승인번호
제 342005 호

2025
정보보호 실태조사

SURVEY ON INFORMATION SECURITY

과학기술정보통신부
Ministry of Science and ICT

×

kisia 한국정보보호산업협회
Korea Information Security Industry Association

2025 정보보호 실태조사

주관기관 과학기술정보통신부

주소 세종특별자치시 갈매로 477, 정부세종청사 4동 3층~6층
홈페이지 www.msit.go.kr

전담기관 한국정보보호산업협회

주소 서울시 송파구 135 IT벤처타워 서관 14층
홈페이지 www.kisia.or.kr
담당부서 02-6748-2000

조사기관 (주)글로벌리서치

주소 서울시 서초구 반포대로 9, 3층~6층
홈페이지 www.globalri.co.kr
대표전화 02-3456-1700
발행일 2026. 02.

일 러 두 기

1 본 보고서의 내용을 인용할 때에는 반드시 과학기술정보통신부와 한국정보보호산업협회의 자료임을 밝혀야 함

2 통계표 및 도표 내의 숫자는 반올림되었으므로 세부 항목의 합이 전체 합계와 일치하지 않을 수 있음

3 복수 응답은 한 개 이상을 응답한 결과치를 집계한 결과임

4 통계표 및 도표에 사용된 기호의 뜻은 다음과 같음

- : 조사는 되었으나, 정보가 없는 경우
0.0 : 조사결과 값이 0이거나 0의 근삿값인 경우

5 일부 업종/규모별(기업부문), 성/연령별(개인부문) 통계량의 경우 표본의 크기가 충분치 않아 상대표준오차(변동계수)가 클 수 있으므로 이용 시 주의 바람(본 보고서의 부록2 – 표본오차 참고)

6 모집단 통계는 모수의 객관성을 확보하기 위해 아래와 같이 통계청 자료를 이용하였음

- 통계청 2024년 4분기 기준 기업통계등록부
- 통계청 2024년 정보화통계조사
- 통계청 2023년 등록센서스 조사구 자료
- 통계청 2024년 장래인구추계

2025

정보보호 실태조사_기업부문

01 정보보호 중요성 인식

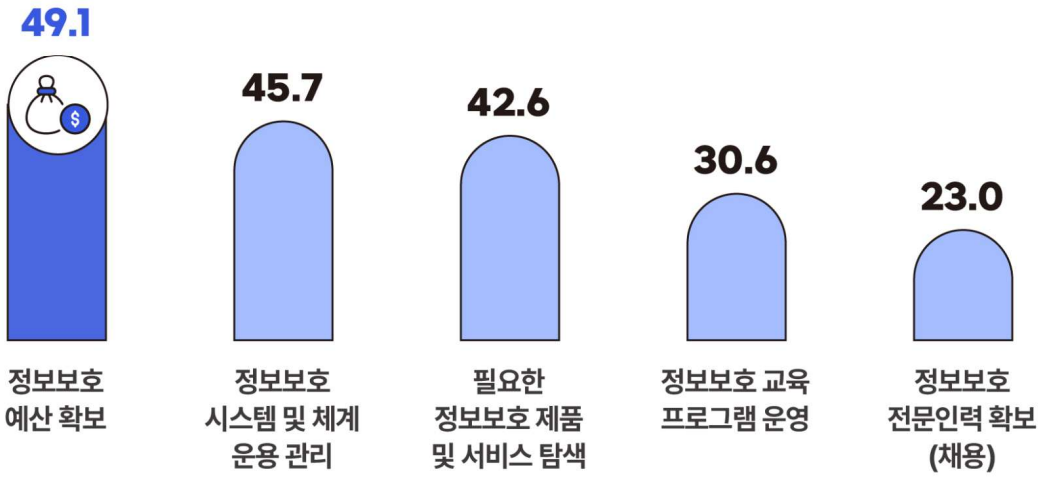
● 기업 및 경영진 정보보호 중요성 인식

● 기업 ● 경영진

Base : 전체 | 단위 : %

● 정보보호 애로사항 Top 5

Base : 전체 | 단위 : %, 복수응답

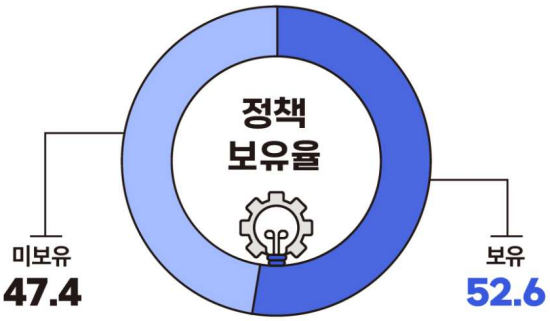


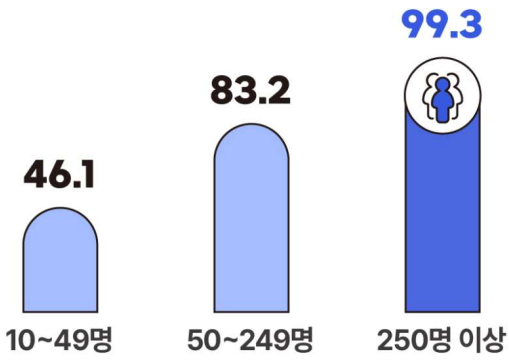
기업부문

02 정보보호 환경

● 정보보호 정책 보유율

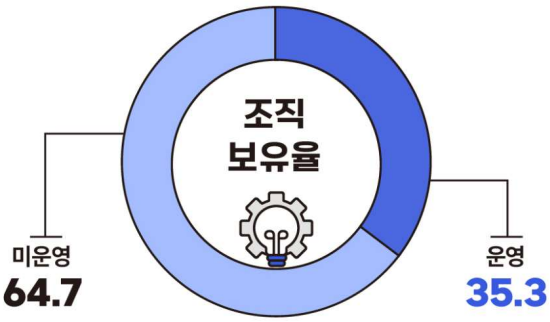
Base : 전체 | 단위 : %

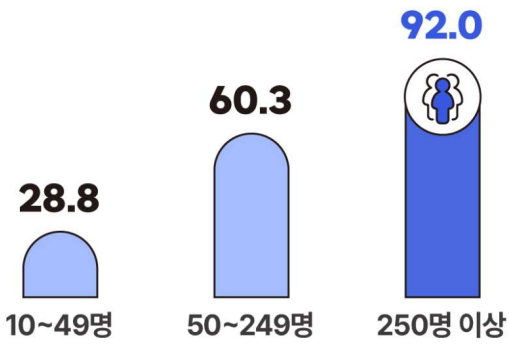




● 정보보호 조직 보유율

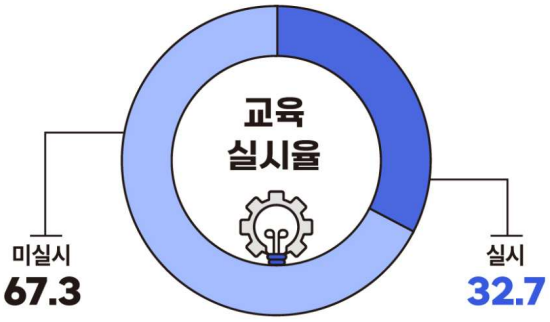
Base : 전체 | 단위 : %

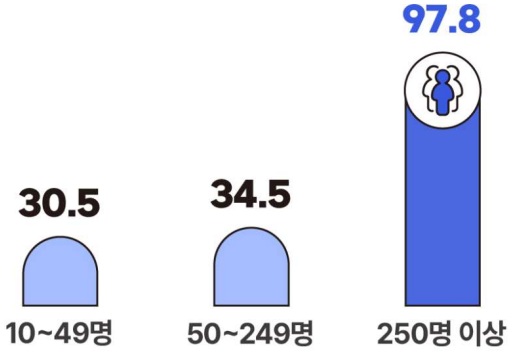




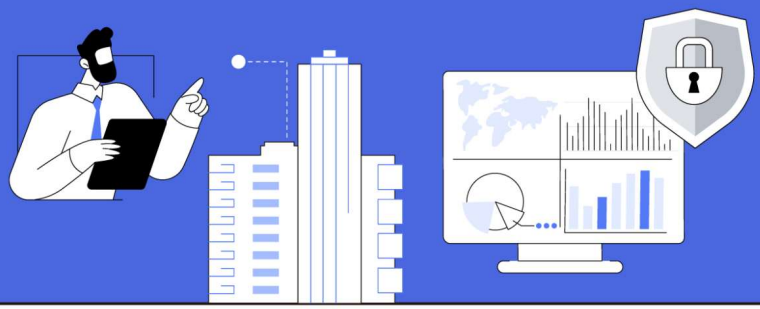
● 정보보호 교육 실시율

Base : 전체 | 단위 : %





기업부문



03 정보보호 인력

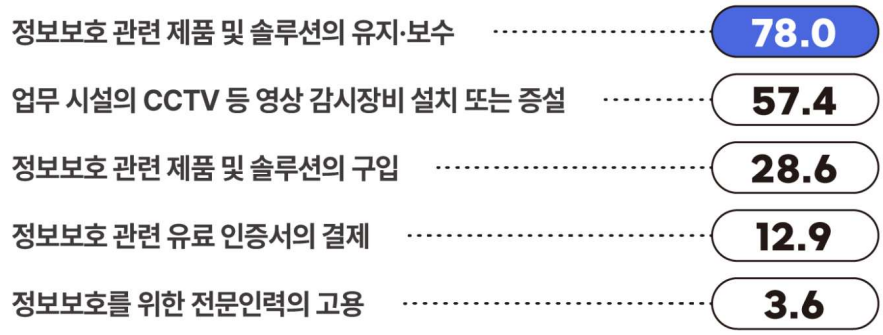
● 정보보호 인력 수

Base : 전체 | 단위 : 명

04 정보보호 예산

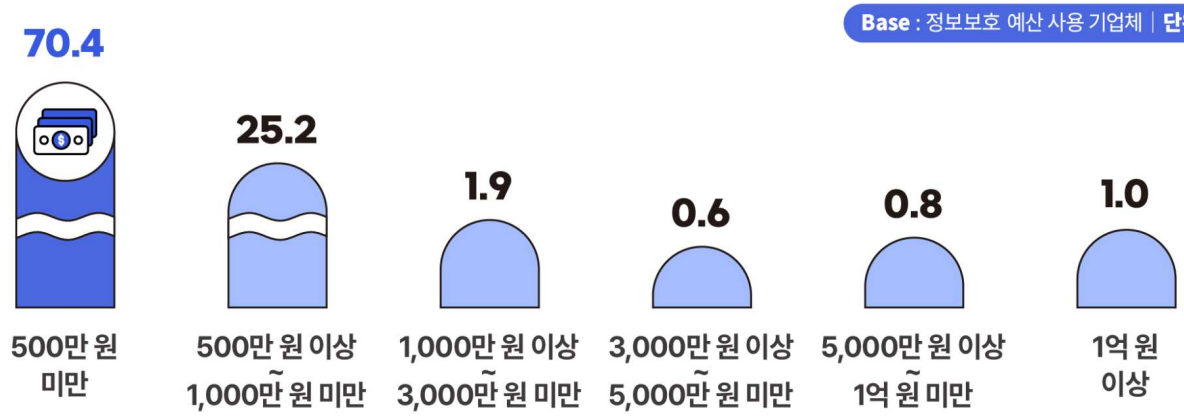
● 정보보호 예산 지출 항목 Top 5

Base : 정보보호 예산 사용 기업체 | 단위 : %, 복수응답



● 예산 총액

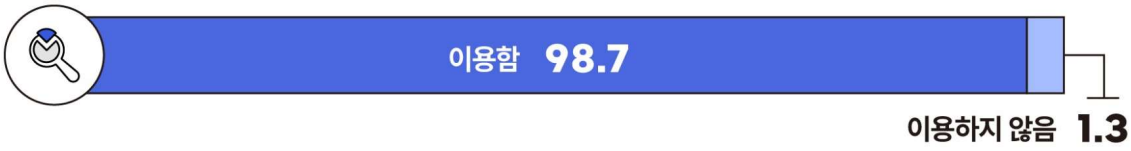
Base : 정보보호 예산 사용 기업체 | 단위 : %



05 정보보안 예방활동

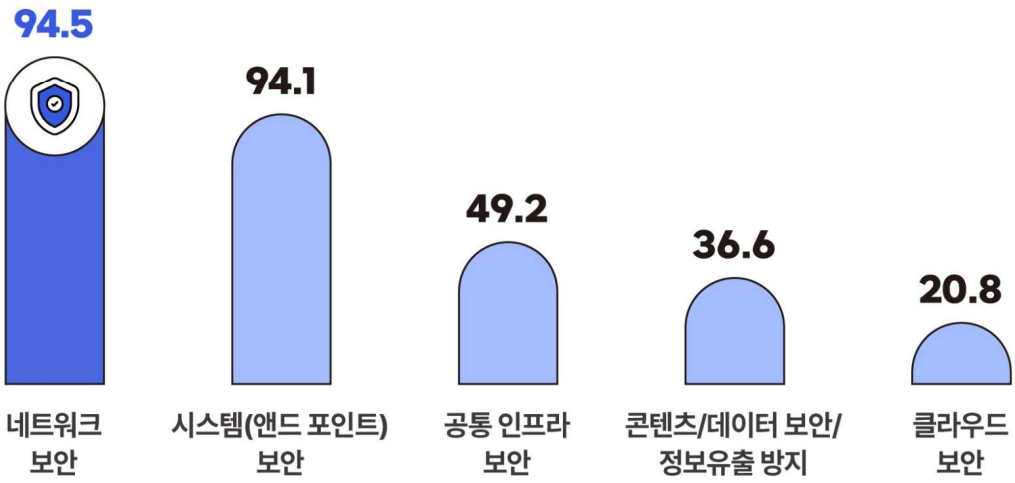
● 침해사고 예방 제품 및 서비스 이용률

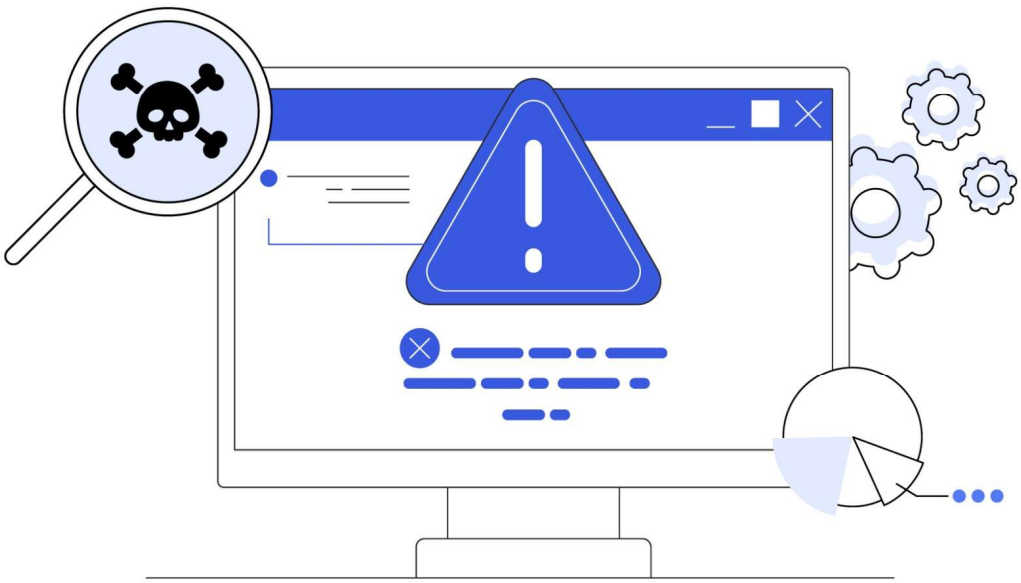
Base : 전체 | **단위** : %



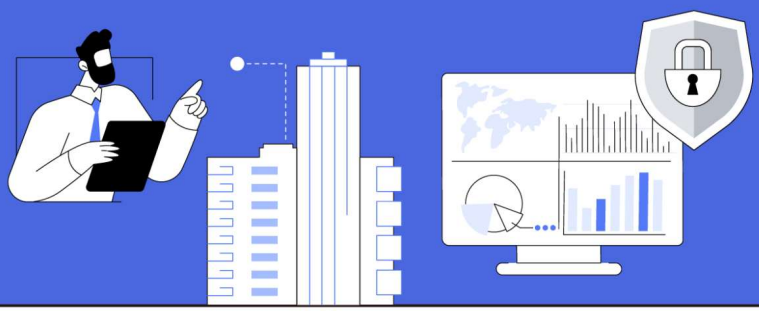
● 이용 정보보안 제품 및 서비스 유형 Top 5

Base : 정보보호 제품 및 서비스 이용 기업체 | **단위** : %, 복수응답





기업부문



06 침해사고

침해사고 경험률

Base : 전체 | 단위 : %

전체	기업규모별	
0.2	10-49명	0.1
	50-249명	0.5
	250명 이상	1.8

침해사고 신고율

Base : 침해사고 경험한 기업체 | 단위 : %

전체	기업규모별	
31.4	10-49명	32.9
	50-249명	22.3
	250명 이상	43.6

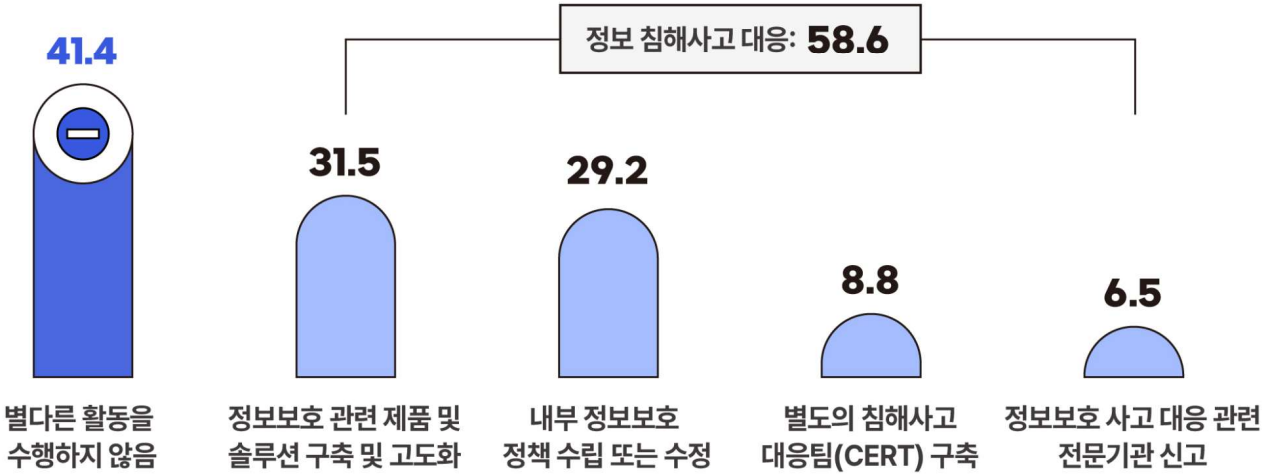
경험한 침해사고 유형

Base : 침해사고 경험한 기업체 | 단위 : %, 복수응답

- 외부로부터 침투한 비인가 접근(해킹) 73.0
- 컴퓨터 바이러스, 웜, 트로이잔, APT 공격으로 인한 IT 시스템 마비 30.6
- 랜섬웨어감염 20.0
- 내부인력에 의한 중요 데이터 유출 8.6
- 피싱, 스미싱 등에 의한 금전 또는 중요 데이터 유출 2.5
- 중요 자산(디지털 자산 포함)에 대한 의도적인 손·망실 1.9

정보 침해사고 대응활동 Top 5

Base : 침해사고 경험한 기업체 | 단위 : %, 복수응답



2025

정보보호 실태조사_개인부문

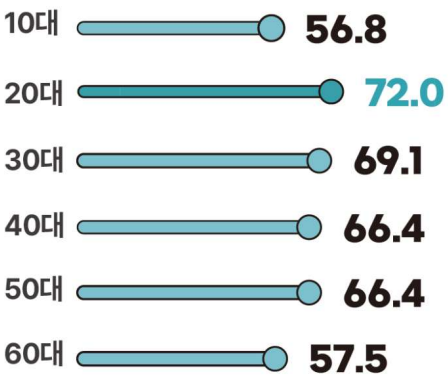
01 정보보호 인식

정보보호 이슈 관심도

Base : 전체 | 단위 : %

남자 64.4 | 여자 66.1

전체 65.3

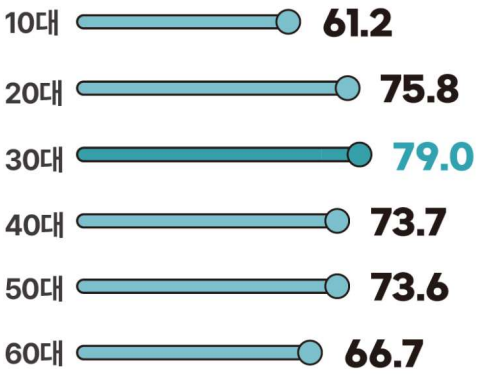


정보보호 침해 우려도

Base : 전체 | 단위 : %

남자 71.5 | 여자 73.6

전체 72.5

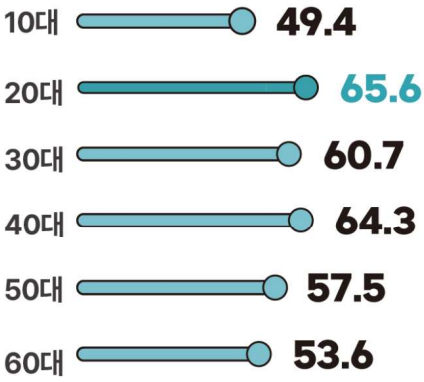


정보 침해사고 소식에 대한 관련성 인식

Base : 전체 | 단위 : %

남자 58.0 | 여자 60.4

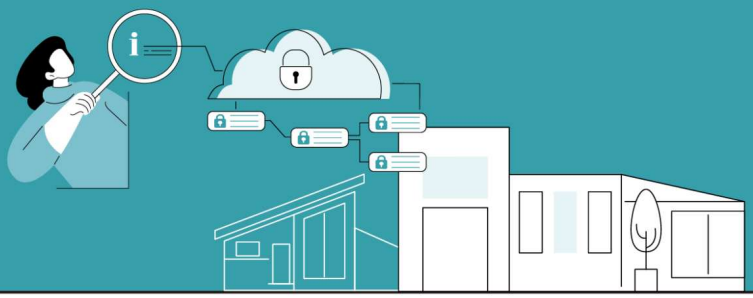
전체 59.2



정보보호 안전 체감도

Base : 전체 | 단위 : %

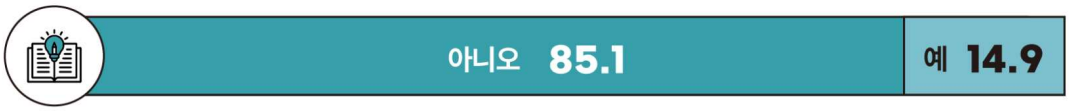
개인부문



02 정보보호 교육 활동

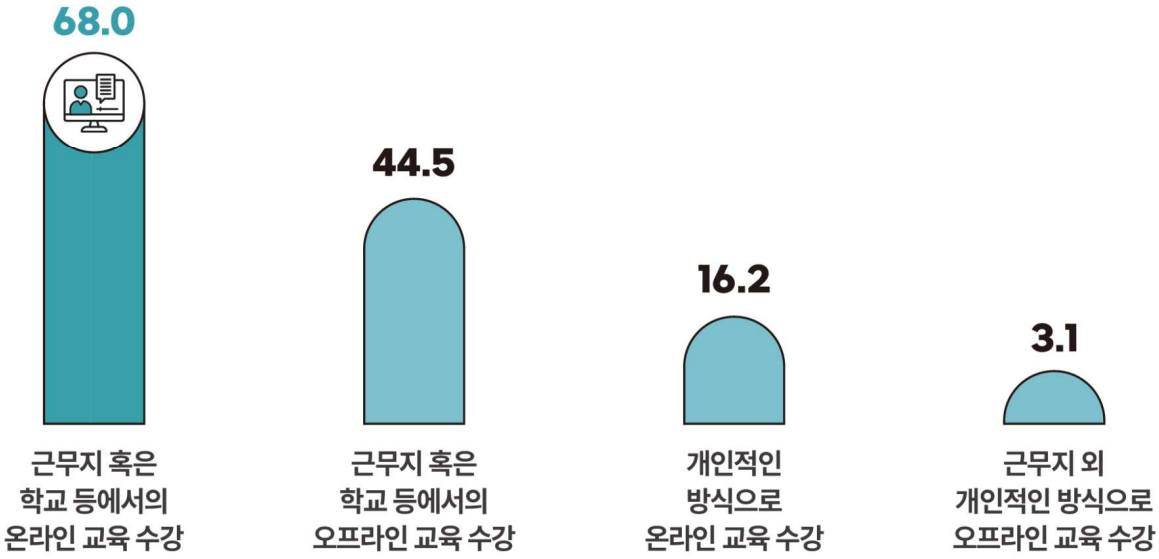
● 정보보호 교육 경험률

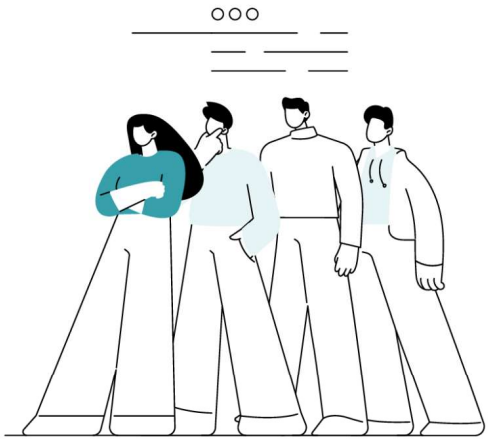
Base : 전체 | **단위** : %



● 정보보호 교육 방식

Base : 정보보호 교육 경험자 | **단위** : %, 복수응답



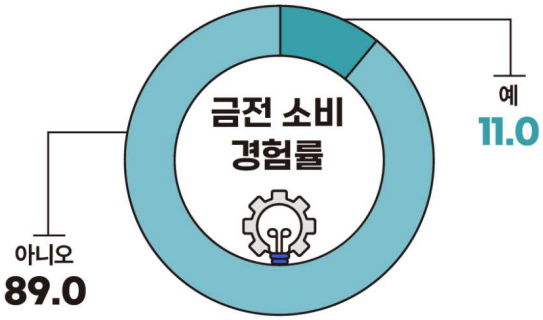


개인부문

03 정보보호 관련 소비 활동

● 정보보호 금전 소비 경험률

Base : 전체 | 단위 : %



● 정보보호 금전 소비 규모

Base : 정보보호 금전 소비 경험자 | 단위 : %

1만 원 미만	14.5
1만 원 이상 ~ 10만 원 미만	44.1
10만 원 이상 ~20만 원 미만	19.8
20만 원 이상 ~ 30만 원 미만	10.9
30만 원 이상 ~ 40만 원 미만	6.1
40만 원 이상 ~ 50만 원 미만	3.6
50만 원 이상	1.1

● 정보보호 금전 소비 비용 증감 여부

Base : 정보보호 금전 소비 경험자 | 단위 : %

정보보호 금전 소비 규모	감소 예정	5.7
	유지 예정	59.1
	증가 예정	35.2

● 정보보호 비용 지출 의향

Base : 정보보호 금전 소비 비경험자 | 단위 : %

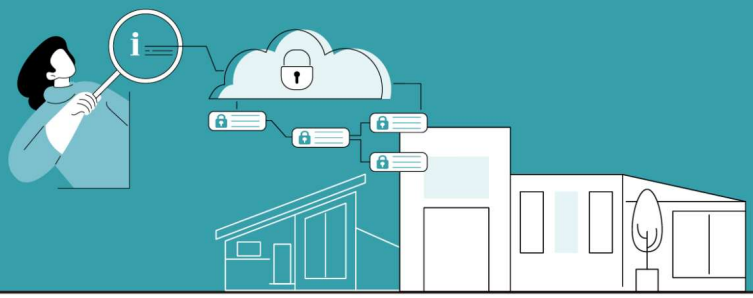
정보보호 금전 소비 의향	28.6

● 정보보호 금전 소비 유형

Base : 정보보호 금전 소비 경험자 | 단위 : %, 복수응답

정보보호 관련 유료 인증서의 결제	정보보호 관련 제품 및 솔루션의 구입	자택 또는 개인 생활 공간의 CCTV 등 영상 감시장비 설치/증설	자택 또는 개인 생활 공간을 위한 출동보안 서비스 이용	정보보호 관련 학습 정보 습득
74.0	72.3	33.9	32.5	26.9

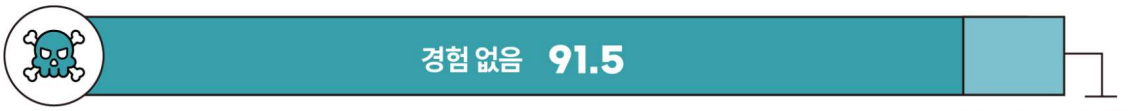
개인부문



04 침해사고 대응 및 예방조치

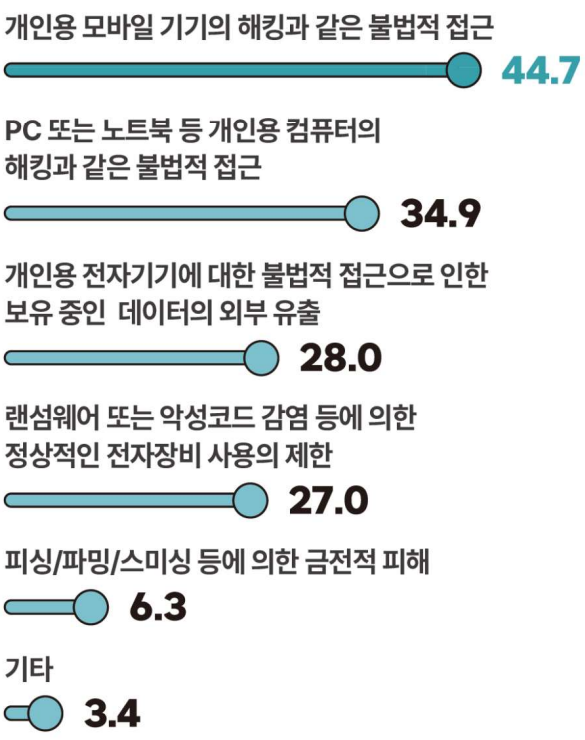
침해사고 경험률

Base : 전체 | 단위 : %



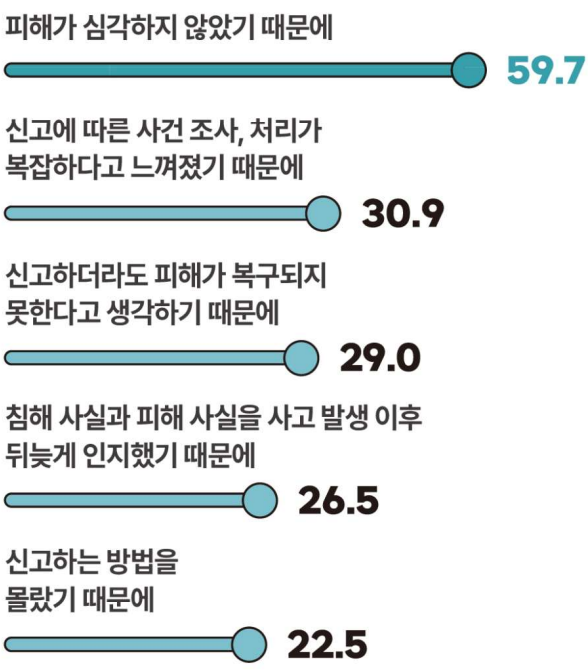
침해사고 경험 유형

Base : 침해사고 경험자 | 단위 : %, 복수응답



침해사고 미신고 이유 Top 5

Base : 침해사고 미신고자 | 단위 : %, 복수응답



침해사고 피해 심각도

Base : 침해사고 경험자 | 단위 : %

침해사고 신고율

Base : 침해사고 경험자 | 단위 : %

CONTENTS

제1부 기업 부문

CONTENTS

CONTENTS

CONTENTS

CONTENTS

부록

제 1 부

기업부문

제 1 장 조사 개요

1 조사 목적

- 급속하게 변화하는 인터넷 환경과 사물인터넷(IoT), IP카메라 등 새로운 기술의 끊임없는 등장으로 사이버 세계의 위협이 현실 세계로 확대되고 그 위협 또한 고도화·지능화되고 있음. 이에 따라 정보보호 관련된 현황 및 인터넷 이용자들의 인식 수준, 대응 활동 등을 파악하고, 인터넷 이용자의 정보보호 수준 제고에 활용하고자 정보보호 실태조사를 실시하였음
- 본 조사는 이러한 필요에 근거하여 향후 효과적인 정보보호 관련 정책수립의 기초자료를 확보하고, 나아가 업계의 비즈니스 전략 수립, 학계의 연구 활동 등 다양한 영역에서 활용할 수 있는 통계 정보를 제공하는데 그 목적이 있음
- 본 조사의 구체적인 목적은 다음과 같음
  1. 정부, 기업, 개인 등 사회구성원 전체의 정보보호 수준 제고에 활용하기 위한 기초자료 제공
  2. 국가정보보호백서 등의 정보보호 통계자료 제공
  3. 국제기구(OECD)의 ICT 통계지표 기초자료 제공
  4. 업계 및 학계의 현장, 연구 활동 등에 활용

2 조사 연혁

2001년
- 국내 500개 기업체 대상 「민간부문 정보보호 실태조사」 실시

2005년
- '전국의 종사자수 5명 이상, 네트워크로 연결된 컴퓨터를 1대 이상 보유한 사업체'로 조사대상 변경

2006년
- 정보보안 침해사고의 피해 현황 파악을 위한 조사지표 추가

2007년
- 조사 결과의 신뢰도 제고를 위한 표본 수 확대 ('06년 1,200개 → '07년 2,500개)
- 기업의 정보화 기반 특성에 따라 4개 유형으로 조사표 구분
- 「민간기업 정보보호 실태조사」 통계청 작성 승인 (일반통계 제34201호)

2009년
- 개인정보 보호조치 기준 개정에 따른 기업체 준수 여부 확인을 위한 조사항목 추가

2010년
- 조사 결과의 신뢰도 제고를 위한 표본 수 확대 ('09년 2,234개 → '10년 6,000개)

2011년
- 조사의 효율성 향상을 위한 표본 수 축소 ('10년 6,000개 → '11년 5,000개)

2012년
- 개인정보보호의 중요성 강화에 따른 개인정보보호 분야 신규 조사항목 추가

2013년
- 개인정보보호 정책성과 평가 항목 축소 및 세부 문항 수정·보완
- 한국인터넷진흥원에서 미래창조과학부로 통계작성기관 변경

2014년
- 소규모 사업체 정보보호 실태 파악을 위해 사업체 종사자 수 5인 이상에서 1인 이상으로 조사대상 범위 확대
- 조사대상 범위 변경으로 인한 표본 수 확대 ('13년 5,000개 → '14년 7,000개)

2015년
- 조사 결과의 신뢰도 제고를 위한 표본 수 확대 ('14년 7,000개 → '15년 8,000개)
- 승인통계 통합 관리를 위해 정보보호 실태조사 승인번호 단일화 (개인부문 승인번호인 제34205호로 통합)

2016년
- 조사 결과의 신뢰도 제고를 위한 표본 수 확대 (‘15년 8,000개 → ‘16년 9,000개)
- ICT 통계업무 조정으로 「정보화실태조사의 정보보호 파트」 본 조사에서 실시, OECD에 데이터 2개 제출(정보보호 및 개인정보보호 정책률, 침해사고 경험률)

2017년
- ICT 환경변화에 따른 정보보호 이슈를 반영하기 위해 사이버(정보보호, 개인정보보호) 보험 등의 조사항목 추가
- 통계작성기관명 변경(미래창조과학부→과학기술정보통신부)

2018년
- ‘2016년 기준 전국사업체조사’와 ‘2017년 정보화통계조사’ 결과를 기반으로 표본 재설계

2019년
- 전담기관 변경(한국인터넷진흥원→한국정보보호산업협회)
- 한국표준산업분류 10차 개정(KSIC Rev.10)에 의해 업종 재분류

2020년
- ‘2018년 기준 전국사업체조사’와 ‘2019년 정보화통계조사’ 결과를 기반으로 표본 재설계

2021년
- 조사의 효율성 향상을 위한 표본 수 축소 (‘20년 9,000개 → ‘21년 7,500개)
- ‘2019년 기준 전국사업체조사’와 ‘2020년 정보화통계조사’ 결과를 기반으로 표본 재설계

2022년
- 조사의 효율성 향상을 위한 표본 수 축소 (‘21년 7,500개 → ‘22년 6,500개)
- 통계청, ‘2021년 4분기 기준 기업통계등록부(SBR)’와 ‘2021년 정보화통계조사’ 결과를 기반으로 표본 재설계

2023년
- 통계청, ‘2022년 4분기 기준 기업통계등록부(SBR)’와 ‘2022년 정보화통계조사’ 결과를 기반으로 표본 재설계

2024년
- 통계청, ‘2023년 4분기 기준 기업통계등록부(SBR)’와 ‘2023년 정보화통계조사’ 결과를 기반으로 표본 재설계

2025년
- 조사의 효율성 향상을 위한 표본 수 축소 (‘24년 6,500개 → ‘25년 5,500개)
- 통계청, ‘2024년 4분기 기준 기업통계등록부(SBR)’와 ‘2024년 정보화통계조사’ 결과를 기반으로 표본 재설계

3 조사 내용 및 범위

- 본 조사는 국내 기업체의 정보보호 기반 및 환경, 정보 침해사고 예방, 정보 침해사고 경험 및 대응, 정보보호 인식 등 실태를 파악할 수 있는 지표로 구성하였음
- 본 조사의 주요 내용은 다음과 같음
  1. 정보보호 인식
  2. 정보보호 정책 및 조직
  3. 정보보호 교육
  4. 정보보호 예산
  5. 정보 침해사고 예방
  6. 정보 침해사고 경험
  7. 사이버 보험
  8. 원격근무

4 주요 용어 및 정의

- **정보보호** : 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 활동
- **악성코드** : 시스템을 파괴하거나 정보를 유출하는 등 악의적 활동을 수행하도록 의도적으로 제작된 소프트웨어(바이러스, 웜, 애드웨어, 스파이웨어 등)
- **정보관리책임자(CIO)** : Chief Information Officer의 약자로 조직의 경영과 전략적 관점에서 정보기술 및 정보시스템을 총괄 관리하는 최고 책임자
- **정보보호최고책임자(CISO)** : Chief Information Security Officer의 약자로 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임명된 최고 책임자
- **개인정보보호책임자(CPO)** : Chief Privacy Officer의 약자로 이용자의 개인정보를 보호하고, 개인정보와 관련한 이용자의 고충을 처리하는 최고 책임자
- **정보보호 관리체계 인증(ISMS)** : Information Security Management System의 약자로 정보통신망의 안전성 확보를 위하여 한국인터넷진흥원에서 인증하고 있는 기술적, 물리적 보호조치 등 종합적인 정보 관리체계에 대한 인증 제도
- **취약점 분석** : 시스템, 네트워크 혹은 물리적 시설의 소프트웨어나 하드웨어상의 문제로 인해 해커가 공격하는데 이용할 수 있는 보안상의 문제점을 찾아내는 활동
- **정보 침해사고** : 모든 사이버 공격 행위나 그 결과에 따라 생긴 여러 가지 피해, 해킹, 컴퓨터 바이러스, 논리 폭탄, 메일 폭탄, 서비스 거부 또는 고출력 전자기파 같은 방법으로 정보통신망 또는 이와 관련한 네트워크 및 시스템이 공격을 당하여 생긴 문제 등을 의미
- **해킹** : 사내 데이터나 전산 시스템에 대한 외부로부터의 비인가 접근
- **랜섬웨어(Ransomware)** : 몸값을 의미하는 'Ransom'과 'Software'의 합성어로, 인터넷 사용자의 시스템을 잠그거나 데이터를 사용할 수 없도록 암호화한 뒤에 그 데이터를 인질로 금전을 요구하는 악성 프로그램을 의미
- **APT 공격** : Advanced Persistent Threat(지능적 지속 위협)의 약자로 정교한 수준의 전문 기술 또는 방대한 리소스를 가진 공격자가 특정 기업 또는 기관을 대상으로 여러 공격 경로를 사용하여 공격하는 것을 의미
- **침해사고 대응팀(CERT)** : 정보통신망 등의 침해사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해사고의 접수 및 처리 지원을 비롯해 예방, 피해 복구 등의 임무를 수행하는 조직
- **클라우드(Cloud Service)** : 하드웨어, 소프트웨어 등 각종 IT자원(서버, 스토리지, 응용 프로그램 등 모든 종류의 HW 및 SW)을 인터넷을 통해 전기나 수도처럼 빌려 쓸 수 있는 기술 및 서비스 방식
- **사물인터넷(IoT)** : Internet of Things의 약자로 모든 사물을 인터넷으로 연결하여 사람과 사물, 사물과 사물 간의 정보를 상호 소통하는 지능형 기술 및 서비스
- **사이버 보험** : 기업이 사이버 공간에서 일어난 해킹, DDoS 등의 의도적인 공격으로 인해 겪게 되는 피해를 보장하는 보험

5 조사 체계

- **조사대상** : 전국 종사자 수 10인 이상의 기업체 중 네트워크에 연결된 컴퓨터를 1대 이상 보유하고 있는 기업체
- **유효 응답 업체 수** : 5,500개
- **조사주기** : 연 1회
- **조사기간** : 2025년 9월 15일 ~ 12월 15일 (3개월)
- **조사방법** : 기업체 방문 면접조사(이메일, 팩스조사 등 병행)
- **조사기관**
  - 주관기관 : 과학기술정보통신부(Ministry of Science and ICT)
  - 전담기관 : 한국정보보호산업협회(Korea Information Security Industry Association)
- **법적근거**
  - 정보보호산업의 진흥에 관한 법률 시행령 제20조
  - 통계법 제18조(통계작성의 승인)

6 표본 설계

가 모집단

- **목표 모집단(Target Population)** : 네트워크에 연결된 컴퓨터를 보유한 기업체
- **조사 모집단(Survey Population)**
  - 네트워크에 연결된 컴퓨터를 1대 이상 보유하고 있는 종사자 규모 10인 이상의 국내 기업체
- **모집단 자료**
  - 통계청『2024년 4분기 기준 기업통계등록부(SBR)』의 업종별, 규모별 기업체 수 및 분포
  - 한국지능정보사회진흥원『2024년 정보화통계조사』결과에서 파악된 네트워크 구축 비율
- **규모(종사자 수)** : 10~49명/50~249명/250~999명/1,000명 이상

표 1-1-1 종사자 규모별 분류 기준

구분	규모 분류 기준
규모 1층	10~49명
규모 2층	50~249명
규모 3층	250~999명
규모 4층	1,000명 이상

- **업종** : 본 조사를 위한 업종 분류는 OECD의 분류 권고안과 한국표준산업분류를 기준으로 16개 업종으로 구분함
  - 한국표준산업분류 중 가사서비스업, 국제 및 외국기관, 공공행정, 국방 및 사회 보장 행정은 제외함

표 1-1-2 업종 분류 기준

한국표준산업분류 (10차 개정)	업종 분류 기준 (본 조사)	국제기구 분류 기준 (ISIC ver 4.0)
A. 농업, 임업 및 어업	1. 농림수산업(광업포함)	-
B. 광업		
C. 제조업	2. 제조업	제조업(ISIC C)
D. 전기, 가스, 증기 및 공기조절 공급업	3. 전기, 가스, 증기 및 공기조절 공급업/수도, 하수·폐기물 처리, 원료재생업	-
E. 수도, 하수·폐기물 처리, 원료재생업		
F. 건설업	4. 건설업	건설업(ISIC F)
G. 도매 및 소매업	5. 도매 및 소매업	도소매업(ISIC G): 자동차 및 모터사이클 수리업
H. 운수 및 창고업	6. 운수 및 창고업	운수업(ISIC H)
I. 숙박 및 음식점업	7. 숙박 및 음식점업	숙박 및 음식점업(ISIC I)
J. 정보통신업	8. 정보통신업	정보통신업(ISIC J)
K. 금융 및 보험업	9. 금융 및 보험업	-
L. 부동산업	10. 부동산업	부동산업(ISIC L)
M. 전문, 과학 및 기술 서비스업	11. 전문, 과학 및 기술서비스업	전문, 과학 및 기술서비스업 (M75 수의업 제외)
N. 사업시설 관리, 사업 지원 및 임대 서비스업	12. 사업시설관리, 사업지원 및 임대 서비스업	사업관리 및 지원서비스업(ISIC N)
P. 교육 서비스업	13. 교육 서비스업	-
Q. 보건업 및 사회복지 서비스업	14. 보건업 및 사회복지 서비스업	-
R. 예술, 스포츠 및 여가관련 서비스업	15. 예술, 스포츠 및 여가관련 서비스업	-
S. 협회 및 단체, 수리 및 기타 개인서비스업	16. 협회, 단체, 수리 및 기타 개인서비스업(협회 및 단체 제외)	기타 서비스업 (ISIC S, S95 수리업 포함) - ISIC S94 협회 및 단체 - ISIC S95 컴퓨터, 개인 및 가정용품 수리업 포함 - ISIC S96 기타 개인서비스업

- **모집단 분포**

  - 통계청『2024년 4분기 기준 기업통계등록부(SBR)』및 한국지능정보사회진흥원『2024년 정보화 통계조사』에서 조사된 기업체 중 종사자 수 10인 이상 기업체 현황은 다음과 같이 나타남

표 1-1-3 종사자 수 10인 이상 기업체 및 네트워크 구축 기업체 현황

(단위: 개)

구분	업종/규모	종사자 수 10인 이상 기업체	컴퓨터 보유/ 네트워크 구축 기업체
업종별	1. 농림수산업(광업포함)	1,952	1,361
	2. 제조업	64,275	52,106
	3. 전기, 가스, 증기 및 공기조절 공급업/ 수도, 하수·폐기물 처리, 원료재생업	2,592	2,122
	4. 건설업	30,400	28,142
	5. 도매 및 소매업	27,694	24,473
	6. 운수 및 창고업	8,161	7,097
	7. 숙박 및 음식점업	10,591	7,770
	8. 정보통신업	11,609	10,685
	9. 금융 및 보험업	4,216	4,164
	10. 부동산업	4,345	2,756
	11. 전문, 과학 및 기술서비스업	19,981	17,900
	12. 사업시설관리, 사업지원 및 임대 서비스업	4,250	3,795
	13. 교육 서비스업	6,268	5,905
	14. 보건업 및 사회복지 서비스업	48,817	42,549
	15. 예술, 스포츠 및 여가관련 서비스업	2,097	1,626
	16. 협회, 단체, 수리 및 기타 개인서비스업 (협회 및 단체 제외)	4,334	3,440
규모별	10~49명	214,821	180,452
	50~249명	31,453	30,172
	250~999명	4,334	4,293
	1,000명 이상	974	974

※ 출처: 「2024년 4분기 기준 기업통계등록부(SBR)」(통계청), 「2024년 정보화통계조사」(한국지능정보사회진흥원)

표 1-1-4 업종*규모별 종사자 수 10인 이상 기업체 및 네트워크 구축 기업체 현황

업종 분류	규모 분류	컴퓨터 보유/ 네트워크 구축 기업체	구성비	업종 분류	규모 분류	컴퓨터 보유/ 네트워크 구축 기업체	구성비
농림수산업 (광업포함)	10~49명	1,270	0.59	금융 및 보험업	10~49명	2,787	1.29
	50~249명	84	0.04		50~249명	1,124	0.52
	250~999명	5	0.00		250~999명	177	0.08
	1,000명 이상	2	0.00		1,000명 이상	76	0.04
제조업	10~49명	43,148	19.99	부동산업	10~49명	2,093	0.97
	50~249명	7,919	3.67		50~249명	462	0.21
	250~999명	913	0.42		250~999명	149	0.07
	1,000명 이상	126	0.06		1,000명 이상	52	0.02
전기, 가스, 증기 및 공기 조절 공급업/수도, 하수·폐기물 처리, 원료재생업	10~49명	1,755	0.81	전문, 과학 및 기술 서비스업	10~49명	14,216	6.58
	50~249명	320	0.15		50~249명	2,878	1.33
	250~999명	37	0.02		250~999명	587	0.27
	1,000명 이상	10	0.00		1,000명 이상	219	0.10
건설업	10~49명	24,703	11.44	사업시설관리, 사업지원 및 임대 서비스업	10~49명	2,707	1.25
	50~249명	2,939	1.36		50~249명	770	0.36
	250~999명	420	0.19		250~999명	251	0.12
	1,000명 이상	80	0.04		1,000명 이상	67	0.03
도매 및 소매업	10~49명	21,938	10.16	교육 서비스업	10~49명	4,843	2.24
	50~249명	2,208	1.02		50~249명	811	0.38
	250~999명	256	0.12		250~999명	173	0.08
	1,000명 이상	71	0.03		1,000명 이상	78	0.04
운수 및 창고업	10~49명	5,190	2.40	보건업 및 사회복지 서비스업	10~49명	35,557	16.47
	50~249명	1,633	0.76		50~249명	6,197	2.87
	250~999명	229	0.11		250~999명	714	0.33
	1,000명 이상	45	0.02		1,000명 이상	81	0.04
숙박 및 음식점업	10~49명	7,295	3.38	예술, 스포츠 및 여가관련 서비스업	10~49명	1,278	0.59
	50~249명	427	0.20		50~249명	302	0.14
	250~999명	40	0.02		250~999명	39	0.02
	1,000명 이상	8	0.00		1,000명 이상	7	0.00
정보통신업	10~49명	8,418	3.90	협회, 단체, 수리 및 기타 개인 서비스업 (협회 및 단체 제외)	10~49명	3,254	1.51
	50~249명	1,938	0.90		50~249명	160	0.07
	250~999명	279	0.13		250~999명	24	0.01
	1,000명 이상	50	0.02		1,000명 이상	2	0.00
총 합계						215,891	100.00

※ 출처: 「2024년 4분기 기준 기업통계등록부(SBR)」(통계청), 「2024년 정보화통계조사」(한국지능정보사회진흥원)

나 표본 추출

- **개요** : 다단계층화계통추출법
  - 업종*규모별로 2단 층화한 후 각 기업체를 지역별로 정렬하여 계통추출
- **표본의 규모 산정**
  - 허용오차에 따른 표본의 크기 결정식

$$n = \frac{\left(\sum_{h=1}^{L} N_h \sqrt{p_h q_h}\right)^2}{N^2 D + \sum_{h=1}^{L} N_h p_h q_h}$$

여기에서 n : 총표본의 크기,

$$D = \left(\frac{B}{t_{n-1,\frac{\alpha}{2}}}\right)^2,$$

$$B = t_{n-1,\frac{\alpha}{2}} \sqrt{\hat{V}(p_{st})}$$

p_h: 층h의 "공식문서화된 정보보호 정책 수립여부" 추정치

$q_h = 1 - p_h$

$t_{n-1,\frac{\alpha}{2}}$: 유의수준 α%에서의 t 값

  - 정보보호 정책 수립 여부에 대한 모수를 이용하여 표본의 크기를 결정하며, 허용오차에 따른 표본의 크기는 아래와 같음

표 1-1-5 허용오차별 표본의 크기

단위: 개, %

표본 크기	5,899	5,715	5,540	5,372	5,212	5,059
허용오차	1.22	1.24	1.26	1.28	1.30	1.32

  - 최종 표본의 크기는 허용오차가 1.26% 내외가 되도록 5,500개로 결정함

- **표집틀(Sampling frame)**
  - 1차 표집틀 : 「2024년 4분기 기준 기업통계등록부(SBR)」 대상 기업체
  - 2차 표집틀 : 「2024년 정보화통계조사」 대상 기업체 중 종사자 수 10인 이상 네트워크 구축 기업체
- **표본할당 및 추출방법**
  - 멱등할당(Power allocation) : 2024년도 정보보호 실태조사 결과 중 '공식 문서화된 정보보호 정책 수립 여부'에 대한 추정량을 이용하여 표본오차를 계산하고, p=0.4인 경우를 최종 할당으로 결정
  - 절사추출 : 종사자 수가 1,000명 이상인 기업체와 250~999명인 기업체 일부 전수 조사 실시

7 실사

가 실사 개요

- **조사기간**
  - 2025년 9월 15일 ~ 12월 15일 (3개월)
- **조사기준 시점**
  - 2024년 12월 31일
    * 정보보호 교육 실시, 정보보호 예산, 정보 침해사고 경험, 원격근무 경험은 2024년 1월 1일 ~ 12월 31일을 기준으로 조사함
- **조사대상**
  - 네트워크에 연결된 컴퓨터 보유 기업체(종사자 수 10인 이상)
- **조사방법**
  - 전문 조사원이 표본으로 선정된 기업체를 방문하여 설문 응답을 받는 형태의 기업체 방문 면접조사
- **조사절차**
  - 면접원의 기업체 면접조사 → 지역별 실사 감독원의 관리 및 통제 → 설문지 집계 → 보완조사 및 재조사 → 최종 자료 검증

나 표본 관리

- **본표본 관리**
  - 사전 추출된 기업체 5,500개를 대상으로 조사하는 것을 원칙으로 하며, 해당 기업체의 휴·폐업 및 강력한 응답거부 등으로 조사가 불가능한 경우에는 동일한 업종, 규모 특성으로 추출된 예비 표본으로 대체하여 조사를 진행함

8 자료 입력 및 처리

가 자료 검증 및 대체

- **실사 과정에서의 자료 검증**
  - 지역별 실사 감독원이 회수된 설문지의 30% 이상을 무작위 추출하여 조사원 방문 여부, 응답의 정확성 등에 대한 전화 검증을 실시함
  - 실사 감독원의 1차 검증에서 합격된 설문지는 에디팅 및 입력 과정에서 전산 프로그램에 의해 2차 검증함
  - 입력된 자료는 자료 처리 과정에서 내검 프로그램에 의해 3차 검증함
  - 검증 단계별로 불합격된 설문지에 대한 보완조사 및 재조사를 실시함
- **분석 과정에서의 자료 검증**
  - 동일한 업종·규모별 평균치 및 이전 조사결과와의 시계열 비교 및 검증을 실시함
- **무응답 대체**
  - 단위무응답 및 항목무응답 발생 시 해당 기업체 방문 및 전화 재조사를 통하여 무응답률을 최소화함
  - 단위무응답 발생 시 예비 표본의 범위 내에서 대체하여 단위무응답을 제거함
  - 항목무응답 발생 시 결측값을 해당 기업체 특성(업종, 규모)과 동일한 그룹의 평균값으로 대체하여 항목무응답을 제거함

나 자료 입력 및 분석

- 수집된 자료는 부호화(coding) 과정을 통해 전산 입력되며, 다단계 검증 과정에서 최종 합격된 자료는 SPSS for Windows(통계 패키지 프로그램)를 이용하여 분석함
  - 응답 기업체명, 주소, 전화번호 등 기업체를 식별할 수 있는 정보는 일련번호로 부호화하거나 자료 입력 시 제외함

9 추정 및 표본오차

가 가중치 산출

- **사후층화**
  - 본 조사는 모집단의 특성을 그대로 반영하는 층별 비례할당 조사로 진행되지 않았기 때문에 조사된 표본이 모집단의 특성을 그대로 나타내지 않음
  - 따라서 실제 조사된 표본만의 특성을 반영하지 않고 표본설계된 모집단의 특성을 반영하기 위해 사후 층화(post-stratification) 방법을 이용하여 모집단과 표본 간 편차를 최소화하는 작업을 수행함
  - 이 작업은 조사가 완료된 후 모집단의 업종·규모별 특성 가중치를 각 표본에 적용하여 최종 결과를 산출하는 방식으로 진행됨
- **모총계의 추정**
  - 본 조사는 '다단계층화계통추출' 방식을 적용하여 추출된 표본의 업종·규모별 모집단 특성을 반영하기 위해 모총계를 추정함
  - 전체 모집단 총계 $\hat{\tau} = \tau_{\text{전수층}} + \hat{\tau}_{\text{표본층}}$ 를 추정함
  - 표본설계 시 모집단을 전수층과 표본층으로 구분하였으므로 모집단 총계는 다음과 같이 추정함

$$\hat{\tau} = \sum_{h=1}^{L} {}_c\tau_h + \sum_{h=1}^{L} {}_s W_h \, y_{hsk}$$

여기에서

$_c\tau_h$: 전수층 총계

L : 층의 개수 (업종×규모)

y_{hsk} : 표본층 h의 k번째 관찰값

$_c\tau_h$: 전수층에서 각 층의 총계

$_s\hat{\tau}_h$: 표본층에서 각 층의 총계에 대한 추정량의 합계

나 추정

- 전체 모비율 추정 산출 공식은 다음과 같음

$$\hat{p}_{st} = \frac{\hat{\tau}}{N} = \frac{\sum_{h=1}^{L} {}_c\hat{\tau}_h + \sum_{h=1}^{L} {}_s W_h \sum_{k=1}^{{}_s n_h} {}_s y_{hk}}{N}$$

다 표본오차

- **모집단 총계의 분산 및 표본오차 추정**

  - 모총계 추정량에 대한 분산 추정(표본층에서만 표본오차가 발생함)

$$\hat{Var}(\hat{\tau}) = \hat{Var}\left(\sum_{h=1}^{L} {}_{s}W_h \sum_{k=1}^{{}_{s}n_h} {}_{s}y_{hk}\right)$$

$$= \sum_{h=1}^{L} {}_{s}W_h \frac{1}{{}_{s}n_h - 1} \sum_{k=1}^{{}_{s}n_h} ({}_{s}y_{hk} - {}_{s}\bar{y}_h)^2$$

- **모비율 분산 및 표본오차 추정**

$$\hat{p}_{st} = \frac{\hat{\tau}}{N} = \frac{\sum_{h=1}^{L} {}_{c}\hat{\tau}_h + \sum_{h=1}^{L} \frac{{}_{s}N_h}{{}_{s}n_h} \sum_{k=1}^{{}_{s}n_h} {}_{s}y_{hk}}{N}$$

$$\hat{V}(\hat{p}_{st}) = \sum_{h=1}^{L} \left(\frac{{}_{s}N_h}{N}\right)^2 \left(1 - \frac{{}_{s}n_h}{{}_{s}N_h}\right) \frac{{}_{s}\hat{p}_h \, {}_{s}\hat{q}_h}{{}_{s}n_h - 1}$$

여기에서 ${}_{s}\hat{p}_h$: h층에서 표본 비율

${}_{s}\hat{q}_h = 1 - {}_{s}\hat{p}_h$

표 1-1-6 정보보호 정책 보유율 추정 결과 및 표본오차

정보보호 정책 보유율 표본오차	± 1.30%p (95% 신뢰수준)
정보보호 정책 보유율 추정 결과	52.6% ± 1.30%p

10 결과 공표 및 활용 분야

- 「2025년 정보보호 실태조사(기업부문)」 보고서는 한국정보보호산업협회 홈페이지 (https://www.kisia.or.kr)를 통해 게시함
- 본 통계자료는 과학기술정보통신부 등 정부부처 및 연구기관의 정책수립의 기초자료 및 국제기구(OECD) 등에 제출되어 국가별 정보보호 현황 비교 등을 위한 통계자료로 활용됨

11 모집단 및 표본 현황

표 1-1-7 모집단 및 표본 현황

단위: 개, %

업종 분류	규모 분류	컴퓨터 보유 / 네트워크 구축 기업체		응답 표본 현황	
		모집단 수	구성비	표본 수	구성비
농림수산업 (광업포함)	10~49명	1,270	0.59	60	1.09
	50~249명	84	0.04	32	0.58
	250~999명	5	0.00	5	0.09
	1,000명 이상	2	0.00	2	0.04
제조업	10~49명	43,148	19.99	216	3.93
	50~249명	7,919	3.67	207	3.76
	250~999명	913	0.42	170	3.09
	1,000명 이상	126	0.06	100	1.82
전기, 가스, 증기 및 공기 조절 공급업 / 수도, 하수·폐기물 처리, 원료재생업	10~49명	1,755	0.81	71	1.29
	50~249명	320	0.15	51	0.93
	250~999명	37	0.02	28	0.51
	1,000명 이상	10	0.00	8	0.15
건설업	10~49명	24,703	11.44	165	3.00
	50~249명	2,939	1.36	136	2.47
	250~999명	420	0.19	108	1.96
	1,000명 이상	80	0.04	66	1.20
도매 및 소매업	10~49명	21,938	10.16	155	2.82
	50~249명	2,208	1.02	124	2.25
	250~999명	256	0.12	97	1.76
	1,000명 이상	71	0.03	54	0.98
운수 및 창고업	10~49명	5,190	2.40	105	1.91
	50~249명	1,633	0.76	110	2.00
	250~999명	229	0.11	87	1.58
	1,000명 이상	45	0.02	33	0.60
숙박 및 음식점업	10~49명	7,295	3.38	94	1.71
	50~249명	427	0.20	64	1.16
	250~999명	40	0.02	25	0.45
	1,000명 이상	8	0.00	6	0.11
정보통신업	10~49명	8,418	3.90	115	2.09
	50~249명	1,938	0.90	127	2.31
	250~999명	279	0.13	100	1.82
	1,000명 이상	50	0.02	43	0.78

단위: 개, %

업종 분류	규모 분류	컴퓨터 보유 / 네트워크 구축 기업체		응답 표본 현황	
		모집단 수	구성비	표본 수	구성비
금융 및 보험업	10~49명	2,787	1.29	74	1.35
	50~249명	1,124	0.52	112	2.04
	250~999명	177	0.08	95	1.73
	1,000명 이상	76	0.04	62	1.13
부동산업	10~49명	2,093	0.97	74	1.35
	50~249명	462	0.21	69	1.25
	250~999명	149	0.07	84	1.53
	1,000명 이상	52	0.02	43	0.78
전문, 과학 및 기술 서비스업	10~49명	14,216	6.58	140	2.55
	50~249명	2,878	1.33	140	2.55
	250~999명	587	0.27	147	2.67
	1,000명 이상	219	0.10	190	3.45
사업시설 관리, 사업지원 및 임대 서비스업	10~49명	2,707	1.25	82	1.49
	50~249명	770	0.36	85	1.55
	250~999명	251	0.12	91	1.65
	1,000명 이상	67	0.03	56	1.02
교육 서비스업	10~49명	4,843	2.24	85	1.55
	50~249명	811	0.38	93	1.69
	250~999명	173	0.08	80	1.45
	1,000명 이상	78	0.04	61	1.11
보건업 및 사회복지 서비스업	10~49명	35,557	16.47	196	3.56
	50~249명	6,197	2.87	184	3.35
	250~999명	714	0.33	134	2.44
	1,000명 이상	81	0.04	61	1.11
예술, 스포츠 및 여가관련 서비스업	10~49명	1,278	0.59	62	1.13
	50~249명	302	0.14	55	1.00
	250~999명	39	0.02	31	0.56
	1,000명 이상	7	0.00	6	0.11
수리 및 기타 개인 서비스업	10~49명	3,254	1.51	80	1.45
	50~249명	160	0.07	43	0.78
	250~999명	24	0.01	19	0.35
	1,000명 이상	2	0.00	2	0.04
총 합계		**215,891**	**100.00**	**5,500**	**100.00**

※ 출처: 「2024년 4분기 기준 기업통계등록부(SBR)」(통계청), 「2024년 정보화통계조사」(한국지능정보사회진흥원)

제 2 장 조사 결과 요약

Ⅰ. 정보보호 인식 | Ⅱ. 정보보호 정책 및 조직 | Ⅲ. 정보보호 교육 | Ⅳ. 정보보호 예산 | Ⅴ. 정보 침해사고 예방 | Ⅵ. 정보 침해사고 경험

Ⅰ 정보보호 인식

1 정보보호 인식

» 기업의 정보보호 중요성 인식률은 80.6%임

- 기업의 80.6%가 정보보호에 대해 '중요하다(중요한 편이다+매우 중요하다)'고 인식하고 있으며, 2024년(79.0%) 대비 1.6%p 증가함

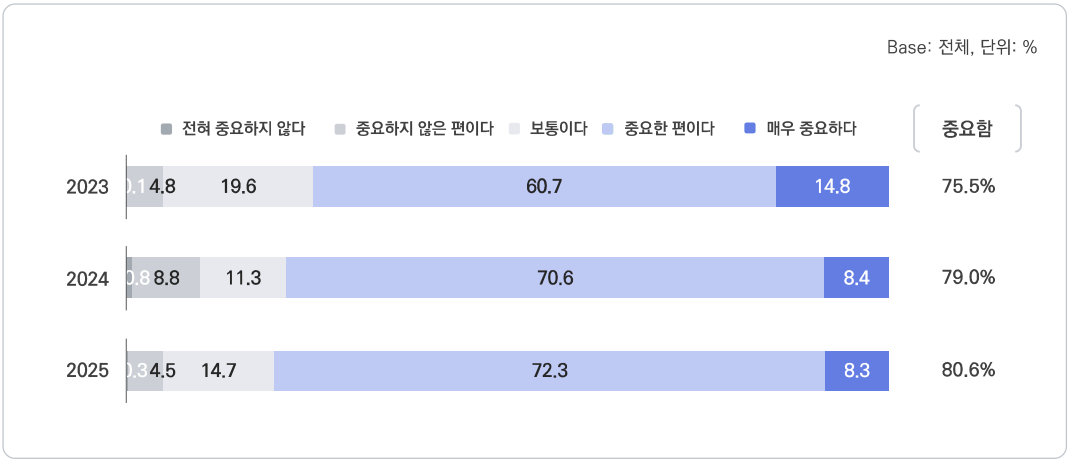


그림 1-2-1 기업의 정보보호 중요성 인식률

» 기업 경영진의 정보보호 중요성 인식률은 77.6%임

- 기업 경영진의 77.6%가 정보보호의 중요성을 인식하고 있으며, 2024년(76.0%) 대비 1.6%p 증가함

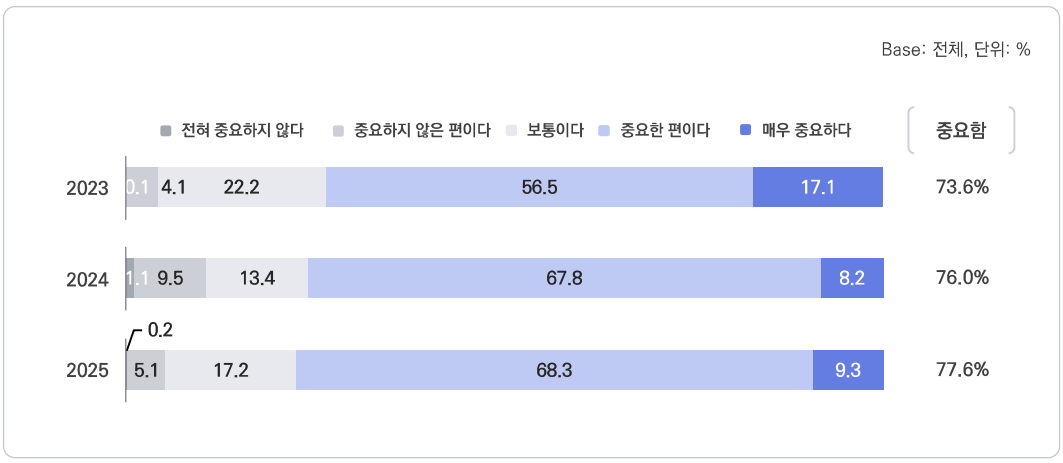


그림 1-2-2 경영진의 정보보호 중요성 인식률

» 정보보호 업무 중 가장 큰 애로사항은 '정보보호 예산 확보(49.1%)'임

- 정보보호 관련 업무 시 애로사항으로는 '정보보호 예산 확보'가 49.1%로 가장 높고, 다음으로 '정보보호 시스템 및 체계 운용 관리(45.7%)', '필요한 정보보호 제품 및 서비스 탐색(42.6%)' 등의 순임

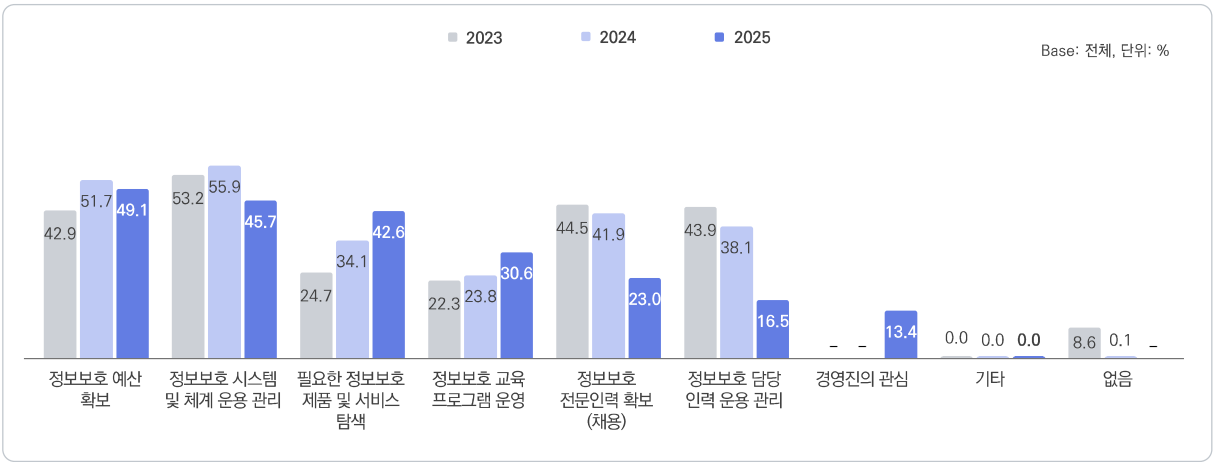


그림 1-2-3 정보보호 애로사항(1+2+3순위)

Ⅱ 정보보호 정책 및 조직

1 정보보호 정책

» 기업체의 52.6%가 정보보호 정책을 보유함

- 기업체의 정보보호 정책 보유율은 52.6%로 2024년(51.6%) 대비 1.0%p 증가함
  - 규모가 커질수록 정보보호 정책 보유율이 높음

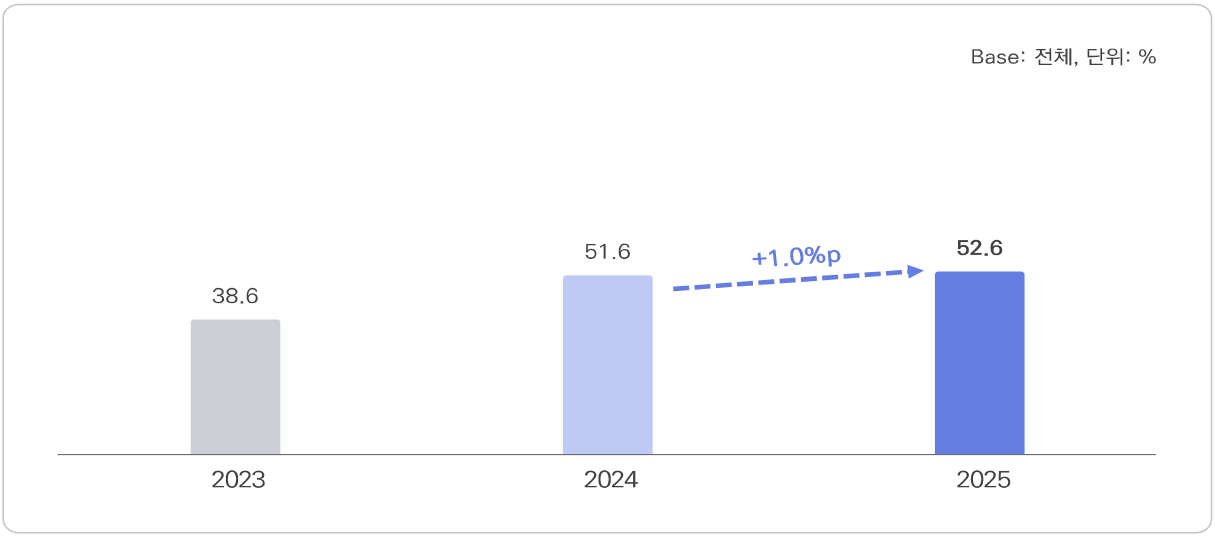


그림 1-2-4 정보보호 정책 보유율

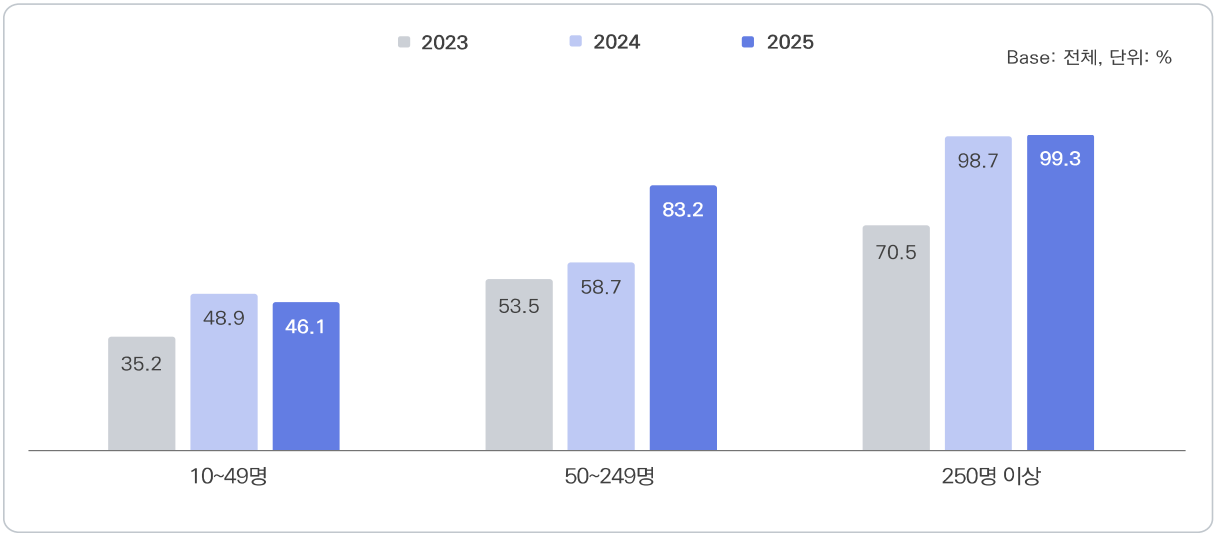
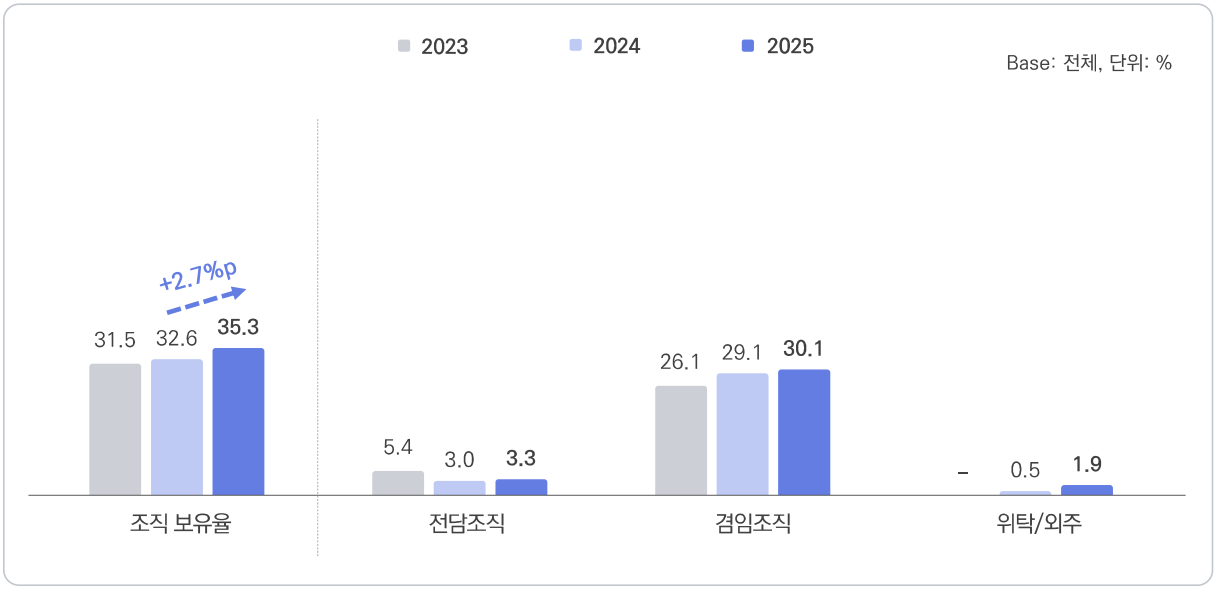


그림 1-2-5 규모별 정보보호 정책 보유율

2 정보보호 조직

» 기업체의 35.3%가 정보보호 조직을 보유함

- 기업체의 정보보호 조직 보유율은 35.3%로 2024년(32.6%) 대비 2.7%p 증가함
  - 규모가 커질수록 대체로 정보보호 조직 보유율이 높아지는 경향을 보임



※ '위탁/외주' 보기는 2024년 신설된 보기 문항

그림 1-2-6 정보보호 조직 보유율

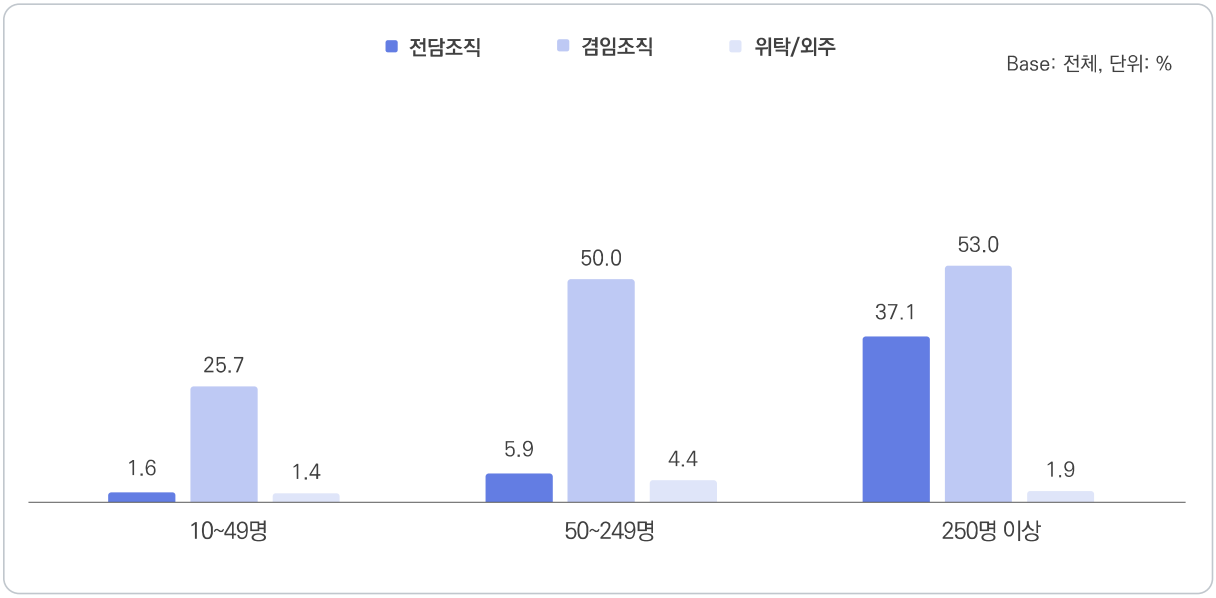


그림 1-2-7 규모별 정보보호 조직 보유율

3 정보보호 관련 인력

» 정보보호 담당 인력은 평균 1.4명이고, 대부분 내부인력임

- 기업체당 정보보호 담당 인력은 1.4명, IT 인력(주 업무: IT, 부가 업무: 정보보호)은 0.2명, 일반 사무직 인력(주 업무: 일반 사무, 부가 업무: 정보보호)은 1.3명으로 나타남
  - 2024년 대비 정보보호 담당 인력은 증가한 반면, IT 인력 및 일반 사무직 인력은 감소함

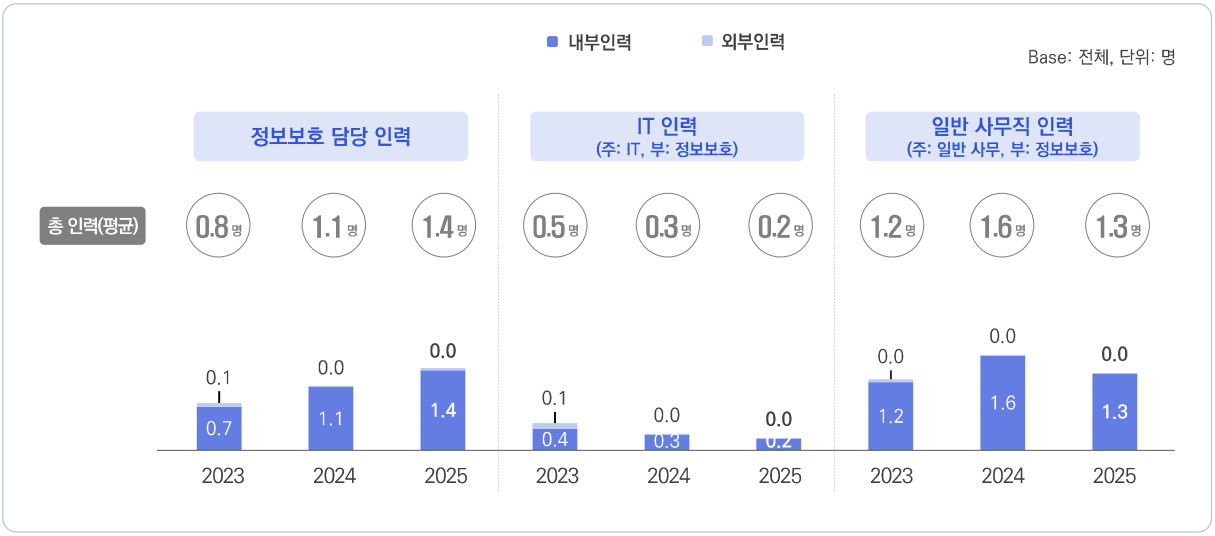


그림 1-2-8 정보보호 관련 인력(요약)

Ⅲ 정보보호 교육

» 기업체의 32.7%가 정보보호에 대해 교육함

- 기업체의 정보보호 교육 실시율은 32.7%로 2024년(36.7%) 대비 4.0%p 감소함
  - 규모가 커질수록 대체로 정보보호 교육 실시율이 높아지는 경향을 보임

