 및 대응, 업무 연속성, 기록 관리까지 폭 넓은 항목들을 담고 있다. ISMS 와 차이점은 기술적이나 인적인 부분도 조직 레벨에서 관리가 필요한 사항은 조직적 영역이라는 점이다.

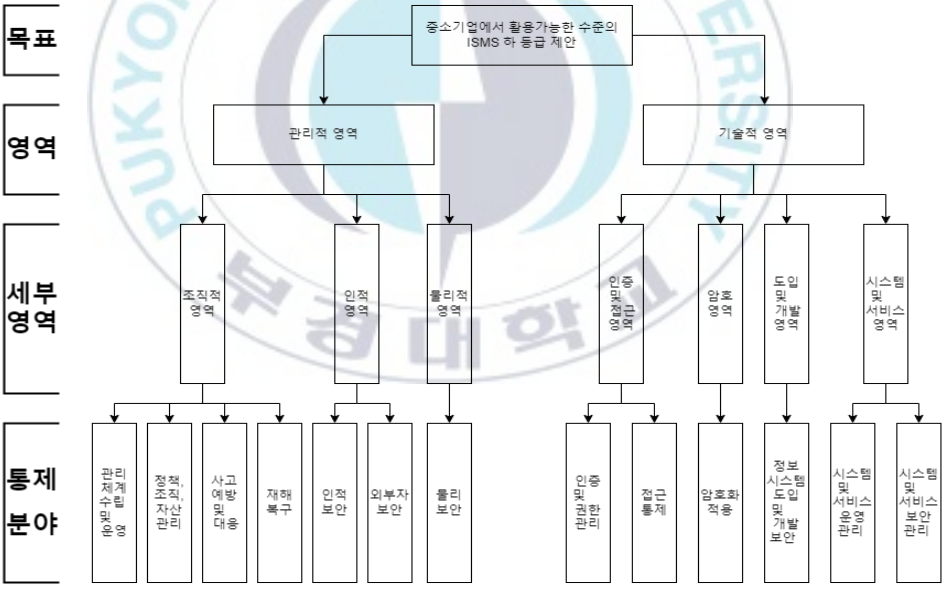
예를 들어 ISMS 의 인적 보안 분야인 주요 직무자 지정 및 관리, 직무 분리의 경우에는 인적 보안의 영역이지만 실무자가 아닌 조직 레벨에서의 관리가 필요하기에 ISO 27001:2022 에서는 조직적 분야에 속하며 비슷한 개념으로 접근 권한에 관해서도 실무자는 적용만 하고 조직 레벨에서 누구에게 어떤 권한을 줄 것인지 정하기에 조직적 분야에 속한다.

ISO 27001 의 방식이 좀 더 옳은 방식이라고 판단되지만 이를 그대로 ISMS 에 적용하면 혼란이 발생할 수 있기에 그대로 적용하지는 않고 어느 정도 ISO 27001 의 방식을 받아들여 조직적 레벨에서의 통제가 필요하다고 판단한 관리체계 수립 및 운영, 정책, 조직, 자산 관리, 사고 예방 및 대응, 재해 복구 분야를 묶어서 조직적 영역으로 분류하였다.

인적 보안과 외부자 보안의 인적 영역은 어떻게 보면 조직적 영역에 속한다고 할 수 있지만 해당 항목의 경우 조직 레벨의 통제보다 실무자의 의한 통제에 가깝다고 생각하며 내부자에 의한 정보 유출이 늘어남에 중요성이 올라가고 있기에 따로 분류하였다.

물리보안의 경우 보통 기술적 영역과 분류를 하는 경우가 많지만 관리적 영역과 좀 더 가깝다고 생각하여 관리적 영역의 안에 포함시켰다.

이를 정리하면 최상위 0 계층은 연구 목표, 1 계층의 2 개 상위 항목인 관리적 영역과 기술적 영역, 관리적 영역을 좀더 세분화한 1.5 계층의 7 개항목이 있으며 2 계층의 13 개의 하위 항목으로 구성하였다.



<그림 3-1> 연구모형의 계층 구조

여기서의 관리 체계 수립 및 운영은 ISMS 와는 성격이 다르다. 목표가 중소기업에서 활용가능한 수준의 ISMS 이며 그것을 위해 기존의 ISMS 항목 중에서 중요도와 중소기업 수행가능성을 고려하여 자신의 기업 사정에

맞게 선택하여 순차적으로 구현하는 것을 상정하였기 때문이다. 그러므로 관리 체계 및 운영의 모든 부분이 아닌 일부 항목만 본 연구에 속 한다.

본 연구에서 사용한 계층별 조작적 정의는 ISMS-P 인증기준 안내서를 참조하였으며 자세한 사항은 아래와 같다.

〈표 3-1〉 1 계층의 조작적 정의

1 계층 (영역)	조작적 정의
관리적 영역	관리적 측면에서 검토하고 준비해야 하는 정보보호 영역
기술적 영역	기술적 측면에서 검토하고 준비해야 하는 정보보호 영역

〈표 3-2〉 관리적 영역 1.5 계층의 조작적 정의

1.5 계층 (세부영역)	조작적 정의
조직적 영역	조직 레벨에서 검토하고 준비해야 하는 정보보호 영역
인적 영역	사람을 대상으로 검토하고 준비해야 하는 정보보호 영역
물리적 영역	물리적 환경을 바탕으로 검토하고 준비해야 하는 정보보호 영역

〈표 3-3〉 기술적 영역 1.5 계층의 조작적 정의

1.5 계층 (세부영역)	조작적 정의
인증 및 접근 영역	인증 및 접근 통제에 대한 사항을 검토하고 준비해야 하는 정보보호 영역
암호 영역	암호화 적용에 대하여 검토하고 준비해야 하는 정보보호 영역
도입 및 개발 영역	도입 및 개발에 관한 사항을 검토하고 준비해야 하는 정보보호 영역
시스템 및 서비스 영역	시스템 및 서비스에 대한 사항을 검토하고 준비해야 하는 정보보호 영역

〈표 3-4〉 관리적 영역 2계층의 조작적 정의

2계층 (통제분야)	조작적 정의
관리체계 수립 및 운영	정보보호 활동에 필요한 기초적인 사항을 정의하고 이를 적용하며 법적 준거성도 검토해야 함.
정책, 조직, 자산 관리	정책, 조직, 자산을 주기적으로 검토하며 유지 관리하여 적정성과 최신성을 유지해야 함.
사고 예방 및 대응	취약점 점검 및 이상행위 모니터링 등의 보안사고 예방 활동을 하며 보안사고가 발생했을 시의 상황을 상정하여 조치 및 대응에 대한 체계를 구축하며 이를 훈련하고 개선해야함.
재해 복구	업무 연속성을 위협할 수 있는 재해 유형을 식별 및 분석하여 대응 체계를 구축하며 이에 대한 시험 및 개선 활동을 해야함.
인적 보안	주요 시스템 접근에 접근 가능한 직무자를 지정하고 보안서약과 위반시 조치 등의 관리 대책을 수립하고 내부 직원들의 보안 인식제고를 위하여 주기적으로 교육을 실시하며 직무 변경 및 퇴직 등의 변경 사항에 조치해야함.
외부자 보안	업무를 외부에 위탁하거나 외부의 시설 또는 서비스를 이용할 경우 그 현황을 식별하고 발생되는 위험을 파악하여 이를 계약 시 반영하고 이행관리를 해야 한다. 또한 계약이 변경되거나 만료 시 그에 맞는 조치를 해야함.
물리 보안	보호구역을 지정하고 출입을 통제해야 하며 물리적으로 시스템을 보호하기 위한 조치와 설비를 운영해야 한다. 또한 보호구역 내의 작업을 관리하고 반출입 기기와 업무환경을 관리한다.

〈표 3-5〉 기술적 영역 2계층의 조작적 정의

2계층 (통제분야)	조작적 정의
인증 및 권한관리	비인가 접근을 통제하고 목적에 따라 권한을 최소한으로 부여할 수 있도록 사용자 계정을 관리하며 식별하며 안전한 인증 절차를 수립 이행하여야 한다. 또한 비밀번호와 특수계정을 관리하고 접근 권한을 주기적으로 검토해야 함.
접근통제	정보자산의 유형에 맞게 접근을 통제하기 위해 대책을 수립 및 이행하여야 함. (네트워크, 정보시스템, 응용프로그램, 데이터베이스, 무선 네트워크, 원격접근, 인터넷 접속 등)
암호화 적용	정보를 보호하고 법적 요구사항을 반영하기 위하여 암호사용 정책을 수립하고 적용하며 키 관리를 해야 함.
정보시스템 도입 및 개발 보안	정보시스템 도입 시 필요한 보안 요구사항을 정의하고 검토 및 시험을 하며 환경을 분리해야 한다. 또한 시험 데이터와 소스 프로그램을 관리하고 이관을 위한 절차에 따라 실행하여야 함.
시스템 및 서비스 운영 관리	시스템 및 서비스를 안전하게 운영하기 위하여 변경관리 및 성능과 장애관리를 해야 하며 주기적으로 백업하며 복구할 수 있도록 절차를 수립 및 이행하여야 한다. 또한 로그 및 접속기록을 관리, 점검해야 하며 정보 시스템간 시간을 동기화하고 정보자산의 재사용 및 폐기 절차를 수립·이행해야 함.
시스템 및 서비스 보안 관리	보안시스템을 운영하며 이용하거나 제공하는 시스템에 맞는 보안대책을 수립·이행하여야 한다. (클라우드, 공개서버, 전자거래 및 핀테크) 또한 정보전송 시 안전한 전송 정책을 수립 및 이행하고 업무용 단말기기와 보조매체 관리를 해야 하며 패치관리 및 악성코드 통제를 해야 함.

2. 프로세스

먼저 중소기업에서 활용가능한 수준의 정보보호 관리체계를 도출을 위한 기준(적용대상, 양적 기준, 질적 기준)을 정립한다. 다음으로 클라우드 하 인증과 ISMS 를 비교분석 후 매핑하여 1 차적으로 정보보호 관리체계를 도출한 후 참고를 위한 1 차 설문조사를 실시한다.

설문조사와 선행연구를 참고하여 기존의 항목을 삭제 및 추가하여 최종적으로 정보보호 관리체계 최종적으로 도출하여 3 계층까지 포함하여 최종 연구모형을 설정한 뒤 2 차 설문조사를 통하여 연구 모형의 2 계층은 중요도를 3 계층은 금전적, 인력적, 시간적 비용을 고려하여 항목별 수행 난이도를 상, 중, 하로 등급을 설정한다. 2 차 설문조사의 결과를 반영하여 중소기업에서 활용가능한 수준의 정보보호 관리체계를 제안한다.

<그림 3-2> 연구의 프로세스

3. 기준 정립

기존 ISMS 에서 중소기업을 위한 ISMS 로 수정하기 위해서 다른 등급이 있는 인증이나 가이드 및 선행연구를 참고하여 기준을 정하기로 하였다.

가. 적용 대상

정보보안 인증 등급제가 있는 인증제도는 클라우드 보안 인증과 정보보호 준비도 평가 등이 있으며 클라우드 보안 인증은 상, 중, 하의 3 등급, 정보보호 준비도 평가는 AAA 등급부투 B 까지 5 등급이 존재한다. 먼저 클라우드 보안인증의 등급 기준은 아래와 같다.

〈표 3-6〉 클라우드 보안 인증의 등급 적용 기준[26]

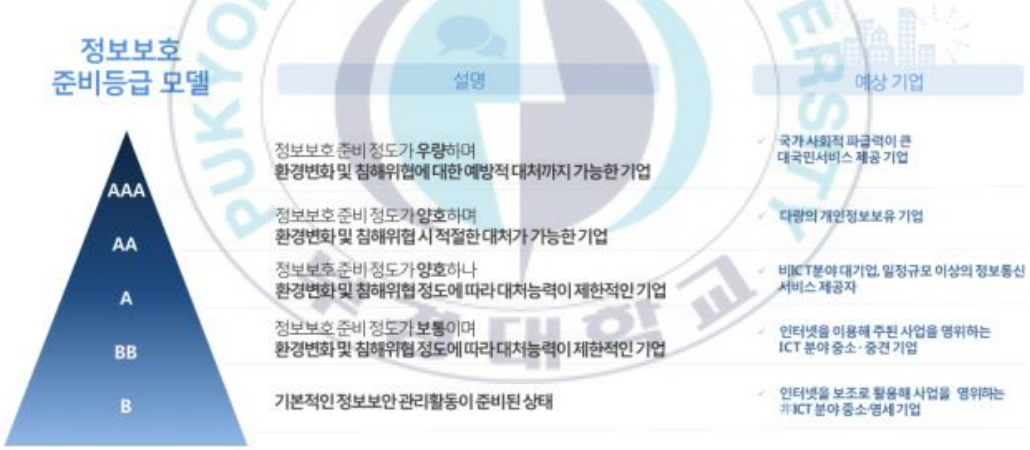
분류 등급	세부사항	
상	파급영향	해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 치명적인 악영향을 미칠 수 있음
	분류기준	국가 중대 이익(안보, 국가안전, 국방, 통일, 외교 등), 수사·재판 등 민감정보를 포함하거나 행정 내부 업무 등을 운영하는 시스템
중	파급영향	해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 심각한 영향을 미칠 수 있음
	분류기준	비공개 업무자료를 포함 또는 운영하는 시스템
하	파급영향	해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 제한적인 영향을 미칠 수 있음
	분류기준	개인정보를 포함하지 않고 공개된 공공데이터를 포함 또는 운영하는 시스템

클라우드 보안인증의 경우 공공기관에 서비스를 제공하는 것이 목적이기에 기준을 그대로 중소기업을 위한 정보보호 관리체계에 적용시키긴 어렵다고 판단된다. 파급영향은 기업의 규모를 기준으로

변경하는 것이 바람직하다고 생각하며 분류기준은 조금 수정을 하면 적용이 가능할 것이다.

정보보호 준비도 평가의 경우 도입 배경은 본 논문의 취지와 유사하나 민간인증의 한계점으로 인하여 지금은 유명무실해진 인증으로 개인정보를 포함하면 30 개의 세부 평가지표를 제외하면 23 개의 평가지표를 가지고 있으며 각 평가 항목 당 점수가 존재하여 모든 항목을 충족할 시 100 점으로 평가한다.

A 등급 이상은 각 항목 당 2 점이상 이하는 1 점 이상은 반드시 충족하여야 한다. 정보보호 준비도 평가의 등급 기준은 아래와 같다.



