2022

정보보호 실태조사

SURVEY ON INFORMATION SECURITY

과학기술정보통신부

kisia 한국정보보호산업협회

일러두기

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

2. 통계표 및 도표의 모든 수치는 반올림된 것으로, 세부 항목의 합이 전체 합계와 일치하지 않을 수 있음

3. 일부 업종, 규모별(기업부문), 성, 연령별(개인부문) 통계량의 경우 표본의 크기가 충분치 않아 상대표준오차(변동계수)가 클 수 있으므로 이용 시 주의 바람(부록 1 참조)

4. 통계 및 도표에 사용된 기호의 뜻은 다음과 같음
   0 : 조사결과 값이 0이거나 0에 근사한 경우

5. 복수 응답의 경우, 응답 업체 수를 기준으로 비율을 계산하였으므로 각 항목 비율의 합이 100을 초과할 수 있음

보고서 이용 유의사항

1. 시계열 정보

[기업 부문]

* 기업 부문 조사 모집단의 기준인 '전국사업체조사'가 2021년 이후 1인 이상의 사업체에서 10인 이상의 기업체로 변경됨
* 본 보고서부터 기업부문 조사 기준이 동일하게 변경됨
* 모집단 기준의 변경에 따라 본 보고서는 지난해까지의 데이터와 직접 비교 불가
* 이에 따라 시계열 분석 데이터를 제공하지 않음

2. 개인정보보호 관련 항목

[공통사항]

* 개인정보보호 실태조사와의 중복 회피를 위해 기업 및 개인부문 실사 내용 중 개인정보보호 관련 항목을 일괄 삭제함
* 보고서 내용 중 일부 문항을 제외한 전체 내용은 개인정보보호 관련 사항이 제외된 응답 결과임

작성자 정보

2022 정보보호 실태조사

발 행 처 : 과학기술정보통신부 최고석 사무관
김명호 주무관

수행기관 : 한국정보보호산업협회 조연호 실장
이주영 선임
최다인 선임
안희철 주임

실사기관 : (주)글로벌리서치

발 행 일 : 2023년 3월

기업부문

01 정보보호 중요성 인식

기업체의 **88.9%**가 정보보호가 **중요하다고 인식.**
기업체 규모가 클수록 **정보보호 중요성에 대한 임원의 인식이 높음.**

● 기업 ● 임원 | Base : 전체 | 단위 : %

기업체 규모

정보보호 애로사항 Top 5

Base : 전체 | 단위 : %, 복수응답

정보보호 예산 확보	정보보호 시스템 및 체계 운용 관리	정보보호 전문인력 확보	필요한 정보보호 제품 및 서비스 탐색	정보보호 담당 인력 운용 관리
64.9	55.9	44.7	41.6	39.5

02

정보보호 환경

기업체 **규모가 클수록** 정보보호 정책 및
조직의 **보유율과 정보보호 교육 실시율이 높음.**

Base : 전체 | 단위 : %

정보보호 정책 보유율

정보보호 조직 보유율

정보보호 교육 실시율

기업부문

03 정보보호 인력

정보보호 업무 수행 인력은 평균 1.6명 중 **평균 1.2명**은 **내부인력으로 구성됨.**

정보보호 인력 수

Base : 전체 | 단위 : 명

정보보호 업무 수행 인력		1.6명
부가 업무로 정보보호 업무 수행 인력	IT 직원	1.1명
부가 업무로 정보보호 업무 수행 인력	일반 사무직	1.6명

04 정보보호 예산

기업체 규모가 **클수록** 정보보호 예산 **사용률이 높음**

Base : 정보보호 예산 사용 기업체 | 단위 : %, 복수응답

정보보호 예산 사용률 **67.9%**

정보보호 예산 지출 항목 Top 5

업무 시설의 CCTV 등 영상감시장비 설치 또는 증설	정보보호 제품 및 솔루션의 유지·보수	정보보안을 위한 출동 보안 서비스 이용	정보보호 관련 정보보호 제품 및 솔루션의 구입	정보보호를 위한 전문인력의 고용
64.5	49.2	35.8	31.0	26.2

예산 총액

Base : 정보보호 예산 사용 기업체 | 단위 : %

규모별 예산 사용률

Base : 전체 | 단위 : %

05 정보보안 예방활동

침해사고 예방 제품 및 서비스 이용률

Base : 전체 | 단위 : %

정보보안 제품 및 서비스 유형 Top 5

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

기업부문

06 침해사고

침해사고 경험률

3.7 %

Base : 전체 | 단위 : %

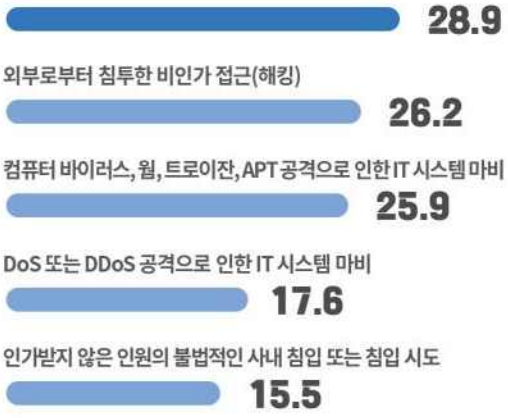
침해사고 신고율

미신고 **94.2 %**

Base : 침해사고 경험한 기업체 | 단위 : %

경험한 침해사고 유형 Top5

Base : 침해사고 경험한 기업체 | 단위 : %, 복수응답



07 침해사고 대응 활동

침해사고를 경험한 기업체의 **55.5%**는 침해사고에 대응하기 위한 **별다른 활동을 수행하지 않음.** 침해사고에 대응하는 활동 중 **'정보보호 관련 제품·솔루션 구축 및 고도화'**가 **24.6%**로 가장 높게 나타남.

침해사고 대응활동 수행률 Top 5

Base : 침해사고 경험한 기업체 | 단위 : %, 복수응답

개인부문

01 정보보호 인식

정보보호 이슈 관심도

Base : 전체 | 단위 : %

남자 59.2

여자 52.9

전체 56.1

10대	45.7
20대	65.2
30대	64.4
40대	57.0
50대	54.5
60대	45.2

정보보호 침해 우려도

Base : 전체 | 단위 : %

남자 62.3

여자 63.3

전체 62.8

10대	59.9
20대	69.4
30대	64.1
40대	65.6
50대	61.4
60대	54.8

정보보호 침해사고 소식에 대한 관련성 인식

Base : 전체 | 단위 : %

남자 48.1

여자 46.7

전체 47.4

10대	33.2
20대	55.4
30대	54.9
40대	51.2
50대	44.9
60대	38.2

정보보호 안전 체감도

Base : 전체 | 단위 : %, 복수응답

전자기기 악성코드 감염	25.9
전자기기 분실 정보 유출	23.2
사생활 침해	29.0
개인 생활 공간 불법 접근	37.7
기타	23.8

02 정보보호 교육 활동

정보보호 교육 경험률

Base : 전체 | 단위 : %

정보보호 교육 경험률 **15.3**

정보보호 교육 방식

Base : 정보보호 교육 경험자 | 단위 : %, 복수응답

근무지 혹은 학교 등에서의 온라인 교육 수강	근무지 혹은 학교 등에서의 오프라인 교육 수강	개인적인 방식으로 온라인 교육 수강	근무지 외 개인적인 방식으로 오프라인 교육 수강
67.3	32.9	21.9	5.8

개인부문

03 정보보호 관련 소비 활동

정보보호 금전 소비 경험률

Base : 전체 | 단위 : %

정보보호 금전 소비 경험률 **13.2**

정보보호 금전 소비 규모

Base : 정보보호 금전 소비 경험자 | 단위 : %

정보보호 금전 소비 비용 증감 여부

Base : 정보보호 금전 소비 경험자 | 단위 : %

정보보호 금전 소비 규모 유지율 **62.8 %**

정보보호 비용 지출 의향

Base : 정보보호 금전 소비 비경험자 | 단위 : %

정보보호 금전 소비 의향 **25.8 %**

정보보호 금전 소비 유형

Base : 정보보호 금전 소비 경험자 | 단위 : %, 복수응답

정보보호 관련 유료 인증서의 결제	정보보호 관련 제품 및 솔루션의 구입	자택·개인 생활 공간의 CCTV 등 영상감시장비 설치/증설	자택·개인 생활 공간을 위한 출동보안 서비스 이용	정보보호 관련 학습 정보 습득	정보보호 관련 과태료 납부
41.1	36.4	22.6	19.6	10.7	6.3

04 침해사고 대응 및 예방조치

침해사고 경험률

Base : 전체 | 단위 : %

침해사고 경험률 **7.5**

침해사고 경험 유형

Base : 침해사고 경험자 | 단위 : %, 복수응답

- PC 또는 노트북 등 개인용 컴퓨터의 해킹과 같은 불법적 접근 **36.8**
- 개인용 모바일 기기(스마트폰, 태블릿, 패드 등)의 해킹과 같은 불법적 접근 **31.8**
- 랜섬웨어 또는 악성코드 감염 등에 의한 정상적인 전자장비 사용의 제한 **27.9**
- 피싱, 파밍, 스미싱 등에 의한 금전적 피해 **20.8**
- 개인 전자기기에 대한 불법적 접근으로 인한 보유 중인 데이터의 외부 유출 **19.4**
- 기타 **8.1**

침해사고 미신고 이유 Top 5

Base : 침해사고 미신고자 | 단위 : %, 복수응답

- 피해가 심각하지 않았기 때문에 **59.2**
- 신고에 따른 사건 조사, 처리가 복잡하고 불편하다고 느껴졌기 때문에 **34.3**
- 신고하더라도 범인을 체포하거나 처벌할 수 없다고 생각하기 때문에 **31.1**
- 신고하더라도 피해가 복구되지 못한다고 생각하기 때문에 **24.3**
- 신고할 수 있다는 사실을 몰랐기 때문에 **16.1**

침해사고 피해 심각도

Base : 침해사고 경험자 | 단위 : %

경미함	보통	심각함
44.7	15.9	39.4

침해사고 신고율

Base : 침해사고 경험자 | 단위 : %

침해사고 신고율 **38.6**

1 기업 부문

CONTENTS

CONTENTS

CONTENTS

2 개인 부문

CONTENTS

그림 목차

제1부 기업 부문

CONTENTS

CONTENTS

제2부 개인 부문

CONTENTS

제 1 부

기업부문

제 1 장

조사개요

1

1 조사 목적

- 급속하게 변화하는 인터넷 환경과 사물인터넷(IoT), IP카메라, 인공지능(AI) 등 새로운 기술의 끊임없는 등장으로 사이버 세계의 위협이 현실세계로 확대되고 그 위협 또한 고도화·지능화 되고 있다. 이에 따라 정보보호와 관련된 현황 및 인터넷 이용자들의 인식 수준, 대응활동 등을 파악하고, 인터넷 이용자의 정보보호 수준 제고에 활용하고자 정보보호 실태조사를 실시하였다.
- 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 제공하는 데 그 목적이 있다.
- 본 조사의 구체적인 목적은 다음과 같다.

  1. 정부, 기업, 개인 등 사회구성원 전체의 정보보호 수준 제고에 활용하기 위한 기초자료 제공
  2. 국가정보보호백서, 한국인터넷백서 등의 정보보호 통계자료 제공
  3. 국제기구(OECD)의 ICT 통계지표 기초자료 제공
  4. 업계 및 학계의 현장, 연구활동 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
- 조사결과의 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)
- 승인번호 제342005호로 변경

2017년
- ICT 환경변화에 따른 정보보호 이슈를 반영하기 위해 정보보호(사이버) 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
- ‘2017년 기준 전국사업체조사’와 ‘2018년 정보화통계조사’결과를 기반으로 표본 재설계

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

3 조사 내용 및 범위

- 본 조사는 국내 기업체의 정보보호 기반 및 환경, 침해사고 예방, 침해사고 경험 및 대응, 정보보호 인식 등 실태를 파악할 수 있는 지표로 구성하였다.

  본 조사의 주요 내용은 다음과 같다.

  1. 정보보호 인식
  2. 정보보호 정책 및 조직
  3. 정보보호 교육
  4. 정보보호 예산
  5. 침해사고 예방
  6. 침해사고 경험
  7. 사이버 보험
  8. 재택근무

4 주요 용어 및 정의

- **정보보호** : 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 활동
- **개인정보보호** : 특정 개인을 알아볼 수 있는 정보(성명, 주민등록번호, 영상정보 등)가 유출되는 위협으로부터 보호하는 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 점검** : 시스템, 네트워크, 혹은 물리적 시설의 소프트웨어나 하드웨어상의 문제로 인해 해커가 공격하는데 이용할 수 있는 보안상의 문제점을 찾아내는 활동
- **보안패치** : 운영체제(OS)나 응용 프로그램에 내재된 보안 취약점을 보완하는 소프트웨어
- **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 정보 통신망 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
- **침해사고대응팀(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(정보보호) 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** : 6,500개
- **조사주기** : 연 1회
- **조사기간** : 2022년 9월 28일 ~ 11월 23일 (2개월)
- **조사방법** : 기업체 방문 면접조사(이메일, 팩스 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『2021년 기준 기업통계등록부』의 업종별, 규모별 기업체 수 및 분포 결과와 한국정보화진흥원『2021년 정보화통계조사』결과에서 파악된 네트워크 구축 비율을 이용
- **규모(종사자 수)** : 10 ~ 49명/50 ~ 249명/250 ~ 999명/1,000명 이상

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

표 1-1-1 업종 분류 기준

한국표준산업분류 (10차 개정)	업종 분류기준 (본 조사)	국제기구 분류기준 (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 오토바이 도매업 제외*
		소매업 (ISIC G); *자동차 및 오토바이 소매업 제외*
H. 운수업 및 창고업	6. 운수업 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)
		사업관리 및 지원서비스업 (ISIC N)
M. 전문, 과학 및 기술 서비스업	11. 전문, 과학 및 기술서비스업	전문, 과학 및 기술 서비스업 (M75 수의업 제외)
N. 사업시설관리, 사업지원 및 서비스업	12. 사업시설관리, 사업지원 및 서비스업	사업관리 및 지원서비스업(ISIC N)
P. 교육 서비스업	13. 교육 서비스업	-
Q. 보건업 및 사회복지서비스업	14. 보건업 및 사회복지서비스업	-
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

표 1-1-2 종사자 규모별 적용 기준

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

• 모집단 분포

- 『2021년 기준 기업통계등록부(SBR)』 및 한국지능정보사회진흥원 『2021년 정보화통계조사』에서 조사된 기업체 중 종사자 수 10명 이상 기업체 현황 및 분포는 다음과 같이 나타남

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

구분	업종/규모	기업체 수	컴퓨터 보유/ 네트워크 구축 기업체수
업종별	1. 농림수산업(광업포함)	2,896	1,733
	2. 제조업	81,277	63,982
	3. 전기,가스,증기 및 공기조절 공급업/수도, 하수·폐기물 처리, 원료재생업	3,528	2,425
	4. 건설업	39,200	32,347
	5. 도매 및 소매업	34,323	29,121
	6. 운수업 및 창고업	8,786	7,959
	7. 숙박 및 음식점업	11,011	8,402
	8. 정보통신업	11,963	11,437
	9. 금융 및 보험업	4,124	4,089
	10. 부동산업	6,051	4,749
	11. 전문, 과학 및 기술서비스업	20,560	18,811
	12. 사업시설관리, 사업지원 및 서비스업	15,873	11,821
	13. 교육 서비스업	2,880	2,456
	14. 보건업 및 사회복지서비스업	13,166	12,389
	15. 예술, 스포츠 및 여가관련 서비스업	1,644	1,363
	16. 협회, 단체, 수리 및 기타 개인서비스업[협회 및 단체 제외]	5,399	4,107
규모별	10 ~ 49명	230,046	185,056
	50 ~ 249명	27,903	27,445
	250 ~ 999명	3,844	3,802
	1,000명 이상	888	888

※ 출처: 『2021년 기준 기업통계등록부(SBR)』(통계청), 『2021년 정보화통계조사』(한국지능정보사회진흥원)

표 1-1-4 업종*규모별 모집단 분포

업종 분류	규모 분류	컴퓨터 보유/네트워크 구축 기업체	구성비	업종 분류	규모 분류	컴퓨터 보유/네트워크 구축 기업체	구성비
농림수산업 (광업포함)	10~49명	1,619	0.75	금융 및 보험업	10~49명	2,768	1.27
	50~249명	106	0.05		50~249명	1,090	0.50
	250~999명	6	0.00		250~999명	156	0.07
	1,000명 이상	2	0.00		1,000명 이상	75	0.03
제조업	10~49명	55,069	25.36	부동산업	10~49명	3,991	1.84
	50~249명	7,965	3.67		50~249명	554	0.26
	250~999명	840	0.39		250~999명	143	0.07
	1,000명 이상	108	0.05		1,000명 이상	61	0.03
전기,가스, 증기 및 공기조절 공급업/수도, 하수·폐기물 처리,원료 재생업	10~49명	2,085	0.96	전문, 과학 및 기술 서비스업	10~49명	15,397	7.09
	50~249명	307	0.14		50~249명	2,689	1.24
	250~999명	25	0.01		250~999명	547	0.25
	1,000명 이상	8	0.00		1,000명 이상	178	0.08
건설업	10~49명	28,556	13.15	사업시설 관리, 사업지원 및 서비스업	10~49명	7,957	3.66
	50~249명	3,258	1.50		50~249명	2,967	1.37
	250~999명	448	0.21		250~999명	715	0.33
	1,000명 이상	85	0.04		1,000명 이상	182	0.08
도매 및 소매업	10~49명	26,518	12.21	교육 서비스업	10~49명	2,275	1.05
	50~249명	2,248	1.04		50~249명	149	0.07
	250~999명	278	0.13		250~999명	30	0.01
	1,000명 이상	77	0.04		1,000명 이상	2	0.00
운수업 및 창고업	10~49명	5,951	2.74	보건업 및 사회복지 서비스업	10~49명	10,323	4.75
	50~249명	1,753	0.81		50~249명	1,972	0.91
	250~999명	211	0.10		250~999명	92	0.04
	1,000명 이상	44	0.02		1,000명 이상	2	0.00
숙박 및 음식점업	10~49명	8,038	3.70	예술, 스포츠 및 여가관련 서비스업	10~49명	1,144	0.53
	50~249명	307	0.14		50~249명	200	0.09
	250~999명	48	0.02		250~999명	13	0.01
	1,000명 이상	9	0.00		1,000명 이상	6	0.00
정보통신업	10~49명	9,404	4.33	협회, 단체, 수리 및 기타 개인 서비스업 [협회 및 단체 제외]	10~49명	3,961	1.82
	50~249명	1,749	0.81		50~249명	131	0.06
	250~999명	238	0.11		250~999명	12	0.01
	1,000명 이상	46	0.02		1,000명 이상	3	0.00
총 합계						217,191	100.0

※ 출처: 『2021년 기준 기업통계등록부(SBR)』(통계청), 『2021년 정보화통계조사』(한국지능정보사회진흥원)

나 표본추출

- **개요** : 다단계층화계통추출법

  - 업종·규모별로 2단 층화한 후 각 기업체들을 지역별로 정렬하여 계통추출

- **표본의 규모산정**

  - 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,

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

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

p_h : 층 h의 "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 표본크기를 결정하며, 허용오차에 따른 표본의 크기는 아래와 같음

표 1-1-5 표본오차별 표본의 크기

(단위: 개, %)

표본 크기	7,827	6,386	5,306	4,476	3,826	3,307
표본 오차	0.9	1.0	1.1	1.2	1.3	1.4

- 최종 표본의 크기는 표본오차가 1.0% 내외가 되도록 6,500개로 결정함

- **표집틀(Sampling frame)**
  - 1차 표집틀 : 『2021년 기준 기업통계등록부』 대상 기업체
  - 2차 표집틀 : 『2021년 정보화통계조사』 대상 기업체 중 10인 이상 네트워크 구축 기업체
- **표본할당 및 추출방법**
  - 멱등할당(Power allocation) : 2021년도 정보보호 실태조사 결과 중 '공식문서화된 정보보호 정책 수립 여부'에 대한 추정량을 이용하여 표본오차를 계산하고, p=0.4 인 경우를 최종 할당으로 결정
  - 절사추출 : 종사자 수가 1,000명 이상인 기업체와 250~999명인 기업체 일부 전수 조사 실시

7 실사

가 실사 개요

- **조사기간**
  - 2022년 9월 28일 ~ 11월 23일 (2개월)
- **조사기준 시점**
  - 2021년 12월 31일
  - 교육 실시, 예산, 침해사고 경험, 재택근무 경험은 2021년 1월 1일 ~ 12월 31일
  - 현재 시스템 및 네트워크 보안 점검 실시 시점은 2022년 7월 1일
- **조사대상**
  - 네트워크에 연결된 컴퓨터 보유 기업체(종사자 수 10인 이상)
- **조사방법**
  - 전문 조사원이 표본으로 선정된 기업체를 방문하여 설문에 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 6,500개를 대상으로 조사하는 것을 원칙으로 하며, 해당 기업체의 휴폐업 및 강력한 응답 거부 등으로 조사가 불가능한 경우에는 동일한 업종, 규모 특성으로 추출된 예비 표본으로 대체하여 조사 진행

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 검증 실시
  - 실사 감독원의 1차 검증에서 합격된 설문지는 에디팅 및 입력 과정에서 전산 프로그램에 의해 2차 검증
  - 입력된 자료는 자료 처리 과정에서 내검 프로그램에 의해 3차 검증
  - 검증 단계별로 불합격된 설문지에 대한 보완조사 및 재조사 실시
- **분석 과정에서 자료 검증**
  - 동일한 업종·규모별 평균치 및 이전 조사결과와의 시계열 비교 및 검증 실시
- **무응답 대체**
  - 단위무응답 및 항목무응답 발생 시 해당 기업체 방문 및 전화 재조사를 통하여 무응답률 최소화
  - 단위무응답 발생 시 예비 표본의 범위 내에서 대체하여 단위무응답 제거
  - 항목무응답 발생 시 결측값을 해당 기업체 특성(업종, 규모)과 동일한 그룹의 평균값으로 대체하여 항목무응답 제거

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 분석

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 사후층화(post-stratification) 방법을 이용하여 모집단과 표본 간 편차 최소화 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 $\hat{Y}= Y_{\text{전수층}} + \hat{Y}_{\text{표본층}}$ 를 추정 표본설계 시 모집단을 전수층과 표본층으로 구분하였으므로 모집단 총계는 다음과 같이 추정함

$$\hat{Y} = \sum_{h=1}^{L} {}_{c}Y_h + \sum_{h=1}^{L} \frac{{}_{s}N_h}{{}_{s}n_h} \sum_{k=1}^{{}_{s}n_h} y_{hsk}$$

여기에서 ${}_{c}Y_h$: 전수층 총계

L : 층의 개수 (업종×규모)

${}_{s}N_h$: 표본층 h의 모집단 크기

${}_{s}n_h$: 표본층 h의 표본 크기

${}_{s}y_{hk}$: 표본층 h의 k번째 관찰값

$\frac{{}_{s}N_h}{{}_{s}n_h}$: 표본층 h의 가중치

${}_{c}\hat{Y}_h$: 전수층에서 각 층의 총계에 대한 추정량의 합계

${}_{s}\hat{Y}_h$: 표본층에서 각 층의 총계에 대한 추정량의 합계

나 추정

- 전체 모비율 추정 산출 공식은 다음과 같음

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

다 표본오차

- **모집단 총계의 분산 및 표본오차 추정**
  - 모총계 추정량에 대한 분산 추정(표본층에서만 표본오차가 발생)

$$\hat{Var}(\hat{Y}) = \hat{Var}\left(\sum_{h=1}^{L}\frac{{}_sN_h}{{}_sn_h}\sum_{k=1}^{{}_sn_h}y_{hsk}\right)$$

$$= \sum_{h=1}^{L}\left(\frac{{}_sN_h}{{}_sn_h}\right)^2\frac{1}{{}_sn_h-1}\sum_{k=1}^{{}_sn_h}({}_sy_{hk}-{}_s\bar{y}_h)^2$$

- **모집단 분산 및 표본오차 추정**
- 표본층에서만 표본오차가 발생

$$\hat{P}_{st} = \frac{\hat{Y}}{N} = \frac{\sum_{h=1}^{L}{}_c\hat{Y}_h + \sum_{h=1}^{L}\frac{{}_sN_h}{{}_sn_h}\sum_{k=1}^{{}_sn_h}{}_sy_{hk}}{N}$$

$$\hat{V}(\hat{p}_{st}) = \sum_{h=1}^{L}(\frac{{}_sN_h}{N})^2(1-\frac{{}_sn_h}{{}_sN_h})\frac{{}_s\hat{p}_h\,{}_s\hat{q}_h}{{}_sn_h-1}$$

여기에서 ${}_s\hat{p}_h$: h층에서 표본 비율

$${}_s\hat{q}_h = 1-{}_s\hat{p}_h$$

표 1-1-6 정보보호 정책 수립률 추정 결과 및 표본오차

정보보호 정책 수립률 표본오차	±0.88%p (95% 신뢰수준)
정보보호 정책 수립률 추정 결과	35.3% ± 0.88%p

10 결과 공표 및 활용 분야

- 『2022년 정보보호실태조사(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

업종 분류	규모 분류	컴퓨터 보유/네트워크 구축 기업체		조사표본 기업체	
		기업체 수	비율	기업체 수	비율
농림수산업 (광업포함)	10~49명	1,619	0.75	52	0.80
	50~249명	106	0.05	31	0.48
	250~999명	6	0.00	4	0.06
	1,000명 이상	2	0.00	1	0.02
제조업	10~49명	55,069	25.36	281	4.32
	50~249명	7,965	3.67	270	4.15
	250~999명	840	0.39	185	2.85
	1,000명 이상	108	0.05	101	1.55
전기,가스, 증기 및 공기조절 공급업/수도, 하수·폐기물 처리,원료 재생업	10~49명	2,085	0.96	67	1.03
	50~249명	307	0.14	76	1.17
	250~999명	25	0.01	19	0.29
	1,000명 이상	8	0.00	6	0.09
건설업	10~49명	28,556	13.15	223	3.43
	50~249명	3,258	1.50	180	2.77
	250~999명	448	0.21	136	2.09
	1,000명 이상	85	0.04	83	1.28
도매 및 소매업	10~49명	26,518	12.21	200	3.08
	50~249명	2,248	1.04	170	2.62
	250~999명	278	0.13	120	1.85
	1,000명 이상	77	0.04	70	1.08
운수업 및 창고업	10~49명	5,951	2.74	175	2.69
	50~249명	1,753	0.81	166	2.55
	250~999명	211	0.10	108	1.66
	1,000명 이상	44	0.02	33	0.51
숙박 및 음식점업	10~49명	8,038	3.70	105	1.62
	50~249명	307	0.14	87	1.34
	250~999명	48	0.02	23	0.35
	1,000명 이상	9	0.00	6	0.09
정보통신업	10~49명	9,404	4.33	153	2.35
	50~249명	1,749	0.81	154	2.37
	250~999명	238	0.11	113	1.74
	1,000명 이상	46	0.02	38	0.58

업종 분류	규모 분류	컴퓨터 보유/네트워크 구축 기업체		조사표본 기업체	
		기업체 수	비율	기업체 수	비율
금융 및 보험업	10~49명	2,768	1.27	118	1.82
	50~249명	1,090	0.50	122	1.88
	250~999명	156	0.07	104	1.60
	1,000명 이상	75	0.03	75	1.15
부동산업	10~49명	3,991	1.84	93	1.43
	50~249명	554	0.26	103	1.58
	250~999명	143	0.07	92	1.42
	1,000명 이상	61	0.03	58	0.89
전문, 과학 및 기술 서비스업	10~49명	15,397	7.09	181	2.78
	50~249명	2,689	1.24	182	2.80
	250~999명	547	0.25	160	2.46
	1,000명 이상	178	0.08	174	2.68
사업시설 관리, 사업지원 및 서비스업	10~49명	7,957	3.66	142	2.18
	50~249명	2,967	1.37	188	2.89
	250~999명	715	0.33	183	2.82
	1,000명 이상	182	0.08	178	2.74
교육 서비스업	10~49명	2,275	1.05	80	1.23
	50~249명	149	0.07	92	1.42
	250~999명	30	0.01	20	0.31
	1,000명 이상	2	0.00	1	0.02
보건업 및 사회복지 서비스업	10~49명	10,323	4.75	151	2.32
	50~249명	1,972	0.91	155	2.38
	250~999명	92	0.04	71	1.09
	1,000명 이상	2	0.00	2	0.03
예술, 스포츠 및 여가관련 서비스업	10~49명	1,144	0.53	95	1.46
	50~249명	200	0.09	71	1.09
	250~999명	13	0.01	5	0.08
	1,000명 이상	6	0.00	3	0.05
협회, 단체, 수리 및 기타 개인 서비스업 [협회 및 단체 제외]	10~49명	3,961	1.82	89	1.37
	50~249명	131	0.06	65	1.00
	250~999명	12	0.01	9	0.14
	1,000명 이상	3	0.00	2	0.03
합계		217,191	100.0	6,500	100.0

01 정보보호 인식 | 02 정보보호 정책 및 조직 | 03 정보보호 교육 | 04 정보보호 예산
05 침해사고 예방 | 06 침해사고 경험

제 2 장

조사결과 요약

2

Ⅰ 정보보호 인식

1 정보보호 인식

» 기업의 정보보호 중요성 인식률 88.9%, 임원의 정보보호 중요성 인식률 63.4%

- 국내 기업체 88.9%가 정보보호의 중요성에 대해 인식하고 있고, 기업 임원들의 63.4%가 정보보호를 중요하게 인식한다고 응답함
  - — 정보보호 관련 애로사항으로 '정보보호 예산 확보'가 64.9%로 가장 높고, '정보보호 시스템 및 체계 운용 관리(55.9%)', '정보보호 전문인력 확보(44.7%)' 등의 순으로 조사됨

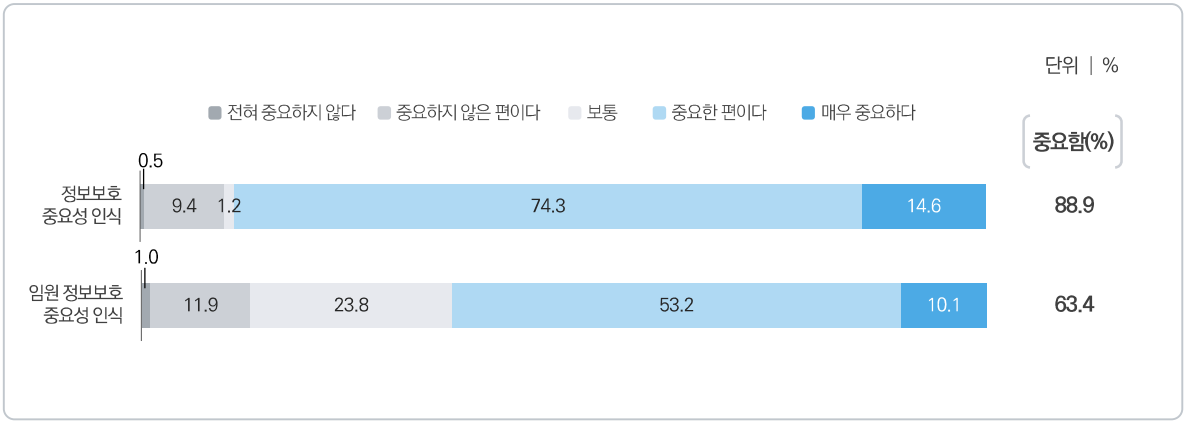


그림 1-2-1 기업·임원 정보보호 중요성 인식률

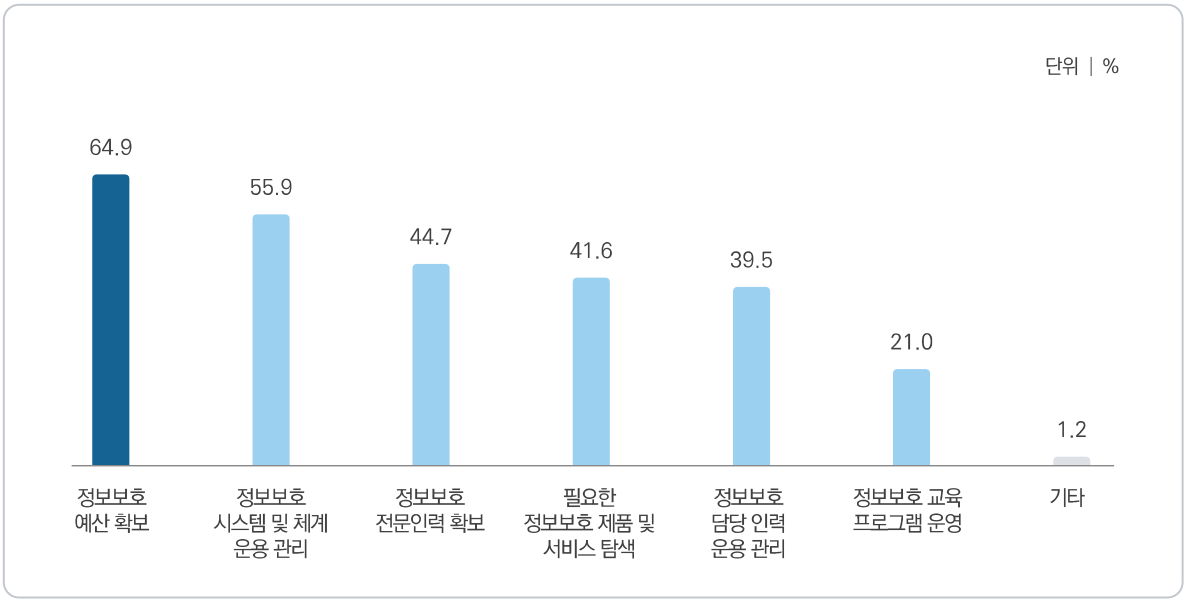


그림 1-2-2 정보보호 애로사항(복수응답)

Ⅱ 정보보호 정책 및 조직

1 정보보호 정책

» 기업체의 35.3%는 정보보호 정책 보유

- 기업체의 35.3%는 정보보호 정책을 보유하고 있는 것으로 조사되었으며, 79.2%의 기업은 정보보호 정책에 개인정보보호 규정을 포함하는 것으로 나타남

  — 규모별로 '250명 이상(85.6%)' 기업체의 정책 보유율이 가장 높게 나타남

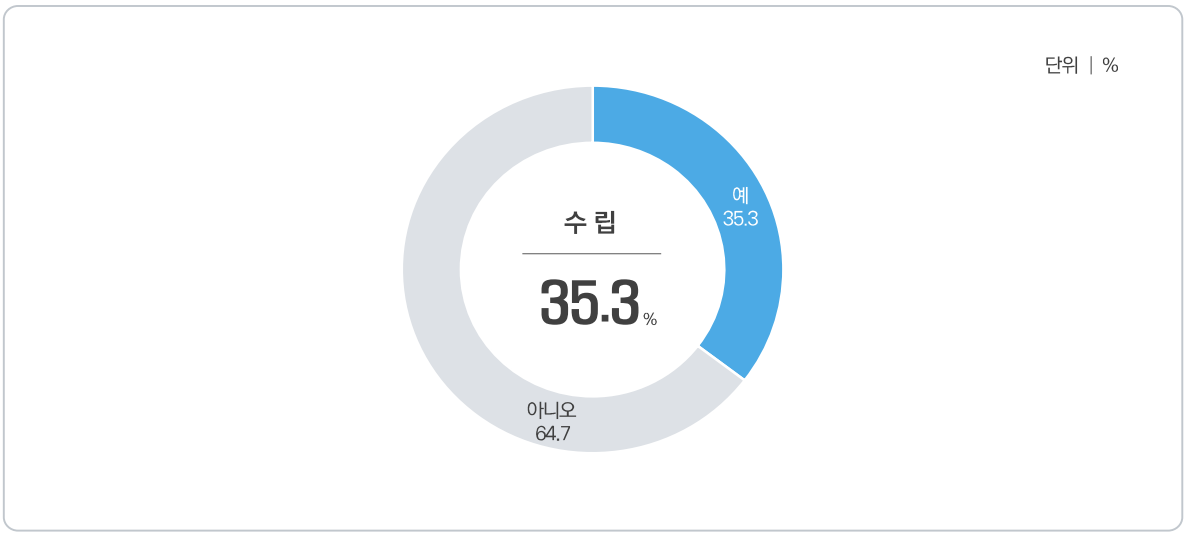


그림 1-2-3 정보보호 정책 보유율

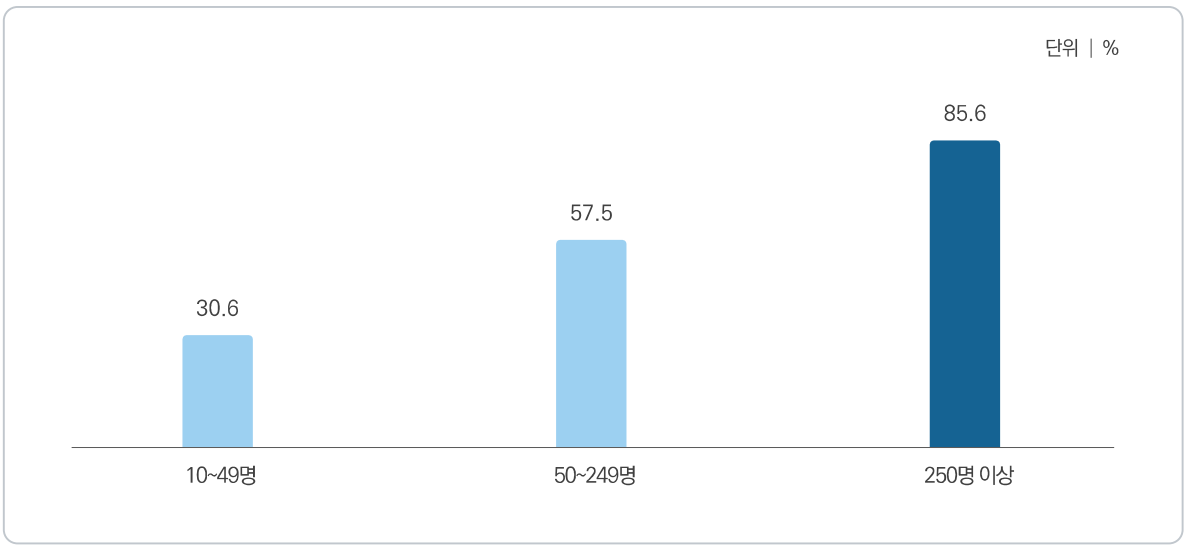


그림 1-2-4 규모별 정보보호 정책 보유율

2 정보보호 조직

» 기업체의 40.3%는 정보보호 조직 보유

- 기업체의 40.3%는 정보보호 조직을 보유하고 있고, 조직 운영 방식은 '전담조직'이 6.9%, '겸임조직'이 33.4%로 나타남
  - 규모별로 '250명 이상(79.1%)' 기업체의 정보보호 조직 보유율이 가장 높고, 규모가 커질수록 전담 비율이 높음

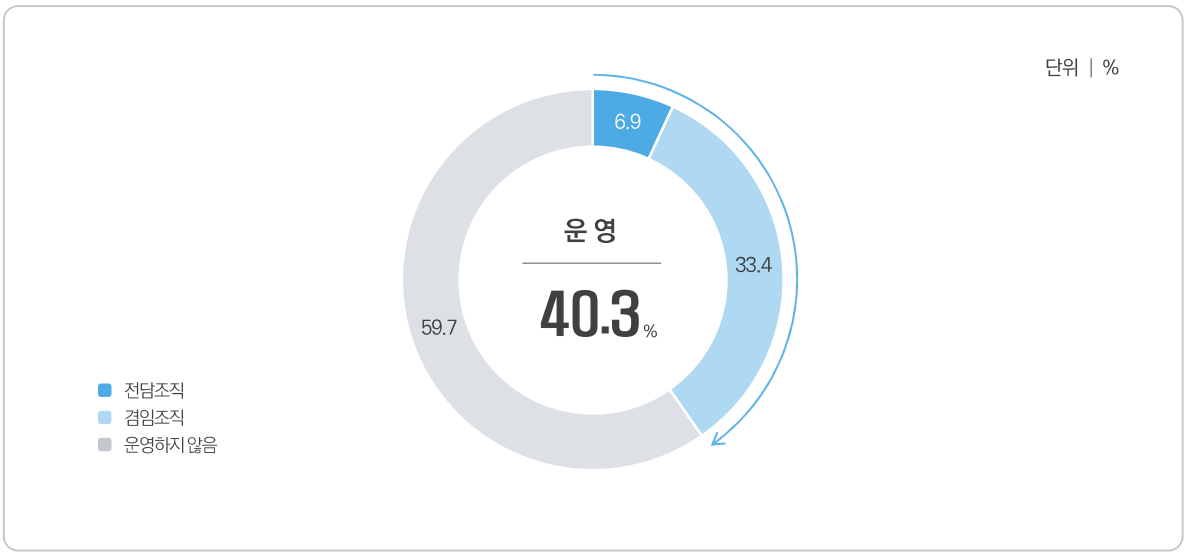


그림 1-2-5 정보보호 조직 보유율

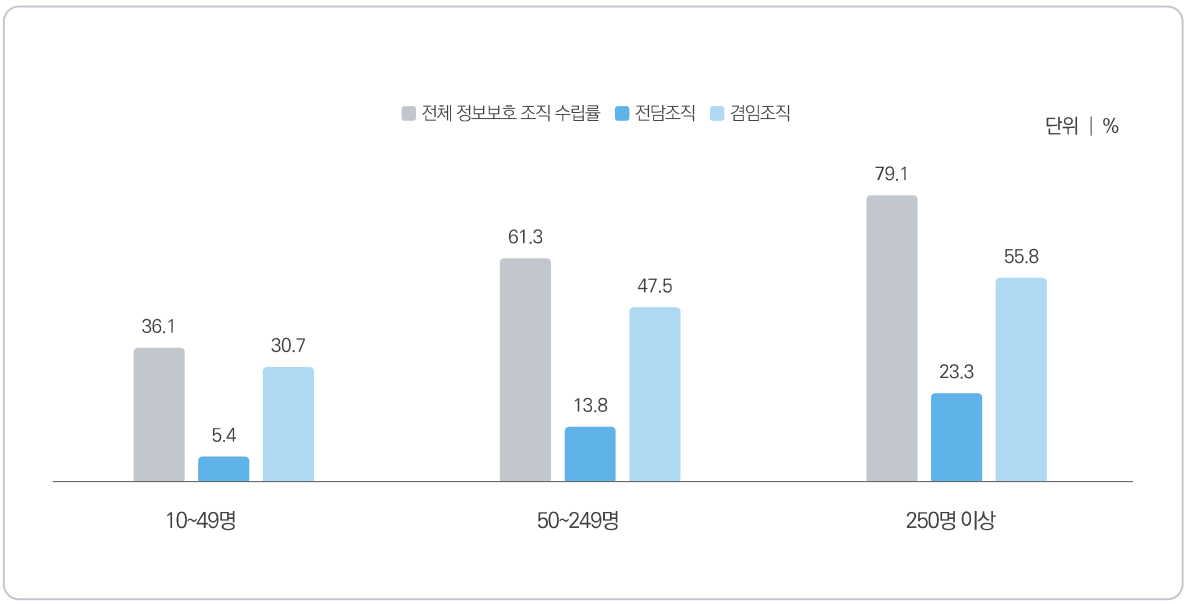


그림 1-2-6 규모별 정보보호 조직 보유율

3 정보보호 관련 인력

» 정보보호 업무 수행 인력은 평균 1.6명, 이 중 내부 인력은 평균 1.2명

- 기업체 당 평균적으로 정보보호 업무를 수행하는 인력수는 약 1.6명으로 이 중 내부 인력은 1.2명, 외부 인력은 0.4명으로 조사됨
  - — 부가 업무로 정보보호 업무를 수행하는 IT 인력은 약 1.1명(내부 인력 0.8명, 외부 인력 0.3명), 일반 사무직 인력은 약 1.6명(내부 인력 1.3명, 외부 인력 0.3명)으로 나타남

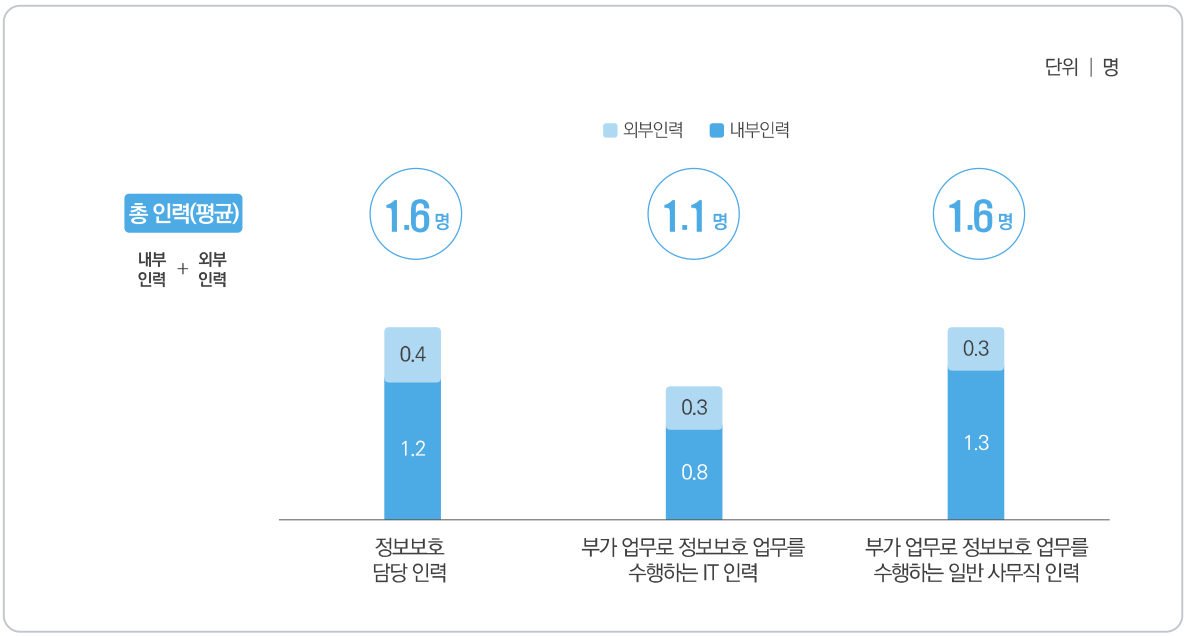


그림 1-2-7 정보보호 관련 인력

Ⅲ 정보보호 교육

1 정보보호 교육

» 기업체의 32.6%는 정보보호 교육 실시

- 기업체의 32.6%는 정보보호 교육을 실시하는 것으로 조사됨
  - — 규모별로 '250명 이상(69.8%)' 기업체의 교육 실시율이 가장 높게 나타남

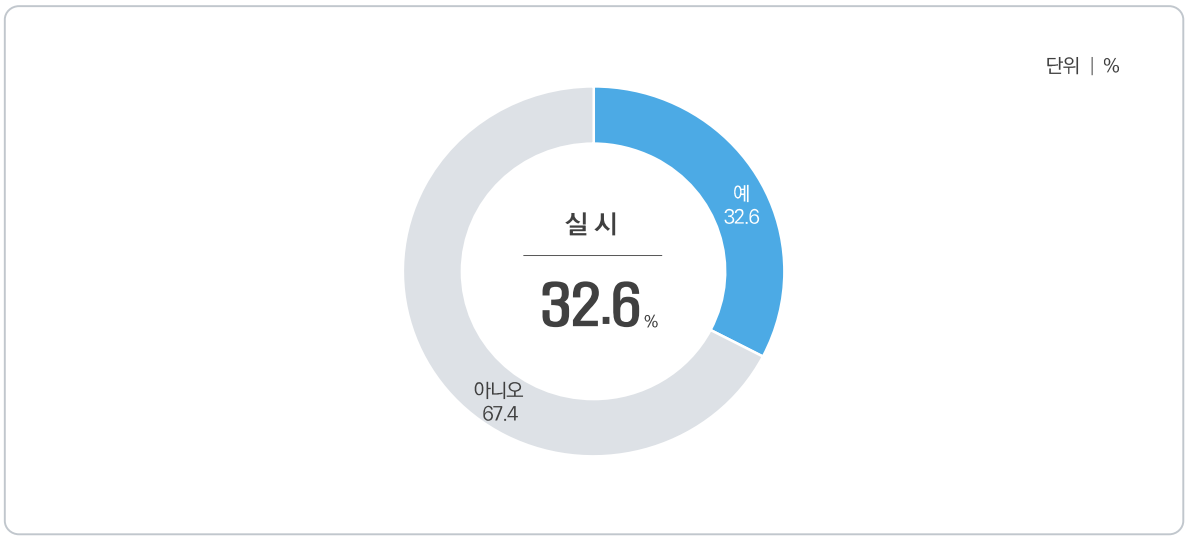


그림 1-2-8 정보보호 교육 실시율

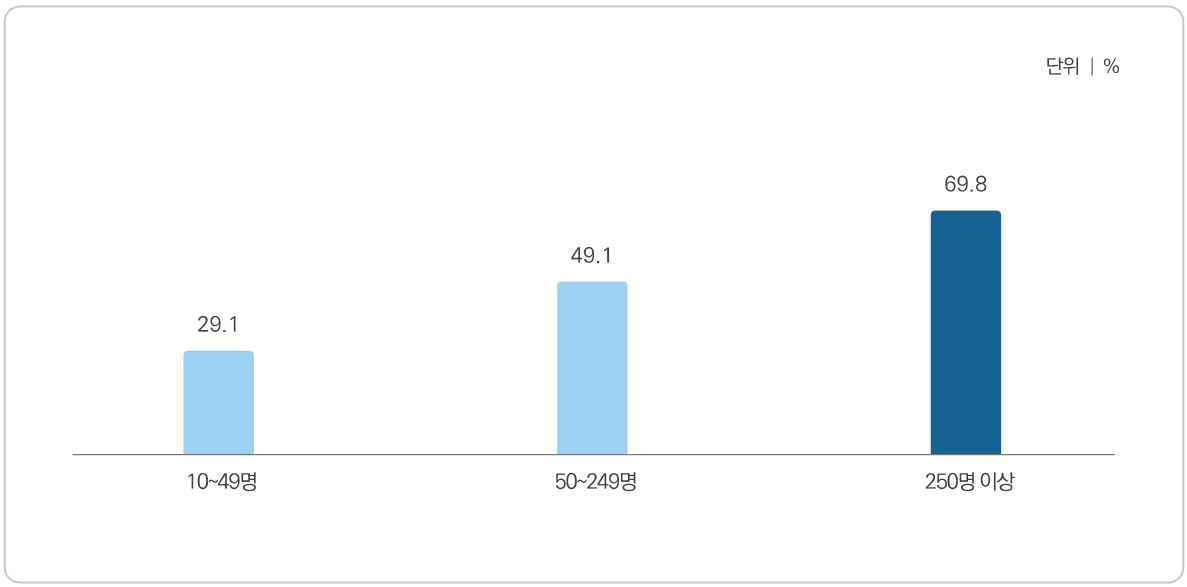


그림 1-2-9 규모별 정보보호 교육 실시율

Ⅳ 정보보호 예산

1 정보보호 예산

» 정보보호 예산 사용 경험 67.9%, 총액은 '1,000만원 이상 ~ 5,000만원 미만' 59.1%

- 기업체의 67.9%는 최근 1년간 정보보호 관련 예산 사용 경험이 있는 것으로 조사되었고, 예산 사용 경험이 있는 기업체 중 59.1%는 정보보호 예산 총액이 '1,000만 원 이상 ~ 5,000만 원 미만'인 것으로 나타남

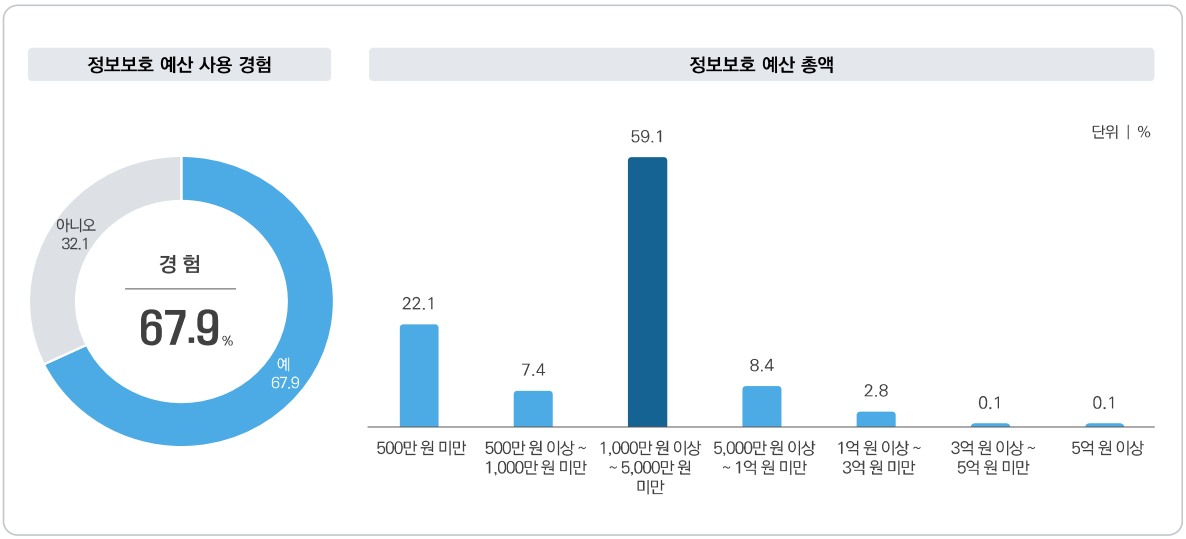


그림 1-2-10 정보보호 예산 사용 경험 – 전체 / 예산 총액 – 정보보호 예산 사용 기업체

» 정보보호 예산 활용 분야는 '영상감시장비'를 위한 예산 활용'이 64.5%로 가장 높음

— 정보보호 예산 활용 분야는 '업무 시설의 CCTV 등 영상감시장비 설치 또는 증설(유지 · 보수 포함)(64.5%)', '정보보호 관련 제품 및 솔루션의 유지·보수(49.2%)', '정보보안을 위한 출동 보안 서비스 이용(35.8%)', '정보보호 관련 제품 및 솔루션의 구입(31.0%)' 등의 순으로 나타남

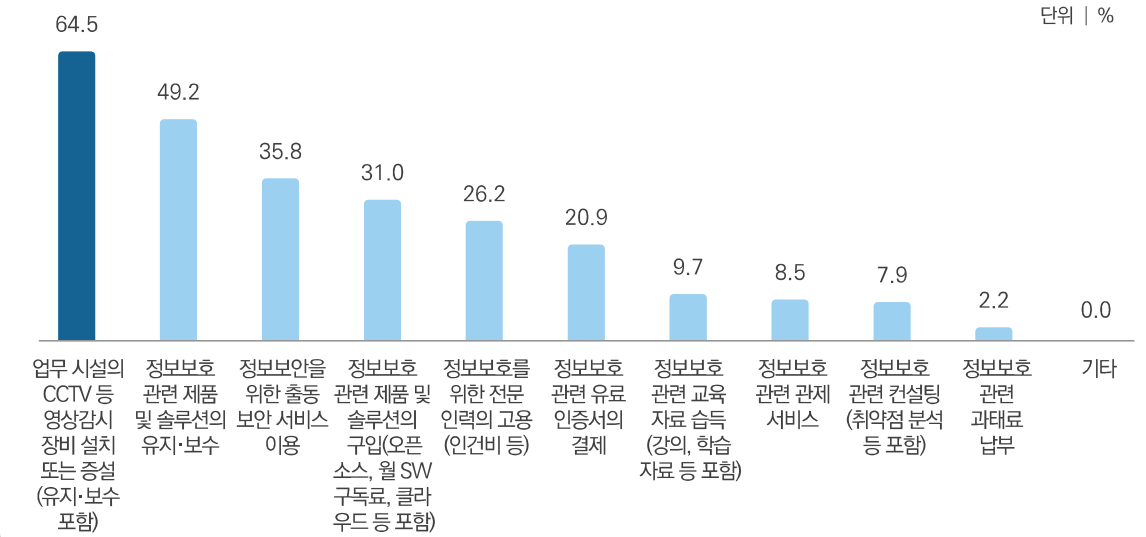


그림 1-2-11 정보보호 예산 활용 분야(복수응답) – 정보보호 예산 사용 기업체

V 침해사고 예방

1 정보보호 제품 및 솔루션

» 정보보호 침해사고 예방을 위한 제품 및 솔루션 이용 경험 80.7%

- 기업체의 80.7%는 정보보호 침해사고 예방을 위한 제품 및 솔루션을 이용한 경험이 있다고 조사됨

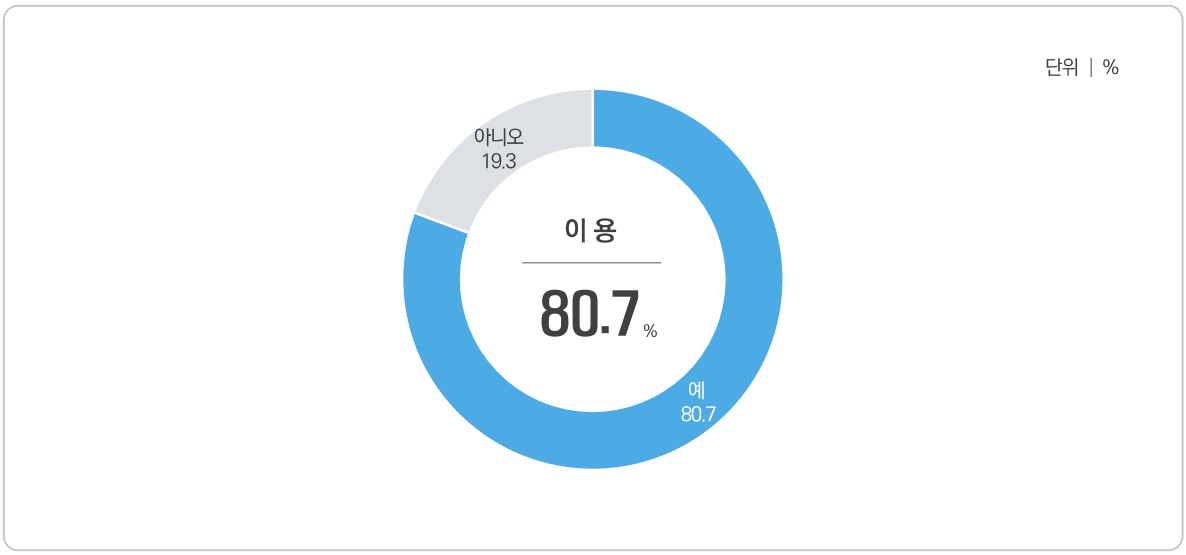


그림 1-2-12 정보보호 제품 및 솔루션 이용 경험

» 이용한 정보보안 제품 및 솔루션 중 '시스템 보안 장비'가 73.6%를 차지

- '시스템(앤드 포인트) 보안 장비'를 이용한 경우가 73.6%로 가장 높게 나타남
  - 다음으로 '네트워크 보안 장비(62.1%)', '보안 시스템 유지/관리 서비스(9.6%)', '콘텐츠/데이터 보안/정보유출 방지 장비(8.6%)' 등의 순으로 나타남

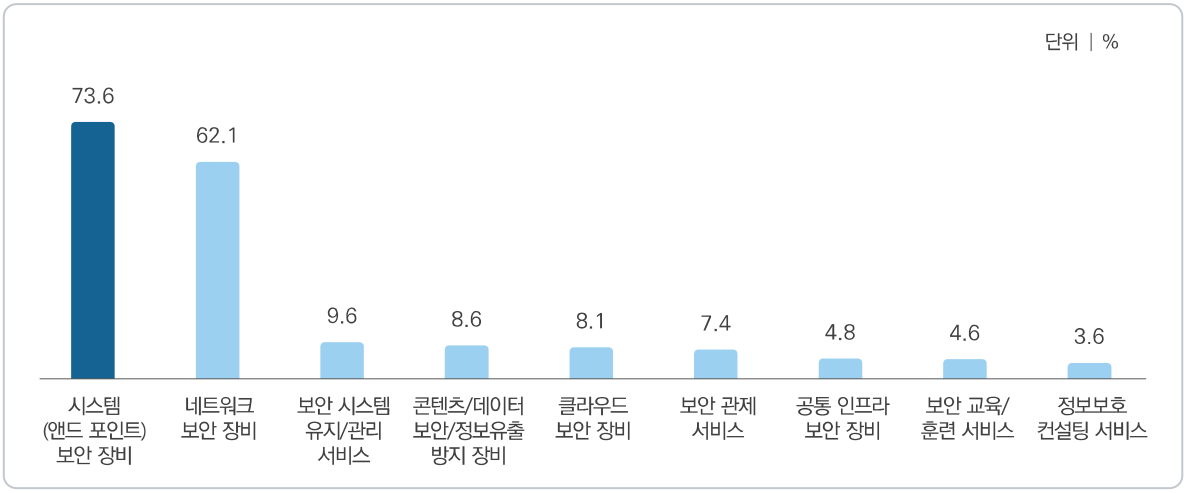


그림 1-2-13 이용한 정보보호 제품 및 솔루션_정보보안(복수응답) - 정보보호 제품 및 솔루션 사용 기업체

» 이용한 물리보안 제품 및 솔루션 중 '출입통제 관리 시스템'이 77.7%를 차지

- '출입통제 관리 시스템(출입통제 게이트, 디지털 도어락)'을 이용한 경우가 77.7%로 가장 높게 나타남
  - 다음으로 '영상 보안 시스템(IP카메라, CCTV 등)(48.8%)', '출동 보안 서비스(사설 경비 업체 등)(43.2%)', '불법 도·감청 탐지 서비스(몰래카메라, 초소형 도청장치 등 탐지)(2.8%)'의 순으로 나타남

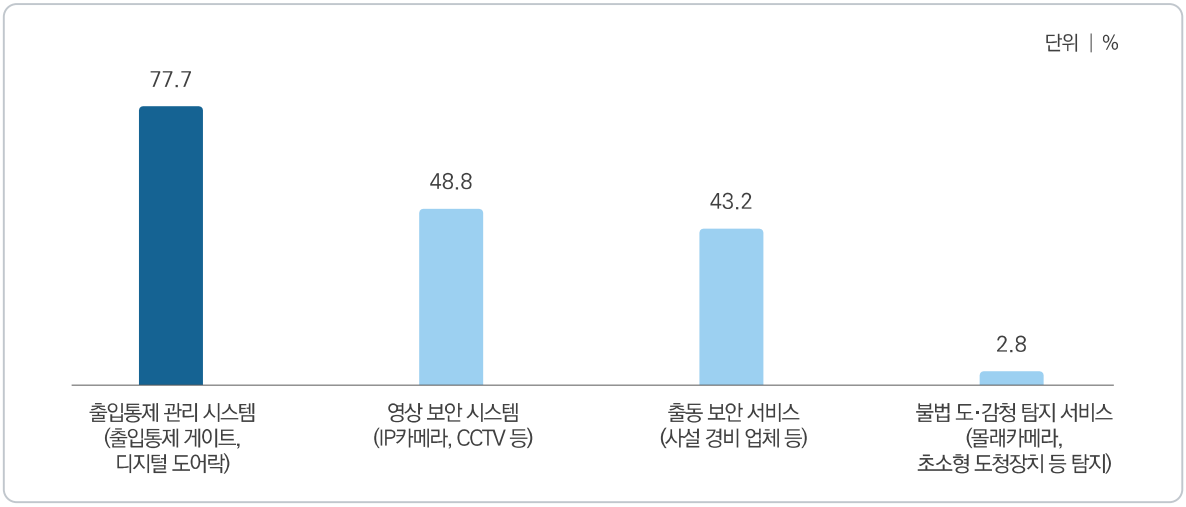


그림 1-2-14 이용한 정보보호 제품 및 솔루션_물리보안(복수응답) - 정보보호 제품 및 솔루션 사용 기업체

2 보안 점검

» 기업체의 81.2%가 사내 IT 시스템 및 네트워크에 대한 보안 점검을 실시

- 기업체의 81.2%는 사내 IT시스템 및 네트워크에 대한 보안 점검을 실시하는 것으로 조사됨
  - — 보안 점검 실시 시기로는 '6개월 이상 1년 미만'이 25.5%로 가장 높게 나타났고, '1개월 이상 ~ 6개월 미만'이 23.3%로 다음으로 높게 나타남