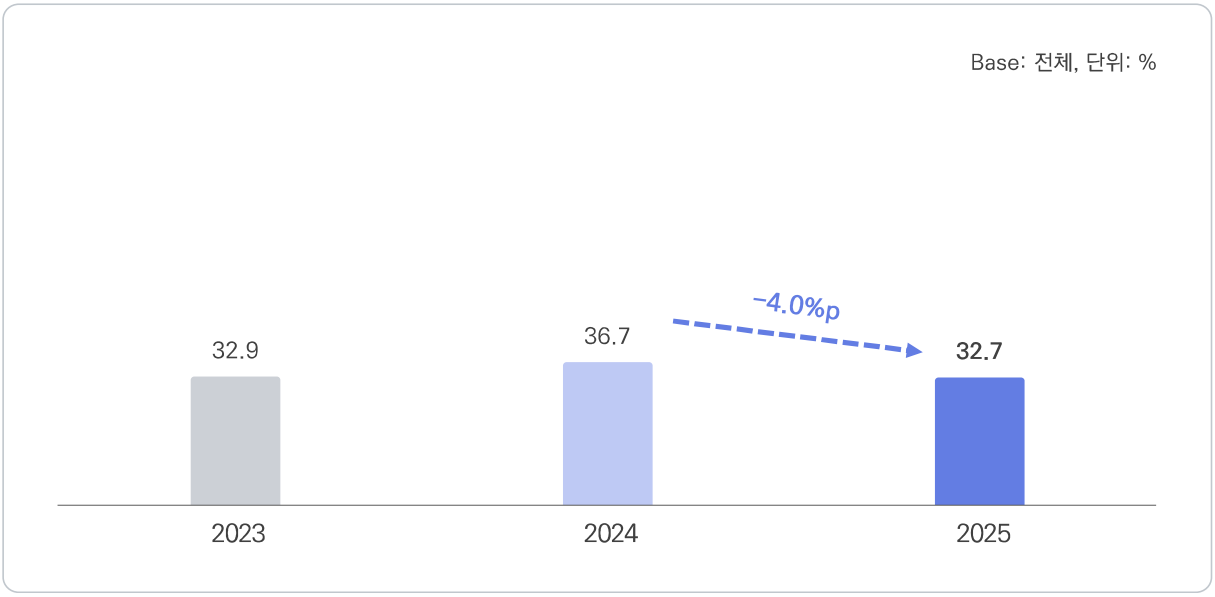


그림 1-2-9 정보보호 교육 실시

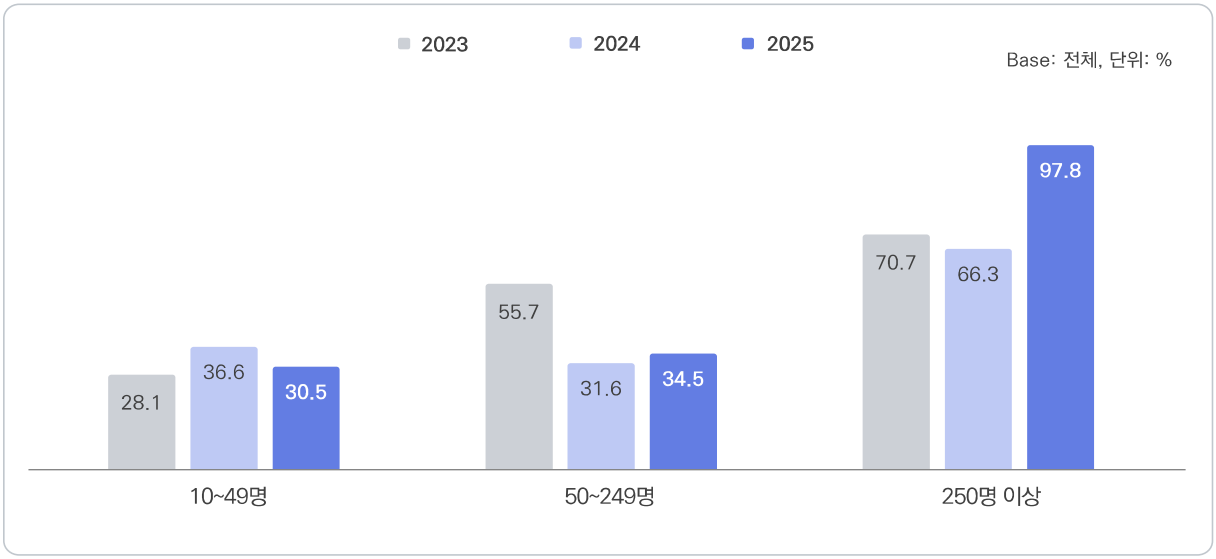


그림 1-2-10 규모별 정보보호 교육 실시

Ⅳ 정보보호 예산

기업체의 54.8%가 정보보호 예산을 사용하고, 그 중 70.4%가 1년간 '500만 원 미만' 정도 예산을 사용함

- 기업체의 정보보호 예산 사용률은 54.8%로 2024년(49.9%) 대비 4.9%p 증가함
- 정보보호 예산을 사용한 기업체 중 70.4%가 예산 총액이 '500만 원 미만'인 것으로 나타남

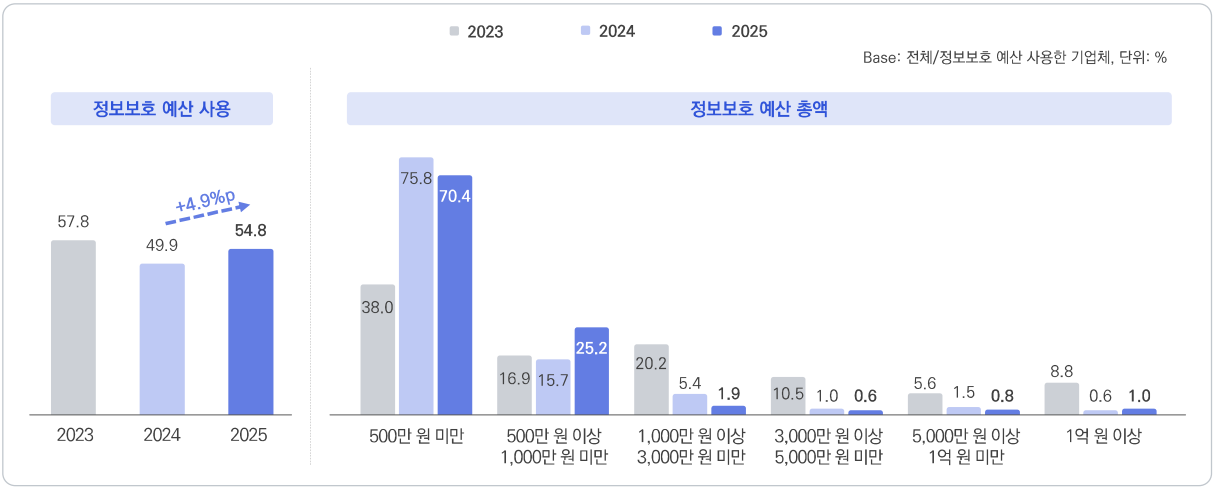


그림 1-2-11 정보보호 예산 사용 및 총액

1년간 정보보호 예산 활용 비중이 가장 큰 유형은 '정보보호 제품 및 솔루션의 유지·보수(78.0%)'임

- 정보보호 예산을 활용한 유형으로는 '정보보호 제품 및 솔루션의 유지·보수'가 78.0%로 가장 높고, 다음으로 '업무 시설의 CCTV 등 영상 감시 장비 설치 또는 증설(유지·보수 포함)(57.4%)', '정보보호 제품 및 솔루션의 구입(28.6%)' 등의 순임

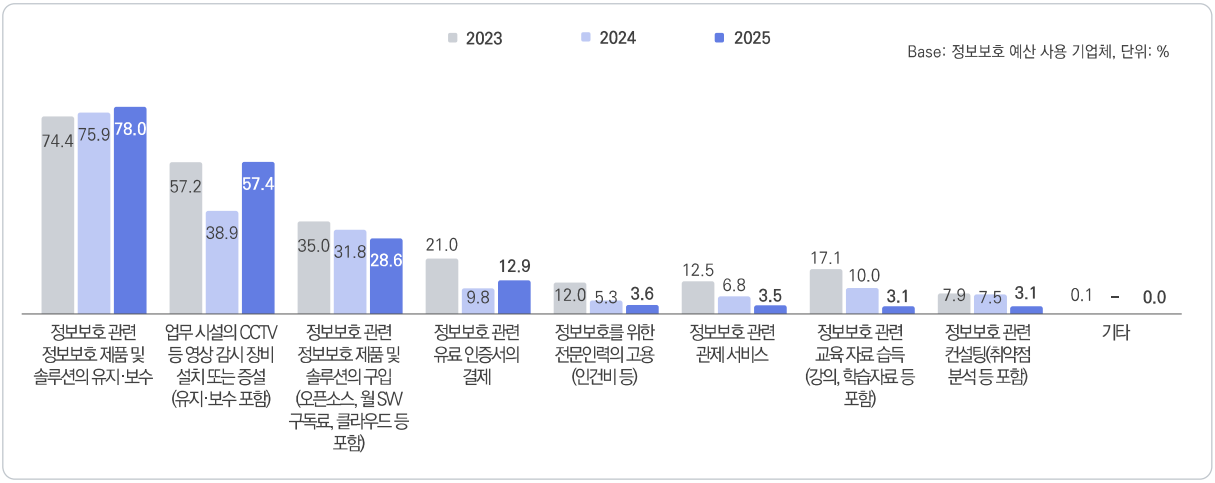


그림 1-2-12 정보보호 예산 활용 유형(1+2+3순위)

V 정보 침해사고 예방

1 정보보호 제품 및 서비스

» 기업체의 98.7%가 정보보호 제품 및 서비스를 이용함

- 기업체의 정보보호 제품 및 서비스 이용률은 98.7%로 2024년(98.1%) 대비 0.6%p 증가함

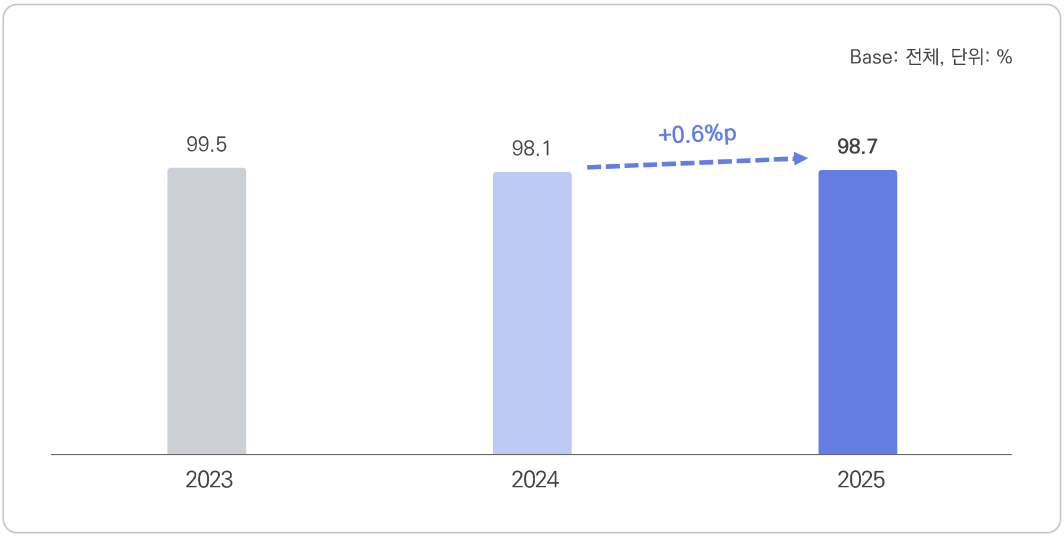


그림 1-2-13 정보보호 제품 및 서비스 이용

» 정보보안 제품 및 서비스 이용률 1위는 '네트워크 보안(94.5%)'임

- 이용하는 정보보안 제품 및 서비스로는 '네트워크 보안'이 94.5%로 가장 높고, 다음으로 '시스템(앤드포인트) 보안(94.1%)', '공통 인프라 보안(49.2%)' 등의 순임

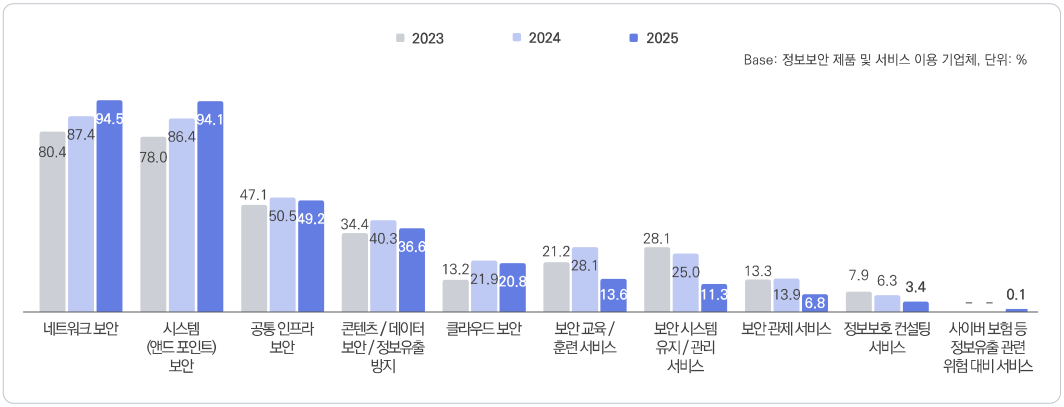


그림 1-2-14 이용하는 정보보호 제품 및 서비스_정보보안(복수응답)

» 물리적 보안 제품 및 서비스 이용률 1위는 '영상 보안 시스템(96.1%)'임

- 이용하는 물리적 보안 제품 및 서비스로는 '영상 보안 시스템'이 96.1%로 가장 높고, 다음으로 '출동 보안 서비스(89.4%)', '출입 통제 관리 시스템(84.9%)', '불법 도·감청 탐지 서비스(0.3%)'의 순임

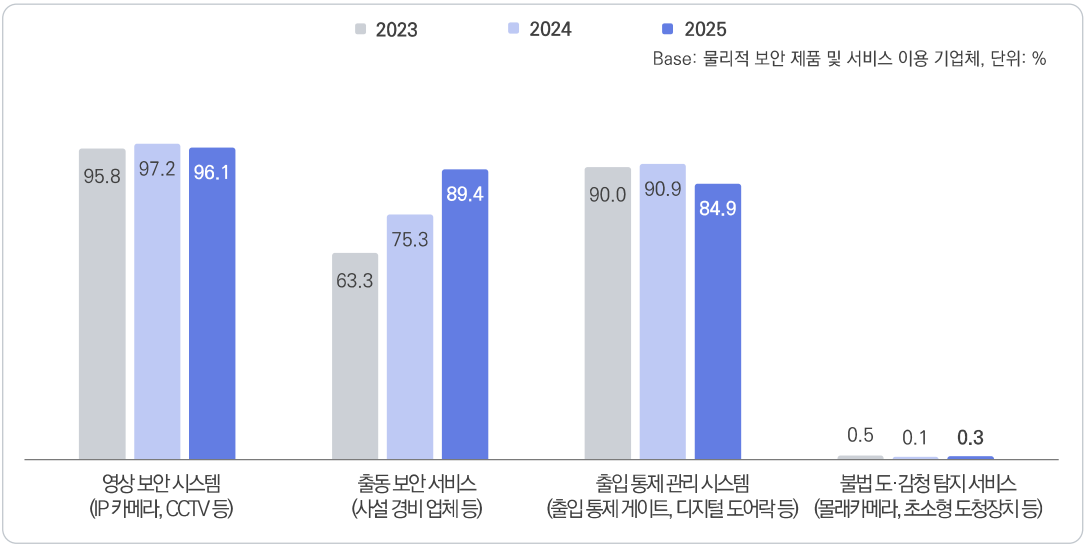


그림 1-2-15 이용하는 정보보호 제품 및 서비스_물리적 보안(복수응답)

2 사내 IT 시스템 및 네트워크 보안 점검

» 기업체의 88.1%가 사내 IT 시스템 및 네트워크 보안을 점검함

- 기업체의 사내 IT 시스템 및 네트워크 보안 점검 실시율은 88.1%로 2024년(82.4%) 대비 5.7%p 증가함
  - 보안 점검 시기는 '1개월 이상 6개월 미만'이 29.1%로 가장 높음

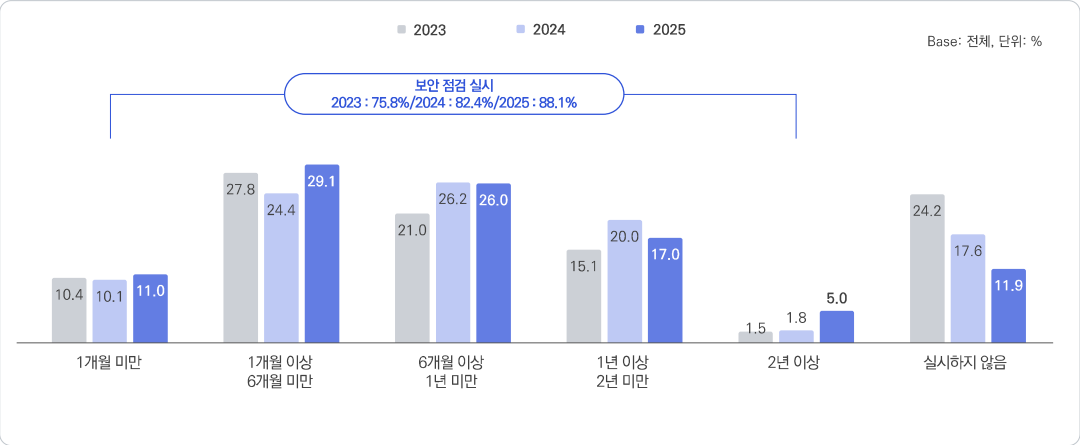


그림 1-2-16 사내 IT 시스템 및 네트워크 보안 점검

3 백업 실시

» 기업체의 99.0%가 데이터를 백업함

- 기업체의 데이터 백업 실시율은 99.0%로 2024년(99.2%) 대비 0.2%p 감소함
  - 데이터 유형 중 '중요 데이터'의 백업 실시율이 94.0%로 가장 높음

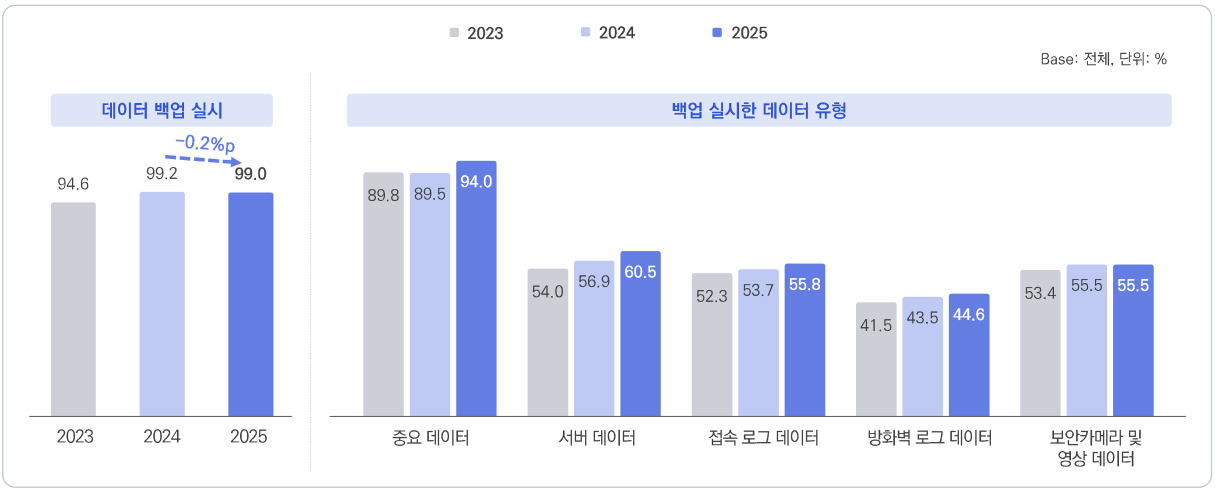


그림 1-2-17 데이터 백업 실시 및 유형(복수응답)

Ⅵ 정보 침해사고 경험

1 정보 침해사고 경험

» 기업체의 0.3%는 정보 침해사고를 의심한 경험이 있고, 0.2%는 정보 침해사고를 직접 경험함

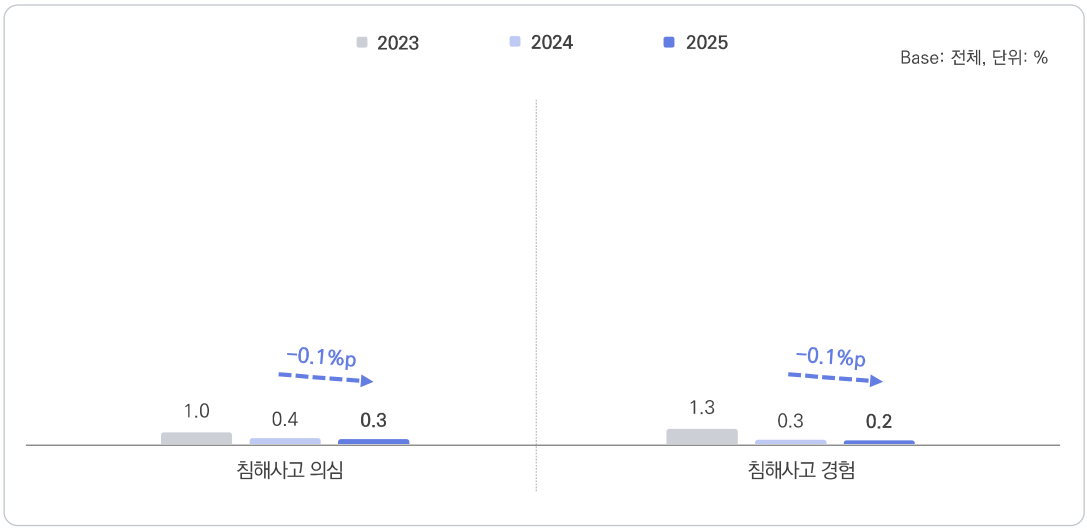


그림 1-2-18 정보 침해사고 의심 및 경험

» 정보 침해사고 중 '외부로부터 침투한 비인가 접근(해킹)(73.0%)' 유형이 가장 많음

- 경험한 정보 침해사고의 유형으로는 '외부로부터 침투한 비인가 접근(해킹)(73.0%)'이 가장 높고, 다음으로 '컴퓨터 바이러스, 웜, 트로이잔, APT 공격으로 인한 IT시스템 마비(30.6%)', '랜섬웨어 감염(20.0%)' 등의 순임

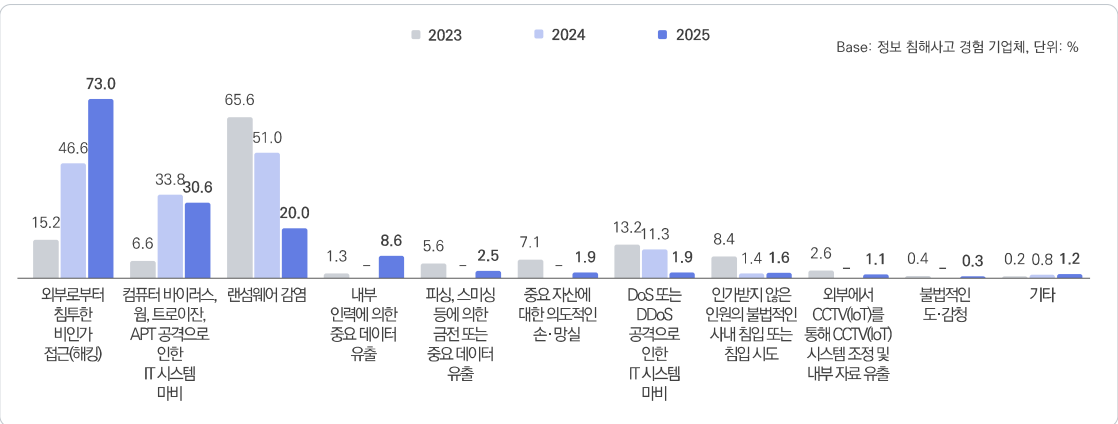


그림 1-2-19 정보 침해사고 경험 유형(복수응답)

2 정보 침해사고 대응

» 정보 침해사고 경험 후 신고한 비율은 31.4%임

- 정보 침해사고를 경험한 기업체 중 관련 기관 또는 수사 기관에 침해사고를 신고한 비율은 31.4%로 2024년(19.6%) 대비 11.8%p 증가함
  - 침해사고를 신고하지 않은 이유로는 '피해 규모가 경미하기 때문에'가 89.2%로 가장 높고, 다음으로 '신고에 따른 업무가 복잡하기 때문에(41.2%)', '피해 사실이 알려지는 것이 두렵기 때문에(8.4%)' 등의 순임

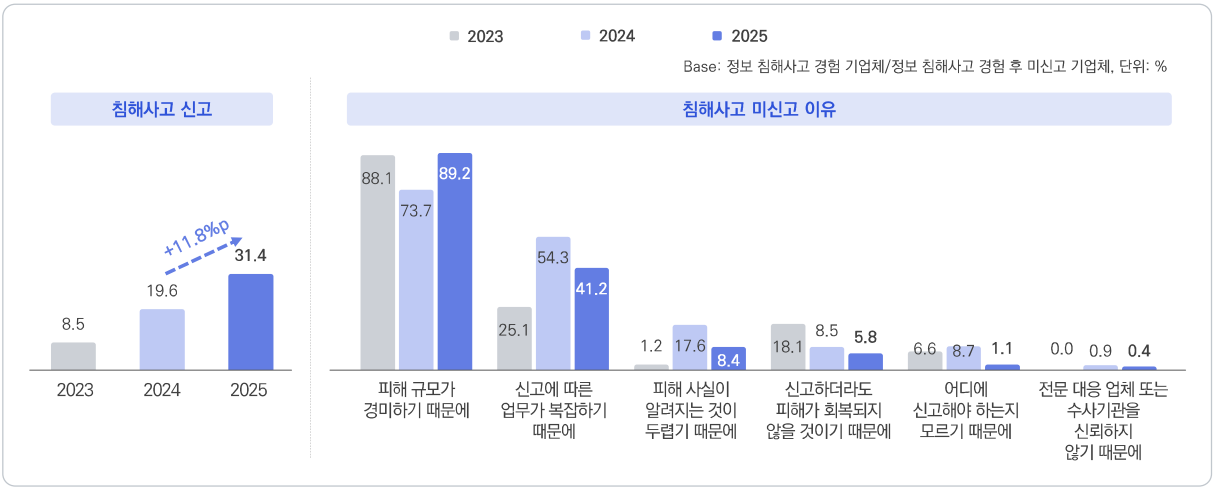


그림 1-2-20 정보 침해사고 신고 및 미신고 이유(1+2순위)

» 정보 침해사고 경험 후 대응한 비율은 58.6%임

- 정보 침해사고를 경험한 기업체 중 침해사고 경험 후 대응한 비율은 58.6%로 2024년(32.3%) 대비 26.3%p 증가함
  - 정보 침해사고 대응 활동으로는 '정보보호 관련 제품 및 솔루션 구축 및 고도화'가 31.5%로 가장 높고, 다음으로 '내부 정보보호 정책 수립 또는 수정(29.2%)' 등의 순임

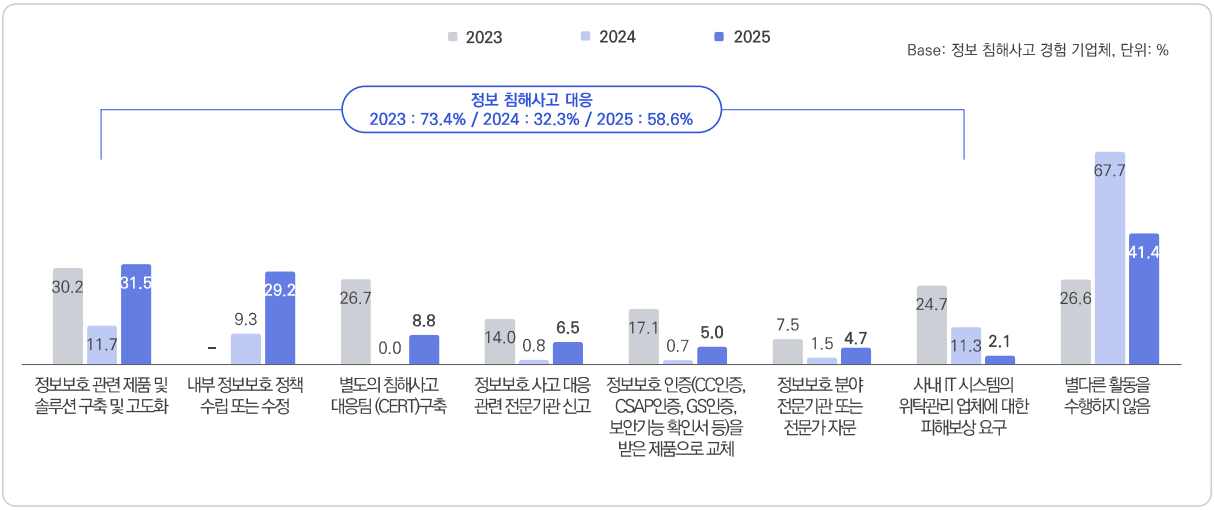


그림 1-2-21 정보 침해사고 대응(복수응답)

제 3 장 조사 결과

Ⅰ. 정보보호 인식 | Ⅱ. 정보보호 정책 및 조직 | Ⅲ. 정보보호 교육 | Ⅳ. 정보보호 예산 |
Ⅴ. 정보 침해사고 예방 | Ⅵ. 정보 침해사고 경험 | Ⅶ. 사이버 보험 | Ⅷ. 원격근무

I 정보보호 인식

1 IT 기술 중요성 인식

- 기업체 중 49.4%가 영위하고 있는 사업 분야에 IT 관련 기술이 '중요하다(중요한 편이다+매우 중요하다)'고 응답함

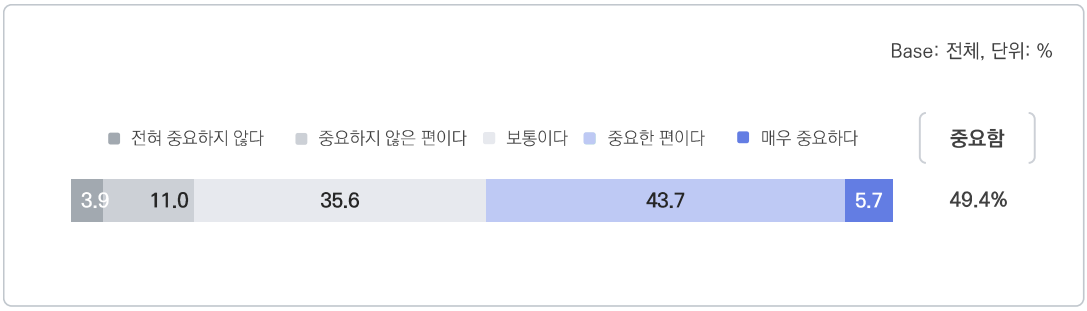


그림 1-3-1 IT 기술 중요성 인식률

2 정보보호 중요성 인식

- 기업체 중 80.6%가 기업의 정보보호가 '중요하다(중요한 편이다+매우 중요하다)'고 응답함

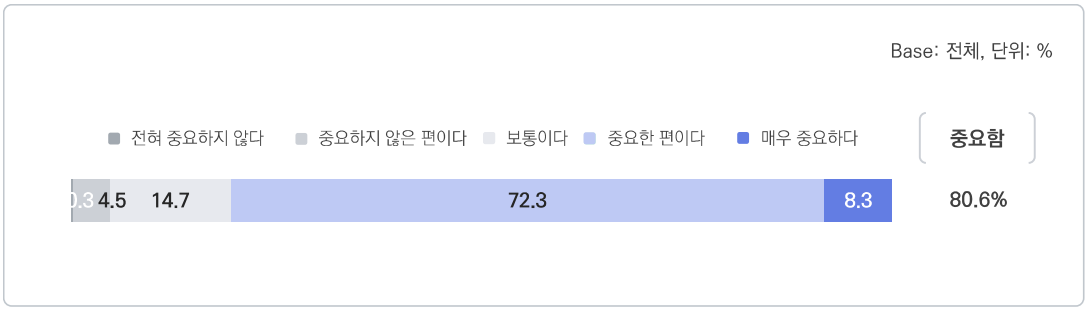


그림 1-3-2 정보보호 중요성 인식률

3 경영진의 정보보호 중요성 인식

- 기업체 중 77.6%가 경영진이 기업의 정보보호가 '중요하다(중요한 편이다+매우 중요하다)'고 응답함

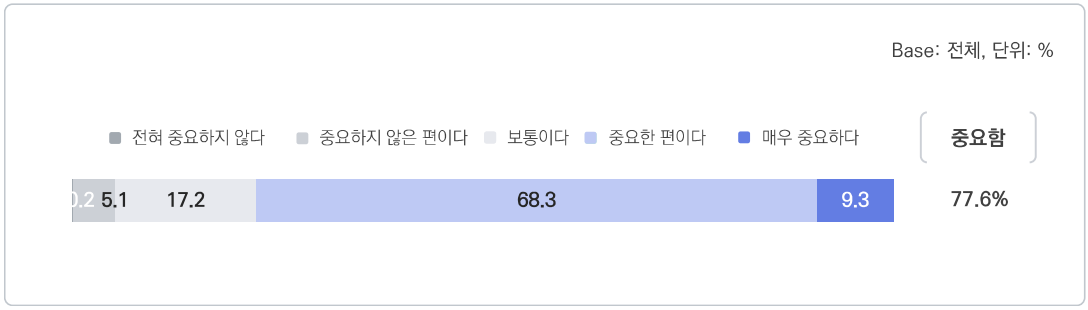


그림 1-3-3 경영진의 정보보호 중요성 인식률

4 정보보호 위협요인

- 우려하는 정보보호 위협요인으로는 '고객 개인정보 유출 위협'이 37.0%로 가장 높고, 다음으로 '인터넷을 통한 사내 전산 시스템 침해사고 위협(34.8%)', '내부 영업정보 및 데이터 손·망실(32.5%)' 등의 순임

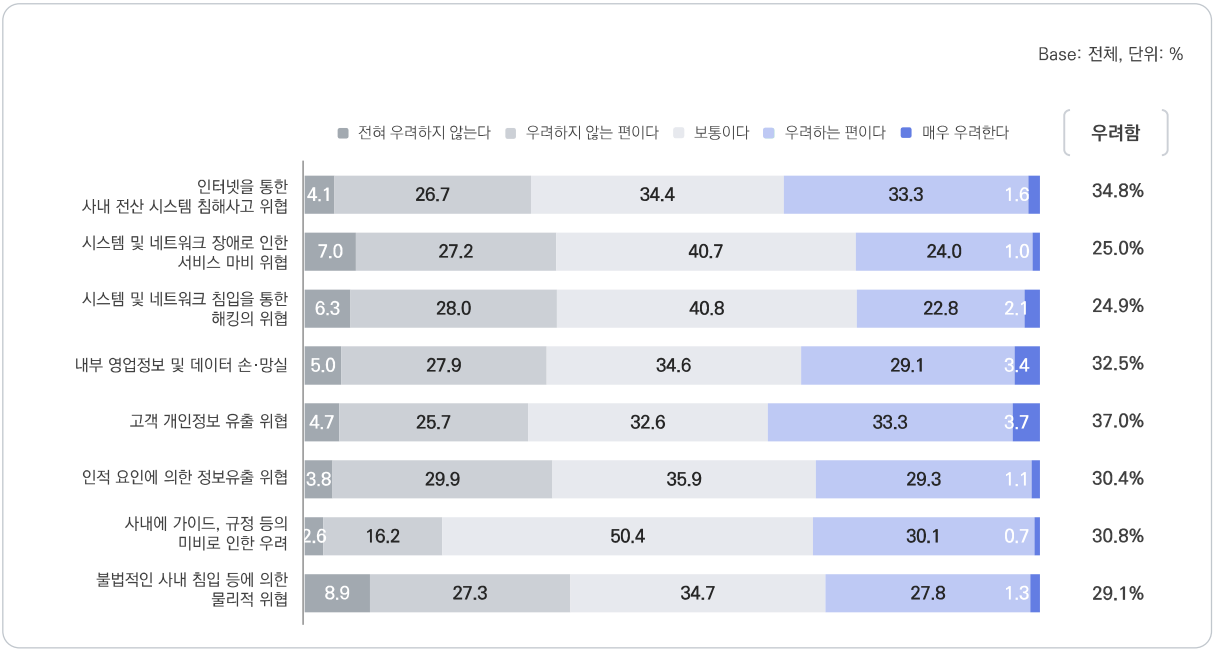


그림 1-3-4 정보보호 위협요인 우려 정도

5 정보보호 애로사항

- 정보보호 관련 업무 시 느끼는 애로사항으로는 '정보보호 예산 확보'가 49.1%로 가장 높고, 다음으로 '정보보호 시스템 및 체계 운용 관리(45.7%)', '필요한 정보보호 제품 및 서비스 탐색(42.6%)' 등의 순임

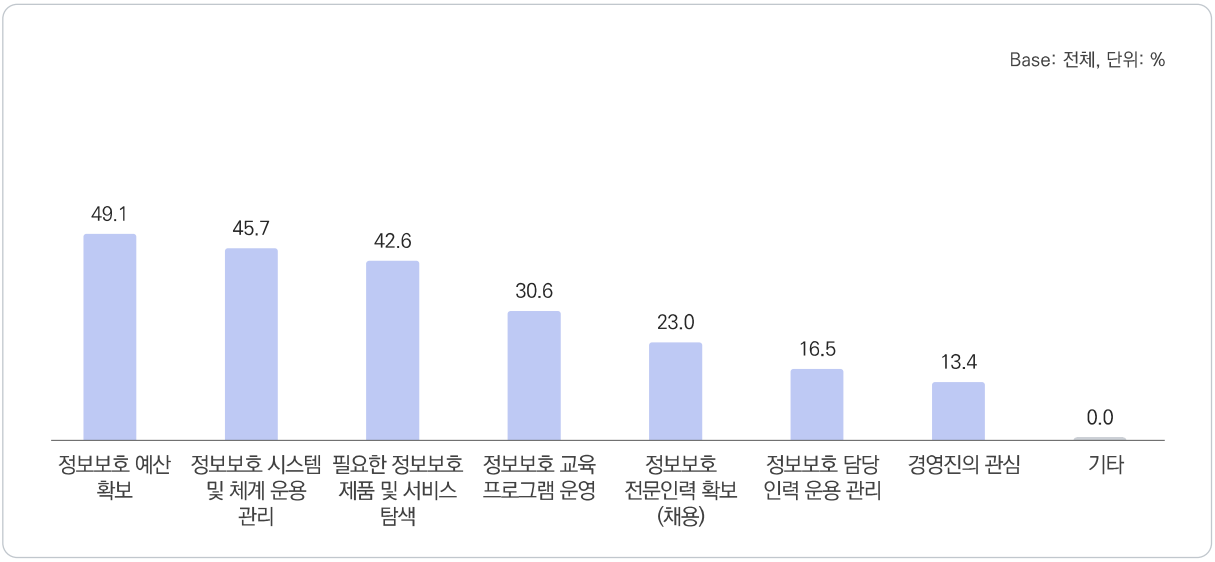


그림 1-3-5 정보보호 애로사항(1+2+3순위)

6 정보보호 규정 적용의 엄격함 정도

- 기업체의 53.4%는 정보보호 관련 규정을 제정, 변경 또는 강화하였을 때 해당 사항을 조직 구성원에게 '엄격하게 적용한다(엄격하게 적용할 것이다+매우 엄격하게 적용할 것이다)'고 응답함

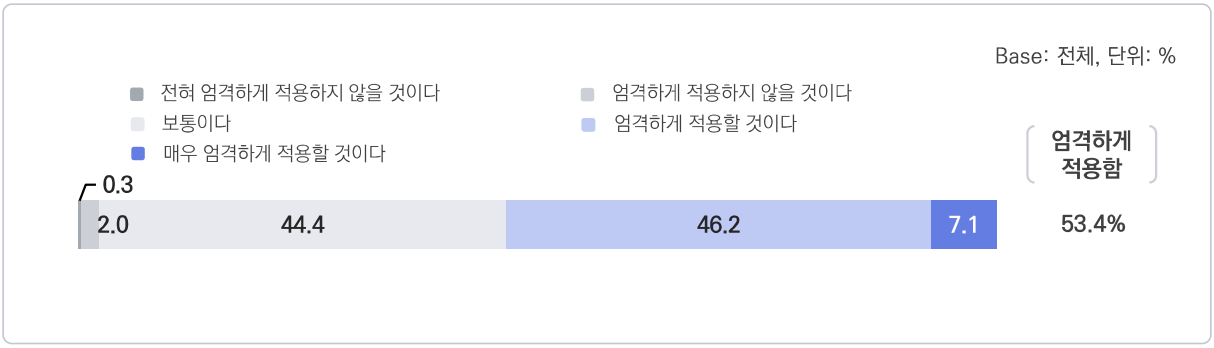


그림 1-3-6 정보보호 규정 적용의 엄격함 정도

Ⅱ 정보보호 정책 및 조직

1 정보보호 정책

가 정보보호 정책 보유

- 기업체 중 52.6%가 공식 문서로 작성된 사내 정보보호 정책 또는 규정집을 보유하고 있다고 응답함

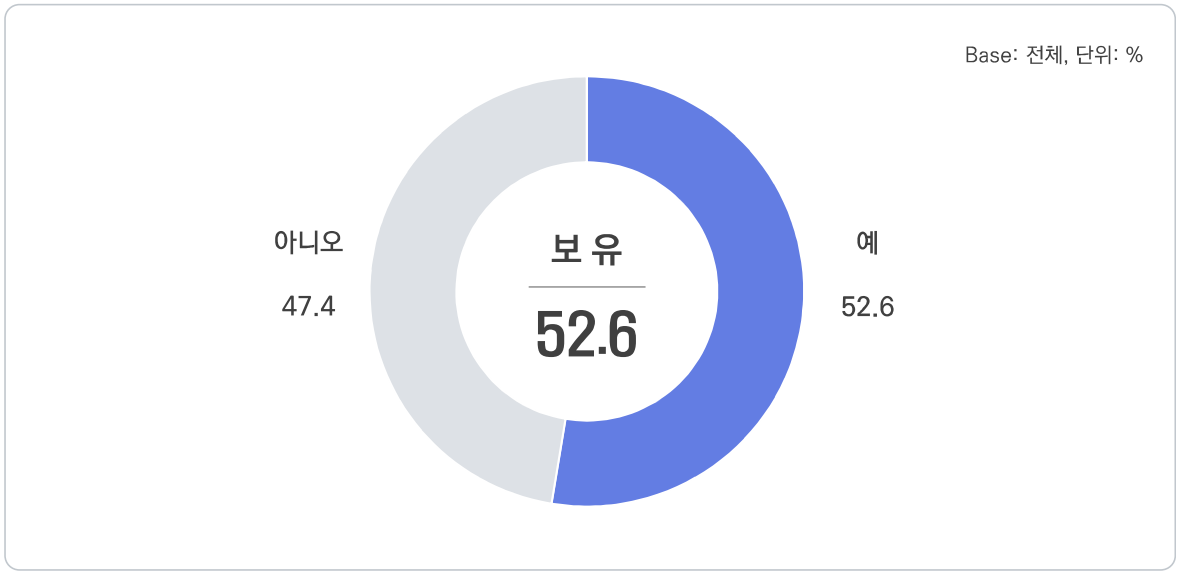


그림 1-3-7 정보보호 정책 보유율

- 업종별로 보면 '금융 및 보험업'의 정보보호 정책 보유율이 92.7%로 가장 높고, 다음으로 '정보통신업(70.5%)', '전문, 과학 및 기술 서비스업(64.5%)' 등의 순임

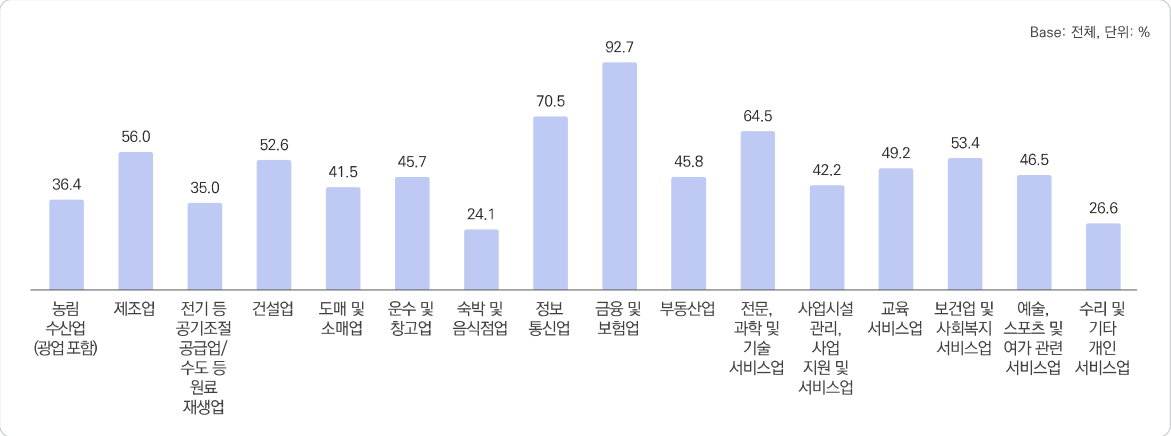


그림 1-3-8 **업종별 정보보호 정책 보유율**

- 규모가 클수록 정보보호 정책 보유율이 높음

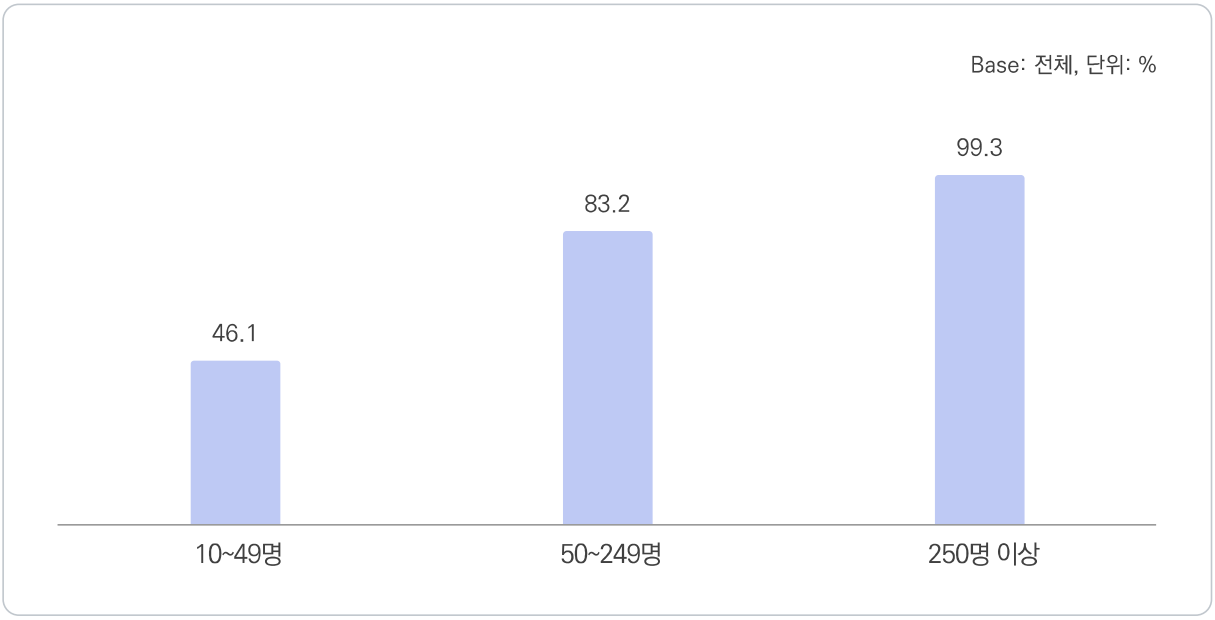


그림 1-3-9 **규모별 정보보호 정책 보유율**

나 정보보호 정책 중 개인정보보호 포함 여부

- 정보보호 정책을 보유한 기업체 중 56.7%는 정보보호 정책에 개인정보보호 관련 규정이 포함되어 있다고 응답함

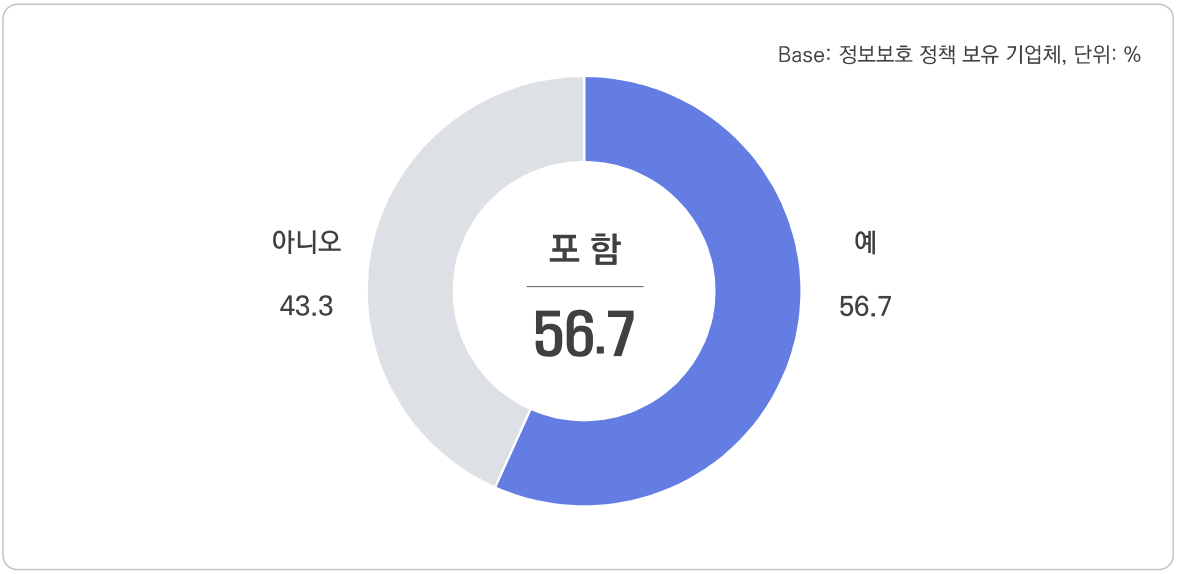


그림 1-3-10 정보보호 정책 중 개인정보보호 포함 여부

- 업종별로 보면 '금융 및 보험업'의 정보보호 정책 보유율이 92.9%로 가장 높고, 다음으로 '운수 및 창고업(78.9%)', '사업시설 관리, 사업 지원 및 서비스업(75.9%)' 등의 순임

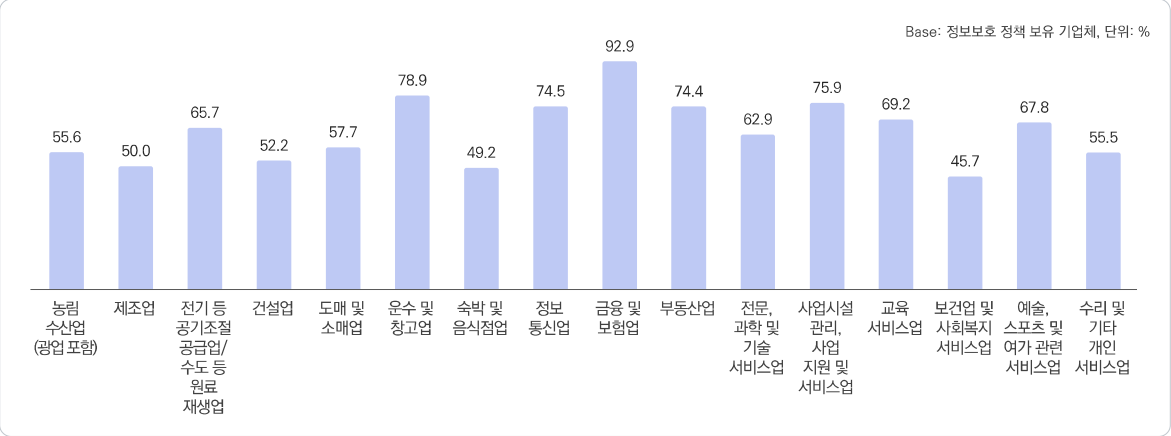


그림 1-3-11 업종별 정보보호 정책 중 개인정보보호 포함 여부

- 규모가 클수록 정보보호 정책 중 개인정보보호 규정 포함률이 높음

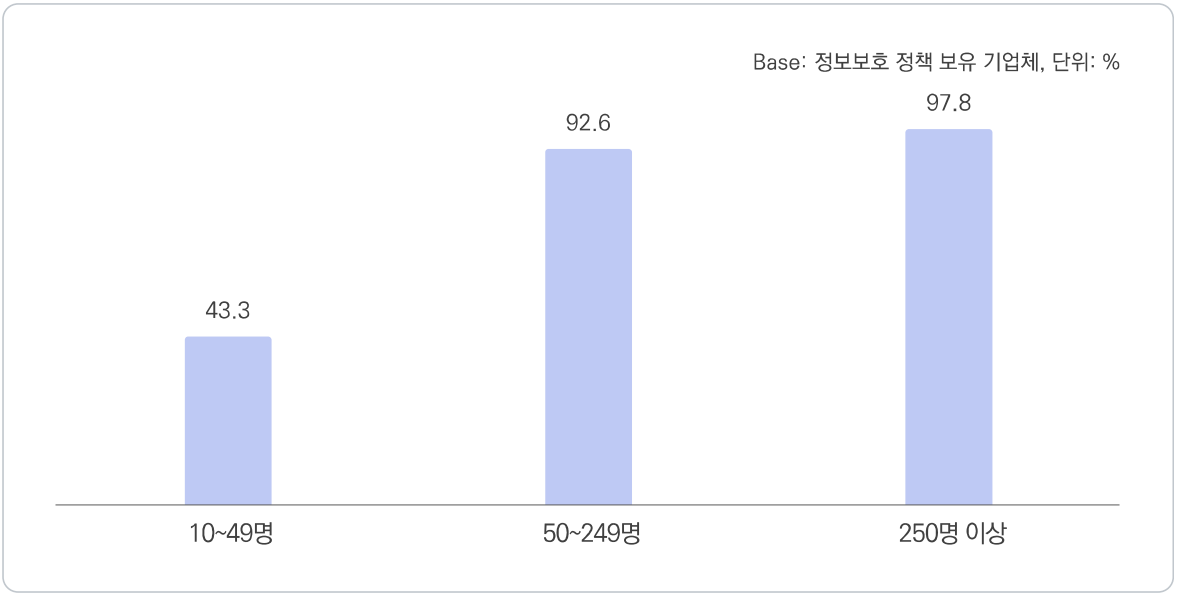


그림 1-3-12 규모별 정보보호 정책 중 개인정보보호 포함 여부

2 정보보호 조직

- 기업체의 79.9%가 정보보호 업무를 수행하는 것으로 나타남

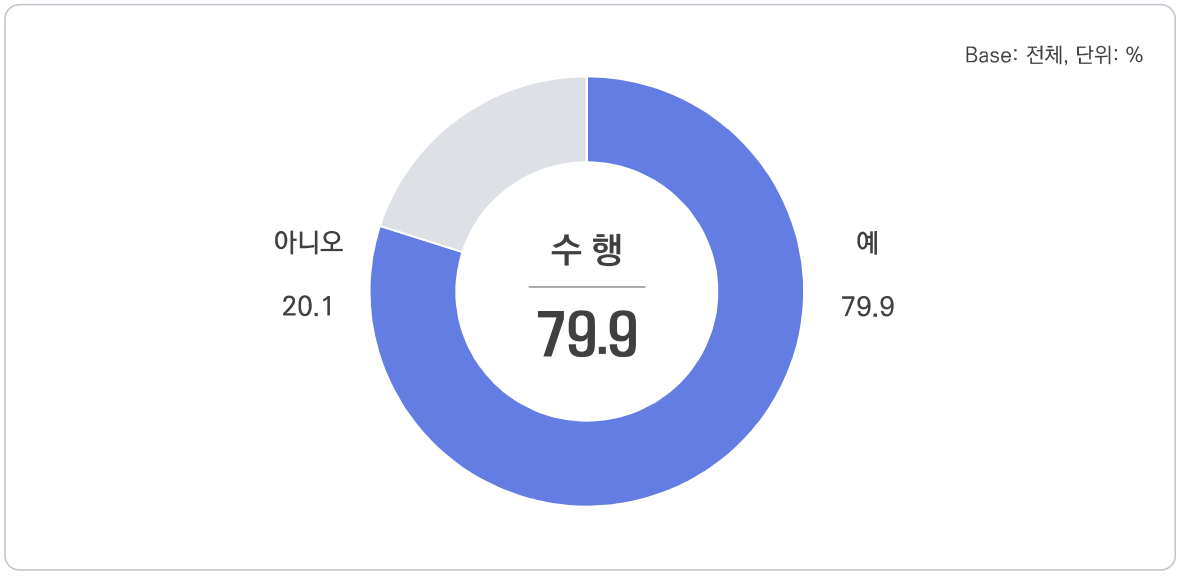


그림 1-3-13 정보보호 업무 수행 여부

- 기업체의 정보보호 조직 보유율은 35.3%로 나타남
  - 전담조직 보유율은 3.3%, 겸임조직 보유율은 30.1%, 위탁/외주조직 보유율은 1.9%임

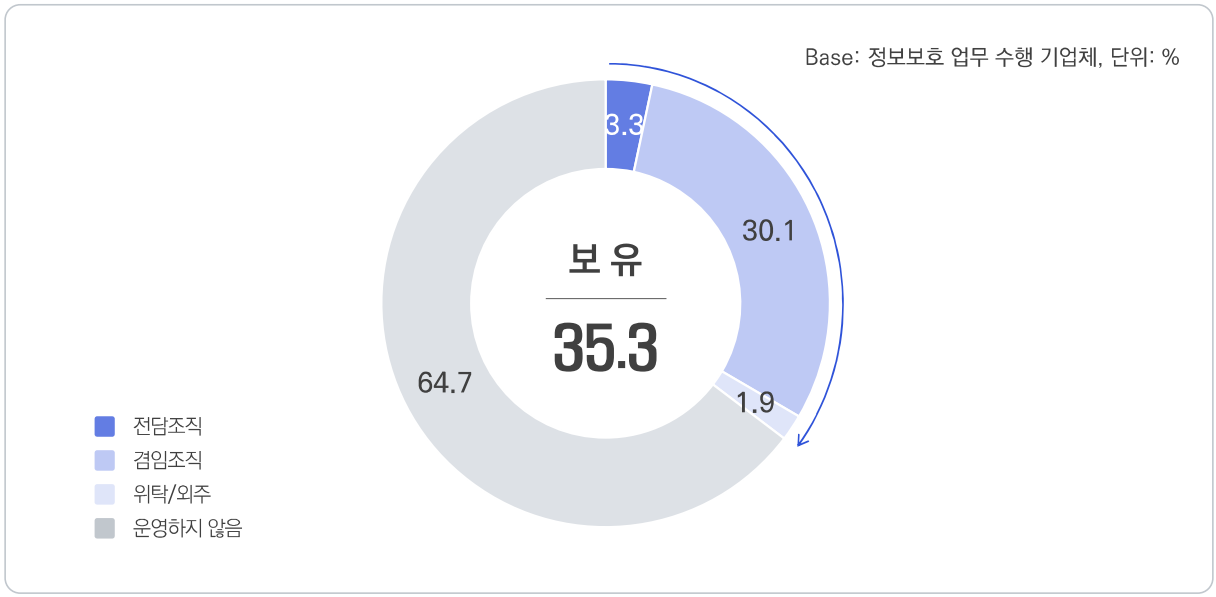


그림 1-3-14 정보보호 조직 보유율

- 업종별로 보면 '정보통신업'의 전담조직 보유율(11.8%), '금융 및 보험업'의 겸임조직 보유율(62.2%)이 가장 높음

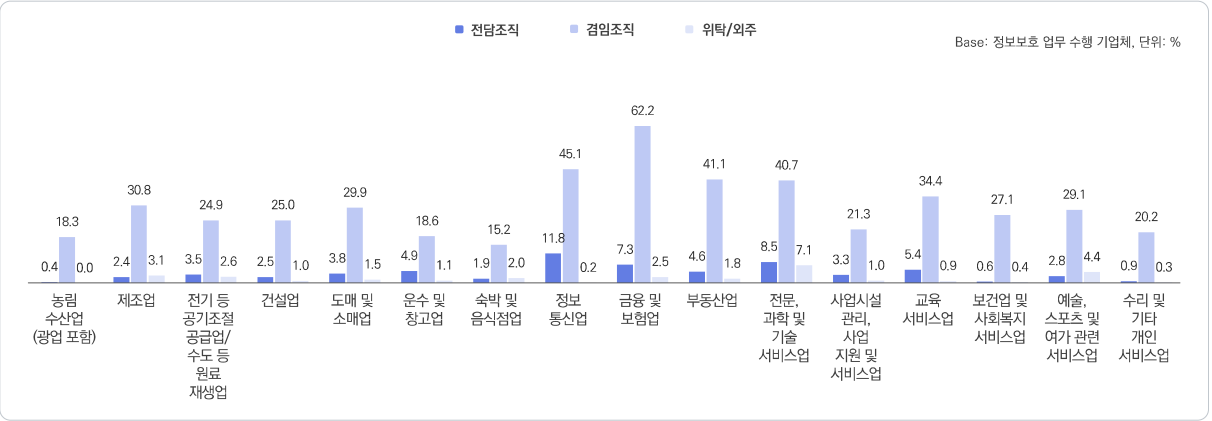


그림 1-3-15 업종별 정보보호 조직 보유율

- 규모가 '250명 이상'인 경우 전담조직 보유율이 37.1%, 겸임조직 보유율이 53.0%로 가장 높음
  - 한편, 위탁/외주 보유율은 '50~249명'에서 4.4%로 가장 높게 나타남

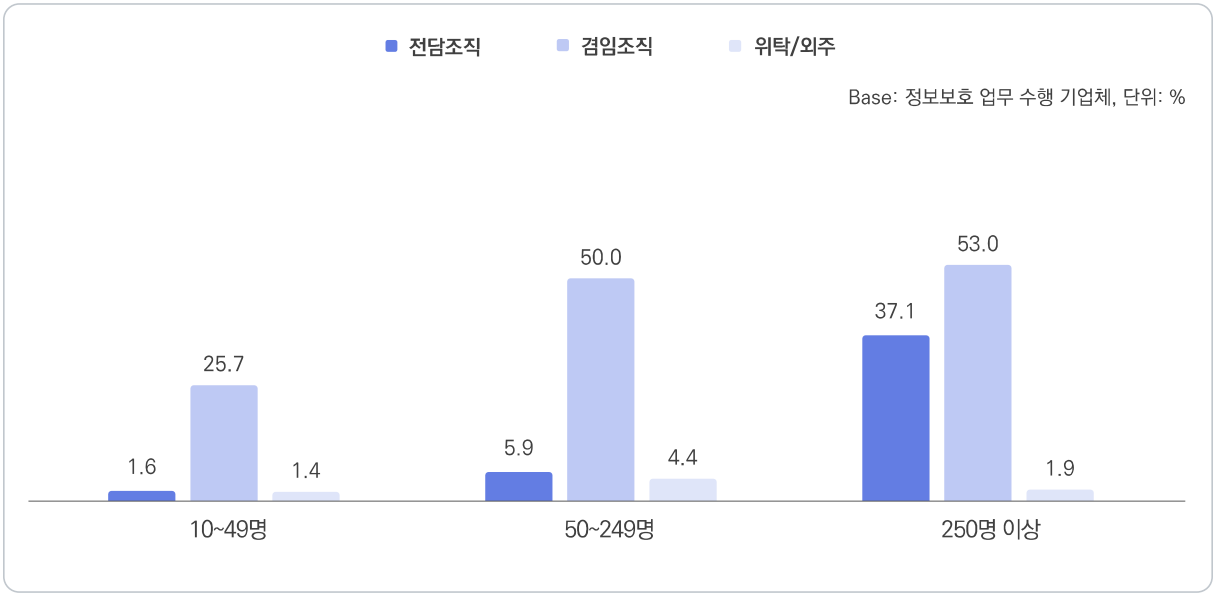


그림 1-3-16 규모별 정보보호 조직 보유율

- 전담조직 혹은 겸임조직 형태로 정보보호 업무를 담당하는 기업체 중 5.1%가 정보보호 조직 운영하는 데에 있어 위탁/외주를 병행하는 것으로 나타남

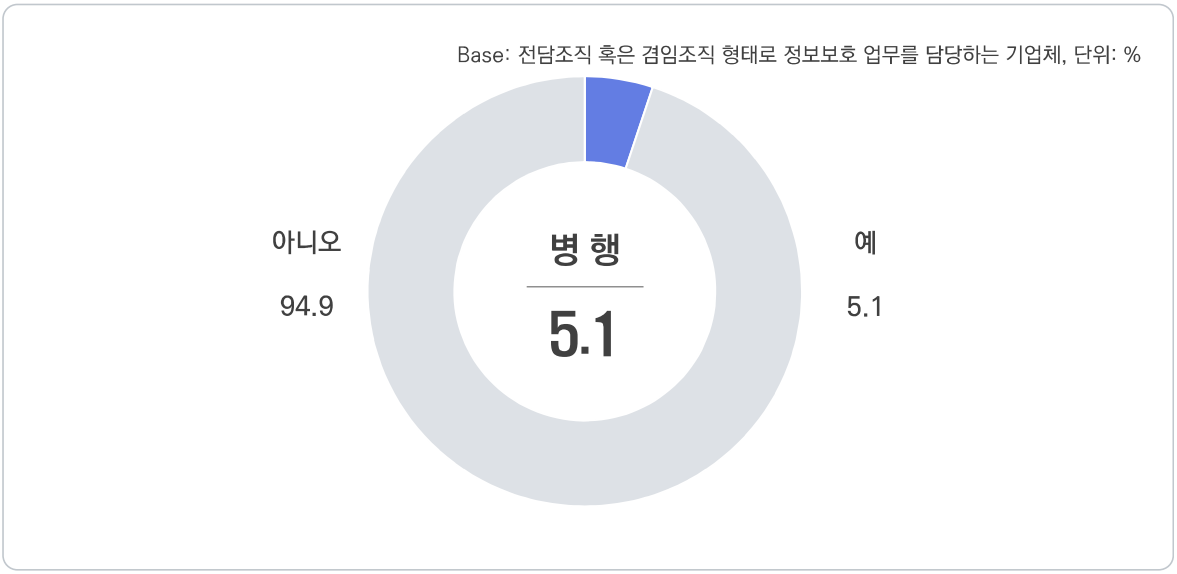


그림 1-3-17 정보보호 조직 운영 외탁/외주 병행 여부

3 정보보호 인력

가 정보보호 관련 인력

- 기업체의 정보보호 담당 인력은 1.4명(내부인력 1.4명, 외부인력 0.0명)으로 나타남
- 주 업무가 IT이고 부가 업무가 정보보호인 IT 인력은 0.2명(내부인력 0.2명, 외부인력 0.0명)으로 나타남
- 주 업무가 일반 사무이고 부가 업무가 정보보호인 일반 사무직 인력은 1.3명(내부인력 1.3명, 외부인력 0.0명)으로 나타남

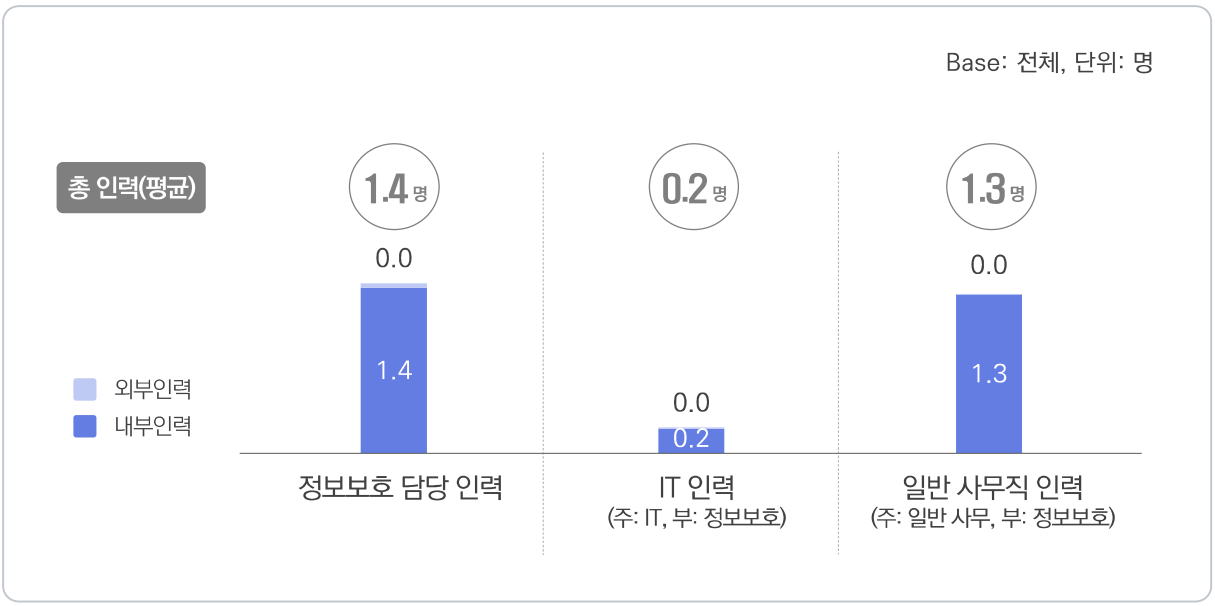


그림 1-3-18 정보보호 관련 인력(요약)

- 업종별로 보면 '금융 및 보험업'의 정보보호 담당 인력이 1.8명으로 가장 많음

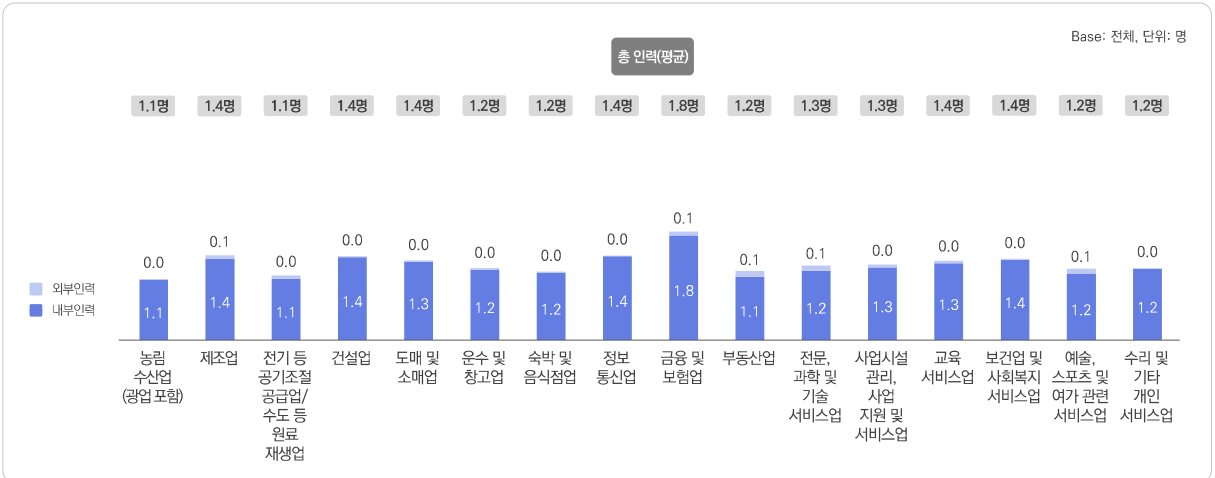


그림 1-3-19 업종별 정보보호 담당 인력

- 규모별로 보면 종사자 규모 '250명 이상'의 정보보호 담당 인력이 4.4명(내부인력 4.0명, 외부인력 0.5명)으로 가장 많음

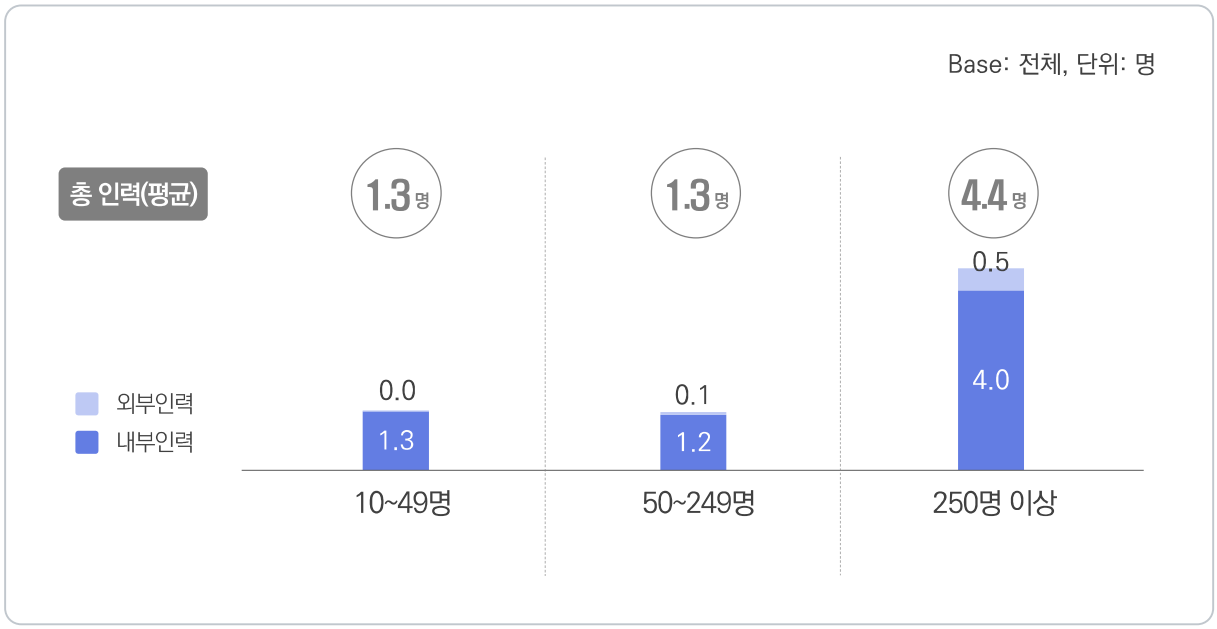


그림 1-3-20 규모별 정보보호 담당 인력

- 업종별로 보면 '정보통신업'의 정보보호 업무를 부가적으로 하는 IT 인력이 0.5명으로 가장 많음

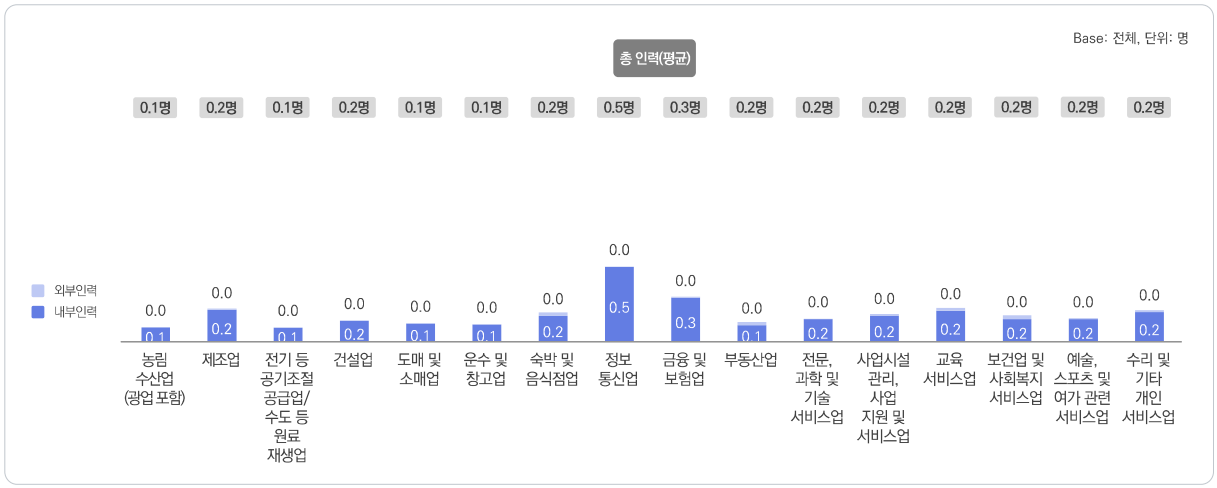


그림 1-3-21 업종별 IT 인력(주 업무 : IT, 부가 업무 : 정보보호)

- 규모별로 보면 종사자 규모 '250명 이상'의 정보보호 업무를 부가적으로 하는 IT 인력이 1.2명(내부인력 1.1명, 외부인력 0.1명)으로 가장 많음

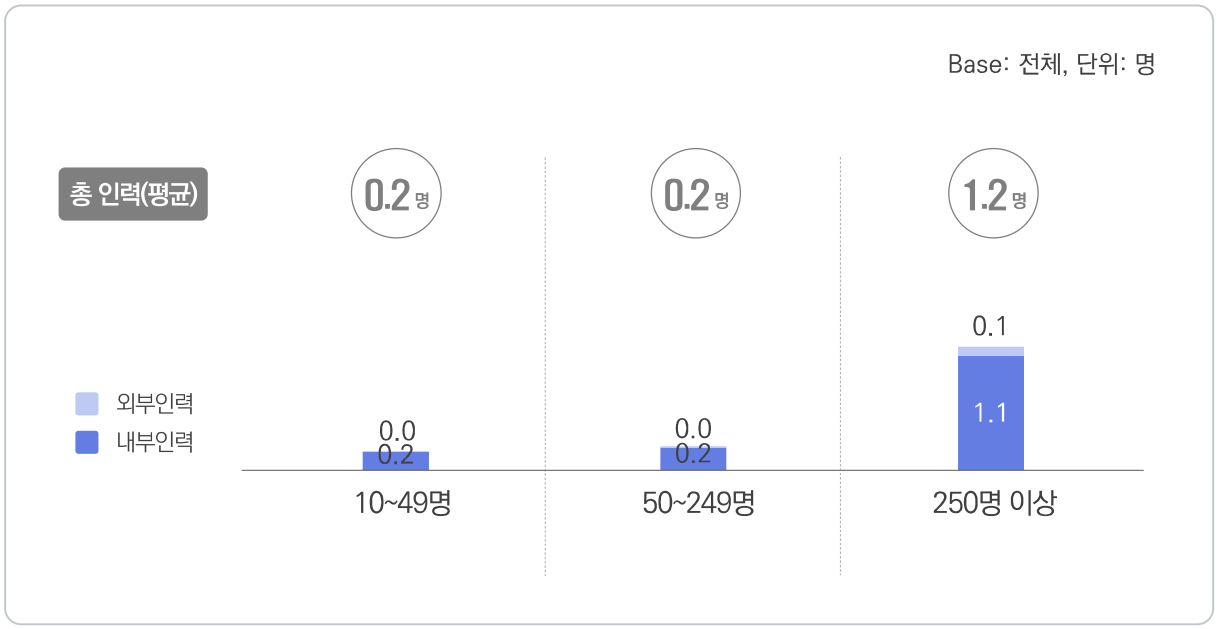


그림 1-3-22 규모별 IT 인력(주 업무 : IT, 부가 업무 : 정보보호)

- 업종별로 보면 '운수 및 창고업'의 정보보호 업무를 부가적으로 하는 일반 사무직 인력(내부인력 1.5명, 외부인력 0.0명)이 가장 많음

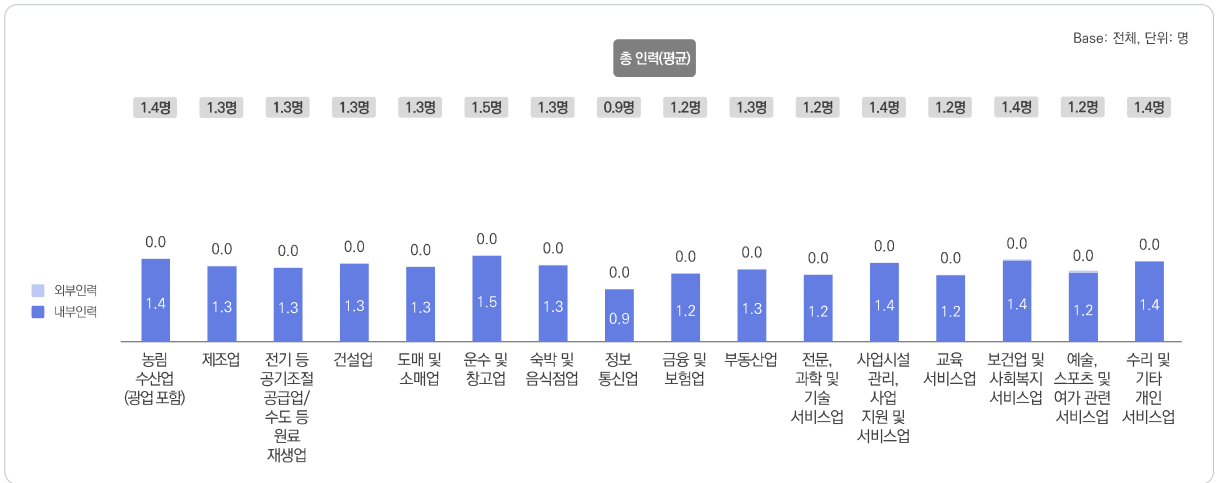


그림 1-3-23 업종별 일반 사무직 인력(주 업무 : 일반 사무, 부가 업무 : 정보보호)

- 규모와 상관없이 정보보호 업무를 부가적으로 하는 일반 사무직 인력은 비슷한 수준을 보임

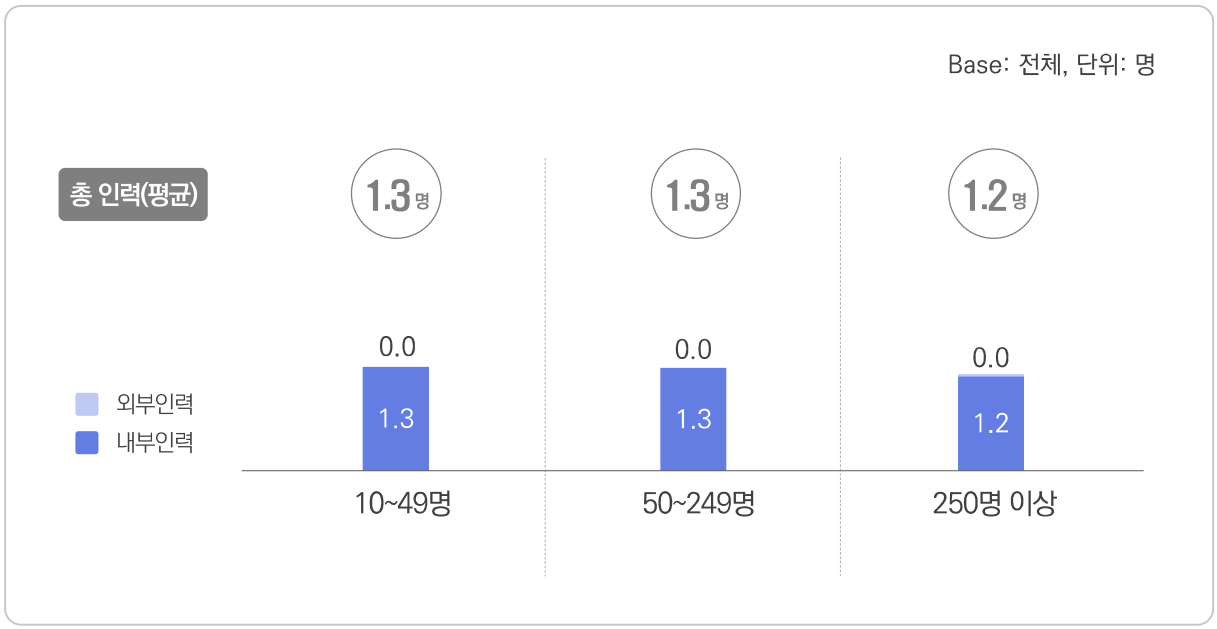


그림 1-3-24 규모별 일반 사무직 인력(주 업무 : 일반 사무, 부가 업무 : 정보보호)

나 개인정보보호 업무 겸직 여부

- 정보보호 담당 인력을 보유하고 있는 기업체 중 정보보호 담당 인력이 개인정보보호 업무를 겸직하는 비율은 내부인력이 53.7%, 외부인력이 26.8%로 나타남