<그림 3-3> 정보보호 준비등급 인증 분류기준[27]

정보보호 준비등급의 경우 등급기준이 명확하지 않기에 이를 좀더 구체화할 필요가 있어 보이며 위의 인증 2 개를 참고하여 적용 대상기준을 정해보았다. 우선 기업규모로 재직자 50 인 이하의 기업들은 체계적인 정보보호 관리체계를 운영하기가 불가능하다고 판단하기에 제외하였으며. 매출액 기준으로는 200 억 이하의 기업으로 정하였는데 그 이유는 ISMS 인증을 받은 중소기업들 대부분이 매출액이 200 억을 넘기 때문이다.

다음으로 분류기준으로는 민감정보 및 개인정보 또는 암호화폐를 포함하지 않거나 공개된 데이터를 포함 또는 운영하는 시스템으로 정하였다.

그 이유는 ISMS 인증을 받은 중소기업의 경우 대부분 IT 나 쇼핑몰로 기업이 사업을 함에 대량의 개인정보 수집이 필수적인 기업이 대부분이었으며 대량의 개인정보를 포함할 경우 개인정보 보호법의 영향으로 ISMS 와 상관없이 기본적으로 보호 수준이 높아질 수밖에 없다. 이를 고려한 대상은 아래와 같다.

〈표 3-7〉 정보보호 관리체계 적용 기준의 예시

구 분	세부 사항
분류 기준	민감정보 및 개인정보 또는 암호화폐를 포함하지 않으며 공개된 데이터를 포함 또는 운영하는 기업
기업 규모	상한: 매출액 200 억 이하의 기업 하한: 재직자 50 인 이상의 기업

나. 양적 기준

기존의 ISMS 에서 어느 정도의 양을 조정해야 하는지를 알아보기 위해 등급이 존재하는 다른 인증과 자료들을 분석하여 정리하였다. ISMS 를 기준으로 중소기업 지원사원의 ISMS 점검 항목, 클라우드 보안인증 하 등급, 주요정보통신기반시설 취약점 분석, 평가 기준 상과 중하를 분석하여 통제 방향성에 맞게 순서를 조절하여 매핑하였다.

ISMS 의 경우 한 통제항목에 여러 개의 세부항목이 있으며 주요정보통신기반시설 같은 경우는 각각 하나의 항목 들로만 구성되어 있기에 단순 숫자에 의한 비교는 어렵지만 기존의 전체적인 항목에서 등급을 나누는 과정에서 조정된 비율은 알 수 있다고 생각하며 KISA 에서 발주한 ISMS-P 의 등급 용역화의 경우 통제 항목은 줄어들지 않으며

요구수준을 조정하였다. 먼저 참조를 위해 중소기업 컨설팅 지원사업에서 사용한 ISMS 점검 항목과 클라우드 보안인증이 하등급이 생기면서 얼마나 조정되었는지 알아보았다.

<표 3-8> 등급제의 인증 및 자료의 조정 비율 1

중소기업 지원사업 ISMS 점검	항목	클라우드 보안인증 하 등급	항목
관리체계 기반 마련 및 운영	4	1. 정보보호정책 및 조직	2
위험 관리	2	3. 자산관리	3
관리체계 점검 및 개선	3		
		7. 준거성	2
인적 보안	4	2. 인적보안	2
외부자 보안	2	4. 서비스공급망관리	2
물리 보안	4	8. 물리적보안	2
업무환경 보안	2		
인증 및 권한관리	5	10. 접근통제	9
접근통제	9	11. 네트워크 보안	5
정보시스템 개발 보안	2	13. 시스템개발 및 도입보안	6
시스템 보안 관리 및 암호화	4	12. 데이터 보호 및 암호화	3
		9. 가상화보안	6
업무용 단말기기/보조저장매체관리	4		
악성코드 및 패치관리	3	5. 침해사고관리	6
사고 예방 및 대응체계 구축	1	6. 서비스연속성관리	5
재해 복구	1		
합계	50	합계	53
조정 비율	38%	조정 비율	50%

중소기업 ISMS 점검항목은 기존 80 개에서 50 개로 35%, 클라우드 보안인증 하는 106 개에서 53 개로 50%가 삭제되었다.

다음은 주요정보통신기반시설 취약점 분석, 평가 기준으로 총 131 개의 항목들을 중~하 등급 81 개, 상 등급 50 개로 구분하였다.

<표 3-9> 등급제의 인증 및 자료의 조정 비율 2

주요정보통신기반시설 취약점 분석, 평가 기준 중~하	항목	주요정보통신기반시설 취약점 분석, 평가 기준 상	항목
정보보호정책	3	정보보호정책	4
정보보호조직	2	정보보호조직	1
자산분류	2	자산분류	3
감사	5	감사	–
교육 및 훈련	3	교육 및 훈련	2
인적보안	3	인적보안	2
외부자보안	3	외부자보안	2
물리적 분야	11	물리적 분야	7
접근 통제	14	접근 통제	7
운영관리	19	운영관리	16
매체관리	3	매체관리	2
사고대응	9	사고대응	3
모의해킹	1	모의해킹	–
업무 연속성관리	3	업무 연속성관리	1
합계	81	합계	50
조정 비율	38%	조정 비율	62%

주요정보통신기반시설 취약점 분석, 평가 기준은 조정을 했다고 보다는 구분을 한 것에 가까우면 상의 항목들이 평가점수가 더 높기에 상대적으로 더 중요한 항목들이라고 할 수 있다. 위의 사항들을 대입하면 중소기업을 위한 정보보호 관리체계의 항목 수는 대략 40~50 개로 예상된다.

다. 질적 기준

양적 기준에 대해서는 어느 정도 공식적이며 객관적인 자료가 존재하지만 질적 기준은 객관화가 불가능한 기준이라고 생각한다. 그리고 통제항목 각각에 대한 중요도를 구하기에는 판단하는 대상에 따라 결과 값을 차이가 크다고 생각하기에 통제 분야 까지만 중요도를 구하기로 하였다.

질적 기준을 정하기 위한 중요도 분석은 이미 등급제가 존재하는 클라우드 보안인증 하를 역으로 분석해서 왜 이렇게 조정했는지 유추를 하여 중요도를 구해보는 방식과 기존의 선행연구에서 설문조사를 통하여 중요도를 산출한 결과를 모아서 분석하는 방법 2 가지로 나눠서 하기로 하였다.

1) 중요도

중요도를 구하기 위해 클라우드 보안 인증을 참고하기로 하였다. 클라우드 보안인증 하 등급의 경우 기존 인증에 비해서 세부항목이 116 개에서 64 개로 45%의 항목이 줄어들었으며 14. 국가기관 등의 보안 요구사항을 제외하고 계산하면 106 개에서 53 개로 50%가 삭제되었다. 이를 역 분석하여 어떤 기준으로 하 등급을 만들었는지 유추할 수 있다.

기존 인증에서 하 항목으로 변경 시 삭제된 항목의 수를 구하였으며 이를 기존 항목과 비교하여 삭제 비율을 구하여 삭제된 항목이 많아 비율이 높은 항목이 중요도가 낮은 항목이라고 할 수 있다.

1 계층의 삭제 항목의 비율로 유추한 중요도는 아래 표 와 같다.

〈표 3-10〉 클라우드 보안 인증 1 계층 중요도 분석

1 계층 항목	기존	하 등급	삭제	삭제 비율	중요도
1. 정보보호 정책 및 조직	5	2	3	60.00%	9
2. 인적보안	11	2	9	81.82%	12
3. 자산관리	10	3	7	70.00%	10
4. 서비스 공급망 관리	4	2	2	50.00%	6
5. 침해사고관리	7	6	1	14.29%	2
6. 서비스 연속성 관리	7	5	2	28.57%	4
7. 준거성	4	2	2	50.00%	6
8. 물리적 보안	11	2	9	81.82%	12
9. 가상화 보안	10	6	4	40.00%	5
10. 접근통제	9	9	0	0%	1
11. 네트워크 보안	6	5	1	16.67%	3
12. 데이터 보호 및 암호화	10	3	7	70.00%	10
13. 시스템 개발 및 도입 보안	12	6	6	50.00%	6
합계	106	53	53	50.00%	-

제일 많은 비율로 삭제된 항목은 11 개의 항목에서 9 개가 삭제된 인적보안과 물리적 보안이다. 제일 적게 삭제된 항목은 접근통제로 단 하나의 항목도 삭제되지 않았으며 그 다음으로 침해사고관리 7 개항목 중 1 개, 네트워크 보안이 6 개의 항목 중 1 개가 삭제되었다.

결과 값을 보면 인적보안이 너무 낮게 나왔다고 생각하지만 주관적인 생각이 아닌 데이터로만 판단하면 접근통제의 항목이 단 하나의 항목도 삭제되지 않아 중요도 가장 높은 것으로 산출되었으며 그 다음으로 침해사고관리, 네트워크 보안, 서비스 연속성 관리순으로 나왔다.

다음으로 2 계층에서는 극단적으로 하나도 삭제되지 않은 분야와 모든 항목이 삭제된 분야가 다수 나왔다. 계층의 삭제 항목의 비율로 유추한 중요도는 아래 표와 같다.

〈표 3-11〉 클라우드 보안 인증 2계층 중요도 분석

2계층 항목	기존	하 등급	삭제	삭제 비율	중요도
1.1. 정보보호 정책	3	1	2	66%	20
1.2. 정보보호 조직	2	1	1	50%	12
2.1. 내부인력 보안	5	1	4	80%	26
2.2. 외부인력 보안	3	0	3	100%	27
2.3. 정보보호 교육	3	1	2	66%	20
3.1. 자산 식별 및 분류	3	2	1	33%	10
3.2. 자산 변경관리	3	0	3	100%	27
3.3. 위험관리	4	1	3	75%	24
4.1. 공급망 관리 정책	2	1	1	50%	12
4.2. 공급망 변경관리	2	1	1	50%	12
5.1. 침해사고 대응 절차 수립 및 체계	3	3	0	0%	1
5.2. 침해사고 대응	2	2	0	0%	1
5.3. 사후관리	2	1	1	50%	12
6.1. 장애대응	4	4	0	0%	1
6.2. 서비스 가용성	3	1	2	66%	20
7.1. 법 및 정책 준수	2	1	1	50%	12
7.2. 보안 감사	2	1	1	50%	12
8.1. 물리적 보호구역	5	2	3	60%	19
8.2. 정보처리 시설 및 장비보호	6	0	6	100%	27
9.1. 가상화 인프라	6	5	1	16%	7
9.2. 가상 환경	4	1	3	75%	24
10.1. 접근통제 정책	2	2	0	0%	1
10.2. 접근 권한 관리	3	3	0	0%	1
10.3. 사용자 식별 및 인증	4	4	0	0%	1
11.1. 네트워크 보안	6	5	1	16%	7
12.1. 데이터 보호	6	2	4	66%	20
12.2. 매체 보안	2	0	2	100%	27
12.3. 암호화	2	1	1	50%	12
13.1. 시스템 분석 및 설계	5	3	2	40%	11
13.2. 구현 및 시험	4	3	1	25%	9
13.3. 외주 개발 보안	1	0	1	100%	27
13.4. 시스템 도입 보안	1	0	1	100%	27

삭제가 안된 분야는 침해사고 대응 절차 수립 및 체계, 침해사고 대응, 장애 대응, 접근통제 정책, 접근 권한 관리, 사용자 식별 및 인증이다. 모든

항목이 삭제된 분야는 외부 인력보안, 자산 변경관리, 정보처리 시설 및 장비보호, 매체 보안, 외주 개발 보안, 시스템 도입 보안이다.

2) 중소기업 수행 가능성

중소기업 수행 가능성은 박재성(2022)의 연구[24] 자료를 참고하였다. 위 연구의 경우 ISMS와 주요정보통신기반시설 취약점 분석평가를 비교하여 19 개 분야로 구분한 97 항목에 대해서 중소기업 담당자 103 명에게 수행 가능성에 대해서 설문조사를 하였으며 그 결과를 바탕으로 중소기업 유형별 정보보호관리체계를 도출하여 제안하였다.

<표 3-12> 박재성(2022)의 연구[24] 설문조사 결과 분야별 정리

통제 분야	수행가능성[24]	순위
정보보호 정책수립 및 관리	54.17%	5
정보보호 계획 수립 및 검토	26.94%	18
정보보호 조직 구성	25.24%	19
정보자산 식별 및 관리	47.90%	10
정보보호 교육	53.16%	7
인적 보안	56.50%	3
보호구역 지정 및 보안	42.60%	14
시스템 보호 및 설비관리	43.27%	13
업무환경 보안	68.61%	2
시스템 인증 및 권한관리	55.50%	4
접근통제	37.76%	15
암호화 적용	46.84%	11
시스템 도입 및 개발 보안	51.46%	8
시스템 운영관리	44.50%	12
시스템 보안관리	53.98%	6
업무용 단말기 및 매체 보안	51.07%	9
악성코드 통제	70.87%	1
사고 예방 및 대응	30.22%	17
재해 복구	33.25%	16

설문조사 결과를 19 개 분야별로 정리하면 제일 높은 항목은 악성코드 통제 70,87% 다음이 업무환경 보안이 68.61%이다. 제일 낮은 항목은 정보보호 조직 구성 25.24% 다음이 정보보호 계획 수립 및 검토 26.94%이다. 그 외에도 사고 예방 및 대응 30.22%, 재해 복구 33.25% 등도 상당히 중요한 분야이지만 수행 가능성이 낮다고 답변하였다.

타 인증 및 선행연구를 바탕으로 중소기업에서 활용가능한 수준의 중소기업을 위한 정보보호 관리체계 도출에 필요한 기준들을 알아보았으며 그 사항은 인증 대상, 양적 기준, 질적 기준이며 질적 기준에는 중요도만 아니라 중소기업의 수행가능성도 고려하였다. 이를 정리하여 표로 나타내면 아래와 같다.

<표 3-13> ISMS 하 등급 도출에 필요한 기준정리

기준	세부 사항	
인증 대상	기업 규모	상한: 매출액 200 억 이하의 기업 하한: 재직자 50 인 이상의 기업
	분류 기준	개인정보를 포함하지 않고 공개된 데이터를 포함 또는 운영하는 시스템
항목의 수	등급제의 타 인증 및 자료 참고	
중요도	클라우드 보안 인증 하 등급 삭제 항목 분석 참고 설문조사 참고 선행연구 참고	
중소기업 수행가능성	2022, 박재성의 연구 참고 설문조사 참고	

4. 클라우드 보안 인증 하 등급과 ISMS 매핑

ISMS와 유사성을 찾지 못한 8개 항목을 제외하였으며 ISMS와 유사성이 있는 클라우드 보안인증의 45 개의 항목을 ISMS 의 항목과 매핑 한 후 중복제거를 하면 34 개의 ISMS 항목이 도출된다.