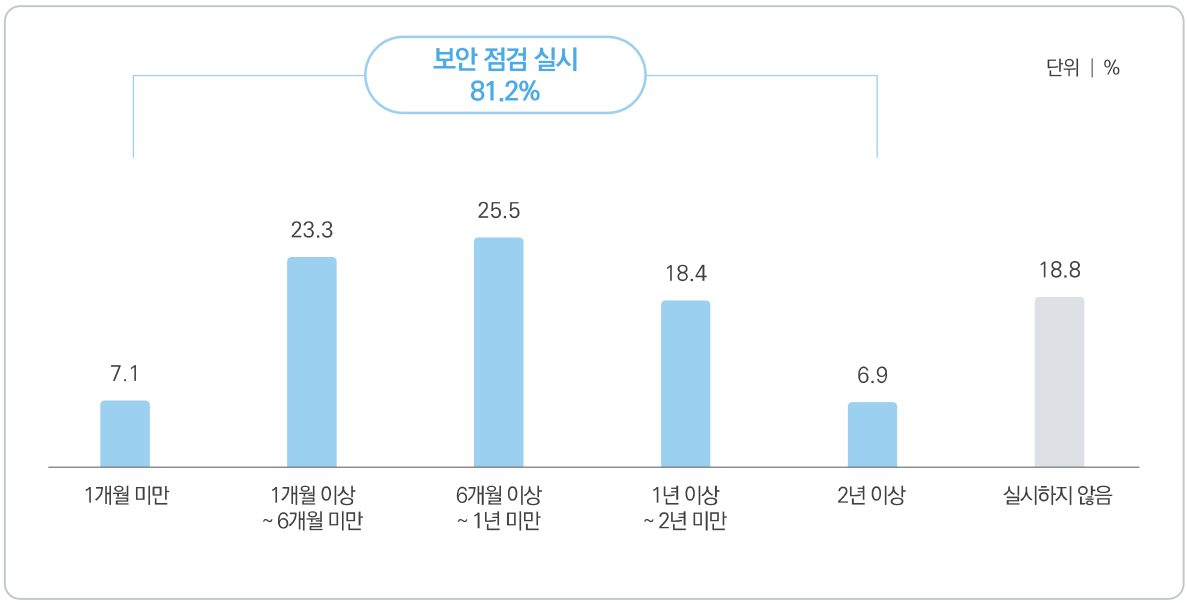


그림 1-2-15 시스템 및 네크워크 보안 점검

3 백업 실시

» 기업체의 89.1%가 데이터 백업 실시, 백업 유형별로 '중요 데이터' 백업 80.0%

- 응답 기업체의 89.1%는 데이터 백업을 실시하고 있으며, 데이터 유형별로는 '중요 데이터' 백업 실시율이 80.0%로 가장 높게 나타남

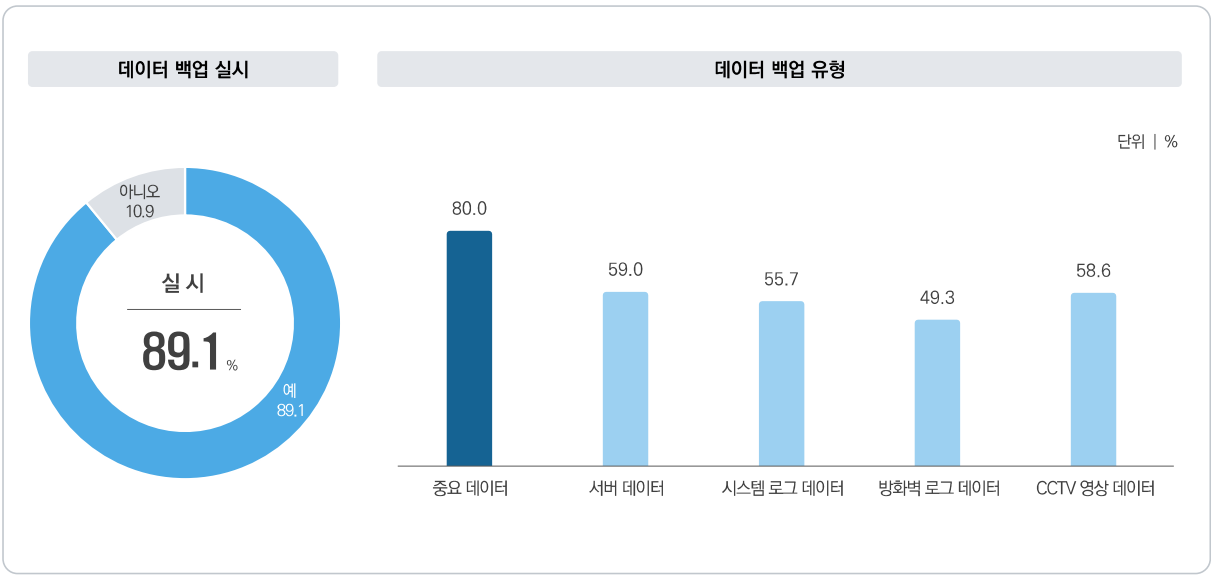


그림 1-2-16 데이터 백업 실시 및 유형

Ⅵ 침해사고 경험

1 침해사고 경험

» 정보보호 관련 침해사고 직접 경험 3.7%

- 정보보호 관련 침해사고를 직접적으로 경험한 비율은 3.7%로 나타났고, 침해사고를 의심한 비율은 6.3%로 나타남
  - — 경험한 정보보호 관련 침해사고 유형으로는 '랜섬웨어 감염(28.9%)', '외부로부터 침투한 비인가 접근(해킹)(26.2%)', '컴퓨터 바이러스, 웜, 트로이잔, APT 공격으로 인한 IT 시스템 마비(25.9%)', 'DoS 또는 DDoS 공격으로 인한 IT 시스템 마비(17.6%)' 등의 순으로 나타남

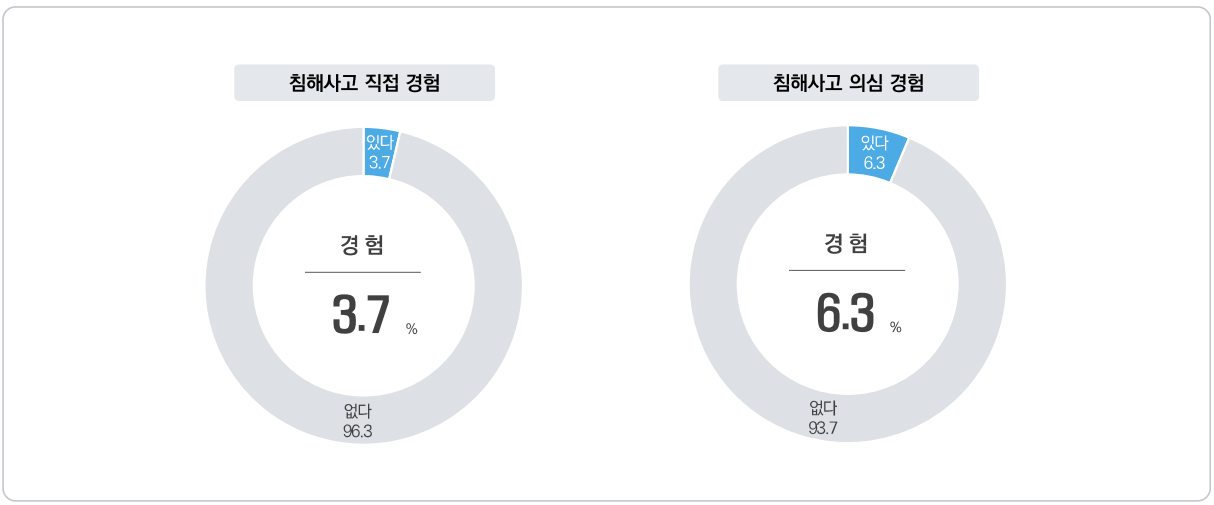


그림 1-2-17 침해사고 경험

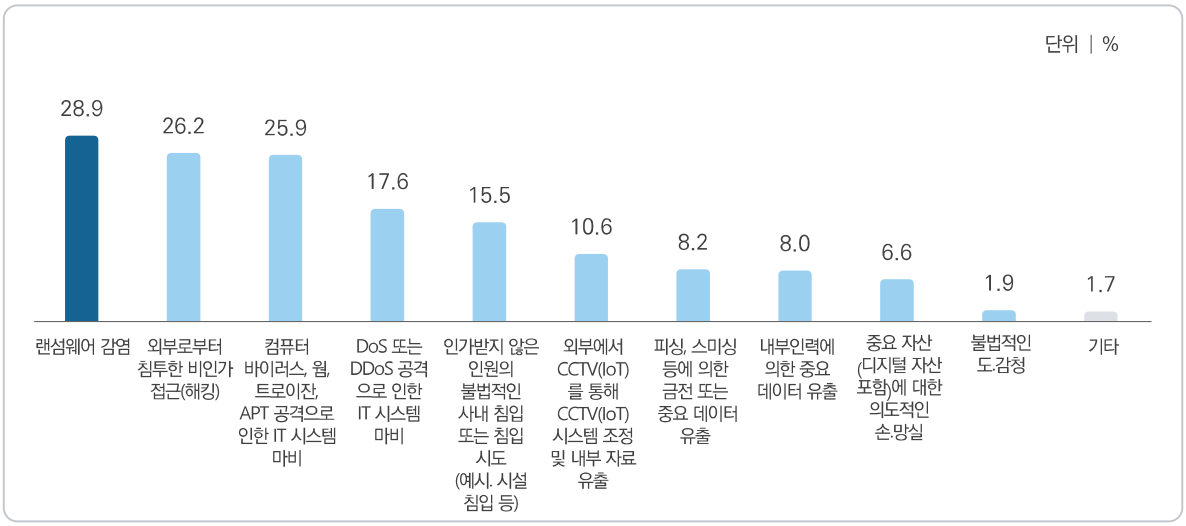


그림 1-2-18 침해사고 경험 유형(복수응답) - 침해사고 경험 기업체

2 침해사고 대응

» 침해사고 경험 기업체 대부분이 침해사고 시 관련 기관 또는 수사기관에 미신고

- 침해사고를 경험한 기업체 중 94.2%가 침해사고 시 관련 기관 또는 수사기관에 신고하지 않는 것으로 나타남
  - — 침해사고 시 신고하지 않는 이유로는 '피해 규모가 경미하기 때문에(69.8%)', '신고에 따른 업무가 복잡하기 때문에(35.8%)', '신고하더라도 피해가 회복되지 않을 것이기 때문에(27.9%)', '어디에 신고해야 하는지 모르기 때문에(23.7%)' 등의 순으로 나타남

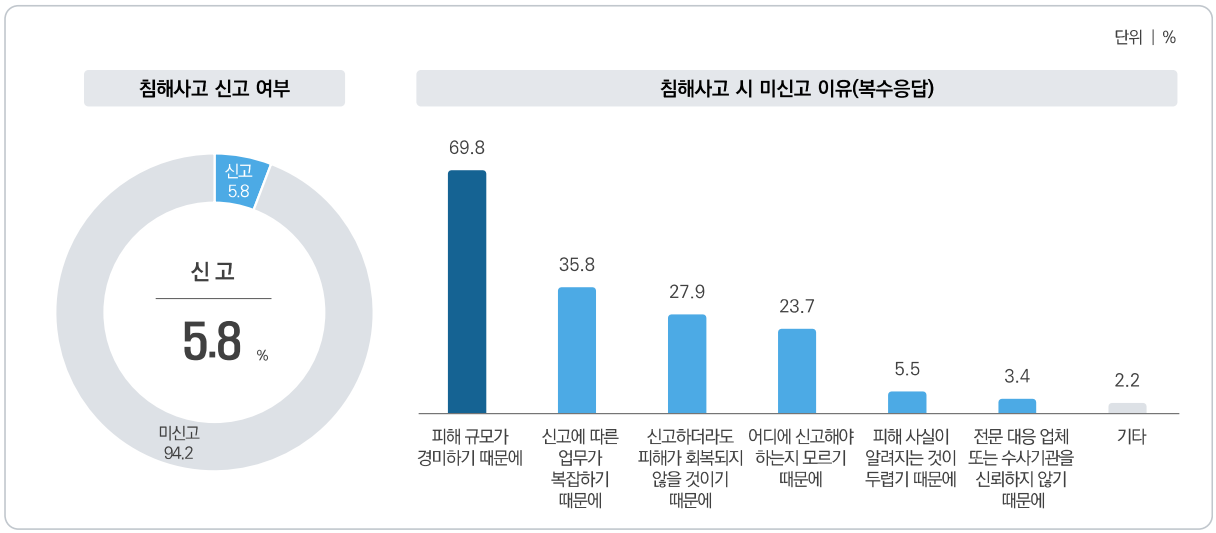


그림 1-2-19 침해사고 신고 여부 및 미신고 이유(복수응답) - 침해사고 경험 기업체

» 침해사고를 경험한 기업체 중 44.5%는 대응 활동 수행

- 침해사고를 경험한 기업체 중 44.5%가 대응활동을 수행하는 것으로 조사됨
  - — 침해사고 대응 유형으로는 '정보보호 관련 제품 및 솔루션 구축 및 고도화(24.6%)', '정보보호 인증을 받은 제품으로 교체(15.3%)', '정보보호 분야 전문기관 또는 전문가 자문(15.1%)' 등의 순으로 나타남

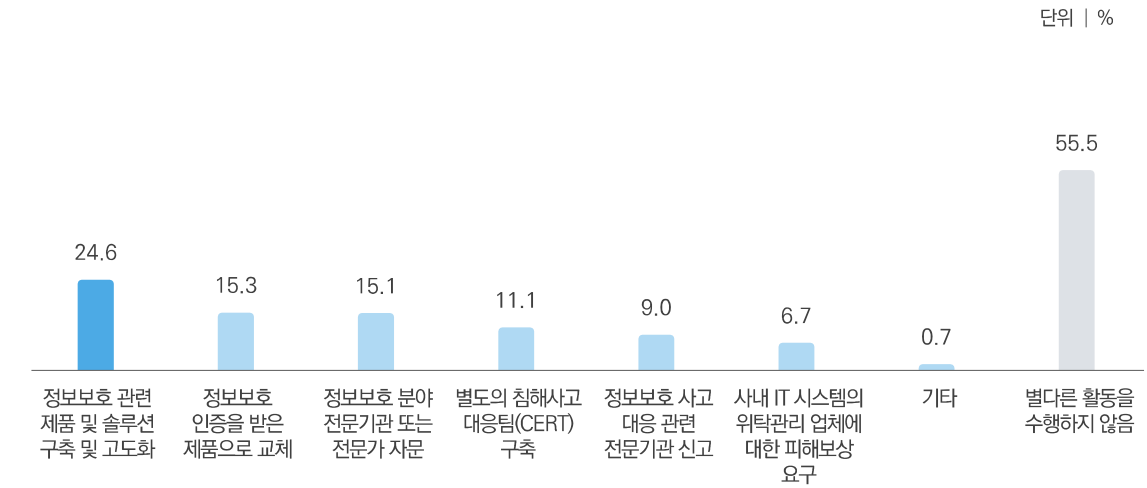


그림 1-2-20 침해사고 대응(복수응답) - 침해사고 경험 기업체

01 정보보호 인식 | 02 정보보호 정책 및 조직 | 03 정보보호 교육 | 04 정보보호 예산
05 침해사고 예방 | 06 침해사고 경험 | 07 사이버 보험 | 08 재택근무

제 3 장

조사결과

3

I 정보보호 인식

1 IT 기술 중요성 인식

- 국내 기업체 중 65.3%는 영위하고 있는 사업 분야에 있어 IT 기술의 중요성에 대해 중요하다(중요한 편이다 + 매우 중요하다)고 응답했다.

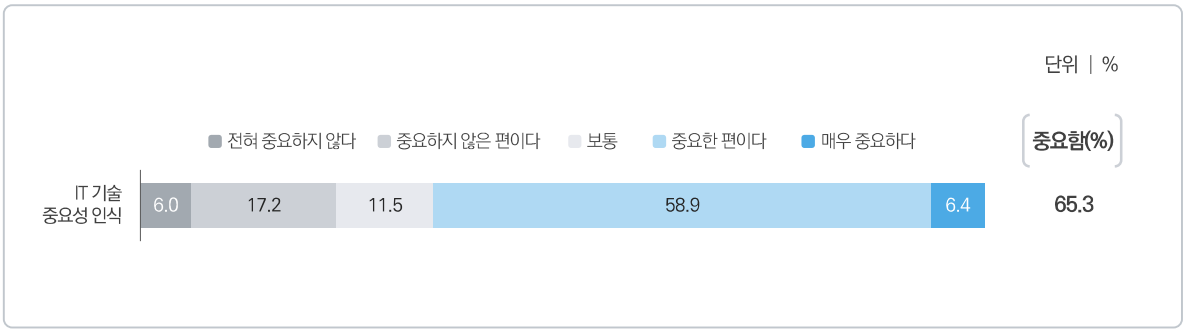


그림 1-3-1 IT 기술 중요성 인식

2 정보보호 중요성 인식

- 국내 기업체 중 88.9%는 기업의 정보보호가 중요하다(중요한 편이다 + 매우 중요하다)고 응답했다.

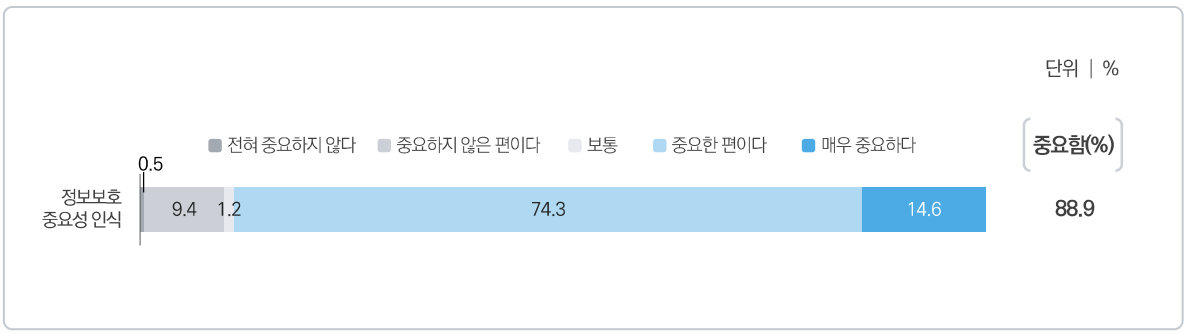


그림 1-3-2 정보보호 중요성 인식

3 임원의 정보보호 중요성 인식

- 국내 기업체의 63.4%는 임원의 정보보호 중요성 인식에 대해 정보보호가 중요하다(중요한 편이다 + 매우 중요하다)고 응답했다.

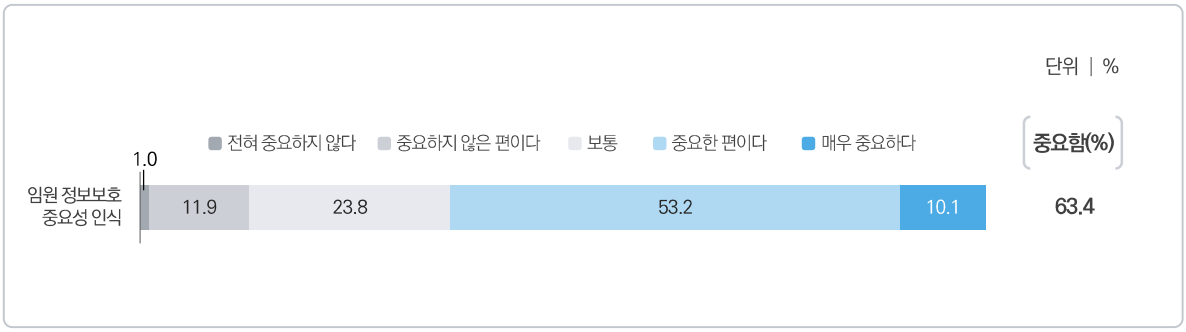


그림 1-3-3 임원의 정보보호 중요성 인식

4 정보보호 위협요인

- 국내 기업체가 우려하는 정보보호 위협요인으로는 '시스템 및 네트워크 장애로 인한 서비스 마비 위협'이 33.4%로 가장 높게 나타났으며, 다음으로 '시스템 및 네트워크 침입을 통한 해킹의 위협(31.0%)', '인적 요인에 의한 정보유출 위협(30.8%)', '외부 공격에 의한 저장된 데이터 자산의 손·망실(30.7%)' 등의 순으로 조사되었다.

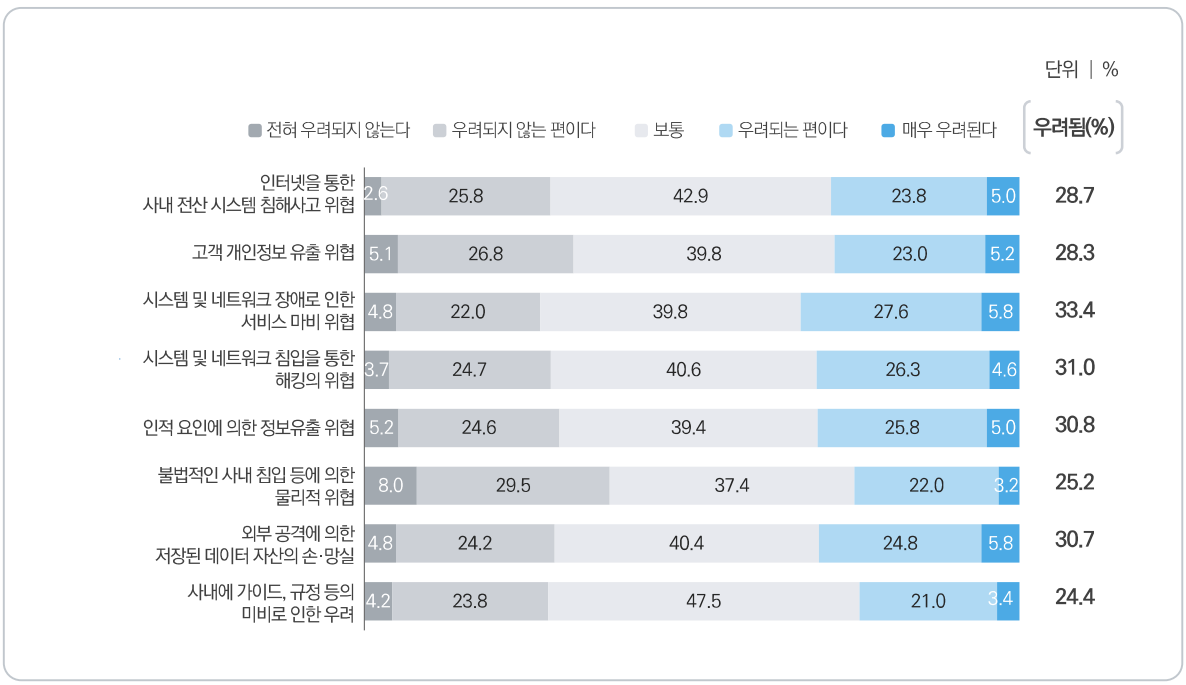


그림 1-3-4 정보보호 위협요인

5 정보보호 애로사항

- 국내 기업체가 정보보호에 대해 어려움을 느끼는 사항으로는 '정보보호 예산 확보'가 64.9%로 가장 높게 나타났으며, 다음으로 '정보보호 시스템 및 체계 운용 관리(55.9%)', '정보보호 전문인력 확보(44.7%)', '필요한 정보보호 제품 및 서비스 탐색(41.6%)' 등의 순이었다.

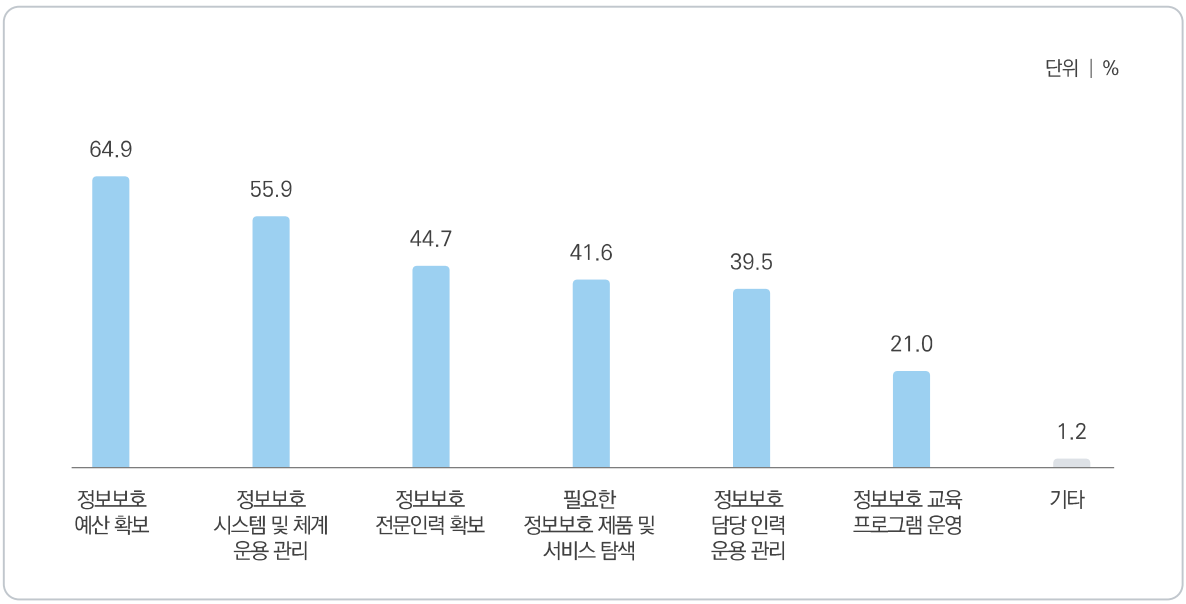


그림 1-3-5 정보보호 애로사항(복수응답)

6 정보보호 규정 적용의 엄격함 정도

- 국내 기업체의 60.2%는 정보보호 규정이 제정, 변경 또는 강화되었을 때, 해당 사항을 조직 구성원에게 엄격하게 적용한다(엄격한 편이다 + 매우 엄격하다)고 응답했다.

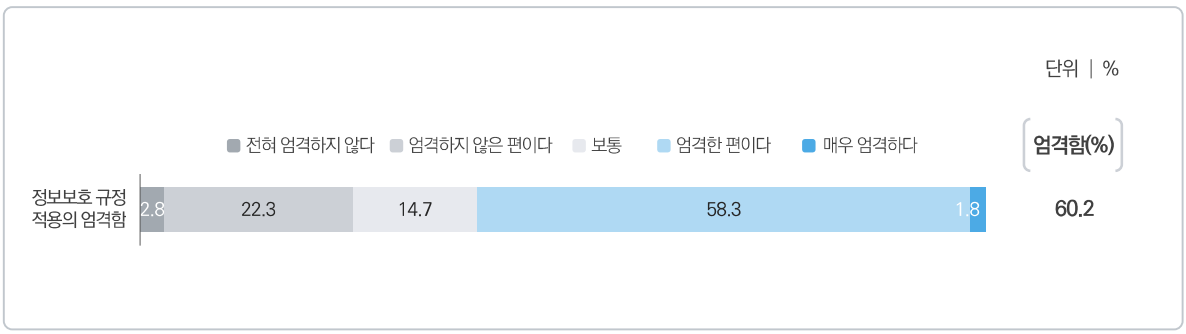


그림 1-3-6 정보보호 규정 적용의 엄격함 정도

Ⅱ 정보보호 정책 및 조직

1 정보보호 정책

가 정보보호 정책 수립

- 국내 기업체 중 35.3%가 공식문서로 정보보호 정책을 수립한 것으로 나타났다.

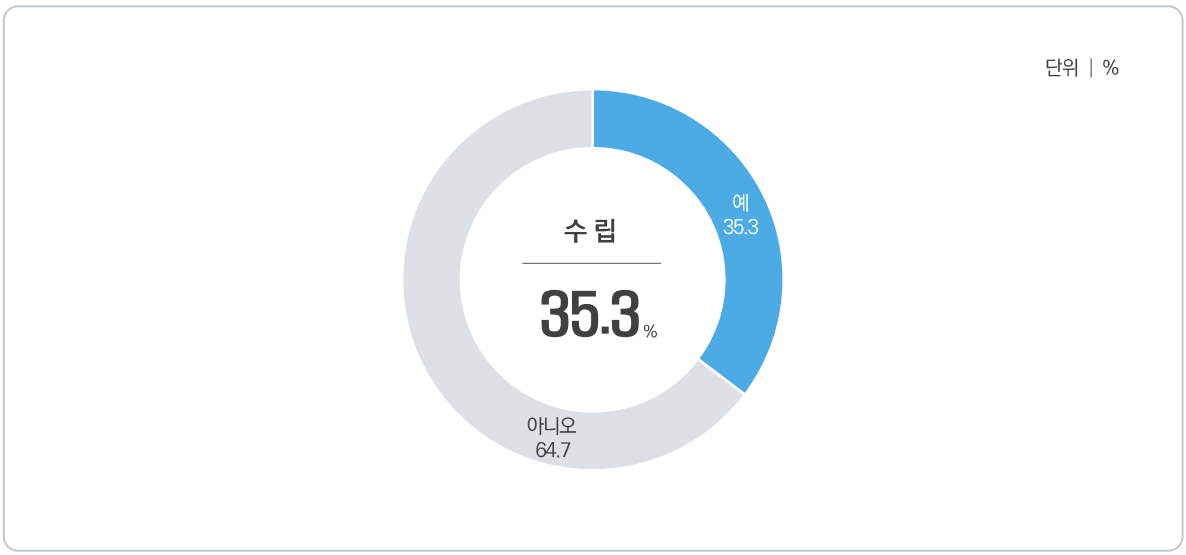


그림 1-3-7 정보보호 정책 수립

- 업종별 분석 결과, ‘금융 및 보험업’이 77.4%로 가장 높게 나타났고, 다음으로 ‘정보통신업(72.0%)’, ‘전문, 과학 및 기술 서비스업(65.3%)’ 등의 순으로 조사되었다.

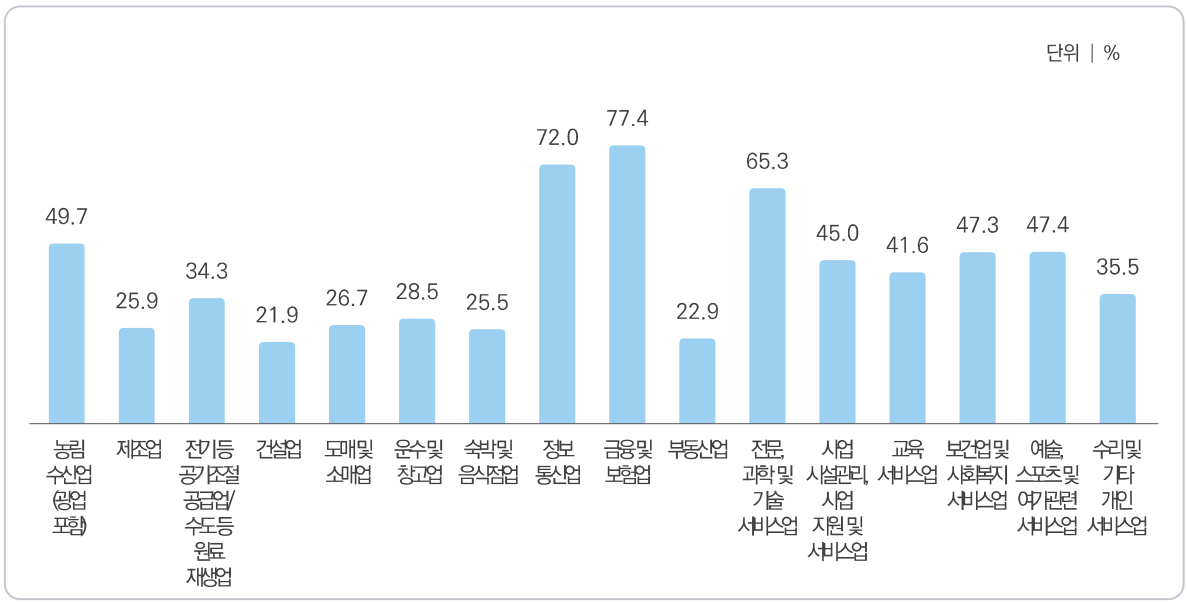


그림 1-3-8 업종별 정보보호 정책 수립

- 규모별 분석 결과, 종사자 수가 많을수록 정보보호 정책 수립률이 높은 것으로 나타났다.

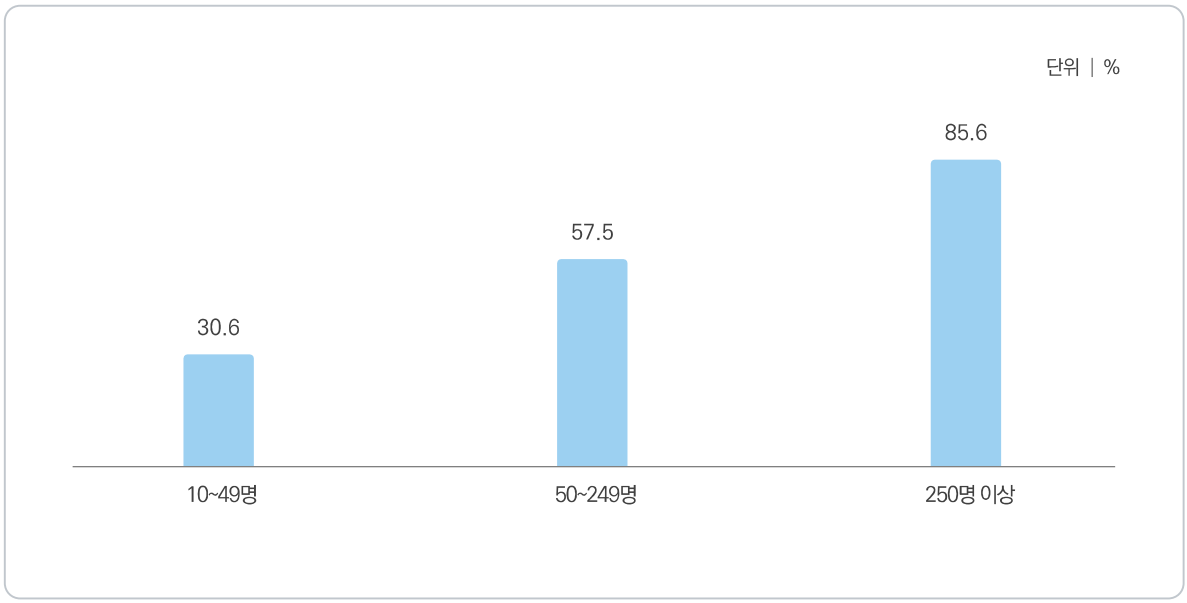


그림 1-3-9 규모별 정보보호 정책 수립

나 정보보호 정책 중 개인정보보호 포함 여부

- 정보보호 정책을 보유하고 있는 국내 기업체 중 79.2%가 정보보호 정책 내 개인정보보호 규정이 포함되어 있는 것으로 나타났다.

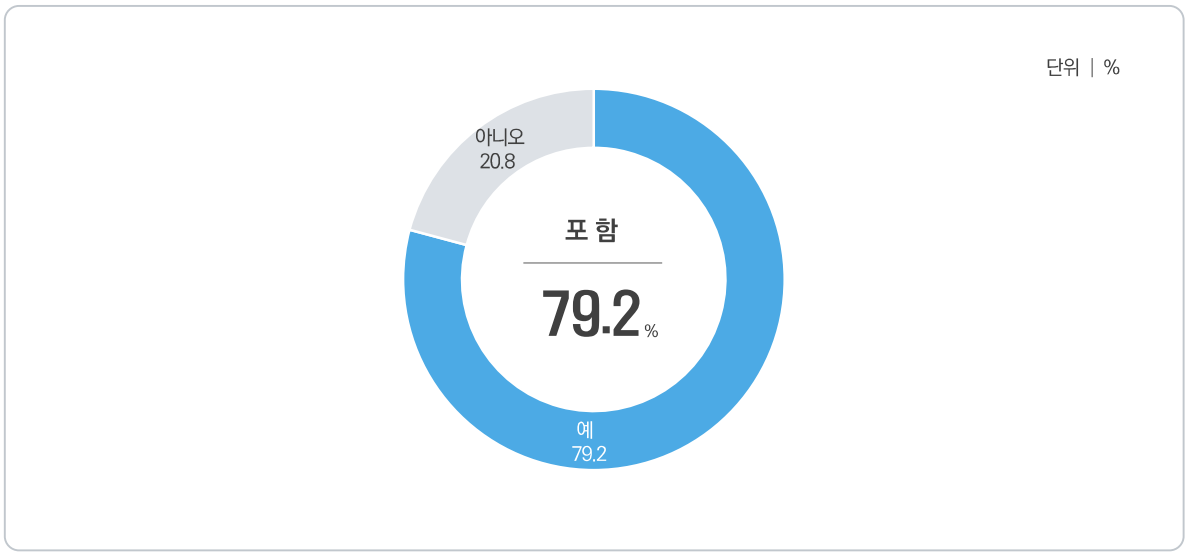


그림 1-3-10 정보보호 정책 중 개인정보보호 포함 여부 - 정보보호 정책 수립 기업체

- 업종별 분석 결과, '교육 서비스업'이 99.4%로 가장 높게 나타났고, 다음으로 '농림수산업(광업포함)(97.2%)', '부동산업(91.5%)' 등의 순으로 조사되었다.

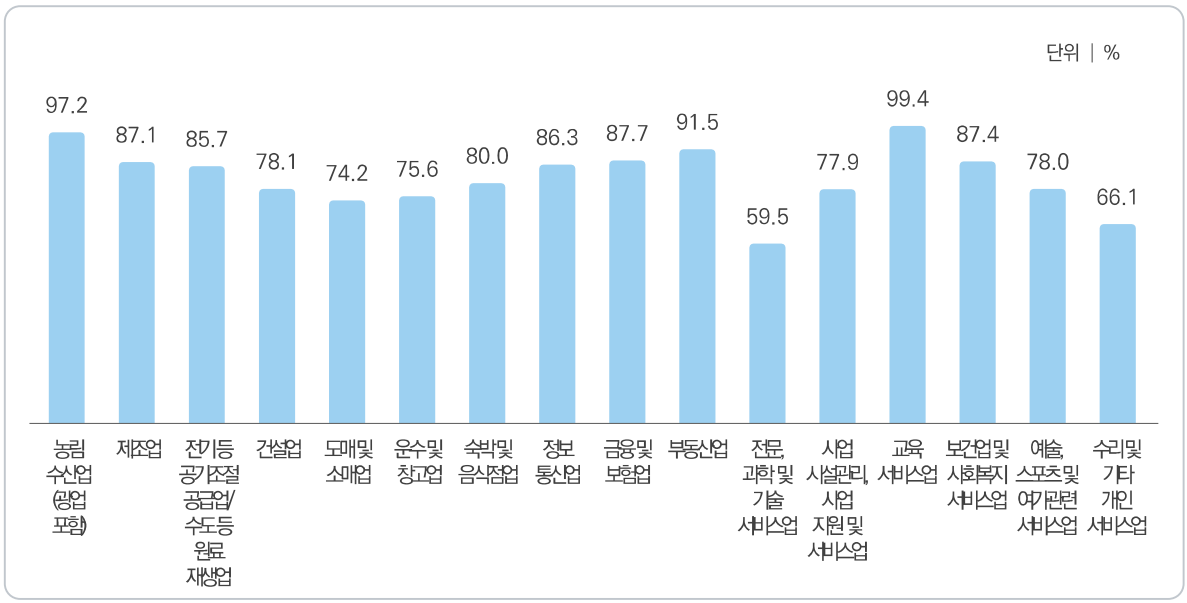


그림 1-3-11 업종별 정보보호 정책 중 개인정보보호 포함 여부 - 정보보호 정책 수립 기업체

- 규모별 분석 결과, 종사자 수가 많을수록 정보보호 정책 내 개인정보보호 규정이 포함되어 있는 비율이 높은 것으로 나타났다.

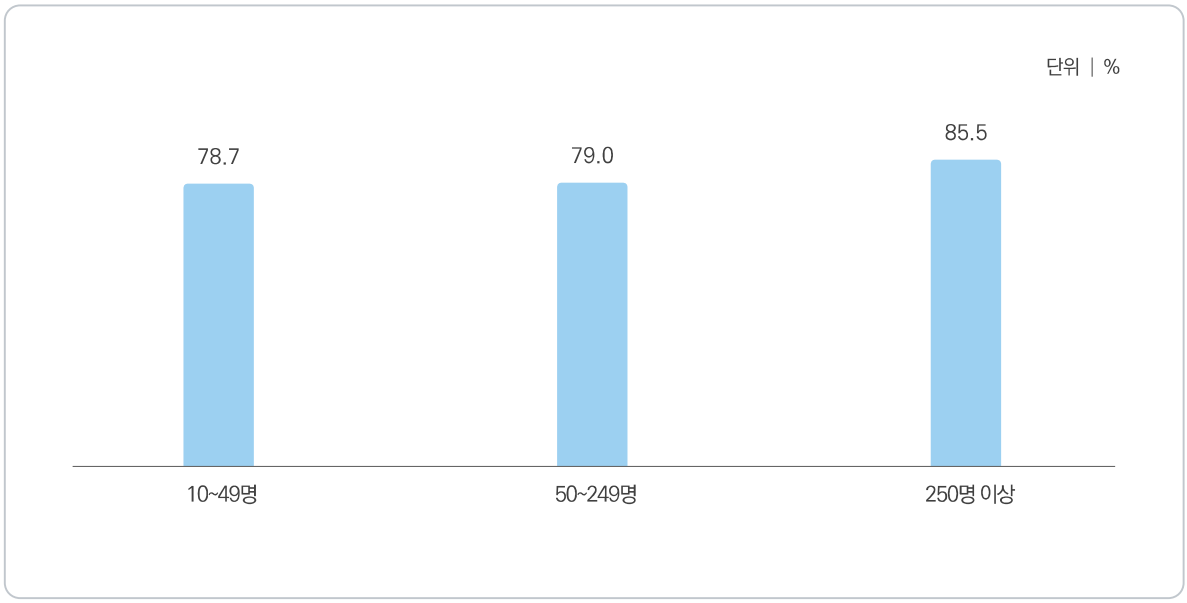


그림 1-3-12 **규모별 정보보호 정책 중 개인정보보호 포함 여부 - 정보보호 정책 수립 기업체**

2 정보보호 조직

- 국내 기업체의 정보보호 조직 수립률은 40.3%이며, 이 중 전담조직을 운영하는 경우는 6.9%, 겸임조직을 운영하는 경우는 33.4%로 나타났다.

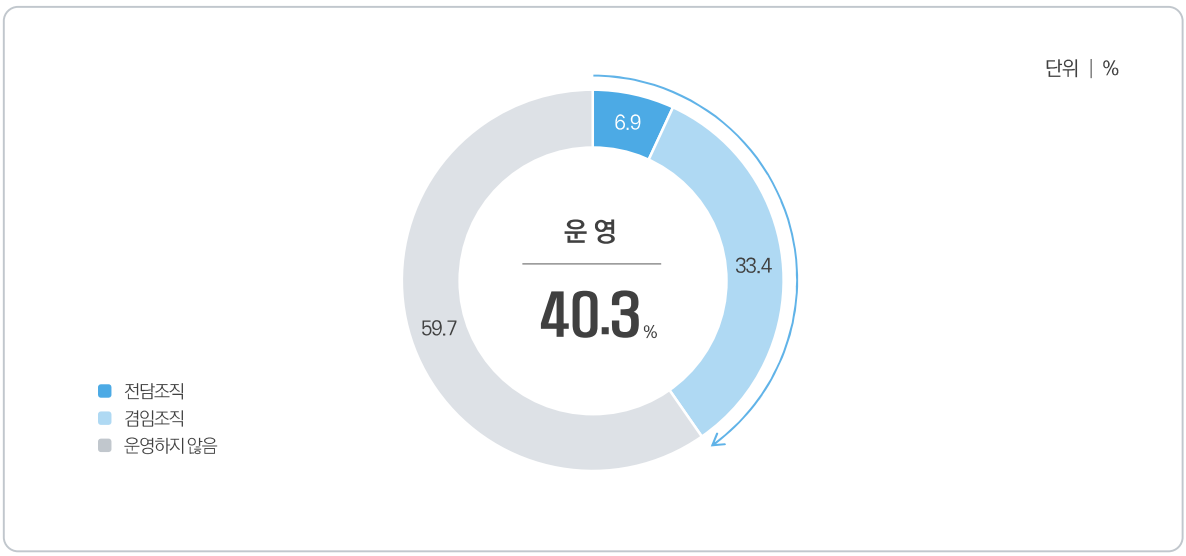


그림 1-3-13 정보보호 조직

- 업종별 분석 결과, '금융 및 보험업'의 정보보호 조직의 전담 비율이 18.9%로 가장 높고, 다음으로 '농림수산업(광업포함)(14.6%)', '정보통신업(12.7%)' 등의 순으로 나타났다.

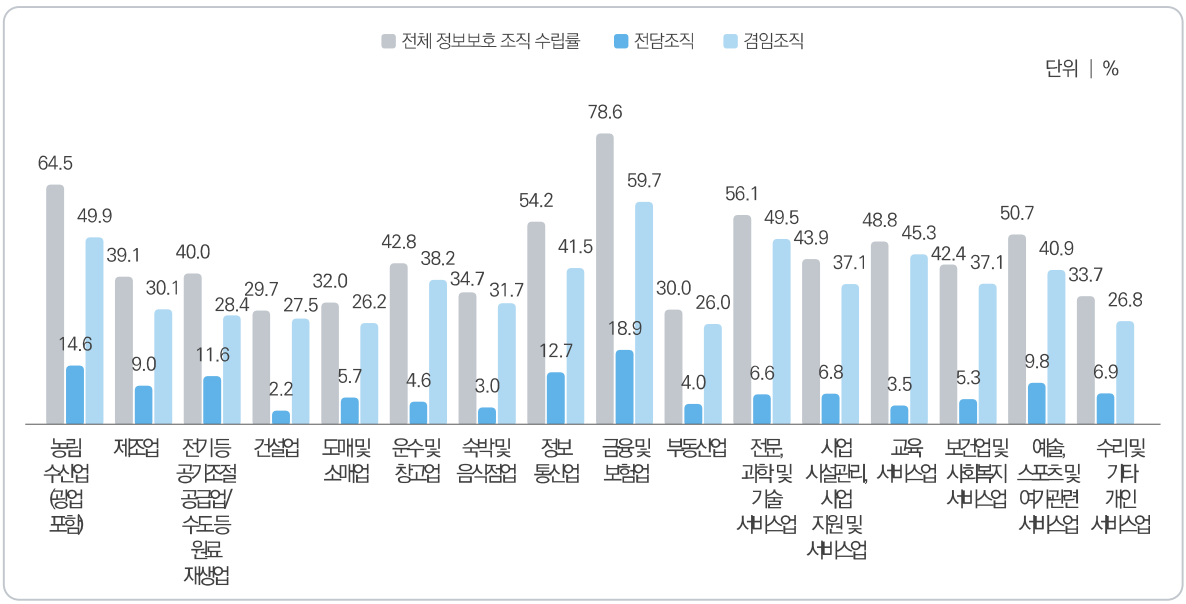


그림 1-3-14 업종별 정보보호 조직

- 규모별 분석 결과, 종사자 수가 많을수록 정보보호 조직의 전담 비율이 높았다.

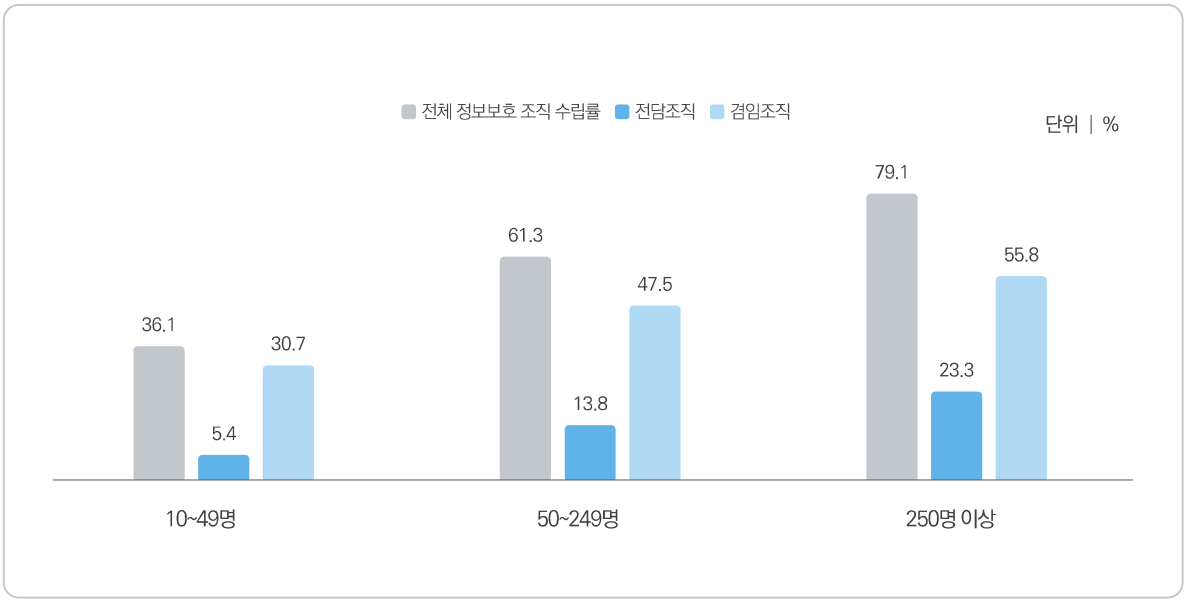


그림 1-3-15 규모별 정보보호 조직

3 정보보호 인력

가 정보보호 관련 책임자

- 정보보호 관련 책임자가 임명된 국내 기업체의 비율은 '정보관리책임자(Chief Information Officer)' 28.9%, '정보보호최고책임자(Chief Information Security Officer)' 19.2%로 각각 나타났다.

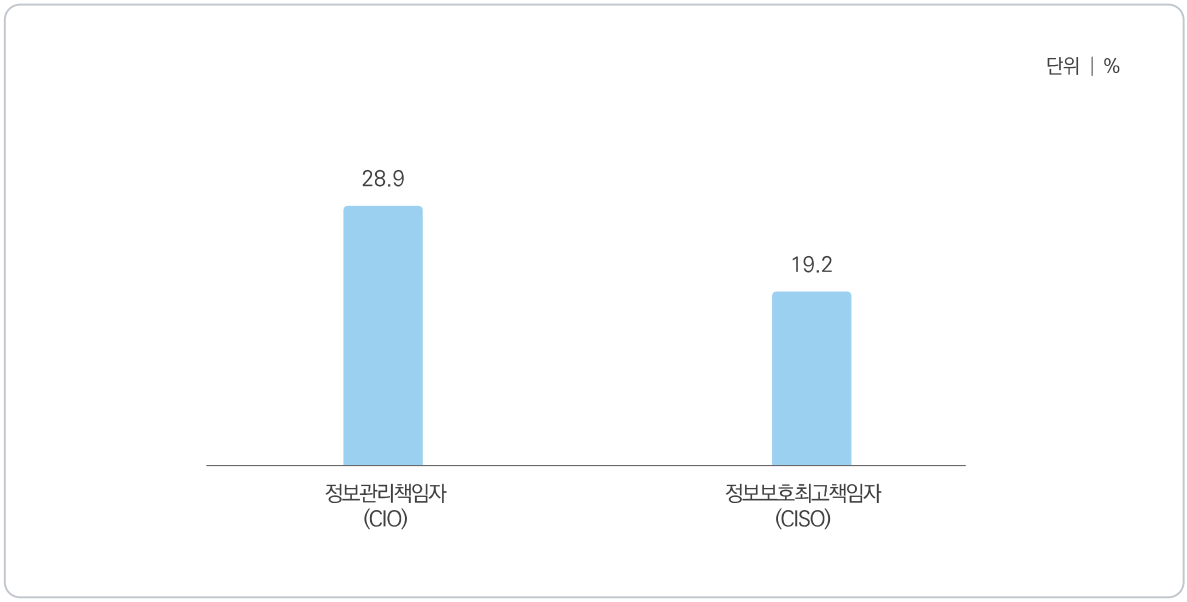


그림 1-3-16 정보보호 관련 책임자 임명(복수응답)

- 업종별 분석 결과, '금융 및 보험업'이 '정보관리책임자(CIO)' 70.6%, '정보보호최고책임자(CISO)' 48.6%로 전 업종 중 가장 높은 것으로 나타났다.

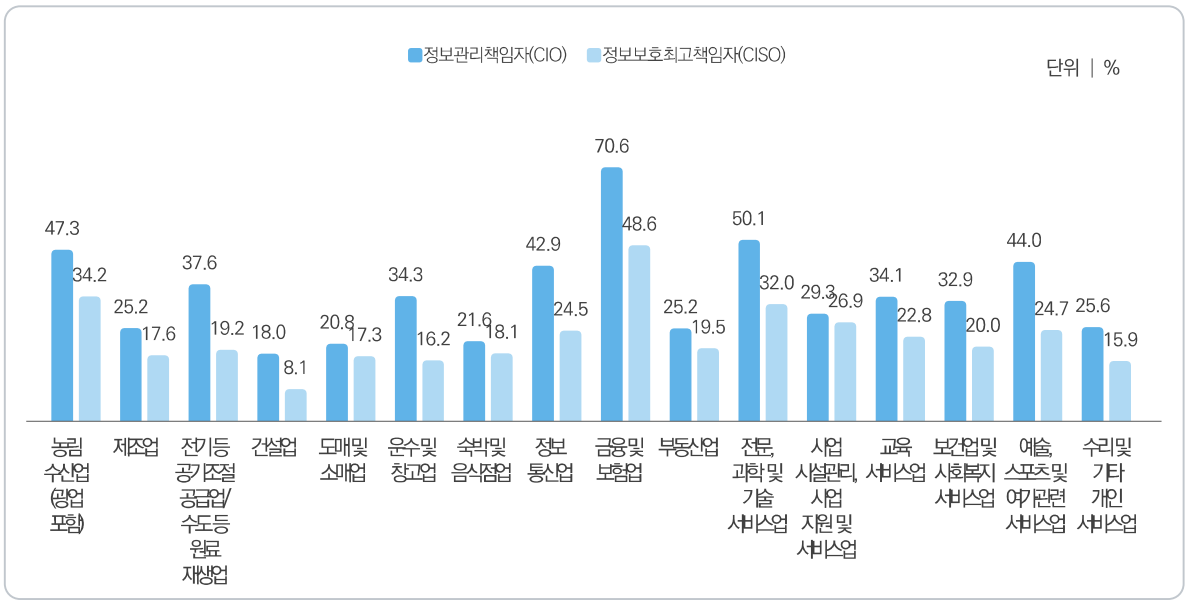


그림 1-3-17 업종별 관련 책임자 임명(복수응답)

- 규모별 분석 결과, 종사자 수가 많을수록 정보보호 관련 책임자 임명 비율이 높은 것으로 나타났다.

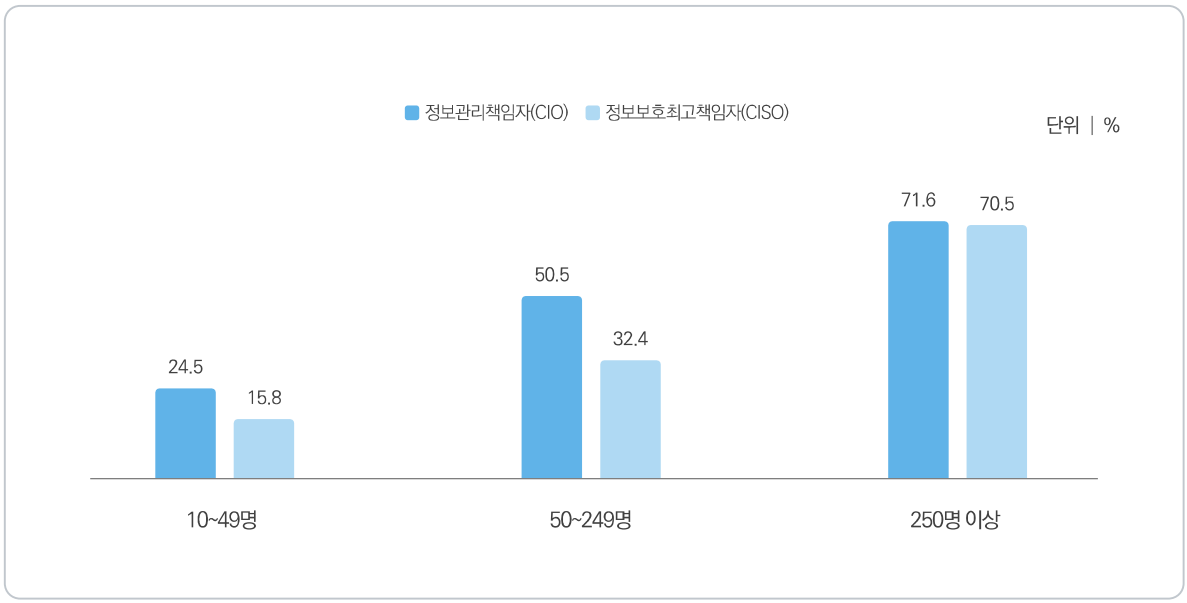


그림 1-3-18 **규모별 관련 책임자 임명(복수응답)**

- 정보보호 관련 책임자 전담 비율은 '정보관리책임자(CIO)' 35.1%, '정보보호최고책임자(CISO)' 39.3%로 각각 나타났다.

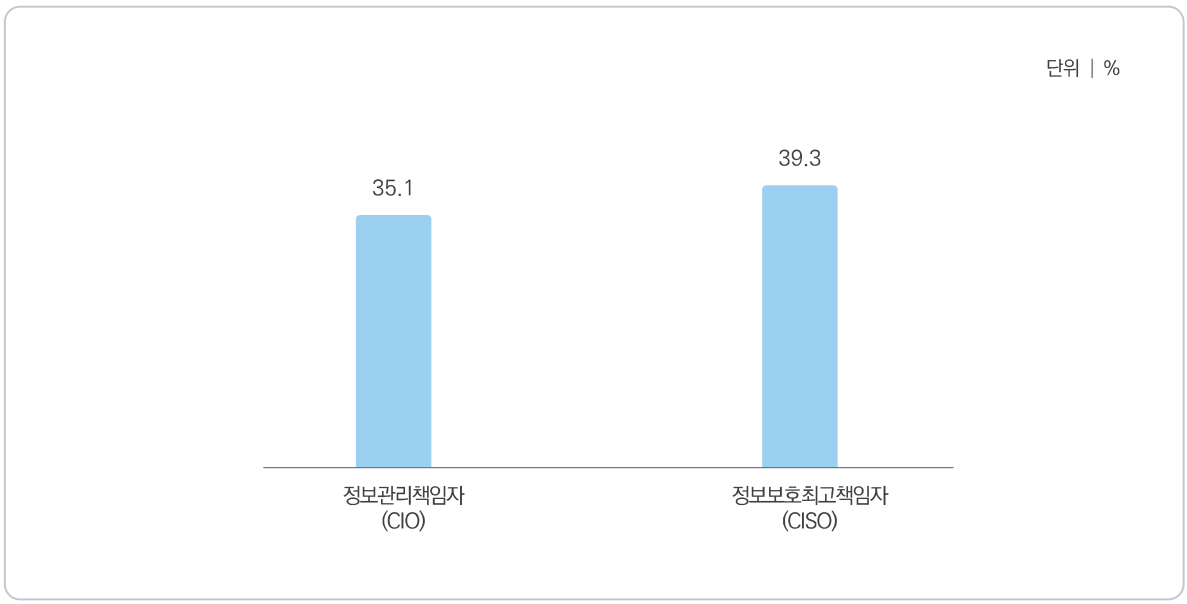


그림 1-3-19 **관련 책임자 전담 비율 – 책임자 임명 기업체**

- 업종별 관련 책임자 전담 비율 분석 결과, '교육 서비스업'이 '정보관리책임자(CIO)' 79.5%, '정보보호최고책임자(CISO)' 70.6%로 전 업종 중 전담 비율이 가장 높은 것으로 나타났다.

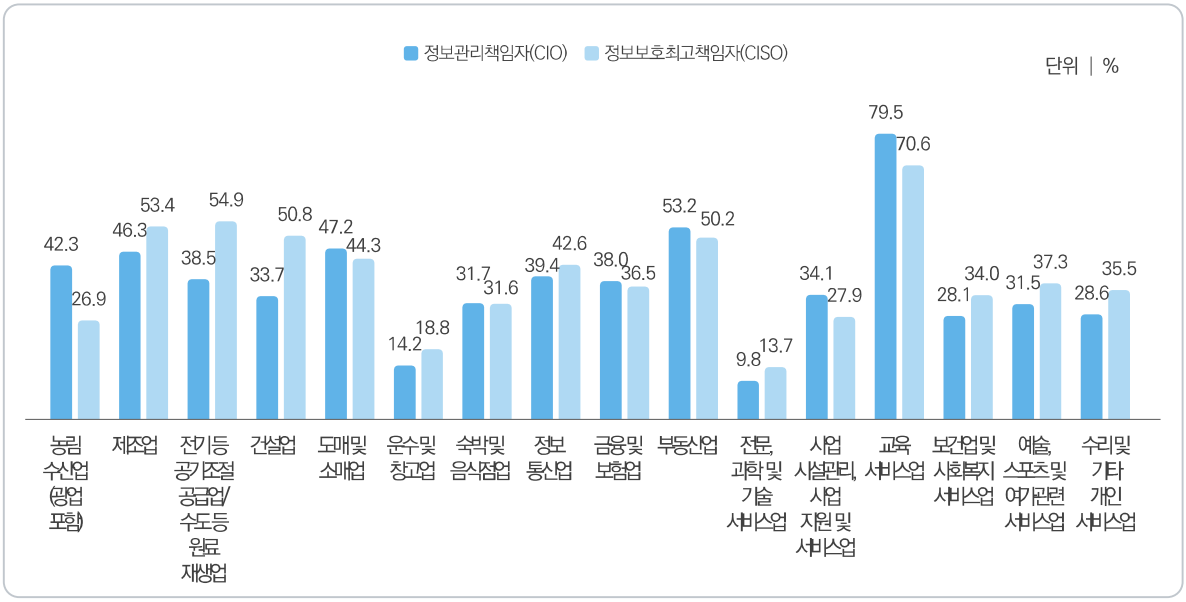


그림 1-3-20 업종별 관련 책임자 전담 비율 – 책임자 임명 기업체

- 규모별 분석 결과, 종사자 수와 관계없이 정보보호 관련 책임자 전담 비율은 30%대로 비슷한 수준을 보이는 것으로 나타났다.