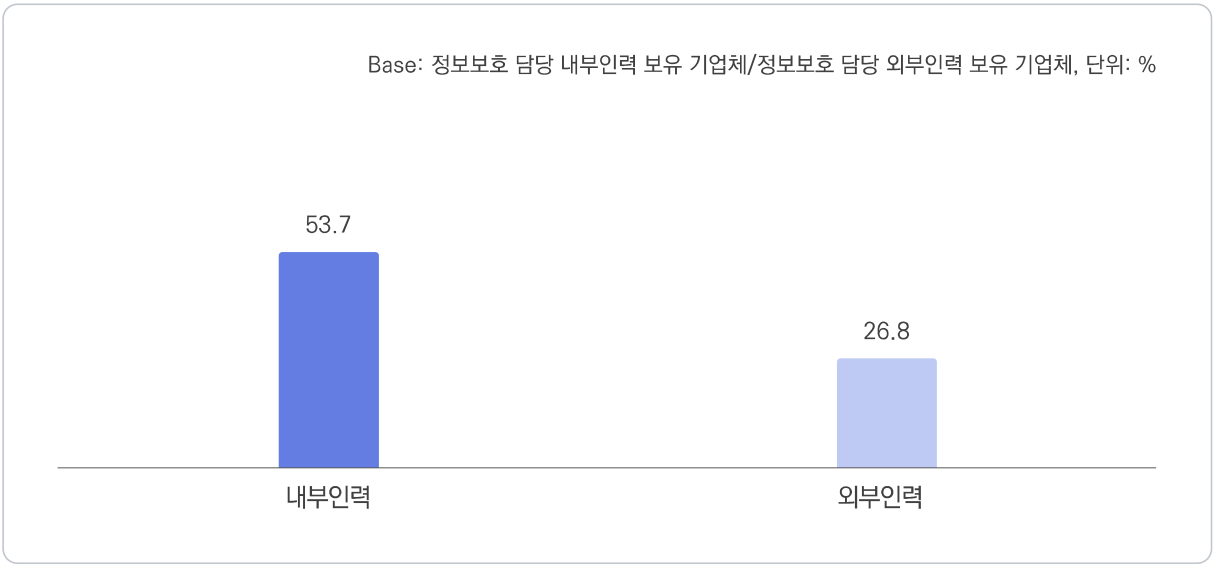


그림 1-3-25 정보보호 담당 인력의 개인정보보호 업무 겸직 여부

- 업종별로 보면 내부인력의 개인정보보호 업무 겸직 비율은 '금융 및 보험업'이 69.4%로 가장 높고, 외부인력의 개인정보보호 업무 겸직 비율은 '도매 및 소매업'이 51.9%로 가장 높음

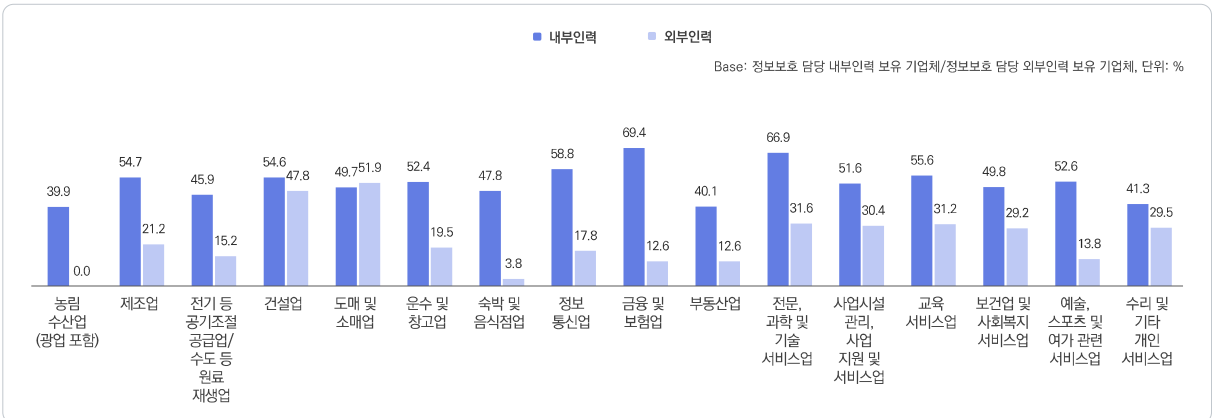


그림 1-3-26 업종별 정보보호 담당 인력의 개인정보보호 업무 겸직 여부

- 규모별로 보면 내부인력의 개인정보보호 업무 겸직 비율은 종사자 규모 '250명 이상(82.2%)'이 가장 높고, 외부인력의 개인정보보호 업무 겸직 비율은 종사자 규모 '50~249명(32.9%)'이 가장 높음

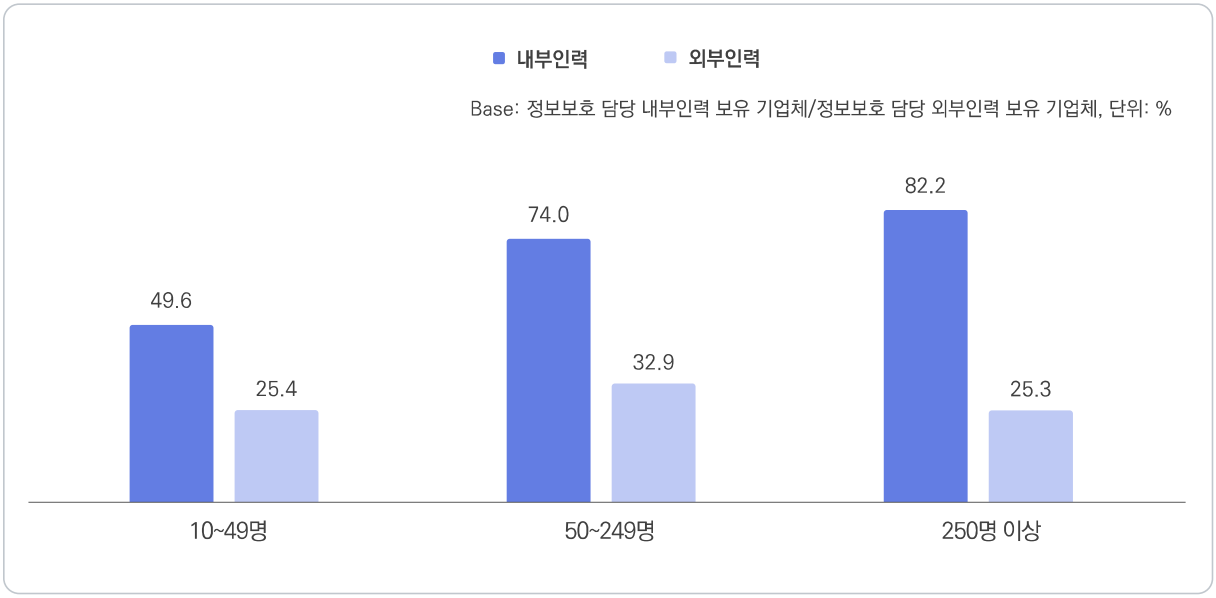


그림 1-3-27 **규모별 정보보호 담당 인력의 개인정보보호 업무 겸직 여부**

다 정보보호 관련 책임자

- 기업체의 정보관리책임자(Chief Information Officer, CIO) 임명 비율은 58.6%, 정보보호최고책임자(Chief Information Security Officer, CISO) 임명 비율은 21.0%, 최고기술책임자(Chief Technology Officer, CTO) 임명 비율은 6.9%로 나타남

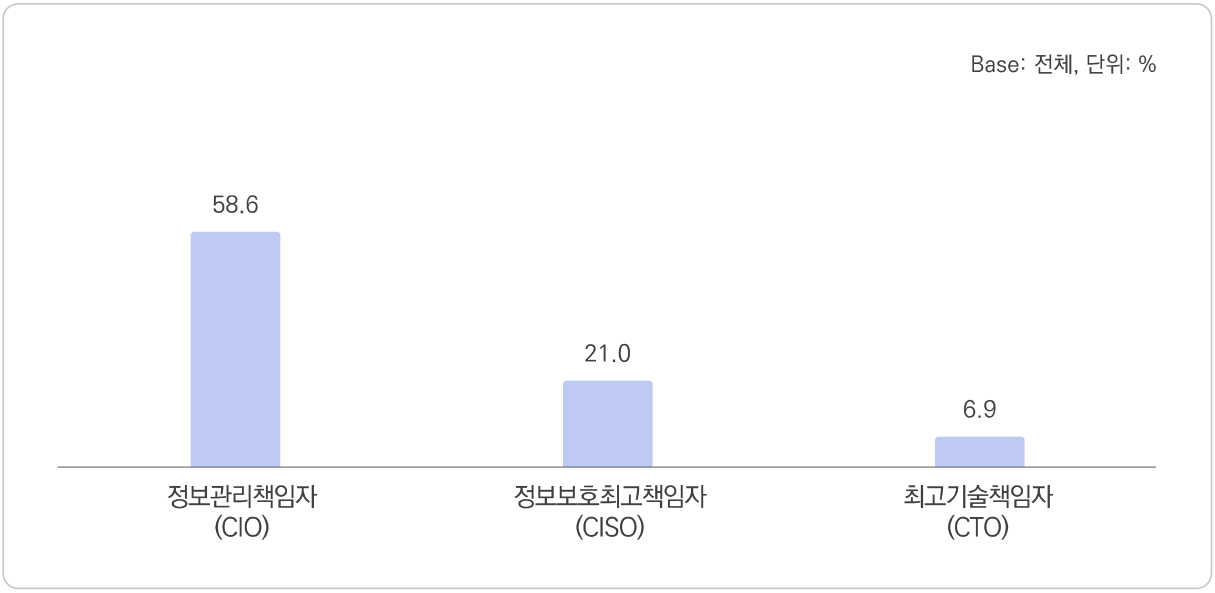


그림 1-3-28 정보보호 관련 책임자 임명 여부(복수응답)

- 업종별로 보면 '도매 및 소매업'의 정보관리책임자(CIO) 임명 비율(67.2%), '금융 및 보험업'의 정보보호최고책임자(CISO) 임명 비율(44.4%), '운수 및 창고업'의 최고기술책임자(CTO)의 임명 비율(10.9%)이 가장 높음

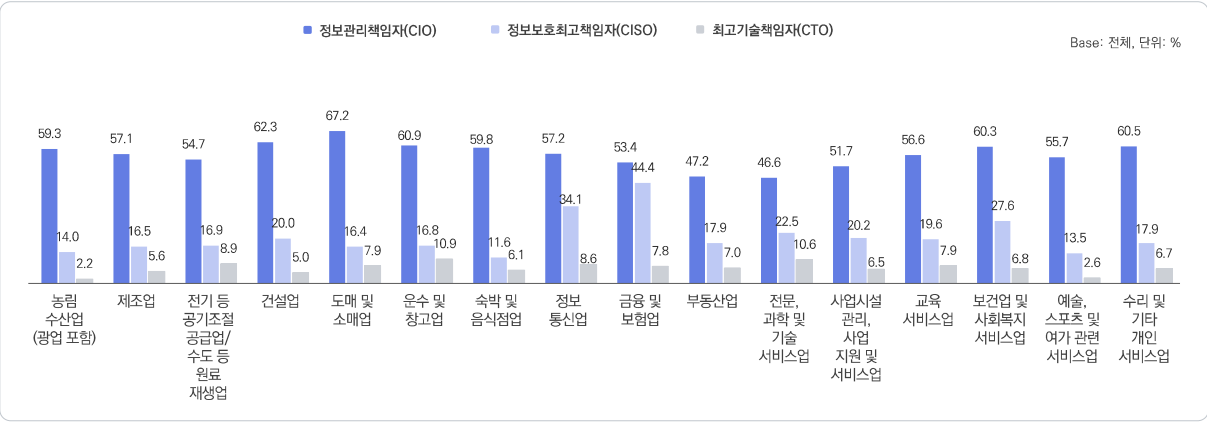


그림 1-3-29 업종별 정보보호 관련 책임자 임명 여부(복수응답)

- ‘250명 이상’ 기업에서 정보관리책임자(CIO), 정보보호최고책임자(CISO), 최고기술책임자(CTO) 임명 비율이 가장 높음

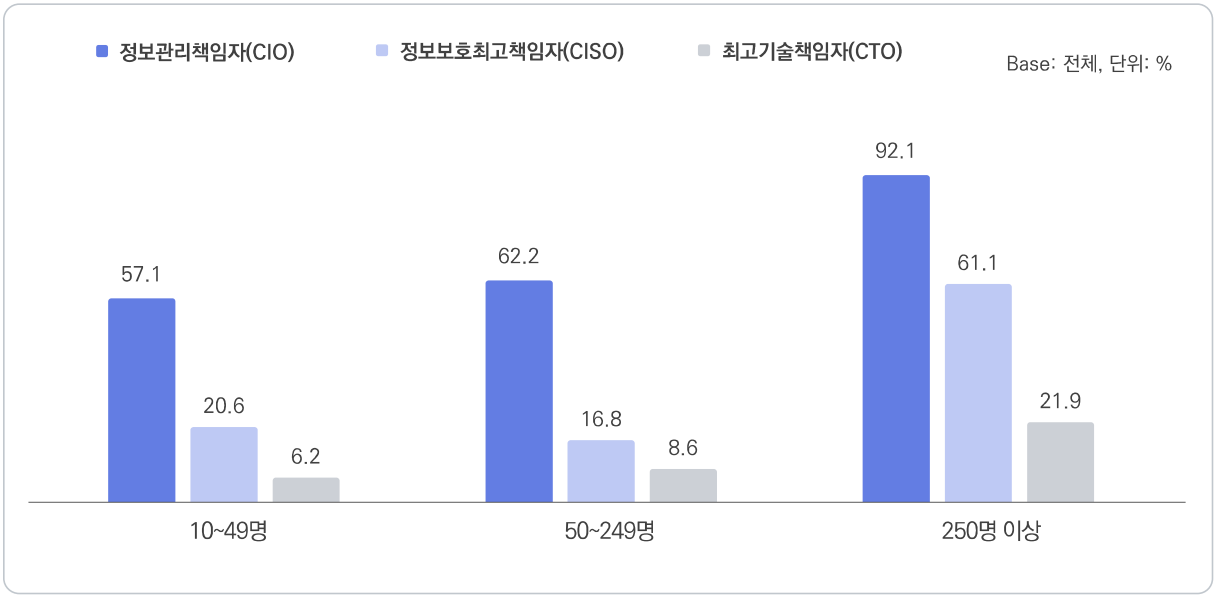


그림 1-3-30 규모별 정보보호 관련 책임자 임명 여부(복수응답)

- 전담 비율은 최고기술책임자(CTO)가 32.2%, 정보관리책임자(CIO)가 27.4%, 정보보호최고책임자(CISO)가 26.1%로 나타남

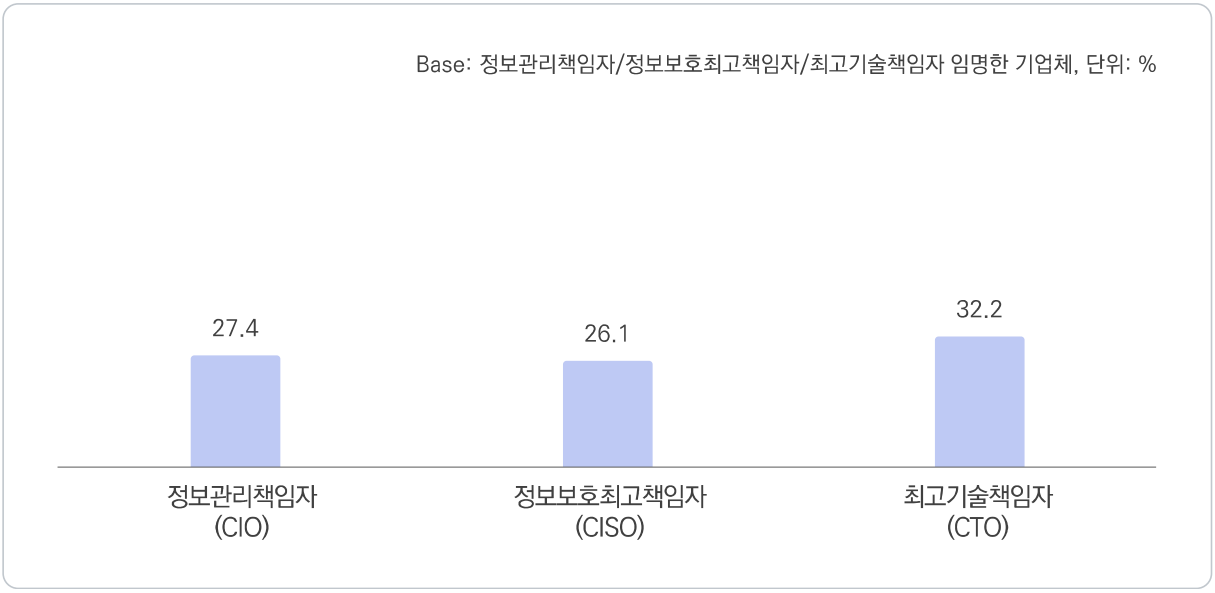


그림 1-3-31 정보보호 관련 책임자 전담 비율(복수응답)

- 업종별로 보면 정보관리책임자(CIO)의 전담 비율은 '운수 및 창고업(39.9%)'이 가장 높고, 정보보호최고책임자(CISO)의 전담 비율은 '부동산업(50.6%)'이 가장 높았으며, 최고기술책임자(CTO)의 전담 비율은 '농림수산업(광업 포함)(87.9%)'이 가장 높게 나타남

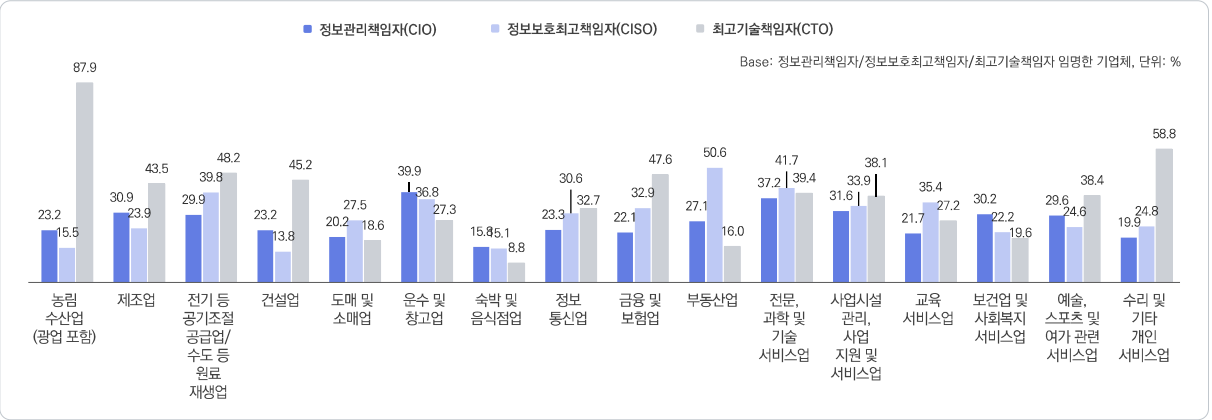


그림 1-3-32 업종별 정보보호 관련 책임자 전담 비율(복수응답)

- '50~249명' 기업에서 정보관리책임자(CIO) 및 최고기술책임자(CTO) 전담 비율이 가장 높고, '250명 이상' 기업에서 정보보호최고책임자(CISO) 전담 비율이 83.0%로 가장 높게 나타남

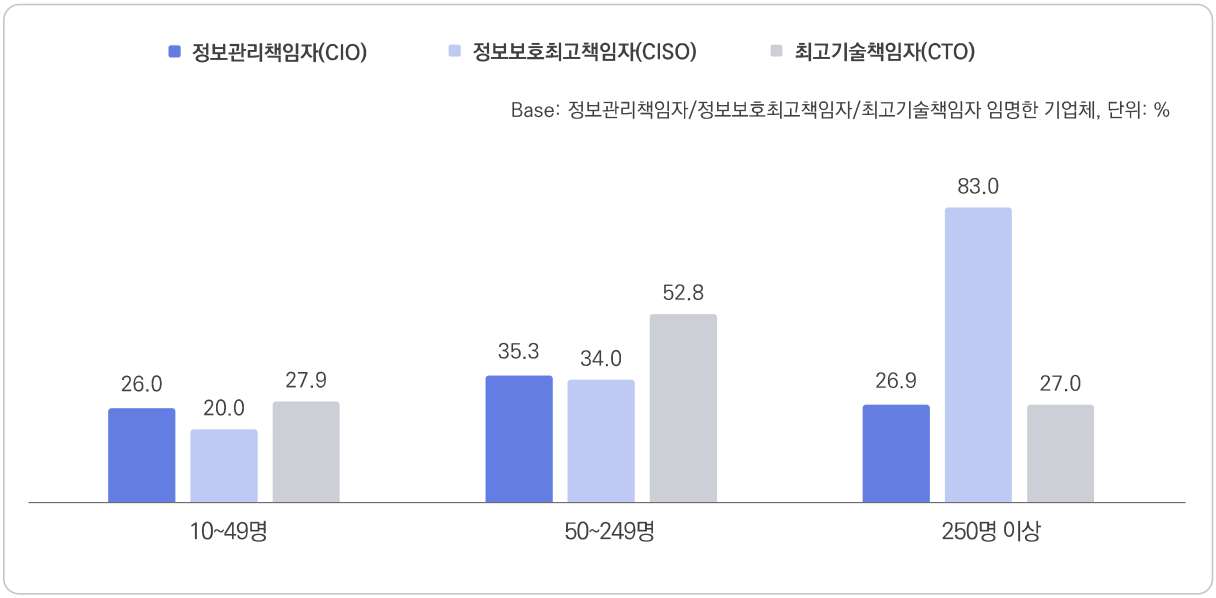


그림 1-3-33 규모별 정보보호 관련 책임자 전담 비율(복수응답)

라 정보보호 관련 책임자 겸직 업무

- 정보관리책임자(CIO)의 '정보보호최고책임자(CISO)' 업무 겸직 비율이 61.0%로 가장 높고, 다음으로 '개인정보보호최고책임자(CPO)(39.7%)', '최고기술책임자(CTO)(0.3%)' 등의 순임

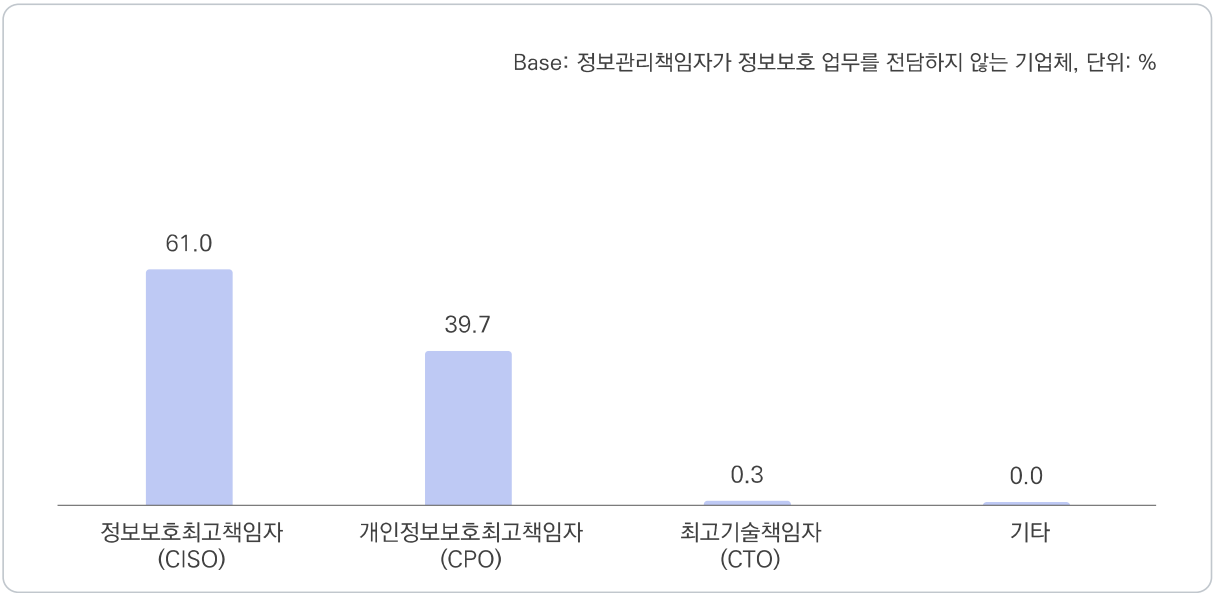


그림 1-3-34 정보관리책임자(CIO) 겸직 업무(복수응답)

- 정보보호최고책임자(CISO)의 '개인정보보호최고책임자(CPO)' 업무 겸직 비율이 65.0%로 가장 높고, '정보관리책임자(CIO)(34.3%)', '최고기술책임자(CTO)(0.9%)' 등의 순임

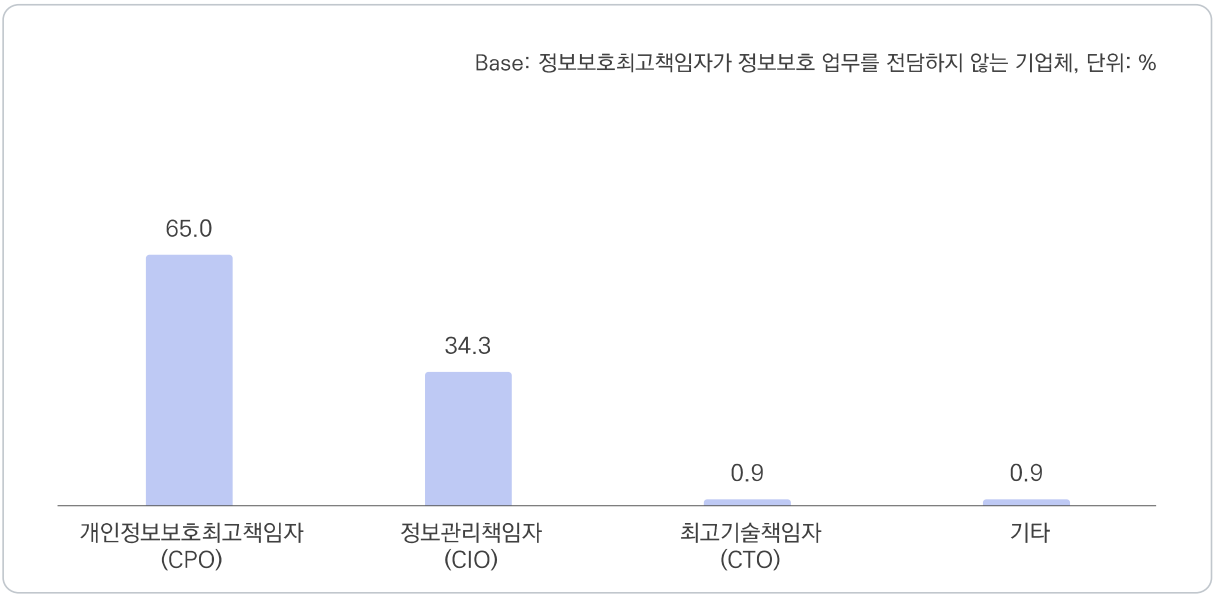


그림 1-3-35 정보보호최고책임자(CISO) 겸직 업무(복수응답)

- 최고기술책임자(CTO)의 ‘정보관리책임자(CIO)’ 업무 겸직 비율이 68.8%로 가장 높고, ‘개인정보보호 최고책임자(CPO)(18.3%)’, ‘정보보호최고책임자(CISO)(13.0%)’ 등의 순임

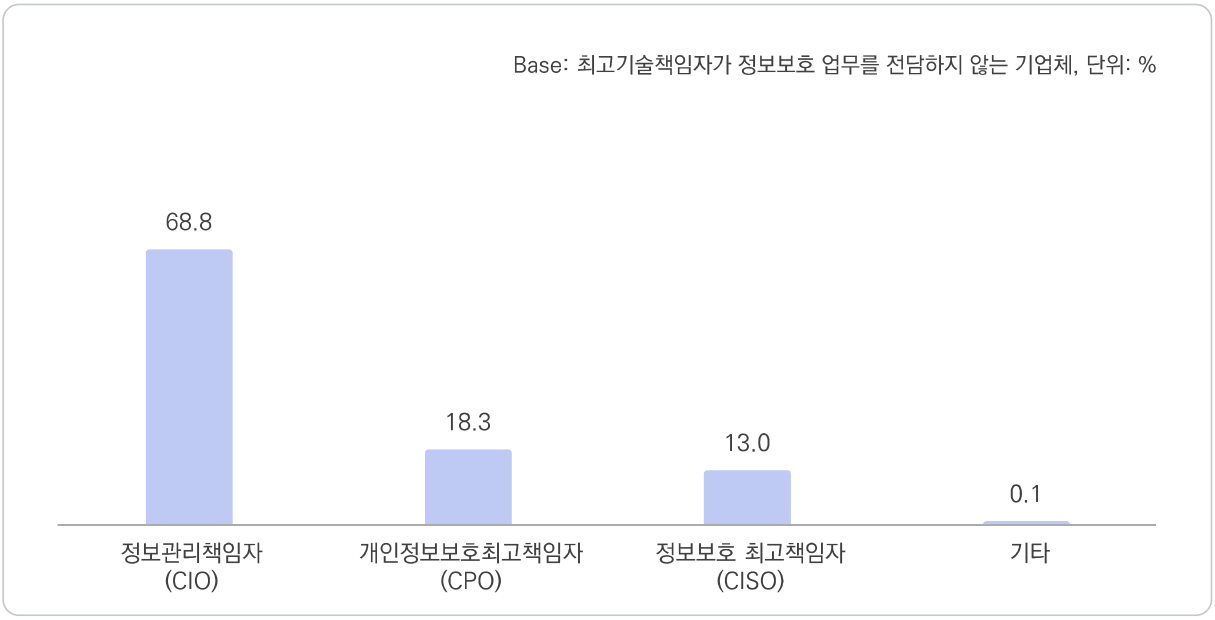


그림 1-3-36 최고기술책임자(CTO) 겸직 업무(복수응답)

Ⅲ 정보보호 교육

1 정보보호 교육

가 중소기업 대상 정보보호 무료 교육 인지 여부

- 기업체 중 39.7%가 중소기업 대상 정보보호 무료 교육에 대해 인지하고 있는 것으로 나타남

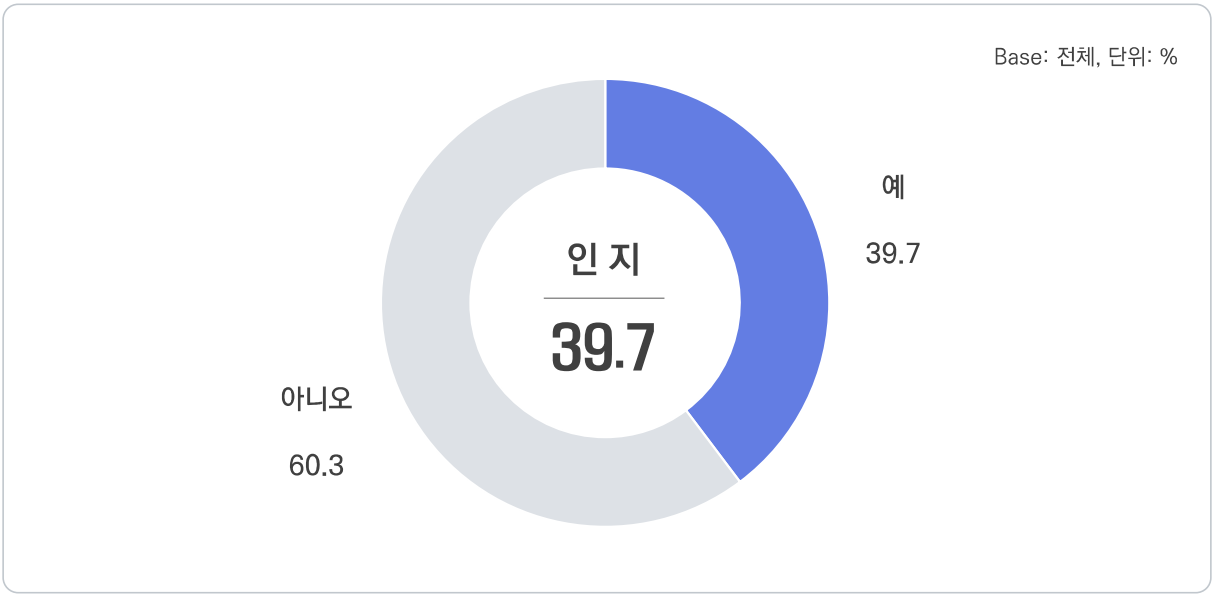


그림 1-3-37 중소기업 대상 정보보호 무료 교육 인지 여부

나 정보보호 교육 실시

- 기업체 중 32.7 최근 1년간 임직원을 대상으로 정보보호 교육을 실시했다고 응답함

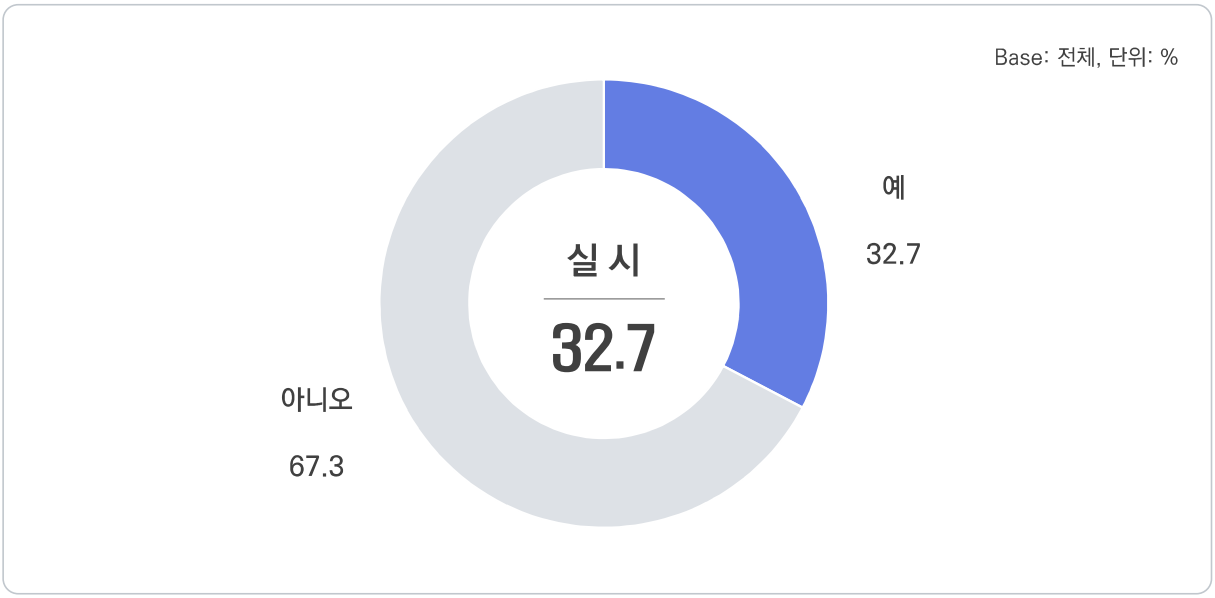


그림 1-3-38 정보보호 교육 실시

- 업종별로 보면 '금융 및 보험업'의 정보보호 교육 실시율이 70.0%로 가장 높고, 다음으로 '정보통신업(44.9%)', '교육 서비스업(43.9%)' 등의 순임

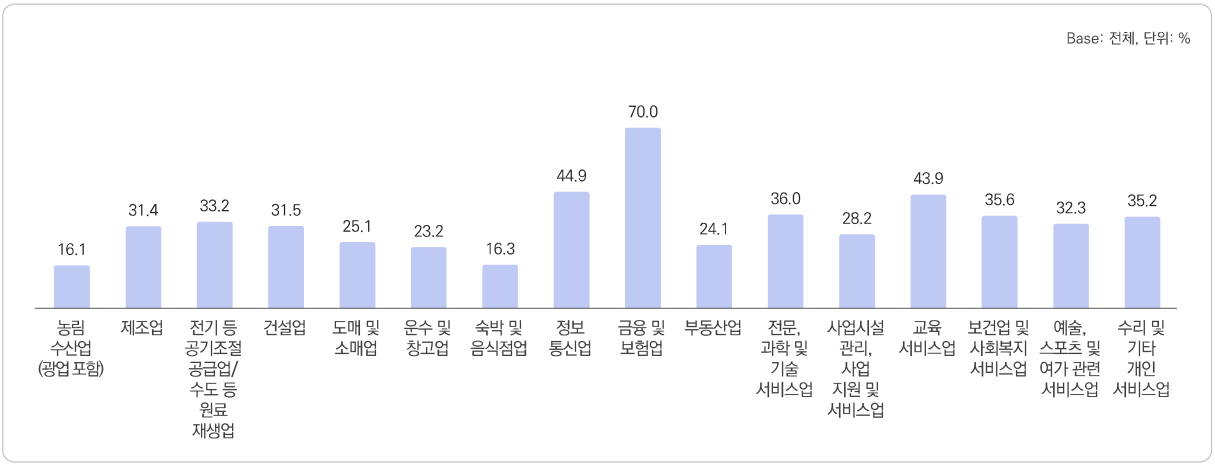


그림 1-3-39 업종별 정보보호 교육 실시

- 정보보호 교육 실시율은 종사자 규모 '250명 이상(97.8%)'에서 가장 높음

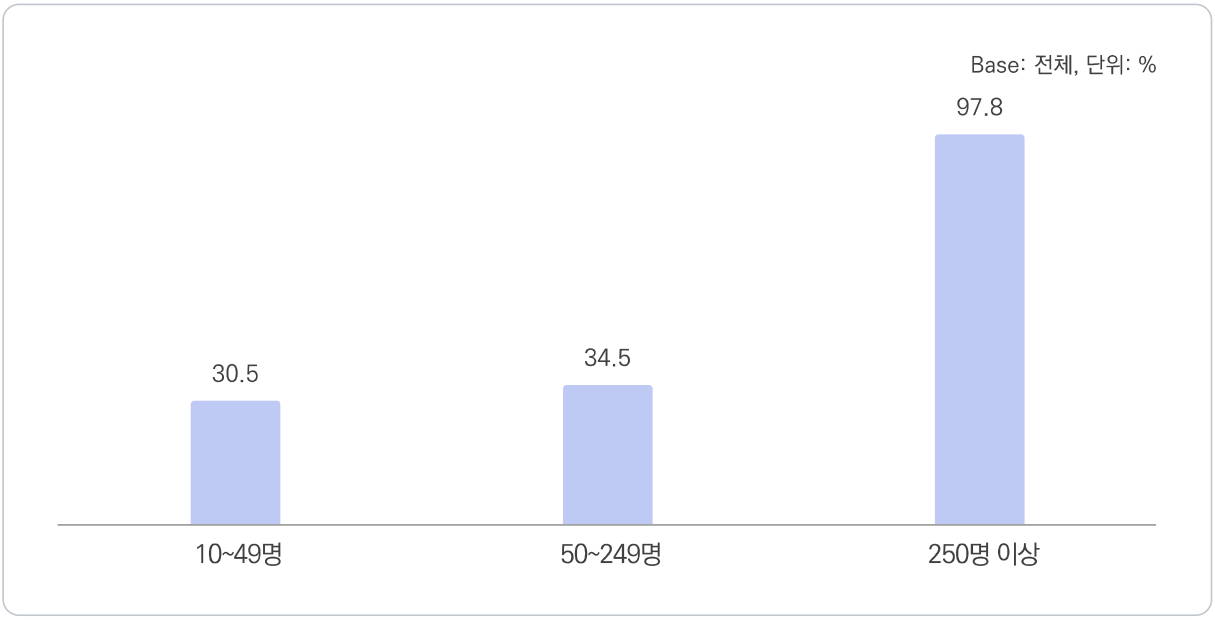


그림 1-3-40 규모별 정보보호 교육 실시

다 대상별 정보보호 교육 실시 현황

- 정보보호 교육 실시율은 '정보보호 담당 인력'이 96.3%로 가장 높고, 다음으로 'CEO 및 경영진(90.8%)', '일반 직원(IT 직원 제외)(85.3%)' 등의 순임

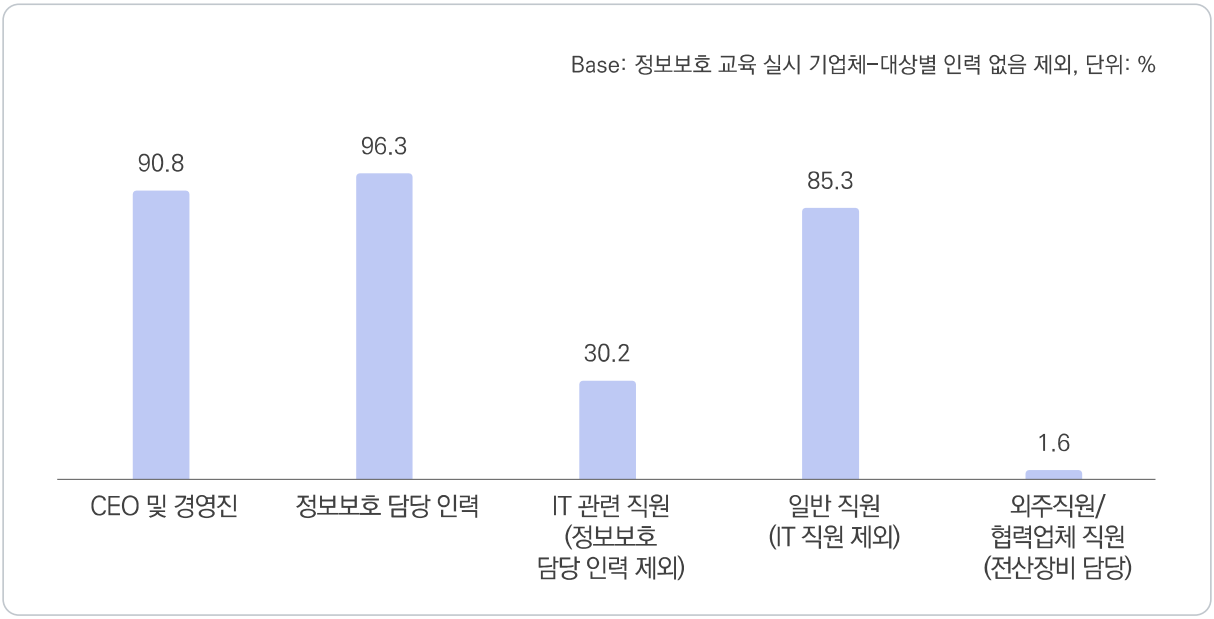


그림 1-3-41 대상별 정보보호 교육 실시 현황

라 정보보호 교육 방법

- 정보보호 교육 방법에 대해 외주직원/협력업체 직원(전산장비 담당)은 '자체 교육(내부 강사)'의 비율(43.2%)이 가장 높고, CEO 및 경영진은 '정부/지자체/공공기관 교육 참여'의 비율(53.9%)이 타 대상 대비 높음

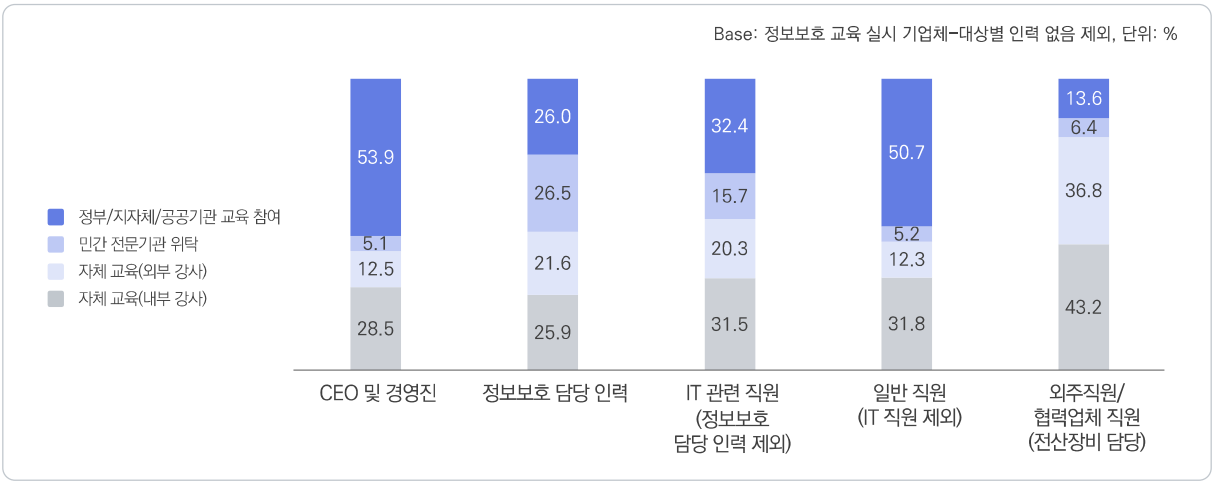


그림 1-3-42 대상별 정보보호 교육 방법

마 정보보호 교육 방식

- 정보보호 교육 방식에 대해 모든 교육 대상의 '온라인 교육' 비율이 높게 나타남

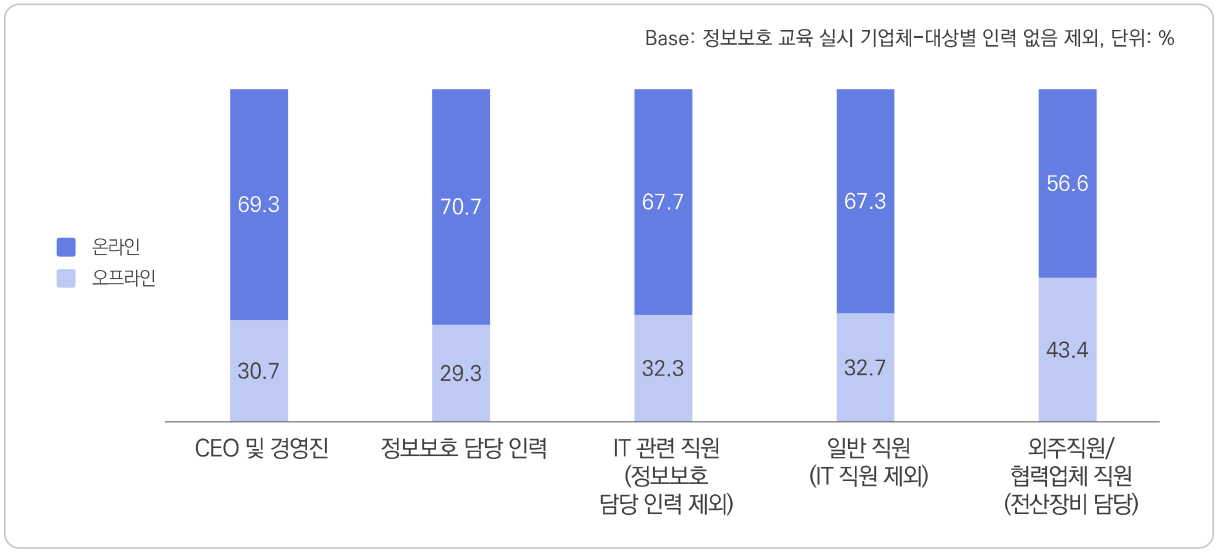


그림 1-3-43 대상별 정보보호 교육 방식

바 정보보호 교육 자료 출처

- 정보보호 교육 자료의 출처로는 '정부 또는 공공기관에서 제공하는 공식적인 온라인 교육 자료 활용'이 63.2%로 가장 높고, 다음으로 '사내에서 자체 제작한 교육 자료 활용(37.4%)', '외부 전문 위탁 기관에 의뢰하여 제작한 교육 자료 활용(16.2%)' 등의 순임

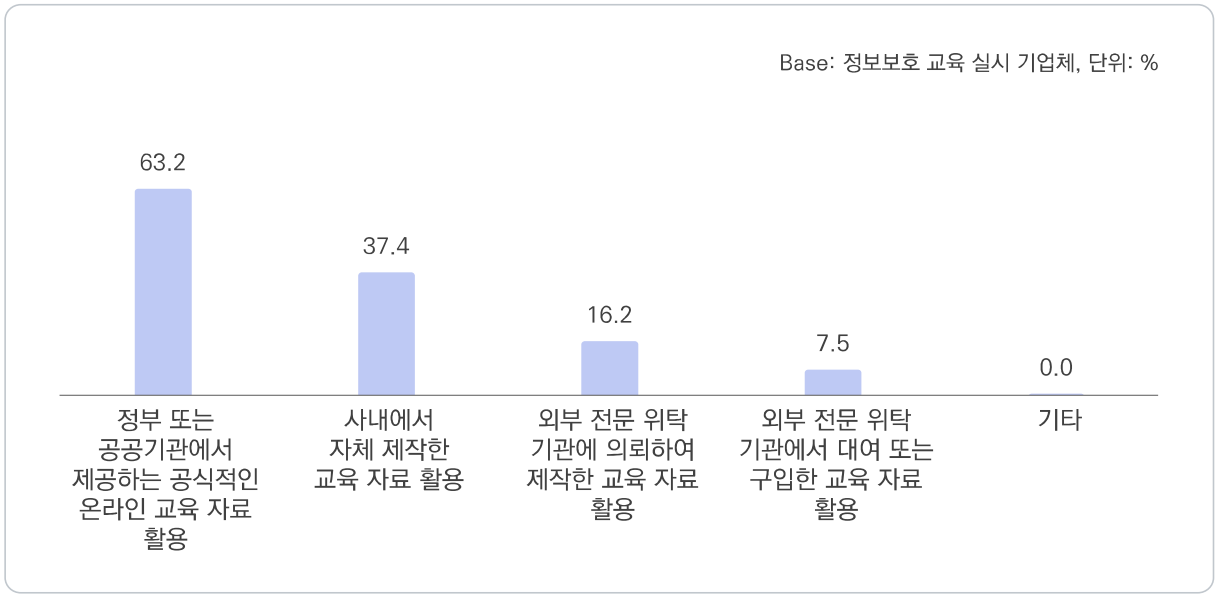


그림 1-3-44 정보보호 교육 자료 출처(복수응답)

사 정보보호 교육 효과

- 정보보호 교육을 실시하는 기업체 중 68.6%가 정보보호 교육에 대한 효과가 '있다(효과가 있는 편이다+매우 효과적이다)'고 응답함

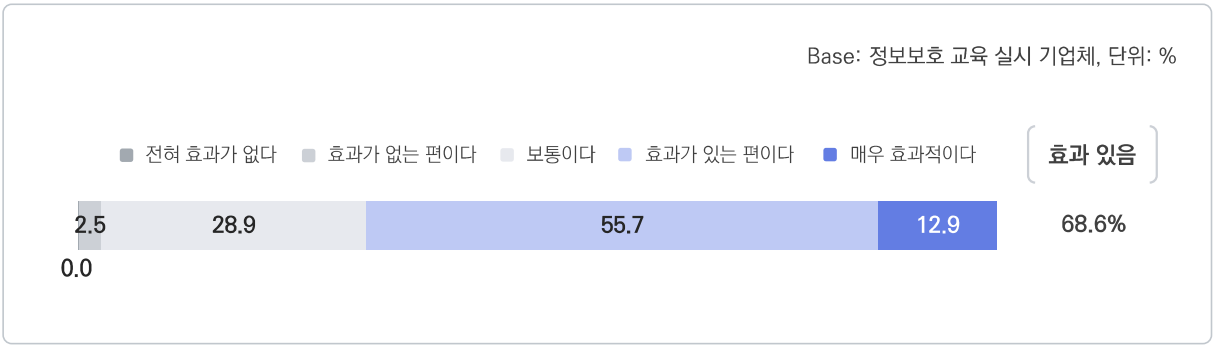


그림 1-3-45 정보보호 교육 효과

아 정보보호 교육 만족도

- 정보보호 교육을 실시하는 기업체 중 62.8%가 정보보호 교육에 대한 만족도가 '높다(높은 편이다+매우 높다)'고 응답함

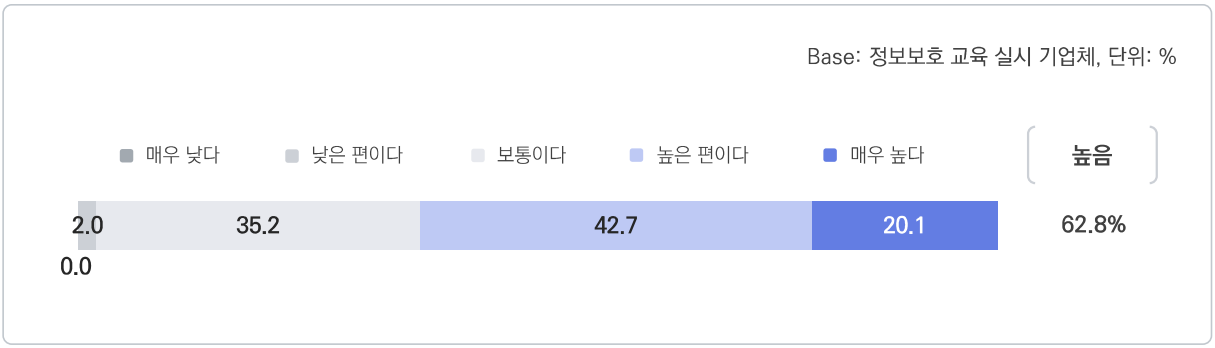


그림 1-3-46 정보보호 교육 만족도

Ⅳ 정보보호 예산

1 정보보호 예산

가 정보보호 예산 사용

- 기업체 중 54.8%는 최근 1년간 정보보호 관련 활동을 위해 예산을 사용한 적 있다고 응답함

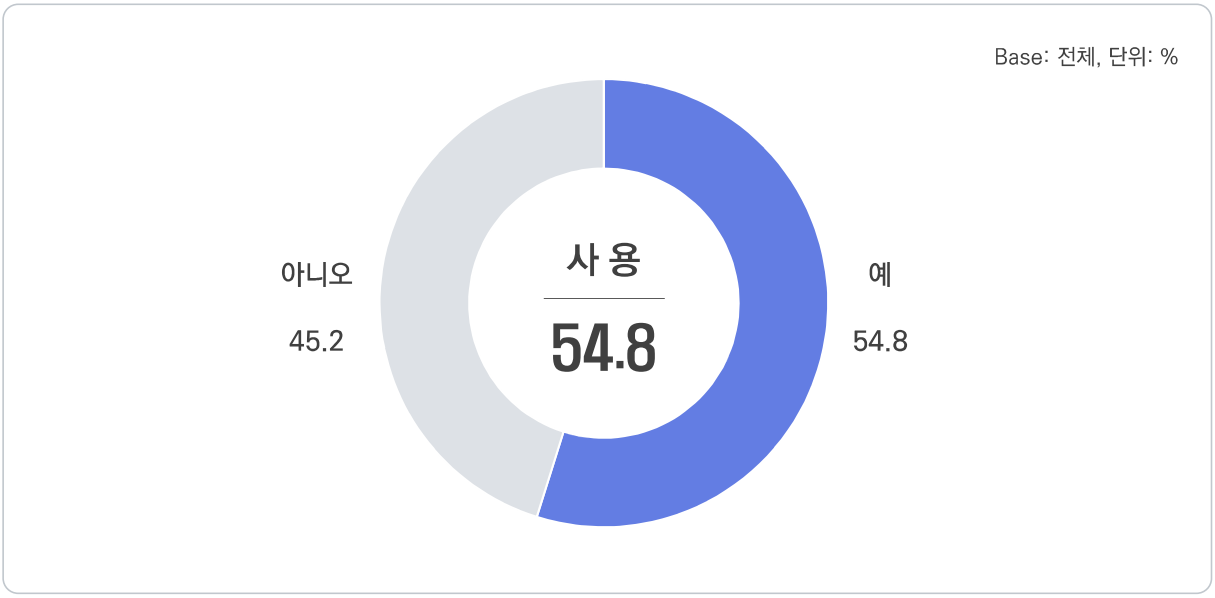


그림 1-3-47 정보보호 예산 사용

- 업종별로 보면 '전문, 과학 및 기술 서비스업'의 정보보호 예산 사용률이 69.4%로 가장 높고, 다음으로 '사업시설 관리, 사업 지원 및 서비스업(61.6%)', '부동산업(60.4%)' 등의 순임

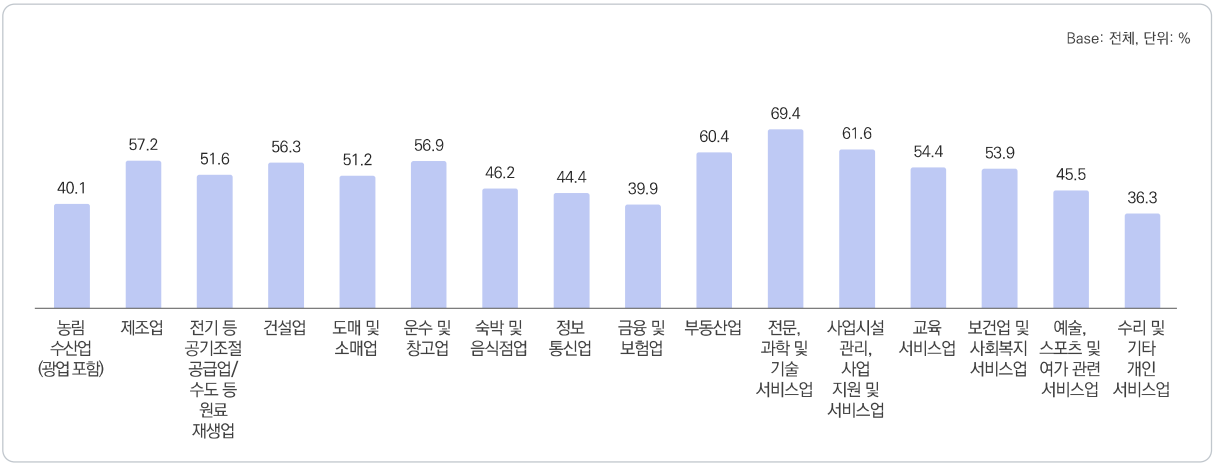


그림 1-3-48 업종별 정보보호 예산 사용

- 정보보호 예산 사용 비율은 종사자 규모 '250명 이상(88.3%)'에서 가장 높음

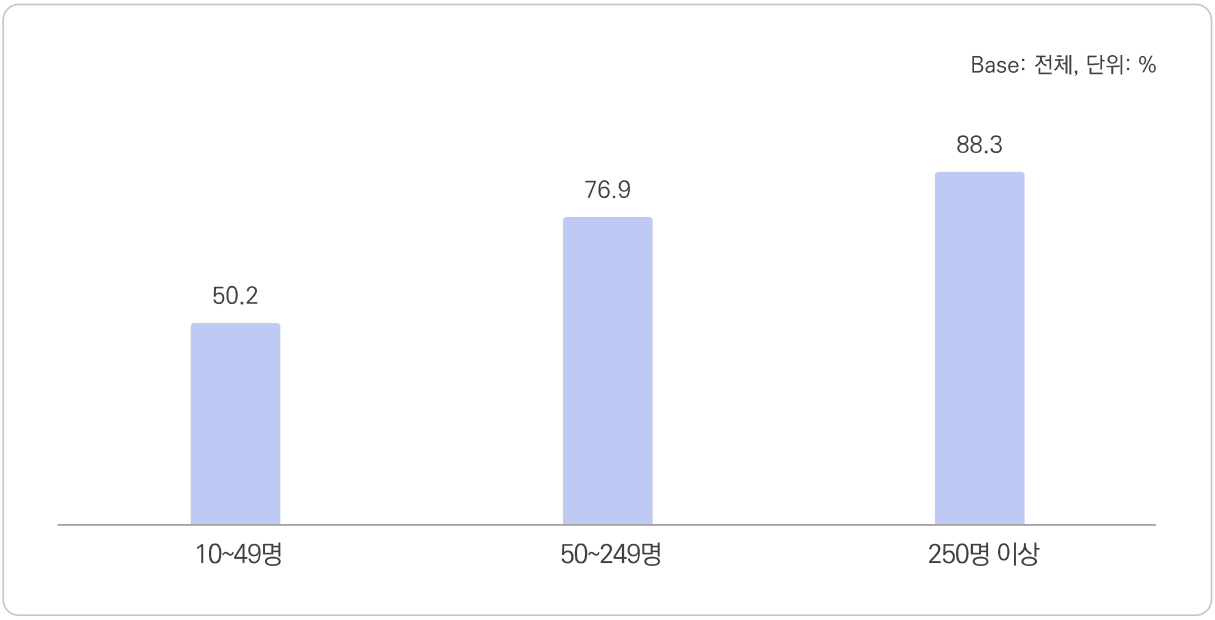


그림 1-3-49 규모별 정보보호 예산 사용

나 정보보호 예산 미사용 이유

- 정보보호 예산을 사용하지 않는 이유로는 '현재 사업 영역이 정보보호와 무관함'이 37.0%로 가장 높고, 다음으로 '필요한 정보보호 관련 활동이 무엇인지 모름(33.4%)', '침해사고 완벽 방어 미보장(32.7%)' 등의 순임

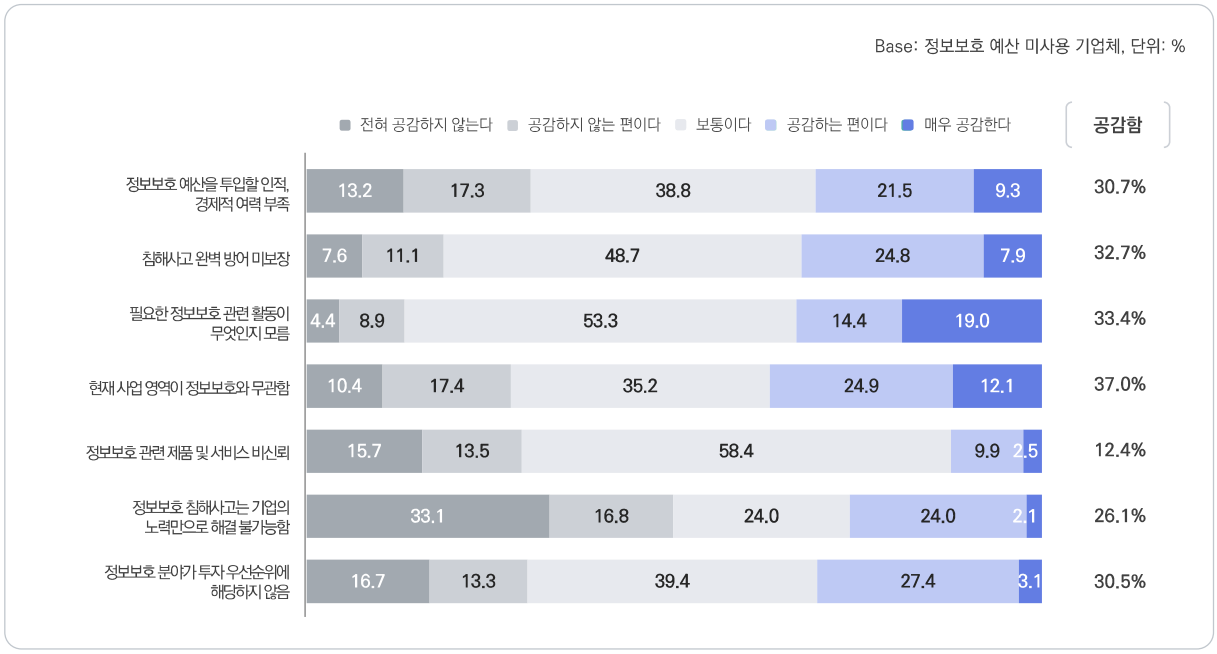


그림 1-3-50 정보보호 예산 미사용 이유

다 정보보호 예산 총액

- 기업체의 정보보호 예산 총액은 '500만 원 미만'이 70.4%로 가장 높고, 다음으로 '500만 원 이상 1,000만 원 미만(25.2%)', '1,000만 원 이상 3,000만 원 미만(1.9%)' 등의 순임

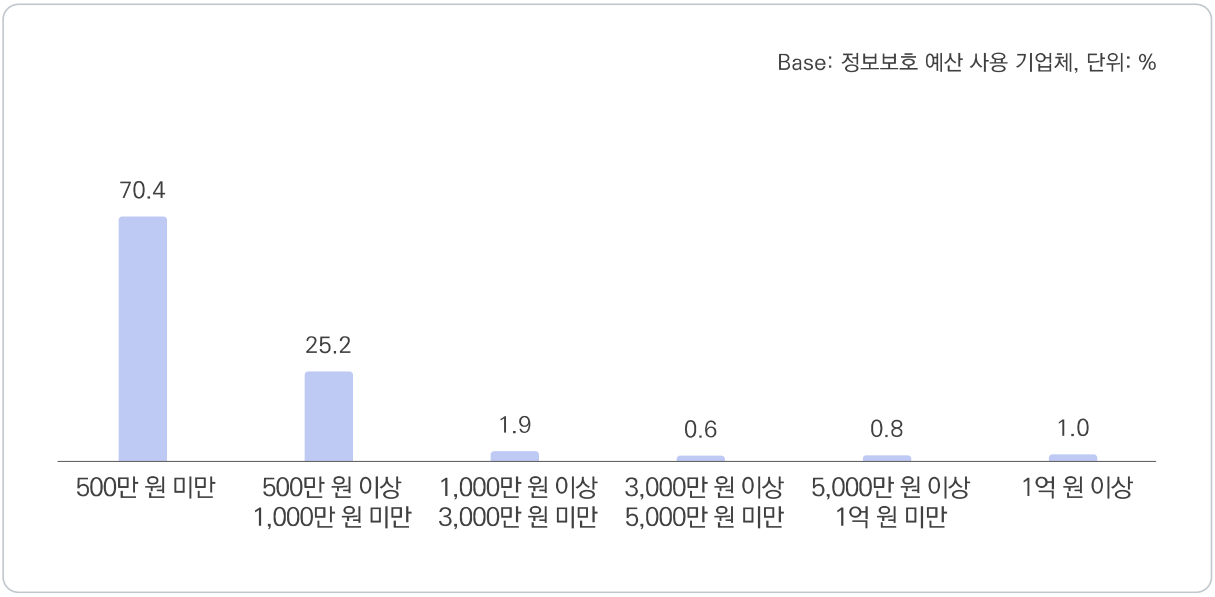


그림 1-3-51 정보보호 예산 총액

라 정보보호 예산 총액 변화

- 정보보호 예산을 사용한 기업체의 2023년 대비 2024년 예산 총액 변화 정도로 '현상 유지'가 82.9%로 가장 높고, 다음으로 '증가(13.4%)', '감소(3.6%)', '신설(0.0%)'의 순임

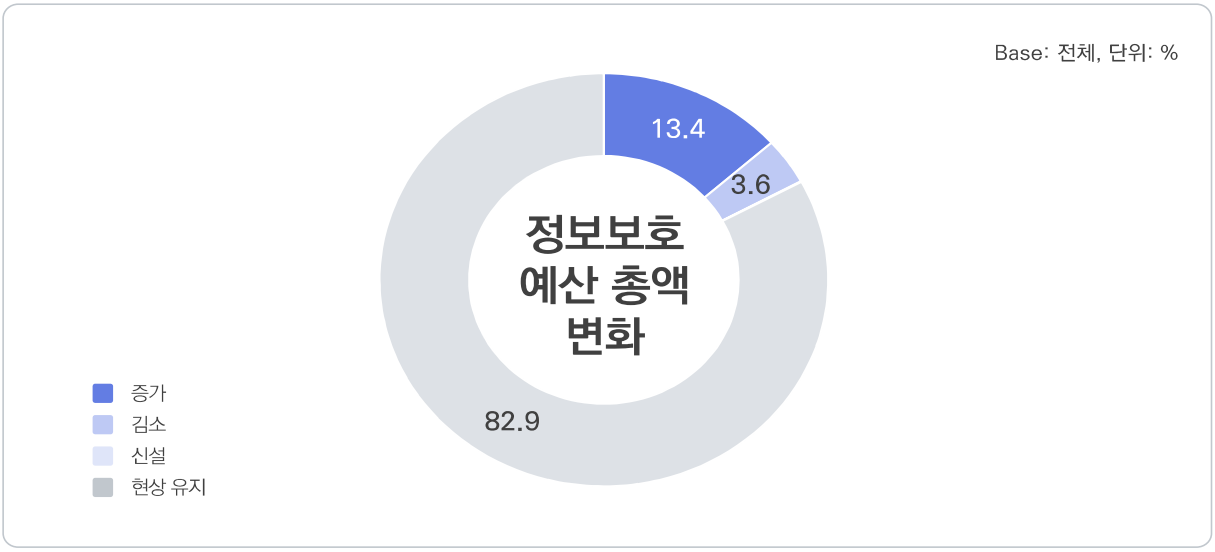


그림 1-3-52 정보보호 예산 총액 변화

- 정보보호 예산이 신설된 기업체의 예산 신설 이유로 '정보보호 제품 구입 비용 신설'이 50.3%로 가장 높고, 다음으로 '정보보호 사고 대응 관련 비용 신설(37.6%)', '정보보호 인력 인건비 신설(15.9%)' 등의 순임

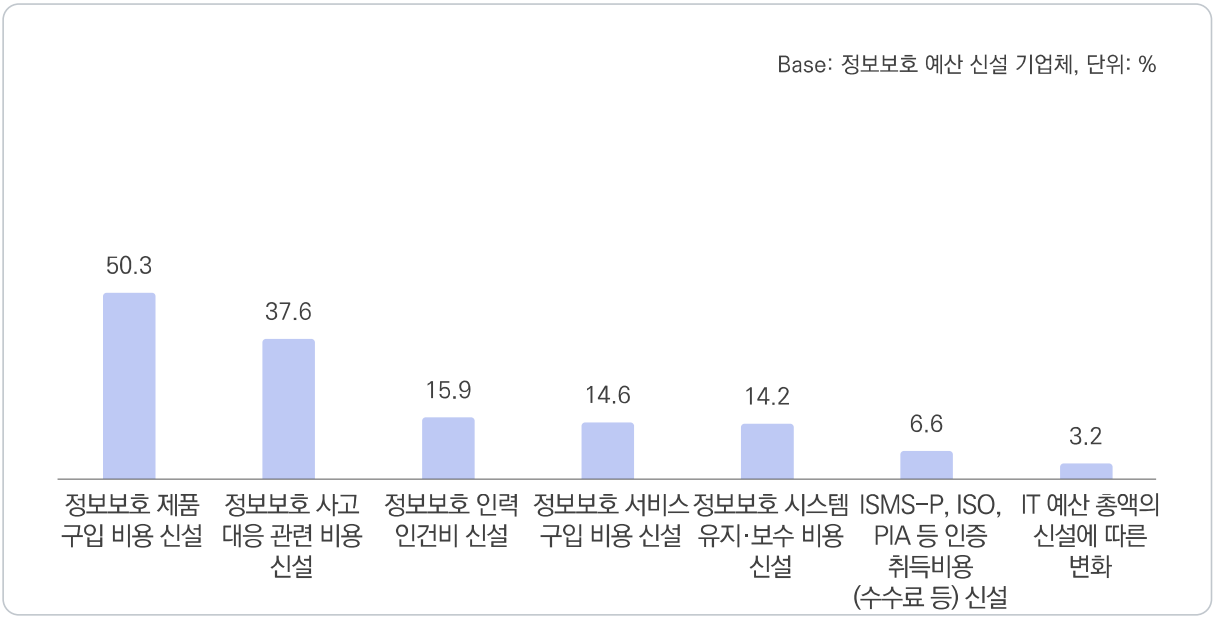


그림 1-3-53 정보보호 예산 총액 신설 이유(1+2+3순위)

- 정보보호 예산이 증가한 기업체의 예산 증가 이유로 '정보보호 시스템 유지·보수 비용 증가'가 63.4%로 가장 높고, 다음으로 '정보보호 제품 구입 비용 증가(53.9%)', '정보보호 서비스 구입 비용 증가(50.1%)' 등의 순임

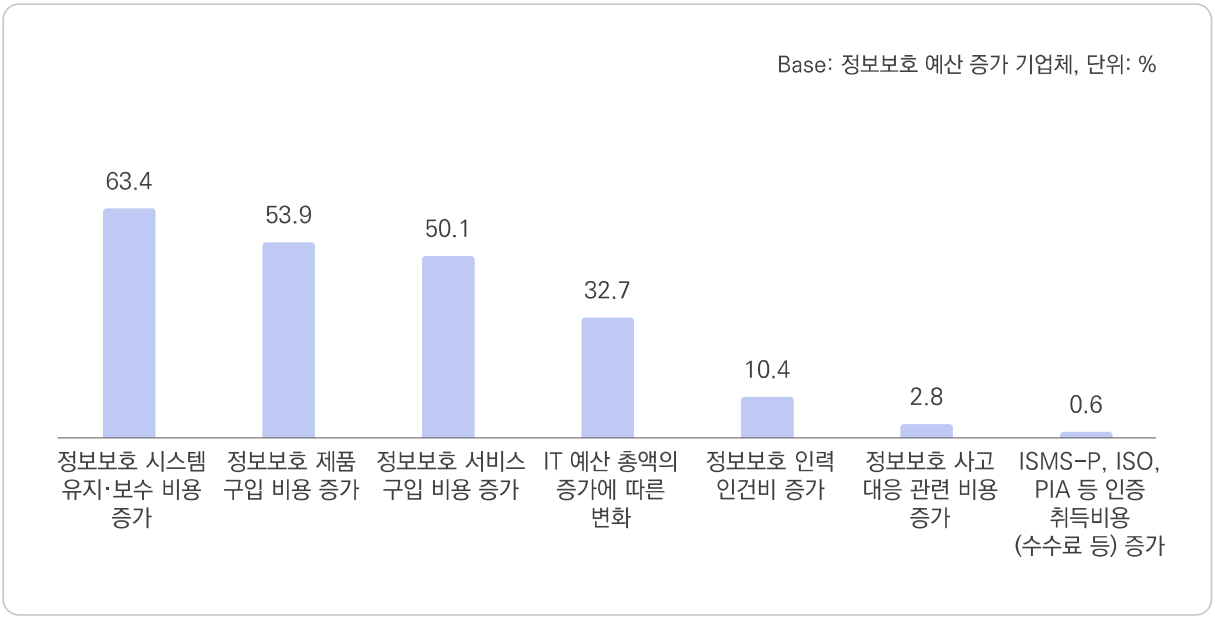


그림 1-3-54 정보보호 예산 총액 증가 이유(1+2+3순위)

- 정보보호 예산이 감소한 기업체의 예산 감소 이유로 'IT 예산 총액의 감소에 따른 변화'가 77.8%로 가장 높고, 다음으로 '정보보호 제품 구입 비용 감소(42.5%)', '정보보호 시스템 유지·보수 비용 감소(41.9%)' 등의 순임

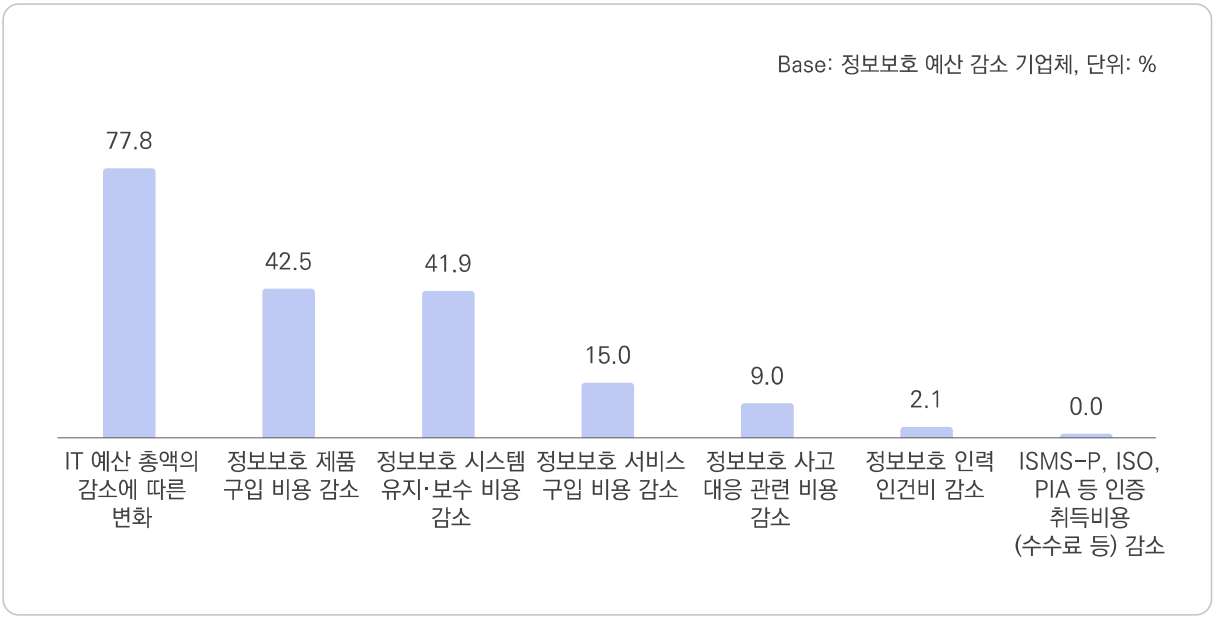


그림 1-3-55 정보보호 예산 총액 감소 이유(1+2+3순위)

마 정보보호 예산 총액 변화 예상

- 정보보호 예산을 사용한 기업체 중 16.7%가 향후 정보보호 예산 총액 변화에 대해 '늘릴 것이다(소폭 늘릴 것이다+대폭 늘릴 것이다)'라고 응답함

그림 1-3-56 정보보호 예산 총액 변화 예상

바 정보보호 예산 활용 유형

- 정보보호 예산 활용 유형으로는 '정보보호 관련 정보보호 제품 및 솔루션의 유지·보수'가 78.0%로 가장 높고, 다음으로 '업무 시설의 CCTV 등 영상 감시장비 설치 또는 증설(57.4%)', '정보보호 관련 정보보호 제품 및 솔루션의 구입(28.6%)' 등의 순임

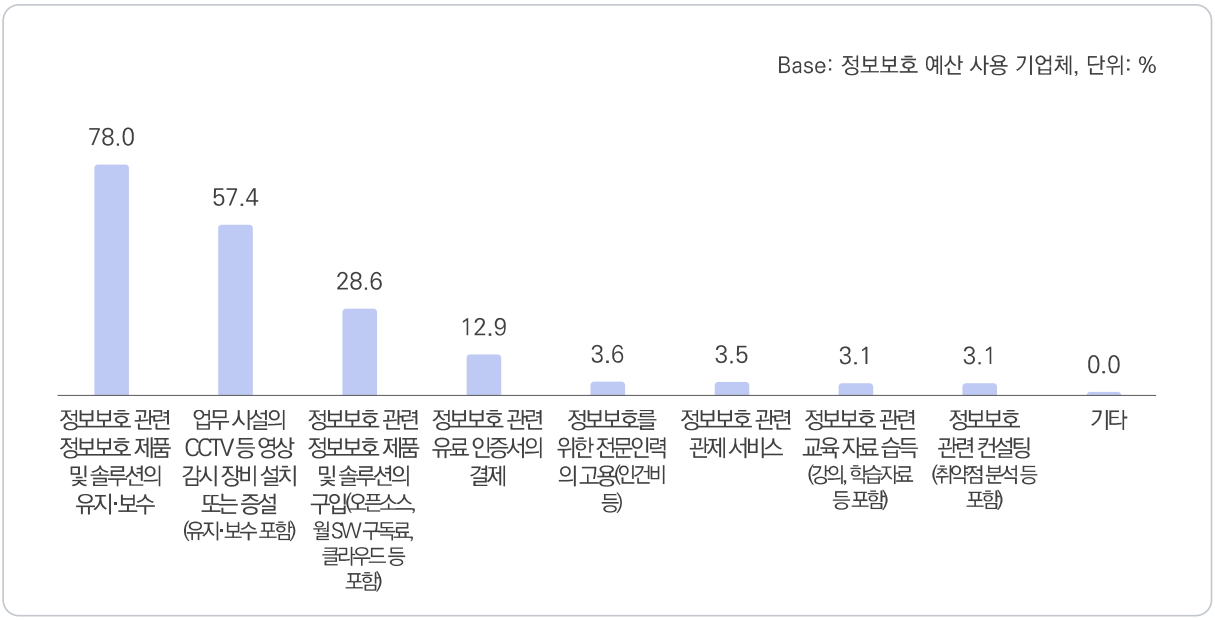


그림 1-3-57 정보보호 예산 활용 유형(1+2+3순위)

사 정보보호 예산 사용 계기

- 정보보호 예산 사용 계기로는 'TV 또는 온라인 매체를 통한 정보 습득으로 위험성을 인지한 이후'가 40.9%로 가장 높고, 다음으로 '주변 거래처/지인의 추천을 통해(40.2%)', '정보보호 기업체의 홍보 자료 또는 영업을 접한 이후(36.2%)' 등의 순임

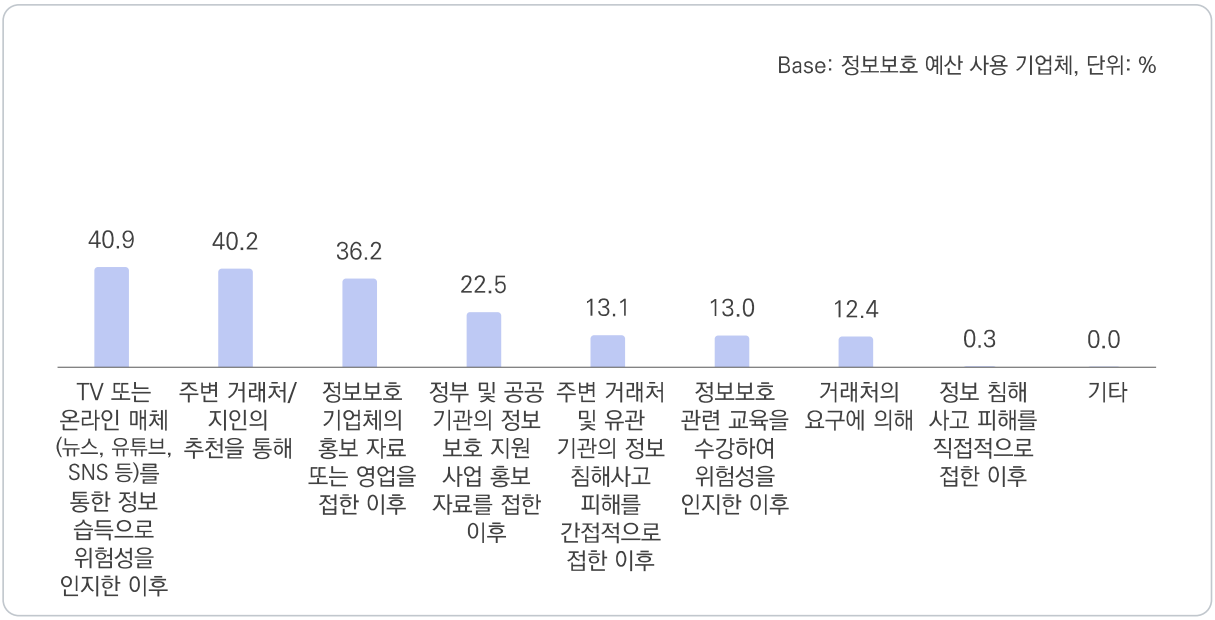


그림 1-3-58 정보보호 예산 사용 계기(1+2+3순위)