〈표 3-14〉 클라우드 보안인증 하 통제항목과 ISMS 매핑 결과

영역	통제 분야	통제 항목
1. 관리체계 수립 및 운영	1.1 관리체계 기반 마련	1.1.3 조직 구성
		1.1.5 정책 수립
	1.2 위험 관리	1.2.1 정보자산 식별
	1.4 관리체계 점검 및 개선	1.4.1 법적 요구사항 준수 검토
2. 보호대책 요구사항	2.1 정책, 조직, 자산 관리	2.1.3 정보자산 관리
	2.2 인적 보안	2.2.1 주요 직무자 지정 및 관리
		2.2.4 인식제고 및 교육훈련
	2.4 물리 보안	2.4.1 보호구역 지정
		2.4.2 출입통제
	2.5 인증 및 권한관리	2.5.1 사용자 계정 관리
		2.5.2 사용자 식별
		2.5.3 사용자 인증
		2.5.4 비밀번호 관리
		2.5.5 특수 계정 및 권한관리
		2.5.6 접근권한 검토
	2.6 접근통제	2.6.1 네트워크 접근
	2.7 암호화 적용	2.7.1 암호정책 적용
	2.8 정보시스템 도입 및 개발 보안	2.8.1 보안 요구사항 정의
		2.8.2 보안 요구사항 검토 및 시험
		2.8.3 시험과 운영 환경 분리
		2.8.5 소스 프로그램 관리
	2.9 시스템 및 서비스 운영관리	2.9.2 성능 및 장애관리
		2.9.4 로그 및 접속기록 관리
		2.9.6 시간 동기화
	2.10 시스템 및 서비스 보안관리	2.10.1 보안시스템 운영
		2.10.3 공개서버 보안
		2.10.9 악성코드 통제
	2.11 사고 예방 및 대응	2.11.1 사고 예방 및 대응체계 구축
		2.11.2 취약점 점검 및 조치
	2.12 재해 복구	2.12.1 재해 · 재난 대비 안전조치

다음은 통제 분야를 매핑한 결과이며 중요도는 앞의 클라우드 보안 인증 하로 변경되면서 삭제된 항목의 비율로 유추한 중요도이며 빈칸의 경우 ISMS 와 매핑이 되는 항목이 없는 경우이다. 자세한 내용은 아래의 표와 같다.

〈표 3-15〉 클라우드 보안인증 하 1 계층과 ISMS 통제 분야 매핑

클라우드 보안 인증 하 1 계층	중요도	ISMS 통제 분야
1. 정보보호정책 및 조직	8	1.1 관리체계 기반 마련
		2.1 정책, 조직, 자산 관리
3. 자산관리	9	
		1.2 위험 관리
–	–	1.3 관리체계 운영
7. 준거성	6	1.4 관리체계 점검 및 개선
2. 인적보안	11	2.2 인적 보안
–	–	2.3 외부자 보안
8. 물리적보안	11	2.4 물리 보안
10. 접근통제	1	2.5 인증 및 권한관리
		2.6 접근통제
11. 네트워크 보안	3	
		2.10 시스템 및 서비스 보안관리
9. 가상화보안	5	2.9 시스템 및 서비스 운영관리
6. 서비스연속성관리	4	
		2.12 재해 복구
5. 침해사고관리	2	2.11 사고 예방 및 대응
12. 데이터 보호 및 암호화	9	2.7 암호화 적용
13. 시스템 개발 및 도입 보안	6	2.8 정보시스템 도입 및 개발 보안

위의 결과는 삭제된 항목의 비율로 유추한 중요도를 아무 해석 없이 그대로 매칭한 결과이며 1 계층의 특성 상 범위가 넓기 때문에 매칭이 여러 항목에 걸치기 때문에 정확도 있는 분석은 어렵지만 경향은 알 수 있었는데 클라우드 보안인증 하를 조정을 한 기준으로 ISMS 에 대입하면 인증 및 권한관리, 접근 통제, 사고 예방 및 대응, 재해 복구 등의 항목을 중요시하는 의도가 있다고 판단된다.

다음은 클라우드 보안인증 하의 2 계층과 ISMS 통제분야를 매핑한 결과로 자세한 내용은 아래의 표와 같다.

<표 3-16> 클라우드 보안인증 하 2 계층과 ISMS 통제 분야 매핑

클라우드 보안 인증 하 통제분야	중요도	ISMS 통제 분야
1. 정보보호정책 및 조직	8	1.1 관리체계 기반 마련
		2.1 정책, 조직, 자산 관리
3. 자산관리	9	
		1.2 위험 관리
–	–	1.3 관리체계 운영
7. 준거성	6	1.4 관리체계 점검 및 개선
2. 인적보안	11	2.2 인적 보안
–	–	2.3 외부자 보안
8. 물리적보안	11	2.4 물리 보안
10. 접근통제	1	2.5 인증 및 권한관리
		2.6 접근통제
11. 네트워크 보안	3	
		2.10 시스템 및 서비스 보안관리
9. 가상화보안	5	2.9 시스템 및 서비스 운영관리
6. 서비스 연속성 관리	4	
		2.12 재해 복구
5. 침해사고 관리	2	2.11 사고 예방 및 대응
12. 데이터 보호 및 암호화	9	2.7 암호화 적용
13. 시스템 개발 및 도입 보안	6	2.8 정보시스템 도입 및 개발 보안

클라우드 보안인증의 2 계층은 32 항목이었지만 모든 통제항목이 삭제되었거나 ISMS 와 매핑이 되지 않아 7 개의 항목이 제거되어 25 개의 항목이 ISMS 와 매핑 되었다.

1 계층의 결과보다 좀 더 자세한 중요도가 나왔으며 클라우드 보안인증 하를 조정한 의도를 그대로 ISMS 에 대입하면 인증 및 권한관리가 제일 높은 중요도를 가졌으며 다음으로 사고 예방 및 대응과 접근통제 순이다.

반대로 제일 낮은 중요도는 관리체계 운영, 외부자 보안이며 그 다음이 물리 보안 순이다. 관리체계 운영은 중요도가 낮다고 판단하기 보다는 클라우드 보안인증과 유사성이 없다고 할 수 있지만 외부자 보안과 물리 보안은 유사성이 있으면서도 중요도가 낮게 도출되었다.

1 계층과 ISMS 를 매핑했을 때와 마찬가지로 2 계층과의 매핑에서도 기술적 분야와 사후 관리적 분야의 중요도가 높았다. 이 부분에 대해서는 단순히 이 분야가 중요하다고 판단하기 보다는 하 등급을 도출하는 과정에서 우선시되었다고도 할 수 있을 것이다.

ISMS 를 조정하기 위한 기준 중에 질적 기준을 구해보기 위하여 클라우드 보안인증에서 하 등급으로 조정되는 과정 중 삭제된 항목들을 기반으로 역분석하여 중요도를 유추해서 ISMS 에 대입해 본 결과 인증 및 권한관리가 제일 높은 중요도를 가졌으며 다음으로 사고 예방 및 대응과 접근통제 순이다. 반대로 제일 낮은 중요도는 관리체계 운영, 외부자 보안이며 그 다음이 물리 보안 순이다.

경향적으로는 기술적 분야, 사후 관리적 분야, 사전 관리적 분야, 인적 분야, 물리적 분야순으로의 중요도 혹은 우선시되었다.

다음으로 클라우드 보안 인증 하와 ISMS 를 매핑 후 중복제거 한 34 개의 항목에 대해서 중소기업 수행 가능성을 대입하여 분석하였다. 매핑 항목이 없는 경우도 있는데 이 부분은 주요정보통신기반시설 취약점평가 항목에 이 부분이 없기 때문이라고 생각한다.

<표 3-17> 매핑 한 ISMS 항목과 중소기업 수행 가능성[24] 대입 결과

통제 항목	수행 가능성[24]	항목별 순위
1.1.3 조직 구성	25.24%	24
1.1.5 정책 수립	58.98%	8
1.2.1 정보자산 식별	50.49%	12
1.4.1 법적 요구사항 준수 검토	–	–
2.1.3 정보자산 관리	42.72%	17
2.2.1 주요 직무자 지정 및 관리	43.69%	16
2.2.4 인식제고 및 교육훈련	53.16%	11
2.4.1 보호구역 지정	70.39%	2
2.4.2 출입통제	33.50%	20
2.5.1 사용자 계정 관리	69.42%	4
2.5.2 사용자 식별	–	–
2.5.3 사용자 인증	48.54%	13
2.5.4 비밀번호 관리	68.93%	5
2.5.5 특수 계정 및 권한관리	–	–
2.5.6 접근권한 검토	28.16%	21
2.6.1 네트워크 접근	55.98%	9
2.7.1 암호정책 적용	69.42%	3
2.8.1 보안 요구사항 정의	45.63%	14
2.8.2 보안 요구사항 검토 및 시험	65.05%	6
2.8.3 시험과 운영 환경 분리	61.17%	7
2.8.5 소스 프로그램 관리	33.98%	19
2.9.2 성능 및 장애관리	27.18%	22
2.9.4 로그 및 접속기록 관리	–	–
2.9.6 시간 동기화	–	–
2.10.1 보안시스템 운영	53.40%	10
2.10.3 공개서버 보안	–	–
2.10.9 악성코드 통제	70.87%	1
2.11.1 사고 예방 및 대응체계 구축	26.21%	23
2.11.2 취약점 점검 및 조치	38.51%	18
2.11.3 이상행위 분석 및 모니터링	–	–
2.11.4 사고 대응 훈련 및 개선	24.27%	26
2.11.5 사고 대응 및 복구	24.76%	25
2.12.1 재해 · 재난 대비 안전조치	45.15%	15
2.12.2 재해 복구 시험 및 개선	21.36%	27

5. 1 차 설문조사

해당 설문조사는 앞의 내용의 대한 평가와 ISMS 와 클라우드 보안인증 하를 비교 분석하여 1 차 도출된 값을 어떤 방향과 분야를 수정할 지에 대해서 참고하기 위한 단순 앙케이트로 이 설문의 결과가 유의미한 영향을 주진 않는다.

폭 넓은 의견을 모으기 위해 사원부터 임원까지 보안인증 심사 수행 경험이 있는 인원부터 단순 IT 직무자까지 다양한 대상에 대하여 간단한 설문조사를 진행하였으며 설문조사 대상에 대한 자세한 내용은 아래와 같다.

<표 3-18> 1 차 설문조사 대상(30 명)

구분	세부구분	설문자 수	비율
직급	사원	3	10%
	대리	2	7%
	과장	9	30%
	차장 ~ 부장	11	37%
	임원	1	3%
업무 경력	1 년 이상 ~ 3 년 이하	2	7%
	3 년 이상 ~ 5 년 이하	1	3%
	5 년 이상~ 7 년 이하	1	3%
	7 년 이상 ~ 10 년 이하	5	17%
	10 년 이상	16	53%
관련 지식	보안인증 심사자격 소지자 및 수행 경험이 있다.	6	20%
	기업서 ISMS 인증을 받았거나 ISMS 에 대한 컨설팅 경험	9	30%
	컨설팅이나 진단 업무 수행	1	3%
	보안담당자 및 전산담당자	7	23%
	보안 및 IT 회사의 업무	7	23%

이 설문조사의 자세한 내용은 부록 1 에 있으며 답변 중 몇 가지를 요약하자면 ISMS 하 등급 항목의 수는 40~60 개가 적당하다는 의견이 많았으며 중요도가 떨어지더라도 한 분야의 모든 항목을 삭제하는 건 바람직하지 않다 라는 의견이 생각보다 많았다. 클라우드 보안인증을 등급하로 조정하는 과정에서 삭제한 항목으로 유추한 중요도를 평가받았을 때 범위가 넓은 1 계층이 보다 세분화된 2 계층보다 정확도가 높다고 평가받은 걸 생각하면 중요도에 대해서 하위 계층으로 갈수록 의견이 달라진다는 점이다.

항목을 추가할 때 기준은 중요도 53.3%, 비용이 적게 드는 항목 26.7%, 인력 및 시간적 소모가 적은 항목 20%로 나왔지만 삭제할 때의 기준은 중요도가 낮은 항목 43.3%, 중요도가 높아도 비용이 많이 드는 항목 33.3%, 중요도가 높아도 인력 및 시간적 소모가 높은 항목 23.3%로 추가할 항목보다 삭제할 항목을 고려할 때 비용이 많이 드는 항목의 증가가 있었다.

추가를 추천하는 분야는 인적 분야가 33.3%, 관리적 분야가 26.7%로 가장 많았으며 이 항목들이 중요하다고 생각하거나 부족하다는 의견이 많았으며 삭제를 추천하는 분야는 사후 관리적 분야(사고 예방 및 대응, 재해 복구)와 물리적 분야였는데 사후 관리적 분야는 중요는 하지만 비용이 많이 들기 때문인 거 같으며 물리적 분야는 상대적으로 중요도가 낮다고 생각하는 경향이 있다고 판단된다.

6. 통제항목 조정

가. 삭제

설문조사와 선행연구를 참고하여 7 개의 항목을 삭제하였으며 삭제를 위한 기준과 결과는 아래와 같다.

1. 항목의 세부사항을 수행하기 위한 금전적 비용이 높다.

2. 항목의 세부사항을 수행하기 위한 인력 및 시간적 소모가 높다.

3. 중요도가 낮다.

〈표 3-19〉 삭제한 항목과 중소기업 수행가능성

삭제한 ISMS 항목	중소기업 수행가능성[24]
2.5.6 접근권한 검토	28.16%
2.8.5 소스 프로그램 관리	33.98%
2.9.4 로그 및 접속기록 관리	-
2.11.3 이상행위 분석 및 모니터링	-
2.11.4 사고 대응 훈련 및 개선	24.27%
2.11.5 사고 대응 및 복구	26.21%
2.12.2 재해 복구 시험 및 개선	21.36%

1 에 해당하는 항목은 2.11.3 이상행위 분석 및 모니터링, 2.11.4 사고 대응 훈련 및 개선, 2.11.5 사고 대응 및 복구, 2.12.2 재해 복구 시험 및 개선이다.