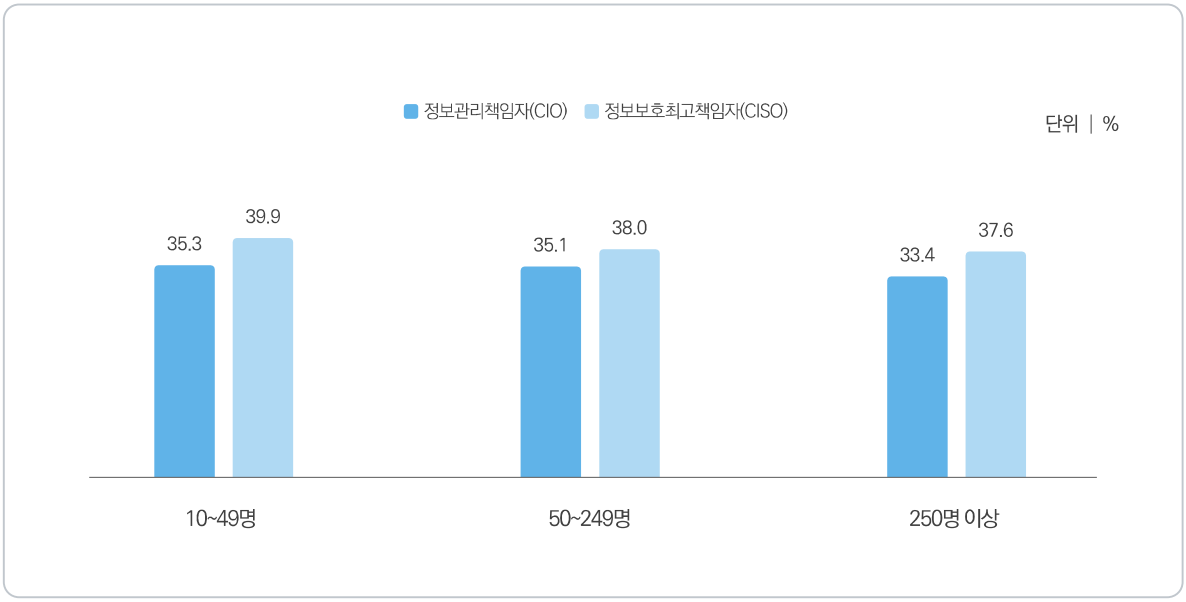


그림 1-3-21 규모별 관련 책임자 전담 비율 – 책임자 임명 기업체

나 개인정보보호책임자 겸직 여부

- 정보보호 관련 책임자가 임명된 국내 기업체 중 개인정보보호책임자(CPO) 업무를 겸직하는 비율은 56.4%로 조사되었다.

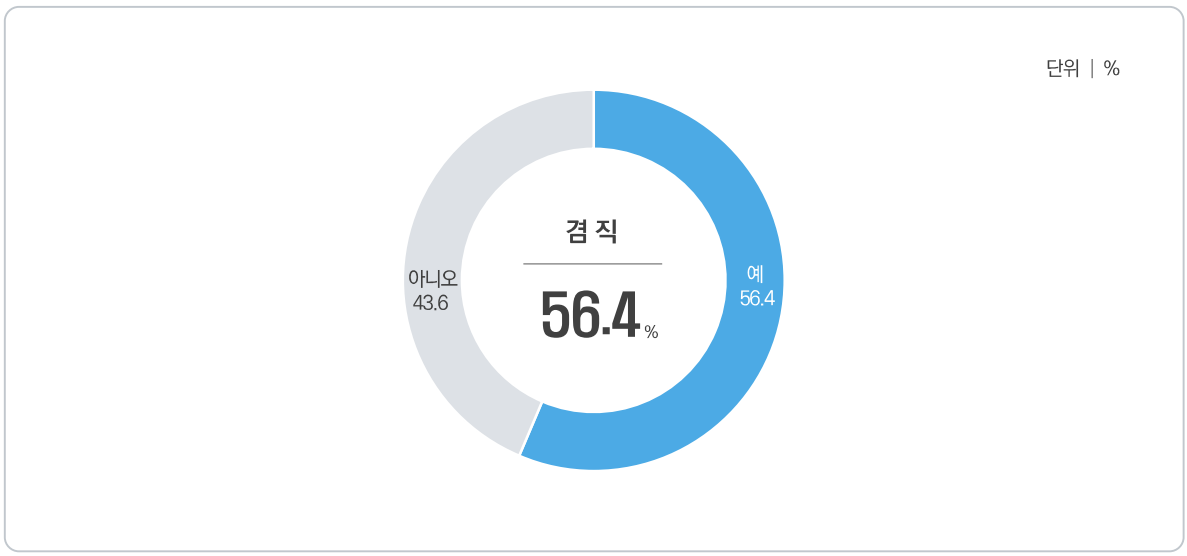


그림 1-3-22 개인정보보호책임자 겸직 여부 - 책임자 임명 기업체

- 업종별 분석 결과, '농림수산업(광업포함)'이 80.3%로 가장 높게 나타났고, 다음으로 '보건업 및 사회복지 서비스업(71.4%)', '사업시설관리, 사업지원 및 서비스업(70.2%)' 등의 순으로 조사되었다.

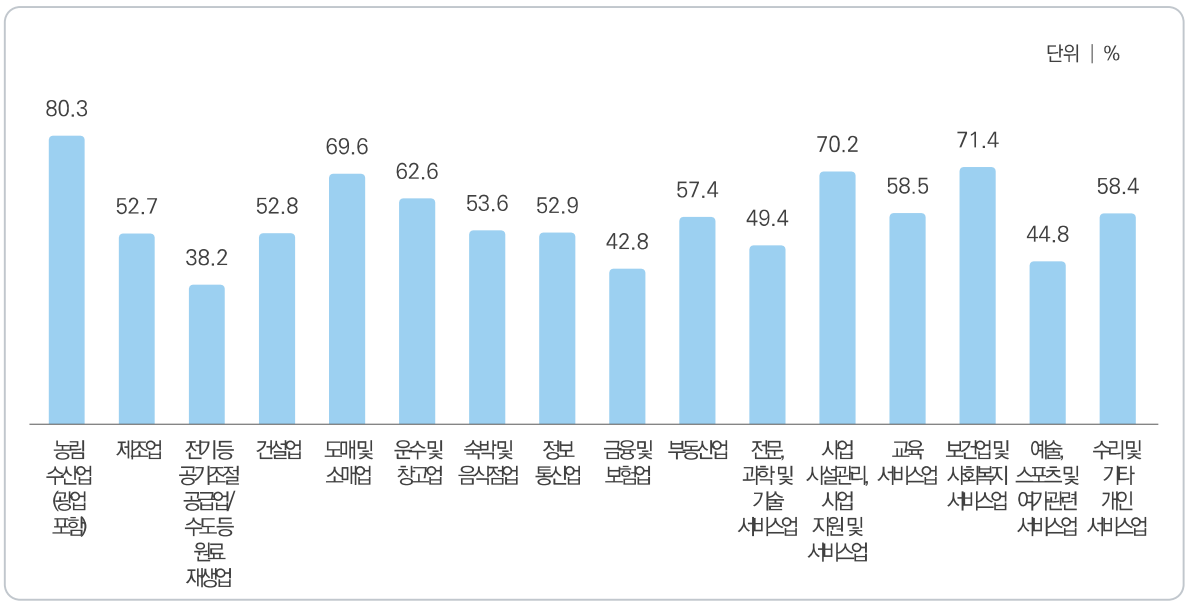


그림 1-3-23 업종별 개인정보보호책임자 겸직 여부 - 책임자 임명 기업체

- 규모별 분석 결과, 모든 규모에서 정보보호책임자가 개인정보보호 업무를 겸직하는 비율이 과반 이상으로 나타났다.

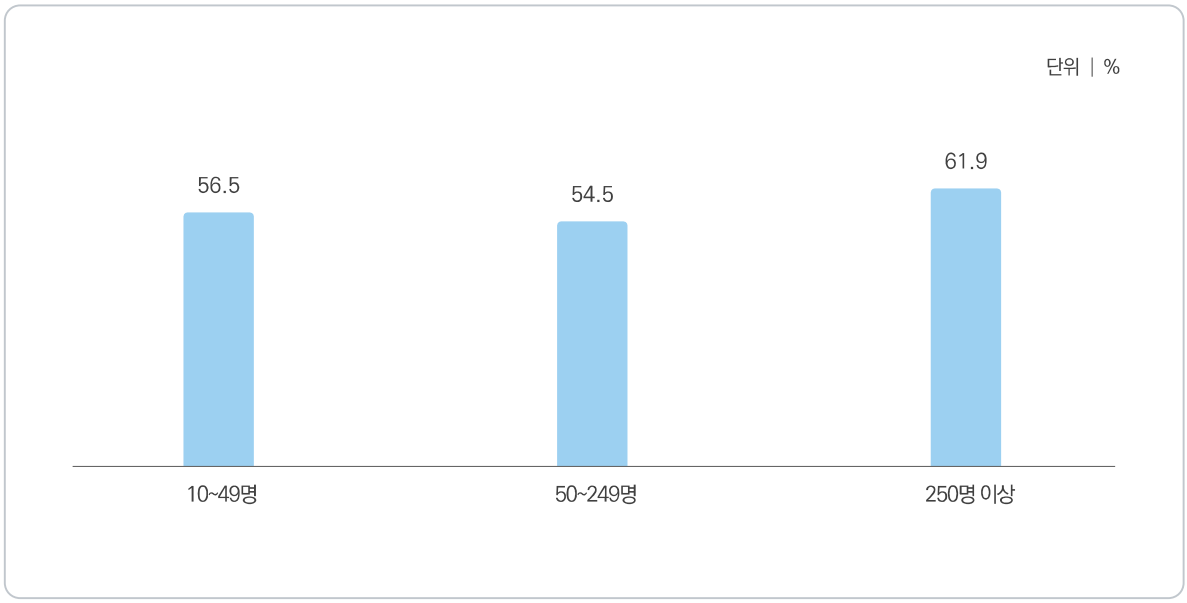


그림 1-3-24 규모별 개인정보보호책임자 겸직 여부 - 책임자 임명 기업체

다 정보보호 관련 인력

- 국내 기업체의 정보보호 담당 인력은 내부인력 평균 1.2명, 외부인력 0.4명으로 조사되었다.
- IT 인력 중 정보보호 업무를 부가적으로 수행하는 인력은 내부인력 평균 0.8명, 외부인력 0.3명으로 조사되었다.
- 사무직 인력 중 정보보호 업무를 부가적으로 수행하는 인력은 내부인력 평균 1.3명, 외부인력 0.3명이었다.

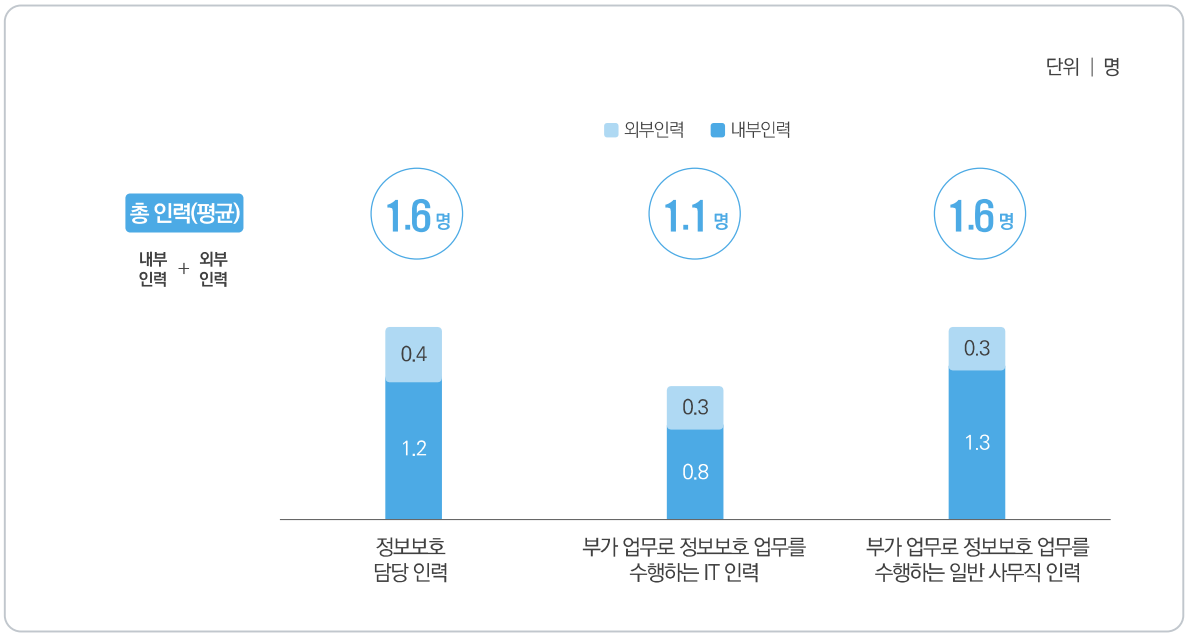


그림 1-3-25 정보보호 관련 인력(요약)

- 업종별 분석 결과, '금융 및 보험업'이 내부인력 2.3명, 외부인력 0.8명으로 전 업종 중 가장 많았다.

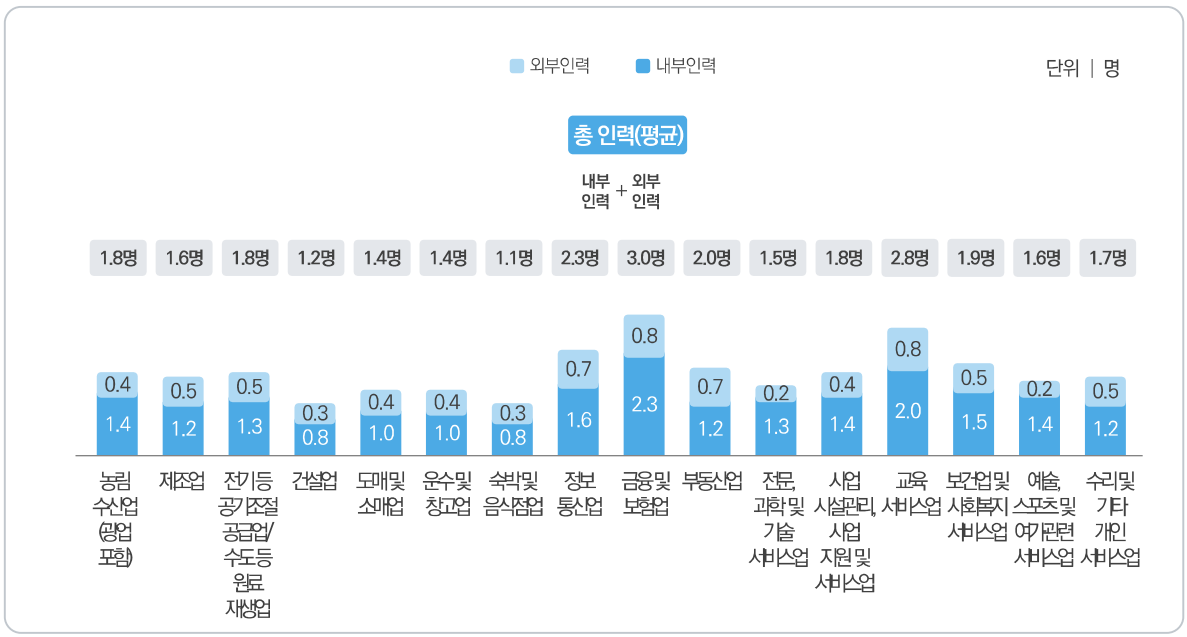


그림 1-3-26 업종별 정보보호 관련 인력

- 규모별 분석 결과, 종사자 수가 많을수록 정보보호 담당자가 많은 것으로 나타났다.

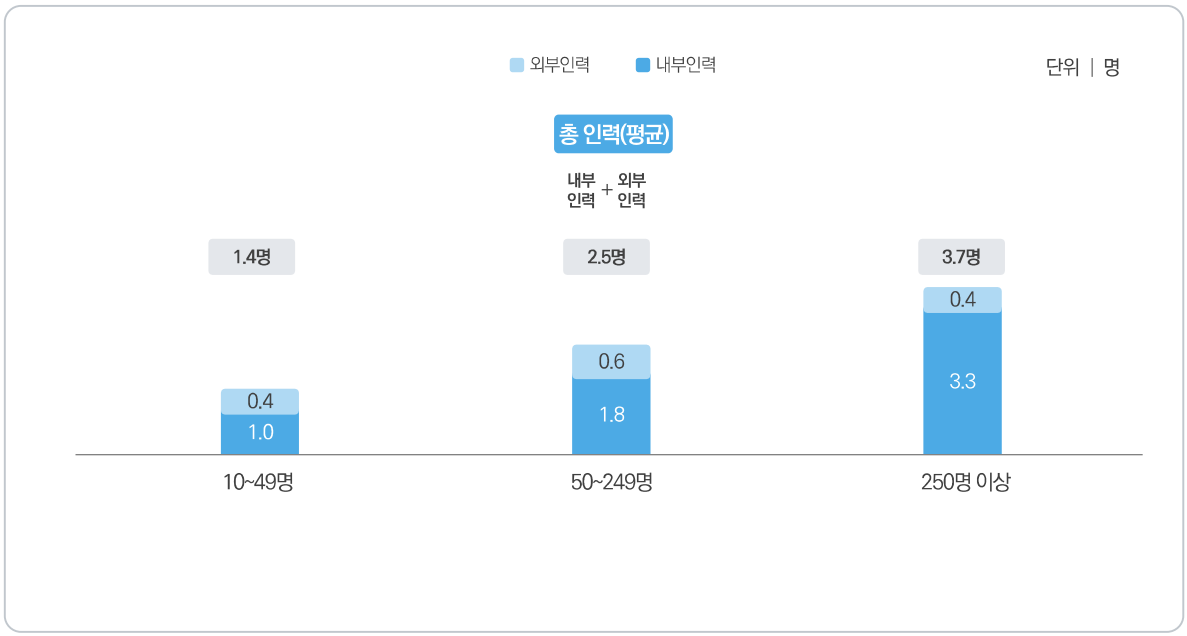


그림 1-3-27 규모별 정보보호 관련 인력

- 업종별 분석 결과, '교육 서비스업'이 내부인력 1.7명, 외부인력 0.7명으로 전 업종 중 가장 많았다.

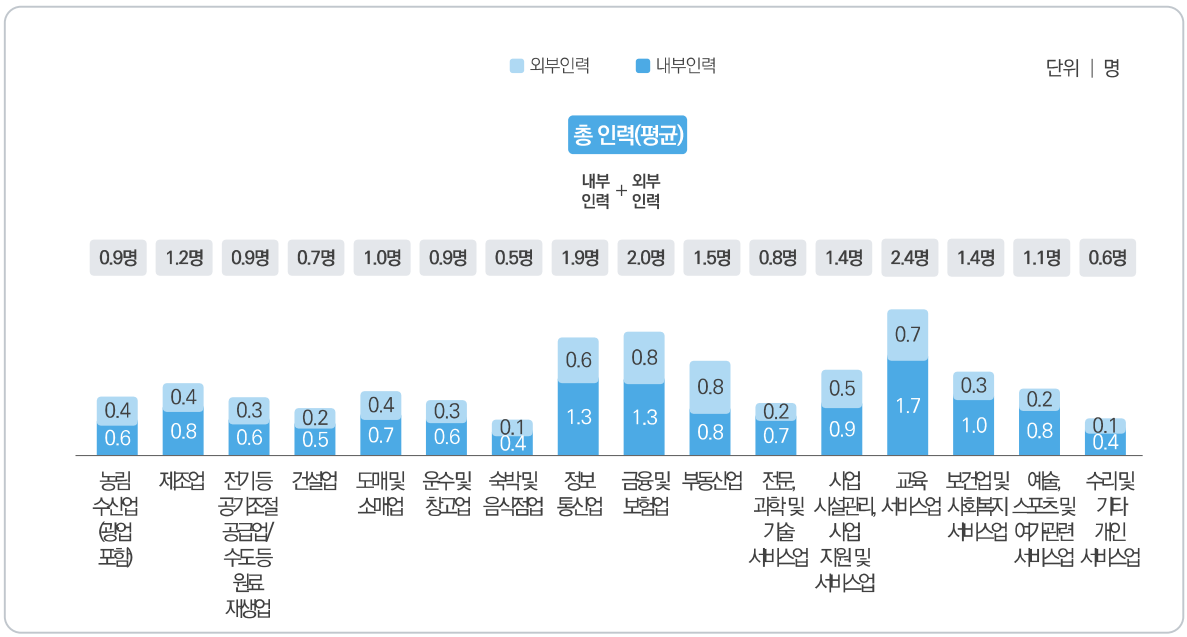


그림 1-3-28 업종별 IT 인력 중 정보보호 업무 수행 인력

- 규모별 분석 결과, 종사자 수 규모가 '50~249명'인 경우 내부인력 1.4명, 외부인력 0.6명으로 가장 높은 것으로 나타났다.

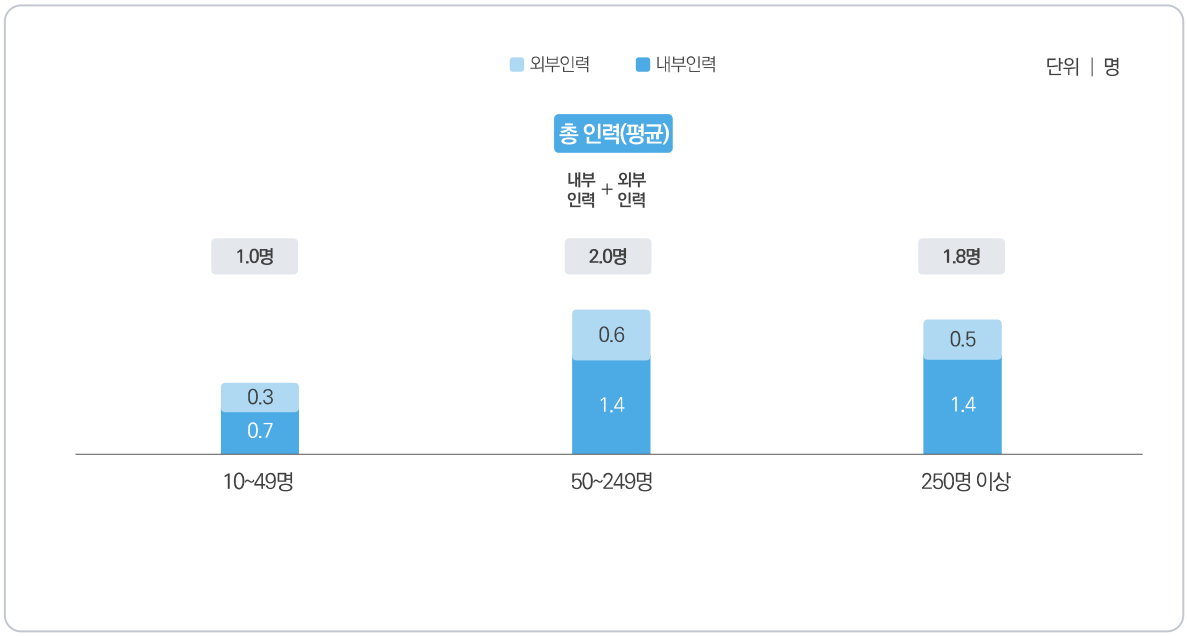


그림 1-3-29 규모별 IT 인력 중 정보보호 업무 수행 인력

- 업종별 분석 결과, '교육 서비스업'이 내부인력 2.5명, 외부인력 0.6명으로 전 업종 중 가장 높은 것으로 나타났다.

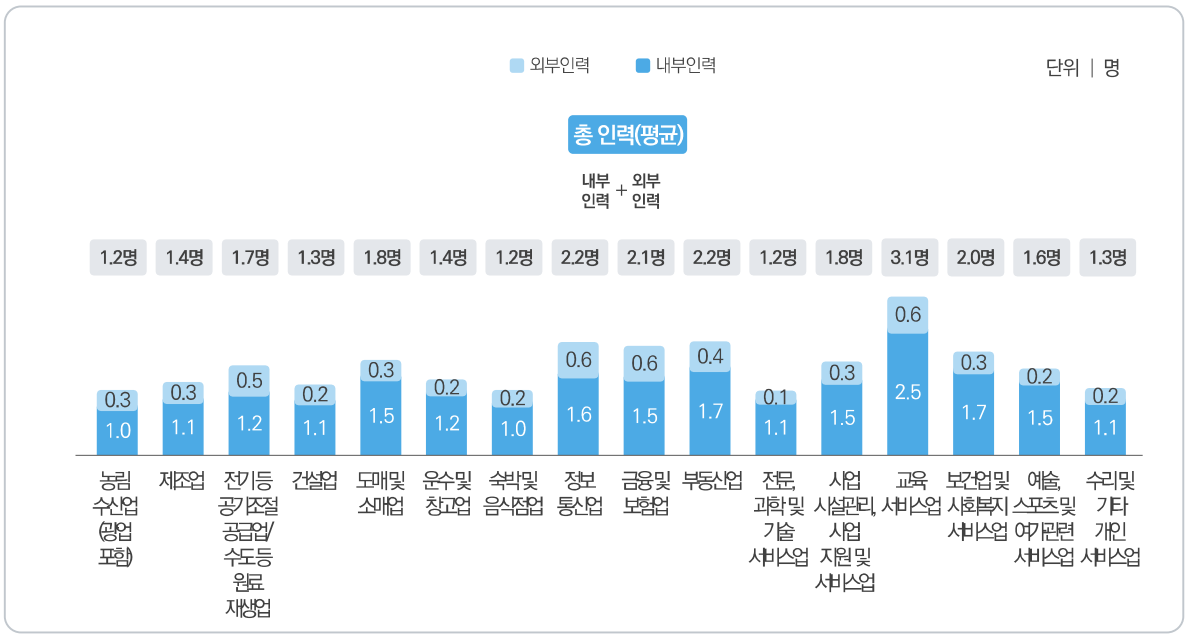


그림 1-3-30 업종별 사무직 인력 중 정보보호 업무 수행 인력

- 규모별 분석 결과, 종사자 수 규모가 '50~249명'인 경우 내부인력 1.8명, 외부인력 0.5명으로 가장 높은 것으로 나타났다.

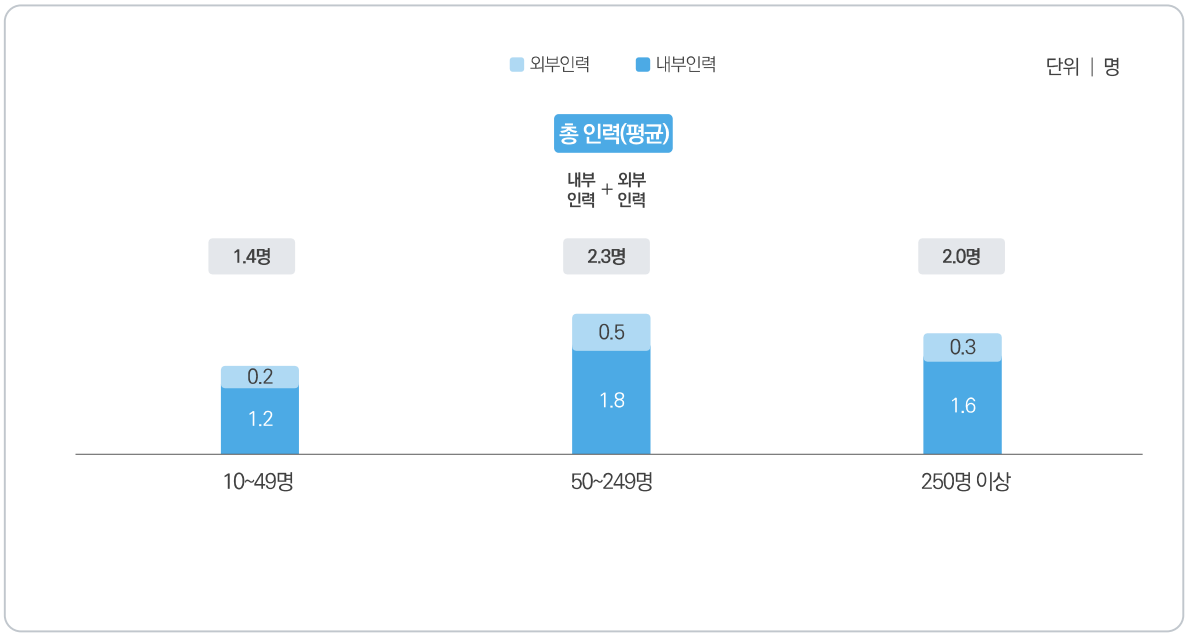


그림 1-3-31 규모별 사무직 인력 중 정보보호 업무 수행 인력

라 개인정보보호 업무 겸직 여부

- 정보보호 담당 인력을 보유하고 있는 기업체 중 개인정보보호 업무를 겸직하는 비율은 내부인력 76.3%, 외부인력 44.2%로 조사되었다.

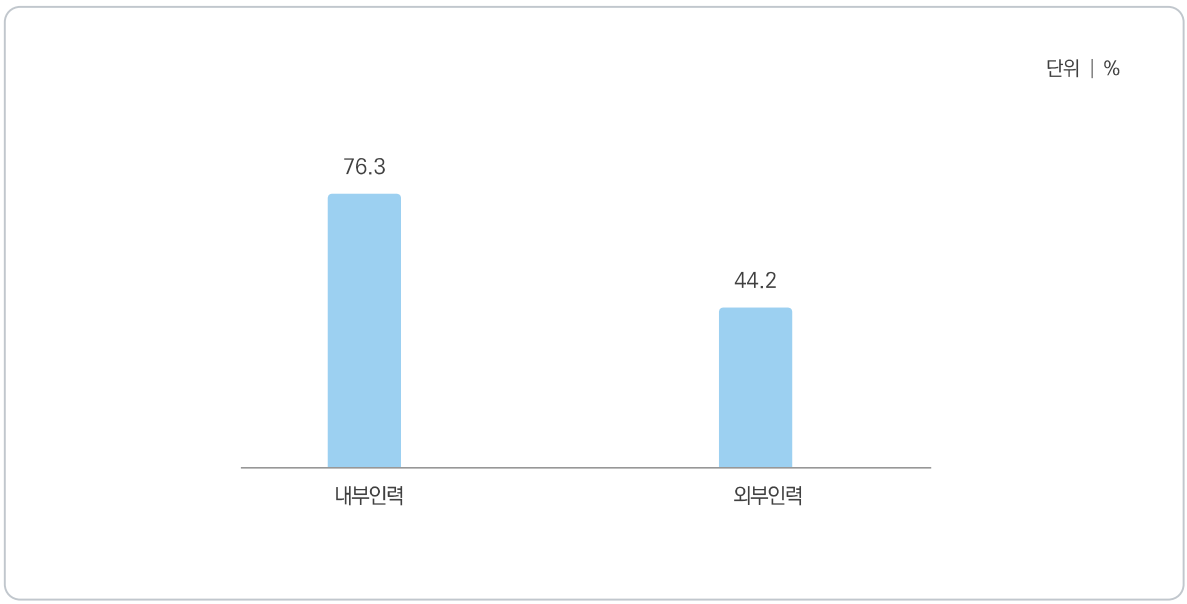


그림 1-3-32 개인정보보호 업무 겸직 여부 - 정보보호 담당 인력 보유 기업체

- 업종별 분석 결과, '농림수산업(광업포함)'의 내부인력이 이 86.1%로 가장 높게 나타났고, 다음으로 '예술, 스포츠 및 여가관련 서비스업(85.0%)', '보건업 및 사회복지 서비스업(84.4%)' 등의 순으로 조사되었다.

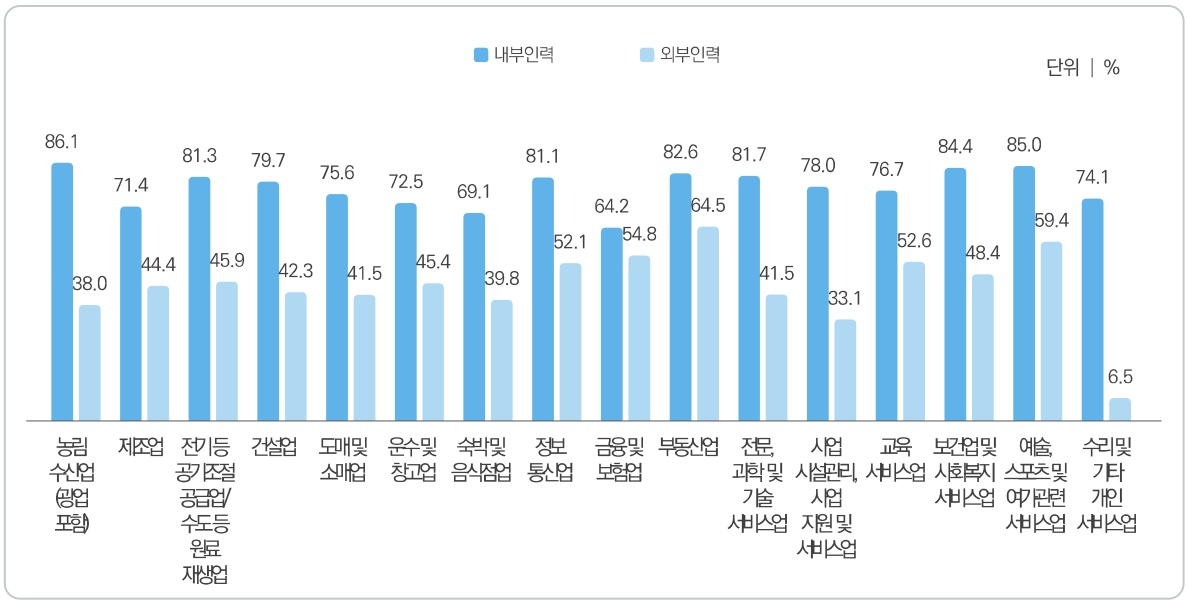


그림 1-3-33 업종별 개인정보보호 업무 겸직 여부 - 정보보호 담당 인력 보유 기업체

- 규모별 분석 결과, 종사자 규모가 '50~249명'인 경우 개인정보보호 업무를 겸직하는 비율이 높게 나타났다.

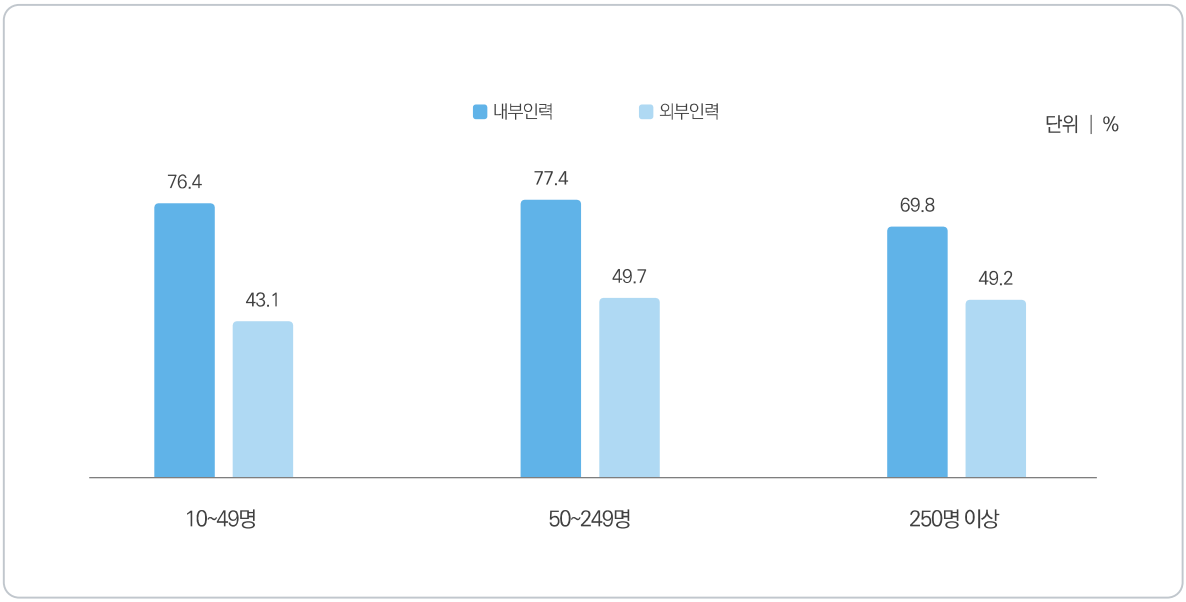


그림 1-3-34 규모별 개인정보보호 업무 겸직 여부 - 정보보호 담당 인력 보유 기업체

Ⅲ 정보보호 교육

1 정보보호 교육

가 정보보호 교육 실시

- 국내 기업체 중 32.6%는 임직원을 대상으로 정보보호 교육을 실시한 것으로 나타났다.

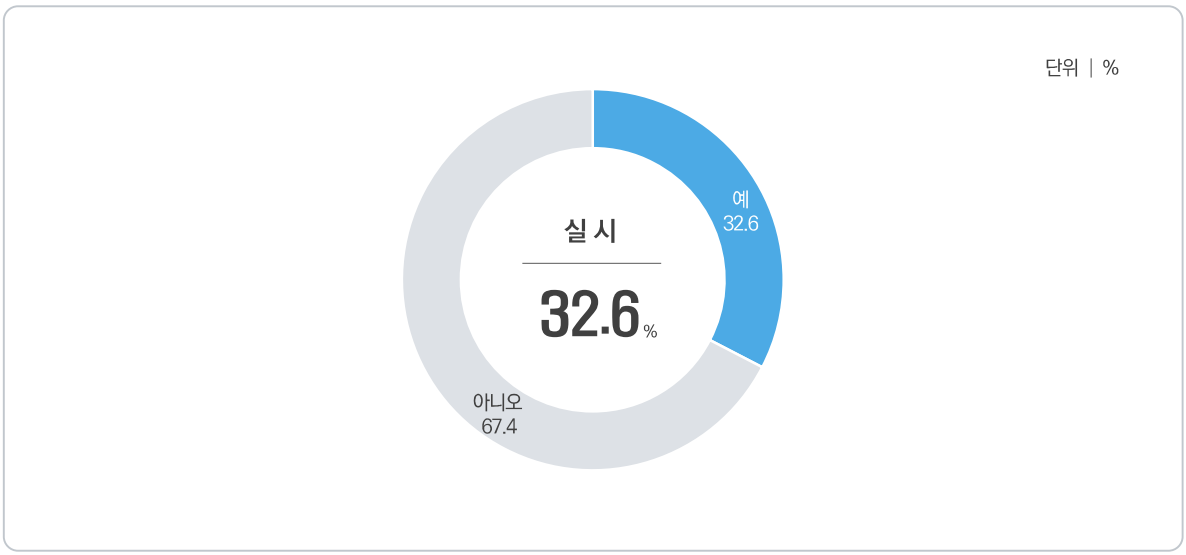


그림 1-3-35 정보보호 교육 실시

- 업종별 분석 결과, '금융 및 보험업'이 60.7%로 가장 높게 나타났고, 다음으로 '농림수산업(광업포함)(49.4%)', '보건업 및 사회복지 서비스업(44.1%)' 등의 순으로 조사되었다.

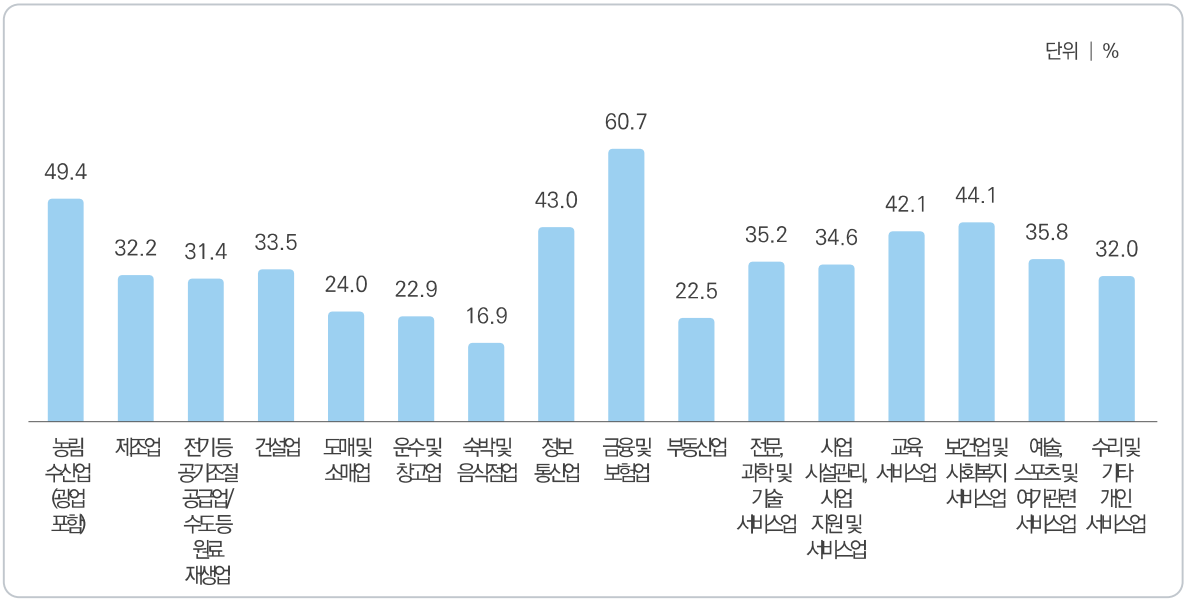


그림 1-3-36 업종별 정보보호 교육 실시

- 규모별 분석 결과, 종사자 수가 많을수록 정보보호 교육 실시 비율이 높게 나타났다.

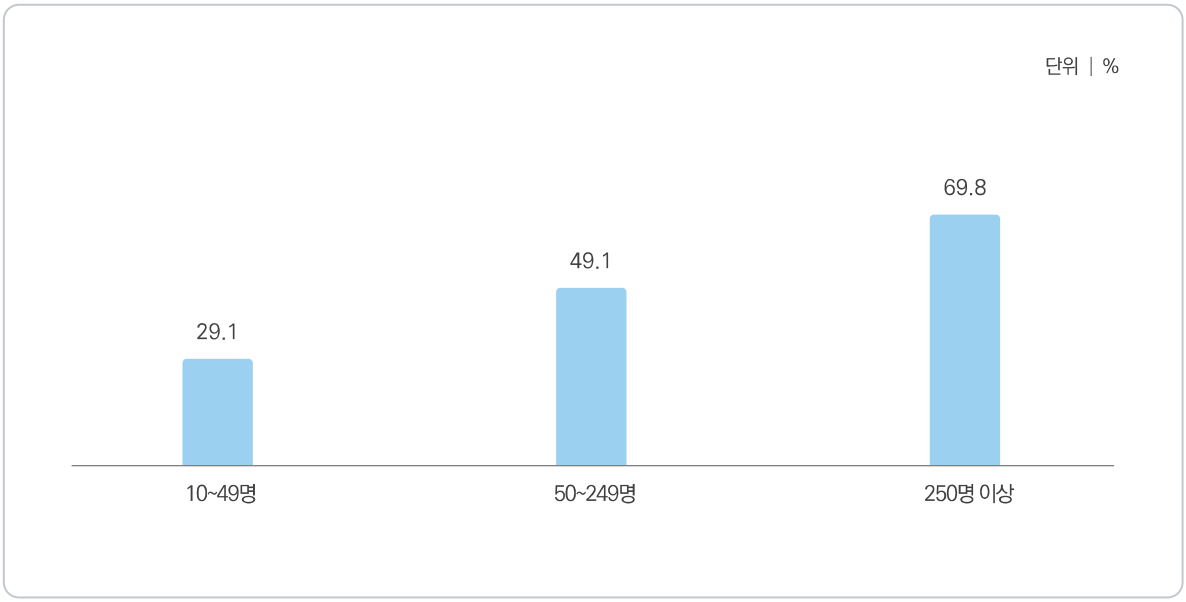


그림 1-3-37 규모별 정보보호 교육 실시

나 대상별 교육 실시 현황

- 교육 대상별 분석 결과, 정보보호 교육을 받는 대상으로는 '일반직원'이 82.4%로 가장 높게 나타났고, 다음으로 'CEO 및 경영진(75.9%)', 'IT 관련 직원(59.9%)' 등의 순으로 조사되었다.

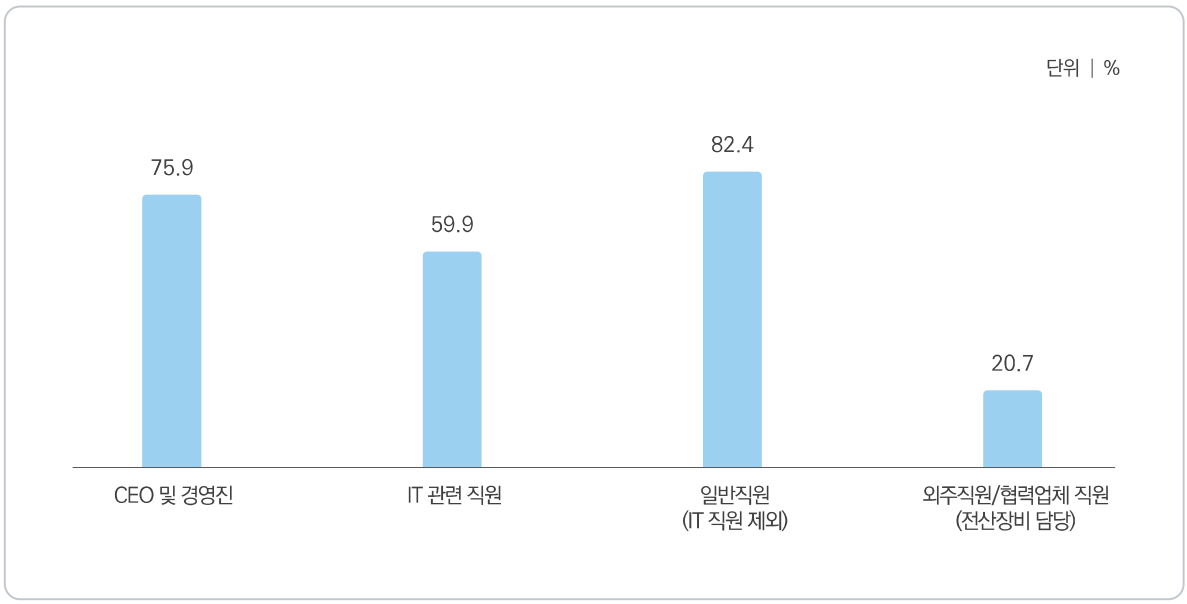


그림 1-3-38 대상별 교육 실시 현황(복수응답) – 정보보호 교육 실시 기업체

다 정보보호 교육 방법

- 정보보호 교육 방법은 정보보호 교육을 받는 모든 대상에서 '자체 교육(외부 강사)'이 가장 높게 조사되었다.

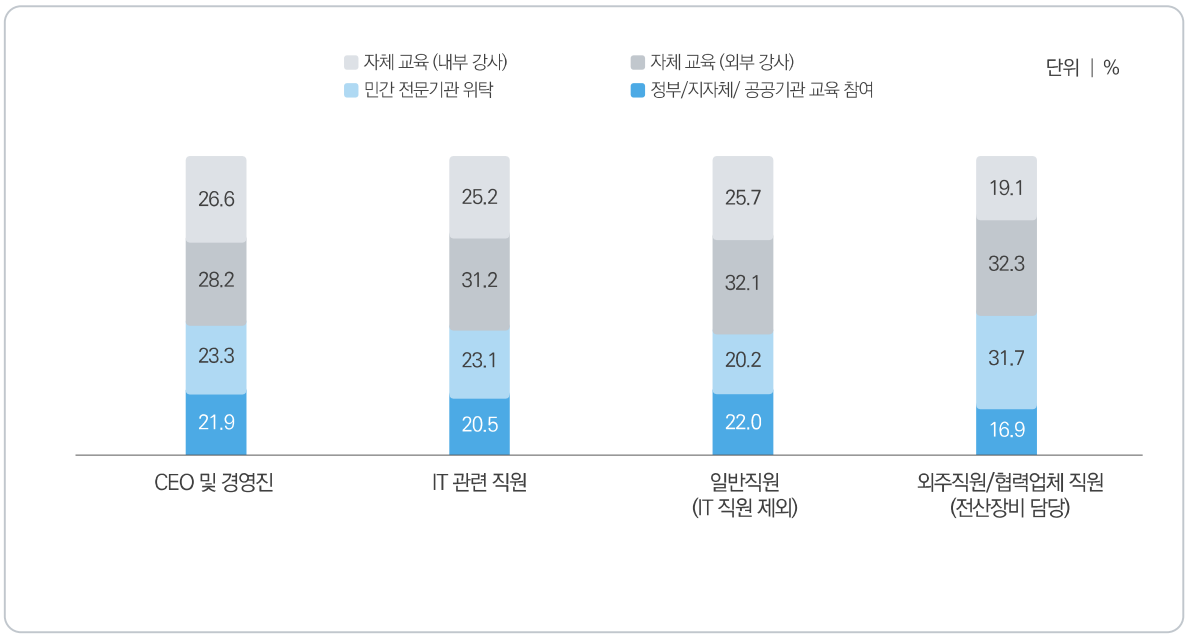


그림 1-3-39 대상별 교육 방법(복수응답) – 정보보호 교육 실시 기업체

라 정보보호 교육 방식

- 정보보호 교육 방식은 외주직원/협력업체 직원(전산장비 담당)을 제외한 정보보호 교육을 받는 모든 대상에서 온라인 교육이 60%대, 오프라인 교육이 30%대로 조사되었다.

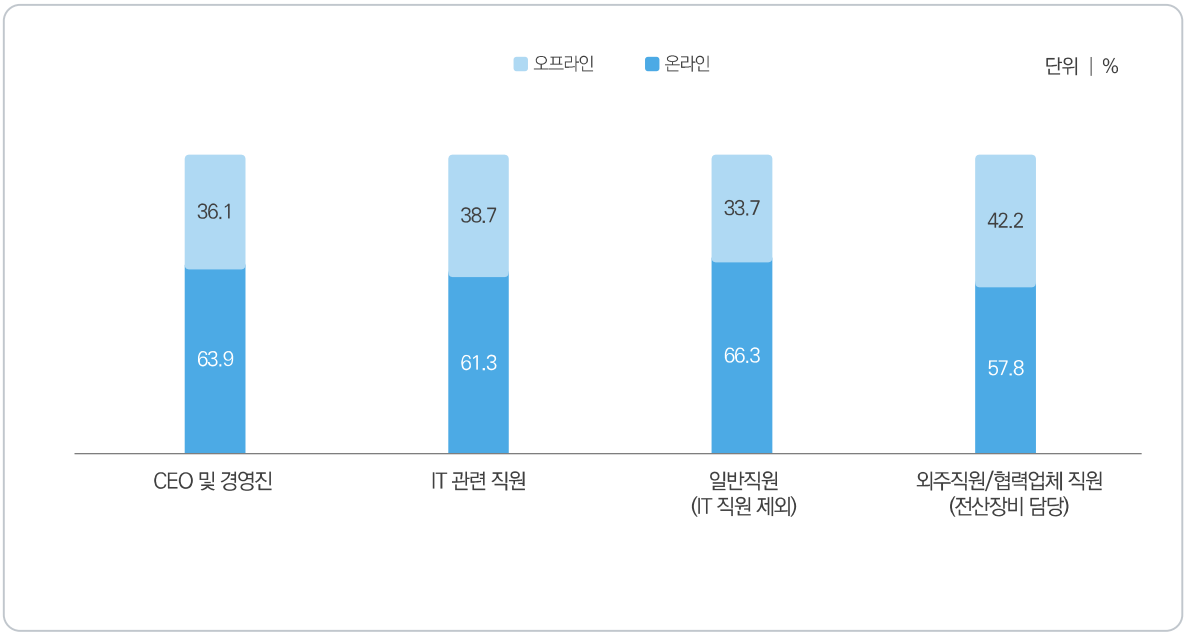


그림 1-3-40 대상별 교육 방식(복수응답) – 정보보호 교육 실시 기업체

마 정보보호 교육 자료 출처

- 정보보호 교육 자료의 출처로는 '정부 또는 공공기관에서 제공하는 공식적인 온라인 교육 자료 활용'이 46.3%로 가장 높고, 다음으로 '외부 전문 위탁 기관에 의뢰하여 제작한 교육 자료 활용(30.2%)', '외부 전문 위탁 기관에서 대여 또는 구입한 교육 자료 활용(20.6%)', '사내 보안 부서에서 자체 제작한 교육 자료 활용(19.1%)' 등의 순으로 나타났다.

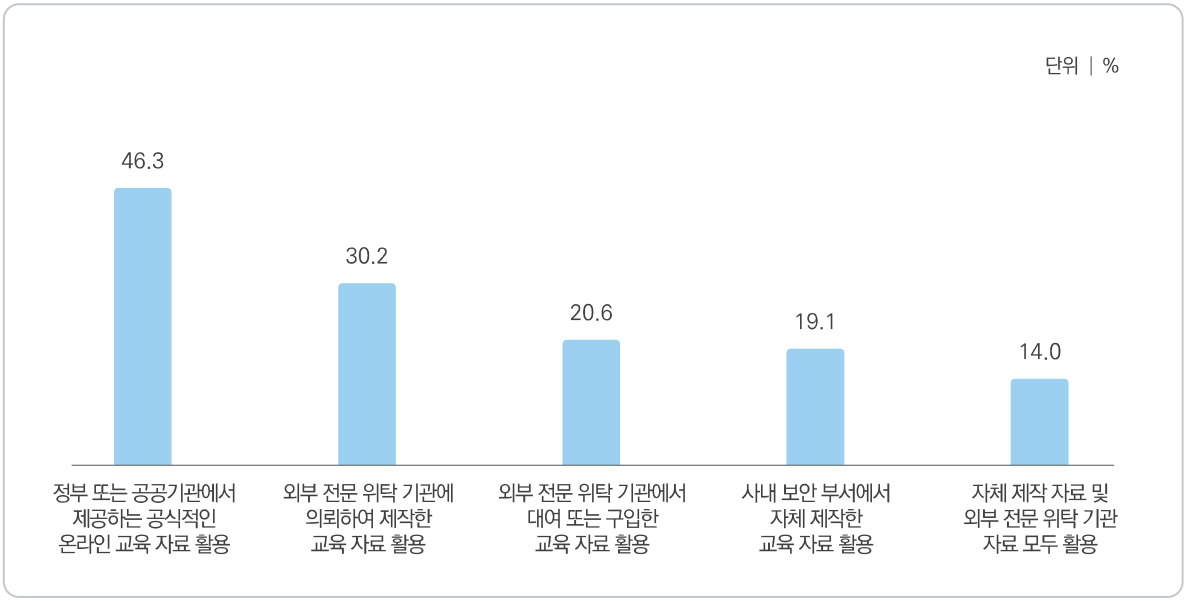


그림 1-3-41 정보보호 교육 자료 출처(복수응답) - 정보보호 교육 실시 기업체

바 정보보호 교육 효과

- 정보보호 교육을 실시한 국내 기업체의 92.3%가 교육이 효과적이다(효과가 있는 편이다 + 매우 효과적이다)고 응답했다.

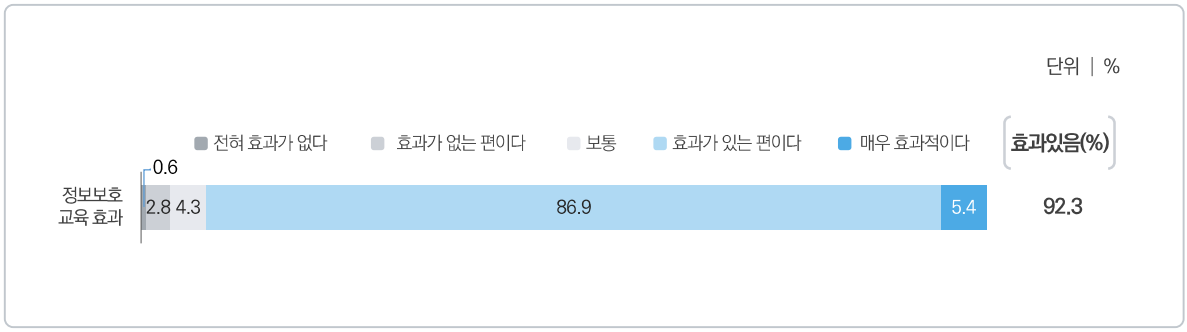


그림 1-3-42 정보보호 교육 효과 - 정보보호 교육 실시 기업체

사 정보보호 교육 만족도

- 정보보호 교육을 실시한 국내 기업체의 89.9%가 교육이 만족스럽다(높은 편이다 + 매우 높다)고 응답했다.

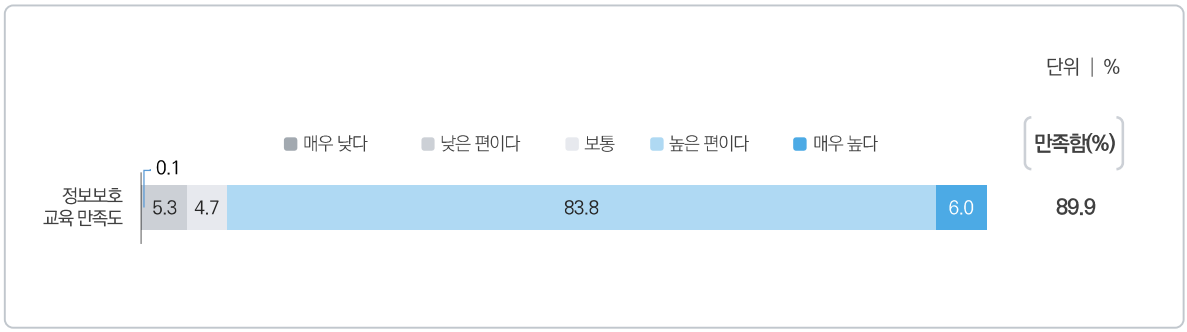


그림 1-3-43 정보보호 교육 만족도 - 정보보호 교육 실시 기업체

Ⅳ 정보보호 예산

1 정보보호 예산

가 정보보호 예산 사용

- 국내 기업체 중 67.9%는 정보보호 예산을 사용해 본 경험이 있는 것으로 조사되었다.

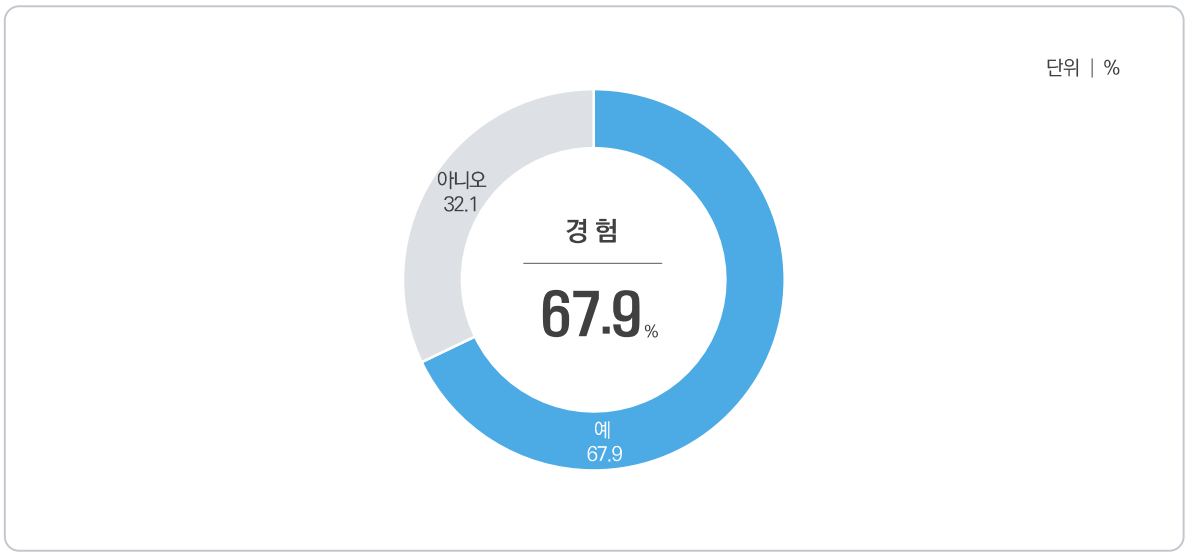


그림 1-3-44 정보보호 예산 사용

- 업종별 분석 결과, '전문, 과학 및 기술 서비스업'이 85.9%로 가장 높게 나타났고, 다음으로 '금융 및 보험업(84.7%)', '숙박 및 음식점업(84.1%)' 등의 순으로 조사되었다.

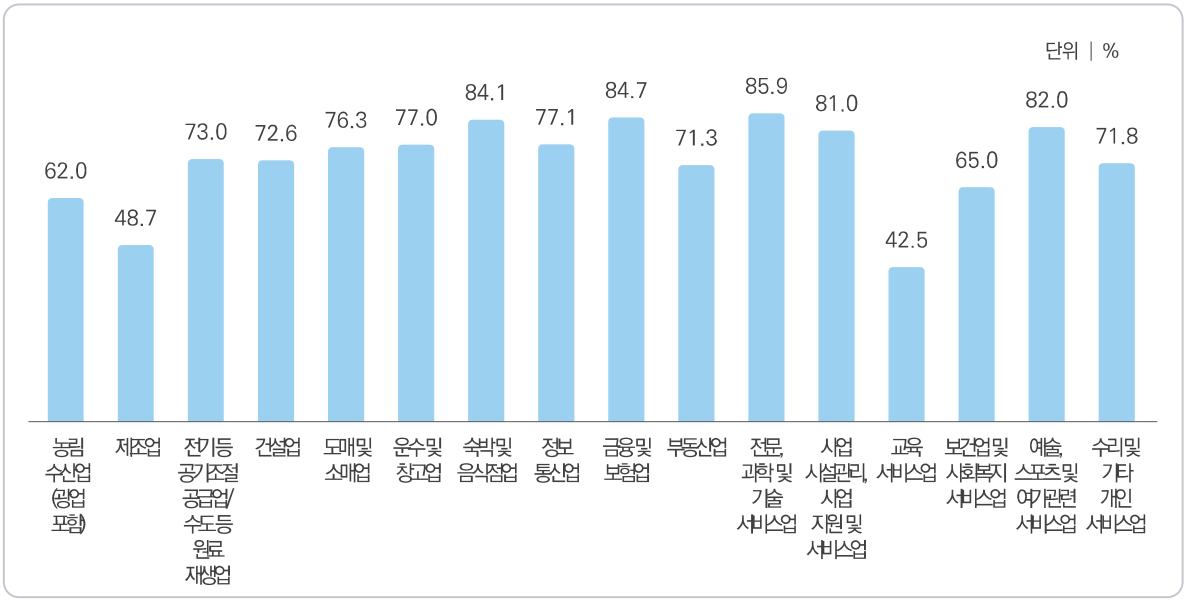


그림 1-3-45 업종별 정보보호 예산 사용

- 규모별 분석 결과, 종사자 수가 많을수록 정보보호 예산 사용 비율이 높게 나타났다.