아 정보보호 예산 사용 적절성

- 정보보호 예산을 사용한 기업체 중 28.1%는 정보보호 예산 사용이 '적절하다(그렇다+매우 그렇다)'고 응답함

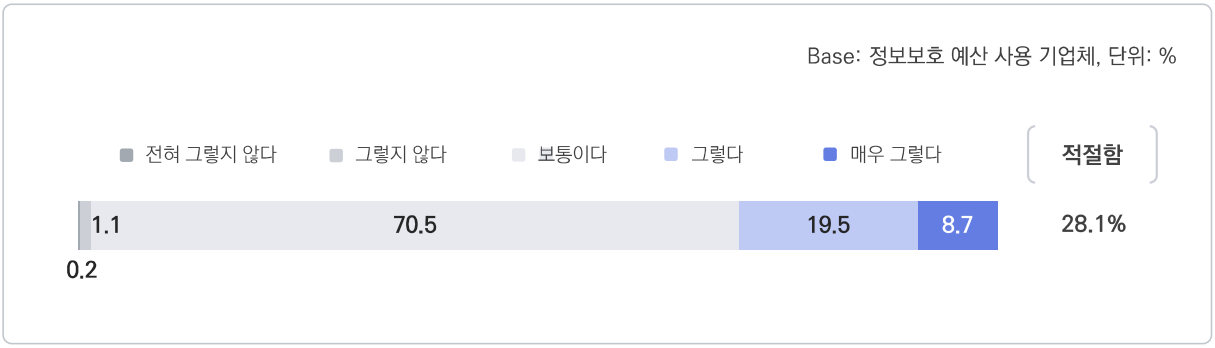


그림 1-3-59 정보보호 예산 사용 적절성

자 정보보호 예산 사용 부적절 이유

- 정보보호 예산 사용이 적절하지 않다고 응답한 이유로는 '정보보호 제품·솔루션·서비스의 높은 단가'가 44.8%로 가장 높고, 다음으로 '정보보호는 전문적인 영역으로 합리적 소비 판단이 어려움(26.3%)', '정보보호 제품·솔루션·서비스의 필요성이 명확하지 않음(24.7%)', '기업의 투자자·소유자가 불필요한 낭비로 인식함(16.0%)' 등의 순임

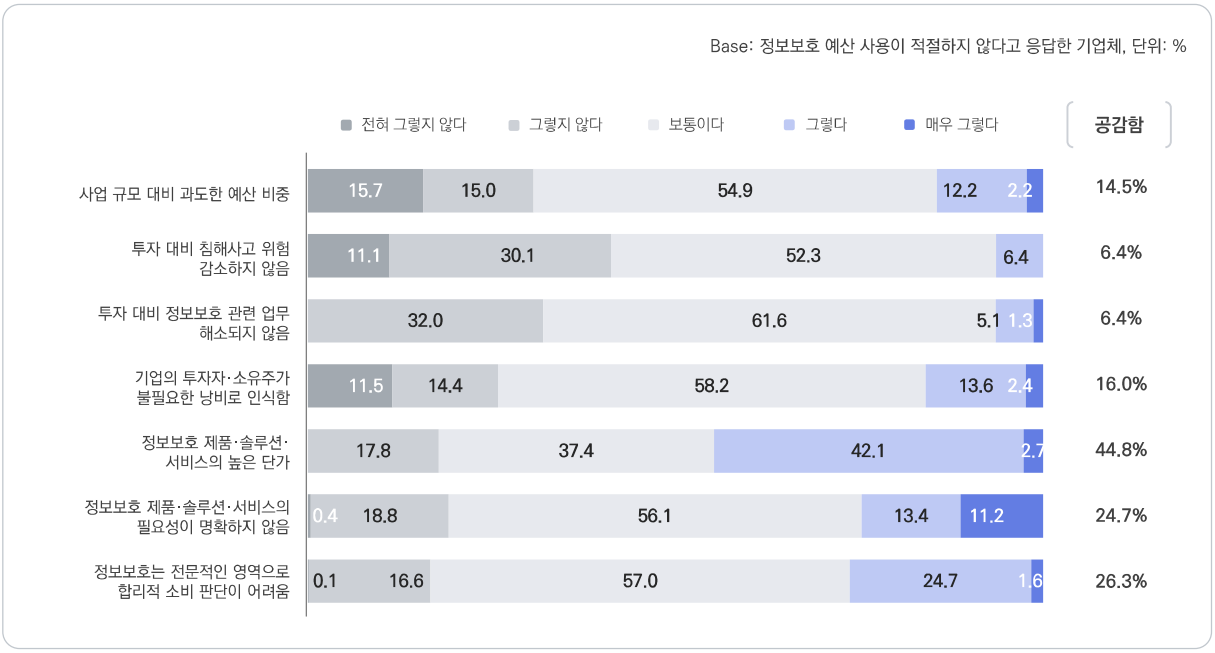


그림 1-3-60 정보보호 예산 사용 부적절 이유

2 국내외 정보보호 제품 및 서비스 선호도

- 정보보호 제품 및 서비스 모두 국내 선호 비율(제품: 47.8%, 서비스: 47.0%)이 해외 선호 비율(제품: 1.8%, 서비스: 2.1%)보다 높음
  - 특별히 선호도를 구분하지 않는 비율은 제품 50.4%, 서비스 50.9%로 나타남

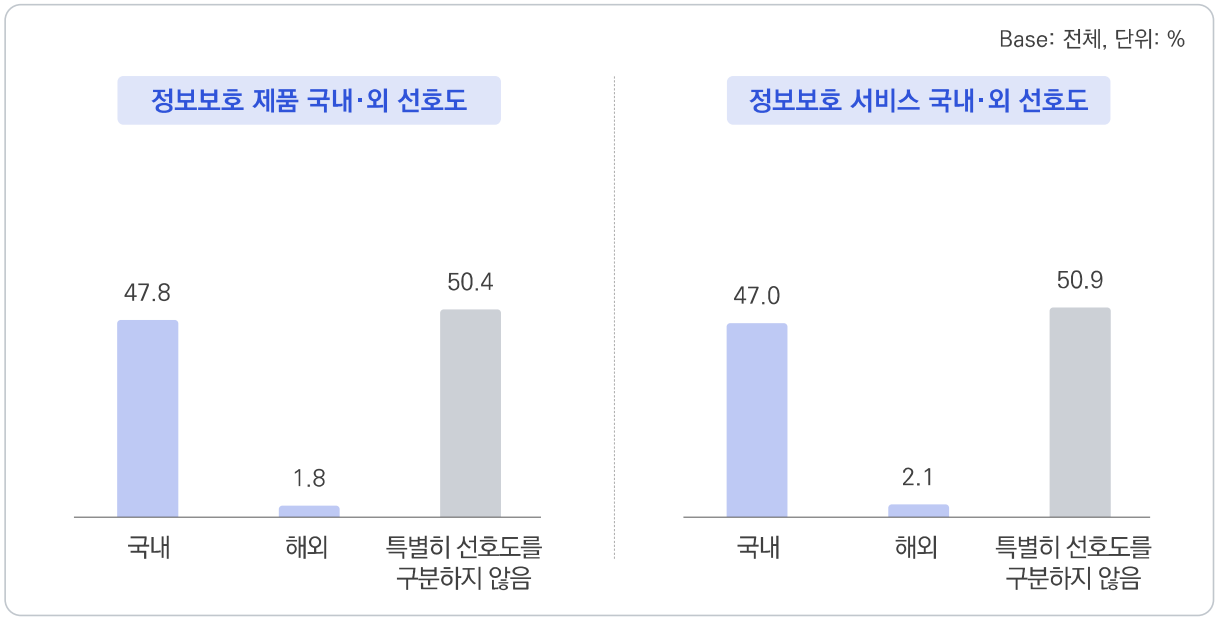


그림 1-3-61 **국내외 정보보호 제품 및 서비스 선호도**

- 국내/해외, 제품/서비스 관계 없이 모두 '성능'을 이유로 선호하는 비율이 높음

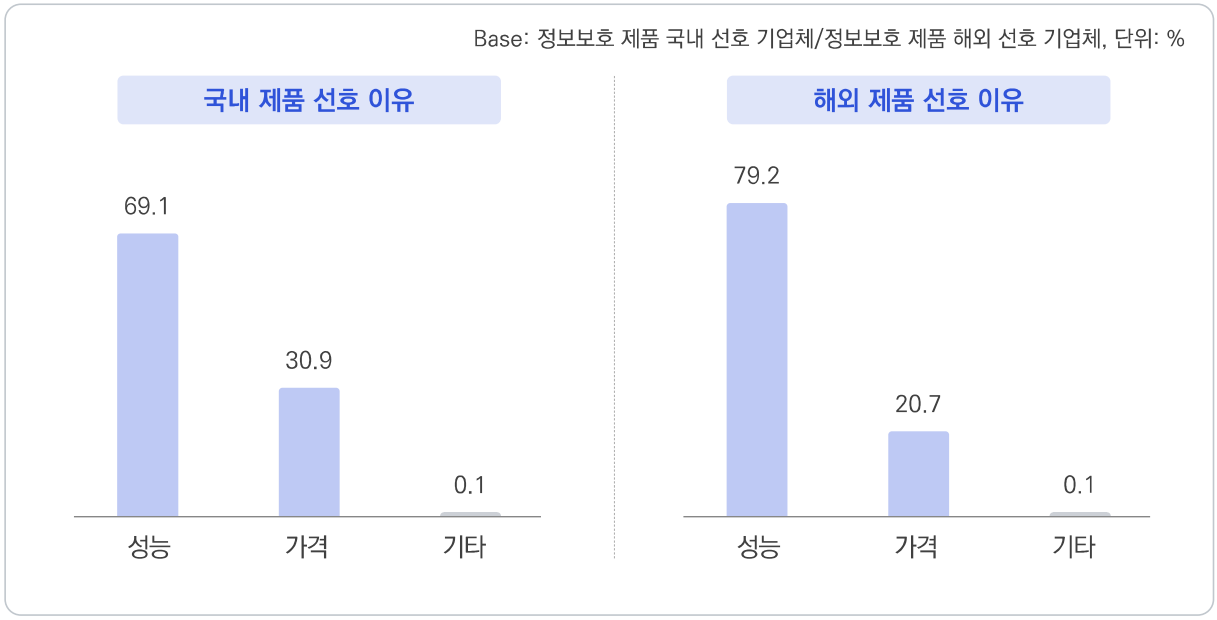


그림 1-3-62 **정보보호 제품 국내외 선호 이유**

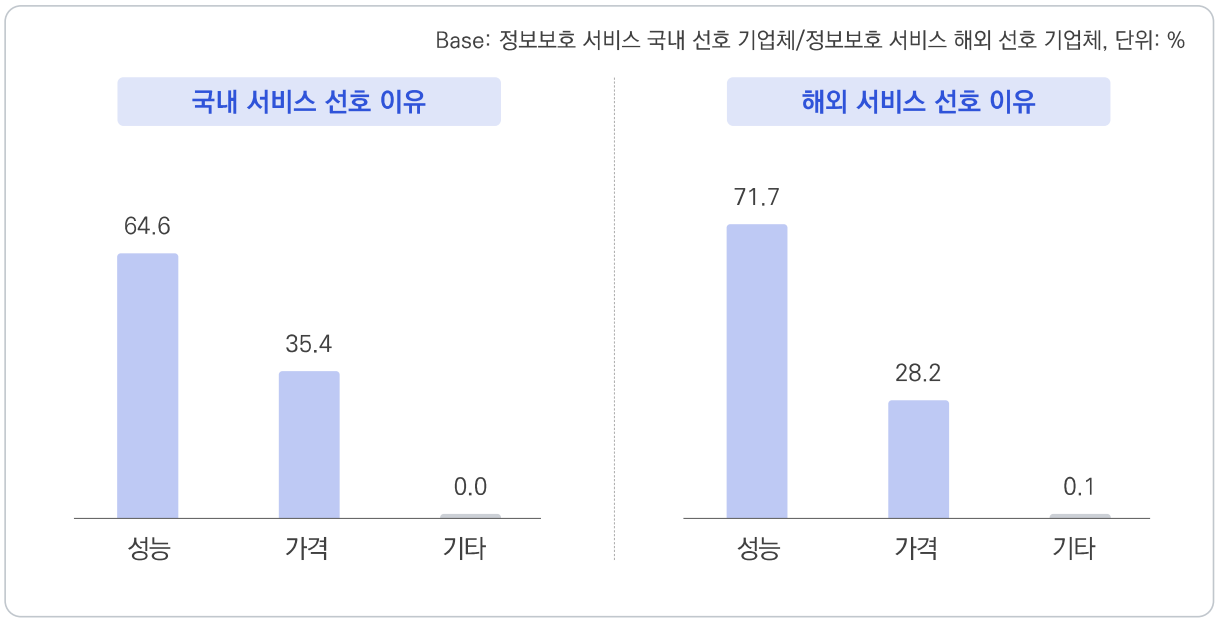


그림 1-3-63 정보보호 서비스 국내외 선호 이유

V 정보 침해사고 예방

1 정보보호 제품 및 서비스

- 기업체 중 98.7%는 정보보호 제품 및 서비스를 이용한다고 응답함

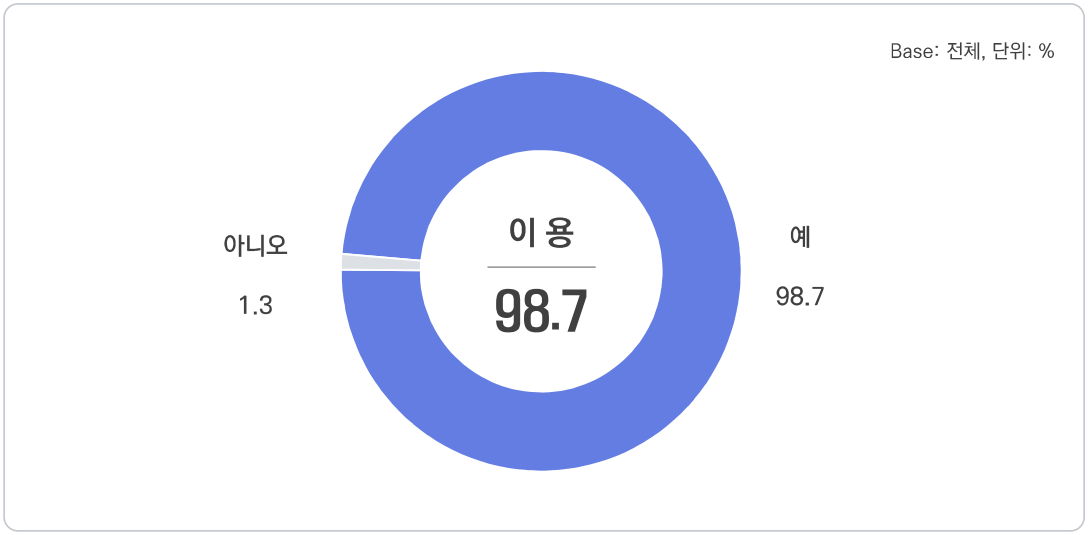


그림 1-3-64 정보보호 제품 및 서비스 이용

- 이용하고 있는 정보보안 제품 및 서비스로는 '네트워크 보안'이 94.5%로 가장 높고, 다음으로 '시스템(앤드포인트) 보안(94.1%)', '공통 인프라 보안(49.2%)' 등의 순임

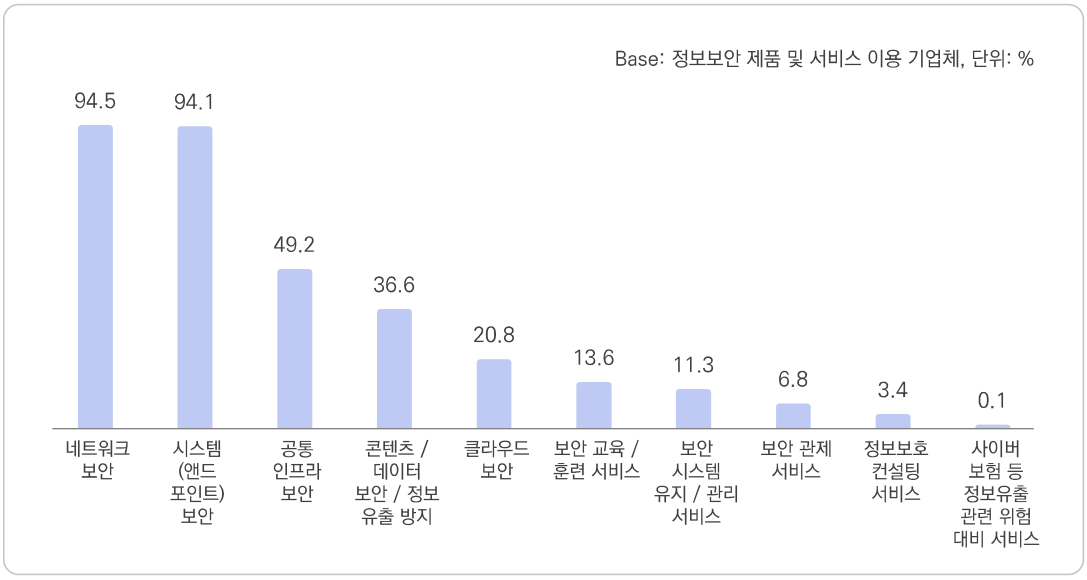


그림 1-3-65 이용하는 정보보호 제품 및 서비스_정보보안(복수응답)

- 이용하는 정보보호 제품의 유형으로 '네트워크 보안' 제품, '시스템(앤드 포인트) 보안' 제품, '콘텐츠/데이터 보안/정보유출 방지' 제품, '공통 인프라 보안' 제품은 '설치형' 제품을 많이 이용하고 있는 것으로 나타났고, '클라우드 보안' 제품은 '클라우드형' 제품을 상대적으로 많이 이용하는 것으로 나타남

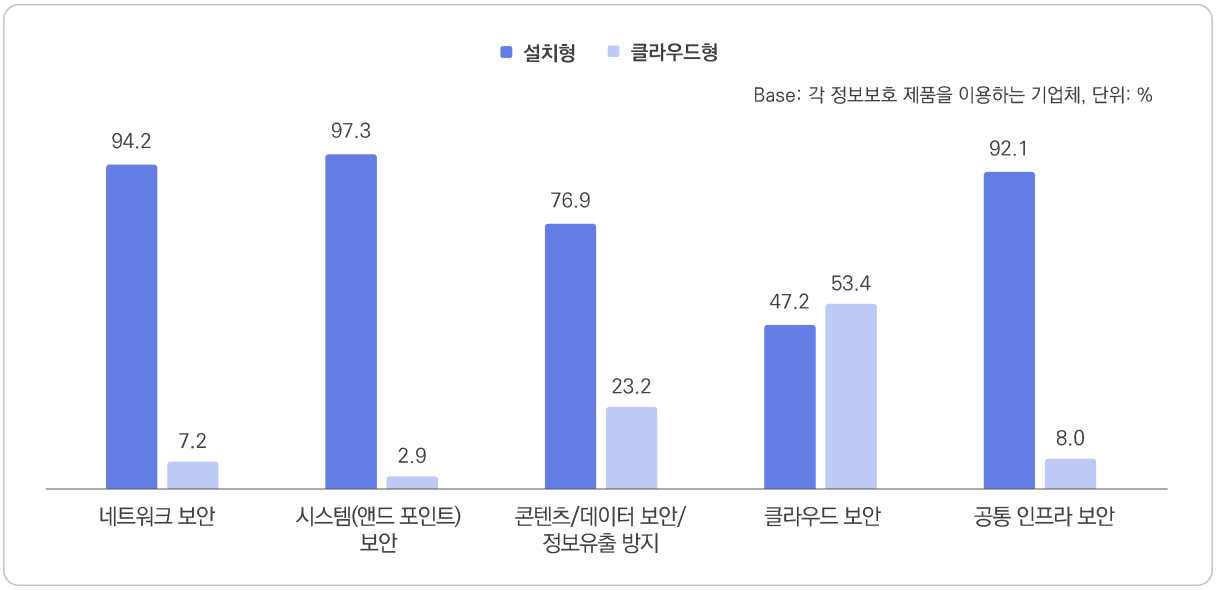


그림 1-3-66 이용하는 정보보호 제품의 유형

- 이용하고 있는 물리적 보안 제품 및 서비스로는 '영상 보안 시스템'이 96.1%로 가장 높고, 다음으로 '출동 보안 서비스(89.4%)', '출입 통제 관리 시스템(84.9%)', '불법 도·감청 탐지 서비스(0.3%)'의 순임

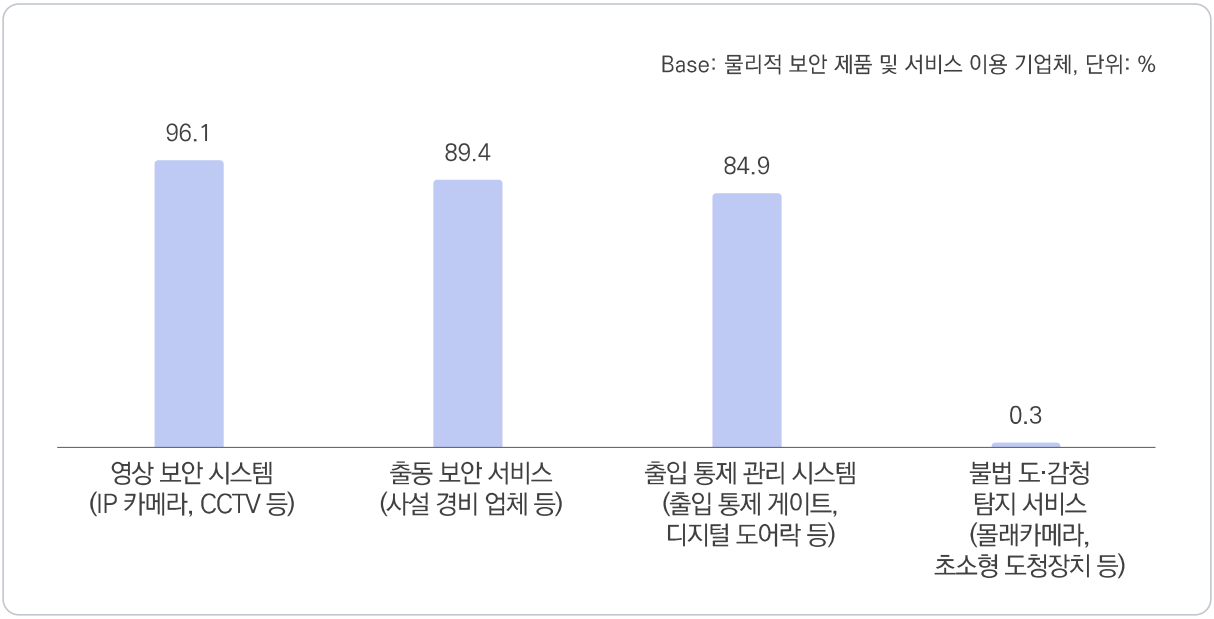


그림 1-3-67 이용하는 정보보호 제품 및 서비스_물리적 보안(복수응답)

- 정보보안 또는 물리적 보안 제품 및 서비스를 이용하는 기업체 중 19.8%가 사용 중인 제품 및 서비스의 정보보호 인증 여부를 인지하고 있는 것으로 나타남

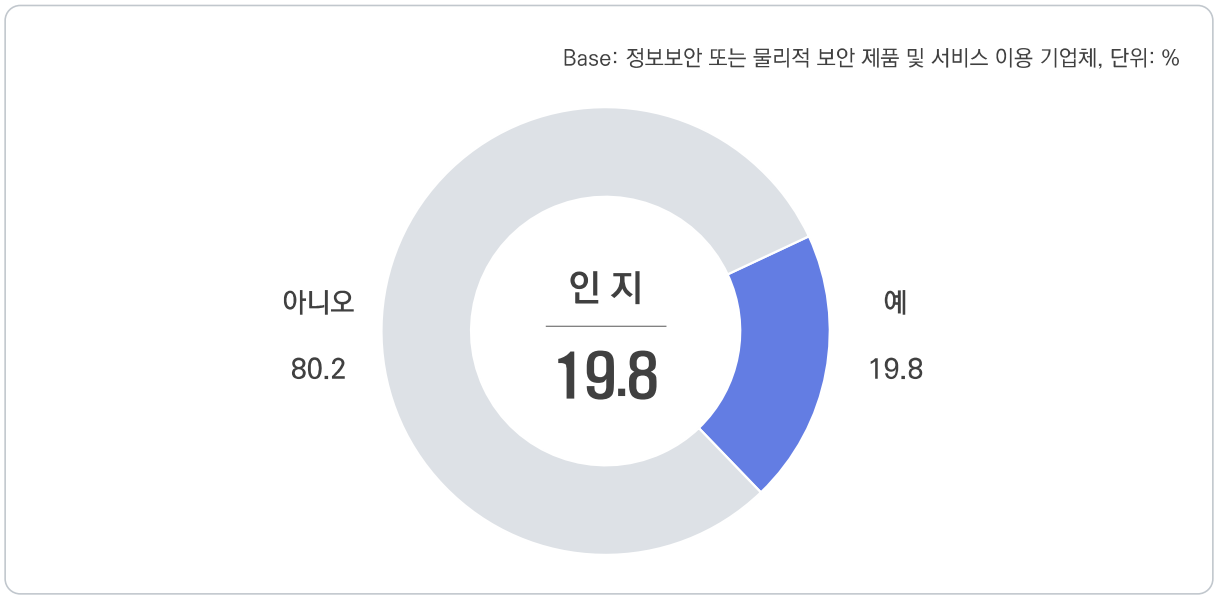


그림 1-3-68 이용하는 정보보호 제품 및 서비스의 정보보호 인증 인지

2 CCTV 관리 현황

가 주 사업장

- 주 사업장의 CCTV 관리 방법으로 '간접(업체 위탁) 관리'가 55.3%로 가장 높고, 다음으로 '직접 관리(31.4%)', '건물 자체 관리(18.8%)' 순임
- 관리 중인 CCTV 대수는 '간접(업체 위탁) 관리'가 15.3대로 가장 많고, 다음으로 '직접 관리(13.1대)', '건물 자체 관리(5.9대)' 순임

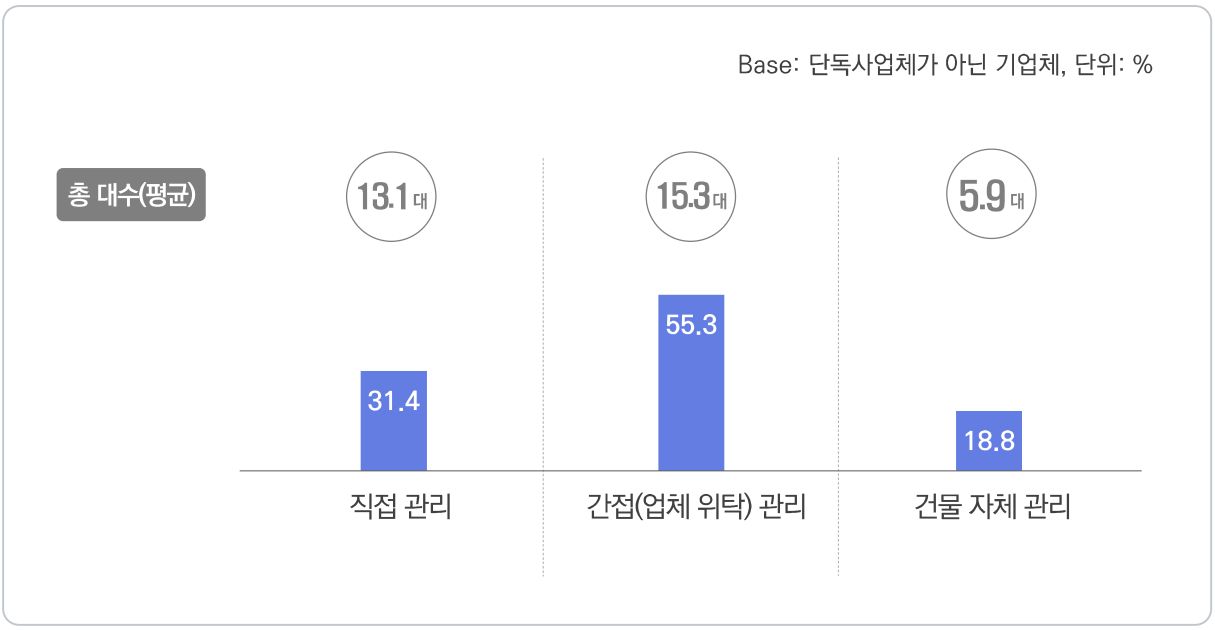


그림 1-3-69 CCTV 관리 현황_주 사업장(복수응답)

나 본사/본점

- 본사/본점의 CCTV 관리 방법으로 '직접 관리'가 78.0%로 가장 높고, 다음으로 '간접(업체 위탁) 관리(16.8%)', '건물 자체 관리(12.7%)' 순임
- 관리 중인 CCTV 대수는 '간접(업체 위탁) 관리'가 15.3대로 가장 많고, 다음으로 '직접 관리(10.8대)', '건물 자체 관리(5.6대)' 순임

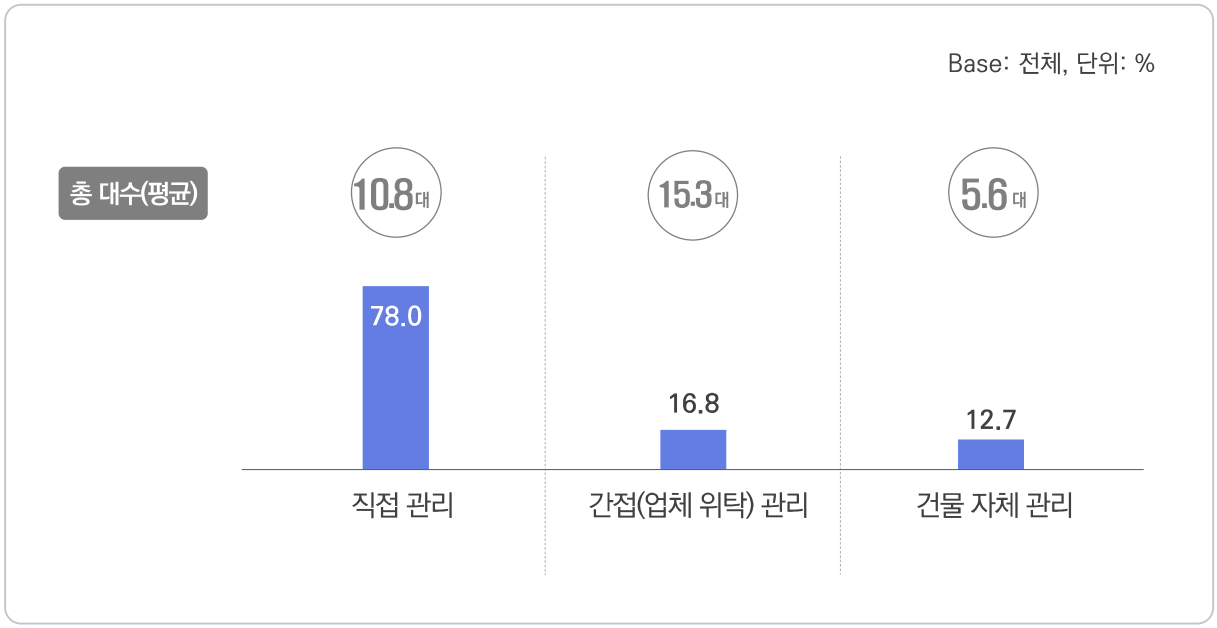


그림 1-3-70 CCTV 관리 현황_본사/본점(복수응답)

3 정보보호 관리

가 사내 IT 시스템 및 네트워크 보안 점검

- 기업체 중 88.1%가 사내 IT 시스템 및 네트워크에 대해 보안 점검을 실시하고 있다고 응답함
  - 실시 주기는 '1개월 이상 6개월 미만'이 29.1%로 가장 높음

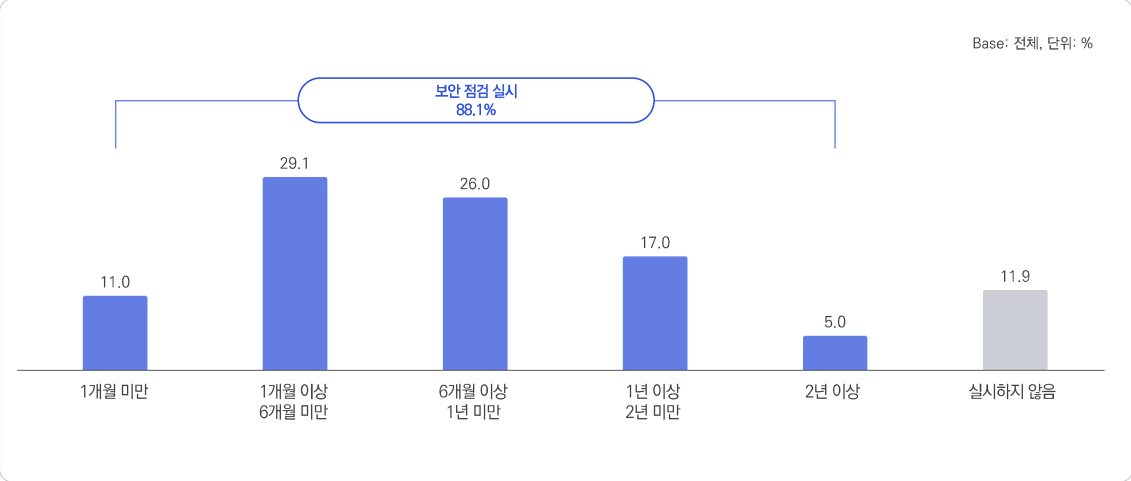


그림 1-3-71 사내 IT 시스템 및 네트워크 보안 점검

나 로그 기록 관리

- 사내 보안 점검을 실시하는 기업체 중 66.0%가 시스템 및 방화벽 로그 기록을 관리하고 있다고 응답함
- 로그 기록을 관리하는 기업체 중 '6개월 이상(30.1%)'의 주기로 로그 기록을 관리하는 비율이 가장 높음

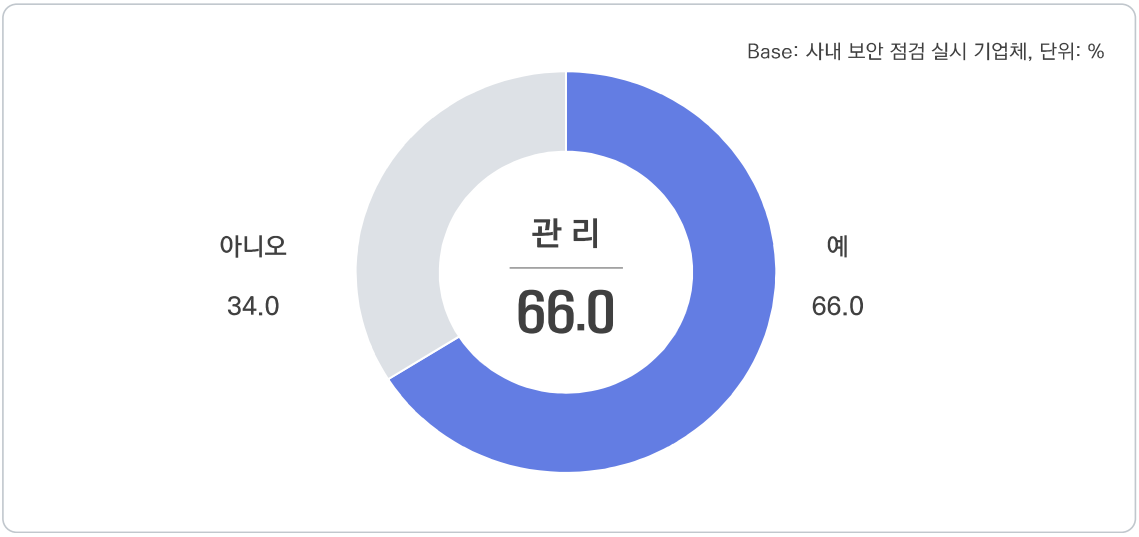


그림 1-3-72 시스템 및 방화벽 로그 기록 관리

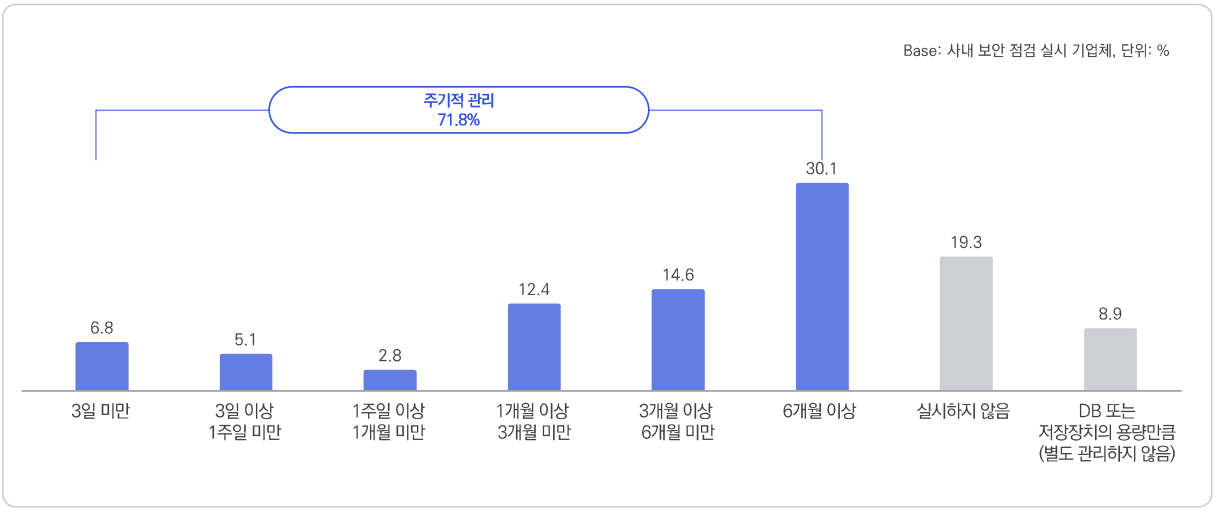


그림 1-3-73 시스템 및 방화벽 로그 기록 관리 주기

다 데이터 백업 관리

- 기업체 중 22.8%가 공식 문서로 작성된 백업 관련 정책 또는 규정집을 보유하고 있다고 응답함

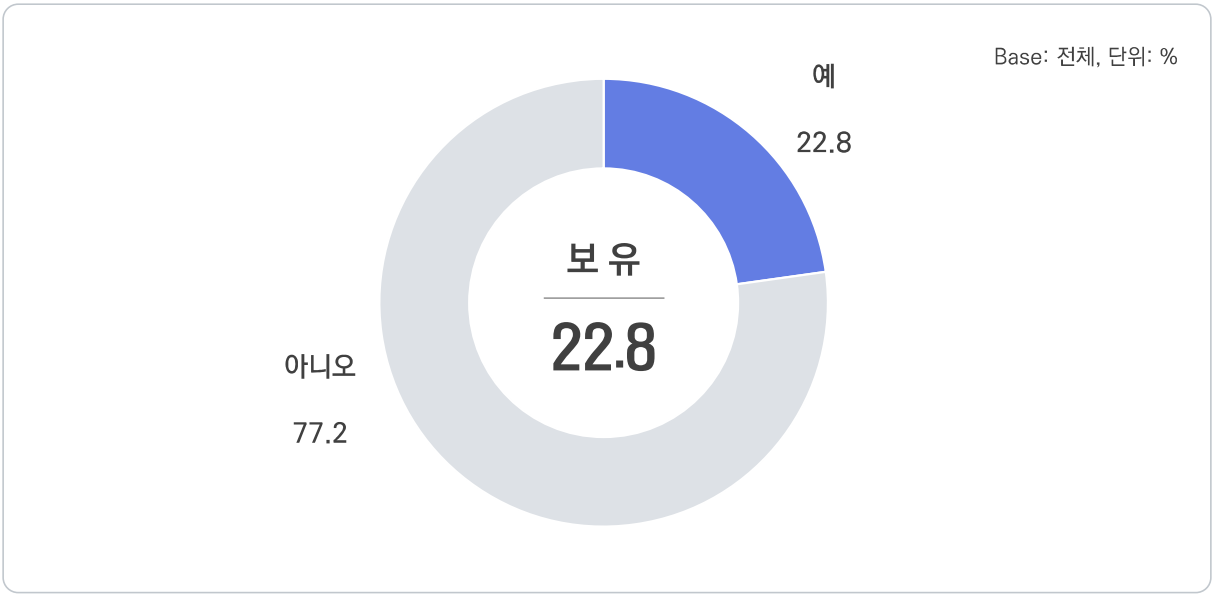


그림 1-3-74 백업 관련 정책·규정집 보유율

- 기업체 중 99.0%가 데이터 백업을 실시한다고 응답함

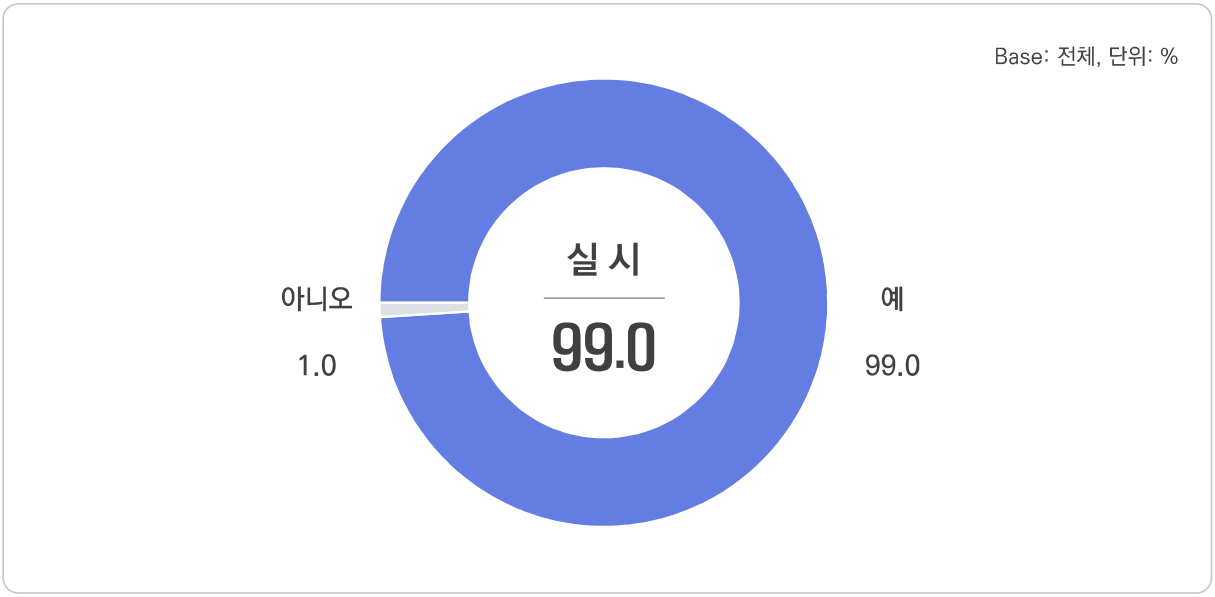


그림 1-3-75 데이터 백업 실시

- 데이터 유형별로는 '중요 데이터'의 백업 실시율이 94.0%로 가장 높고, 다음으로 '서버 데이터(60.5%)', '접속 로그 데이터(55.8%)' 등의 순임

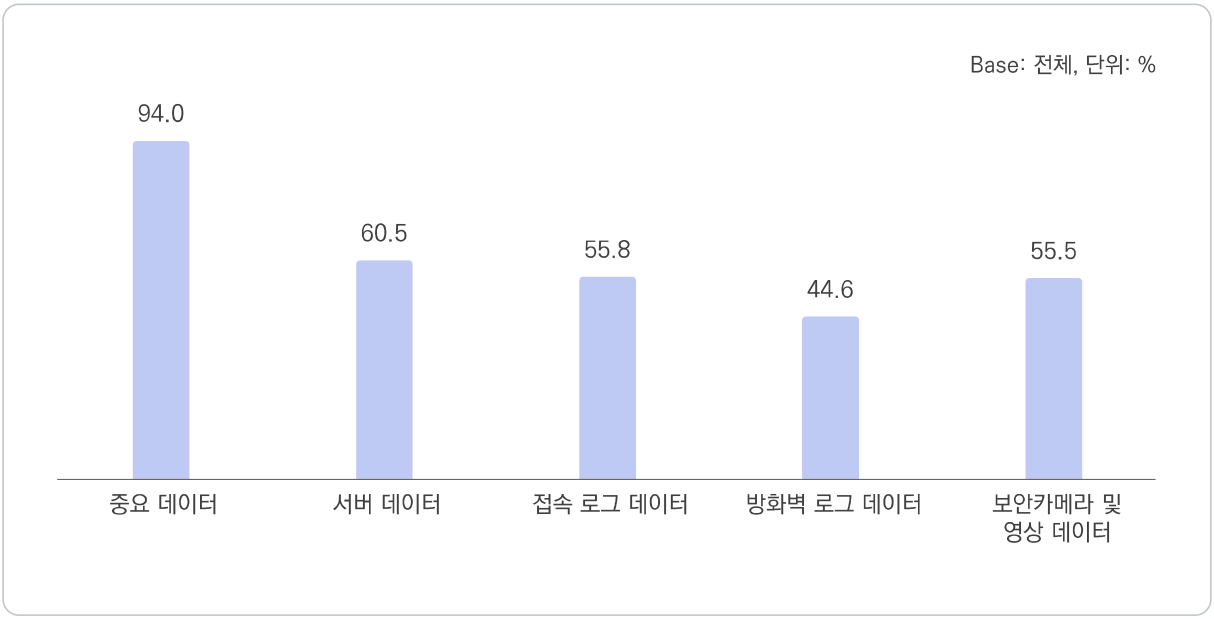


그림 1-3-76 데이터 유형별 백업 실시율

- 데이터 백업 방식으로는 ‘USB, 외장하드 등 별도 저장장치 활용’이 57.2%로 가장 높고, 다음으로 ‘운영 체제 백업 기능 사용(20.2%)’, ‘클라우드 서버 활용(15.0%)’ 등의 순임

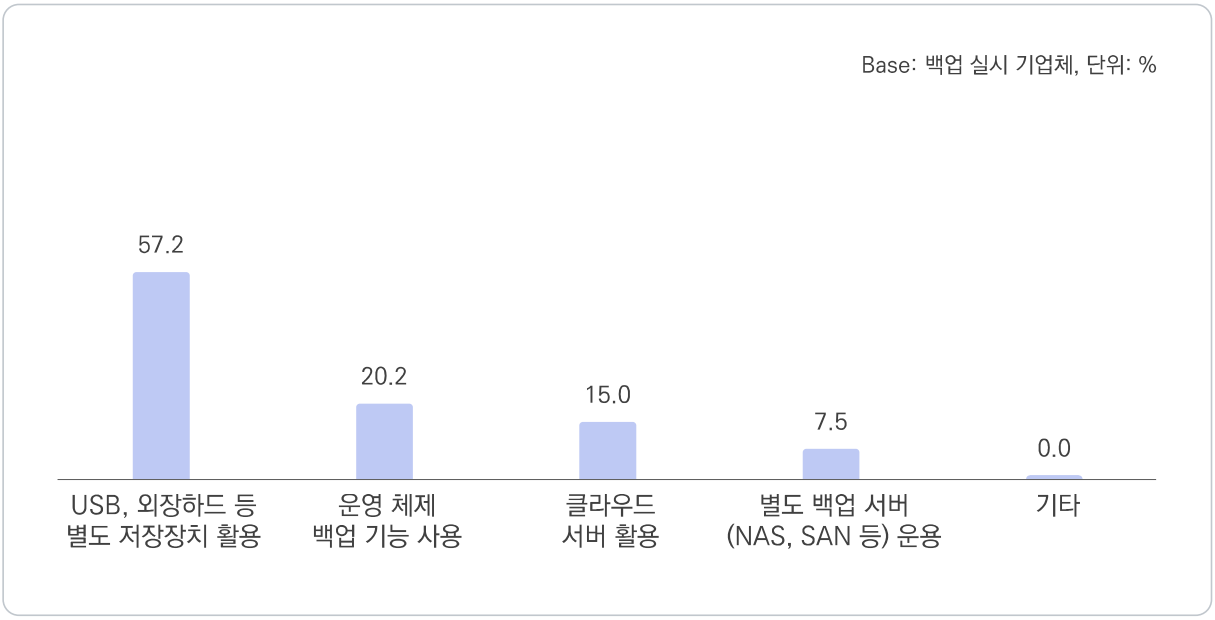


그림 1-3-77 데이터 백업 방식

- 데이터 백업 주기로는 ‘6개월에 1회 실시’가 21.1%로 가장 높고, 다음으로 ‘3개월에 1회 실시(18.6%)’, ‘1개월에 1회 실시(13.3%)’, ‘1년에 1회 실시(12.5%)’ 등의 순임
  - 정해진 주기 없이 백업을 실시하는 비율은 16.6%로 나타남

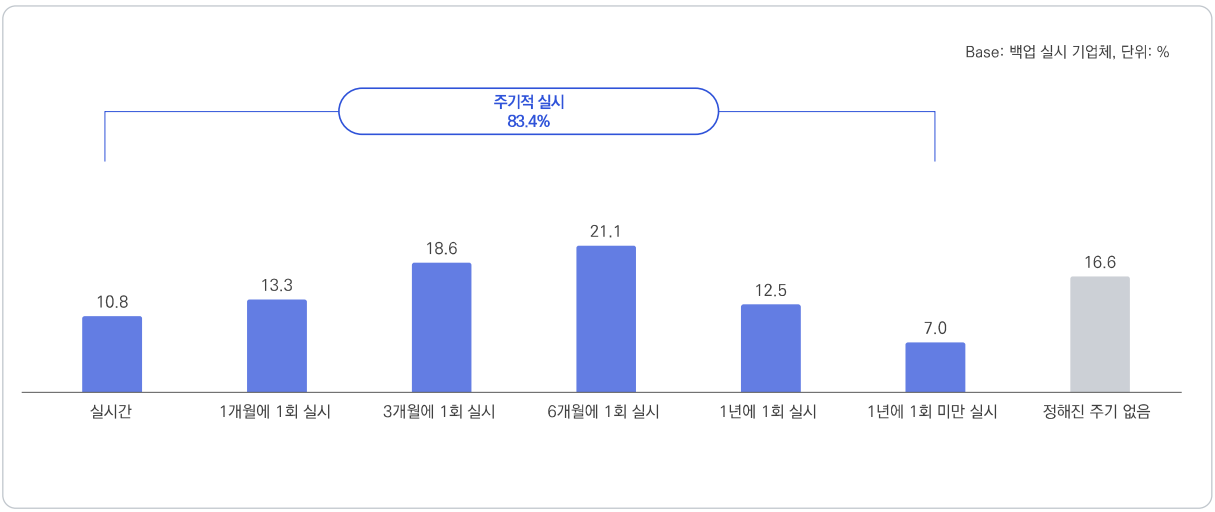


그림 1-3-78 데이터 백업 주기

라 정보 침해사고 사전 예방 능력

- 기업체의 정보 침해사고 사전 예방 능력에 대해 정보보안은 35.9%, 물리적 보안은 39.1%가 '안전하다(안전한 편이다+매우 안전하다)'고 응답함

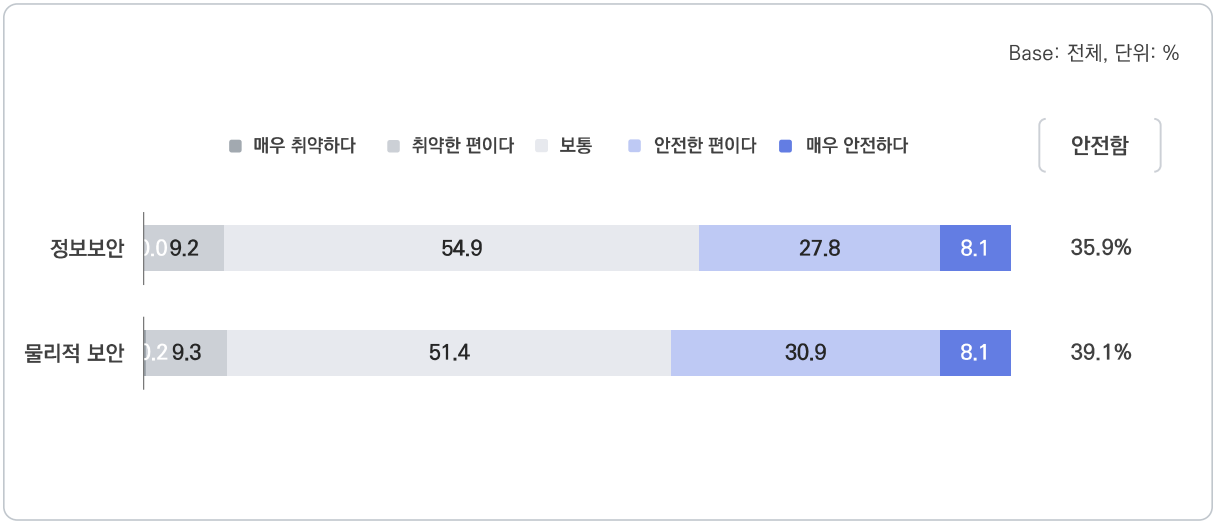


그림 1-3-79 정보 침해사고 사전 예방 능력

VI 정보 침해사고 경험

1 정보 침해사고 경험

가 정보 침해사고 발생 가능성

- 기업체 중 7.0%가 정보 침해사고의 발생 가능성이 '크다(그렇다+매우 그렇다)'고 응답함

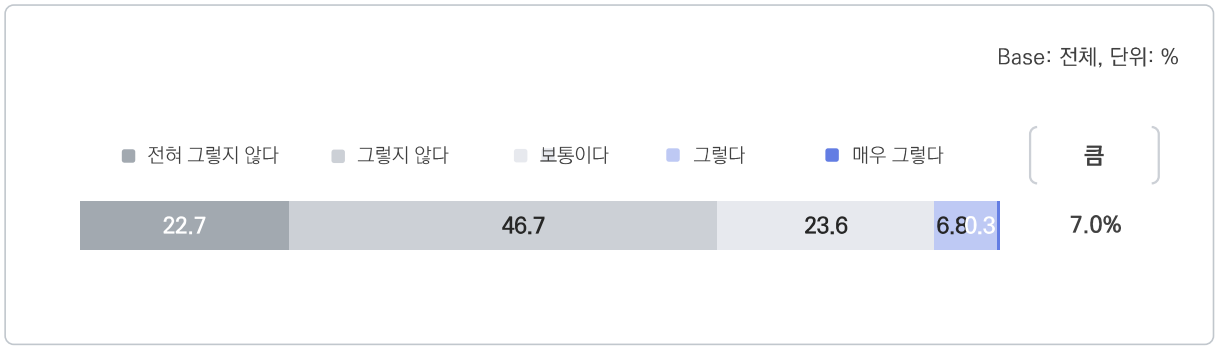


그림 1-3-80 정보 침해사고 발생 가능성

나 정보 침해사고 직접 경험

- 기업체 중 0.2%가 최근 1년간 정보 침해사고를 경험했다고 응답함

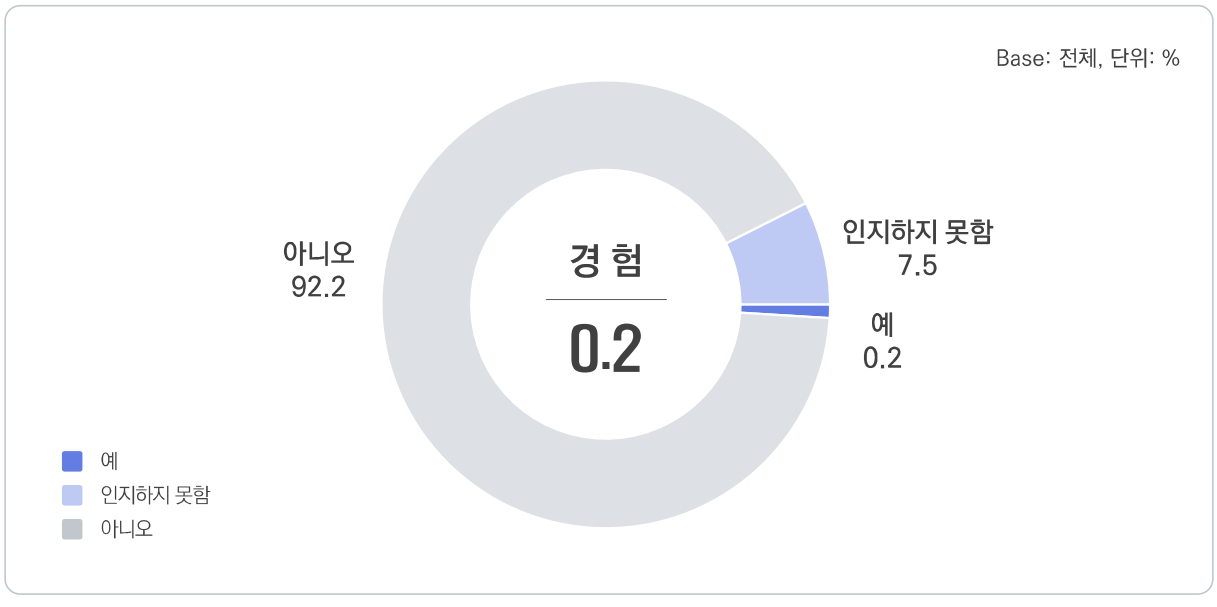


그림 1-3-81 정보 침해사고 직접 경험

- 업종별로 보면 최근 1년간 정보 침해사고를 직접 경험한 비율은 '사업시설 관리, 사업 지원 및 서비스업'이 3.2%로 가장 높고, 뒤이어 '전문 과학 및 기술 서비스업(0.7%)', '예술, 스포츠 및 여가 관련 서비스업'(0.4%) 등의 순임

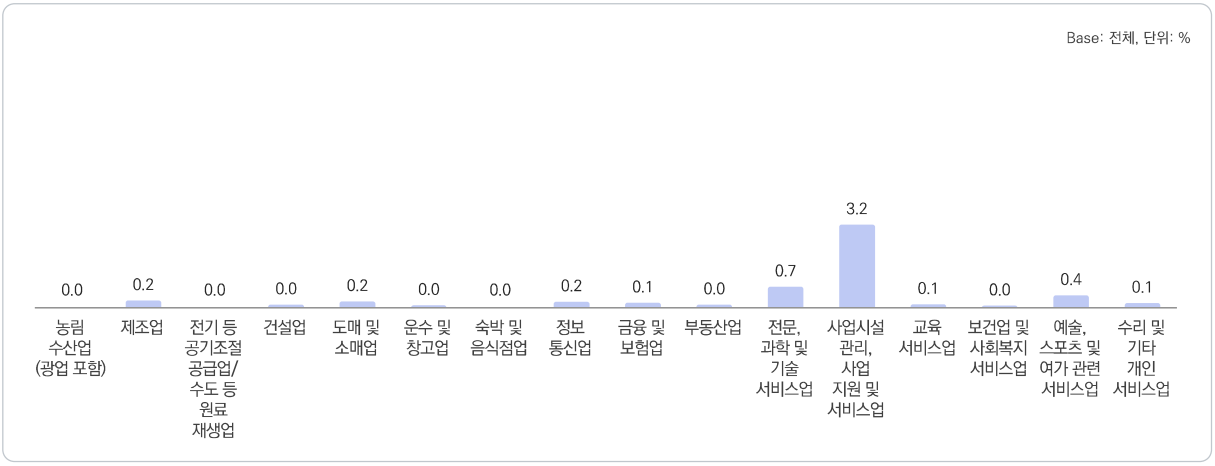


그림 1-3-82 업종별 정보 침해사고 직접 경험

- 규모가 클수록 최근 1년간 정보 침해사고를 직접 경험한 비율이 높음

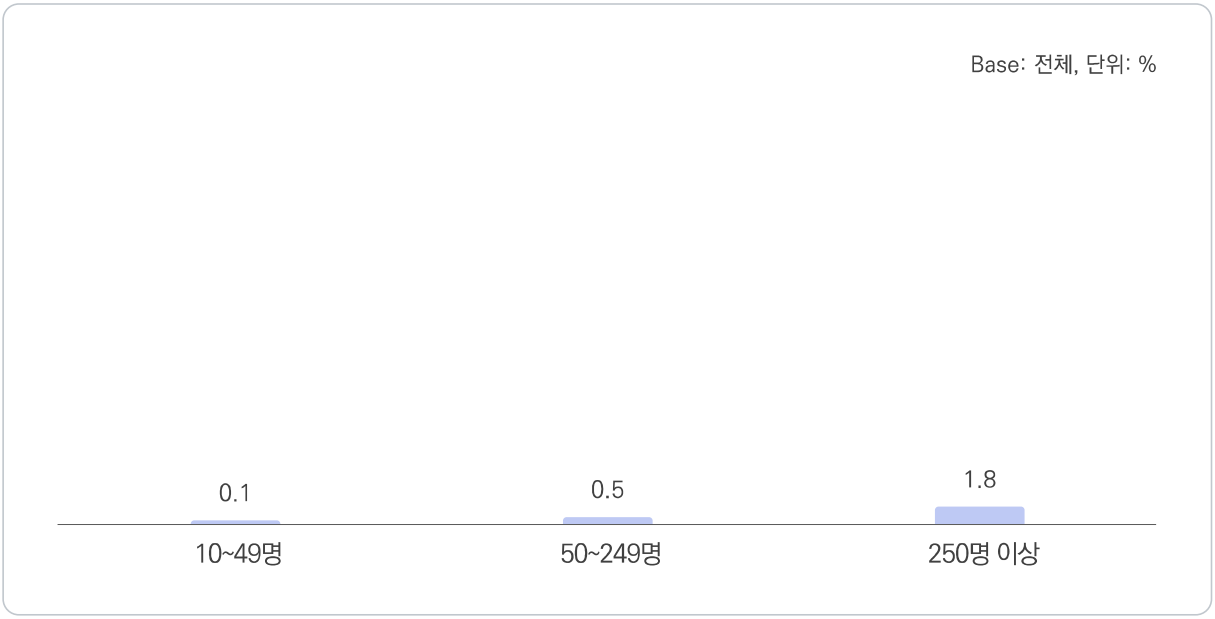


그림 1-3-83 규모별 정보 침해사고 직접 경험

다 기타 정보 침해사고 관련 경험

- 기업체 중 0.3%는 정보 침해사고를 의심한 경험*이 있다고 응답함
  * 의심 경험: 정보 침해사고 여부가 확실히 증명된 것은 아니지만 정황상 직·간접적으로 침해를 예상했던 경우
- 기업체 중 2.3%는 가까운 협력 또는 유관 업체의 정보 침해사고 피해 사실을 인지한 적 있다고 응답함

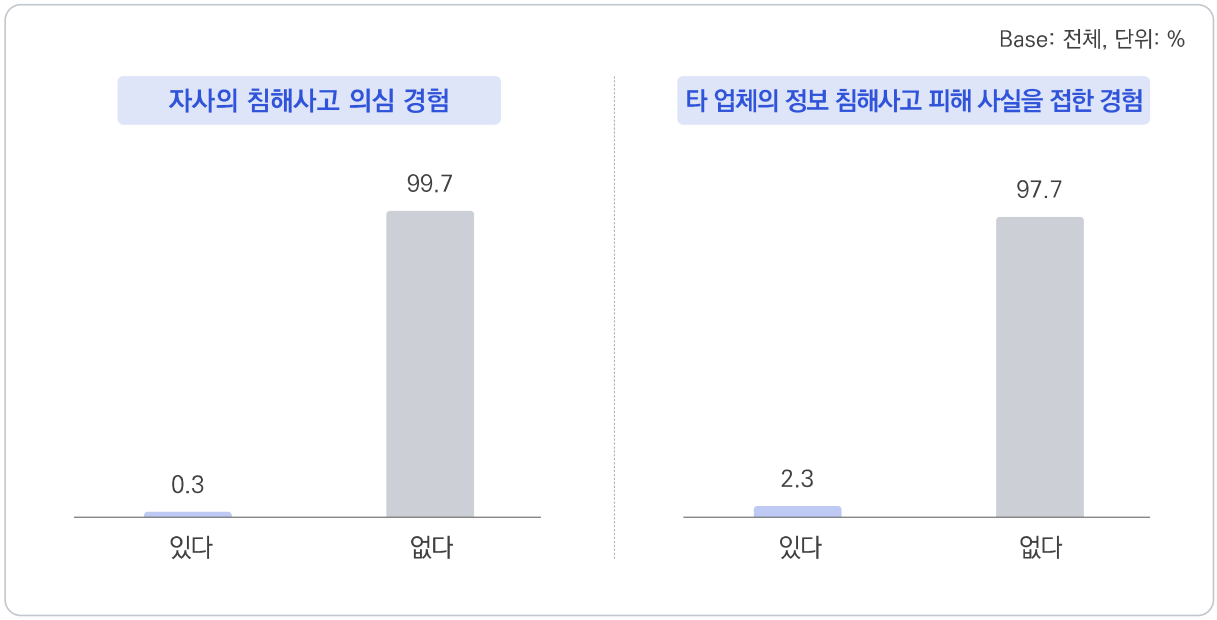


그림 1-3-84 기타 정보 침해사고 관련 경험

라 정보 침해사고 경험 유형

- 정보 침해사고 경험 유형별로 보면 '외부로부터 침투한 비인가 접근(해킹)'이 73.0%로 가장 높고, 다음으로 '컴퓨터 바이러스, 웜, 트로이잔, APT 공격으로 인한 IT시스템 마비(30.6%)', '랜섬웨어 감염(20.0%)' 등의 순임

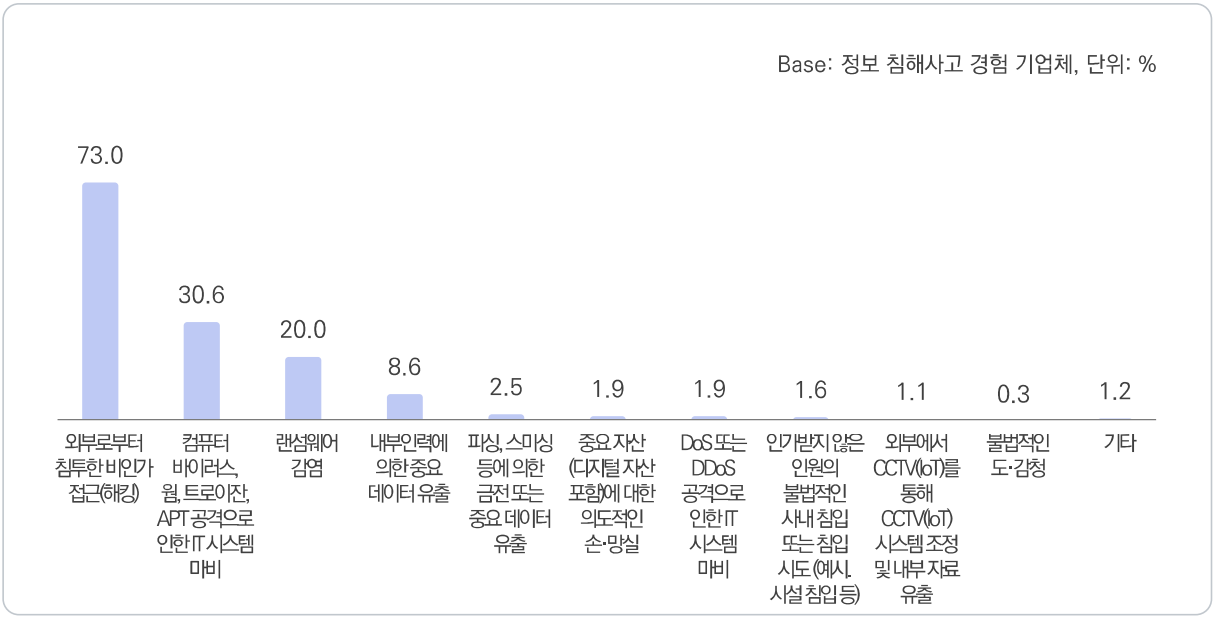


그림 1-3-85 정보 침해사고 경험 유형(복수응답)

마 정보 침해사고 인지 경로

- 정보 침해사고 인지 경로는 '보안 시스템의 침해사고 경보(알림)'가 61.3%로 가장 높고, 다음으로 '기존과는 다른 시스템 설정의 변경 또는 보유하고 있는 데이터의 위변조 사항 발견(33.3%)', '보안 시스템의 임의적 해제 또는 침입 흔적 발견(물리적 침입 포함)(6.3%)' 등의 순임

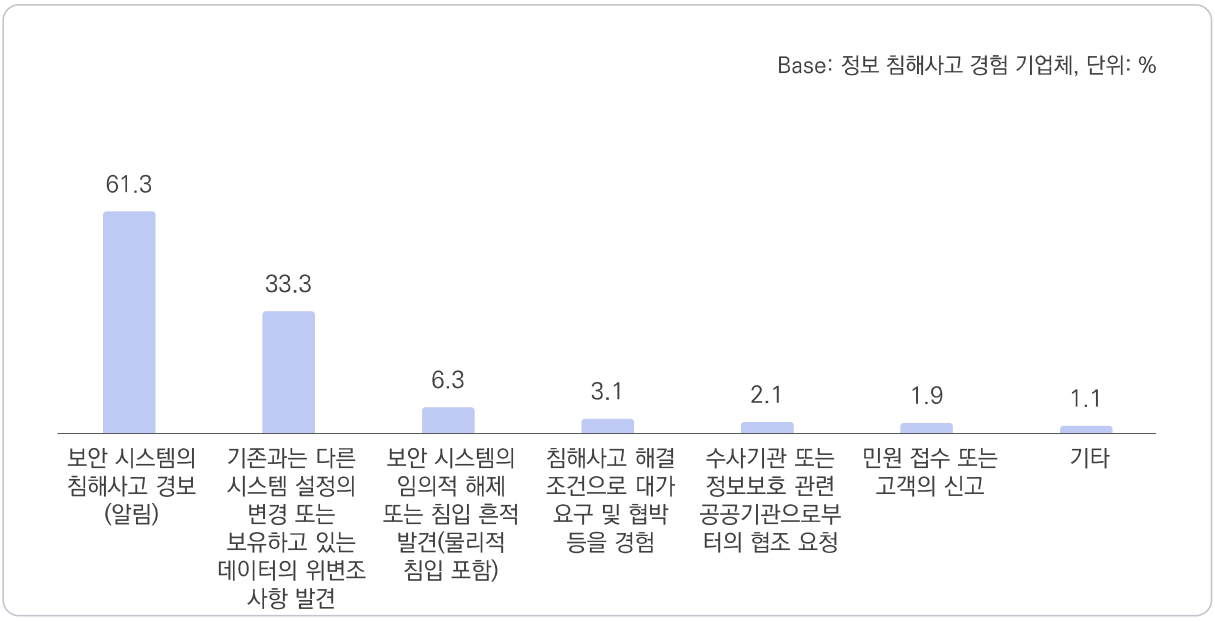
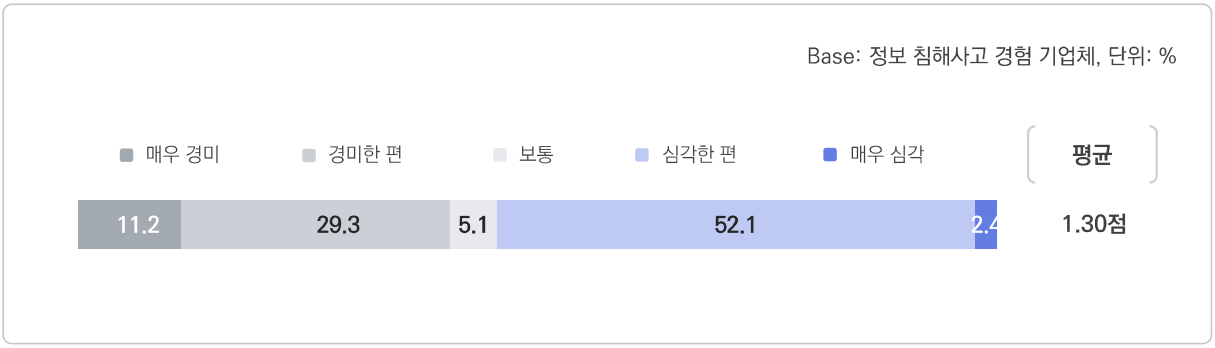


그림 1-3-86 정보 침해사고 인지 경로(복수응답)

바 정보 침해사고 심각성 정도

- 정보 침해사고를 경험한 기업체의 피해 심각성은 평균 1.30점으로 다소 심각한 편으로 나타남



* '평균'은 -5점(침해사고는 있었으나, 경제적 피해는 매우 경미하다)부터 5점(단시간에 회복되기 어려운 경제적 피해가 있었다) 중에 응답한 점수를 평균화한 것임

그림 1-3-87 정보 침해사고 심각성 정도

2 정보 침해사고 대응

가 정보 침해사고 단계별 소요 시간

- 정보 침해사고를 경험한 기업체의 단계별 소요 시간에 대해 인지 단계에서 '1일 이내'의 비율이 57.0%로 가장 높게 나타남
- 문제 해결 및 서비스 복원 단계에서 '1시간 이내'의 비율이 35.0%로 가장 높았음

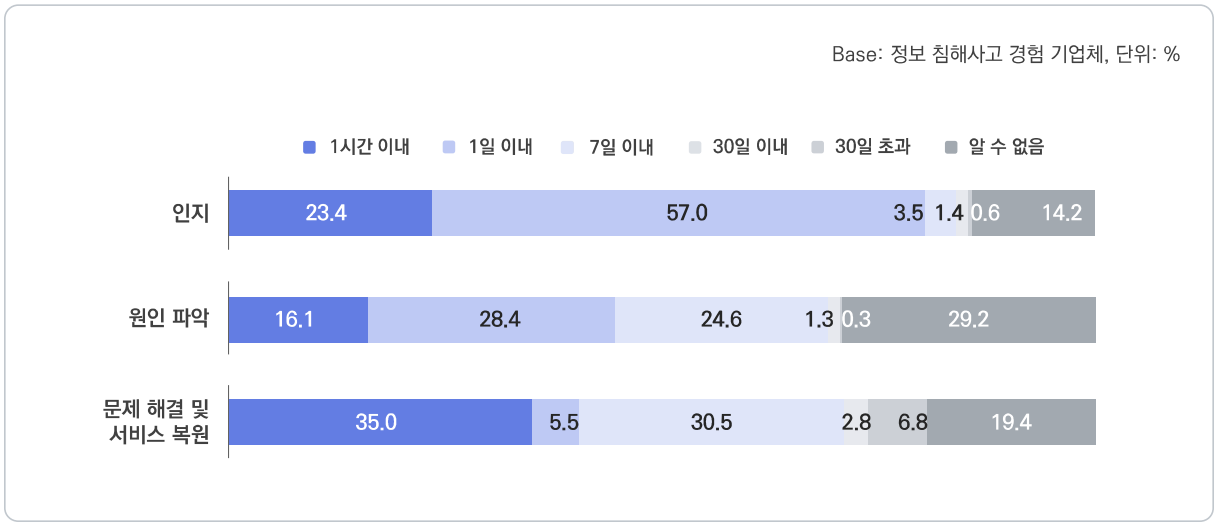


그림 1-3-88 정보 침해사고 단계별 소요 시간

나 정보 침해사고 시 신고 여부

- 정보 침해사고를 경험한 기업체 중 31.4%가 관련 기관 또는 수사기관에 신고했다고 응답함

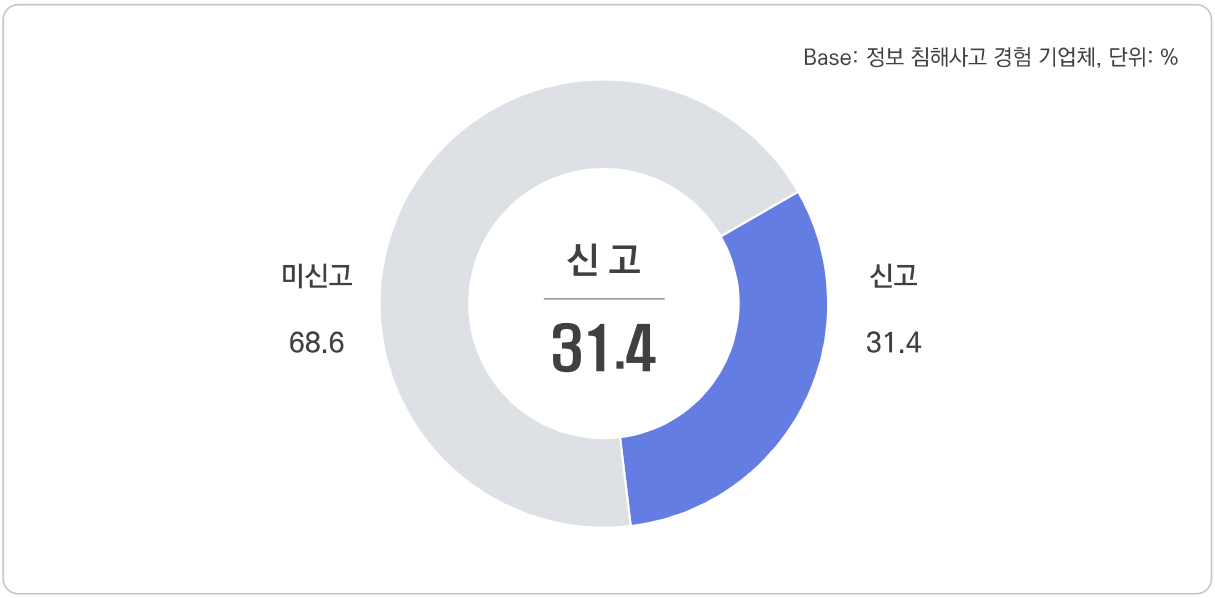


그림 1-3-89 정보 침해사고 시 신고 여부

- 정보 침해사고를 경험한 기업체의 침해사고 시 신고율은 종사자 규모 '250명 이상(43.6%)'에서 가장 높음

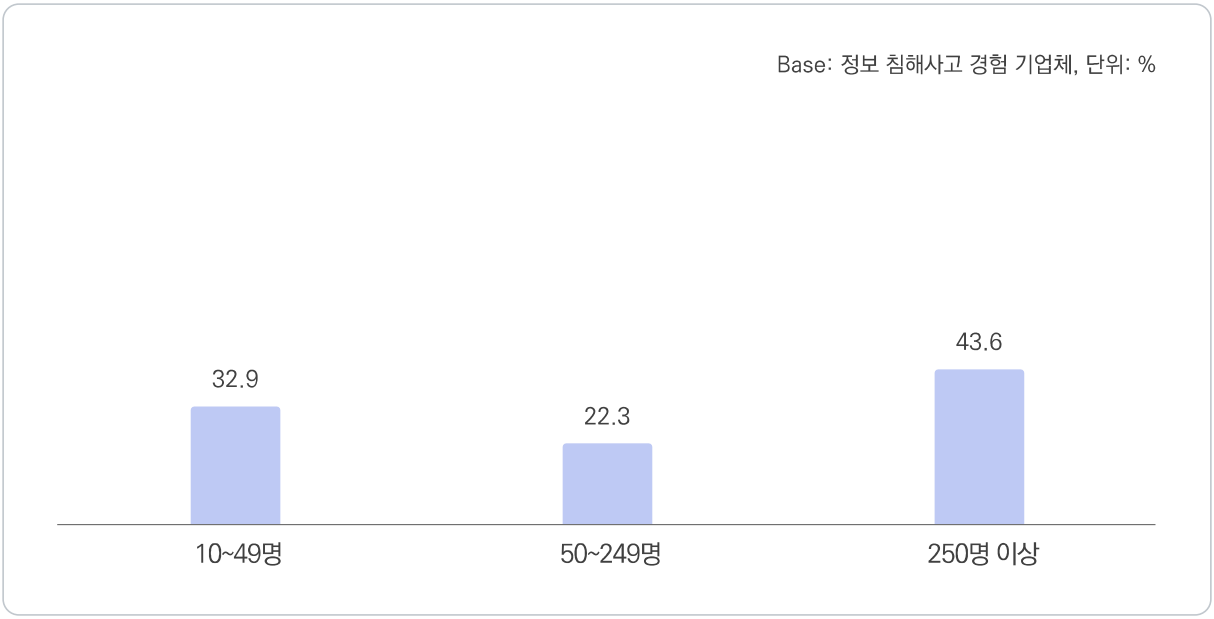


그림 1-3-90 규모별 정보 침해사고 시 신고율

- 정보 침해사고 경험 후 신고하지 않은 이유로는 '피해 규모가 경미하기 때문에'가 89.2%로 가장 높고, 다음으로 '신고에 따른 업무가 복잡하기 때문에(41.2%)', '피해 사실이 알려지는 것이 두렵기 때문에(8.4%)' 등의 순임

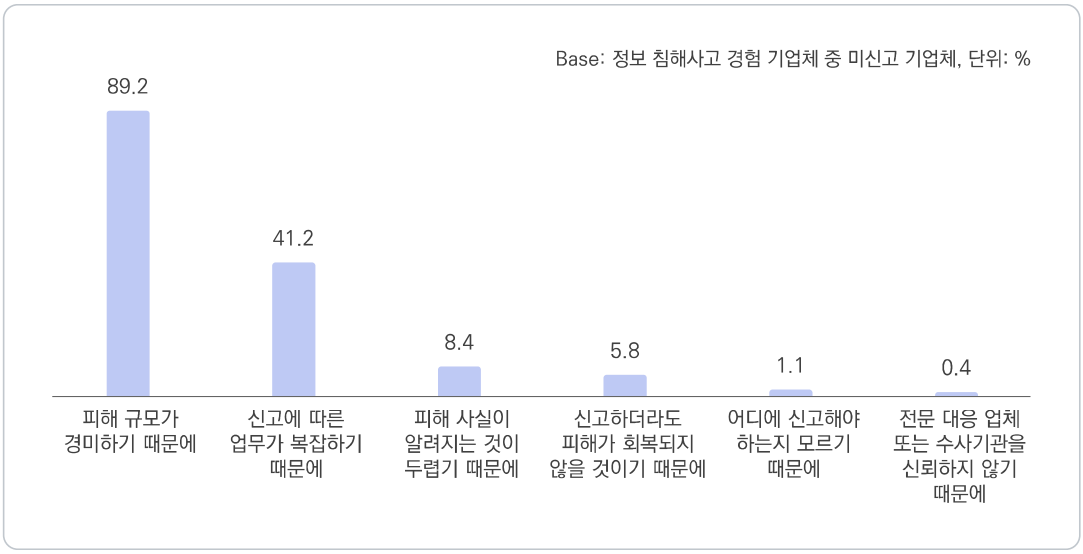


그림 1-3-91 **정보 침해사고 시 미신고 이유(1+2순위)**

다 정보 침해사고 대응

- 정보 침해사고 경험 이후 대응 활동으로는 '정보보호 관련 제품 및 솔루션 구축 및 고도화'가 31.5%로 가장 높고, 다음으로 '내부 정보 보호 정책 수립 또는 수정(29.2%)', '별도의 침해사고 대응팀(CERT) 구축(8.8%)' 등의 순임
  - 정보 침해사고 경험 이후 별다른 활동을 수행하지 않은 비율은 41.4%임