설문조사에서도 사후 관리적 분야(2.11 사고 예방 및 대응, 2.12 재해 복구)가 가장 높은 삭제 추천 항목이었으며 대기업에서도 자체적으로 하기가 어려워서 보안관제서비스 등 외부업체를 이용하는 경우가 많을 정도로 난이도와 그에 필요한 금전적 비용이 높기에 중소기업에서 하기는 어렵다고 판단했으며 2.11.2 취약점 점검 및 조치의 경우 KISA 에서 중소기업 보안 취약점 점검 지원사업도 하고 있으며 중소기업 자체적으로도 스캔이나 간단한 툴로도 할 수는 있다고 판단되어 제외하지 않았다.

2 에 해당하는 항목은 2.5.6 접근권한 검토, 2.8.5 소스 프로그램 관리, 2.9.4 로그 및 접속기록 관리이다. 이 항목들은 중소기업의 인력 부족 때문에 지속적인 관리가 힘들다는 의견을 고려한 것이다.

3 에 해당하는 항목은 없다.

나. 추가

설문조사와 선행연구를 참고하여 17 개의 항목을 추가하였다. 설문조사에서도 관리적 분야와 인적분야를 추가해야 한다는 의견이 가장 많았으며 앞의 중소기업 정보보호 실태에서도 인적 보호 관리분야의 역량 점수가 가장 낮았는 걸 감안하였다. 추가를 위한 기준과 결과는 아래와 같다.

1. 중요도가 높다.

2. 중요도에 비해 항목의 세부사항을 수행하기 위한 인력 및 시간적 소모가 낮다.

3.중요도에 비해 항목의 세부사항을 수행하기 위한 금전적인 비용이 낮다.

<표 3-20> 추가한 항목과 중소기업 수행가능성

추가한 ISMS 항목	중소기업 수행가능성[24]
1.1.1 경영진의 참여	27.18%
1.1.2 최고책임자의 지정	-
2.1.1 정책의 유지관리	34.95%
2.1.2 조직의 유지관리	-
2.2.3 보안 서약	86.41%
2.2.5 퇴직 및 직무변경 관리	69.90%
2.2.6 보안 위반 시 조치	56.31%
2.3.1 외부자 현황 관리	-
2.3.4 외부자 계약 변경 및 만료 시 보안	-
2.4.3 정보시스템 보호	75.73%
2.4.7 업무환경 보안	68.61%
2.6.2 정보시스템 접근	-
2.6.4 데이터베이스 접근	-
2.6.6 원격접근 통제	27.67%
2.9.3 백업 및 복구관리	55.83%
2.9.7 정보자산의 재사용 및 폐기	51.46%
2.10.6 업무용 단말기기 보안	54.69%

또한 기술노출의 제일 높은 원인이 내부자에 의한 노출인 점도 고려하여 인적보안 분야의 항목들을 가장 중점적으로 추가하였으며 다음으로는 관리적 분야와 기술적 분야 순이었으며 물리적 분야가 가장 낮았다.

1 에 해당하는 항목은 1.1.1 경영진의 참여, 1.1.2 최고책임자의 지정, 2.1.1 정책의 유지관리, 2.1.2 조직의 유지관리, 2.6.4 데이터베이스 접근 ,2.6.6 원격접근 통제, 2.9.3 백업 및 복구관리이다.

2 에 해당하는 항목은 2.2.3 보안 서약, 2.2.5 퇴직 및 직무변경 관리, 2.2.6 보안 위반 시 조치, 2.3.1 외부자 현황 관리, 2.3.4 외부자 계약 변경 및 만료 시 보안, 2.4.7 업무환경 보안, 2.6.2 정보시스템 접근이다.

3 에 해당하는 항목은 2.4.3 정보시스템 보호, 2.9.7 정보자산의 재사용 및 폐기이다.

1.1.1 경영진의 참여, 1.1.2 최고책임자의 지정, 2.1.1 정책의 유지관리, 2.1.2 조직의 유지관리 같은 경우 정보보호 활동에 대한 근본적인 부분으로 이 부분이 확립되지 않고 서는 기업의 효율적인 정보보호가 이루어지지 않는다고 판단하여 추가하였다.

넷 중에서 가장 중요한 것은 정책의 유지관리라고 생각하며 조직, 자산 같은 경우는 한번 만들어 놓으면 그 뒤로 관리를 꼼꼼히 하지 않아도 효과가 어느 정도 유지되지만 정책의 경우 관련 법이 변경되거나 조직의 대내외 환경에 맞게 주기적으로 검토하고 그에 맞게 최신화를 하지 않으면 효과가 반감되기 때문이다.

2.2.3 보안 서약, 2.2.5 퇴직 및 직무변경 관리, 2.2.6 보안 위반 시 조치, 2.3.1 외부자 현황, 2.3.4 외부자 계약 변경 및 만료 시 보안의 경우 인적 관리에 관한 항목들로 보안 서약은 단순한 실속이 없는 요식행위라고 생각할 수 있지만 대상에게 비밀준수의무 같은 보안에 대한 책임을 인식할 수 있게 하는 유용한 방법이며 무언가 변경이 있을 때 그에 대한 적절한 조치가 없는 경우 보안은 취약해지는 경우가 발생한다.

퇴직한 직원의 접근 권한이 삭제되지 않아 정보가 유출되거나 계약이 만료되어 외주업체가 철수할 때 관리가 소홀하거나 악의를 가지고 정보가 유출되는 경우도 발생하였다. 그러므로 인적 관리의 경우 시작보다 끝 부분에서 문제가 발생할 요지가 크다고 할 수 있다.

외부자 현황 관리는 외부자 보안을 관리할 때 필수적인 요소라고 생각하며 보안 위반 시 조치는 구성원들의 지속적인 보안인식 제고를 위해 필요하다고 생각한다.

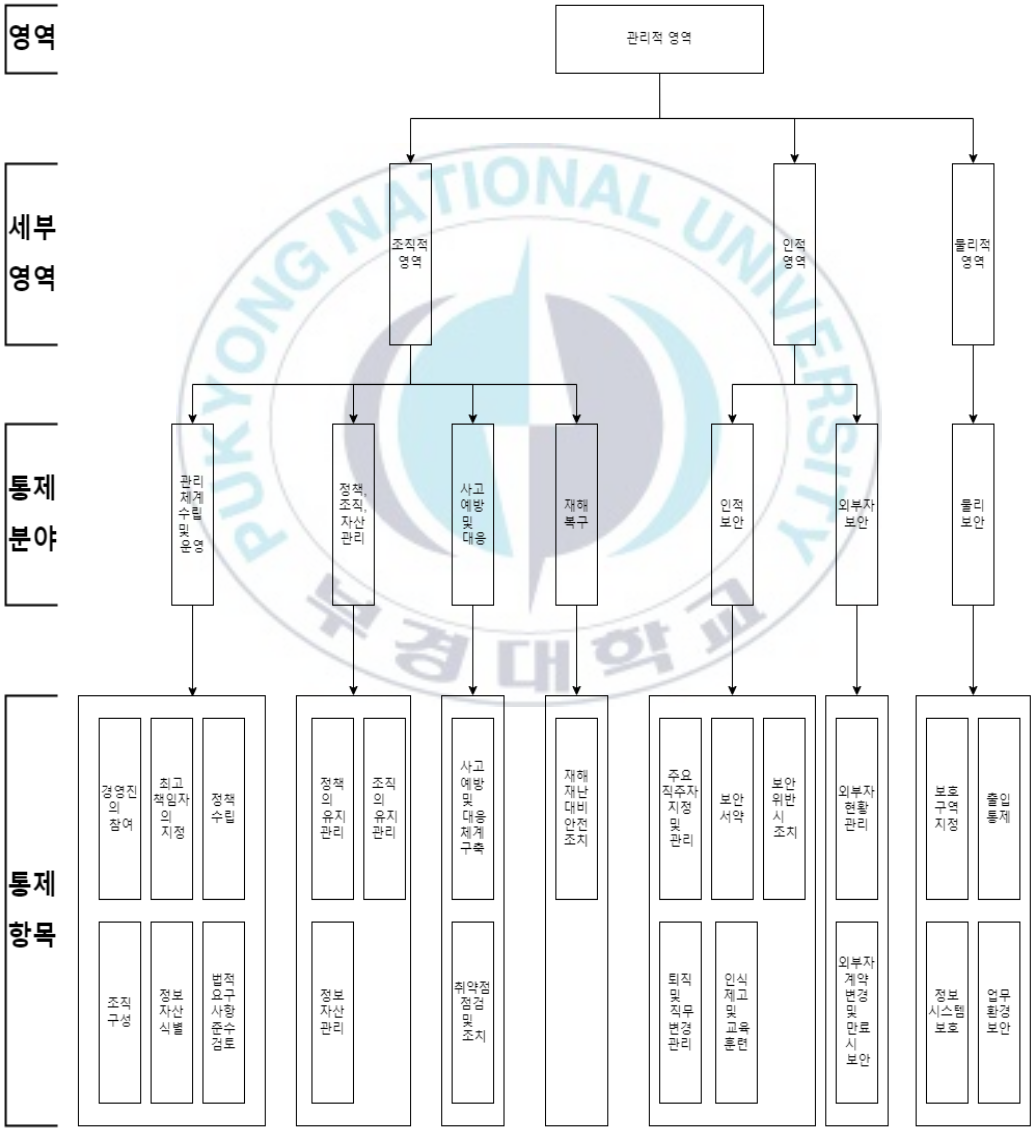
물리 보안 부분에서는 2.4.3 정보시스템 보호와 2.4.7 업무환경 보안을 추가하였으며 이유는 정보시스템 보호와 업무환경 보안은 비교적 손 쉽게 할 수 있는 것에 비해 효과가 크다고 판단하였다.

2.6 접근통제의 항목들은 2.6.2 정보시스템 접근, 2.6.4 데이터베이스 접근, 2.6.6 원격접근 통제를 추가하였으며 원격접근 통제의 경우 코로나의 영향으로 재택근무가 많이 늘어났고 팀뷰어 같은 사설 원격접속 프로그램의 경우 해커가 크리덴셜스터핑으로 노출된 계정을 이용하여 회사 내부에 접속해서 정보가 노출되는 등의 보안사고도 발생하기에 중요도가 높아졌으며 정보시스템의 취약점을 잘 방어해도 접근이 쉽게 되면 무용지물이라 생각하여 추가하였다. 그리고 데이터베이스 접근은 난이도가 높지만 중요도가 높아서 추가하였다.

운영관리에서는 2.9.3 백업 및 복구관리와 2.9.7 정보자산의 재사용 및 폐기를 추가하였으며 백업 및 복구관리의 경우 비록 금전적인 비용이 많이 들지만 업무 연속성 측면이나 랜섬웨어 대응 측면에서나 너무나도 중요도가 높다고 판단되어 추가하였으며 정보자산의 재사용 및 폐기는 중요도에 비해 금전적, 인적 비용이 낮다고 생각하여 추가하였다.

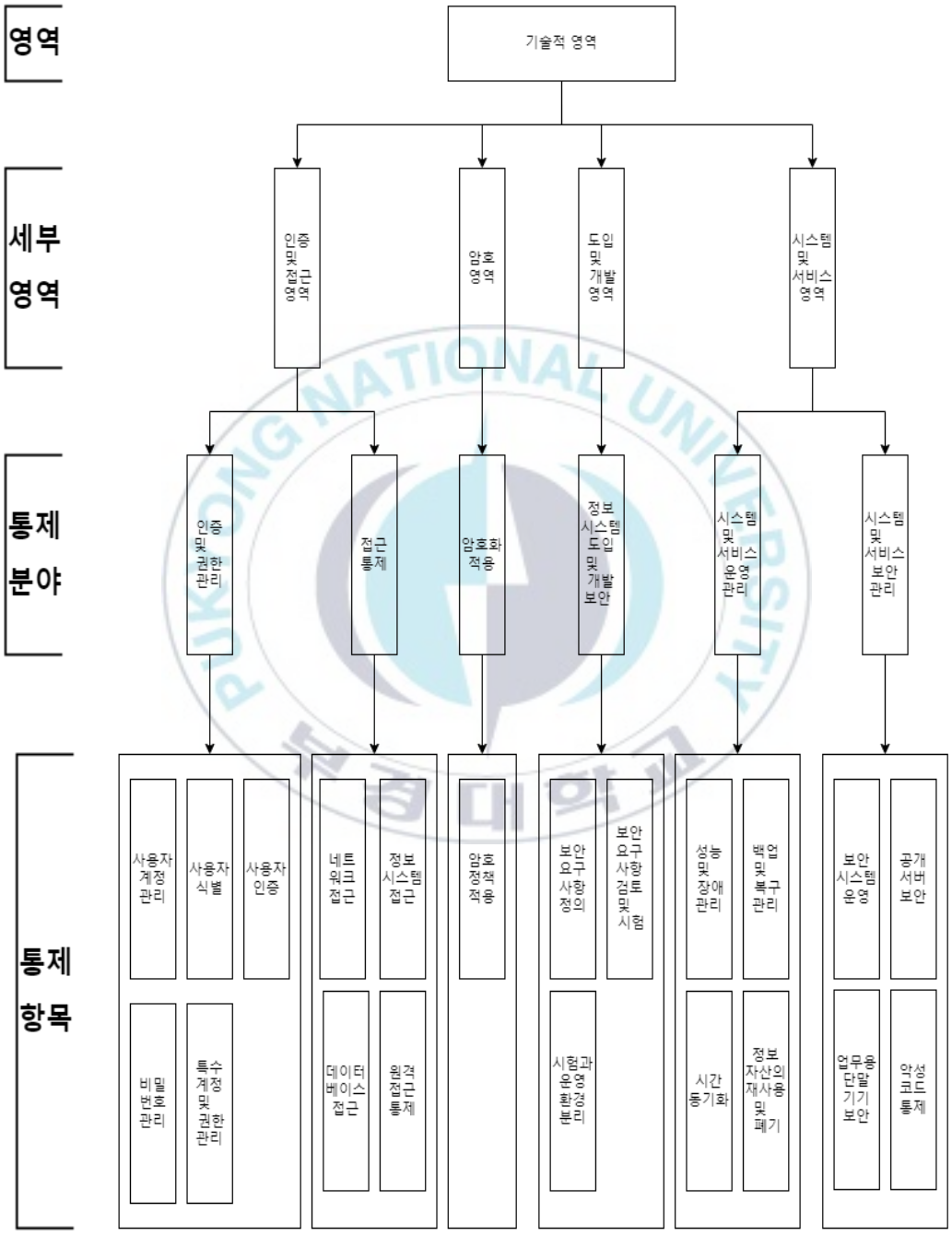
7. 최종 연구모형

위의 과정을 거쳐 도출된 3 계층 항목들을 반영하여 최종 연구모형을 만들었으며 실무자들의 편의를 위해 관리적 영역과 기술적 영역을 구분하였다. 먼저 최종 연구모형의 관리적 영역은 아래와 같다.