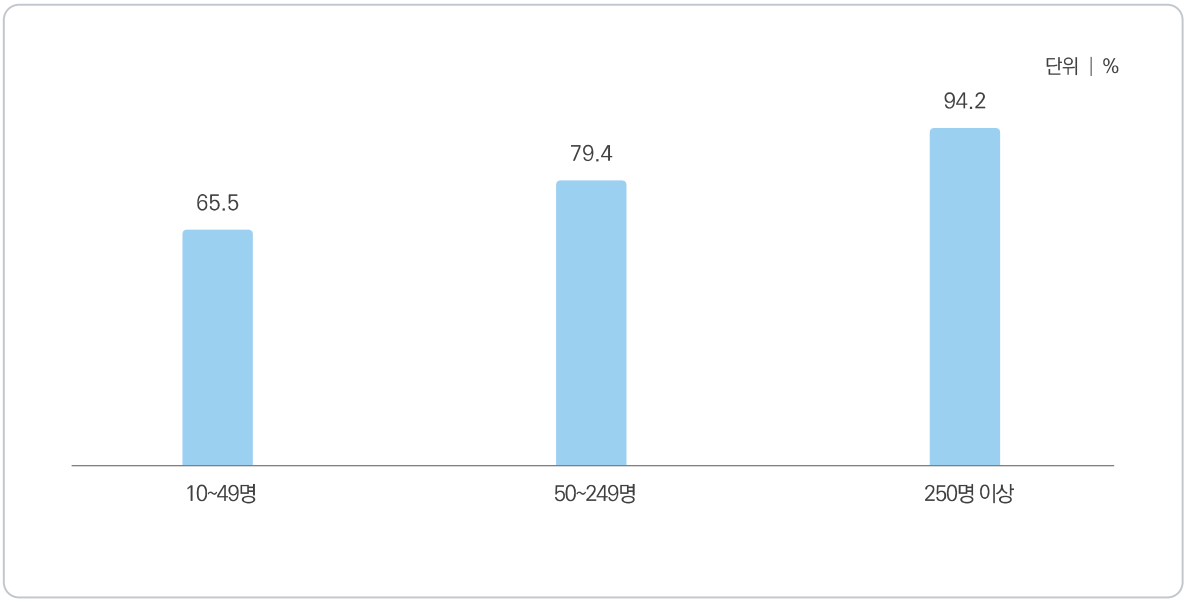


그림 1-3-46 규모별 정보보호 예산 사용

나 정보보호 예산 미사용 이유

- 국내 기업체의 정보보호 예산 미사용 이유로는 '정보보호 예산을 투입할 인적, 경제적 여력 부족'이 51.5%로 가장 높게 나타났으며, 다음으로 '필요한 정보보호 관련 활동이 무엇인지 모름(41.6%)', '현재 사업 영역이 정보보호와 무관함(40.9%)', '정보보호 침해사고는 기업의 노력만으로 해결 불가능함(37.4%)' 등의 순으로 조사되었다.

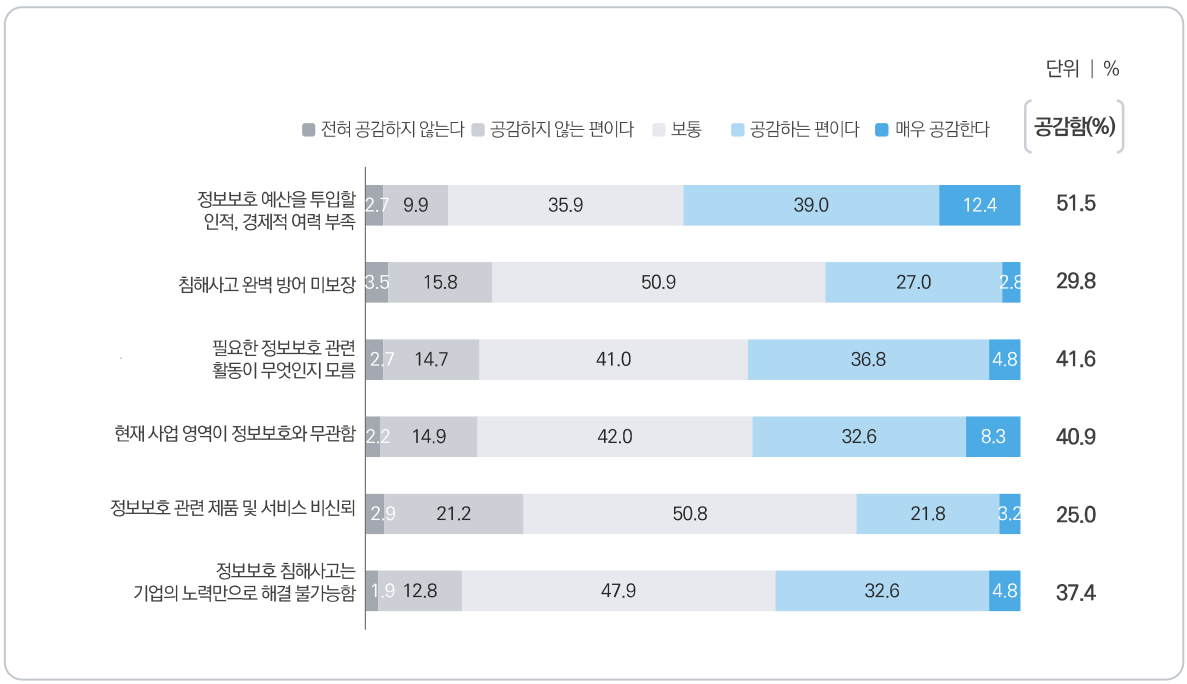


그림 1-3-47 정보보호 예산 미사용 이유 - 정보보호 예산 미사용 기업체

다 정보보호 예산 총액

- 국내 기업체의 정보보호 예산 총액은 '1,000만 원 이상 ~ 5,000만 원 미만'이 59.1%로 가장 높게 나타났으며, 다음으로 '500만 원 미만(22.1%)', '5,000만 원 이상 ~ 1억 원 미만(8.4%)', '500만 원 이상 ~ 1,000만 원 미만(7.4%)' 등의 순으로 조사되었다.

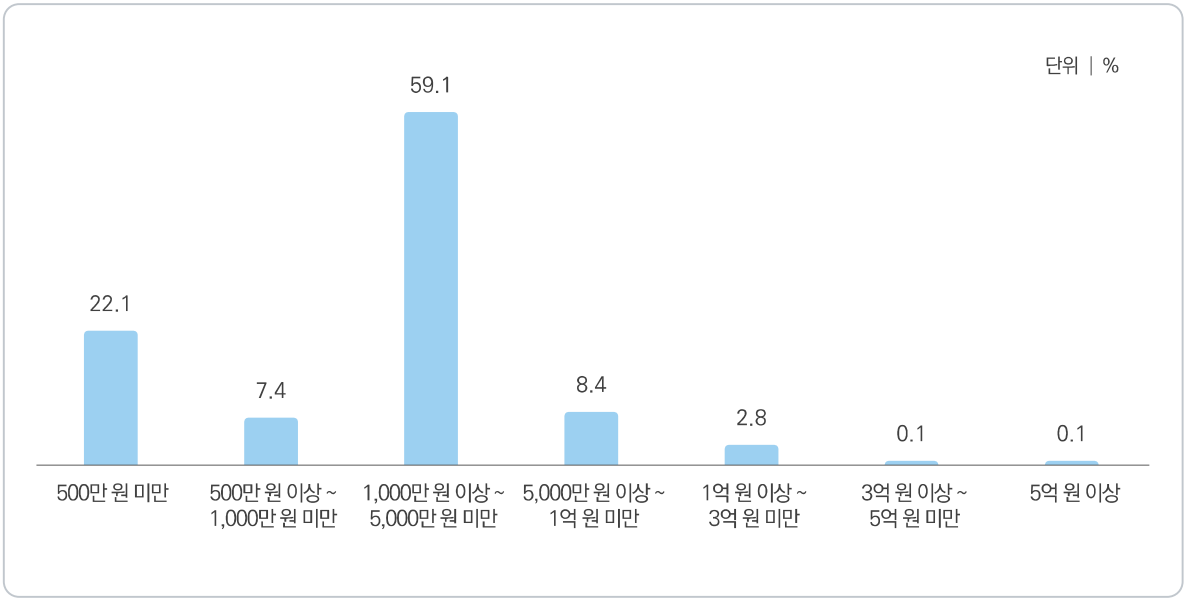


그림 1-3-48 정보보호 예산 총액 – 정보보호 예산 사용 기업체

라 정보보호 예산 총액 변화

- 정보보호 예산 사용 경험이 있는 기업체의 2020년 대비 2021년 관련 예산 총액의 변화는 '현상 유지'가 76.7%로 가장 높고, '증가(16.1%)', '감소(5.2%)', '신설(1.9%)'의 순으로 조사되었다.

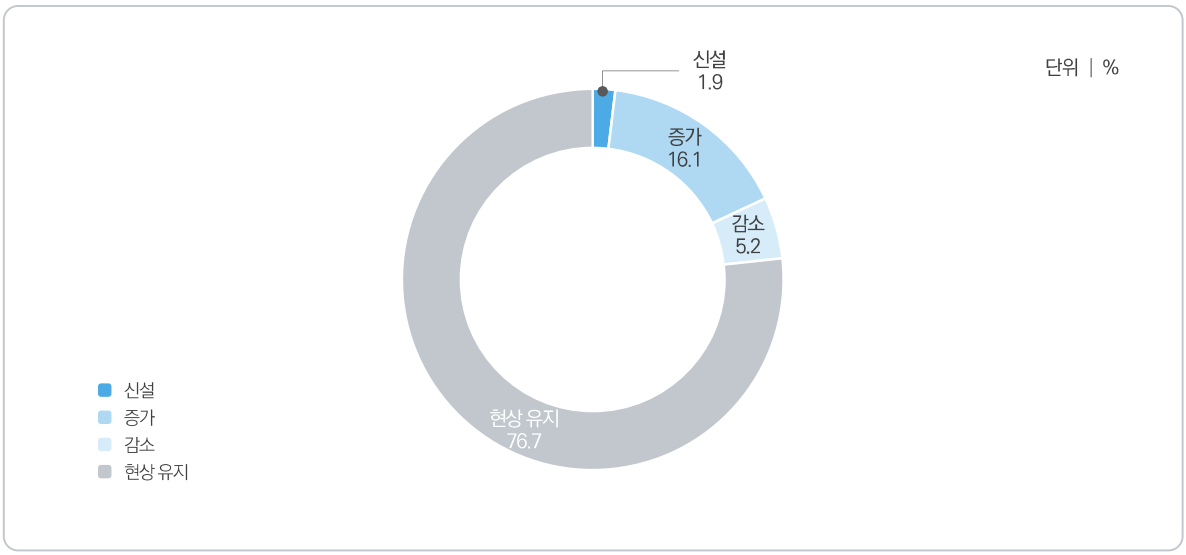


그림 1-3-49 정보보호 예산 총액 변화 – 정보보호 예산 사용 기업체

- 정보보호 예산이 신설된 기업체의 경우, 신설 이유로 '정보보호 사고 대응 관련 비용 증가'가 46.7%로 가장 높고, 다음으로 '정보보호 시스템 유지·보수 비용 증가(37.8%)', '정보보호 제품 구입 비용 증가(30.3%)', 'IT 예산 총액의 증가에 따른 변화(23.6%)' 등의 순으로 나타났다.

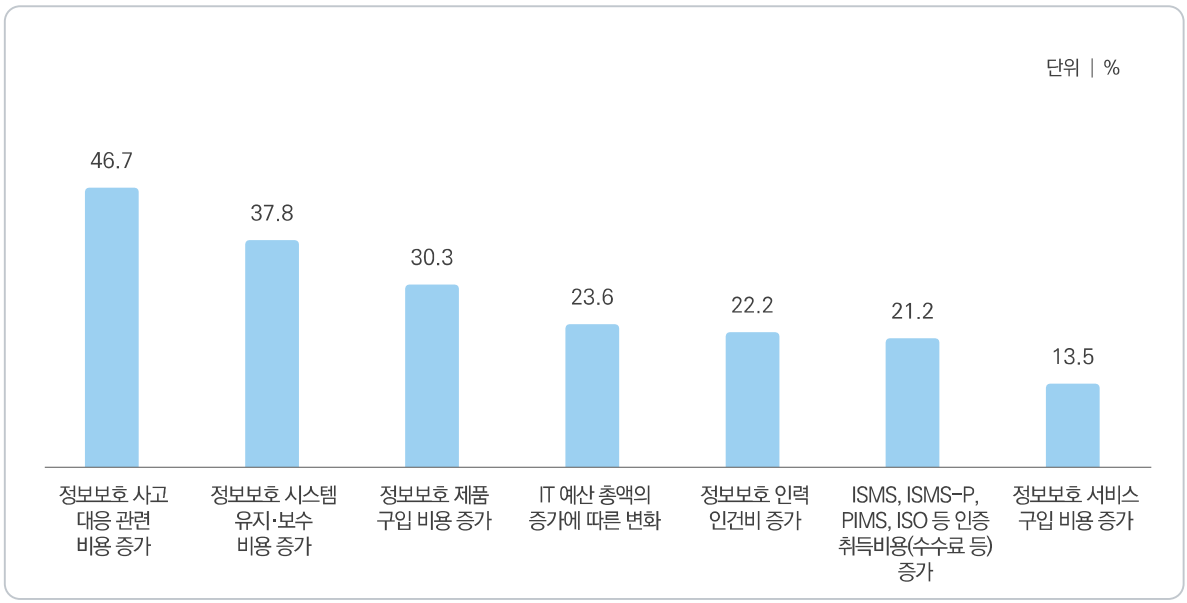


그림 1-3-50 정보보호 예산 총액 신설 이유(복수응답) – 정보보호 예산 신설 기업체

- 정보보호 예산이 증가한 기업체의 경우, 증가 이유로 '정보보호 인력 인건비 증가'가 50.8%로 가장 높고, 다음으로 '정보보호 시스템 유지·보수 비용 증가(32.5%)', '정보보호 제품 구입 비용 증가(30.5%)', 'IT 예산 총액의 증가에 따른 변화(27.3%)' 등의 순으로 나타났다.

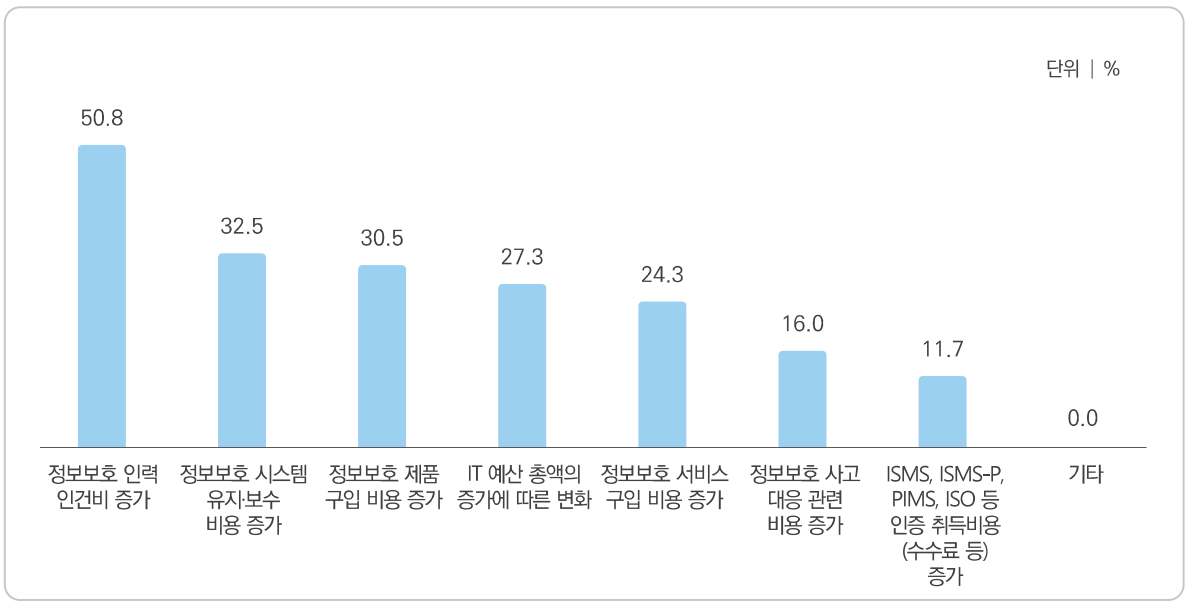


그림 1-3-51 정보보호 예산 총액 증가 이유(복수응답) – 정보보호 예산 증가 기업체

- 정보보호 예산이 감소한 기업체의 경우, 감소 이유로 '정보보호 제품 구입 비용 감소'가 51.9%로 가장 높고, 다음으로 'IT 예산 총액의 감소에 따른 변화(42.3%)', '정보보호 시스템 유지·보수 비용 감소(30.1%)', '정보보호 인력 인건비 감소(29.4%)' 등의 순으로 나타났다.

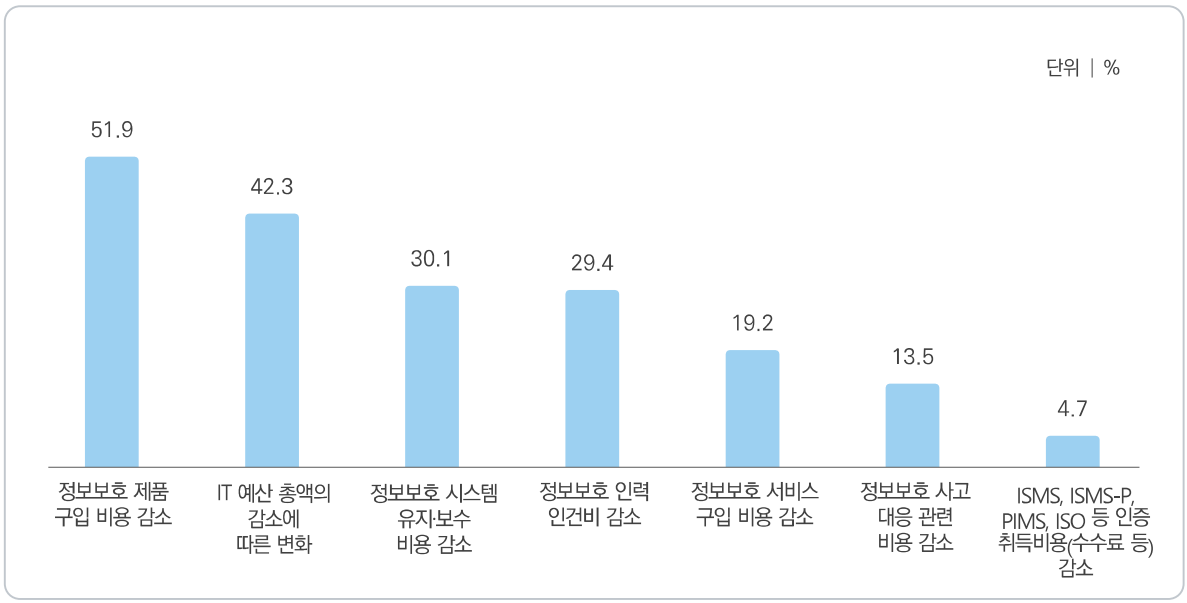


그림 1-3-52 정보보호 예산 총액 감소 이유(복수응답) – 정보보호 예산 감소 기업체

마 정보보호 예산 총액 변화 예상

- 국내 기업체의 향후 정보보호 예산 총액 변화에 대하여 증액할 것이라는 응답은 22.2%, 감액은 3.2%, 현상 유지는 74.6%로 나타났다.

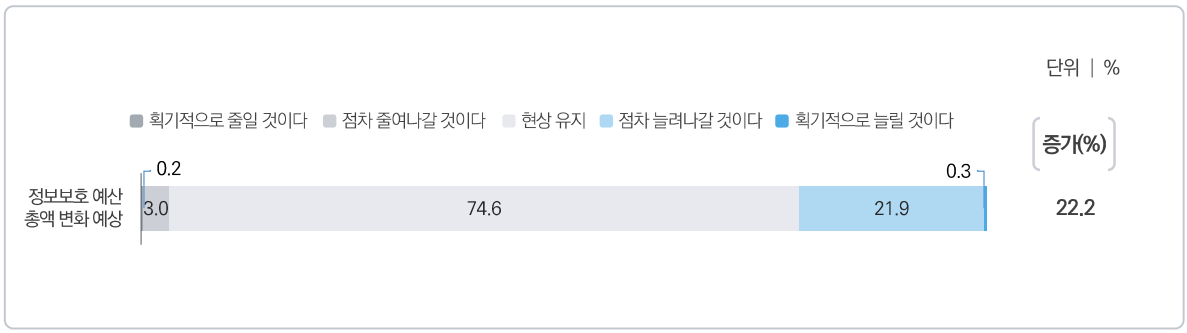


그림 1-3-53 정보보호 예산 총액 변화 예상 – 정보보호 예산 사용 기업체

바 정보보호 예산 활용 분야

- 정보보호 예산을 사용한 기업체는 2021년 1년간 '업무 시설의 CCTV 등 영상감시장비 설치 또는 증설(유지·보수 포함)(64.5%)'에 가장 많은 예산을 활용한 것으로 나타났고, 다음으로 '정보보호 관련 제품 및 솔루션의 유지·보수(49.2%)', '정보보안을 위한 출동 보안 서비스 이용(35.8%)' 등의 순으로 조사되었다.

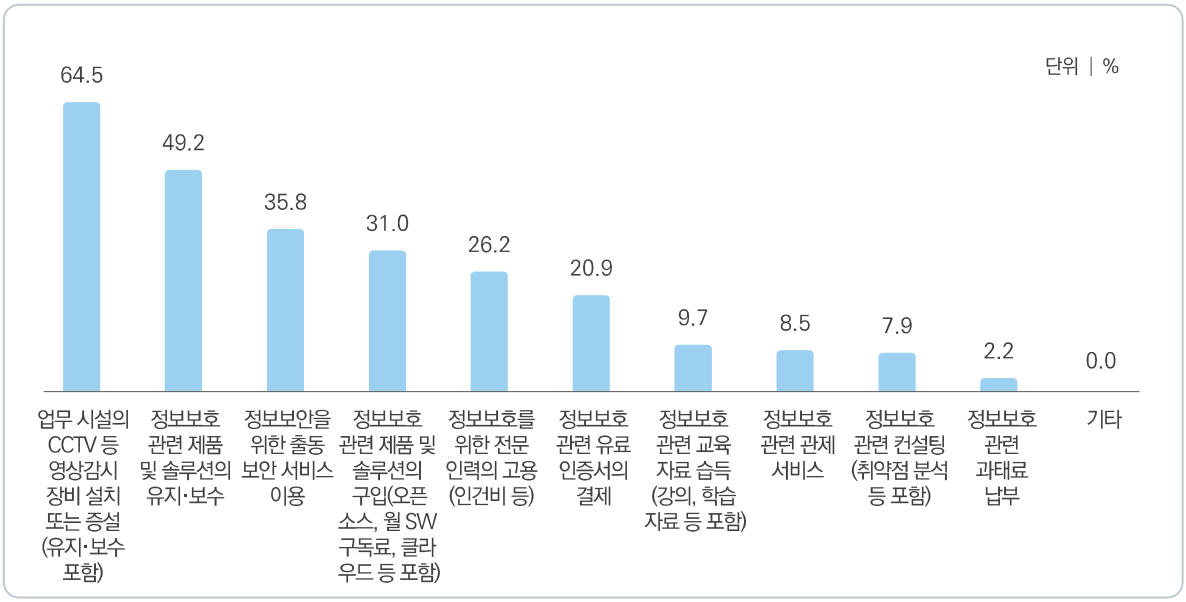


그림 1-3-54 정보보호 예산 활용 분야(복수응답) - 정보보호 예산 사용 기업체

사 정보보호 예산 활용 계기

- 정보보호 예산을 사용한 기업체의 예산 활용 계기는 'TV 또는 온라인 매체(뉴스, 유튜브, SNS 등)를 통한 정보 습득으로 위험성을 인지한 이후'가 31.0%로 가장 높고, 다음으로 '정보보호 기업체의 홍보 자료 또는 영업을 접한 이후(19.1%)', '주변 지인의 추천을 통해(18.6%)', '정보보호 관련 교육을 수강하여 위험성을 인지한 이후(14.6%)' 등의 순으로 조사되었다.

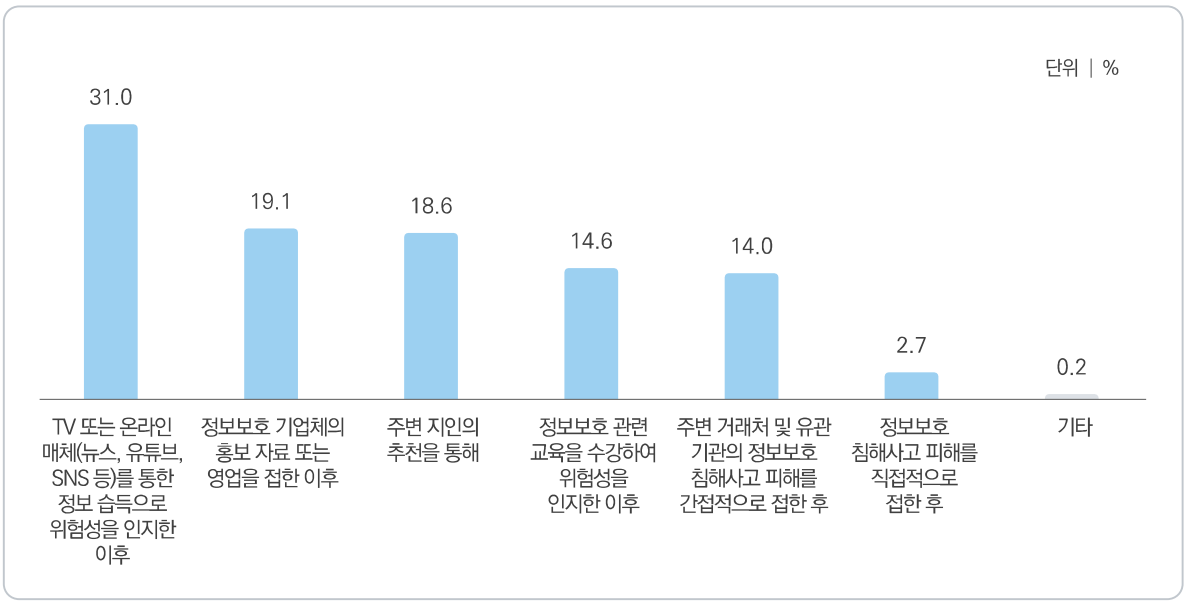


그림 1-3-55 정보보호 예산 활용 계기 – 정보보호 예산 사용 기업체

아 정보보호 예산 소비 적절성

- 정보보호 예산을 사용하는 국내 기업체 중 40.9%는 소비가 적절하다(그렇다 + 매우 그렇다)고 응답했다.

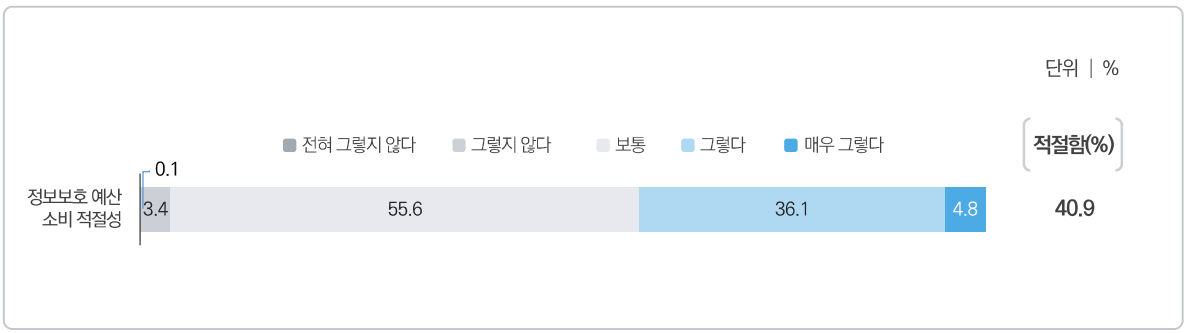


그림 1-3-56 정보보호 예산 소비 적절성 – 정보보호 예산 사용 기업체

자 정보보호 예산 소비 부적절 이유

- 예산을 사용하는 기업체 중 예산 소비가 적절하지 않다고 생각하는 기업체의 경우 '기업의 투자자·소유주가 불필요한 낭비로 인식'이 63.4%로 가장 높고, 다음으로 '정보보호 제품·솔루션·서비스의 높은 단가(55.1%)', '정보보호 제품·솔루션·서비스의 필요성이 명확하지 않음(53.2%)', '정보보호는 전문적인 영역으로 합리적 소비 판단이 어려움(37.3%)' 등의 순으로 조사되었다.

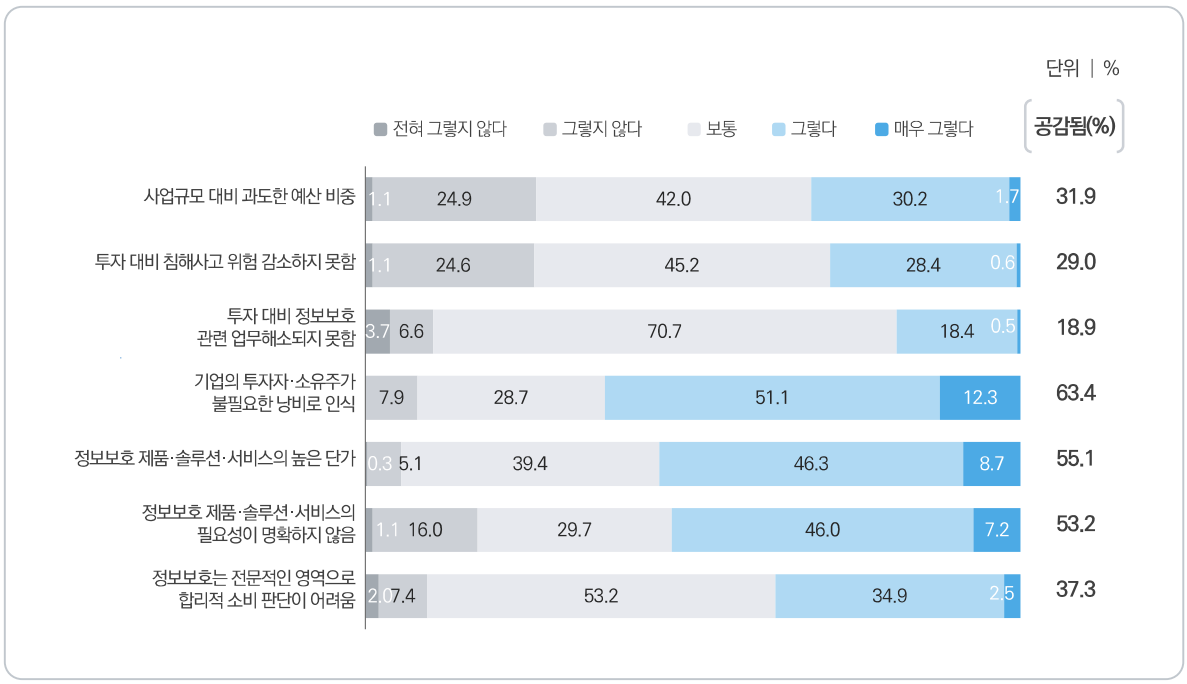


그림 1-3-57 정보보호 예산 소비 부적절 이유 – 정보보호 예산 사용이 적절하지 않다고 응답한 기업체

2 국내외 정보보호 제품 및 서비스 선호도

- 국내 기업체의 국산/외산 제품 및 서비스 선호도는 국산이 48.8%, 외산이 5.6%로 조사되었으며, 45.7%의 기업체는 특별히 선호도를 구분하지 않는다고 응답하였다.

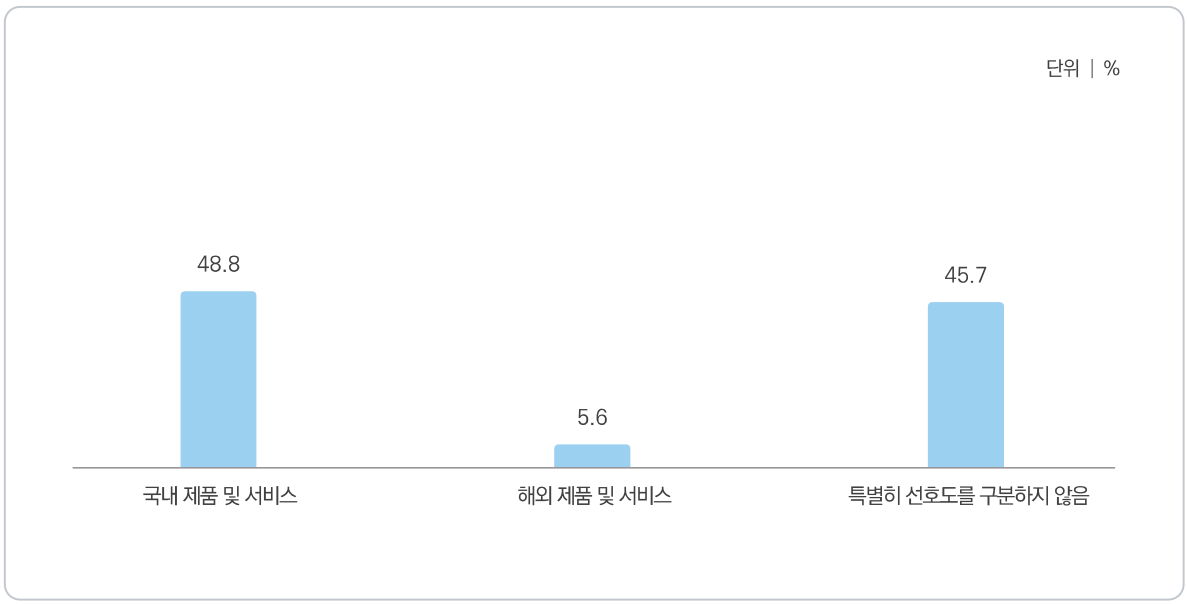


그림 1-3-58 국내외 정보보호 제품 및 서비스 선호도

V 침해사고 예방

1 정보보호 제품 및 솔루션

- 국내 기업체 중 80.7%는 정보보호(정보보안 또는 물리보안)를 위해 관련 제품 및 솔루션을 사용하고 있는 것으로 나타났다.

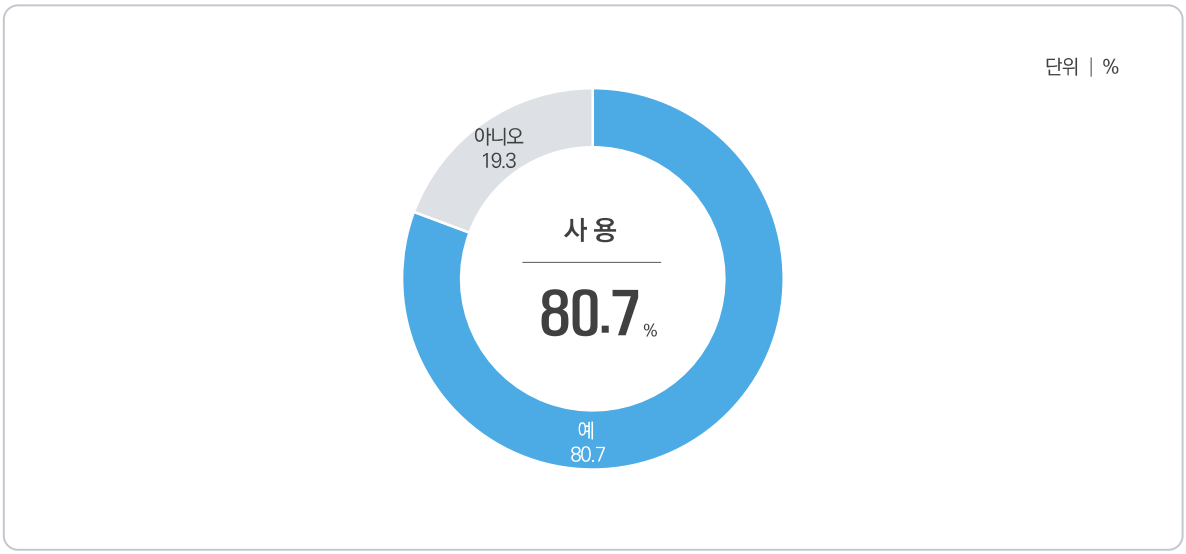


그림 1-3-59 정보보호 제품 및 솔루션 사용

- 정보보안 제품군 중 '시스템(앤드 포인트) 보안 장비' 이용률이 73.6%로 가장 높게 나타났고, 다음으로 '네트워크 보안 장비(62.1%)', '보안 시스템 유지/관리 서비스(9.6%)', '콘텐츠/데이터 보안/정보유출 방지 장비(8.6%)' 등의 순으로 조사되었다.

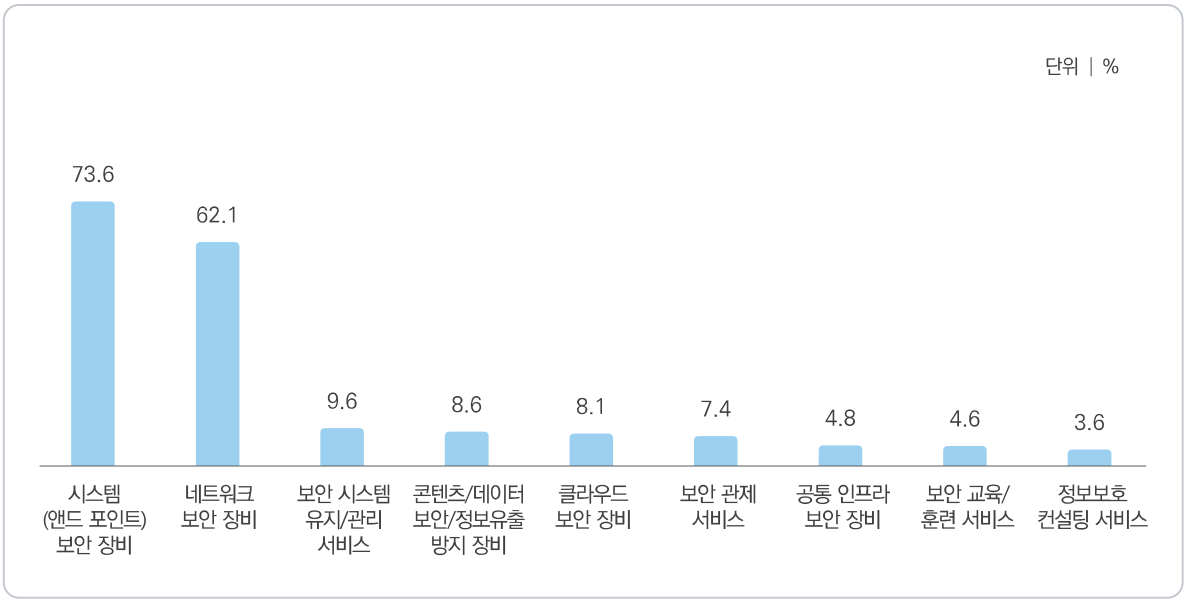


그림 1-3-60 정보보호 제품 및 솔루션 사용 중 정보보안(복수응답) - 정보보호 제품 및 솔루션 사용 기업체

- 물리보안 제품군 중 '출입통제 관리 시스템(출입통제 게이트, 디지털 도어락)' 이용률은 77.7%로 가장 높고, 다음으로 '영상 보안 시스템(IP카메라, CCTV 등)(48.8%)', '출동 보안 서비스(사설 경비 업체 등)(43.2%)' 등의 순으로 조사되었다.

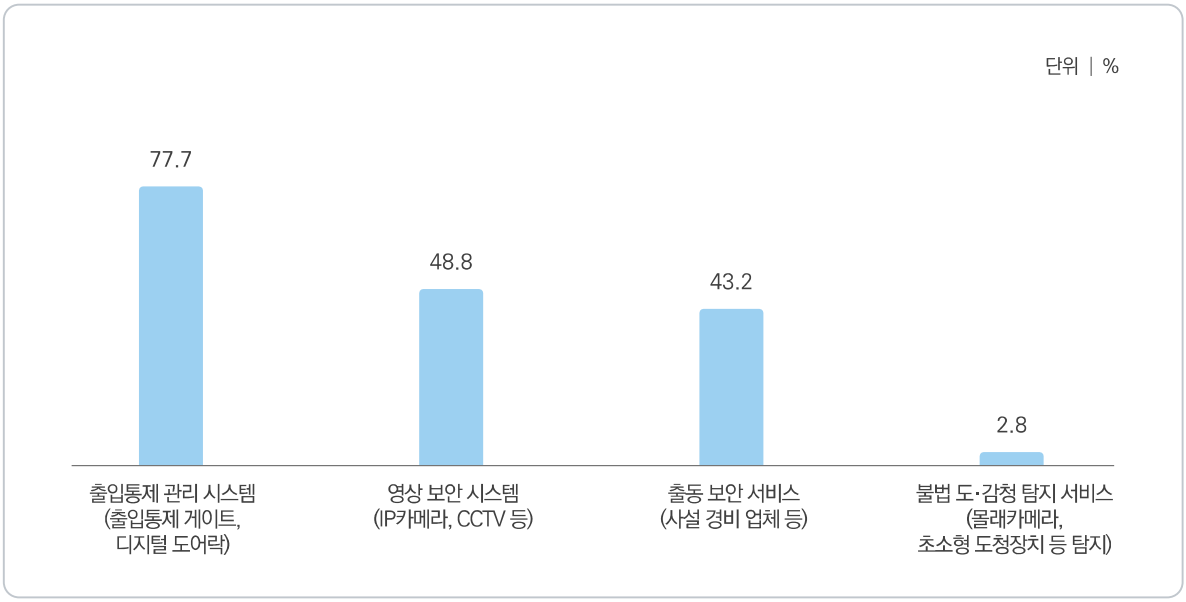


그림 1-3-61 정보보호 제품 및 솔루션 사용 중 물리보안(복수응답) - 정보보호 제품 및 솔루션 사용 기업체

- 정보보호 제품 및 솔루션을 활용하는 국내 기업체 중 20.6%가 사용 중인 제품 및 솔루션에 대해 정보보호 인증을 받은 것으로 조사되었다.

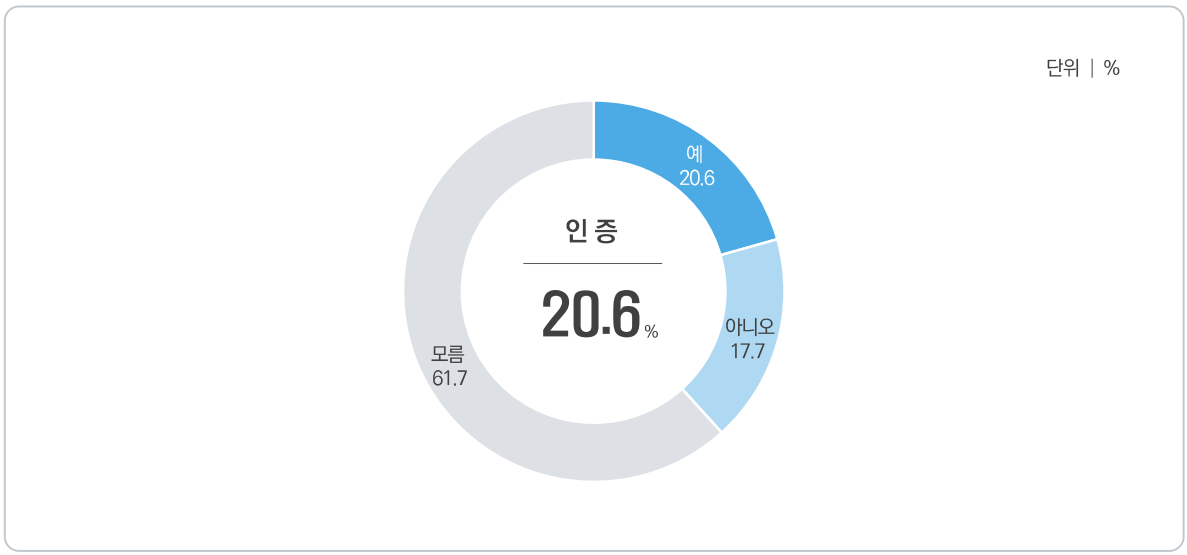


그림 1-3-62 활용 제품 정보보호 인증 인지 여부 – 정보보호 제품 및 솔루션 사용 기업체

2 CCTV 활용 현황

가 주 사업장

- 주 사업장의 CCTV 활용 현황에 대해 관리 방법은 '간접(업체 위탁) 관리'가 54.5%로 가장 높고, 다음으로 '직접 관리(48.5%)', '건물 자체 관리(38.3%)' 순으로 나타났다.

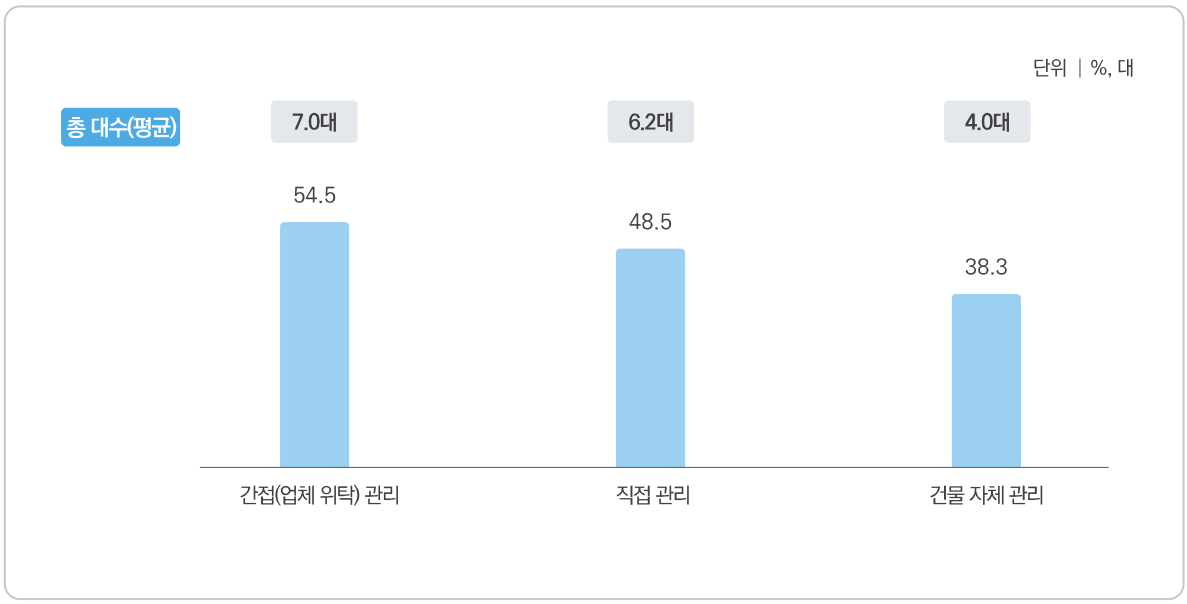


그림 1-3-63 CCTV 활용 현황(복수응답) - 주 사업장

나 본사

- 본사의 CCTV 활용 현황에 대해 관리 방법은 '간접(업체 위탁) 관리'가 54.1%로 가장 높고, 다음으로 '직접 관리(48.2%)', '건물 자체 관리(38.3%)' 순으로 나타났다.

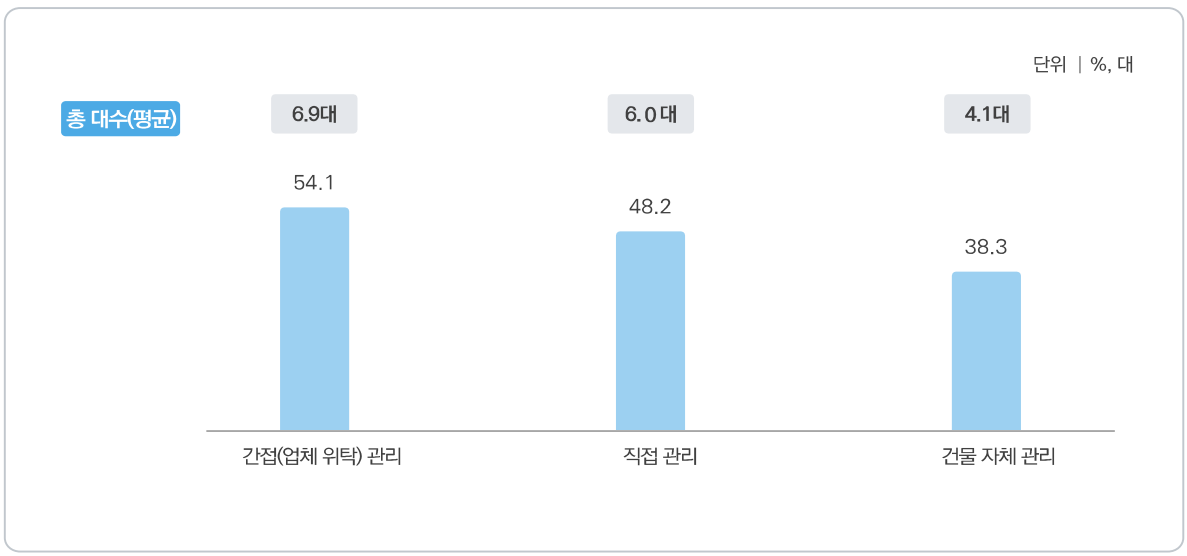


그림 1-3-64 CCTV 활용 현황(복수응답) - 본사

3 정보보호 관리

가 보안 점검

- 국내 기업체 중 81.2%가 IT 시스템 및 네트워크에 대한 보안 점검을 실시하는 것으로 나타났다. 최근 점검 실시 시점은 '6개월 이상 ~ 1년 미만'이 25.5%로 가장 높고, 다음으로 '1개월 이상 ~ 6개월 미만(23.3%)', '1년 이상 ~ 2년 미만(18.4%)' 등의 순으로 나타났다.

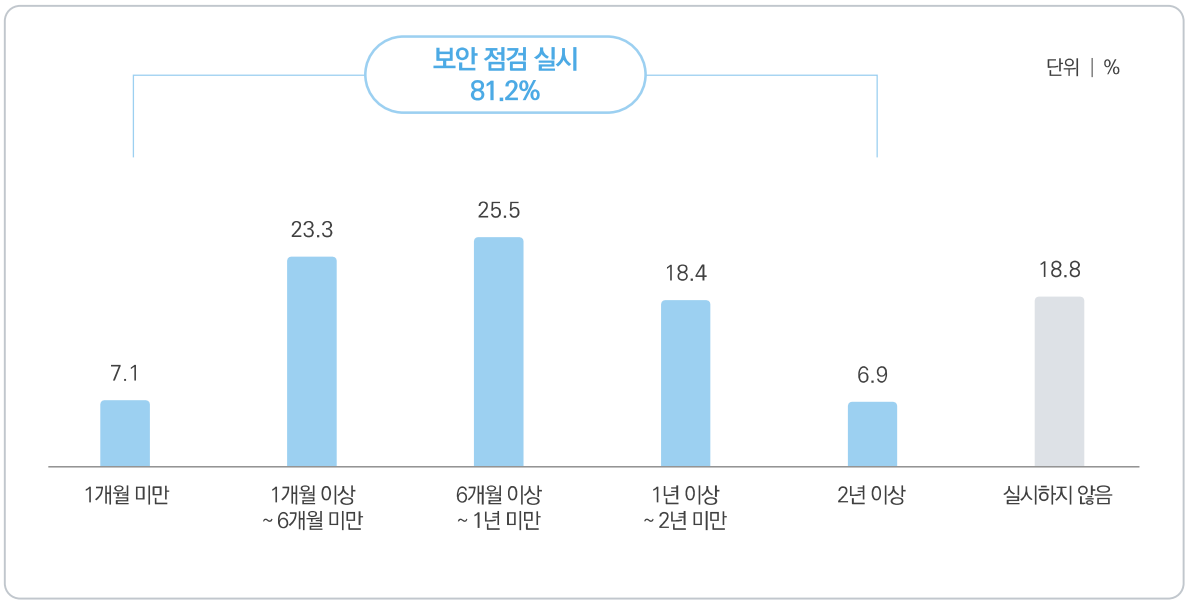


그림 1-3-65 IT 시스템 및 네트워크 보안 점검

나 로그 기록 관리

- 국내 기업체 중 69.9%가 시스템 및 방화벽 로그 기록을 관리하는 것으로 조사되었다.

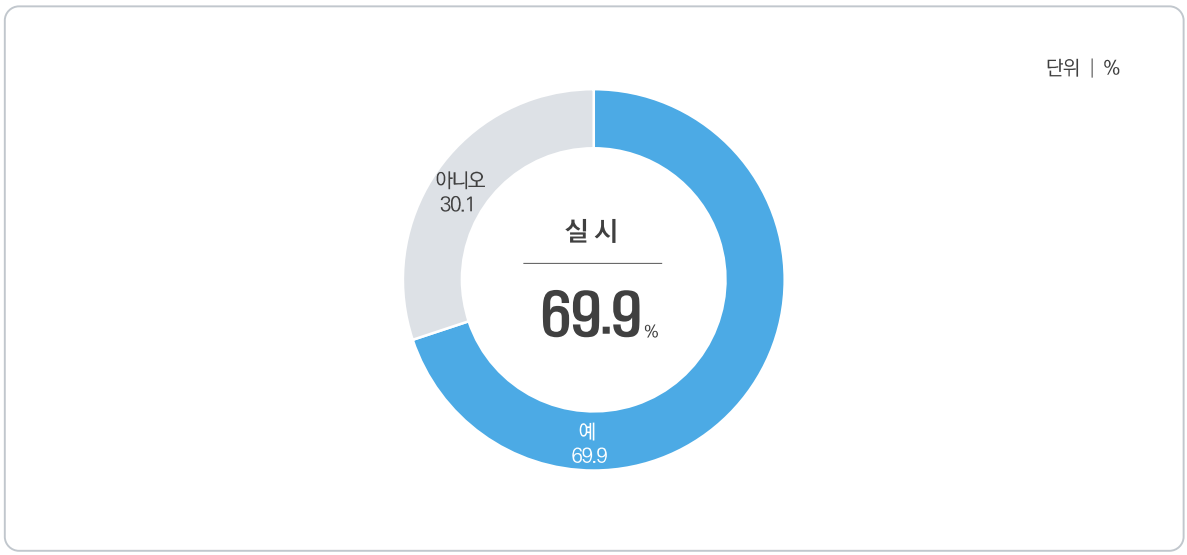


그림 1-3-66 시스템 및 방화벽 로그 기록 관리

- 시스템 및 방화벽 로그 기록 관리의 주기는 '6개월 이상'이 23.7%로 가장 높고, 다음으로 '1개월 이상 ~ 3개월 미만(16.8%)', '3개월 이상 ~ 6개월 미만(16.4%)' 등의 순으로 나타났다.

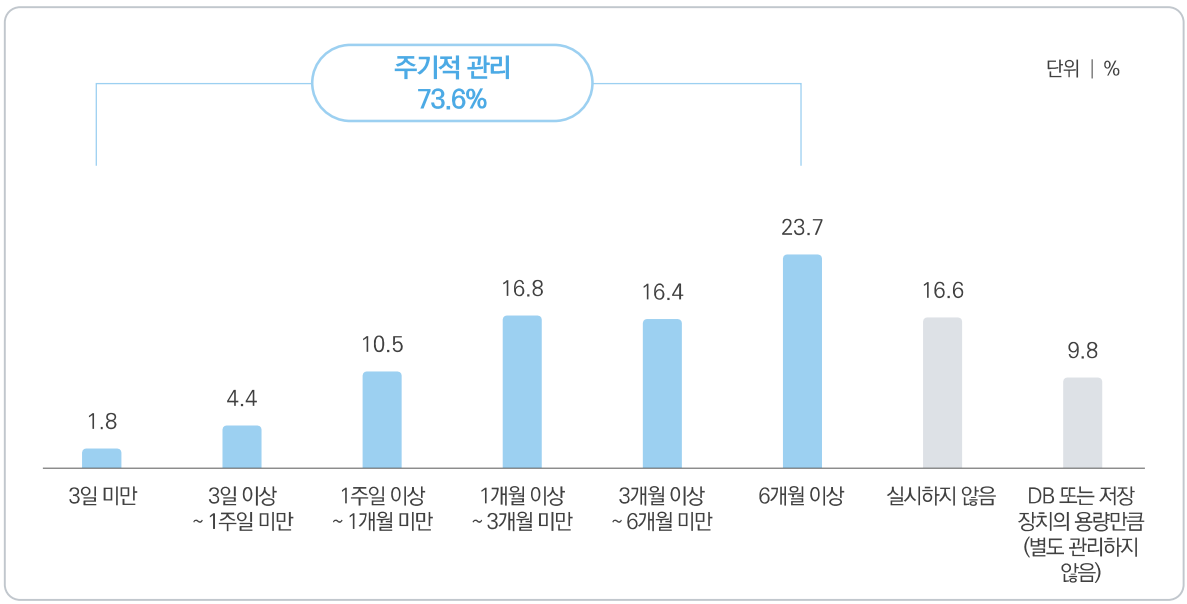


그림 1-3-67 시스템 및 방화벽 로그 기록 관리 주기 - 로그 기록을 관리하는 기업체

다 백업 실시

- 국내 기업체 중 89.1%가 데이터 백업을 실시하는 것으로 나타났다.

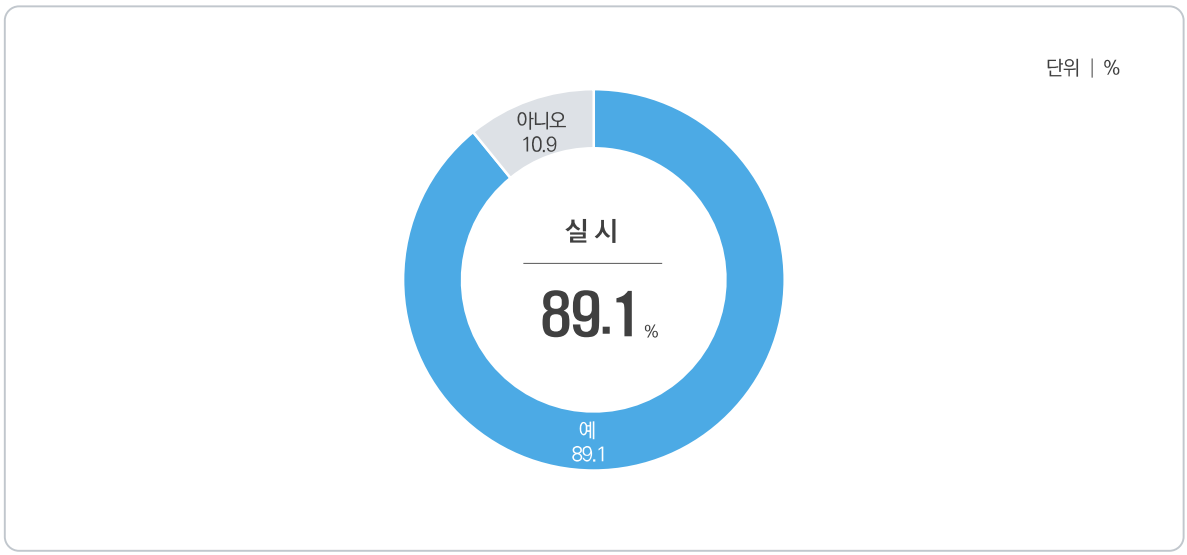


그림 1-3-68 백업 실시

- 백업 실시 유형으로는 '중요 데이터'가 80.0%로 가장 높고, 다음으로 '서버 데이터(59.0%)', 'CCTV 영상 데이터(58.6%)', '시스템 로그 데이터(55.7%)' 등의 순으로 나타났다.

그림 1-3-69 백업 유형 - 백업 실시 기업체

- 백업 방식은 'USB, 외장 하드 등 별도 저장장치 활용'이 53.3%로 가장 높고, 다음으로 '클라우드 서버 활용(18.8%)', '별도 백업 서버(NAS, SAN 등) 운용(14.1%)', '운영 체제 백업 기능 사용(13.5%)' 등의 순으로 나타났다.

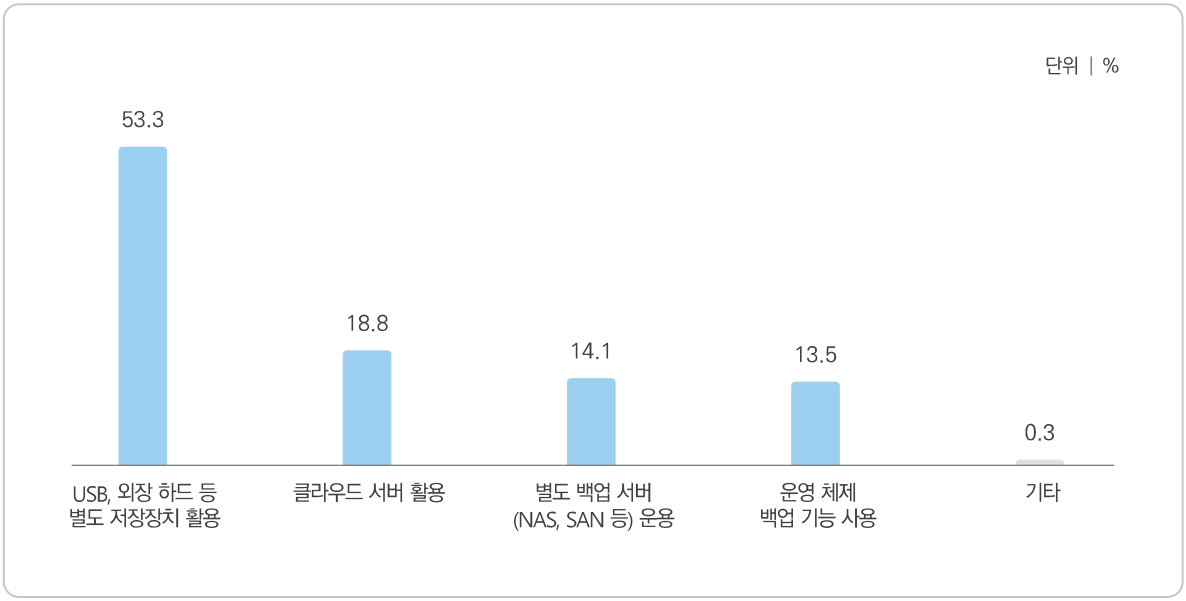


그림 1-3-70 백업 방식 - 백업 실시 기업체

- 백업 주기는 '주기적으로 실시'한다는 응답은 82.0%로 나타났으며, 주기적으로 실시한다는 응답에 대해 '6개월에 1회 실시'가 22.6%로 가장 높고, 다음으로 '1년에 1회 실시(16.9%)', '3개월에 1회 실시(15.6%)' 등의 순으로 나타났다.