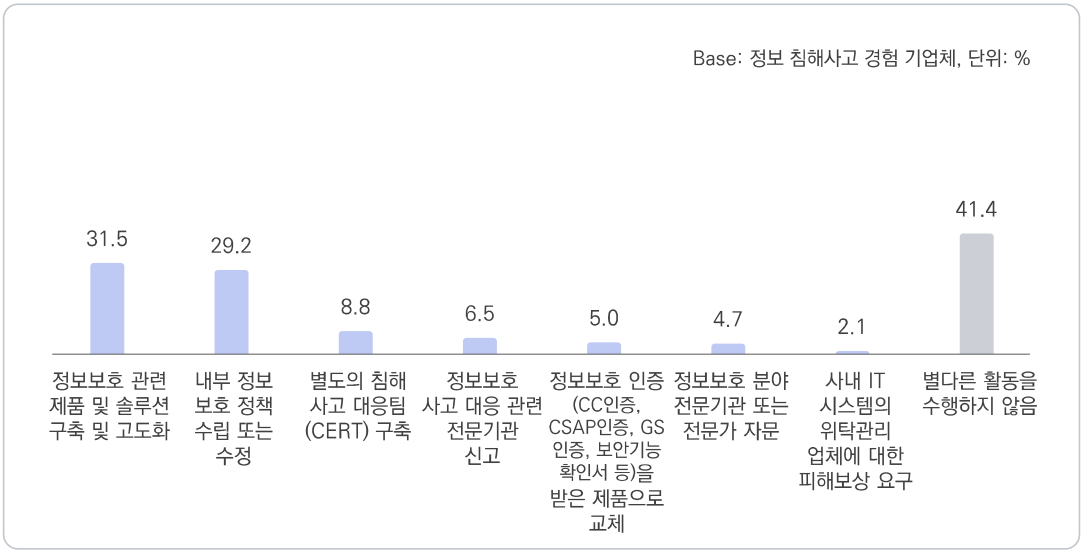


그림 1-3-92 **정보 침해사고 대응(복수응답)**

라 정보 침해사고 사후 대응 능력

- 정보 침해사고 경험 이후 기업의 종합적인 정보 침해사고 사후 대응 능력에 대해 정보보안은 31.2%, 물리적 보안은 25.7%가 '안전하다(안전한 편이다+매우 안전하다)'고 응답함

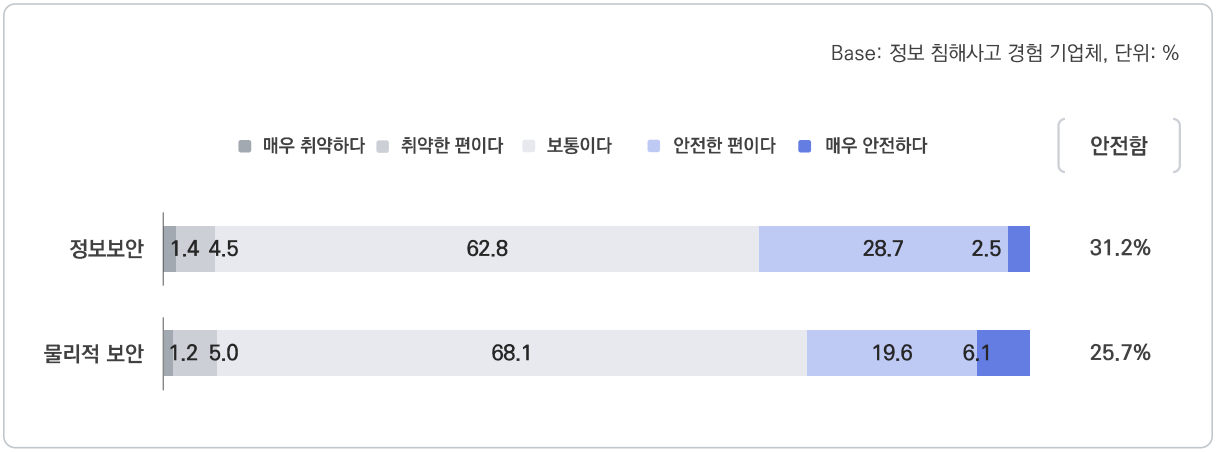


그림 1-3-93 정보 침해사고 사후 대응 능력

마 정보 침해사고 경험 후 관심 변화

- 정보 침해사고를 경험한 기업체 중 99.5%가 사고 이후 정보 침해사고에 대한 관심이 '증가했다(관심이 커졌다+관심이 매우 커졌다)'고 응답함

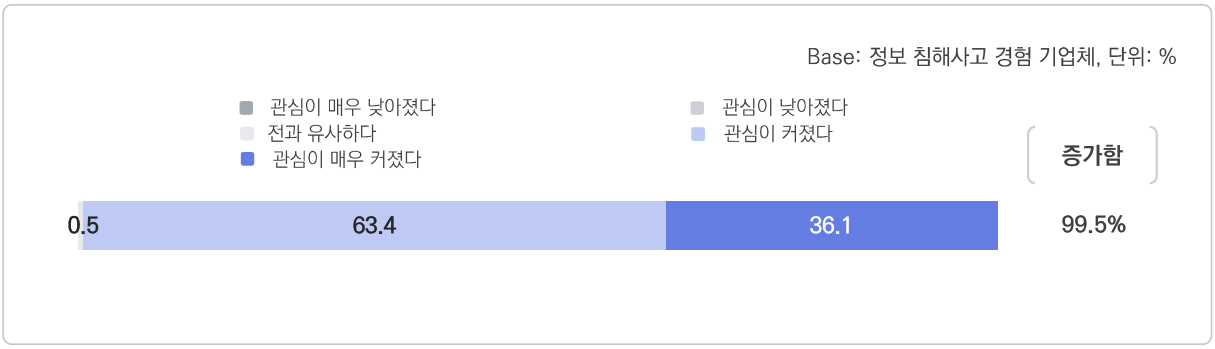


그림 1-3-94 정보 침해사고 경험 후 관심 변화

Ⅶ 사이버 보험

1 사이버 보험 인지

- 기업체 중 14.0%가 사이버 보험에 대해 '알고 있다(잘 알고 있다+대략적인 의미와 특징만 알고 있다+용어 정도만 들어본 적 있다)'고 응답함

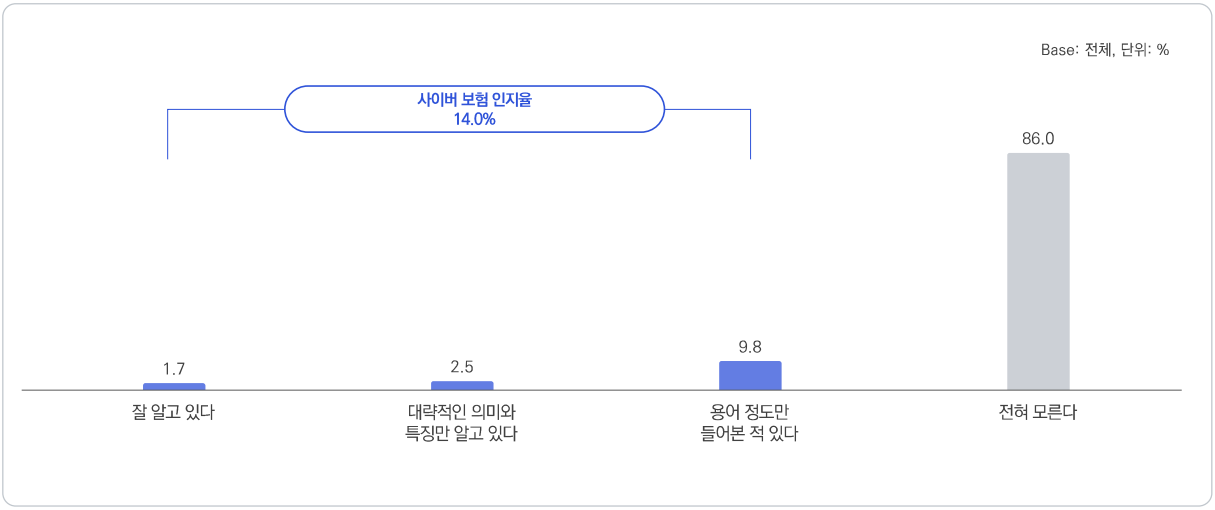


그림 1-3-95 사이버 보험 인지

2 사이버 보험 가입 또는 이용

가 사이버 보험 가입 또는 이용

- 사이버 보험을 알고 있는 기업체 중 3.1%가 가입 경험이 있다고 응답함

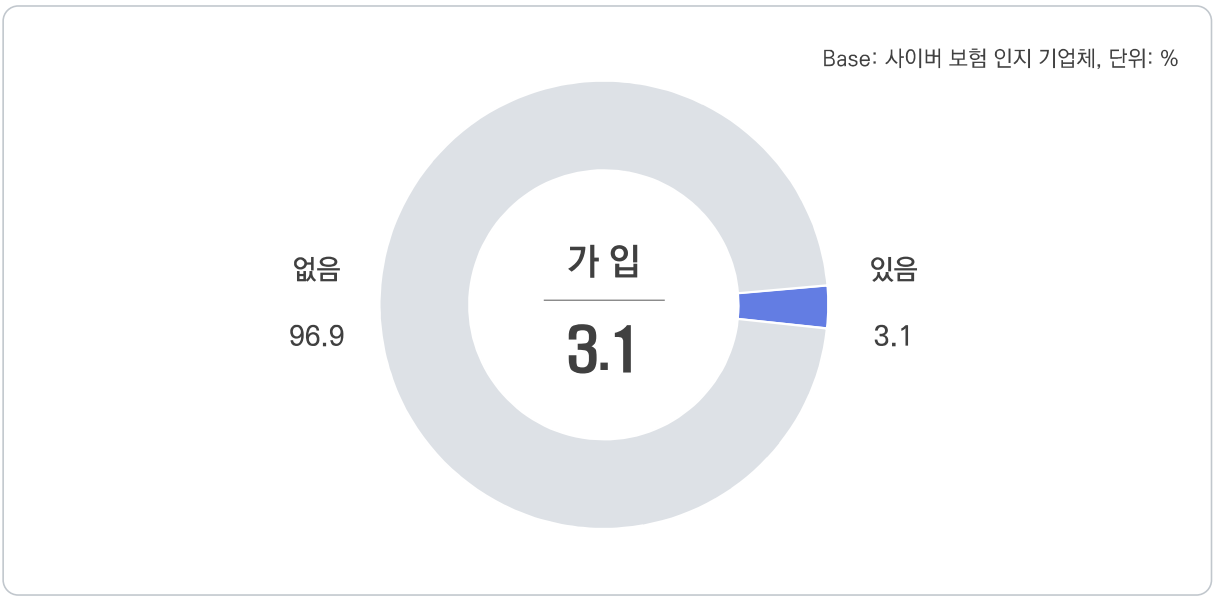


그림 1-3-96 사이버 보험 가입 경험

- 사이버 보험 가입 경험이 있는 기업체 중 51.7%가 현재 사이버 보험을 이용 중인 것으로 나타남

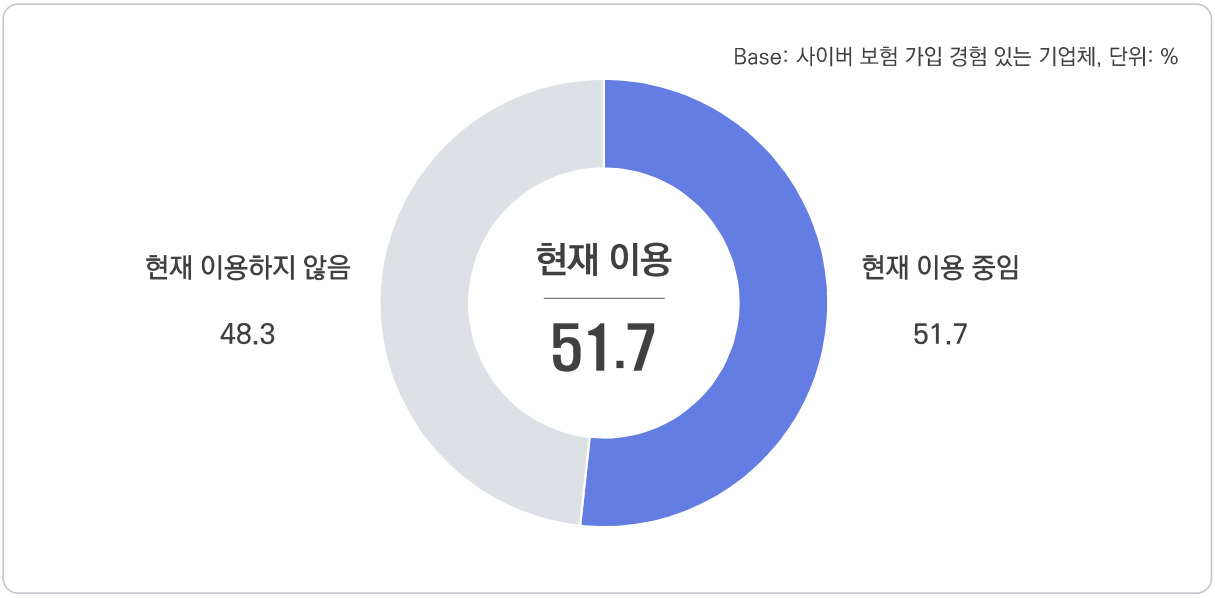


그림 1-3-97 사이버 보험 현재 이용

나 사이버 보험 향후 가입·유지 계획

- 사이버 보험을 알고 있는 기업체 중 2.6%가 향후 사이버 보험을 신규로 가입하거나 현재 가입 상태를 유지할 계획이 있다고 응답함

그림 1-3-98 사이버 보험 가입·유지 계획

- 향후 사이버 보험에 대한 가입 또는 유지 계획이 있는 기업체가 사이버 보험 가입 시 보장받고자 하는 항목으로는 '기업 사이버 공격 발생 시 시스템 복구 또는 정상화 비용'이 56.4%로 가장 높고, 다음으로 '기업 기밀 유출 관련 소송 비용(42.3%)', '사이버 갈취로 인한 손해(25.1%)' 등의 순임

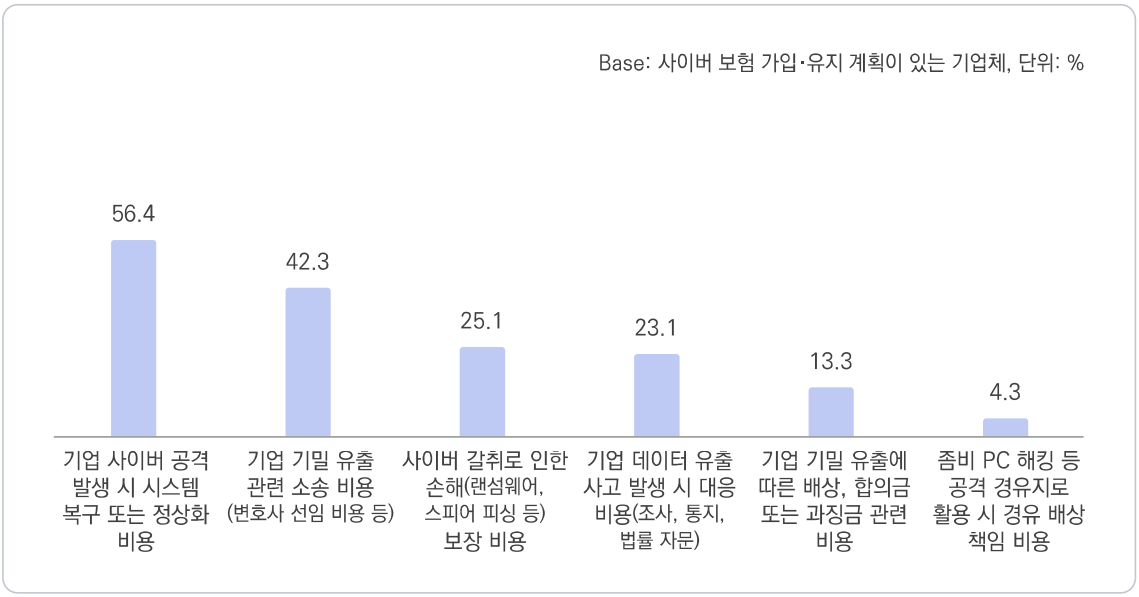


그림 1-3-99 사이버 보험 가입 시 보장받고자 하는 항목(1+2순위)

Ⅷ 원격근무

- 기업체 중 5.4%가 최근 1년간 원격근무를 시행했다고 응답함

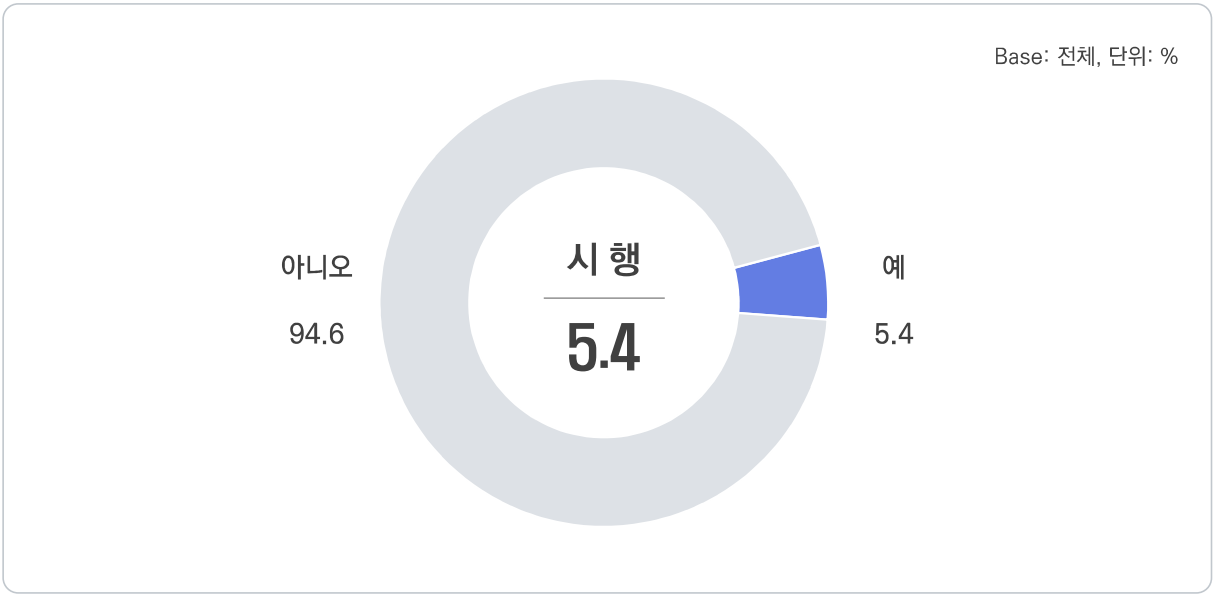


그림 1-3-100 원격근무 시행

- 원격근무 시행 시 직원에게 보안 솔루션을 지원한 비율은 82.6%로 나타남
- 지원한 보안 솔루션으로는 '자체 구축한 가상사설망(VPN)'이 26.3%로 가장 높음

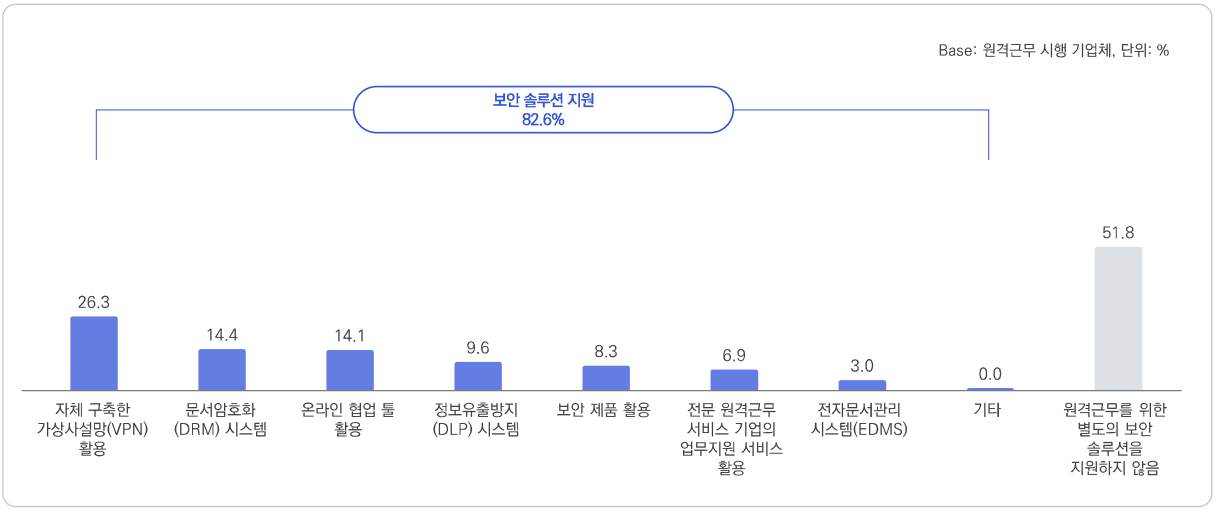


그림 1-3-101 원격근무 시 직원에게 지원한 보안 솔루션(복수응답)

- 원격근무를 시행한 기업체 중 34.5%가 원격근무 시 정보보호 위험성을 '인지하고 있다(그런 편이다+매우 그렇다)'고 응답함

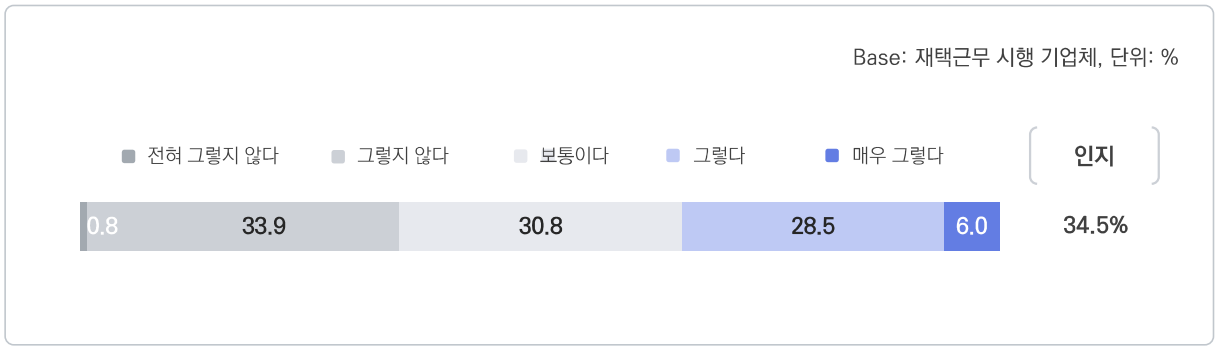


그림 1-3-102 원격근무 시 정보보호 위험성 인지

- 원격근무를 시행한 기업체 중 정보 침해사고 경험이 있거나 의심한 경험에 대해 경험이 없다는 비율이 99.9%로 나타남

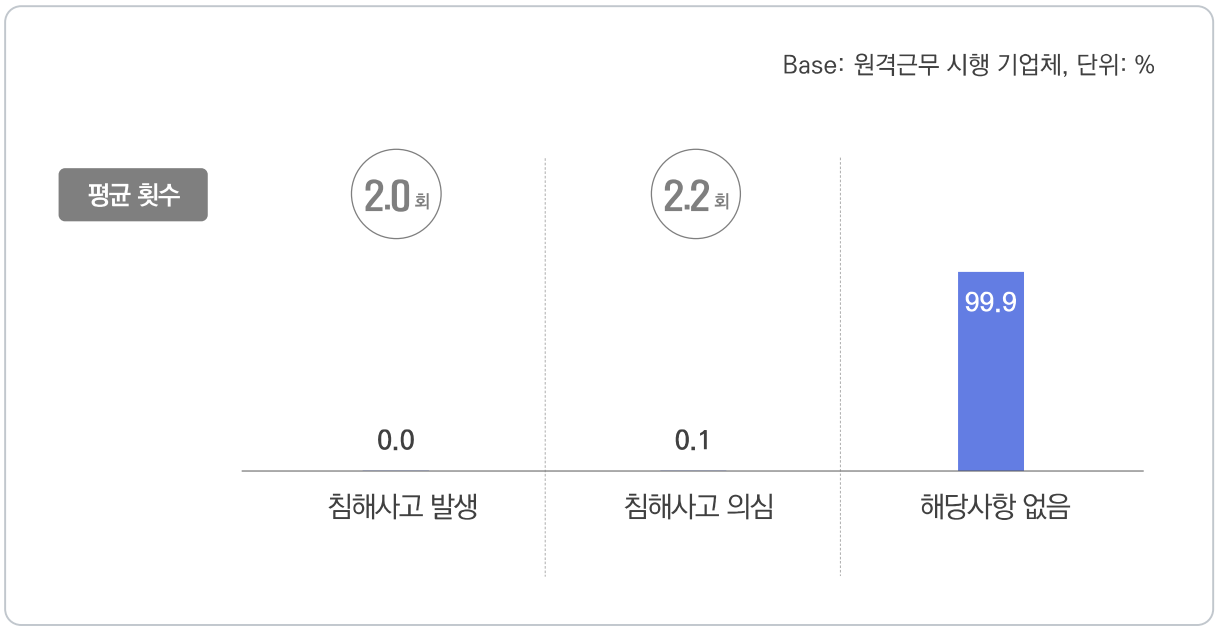


그림 1-3-103 원격근무 시 정보 침해사고 발생 또는 의심 경험

제 2 부

개인부문

제 1 장 조사 개요

1 조사 목적

- 급속하게 변화하는 인터넷 환경과 사물인터넷(IoT), IP카메라 등 새로운 기술의 끊임없는 등장으로 사이버 세계의 위협이 현실 세계로 확대되고 그 위협 또한 고도화·지능화되고 있음. 이에 따라 정보보호 관련된 현황 및 인터넷 이용자들의 인식 수준, 대응 활동 등을 파악하고, 인터넷 이용자의 정보보호 수준 제고에 활용하고자 정보보호 실태조사를 실시하였음
- 본 조사는 이러한 필요에 근거하여 향후 효과적인 정보보호 관련 정책수립의 기초자료를 확보하고, 나아가 업계의 비즈니스 전략 수립, 학계의 연구 활동 등 다양한 영역에서 활용할 수 있는 통계 정보를 제공하는데 그 목적이 있음
- 본 조사의 구체적인 목적은 다음과 같음
  1. 정부, 기업, 개인 등 사회구성원 전체의 정보보호 수준 제고에 활용하기 위한 기초자료 제공
  2. 국가정보보호백서 등의 정보보호 통계자료 제공
  3. 국제기구(OECD)의 ICT 통계지표 기초자료 제공
  4. 업계 및 학계의 현장, 연구 활동 등에 활용

2 조사 연혁

1998년
- 국내 만15세 이상 인터넷 이용자(1,500명)를 대상으로 『인터넷 역기능 실태조사』 실시

2001년
- 만13세 이상 인터넷 이용자(2,000명)로 조사 대상 확대

2004년
- 전국의 만13~59세 인터넷 이용자로 조사 대상 변경

2006년
- 『개인인터넷이용자 정보보호 실태조사』로 명칭 변경
- 정보통신부가 통계청으로부터 작성 승인(일반통계 제34205호)

2007년
- 정보통신부로부터 한국정보보호진흥원으로 통계작성기관 변경
- 인터넷 이용자 4,000명으로 표본규모 확대

2009년
- 한국인터넷진흥원으로 통합되면서 통계 작성주체 변경
  (한국정보보호진흥원 → 한국인터넷진흥원)

2010년
- '전국의 만12~59세 인터넷 이용자'로 조사 대상 변경
- 인터넷 이용자 5,000명으로 표본규모 확대

2011년
- '가구방문 면접조사'로 조사 방법 변경
- 조사 방법 변경에 따라 인터넷 이용자 2,500명으로 표본규모 변경
- '2010년 인구주택총조사'와 '2010년 인터넷이용실태조사' 결과를 기반으로 표본 재설계
- 조사구 추출 – 가구 추출 – 가구원 추출의 다단계층화추출로 표본 추출 방법 변경

2012년
- '2010년 인구주택총조사'와 '2011년 인터넷이용실태조사' 결과를 기반으로 표본 재설계

2013년
- 한국인터넷진흥원에서 미래창조과학부로 통계작성기관 변경
- '2010년 인구주택총조사'와 '2012년 인터넷이용실태조사' 결과를 기반으로 표본 재설계

2014년
- '2010년 인구주택총조사'와 '2013년 추계인구', '2013년 인터넷이용실태조사' 결과를 기반으로 표본 재설계

2015년
- '2010년 인구주택총조사'와 '2014년 추계인구', '2014년 인터넷이용실태조사' 결과를 기반으로 표본 재설계
- 전국(17개 시도) 인터넷 이용자 4,000명으로 표본규모 변경
- 승인통계 통합 관리를 위해 정보보호 실태조사 승인번호 단일화 (개인부문 승인번호인 제34205호로 통합)

2016년
- 승인통계 번호체계 변경 (정보보호 실태조사 승인번호인 제34205호→제342005호)

2017년
- '2010년 인구주택총조사'와 '2016년 추계인구', '2016년 인터넷이용실태조사' 결과를 기반으로 표본 재설계

2018년
- '2015년 인구주택총조사'와 '2017년 추계인구', '2017년 인터넷이용실태조사' 결과를 기반으로 표본 재설계
- 조사대상 확대(만12세~59세 → 만12세~69세)
- PC 기반의 주요 문항을 PC와 모바일로 구분하여 설문 구성

2019년
- 한국인터넷진흥원(KISA)에서 한국정보보호산업협회(KISIA)로 업무 이관
- 전국(17개 시도) 인터넷 이용자 4,500명으로 표본규모 변경
- '2018년 추계인구'와 '2018년 인터넷이용실태조사' 결과를 기반으로 표본 재설계

2020년
- '2019년 추계인구'와 '2019년 인터넷이용실태조사' 결과를 기반으로 표본 재설계

2021년
- 전국(17개 시도) 인터넷 이용자 4,000명으로 표본규모 변경
- '2020년 추계인구'와 '2020년 인터넷이용실태조사' 결과를 기반으로 표본 재설계

2022년
- '2021년 추계인구'와 '2021년 인터넷이용실태조사' 결과를 기반으로 표본 재설계

2023년
- '2022년 추계인구'와 '2022년 인터넷이용실태조사' 결과를 기반으로 표본 재설계

2024년
- '2023년 추계인구'와 '2023년 인터넷이용실태조사' 결과를 기반으로 표본 재설계

2025년
- '2024년 추계인구'와 '2024년 인터넷이용실태조사' 결과를 기반으로 표본 재설계
- 전국(17개 시도) 인터넷 이용자 3,000명으로 표본규모 변경

3 조사 내용 및 범위

- 본 조사는 개인(인터넷 이용자)의 정보보호 인식, 정보보호 교육 및 예산, 침해사고 경험과 위협 인식에 관한 현황을 파악할 수 있는 설문으로 구성하였음
- 본 조사의 주요 내용은 다음과 같음
  1. 정보보호 인식
  2. 정보보호 교육
  3. 정보보호 예산
  4. 일상 생활 속의 정보보호
  5. 정보 침해사고 경험과 위협 인식

4 주요 용어 및 정의

- **정보보호** : 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 활동
- **악성코드** : 시스템을 파괴하거나 정보를 유출하는 등 악의적 활동을 수행하도록 의도적으로 제작된 소프트웨어(바이러스, 웜, 애드웨어, 스파이웨어 등)
- **피싱** : 개인정보(Private data)와 낚시(Fishing)의 합성어로 개인정보를 낚는다는 의미. 금융기관 또는 공공기관을 가장해 전화나 이메일로 인터넷 사이트에서 보안카드 일련번호와 코드번호 일부 또는 전체를 입력하도록 요구해 금융 정보를 몰래 빼가는 수법
- **파밍** : 악성코드에 감염된 PC를 조작해 이용자가 인터넷 즐겨찾기 또는 포털사이트 검색을 통하여 금융회사 등의 정상적인 홈페이지 주소로 접속하여도 피싱(가짜) 사이트로 유도되어 범죄자가 개인 금융 정보 등을 몰래 빼가는 수법
- **스미싱** : 문자 메시지를 이용한 새로운 휴대폰 해킹 기법. 웹사이트 링크가 포함된 문자 메시지를 보내 휴대폰 사용자가 링크를 클릭하면 트로이목마를 주입해 범죄자가 휴대폰을 통제하는 등의 수법
- **랜섬웨어** : 몸값을 의미하는 'Ransom'과 'Software'의 합성어로 인터넷 사용자의 시스템을 잠그거나 데이터를 사용할 수 없도록 암호화한 뒤에, 그 데이터를 인질로 금전을 요구하는 악성 프로그램을 의미
- **IP카메라** : 유선 또는 무선으로 인터넷에 연결되어 PC나 모바일 기기 등을 통해 실시간으로 영상을 송출할 수 있는 단말기

5 조사 체계

- **조사대상** : 최근 1개월 내 인터넷 이용자(만12~69세)
- **유효 응답자 수** : 3,000명
- **조사주기** : 연 1회
- **조사기간** : 2025년 9월 15일 ~ 12월 15일 (3개월)
- **조사방법** : 가구방문 면접조사(유치조사 병행)
- **조사기관**
  - 주관기관 : 과학기술정보통신부(Ministry of Science and ICT)
  - 전담기관 : 한국정보보호산업협회(Korea Information Security Industry Association)
- **법적근거**
  - 정보보호산업의 진흥에 관한 법률 시행령 제20조
  - 통계법 제18조(통계작성의 승인)

6 표본 설계

가 모집단

- **목표 모집단(Target Population)** : 국내 만12~69세 인터넷 이용자
- **조사 모집단(Survey Population)**
  - 국내 만12~69세 인터넷 이용자 중 최근 1개월 이내 인터넷 이용자
- **모집단 자료**
  - 통계청『2024년 장래인구추계』및 한국지능정보사회진흥원의『2024년 인터넷이용실태조사』에서 파악된 지역별, 성별, 연령별 국내 인터넷 이용률을 이용하여 파악한 최근 1개월 이내 인터넷 이용자 수 및 분포를 활용함
  - 단, 통계청 조사구 중 일반조사구와 아파트조사구를 조사 모집단으로 정의함

나 표본 추출

- **개요** : 다단계층화추출법(Multi-Stage Stratified Sampling)
  - 17개 시도별 인터넷 이용자 크기에 비례하여 600개 조사구를 배분하고, 각 조사구에서 평균 5가구씩 추출하여 가구 내에서 적격 조사대상자를 선정·조사함
- **표본의 규모 산정**
  - 표본오차(허용오차)별 표본의 크기를 계산한 결과는 아래와 같음

표 2-1-1 표본오차별 표본의 크기

단위: 개, %

표본 크기	3,000	3,500	3,600	3,800	4,000	4,200	4,400	4,500
표본 오차	1.79	1.66	1.63	1.59	1.55	1.51	1.48	1.46

  - 최종 표본의 크기는 표본오차가 ±1.79%p 내에서 통제되도록 3,000명으로 결정함(95% 신뢰수준)

- **층화변수**
  - 권역(17개) : 서울, 부산, 대구, 인천, 광주, 대전, 울산, 세종, 경기, 강원, 충북, 충남, 전북, 전남, 경북, 경남, 제주
  - 성(2개) : 남성, 여성
  - 연령(6개) : 만12~19세, 20대, 30대, 40대, 50대, 60대

- **표본틀** : 통계청『2024년 장래인구추계』및 한국지능정보사회진흥원의『2024년 인터넷이용실태조사』에서 파악된 지역별, 성별, 연령별 국내 인터넷 이용자 수 및 분포를 활용함

- **표본 할당 및 추출 방법**

① 표본 할당

- 만 12~69세 인터넷 이용자 크기에 비례하여 3,000명을 지역별 비례할당 후, 각 지역에 표본을 우선 할당하고, 성X연령 셀에 할당하는 방법을 최종 표본 할당 방법으로 결정함

② 조사구 할당

- 조사구당 평균 5명이 조사되도록 총 600개 조사구 배분
- 1차 : 17개 시도별 조사구 배분
  * 통계청의『2024년 장래인구추계』, 한국지능정보사회진흥원의『2024년 인터넷 이용 실태조사』의 인터넷 이용률 결과를 바탕으로 17개 시도별 인터넷 이용자 크기에 비례하여 600개 조사구를 배분함
- 2차 : 시도 내 주거 형태별 조사구 배분
  * 통계청의『2023년 등록센서스』기준 17개 시도별 주거 형태(일반 및 아파트) 분포에 비례하여, 일반 조사구와 아파트 조사구를 배분함

③ 조사구 추출

- 404,760개 조사구를 행정구역 코드에 따라 정렬하여 계통 추출
  * 시도 내 조사구 수 m개, 목표 조사구 수 n개, m/(n-1)의 몫을 k라고 할 때 시도별로 1-m 범위 내에서 난수표를 사용하여 임의의 순번 i번째 조사구를 첫 번째 조사구로 추출하고, 이어 i+k, i+2k, i+3k... i+nk번째 조사구를 순차적으로 추출함

④ 가구 추출

- 한국통계진흥원으로부터 제공받은 표본조사구의 가구명부 리스트 번호 중 임의로 하나를 선택한 후 해당 가구를 출발점으로 가구를 계통추출하고 순서대로 방문하여 적격 조사대상 5가구를 조사함
- 3회까지 접촉이 이루어지지 않거나 가구 내 적격 조사대상자가 없는 경우, 가구 명부를 기준으로 원표본(i)의 다음 가구(i-1, i+1)로 대체함

⑤ 조사대상 추출

- 가구 내에 상주하는 만12~69세 가구원을 대상으로 적격 조사대상자 여부를 확인함
- 적격 조사대상자가 복수일 경우에는 생월법에 따라 생일의 일자가 가장 가까운 가구원을 조사함

7 실사

가 실사 개요

- **조사기간**
  - 2025년 9월 15일 ~ 12월 15일 (3개월)
- **조사기준 시점**
  - 2024년 8월 1일 ~ 2025년 7월 31일
    * 침해사고 경험은 2024년 1월 1일 ~ 2024년 12월 31일 기준임
- **조사대상**
  - 최근 1개월 내 인터넷 이용자(만 12~69세)
- **조사방법**
  - 전문 조사원이 표본으로 선정된 가구를 방문하여 설문에 응답을 받는 형태의 가구방문 면접조사
- **조사절차**
  - 전문 조사원의 조사대상 가구방문 면접조사 → 지역별 실사 감독원의 관리 및 통제 → 설문지 집계 → 보완조사 및 재조사 → 최종 자료 검증

나 표본 관리

- **조사구 관리**
  - 사전 추출된 조사구(읍면동)를 대상으로 조사하는 것을 원칙으로 하며, 재개발, 행정구역 통폐합, 천재지변 등으로 조사가 불가능한 경우에는 유사 특성을 가진 조사구로 대체함
- **가구 관리**
  - 사전 추출된 가구를 대상으로 조사하는 것을 원칙으로 하며, 가구원의 장기 부재, 강력한 응답 거부 등으로 조사가 불가능한 경우에는 동일 조사구 내에서 1차 추출된 원표본과 동일한 가구 특성으로 추출된 예비 표본으로 대체하여 조사를 진행함

8 자료 입력 및 처리

가 자료 검증 및 대체

- **실사 과정에서 자료 검증**
  - 지역별 실사 감독원이 회수된 설문지의 30% 이상을 무작위 추출하여 조사원 방문 여부, 응답의 정확성 등에 대한 전화 검증을 실시함
  - 실사 감독원의 1차 검증에서 합격된 설문지는 에디팅 및 입력 과정에서 전산 프로그램에 의해 2차 검증을 실시함
  - 입력된 자료는 자료 처리 과정에서 내검 프로그램에 의해 3차 검증을 실시함
  - 검증 단계별로 불합격된 설문지에 대해 보완조사 및 재조사를 실시함
- **분석 과정에서 자료 검증**
  - 동일한 그룹(성, 연령, 지역, 학력, 직업, 가구소득 등)별 평균치 및 이전 조사 결과와의 시계열 비교 및 검증을 실시함
- **무응답 대체**
  - 단위무응답 및 항목무응답 발생 시 해당 가구를 3회 이상 재방문 및 전화 검증을 통해 무응답률을 최소화함
  - 단위무응답 발생 시 예비표본의 범위 내에서 대체하여 단위무응답을 제거함
  - 항목무응답 발생 시 결측값을 해당 응답자 특성(성, 연령, 학력, 직업, 가구소득 등)과 유사한 응답자 그룹의 평균값으로 대체하여 항목무응답을 제거함

나 자료 입력 및 분석

- 수집된 자료는 부호화(coding) 과정을 통해 전산 입력되며, 다단계 검증 과정에서 최종 통과된 자료는 SPSS for Windows(통계패키지 프로그램)를 이용하여 분석됨
  - 응답자의 이름, 주소, 전화번호 등 개인을 식별할 수 있는 정보는 일련번호로 부호화하거나 자료 입력 시 제외함

9 추정 및 표본오차

가 가중치 산출

- **'사후층화(post-stratification)' 방법에 따라 가중치 산출 및 적용**
  - 본 조사는 조사구를 활용한 가구방문 면접조사로 진행되어 표본의 구성 비율이 모집단 구성 비율과 차이가 있으므로 가중치에 의한 사후 추정이 필요함
- 통계청의 『2024년 추계인구』, 한국지능정보사회진흥원의 『2024년 인터넷이용실태조사』의 인터넷 이용률 결과를 모집단으로 활용하여 지역×성×연령별 가중치 $w_{(h,s,k)}$를 산출하였으며, 가중치 산출 공식은 다음과 같음

$$w_{(h,s,k)} = \frac{N_{(h,s,k)}}{n_{(h,s,k)}}$$

- 여기에서 $w_{(h,s,k)}$: (h,s,k)셀의 가중치
  $N_{(h,s,k)}$: (h,s,k)셀의 모집단 수
  $n_{(h,s,k)}$: (h,s,k)셀의 표본 수
  k : 연령(만12~19세, 20대, 30대, 40대, 50대, 60대)을 나타내는 첨자(k=1~6)
  s : 성(남성, 여성)을 나타내는 첨자(s=1, 2)
  h : 지역(17개 시도)을 나타내는 첨자(h=1~17)

나 추정

- 전체 모비율 추정 산출 공식은 다음과 같음

$$\hat{p}_{st} = \sum_{h=1}^{17}\sum_{s=1}^{2}\sum_{k=1}^{6} w_{(h,s,k)}\,\hat{p}_{(h,s,k)}$$

- 여기에서 $\hat{p}_{st}$: 특정 변수에 대한 모비율
  $\hat{p}_{(h,s,k)}$: 특정 변수에 대한 (h,s,k)셀의 모비율
  $w_{(h,s,k)}$: (h,s,k)셀의 가중치

다 표본오차

- 본 조사는 '다단계층화추출' 방식이 적용되었으며, 전체 및 각 층(성, 연령, 시도)별 모비율에 대한 표본오차 산출 공식은 다음과 같음

$$1.96 \times \sqrt{V(\hat{p}_{st})}$$

전체 모비율의 표본오차 = $1.96 \times \sqrt{\hat{V}(\hat{p}_{st})}$

층별 모비율의 표본오차 = $1.96 \times \sqrt{\hat{V}(\hat{p}_{hsk})}$

여기에서 $\hat{V}(\hat{p}_{st})$: 전체 모비율에 대한 분산
$\hat{V}(\hat{p}_{hsk})$: 층별 모비율에 대한 분산

- 분산 산출 공식은 다음과 같음

$$\hat{V}(\hat{p}_{hsk}) = \sum_{h=1}^{L} w_{hsk}^2 \left(\frac{N_{hsk} - n_{hsk}}{N_{hsk}} \right) \frac{\hat{p}_{hsk}(1-\hat{p}_{hsk})}{n_{hsk}}$$

표 2-1-2 보안 점검 수행률 추정 결과 및 표본오차

보안 점검 수행률 표본오차	± 1.77%p (95% 신뢰수준)
보안 점검 수행률 추정 결과	41.9% ± 1.77%p

10 결과 공표 및 활용 분야

- 『2025년 정보보호 실태조사(개인부문)』 보고서는 한국정보보호산업협회 홈페이지 (https://www.kisia.or.kr)를 통해 게시함
- 본 통계자료는 과학기술정보통신부 등 정부부처 및 연구기관의 정책수립의 기초자료 및 국제기구(OECD) 등에 제출되어 국가별 정보보호 현황 비교 등을 위한 통계자료로 활용됨

11 모집단 및 표본 현황

표 2-1-3 모집단 및 표본 현황

단위: 명, %

구분		만12~69세 최근 1개월 이내 인터넷 이용자		응답 표본 현황	
		모집단 수	구성비	표본 수	구성비
전체		40,652,223	100.0	3,000	100.0
성별	남	20,793,836	51.2	1,540	51.3
	여	19,858,387	48.8	1,460	48.7
연령	12~19세	3,637,693	8.9	276	9.2
	20대	6,345,829	15.6	462	15.4
	30대	6,880,465	16.9	490	16.3
	40대	7,802,078	19.2	572	19.1
	50대	8,601,035	21.2	642	21.4
	60대	7,385,123	18.2	558	18.6
지역	서울	7,547,557	18.6	348	11.6
	부산	2,501,809	6.2	200	6.7
	대구	1,847,254	4.5	172	5.7
	인천	2,446,580	6.0	198	6.6
	광주	1,161,301	2.9	137	4.6
	대전	1,174,697	2.9	137	4.6
	울산	887,552	2.2	119	4.0
	세종	306,280	0.8	70	2.3
	경기	11,188,449	27.5	424	14.1
	강원	1,066,574	2.6	131	4.4
	충북	1,263,777	3.1	142	4.7
	충남	1,692,992	4.2	165	5.5
	전북	1,319,548	3.2	146	4.9
	전남	1,291,594	3.2	144	4.8
	경북	1,957,308	4.8	177	5.9
	경남	2,478,785	6.1	199	6.6
	제주	520,166	1.3	91	3.0

제 2 장 조사 결과 요약

Ⅰ. 정보보호 인식 | Ⅱ. 정보보호 예방 활동

Ⅰ 정보보호 인식

1 정보보호 인식

» 인터넷 이용자의 정보보호 이슈 관심도는 65.3%임

- ‘정보보호 관련 이슈에 대해 관심 있다(있는 편이다+자주 있다)’고 응답한 비율은 65.3%로 2024년(63.6%) 대비 1.7%p 증가함
  - 성별로는 여성이, 연령별로는 50대~60대의 관심도가 전년 대비 크게 증가함

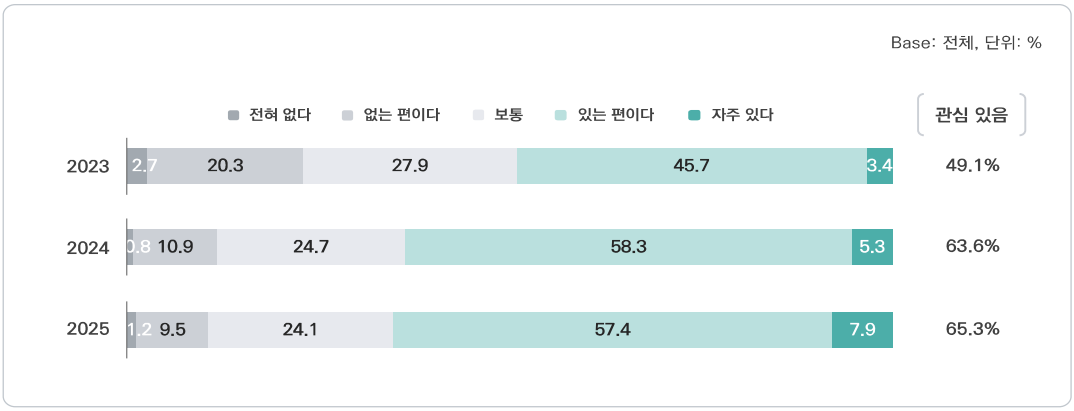


그림 2-2-1 정보보호 이슈 관심도

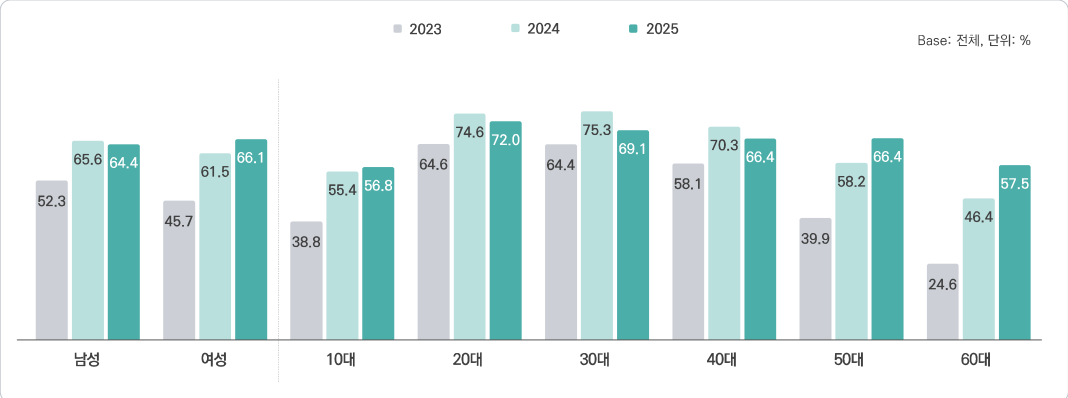


그림 2-2-2 성·연령별 정보보호 이슈 관심도

» 인터넷 이용자의 정보 침해사고에 대한 우려 정도는 72.5%임

- 정보 침해사고에 대해 '우려한다(우려하는 편이다+매우 우려한다)'고 응답한 비율은 72.5%로 2024년(64.4%) 대비 8.1%p 증가함

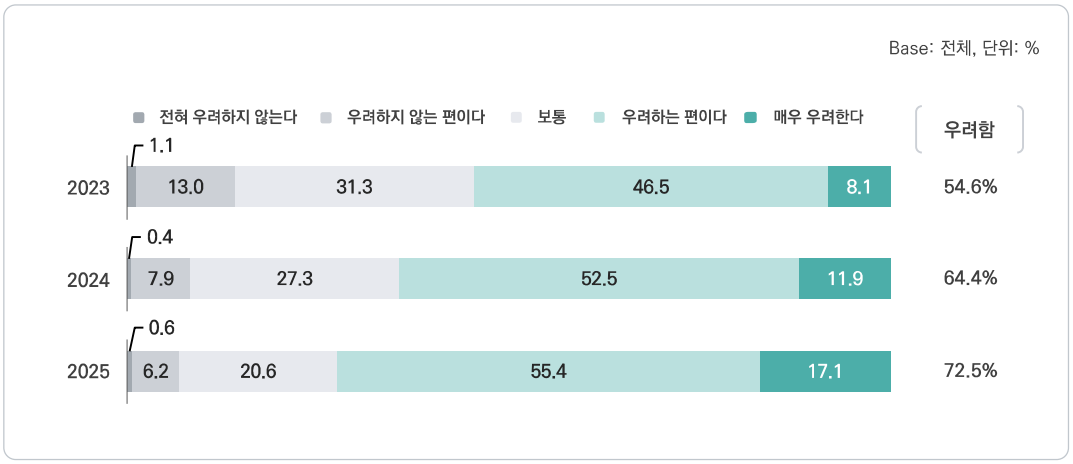


그림 2-2-3 정보 침해 우려 정도

» 정보 침해사고 소식에 대한 본인과의 관련성 인식 정도는 59.2%임

- 본인이 정보 침해사고와 '관련 있다(관련 있는 편이다+매우 관련 있다)'고 응답한 비율은 59.2%로 2024년(52.6%) 대비 6.6%p 증가함

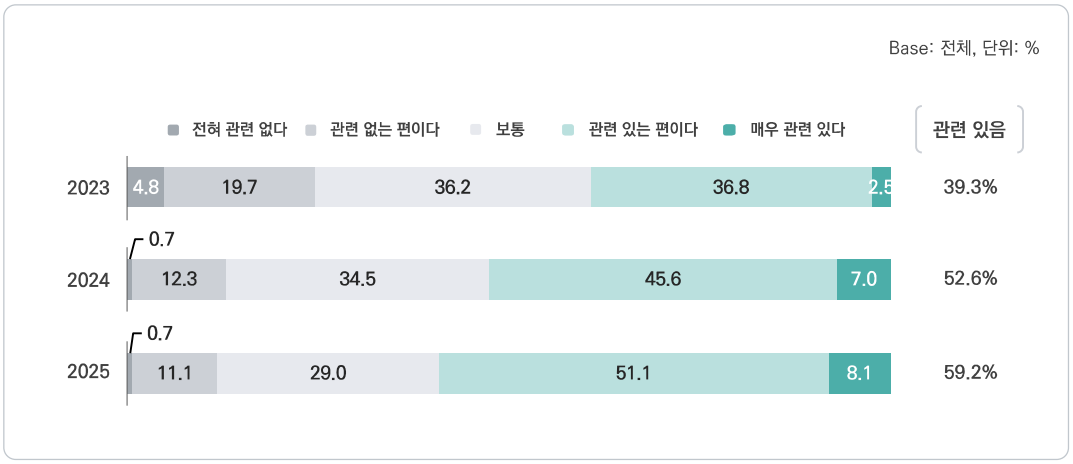
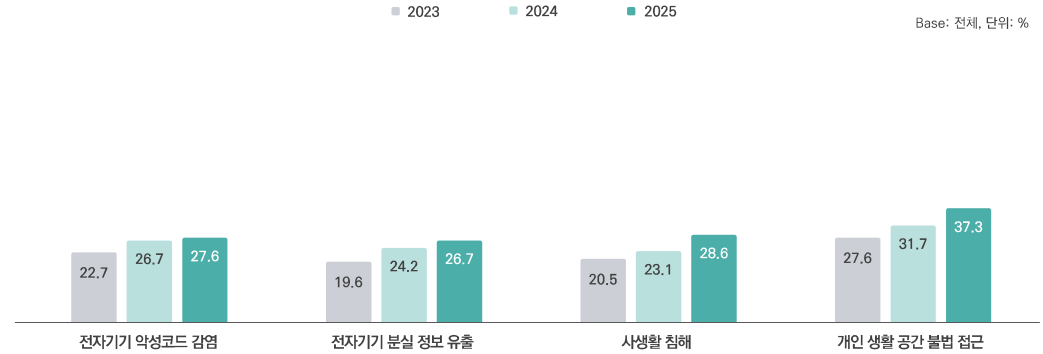


그림 2-2-4 정보 침해사고 소식에 대한 관련성 인식

» 정보보호 관련 이슈 중 안전 체감도가 가장 높은 항목은 '개인 생활 공간 불법 접근(37.3%)'임

- 정보보호 관련 이슈별 안전 체감도는 '개인 생활 공간 불법 접근'이 37.3%로 가장 높고, 다음으로 '사생활 침해(28.6%)', '전자기기 악성코드 감염(27.6%)', '전자기기 분실 정보 유출(26.7%)'의 순임
  - 정보보호 관련 모든 이슈에서 2024년 대비 안전 체감도가 증가함



* 안전 체감도 = 안전한 편이다+매우 안전하다

그림 2-2-5 안전 체감도(요약)

Ⅱ 정보보호 예방 활동

1 정보보호 교육

» 인터넷 이용자의 14.9%가 정보보호 교육을 수강함

- 최근 1년간 정보보호 교육을 수강한 경험이 있다고 응답한 비율은 14.9%로 2024년(12.0%) 대비 2.9%p 증가함

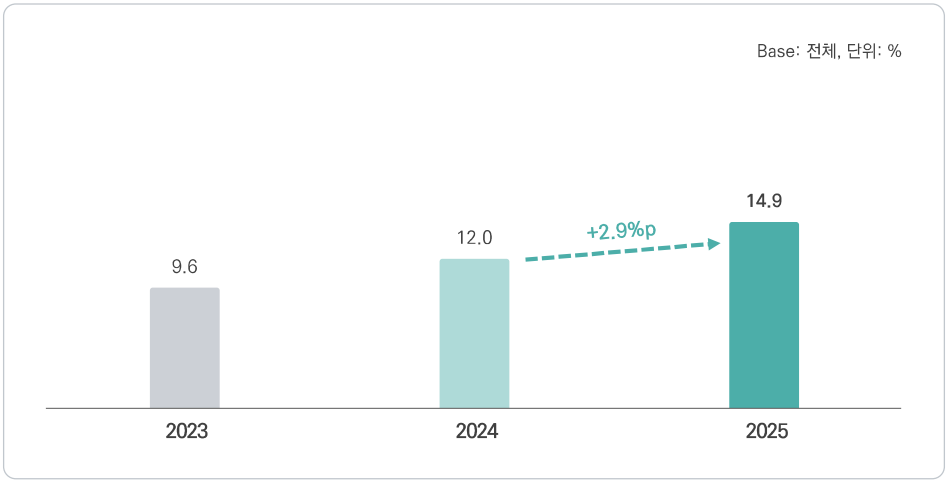


그림 2-2-6 정보보호 교육 수강 경험

» 가장 많이 이용하는 교육 방식은 '근무지 혹은 학교 등에서의 온라인 교육 수강'임

- 정보보호 교육을 수강한 방식으로는 '근무지 혹은 학교 등에서의 온라인 교육 수강'이 68.0%로 가장 높고, '근무지 혹은 학교 등에서의 오프라인 교육 수강(44.5%)', '개인적인 방식으로 온라인 교육 수강(16.2%)' 등의 순임
  - 정보보호 교육 방식 중 '근무지 혹은 학교 등에서의 오프라인 교육 수강'이 상대적으로 가장 많이 증가함(+11.1%p)

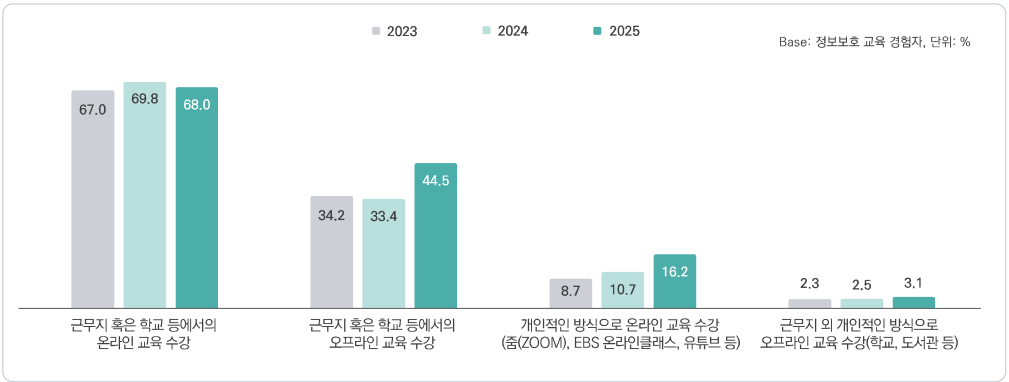


그림 2-2-7 정보보호 교육 방식(복수응답)

2 정보보호 예산

가 정보보호 금전 소비 경험 및 소비 유형

» 인터넷 이용자의 11.0%가 개인적인 목적으로 정보보호 관련 금전적 소비를 한 경험이 있음

- 최근 1년간 개인적인 목적으로 정보보호 관련 금전적인 소비를 한 경험이 있다고 응답한 비율은 11.0%로 2024년(11.4%) 대비 0.4%p 감소함

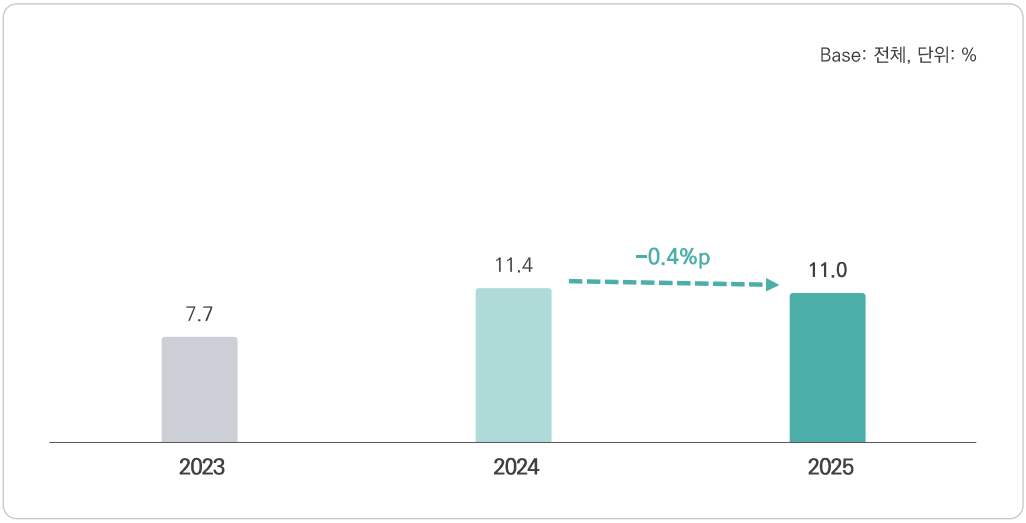


그림 2-2-8 정보보호 금전 소비 경험

» 정보보호 금전 소비 경험자의 44.1%가 '1만 원 이상 ~ 10만 원 미만' 정도로 소비함

- 정보보호 관련 금전적인 소비 규모는 '1만 원 이상 ~ 10만 원 미만'이 44.1%로 가장 높고, 다음으로 '10만 원 이상 ~ 20만 원 미만(19.8%)', '1만 원 미만(14.5%)' 등의 순임
  - 정보보호 금전 소비 경험자의 소비 규모 '30만 원 이상 ~ 40만 원 미만'은 6.1%로 2024년(2.1%) 대비 4.0%p 증가함

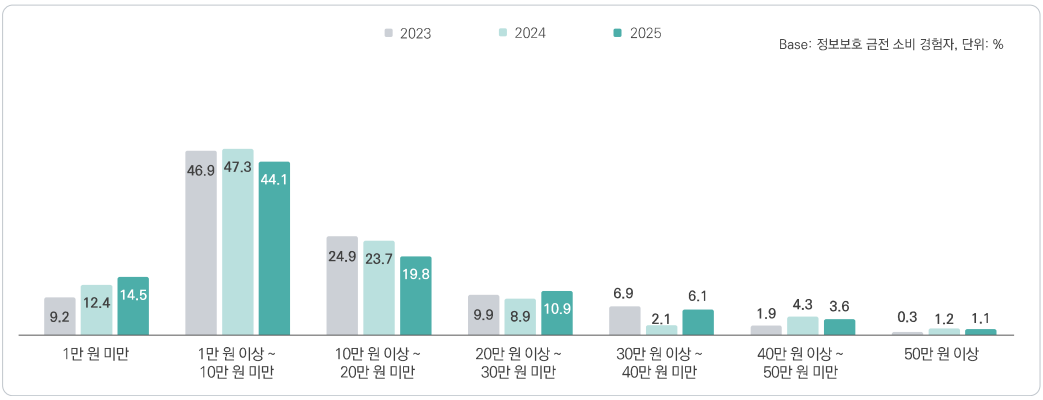


그림 2-2-9 정보보호 금전 소비 규모

정보보호 관련 금전 소비 비중이 가장 큰 분야는 '정보보호 관련 유료 인증서의 결제(74.0%)'임

- 정보보호 관련 금전적인 소비 중 가장 큰 비중을 차지하는 유형에 대해 '정보보호 관련 유료 인증서의 결제'가 74.0%로 가장 높게 나타남
  - 소비 유형 중 '정보보호 관련 유료 인증서의 결제'가 74.0%로 다른 유형 대비 상대적으로 가장 크게 증가함(+23.5%p)

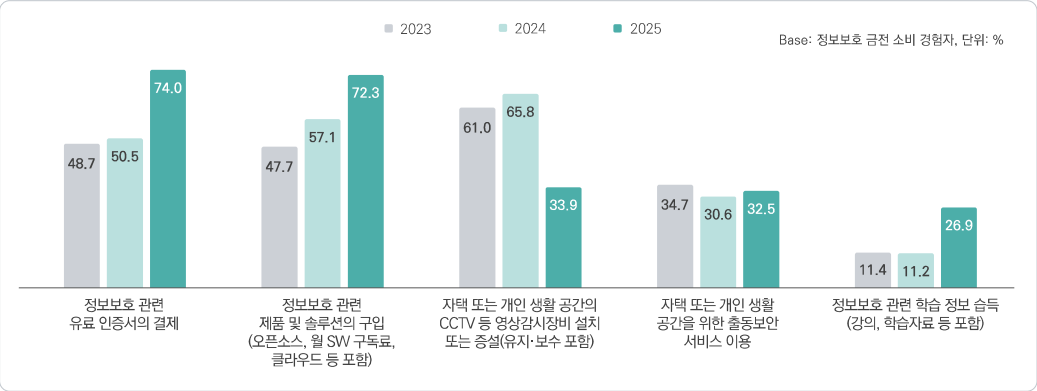


그림 2-2-10 정보보호 금전 소비 유형(종합순위)

나 정보보호 금전 소비 적절성

정보보호 금전 소비 경험자의 65.5%는 현재의 금전 소비가 적절하다고 생각함

- 정보보호 금전 소비 경험자 중 정보보호 관련 금전적인 소비를 '적절하다(그렇다+매우 그렇다)'고 응답한 비율은 65.5%로 2024년(50.4%) 대비 15.1%p 증가함

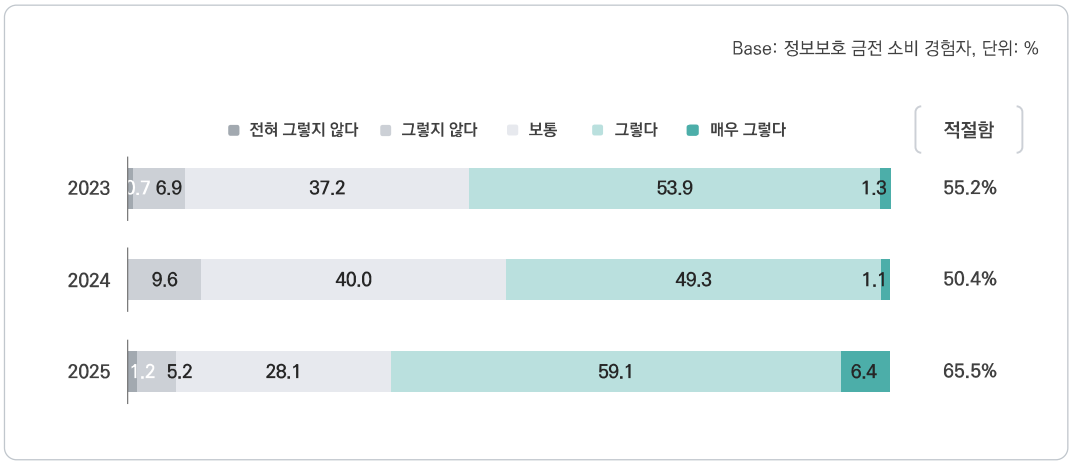


그림 2-2-11 정보보호 금전 소비 적절성

다 정보보호 금전 소비 계획

» 정보보호 금전 소비 경험자의 35.2%는 향후 금전 소비 규모가 증가할 예정임

- 정보보호 금전 소비 경험자 중 향후 정보보호 관련 금전 소비 비용을 '증가할 예정(늘릴 예정이다+크게 늘릴 예정이다)'이라고 응답한 비율은 35.2%로 2024년(21.8%) 대비 13.4%p 증가함

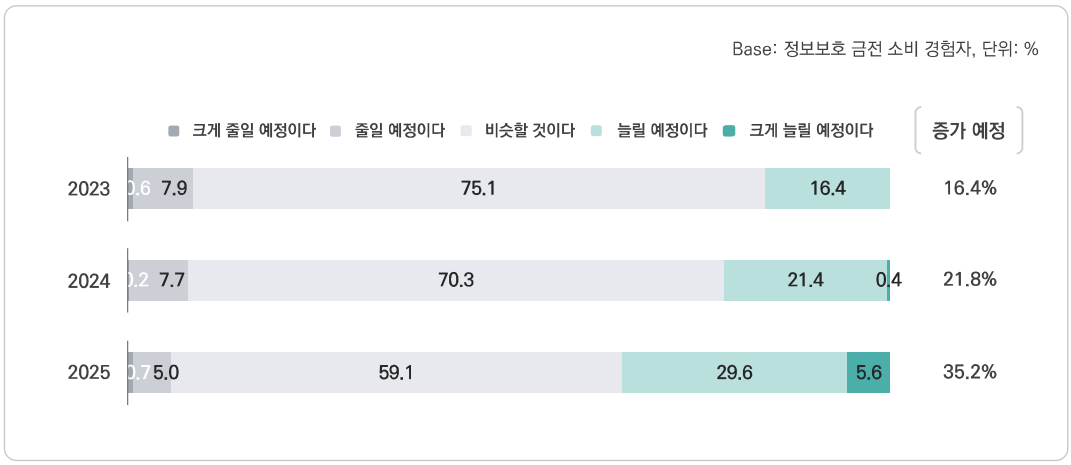


그림 2-2-12 정보보호 금전 소비 증감 여부

» 정보보호 금전 소비 비경험자의 28.6%는 향후 정보보호 관련 금전적 소비 의향 있음

- 정보보호 금전 소비 비경험자 중 향후 정보보호 활동을 위해 비용을 지출할 '의향 있다(그렇다+매우 그렇다)'고 응답한 비율은 28.6%로 2024년(21.7%) 대비 6.9%p 증가함
  - '의향 없다(전혀 그렇지 않다+그렇지 않다)'는 비율이 2024년(41.5%) 대비 2025년(33.1%)에 8.4%p 감소함

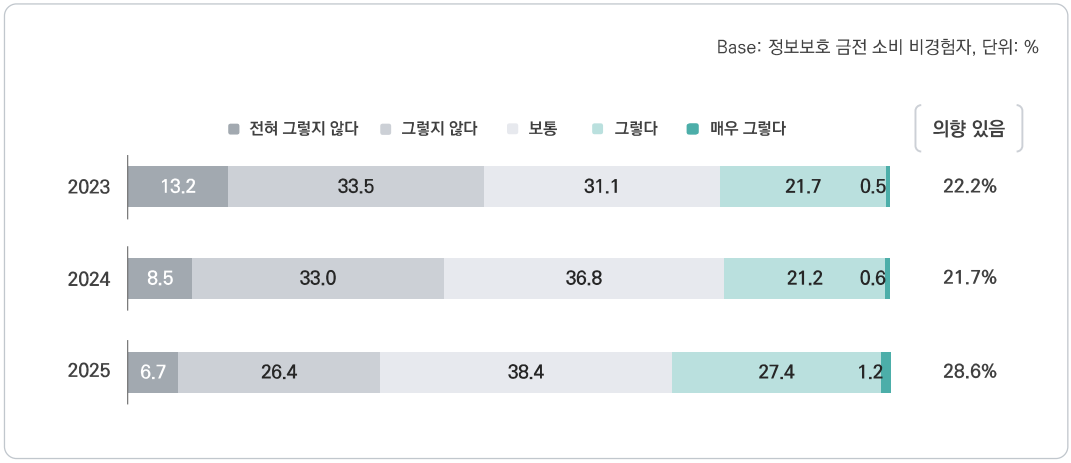


그림 2-2-13 정보보호 금전 소비 지출 의향

3 일상생활 속의 정보보호

가 무료 인터넷 연결 빈도 및 불특정 다수 이용 전자장비 이용 시 예방 활동

» 인터넷 이용자의 44.5%는 공공장소에서 무료 인터넷 연결을 사용함

- 공공장소에서 제공되는 무료 인터넷(Wi-Fi)에 노트북, 스마트폰, 패드 등을 연결하여 '사용한다(자주 사용하는 편이다+항상 사용한다)'고 응답한 비율은 44.5%로 2024년(40.4%) 대비 4.1%p 증가함

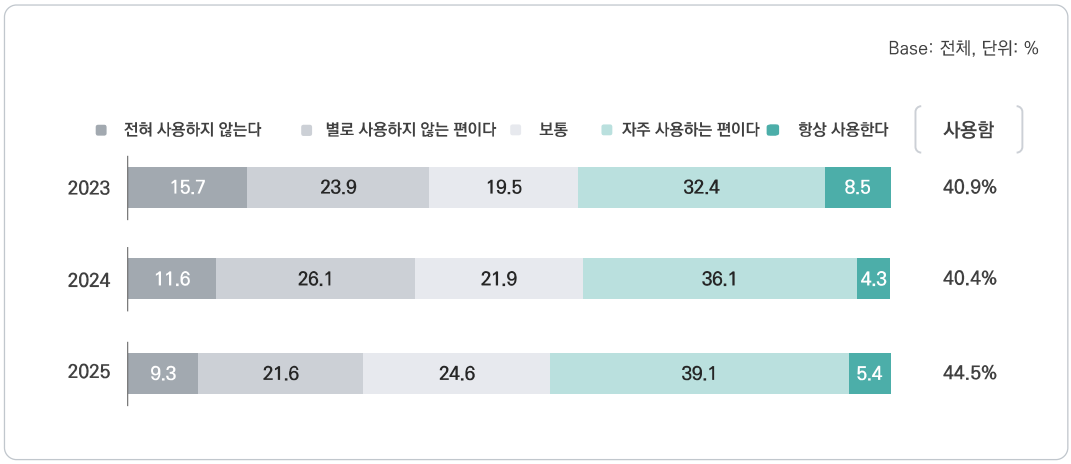


그림 2-2-14 공공장소 무료 인터넷 연결 빈도

» 불특정 다수가 사용하는 전자장비를 이용하는 경우, 정보보호 예방 활동 수행률은 39.7%임

- 공공장소, PC방 등 불특정 다수가 사용하는 전자장비에 개인 계정으로 접속할 경우, 별도의 로그아웃(Log-out), 접속기록(쿠키) 삭제 등과 같은 예방 활동을 '수행한다(대체로 수행하는 편이다+반드시 수행한다)'고 응답한 비율은 39.7%로 2024년(37.4%) 대비 2.3%p 증가함

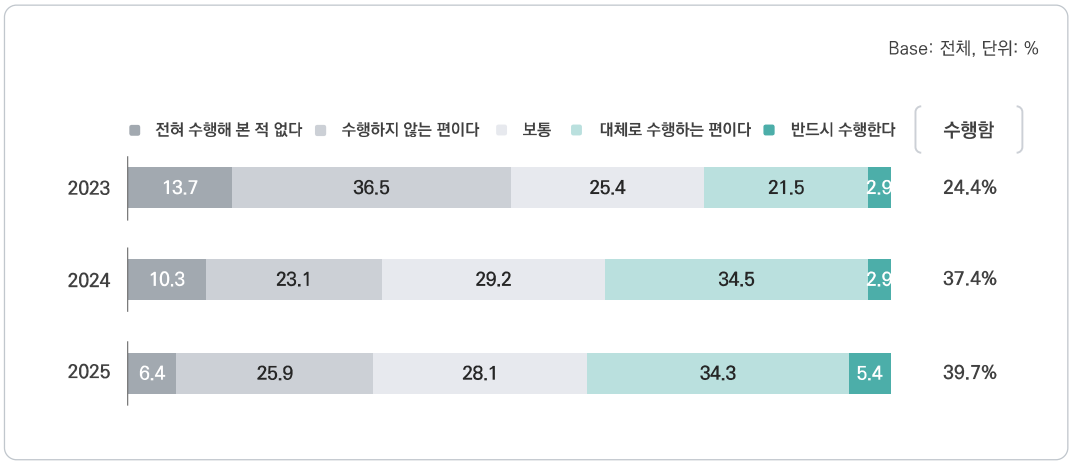


그림 2-2-15 불특정 다수 이용 전자장비 이용 시 정보보호 예방 활동 수행

나 정보보호 활동

» 정보보호 활동 수행 비율은 '보안 점검 수행(41.9%)'이 가장 높음

- 정보보호 활동 수행 비율은 '보안 점검 수행'이 41.9%로 가장 높고, 다음으로 '비밀번호 즉시 변경(35.3%)', '디지털 데이터 백업(34.5%)', '일상 공간 CCTV 또는 IP카메라 활용(8.5%)'의 순임
  - 2024년 대비 수행 비율이 가장 큰 폭으로 감소한 활동은 '비밀번호 즉시 변경'임(-7.5%p)

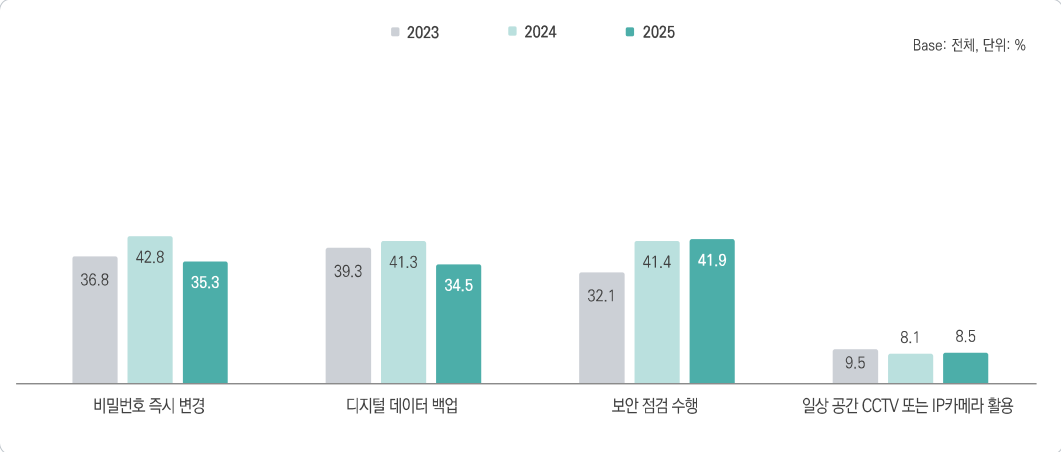


그림 2-2-16 정보보호 활동

다 비대면 환경의 정보보호 활동

» 인터넷 이용자의 20.6%는 원격근무 경험이 있음

- 원격근무 수행 경험은 20.6%로 2024년(14.2%) 대비 6.4%p 증가함
- 비대면 환경을 활용한 인터넷 이용자의 주요 정보보호 활동으로는 '비대면 환경을 활용하고 있는 컴퓨터로 의심스러운 URL 클릭 등을 하지 않음'이 28.5%로 가장 높고, 다음으로 '학교, 회사 등에서 제공한 정보보호 제품을 사용(27.0%)', '원격근무 화상회의 등 이용 시 관련 프로그램 이외의 프로그램을 사용하거나 작동하지 않음(19.7%)' 등의 순임
  - 비대면 환경의 정보보호 활동 중 '비대면 환경을 활용하고 있는 컴퓨터로 의심스러운 URL 클릭 등을 하지 않음(28.5%)'이라고 응답한 비율이 2024년(13.4%) 대비 상대적으로 가장 크게 증가함(+15.1%p)

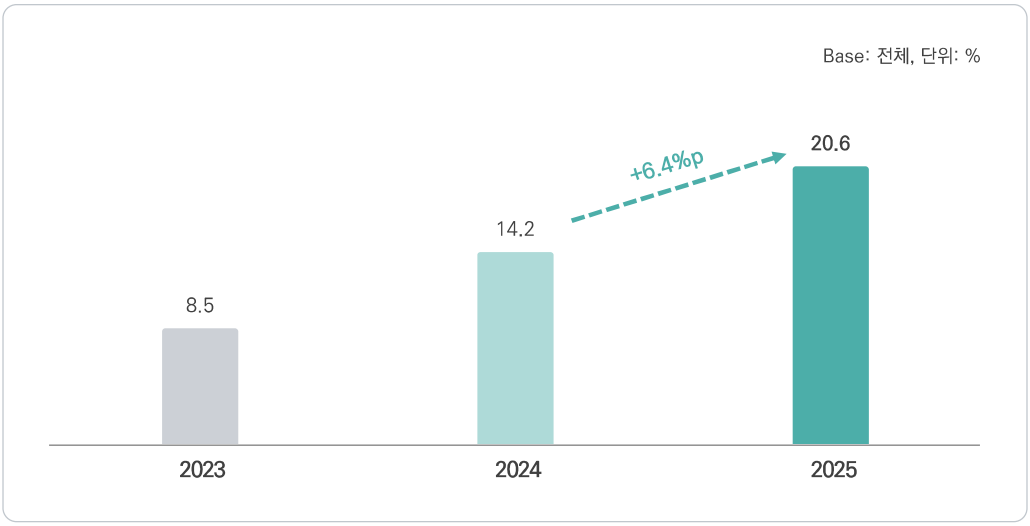


그림 2-2-17 원격근무 수행 경험

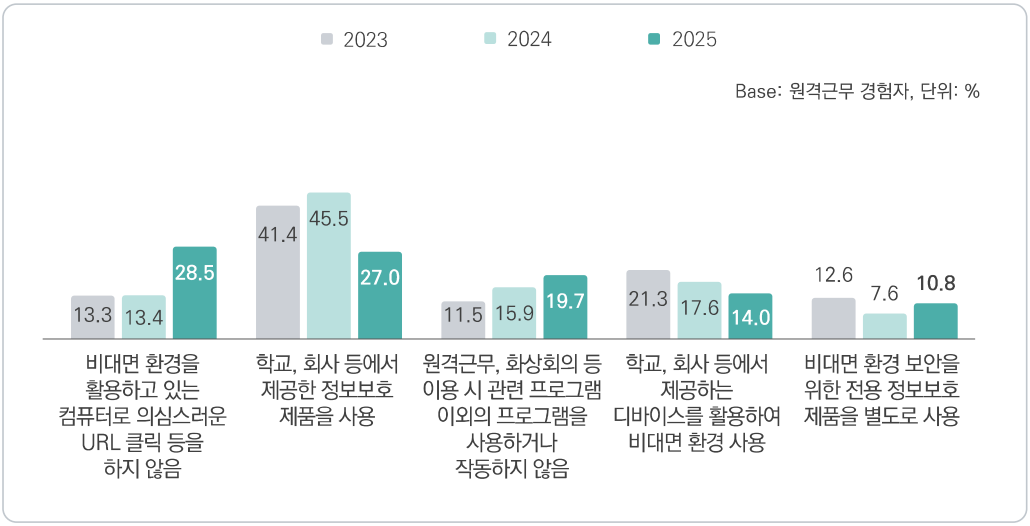


그림 2-2-18 비대면 환경 활용 시 정보보호 활동

4 정보 침해사고 경험과 위협 인식

가 정보 침해사고 의심 및 경험

인터넷 이용자의 22.0%는 정보 침해사고를 의심한 경험이 있고, 8.5%는 정보 침해사고를 직접 경험함

- 최근 1년간 정보 침해사고를 의심한 경험이 있다고 응답한 비율은 22.0%로 2024년(20.5%) 대비 1.5%p 증가함
- 최근 1년간 정보 침해사고를 경험한 적 있다고 응답한 비율은 8.5%로 2024년(2.9%) 대비 5.6%p 증가함

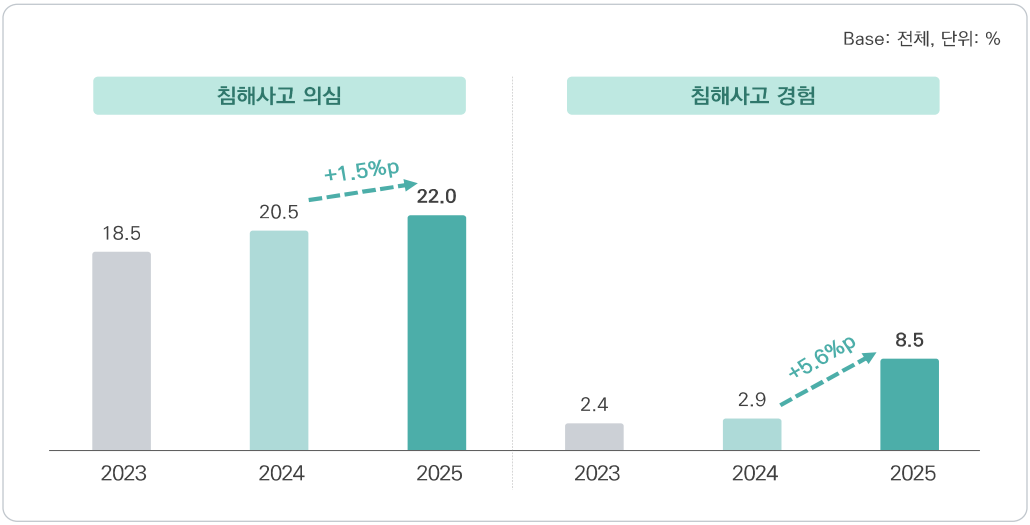
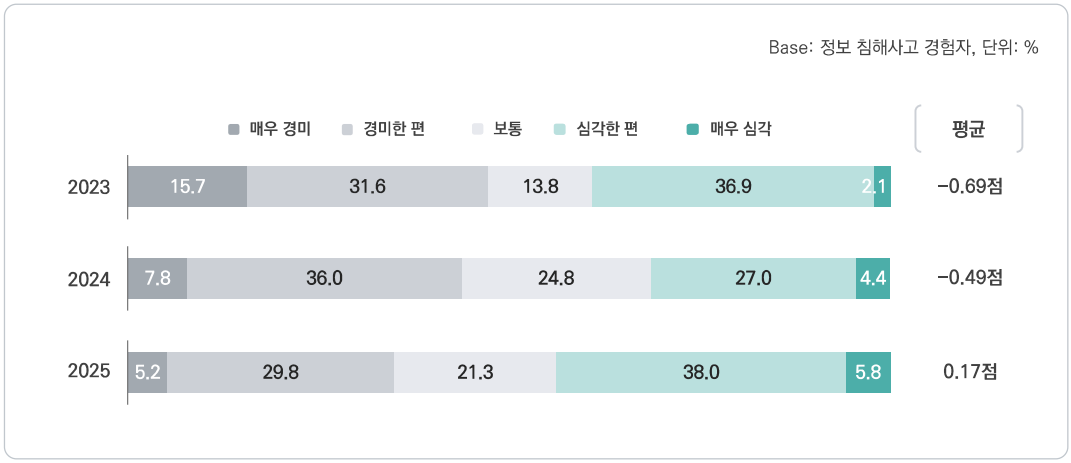