<그림 3-4> 최종 연구모형의 관리적 영역 계층 구조

다음으로 최종 연구모형의 기술적 영역은 아래와 같다.



〈그림 3-5〉 연구모형의 기술적 영역 계층 구조

8. 2 차 설문조사

가. 설문 대상

최종 연구모형의 측정지표에 대한 중요도와 중소기업에서의 수행 난이도 결정을 위해 정보보안 분야에 근무하는 전문가를 대상으로 설문조사를 실시하였다. 정보보안 업계 종사자의 출신은 기업 보안 담당자, 정보보안 기업의 임원(보안관제, 보안운영, Cert, 취약점 진단), 보안 컨선턴트 등이며 경력은 최소 3 년 이상의 인원들만 모집하였다. 지금도 전원 정보보호 분야에서 관련 업무를 수행중인 현직자들 25 명을 대상으로 설문조사를 진행하였다.

나. 설문지 구성

이번 설문지는 클라우드 보안인증 하를 기반으로 선행연구와 1 차 설문조사를 참고하여 수정하고 도출한 최종 연구모형에 대하여 2 계층의 경우 관리적 영역과 기술적 영역의 구분하여 중요도를 도출하기 위해 각 설문 문항은 쌍대비교의 6 점 척도를 사용하였다. 관리적 영역에서는 ISMS 의 기반이 되는 관리 체계 수립 및 운영을 제외한 6 개 분야를 15 문항으로 중요도를 구했으며 기술적 영역 역시 6 개 분야 15 문항으로 2 계층 중요도에 관한 문항은 총 30 문항으로 이루어져 있다.

3 계층이 아닌 2 계층에서 중요도를 구한 것은 3 계층 44 개 항목을 쌍대비교 설문조사를 하기에는 어렵다고 판단했으며 3 계층의 중요도를 판단하는 기준이 사람마다 너무 편차가 크며 2 계층의 경우 그 보다 좀더 일관성을 보이는 것을 선행연구와 1 차 설문조사로 알았기 때문이다.

3 계층의 경우 44 개 항목에 대한 중소기업에서 수행할 때의 난이도를 물었는데 비용, 인력·시간적 소모, 항목 자체의 난이도 등의 모든 요소를 포함한 난이도를 상, 중, 하로 등급을 설문조사 하였다.

정리하면 2 계층 중요도 문항 30 개, 3 계층 난이도 문항 44 개, 설문 대상 정리를 위한 문항 3 개로 2 차 설문조사를 총 77 개의 문항으로 구성되어 있다.

다. 2 계층 중요도 AHP 적용 절차

AHP 기법을 이용할 때 다음과 같은 과정을 거쳐서 중요도를 도출해낸다. 먼저 대상을 계층적으로 구조화하고 각 계층내의 대상들을 쌍대비교를 위해 비교행렬을 만든다.

다음으로 쌍대비교의 척도를 정해야 하는데 1 점은 고정적으로 동등의 의미를 가지며 정교하게 구분을 하는 경우에는 10 점 척도를 사용한다. 하지만 본 연구에서 중요도는 보조적인 의미를 가지기에 6 점 척도를 사용하기로 하였다. 항목 간의 쌍대비교 척도의 의미는 아래와 같다.

<표 3-21> 6 점 척도 각 점수의 의미

중요도 차이	점수
동등하다	1
조금	2
약간	3
상당히	4
많이	5
매우 많이	6

위에서 정한 점수를 쌍대비교를 위해 비교행렬에 입력해야 하며 같은 항목은 자동적으로 1 점을 한 항목에 점수 n 을 입력하면 대칭하는 항목에는 1/n 의 점수를 입력한다. 예를 들어 인적 보안과 외부자 보안을 쌍대비교를

할 시 인적 보안에 상대적으로 상당히 중요하다고 판단되어 3 점을 입력할 시 자동적으로 외부자 보안은 인적 보안에 비해 1/3 만큼 중요하다고 입력을 한 것과 마찬가지이다. 예를 들어 비교 행렬로 표시하면 아래와 같다.

〈표 3-22〉 각 평가 대상들간의 상대적 중요도 평가 (예)

–	정책, 조직, 자산관리	인적 보안	외부자 보안
정책, 조직, 자산관리	1	2(조금)	4(상당히)
인적 보안	1/2	1	1/3(약간)
외부자 보안	1/4	3	1

위의 표에서 음영이 없는 부분은 입력 값이며 음영이 있는 부분은 입력 값을 받아 자동으로 채워진 부분이다. 이를 모든 항목간 상대적 중요도 평가를 해야 하며 본 논문의 설문조사에서는 관리적 영역과 기술적 영역의 나눠서 하였으며 관리적 분야의 ISMS 의 기반이 되는 관리 체계 수립 및 운영을 제외하여 6 분야의 항목을 15 번 상대적 중요도 평가를 실시했으며 기술적 영역도 6 분야의 항목을 15 번 번 상대적 중요도 평가를 실시하여 2 계층 중요도 평가는 총 30 문항으로 이루어져 있다.

다음으로 각 항목의 가중치를 계산하기 위하여 먼저 행렬 곱을 계산하여야 하며 앞의 값이 들어간 비교행렬을 액셀의 함수를 이용하여 행렬 곱을 계산할 수 있다. 액셀의 함수는 MMULT 이며 행렬 곱의 계산 방법은 아래와 같다.

$$(AB)_{ij} = \sum_k A_{ik} B_{kj}$$

다음으로 실제 중요도라고 할 수 있는 가중치를 구해야 하는데 각 항목들을 행렬 곱의 합계에서 나누기 하면 된다. 예를 들어 행렬 곱의 합계를 100 이라 하고 인적 보안의 행렬 곱이 10 이라고 하면 인적보안의

가중치는 0.1 이며 인적보안이 모든 항목의 중요도중에 10%의 비중을 가지고 있다고 할 수 있다.

단순히 중요도만 구하려면 이 단계까지의 값만으로 가능하지만 도출된 값의 신뢰성을 검증하는 일관성 검사라는 게 존재하며 이 부분도 0.1~0.2 정도의 수치 이하의 값만 신뢰성이 있다고 판단하며 그 이상의 값은 신뢰성이 없다고 판단하여 폐기하는 편이다.

일관성 비율(Consistency Rate, C.R)을 구하기 위해서는 먼저 일관성 지수(Consistency Index, C.I)를 구해야 하며 일관성 지수를 구하기 위해서는 비교행렬과 가중치의 평균을 항목 수 −1 의 값으로 나눠야 한다. 일관성 지수를 구하는 수식은 아래와 같다.

$$\mathrm{CI} = \frac{(\lambda\mathrm{max} - \mathrm{n})}{\mathrm{n} - 1}$$

다음으로 도출된 CI 값을 RI(Random Consistency Index)값으로 나누면 일관성 비율이 도출되는데 본 연구에서 사용한 RI 값은 아래와 같다.

<표 3-23> 연구에서 사용한 RI 값

구 분	항목수 별 RI 값					
항목수	1	2	3	4	5	6
RI	0	0	0.52	0.89	1.25	1.35

본 연구에서는 관리적 영역 6 항목, 기술적 영역 6 항목이기에 RI 값은 1.35 가 된다. 이를 이용해서 일관성 비율을 구할 수 있으며 수식은 아래와 같다.

$$\mathrm{CR} = \frac{CI}{\mathrm{RI}(1.35)}$$

본 연구에서는 CR 값이 0.2 이상인 설문조사 값은 폐기하기로 하였으며 총 25 명의 응답에서 8 명이 이에 속한다. CR 값이 0.2 ALAKSDLS 17 명의 설문조사 값으로 중요도를 도출하였다.

라. 3 계층 중소기업 수행 난이도 적용 절차

3 계층의 경우 중소기업에서의 수행 난이도에 대해서 설문조사를 하였으며 이 때 수행난이도는 금전적 비용, 인력 및 시간적 소모 등 중소기업의 모든 애로사항을 포함한 난이도이다.

3 점 척도로 응답을 상, 중, 하로 받았는데 상은 3 점, 중은 2 점, 하는 1 점으로 변환하였으며 이를 합산해서 항목의 점수 합계가 29 점 이하는 하, 30~39 점은 중, 40 점 이상은 상으로 분류하였다. 이에 대한 자세한 사항은 아래의 표와 같다.

<표 3-24> 3 점 척도 각 등급과 점수의 의미

개별 등급	개별 점수	종합 등급	종합 점수
상	3	상	40 점 이상
중	2	중	30~39 점
하	1	하	29 점 이하

마. 최종 설문조사 대상

25 명의 설문조사 참여자 중에 8 명을 일관성 비율 부족으로 제외하였으며 나머지 17 명의 대한 정보는 아래와 같다.

<표 3-25> 최종 설문조사 대상

구분	세부구분	설문자 수	비율
직급	사원	3	17.6%
	대리	3	17.6%
	과장	5	29.4%
	차장 ~ 부장	6	35.3%
업무 경력	3 년 이상 ~ 5 년 이하	3	17.6%
	5 년 이상~ 7 년 이하	3	17.6%
	7 년 이상 ~ 10 년 이하	3	17.6%
	10 년 이상	8	47.1%
관련 지식	보안인증 심사자격 소지자 및 수행 경험이 있다.	2	12.5%
	기업서 ISMS 인증을 받았거나 ISMS 에 대한 컨설팅 경험	3	18.8%
	컨설팅이나 진단 업무 수행	2	12.5%
	보안담당자 및 전산담당자	9	56.3%

직급으로는 차장 이상급이 경력으로는 10 년이상 관련 지식으로는 기업의 보안 및 전산 담당자가 가장 많은 비중을 가지고 있다.

Ⅳ. 연구 결과

1. 2 차 설문조사 결과

2 계층 관리적 영역의 중요도에 대한 설문조사 결과는 정책, 조직, 자산 관리, 인적 보안, 사고 예방 및 대응 순으로 도출되었다.

<표 4-1> 2 계층 관리적 영역의 중요도 설문조사 결과

구분	정책, 조직, 자산 관리	인적 보안	외부자 보안	물리 보안	사고예방 및 대응	재해 복구
4 번	0.17	0.11	0.14	0.09	0.28	0.22
5 번	0.07	0.32	0.04	0.07	0.22	0.29
6 번	0.17	0.28	0.22	0.14	0.09	0.11
10 번	0.21	0.15	0.24	0.16	0.11	0.13
11 번	0.38	0.18	0.04	0.07	0.17	0.17
13 번	0.49	0.11	0.09	0.18	0.07	0.05
14 번	0.49	0.11	0.09	0.18	0.07	0.05
16 번	0.04	0.11	0.13	0.28	0.41	0.02
17 번	0.38	0.25	0.04	0.02	0.21	0.09
18 번	0.2	0.47	0.04	0.03	0.16	0.09
19 번	0.25	0.4	0.03	0.02	0.21	0.08
20 번	0.34	0.29	0.05	0.03	0.22	0.08
21 번	0.4	0.2	0.05	0.07	0.21	0.07
22 번	0.39	0.15	0.04	0.02	0.32	0.08
23 번	0.08	0.27	0.12	0.07	0.42	0.04
24 번	0.26	0.38	0.04	0.07	0.2	0.04
25 번	0.12	0.43	0.25	0.08	0.06	0.05
중요도	1	2	4	6	3	5

2 계층 관리적 영역의 중요도에 대한 설문조사 결과는 인증 및 권한관리, 접근통제, 시스템 및 서비스 보안관리 순으로 도출되었다.

<표 4-2> 2 계층 기술적 영역의 중요도 설문조사 결과

구분	인증 및 권한관리	접근통제	암호화 적용	정보시스템 도입 및 개발 보안	시스템 및 서비스 운영관리	시스템 및 서비스 보안관리
4 번	0.21	0.24	0.22	0.1	0.06	0.18
5 번	0.27	0.15	0.22	0.08	0.14	0.14
6 번	0.3	0.21	0.08	0.09	0.17	0.13
10 번	0.18	0.2	0.1	0.11	0.18	0.23
11 번	0.22	0.22	0.15	0.08	0.15	0.17
13 번	0.28	0.22	0.09	0.11	0.17	0.14
14 번	0.28	0.22	0.09	0.11	0.17	0.14
16 번	0.44	0.21	0.15	0.07	0.05	0.08
17 번	0.48	0.24	0.04	0.03	0.09	0.12
18 번	0.38	0.31	0.04	0.03	0.13	0.1
19 번	0.42	0.27	0.04	0.03	0.11	0.13
20 번	0.42	0.21	0.05	0.05	0.1	0.18
21 번	0.06	0.35	0.19	0.08	0.12	0.19
22 번	0.27	0.43	0.05	0.03	0.08	0.14
23 번	0.27	0.43	0.05	0.03	0.08	0.14
24 번	0.44	0.2	0.05	0.05	0.16	0.11
25 번	0.1	0.19	0.34	0.07	0.13	0.16
중요도	1	2	5	6	4	3

설문조사의 결과를 선행연구와 비교하면 아래와 같다.

〈표 4-3〉 본 연구와 선행연구의 중요도 비교 (관리적 영역)

통제분야	본 연구	통제분야	공우진 [23]	통제분야	김진 [21]
정책, 조직, 자산 관리	1	내부자 보안	1	침해사고 관리	1
인적 보안	2	정책, 조직, 자산 보안	2	인적보안	2
사고 예방 및 대응	3	정보보안 사고 대응	3	IT 재해복구	3
외부자 보안	4	정보보안 업무연속성	4	정보보호 교육	4
재해 복구	5	외부자 보안	5	물리적 보안	5
물리 보안	6	시설 보안	6	정보보호 정책	6
-				정보보호 조직	7
				정보자산 분류	8

인적 보안과 사고 예방 및 대응의 경우 대부분의 연구에서 중요도가 높았으며 물리적 보안의 경우 대부분의 연구에서 중요도가 낮게 도출되었다.