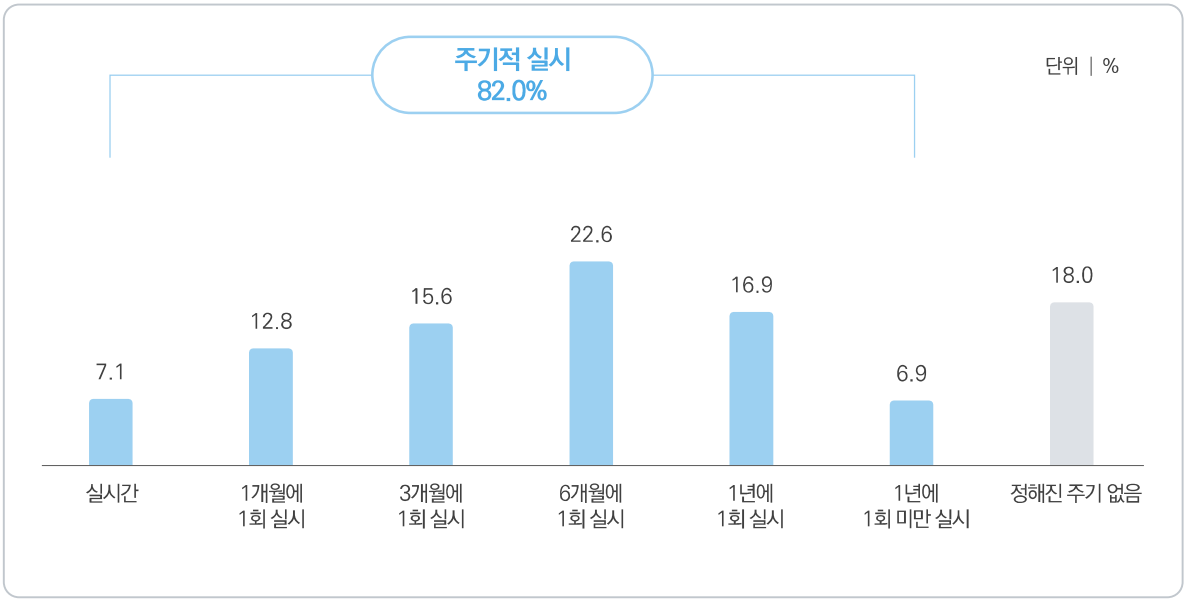


그림 1-3-71 백업 주기 - 백업 실시 기업체

라 정보보호 침해사고 사전 예방 능력

- 정보보호 침해사고 사전 예방 능력에 대해 정보보안은 27.4%, 물리보안은 30.2%가 안전하다(안전한 편이다 + 매우 안전하다)고 응답하였다.

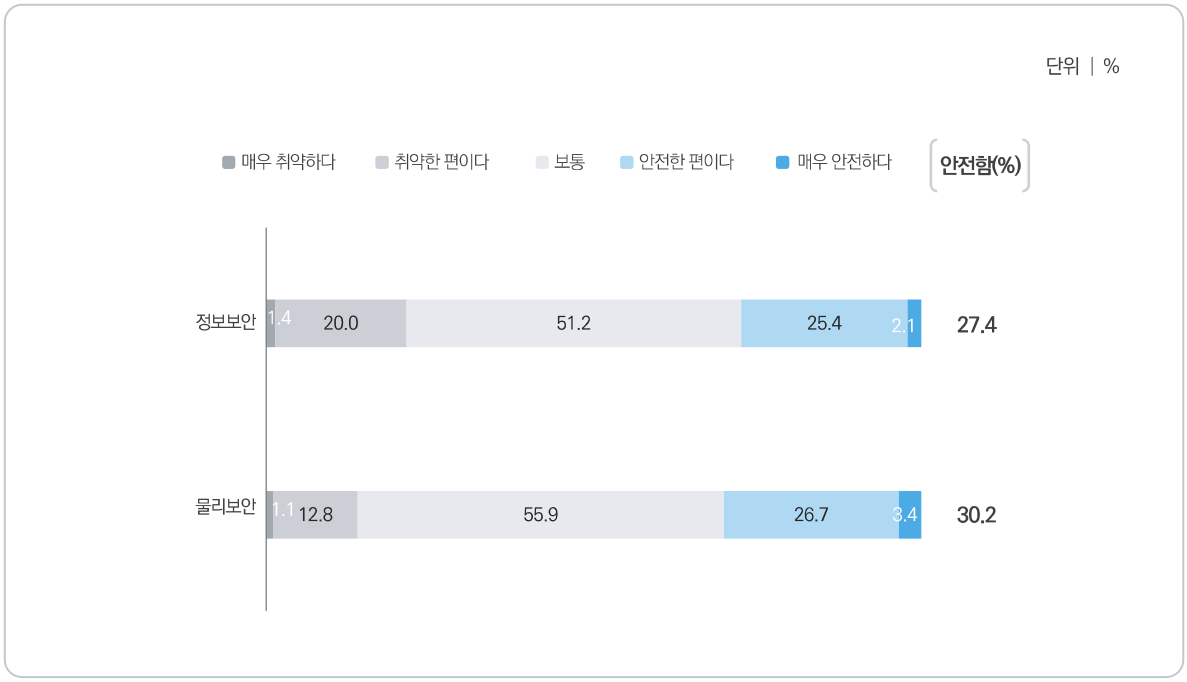


그림 1-3-72 정보보호 침해사고 사전 예방 능력

VI 침해사고 경험

1 침해사고 경험

가 침해사고 발생 가능성

- 국내 기업체 중 30.8%는 자사의 정보보호 침해사고 발생 가능성이 큰 편(그렇다 + 매우 그렇다)이라고 응답하였다.

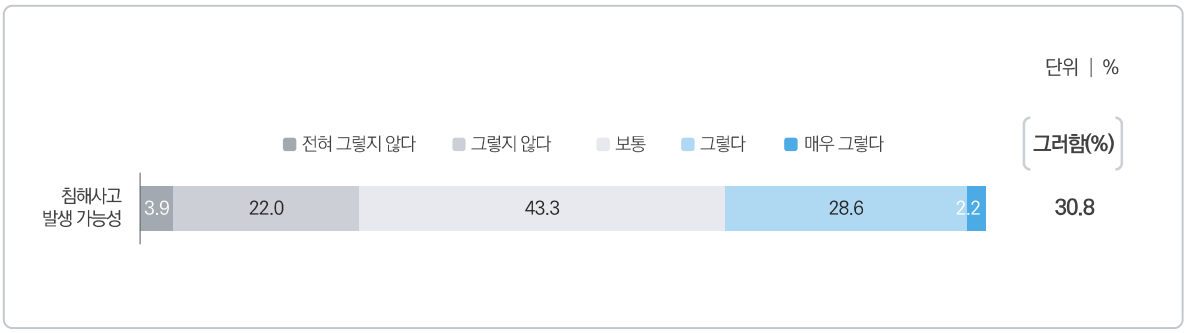


그림 1-3-73 침해사고 발생 가능성

나 침해사고 직접 경험

- 국내 기업체 중 3.7%는 정보보호 침해사고를 직접적으로 경험한 것으로 나타났다.

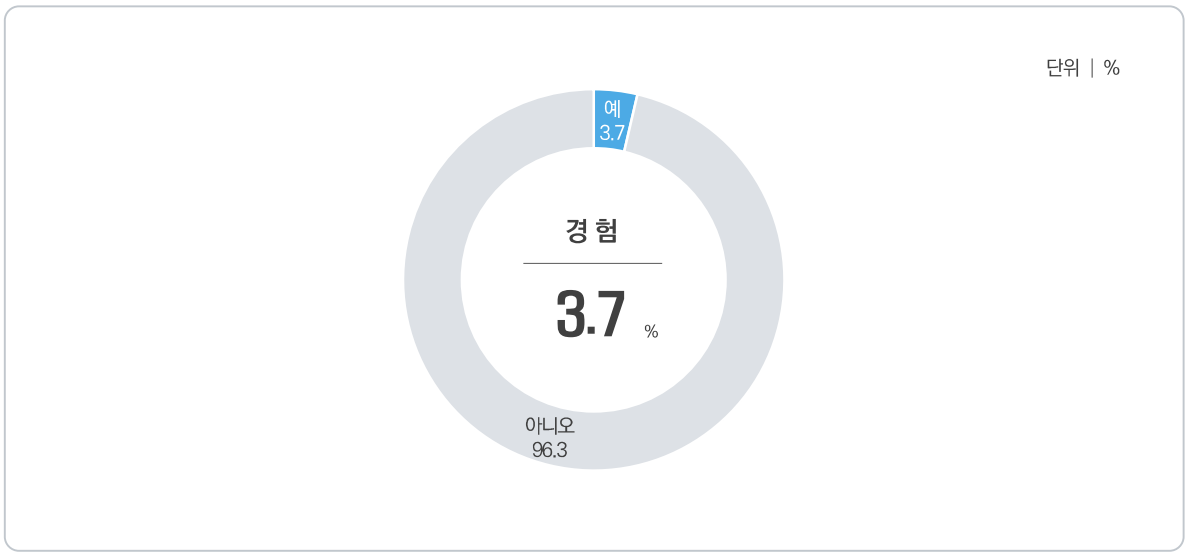


그림 1-3-74 침해사고 직접 경험

- 업종별 분석 결과, '교육 서비스업'이 6.0%로 가장 높게 나타났고, 다음으로 '농림수산업(광업포함)(5.4%)', '전기 등 공기조절 공급업/수도 등 원료 재생업(5.0%)' 등의 순으로 조사되었다.

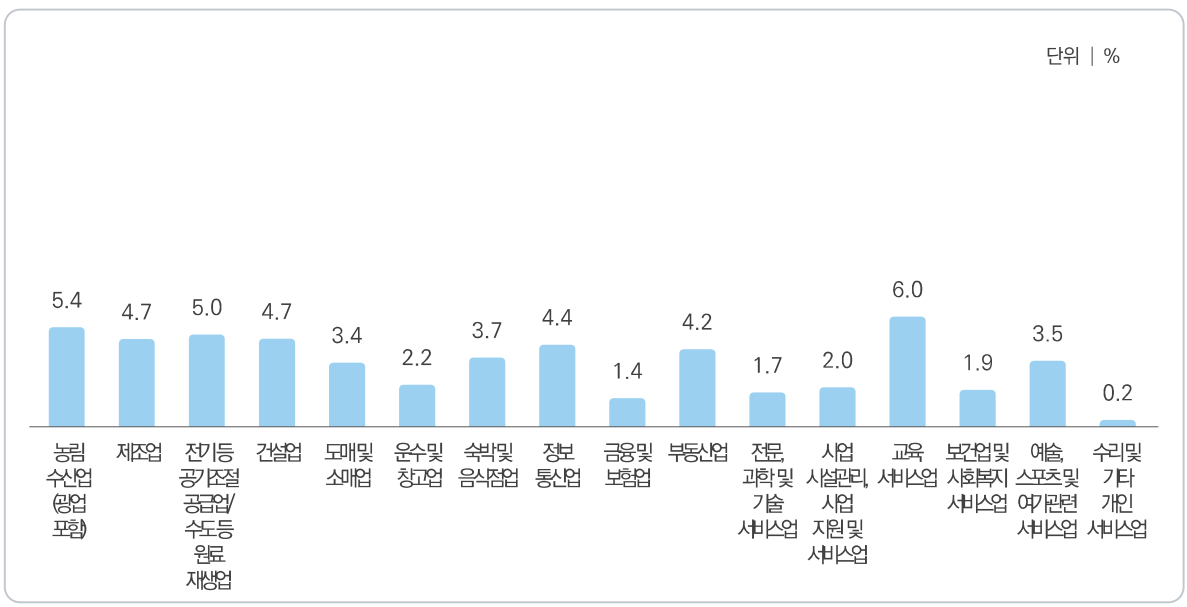


그림 1-3-75 업종별 침해사고 직접 경험

- 규모별 분석 결과, 종사자 수 '50~249명'의 침해사고 경험율이 5.5%로 가장 높게 나타났다.

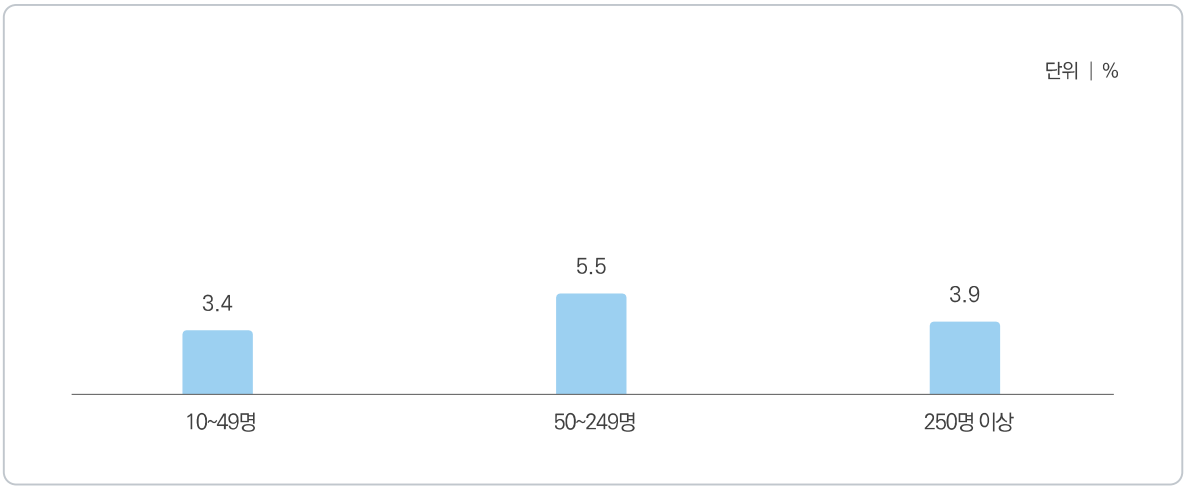


그림 1-3-76 규모별 침해사고 직접 경험

다 기타 침해사고 관련 경험

- 국내 기업체 중 6.3%는 정보보호 침해사고를 의심한 경험이 있다고 응답하였다.

  ※ **의심 경험** : 침해사고 여부가 확실히 증명된 것은 아니지만, 정황상 직·간접적으로 침해를 예상했던 경우

- 국내 기업체 중 9.8%는 협력 또는 유관 업체의 침해사고 피해 사실을 인지한 적이 있다고 응답하였다.

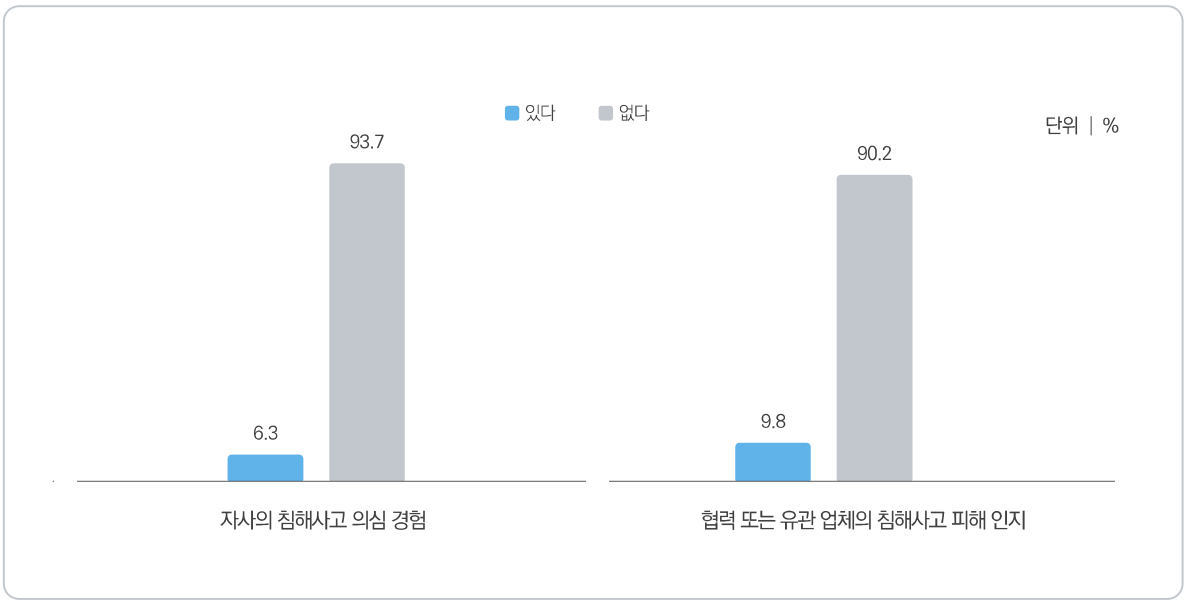


그림 1-3-77 기타 침해사고 관련 경험

라 침해사고 경험 유형

- 침해사고 경험 유형별로는 '랜섬웨어 감염'이 28.9%로 가장 높고, 다음으로 '외부로부터 침투한 비인가 접근(해킹)(26.2%)', '컴퓨터 바이러스, 웜, 트로이잔, APT 공격으로 인한 IT 시스템 마비(25.9%)', 'DoS 또는 DDoS 공격으로 인한 IT 시스템 마비(17.6%)' 등의 순으로 조사되었다.

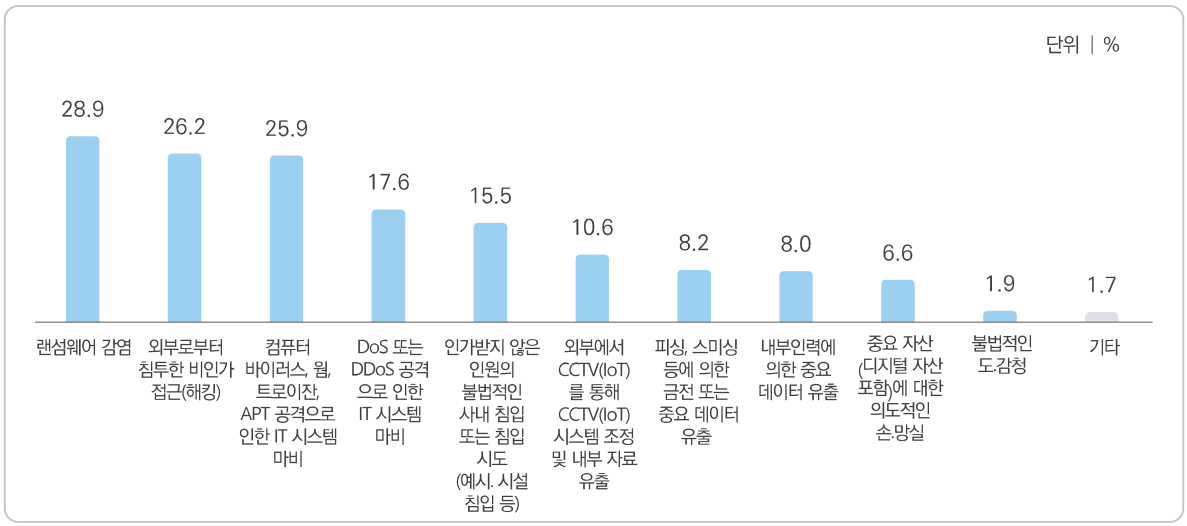


그림 1-3-78 침해사고 경험 유형(복수응답) - 침해사고 경험 기업체

마 침해사고 인지 경로

- 침해사고 인지 경로는 '보안 시스템의 임의적 해제 또는 침입 흔적 발견(물리적 침입 포함)'이 33.5%로 가장 높고, 다음으로 '기존과는 다른 시스템 설정의 변경 또는 보유하고 있는 데이터의 위변조 사항 발견(32.2%)', '보안 시스템의 침해사고 경보(알림)(31.5%)' 등의 순으로 조사되었다.

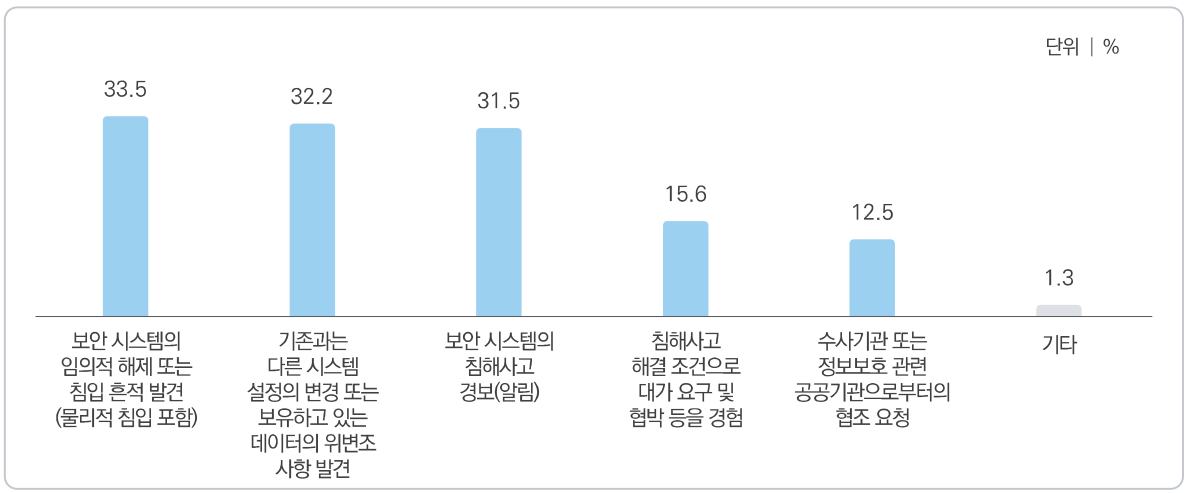


그림 1-3-79 침해사고 인지 경로(복수응답) - 침해사고 경험 기업체

바 침해사고 심각성 정도

- 침해사고를 직접적으로 경험한 기업체의 피해 심각성 정도는 '심각'이 38.2%, '경미'가 51.6%로 나타났다.
- 침해사고의 심각도 점수는 평균 -0.16점으로 대체로 보통 수준인 것으로 조사되었다.

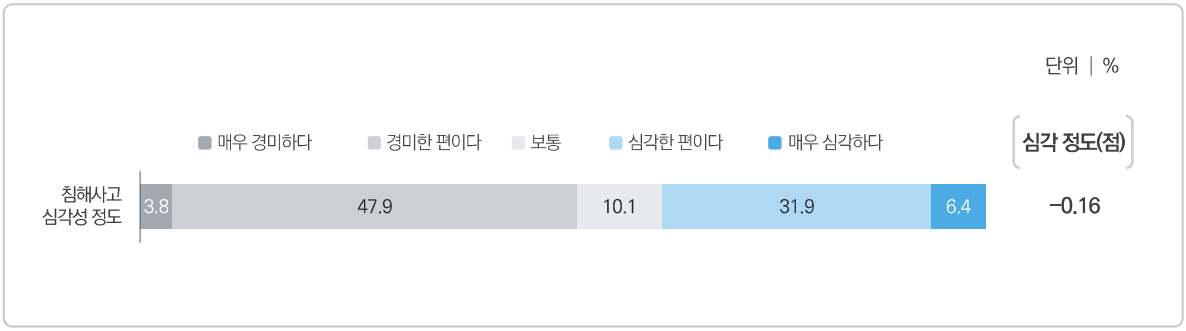


그림 1-3-80 침해사고 심각성 정도 - 침해사고 경험 기업체

사 침해사고 단계별 소요 시간

- 침해사고를 경험한 기업체의 단계별 소요 시간에 대해서 인지 단계는 '1일 이내'가 33.6%로 가장 높고, 원인 파악 단계 또한 '1일 이내(35.4%)', 문제 해결 및 서비스 복원은 '7일 이내(27.0%)'가 가장 높았다.

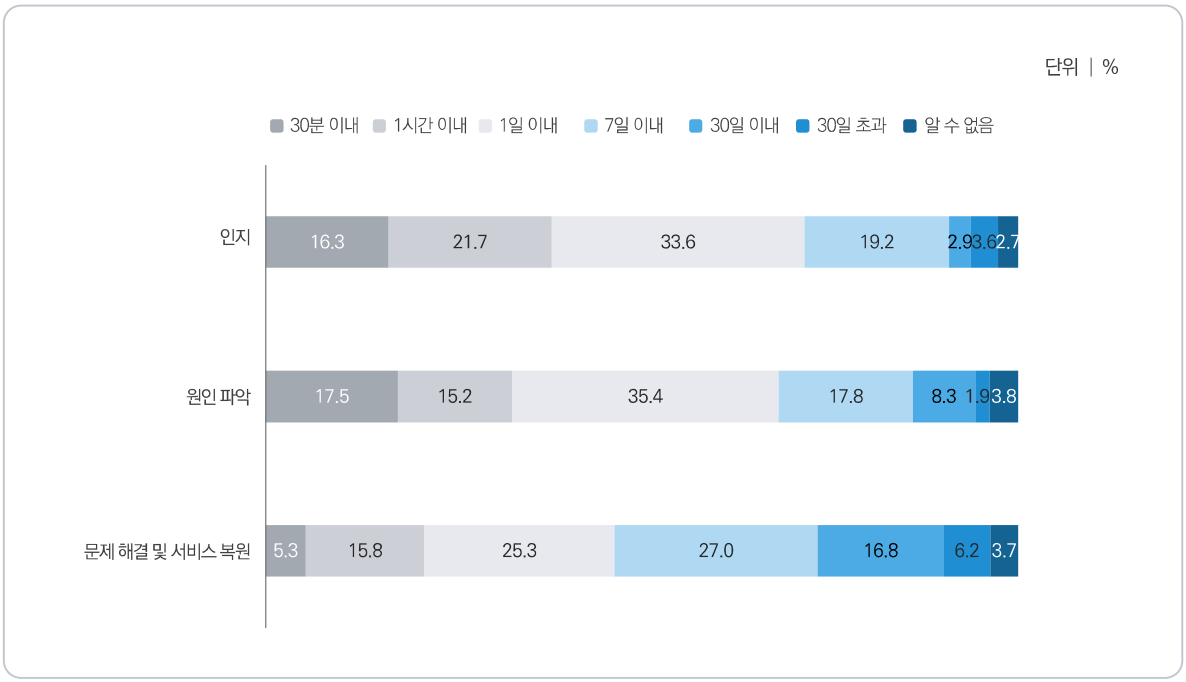


그림 1-3-81 침해사고 단계별 소요 시간 - 침해사고 경험 기업체

아 침해사고 시 신고 여부

- 침해사고 경험 기업체의 5.8%가 피해를 입었을 때 관련 기관 또는 수사기관에 신고하는 것으로 나타났다.

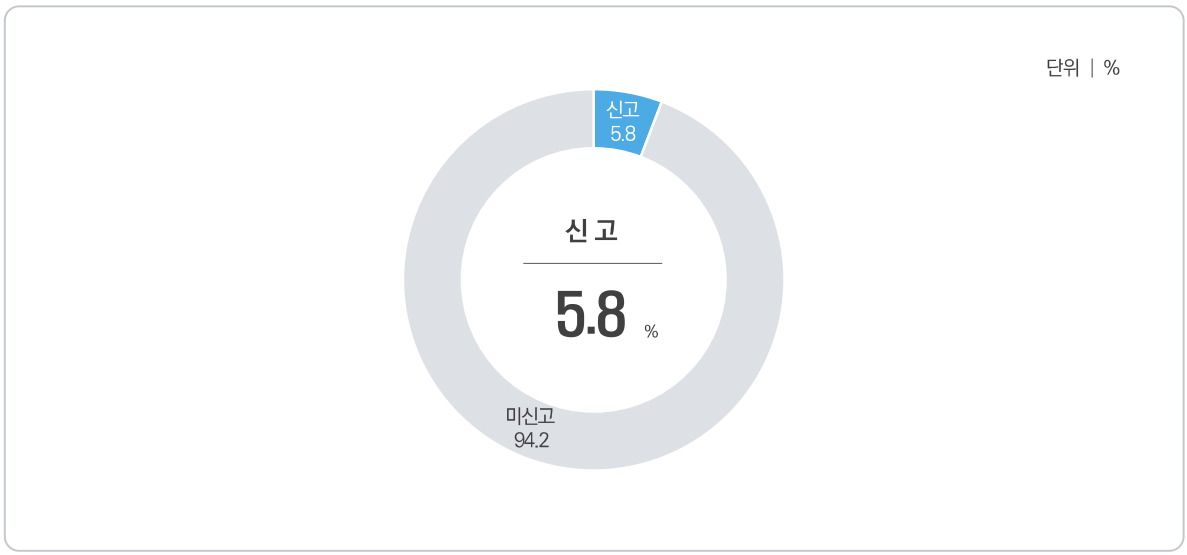


그림 1-3-82 침해사고 시 신고 여부 - 침해사고 경험 기업체

- 침해사고 경험 후 신고하지 않은 기업체의 경우, 피해 사실을 신고하지 않은 이유에 대해 '피해 규모가 경미하기 때문에'가 69.8%로 가장 높고, 다음으로 '신고에 따른 업무가 복잡하기 때문에(35.8%)', '신고하더라도 피해가 회복되지 않을 것이기 때문에(27.9%)', '어디에 신고해야 하는지 모르기 때문에(23.7%)' 등의 순으로 응답했다.

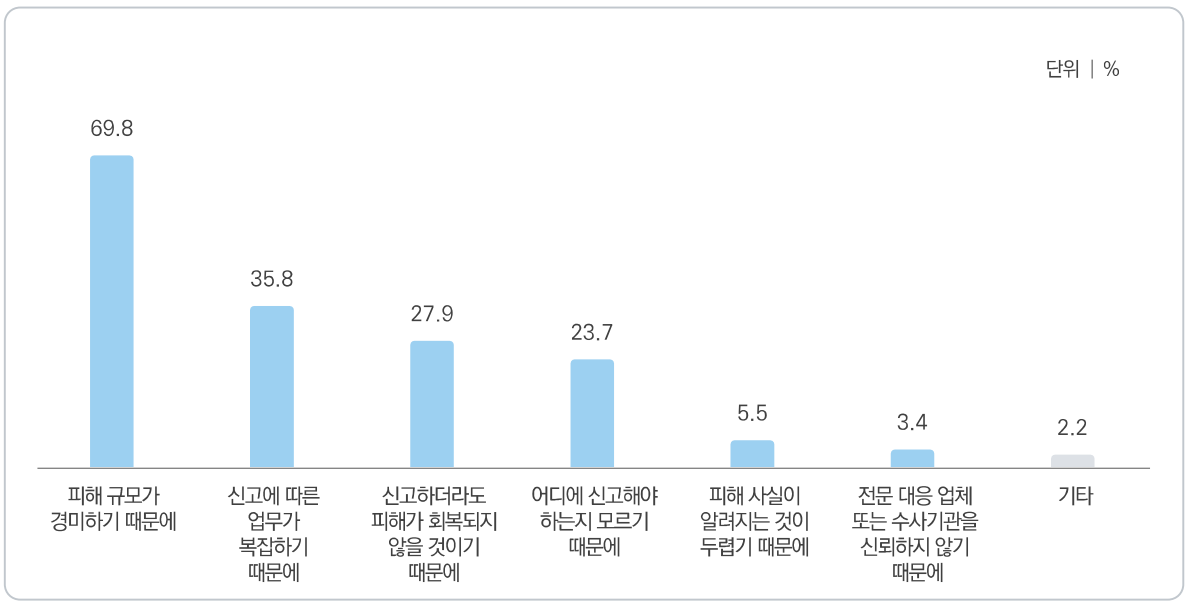


그림 1-3-83 침해사고 시 미신고 이유(복수응답) - 침해사고 미신고 기업체

자 침해사고 대응

- 국내 기업체 중 44.5%가 침해사고에 대응하기 위한 활동을 수행한 것으로 나타났다.
- 침해사고 대응 활동 유형별로는 '정보보호 관련 제품 및 솔루션 구축 및 고도화'가 24.6%로 가장 높고, 다음으로 '정보보호 인증을 받은 제품으로 교체(15.3%)', '정보보호 분야 전문기관 또는 전문가 자문(15.1%)' 등의 순으로 조사되었다.

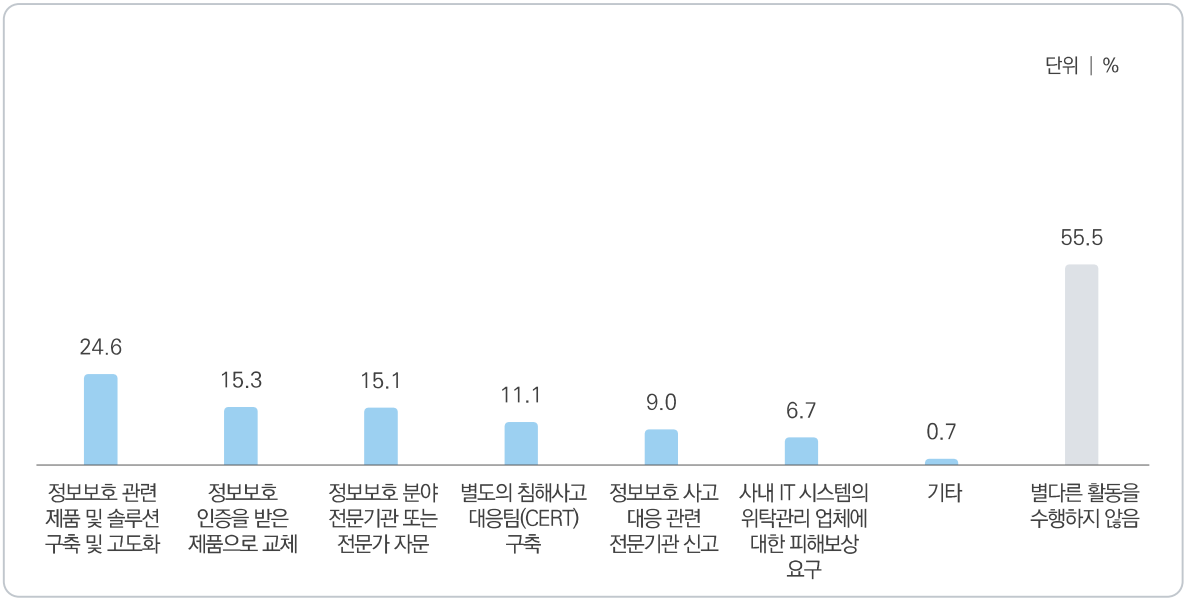


그림 1-3-84 침해사고 대응(복수응답) - 침해사고 경험 기업체

차 정보보호 침해사고 사후 대응 능력

- 정보보호 침해사고 사후 대응 능력에 대해 정보보안은 30.6%, 물리보안은 26.1%가 안전하다(안전한 편이다 + 매우 안전하다)고 응답하였다.

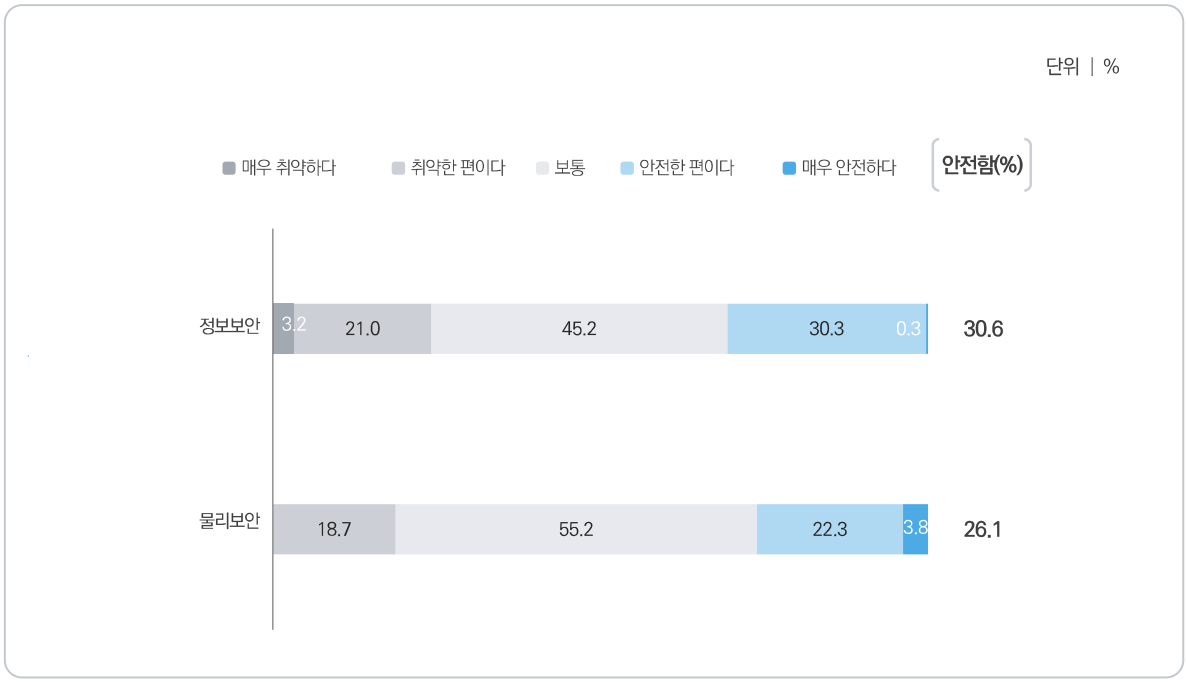


그림 1-3-85 정보보호 침해사고 사후 대응 능력 - 침해사고 경험 기업체

카 침해사고 경험 후 관심 변화

- 침해사고 경험 후 침해사고에 대한 관심 정도에 대해 62.2%가 관심이 커졌다(관심이 커졌다 + 관심이 매우 커졌다)고 응답하였다.

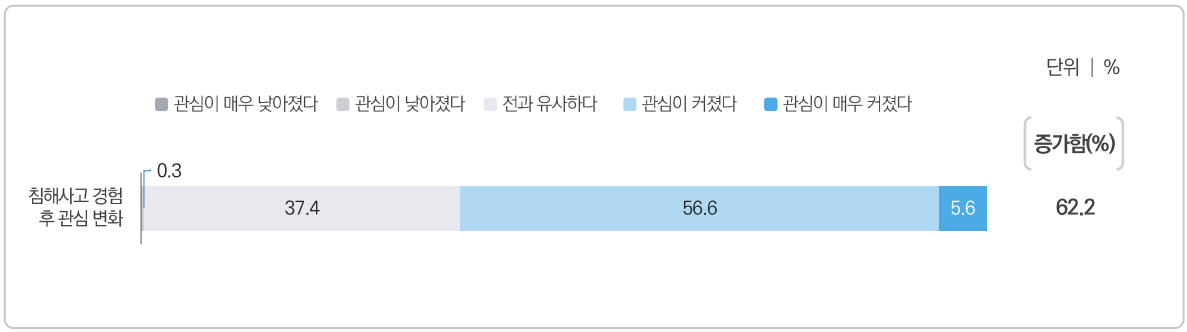


그림 1-3-86 침해사고 경험 후 관심 변화 - 침해사고 경험 기업체

Ⅶ 사이버 보험

1 사이버 보험

가 사이버 보험 인지

- 국내 기업체 중 25.4%가 사이버 보험에 대해 인지(잘 알고 있다 + 대략적인 의미와 특징만 알고 있다 + 용어 정도만 들어본 적 있다)하고 있는 것으로 나타났다.

그림 1-3-87 사이버 보험 인지

나 사이버 보험 이용

- 사이버 보험을 인지하고 있는 기업체 중 1.5%가 사이버 보험에 가입한 경험이 있는 것으로 나타났다.

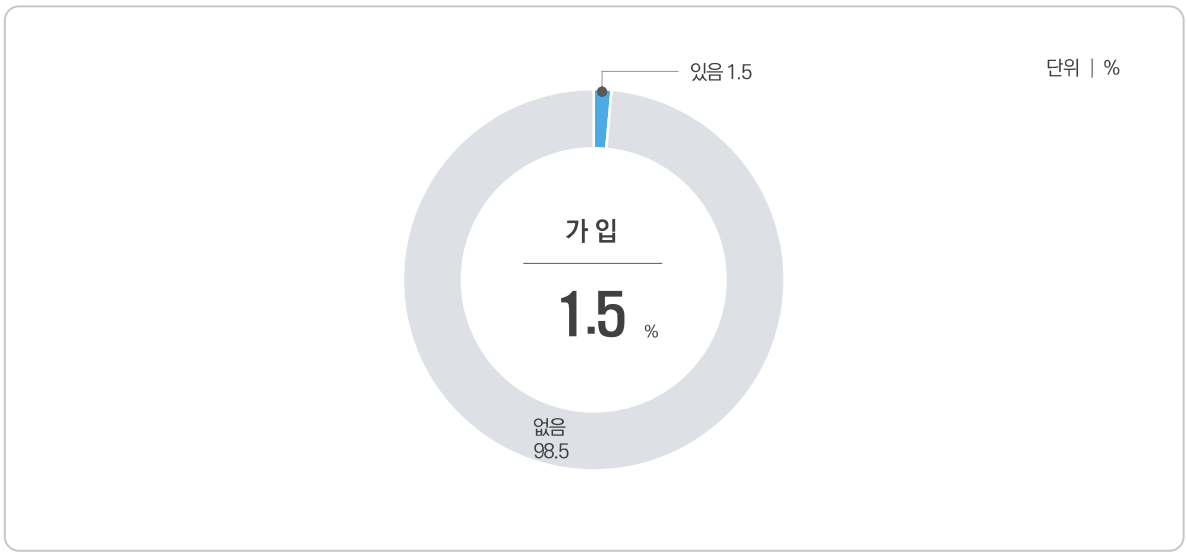


그림 1-3-88 사이버 보험 가입 - 사이버 보험 인지 기업체

- 사이버 보험 가입 경험이 있는 기업체 중 72.4%가 현재에도 가입 상태를 유지하고 있는 것으로 나타났다.

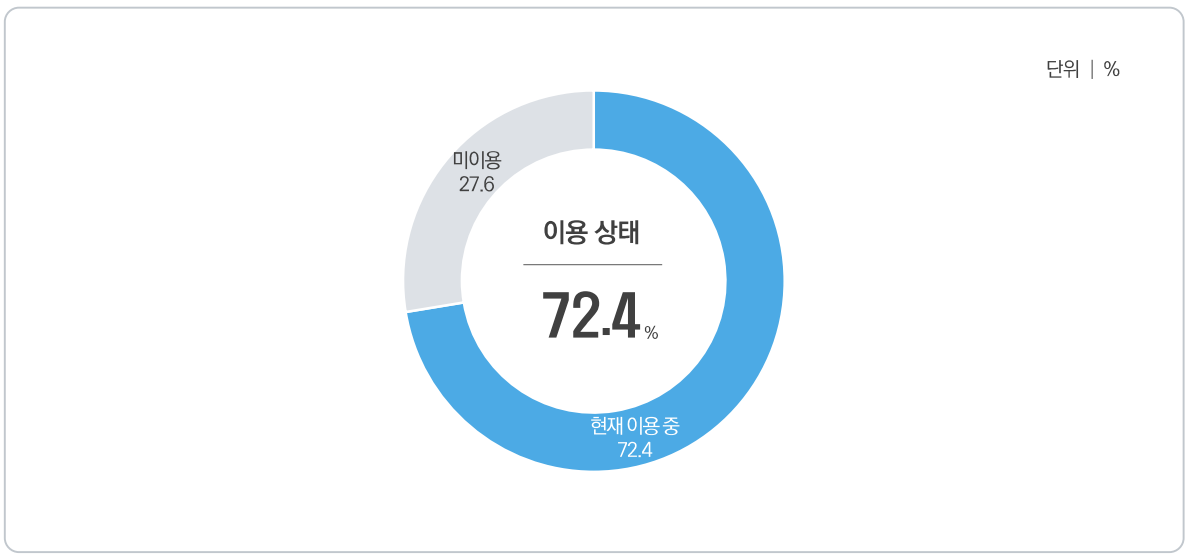


그림 1-3-89 사이버 보험 이용 - 사이버 보험 가입 경험 있는 기업체

- 사이버 보험을 인지하고 있는 기업체 중 2.6%가 사이버 보험 가입 계획이 있거나, 유지할 의향이 있는 것으로 나타났다.

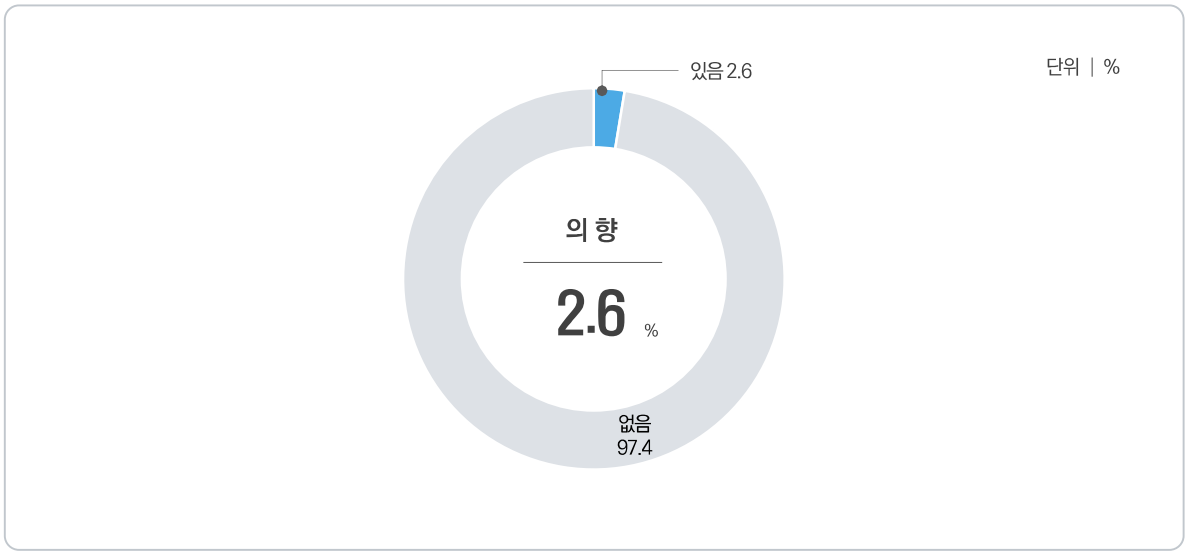


그림 1-3-90 사이버 보험 가입·유지 계획 – 사이버 보험 인지 기업체

- 향후 사이버 보험을 신규로 가입하거나, 현재 이용 중인 보험을 유지할 계획이 있는 기업체가 희망하는 보장 항목은 '기업 사이버 공격 발생 시 시스템 복구 또는 정상화 비용'이 59.8%로 가장 높고, 다음으로 '기업 데이터 유출 사고 발생 시 대응 비용(조사, 통지, 법률 자문)(48.1%)', '기업 기밀 유출 관련 소송 비용(변호사 선임 비용 등)(24.7%)', '사이버 갈취로 인한 손해(랜섬웨어, 스피어 피싱 등) 보장 비용(21.0%)' 등의 순으로 조사되었다.

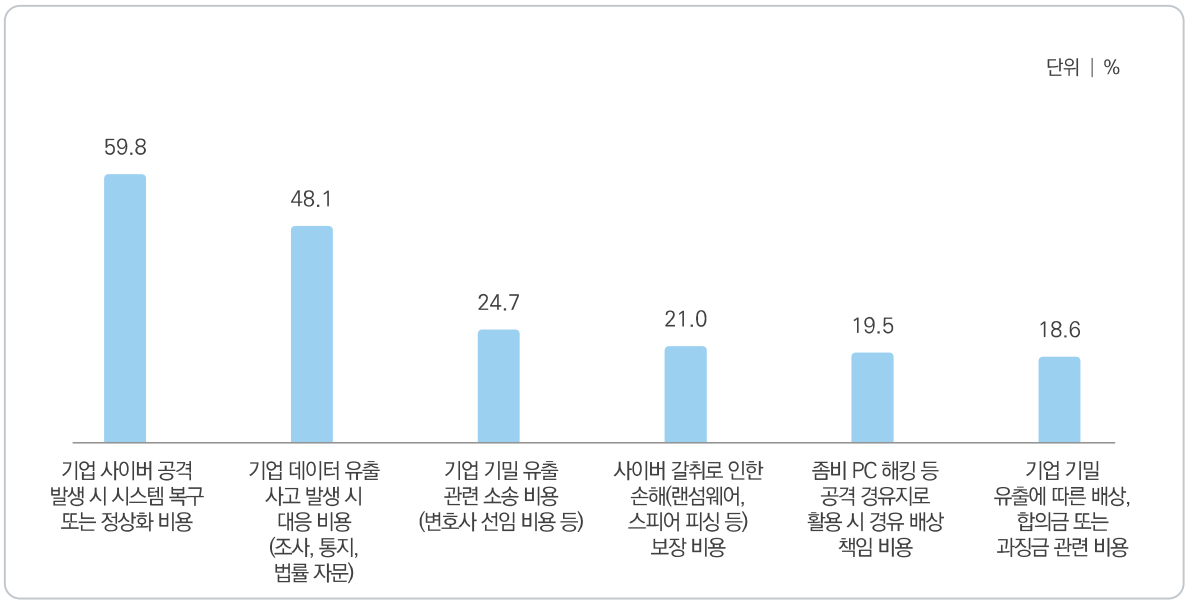


그림 1-3-91 사이버 보험 희망 보장 항목(복수응답) – 향후 사이버 보험 가입·유지 계획이 있는 기업체

Ⅷ 재택근무

1 재택근무

- 국내 기업체 중 26.1%가 재택근무를 시행하고 있는 것으로 조사되었다.

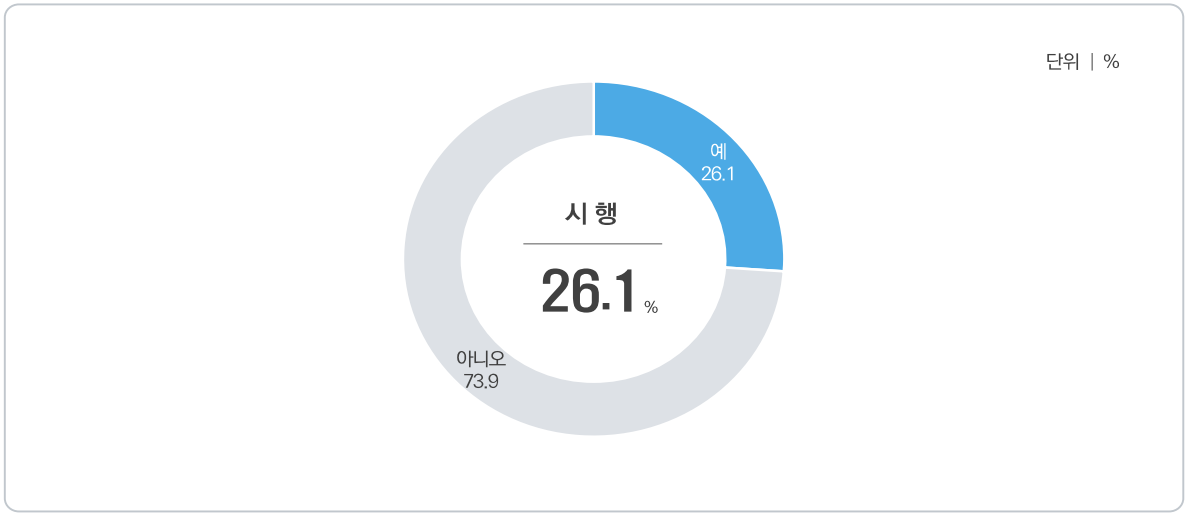


그림 1-3-92 코로나19로 인한 재택근무 시행 여부

- 국내 기업체 중 53.6%가 재택근무 시 보안 솔루션을 제공하는 것으로 나타났다.
- 보안 솔루션 유형별로는 '온라인 협업 툴 활용'이 18.6%로 가장 높게 나타났고, 다음으로 '자체 구축한 가상사설망(VPN) 활용(18.2%)', '문서암호화(DRM) 시스템(15.2%)' 등의 순으로 조사되었다.

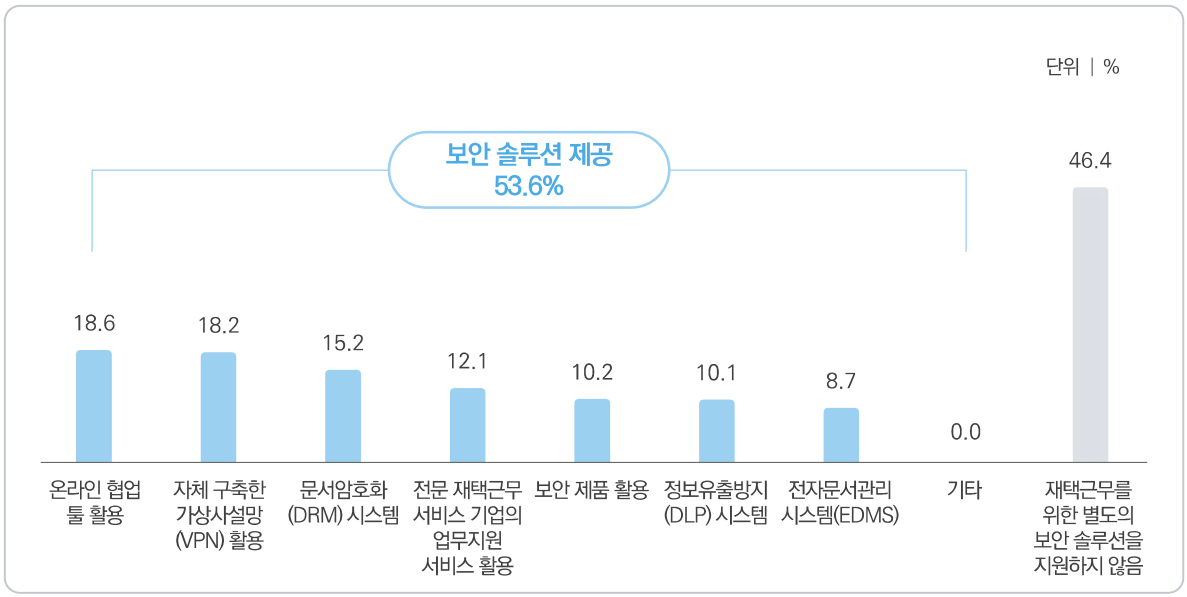


그림 1-3-93 재택근무 시 제공한 보안 솔루션(복수응답) - 재택근무 시행 기업체

- 재택근무를 시행하는 기업체 중 38.6%는 재택근무 시 정보보호 위험성에 대해 위험하다(그런 편이다 + 매우 그렇다)고 응답하였다.

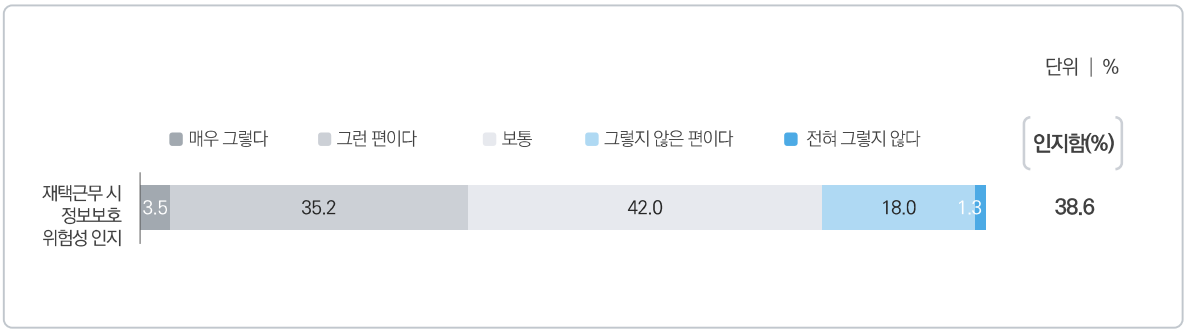


그림 1-3-94 재택근무 시 정보보호 위험성 인지 – 재택근무 시행 기업체

- 재택근무를 시행하는 기업체 중 침해사고 발생 또는 의심을 경험한 비율은 '발생'이 5.6%로 나타났다. (해당사항 없음: 94.4%)

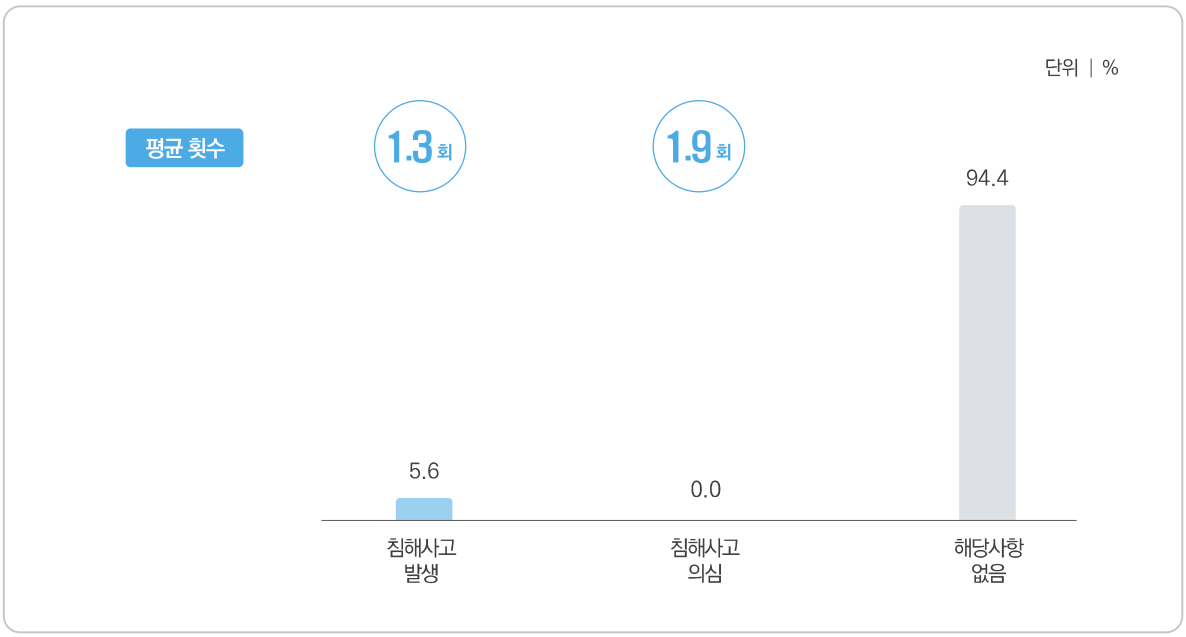


그림 1-3-95 재택근무 시 침해사고 발생 또는 의심 경험 – 재택근무 시행 기업체

제 2 부

개인부문

제 1 장

조사개요

1

1 조사 목적

- 급속하게 변화하는 인터넷 환경과 사물인터넷(IoT), IP카메라, 인공지능(AI) 등 새로운 기술의 끊임없는 등장으로 사이버 세계의 위협이 현실세계로 확대되고 그 위협 또한 고도화·지능화 되고 있다. 이에 따라 정보보호와 관련된 현황 및 인터넷 이용자들의 인식 수준, 대응활동 등을 파악하고, 인터넷 이용자의 정보보호 수준 제고에 활용하고자 정보보호 실태조사를 실시하였다.
- 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 제공하는 데 그 목적이 있다.
- 본 조사의 구체적인 목적은 다음과 같다.

1. 정부, 기업, 개인 등 사회구성원 전체의 정보보호 수준 제고에 활용하기 위한 기초자료 제공
2. 국가정보보호백서, 한국인터넷백서 등의 정보보호 통계자료 제공
3. 국제기구(OECD)의 ICT 통계지표 기초자료 제공
4. 업계 및 학계의 현장, 연구활동 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
- 승인번호체계 변경(2016.08.28.)(제34205호 → 제342005호)

2017년
- '2010년 인구주택총조사'와 '2016년 추계인구', '2016년 인터넷이용실태조사' 결과를 기반으로 표본 재설계
- 추정 오차 감소를 위해 조사구 수 확대(400개 → 800개)
- 조사구 내 추출 가구 수 감소(조사구 당 10가구 → 조사구 당 5가구)
- 통계작성기관명 변경(미래창조과학부 → 과학기술정보통신부)

2018년
- 조사대상 확대(만12~59세 → 만12~69세)
- '2015년 인구주택총조사'와 '2017년 추계인구', '2017년 인터넷이용실태조사' 결과를 기반으로 표본 재설계
- 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

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 구성하였다.

  본 조사의 주요 내용은 다음과 같다.