그림 2-2-19 정보 침해사고 의심 및 경험

나 정보 침해사고 피해 심각성

» 정보 침해사고 경험자의 피해 심각성은 0.17점으로 다소 심각함

- 정보 침해사고를 경험한 경우, 피해 심각성은 평균 0.17점으로 2024년(-0.49점) 대비 증가함



* '평균'은 -5점(침해사고는 있었으나 피해는 매우 경미하다)부터 5점(단시간에 회복되기 어려운 피해가 있었다) 중에 응답한 점수를 평균화한 것임

그림 2-2-20 정보 침해사고 피해 심각성

다 정보 침해사고 경험 유형

» 정보 침해사고 유형으로는 '개인용 모바일 기기의 해킹과 같은 불법적 접근(44.7%)'이 가장 많음

- 최근 1년간 경험한 정보 침해사고의 유형에 대해 '개인용 모바일 기기(스마트폰, 태블릿, 패드 등)의 해킹과 같은 불법적 접근'이 44.7%로 가장 높음
  - 정보 침해사고 유형에서 '개인용 전자기기에 대한 불법적 접근으로 인한 보유 중인 데이터의 외부 유출' 응답 비율이 2024년(11.1%) 대비 16.9%p 증가한 28.0%로 나타남

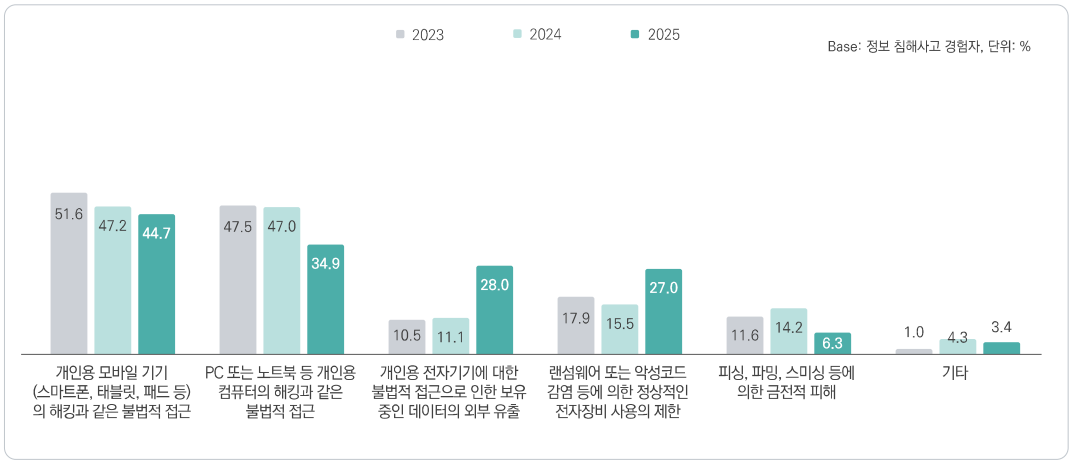


그림 2-2-21 정보 침해사고 경험 유형(복수응답)

라 정보 침해사고 대응

» 정보 침해사고 경험자의 41.2%는 관련 기관에 피해 사실을 신고함

- 정보 침해사고가 발생했을 때 관련 기관에 피해 사실을 신고했다고 응답한 비율은 41.2%로 2024년(34.7%) 대비 6.5%p 증가함

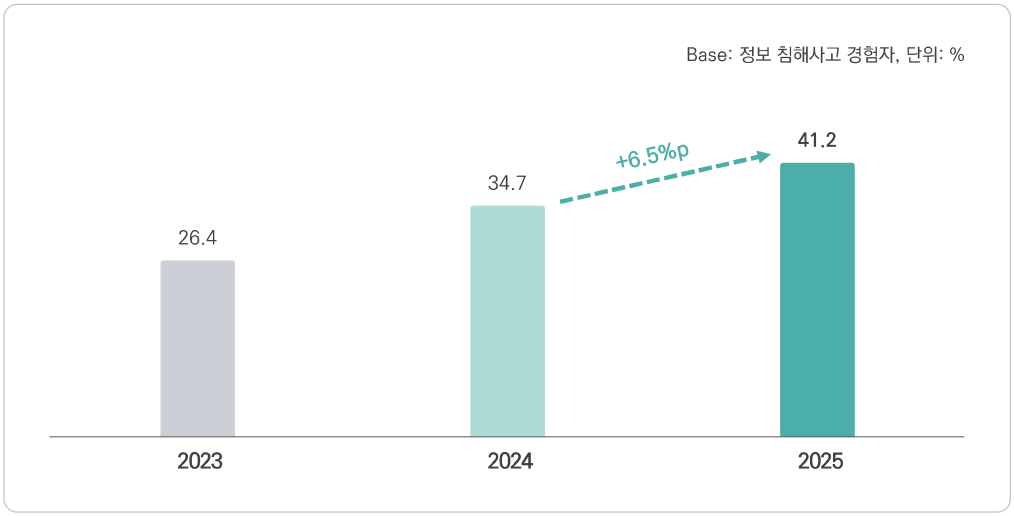


그림 2-2-22 정보 침해사고 신고 여부

» 신고하지 않는 주된 이유는 '피해가 심각하지 않았기 때문에(59.7%)'임

- 침해사고 미신고자가 침해사고를 신고하지 않은 이유로는 '피해가 심각하지 않았기 때문에'가 59.7%로 가장 높음
  - 침해사고를 신고하지 않는 이유에서 '침해 사실과 피해 사실을 사고 발생 이후 뒤늦게 인지했기 때문에(최소 1개월 이상)(26.5%)' 응답 비율이 2024년(6.3%) 대비 상대적으로 가장 크게 증가함(+20.2%p)

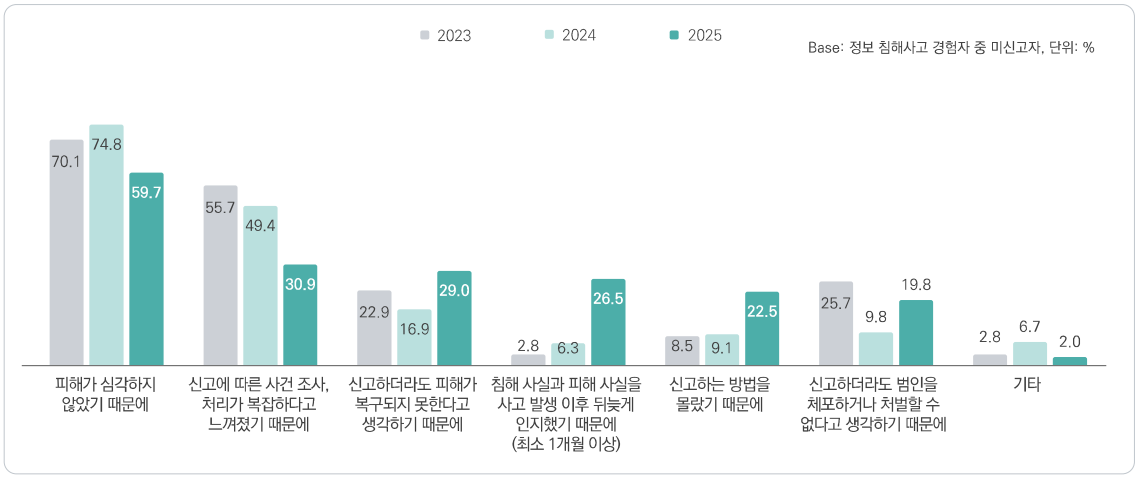


그림 2-2-23 정보 침해사고 미신고 이유(종합순위)

제 3 장 조사 결과

Ⅰ. 인터넷 활용 현황 | Ⅱ. 정보보호 인식 | Ⅲ. 정보보호 교육 | Ⅳ. 정보보호 예산 |
Ⅴ. 일상생활 속의 정보보호 | Ⅵ. 정보 침해사고 경험과 위협 인식

Ⅰ 인터넷 활용 현황

1 인터넷 활용 현황

가 인터넷 접속 시 사용한 전자기기

- 인터넷 이용자가 인터넷 접속 시 사용한 전자기기로는 '모바일 기기(스마트폰, 태블릿 PC 등)'가 99.5%로 가장 높고, 다음으로 '컴퓨터(데스크탑 PC, 노트북 등)(70.8%)', 'IoT 가전제품(스마트 TV, 인공지능 비서 제품 등)(25.6%)'의 순임

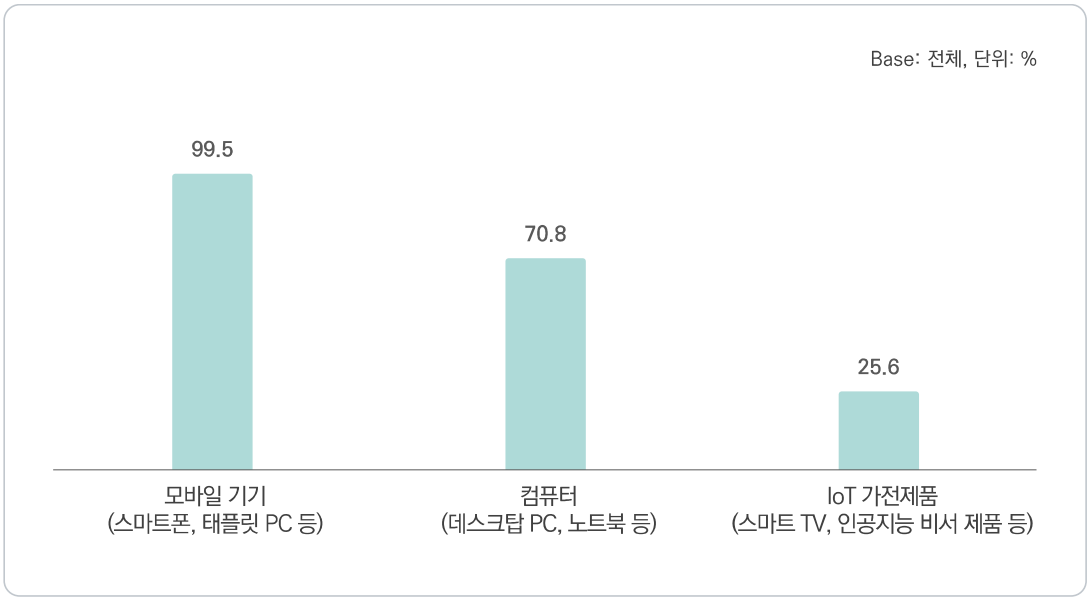


그림 2-3-1 인터넷 접속 시 사용한 전자기기(복수응답)

나 인터넷 접속 시간

- 하루 중 인터넷 접속 시간은 '1시간 초과 3시간 이하'가 34.9%로 가장 높고, 다음으로 '3시간 초과 6시간 이하(33.0%)', '6시간 초과 9시간 이하(16.2%)' 등의 순임

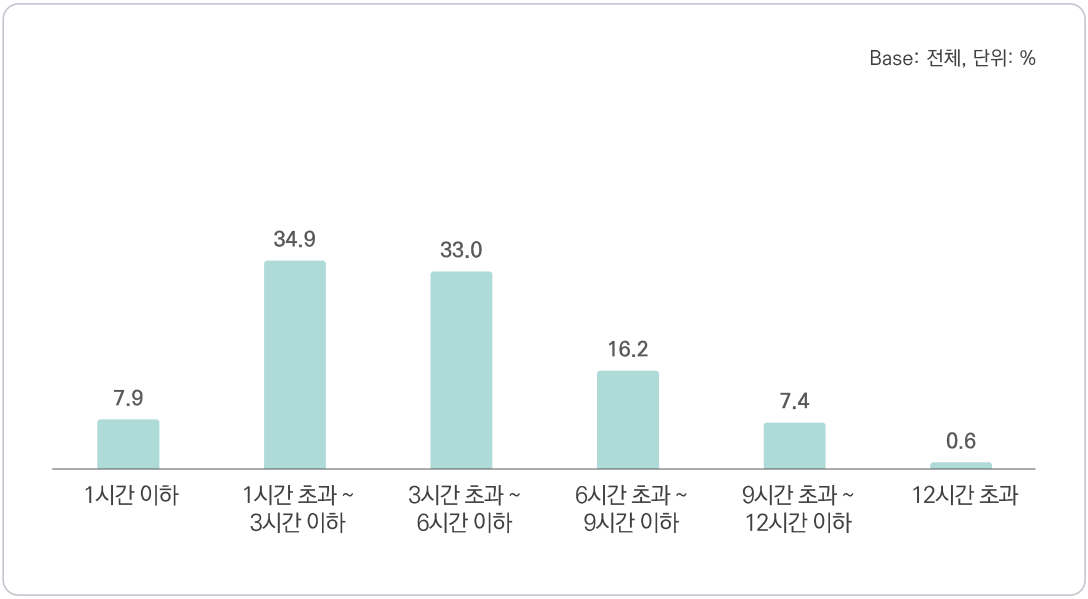


그림 2-3-2 인터넷 접속 시간

다 인터넷 정보 신뢰도

- 인터넷에서 접하는 다양한 정보에 대해 62.6%가 '신뢰한다(신뢰하는 편이다+매우 신뢰한다)'고 응답함

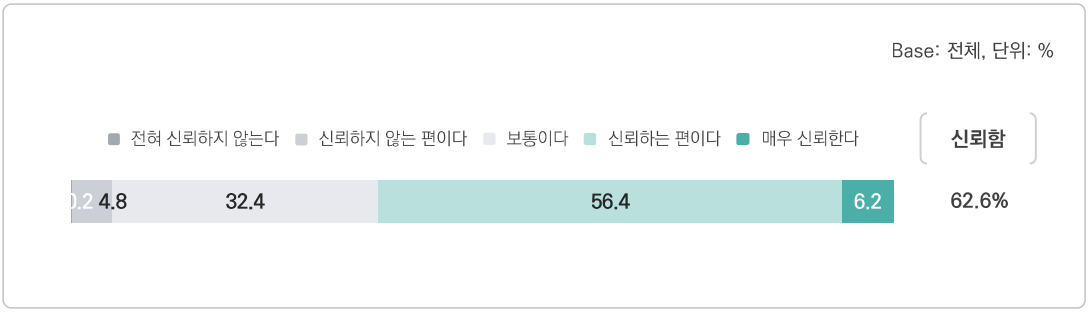


그림 2-3-3 인터넷 정보 신뢰도

라 의사결정 시 인터넷 중요성

- 일상생활에서 의사결정 시 인터넷의 중요성에 대해 78.1%가 '중요하다(중요한 편이다+매우 중요하다)'고 응답함

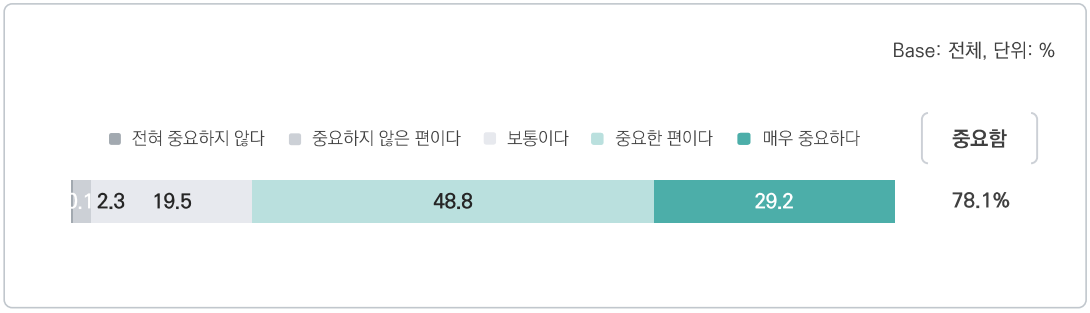


그림 2-3-4 의사결정 시 인터넷 중요성

마 인터넷 사용 시간 과도함

- 일상생활에서 인터넷을 사용하는 시간에 대해 35.3%가 '과도하다(그렇다+매우 그렇다)'고 응답함

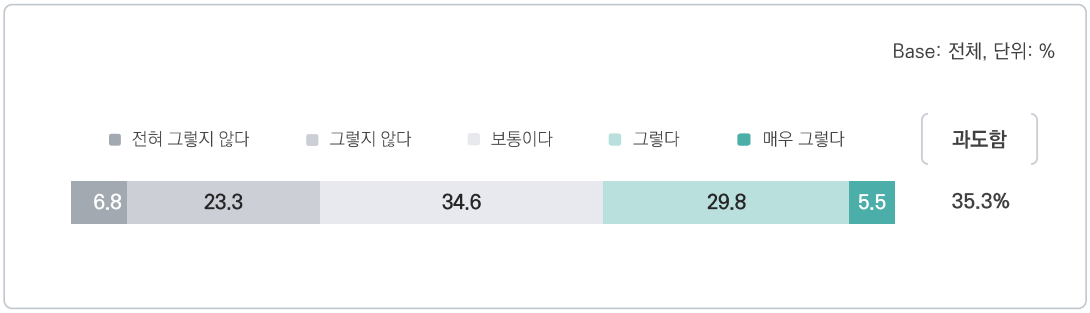


그림 2-3-5 인터넷 사용 시간 과도함

바 정보보호 범죄·사고 보호 체감도

- 일상생활에서 정보보호 관련 각종 범죄 또는 사고와 관련하여 36.9%가 국가 및 공공기관으로부터 충분히 '보호받는다(그렇다+매우 그렇다)'고 응답함

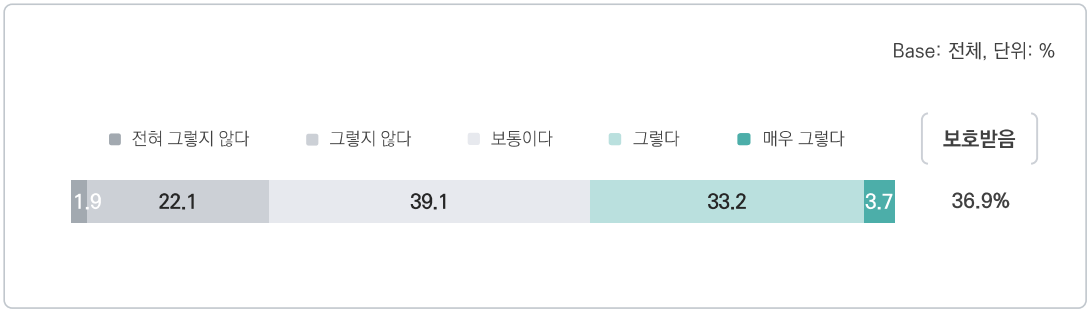


그림 2-3-6 정보보호 범죄·사고 보호 체감도

Ⅱ 정보보호 인식

1 정보보호 인식

가 정보보호 이슈 관심도

- 정보보호 관련 이슈에 대해 65.3%는 '관심 있다(있는 편이다+자주 있다)'고 응답함

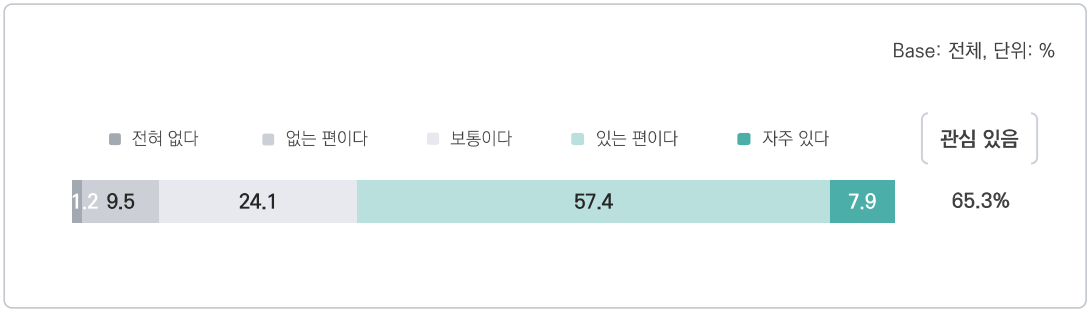


그림 2-3-7 정보보호 이슈 관심도

- 성별로 보면, 여성(66.1%)이 남성(64.4%) 대비 관심도가 높게 나타남
- 연령별로 보면, 20대(72.0%) 및 30대(69.1%)의 관심도가 상대적으로 높고, 10대(56.8%)는 다른 연령대보다 관심도가 상대적으로 낮게 나타남

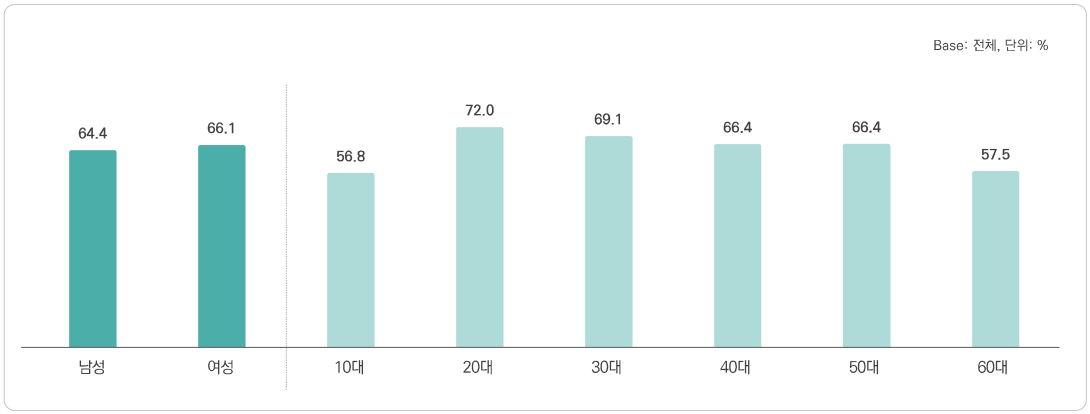


그림 2-3-8 성·연령별 정보보호 이슈 관심도

나 정보보호 침해 우려 정도

- 정보 침해사고에 대해 우려하는 정도에 대해 72.5%가 '우려한다(우려하는 편이다+매우 우려한다)'고 응답함

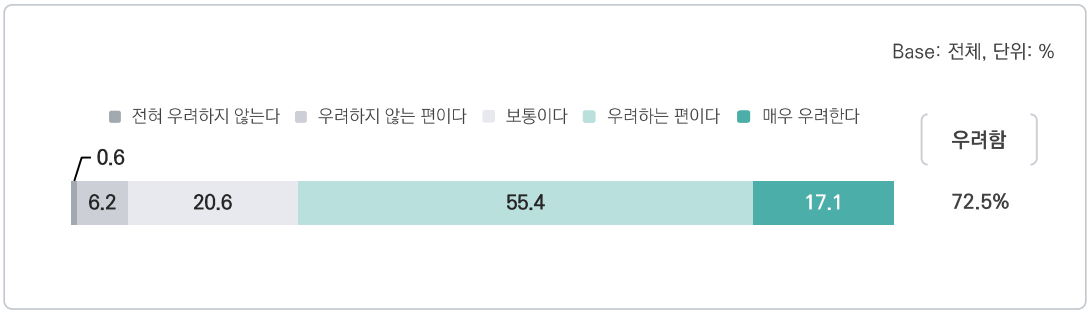


그림 2-3-9 정보보호 침해 우려 정도

다 정보보호 침해사고 소식에 대한 관련성 인식

- 정보 침해사고 소식을 접할 때 자신과 관련성이 있다고 인식하는 비율은 59.2%(관련 있는 편이다+매우 관련 있다)임

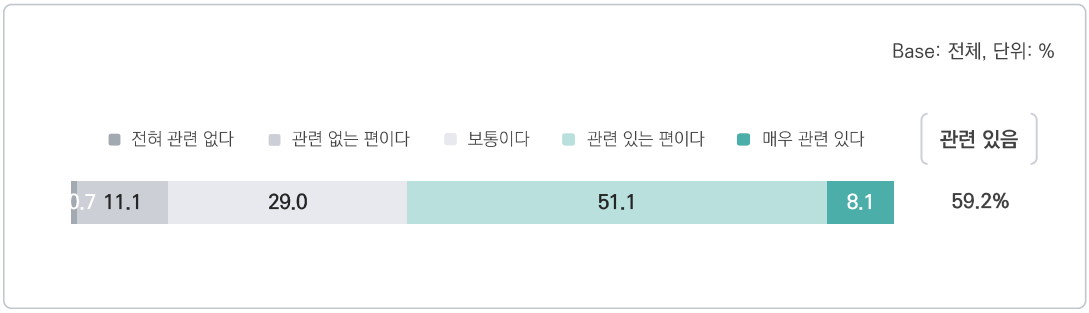


그림 2-3-10 정보보호 침해사고 소식에 대한 관련성 인식

라 안전 체감도

- 정보보호 관련 이슈별 안전 체감도는 '개인 생활 공간 불법 접근'이 37.3%로 가장 높고, 다음으로 '사생활 침해(28.6%)', '전자기기 악성코드 감염(27.6%)', '전자기기 분실 정보 유출(26.7%)'의 순임

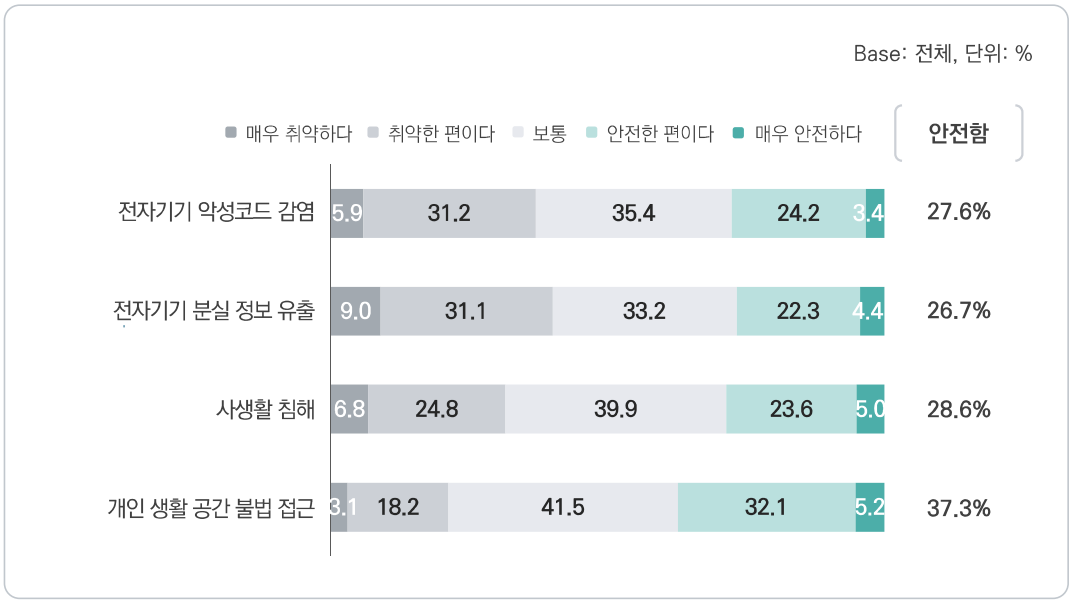


그림 2-3-11 안전 체감도(요약)

마 정보 침해사고 발생 시 피해 복구 가능성

- 정보 침해사고 발생 시 피해 복구 가능성에 대해 23.9%가 '복구 가능성이 있다(그렇다+매우 그렇다)'고 응답함

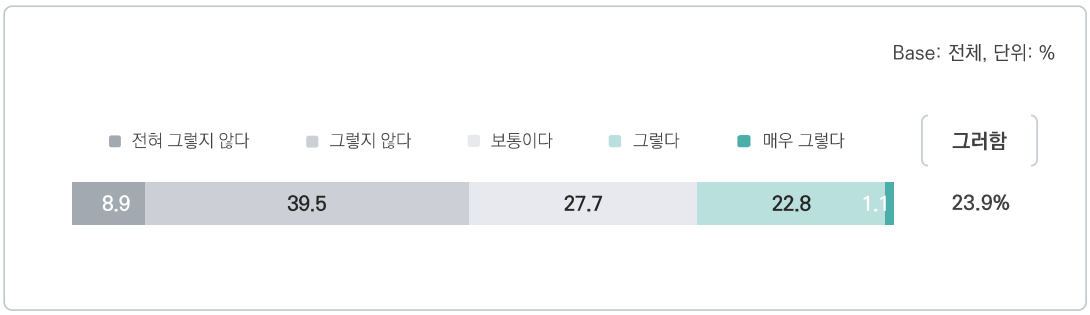


그림 2-3-12 침해사고 발생 시 피해 복구 가능성

바 정보 침해사고 발생 원인

- 인터넷 이용자가 생각하는 정보 침해사고의 주요 발생 원인으로는 '낮은 처벌기준·형량'이 79.3%로 가장 높고, 다음으로 '정보통신 서비스 제공 기업 사고방지 노력 부족(76.1%)', '사법기관 범죄 처벌 노력 부족(74.4%)' 등의 순임

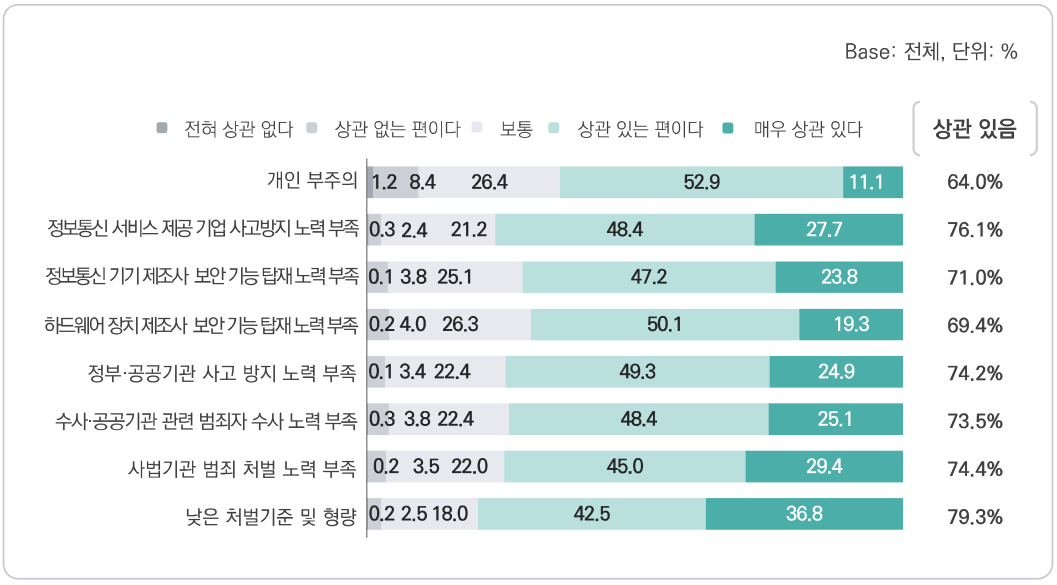


그림 2-3-13 정보 침해사고 발생 원인(요약)

사 정보 침해사고 방지 주체

- 정보 침해사고 방지를 위해 주도적으로 노력해야 하는 주체에 대해 '기업 또는 공공'이 62.8%로 '개인(37.2%)'에 비해 높게 나타남

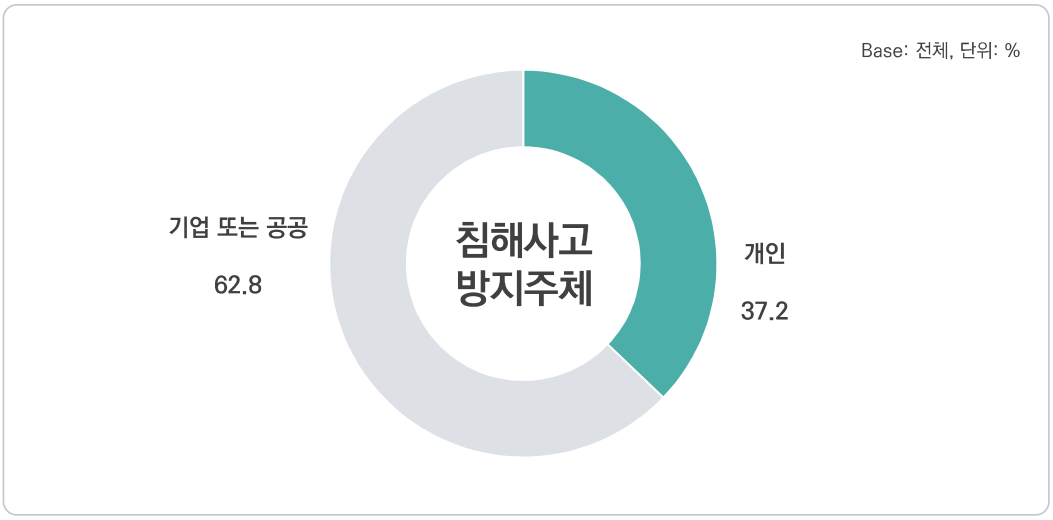


그림 2-3-14 침해사고 방지 주체

아 정보보호 관련 기관·업체 신뢰도

- 정보보호와 관련하여 각 기관·업체별 신뢰도에 대해 '정부부처·공공기관'이 45.6%로 가장 높고, 다음으로 '인터넷 서비스 제공자(31.2%)', '민간업체(29.3%)'의 순임

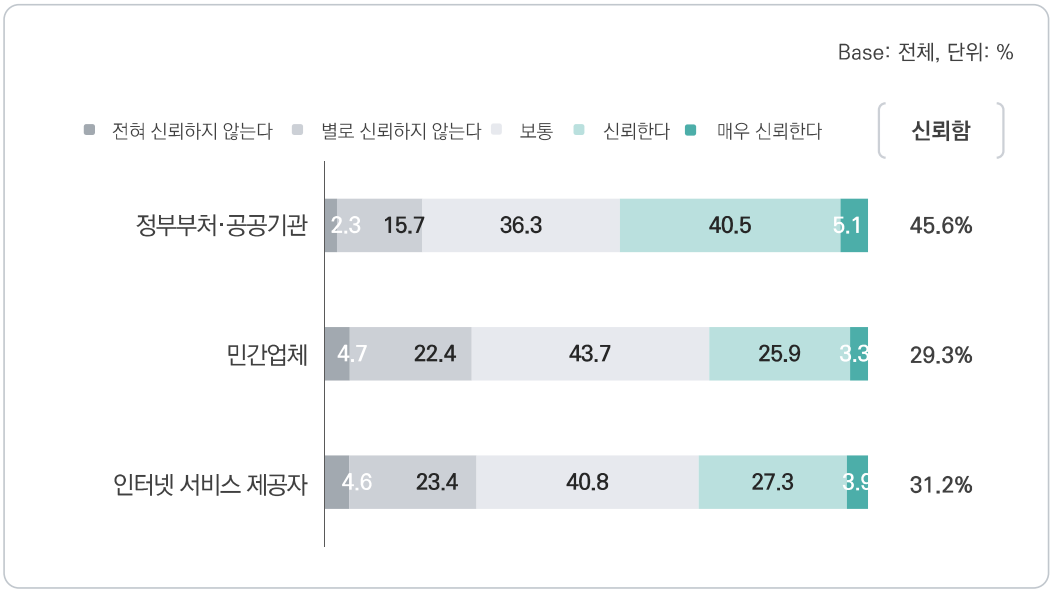


그림 2-3-15 정보보호 관련 기관·업체 신뢰도

Ⅲ 정보보호 교육

1 정보보호 교육

가 정보보호 정보 수집 경로

- 정보보호 정보 수집 경로에 대해 '인터넷 검색(블로그, 포털 등)'이 62.8%로 가장 높고, 다음으로 '방송·언론 매체(뉴스, 신문 등)(44.9%)', '유튜브·동영상 플랫폼(44.5%)' 등의 순으로 나타남

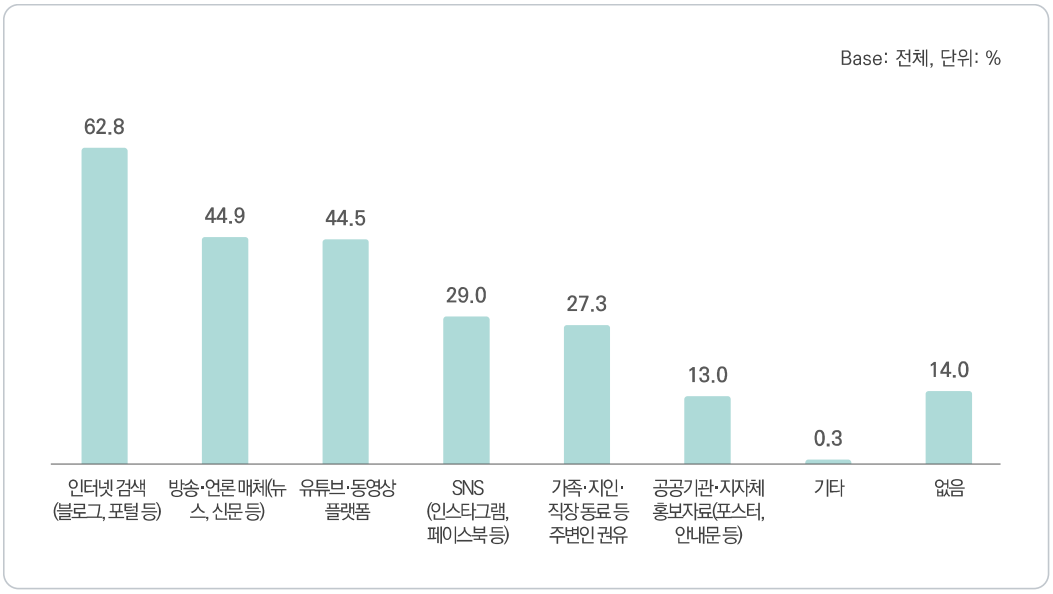


그림 2-3-16 정보보호 정보 수집 경로

나 정보보호 교육 수강 경험

- 인터넷 이용자의 14.9%가 최근 1년간 정보보호 교육을 수강한 경험이 있다고 응답함

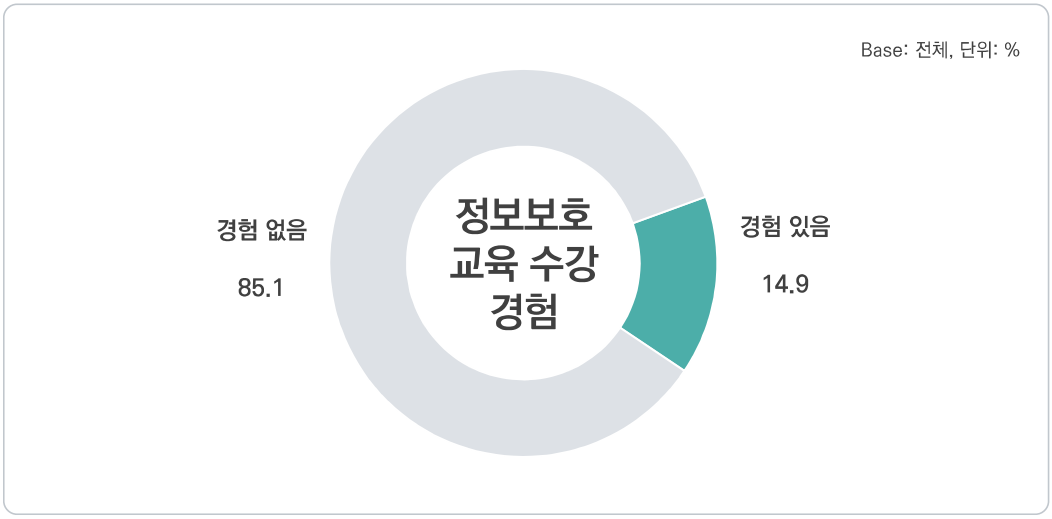


그림 2-3-17 정보보호 교육 수강 경험

- 성별로 보면, 남성(17.6%)이 여성(12.1%) 대비 교육 수강 경험률이 높게 나타남
- 연령별로 보면, 10대(36.0%)의 수강 경험률이 가장 높고, 60대(4.2%)가 가장 낮게 나타남

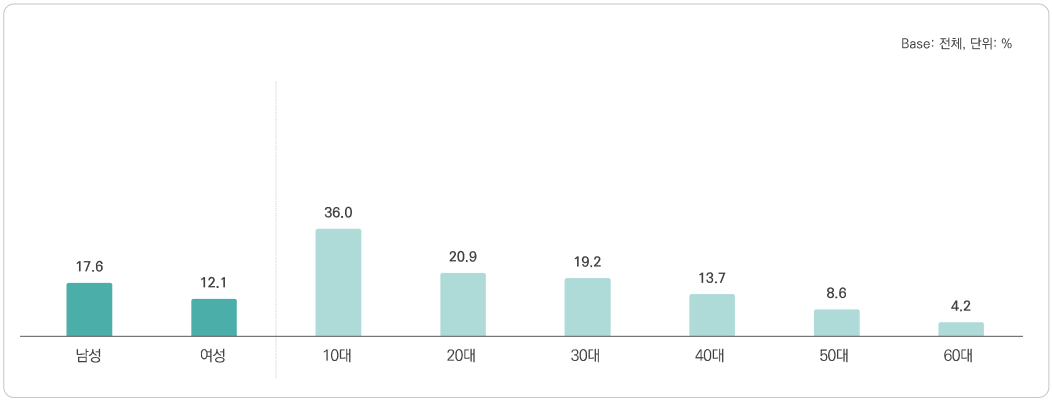


그림 2-3-18 성·연령별 정보보호교육 수강 경험

다 정보보호 교육 방식

- 정보보호 교육을 수강한 방식으로는 '근무지 혹은 학교 등에서의 온라인 교육 수강'이 68.0%로 가장 높고, '근무지 혹은 학교 등에서의 오프라인 교육 수강(44.5%)', '개인적인 방식으로 온라인 교육 수강(줌(ZOOM), EBS 온라인클래스, 유튜브 등)(16.2%)' 등의 순임

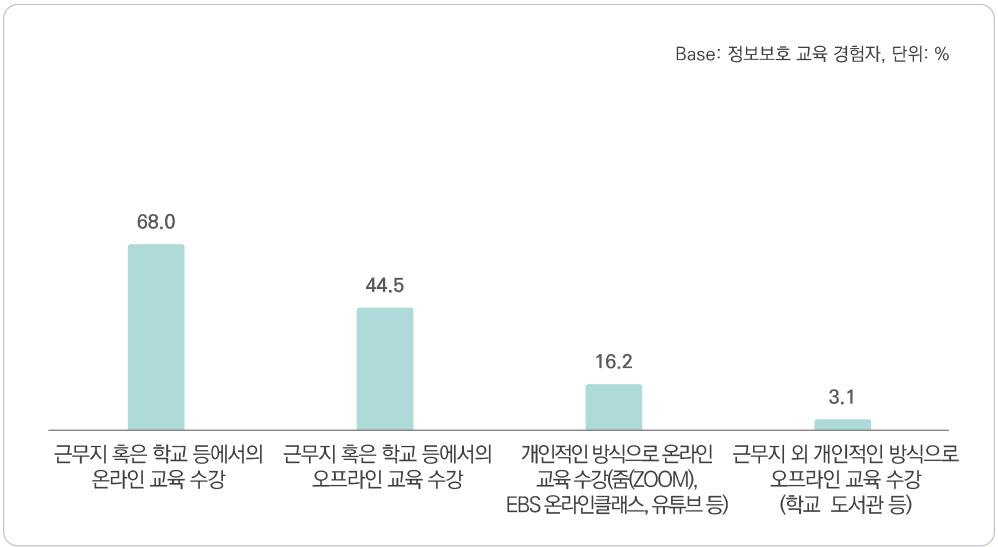


그림 2-3-19 **정보보호 교육 방식(복수응답)**

라 정보보호 교육 주제

- 수강한 정보보호 교육의 주제로는 '정보보호를 위한 사고 예방 방법'이 81.5%로 가장 높고, 다음으로 '정보보호의 중요성(75.6%)', '정보보호 피해 사례(66.6%)', '정보보호에 대한 기본 소양(배경 지식 등)(64.8%)' 등의 순임

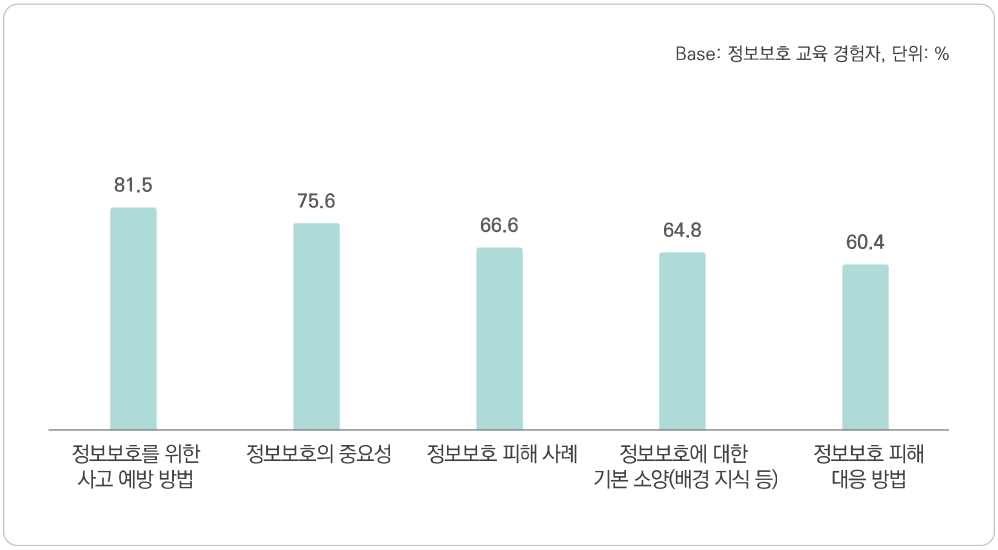


그림 2-3-20 **정보보호 교육 주제(복수응답)**

마 정보보호 교육 학습 효과

- 수강한 정보보호 교육의 학습 효과에 대해 '정보보호 피해 사례에 대한 인식'이 79.9%로 가장 높고, 다음으로 '정보보호에 대한 기본 소양(배경지식 등)의 함양(76.6%)', '정보보호 피해 대응 방법 습득(73.3%)', '정보보호의 중요성에 대한 인식(72.9%)' 등의 순임

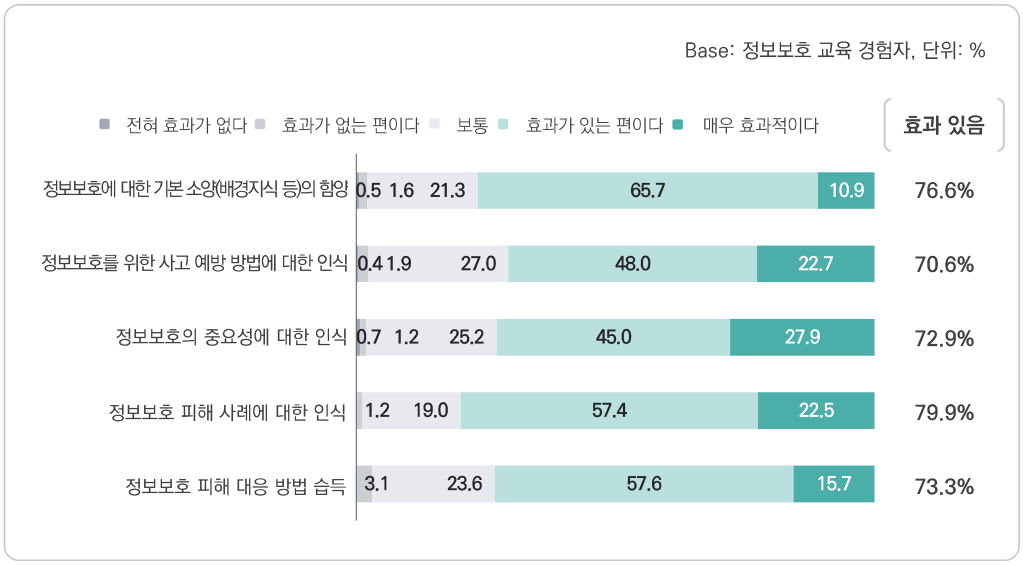


그림 2-3-21 정보보호 교육 학습 효과(요약)

바 정보보호 교육 학습 난이도

- 수강한 정보보호 교육이 이해되는 정도에 대해 '정보보호의 중요성'이 79.3%로 가장 높고, 다음으로 '정보보호에 대한 기본 소양(배경지식 등)(78.6%)', '정보보호 피해 사례(78.3%)' 등의 순임

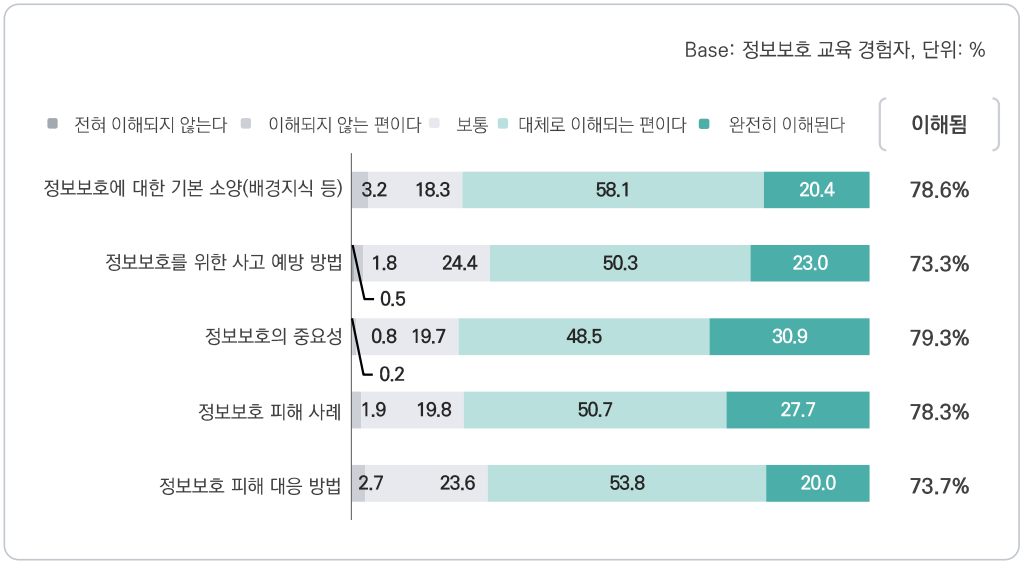


그림 2-3-22 정보보호 교육 학습 난이도(요약)

사 정보보호 학습의 어려움

- 정보보호 관련 학습이 어려운 이유에 대해 '정보의 양이 많고 복잡함'이 44.2%로 가장 높고, 다음으로 '정보보호 관련 용어가 생소하고 어려움(42.7%)', '정보보호 관련 신규 이슈가 계속 발생하여 학습이 어려움(41.1%)' 등의 순임

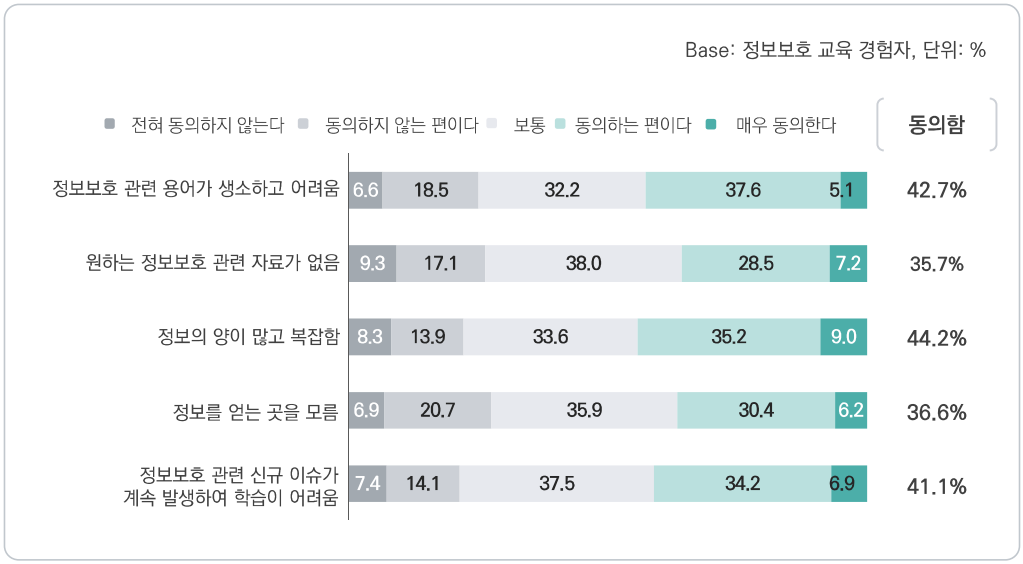


그림 2-3-23 정보보호 학습의 어려움(요약)

아 정보보호 홍보물 경험 여부

- 인터넷 이용자의 41.2%가 정보보호 관련 캠페인 또는 공익광고 등 홍보물을 접한 경험이 있다고 응답함

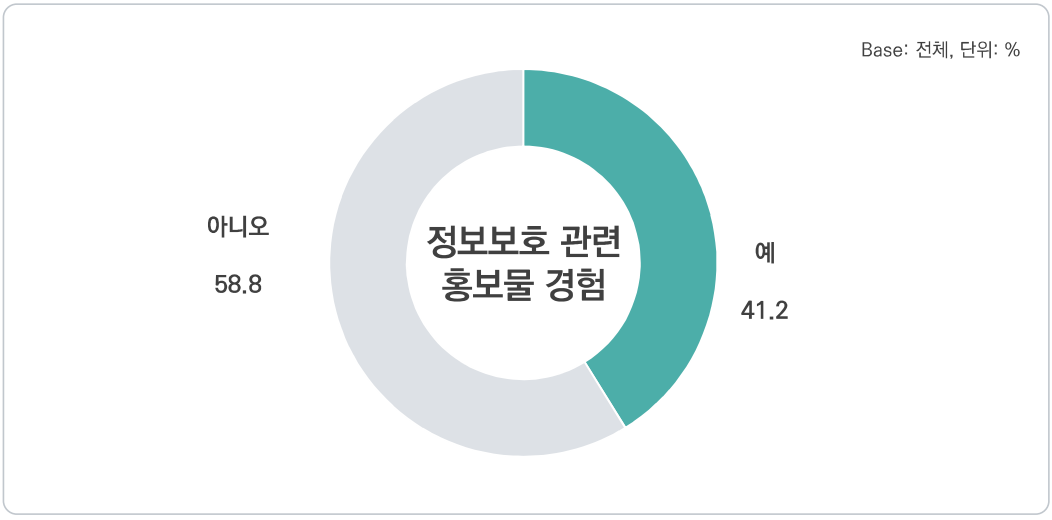


그림 2-3-24 정보보호 홍보물 경험 여부

자 정보보호 홍보물 경험 경로

- ‘방송매체(TV, IPTV, 영화, 라디오 등)’를 통해 정보보호 관련 홍보물을 접했다는 응답이 47.6%로 가장 높고, 다음으로 ‘온라인 매체(웹배너·팝업 등)(37.6%)’, ‘옥외광고(지하철·버스·마트·전광판 등)(11.3%)’ 등의 순임

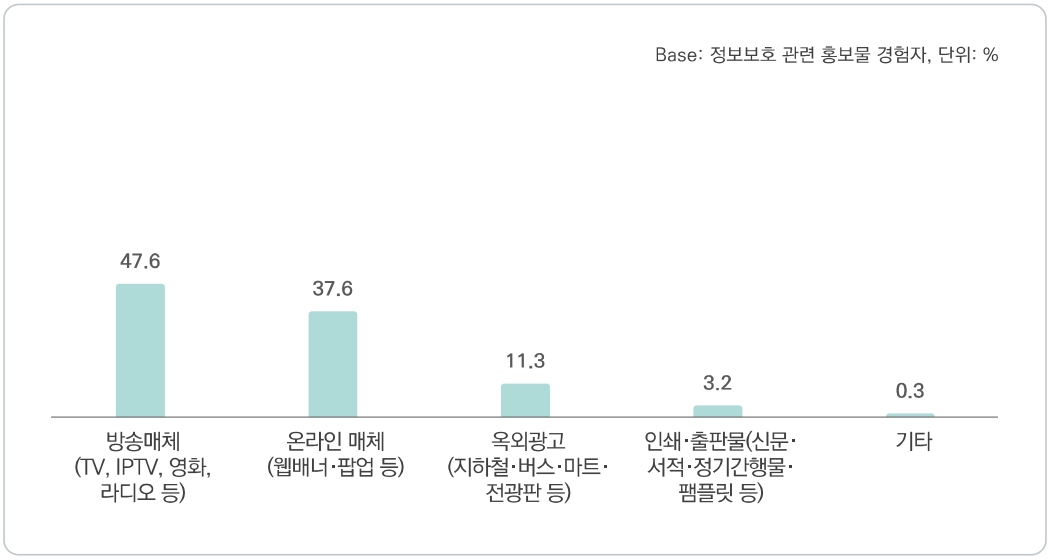


그림 2-3-25 정보보호 홍보물 경험 경로

Ⅳ 정보보호 예산

1 정보보호 예산

가 정보보호 금전 소비 경험

- 인터넷 이용자의 11.0%가 최근 1년간 개인적인 목적으로 정보보호와 관련하여 금전적인 소비를 한 경험이 있다고 응답함

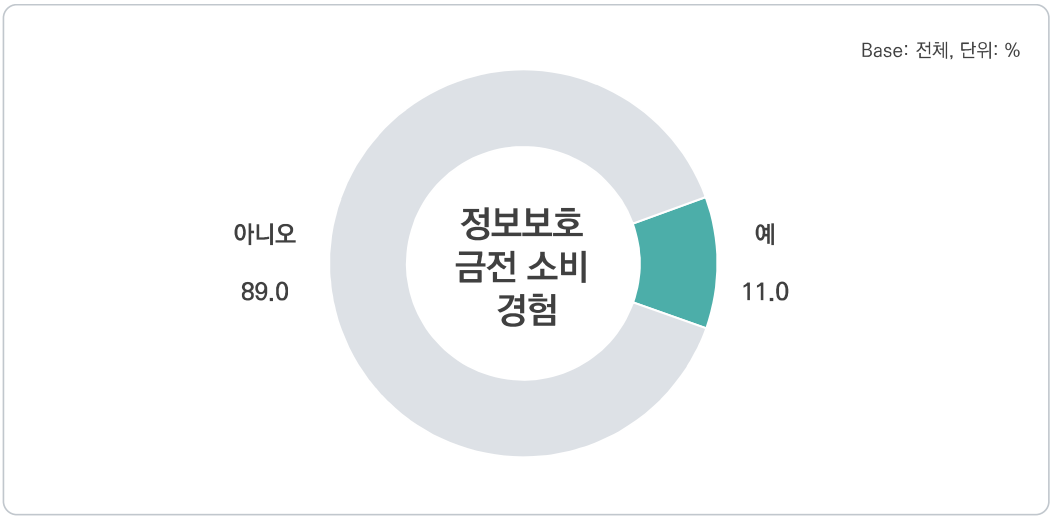


그림 2-3-26 정보보호 금전 소비 경험

- 성별로 보면 남성(12.5%)이 여성(9.4%) 대비 정보보호 금전 소비 경험률이 높게 나타남
- 연령별로 보면 40대(16.4%)의 정보보호 금전 소비 경험률이 가장 높고, 60대(4.5%)의 경험률이 상대적으로 낮게 나타남

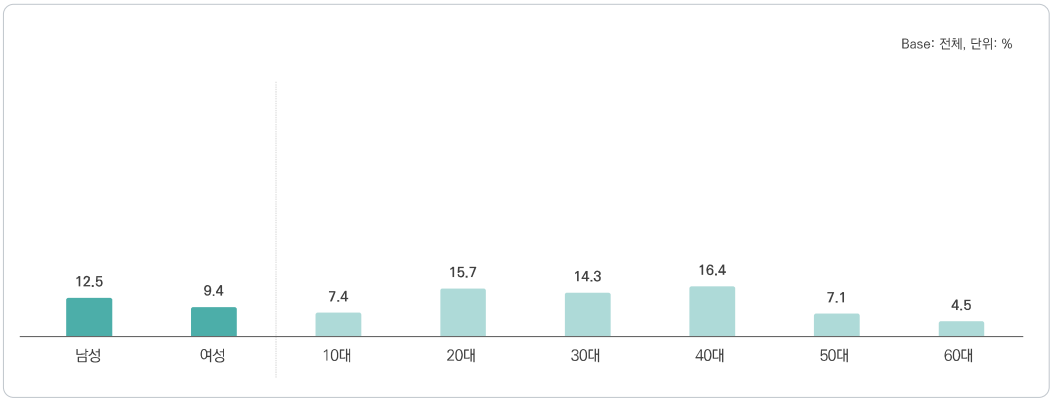


그림 2-3-27 성·연령별 정보보호 금전 소비 경험

나 정보보호 금전 소비 유형

- 정보보호 관련 금전적인 소비 중 가장 큰 비중을 차지하는 유형에 대해 '정보보호 관련 유료 인증서의 결제'가 74.0%로 가장 높고, 다음으로 '정보보호 관련 제품 및 솔루션의 구입(오픈소스, 월 SW 구독료, 클라우드 등 포함)(72.3%)', '자택 또는 개인 생활 공간의 CCTV 등 영상 감시장비 설치 또는 증설(유지·보수 포함)(33.9%)' 등의 순임

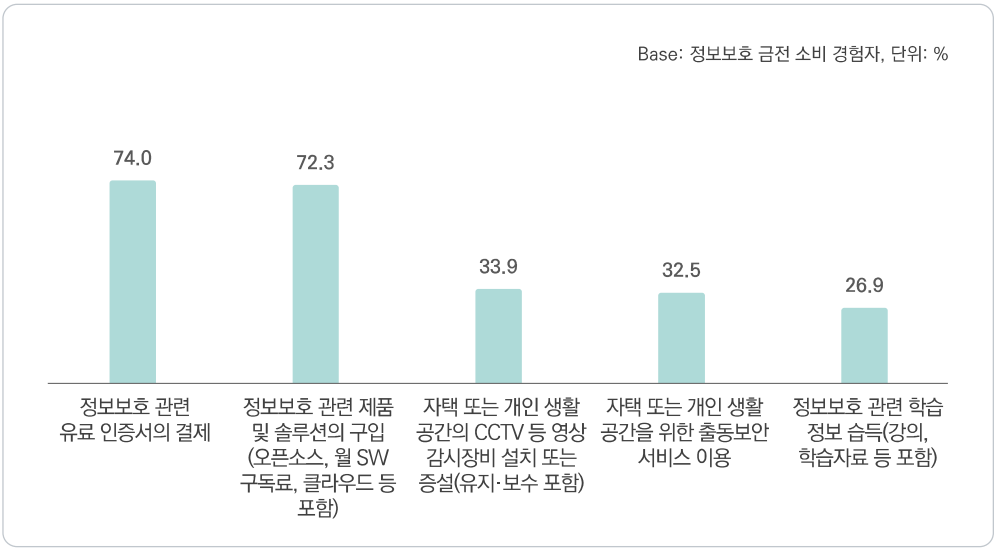


그림 2-3-28 정보보호 금전 소비 유형(종합순위)

다 정보보호 금전 소비 규모

- 최근 1년간 정보보호 관련 금전적인 소비 규모에 대해 '1만 원 이상 ~ 10만 원 미만'이 44.1%로 가장 높고, 다음으로 '10만 원 이상 ~ 20만 원 미만(19.8%)', '1만 원 미만(14.5%)' 등의 순임

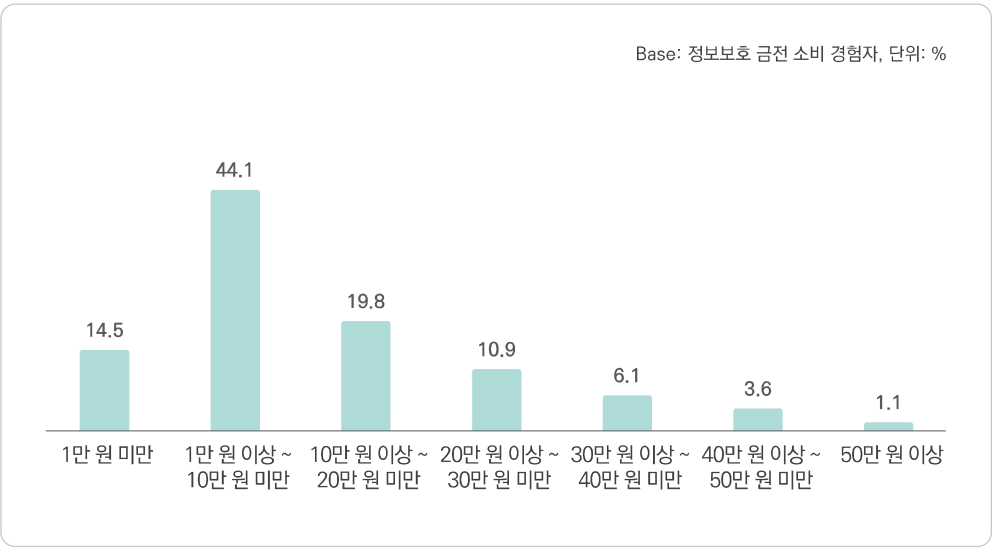


그림 2-3-29 정보보호 금전 소비 규모

라 정보보호 금전 소비 계기

- 정보보호 관련 금전적 소비를 결정하게 된 계기에 대해 '주변 지인의 정보 침해사고 피해를 간접적으로 접한 이후'가 71.1%로 가장 높고, 다음으로 'TV 또는 온라인 매체(뉴스, 유튜브, SNS 등)를 통한 정보 습득으로 위험성을 인지한 이후(56.4%)', '주변 지인의 추천을 통해(52.0%)' 등의 순임

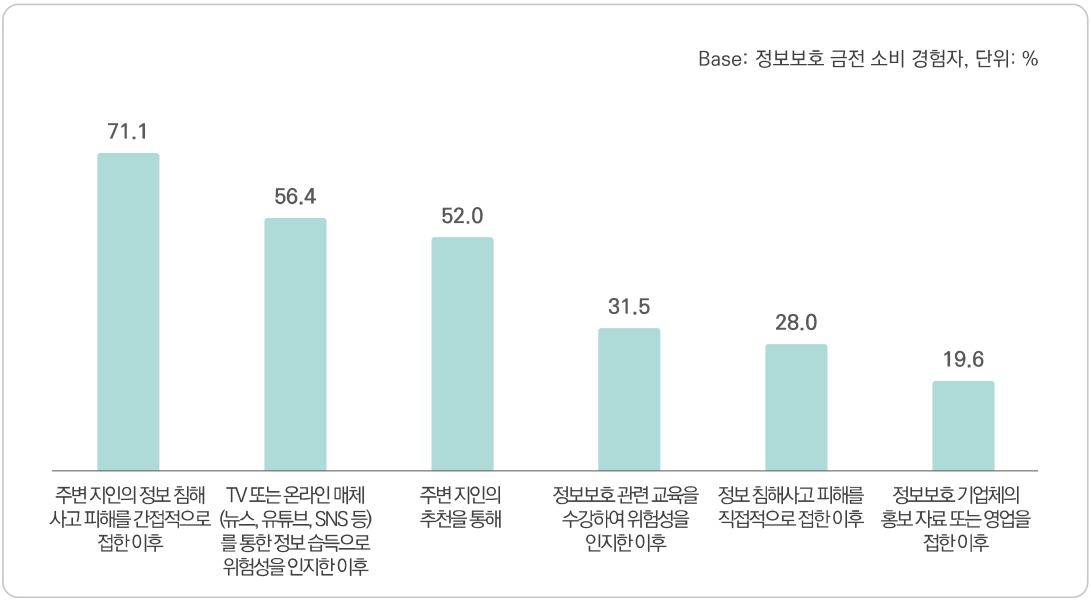


그림 2-3-30 정보보호 금전 소비 계기(종합순위)

마 정보보호 금전 소비 적절성

- 정보보호 금전 소비 경험자는 정보보호 관련 금전적인 소비의 적절성에 대해 65.5%가 '적절하다(그렇다+매우 그렇다)'고 응답함

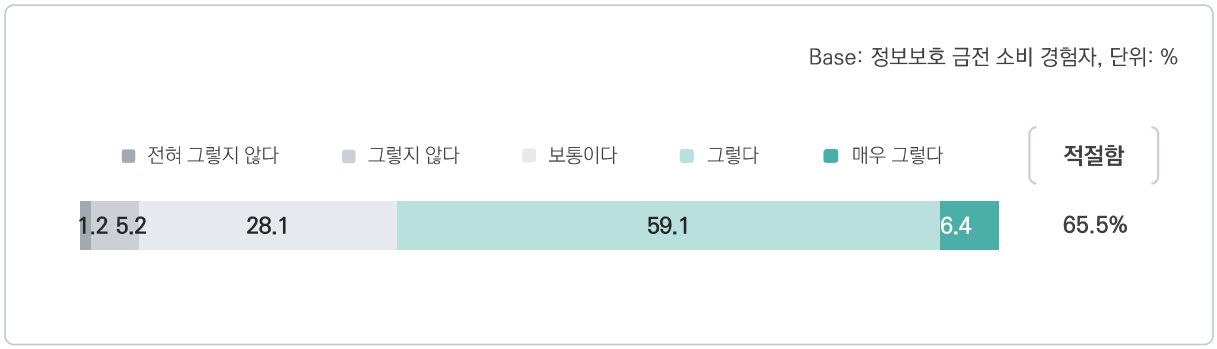


그림 2-3-31 정보보호 금전 소비 적절성

바 정보보호 금전 소비 비용 증감 여부

- 정보보호 금전 소비 경험자의 35.2%가 향후 정보보호 관련 금전 소비 비용 증감 여부에 대해 '증가 예정(늘릴 예정이다+크게 늘릴 예정이다)'이라고 응답함
  - 현재와 '비슷할 것이다'라고 응답한 비율이 59.1%로 가장 높음

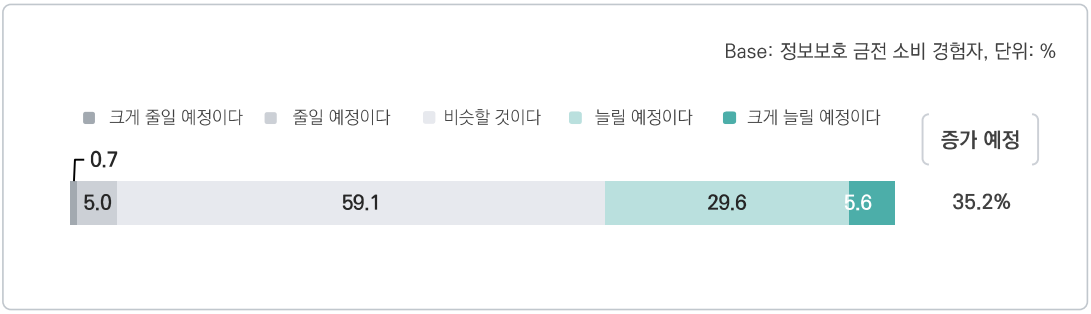


그림 2-3-32 정보보호 금전 소비 비용 증감 여부

사 향후 정보보호 비용 지출 의향

- 정보보호 금전 소비 비경험자의 28.6%가 향후 정보보호 활동을 위해 비용을 지출할 의향에 대해 '의향 있다(그렇다+매우 그렇다)'고 응답함
  - 향후 비용을 지출할 '의향 없다(전혀 그렇지 않다+그렇지 않다)'고 응답한 비율은 33.1%로 나타남

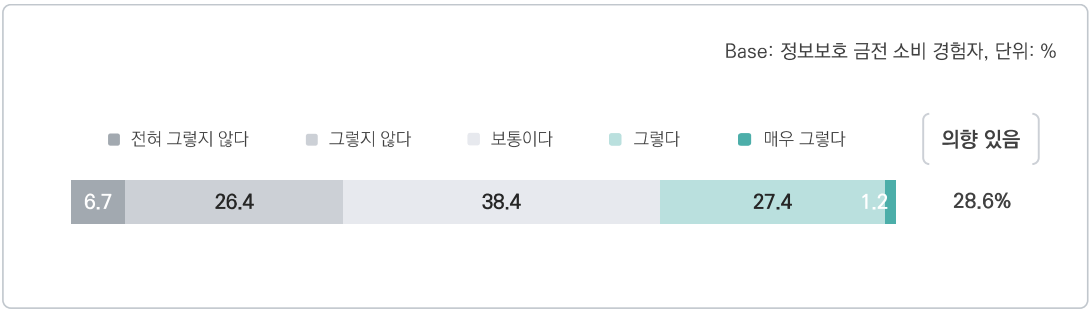


그림 2-3-33 향후 정보보호 비용 지출 의향

V 일상생활 속의 정보보호

1 일상생활 속의 정보보호

가 무료 인터넷 연결 빈도

- 인터넷 이용자의 44.5%는 공공장소에서 제공되는 무료 인터넷(Wi-fi)에 노트북, 스마트폰, 패드 등을 연결하여 '사용한다(자주 사용하는 편이다+항상 사용한다)'고 응답함

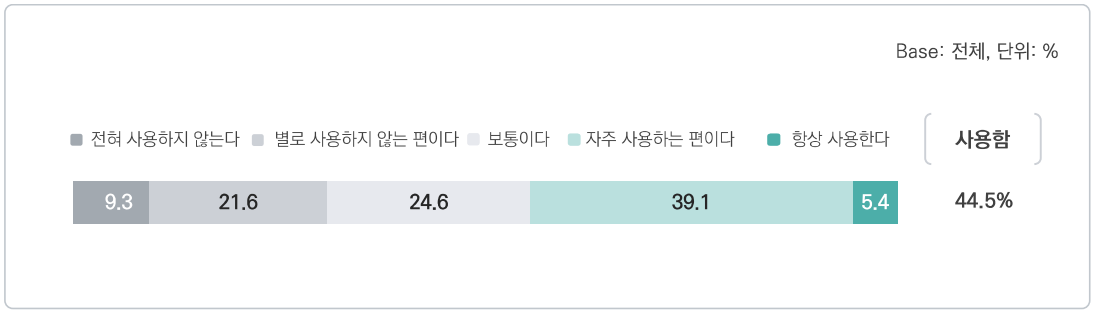


그림 2-3-34 무료 인터넷 연결 빈도

나 불특정 다수 이용 전자장비 이용 시 예방 활동

- 인터넷 이용자의 39.7%는 공공장소, PC방 등 불특정 다수가 사용하는 전자장비에 개인 계정으로 접속할 경우, 별도의 로그아웃(Log-out), 접속기록(쿠키) 삭제 등과 같은 예방 활동을 '수행한다(대체로 수행하는 편이다+반드시 수행한다)'고 응답함

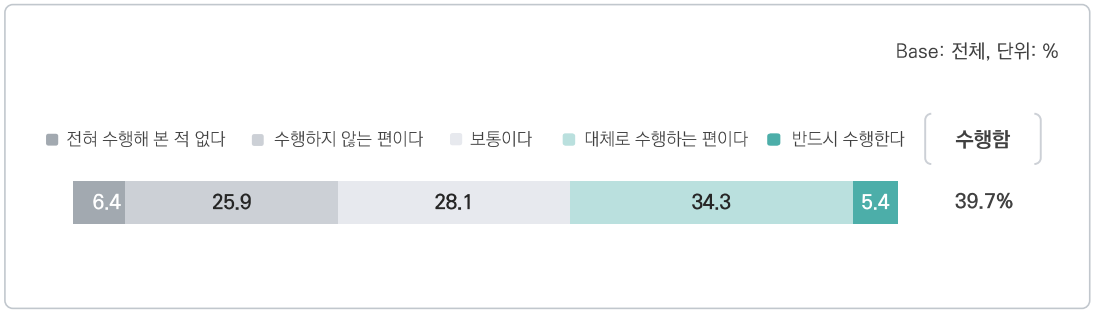


그림 2-3-35 불특정 다수 이용 전자장비 이용 시 예방 활동

다 비밀번호 변경 필요 안내 시 비밀번호 즉시 변경

- 인터넷 이용자의 35.3%는 인터넷 서비스를 이용하면서 비밀번호 변경이 필요함을 안내받았을 때 비밀번호를 즉시 변경하는 것으로 응답함

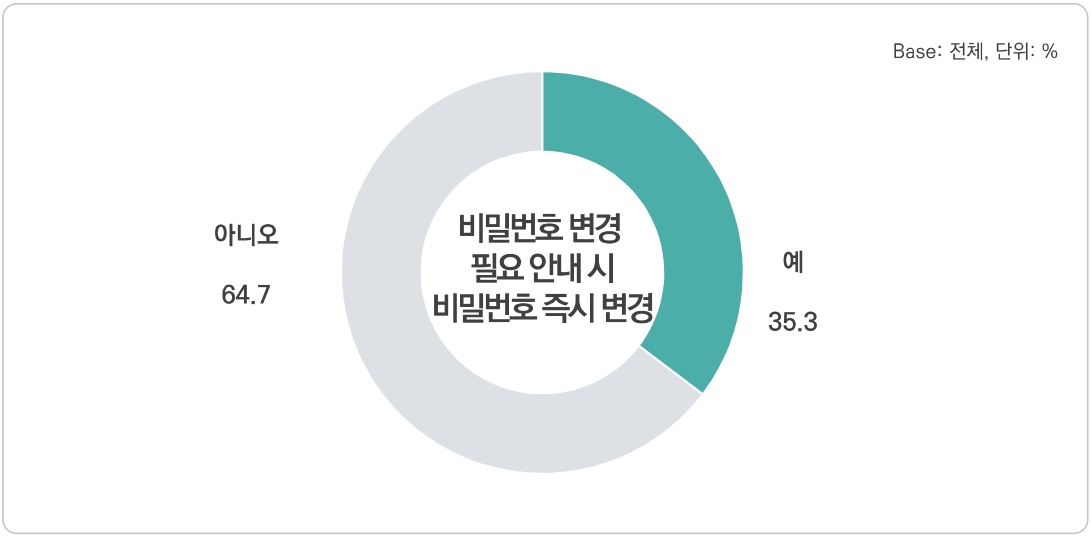


그림 2-3-36 비밀번호 변경 필요 안내 시 비밀번호 즉시 변경

- 성별로 보면, 남성(36.0%)이 여성(34.7%) 대비 비밀번호 즉시 변경 수행률이 높게 나타남
- 연령별로 보면, 20대(44.1%)의 비밀번호 즉시 변경 수행률이 가장 높고, 60대(25.6%)가 가장 낮게 나타남

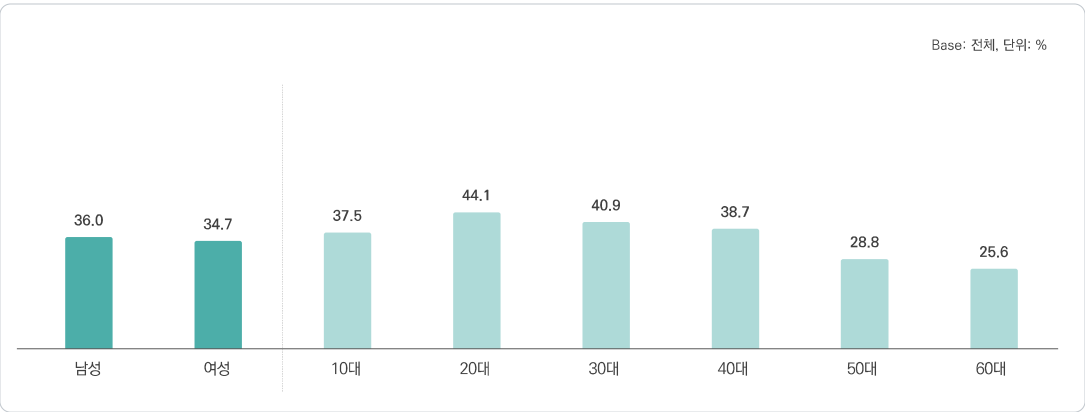


그림 2-3-37 성·연령별 비밀번호 변경 필요 안내 시 비밀번호 즉시 변경

라 디지털 데이터 백업

- 인터넷 이용자의 34.5%는 최근 1년간 정보보호를 위해 PC(노트북 포함), 스마트폰 등 개인 전자장비에 저장된 디지털 데이터(사진 포함)를 백업한 경험이 있는 것으로 응답함

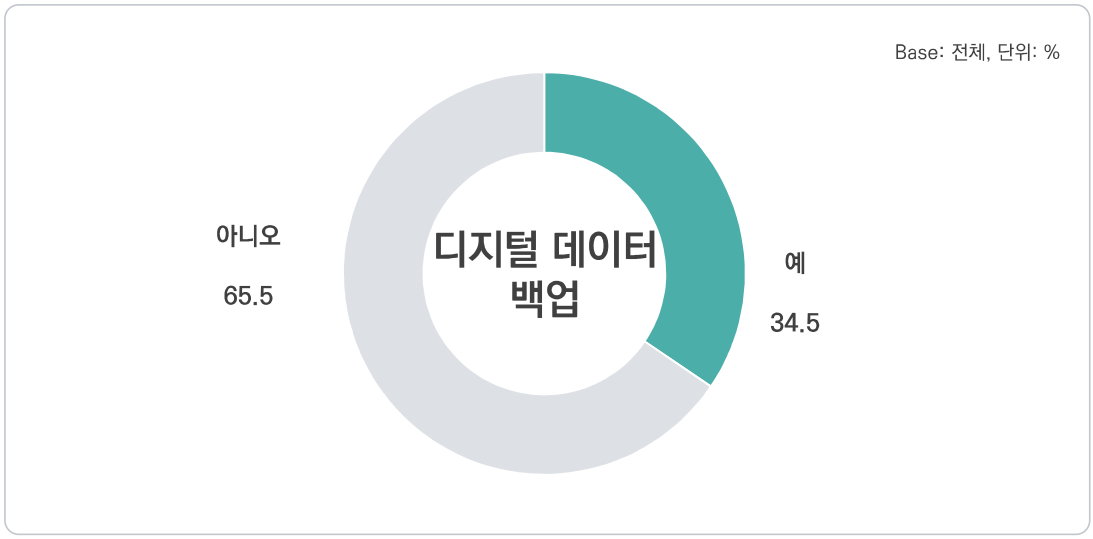


그림 2-3-38 디지털 데이터 백업

- 성별로 보면, 남성(36.5%)이 여성(32.4%) 대비 디지털 데이터 백업 수행률이 높게 나타남
- 연령별로 보면, 20대(44.7%) 및 30대(44.6%)의 백업 수행률이 가장 높고, 60대(21.3%)가 가장 낮게 나타남