〈표 4-4〉 본 연구와 선행연구의 중요도 비교 (기술적 영역)

통제분야	본 연구	통제분야	김진 [21]	통제분야	조경재 [22]
인증 및 권한관리	1	접근통제	1	접근통제	1
접근통제	2	시스템 개발 보안	2	운영보안	2
시스템 및 서비스 보안관리	3	운영보안	3	암호통제	3
시스템 및 서비스 운영관리	4	암호통제	4	시스템 개발 보안	4
암호화 적용	5	-			
정보시스템 도입 및 개발 보안	6				

접근통제의 경우 대부분의 연구에서 중요도가 높았으며 나머지 항목은 연구마다 틀리지만 암호통제보다는 운영보안의 중요도가 높은 경향이 있다.

다음으로 3 계층의 중소기업 수행 난이도에 대한 결과로 먼저 관리적 영역의 3 계층 항목에서 가장 난이도가 높은 항목은 재해·재난 대비 안전조치, 사고 예방 및 대응체계 구축, 조직 구성 순이었으며 가장 난이도가 낮은 항목은 보안서약, 보호구역 지정, 외부자 계약 변경 및 만료 시 보안 순으로 도출되었다.

<표 4-5> 3 계층 관리적 영역의 중요도 설문조사 결과

통제 항목	상	중	하	점수	등급	순위
경영진의 참여	2	10	5	31	중	13
최고책임자의 지정	2	10	5	31	중	13
조직 구성	10	5	2	42	상	3
정책 수립	5	11	1	38	중	6
정보자산 식별	5	7	5	34	중	9
법적 요구사항 준수 검토	8	6	3	39	중	5
정책의 유지관리	7	6	4	37	중	7
조직의 유지관리	5	9	3	36	중	8
정보자산 관리	2	10	5	31	중	13
주요 직무자 지정 및 관리	3	8	6	31	중	13
보안 서약	2	3	12	24	하	22
인식제고 및 교육훈련	5	7	5	34	중	9
퇴직 및 직무변경 관리	3	6	8	29	하	19
보안 위반 시 조치	2	7	8	28	하	20
외부자 현황 관리	3	11	3	34	중	9
외부자 계약 변경 및 만료 시 보안	2	6	9	27	하	21
보호구역 지정	0	7	10	24	하	22
출입통제	2	10	5	31	중	13
정보시스템 보호	4	5	8	30	중	18
업무환경 보안	5	5	7	32	중	12
사고 예방 및 대응체계 구축	13	3	1	46	상	2
취약점 점검 및 조치	7	9	1	40	상	4
재해·재난 대비 안전조치	16	0	1	49	상	1

기술적 영역의 3계층 항목에서 가장 난이도가 높은 항목은 원격접근 통제, 백업 및 복구관리, 공개서버 보안 순이었으며 가장 난이도가 낮은 항목은 시간 동기화, 비밀번호 관리, 특수 계정 및 권한관리 순으로 도출되었다.

〈표 4-6〉 3계층 기술적 영역의 중요도 설문조사 결과

통제 항목	상	중	하	점수	등급	순위
사용자 계정 관리	5	11	1	38	중	12
사용자 식별	3	13	1	36	중	15
사용자 인증	8	4	5	37	중	14
비밀번호 관리	1	2	14	21	하	20
특수 계정 및 권한관리	1	5	11	24	하	19
네트워크 접근	12	3	2	44	상	4
정보시스템 접근	4	10	3	35	중	17
데이터베이스 접근	7	8	2	39	중	8
원격접근 통제	12	4	1	45	상	1
암호정책 적용	6	10	1	39	중	8
보안 요구사항 정의	7	8	2	39	중	8
보안 요구사항 검토 및 시험	6	9	2	38	중	12
시험과 운영 환경 분리	10	5	2	42	상	5
성능 및 장애관리	8	7	2	40	상	6
백업 및 복구관리	12	4	1	45	상	1
시간 동기화	1	1	15	20	하	21
정보자산의 재사용 및 폐기	0	9	8	26	하	18
보안시스템 운영	7	8	2	39	중	8
공개서버 보안	11	6	0	45	상	1
업무용 단말기기 보안	8	7	2	40	상	6
악성코드 통제	7	5	5	36	중	15

2. 중소기업에서 활용가능한 정보보호 관리체계 제안

클라우드 보안 인증 하 등급과 ISMS 를 매핑한 후 항목을 조정하였으며 항목들의 중요도와 난이도에 대해서 2 차 설문조사를 하여 그 결과를 반영하여 도출된 관리적 영역의 연구 결과는 아래와 같다.

<표 4-7> 관리적 영역의 연구 결과

중소기업에서 활용가능한 수준의 정보보호 관리체계 관리적 영역 제안 (7 분야 23 개 항목)					
	세부 영역	2 계층	중요도	3 계층	난이도
관리적 영역	조직적 영역	관리 체계 수립 및 운영	필수	경영진의 참여	중
				최고책임자의 지정	중
				조직 구성	상
				정책 수립	중
				정보자산 식별	중
				법적 요구사항 준수 검토	중
		정책, 조직, 자산 관리	1	정책의 유지관리	중
				조직의 유지관리	중
				정보자산 관리	중
		사고 예방 및 대응	3	사고 예방 및 대응체계 구축	상
				취약점 점검 및 조치	상
		재해 복구	5	재해 · 재난 대비 안전조치	상
	인적 영역	인적 보안	2	주요 직무자 지정 및 관리	중
				보안 서약	하
				인식제고 및 교육훈련	중
				퇴직 및 직무변경 관리	하
				보안 위반 시 조치	하
		외부자 보안	4	외부자 현황 관리	중
				외부자 계약 변경 및 만료 시 보안	하
	물리적 영역	물리 보안	6	보호구역 지정	하
				출입통제	중
				정보시스템 보호	중
				업무환경 보안	중

관리적 영역의 중요도에서 관리체계 수립 및 운영부분은 필수적인 부분으로 제외하였으며 그 외에는 정책·조직·자산 관리, 인적 보안, 사고예방 및 대응, 외부자 보안, 재해 복구, 물리 보안순으로 중요도가 도출되었으며 난이도는 상 4 항목, 중 14 항목, 하 5 항목으로 사고예방 및 대응과 재해복구의 항목이 난이도가 높았으며 지속적인 관리가 아닌 1 회성 혹은 관리 빈도가 적은 항목들이 주로 난이도가 낮게 도출되었다.

다음으로 기술적 영역의 연구 결과는 아래와 같다.

<표 4-8> 기술적 영역의 연구 결과

중소기업에서 활용가능한 수준의 정보보호 관리체계 기술적 영역 제안 (6 분야 21 개 항목)					
	세부 영역	2 계층	중요도	3 계층	난이도
기술적 영역	인증 및 접근 영역	인증 및 권한관리	1	사용자 계정 관리	중
				사용자 식별	중
				사용자 인증	중
				비밀번호 관리	하
				특수 계정 및 권한관리	하
		접근통제	2	네트워크 접근	상
				정보시스템 접근	중
				데이터베이스 접근	중
				원격접근 통제	상
	암호 영역	암호화 적용	5	암호정책 적용	중
	도입 및 개발 영역	정보시스템 도입 및 개발 보안	6	보안 요구사항 정의	중
				보안 요구사항 검토 및 시험	중
				시험과 운영 환경 분리	상

	시스템 및 서비스 영역	시스템 및 서비스 운영관리	4	성능 및 장애관리	상
				백업 및 복구관리	상
				시간 동기화	하
				정보자산의 재사용 및 폐기	하
		시스템 및 서비스 보안관리	3	보안시스템 운영	중
				공개서버 보안	상
				업무용 단말기기 보안	상
				악성코드 통제	중

기술적 영역의 중요도는 인증 및 권한관리, 접근통제, 시스템 및 서비스 보안관리, 시스템 및 서비스 운영관리, 암호화 적용, 정보시스템 도입 및 개발 보안순으로 도출되었으며 난이도는 상 7 항목, 중 10 항목, 하 4 항목으로 관리적 영역보다 전체 항목의 수가 적지만 난이도가 상인 항목이 3 개가 더 많았으며 비용이 많이 들며 기술적인 요구치가 높은 항목들이 난이도가 높게 도출된 것으로 판단된다.

Ⅴ. 결론

사이버 공격은 매년 증가하고 있으며 대부분의 피해가 중소기업에서 발생하고 있다. 중소기업 역시 정보보호의 중요성을 인식하고 있지만 예산 및 인력 부족으로 정보보호에 대한 투자 및 관리를 못하는 실정이다.

본 연구는 이러한 상황에 도움을 주기위해 클라우드 보안인증 하 등급과 ISMS 를 기반하여 단순히 중요도 중점이 아닌 중소기업의 애로사항인 예산과 인력부족을 반영한 중소기업에서 활용가능한 수준의 정보보호 관리체계에 대해 연구하고자 하였다.

먼저 이를 위한 기준을 정하였고 그 다음 클라우드 보안인증 하 등급과 ISMS 를 비교분석으로 34 개의 항목을 도출한 뒤 설문조사 및 선행연구를 바탕으로 7 개의 항목을 삭제하였으며 75 개의 항목을 추가하여 44 개의 항목을 도출하였다. 그리고 44 개의 항목을 관리적 영역과 기술적 영역으로 구분한 후 2 차 설문조사를 통하여 2 계층의 통제분야의 중요도와 3 계층 통제항목의 중소기업 수행 난이도를 도출하였다.

본 연구는 중요도 및 수행 난이도를 고려하여 중소기업에서 활용할 수 있는 수준의 정보보호 관리체계를 제안하였다는 점에서 학문적 기여도가 있다고 생각하며 이를 이용하여 중소기업의 정보보호 발전에 도움이 되기를 기대한다.

하지만 ISMS 를 평가하고 개선하기에는 본인의 전문성이 떨어진다고 생각하며 이를 위해서 제대로 항목들을 도출하고 평가하기 위해서는 ISMS 를 실제 심사하는 위원들과 ISMS 를 구축을 해본 실무자들의 대상으로 한 심도 있는 설문조사는 필수라고 판단된다. 그 후에 실제로

중소기업에 적용하여 실제 효율적으로 효과가 있는지, 보완사항의 유무 등 많은 평가를 해보고 다시 수정하는 작업들이 이루어져야 하며 그리고 무엇보다 중소기업에서 정보보호 관리체계에 투자를 할 수 있는 환경을 조성해야 할 것이다.

참고문헌

[1] IBM 세큐리티(2022), “2022년 데이터 유출 비용 보고서”

[2] 한국인터넷진흥원(2022), “2021년 정보보호 실태조사”

[3] 최동권, 윤현식. "기업의 정보보호관리가 영업성과와 기업가치에 미치는 영향: 정보보호관리체계(ISMS)를 중심으로." 한국디지털콘텐츠학회논문지 20.8 (2019): 1567-1576.

[4]김동현, 이윤호. "보안 7대 위협을 이용한 ISMS-P 인증효과에 관한 연구: 기업 규모와 경력 중심으로." 한국정보기술학회논문지 18.4 (2020): 109-119.

[5] 한국인터넷진흥원 (2010). “ISMS인증제도소개_브로슈어(4P)”

[6] 장상수, 김상춘. "정보보호 관리체계(ISMS)가 기업성과에 미치는 영향에 관한 실증적 연구." 융합보안 논문지 15.3_2 (2015): 107-114.

[7] '해커 먹잇감'된 중소기업들, 매년 수백번 털리지만..."돈도 사람도 없다"

(머니투데이), news.mt.co.kr/mtview.php?no=2022101108440814796

[8] 중소벤처기업부(2022). “알기 쉽게 풀어 쓴 중소기업 범위해설”

[9] 중소벤처기업부(2022). “2022 중소기업 기술보호 수준 실태조사 보고서”

[10] 한국정보보호산업협회(2022) “2021 정보보호 실태조사 “

[11] 한국인터넷진흥원 (2021). “ISMS-P_인증제도_안내서(2021.7)”

[12] 한국인터넷진흥원 (2022). “ISMS-P 인증기준 안내서(2022.4.22)”

[13] 행안부,과기정통부,방통위(2018). “180910 참고 (개인정보보호협력과) ISMS-PIMS 통합 추진”

[14] 한국인터넷진흥원 (2023). “클라우드서비스_보안인증제도_안내서

[15]ISO (2021).” ISO-CASCO_0. Explanatory note and overview on ISO Survey 2021 results” www.iso.org/the-iso-survey.html

[16] ISO (2022). ISO 27001: 2022

[17] advisera.com (2022). “Overview of new security controls in ISO 27002:2022”

[18] Andrey Prozorro (2022). “The ISO 27000 Family of Standards”,

[19] ISO, ISO 27000 Family of Standards

www.iso.org/standard/27001~27041

[20] 한국인터넷진흥원 (2023). “클라우드서비스(IaaS)_보안인증기준_해설서

[21] 김진. "정보보호 항목의 중요도 및 정보보호투자와의 우선순위 차이에 관한 연구." 국내석사학위논문 연세대학교 정보대학원, 2014. 서울

[22] 조경재. "콜센터 정보보호관리체계(ISMS) 인증항목의 우선순위 선정에 관한 연구." 국내석사학위논문 서울과학기술대학교, 2018. 서울

[23] 공우진. "정보보안 효과성 측정 모델에 관한 연구." 국내박사학위논문 호서대학교 기술경영전문대학원, 2022. 충청남도

[24] 김이헌. "중소기업의 특성을 고려한 정보보호 관리체계 평가 모델 개선." 국내석사학위논문 충북대학교, 2021. 충청북도

[25] 박재성. "중소기업을 위한 정보보호관리체계 연구." 국내석사학위논문 고려대학교 컴퓨터정보통신대학원, 2022. 서울

[26] 국가정보원 (2023). “국가 클라우드 컴퓨팅 보안 가이드라인”

[27] 정보공유분석센터(ISAC), “정보보호_준비도_평가_기준 및 방법”

[28] 한국인터넷진흥원 (2023). 클라우드서비스(하등급)_보안인증기준_해설서

[29] 박정민(2014), 델파이기법/ AHP기법(2014.12.14.),
https://blog.naver.com/parkstwo/220209356245

[부록 1] 1차 설문조사

중소기업을 위한 정보보호 관리체계에 대한 설문

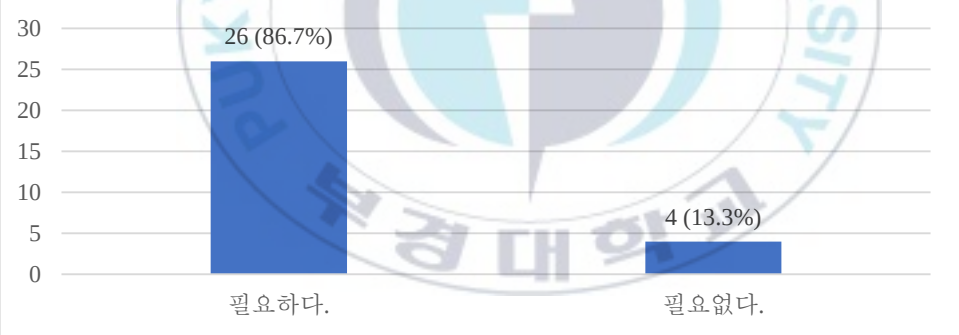
안녕하십니까? 바쁘신 와중에도 불구하고 귀중한 시간을 내어 본 설문에 참여해 주셔서 진심으로 감사드립니다.