  1. 정보보호 인식
  2. 정보보호 교육
  3. 정보보호 예산
  4. 일상 생활 속의 정보보호
  5. 정보보호 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
- **개인정보보호** : 특정 개인을 알아볼 수 있는 정보(성명, 주민등록번호, 영상정보 등)가 유출되는 위협으로부터 보호하는 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 의미하며, 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
- **클라우드 서비스** : 개인의 사진 · 문서 · 동영상 등 각종 콘텐츠를 '클라우드'라는 가상공간 서버에 저장한 뒤 인터넷으로 접속해 노트북, 스마트폰 등 다양한 기기로 이용할 수 있는 서비스를 말함
- **IP카메라** : 유선 또는 무선으로 인터넷에 연결되어 PC나 모바일 기기 등을 통해 실시간으로 영상을 송출할 수 있는 단말

5 조사 체계

- **조사대상** : 최근 1개월 내 인터넷 이용자(만12~69세)
- **유효 응답자 수** : 4,000명
- **조사주기** : 연 1회
- **조사기간** : 2022년 9월 28일 ~ 11월 23일 (2개월)
- **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 만 12~69세 인터넷 이용자
- **조사 모집단(Survey Population)**
  - 국내 만 12~69세의 인터넷 이용자 중 최근 1개월 이내 인터넷 이용자
- **모집단 자료**
  - 통계청『2021년 추계인구』및 한국지능정보사회진흥원의『2021년 인터넷이용실태조사』에서 파악된 지역별, 성별, 연령별 국내 인터넷이용률을 이용하여 파악한 최근 1개월 이내 인터넷 이용자 수 및 분포 활용
  - 단, 통계청 조사구 중 보통조사구와 아파트조사구를 조사 모집단으로 정의함

나 표본 추출

- **개요** : 다단계층화추출법(Multi-Stage Stratified Sampling)
  - 17개 시도별 인터넷 이용자 크기에 비례하여 800개 조사구를 배분하고, 각 조사구에서 평균 5가구씩 추출하여 가구 내에서 적격 조사대상자를 선정·조사
- **표본의 규모산정**
  - 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	1.17	1.08	1.07	1.04	1.01	0.99	0.97	0.96

  - 최종 표본의 크기는 표본오차가 ±1.01%p 내에서 통제되도록 4,000명으로 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) : 만 12~19세, 20대, 30대, 40대, 50대, 60대
- **표본틀** : 통계청 2021년 '추계인구' 및 한국지능정보사회진흥원 '2021년 인터넷이용실태조사'에서 파악된 성별, 연령별, 국내 인터넷 이용자 수 및 분포 활용

• 표본 할당 및 추출 방법

① 표본 할당

- 만 12~69세 인터넷 이용자 크기에 비례하여 4,000명을 지역별 비례할당 후, 각 지역에 표본을 우선 할당하고, 성X연령 셀에 할당하는 방법을 최종 표본 할당 방법으로 결정함

② 조사구 할당

- 조사구당 5명이 조사되도록 총 800개 조사구 배분
- 1차 : 17개 시도별 조사구 배분
  * 통계청의『2021년 추계인구』, 한국지능정보사회진흥원의『2021년 인터넷이용실태조사』 인터넷 이용률 결과를 기반으로 17개 시도별 인터넷 이용자 크기에 비례하여 800개 조사구 배분
- 2차 : 시도 내 주거형태별 조사구 배분
  * 통계청의『2020년 등록센서스』기준 17개 시도별 주거 형태(아파트 및 아파트 외) 분포에 비례하여, 아파트 조사구와 비아파트 조사구 배분

③ 조사구 추출

- 341,309개 조사구를 행정구역 코드에 따라 정렬하여 계통 추출
- 계통 추출 17개 지역*2개 동읍면부*4개 주거형태별 셀 내에 조사구를 행정구역코드별로 정렬 후 계통 추출함
  * 시도 내 조사구수 m개, 목표 조사구수 n개, m/(n-1)의 몫을 k라고 할 때 시도별로 1-m범위 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

- 통계진흥원으로부터 제공받은 표본조사구의 가구명부 리스팅 번호 중에서 임의로 하나를 선택한 후 해당 가구를 출발점으로 가구를 계통추출하고 순서대로 방문하여 적격 조사대상 5가구 조사
- 3회까지 접촉이 이루어지지 않거나 가구 내 적격조사대상자가 없는 경우, 가구 명부를 기준으로 원표본(i)의 다음 가구($i-1$, $i+1$)로 대체함

⑤ 조사대상 추출

- 가구 내에 상주하는 만 12~69세 가구원을 대상으로 적격 조사대상자 여부 확인
- 적격 조사대상자가 복수일 경우에는 생월법에 따라 생일의 일자가 가장 가까운 가구원을 조사함

7 실사

가 실사 개요

- **조사기간**
  - 2022년 9월 28일 ~ 11월 23일 (2개월)
- **조사기준 시점**
  - 2021년 7월 1일 ~ 2022년 6월 30일
  - 침해사고 경험은 2021년 1월 1일 ~ 12월 31일
- **조사대상**
  - 최근 1개월 내 인터넷 이용자(만 12~69세)
- **조사방법**
  - 전문 조사원이 표본으로 선정된 가구를 방문하여 설문에 응답을 받는 형태의 가구방문 면접조사
- **조사절차**
  - 면접원의 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 유사특성을 가진 조사구로 대체
- **가구관리**
  - 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 예비표본으로 대체하여 조사 진행

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 검증
  - 실사 감독원의 1차 검증에서 합격된 설문지는 에디팅 및 입력 과정에서 전산 프로그램에 의해 2차 검증
  - 입력된 자료는 자료 처리 과정에서 내검 프로그램에 의해 3차 검증
  - 검증 단계별로 불합격된 설문지에 대한 보완조사 및 재조사 실시
- **분석 과정에서 자료 검증**
  - 동일한 그룹(성, 연령, 지역, 학력, 직업, 가구소득 등)별 평균치 및 이전 조사 결과와의 시계열 비교 및 검증
- **무응답 대체**
  - 단위무응답 및 항목무응답 발생 시 해당 가구를 3회 이상 재방문 및 전화 검증을 통해 무응답률 최소화
  - 단위무응답 발생 시 예비표본의 범위 내에서 대체하여 단위무응답 제거
  - 항목무응답 발생 시 결측값을 해당 응답자 특성(성, 연령, 지역, 학력, 직업, 가구소득 등)과 유사한 응답자 그룹의 평균값으로 대체하여 항목무응답 제거

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 의한 가중치 산출**

  - 본 조사는 조사구를 활용한 가구방문 면접조사로 진행되어 표본의 구성 비율이 모집단 구성 비율과 차이가 있으므로 가중치에 의한 사후추정 필요

- 통계청의 『2021년 추계인구』와 한국지능정보사회진흥원의 『2021년 인터넷이용실태조사』 인터넷이용률 결과를 모집단으로 활용하여 지역별×성별×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 모집단수
  $n_{(h,s,k)}$: (h,s,k)셀의 표본수
  k : 연령(12-19세, 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

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

- 여기에서 $\hat{p}_{st}$: 특정 변수에 대한 모비율
  $\hat{p}_{hsk}$: 특정 변수에 대한 (h,s,k)셀의 모비율
  w_{hsk} : (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 실시율 추정 결과 및 표본오차

보안 점검 실시율 표본오차	±1.55%p (95% 신뢰수준)
보안 점검 실시율 추정 결과	51.2% ± 1.55%p

10 결과 공표 및 활용 분야

- 『2022 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

		만12~69세 최근 1개월 이내 인터넷이용자		응답 현황	
		모집단 수(명)	비율(%)	표본 수(명)	비율(%)
전체		40,579,084	100.0	4,000	100.0
성별	남성	20,771,580	51.2	2,046	51.2
	여성	19,807,504	48.8	1,954	48.9
연령별	12~19세	3,621,519	8.9	357	8.9
	20대	6,717,193	16.6	661	16.5
	30대	6,846,659	16.9	673	16.8
	40대	8,068,809	19.9	796	19.9
	50대	8,517,130	21.0	843	21.1
	60대	6,807,774	16.8	670	16.8
지역별	서울	7,618,851	18.8	748	18.7
	부산	2,580,105	6.4	255	6.4
	대구	1,860,392	4.6	184	4.6
	인천	2,357,245	5.8	232	5.8
	광주	1,170,191	2.9	116	2.9
	대전	1,168,694	2.9	116	2.9
	울산	905,294	2.2	89	2.2
	세종	293,656	0.7	29	0.7
	경기	10,970,272	27.0	1,081	27.0
	강원	1,081,510	2.7	106	2.7
	충북	1,274,181	3.1	125	3.1
	충남	1,661,125	4.1	164	4.1
	전북	1,324,184	3.3	131	3.3
	전남	1,281,815	3.2	125	3.1
	경북	1,969,328	4.9	195	4.9
	경남	2,560,263	6.3	255	6.4
	제주	501,978	1.2	49	1.2

제 2 장 조사결과 요약

2

Ⅰ 정보보호 인식

1 정보보호 인식

» 인터넷 이용자의 정보보호 관심도는 56.1%

- 국내 인터넷 이용자의 정보보호 관심도는 56.1%로 조사되었음
  - — 성별로는 '남성(59.2%)'이 '여성(52.9%)' 대비 다소 정보보호 이슈에 대한 관심도가 높게 나타남
  - — 연령별로는 20대(65.2%)의 정보보호 이슈 관심도가 가장 높고, 60대(45.2%)의 관심도가 가장 낮음

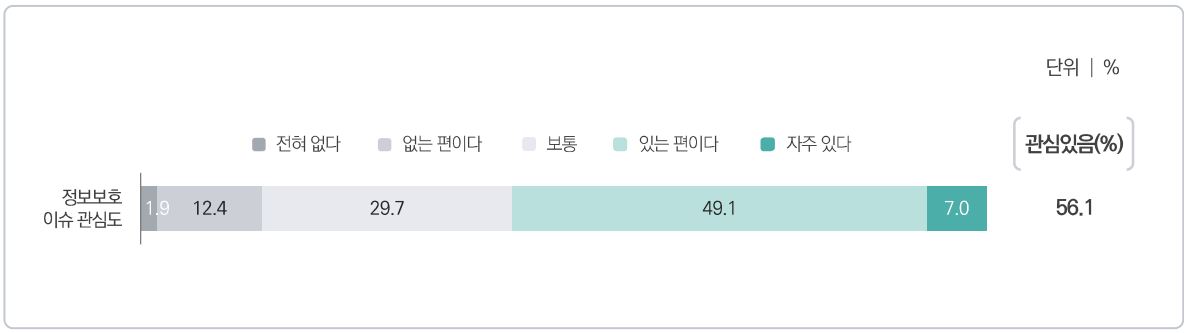


그림 2-2-1 정보보호 이슈 관심도

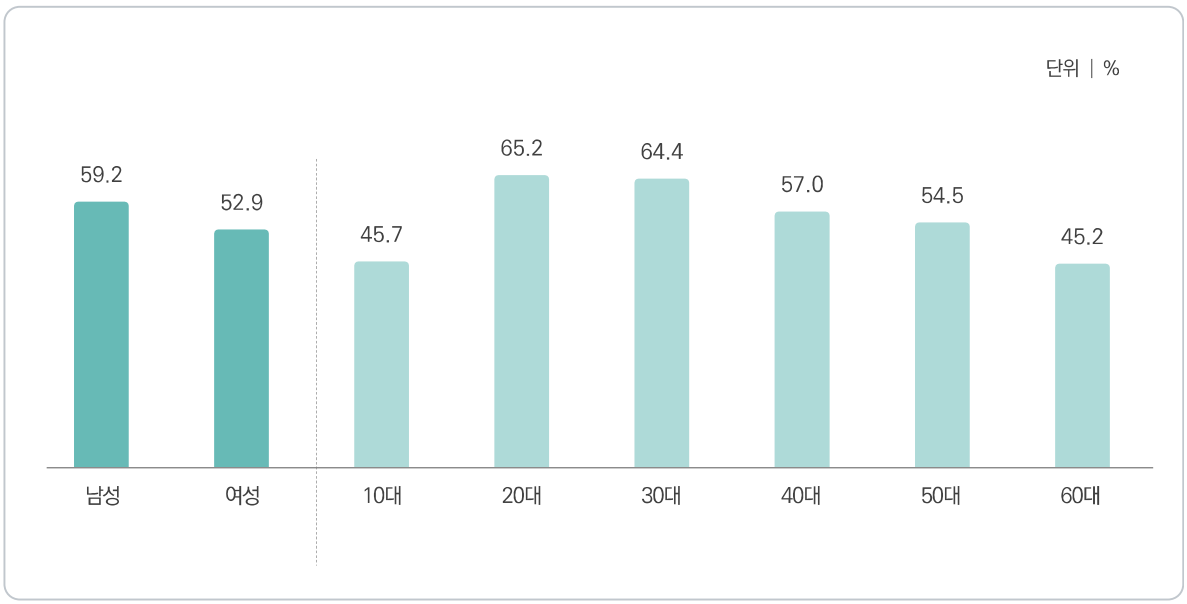


그림 2-2-2 성·연령별 정보보호 이슈 관심도

인터넷 이용자의 정보보호 침해 우려 정도 62.8%, 정보보호 침해사고 소식에 대한 관련성 인식 47.4%

- 정보보호 침해에 대해 인터넷 이용자의 62.8%는 우려한다고 응답했으며, 47.4%는 자신이 정보보호 사고와 관련이 있다고 인식함

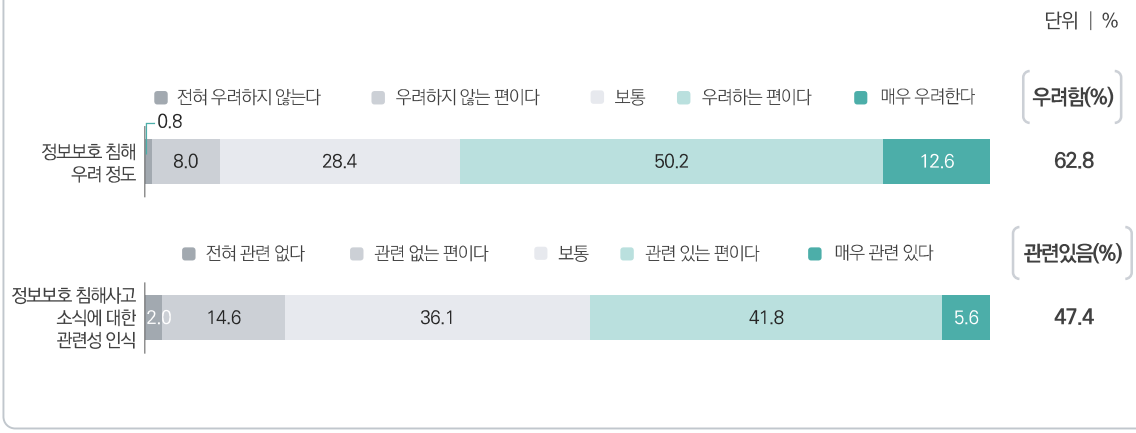


그림 2-2-3 정보보호 침해 우려 정도 및 정보보호 침해사고 소식에 대한 관련성 인식

안전 체감도 항목 중 '개인 생활 공간 불법 접근(37.7%)' 에 대한 체감도가 높음

- 안전 체감도 항목 중 '개인 생활 공간 불법 접근(37.7%)'이 가장 높은 응답을 보였고, '사생활 침해(29.0%)', '전자기기 악성코드 감염(25.9%)', '전자기기 분실 정보 유출(23.2%)' 순으로 안전하다고 체감하였음

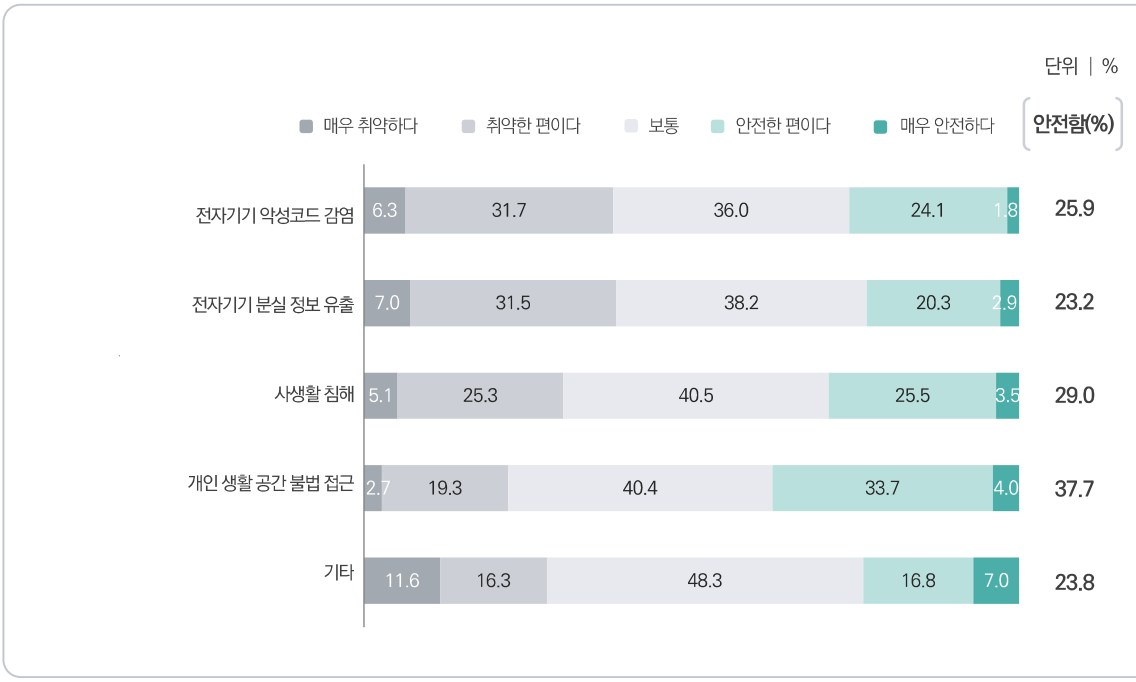


그림 2-2-4 안전 체감도(요약)

Ⅱ 정보보호 예방 활동

1 정보보호 교육

» 인터넷 이용자의 15.3%가 정보보호 교육 수강

- 인터넷 이용자의 15.3%가 최근 1년간 정보보호 교육을 수강한 경험이 있는 것으로 조사됨
  - — 정보보호 교육 방식에 대해 정보보호 교육 수강자의 67.3%는 '근무지·학교 등에서의 온라인 교육'을 수강했다고 응답했으며, 다음으로는 '근무자·학교 등에서의 오프라인 교육 수강(32.9%)', '개인적인 방식으로 온라인 교육 수강(줌(ZOOM) 등)(21.9%)' 등의 순으로 조사됨

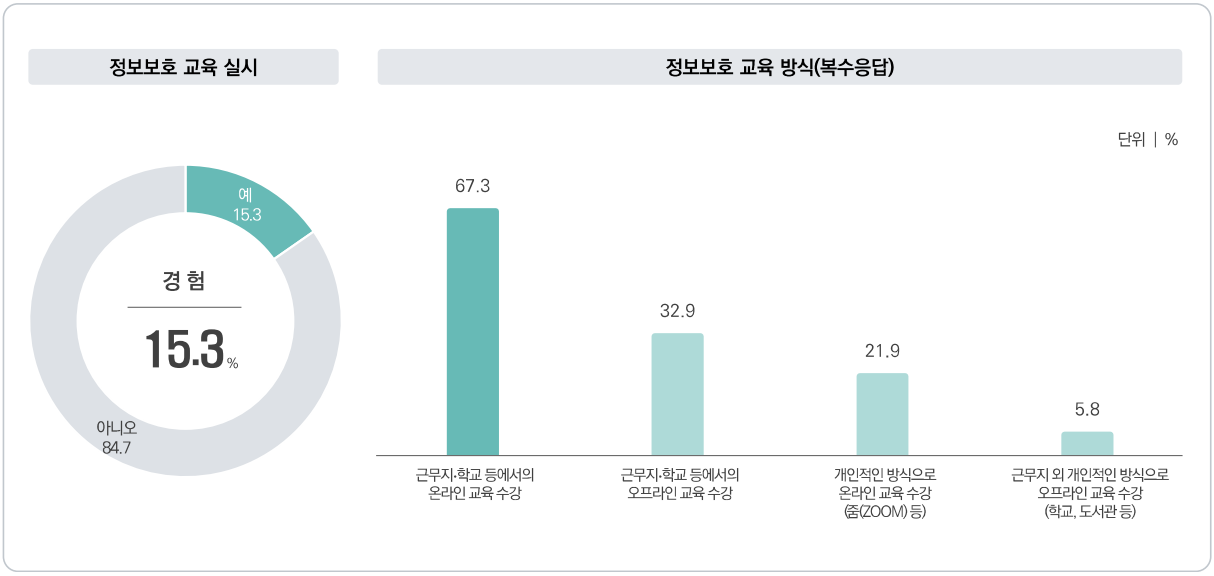


그림 2-2-5 정보보호 교육 실시 및 교육 방식(복수응답)

2 정보보호 예산

가 정보보호 금전 소비 경험 및 소비 유형

» 인터넷 이용자의 정보보호 금전 소비 경험 13.2%

- 최근 1년간 개인적 목적의 정보보호 관련 소비 경험에 대해 인터넷 이용자의 13.2%는 경험이 있다고 응답함
  - 정보보호 금전 소비 경험이 있는 인터넷 이용자의 경우, 소비 유형으로는 '정보보호 관련 유료 인증서의 결제'가 41.1%로 가장 높고, 다음으로 '정보보호 관련 제품 및 솔루션의 구입(오픈소스 등 포함)(36.4%)', '자택·개인 생활 공간의 CCTV 등 영상감시장비 설치 및 증설(유지·보수 포함)(22.6%)' 등의 순으로 조사됨

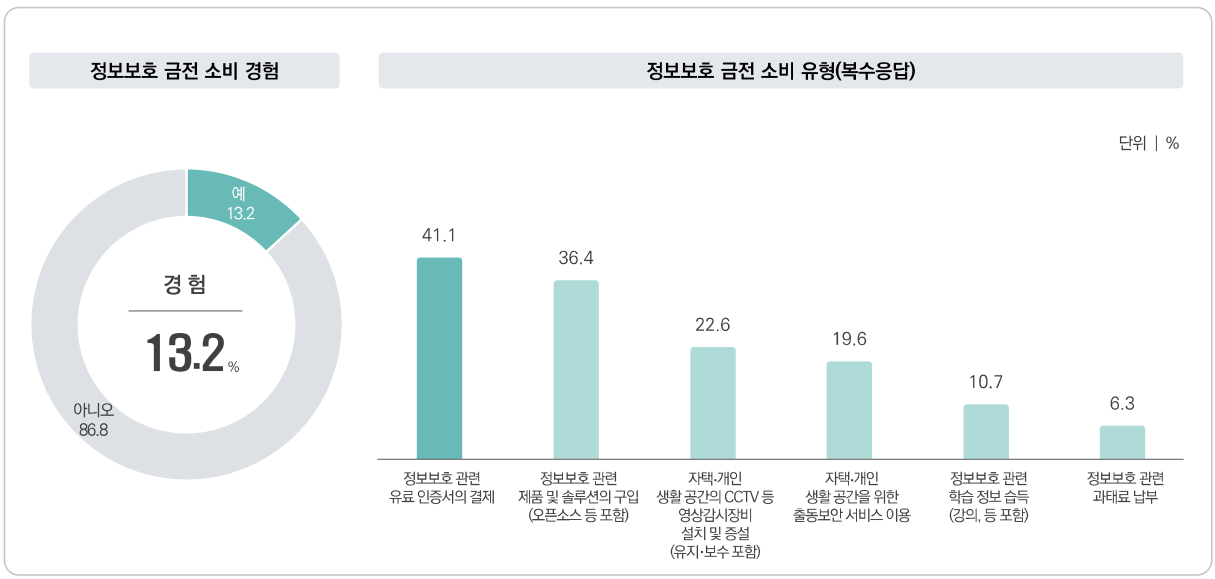


그림 2-2-6 정보보호 금전 소비 경험 및 소비 유형(복수응답)

나 정보보호 금전 소비 규모

» 정보보호 금전 소비 경험자의 50.1%가 '1만 원 이상~10만 원 미만' 소비

- 정보보호 관련 금전 소비 규모는 '1만 원 이상 ~ 10만 원 미만'이 50.1%로 가장 높고, 다음으로는 '1만 원 미만(19.0%)', '10만 원 이상 ~ 20만 원 미만(14.8%)' 등의 순으로 나타남

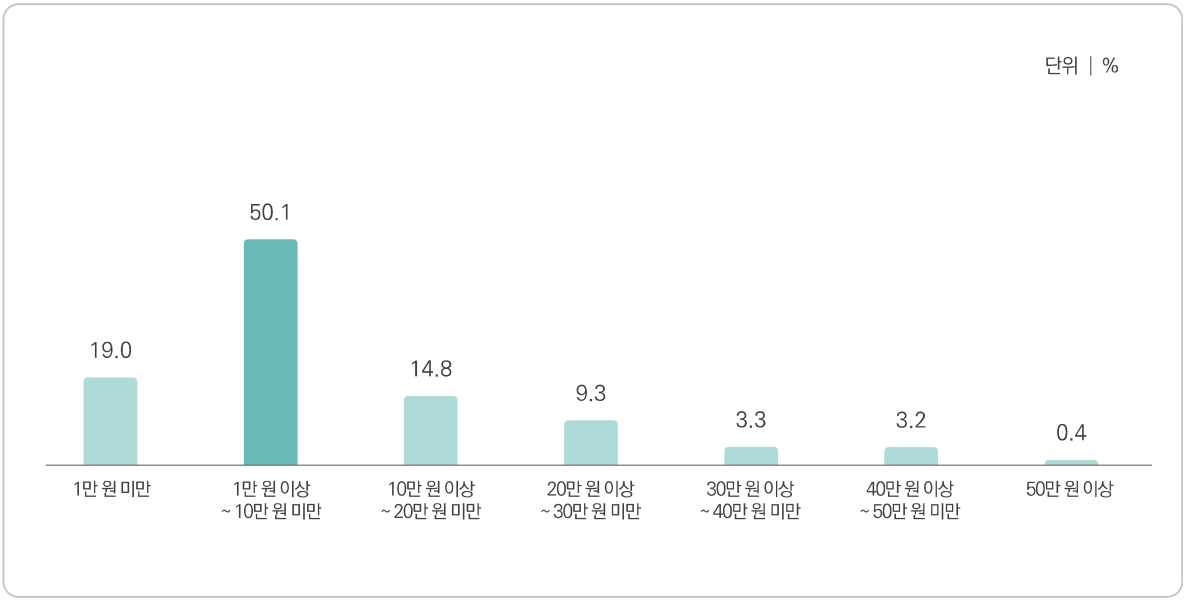


그림 2-2-7 정보보호 금전 소비 규모 - 정보보호 금전 소비 경험자

다 정보보호 금전 소비 계획

» 정보보호 금전 소비 경험자의 금전 소비 적절성 64.9%, 금전 소비 규모 증가 예정 32.7%

- 정보보호 금전 소비의 적절성에 대해 소비가 적절하다고 인식하는 비율이 64.9%로 조사됨
  - 정보보호 금전 소비 증감 여부에 대해 증가 예정이라는 비율이 32.7%로 조사됨

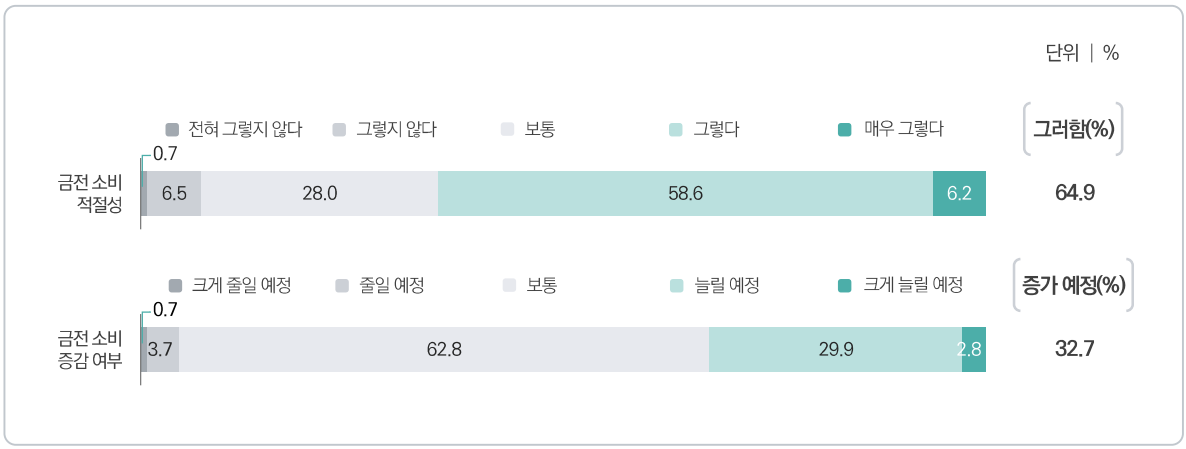


그림 2-2-8 정보보호 금전 소비 계획 – 정보보호 금전 소비 경험자

라 정보보호 금전 소비 지출 의향

» 정보보호 금전 소비 비경험자의 25.8%는 향후 정보보호 금전 소비 지출 의향 있음

- 정보보호 금전 소비 비경험자의 경우, 정보보호 비용 지출 의향에 대해 있다는 응답이 25.8%로 조사됨

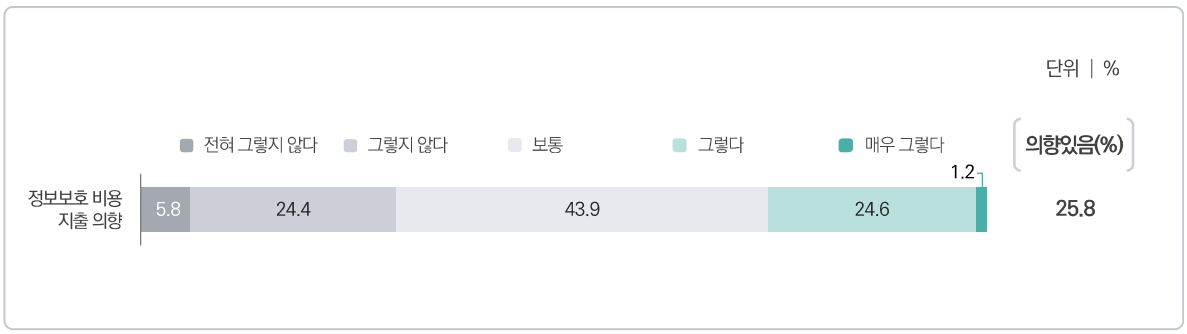


그림 2-2-9 정보보호 금전 소비 지출 의향 – 정보보호 금전 소비 비경험자

3 일상 속의 정보보호

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

인터넷 이용자의 무료 인터넷 연결 사용률 50.3%,
불특정 다수 이용 전자장비 이용 시 예방 활동 수행률 37.7%

- 무료 인터넷 연결 빈도에 대해 인터넷 이용자의 50.3%가 사용한다고 응답함
- 불특정 다수가 이용하는 전자장비 이용 시 예방 활동을 수행한다는 응답이 37.7%로 조사됨

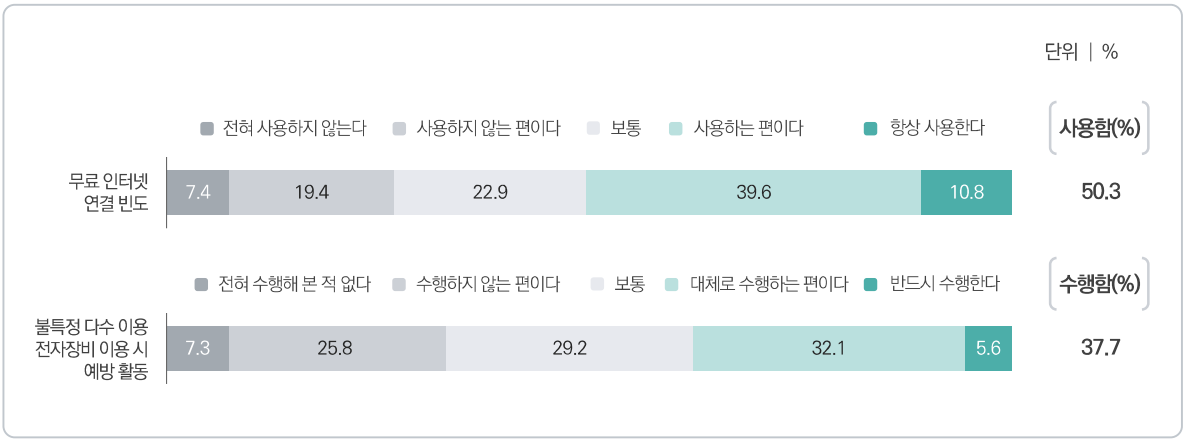


그림 2-2-10 공공장소 무료 인터넷 연결 및 불특정 다수 이용 전자장비 이용 시 예방 활동

나 정보보호 활동

» 인터넷 이용자의 정보보호 활동 수행 비율은 비밀번호 즉시 변경(36.2%), 디지털 데이터 백업(54.3%), 보안 점검 수행(51.2%), 일상 공간 CCTV 활용(14.8%)

- 정보보호 활동 수행률은 '비밀번호 즉시 변경(36.2%)', '디지털 데이터 백업(54.3%)', '보안 점검 수행(51.2%)', '일상 공간 CCTV 활용(14.8%)'으로 조사됨

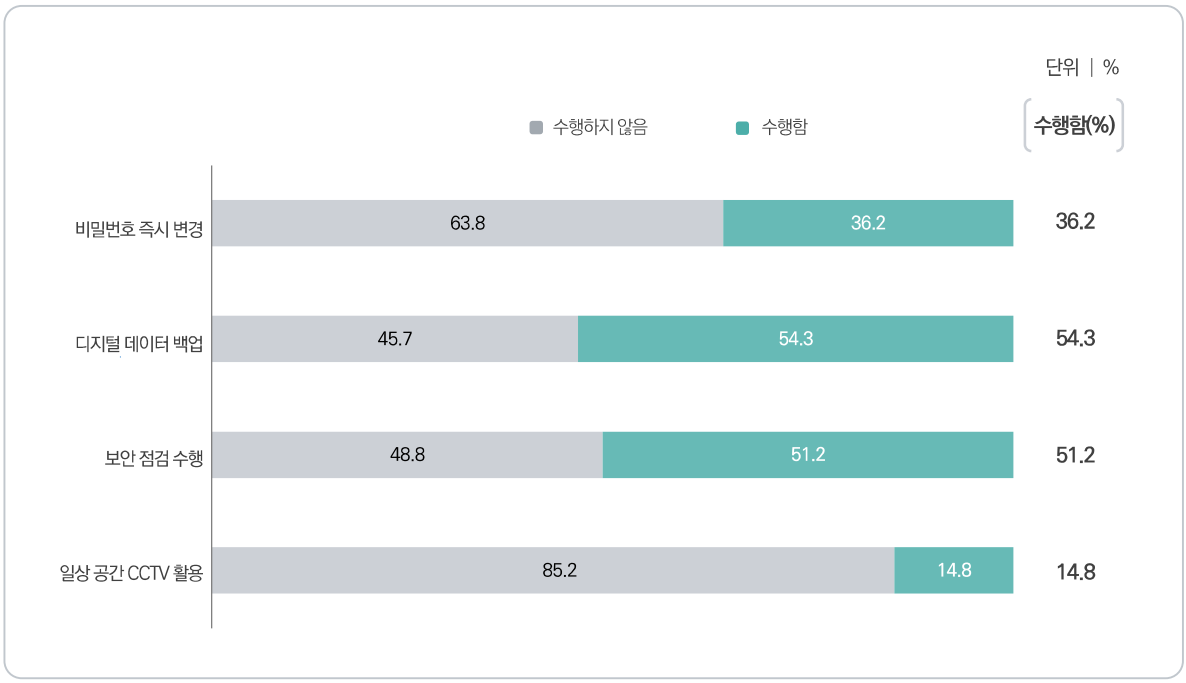


그림 2-2-11 정보보호 활동(요약)

다 비대면 환경의 정보보호 활동

» 인터넷 이용자의 24.1%는 비대면 재택근무·교육 경험

- 비대면 재택근무·교육 경험에 대해 인터넷 이용자의 24.1%가 경험이 있는 것으로 조사됨
  - — 비대면 재택근무·교육 경험자의 경우, 비대면 환경의 정보보호 활동으로 '비대면 환경을 활용하고 있는 컴퓨터로 의심스러운 URL 클릭 등을 하지 않음'이 24.7%로 가장 높고, 다음으로는 '학교·회사 등에서 제공한 정보보호 제품 사용(24.3%)', '재택근무, 화상회의 등 이용 시 관련 프로그램 이외의 프로그램을 사용하거나 작동하지 않음(23.4%)' 등의 순으로 조사됨

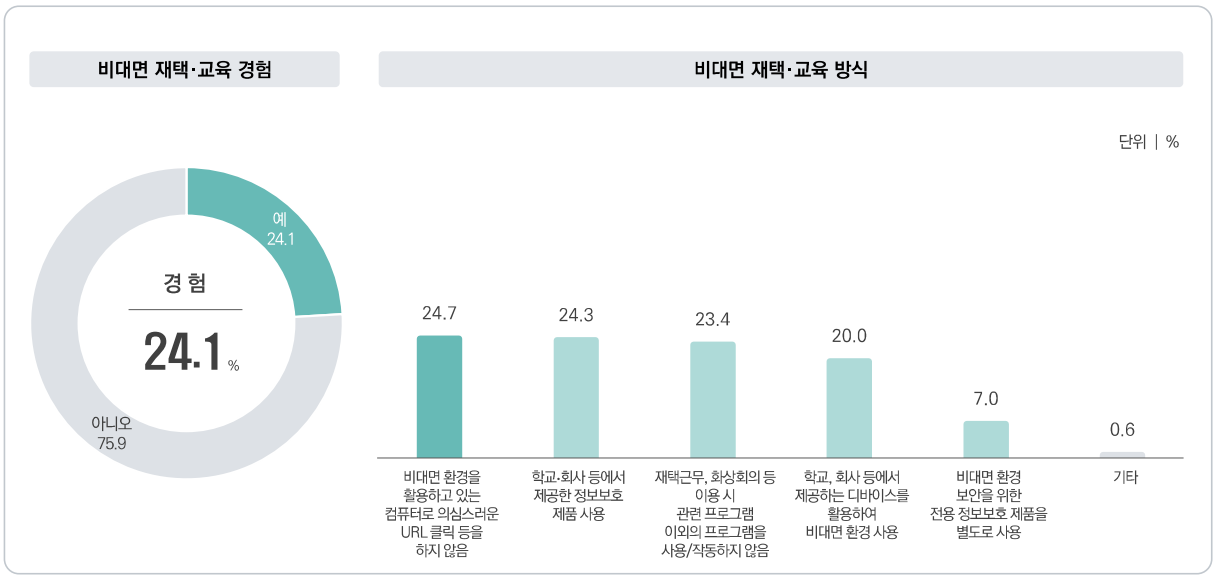


그림 2-2-12 비대면 환경의 정보보호 활동

4 침해사고 경험과 위협 인식

가 침해사고 의심 및 경험

» 인터넷 이용자의 침해사고 의심 경험(23.4%), 침해사고 경험(7.5%)

- 인터넷 이용자의 23.4%는 침해사고를 의심한 적 있다고 응답했으며, 7.5%는 침해사고를 경험한 적 있다고 응답함

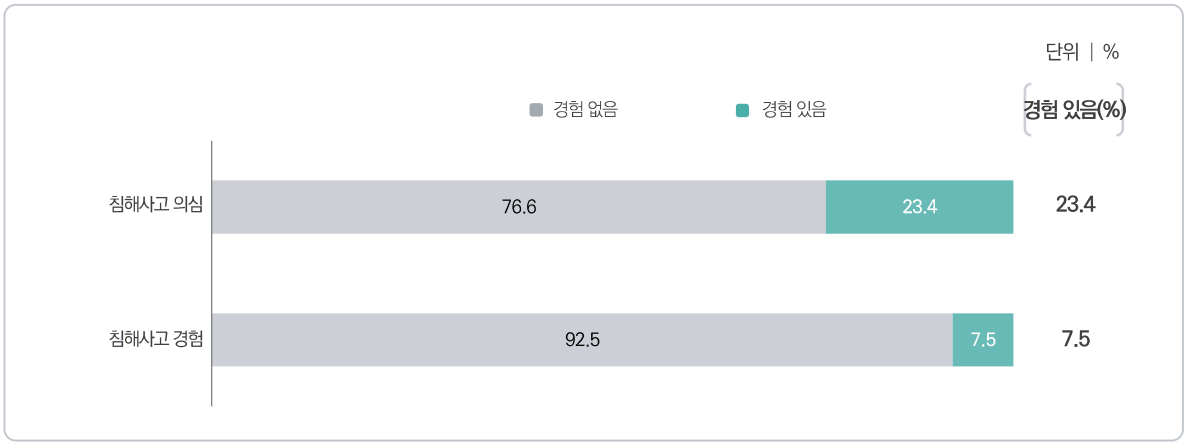


그림 2-2-13 침해사고 의심 및 경험

나 침해사고 피해 심각도

» 인터넷 이용자의 침해사고 피해 심각도는 평균 -0.49점으로 다소 경미

- 침해사고 피해 심각도에 대해 심각하다(심각한 편 + 매우 심각)는 응답이 39.4%로 조사되었으며, 평균은 -0.49점으로 다소 경미한 편으로 인식됨

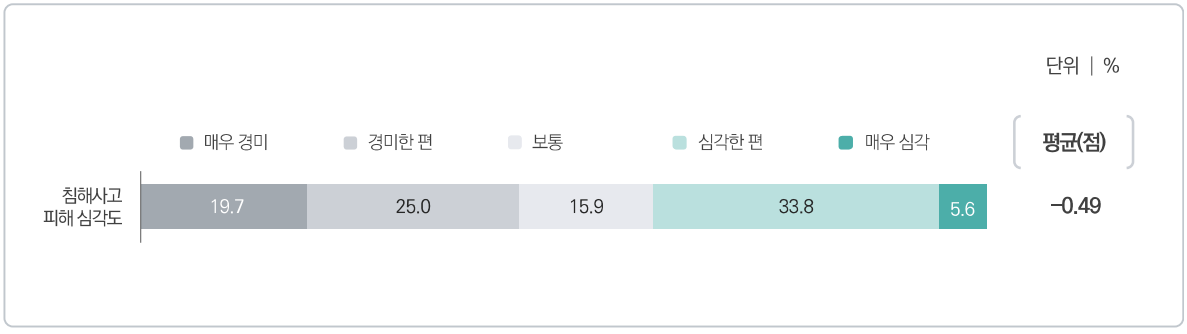


그림 2-2-14 침해사고 피해 심각도

다 침해사고 경험 유형

침해사고 유형 중 'PC·노트북 등 개인용 컴퓨터의 해킹과 같은 불법적 접근'이 36.8%로 가장 높음

- 인터넷 이용자가 경험한 침해사고 유형으로는 'PC·노트북 등 개인용 컴퓨터의 해킹과 같은 불법적 접근'이 36.8%로 가장 높고, 다음으로는 '개인용 모바일 기기(스마트폰, 태블릿, 패드 등)의 해킹과 같은 불법적 접근(31.8%)', '랜섬웨어 또는 악성코드 감염 등에 의한 정상적인 전자장비 사용의 제한(27.9%)' 등의 비율이 뒤를 이음

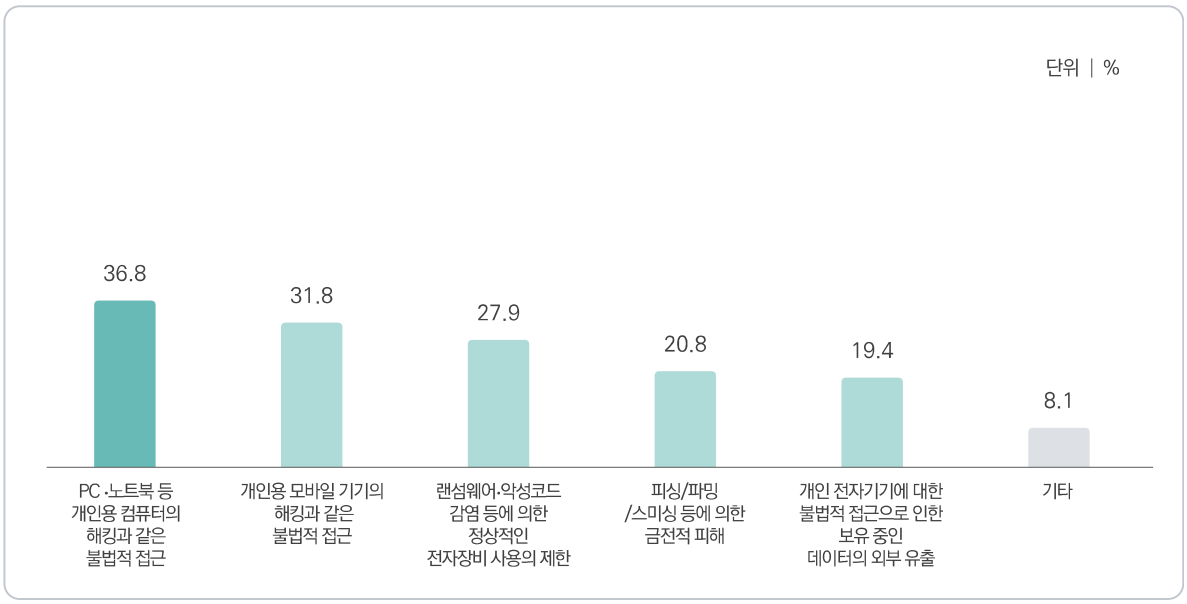


그림 2-2-15 침해사고 경험 유형(복수응답) - 침해사고 경험자

라 침해사고 대응

» 인터넷 이용자의 38.6%는 경험한 침해사고를 신고

- 침해사고 신고에 대해 인터넷 이용자의 38.6%가 경험한 침해사고를 신고한 경험이 있음
  - — 침해사고 미신고자의 경우, 침해사고가 발생했을 당시 관련 기관에 피해 사실을 신고하지 않았던 이유로는 '피해가 심각하지 않았기 때문에'라는 응답이 59.2%로 가장 높음
  - — 다음으로는 '신고에 따른 사건 조사, 처리가 복잡하고 불편하다고 느껴졌기 때문에(34.3%)', '신고하더라도 범인을 체포하거나 처벌할 수 없다고 생각하기 때문에(31.1%)' 등의 순으로 조사됨

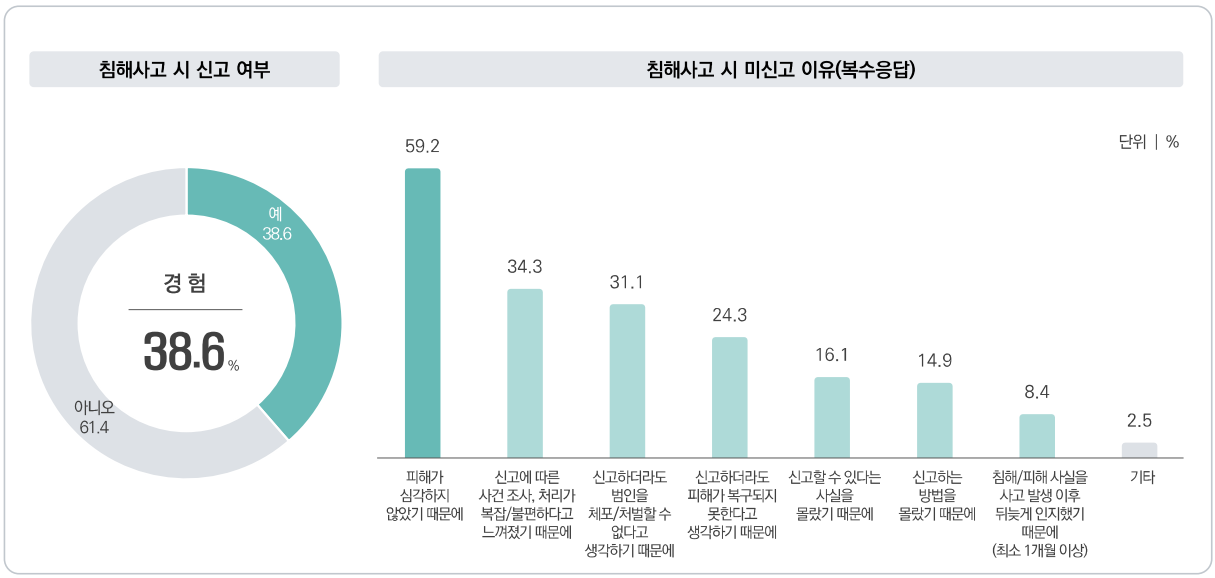


그림 2-2-16 침해사고 신고 및 미신고 이유(복수응답)

01 인터넷 활용 현황 | 02 정보보호 인식 | 03 정보보호 교육 | 04 정보보호 예산
05 일상생활 속의 정보보호 | 06 정보보호 침해사고 경험과 위협 인식

제 3 장

조사결과

3

Ⅰ 인터넷 활용 현황

1 인터넷 활용 현황

가 인터넷 접속 시 사용한 전자기기

- 인터넷 이용자의 인터넷 접속 시 사용한 전자기기로는 '모바일 기기(스마트폰, 태블릿 PC 등)(99.8%)'를 가장 많이 사용하고 있고, 다음으로 '컴퓨터(데스크탑 PC, 노트북 등)(75.4%)', 'IoT 가전제품(스마트 TV, 인공지능 비서 제품 등)(19.0%)' 순으로 나타났다.

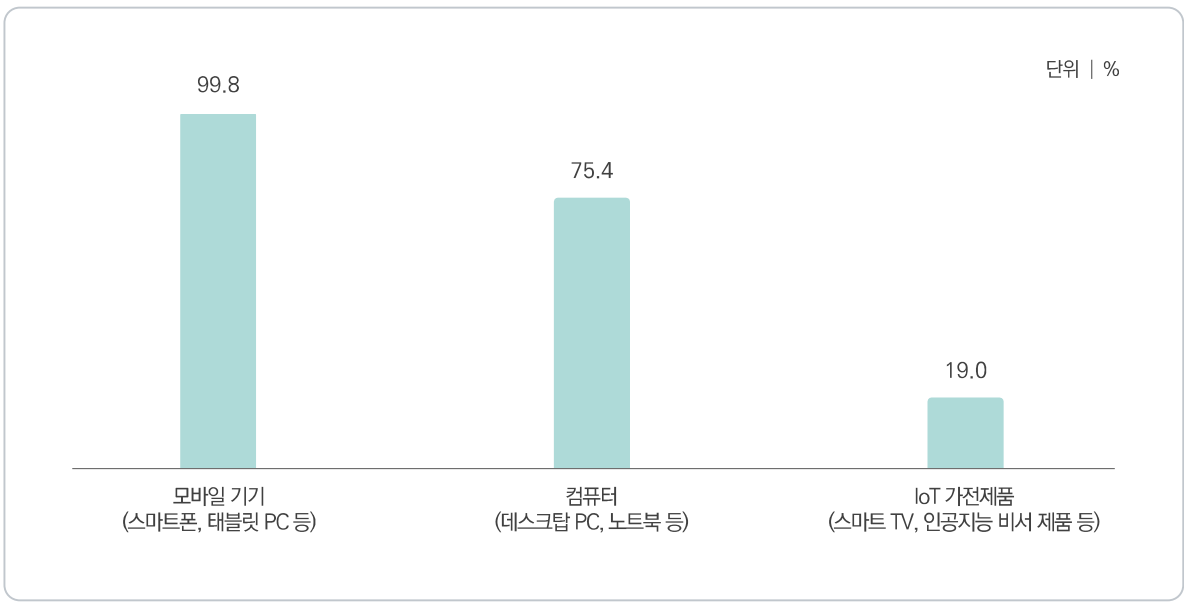


그림 2-3-1 인터넷 접속 시 사용한 전자기기(복수응답)

나 인터넷 접속 시간

- 하루 인터넷 접속 시간으로는 '3시간 초과 ~ 6시간 이하'가 32.4%로 가장 많고, 다음으로 '1시간 초과 ~ 3시간 이하(31.2%)', '6시간 초과 ~ 9시간 이하(17.4%)', '9시간 초과 ~ 12시간 이하(9.8%)' 등의 순으로 나타났다.

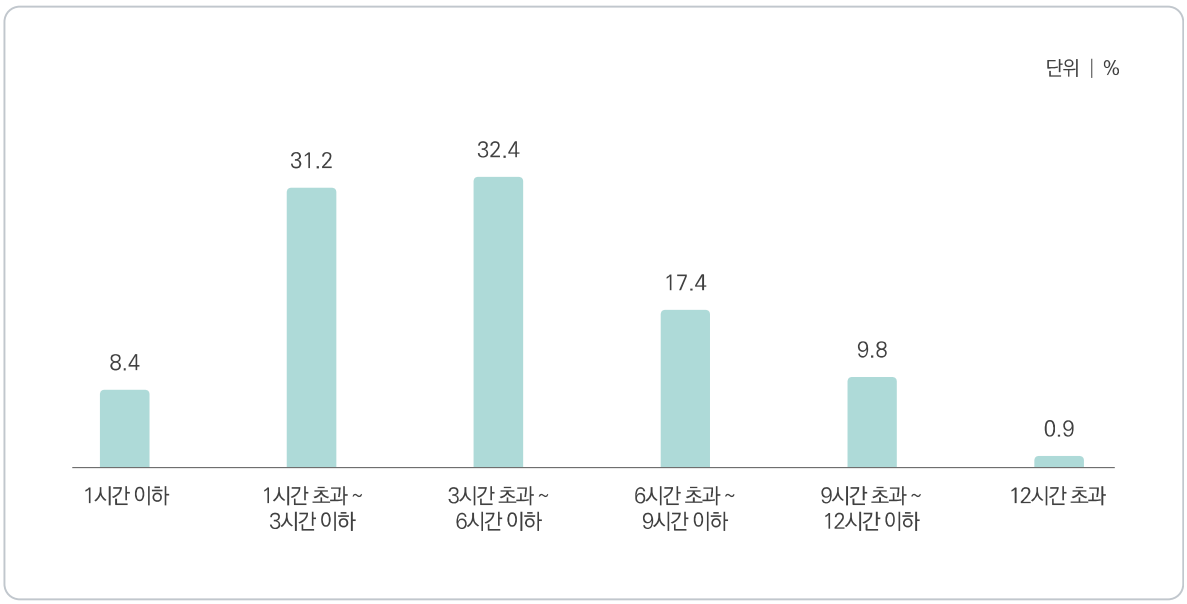


그림 2-3-2 인터넷 접속 시간

다 인터넷 정보 신뢰

- 인터넷에서 접하는 다양한 정보를 신뢰하는 정도는 58.6%가 신뢰한다(신뢰하는 편이다 + 매우 신뢰한다)고 응답했다.

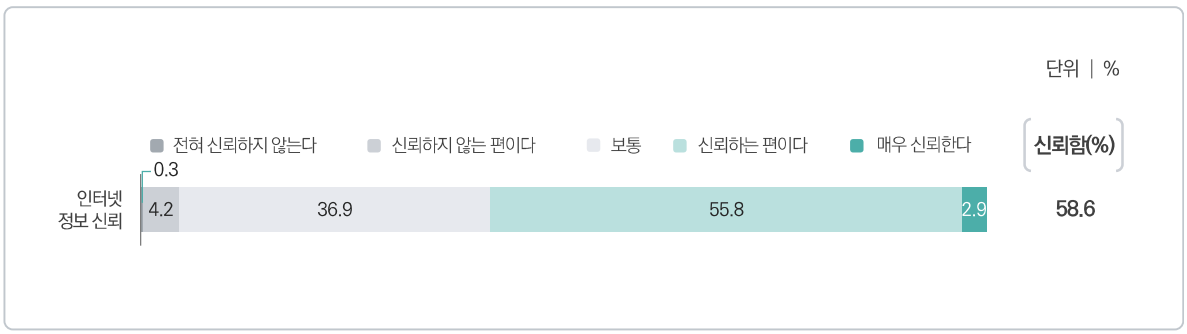


그림 2-3-3 인터넷 정보 신뢰

라 의사결정 시 인터넷 중요도

- 일상생활에서 의사결정 시 인터넷의 중요성에 대해 79.0%가 중요하다(중요한 편이다 + 매우 중요하다)고 응답했다.

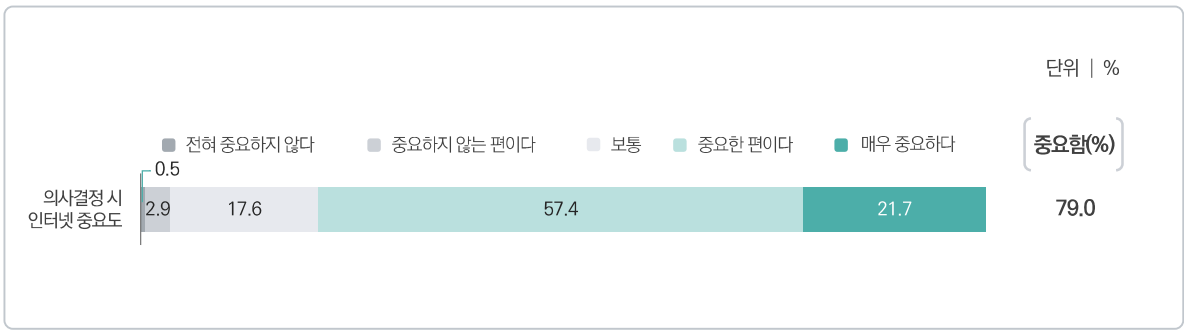


그림 2-3-4 의사결정 시 인터넷 중요도

마 인터넷 사용 시간 과도함

- 일상생활에서 인터넷을 사용하는 시간의 과도함에 대해 40.1%가 과도하다(그렇다 + 매우 그렇다)고 응답했다.

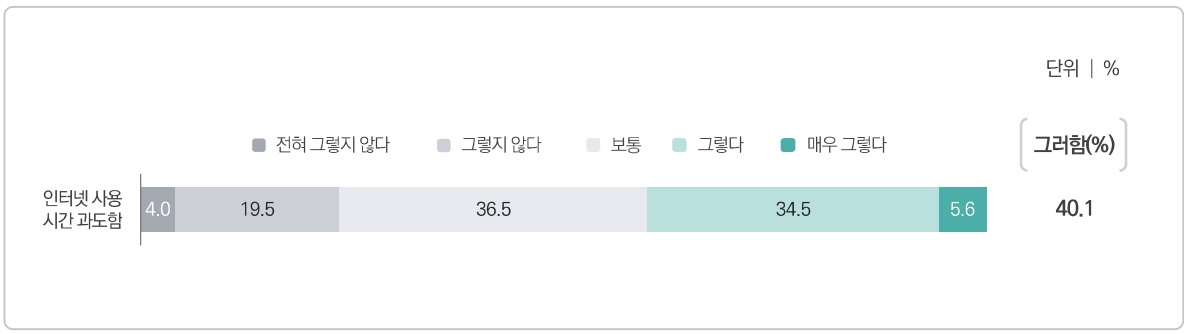


그림 2-3-5 인터넷 사용 시간 과도함

바 정보보호 범죄·사고 보호 체감도

- 일상생활에서 정보보호 관련 각종 범죄 또는 사고와 관련하여 충분히 보호받고 있다고 생각하는 비율은 35.3%가 보호받는다(대체로 보호받는 편이다 + 충분히 보호받고 있다)고 응답했다.

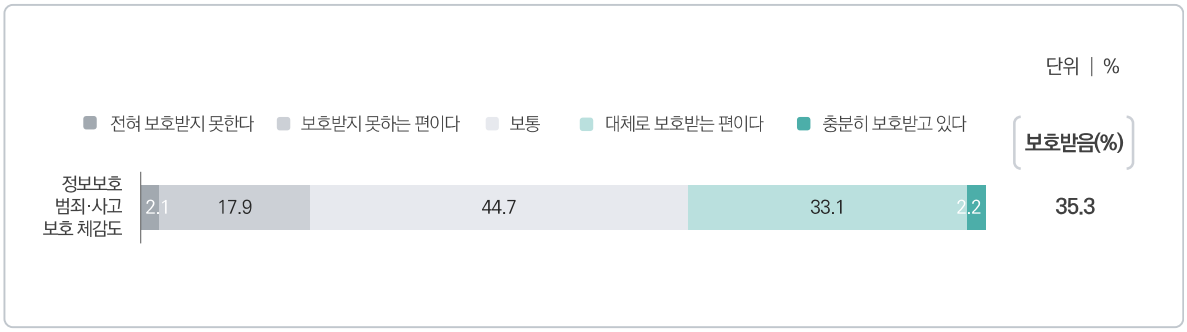


그림 2-3-6 정보보호 범죄·사고 보호 체감도

Ⅱ 정보보호 인식

1 정보보호 인식

가 정보보호 이슈 관심도

- 인터넷 이용자의 56.1%는 정보보호 관련 이슈에 대한 관심이 있다(있는 편이다 + 자주 있다)고 응답했다.

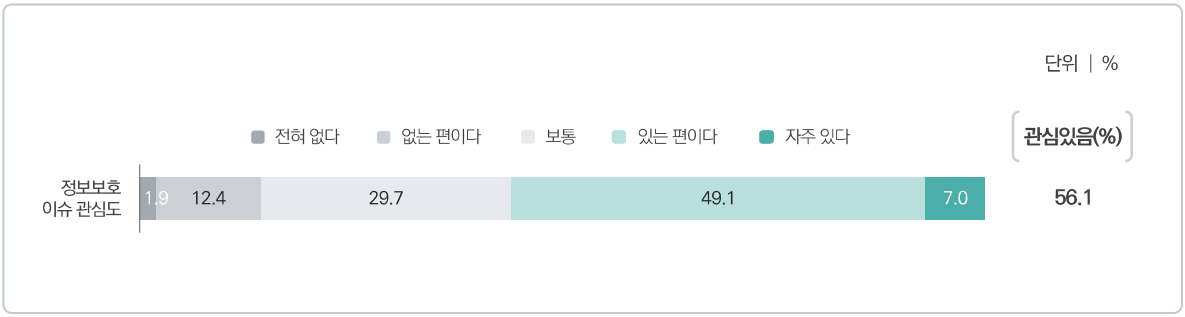


그림 2-3-7 정보보호 이슈 관심도

- 성별로는 '남성(59.2%)'이 '여성(52.9%)' 대비 다소 정보보호 이슈에 대한 관심도가 높게 나타났다.
- 연령별로는 '20대(65.2%)'에서 가장 높게 조사되었다.
  반면, '60대(45.2%)'의 정보보호 이슈 관심도는 타 연령대 대비 상대적으로 낮게 나타났다.

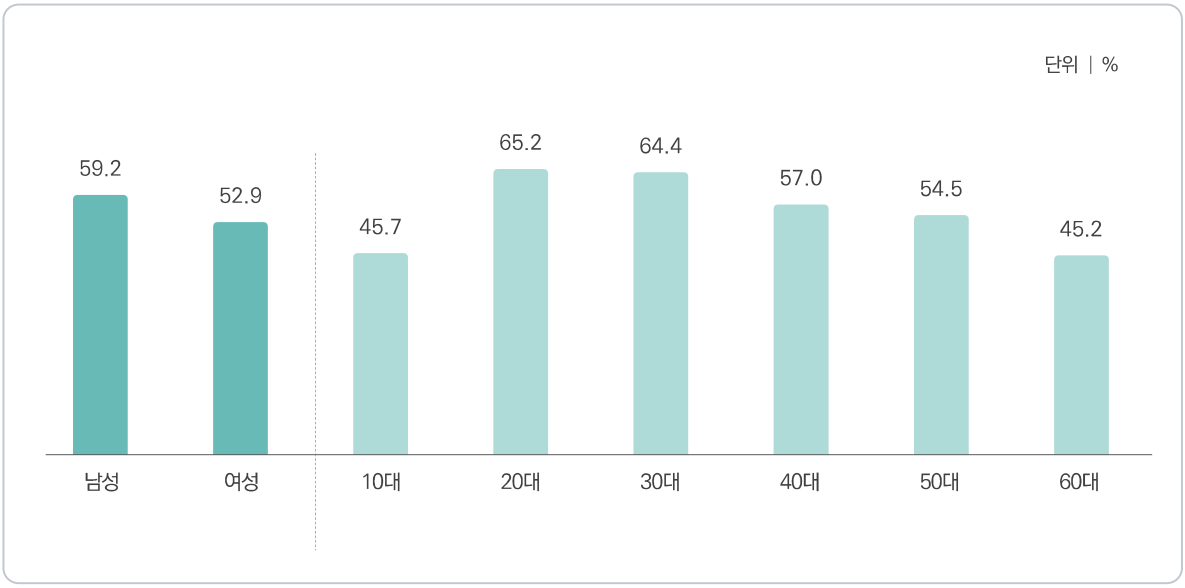


그림 2-3-8 성·연령별 정보보호 이슈 관심도

나 정보보호 침해 우려 정도

- 정보보호 침해 우려 정도에 대해 62.8%는 우려한다(우려하는 편이다 + 매우 우려한다)고 응답했다.

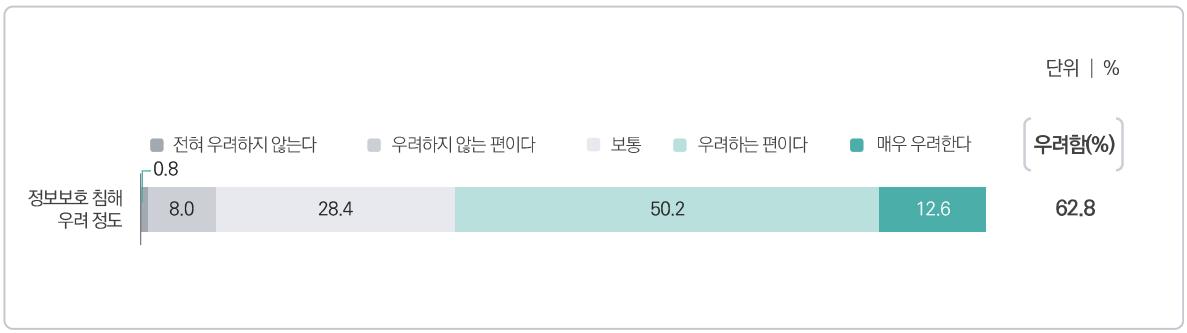


그림 2-3-9 정보보호 침해 우려 정도

다 정보보호 침해사고 소식에 대한 관련성 인식

- 정보보호 관련 사고 소식에 대하여 일반 개인이 자신과 관련성이 있다고 여기는 비율은 47.4%(관련있는 편이다 + 매우 관련있다)인 것으로 조사되었다.