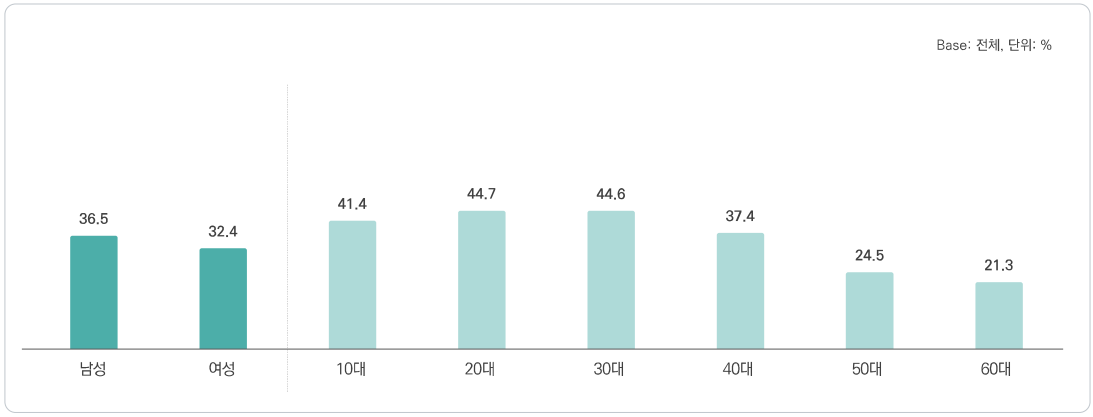


그림 2-3-39 성·연령별 디지털 데이터 백업

마 보안 점검 수행

- 인터넷 이용자의 41.9%는 최근 1년간 정보보호를 위해 PC(노트북 포함), 스마트폰 등 개인용 전자기기에 설치된 보안 프로그램을 활용하여 보안 점검을 수행한 경험이 있는 것으로 응답함

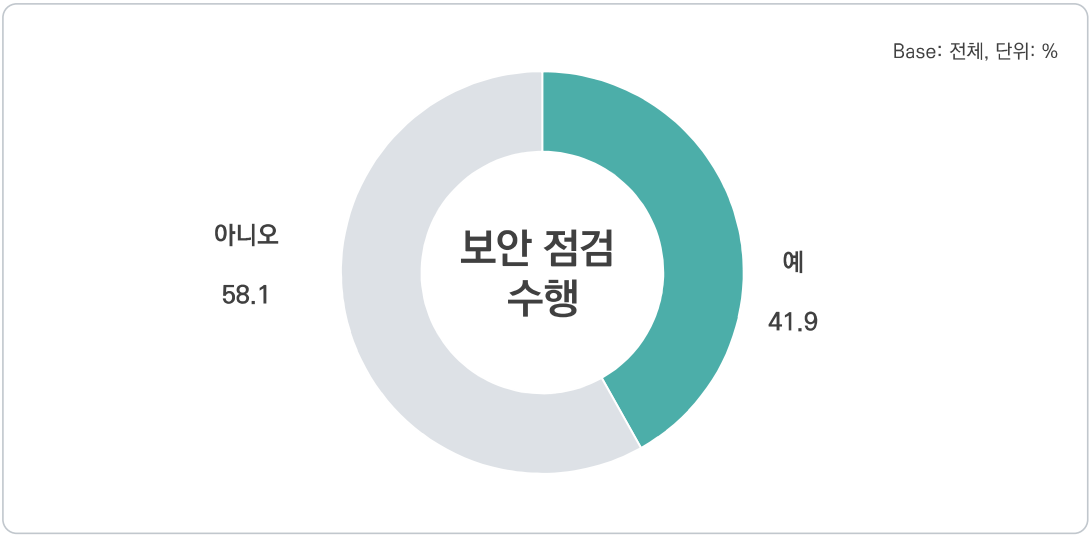


그림 2-3-40 보안 점검 수행

- 성별로 보면, 남성(45.7%)이 여성(37.9%) 대비 보안 점검 수행률이 높게 나타남
- 연령별로 보면, 40대(50.2%)의 보안 점검 수행률이 가장 높고, 60대(28.5%)가 가장 낮게 나타남

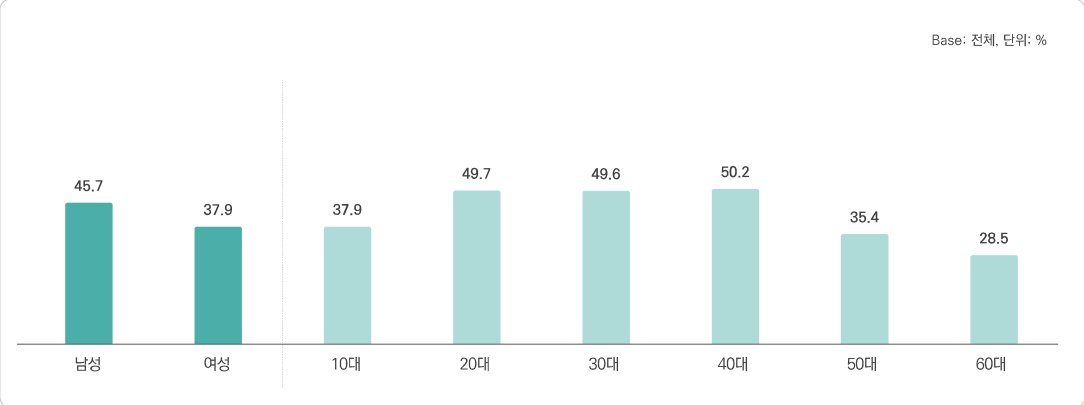


그림 2-3-41 성·연령별 보안 점검 수행

바 정보보호를 위한 보안 예방 조치

- 정보보호를 위해 수행하는 보안 예방 조치로는 '의심스러운 URL 링크 클릭하지 않음'이 77.9%로 가장 높고, 다음으로 '웹사이트의 파일을 함부로 다운로드하지 않음(71.2%)', '금융권 이용 시 정보가 노출되지 않도록 주의(49.7%)' 등의 순임

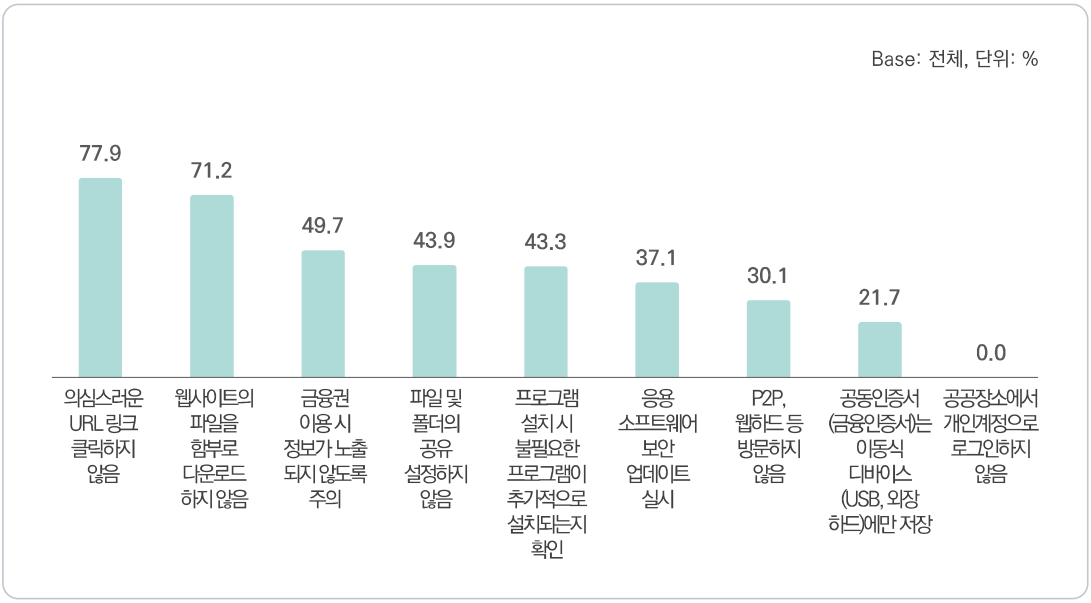


그림 2-3-42 정보보호를 위한 보안 예방 조치(복수응답)

사 원격근무 경험

- 인터넷 이용자의 20.6%는 원격근무를 수행한 경험이 있는 것으로 응답함

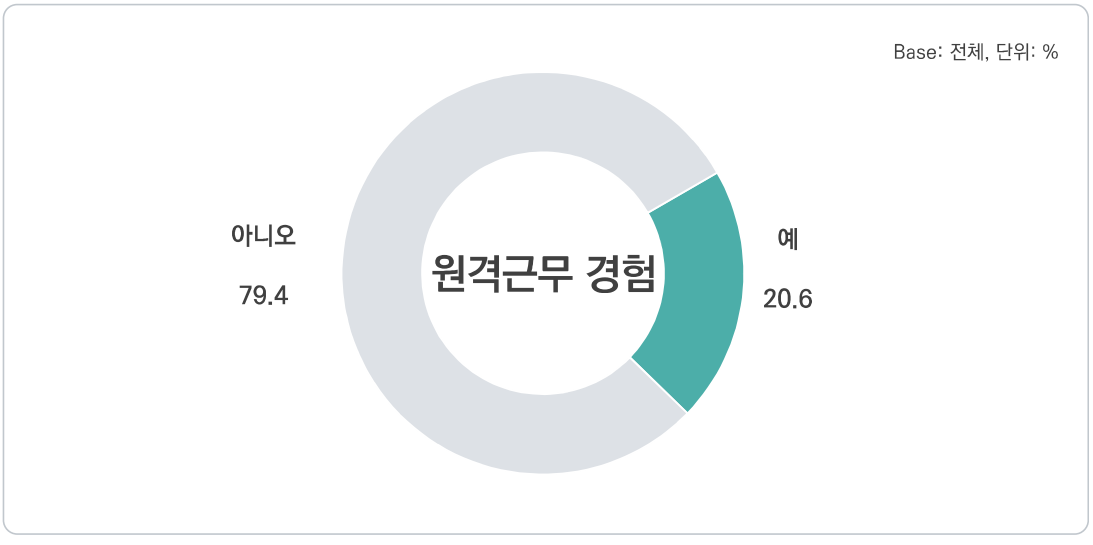


그림 2-3-43 원격근무 경험

아 비대면 환경의 정보보호 활동

- 원격근무 경험자의 주요 정보보호 활동으로는 '비대면 환경을 활용하고 있는 컴퓨터로 의심스러운 URL 클릭 등을 하지 않음'이 28.5%로 가장 높고, 다음으로 '학교, 회사 등에서 제공한 정보보호 제품을 사용(27.0%)', '원격근무 화상회의 등 이용 시 관련 프로그램 이외의 프로그램을 사용하거나 작동하지 않음(19.7%)' 등의 순임

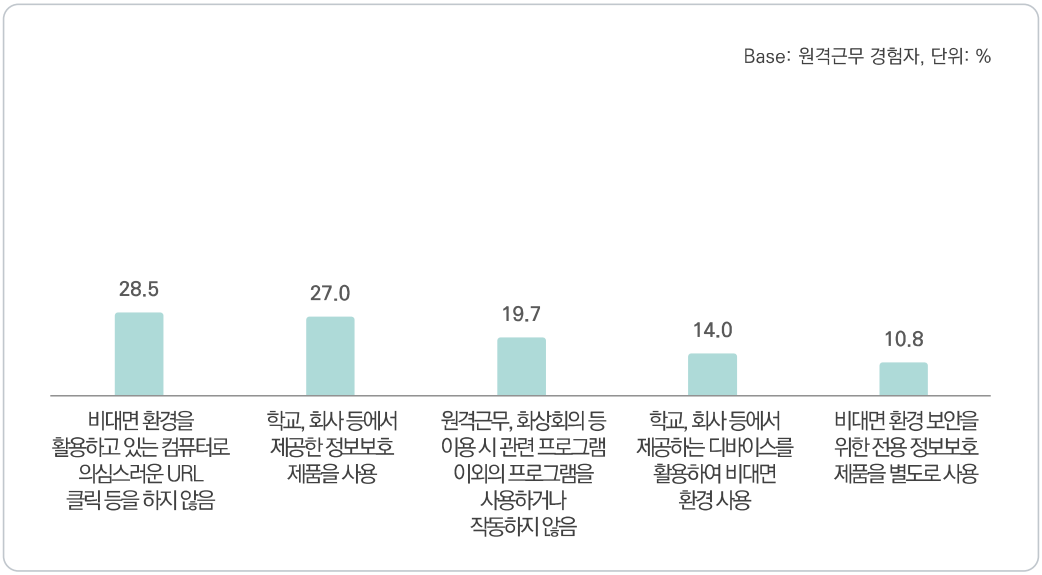


그림 2-3-44 비대면 환경의 정보보호 활동

자 일상 생활 공간 중 영상 감시 장비 활용

- 인터넷 이용자의 8.5%는 개인적인 일상생활 공간에서 CCTV 또는 IP 카메라와 같은 영상 감시 장비를 사용하고 있는 것으로 응답함

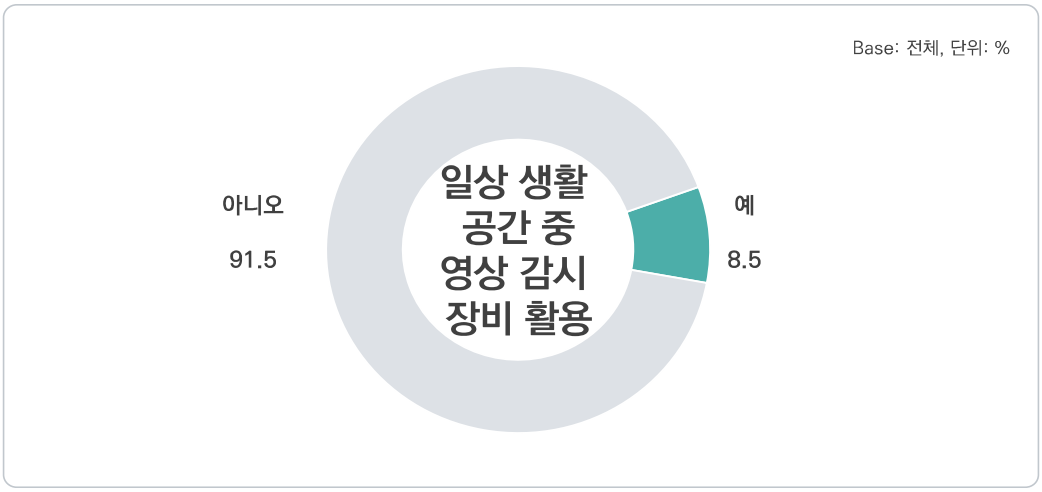


그림 2-3-45 일상 생활 공간 중 영상 감시 장비 활용

Ⅵ 정보 침해사고 경험과 위협 인식

1 정보 침해사고 경험

가 침해사고 공식 신고·상담 창구 인지

- 인터넷 이용자의 41.1%는 침해사고 공식 신고·상담 창구에 대해 인지하고 있다고 응답함

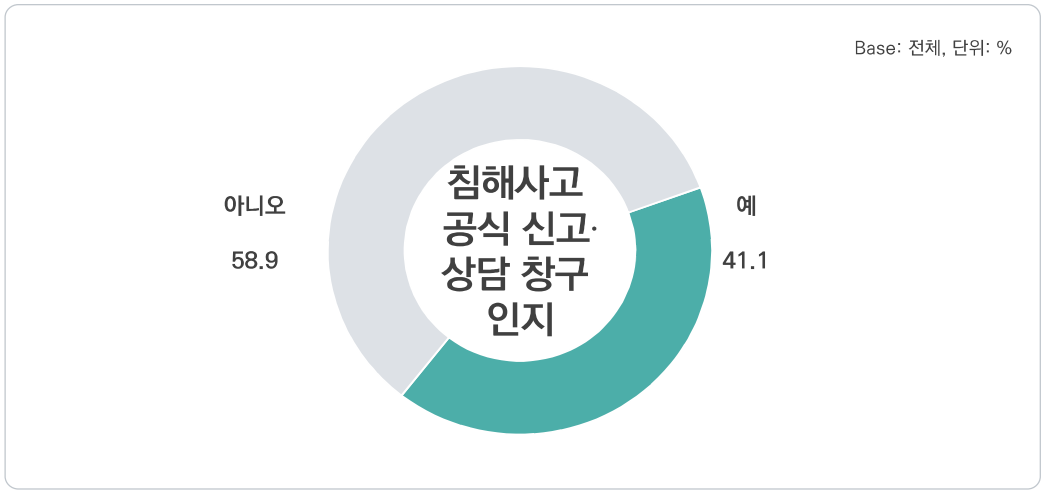


그림 2-3-46 침해사고 공식 신고·상담 창구 인지

나 정보 침해사고 의심

- 인터넷 이용자의 22.0%는 최근 1년간 정보 침해사고를 의심한 경험이 있다고 응답함

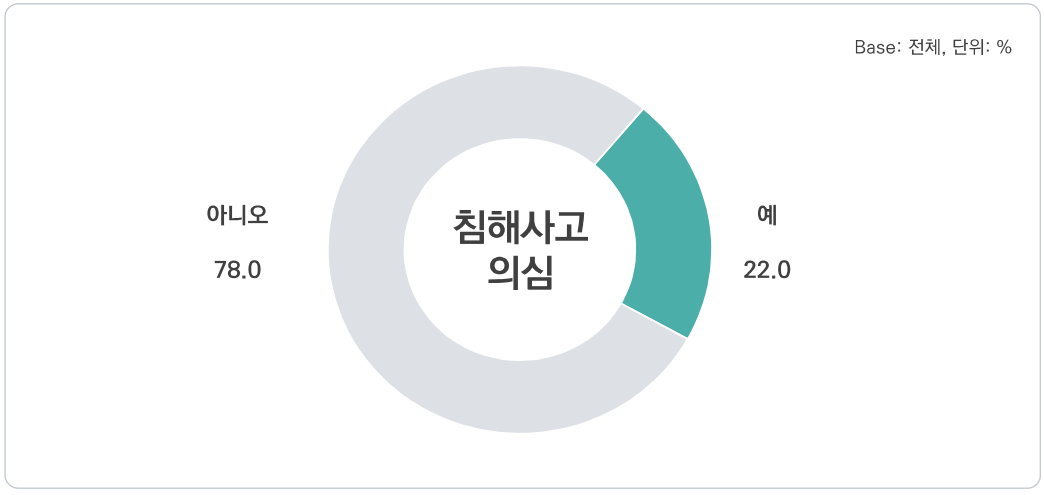


그림 2-3-47 정보 침해사고 의심

다 정보 침해사고 경험

- 인터넷 이용자의 8.5%는 최근 1년간 정보 침해사고를 경험한 적 있다고 응답함

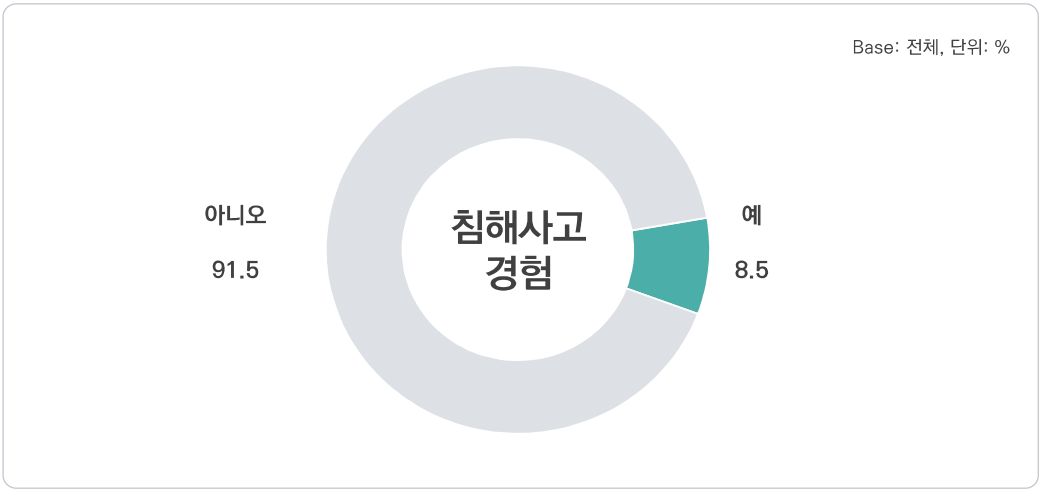


그림 2-3-48 정보 침해사고 경험

라 정보 침해사고 피해 인지 소요 시간

- 정보 침해사고를 경험하였을 때, 피해 사실을 인지하기까지 소요된 시간에 대해 '7일(일주일) 이내'가 27.3%로 가장 높고, 다음으로 '1일 이내(16.1%)' 및 '30일(1개월) 이내(16.1%)', '1시간 이내(13.5%)' 등의 순임

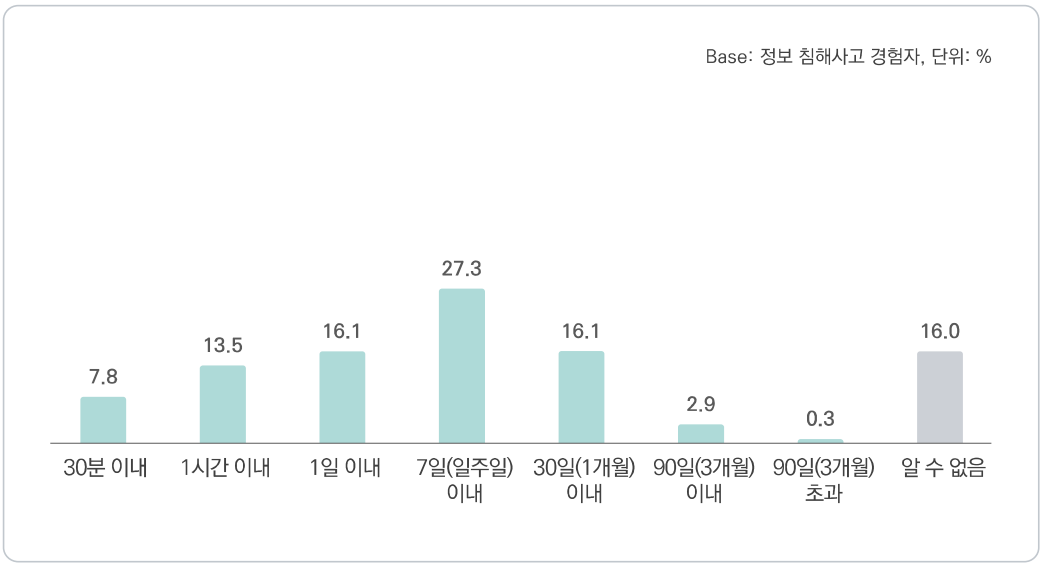


그림 2-3-49 정보 침해사고 피해 인지 소요 시간

마 정보 침해사고 인지 경로

- 정보 침해사고 피해 여부를 인지한 경로에 대해 '침해사고 발생한 기업(쇼핑몰·카드사 등) 온라인 서비스 포털 등으로부터 침해 안내 메일 또는 문자를 받음'이 28.2%로 가장 높고, 다음으로 '언론 보도를 통해 침해사고를 인지함(20.0%)', '보안 시스템의 침해사고 경보(알림)(16.2%)' 등의 순임

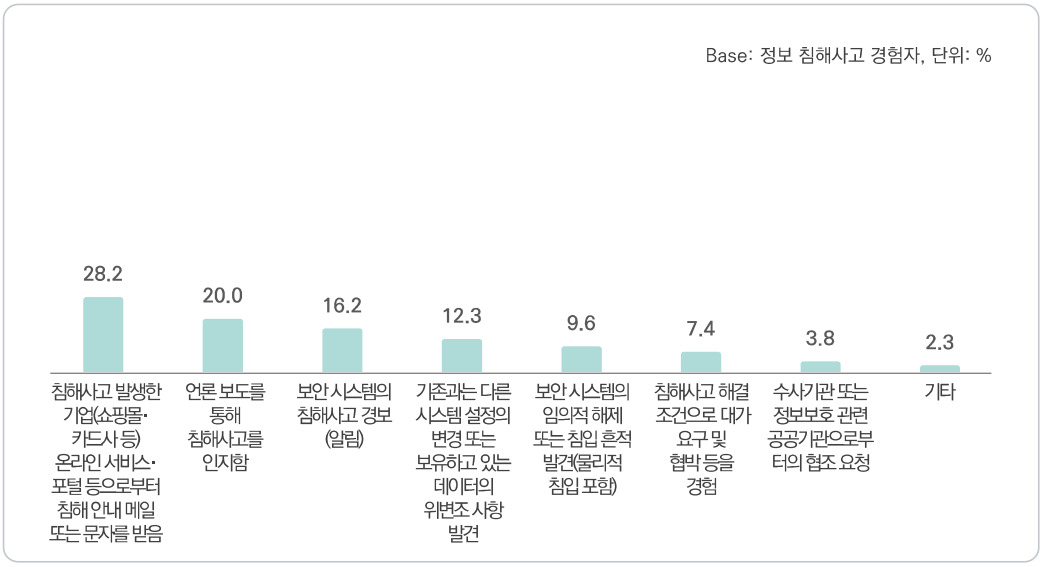
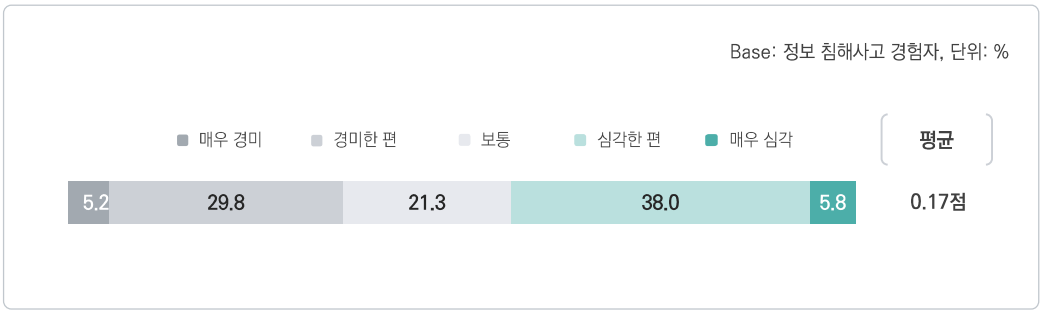


그림 2-3-50 정보 침해사고 인지 경로

바 정보 침해사고 피해 심각도

- 정보 침해사고를 경험한 경우, 피해 심각성은 평균 0.17점으로 다소 심각한 편으로 나타남



* '평균'은 -5점(침해사고는 있었으나 피해는 매우 경미하다)부터 5점(단시간에 회복되기 어려운 피해가 있었다) 중에 응답한 점수를 평균화한 것임

그림 2-3-51 정보 침해사고 피해 심각도

사 침해사고 금전적 손실

- 침해사고 경험자의 21.7%가 침해사고 금전적 손실을 경험한 적이 있다고 응답함

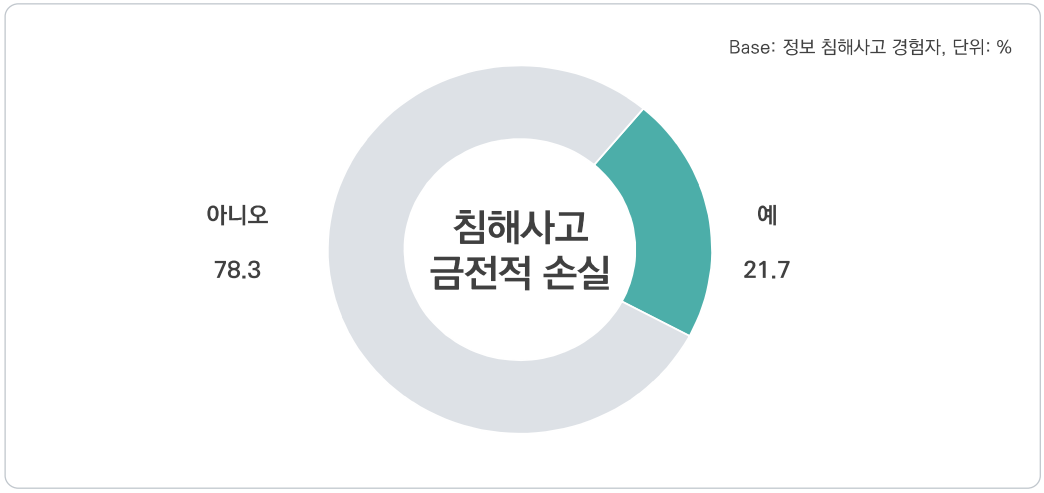


그림 2-3-52 침해사고 금전적 손실

아 침해사고 복구 비용 지출

- 침해사고 경험자의 23.1%가 침해사고 복구 비용 지출 경험이 있다고 응답함

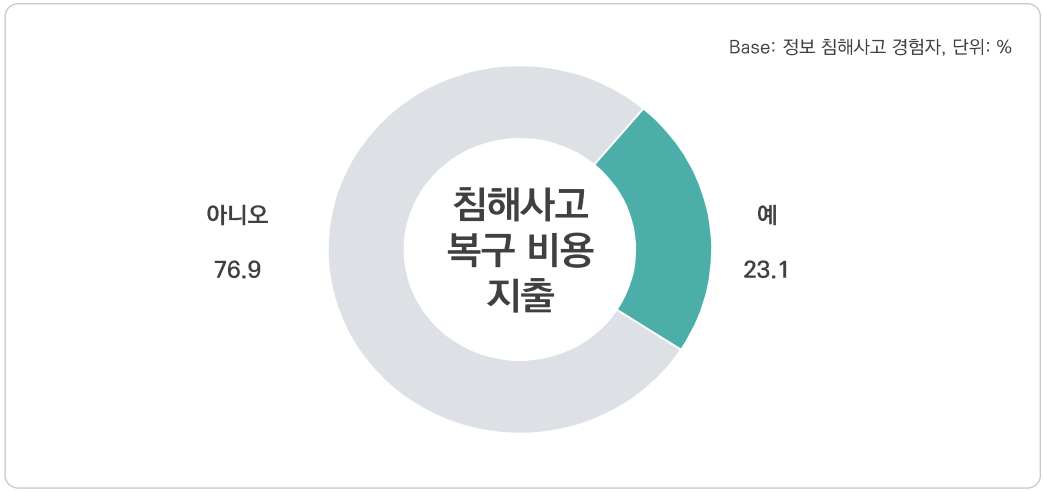


그림 2-3-53 침해사고 복구 비용 지출

자 정보 침해사고 경험 유형

- 최근 1년간 경험한 정보 침해사고의 유형에 대해 '개인용 모바일 기기(스마트폰 태블릿 패드 등)의 해킹과 같은 불법적 접근'이 44.7%로 가장 높고, 다음으로 'PC 또는 노트북 등 개인용 컴퓨터의 해킹과 같은 불법적 접근(34.9%)', '개인용 전자기기에 대한 불법적 접근으로 인한 보유 중인 데이터의 외부 유출(28.0%)' 등의 순임

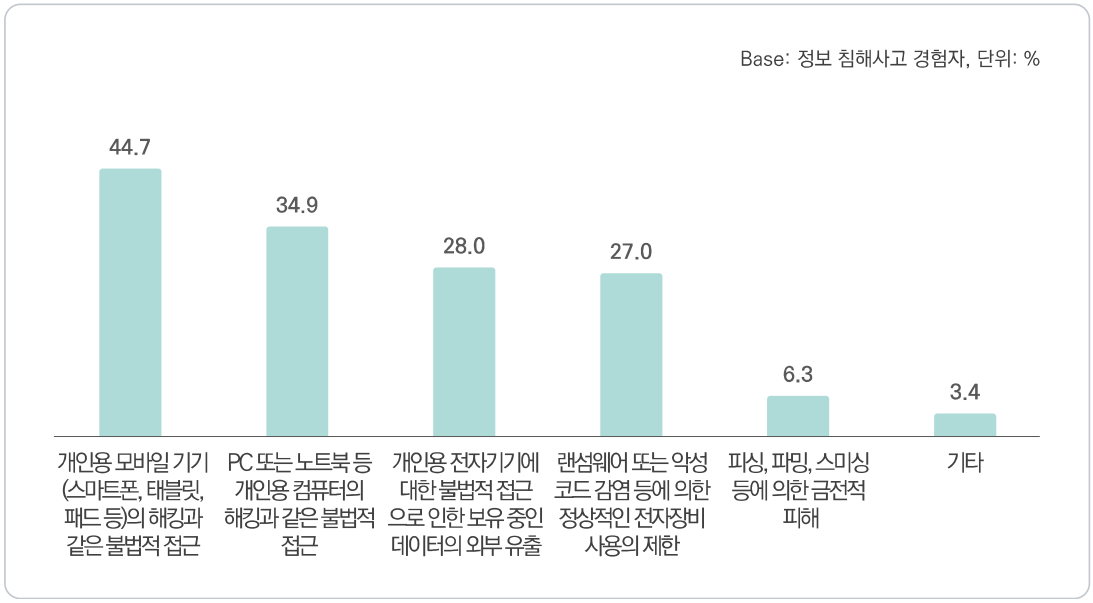


그림 2-3-54 정보 침해사고 경험 유형(복수응답)

차 정보 침해사고 관심도 변화

- 침해사고 경험자의 77.8%가 정보 침해사고 경험 이후 정보 침해사고에 대한 관심도 변화에 대해 '증가함(관심이 커졌다+관심이 매우 커졌다)'으로 응답함

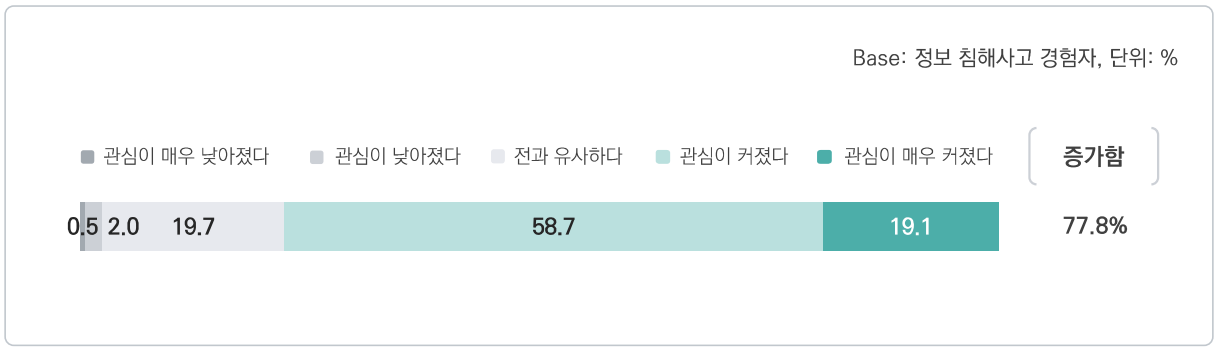


그림 2-3-55 정보 침해사고 관심도 변화

카 정보 침해사고 신고

- 침해사고 경험자의 41.2%는 침해사고가 발생했을 때 관련 기관에 피해 사실을 신고한 것으로 나타남

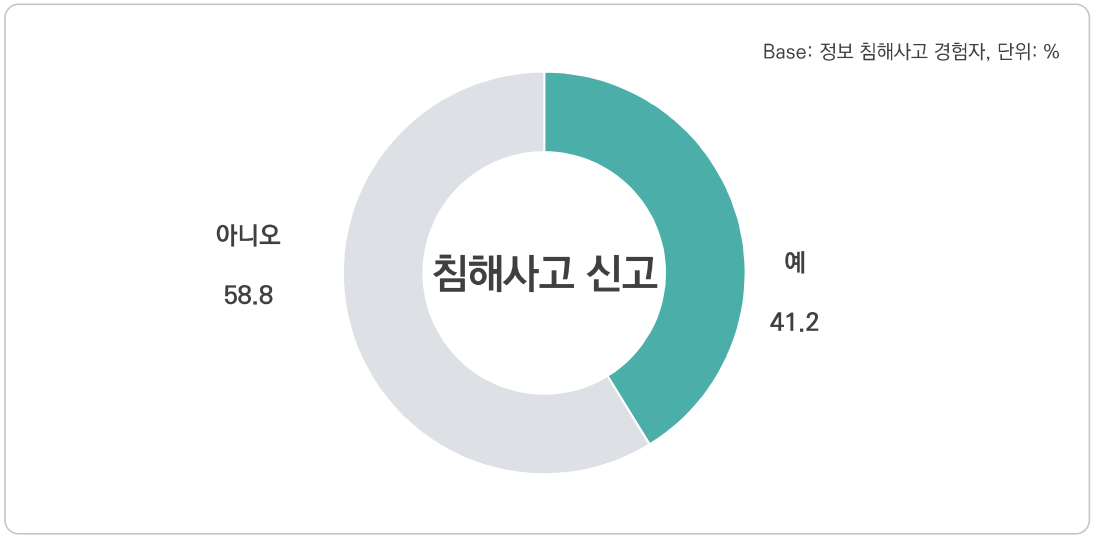


그림 2-3-56 정보 침해사고 신고

타 정보 침해사고 미신고 이유

- 침해사고 미신고자가 침해사고를 신고하지 않은 이유로는 '피해가 심각하지 않았기 때문에'가 59.7%로 가장 높고, 다음으로 '신고에 따른 사건 조사, 처리가 복잡하다고 느껴졌기 때문에(30.9%)', '신고하더라도 피해가 복구되지 못한다고 생각하기 때문에(29.0%)' 등의 순임

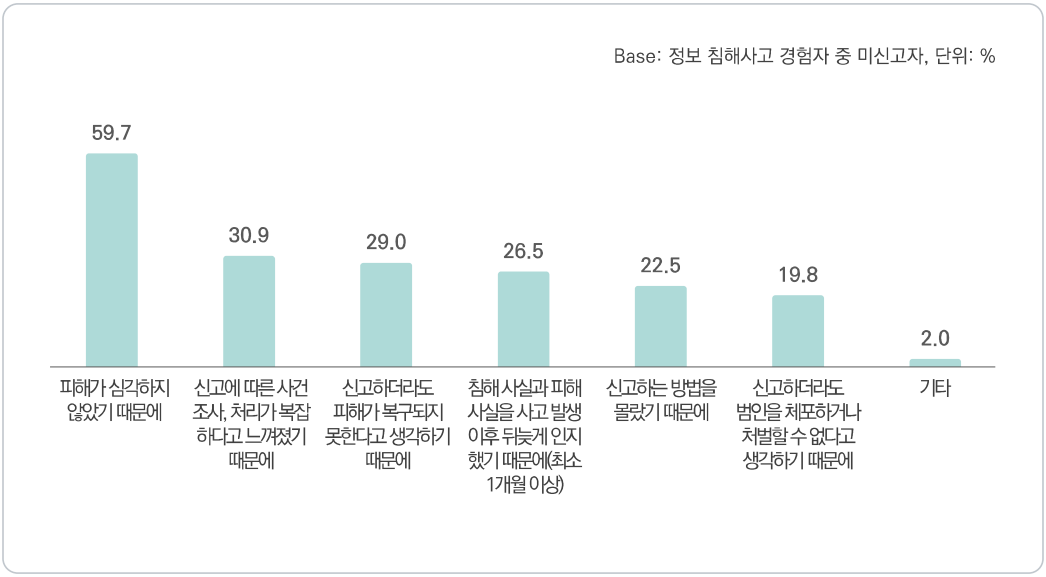
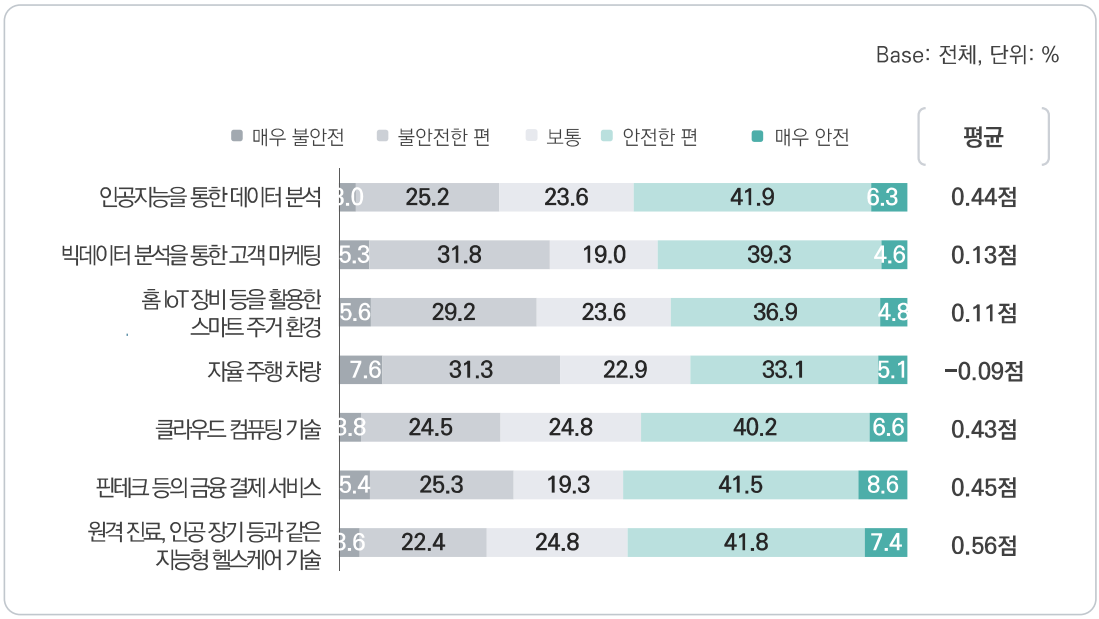


그림 2-3-57 정보 침해사고 미신고 이유(종합순위)

2 정보 침해사고 위협 인식

가 최신 IT 기술 이용 시 정보 침해사고로부터의 안전도

- 최신 IT 기술 중에 '원격 진료, 인공 장기 등과 같은 지능형 헬스케어 기술'이 안전도 0.56점으로 정보 침해사고로부터 가장 안전하다고 인식되고 있으며, 다음으로 '핀테크 등의 금융 결제 서비스(0.45점)', '인공지능을 통한 데이터 분석(0.44점)' 등의 순임
  - 정보 침해사고로부터 가장 취약하다고 인식되고 있는 최신 IT 기술은 '자율 주행 차량(-0.09점)'이며, 다음으로 '홈 IoT 장비 등을 활용한 스마트 주거 환경(0.11점)' 등의 순임

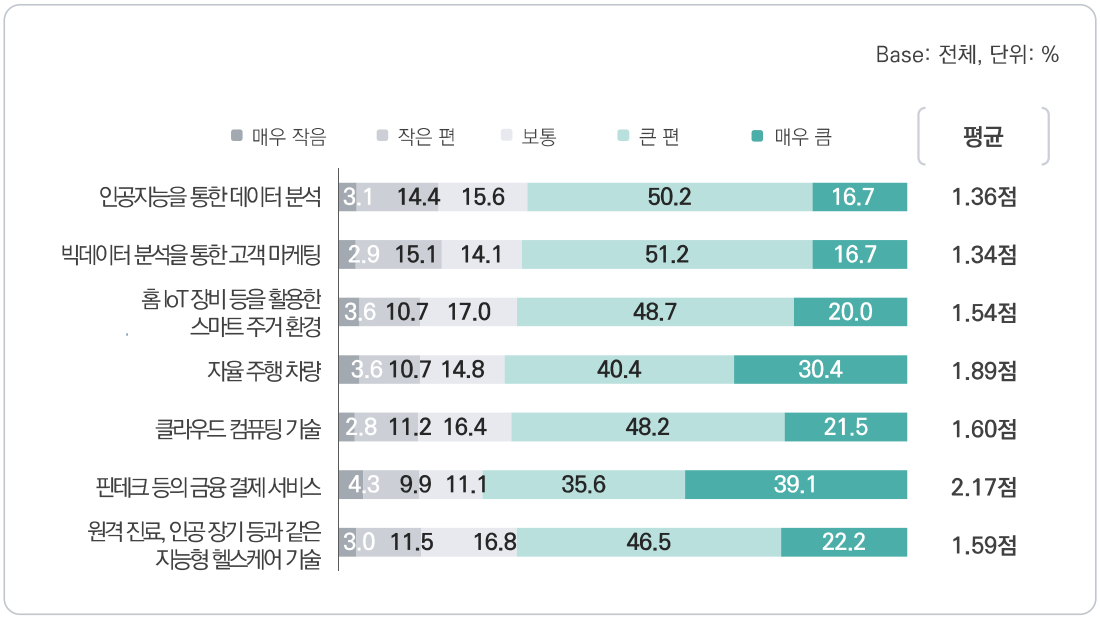


* '평균'은 -5점(전혀 안전하지 않다)부터 5점(매우 안전하다) 중에 응답한 점수를 평균화한 것임

그림 2-3-58 최신 IT 기술 이용 시 정보 침해사고로부터의 안전도(요약)

나 최신 IT 기술 정보 침해사고 발생 시 피해 파급효과

- 최신 IT 기술과 관련된 정보 침해사고 발생 시, 해당 침해사고가 우리 사회에 미치는 피해의 파급효과에 대해 '핀테크 등의 금융 결제 서비스'가 2.17점으로 파급효과가 가장 크다고 인식되고 있으며, 다음으로 '자율 주행 차량(1.89점)', '클라우드 컴퓨팅 기술(1.60점)' 등의 순임



* '평균'은 -5점(매우 작다)부터 5점(매우 크다) 중에 응답한 점수를 평균화한 것임

그림 2-3-59 최신 IT 기술 정보 침해사고 발생 시 피해 파급효과(요약)

부 록

부 록 1

주요 변경내역

Ⅰ. 기업 부문 | Ⅱ. 개인 부문

Ⅰ 기업 부문

부록 표 1-1 기업 부문 조사표 주요 변경내역

분야	항목	세부 항목	조사 시기
Ⅰ. 정보보호 기반 및 환경	A. 정보보호 인식	기업의 정보보호 중요성 인식	'19-'25
		개인정보보호 중요성 인식	'19-'21
		경영진의 정보보호 중요성 인식	'10-'17, '24-'25
		경영진의 개인정보보호 중요성 인식	'14
		일반직원들의 정보보호 중요성 인식	'10-'17
		일반직원들의 개인정보보호 중요성 인식	'10-'17
		일반직원의 정보보호 관련 지식수준	'14
		정보보호 위협요인별 우려 정도	'13-'25
		사이버 환경상의 안정성 정도	'07-'10
		우려하는 개인정보 유출요인	'12-'20
		정보보호 업무 관련 애로사항	'15-'25
		정보보호 규제 동의 수준	'15-'16
		보안 규정 변경 시 수용 노력 정도	'21
		정보보호 관련 규정 적용의 엄격함 정도	'22-'25
	B. 정보보호 정책 및 조직	정보보호(개인정보보호) 정책 또는 규정집 보유*	'06-'25
		정보보호 정책 포함 위협요소	'14-'21
		정보보호 정책에 포함된 내용	'09-'14
		정보보호 정책 검토 및 수정, 보완 주기	'14
		정책 수립 적용기준 가이드라인	'10
		직원 개인용 PC 정보보호 지침 제정·운영 현황	'07-'12
		정보보호 업무 수행 여부	'25
		정보보호(개인정보보호) 조직 운영*	'06-'13, '15-'25
		정보보호 조직 운영 시 위탁/외주 병행 여부	'25
		정보보호 관련 인력 현황	'24-'25
		정보보호 관련 책임자 임명 및 전담	'06-'25
		정보보호 관련 책임자 겸직 업무	'25
		정보관리책임자(CIO)와 겸직 여부	'16
		정보보호 조직 및 담당 인력 현황과 향후 계획	'14
		IT인력 중 정보보호 담당 인력 비중	'14, '16-'21
		IT인력 대비 정보보호 전담인력 투입 비율	'10
		정보보호 담당 인력 신규 채용계획	'17-'21

* 개인정보보호는 2022년~2024년에는 제외

분야	항목	세부 항목	조사 시기
Ⅰ. 정보보호 기반 및 환경	C. 정보보호 교육	중소기업 대상 정보보호 무료 교육 인지도	'25
		정보보호 교육의 필요성	'07-'09
		정보보호(개인정보보호) 교육 실시*	'06-'25
		교육 대상별 교육 실시 현황	'06-'25
		정보보호(개인정보보호) 교육 방법*	'21-'25
		정보보호 교육 프로그램별 교육 횟수, 교육시간	'07-'14
		정보보호 교육프로그램별 교육 시간, 교육평가 여부	'16
		정보보호 교육에 대한 직원들의 이해 정도	'10
		필요한 정보보호 교육 내용	'15
		실시된 정보보호 교육의 포함 내용	'16
		정보보호 교육 자료 출처	'22-'25
		정보보호 교육 효과	'22-'25
		정보보호 교육 만족도	'22-'25
	D. 정보보호 예산	정보보호 예산 사용 경험	'22-'25
		정보보호 예산 미사용 이유	'22-'25
		IT예산 중 정보보호 관련 예산 비중	'06-'21
		정보보호 예산 총액	'22-'25
		정보보호 예산 총액 중 분야별 비율	'14
		정보보호 관련 예산 총액 변화	'11-'25
		정보보호 관련 예산 총액 전년 대비 변화 이유	'19-'25
		향후 정보보호 예산 총액 변화	'22-'25
		정보보호 예산 활용 유형	'13-'25
		정보보호 지출 시기	'15
		정보보호 지출금액 증감 여부	'14-'15
		상반기 지출 정보보호 지출 변동	'15
		정보보호 관련 예산 지출 경향	'15-'16
		정보보호 투자 목적	'15-'16
		정보보호 예산 활용 결정 계기	'22-'25
		정보보호 지출금액 증감 정도	'14
		정보보호 관련 예산 편성하지 않은 이유	'06-'16
		정보보호 관련 지출 정도	'07-'13
		정보보호 예산 소비 적절성	'22-'25
		정보보호 예산 소비 부적절 이유	'22-'25
		정보보호 관련 투자 증감	'10-'13

* 개인정보보호는 2022년~2024년에는 제외

분야	항목	세부 항목	조사 시기
Ⅰ. 정보보호 기반 및 환경	D. 정보보호 예산	정보보호 관련 지출이 없는 이유	'07-'13
		예산 항목별 정보보호 지출 비율	'09
		국내·외 정보보호 제품 및 서비스 선호도	'22-'25
		국내·외 정보보호 제품 및 서비스 선호 이유	'23-'25
Ⅱ. 침해사고 예방	A. 정보보호 제품 및 서비스	침해사고로부터 보호해야 할 자산	'12-'13
		침해사고 예방을 위한 제품 및 솔루션 사용 여부	'22
		정보보호 제품 및 서비스 이용	'06-'25
		정보보호 제품 유형(설치형/클라우드형)	'25
		이용하는 정보보호 제품 및 서비스의 정보보호 인증 인지	'22-'25
		CCTV/IP카메라 보유 대수	'16-'20
		CCTV 보유 대수 및 관리 현황	'22-'25
		IP카메라 최초 비밀번호 변경 여부	'19
		정보보호 제품 국산/외중 비중	'15-'19
		외산 정보보호 제품 및 서비스 지출 여부	'19-'20
		외산 정보보호 제품 구매 이유	'16-'20
		보안컨설팅 서비스 이용 기간	'20
		보안컨설팅 서비스 이용 분야	'20
		보안컨설팅 서비스 관련 예산 비중	'20
		보안 취약성 점검 도구 사용 현황	'09
		정보보호 업무 아웃소싱 현황	'06-'16
		정보보호 업무 아웃소싱 서비스 내용	'06-'16
		신규 정보통신망 및 서비스 구축 시 정보보호 고려 여부	'13
		신규 정보통신망 및 서비스 구축 시 정보보호 비고려 이유	'16
	B. 정보보호 관리	정보자산 관리를 위한 수행활동	'14
		시스템 및 네트워크 보안 점검(취약점 점검) 실시	'09-'25
		시스템 및 네트워크 보안 점검(취약점 점검) 항목	'14-'21
		보안패치 적용 방법	'07-'21
		사내 정보시스템 사용자 인증 방법	'07-'13
		사내 정보시스템 이용 시 차등 권한 부여 현황	'11-'14
		직무변경 또는 퇴사 시 정보시스템 접근금지 변경 여부	'14
		보안패치 업데이트 미실시 이유	'17-'21
		구형 운영체제 사용 이유	'17
		시스템 로그 및 방화벽 로그 기록 관리 여부	'22-'25

분야	항목	세부 항목	조사 시기
Ⅱ. 침해사고 예방	B. 정보보호 관리	시스템 로그 및 방화벽 로그 기록 저장 주기	'22-'25
		공식 문서로 작성된 백업 관련 정책 또는 규정집 보유 여부	'25
		데이터 종류별 백업 실시 여부	'22-'25
		데이터 백업 방식	'22-'25
		데이터 백업 주기	'22-'25
		시스템 로그 및 중요 데이터 백업 실시 여부	'12-'21
		시스템 로그 및 중요 데이터 백업 방식	'17-'21
		시스템 로그 및 중요 데이터 백업 실시 주기	'17-'21
		침해사고 사전 예방 능력	'22-'25
Ⅲ. 침해사고 경험 및 대응	A. 침해사고 경험	침해사고 발생 가능성	'22-'25
		침해사고 피해 직·간접적 경험	'22-'25
		침해사고 의심 경험	'22-'25
		침해사고 피해 경험	'06-'25
		침해사고 경험 유형	'22-'25
		침해사고 피해 사실 인지 경로	'22-'25
		침해사고 피해 유형별 피해 빈도	'07-'14
		침해사고 피해 심각성 정도	'22-'25
		침해사고 피해 경험 유형 및 심각성 정도	'14-'21
		침해사고 피해 발생 경로	'13-'14
		침해사고 피해 사실 인지 시점	'11-'14
		침해사고 원인 파악 시점	'14
		침해사고 문제 해결 및 서비스 복원 시점	'14
		침해사고 단계별 소요 시간	'22-'25
		침해사고 시 관련 기관 또는 수사기관에 신고	'06-'25
		정보보안 침해사고 발생 시 신고정도	'11
		정보보안 침해사고 발생 시 미신고 이유	'06-'11, '14-'16, '22-'25
		인터넷 침해사고 피해 경로	'07-'10
		정보보호 피해 건수 증감률	'10-'13
		정보보호 피해 규모 증감률	'10-'13
		개인정보 유출 및 명의도용으로 인한 피해 경험 여부	'11-'12
		개인정보 유출 및 명의도용 사고 시 신고 여부 및 기관	'11
		개인정보 유출 및 명의도용 정보보안 침해사고 발생 시 신고 정도	'11
		정보보호 피해 양상 유형	'10

분야	항목	세부 항목	조사 시기
Ⅲ. 침해사고 경험 및 대응	B. 침해사고 대응	침해사고 대응활동 수행	'06-'25
		침해사고 사후 대응 능력 수준	'22-'25
		정보보호 침해사고 경험 후 관심 변화	'22-'25
		현재 수행중인 정보보호 활동 평가 수단	'07-'13
		사이버 보안사고 대비 보험 가입 여부	'07-'11
		사이버 보안사고 발생 시 신고 정도	'07-'10
		사이버 보안사고 발생 시 미신고 이유	'07-'10
		재해/침해사고 대비 비상복구계획 수립 여부	'07-'10
		이메일 중 스팸이 차지하는 비율	'07
		메일 서버 운영 여부	'07-'11
		안전한 이메일 송수신을 위한 방안	'07-'11
		이용 중인 이메일 스팸 통제 수단	'07-'11
		이메일 스팸 차단을 위한 계획	'07-'09
		게시판 서비스 운영 여부	'10-'11
		게시판 스팸 현황	'10
		게시판 스팸 대응 현황	'10-'11
		운영 중인 웹사이트 내에 사이버 일탈행위 방지를 위한 조치	'11
		침해사고 대응 대외협력채널	'17-'21
Ⅳ. 개인정보 보호 *	A. 개인정보 수집	개인정보 수집 및 이용	'12-'21
		개인정보 온라인 수집 방법	'14-'21
		이용자(고객) 개인정보 수집 방법	'12
		이용자(고객) 주민등록번호 수집·이용 여부	'12-'13
		주민등록번호 수집·이용 목적	'12-'13
		주민등록번호 미수집 시 서비스 제공에의 영향	'12
		주민등록번호 미수집 이유	'12
		개인정보 수집 유형	'12, '14-'21
		개인정보 수집 및 이용 목적	'12-'21
		보유하고 있는 이용자(고객) 개인정보 규모	'12-'14
	B. 개인정보 침해사고 예방	개인정보 침해사고 예방을 위한 관리적 조치(사후처리)	'07-'21
		개인정보 침해사고 예방을 위한 기술적 조치	'10-'21
		개인정보 암호화	'09-'21
		회원가입, 홈페이지 이용 시 본인 확인 수단	'14

* 개인정보보호는 2022년~2024년에는 제외

분야	항목	세부 항목	조사 시기
Ⅳ. 개인정보 보호 *	B. 개인정보 침해사고 예방	회원가입 시 본인확인 여부	'13
		이용 중인 주민번호 대체 수단	'12-'13
		개인정보보호 내부관리계획 내용	'12
		개인정보보호 예산 배정 여부	'12
		개인정보보호법 인지 여부	'11
		개인정보보호를 위한 조치 여부	'11
		개인정보 취급방침별 공개 여부	'07-'11
		개인정보 수집 이용/제공 시 이용자 동의 확보 여부	'07-'11
		수집한 개인정보의 제3자 제공/취급 위탁 여부	'10-'11
		제3자 제공/취급 위탁의 제공 형태	'09-'11
		제3자 제공 시 공지 및 동의 확보 여부	'07-'11
		제3자 취급 위탁 시 공지 및 동의 확보 여부	'07-'11
		개인정보 파기 절차 및 방법에 대한 지침 확보	'08-'11
		개인정보 침해사고 사후처리방침 문서화 여부	'07-'11
		개인정보 전담조직 내부관리계획 수립 여부	'09
		내부관리계획 항목별 포함 여부	'09
		개인정보보호책임자의 직급 및 직책	'09
		임직원 대상 보안서약서 서명 여부	'09
		개인정보보호책임자/취급자 대상 교육계획 수립 여부	'09
		개인정보보호 교육 계획 내 포함 내용	'09
		개인정보를 이동식 저장매체에 복사 시 기록 저장 여부	'09-'11
		개인정보 암호화 저장 여부	'09-'12
		비밀번호 작성규칙 수립 여부	'09
		개인정보취급자 비밀번호 작성규칙 수립 이행 여부	'09
		개인정보취급자 비밀번호 작성규칙 내용	'09
		개인정보취급자 개인용 컴퓨터 P2P 사용 규제 여부	'09
		개인정보취급자의 개인용 컴퓨터 공유 설정 여부	'09
		공유 설정이 접근제어 수행 여부	'09
		본인인증정보 저장이 일방향 암호화 저장 여부	'09
		이용자 개인정보 개인정보취급자 PC 저장이 암호화 여부	'09
		개인정보 출력 시 용도에 따른 출력 항목 최소화 여부	'09
		개인정보 포함 정보 출력/복사지 CPO 사전 승인 여부	'08-'09

* 개인정보보호는 2022년~2024년에는 제외

분야	항목	세부 항목	조사 시기
Ⅳ. 개인정보 보호 *	B. 개인정보 침해사고 예방	출력/복사지 정보통신망법 위배 확인 여부	'08-'09
		개인정보 불법 유출 시 법적 책임 주지 여부	'09
		개인정보 관련 업무 수행 시 개인정보보호 조치 수행 여부	'09
		개인정보 수집에 대한 인식	'12-'13
		개인정보보호 항목별 중요도	'12-'14
		개인정보 유출사고 원천 우려 수주	'12-'14
	C. 개인정보 침해사고	개인정보 침해사고 경험	'08-'10, '12-'21
		개인정보 침해사고 내용	'12-'13
		유출된 개인정보 유형	'13-'14
		개인정보 침해사고 횟수	'12-'14
		개인정보 침해사고 유형	'12-'14
		개인정보 침해사고의 개인정보 규모	'12-'14
		개인정보 침해사고 인지 시점	'12-'14
		개인정보 침해사고 원인 파악 평균 소요 시간	'14
		개인정보 침해사고 문제해결 및 서비스 복원 평균 소요 시간	'14
		개인정보 침해사고 인지 경로	'13-'14
		개인정보 침해사고 외부 신고 경로	'13
		개인정보 침해사고 시 관계기관에 문의 또는 신고	'12-'21
		개인정보 침해사고 외부 신고 여부	'13
		개인정보 침해사고 발생 시 고지 방법	'12-'13
		개인정보 침해사고 발생 시 신고하지 않은 이유	'12-'13
		개인정보 침해사고 시 보상 여부	'12
		개인정보 침해사고 시 통지 또는 고지	'17-'21
		보안서버 도입 여부	'07-'12
		보안서버 구축 방식	'07-'12
		보안서버 도입 및 확대 계획 여부	'07-'11
		웹사이트 회원 가입 시 본인확인을 위한 방법	'10-'12
		주민번호 대체수단	'11-'12
		인터넷 상 본인확인 수단(i-PIN)서비스 인지 여부	'07-'12
		향후 i-PIN 서비스 이용 의향	'07-'11
		향후 i-PIN 서비스를 이용할 의향이 없는 이유	'11
		개인정보 처리시스템 개인정보 보호조치 내용	'08-'09

* 개인정보보호는 2022년~2024년에는 제외

분야	항목	세부 항목	조사 시기
Ⅳ. 개인정보 보호 *	C. 개인정보 침해사고	개인정보 관리책임자/취급자 변경이 접근권한 변경/말소 여부	'09
		접근권한 부여/변경/말소 내역 기록/보관 여부	'09
		개인정보처리시스템 외부망 접속 가능 여부	'09
		외부망 접속 시 공인인증서/VPN 인증수단 적용 여부	'09
		접속기록 저장/관리 여부	'09
		접속기록 관리 방법	'09
		웹사이트를 통한 주민번호 수집 여부	'07-'10
		정보통신서비스 부문 매출액	'12
		정보통신망법 개정에 따른 신규제도 인지 여부	'12-'13
		신규제도 이행 시 필요한 사항	'12-'13
		신규제도 도입 관련 준비 사항	'12-'13
		사업자 대상 개인정보보호 교육 참석 여부	'12-'13
		개인정보보호 관련 무료 교육 시 참석 의향	'12-'13
		희망하는 개인정보보호 교육 유형	'12-'13
		개인정보보호 관련 교육 만족도	'12-'13
		개인정보 취급자 대상 워크숍 인지 여부	'12-'13
		개인정보 취급자 대상 워크숍 인지 경로	'12-'13
		개인정보 취급자 대상 워크숍 참석 여부	'12-'13
		개인정보 취급자 대상 워크숍 성과 평가	'12-'13
		개인정보보호 포털사이트 인지 여부	'12-'13
		개인정보보호 포털사이트 이용 빈도	'12-'13
		개인정보보호 포털사이트 이용 내용	'12-'13
		개인정보보호 포털사이트 성과 평가	'12-'13
		효율적인 개인정보보호 홍보 매체	'13
Ⅴ. 주요 서비스별 정보보호	A. 무선랜	무선랜 구축 및 운영	'10-'13, '15-'21
		무선랜 관련 보안 우려사항	'12, '15-'21
		사내 무선랜 보안정책 수립 현황	'10-'11, '13, '15-'16
		사내 무선랜 보안 정책 내용	'10-'13
		무선랜 보안을 위한 조치	'10-'11, '13, '15-'21
		외부 사용 무선인터넷 서비스 사용 가능 여부	'11-'13
		외부 상용 무선인터넷 서비스 관리 정책 수립 현황	'11-'13

* 개인정보보호는 2022년~2024년에는 제외

분야	항목	세부 항목	조사 시기
Ⅴ. 주요 서비스별 정보보호	B. 모바일	모바일 오피스 구축·운영 현황	'10-'13
		모바일 오피스 도입 보안 대책 수립 현황	'10-'14
		모바일 오피스 보안 수칙 포함 내용	'13-'14
		모바일 오피스 도입 시 우려사항	'10-'12
		모바일 오피스 도입 계획이 없는 이유	'12-'13
		스마트기기의 정보보호를 위해 이용하는 서비스 및 제품	'14
		개인소유 또는 회사소유 모바일 기기 업무 활용	'14-'21
		개인소유 모바일 기기 활용 시 보안 우려사항	'14-'21
		모바일 기기 활용 시의 보안위협에 대한 대응 방안	'14-'21
	C. 클라우드	클라우드 서비스 이용 및 향후 도입(유지) 계획	'10-'13, '15-'21
		클라우드 컴퓨팅 서비스 보안 대책 확보 현황	'10-'14
		클라우드 컴퓨팅 서비스 보안 대책 및 가이드라인 내용	'12-'14
		클라우드 컴퓨팅 서비스 비이용 이유	'10-'13
		클라우드 서비스 선택 시 고려 사항	'15-'16
		클라우드 서비스 이용(계획) 분야	'17-'21
		클라우드 서비스 보안을 위한 조치	'16-'21
		클라우드 서비스 보안 우려사항	'10-'12, '14-'21
		빅데이터 도입 및 활용 관련 우려사항	'14
	D. 사물인터넷(IoT)	사물인터넷(IoT) 제품 및 서비스 이용 및 향후 도입(유지) 계획	'15-'21
		사물인터넷(IoT) 이용 활성화를 위해 개선되어야 할 사항	'15-'16
		사물인터넷(IoT) 이용(계획) 분야	'17-'21
		사물인터넷(IoT) 보안을 위한 조치	'19-'21
		사물인터넷(IoT) 관련 보안 위협에 대한 우려	'15-'21
	E. 정보보호(사이버) 보험*	사이버(정보보호, 개인정보보호) 보험 인지	'17-'25
		사이버(정보보호, 개인정보보호) 보험 이용 및 향후 가입(유지) 계획	'17-'25
		사이버(정보보호, 개인정보보호) 보험 희망 보장 항목	'17-'25
	F. 원격근무**	코로나19로 인한 재택근무 시행 여부	'21-'22
		원격근무 시행 여부	'23-'25
		원격근무 시 제공한 보안 솔루션	'21-'25
		원격근무 시 정보보호 위험성 인지	'22-'25
		원격근무 시 침해사고 발생 또는 의심 경험	'22-'25
		코로나19 위기 해소 이후 재택근무 활용 계획 여부	'21

* 개인정보보호는 2022년~2024년에는 제외
** 재택근무에서 원격근무로 2024년 용어 변경

Ⅱ 개인 부문

부록 표 1-2 개인 부문 조사표 주요 변경내역

분야	항목	세부 항목	조사 시기
Ⅰ. 정보보호 인식	A. 정보보호 인식	정보보호 중요성 인식	'06-'21
		개인정보보호 중요성 인식	'08-'21
		위협사안에 대한 구체적 인지	'14-'21
		위협사안에 대한 피해의 심각성	'14-'20
		정보보호 관련 관심정보 유형	'12-'16
		정보보호 관련 정보수집 및 학습활동	'06-'20
		향후 정보보호 관련 정보수집 및 학습방법	'19-'21
		정보보호 관련 정보수집 및 학습 애로사항	'12-'16
		정보보호 이슈 관심도	'22-'25
		정보 침해사고 우려 정도	'22-'25
		정보 침해사고 소식에 대한 관련성 인식	'22-'25
		안전 체감도	'22-'25
		정보 침해사고 발생 시 피해 복구 가능성	'22-'25
		정보 침해사고 발생 원인	'22-'25
		정보 침해사고 방지 주체	'22-'25
		정보보호 관련 기관·업체 신뢰도	'22-'25
	B. 정보보호 교육	정보보호 관련 정보 수집 경로	'25
		정보보호 교육	'22-'25
		정보보호 교육 방식	'22-'25
		정보보호 교육 주제	'22-'25
		정보보호 교육 학습 효과	'22-'25
		정보보호 교육 학습 난이도	'22-'25
		정보보호 관련 학습의 어려움	'22-'25
		정보보호 관련 홍보물 경험 여부	'24-'25
		정보보호 관련 홍보물 경험 경로	'24-'25
	C. 정보보호 예산	정보보호 금전 소비 경험	'22-'25
		정보보호 금전 소비 유형	'22-'25
		정보보호 금전 소비 규모	'22-'25
		정보보호 금전 소비 계기	'22-'25

분야	항목	세부 항목	조사 시기
Ⅰ. 정보보호 인식	C. 정보보호 예산	정보보호 금전 소비 적절성	'22-'25
		정보보호 금전 소비 비용 증감 여부	'22-'25
		향후 정보보호 비용 지출 의향	'22-'25
Ⅱ. 침해사고 예방	A. 정보보호 관련 제품	정보보호 제품	'06-'21
		정보보호 제품 미이용 이유	'12-'18
		정보보호 소프트웨어 이용	'14-'19
		정보보호 제품 이용 시 활용 기능	'12-'15
		악성코드 검사 실시 주기	'14-'21
		파일 다운로드 시 바이러스 검사 방법	'11-'15
		백신 프로그램 업데이트1)	'06-'21
		백신 프로그램 업데이트 실시 주기	'14-'21
		운영체제 보안 업데이트2)	'06-'21
		운영체제 보안 업데이트 미실시 이유	'12-'18
		구형 운영체제 사용 이유	'17
		중요 데이터 백업	'15-'21
		중요 데이터 백업 방식	'17-'21
		중요 데이터 백업 실시 주기	'14-'21
		운영체제 보안 업데이트 미실시 이유	'12-'18
		PC 비밀번호 설정	'06-'21
		비밀번호 관리 조치	'12-'21
		비밀번호 변경 주기	'06-'21
	B. 모바일 및 무선랜 보안	모바일 기기 이용	'14-'17
		무선랜 이용 피해 예방 조치	'11-'21
		모바일 기기 데이터 백업	'17
		모바일 기기 데이터 백업 방식	'17
		모바일 기기 데이터 백업 실시 주기	'17
		모바일 기기 피해 예방 조치	'10-'21
	C. SNS 보안	SNS 이용	'11-'21
		SNS 피해 유형별 인지	'10-'15
		SNS 사기 피해, 협박 경험	'21
		SNS 피해 예방 조치	'11-'21
Ⅲ. 침해사고 대응	A. 정보 침해사고 경험	침해사고 공식 신고·상담 창구 인지	'25
		정보 침해사고 의심 경험	'22-'25
		정보 침해사고 경험	'22-'25
		정보 침해사고 피해 인지 소요 시간	'22-'25
		정보 침해사고 인지 경로	'22-'25

분야	항목	세부 항목	조사 시기
Ⅲ. 침해사고 대응	A. 정보 침해사고 경험	정보 침해사고 피해 심각성	'22-'25
		침해사고 금전적 손실	'25
		침해사고 복구 비용 지출	'25
		정보 침해사고 피해 경험 유형	'11-'25
		피싱/파밍/스미싱 등 전자금융사기 피해 경로	'10-'21
	B. 정보 침해사고 대응조치	정보 침해사고 대응활동 수행	'12-'21
		정보 침해사고 신고 또는 상담 문의 기관·업체*	'07-'25
		정보 침해사고 신고 또는 상담하지 않은 이유**	'07-'25
		침해사고 발생 초동대처 주체	'15
		정보보호 규제 방식에 대한 동의 정도	'15
	C. 정보 침해사고 경험과 위협 인식	정보 침해사고 관심도 변화	'22-'25
		최신 IT 기술 이용 시 정보 침해 위협으로부터의 안전도	'22-'25
		최신 IT 기술 정보 침해사고 발생 시 파급효과	'22-'25
Ⅳ. 개인정보 보호	A. 개인정보 보호 조치	인터넷 상 개인정보 제공 목적	'07-'21
		인터넷 상 개인정보 제공 동의 시 선택사항 동의 여부	'19-'21
		인터넷 상 개인정보 제공 동의 시 이용약관 확인 여부	'20-'21
		개인정보 침해사고 예방 조치	'08-'21
		인터넷 서비스 회원가입 시 주민번호 이외 수단 인지·이용·선호도	'11-'15
		개인정보 수집 범위에 대한 인식	'12-'16
		인터넷 서비스 제공자의 개인정보보호 조치 이행 수준	'15
		인터넷 서비스 제공자의 개인정보보호 조치 이행 미비 이유	'15
		정보통신망 이용촉진 및 정보보호 등에 관한 법률 제도 인지 정도	'15
		개인정보 관련 권리 인지도	'12-'15
	B. 개인정보 침해사고 및 대응	개인정보 침해사고 경험	'06-'21
		개인정보 침해사고 경험 유형	'06-'21
		개인정보 침해사고 대응조치	'12-'21
Ⅴ. 주요 서비스별 정보보호	A. 클라우드	클라우드 서비스 이용	'15-'21
		클라우드 서비스 침해사고 예방 조치	'15-'21
	B. IP 카메라	IP카메라 제품 이용	'19-'21
		IP카메라 제품 이용 목적	'19-'21
		IP카메라 보안조치 유형	'19-'21
		IP카메라 보급 확산 시 보안 우려사항	'19-'20
		IP카메라에 추가되어야 하는 보안 기능	'19
	C. 빅데이터	빅데이터 활용 서비스 경험	'17-'18
		빅데이터 활용 서비스 확산 시 보안 우려사항	'15-'19

* 2022년 ~ 2025년에는 신고 여부만 질의
* 2022년 ~ 2025년에는 미신고 이유만 질의

분야	항목	세부 항목	조사 시기
Ⅴ. 주요 서비스별 정보보호	D. 인공지능(AI)	인공지능(AI) 활용 서비스 이용	'17-'19
		이용한 인공지능(AI) 활용 서비스 유형	'17-'19
		인공지능(AI) 활용 서비스 대중화 시 보안 우려사항	'17-'19
	E. 사물인터넷(IoT)	사물인터넷(IoT) 제품 및 서비스 이용	'17-'18
		이용하는 사물인터넷(IoT) 제품 유형	'17-'18
		사물인터넷(IoT) 이용 실시 보안조치 유형	'18
		사물인터넷(IoT) 대중화 시 보안 우려사항	'05-'18
		사물인터넷(IoT) 추가 보완을 원하는 보안 기능	'18
	F. 핀테크	간편결제 서비스 이용	'15-'18
		이용한 간편결제 서비스 본인인증수단	'17-'18
		일반결제 대비 간편결제 서비스 보안성 인식	'15-'18
	G. 일상생활	출입자 명부 작성 경험	'21
		출입자 명부 작성 시 개인정보 유출 우려 정도	'21
		온라인/모바일 제품 구매 경험	'21
		택배 송장 처리 방법	'21
Ⅵ. 일상생활 속의 정보보호	A. 일상생활 속의 정보보호	무료 인터넷(Wi-fi) 연결 빈도	'22-'25
		불특정 다수 이용 전자장비 이용 시 예방 활동	'22-'25
		비밀번호 변경 필요 안내 시 비밀번호 즉시 변경 여부	'22-'25
		디지털 데이터 백업 경험	'22-'25
		보안 점검 수행 경험	'22-'25
		정보보호를 위한 보안 예방 조치	'22-'25
		원격근무(온라인 연결)* 수행 경험	'22-'25
		비대면 환경의 정보보호 활동	'22-'25
		일상생활 공간 중 영상 감시 장비 사용	'22-'25
	B. 향후 지출 계획	향후 정보보호 지출 계획 분야	'19-'21

* 재택근무에서 원격근무로 2024년 용어 변경

부 록 2

표본오차

Ⅰ 기업 부문

1 정보보호 정책 보유율

부록 표 2-1-1 기업 부문 표본오차_정보보호 정책 보유율

구분		정보보호 정책 보유율	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		**52.6**	**1.30**	**1.26**	**51.3**	**53.9**
업종	1. 농림수산업(광업포함)	36.4	9.13	12.80	27.2	45.5
	2. 제조업	56.0	3.67	3.35	52.3	59.7
	3. 전기, 가스, 증기 및 공기조절 공급업/ 수도, 하수·폐기물 처리, 원료 재생업	35.0	7.15	10.43	27.8	42.1
	4. 건설업	52.6	4.45	4.32	48.1	57.1
	5. 도매 및 소매업	41.5	4.62	5.68	36.9	46.1
	6. 운수 및 창고업	45.7	5.21	5.82	40.5	50.9
	7. 숙박 및 음식점업	24.1	6.02	12.75	18.1	30.1
	8. 정보통신업	70.5	4.47	3.23	66.1	75.0
	9. 금융 및 보험업	92.7	2.63	1.45	90.1	95.4
	10. 부동산업	45.8	5.64	6.29	40.1	51.4
	11. 전문, 과학 및 기술 서비스업	64.5	3.71	2.94	60.7	68.2
	12. 사업시설 관리, 사업지원 및 서비스업	42.2	5.23	6.32	37.0	47.5
	13. 교육 서비스업	49.2	5.34	5.53	43.9	54.6
	14. 보건업 및 사회복지 서비스업	53.4	4.05	3.87	49.3	57.4
	15. 예술, 스포츠 및 여가관련 서비스업	46.5	7.50	8.22	39.0	54.0
	16. 협회, 단체, 수리 및 기타 개인 서비스업(협회 및 단체 제외)	26.6	7.07	13.53	19.6	33.7
규모	10~49명	46.1	2.31	2.55	43.8	48.4
	50~249명	83.2	1.77	1.08	81.4	84.9
	250명 이상	99.3	0.27	0.14	99.0	99.6

2 정보관리책임자(CIO) 임명 여부

부록 표 2-1-2 기업 부문 표본오차_정보관리책임자(CIO) 임명 여부

구분		정보관리책임자(CIO) 임명	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		**58.6**	**1.28**	**1.12**	**57.4**	**59.9**
업종	1. 농림수산업(광업포함)	59.3	9.32	8.01	50.0	68.6
	2. 제조업	57.1	3.66	3.27	53.5	60.8
	3. 전기, 가스, 증기 및 공기조절 공급업/수도, 하수·폐기물 처리, 원료 재생업	54.7	7.47	6.97	47.2	62.1
	4. 건설업	62.3	4.32	3.54	58.0	66.6
	5. 도매 및 소매업	67.2	4.40	3.34	62.8	71.6
	6. 운수 및 창고업	60.9	5.10	4.27	55.8	66.0
	7. 숙박 및 음식점업	59.8	6.90	5.89	52.9	66.7
	8. 정보통신업	57.2	4.85	4.33	52.3	62.0
	9. 금융 및 보험업	53.4	5.06	4.84	48.3	58.4
	10. 부동산업	47.2	5.66	6.11	41.5	52.8
	11. 전문, 과학 및 기술 서비스업	46.6	3.87	4.23	42.8	50.5
	12. 사업시설 관리, 사업지원 및 서비스업	51.7	5.29	5.22	46.4	57.0
	13. 교육 서비스업	56.6	5.29	4.77	51.3	61.9
	14. 보건업 및 사회복지 서비스업	60.3	3.97	3.36	56.3	64.3
	15. 예술, 스포츠 및 여가관련 서비스업	55.7	7.46	6.83	48.3	63.2
	16. 협회, 단체, 수리 및 기타 개인 서비스업(협회 및 단체 제외)	60.5	7.82	6.60	52.7	68.3
규모	10~49명	57.1	2.29	2.05	54.8	59.4
	50~249명	62.2	2.29	1.88	59.9	64.5
	250명 이상	92.1	0.90	0.50	91.2	93.0

3 정보보호최고책임자(CISO) 임명 여부

부록 표 2-1-3 기업 부문 표본오차_정보보호최고책임자(CISO) 임명 여부

구분		정보보호 최고책임자 (CISO) 임명	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		21.0	1.06	2.58	20.0	22.1
업종	1. 농림수산업(광업포함)	14.0	6.58	24.02	7.4	20.5
	2. 제조업	16.5	2.74	8.50	13.7	19.2
	3. 전기, 가스, 증기 및 공기조절 공급업/ 수도, 하수·폐기물 처리, 원료 재생업	16.9	5.62	16.97	11.3	22.5
	4. 건설업	20.0	3.57	9.10	16.4	23.6
	5. 도매 및 소매업	16.4	3.47	10.81	12.9	19.8
	6. 운수 및 창고업	16.8	3.91	11.86	12.9	20.7
	7. 숙박 및 음식점업	11.6	4.50	19.87	7.1	16.1
	8. 정보통신업	34.1	4.65	6.96	29.4	38.7
	9. 금융 및 보험업	44.4	5.04	5.79	39.4	49.4
	10. 부동산업	17.9	4.35	12.37	13.6	22.3
	11. 전문, 과학 및 기술 서비스업	22.5	3.24	7.34	19.3	25.7
	12. 사업시설 관리, 사업지원 및 서비스업	20.2	4.26	10.73	16.0	24.5
	13. 교육 서비스업	19.6	4.24	11.03	15.4	23.8
	14. 보건업 및 사회복지 서비스업	27.6	3.63	6.70	24.0	31.3
	15. 예술, 스포츠 및 여가관련 서비스업	13.5	5.14	19.40	8.4	18.6
	16. 협회, 단체, 수리 및 기타 개인 서비스업(협회 및 단체 제외)	17.9	6.13	17.46	11.8	24.1
규모	10~49명	20.6	1.87	4.64	18.7	22.4
	50~249명	16.8	1.76	5.36	15.0	18.6
	250명 이상	61.1	1.62	1.35	59.5	62.8

4 정보보호 제품 및 서비스 이용

부록 표 2-1-4 기업 부문 표본오차_정보보호 제품 및 서비스 이용

구분		정보보호 제품 및 서비스 이용	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		98.7	0.29	0.15	98.4	99.0
업종	1. 농림수산업(광업포함)	100.0	0.00	0.00	100.0	100.0
	2. 제조업	100.0	0.00	0.00	100.0	100.0
	3. 전기, 가스, 증기 및 공기조절 공급업/ 수도, 하수·폐기물 처리, 원료 재생업	100.0	0.00	0.00	100.0	100.0
	4. 건설업	91.8	2.45	1.36	89.3	94.2
	5. 도매 및 소매업	99.4	0.71	0.36	98.7	100.1
	6. 운수 및 창고업	99.8	0.48	0.24	99.3	100.3
	7. 숙박 및 음식점업	100.0	0.00	0.00	100.0	100.0
	8. 정보통신업	100.0	0.00	0.00	100.0	100.0
	9. 금융 및 보험업	100.0	0.00	0.00	100.0	100.0
	10. 부동산업	100.0	0.00	0.00	100.0	100.0
	11. 전문, 과학 및 기술 서비스업	99.9	0.26	0.13	99.6	100.1
	12. 사업시설 관리, 사업지원 및 서비스업	93.9	2.53	1.38	91.4	96.4
	13. 교육 서비스업	100.0	0.00	0.00	100.0	100.0
	14. 보건업 및 사회복지 서비스업	100.0	0.00	0.00	100.0	100.0
	15. 예술, 스포츠 및 여가관련 서비스업	100.0	0.00	0.00	100.0	100.0
	16. 협회, 단체, 수리 및 기타 개인 서비스업(협회 및 단체 제외)	100.0	0.00	0.00	100.0	100.0
규모	10~49명	98.5	0.55	0.29	98.0	99.1
	50~249명	99.7	0.27	0.14	99.4	99.9
	250명 이상	100.0	0.00	0.00	100.0	100.0

Ⅱ 개인 부문

1 정보보호 교육 수강 경험

부록 표 2-2-1 개인 부문 표본오차_정보보호 교육 수강 경험

구분		정보보호 교육 수강 경험	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		**14.9**	**1.28**	**4.36**	**13.7**	**16.2**
성별	남성	17.6	1.90	5.51	15.7	19.5
	여성	12.1	1.68	7.04	10.5	13.8
연령별	12~19세	36.0	5.66	8.03	30.3	41.6
	20대	20.9	3.71	9.04	17.2	24.6
	30대	19.2	3.49	9.27	15.7	22.7
	40대	13.7	2.82	10.49	10.9	16.5
	50대	8.6	2.17	12.89	6.4	10.7
	60대	4.2	1.66	20.29	2.5	5.8

2 정보보호 금전 소비 경험

부록 표 2-2-2 개인 부문 표본오차_정보보호 금전 소비 경험

구분		정보보호 금전 소비 경험	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		**11.0**	**1.12**	**5.20**	**9.9**	**12.1**
성별	남성	12.5	1.65	6.74	10.9	14.2
	여성	9.4	1.50	8.13	7.9	10.9
연령별	12~19세	7.4	3.09	21.26	4.3	10.5
	20대	15.7	3.31	10.80	12.3	19.0
	30대	14.3	3.10	11.07	11.2	17.4
	40대	16.4	3.03	9.44	13.4	19.4
	50대	7.1	1.98	14.31	5.1	9.1
	60대	4.5	1.72	19.53	2.8	6.2

3 디지털 데이터 백업

부록 표 2-2-3 개인 부문 표본오차_디지털 데이터 백업

구분		디지털 데이터 백업	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		**34.5**	**1.70**	**2.52**	**32.8**	**36.2**
성별	남성	36.5	2.40	3.36	34.1	38.9
	여성	32.4	2.40	3.78	30.0	34.8
연령별	12~19세	41.4	5.81	7.16	35.6	47.2
	20대	44.7	4.53	5.17	40.2	49.3
	30대	44.6	4.40	5.03	40.2	49.0
	40대	37.4	3.97	5.41	33.4	41.4
	50대	24.5	3.33	6.92	21.2	27.9
	60대	21.3	3.40	8.13	17.9	24.7

4 보안 점검 수행

부록 표 2-2-4 개인 부문 표본오차_보안 점검 수행

구분		보안 점검 수행	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		**41.9**	**1.77**	**2.15**	**40.1**	**43.6**
성별	남성	45.7	2.49	2.78	43.2	48.2
	여성	37.9	2.49	3.35	35.4	40.3
연령별	12~19세	37.9	5.72	7.71	32.2	43.6
	20대	49.7	4.56	4.68	45.1	54.3
	30대	49.6	4.43	4.56	45.1	54.0
	40대	50.2	4.10	4.16	46.1	54.3
	50대	35.4	3.70	5.33	31.7	39.1
	60대	28.5	3.75	6.70	24.8	32.3

5 정보 침해사고 경험

부록 표 2-2-5 개인 부문 표본오차_정보 침해사고 경험

구분		정보 침해사고 경험	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		**8.5**	**1.00**	**6.01**	**7.5**	**9.5**
성별	남성	8.0	1.35	8.67	6.6	9.3
	여성	9.0	1.47	8.32	7.5	10.5
연령별	12~19세	5.4	2.67	25.14	2.7	8.1
	20대	11.9	2.95	12.66	8.9	14.9
	30대	11.4	2.81	12.62	8.5	14.2
	40대	9.7	2.43	12.74	7.3	12.2
	50대	5.8	1.81	15.92	4.0	7.6
	60대	6.1	1.98	16.62	4.1	8.1

부 록 3

조사표

2025년 정보보호 실태조사 (기업)

승인번호
제 342005 호

안녕하십니까?