클라우드 보안인증 하 등급과 ISMS에 기반하여 중소기업을 위한 정보보호 관리체계 도출 연구에 대한 설문입니다.

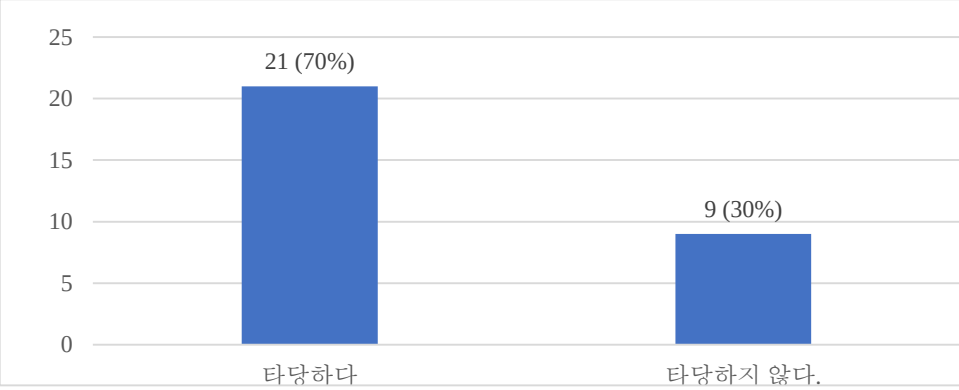
설문에 대한 응답내용은 연구목적으로만 사용될 것이며, 연구 이 외의 다른 목적으로는 절대 사용하지 않을 것을 약속드립니다.

부경대학교 정보보호학과
지도교수: 이현
연구자: 백낙천
E-Mail: qorskrcjs@naver.com

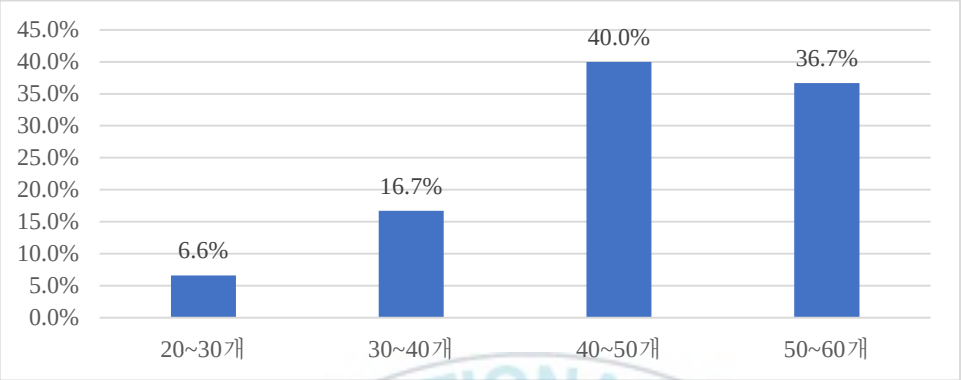
1. ISMS의 등급화는 필요한가?



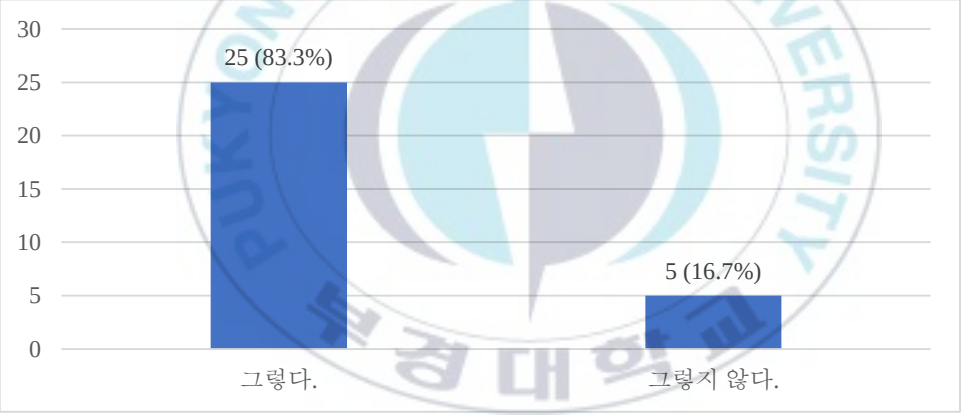
2. 중소기업을 위해서 임의의 ISMS 하 등급을 만든다면 조정 비율을 다른 인증이나 가이드의 비율을 참고하는 것은 타당한가?



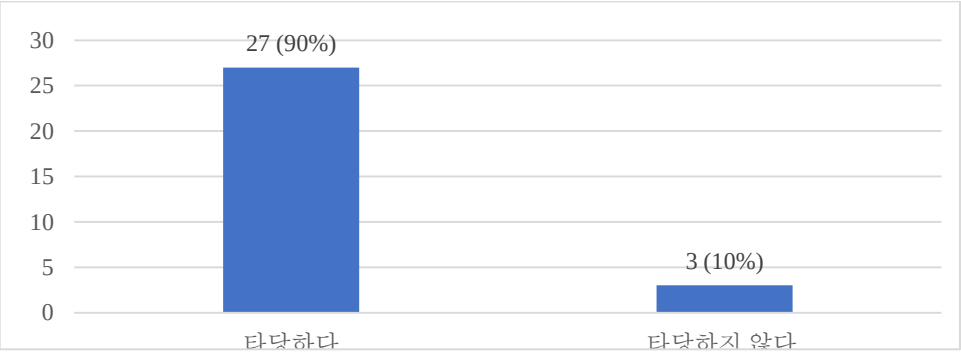
3. 중소기업을 위해서 임의의 ISMS 하 등급을 만들경우 통제항목의 적당한 수는? (기존 80개)



4. ISMS 하 등급을 만드는 과정에서 각 항목의 중요도 외에도 중소기업의 애로사항인 비용 및 인력같은 점도 고려하여 조정을 해야 하는가?

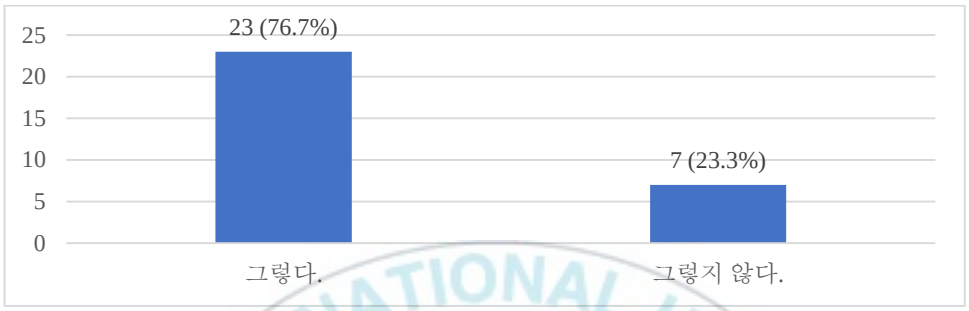


5. 클라우드 보안인증이 23년 3월 등급제로 변경하면서 클라우드 보안인증 하 등급이 생겼다. 이때 삭제된 항목을 분석하여 어떤 의도(중요도, 우선도)로 조정을 했는지 유추하는 방식은 타당한가?



6. 클라우드 보안인증의 1 계층 13 개의 항목을 하 등급으로 조정하는 과정에서 삭제한 항목의 수로 중요도를 유추한 것이다. 방식의 타당성에 관계없이 결과로만 보면 도출된 중요도가 맞다고 생각하는가?

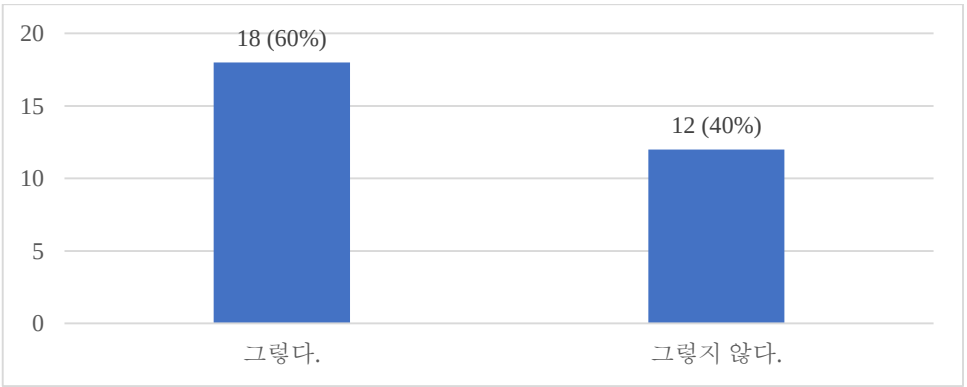
<표 3-8> 클라우드 보안 인증 1 계층(통제 목적) 중요도 분석



7. 클라우드 보안인증의 2계층 32개의 항목을 하 등급으로 조정하는 과정에서 삭제한 항목의 수로 중요도를 유추한 것이다. 방식의 타당성에 관계없이 결과로만 보면 도출된 중요도가 맞다고 생각하는가?

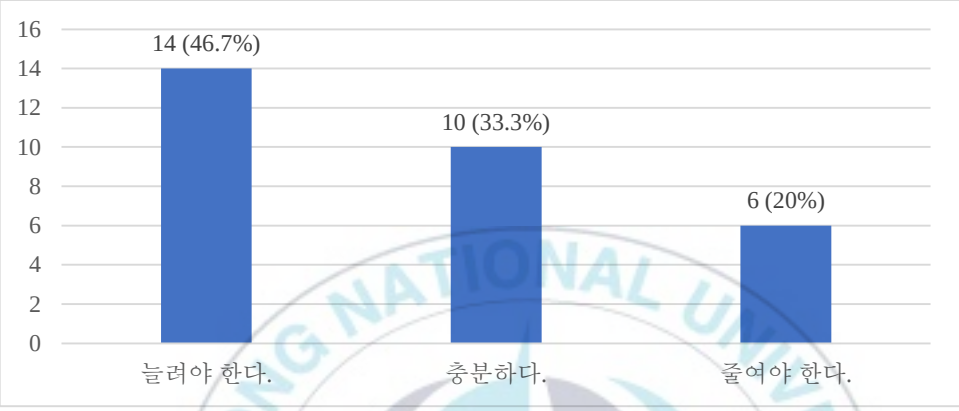
<표 3-9> 클라우드 보안 인증 2 계층(통제 방향) 중요도 분석

8. 통제 분야의 모든 항목이 사라진 경우도 있다. (외부인력 보안, 정보처리 시설 및 장비 보호) 중요성이나 우선도를 고려해서 있을 수 있는 일인가?

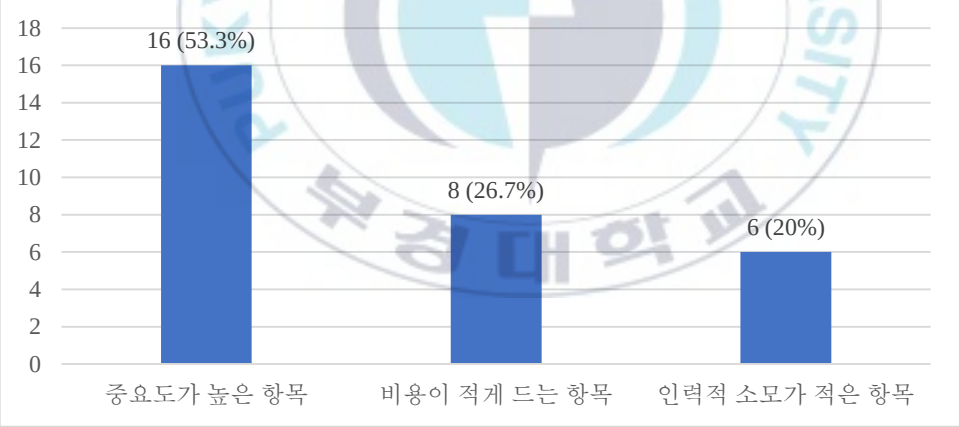


9. 클라우드 보안인증 하의 항목을 ISMS 항목과 매핑하여 도출한 결과이다. 이것이 ISMS 하 등급이라면 이에 대해서 양적으로 어떻게 생각하나? (기존 80 개)

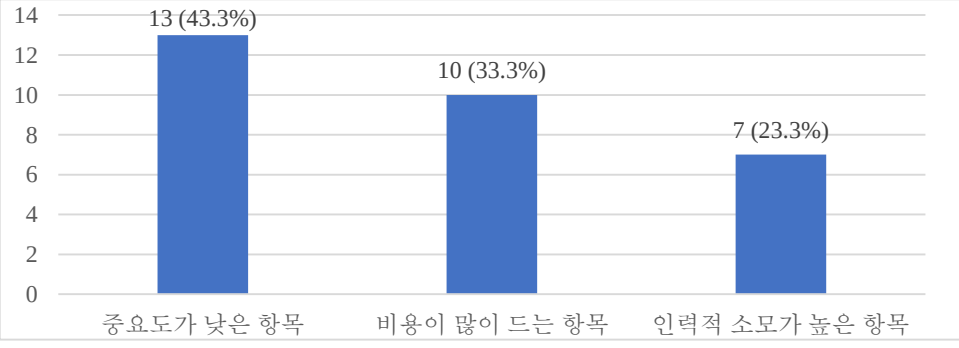
<표 3-12> 클라우드 보안인증 하 통제항목과 ISMS 매핑 결과



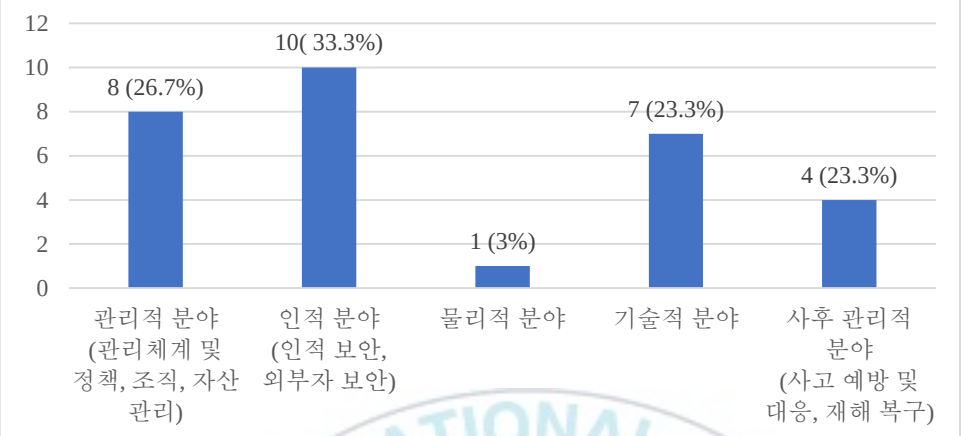
10. 위의 ISMS 34항목에서 추가를 한다면 어떤 기준으로 추가가 필요하겠는가?