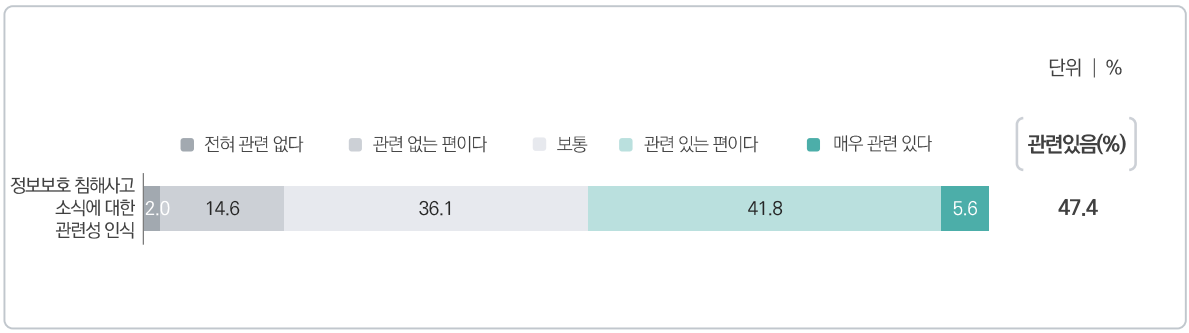


그림 2-3-10 정보보호 침해사고 소식에 대한 관련성 인식

라 안전 체감도

- 정보보호 관련 이슈에 대한 안전 체감도는 '개인 생활 공간 불법 접근'이 37.7%로 가장 높고, 다음으로 '사생활 침해(29.0%)', '전자기기 악성코드 감염(25.9%)', '전자기기 분실 정보 유출(23.2%)' 등의 순으로 조사되었다.

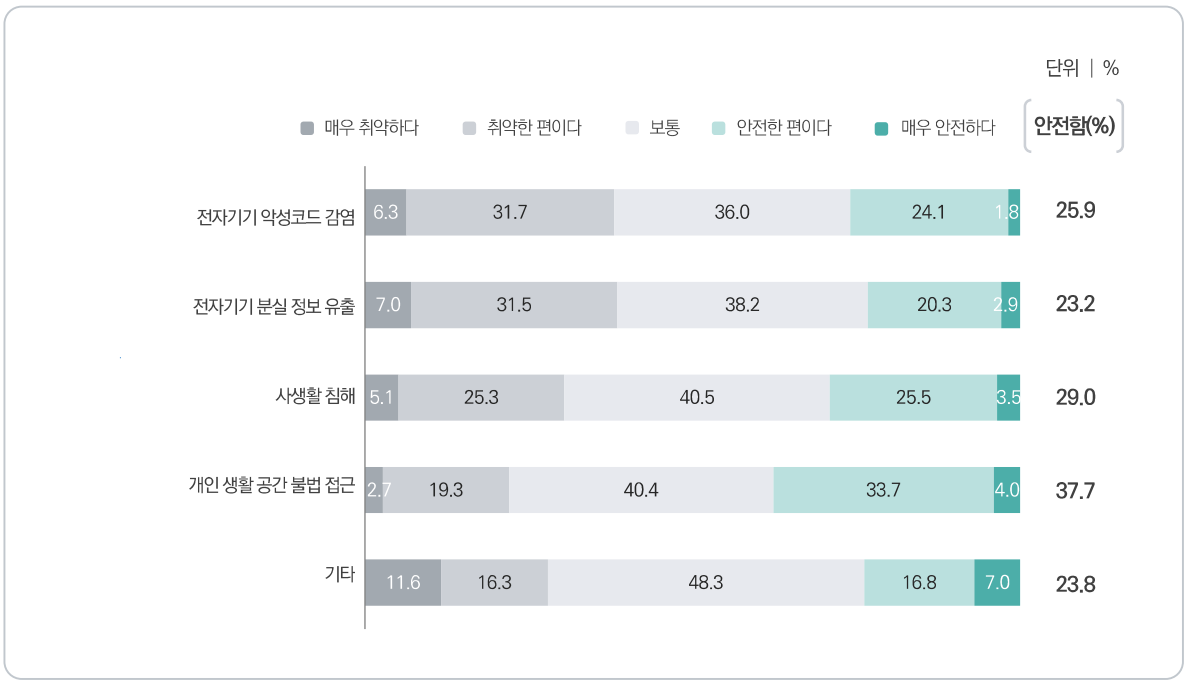


그림 2-3-11 안전 체감도(요약)

마 침해사고 발생 시 피해 복구 가능성

- 침해사고 발생 시 피해 복구 가능성에 대해 25.8%는 복구할 수 있다(그러한 편이다 + 매우 그렇다)고 조사되었다.

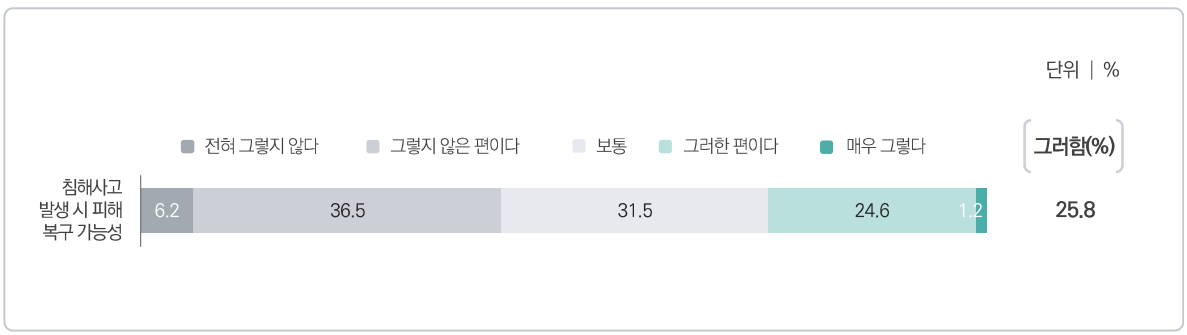


그림 2-3-12 침해사고 발생 시 피해 복구 가능성

바 침해사고 발생 원인

- 일반 개인이 생각하는 정보보호 침해사고 발생 원인으로는 '낮은 처벌 기준 및 형량'이라는 응답이 78.3%로 가장 높으며, '사법기관 범죄 처벌 노력 부족(72.1%)', '정보통신 서비스 제공 기업 사고 방지 노력 부족(67.5%)', '정부·공공기관 사고 방지 노력 부족' 및 '수사·공공기관 관련 범죄자 수사 노력 부족(각 66.0%)' 등의 순으로 조사되었다.

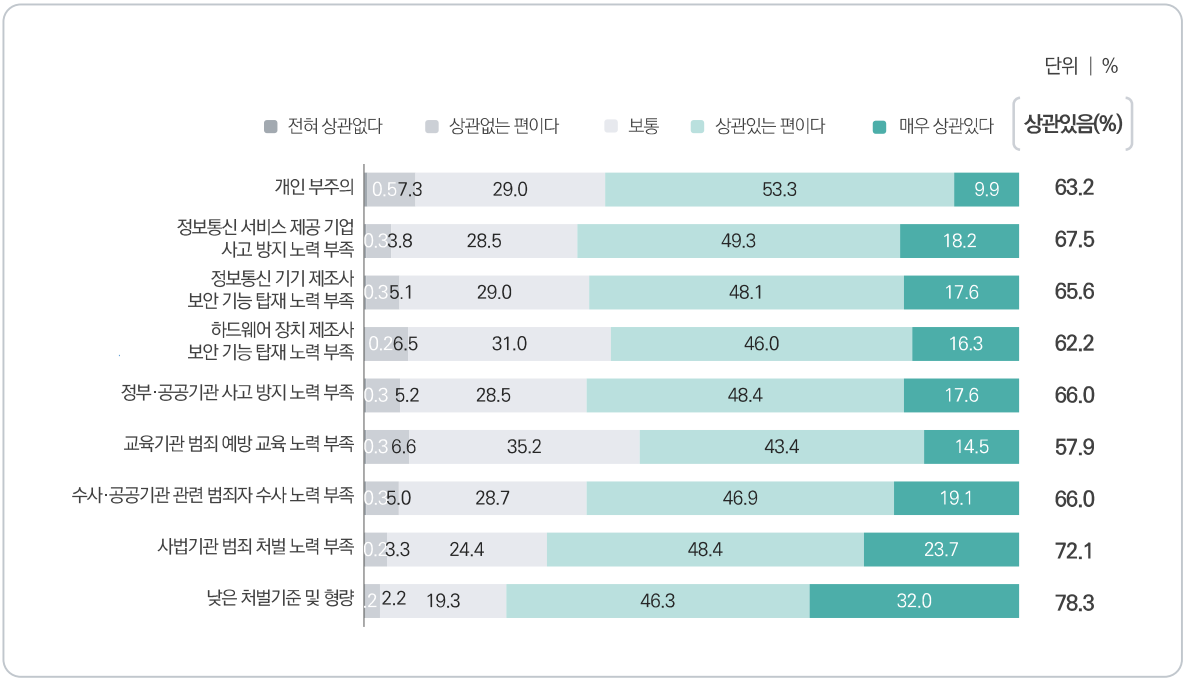


그림 2-3-13 침해사고 발생 원인(요약)

사 침해사고 방지 주체

- 정보보호 침해사고 방지를 위해 주도적으로 노력해야 하는 주체에 대해 '기업 또는 공공'이 56.2%로 '개인(43.8%)'의 노력 대비 높게 조사되었다.

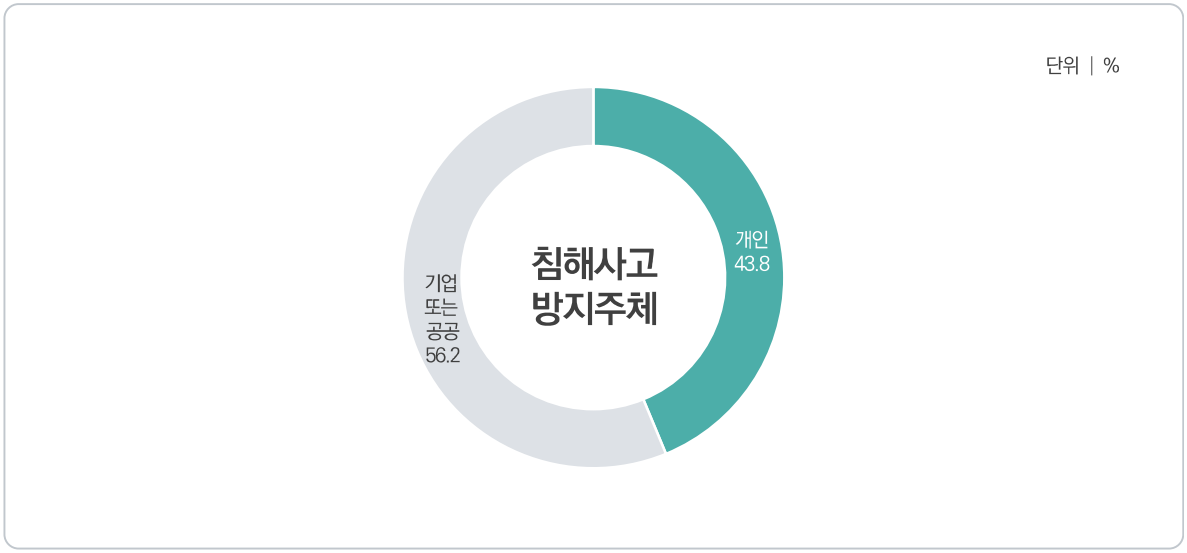


그림 2-3-14 침해사고 방지 주체

아 기관·업체 신뢰도

- 정보보호 관련 기관·업체의 신뢰도에 대해 '정부부처·공공기관'이 48.4%로 가장 높게 나타났고, 다음으로 '민간업체(33.4%)', '인터넷 서비스 제공자(29.0%)' 등의 순으로 나타났다.

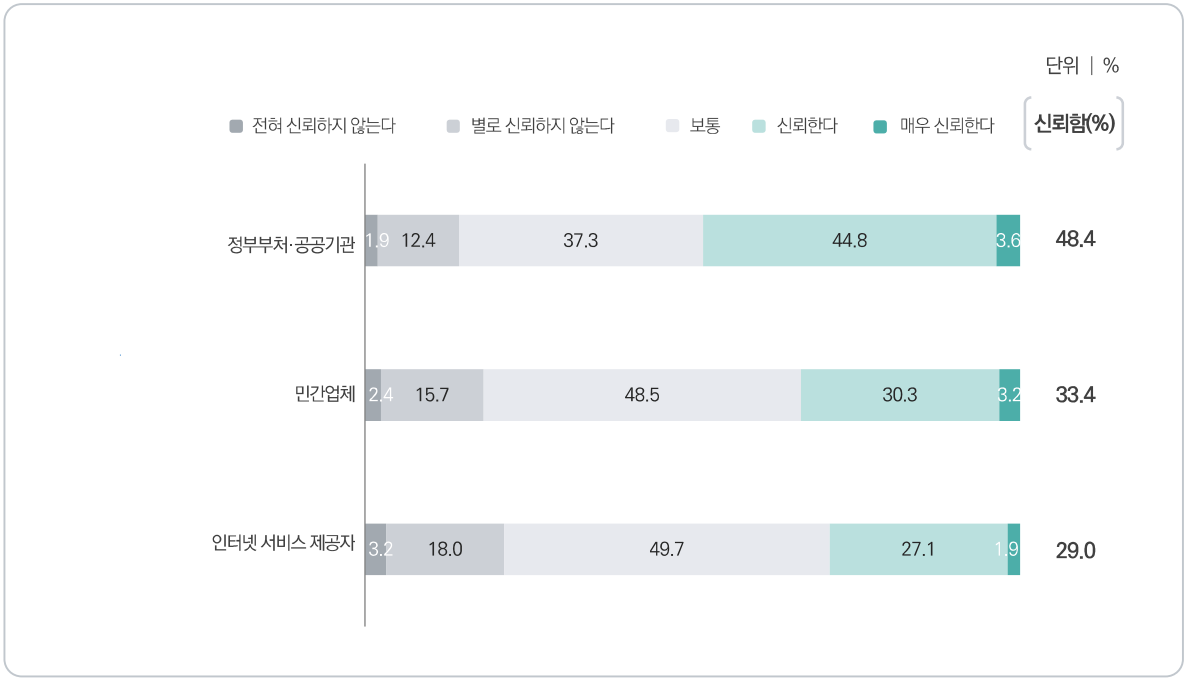


그림 2-3-15 기관·업체 신뢰도(요약)

Ⅲ 정보보호 교육

1 정보보호 교육

가 정보보호 교육

- 인터넷 이용자의 15.3%는 최근 1년간 정보보호 관련 교육을 받은 적이 있다고 응답했다.

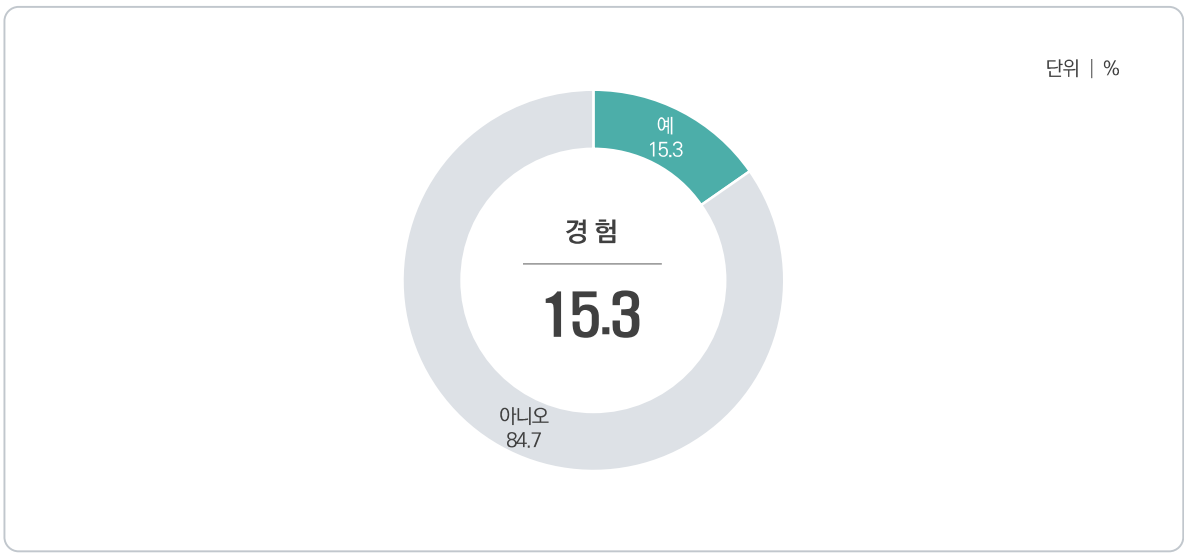


그림 2-3-16 정보보호 교육

- 정보보호 교육에 대해 '남성(16.7%)'이 '여성(13.8%)'보다 교육을 받은 비율이 높게 나타났다.
- 연령별로는 '10대(31.1%)'에서 가장 높게 조사되었다. 반면, '60대(3.7%)'의 교육 진행률은 타 연령대 대비 상대적으로 낮게 나타났다.

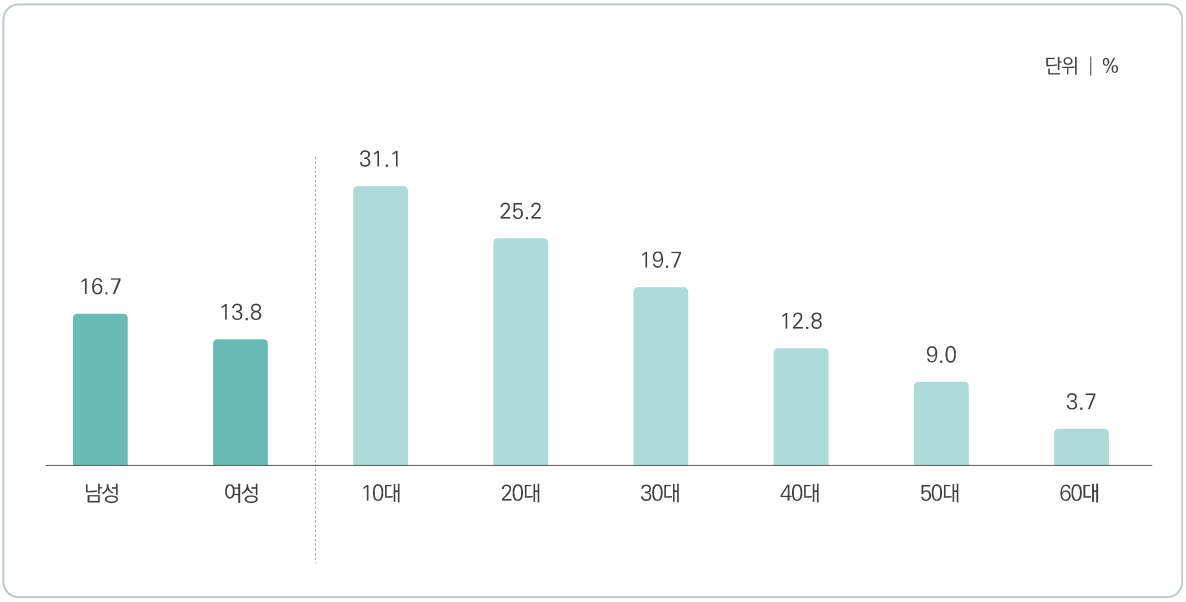


그림 2-3-17 **성·연령별 정보보호 교육**

나 정보보호 교육 방식

- 정보보호 교육의 방식으로는 '근무지 혹은 학교 등에서의 온라인 교육 수강'이 67.3%로 가장 높고, 다음으로 '근무지 혹은 학교 등에서의 오프라인 교육 수강(32.9%)', '개인적인 방식으로 온라인 교육 수강(줌(ZOOM), EBS 온라인클래스, 유튜브 등)(21.9%)', '근무지 외 개인적인 방식으로 오프라인 교육 수강(학교, 도서관 등)(5.8%)'의 순으로 조사되었다.

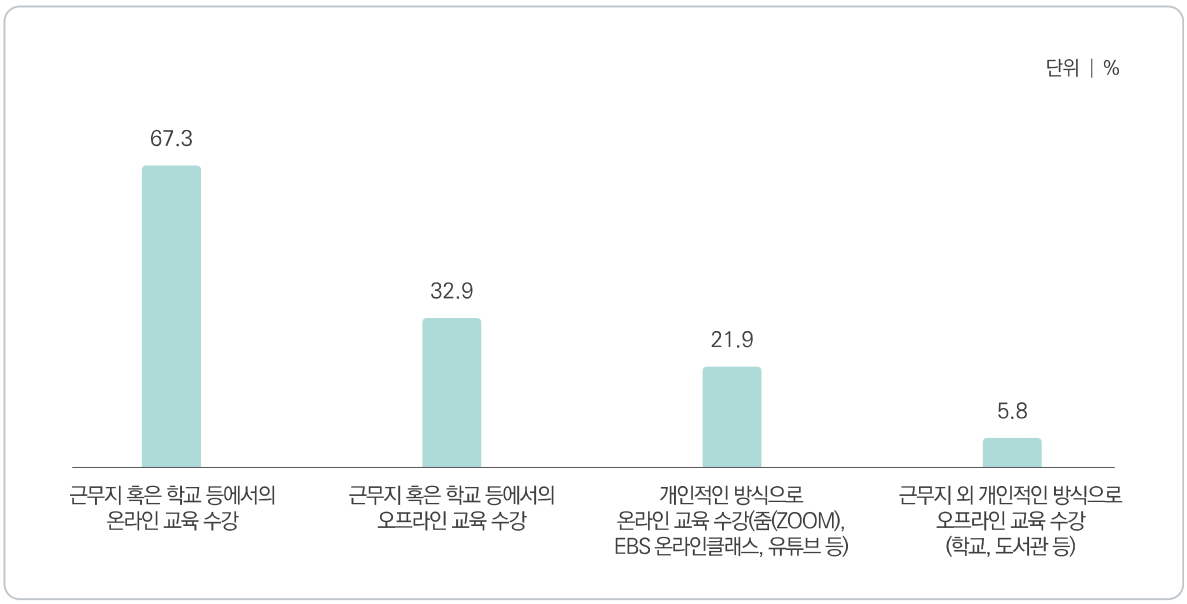


그림 2-3-18 **정보보호 교육 방식(복수응답) - 정보보호 교육 경험자**

다 정보보호 교육 주제

- 정보보호 교육의 주제로는 '정보보호를 위한 사고 예방 방법'이 70.4%로 가장 높고, 다음으로 '정보보호의 중요성(65.7%)', '정보보호 피해 사례(59.3%)', '정보보호 피해 대응 방법(57.7%)' 등의 순으로 나타났다.

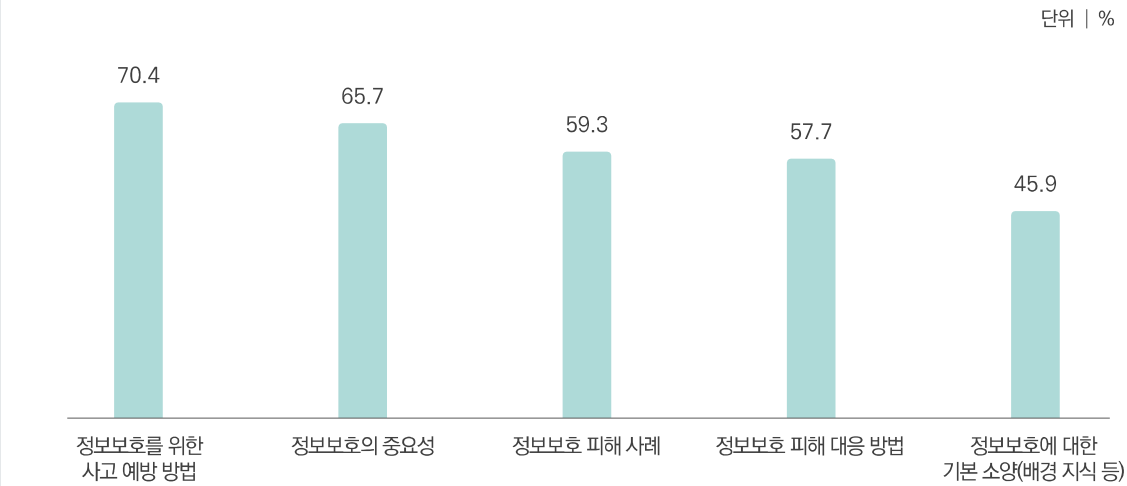


그림 2-3-19 **정보보호 교육 주제(복수응답) - 정보보호 교육 경험자**

라 정보보호 교육 학습 효과

- 정보보호 교육 효과에 대해 '정보보호의 중요성에 대한 인식'이 72.4%로 가장 높고, 다음으로 '정보보호에 대한 기본 소양(배경 지식 등)의 함양(71.6%)', '정보보호 피해 사례에 대한 인식(70.0%)', '정보보호를 위한 사고 예방 방법에 대한 인식(68.8%)' 등의 순으로 나타났다.

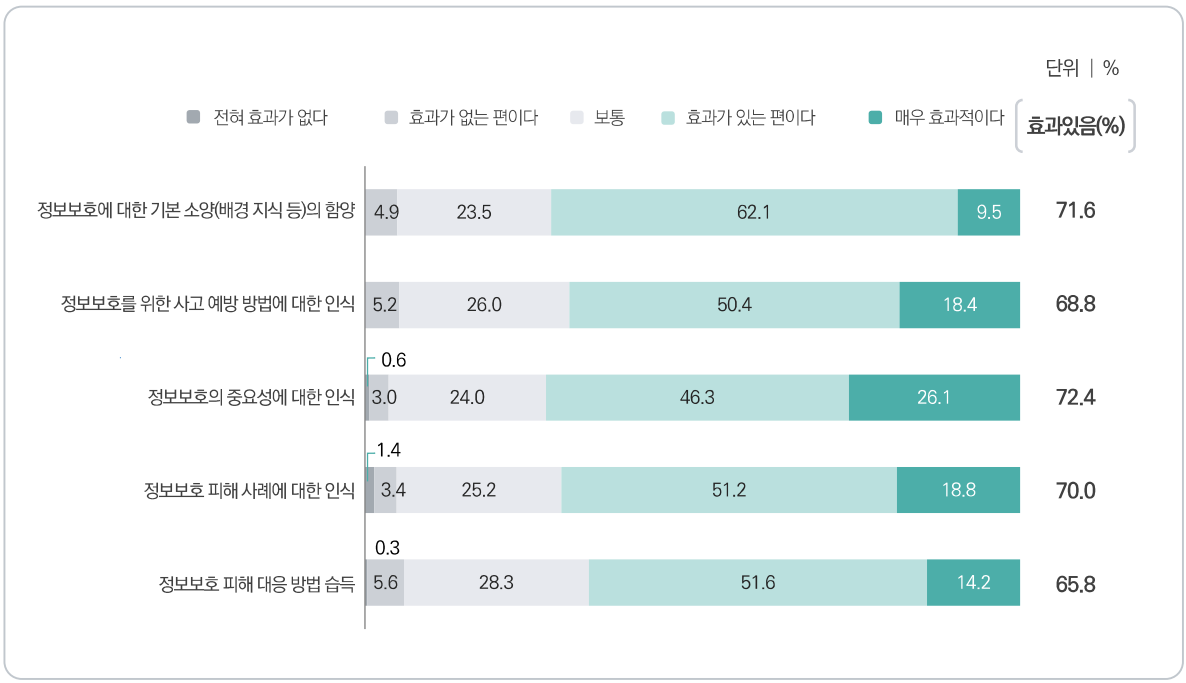


그림 2-3-20 정보보호 교육 학습 효과(요약) – 정보보호 교육 경험자

마 정보보호 교육의 학습 난이도

- 정보보호 관련 교육을 받은 경험자는 학습 난이도와 관련하여 '정보보호 피해 대응 방법'이 가장 이해하기 쉬웠으며, '정보보호의 중요성', '정보보호에 대한 기본 소양(배경 지식 등)' 등의 순으로 이해하기 쉬운 것으로 응답하였다.

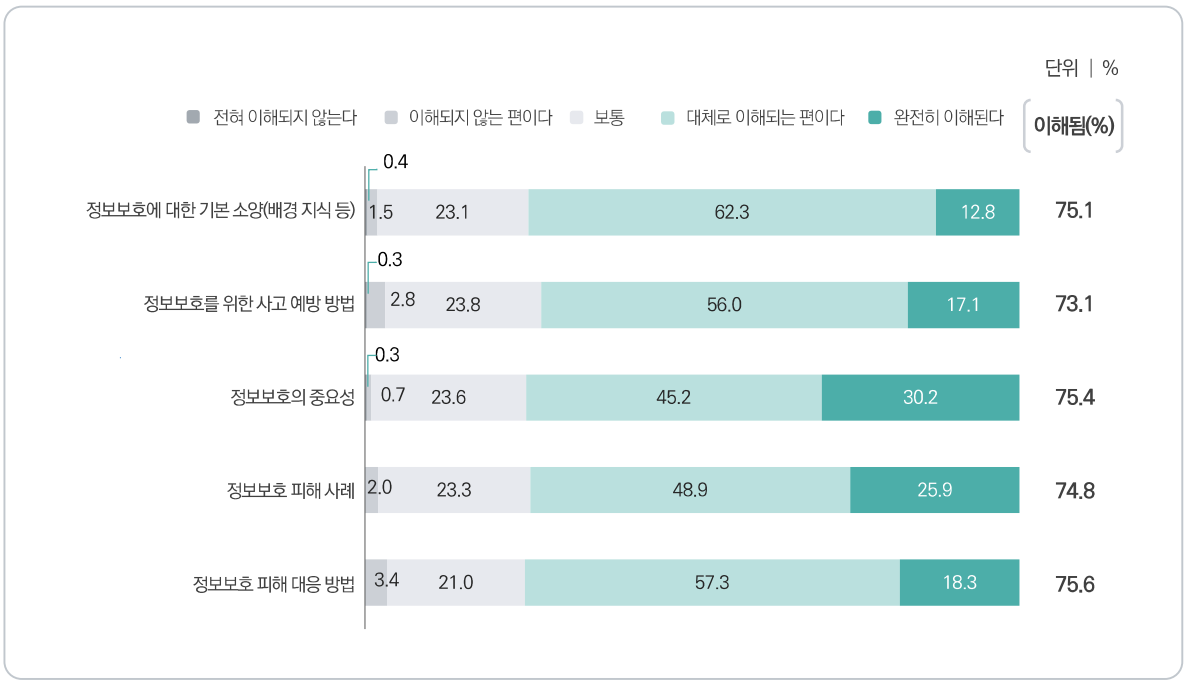


그림 2-3-21 정보보호 교육의 학습 난이도(요약) – 정보보호 교육 경험자

바 정보보호 관련 학습의 어려움

- 정보보호 관련 교육을 받아본 경험자는 학습 간의 어려운 점에 대하여 '정보의 양이 많고 복잡하다'는 응답이 가장 많았으며, '정보보호 관련 용어가 생소하고 어려움', '정보를 얻는 곳을 모름'에 대한 순으로 응답하였다.

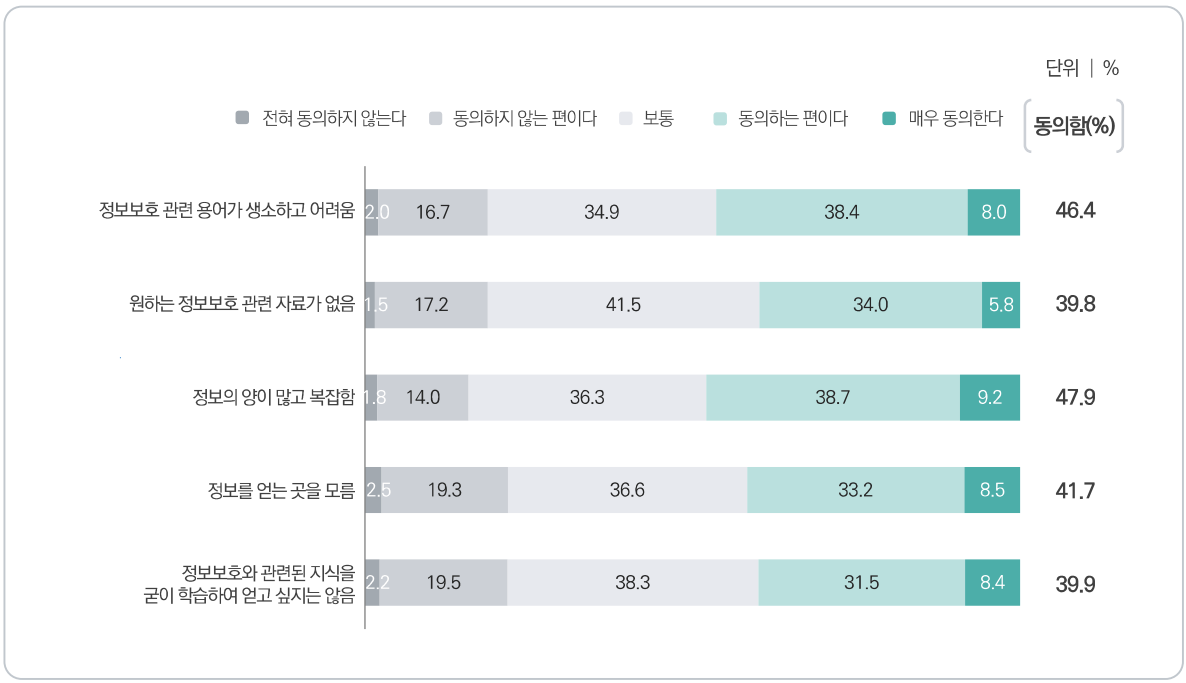


그림 2-3-22 정보보호 관련 학습의 어려움(요약) - 정보보호 교육 경험자

Ⅳ 정보보호 예산

1 정보보호 예산

가 정보보호 금전 소비 경험

- 인터넷 이용자의 13.2%는 최근 1년간 개인적 목적으로 정보보호 관련 소비를 한 경험이 있는 것으로 조사되었다.

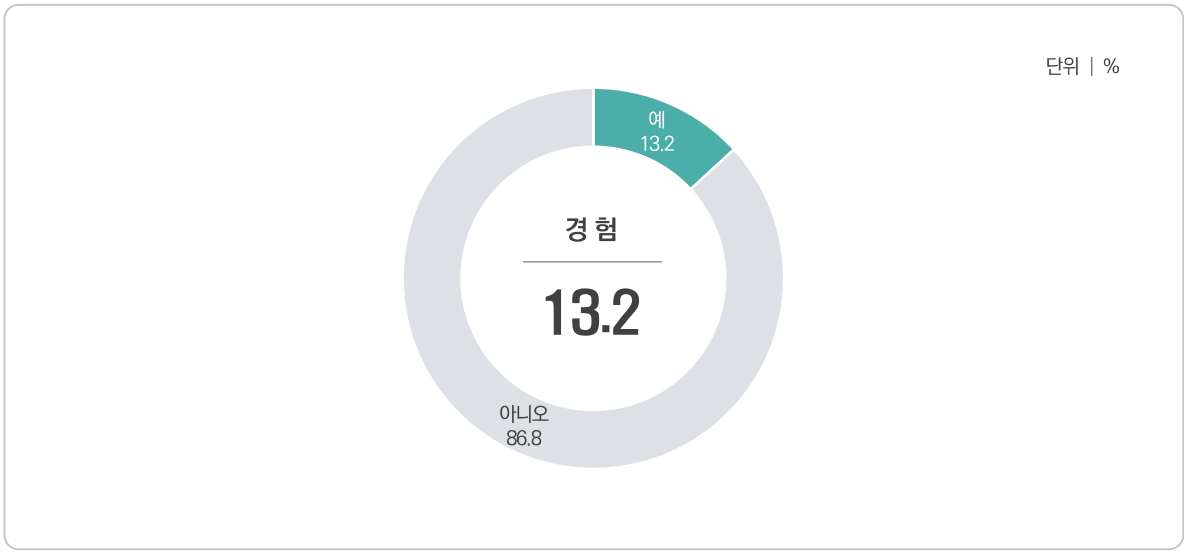


그림 2-3-23 정보보호 금전 소비 경험

- 정보보호 금전 소비 경험은 '남성(14.6%)'이 '여성(11.7%)'보다 소비율이 높게 나타났다.
- 연령별로는 '20대(20.7%)'에서 가장 높게 조사되었다. 반면, '10대(4.7%)'의 소비율은 타 연령대 대비 상대적으로 낮게 나타났다.

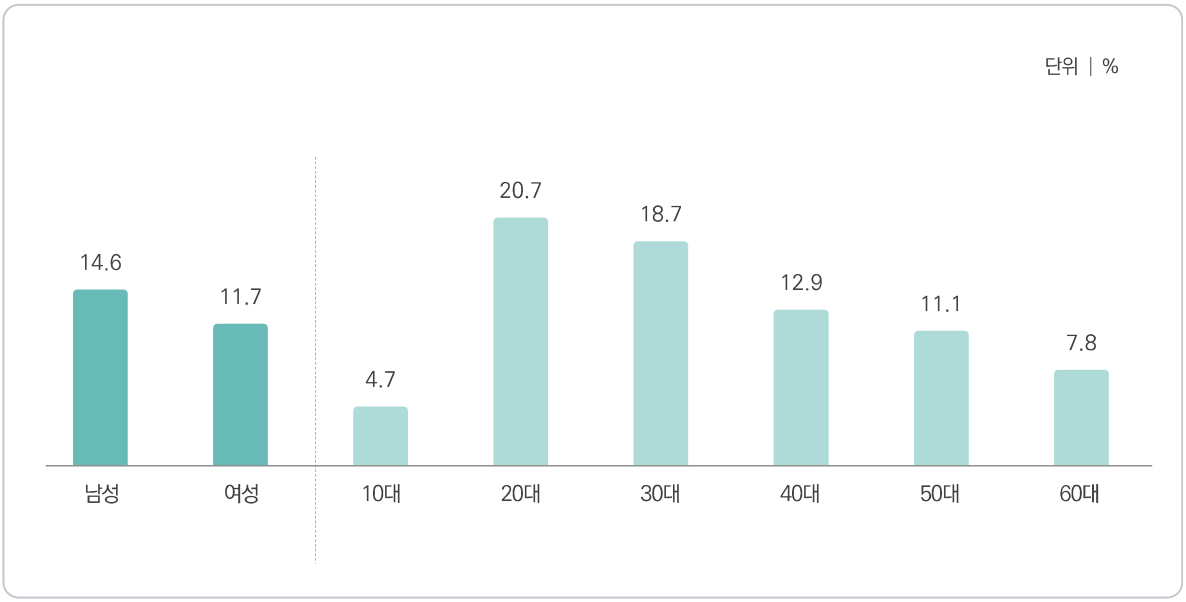


그림 2-3-24 **성·연령별 정보보호 금전 소비 경험**

나 정보보호 금전 소비 유형

- 정보보호 관련 금전 소비를 경험한 적이 있는 인터넷 이용자의 경우, '정보보호 관련 유료 인증서의 결제'가 41.1%로 가장 높고, 다음으로 '정보보호 관련 제품 및 솔루션의 구입(오픈소스, 월 SW 구독료, 클라우드 등 포함)(36.4%)', '자택 또는 개인 생활 공간의 CCTV 등 영상감시장비 설치 또는 증설(유지·보수 포함)(22.6%)', '자택 또는 개인 생활 공간을 위한 출동보안 서비스 이용(19.6%)' 등의 순으로 조사되었다.

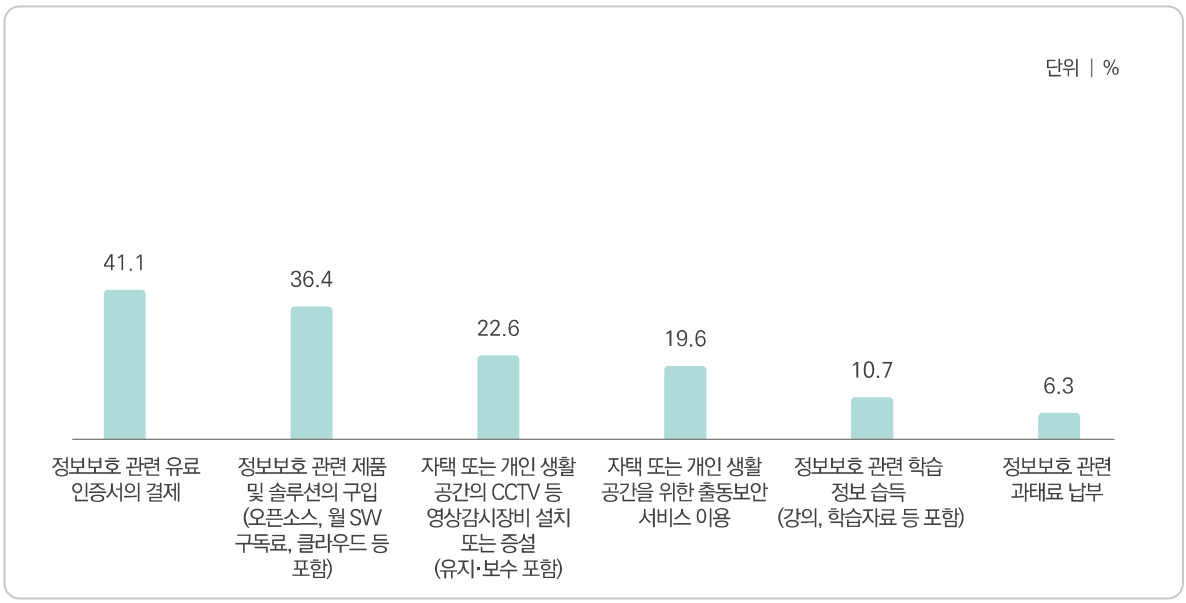


그림 2-3-25 정보보호 금전 소비 유형(복수응답) - 정보보호 금전 소비 경험자

다 정보보호 금전 소비 규모

- 정보보호 관련 금전 소비 규모는 '1만 원 이상 ~ 10만 원 미만'이 50.1%로 가장 높고, 다음으로 '1만 원 미만(19.0%)', '10만 원 이상 ~ 20만 원 미만(14.8%)', '20만 원 이상 ~ 30만 원 미만(9.3%)' 등의 순으로 조사되었다.

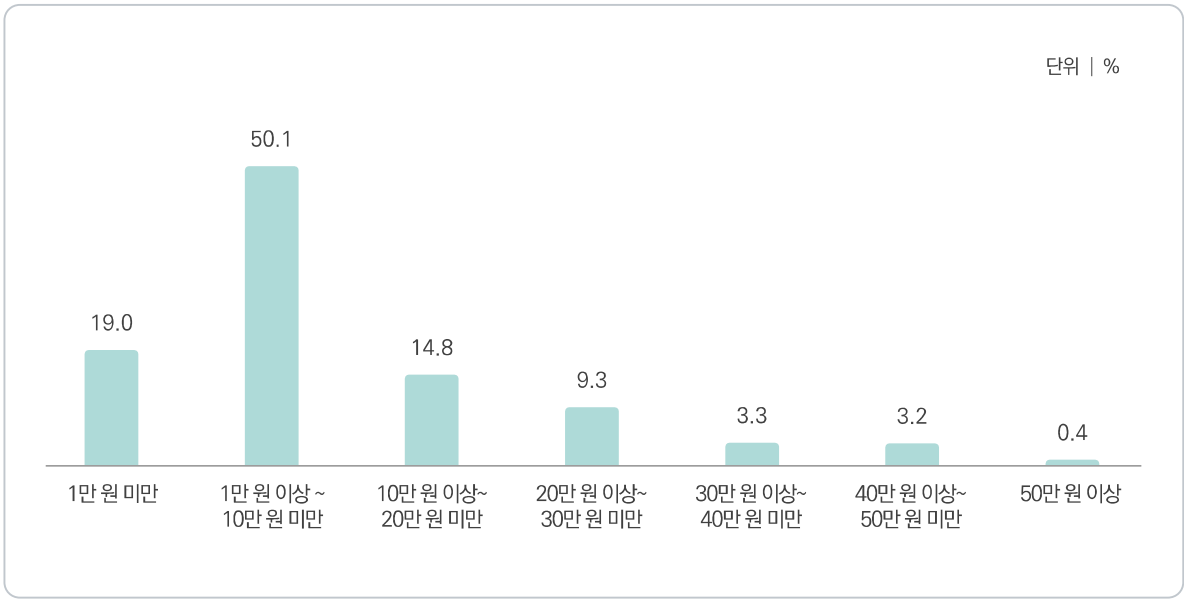


그림 2-3-26 정보보호 금전 소비 규모 - 정보보호 금전 소비 경험자

라 정보보호 금전 소비 계기

- 정보보호 관련 금전 소비 계기는 'TV 또는 온라인 매체(뉴스, 유튜브, SNS 등)를 통한 정보 습득으로 위험성을 인지한 이후'가 59.4%로 가장 높고, 다음으로 '주변 지인의 정보보호 침해사고 피해를 간접적으로 접한 이후(53.6%)', '주변 지인의 추천을 통해(48.8%)', '정보보호 기업체의 홍보자료 또는 영업을 접한 이후(27.8%)' 등의 순으로 조사되었다.

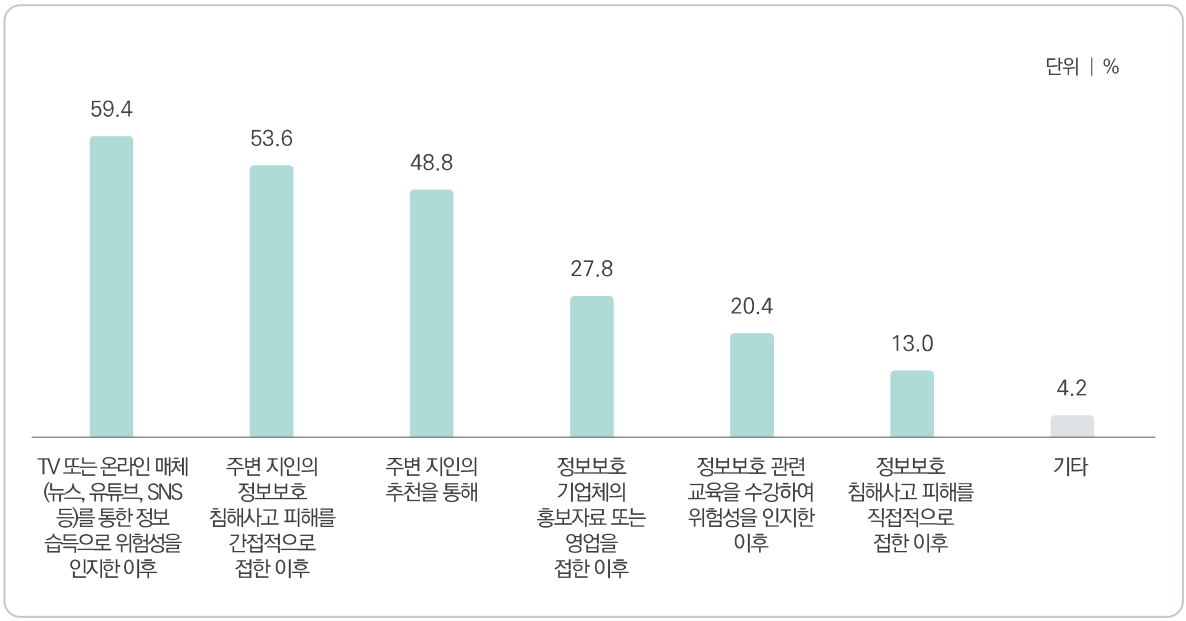


그림 2-3-27 정보보호 금전 소비 계기(복수응답) - 정보보호 금전 소비 경험자

마 정보보호 금전 소비 적절성

- 정보보호 관련 금전 소비 적절성에 대해 64.9%는 소비가 적절하다(그렇다 + 매우 그렇다)고 응답했다.

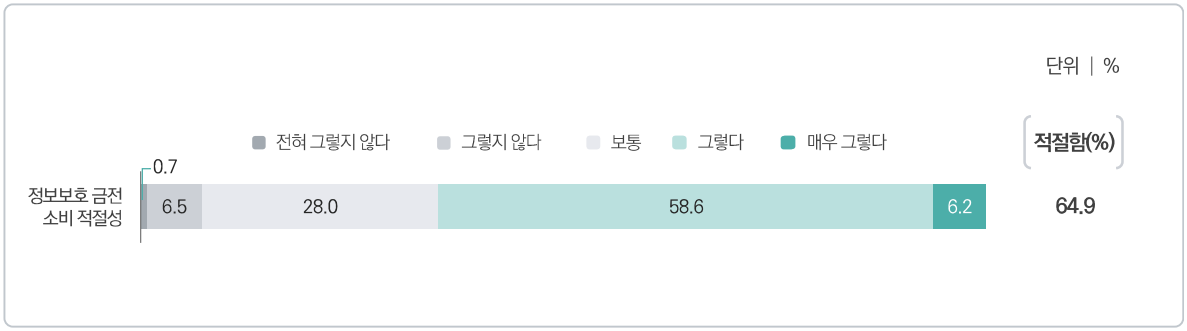


그림 2-3-28 정보보호 금전 소비 적절성 – 정보보호 금전 소비 경험자

바 정보보호 금전 소비 비용 증감 여부

- 정보보호 관련 금전 소비 경험이 있는 일반 개인의 향후 비용 증가 여부에 대하여 '증가 예정이다'라는 응답이 32.7%, '감소 예정이다'라는 응답이 4.5%로 나타났으며, '비슷할 것이다'라는 응답은 62.8%로 조사되었다.

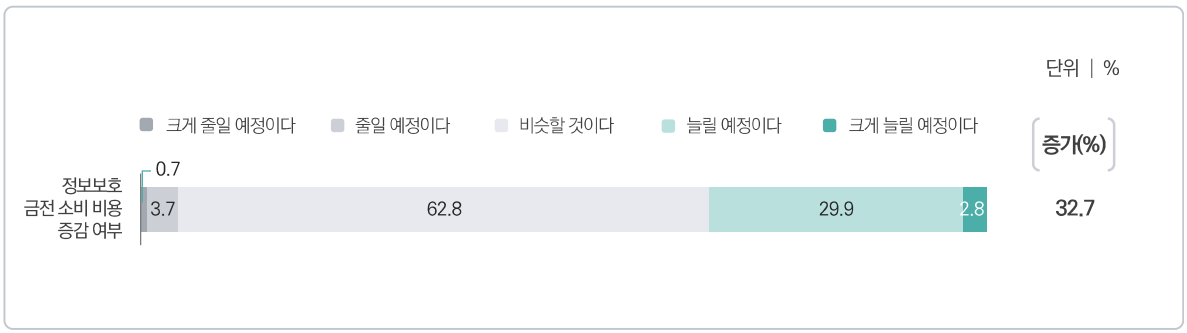


그림 2-3-29 정보보호 금전 소비 비용 증감 여부 – 정보보호 금전 소비 경험자

사 정보보호 비용 지출 의향

- 정보보호 금전 소비를 하지 않은 인터넷 이용자는 정보보호 비용 지출 의향에 대해 의향이 없다(그렇지 않다 + 전혀 그렇지 않다)는 응답이 30.2%로 의향이 있다(그렇다 + 매우 그렇다)는 응답(25.8%) 대비 높게 나타났다. (보통이다: 43.9%)

그림 2-3-30 정보보호 비용 지출 의향 – 정보보호 금전 소비 비경험자

V 일상생활 속의 정보보호

1 일상생활 속의 정보보호

가 무료 인터넷 연결 빈도

- 인터넷 이용자의 50.3%는 공공장소에서 제공되는 무료 인터넷에 자주 연결하여 사용한다(사용하는 편이다 + 항상 사용한다)고 응답했다.

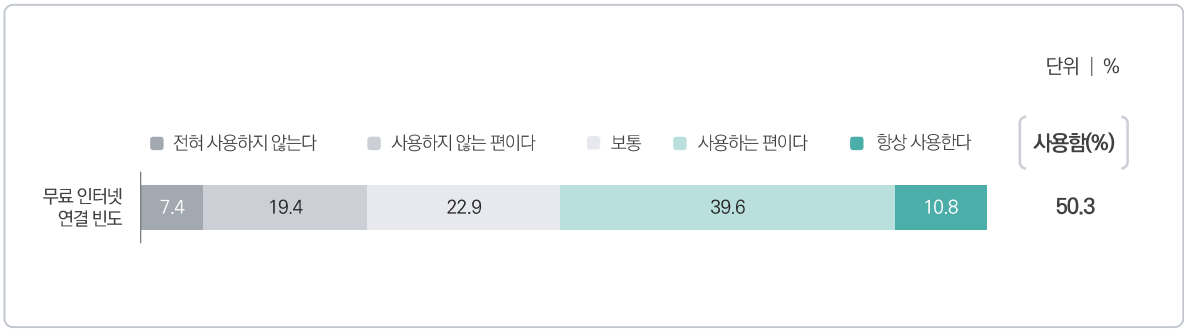


그림 2-3-31 무료 인터넷 연결 빈도

나 불특정 다수 이용 전자장비 이용 시 예방 활동

- 불특정 다수가 이용하는 전자장비 이용 시 정보보호 관련 예방 활동 여부에 대해 37.7%는 수행한다(대체로 수행하는 편이다 + 반드시 수행한다)고 응답했다.

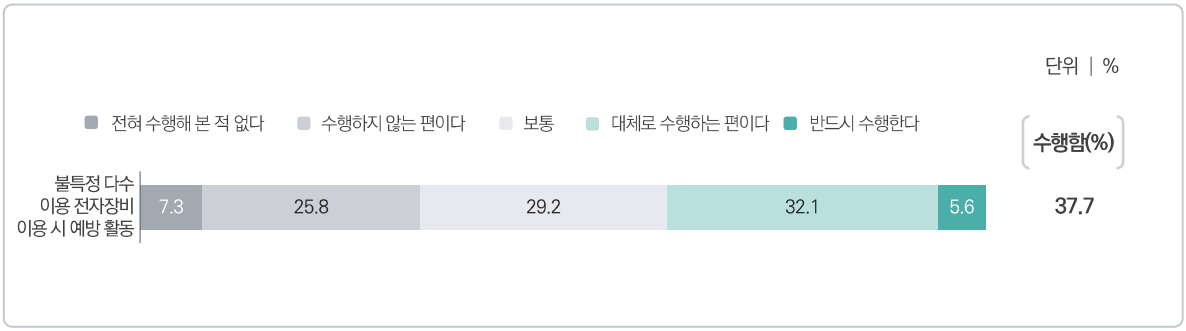


그림 2-3-32 불특정 다수 이용 전자장비 이용 시 예방 활동

다 안내 시 비밀번호 즉시 변경

- 인터넷 서비스 이용 시 비밀번호 변경 필요 안내 시 즉시 변경 여부에 대해 36.2%는 즉시 변경하는 것으로 나타났다.

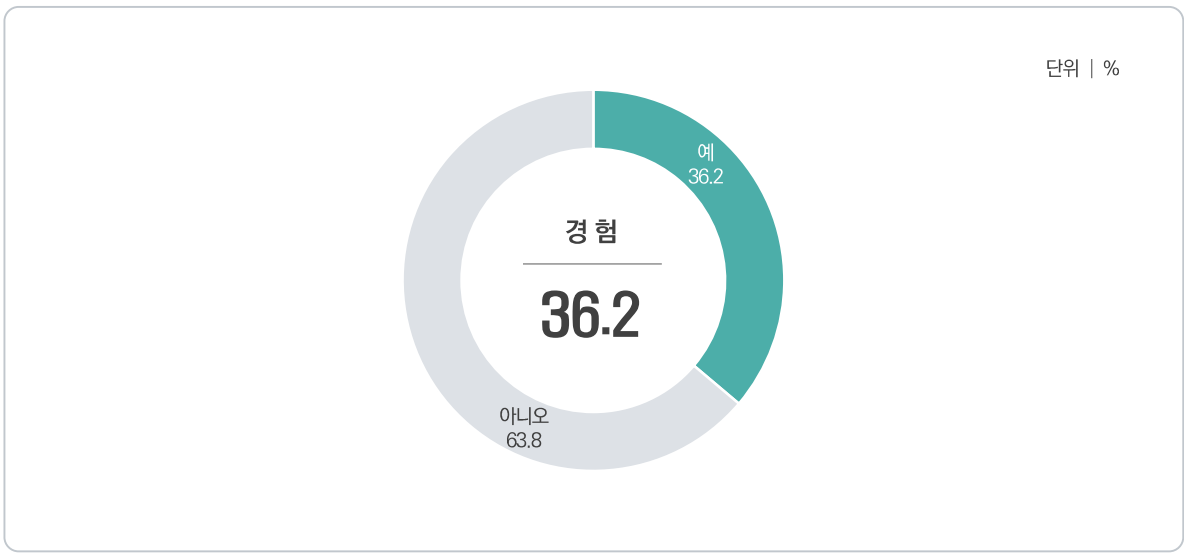


그림 2-3-33 안내 시 비밀번호 즉시 변경

라 디지털 데이터 백업

- 최근 1년간 PC, 스마트폰 등 개인 전자장비에 저장된 디지털 데이터 백업 여부에 대해 54.3%는 수행하는 것으로 조사되었다.

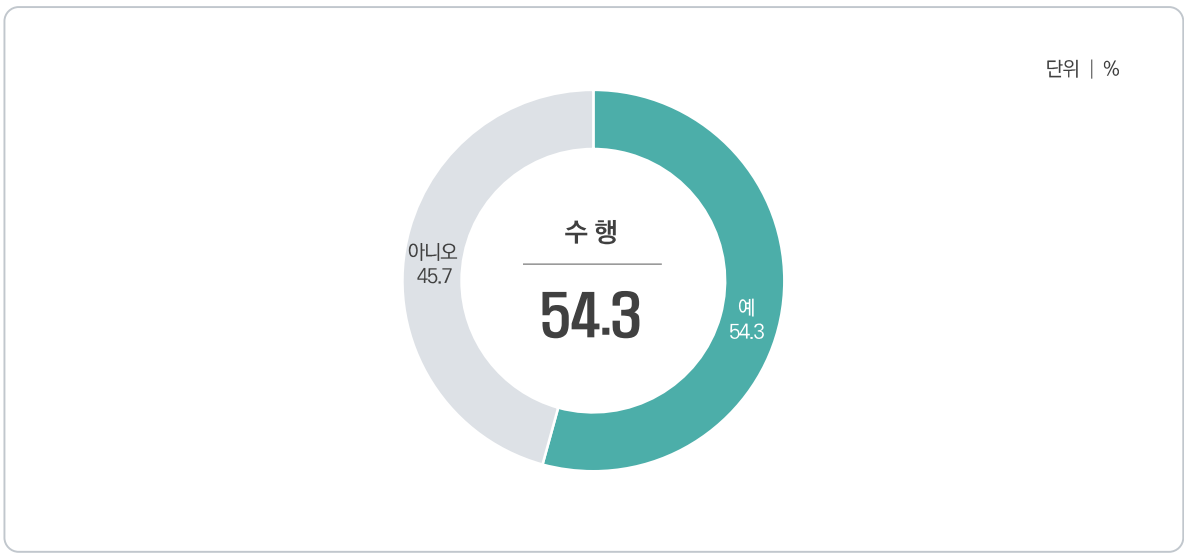


그림 2-3-34 디지털 데이터 백업

- 디지털 데이터 백업은 성별로는 '남성(57.7%)'이 '여성(50.7%)' 대비 높게 나타났다.
- 연령별로는 '20대(71.2%)'에서 가장 높게 조사되었다. 반면, '60대(31.4%)'는 타 연령대 대비 상대적으로 낮게 나타났다.

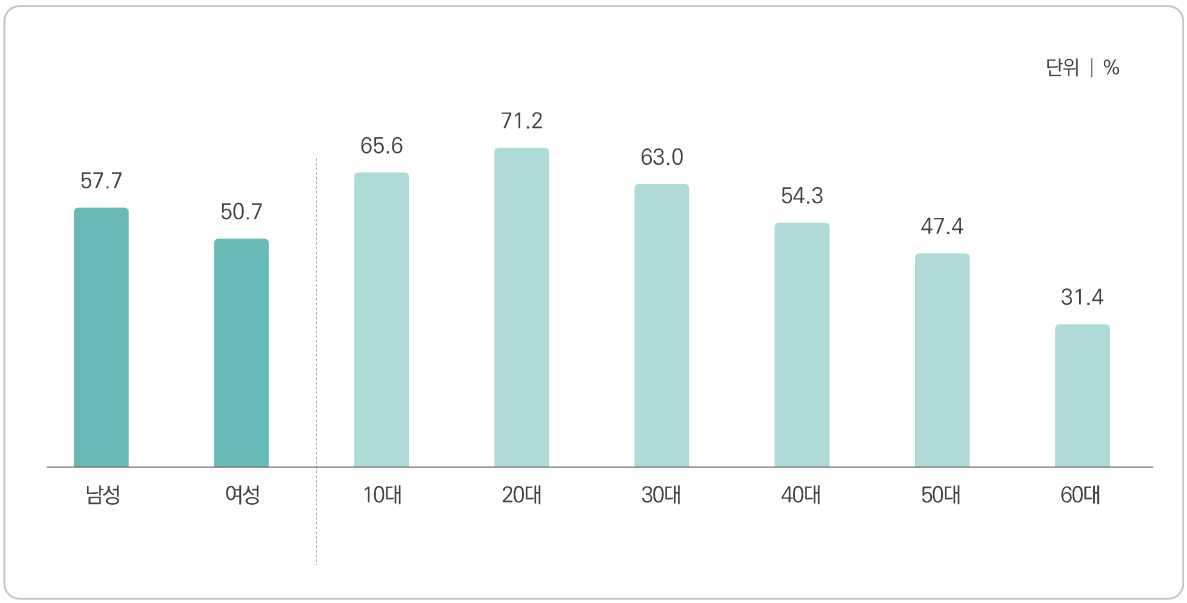


그림 2-3-35 성·연령별 디지털 데이터 백업

마 보안 점검 수행

- 최근 1년간 개인용 전자기기에 설치된 보안 프로그램을 활용한 보안 점검 수행 경험에 대해 51.2%는 '수행 경험이 있다'고 응답하였다.