과학기술정보통신부와 한국정보보호산업협회에서는 우리나라 기업체의 정보보호 현황과 침해사고 피해 실태를 파악하여 관련 정책 수립의 기초자료를 마련하고자 전국의 기업체를 대상으로 "2025년 정보보호 실태조사 (기업)"을 실시하고 있습니다.

정부의 효과적인 정보보호 정책 수립에 도움이 될 수 있도록 귀사의 적극적인 협조를 부탁드립니다.

아울러 작성해 주신 자료는 조사와 연구에 관련된 목적에만 사용될 것이며, 비밀은 철저히 보장될 것을 약속드립니다.
설문조사에 응해 주심에 감사드리며, 귀사의 평안과 번창하심을 기원합니다.

2025년 8월

주관기관	전담기관	조사기관	실사 문의	조사 문의
과학기술정보통신부	한국정보보호산업협회	㈜글로벌리서치		

* 본 조사는 통계법 제33조(비밀의 보호)에 따라 통계 목적으로 이용되며, 귀사의 비밀이 절대 보장됨을 약속드리는 바입니다.

지 역	① 서울 ② 부산 ③ 대구 ④ 인천 ⑤ 광주 ⑥ 대전 ⑦ 울산 ⑧ 세종 ⑨ 경기 ⑩ 강원 ⑪ 충북 ⑫ 충남 ⑬ 전북 ⑭ 전남 ⑮ 경북 ⑯ 경남 ⑰ 제주
기업명	표본번호 ( ) ( ) ( ) - ( ) ( ) ( ) ( ) ( ) 업종번호 ( ) ( ) 규모번호
사업형태	귀사는 지사/사업장/영업소를 보유하고 있는 기업체(본사/본점 등)이십니까? ① 예 (지사/사업장/영업소 수 : _____ 개) * 본사/본점을 제외한 수를 응답해주십시오 ② 아니오(단독사업체임)
조직형태	① 개인사업체 ② 회사법인 ③ 회사 이외의 법인 ④ 비법인단체
업 종	① 농림수산업 ② 제조업 ③ 건설업 ④ 도매 및 소매업 ⑤ 운수 및 창고업 ⑥ 숙박 및 음식점업 ⑦ 정보통신업 ⑧ 금융 및 보험업 ⑨ 부동산업 ⑩ 전문, 과학 및 기술서비스업 ⑪ 사업시설관리, 사업지원 및 임대 서비스업 ⑫ 협회, 단체 수리 및 기타 개인서비스업 ⑬ 기타(_____)
규 모 (비정규직 포함)	① 10 ~ 49명 ② 50 ~ 249명 ③ 250 ~ 499명 ④ 500 ~ 999명 ⑤ 1,000명 이상
연간 총매출액 (2024년 기준)	( ) 백만원

응답 시 유의사항

1 첫 페이지부터 순서대로 차례차례 응답하여 주십시오.
질문 앞에 특별한 언급이 없는 한 모든 질문에 답하여 주십시오.

2 응답은 귀사의 **내·외부 정보보호 업무를 총괄하시는 담당자**(전산, IT, 정보보호 등)께서 해주십시오. 정보보호 업무가 별도로 지정되어 있지 않은 경우, 총무담당자나 대표께서 직접 기입하여 주셔도 됩니다.

3 질문지에 응답하실 때 특별한 지시가 없으면 보기 번호 중 한 개만 선택하여 주십시오.

4 특별한 언급이 없는 한 **모든 설문의 응답 기준 시점은 「2024년 12월 31일 기준」**으로 응답해주시기 바랍니다.

5 설문지 내의 주요 용어는 설문지 하단의 설명과 별도의 보기카드에 상세한 내용이 기입되어 있습니다. 보기카드는 면접원이 지참하고 있으니, 궁금하신 경우에는 확인을 요청하여 주십시오.

6 설문의 이해를 돕기 위한 사업체 또는 제품명의 예시는 가나다순으로 작성하였습니다.

7 본 조사의 대상은 "네트워크(인터넷 또는 인트라넷)에 연결된 컴퓨터장비(PC, 서버, 노트북, POS 등)를 1대 이상 보유하고 있는 기업체"입니다.

SQ 응답자 선정 질문

SQ1 귀사는 **네트워크(인터넷 또는 인트라넷)에 연결된 컴퓨터 장비(PC, 서버, 노트북, POS)**를 사용하고 있습니까?

① 예　　② 아니오 ☞ **조사 중단**

SQ2 귀사가 영위하는 사업 분야는 **IT 관련 기술이 얼마나 중요한 편**입니까?

전혀 중요하지 않다	중요하지 않은 편이다	보통이다	중요한 편이다	매우 중요하다
①	②	③	④	⑤

※ 해당 설문은 개인정보보호를 제외한 '정보보호'를 기준으로 설문에 응답해 주시기 바랍니다.
※ 기업의 정보보호 실태를 알아보는 조사로, '기업'의 입장에서 응답해 주시기 바랍니다.

A 정보보호 인식

A1 귀사는 기업의 **정보보호에 대하여 얼마나 중요하게 생각**하십니까?

전혀 중요하지 않다	중요하지 않은 편이다	보통이다	중요한 편이다	매우 중요하다
①	②	③	④	⑤

A1-1 **귀사의 경영진은 정보보호에 대하여 얼마나 중요하게 생각**하십니까?

전혀 중요하지 않다	중요하지 않은 편이다	보통이다	중요한 편이다	매우 중요하다
①	②	③	④	⑤

A2 다음의 위협요인에 대하여 **귀사가 우려하는 정도**는 어느 정도입니까?

문 항	전혀 우려하지 않는다	우려하지 않는	보통이다	우려하는 편이다	매우 우려한다
A2-1. 인터넷을 통한 사내 전산 시스템 침해사고 위협	①	②	③	④	⑤
A2-2. 시스템 및 네트워크 장애로 인한 서비스 마비 위협	①	②	③	④	⑤
A2-3. 시스템 및 네트워크 침입을 통한 해킹의 위협	①	②	③	④	⑤
A2-4. 내부 영업정보 및 데이터 손·망실	①	②	③	④	⑤
A2-5. 고객 개인정보 유출 위협	①	②	③	④	⑤
A2-6. 인적 요인에 의한 정보유출 위협	①	②	③	④	⑤
A2-7. 사내에 정보보호 가이드, 규정 등의 미비로 인한 우려	①	②	③	④	⑤
A2-8. 불법적인 사내 침입 등에 의한 물리적 위협	①	②	③	④	⑤

A3

귀사가 **정보보호 관련 업무에 대해 어려움을 느끼는 것**은 무엇입니까?
우선순위대로 최대 3가지만 선택하여 주십시오.

1순위 _____ **2순위** _____ **3순위** _____

① 정보보호 시스템 및 체계 운용 관리
② 정보보호 교육 프로그램 운영
③ 필요한 정보보호 제품 및 서비스 탐색
④ 정보보호 예산 확보
⑤ 정보보호 전문인력 확보(채용)
⑥ 정보보호 담당 인력 운용 관리
⑦ 경영진의 관심
⑧ 기타 ( )

A4

귀사에서 **정보보호 관련 규정을 제정, 변경 또는 강화하였**을 때, 귀사의 조직 구성원에게 해당 사항에 대하여 얼마나 **엄격하게 적용**하실 것입니까?

전혀 엄격하게 적용하지 않을 것이다	엄격하게 적용하지 않을 것이다	보통이다	엄격하게 적용할 것이다	매우 엄격하게 적용할 것이다
①	②	③	④	⑤

B 정보보호 정책 및 조직

B1

귀사에는 **공식 문서로 작성**된 사내 정보보호 **정책 또는 규정집**이 있습니까?

문 항	정책 또는 규정집 보유 여부	
	예	아니오
B1-1. 정보보호 정책 또는 규정집	①	②
B1-2. 정보보호 정책 또는 규정집에 개인정보보호 관련 규정이 포함되어 있는 경우 체크	□	

B2

귀사에서는 **정보보호 업무를 수행**하고 있습니까?

① 예 ☞ B2-1 문항으로 이동
② 아니오 ☞ B3 문항으로 이동

B2-1

【B2의 '① 예' 응답자만】

귀사에서 **정보보호 업무를 담당하는 조직의 유형**은 무엇입니까?
※ 정보보호 업무 외 다른 업무를 같이 수행하는 경우 '② 겸임조직', 외주/용역을 이용하여 정보보호를 한다면, '③ 위탁/외주'로 응답해 주시기 바랍니다.

① 전담조직 ② 겸임조직 ③ 위탁/외주 ④ 운영 안 함

【B2-1의 '① 전담조직' 또는 '② 겸임조직' 응답자만】

B2-2

귀사가 **정보보호 조직을 운영하는 데에 있어 위탁/외주를 병행**하십니까?

① 예 ② 아니오

B3

귀사에 **정보보호 관련 인력**은 얼마나 있습니까? 인력 수를 기입해 주십시오.
(겸직일 경우, 주로 담당하시는 업무 위주로 기입)
※ **내부인력**은 귀사에 소속되어 있는 인력, **외부인력**은 귀사에 소속되어 있지 않은 인력(상주 파견 인력)을 의미합니다.

문 항	인력 수		
	1. 내부 인력	2. 외부 인력	3. 총 인력 (1+2)
B3-1. 정보보호 담당 인력	____명	____명	____명
B3-1-1. 개인정보보호 업무 겸직 여부	□	□	
B3-2. IT 인력(주 업무 : IT, 부가 업무 : 정보보호)	____명	____명	____명
B3-3. 일반 사무직 인력(주 업무 : 일반 사무, 부가 업무 : 정보보호)	____명	____명	____명

B4

귀사에는 다음의 **책임자가 임명**되어 있습니까?

【1)의 ① 예 응답자만】

문 항	1) 책임자 임명 여부		2) 전담 여부	
	예	아니오	예	아니오
B4-1. 정보관리책임자 CIO	①	②	①	②
B4-2. 정보보호최고책임자 CISO	①	②	①	②
B4-3. 최고기술책임자 CTO	①	②	①	②

【B4의 '2) 전담 여부'에 한 문항 이상 '② 아니오' 응답자만】

B4-1

귀사의 책임자가 **겸직하는 업무**는 무엇입니까? 모두 선택해 주시기 바랍니다.

문 항	정보관리 책임자 CIO	정보보호 최고책임자 CISO	최고기술 책임자 CTO	개인정보보호 최고책임자 CPO	기타
B4-1-1. 정보관리책임자 CIO		□	□	□	□ ( )
B4-1-2. 정보보호최고책임자 CISO	□		□	□	□ ( )
B4-1-3. 최고기술책임자 CTO	□	□		□	□ ( )

C 정보보호 교육

* **정보보호 교육이란?**
  정보보호 관련 해킹, 랜섬웨어 등 사이버 위협 또는 침입 방지, 내부 문건 보안 관리 등 물리적 위협 방지를 비롯한 각종 **보안 관련 유의사항 등에 대한 정보를 알려주는 교육을 모두 포함**하며, **개인정보보호 관련 법정 필수 교육은 제외함.**
* **정보보호 교육 예시**
  - 정보보안의 이해, 정보보호 기본지침, 사이버범죄 분석 및 예방, 원격근무 보안, 침해사고 유형 분석 및 실무대응 가이드, 교직원을 위한 내부정보 유출 방지, 업무환경에서의 정보보호 등

C1 귀사는 **중소기업 대상으로 실시**하는 **정보보호 무료 교육(오프라인/온라인)**을 알고 계십니까?

① 예 ② 아니오

C2 귀사는 **2024년 1년간** 임직원을 대상으로 **정보보호 교육을 실시**하였습니까?

① 예 ② 아니오 ☞ **"D. 정보보호 예산"으로 이동**

【C2의 '① 예' 응답자만】

C2-1 귀사는 아래의 임직원에 대해 **정보보호 교육을 실시**하였습니까?

*** C2-1의 모든 문항에 '② 아니오' 또는 '③ 해당 없음' 선택이 불가능합니다.**

문 항	정보보호 교육 실시 여부		
	예	아니오	해당 없음
C2-1-1. CEO 및 경영진	①	②	
C2-1-2. 정보보호 담당 인력	①	②	③
C2-1-3. IT 관련 직원(정보보호 담당 인력 제외)	①	②	③
C2-1-4. 일반 직원(IT 직원 제외)	①	②	
C2-1-5. 외주직원/협력업체 직원(전산장비 담당)	①	②	③

【C2의 '① 예' 응답자만】

C2-2 귀사는 아래의 임직원에 대해 **주로 실시한 정보보호 교육 방법**은 무엇입니까?

※ 강사와의 대면 여부에 따라 온라인/오프라인 교육으로 구분
(예시. 한 공간에 임직원이 모여서 교육 영상을 시청할 경우, 강사와의 비대면 진행이므로 '온라인 교육'으로 응답)
* C2-1에서 '① 예'를 선택한 문항만 응답

문 항	정보보호 교육 방법				교육 방식	
	정부/지자체/공공기관 교육 참여	민간 전문기관 위탁	자체 교육 (외부 강사)	자체 교육 (내부 강사)	온라인 교육	오프라인 교육
C2-2-1. CEO 및 경영진	①	②	③	④	①	②
C2-2-2. 정보보호 담당 인력	①	②	③	④	①	②
C2-2-3. IT 관련 직원 (정보보호 담당 인력 제외)	①	②	③	④	①	②
C2-2-4. 일반 직원(IT 직원 제외)	①	②	③	④	①	②
C2-2-5. 외주직원/협력업체 직원 (전산장비 담당)	①	②	③	④	①	②

【C2-1에서 한 문항이라도 '① 예'를 선택한 응답자만】

C2-3 귀사에서 실시하는 정보보호 교육에 활용되는 **교육 자료의 주요 출처**는 어떻게 됩니까? 해당하는 것을 **모두 선택**해 주십시오.

① 정부 또는 공공기관에서 제공하는 공식적인 온라인 교육 자료 활용
② 사내에서 자체 제작한 교육 자료 활용
③ 외부 전문 위탁 기관에 의뢰하여 제작한 교육 자료 활용
④ 외부 전문 위탁 기관에서 대여 또는 구입한 교육 자료 활용
⑤ 기타 ( )

【C2-1에서 한 문항이라도 '① 예'를 선택한 응답자만】

C2-4 귀사에서 실시한 임직원 대상 **정보보호 교육의 효과**는 어떠합니까?

전혀 효과가 없다	효과가 없는 편이다	보통이다	효과가 있는 편이다	매우 효과적이다
①	②	③	④	⑤

【C2-1에서 한 문항이라도 '① 예'를 선택한 응답자만】

C2-5 귀사에서 실시한 임직원 대상 **정보보호 교육의 만족도**는 어떠합니까?

매우 낮다	낮은 편이다	보통이다	높은 편이다	매우 높다
①	②	③	④	⑤

D 정보보호 예산

D1

귀사는 2024년 1년간 **정보보호 관련 활동을 위해 예산을 사용해 본 경험**이 있습니까?
※ 아주 적은 금액이라도 정보보호와 관련되어 비용을 지출한 경험이 있으시다면, "① 예"로 응답해 주십시오.

* **정보보호 예산 포함 항목**
  각종 정보보호 활동을 위한 인건비, 제품 및 서비스 구입비, 정보보호 시스템 유지 보수비, 정보보호 교육·훈련비, 인증 취득 비용 등

* **정보보안**
  해킹, 랜섬웨어 등 사이버 침해사고를 대비하기 위한 활동

* **물리적 보안**
  불법 침입, 직원 출입 관리 등 물리적 침해사고를 대비하기 위한 활동

① 예 ☞ D2 문항으로 이동　　② 아니오 ☞ D1-1 문항으로 이동

【D1의 '② 아니오' 응답자만】

D1-1

정보보호 예산을 사용하지 않는 이유에 대하여 아래 항목에 얼마나 공감하십니까?
* 응답 완료 후 D7 문항으로 이동

문 항	전혀 공감하지 않는다	공감하지 않는 편이다	보통 이다	공감하는 편이다	매우 공감한다
D1-1-1. 정보보호에 예산을 투입할 인적, 경제적 여력이 부족하기 때문에	①	②	③	④	⑤
D1-1-2. 침해사고를 완벽히 방어한다고 보장하지 못하기 때문에	①	②	③	④	⑤
D1-1-3. 회사에 필요한 정보보호 관련 활동이 무엇인지 모르기 때문에	①	②	③	④	⑤
D1-1-4. 현재 회사의 사업 영역은 정보보호와 무관하다고 생각하기 때문에	①	②	③	④	⑤
D1-1-5. 정보보호 관련 제품 및 서비스를 신뢰할 수 없기 때문에	①	②	③	④	⑤
D1-1-6. 정보 침해사고는 기업의 노력만으로 해결할 수 없다고 생각하기 때문에	①	②	③	④	⑤
D1-1-7. 정보보호 분야가 투자 우선순위가 아니기 때문에	①	②	③	④	⑤

【D1의 '① 예' 응답자만】

D2

정보보호 관련 활동을 위해 예산을 사용해 본 경험이 있다면, **2024년 1년간 정보보호 예산 총액**은 어느 정도입니까? **대략적인 예산 총액을 기재**하여 주십시오.

① 500만 원 미만
↳ (_____ 원)

② 500만 원 ~ 1,000만 원 미만
↳ (_____ 원)

③ 1,000만 원 ~ 3,000만 원 미만
↳ (_____ 원)

④ 3,000만 원 ~ 5,000만 원 미만
↳ (_____ 원)

⑤ 5,000만 원 ~ 1억 원 미만
↳ (_____ 원)

⑥ 1억 원 이상
↳ (_____ 원)

【D1의 '① 예' 응답자만】

D2-1

귀사의 2024년 1년간의 **정보보호 예산 총액은 2023년과 비교하여 어떻게 변화**하였습니까?

① 신설 → 2023년까지 정보보호 관련 별도의 예산을 공식적으로 사용하지는 않았으나, **2024년 처음 정보보호 활동을 위해 예산을 사용한 경우**를 의미
☞ **D2-2 문항으로 이동**

② 증가 → 2024년 정보보호 예산이 2023년 정보보호 예산보다 **금액적인 측면에서 증가한 경우**를 의미
☞ **D2-2 문항으로 이동**

③ 감소 → 2024년 정보보호 예산이 2023년 정보보호 예산보다 **금액적인 측면에서 감소한 경우**를 의미
☞ **D2-2 문항으로 이동**

④ 현상 유지 → 2024년 정보보호 예산과 2023년 정보보호 예산이 **금액적인 측면에서 차이가 없는 경우**를 의미
☞ **D3 문항으로 이동**

【D2-1의 ①~③ 응답자만】

D2-2

귀사의 **정보보호 예산의 변화 이유**는 무엇입니까? **우선순위대로 최대 3가지만** 선택하여 주십시오.

1순위 | **2순위** | **3순위**

① IT 예산 총액의 증가(감소)에 따른 변화
② 정보보호 인력 인건비 증가(감소)
③ 정보보호 제품 구입 비용 증가(감소)
④ 정보보호 서비스 구입 비용 증가(감소)
⑤ 정보보호 시스템 유지·보수 비용 증가(감소)
⑥ ISMS-P, ISO, PIA 등 인증 취득비용(수수료 등) 증가(감소)
⑦ 정보보호 사고 대응 관련 비용 증가(감소)
⑧ 기타 ( )

D3

【D1의 '① 예' 응답자만】

향후 2025년 귀사의 **정보보호 예산 총액은 어떻게 변화할 예정**입니까?

대폭 줄일 것이다	소폭 줄일 것이다	현상 유지할 것이다	소폭 늘릴 것이다	대폭 늘릴 것이다
①	②	③	④	⑤

D4

【D1의 '① 예' 응답자만】

2024년 1년간 귀사의 **정보보호 예산 활용 중 가장 큰 비중을 차지하는 유형**은 무엇입니까?
우선순위대로 최대 3가지만 선택하여 주십시오.

1순위 _____ **2순위** _____ **3순위** _____

① 정보보호 관련 정보보호 제품 및 솔루션의 구입(오픈소스, 월 SW 구독료, 클라우드 등 포함)
② 정보보호 관련 정보보호 제품 및 솔루션의 유지·보수
③ 정보보호 관련 관제 서비스
④ 정보보호 관련 유료 인증서의 결제
⑤ 정보보호 관련 컨설팅(취약점 분석 등 포함)
⑥ 정보보호 관련 교육 자료 습득(강의, 학습자료 등 포함)
⑦ 업무 시설의 CCTV 등 영상감시장비 설치 또는 증설(유지·보수 포함)
⑧ 정보보호를 위한 전문인력의 고용(인건비 등)
⑨ 기타 ( )

D5

【D1의 '① 예' 응답자만】

정보보호 관련 예산 활용을 결정하게 된 계기는 무엇입니까?
우선순위대로 최대 3가지만 선택하여 주십시오.

1순위 _____ **2순위** _____ **3순위** _____

① 정보 침해사고 피해를 직접적으로 접한 이후
② 주변 거래처 및 유관기관의 정보 침해사고 피해를 간접적으로 접한 이후
③ 주변 거래처/지인의 추천을 통해
④ 정보보호 관련 교육을 수강하여 위험성을 인지한 이후
⑤ TV 또는 온라인 매체(뉴스, 유튜브, SNS 등)를 통한 정보 습득으로 위험성을 인지한 이후
⑥ 정보보호 기업체의 홍보 자료 또는 영업을 접한 이후
⑦ 거래처의 요구에 의해
⑧ 정보부 및 공공기관의 정보보호 지원사업 홍보자료를 접한 이후
⑨ 기타 경로 (_____)

【D1의 '① 예' 응답자만】

D6

귀사의 **정보보호 관련 예산 소비는 적절**하다고 생각하십니까?

전혀 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
①	②	③	④	⑤

→ D6-1 문항으로 이동 / → D7 문항으로 이동

【D6 '① 전혀 그렇지 않다' 또는 '② 그렇지 않다' 응답자만】

D6-1

예산 소비가 적절하지 않다고 판단한다면, 아래의 항목에 대하여 **어느 정도 공감**하십니까?

문 항	전혀 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
D6-1-1. 사업 규모에 비해 과도한 예산 비중을 차지한다고 판단되기 때문에	①	②	③	④	⑤
D6-1-2. 투자하는 정보보호 예산에 비해 침해사고 위험이 감소하지 못하기 때문에	①	②	③	④	⑤
D6-1-3. 투자하는 정보보호 예산에 비해 정보보호 관련 업무가 해소되지 못하기 때문에	①	②	③	④	⑤
D6-1-4. 기업의 투자자 또는 기업의 소유주가 불필요한 예산 낭비로 인식하고 있기 때문에 (침해사고가 결과적으로 발생하지 않으면 의미 없는 투자가 될 수 있다고 생각하기 때문에)	①	②	③	④	⑤
D6-1-5. 정보보호 제품·솔루션 또는 서비스의 단가가 매우 비싸기 때문에	①	②	③	④	⑤
D6-1-6. 도입하고 있는 제품·솔루션 또는 서비스가 실제 필요한 항목인지 명확히 알지 못하기 때문에	①	②	③	④	⑤
D6-1-7. 정보보호 영역은 지나치게 전문적인 영역으로 기업의 합리적인 소비 판단 자체가 어렵기 때문에	①	②	③	④	⑤

D7

귀사는 **정보보호 관련 제품 및 서비스를 이용할 때 국내·외 제품 및 서비스 중 어떤 것을 선호**하십니까?

문 항	국내	해외	특별히 선호도를 구분하지 않음
D7-1. 정보보호 제품	①	②	③
D7-2. 정보보호 서비스	①	②	③

【D7-1, D7-2의 ①~② 응답자만】

D8

귀사가 **국산 또는 해외 정보보호 관련 제품 및 서비스를 선호하는 이유**가 무엇입니까?

문 항	항목		
D8-1. 정보보호 제품	① 성능	② 가격	③ 기타( )
D8-2. 정보보호 서비스	① 성능	② 가격	③ 기타( )

E 침해사고 예방

E1

귀사에서는 정보 침해사고 예방을 위해 어떠한 유형의 **정보보안 제품(서비스)을 활용**하고 있습니까? **모두** 선택하여 주십시오.

정보보안 제품(서비스)	설명	설치형	클라우드형
① 네트워크 보안	네트워크를 통한 접근 및 침입, 정보 유출 등의 공격에 대응하기 위한 제품 및 솔루션 (방화벽, IPS, VPN, 망분리 시스템 등)	□	□
② 시스템(앤드 포인트) 보안	IT 기기 및 단말 등을 공격하는 악성코드, 랜섬웨어, 스파이웨어 등에 대응하기 위한 제품 및 솔루션 (백신 프로그램, 악성코드, 랜섬웨어 대응, EDR, CDR, 모바일 단말 보안 솔루션 등)	□	□
③ 콘텐츠 / 데이터 보안 / 정보유출 방지	내부 컨텐츠 또는 기밀 정보의 불법 복제, 외부 유출 등을 탐지하고 차단하는 제품 및 솔루션 (DRM, DLP, 비식별화 솔루션, DB보안, 보안USB 등)	□	□
④ 클라우드 보안	클라우드 시스템 자체를 보호하기 위한 각종 기술 및 관리적 수단 등을 포함하는 보안 장비 (워크로드 보안, CASB, 가상화 관리, SASE 등)	□	□
⑤ 공통 인프라 보안	암호, 인증, 접근제어, 로그관리, 백업 등을 포괄하며 기업이 보유한 IT 인프라를 보호할 수 있는 각종 기능이 포함된 보안 장비 (PKI, FIDO, 로그관리시스템, 백업/복구 관리 시스템 등)	□	□
⑥ 정보보호 컨설팅 서비스	정보보호의 목적을 달성하기 위한 기업의 전반적인 보안 위험을 분석하고 적절한 대응 방안을 제안 또는 지원하는 서비스 (정보보호 평가/인증 지원, 취약점 진단, 모의해킹, 정보보호 감사 서비스 등)		
⑦ 보안 관제 서비스	기업의 IT 자원 및 보안 시스템의 운영 관리를 전문적으로 아웃소싱하여 24시간 실시간 감시 및 분석, 대응을 지원하는 서비스(원격/파견 관제 서비스)		
⑧ 보안 교육 / 훈련 서비스	정보보호에 대한 임직원 교육 및 IT/전산 관련 부서 임직원을 위한 정보보호 기능 훈련 등을 제공하는 서비스		
⑨ 보안 시스템 유지 / 관리 서비스	구축한 정보보호 제품 및 인프라를 최적의 상태로 활용할 수 있도록 제품지원, 기술지원, 사용자 지원을 제공하는 서비스		
⑩ 사이버 보험 등 정보유출 관련 위험 대비 서비스	해킹, 랜섬웨어, 정보 유출 등 정보보안 사고 발생 시 금전적 손실이나 배상 책임을 대비하기 위한 보험 상품 및 서비스 (예: 사이버 보험 등)		
⑪ 정보보안 제품(서비스) 활용하지 않음			

E2

귀사에서는 정보 침해사고 예방을 위해 어떠한 유형의 **물리적 보안 제품(서비스)을 활용**하고 있습니까? **모두** 선택하여 주십시오.

① 출입 통제 관리 시스템 (출입통제 게이트, 디지털 도어락 등)
② 영상 보안 시스템 (IP 카메라, CCTV 등)
③ 출동 보안 서비스 (사설 경비 업체 등)
④ 불법 도·감청 탐지 서비스 (몰래카메라, 초소형 도청 장치 등)
⑤ 물리적 보안 제품(서비스) 활용하지 않음

【E1의 '①~⑩' 또는 E2의 '①~④' 응답자만】

E3 귀사에서 활용하고 있는 제품의 **정보보호 인증**(CC인증, CSAP인증, GS인증, 보안기능 확인서 등) **여부**에 대해 알고 있습니까?

① 예 ② 아니오

E4 귀사 **내·외부에 설치된 CCTV는 몇 대**입니까? 그리고, **CCTV를 관리하는 방법**은 무엇입니까?
(직접 관리하지 않을 경우, 일상 업무 중 파악되는 CCTV 대수를 가늠하여 기입)
※ 주 사업장 : 본사/본점 제외한 사업장 중 매출액이 가장 높은 사업장

구분	문 항	CCTV 관리 현황	
		E4-1. CCTV 관리 방법	E4-2. CCTV 대수
1	주 사업장 (설문 1p 기업체의 사업형태에 '① 예'라고 응답한 경우에만 응답)	① 직접 관리	( )대
		② 간접(업체 위탁) 관리	( )대
		③ 건물 자체 관리	( )대
2	본사/본점	① 직접 관리	( )대
		② 간접(업체 위탁) 관리	( )대
		③ 건물 자체 관리	( )대

E5 귀사에서는 최근 **사내 IT 시스템 및 네트워크에 대한 보안 점검을 마지막으로 언제 실시**하였습니까?

① 1개월 미만
② 1개월 이상 ~ 6개월 미만
③ 6개월 이상 ~ 1년 미만
④ 1년 이상 ~ 2년 미만
⑤ 2년 이상
⑥ 실시하지 않음 ☞ **E6 문항으로 이동**

【E5의 ①~⑤ 응답자만】

E5-1 귀사에서는 보안 점검을 위해 **시스템 로그 및 방화벽 로그 기록을 관리**하고 있습니까?

① 예 ② 아니오

【E5의 ①~⑤ 응답자만】

E5-2 귀사에서 **시스템 및 방화벽 로그 기록을 저장하는 주기**는 어떻게 되십니까?

① 3일 미만
② 3일 이상 ~ 1주일 미만
③ 1주일 이상 ~ 1개월 미만
④ 1개월 이상 ~ 3개월 미만
⑤ 3개월 이상 ~ 6개월 미만
⑥ 6개월 이상
⑦ 실시하지 않음
⑧ DB 또는 저장장치의 용량만큼(별도 관리하지 않음)

E6

귀사에는 **공식 문서로 작성**된 **백업 관련 정책 또는 규정집**이 있습니까?

① 예 ② 아니오

E6-1

귀사에서는 다음과 같은 **데이터의 백업을 실시***하고 있습니까?
※ 외부 위탁 업체를 통해 백업을 실시한다면 '실시'로 응답 바랍니다.

문 항	백업 실시 여부		
	실시	미실시	해당없음
E6-1-1. 중요 데이터 (기업 내부정보, 지식재산, 영업비밀 등)	①	②	
E6-1-2. 서버 데이터(운영체제 로그, 웹서버 로그 등)	①	②	
E6-1-3. 접속 로그 데이터	①	②	
E6-1-4. 방화벽 로그 데이터	①	②	③
E6-1-5. 보안카메라(CCTV, IP카메라 등) 및 영상 데이터	①	②	③

* **시스템 로그 데이터**
시스템의 운영 과정에서 발생하는 모든 내용이 시간 등과 함께 기록된 자료를 의미함

* **방화벽 로그 데이터**
네트워크 트래픽을 모니터링하고 사전에 정해진 보안 프로토콜 기반으로 특정 트래픽의 차단, 허용을 결정하는 장비인 '방화벽'에서 기록된 자료(로그 형식, IP/호스트 이름, 시작/종료/유지시간, 방화벽 정책 ID, 출발지/목적지 주소, 목적지 포트, 프로토콜 등)를 의미함

E6-2

【E6-1의 한 문항이라도 '① 실시'를 선택한 응답자만】

귀사에서 주로 실시하는 **백업 방식**은 다음 중 무엇입니까?
* 여러 방식으로 데이터를 백업할 경우, **가장 대표적인 방식을 선택**하여 주십시오.

① USB, 외장하드 등 별도 저장장치 활용 ② 클라우드 서버 활용
③ 운영 체제 백업 기능 사용 ④ 별도 백업 서버(NAS, SAN 등) 운용
⑤ 기타 ( )

E6-3

【E6-1의 한 문항이라도 '① 실시'를 선택한 응답자만】

귀사가 수행하는 **데이터 백업의 주기**는 어떠합니까?
여러 유형의 데이터를 각각 백업할 경우, **가장 대표적인 주기를 선택**하여 주십시오.

① 실시간 ② 1개월에 1회 실시 ③ 3개월에 1회 실시
④ 6개월에 1회 실시 ⑤ 1년에 1회 실시 ⑥ 1년에 1회 미만 실시
⑦ 정해진 주기 없음

E7

귀사의 전체적인 **정보 침해사고의 사전 예방 능력**은 어느 정도의 수준이라고 판단하십니까?

문 항	매우 취약하다	취약한 편이다	보통이다	안전한 편이다	매우 안전하다
E7-1. 정보보안	①	②	③	④	⑤
E7-2. 물리적 보안	①	②	③	④	⑤

F 침해사고 경험

F1 귀사에서는 **정보 침해사고가 발생할 가능성**이 크다고 생각하십니까?

전혀 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
①	②	③	④	⑤

F2 귀사는 가까운 협력 또는 유관 업체의 **침해사고 피해 사실을 직·간접적으로 접한 적**이 있습니까?

① 있다 ② 없다

F3 귀사는 2024년 1년간 **정보 침해사고를 의심한 적**이 있습니까?
(사고 여부가 확실히 증명된 것은 아니지만, 정황상 직·간접적으로 침해 의심이 되는 경우)

① 있다 ② 없다

F4 귀사는 2024년 1년간 **정보 침해사고를 직접적으로 경험한 적**이 있습니까?

① 예 → (_____ 회) ② 아니오 ③ 인지하지 못함

└ F4-1 문항으로 이동 ┘ └ "G. 사이버 보험"으로 이동 ┘

【F4의 '① 예' 응답자만】

F4-1 귀사가 2024년 1년간 **경험한 정보 침해사고는 어떠한 유형**입니까? 해당하는 것을 **모두 선택**해 주십시오.

① 컴퓨터 바이러스, 웜, 트로이잔, APT 공격으로 인한 IT 시스템 마비
② 외부로부터 침투한 비인가 접근(해킹)
③ 랜섬웨어 감염
④ DoS 또는 DDoS 공격으로 인한 IT 시스템 마비
⑤ 피싱, 스미싱 등에 의한 금전 또는 중요 데이터 유출
⑥ 내부인력에 의한 중요 데이터 유출
⑦ 인가받지 않은 인원의 불법적인 사내 침입 또는 침입 시도 (예시. 시설 침입 등)
⑧ 중요 자산(디지털 자산 포함)에 대한 의도적인 손·망실
⑨ 불법적인 도·감청
⑩ 외부에서 CCTV(IoT)를 통해 CCTV(IoT) 시스템 조정 및 내부 자료 유출
⑪ 기타 ( )

【F4의 '① 예' 응답자만】

F4-2

귀사가 2024년 1년간 **경험한 침해사고는 어떻게 인지**하였습니까?
해당하는 것을 **모두 선택**해 주십시오.

① 보안 시스템의 침해사고 경보(알림)
② 침해사고 해결 조건으로 대가 요구 및 협박 등을 경험
③ 기존과는 다른 시스템 설정의 변경 또는 보유하고 있는 데이터의 위변조 사항 발견
④ 보안 시스템의 임의적 해제 또는 침입 흔적 발견(물리적 침입 포함)
⑤ 수사기관 또는 정보보호 관련 공공기관으로부터의 협조 요청
⑥ 민원 접수 또는 고객의 신고
⑦ 기타 (_____)

【F4의 '① 예' 응답자만】

F4-3

귀사가 2024년에 경험한 침해사고 중 **가장 피해규모가 큰 침해사고 기준으로 사고 피해 심각도**는 어느 정도였습니까?

침해사고는 있었으나, 경제적 피해는 매우 경미하다	<				보통이다				>	단시간에 회복되기 어려운 경제적 피해가 있었다
-5	-4	-3	-2	-1	0	+1	+2	+3	+4	+5
매우 경미		경미한 편			보통	심각한 편			매우 심각	

【F4의 '① 예' 응답자만】

F4-4

귀사가 2024년에 경험한 침해사고 중 **가장 피해규모가 큰 침해사고를 기준으로 단계별** (발생 사실 인지/원인 파악/문제 해결 및 서비스 복원)로 **소요된 시간**을 응답해 주십시오.

침해사고 단계 * 단계별 시간 기입	1시간 이내	1일 이내	7일 이내	30일 이내	30일 초과	알 수 없음
F4-4-1. 침해사고 발생시점부터 **사실을 인지**하기까지 **소요된 시간**	①	②	③	④	⑤	⑥
F4-4-2. 발생 사실 인지 시점부터 **원인을 파악**하기까지 소요된 시간	①	②	③	④	⑤	⑥
F4-4-3. 원인 파악 시점부터 **문제 해결 및 서비스 복원**하기까지 소요된 시간	①	②	③	④	⑤	⑥

【F4의 '① 예' 응답자만】

F5

귀사는 침해사고를 겪고 난 뒤, **관련 기관 또는 수사기관에 신고**하였습니까?

① 신고하였다 ☞ F6 문항으로 이동
② 신고하지 않았다 ☞ F5-1 문항으로 이동

【F5의 '② 신고하지 않았다' 응답자만】

F5-1

신고하지 않았다면, 그 이유는 무엇입니까? **우선순위대로 최대 2가지만** 선택하여 주십시오.

*** 응답 완료 후 "G. 사이버 보험"으로 이동**

1순위 _____ **2순위** _____

① 피해 규모가 경미하기 때문에
② 피해 사실이 알려지는 것이 두렵기 때문에
③ 어디에 신고해야 하는지 모르기 때문에
④ 신고하더라도 피해가 회복되지 않을 것이기 때문에
⑤ 신고에 따른 업무가 복잡하기 때문에
⑥ 전문 대응 업체 또는 수사기관을 신뢰하지 않기 때문에

【F4의 '① 예' 응답자만】

F6

귀사는 **침해사고를 겪고 난 뒤, 어떠한 활동**을 취하였습니까? 해당하는 것을 **모두 선택**해 주십시오.

① 별도의 침해사고 대응팀(CERT) 구축
② 정보보호 관련 제품 및 솔루션 구축 및 고도화
③ 정보보호 분야 전문기관 또는 전문가 자문
④ 정보보호 사고 대응 관련 전문기관 신고
⑤ 사내 IT 시스템의 위탁관리 업체에 대한 피해보상 요구
⑥ 정보보호 인증(CC인증, CSAP인증, GS인증, 보안기능 확인서 등)을 받은 제품으로 교체
⑦ 내부 정보보호 정책 수립 또는 수정
⑧ 별다른 활동을 수행하지 않음

【F4의 '① 예' 응답자만】

F7

귀사의 **종합적인 정보 침해사고 사후 대응 능력**은 어느 정도의 수준이라고 판단하십니까?

구 분	매우 취약하다	취약한 편이다	보통이다	안전한 편이다	매우 안전하다
F7-1. 정보보안	①	②	③	④	⑤
F7-2. 물리적 보안	①	②	③	④	⑤

【F4의 '① 예' 응답자만】

F8

정보 침해사고 경험 이후 **정보 침해사고에 대한 관심도**는 침해사고 이전과 비교했을 때, **어떻게 변화**하였습니까?

관심이 매우 낮아졌다	관심이 낮아졌다	전과 유사하다	관심이 커졌다	관심이 매우 커졌다
①	②	③	④	⑤

G 사이버 보험

* **사이버 보험**
사이버 보험이란 사이버 공간에서 일어난 해킹, DDoS 등의 의도적인 공격으로 인해 기업이 겪게 되는 각종 피해에 대하여 회복 또는 복구, 배상을 지원하기 위한 보험을 말합니다.
현재 국내에서는 개인정보보호에 대한 보장을 다루는 상품이 주를 이루고 있지만, 향후 기업 기밀 또는 데이터 유출, 해킹, 랜섬웨어/악성코드 감염 등의 피해에 대한 복구 비용 등을 보장받기 위한 보험 상품의 출시가 더욱 활성화될 예정이므로 이에 대한 민간 기업의 인식 현황을 확인하고자 하오니 설문에 응답해 주시기 바랍니다.

본 G. 사이버 보험 파트에서는 개인정보와 관련된 보험 상품에 대한 응답은 제외하여 주시기 바랍니다.

예시) 공인전자문서보관소 배상책임보험, e-Biz 배상책임보험, 전자금융거래 배상책임보험, 집적정보통신 시설 사업자 배상책임보험 등

G1

귀사는 사이버 보험에 대해 **어느 정도 알고 계십니까?**

전혀 모른다	용어 정도만 들어본 적 있다	대략적인 의미와 특징만 알고 있다	잘 알고 있다
①	②	③	④
"H. 원격근무"로 이동		G2 문항으로 이동	

G2

【G1의 ②~④ 응답자만】

귀사는 사이버 보험에 **가입 또는 이용**하고 계십니까? 해당 항목을 선택해 주십시오.

문 항	해당 여부	
G2-1. 가입 여부	① 가입 경험 있음	② 가입 경험 없음
G2-2. 이용 여부	① 현재 이용 중임 ② 현재 이용하지 않음	
G2-3. 향후 가입(유지) 계획	① 예 ☞ G3 문항으로 이동	② 아니오 ☞ "H. 원격근무"로 이동

G3

【G2-3의 '① 예' 응답자만】

귀사가 향후 사이버 보험 가입 시 **보장받고자 하는 항목**을 **우선순위대로 최대 2가지만** 선택하여 주십시오.

1순위 _____ **2순위** _____

① 기업 데이터 유출 사고 발생 시 대응 비용(조사, 통지, 법률 자문)
② 기업 사이버 공격 발생 시 시스템 복구 또는 정상화 비용
③ 기업 기밀 유출 관련 소송 비용 (변호사 선임 비용 등)
④ 기업 기밀 유출에 따른 배상, 합의금 또는 과징금 관련 비용
⑤ 좀비 PC 해킹 등 공격 경유지로 활용 시 경유 배상 책임 비용
⑥ 사이버 갈취로 인한 손해(랜섬웨어, 스피어 피싱 등) 보장 비용
⑦ 기타 (_____)

H 원격근무

H1 귀사는 2024년 1년간 **원격근무를 시행**하였습니까?

① 예 ☞ H1-1 문항으로 이동 ② 아니오 ☞ 조사 종료

【H1의 '① 예' 응답자만】

H1-1 귀사가 **원격근무 시 직원에게 지원한 보안 솔루션**은 무엇입니까? 해당하는 것을 **모두 선택**해 주십시오.

① 자체 구축한 가상사설망(VPN) 활용
② 전문 원격근무 서비스 기업의 업무지원 서비스 활용
③ 온라인 협업 툴 활용
④ 보안 제품 활용
⑤ 문서암호화(DRM) 시스템
⑥ 정보유출방지(DLP) 시스템
⑦ 전자문서관리 시스템(EDMS)
⑧ 기타 ( )
⑨ 원격근무를 위한 별도의 보안 솔루션을 지원하지 않음

【H1의 '① 예' 응답자만】

H1-2 귀사에서는 **원격근무 시 정보보호에 대한 위험성을 인지**하고 있습니까?

전혀 그렇지 않다	그렇지 않은 편이다	보통이다	그런 편이다	매우 그렇다
①	②	③	④	⑤

【H1의 '① 예' 응답자만】

H2 귀사에서 2024년 1년간 **원격근무 시행 준비 및 운영 간 정보보호 관련 침해사고가 발생했거나, 침해사고가 의심되었던 경우가 있습니까?**

① 침해사고 발생 → (_____ 회) ② 침해사고 의심 → (_____ 회) ③ 해당 사항 없음

Z 조사 기록표 [면접원 기록사항]

Z1 조사 방법

① 방문면접조사
② 현장방문 시 조사가 불가능하여 질문지 배포 후 방문하여 조사 완료서비스 활용
③ 현장방문 시 조사가 불가능하여 질문지 배포 후 이메일이나 팩스로 조사 완료
④ 이메일이나 팩스로 질문지 발송 후 방문하여 조사 완료
⑤ 이메일이나 팩스로 질문지 발송 후 이메일이나 팩스로 조사 완료
⑥ 전화조사
⑦ 기타 ( )

Z2 질문지 작성자 현황

① 정보보호 관련 종사자 ② 정보 관련 종사자 ③ 기업체의 대표
④ 기업체 총무부서 담당자 ⑤ 기타 ( )

Z3 조사일시

월 일 시 분부터 분간

Z4 조사대상 기업체 정보 변경 현황

구 분	변경 여부	변경사항(이전 정보)
기업체명		
업 종		
규 모		
지 역		

Z5 면접원 기록사항

1. 응답자 성명		2. 소속	
3. 직위		4. 전화번호	
5. 이메일		6. 조사원 성명	

- 끝까지 응답해 주셔서 감사합니다. -

2025년 정보보호 실태조사 (개인)

승인번호
제 342005 호

안녕하십니까?

과학기술정보통신부와 한국정보보호산업협회에서는 우리나라 인터넷 이용자의 정보보호 현황과 각종 역기능으로 인한 피해 실태를 파악하여 관련 정책 수립의 기초자료로 활용하고자 전국의 만12~69세 인터넷 이용자를 대상으로 "2025년 정보보호 실태조사 (개인)"을 실시하고 있습니다.

정부의 효과적인 정보보호 정책 수립에 도움이 될 수 있도록 귀하의 적극적인 협조를 부탁드립니다.

아울러 작성해 주신 자료는 조사와 연구에 관련된 목적에만 사용될 것이며, 비밀은 철저히 보장될 것을 약속드립니다.
설문조사에 응해 주심에 감사드리며, 귀하의 평안과 번창하심을 기원합니다.

2025년 8월

주관기관	전담기관	조사기관	실사 문의	조사 문의
과학기술정보통신부	한국정보보호산업협회	㈜글로벌리서치		

* 본 조사는 통계법 제33조(비밀의 보호)에 따라 통계 목적으로 이용되며, 귀하의 비밀이 절대 보장됨을 약속드리는 바입니다.

관리 사항	조사구 번호	가구 번호	주거 유형	면접원 정보	
				이름	연락처
			① 비아파트 ② 아파트		

면접원 기입란	주 소				전 화 번 호	응답자 이름
	시·군·구	읍·면·동	도로명 + 건물번호	동/층/호	이동전화 ( ) -	
			지번		유선전화 ( ) -	
지 역 (시·도)	① 서울 ② 부산 ③ 대구 ④ 인천 ⑤ 광주 ⑥ 대전 ⑦ 울산 ⑧ 세종 ⑨ 경기 ⑩ 강원 ⑪ 충북 ⑫ 충남 ⑬ 전북 ⑭ 전남 ⑮ 경북 ⑯ 경남 ⑰ 제주					
성 별	생 년 월 (만 연령)			직 업		
① 남 ② 여	양력 _____년 _____월 (만____세) ☞ 만 12세 미만, 만 70세 이상은 조사 중단			① 있음	직업명	
					직업코드	
				② 없음	① 학생 ② 전업주부 ③ 기타/무직	

응답 시 유의사항

1 면접원의 안내에 따라 응답해 주십시오.

2 **본 설문지는 귀 댁(가구)에 상주하는 만12~69세 가구원을 대상으로 합니다.**

3 본 설문지는 응답 시점을 기준으로 최근 1년간 「2024년 8월 1일 ~ 2025년 7월 31일」을 기준으로 응답해 주시기 바랍니다.
(단, 침해사고 경험 관련 문항은 「2024.1.1~2024.12.31」을 기준으로 응답해 주시기 바랍니다)

4 설문 응답 및 작성은 질문의 순서대로 보기항목에서 해당 번호를 선택하거나 직접 의견을 말씀해주시면 됩니다.

SQ 응답자 선정 질문

SQ1

귀하께서는 **최근 1개월 이내 인터넷을 이용한 적**이 있습니까?

① 예
② 아니오 ☞ 조사 중단

SQ2

귀하께서는 **인터넷에 접속하기 위해 어떤 전자기기를 사용**하였습니까? 해당하는 것을 **모두 선택**해 주십시오.

① 컴퓨터(데스크탑 PC, 노트북 등)
② 모바일 기기(스마트폰, 태블릿 PC 등)
③ IoT 가전제품(스마트 TV, 인공지능 비서 제품 등)
④ 기타 (_____)

SQ3

귀하의 **하루 24시간 중 인터넷 접속 시간**은 몇 시간입니까?(업무상 접속 포함)

① 1시간 이하
② 1시간 초과 ~ 3시간 이하
③ 3시간 초과 ~ 6시간 이하
④ 6시간 초과 ~ 9시간 이하
⑤ 9시간 초과 ~ 12시간 이하
⑥ 12시간 초과 → (_____ 시간)

SQ4

귀하는 **인터넷에서 접하는 다양한 정보***를 얼마나 **신뢰**합니까?

* **인터넷에서 접하는 다양한 정보**
예시) 건강 및 의료정보(질병 현황, 병원정보, 증상, 영양정보 검색 등을 포함), 상품/서비스 등의 정보, 신문/잡지 등 뉴스(기사), 여행/교통/숙박/위치정보, 소프트웨어(게임 제외)/애플리케이션(앱) 다운로드/업그레이드

전혀 신뢰하지 않는다	신뢰하지 않는 편이다	보통이다	신뢰하는 편이다	매우 신뢰한다
①	②	③	④	⑤

SQ5

귀하는 일상생활에서 의사결정 시 **인터넷이 어느 정도 중요하다고 생각**하십니까?

전혀 중요하지 않다	중요하지 않은 편이다	보통이다	중요한 편이다	매우 중요하다
①	②	③	④	⑤

SQ6

귀하는 일상생활에서 **인터넷을 사용하는 시간이 과도하다고 생각**하십니까?

전혀 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
①	②	③	④	⑤

SQ7

귀하는 일상생활에서 정보보호 관련 각종 범죄 또는 사고와 관련하여 **국가 및 공공기관으로부터 충분히 보호받고 있다고 생각**하십니까?

전혀 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
①	②	③	④	⑤

※ 설문에서는 개인의 입장에서 전반적인 '정보보호'에 대한 인식 및 실태를 묻고 있습니다.
개인정보보호를 제외한 '정보보호'를 기준으로 설문에 응답해주시기 바랍니다.

A 정보보호 인식

A1

귀하는 **최근 1년간 정보보호 관련 이슈*에 관심**을 가져본 적이 있습니까?

* **정보보호 관련 이슈**
- PC 또는 노트북 등 개인용 컴퓨터의 해킹과 같은 불법적 접근
- 개인용 모바일 기기(스마트폰, 태블릿, 패드 등)의 해킹과 같은 불법적 접근
- 랜섬웨어 또는 악성코드 감염 등에 의한 정상적인 전자장비 사용의 제한
- 개인용 전자기기에 대한 불법적 접근으로 인한 보유 중인 데이터의 외부 유출
- 피싱, 파밍, 스미싱 등에 의한 금전적 피해 등

전혀 없다	없는 편이다	보통이다	있는 편이다	자주 있다
①	②	③	④	⑤

A2

귀하는 **정보 침해사고에 대해 얼마나 우려**하십니까?

전혀 우려하지 않는다	우려하지 않는 편이다	보통이다	우려하는 편이다	매우 우려한다
①	②	③	④	⑤

A3

귀하는 최근 발생하는 정보보호 관련 사고*를 접할 때, **자신과 얼마나 관련이 있다고 생각**하십니까?

* **정보보호 관련 사고**
예시) 악성코드/랜섬웨어 감염 등으로 인한 피해, PC, IP카메라 등 개인용 전자기기 해킹 등으로 인한 사생활 침해, 온라인 계정 탈취 및 도용으로 인한 피해, 피싱/ 파밍/스미싱 등으로 인한 금전적 피해 등

전혀 관련 없다	관련 없는 편이다	보통이다	관련 있는 편이다	매우 관련 있다
①	②	③	④	⑤

A4

귀하는 현재 아래의 사항들에 대하여 **얼마나 안전하다고 생각**하십니까?

* **랜섬웨어**
몸값(Ransom)과 소프트웨어(Software)의 합성어로 시스템을 잠그거나 데이터를 암호화해서 사용할 수 없도록 하고 이를 인질로 금전을 요구하는 악성 프로그램을 말하며, 신뢰할 수 없는 사이트, 스팸메일, 파일공유 사이트, 네트워크망을 통해 유포됨

문 항	매우 취약하다	취약한 편이다	보통이다	안전한 편이다	매우 안전하다
A4-1. 개인용 전자기기의 랜섬웨어* 감염 등과 같은 악성코드 감염	①	②	③	④	⑤
A4-2. 개인용 전자기기 분실에 의한 정보 유출	①	②	③	④	⑤
A4-3. 불법 영상 촬영, 녹음기 등을 통한 사생활 침해	①	②	③	④	⑤
A4-4. 개인 생활 공간에 타인의 불법적인 접근 (예시. 주거침입, 절도 등)	①	②	③	④	⑤
A4-5. 기타 (_____)	①	②	③	④	⑤

A5

귀하는 정보 침해사고가 발생할 경우, **피해를 복구할 수 있다**고 느끼십니까?

전혀 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
①	②	③	④	⑤

A6

귀하는 **정보 침해사고의 발생 원인**에 대해 귀하께서 생각하시는 바와 일치하는 것을 선택하여 주십시오.

문 항	전혀 상관 없다	상관 없는 편이다	보통 이다	상관 있는 편이다	매우 상관 있다
A6-1. 개인의 부주의	①	②	③	④	⑤
A6-2. 정보통신 서비스 제공 기업의 사고 방지 노력의 부족	①	②	③	④	⑤
A6-3. 정보통신 기기 제조사*의 보안 기능 탑재 노력의 부족 *삼성, 애플 등	①	②	③	④	⑤
A6-4. 물리적 출입통제 등 하드웨어 장치 제조사의 보안 기능 탑재 노력의 부족	①	②	③	④	⑤
A6-5. 정부 및 공공기관의 사고 방지 노력의 부족	①	②	③	④	⑤
A6-6. 수사기관 및 관련 공공기관의 관련 범죄자 수사 노력의 부족	①	②	③	④	⑤
A6-7. 사법 기관의 관련 범죄 처벌 노력의 부족	①	②	③	④	⑤
A6-8. 처벌기준, 형량이 너무 낮아서	①	②	③	④	⑤

A7

귀하는 **정보 침해사고 방지를 위해 누가 주도적으로 노력**해야 한다고 생각하십니까?
개인과 기업 또는 공공의 비중을 각각 기재하여 주십시오(비중의 합은 100%가 되어야 합니다).

문 항	비 중
A7-1. 개인	_____ %
A7-2. 기업 또는 공공	_____ %
합계(개인 + 기업 또는 공공)	100 %

A8

귀하는 정보보호와 관련하여 각 **기관 및 업체를 어느 정도 신뢰**하십니까?

문 항	전혀 신뢰하지 않는다	별로 신뢰하지 않는다	보통 이다	신뢰 한다	매우 신뢰 한다
A8-1. 정보보호 관련 정부·공공기관	①	②	③	④	⑤
A8-2. 정보보호 관련 민간업체	①	②	③	④	⑤
A8-3. 인터넷 서비스 제공자 (통신사, 클라우드·포털·AI 서비스 등)	①	②	③	④	⑤

※ 설문에서는 개인의 입장에서 전반적인 '정보보호'에 대한 인식 및 실태를 묻고 있습니다.
개인정보보호를 제외한 '정보보호'를 기준으로 설문에 응답해주시기 바랍니다.

B 정보보호 교육

※ 파트 B의 설문 응답 시 '개인정보보호 법정 의무교육'은 제외하고 응답해야 합니다.

B1 귀하는 **최근 1년간 정보보호 관련 정보를 어떤 경로로 수집**하십니까?
해당하는 것을 **모두 선택**해 주십시오. **(개인정보보호 관련 정보는 제외)**

① 인터넷 검색(블로그, 포털 등)
② SNS(인스타그램, 페이스북 등)
③ 유튜브·동영상 플랫폼
④ 방송·언론 매체(뉴스, 신문 등)
⑤ 공공기관·지자체 홍보자료(포스터, 안내문 등)
⑥ 가족·지인·직장 동료 등 주변인 권유
⑦ 기타 (_____)
⑧ 없음

B2 귀하는 **최근 1년간 정보보호 교육을 받아 본 경험**이 있습니까?
(개인정보보호 법정 의무교육은 제외)

① 예 ☞ **B2-1 문항으로 이동**
② 아니오 ☞ **B4 문항으로 이동**

【B2의 '① 예' 응답자만】

B2-1 귀하께서 수강하신 **정보보호 교육의 방식**은 무엇입니까? 해당하는 것을 **모두 선택**해 주십시오.

① 근무지 혹은 학교 등에서의 온라인 교육 수강
② 근무지 혹은 학교 등에서의 오프라인 교육 수강
③ 개인적인 방식으로 온라인 교육 수강(줌(ZOOM), EBS 온라인클래스, 유튜브 등)
④ 근무지 외 개인적인 방식으로 오프라인 교육 수강(학교, 도서관 등)

【B2의 '① 예' 응답자만】

B2-2 귀하께서 수강하신 **정보보호 교육에 포함된 주제를 모두 선택**하여 주시기 바랍니다.

① 정보보호에 대한 기본 소양(배경 지식 등)
② 정보보호를 위한 사고 예방 방법
③ 정보보호의 중요성
④ 정보보호 피해 사례
⑤ 정보보호 피해 대응 방법

【B2의 '① 예' 응답자만】

B2-3 귀하께서 수강하신 **정보보호 교육의 학습 효과**는 어떠하였습니까?

* B2-2에서 선택한 문항만 응답

문 항	전혀 효과가 없다	효과가 없는 편이다	보통 이다	효과가 있는 편이다	매우 효과적 이다
B2-3-1. 정보보호에 대한 기본 소양(배경 지식 등)의 함양	①	②	③	④	⑤
B2-3-2. 정보보호를 위한 사고 예방 방법에 대한 인식	①	②	③	④	⑤
B2-3-3. 정보보호의 중요성에 대한 인식	①	②	③	④	⑤
B2-3-4. 정보보호 피해 사례에 대한 인식	①	②	③	④	⑤
B2-3-5. 정보보호 피해 대응 방법 습득	①	②	③	④	⑤

【B2의 '① 예' 응답자만】

B2-4 해당 **정보보호 교육의 학습 난이도**는 어떠하였습니까?

* B2-2에서 선택한 문항만 응답

문 항	전혀 이해 되지 않는다	이해 되지 않는 편이다	보통 이다	대체로 이해 되는 편이다	완전히 이해 된다
B2-4-1. 정보보호에 대한 기본 소양(배경 지식 등)	①	②	③	④	⑤
B2-4-2. 정보보호를 위한 사고 예방 방법	①	②	③	④	⑤
B2-4-3. 정보보호의 중요성	①	②	③	④	⑤
B2-4-4. 정보보호 피해 사례	①	②	③	④	⑤
B2-4-5. 정보보호 피해 대응 방법	①	②	③	④	⑤

【B2의 '① 예' 응답자만】

B3 귀하께서는 **정보보호 관련 학습의 어려움**에 대해서 각각 얼마나 동의하십니까?

문 항	전혀 동의 하지 않는다	동의 하지 않는 편이다	보통 이다	동의 하는 편이다	매우 동의 한다
B3-1. 정보보호 관련 용어가 생소하고 어려움	①	②	③	④	⑤
B3-2. 원하는 정보보호 관련 자료가 없음	①	②	③	④	⑤
B3-3. 정보의 양이 많고 복잡함	①	②	③	④	⑤
B3-4. 정보를 얻는 곳을 모름	①	②	③	④	⑤
B3-5. 정보보호 관련 신규 이슈가 계속 발생하여 학습이 어려움	①	②	③	④	⑤

B4 귀하께서는 **정보보호 관련 캠페인 또는 공익광고 등 홍보물**을 접하신 경험이 있으십니까?

① 예 ☞ B4-1 문항으로 이동　　② 아니오 ☞ "C. 정보보호 예산"으로 이동

【B4의 '① 예' 응답자만】

B4-1 귀하께서는 어떤 경로를 통해 **정보보호 관련 캠페인 또는 공익광고 등의 홍보물**을 주로 접하고 계십니까?

① 온라인 매체(웹배너·팝업 등)
② 방송매체(TV, IPTV, 영화, 라디오 등)
③ 옥외광고(지하철·버스·마트·전광판 등)
④ 인쇄·출판물(신문·서적·정기간행물·팸플릿 등)
⑤ 기타(　　)

※ 설문에서는 개인의 입장에서 전반적인 '정보보호'에 대한 인식 및 실태를 묻고 있습니다.
개인정보보호를 제외한 '정보보호'를 기준으로 설문에 응답해주시기 바랍니다.

C 정보보호 예산

※ 파트 C의 설문 응답 시 '정보보호에 대한 업무상의 금전적 소비'를 제외하고 응답해야 합니다.

C1 귀하는 최근 1년간 **개인적인 목적으로 정보보호와 관련하여 금전적인 소비***를 한 경험이 있습니까?(업무상 소비 제외)

* **정보보호 관련 금전적인 소비**
정보보호 관련 제품 및 솔루션 구입, 정보보호 관련 유료 인증서 결제, 정보보호 관련 학습 정보 구입, 출동보안 서비스 이용, CCTV 등 영상 감시 장비 관련 소비 등

① 예 ☞ C1-1 문항으로 이동 ② 아니오 ☞ C4 문항으로 이동

【C1의 '① 예' 응답자만】

C1-1 위와 같은 **금전적인 소비 중 가장 큰 비중을 차지하는 유형**은 무엇입니까?
우선순위대로 3가지만 선택하여 주십시오.

1순위 _____ **2순위** _____ **3순위** _____

① 정보보호 관련 제품 및 솔루션의 구입(오픈소스, 월 SW 구독료, 클라우드 등 포함)
② 정보보호 관련 유료 인증서의 결제
③ 정보보호 관련 학습 정보 습득(강의, 학습자료 등 포함)
④ 자택 또는 개인 생활 공간을 위한 출동보안 서비스 이용
⑤ 자택 또는 개인 생활 공간의 CCTV 등 영상감시장비 설치 또는 증설(유지·보수 포함)
⑥ 기타 (_____)

【C1의 '① 예' 응답자만】

C1-2 지난 1년간 **개인적인 목적으로 정보보호와 관련된 금전적 소비의 규모**는 어느 정도입니까?
(1년간 전체 소비 규모 전체를 합산하여 산출)

① 1만 원 미만 ② 1만 원 이상 ~ 10만 원 미만
③ 10만 원 이상 ~ 20만 원 미만 ④ 20만 원 이상 ~ 30만 원 미만
⑤ 30만 원 이상 ~ 40만 원 미만 ⑥ 40만 원 이상 ~ 50만 원 미만
⑦ 50만 원 이상 → (_____ 원)

【C1의 '① 예' 응답자만】

C1-3

정보보호 관련 금전적 소비를 결정하게 된 계기는 무엇입니까? 우선 순위대로 최대 3순위까지 선택하여 주십시오.

1순위 _____ **2순위** _____ **3순위** _____

① 정보 침해사고 피해를 직접적으로 접한 이후
② 주변 지인의 정보 침해사고 피해를 간접적으로 접한 이후
③ 주변 지인의 추천을 통해
④ 정보보호 관련 교육을 수강하여 위험성을 인지한 이후
⑤ TV 또는 온라인 매체(뉴스, 유튜브, SNS 등)를 통한 정보 습득으로 위험성을 인지한 이후
⑥ 정보보호 기업체의 홍보 자료 또는 영업을 접한 이후
⑦ 기타 경로 ( )

【C1의 '① 예' 응답자만】

C2

귀하의 **정보보호 관련 금전적 소비는 적절**하다고 생각하십니까?

전혀 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
①	②	③	④	⑤

【C1의 '① 예' 응답자만】

C3

앞으로 정보보호 활동을 위한 비용이 증가 혹은 감소할 예정이십니까?

크게 줄일 예정이다	줄일 예정이다	비슷할 것이다	늘릴 예정이다	크게 늘릴 예정이다
①	②	③	④	⑤

【C1의 '② 아니오' 응답자만】

C4

귀하께서는 **앞으로 정보보호 활동을 위한 비용을 지출할 의향**이 있으십니까?

전혀 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
①	②	③	④	⑤

※ 설문에서는 개인의 입장에서 전반적인 '정보보호'에 대한 인식 및 실태를 묻고 있습니다. 개인정보보호를 제외한 '정보보호'를 기준으로 설문에 응답해주시기 바랍니다.

D 일상 생활 속의 정보보호

D1

귀하는 최근 1년을 기준으로 **공공장소(지하철, 카페 등)에서 제공되는 무료 인터넷(Wi-fi)에** 노트북, 스마트폰, 패드 등을 **얼마나 연결**하여 사용하십니까?

전혀 사용하지 않는다	별로 사용하지 않는 편이다	보통이다	자주 사용하는 편이다	항상 사용한다
①	②	③	④	⑤

D2 귀하는 공공장소, PC방 등 **불특정 다수가 사용하는 전자장비(PC 등)에 개인 계정으로 접속할 경우,** 별도의 로그아웃(Log-out), 접속기록(쿠키)* 삭제 등과 같은 **예방 활동을 수행**하십니까?

> * **접속기록(쿠키)**
> 인터넷 사용자가 웹사이트에 접속할 때 자동적으로 만들어지는 임시 파일로, 유튜브의 시청 기록, 이용자가 본 내용, 상품 구매 내역, 신용카드 번호, 아이디(ID), IP 주소 등의 정보를 담고 있는 일종의 정보 파일

전혀 수행해 본 적 없다	수행하지 않는 편이다	보통이다	대체로 수행하는 편이다	반드시 수행한다
①	②	③	④	⑤

D3 귀하께서는 인터넷 서비스를 이용하면서 **비밀번호 변경 필요 안내 시 비밀번호를 즉시 변경**하십니까?

① 예 ② 아니오

D4 귀하는 **최근 1년간 정보보호를 위해** PC(노트북 포함), 스마트폰 등 개인용 전자기기에 저장된 **디지털 데이터(사진 포함)를 백업**한 적이 있습니까?

① 예 ② 아니오

D5 귀하는 최근 1년간 PC(노트북 포함), 스마트폰 등 **개인용 전자기기에 설치된 보안 프로그램을 활용하여 보안 점검을 수행해 본 경험**이 있습니까?
(보안 프로그램 또는 운영체제의 보안 업데이트 알림에 대응)

① 예 ② 아니오

D6 귀하께서는 **정보보호를 위해 어떤 노력**을 하십니까? 해당하는 것을 **모두 선택**하여 주십시오.

① 웹사이트의 파일을 함부로 다운로드하지 않음
② 프로그램 설치 시 불필요한 프로그램이 추가적으로 설치되는지 확인
③ 파일 및 폴더의 공유 설정하지 않음
④ 응용 소프트웨어 보안업데이트 실시
⑤ 의심스러운 URL 링크 클릭하지 않음
⑥ P2P, 웹하드 등 방문하지 않음
⑦ 금융권 이용 시 정보가 노출되지 않도록 주의
⑧ 공동인증서(금융인증서)는 이동식 디바이스(USB, 외장하드)에만 저장
⑨ 기타 ( )

D7 귀하는 최근 1년간 **원격근무(온라인 연결)*를 수행**하신 경험이 있습니까?

> * **원격근무 시 온라인 연결 프로그램**
> 예시) 업무용 메신저 : 네이버 웍스, 마이크로소프트 팀스, 네이버 밴드 등
> 화상회의 프로그램 : 시스코 웹엑스, ZOOM 등
> 클라우드 스토리지 : 구글 드라이브, 네이버 BOX 등
> 기타 : vpn 등

① 예 ☞ **D7-1 문항으로 이동** ② 아니오 ☞ **E1 문항으로 이동**

【D7의 '① 예' 응답자만】

D7-1 귀하께서는 **비대면 환경 활용 시 정보보호를 위해서 주로 어떤 활동**을 하셨습니까?

① 학교, 회사 등에서 제공한 정보보호 제품을 사용
② 비대면 환경 보안을 위한 전용 정보보호 제품을 별도로 사용
③ 비대면 환경을 활용하고 있는 컴퓨터로 의심스러운 URL 클릭 등을 하지 않음
④ 학교, 회사 등에서 제공하는 디바이스를 활용하여 비대면 환경 사용
⑤ 원격근무, 화상회의 등 이용 시 관련 프로그램 이외의 프로그램을 사용하거나 작동하지 않음
⑥ 기타 ( )

D8 귀하는 **개인적인 일상 생활 공간에서 CCTV 또는 IP카메라와 같은 영상 감시 장비를 사용**하고 있습니까?(개인이 직접 설치하고 관리하는 CCTV 또는 IP카메라에 대해서만 응답)

① 예 ② 아니오

E 정보 침해사고 경험과 위협 인식

※ 파트 E의 설문 응답 시 '개인정보 유출 등의 침해사고'를 제외하고 응답해야 합니다.
- 정보 침해사고의 예시로 E2-4의 보기항목을 참고해주십시오.

※ 파트 E의 설문 응답 시 응답 기준시점은 '2024년 1월 1일 ~ 2024년 12월 31일'입니다.

※ 설문에서는 개인의 입장에서 전반적인 '정보보호'에 대한 인식 및 실태를 묻고 있습니다.
개인정보보호를 제외한 '정보보호'를 기준으로 설문에 응답해주시기 바랍니다.

E1 귀하는 **정보보호 관련 사고 발생 시 도움을 받을 수 있는 공식 신고·상담 창구**(118 통합신고센터, 경찰청 사이버범죄 신고시스템 등)를 **알고 계십니까?**

① 예 ② 아니오

E2 귀하는 **최근 1년간 자신의 정보 침해사고를 의심한 적**이 있습니까?
(사고 여부가 확실히 증명된 것은 아니지만, 정황상 직·간접적으로 침해 의심이 되는 경우)

① 예 ② 아니오

E3

귀하는 **최근 1년간 실제 정보 침해사고를 경험한 적**이 있습니까?

① 예 ☞ **E3-1 문항으로 이동**　　② 아니오 ☞ **E5 문항으로 이동**

【E3의 '① 예' 응답자만】

E3-1

귀하가 경험한 침해사고 중 **가장 심각한 침해사고 피해**를 입었을 때, **피해 사실을 인지하기까지 소요된 시간**은 어느 정도입니까?

① 30분 이내　　② 1시간 이내
③ 1일 이내　　④ 7일(일주일) 이내
⑤ 30일(1개월) 이내　　⑥ 90일(3개월) 이내
⑦ 90일(3개월) 초과 → (_____ 일)　　⑧ 알 수 없음

【E3의 '① 예' 응답자만】

E3-2

위 침해사고 경험을 **어떻게 인지**하였습니까?
가장 심각한 침해사고 피해를 기준으로 응답해 주시기 바랍니다.

① 보안 시스템의 침해사고 경보(알림)
② 침해사고 해결 조건으로 대가 요구 및 협박 등을 경험
③ 기존과는 다른 시스템 설정의 변경 또는 보유하고 있는 데이터의 위변조 사항 발견
④ 보안 시스템의 임의적 해제 또는 침입 흔적 발견(물리적 침입 포함)
⑤ 수사기관 또는 정보보호 관련 공공기관으로부터의 협조 요청
⑥ 침해사고 발생한 기업(쇼핑몰·카드사 등) 온라인 서비스포털 등으로부터 침해 안내 메일 또는 문자를 받음
⑦ 언론 보도를 통해 침해사고를 인지함
⑧ 기타 (　　)

【E3의 '① 예' 응답자만】

E3-3

해당 경험의 **사고 피해 심각도**는 어느 정도였습니까?

침해사고는 있었으나, 피해는 매우 경미하다	< ———				보통이다			——— >		단시간에 회복되기 어려운 피해가 있었다
-5	-4	-3	-2	-1	0	+1	+2	+3	+4	+5
매우 경미		경미한 편			보통	심각한 편			매우 심각	

【E3의 '① 예' 응답자만】

E3-3-1

위 침해사고로 인해 **금전적 손실이 발생한 경험**이 있습니까?
(예: 유료 서비스 부정 사용, 사이버 사기 피해, 시스템 장애로 인한 비용 손실 등)

① 예　　② 아니오

【E3의 '① 예' 응답자만】

E3-3-2 위 침해사고를 **복구하기 위해 비용을 지출한 경험**이 있습니까?
(예: PC·스마트폰 수리·교체, 데이터 복구, 보안 프로그램 구입 등)

① 예 ② 아니오

【E3의 '① 예' 응답자만】

E3-4 귀하가 **최근 1년간 경험한 정보 침해사고의 유형**은 무엇입니까? 해당하는 것을 **모두 선택**하여 주십시오.

① PC 또는 노트북 등 개인용 컴퓨터의 해킹과 같은 불법적 접근
② 개인용 모바일 기기(스마트폰, 태블릿, 패드 등)의 해킹과 같은 불법적 접근
③ 랜섬웨어 또는 악성코드 감염 등에 의한 정상적인 전자장비 사용의 제한
④ 개인용 전자기기에 대한 불법적 접근으로 인한 보유 중인 데이터의 외부 유출
⑤ 피싱, 파밍, 스미싱 등에 의한 금전적 피해
⑥ 기타 ( )

【E3의 '① 예' 응답자만】

E3-5 정보 침해사고 경험 이후, **정보 침해사고에 대한 관심도**는 침해사고 이전과 비교했을 때, **어떻게 변화**하였습니까?

관심이 매우 낮아졌다	관심이 낮아졌다	전과 유사하다	관심이 커졌다	관심이 매우 커졌다
①	②	③	④	⑤

【E3의 '① 예' 응답자만】

E4 해당 침해사고가 발생(인지)했을 당시 **관련 기관(**침해사고 발생한 기업(쇼핑몰·카드사 등), 공식 신고·상담 창구 등**)에 피해 사실을 신고**하셨습니까?

① 예 ☞ **E5 문항으로 이동** ② 아니오 ☞ **E4-1 문항으로 이동**

【E4의 '② 아니오' 응답자만】

E4-1 위 침해사고가 발생했을 당시 **피해 사실을 신고하지 않은 이유**는 무엇입니까?
우선 순위대로 최대 2순위까지 선택하여 주십시오.

1순위 **2순위**

① 피해가 심각하지 않았기 때문에
② 신고하는 방법을 몰랐기 때문에
③ 신고에 따른 사건 조사, 처리가 복잡하다고 느껴졌기 때문에
④ 침해 사실과 피해 사실을 사고 발생 이후 뒤늦게 인지했기 때문에(최소 1개월 이상)
⑤ 신고하더라도 피해가 복구되지 못한다고 생각하기 때문에
⑥ 신고하더라도 범인을 체포하거나 처벌할 수 없다고 생각하기 때문에
⑦ 기타 ( )

E5

귀하는 E5-1~E5-7의 **최신 IT 기술을 이용하는 것에 대해 정보 침해 위협으로부터 얼마나 안전하다고 생각하십니까?** 전혀 안전하지 않다고 생각하시면 -5점, 매우 안전하다고 생각하시면 +5점으로 기입하여 주십시오.

전혀 안전하지 않다	<				보통이다				>	매우 안전하다
-5	-4	-3	-2	-1	0	+1	+2	+3	+4	+5
매우 불안전		불안전한 편			보통	안전한 편			매우 안전	

문 항	정보보호 안전성
E4-1. 인공지능을 통한 데이터 분석	
E4-2. 빅데이터 분석을 통한 고객 마케팅	
E4-3. 홈 IoT 장비 등을 활용한 스마트 주거 환경	
E4-4. 자율 주행 차량	
E4-5. 클라우드 컴퓨팅 기술	
E4-6. 핀테크 등의 금융 결제 서비스	
E4-7. 원격 진료, 인공 장기 등과 같은 지능형 헬스케어 기술	

E6

귀하는 E6-1~E6-7의 **최신 IT 기술과 관련된 정보 침해사고가 발생할 경우, 해당 침해사고가 우리 사회에 미치는 피해의 파급효과**는 어느 정도라고 생각하십니까? 매우 클 것으로 생각하시면 -5점, 매우 작을 것으로 생각하시면 +5점으로 기입하여 주십시오.

매우 작다	<				보통이다				>	매우 크다
-5	-4	-3	-2	-1	0	+1	+2	+3	+4	+5
매우 작음		작은 편			보통	큰 편			매우 큼	

문 항	침해사고 피해 파급효과
E5-1. 인공지능을 통한 데이터 분석	
E5-2. 빅데이터 분석을 통한 고객 마케팅	
E5-3. 홈 IoT 장비 등을 활용한 스마트 주거 환경	
E5-4. 자율 주행 차량	
E5-5. 클라우드 컴퓨팅 기술	
E5-6. 핀테크 등의 금융 결제 서비스	
E5-7. 원격 진료, 인공 장기 등과 같은 지능형 헬스케어 기술	

DQ 면접원 기록사항

DQ1 귀 **가구 구성원 전체의 월평균 소득** 합계를 표시해 주십시오.

① 100만 원 미만 ② 100 ~ 200만 원 미만 ③ 200 ~ 300만원 미만
④ 300 ~ 400만 원 미만 ⑤ 400 ~ 500만 원 미만 ⑥ 500 ~ 600만 원 미만
⑦ 600 ~ 700만 원 미만 ⑧ 700만 원 이상

DQ2 귀하의 **최종학력(재학 포함)**을 표시해 주십시오.

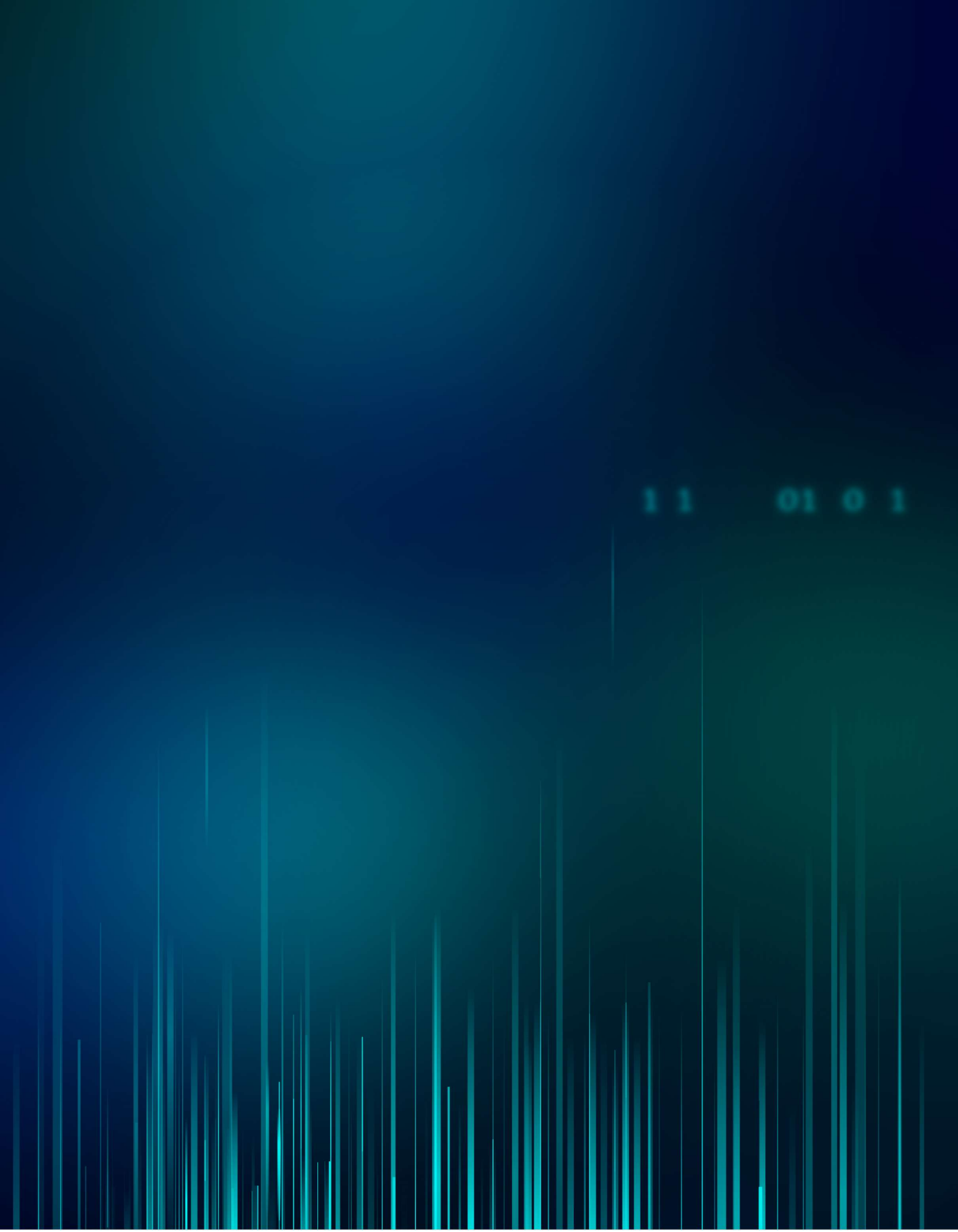
① 무학 ☞ 조사 종료 ② 초등학교 ③ 중학교 ④ 고등학교
⑤ 전문대 ⑥ 대학교 ⑦ 대학원

【DQ3의 ②~⑦ 응답자만】

DQ3 귀하의 **최종학력 이수여부**를 표시해 주십시오.

① 재학 ② 휴학 ③ 중퇴 ④ 수료 ⑤ 졸업

- 끝까지 응답해 주셔서 감사합니다. -



과학기술정보통신부
Ministry of Science and ICT

×

kisia 한국정보보호산업협회
Korea Information Security Industry Association