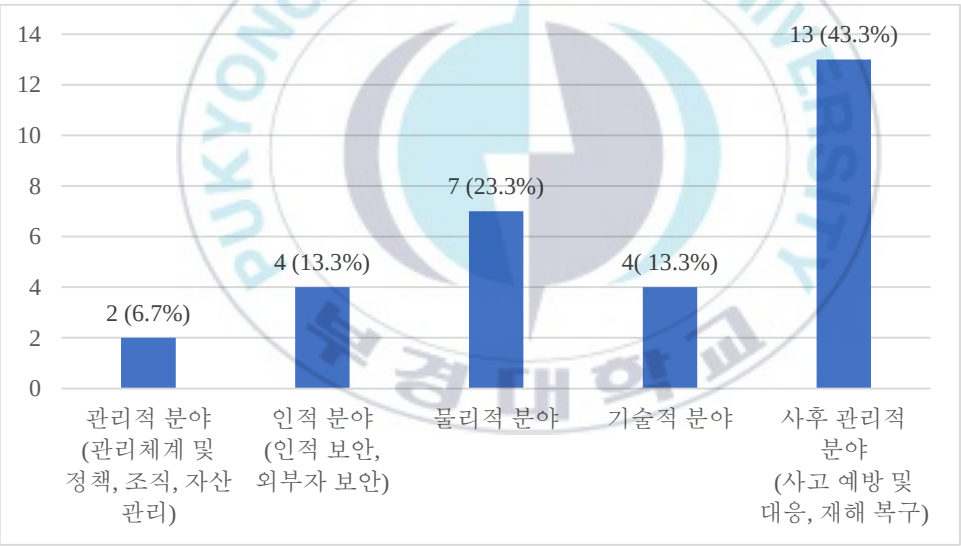
11. 위의 ISMS 34항목에서 삭제를 한다면 어떤 기준으로 삭제가 필요하겠는가?



12. 위의 내용에서 추가를 한다면 어느 분야의 항목을 추천하는가?



13. 위의 내용에서 삭제를 한다면 어느 분야의 항목을 추천하는가?



[부록 2] 2차 설문조사

중소기업을 위한 정보보호 관리체계 2계층 중요도, 3계층 난이도에 대한 설문

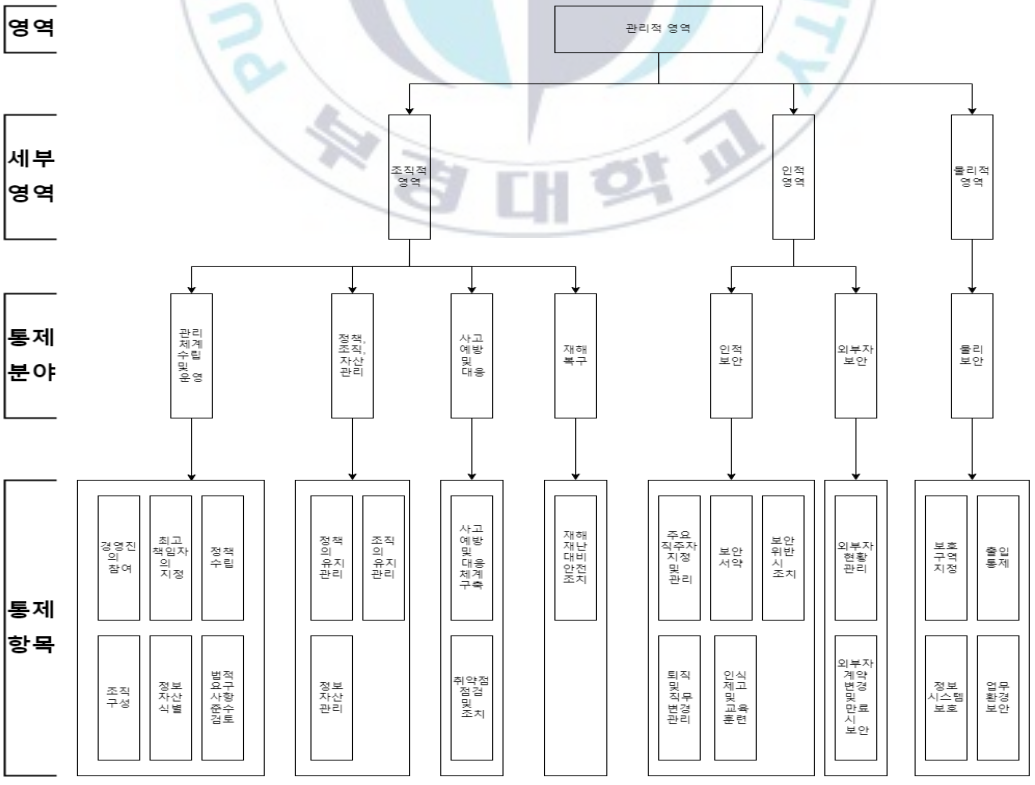
안녕하십니까? 바쁘신 와중에도 불구하고 귀중한 시간을 내어 본 설문에 참여해 주셔서 진심으로 감사드립니다.

클라우드 보안인증 하 등급과 ISMS에 기반하여 중소기업을 위한 정보보호 관리체계 도출 연구에 대한 설문입니다.

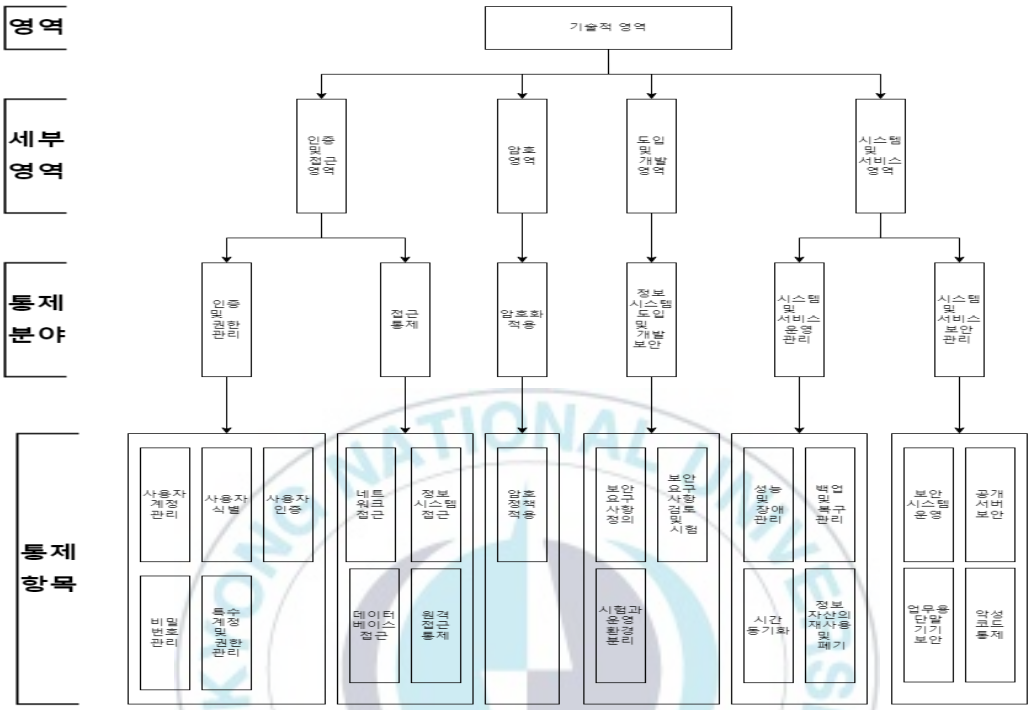
설문에 대한 응답내용은 연구목적으로만 사용될 것이며, 연구 이 외의 다른 목적으로는 절대 사용하지 않을 것을 약속드립니다.

부경대학교 정보보호학과
지도교수: 이현
연구자: 백낙천
E-Mail: qorskrcjs@naver.com

관리적 영역의 연구모형



기술적 영역의 연구모형



1. 설문자 인적 사항 (해당란에 O 표시를 기입해 주십시오.)

구분		해당
직급	사원	
	대리	
	과장	
	차장 ~ 부장	
	임원	
업무 경력	1 년 이상 ~ 3 년 이하	
	3 년 이상 ~ 5 년 이하	
	5 년 이상~ 7 년 이하	
	7 년 이상 ~ 10 년 이하	
	10 년 이상	
관련 지식	보안인증 심사자격 소지자 및 수행 경험이 있다.	

	기업서 ISMS 인증을 받았거나 ISMS 에 대한 컨설팅 경험	
	컨설팅이나 진단 업무 수행	
	보안담당자 및 전산담당자	

2. 설문응답 방법

1) 2계층 통제 분야에 대한 상대적 중요도 측정
- 설문 형식: 가중치 선정을 위한 AHP 설문
- 계층 내의 평가항목 간 상대적 중요도를 6점 척도로 평가
- 작성 예시

평가항	상대적 중요도 쌍대비교										평가항목
	매우많이	상당히	상당히	약간	조금	동등	조금	약간	상당히	상당히	매우많이	
A 항목								O				B 항목
A 항목									O			C 항목
A 항목						O						D 항목
B 항목					O							C 항목
B 항목			O									D 항목
C 항목		O										D 항목

2) 3계층 통제 항목에 대한 중소기업 수행 난이도 측정(중소기업의 모든 애로사항을 고려하여)
- 설문 형식: 난이도 등급 선정을 위한 설문
- 계층 내의 평가항목 간 상대적 중요도를 3점(상, 중, 하) 척도로 평가

– 작성 예시

평가항목	3계층 중소기업 수행 난이도		
	상	중	하
1번 항목			O
2번 항목		O	
3번 항목	O		
4번 항목		O	
5번 항목			O
6번 항목		O	
7번 항목		O	
8번 항목		O	
9번 항목			O
10번 항목	O		

3. 2계층 관리적 영역의 상대적 중요도

평가항목	정책,조직, 자산 관리	정책,조직, 자산 관리	정책,조직, 자산 관리	정책,조직, 자산 관리	정책,조직, 자산 관리
매우많이					
많이					
상당히					
약간					
조금					
동등					
조금					
약간					
상당히					
많이					
매우많이					
평가항목	인적 보안	외부자 보안	물리 보안	사고 예방 및 대응	재해 복구

평가항목	인적 보안	인적 보안	인적 보안	인적 보안	외부자 보안
매우많이					
많이					
상당히					
약간					
조금					
동등					
조금					
약간					
상당히					
많이					
매우많이					
평가항목	외부자 보안	물리 보안	사고 예방 및 대응	재해 복구	물리 보안

평가항목	외부자 보안	외부자 보안	물리 보안	물리 보안	사고 예방 및 대응
매우많이					
많이					
상당히					
약간					
조금					
동등					
조금					
약간					
상당히					
많이					
매우많이					
평가항목	사고 예방 및 대응	재해 복구	사고 예방 및 대응	재해 복구	재해 복구

4. 2계층 기술적 영역의 상대적 중요도

평가항목	인증 및 권한관리	인증 및 권한관리	인증 및 권한관리	인증 및 권한관리	인증 및 권한관리
매우많이					
많이					
상당히					
약간					
조금					
동등					
조금					
약간					
상당히					
많이					
매우많이					
평가항목	접근통제	암호화 적용	정보시스템 도입 및 개발 보안	시스템 및 서비스 운영관리	시스템 및 서비스 보안관리

평가항목	접근통제	접근통제	접근통제	접근통제	암호화 적용
매우많이					
많이					
상당히					
약간					
조금					
동등					
조금					
약간					
상당히					
많이					
매우많이					
평가항목	암호화 적용	정보시스템 도입 및 개발 보안	시스템 및 서비스 운영관리	시스템 및 서비스 보안관리	정보시스템 도입 및 개발 보안

평가항목	암호화 적용	암호화 적용	정보시스템 도입 및 개발 보안	정보시스템 도입 및 개발 보안	시스템 및 서비스 운영관리
매우많이					
많이					
상당히					
약간					
조금					
동등					
조금					
약간					
상당히					
많이					
매우많이					
평가항목	시스템 및 서비스 운영관리	시스템 및 서비스 보안관리	시스템 및 서비스 운영관리	시스템 및 서비스 보안관리	시스템 및 서비스 보안관리

5. 3계층 관리적 영역 중소기업 수행 난이도

평가항목	상	중	하
경영진의 참여			
최고책임자의 지정			
조직 구성			
정책 수립			
정보자산 식별			
법적 요구사항 준수 검토			
정책의 유지관리			
조직의 유지관리			
정보자산 관리			
사고 예방 및 대응체계 구축			
취약점 점검 및 조치			
재해 · 재난 대비 안전조치			
주요 직무자 지정 및 관리			
보안 서약			

인식제고 및 교육훈련			
퇴직 및 직무변경 관리			
보안 위반 시 조치			
외부자 현황 관리			
외부자 계약 변경 및 만료 시 보안			
보호구역 지정			
출입통제			
정보시스템 보호			
업무환경 보안			

6. 3계층 기술적 영역 중소기업 수행 난이도

평가항목	상	중	하
사용자 계정 관리			
사용자 식별			
사용자 인증			
비밀번호 관리			
특수 계정 및 권한관리			
네트워크 접근			
정보시스템 접근			
데이터베이스 접근			
원격접근 통제			
암호정책 적용			
보안 요구사항 정의			
보안 요구사항 검토 및 시험			
시험과 운영 환경 분리			
성능 및 장애관리			
백업 및 복구관리			
시간 동기화			
정보자산의 재사용 및 폐기			
보안시스템 운영			
공개서버 보안			
업무용 단말기기 보안			
악성코드 통제			