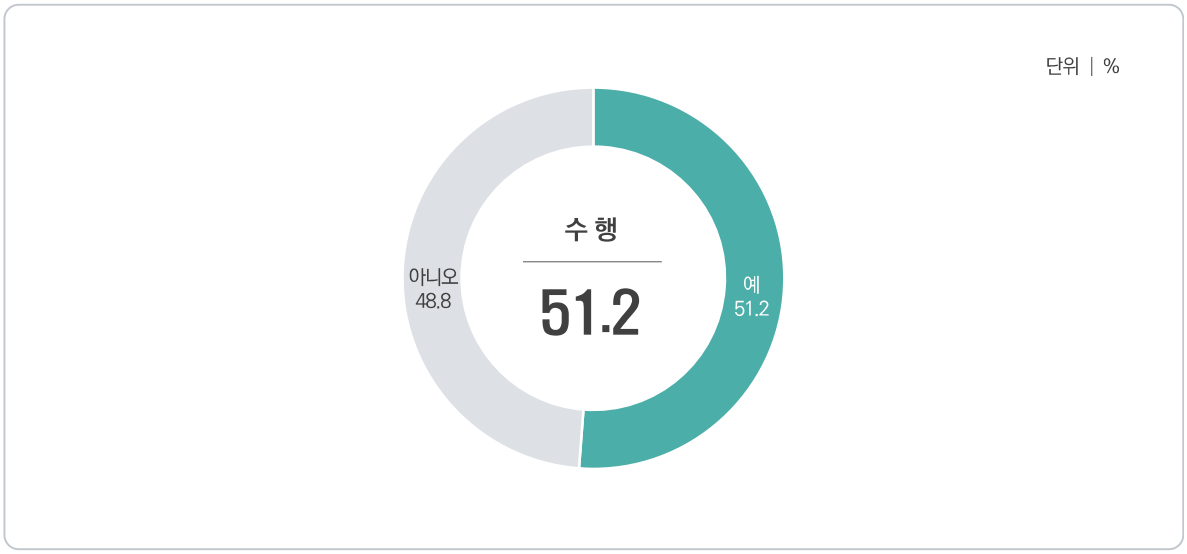


그림 2-3-36 보안 점검 수행

- 보안 점검 수행은 성별로는 '남성(56.2%)'이 '여성(46.0%)' 대비 높게 나타났다.
- 연령별로는 20대(63.7%)에서 가장 높게 조사되었다. 반면, 60대(32.2%)는 타 연령대 대비 상대적으로 낮게 나타났다.

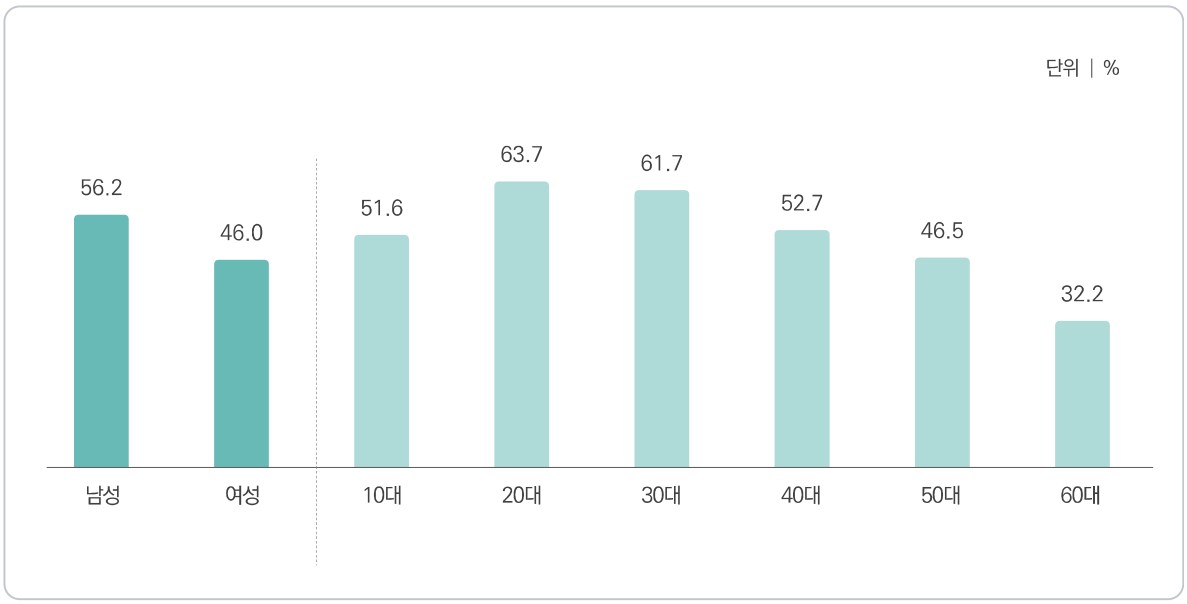


그림 2-3-37 성·연령별 보안 점검 수행

바 일상생활 공간 중 CCTV 활용

- 개인적인 일상생활 공간의 CCTV 활용 여부에 대해 14.8%가 활용되고 있는 것으로 나타났다.

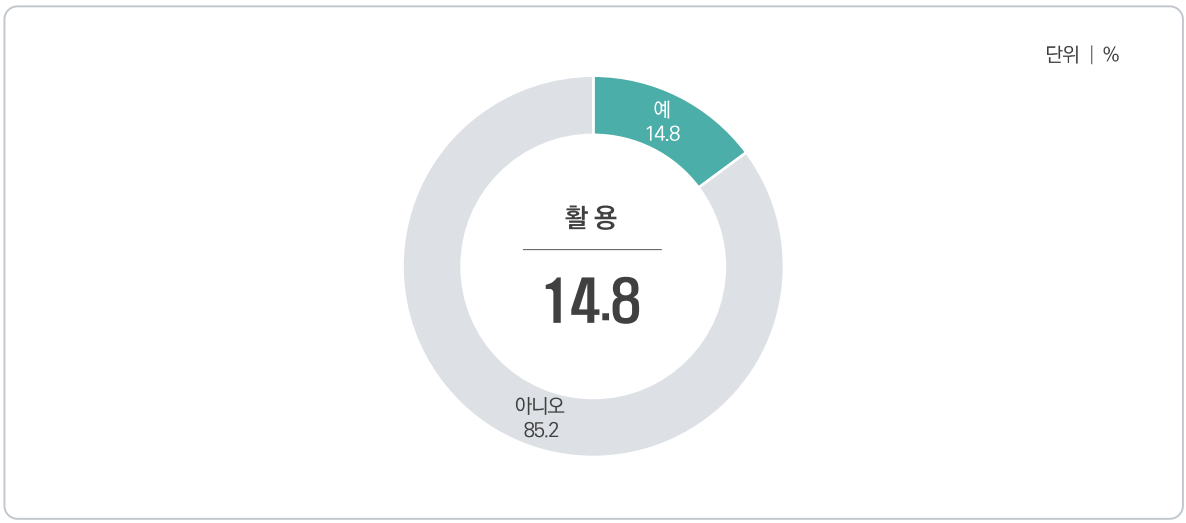


그림 2-3-38 일상생활 공간 중 CCTV 활용

사 보안 예방 조치

- 보안을 위한 예방 조치로는 '의심스러운 URL 링크 클릭하지 않음'이 72.5%로 가장 높고, 다음으로 '웹사이트의 파일을 함부로 다운로드하지 않음(61.6%)', '금융권 이용 시 정보가 노출되지 않도록 주의(46.0%)', '프로그램 설치 시 불필요한 프로그램이 추가적으로 설치되는지 확인(39.9%)' 등의 순으로 조사되었다.

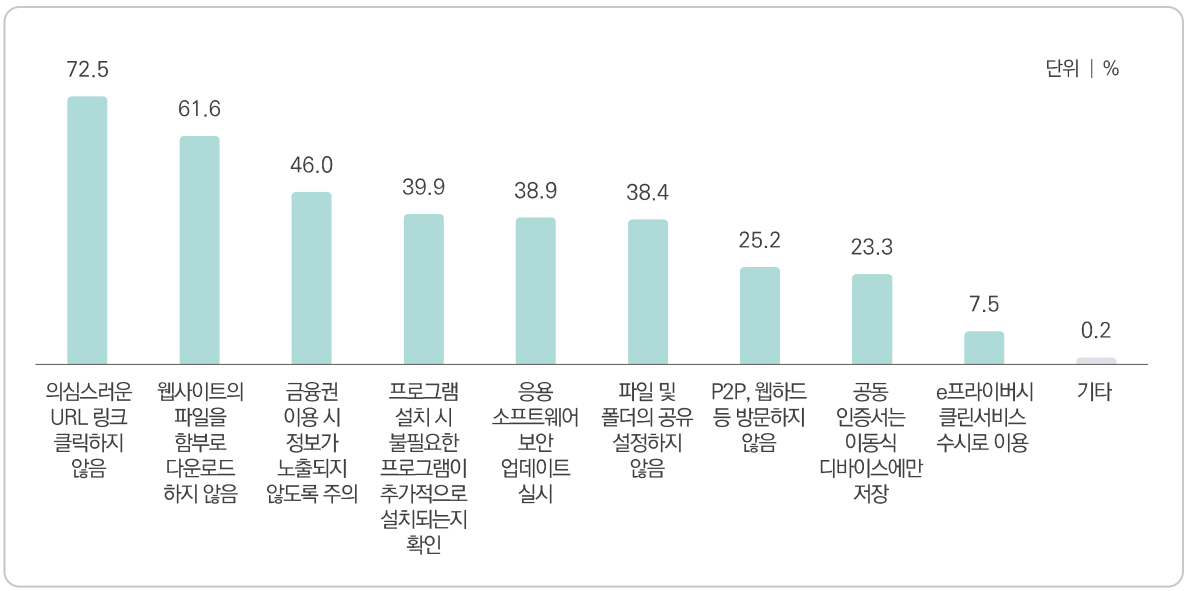


그림 2-3-39 보안 예방 조치(복수응답)

아 비대면 재택·교육 경험

- 비대면 재택근무·교육 경험 여부에 대해 24.1%가 경험이 있는 것으로 조사되었다.

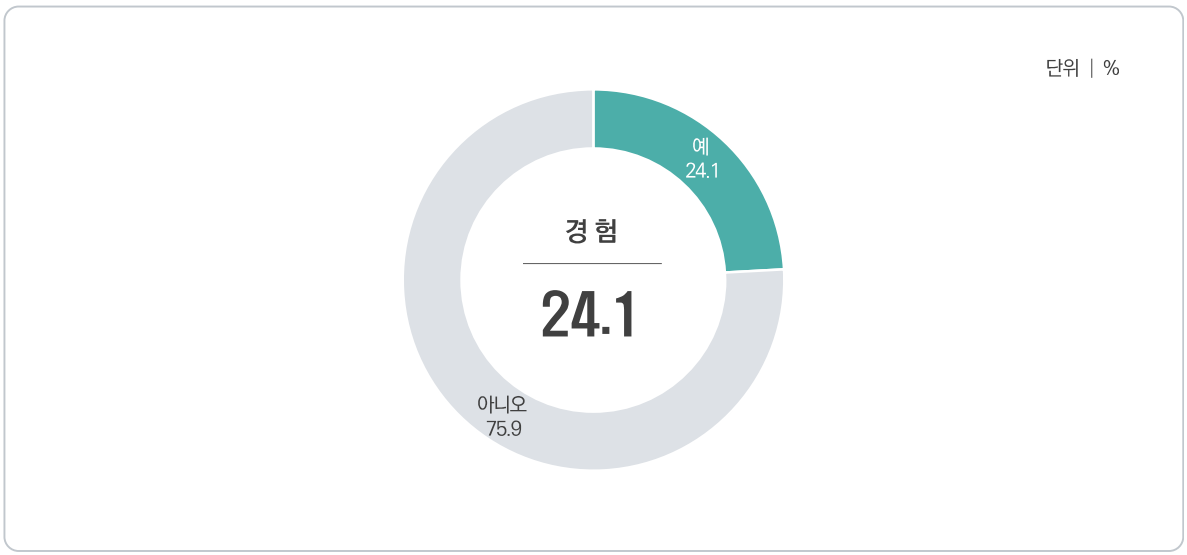


그림 2-3-40 비대면 재택·교육 경험

자 비대면 환경의 정보보호 활동

- 비대면 환경을 경험한 인터넷 이용자의 정보보호 활동으로는 '비대면 환경을 활용하고 있는 컴퓨터로 의심스러운 URL 클릭 등을 하지 않음'이 24.7%로 가장 높고, 다음으로 '학교, 회사 등에서 제공한 정보보호 제품을 사용(24.3%)', '재택근무, 화상회의 등 이용 시 관련 프로그램 이외의 프로그램을 사용하거나 작동하지 않음(23.4%)', '학교, 회사 등에서 제공하는 디바이스를 활용하여 비대면 환경 사용(20.0%)' 등의 순으로 조사되었다.

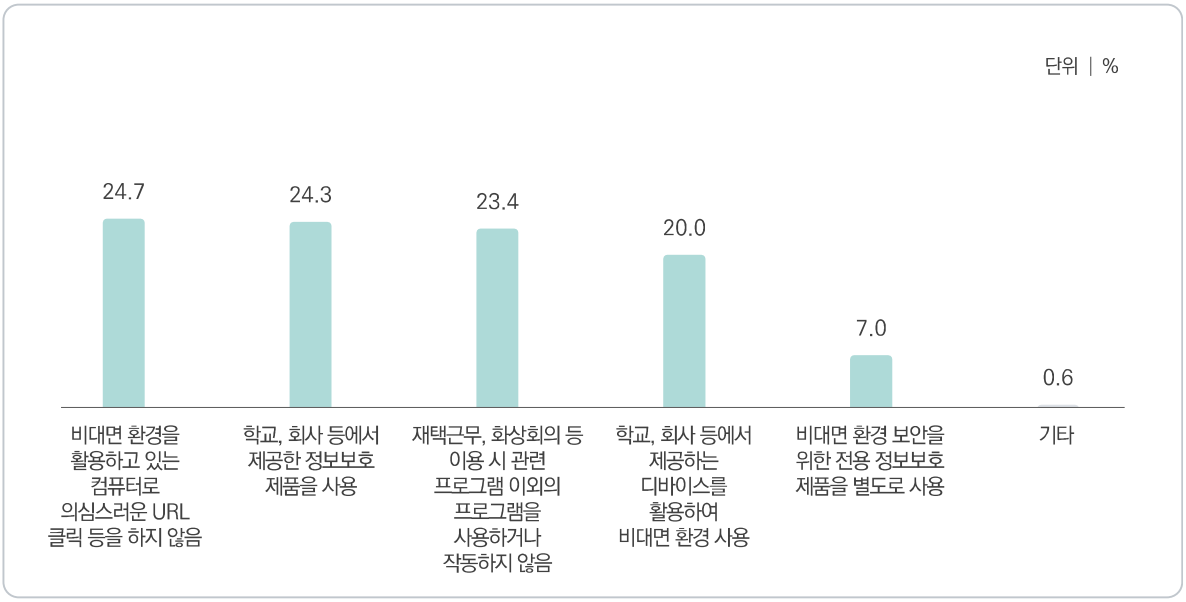


그림 2-3-41 비대면 환경의 정보보호 활동 - 비대면 재택·교육 경험자

Ⅵ 정보보호 침해사고 경험과 위협 인식

1 정보보호 침해사고 경험

가 침해사고 의심

- 최근 1년간 인터넷 이용자의 23.4%는 본인의 정보보호 침해사고를 의심한 적이 있는 것으로 조사되었다.

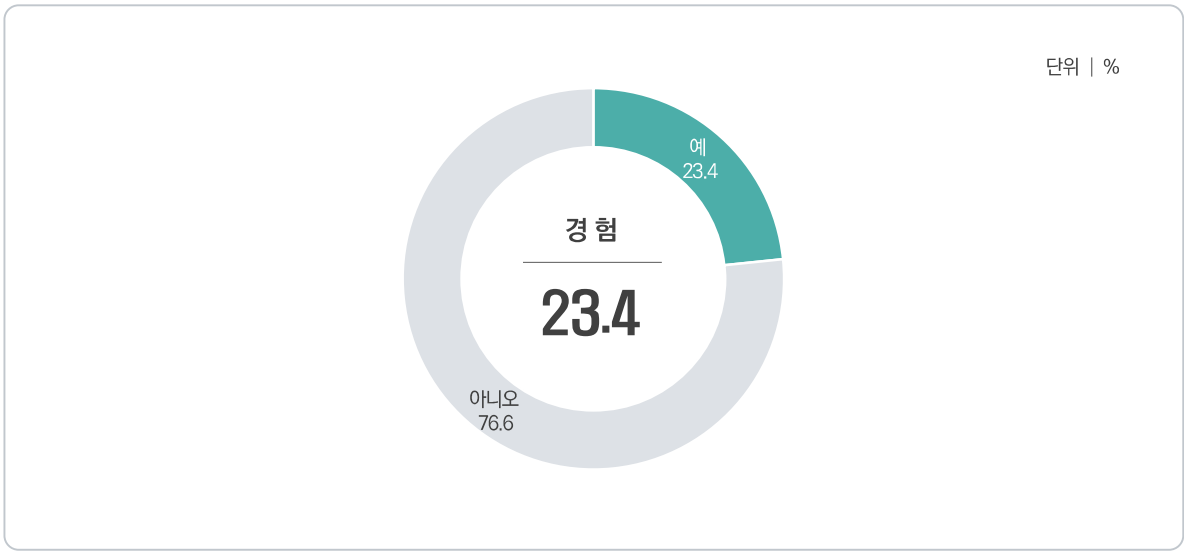


그림 2-3-42 침해사고 의심

나 침해사고 경험

- 최근 1년간 침해사고 경험률은 7.5%로 조사되었다.

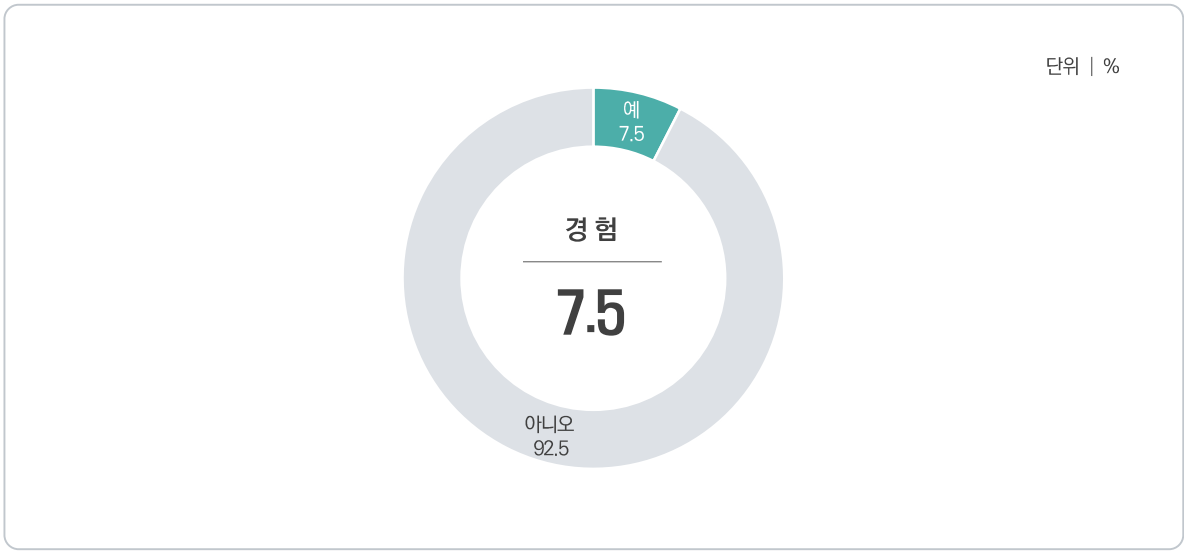


그림 2-3-43 침해사고 경험

다 침해사고 피해 인지 소요 시간

- 침해사고를 경험한 경우, 피해 사실을 인지하기까지 소요된 시간은 '1일 이내'가 22.9%로 가장 높고, 다음으로 '7일(일주일) 이내(22.3%)', '1시간 이내(19.4%)', '30분 이내(18.9%)' 등의 순으로 나타났다.

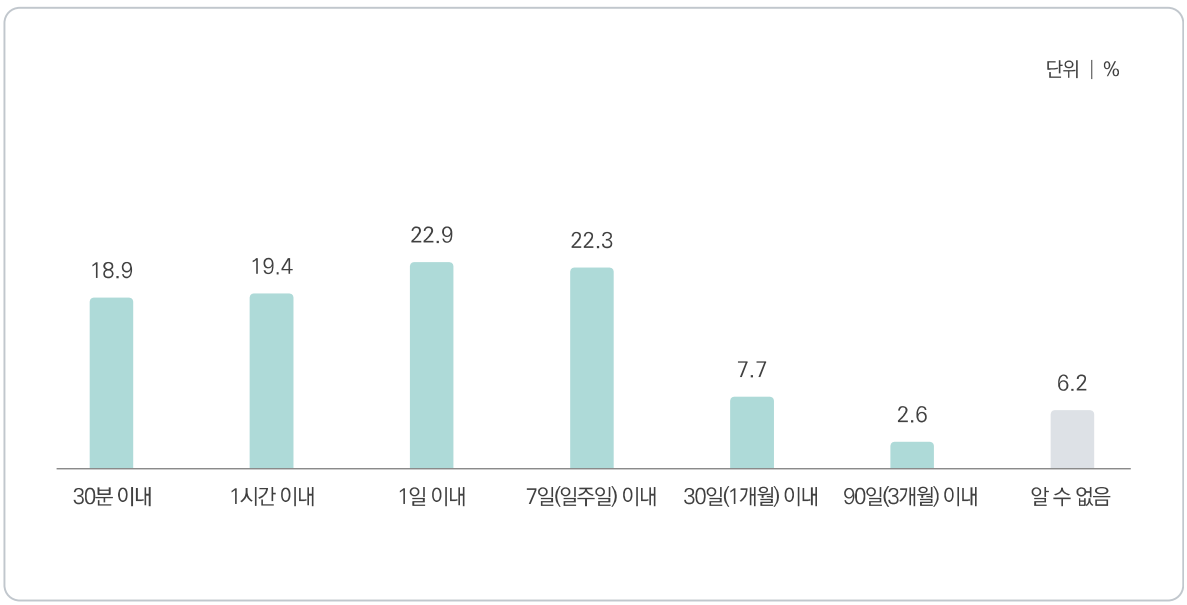


그림 2-3-44 침해사고 피해 인지 소요 시간 – 침해사고 경험자

라 침해사고 인지 경로

- 침해사고를 경험한 경우, 피해사실 인지 경로는 '보안 시스템의 침해사고 경보(알림)'이 29.8%로 가장 높고, 다음으로 '기존과는 다른 시스템 설정의 변경 또는 보유하고 있는 데이터의 위변조 사항 발견(21.2%)', '보안 시스템의 임의적 해제 또는 침입 흔적 발견(물리적 침입 포함)(18.7%)', '침해사고 해결 조건으로 대가 요구 및 협박 등을 경험(13.9%)' 등의 순으로 조사되었다.

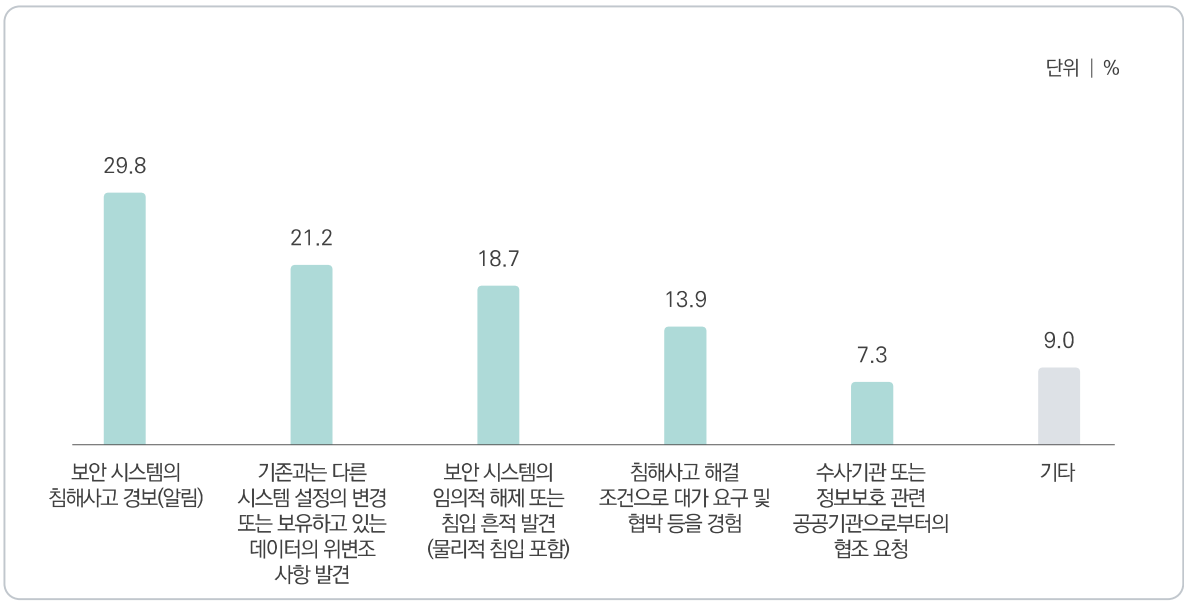


그림 2-3-45 침해사고 인지 경로 - 침해사고 경험자

마 침해사고 피해 심각도

- 침해사고를 직접적으로 경험한 경우 체감하는 피해 심각성 정도는 '심각'이 39.4%, '경미' 44.7%로 나타났고, 평균 -0.49점으로 다소 경미한 편으로 인식되었다.

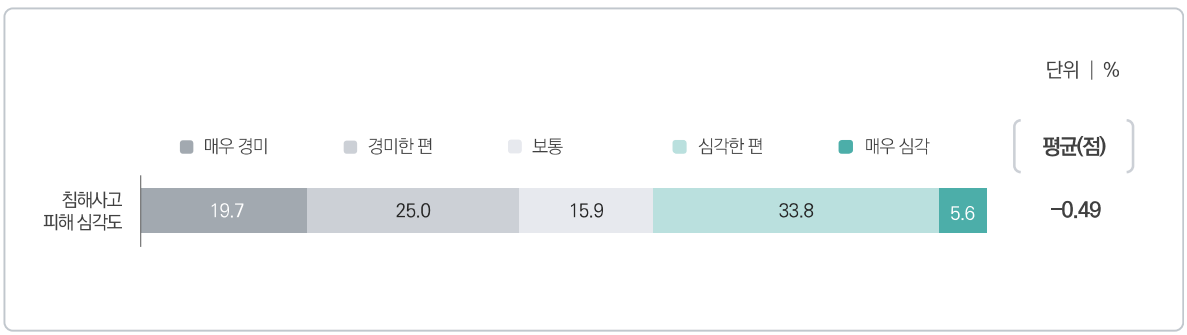


그림 2-3-46 침해사고 피해 심각도 - 침해사고 경험자

바 침해사고 경험 유형

- 경험한 침해사고의 유형으로는 'PC 또는 노트북 등 개인용 컴퓨터의 해킹과 같은 불법적 접근'이 36.8%로 가장 높고, 다음으로 '개인용 모바일 기기(스마트폰, 태블릿, 패드 등)의 해킹과 같은 불법적 접근(31.8%)', '랜섬웨어 또는 악성코드 감염 등에 의한 정상적인 전자장비 사용의 제한(27.9%)', '피싱, 파밍, 스미싱 등에 의한 금전적 피해(20.8%)' 등의 순으로 조사되었다.

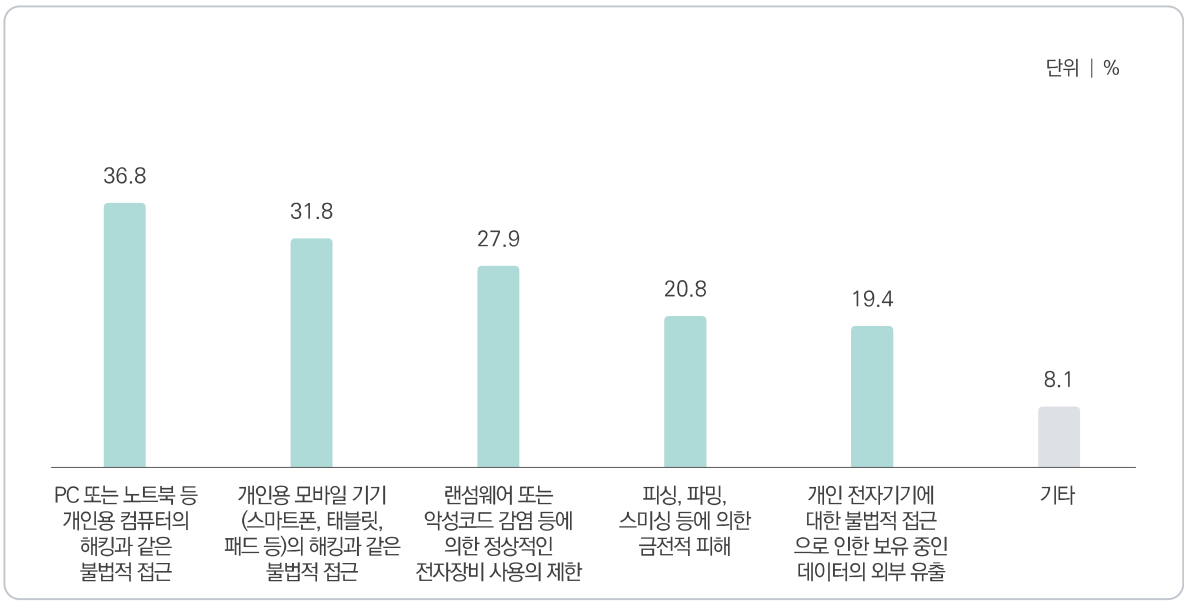


그림 2-3-47 침해사고 경험 유형(복수응답) - 침해사고 경험자

사 침해사고 관심도 변화

- 침해사고를 경험한 인터넷 이용자의 83.8%가 정보보호 침해사고에 대한 관심도는 침해사고 이전 대비 관심이 커졌다(관심이 커졌다 + 관심이 매우 커졌다)고 응답했다.

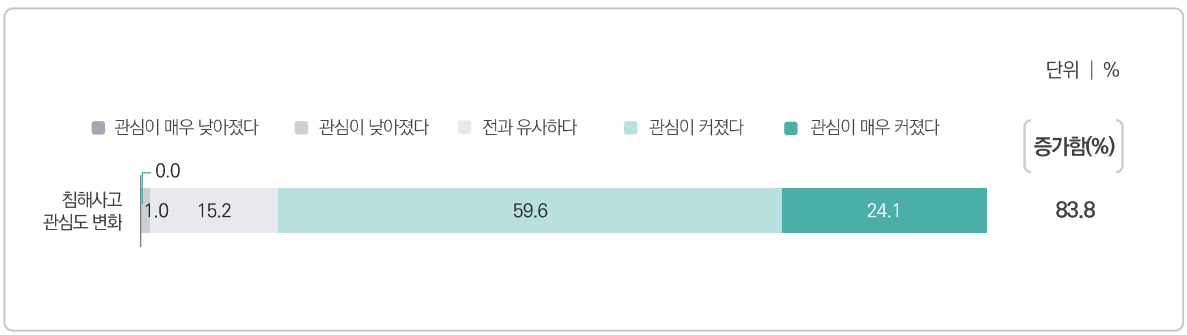


그림 2-3-48 침해사고 관심도 변화 - 침해사고 경험자

아 침해사고 신고

- 침해사고 경험자의 38.6%는 침해사고가 발생한 것을 인지했을 당시, 관련 기관에 피해 사실을 신고한 것으로 조사되었다.

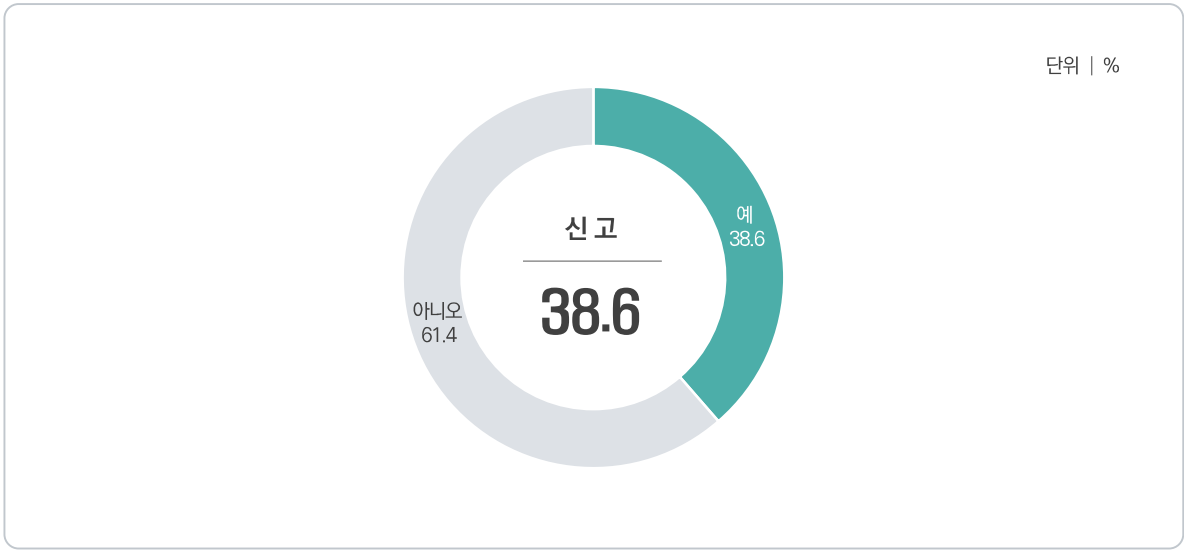


그림 2-3-49 침해사고 신고 - 침해사고 경험자

자 침해사고 미신고 이유

- 침해사고가 발생했을 당시 관련 기관에 피해 사실을 신고하지 않았던 이유로는 '피해가 심각하지 않았기 때문에'가 59.2%로 가장 높고, 다음으로 '신고에 따른 사건 조사, 처리가 복잡하고 불편하다고 느껴졌기 때문에(34.3%)', '신고하더라도 범인을 체포하거나 처벌할 수 없다고 생각하기 때문에(31.1%)', '신고하더라도 피해가 복구되지 못한다고 생각하기 때문에(24.3%)' 등의 순으로 응답했다.

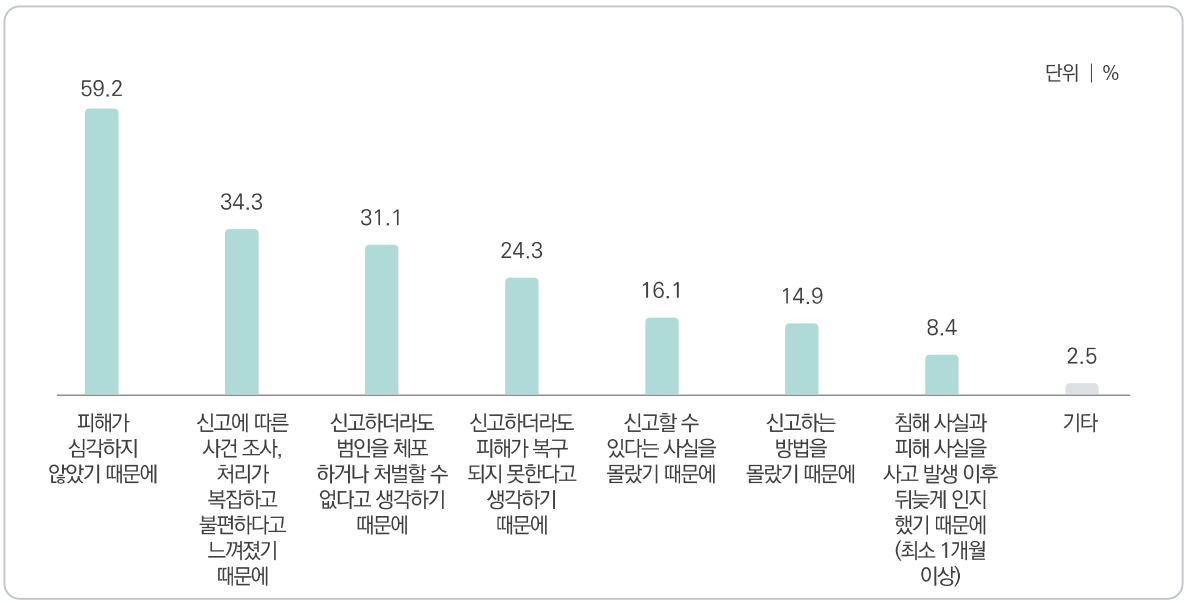


그림 2-3-50 **침해사고 미신고 이유(복수응답) - 침해사고 미신고자**

2 정보보호 침해사고 위협 인식

가 최신 기술 이용 정보보호 위험성

- 최신 기술 이용 관련 정보보호에 대한 위험성에 대해 '자율 주행 차량'이 -0.02점으로 가장 위험에 취약하다고 인식하고 있으며, 다음으로 '빅데이터 분석을 통한 고객 마케팅(0.03점)', '홈 IoT 장비 등을 활용한 스마트 주거 환경'(0.06점) 등의 순으로 조사되었다.

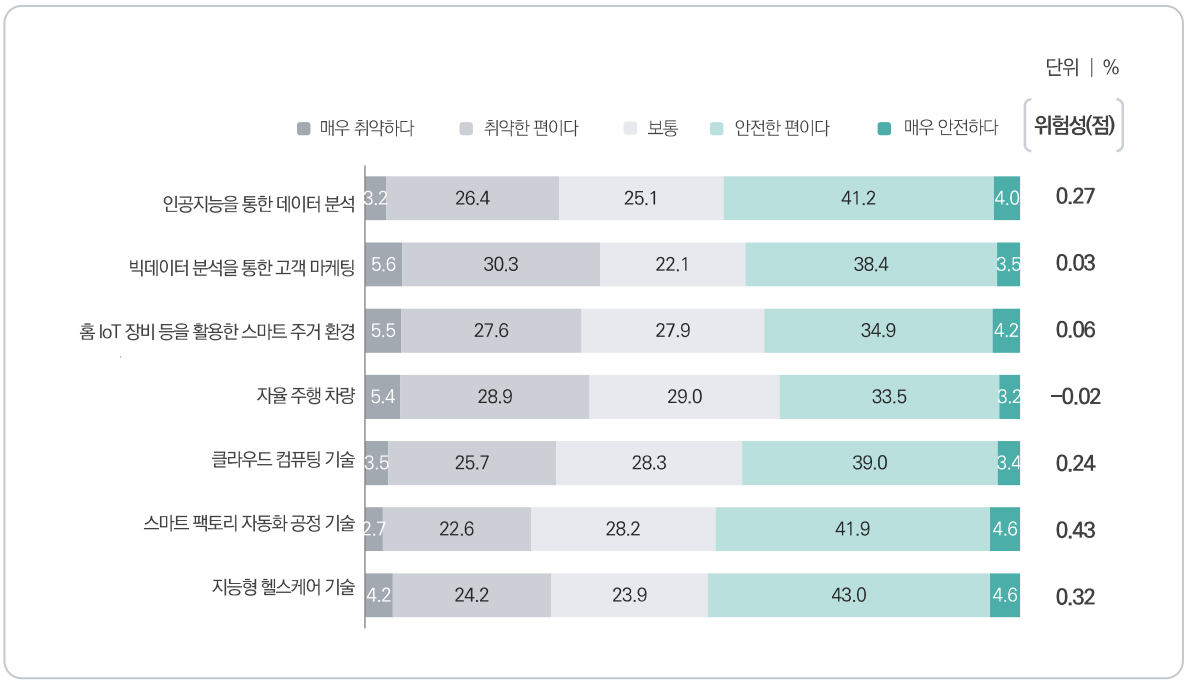


그림 2-3-51 최신 기술 이용 정보보호 위험성(요약)

나 최신 기술 침해사고 파급효과

- 최신 기술 관련 정보보호 침해사고 발생 시 피해의 파급효과에 대해 '자율 주행 차량(-1.17점)'이 가장 심각한 것으로 인식하고 있으며, 다음으로 '홈 IoT 장비 등을 활용한 스마트 주거 환경(-1.07점)', '지능형 헬스케어 기술(-1.04점)' 등의 순으로 조사되었다.

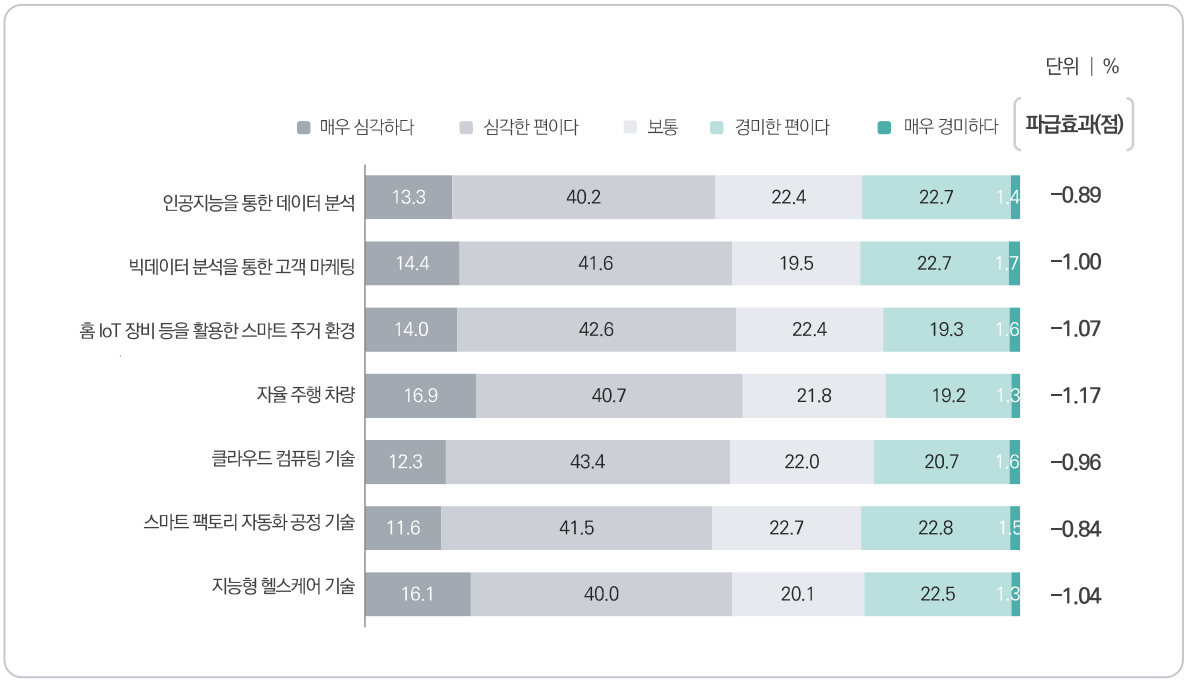
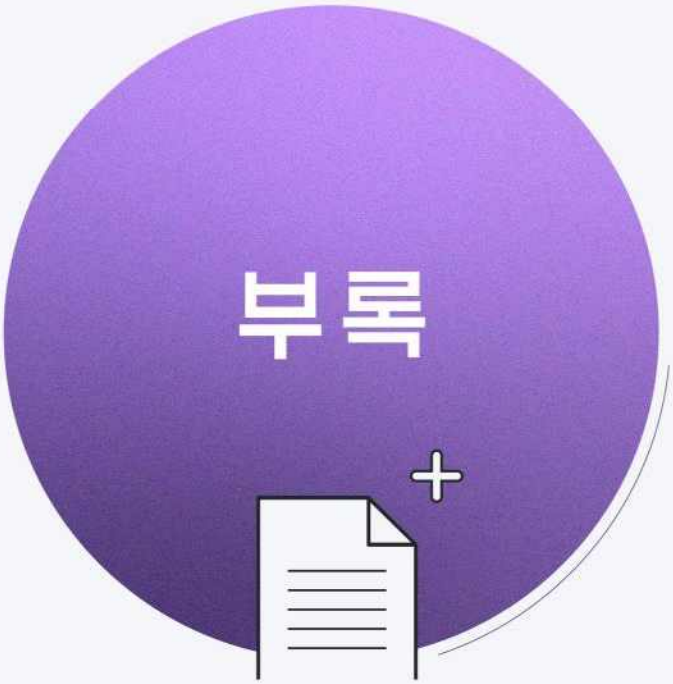


그림 2-3-52 최신 기술 침해사고 파급효과(요약)

부록



부록1

주요 변경내역

1

1 기업 부문

분 야	항 목	세 부 항 목	조 사 시 기
Ⅰ. 정보보호 기반 및 환경	A. 정보보호 인식	정보보호 중요성 인식	'19-'22
		개인정보보호 중요성 인식	'19-'21
		경영진의 정보보호 중요성 인식	'10-'17, '22
		경영진의 개인정보보호 중요성 인식	'14
		일반직원들의 정보보호 중요성 인식	'10-'17
		일반직원들의 개인정보보호 중요성 인식	'10-'17
		일반직원의 정보보호 관련 지식수준	'14
		정보보호 위협요인	'13-'22
		사이버 환경상의 안전성 정도	'07-'10
		우려하는 개인정보 유출요인	'12-'20
		정보보호 애로사항	'15-'22
		정보보호 규제 동의 수준	'15-'16
		보안 규정 변경 시 수용 노력 정도	'21
		정보보호 관련 규정 변경 시 엄격함 정도	'22
	B. 정보보호 정책 및 조직	정보보호(개인정보보호) 정책 수립	'06-'22
		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(개인정보보호) 조직 운영*	'06-'13, '15-'22
		정보보호 관련 책임자 임명 및 전담	'06-'22
		정보관리책임자(CIO)와 겸직 여부	'16
		정보보호 조직 및 담당 인력 현황과 향후 계획	'14
		정보보호 관련 인력 현황	'22
		IT인력 중 정보보호 담당 인력 비중	'14, '16-'21
		IT인력 대비 정보보호 전담인력 투입 비율	'10
		정보보호 담당 인력 신규 채용계획	'17-'21
	C. 정보보호 교육	정보보호 교육의 필요성	'07-'09
		정보보호(개인정보보호) 교육 실시**	'06-'22
		교육 대상별 교육 실시 현황	'06-'22
		정보보호(개인정보보호) 교육 방법	'21-'22
		정보보호 교육 프로그램별 교육 횟수, 교육시간	'07-'14
		정보보호 교육프로그램별 교육 시간, 교육평가 여부	'16
		정보보호 교육에 대한 직원들의 이해 정도	'10

*, ** 개인정보보호는 2022년에는 제외

분 야	항 목	세 부 항 목	조 사 시 기
Ⅰ. 정보보호 기반 및 환경	C. 정보보호 교육	필요한 정보보호 교육 내용	'15
		실시된 정보보호 교육의 포함 내용	'16
		정보보호 교육 자료 출처	'22
		정보보호 교육 효과	'22
		정보보호 교육 만족도	'22
	D. 정보보호 예산	정보보호 예산 사용 경험	'22
		IT예산 중 정보보호 관련 예산 비중	'06-'21
		정보보호 예산 총액	'22
		정보보호 예산 총액 중 분야별 비율	'14
		정보보호 관련 예산 증감	'11-'22
		정보보호 관련 예산 전년대비 증감 이유	'19-'22
		정보보호 예산 총액 변화	'22
		정보보호 지출 분야	'13-'22
		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
		정보보호 지출금액 증감 정도	'14
		정보보호 관련 예산 편성하지 않은 이유	'06-'16
		정보보호 예산 미사용 이유	'22
		정보보호 관련 지출 정도	'07-'13
		정보보호 예산 소비 적절성	'22
		정보보호 예산 소비 부적절 이유	'22
		정보보호 관련 투자 증감	'10-'13
		정보보호 관련 지출이 없는 이유	'07-'13
		예산 항목별 정보보호 지출 비율	'09
		국내외 정보보호 제품 및 서비스 선호도	'22
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 이용	'06-'22
		활용 제품의 정보보호 인증 인지 여부	'22
		CCTV/IP카메라 보유 대수	'16-'20
		CCTV 보유 대수 및 관리 현황	'22

분 야	항 목	세 부 항 목	조 사 시 기
Ⅱ. 침해사고 예방	A. 정보보호 제품 및 서비스	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
		정보보호 서비스 이용	'06-'22
		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	'13
	B. 정보보호 관리	정보자산 관리를 위한 수행활동	'14
		시스템 및 네트워크 보안 점검(취약점 점검) 실시	'09-'22
		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 차등권한 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
		시스템 로그 및 방화벽 로그 기록 저장 주기	'22
		데이터 종류별 백업 실시 여부	'22
		데이터 백업 방식	'22
		데이터 백업 주기	'22
		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	'12-'21
		침해사고 사전 예방 능력	'22
Ⅲ. 침해사고 경험 및 대응	A. 침해사고 경험	침해사고 발생 가능성	'22
		침해사고 피해 직·간접적 경험	'22
		침해사고 의심 경험	'22
		침해사고 피해 경험	'06-'22
		침해사고 경험 유형	'22

분 야	항 목	세 부 항 목	조 사 시 기
Ⅲ. 침해사고 경험 및 대응	A. 침해사고 경험	침해사고 피해 유형별 피해 빈도	'07-'14
		침해사고 피해 심각성 정도	'22
		침해사고 피해 경험 유형 및 심각성 정도	'14-'21
		침해사고 피해 발생 경로	'13-'14
		침해사고 피해 사실 인지 경로	'22
		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
		침해사고 시 관계기관에 문의 또는 신고	'06-'22
		정보보안 침해사고 발생 시 신고정도	'11
		정보보안 침해사고 발생 시 신고하지 않는 이유	'06-'11, '14-'16, '22
		인터넷 침해사고 피해 경로	'07-'10
		정보보호 피해건수 증감률	'10-'13
		정보보호 피해규모 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 피해양상 유형	'10
	B. 침해사고 대응	침해사고 대응활동 수행	'06-'22
		침해사고 사후 대응 능력 수준	'22
		정보보호 침해사고 경험 후 관심 변화	'22
		현재 수행중인 정보보호 활동 평가수단	'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 수립여부	'07-'10
		이메일 중 스팸이 차지하는 비율	'07
		메일서버 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

분 야	항 목	세 부 항 목	조 사 시 기
Ⅲ. 침해사고 경험 및 대응	B. 침해사고 대응	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 본인확인수단	'14
		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 수립여부	'09
		내부관리계획 항목별 포함 여부	'09
		개인정보보호책임자의 직급 및 직책	'09
		임직원 대상 보안서약서 서명 여부	'09

분 야	항 목	세 부 항 목	조 사 시 기
Ⅳ. 개인정보 보호	B. 개인정보 침해사고 예방	개인정보보호책임자/취급자 대상 교육계획 수립여부	'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 수립이행여부	'09
		개인정보취급자 비밀번호 작성규칙 내용	'09
		개인정보취급자 개인용 컴퓨터 P2P 사용규제여부	'09
		개인정보취급자의 개인용 컴퓨터 공유설정여부	'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 출력항목 최소화 여부	'09
		개인정보 포함 정보 출력/복사지 CPO 사전승인 여부	'08-'09
		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 평균소요시간	'14
		개인정보 침해사고 문제해결 및 서비스복원 평균소요시간	'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

분 야	항 목	세 부 항 목	조 사 시 기
Ⅳ. 개인정보 보호	C. 개인정보 침해사고	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
		개인정보 관리책임자/취급자 변경이 접근권한 변경/말소 여부	'09
		접근권한 부여/변경/말소 내역 기록/보관 여부	'09
		개인정보처리시스템 외부망 접속가능 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

분 야	항 목	세 부 항 목	조 사 시 기
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 관리정책 수립 현황	'11-'13
	B. 모바일	모바일 오피스 구축·운영 현황	'10-'13
		모바일 오피스 도입 보안대책 수립 현황	'10-'14
		모바일 오피스 보안수칙 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 대응방안	'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 보안위협에 대한 우려	'15-'21
	E. 정보보호(사이버) 보험***	사이버(정보보호, 개인정보보호) 보험 인지	'17-'22
		사이버(정보보호, 개인정보보호) 보험 이용 및 향후 가입(유지) 계획	'17-'22
		사이버(정보보호, 개인정보보호) 보험 희망 보장 항목	'17-'22

*** 개인정보보호는 2022년에는 제외

분 야	항 목	세 부 항 목	조 사 시 기
Ⅴ. 주요 서비스별 정보보호	F. 재택근무	코로나19로 인한 재택근무 시행 여부	'21-'22
		재택근무 시 제공한 보안 솔루션	'21-'22
		재택근무 시 정보보호 위험성 인지	'22
		재택근무 시 침해사고 발생 또는 의심 경험	'22
		코로나19 위기 해소 이후 재택근무 활용 계획 여부	'21

2 개인 부문

분 야	항 목	세 부 항 목	조 사 시 기
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
		정보보호 침해 우려 정도	'22
		정보보호 침해사고 소식에 대한 관련성 인식	'22
		안전 체감도	'22
		침해사고 발생 시 피해 복구 가능성	'22
		침해사고 발생 원인	'22
		침해사고 방지 주체	'22
		기관·업체 신뢰도	'22
	B. 정보보호 교육	정보보호 교육	'22
		정보보호 교육 방식	'22
		정보보호 교육 주제	'22
		정보보호 교육 학습 효과	'22
		정보보호 교육 학습 난이도	'22
		정보보호 학습 어려움	'22
	C. 정보보호 예산	정보보호 금전 소비 경험	'22
		정보보호 금전 소비 유형	'22
		정보보호 금전 소비 규모	'22
		정보보호 금전 소비 계기	'22
		정보보호 금전 소비 적절성	'22
		정보보호 금전 소비 비용 증감 여부	'22
		정보보호 비용 지출 의향	'22

분 야	항 목	세 부 항 목	조 사 시 기
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. 침해사고 경험	침해사고 의심 경험	'22
		침해사고 경험	'22
		침해사고 피해 인지 소요 시간	'22
		침해사고 인지 경로	'22
		침해사고 피해 심각도	'22
		침해사고 피해 경험 유형	'11-'22
		피싱/파밍/스미싱 등 전자금융사기 피해 경로	'10-'21

분 야	항 목	세 부 항 목	조 사 시 기
Ⅲ. 침해사고 대응	B. 침해사고 대응조치	침해사고 대응활동 수행	'12-'21
		침해사고 신고 또는 상담 문의 기관·업체*	'07-'22
		침해사고 신고 또는 상담하지 않은 이유	'07-'22
		침해사고 발생 초동대처 주체	'15
		정보보호 규제 방식에 대한 동의 정도	'15
	C. 정보보호 침해사고 경험과 위협 인식	침해사고 관심도 변화	'22
		최신 기술 이용 관련 정보보호 위험성	'22
		최신 기술 관련 침해사고의 파급효과	'22
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. IP카메라	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
	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

* 2022년도에는 신고 여부만 질의

분 야	항 목	세 부 항 목	조 사 시 기
Ⅴ. 주요 서비스별 정보보호	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	'15-'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
		불특정 다수 이용 전자장비 이용 시 예방 활동	'22
		비밀번호 변경 필요 안내 시 비밀번호 즉시 변경 여부	'22
		디지털 데이터 백업 경험	'22
		보안 점검 수행 경험	'22
		일상생활 공간 중 CCTV 활용	'22
		보안 예방 조치	'22
		비대면 재택근무 경험	'22
		비대면 환경의 정보보호 활동	'22
	B. 향후 지출 계획	향후 정보보호 지출 계획 분야	'19-'21

부록 2 표본오차

2

1 기업 부문

1 정보보호 정책 수립

		정보보호 정책 수립률	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		35.3	1.14	1.65	34.1	36.4
업종별	1. 농림수산업·광업	49.7	10.18	10.44	39.6	59.9
	2. 제조업	25.9	2.95	5.81	22.9	28.8
	3. 전기·수도업	34.3	6.93	10.30	27.4	41.2
	4. 건설업	21.9	3.22	7.50	18.7	25.1
	5. 도·소매업	26.7	3.63	6.93	23.1	30.4
	6. 운수 및 창고업	28.5	3.91	6.99	24.6	32.4
	7. 숙박 및 음식점업	25.5	5.67	11.34	19.9	31.2
	8. 정보통신업	72.0	4.03	2.86	68.0	76.0
	9. 금융 및 보험업	77.4	3.79	2.50	73.6	81.2
	10. 부동산업	22.9	4.26	9.50	18.6	27.1
	11. 기술서비스업	65.3	3.47	2.71	61.8	68.8
	12. 사설관리/사업 지원 서비스업	45.0	3.60	4.08	41.4	48.6
	13. 교육 서비스업	41.6	6.68	8.18	34.9	48.3
	14. 보건·사회복지업	47.3	4.95	5.34	42.3	52.2
	15. 예술·여가 서비스업	47.4	6.93	7.45	40.5	54.4
	16. 수리·기타 서비스업	35.5	7.15	10.28	28.3	42.6
규모별	10 ~ 49명	30.6	1.91	3.19	28.7	32.5
	50 ~ 249명	57.5	2.03	1.80	55.5	59.6
	250명 이상	85.6	1.08	0.64	84.5	86.6

2 정보관리책임자(CIO) 임명

		정보관리책임자 (CIO) 임명	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		28.9	1.09	1.92	27.8	30.0
업종별	1. 농림수산업·광업	47.3	10.16	10.95	37.2	57.5
	2. 제조업	25.2	2.92	5.91	22.3	28.1
	3. 전기·수도업	37.6	7.07	9.58	30.6	44.7
	4. 건설업	18.0	2.99	8.47	15.0	21.0
	5. 도·소매업	20.8	3.33	8.16	17.5	24.2
	6. 운수 및 창고업	34.3	4.11	6.11	30.2	38.4
	7. 숙박 및 음식점업	21.6	5.35	12.65	16.2	26.9
	8. 정보통신업	42.9	4.44	5.28	38.4	47.3
	9. 금융 및 보험업	70.6	4.13	2.99	66.4	74.7
	10. 부동산업	25.2	4.41	8.92	20.8	29.6
	11. 기술서비스업	50.1	3.64	3.71	46.5	53.8
	12. 시설관리/사업 지원 서비스업	29.3	3.29	5.73	26.1	32.6
	13. 교육 서비스업	34.1	6.42	9.60	27.7	40.6
	14. 보건·사회복지업	32.9	4.66	7.23	28.2	37.5
	15. 예술·여가 서비스업	44.0	6.89	7.99	37.1	50.8
	16. 수리·기타 서비스업	25.6	6.52	13.02	19.0	32.1
규모별	10 ~ 49명	24.5	1.79	3.71	22.8	26.3
	50 ~ 249명	50.5	2.05	2.07	48.5	52.6
	250명 이상	71.6	1.38	0.99	70.2	72.9

3 정보보호최고책임자(CISO) 임명

		정보보호최고책임자(CISO) 임명	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		19.2	0.94	2.51	18.3	20.2
업종별	1. 농림수산업·광업	34.2	9.66	14.41	24.5	43.8
	2. 제조업	17.6	2.56	7.43	15.0	20.1
	3. 전기·수도업	19.2	5.74	15.29	13.4	24.9
	4. 건설업	8.1	2.12	13.42	5.9	10.2
	5. 도·소매업	17.3	3.10	9.14	14.2	20.4
	6. 운수 및 창고업	16.2	3.18	10.06	13.0	19.3
	7. 숙박 및 음식점업	18.1	5.01	14.11	13.1	23.1
	8. 정보통신업	24.5	3.86	8.03	20.7	28.4
	9. 금융 및 보험업	48.6	4.53	4.76	44.0	53.1
	10. 부동산업	19.5	4.02	10.51	15.5	23.5
	11. 기술서비스업	32.0	3.40	5.42	28.6	35.4
	12. 시설관리/사업 지원 서비스업	26.9	3.21	6.09	23.7	30.1
	13. 교육 서비스업	22.8	5.68	12.70	17.1	28.5
	14. 보건·사회복지업	20.0	3.97	10.11	16.0	24.0
	15. 예술·여가 서비스업	24.7	5.98	12.37	18.7	30.7
	16. 수리·기타 서비스업	15.9	5.47	17.52	10.5	21.4
규모별	10 ~ 49명	15.8	1.51	4.88	14.3	17.3
	50 ~ 249명	32.4	1.92	3.02	30.5	34.3
	250명 이상	70.5	1.40	1.01	69.1	71.9

4 침해사고 예방 제품 및 솔루션 사용

		침해사고 예방 제품 및 솔루션 사용	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		80.7	0.94	0.60	79.8	81.7
업종별	1. 농림수산업·광업	92.8	5.26	2.89	87.6	98.1
	2. 제조업	72.4	3.01	2.12	69.4	75.4
	3. 전기·수도업	92.3	3.89	2.15	88.4	96.2
	4. 건설업	81.4	3.03	1.90	78.4	84.4
	5. 도·소매업	79.1	3.34	2.15	75.7	82.4
	6. 운수 및 창고업	95.3	1.83	0.98	93.5	97.1
	7. 숙박 및 음식점업	97.3	2.12	1.11	95.1	99.4
	8. 정보통신업	79.3	3.64	2.34	75.7	82.9
	9. 금융 및 보험업	97.1	1.51	0.80	95.6	98.6
	10. 부동산업	89.2	3.15	1.81	86.0	92.3
	11. 기술서비스업	87.8	2.39	1.39	85.4	90.2
	12. 사설관리/사업 지원 서비스업	92.9	1.86	1.02	91.0	94.7
	13. 교육 서비스업	50.2	6.77	6.88	43.4	57.0
	14. 보건·사회복지업	74.6	4.31	2.95	70.3	78.9
	15. 예술·여가 서비스업	91.2	3.94	2.20	87.2	95.1
	16. 수리·기타 서비스업	85.9	5.20	3.09	80.7	91.1
규모별	10 ~ 49명	77.4	1.74	1.14	75.7	79.1
	50 ~ 249명	100.0	0.00	0.00	100.0	100.0
	250명 이상	100.0	0.00	0.00	100.0	100.0

2 개인 부문

1 정보보호 교육

		정보보호 교육	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		15.3	1.12	3.72	14.2	16.4
성별	남성	16.7	1.62	4.93	15.1	18.4
	여성	13.8	1.53	5.64	12.3	15.4
연령별	12~19세	31.1	4.80	7.88	26.3	35.9
	20대	25.2	3.31	6.71	21.9	28.5
	30대	19.7	3.01	7.78	16.7	22.7
	40대	12.8	2.32	9.26	10.5	15.1
	50대	9.0	1.93	10.95	7.1	10.9
	60대	3.7	1.43	19.63	2.3	5.2

2 정보보호 금전 소비 경험

		정보보호 금전 소비 경험	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		13.2	1.05	4.05	12.2	14.3
성별	남성	14.6	1.53	5.34	13.1	16.2
	여성	11.7	1.43	6.20	10.3	13.2
연령별	12~19세	4.7	2.19	23.90	2.5	6.9
	20대	20.7	3.09	7.60	17.7	23.8
	30대	18.7	2.95	8.04	15.7	21.6
	40대	12.9	2.33	9.23	10.5	15.2
	50대	11.1	2.12	9.73	9.0	13.3
	60대	7.8	2.04	13.24	5.8	9.9

3 디지털 데이터 백업

		디지털 데이터 백업	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		54.3	1.54	1.45	52.7	55.8
성별	남성	57.7	2.14	1.89	55.6	59.8
	여성	50.7	2.22	2.23	48.5	52.9
연령별	12~19세	65.6	4.93	3.83	60.7	70.6
	20대	71.2	3.45	2.47	67.8	74.7
	30대	63.0	3.65	2.96	59.3	66.6
	40대	54.3	3.46	3.25	50.9	57.8
	50대	47.4	3.37	3.63	44.0	50.7
	60대	31.4	3.51	5.71	27.9	34.9

4 보안 점검 수행

		보안 점검 수행	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		51.2	1.55	1.54	49.7	52.8
성별	남성	56.2	2.15	1.95	54.0	58.3
	여성	46.0	2.21	2.45	43.8	48.2
연령별	12~19세	51.6	5.18	5.12	46.5	56.8
	20대	63.7	3.66	2.93	60.1	67.4
	30대	61.7	3.67	3.04	58.0	65.3
	40대	52.7	3.47	3.36	49.2	56.1
	50대	46.5	3.37	3.69	43.2	49.9
	60대	32.2	3.54	5.60	28.7	35.8

5 침해사고 경험

		침해사고 경험	표본오차	상대 표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전체		7.5	0.82	5.53	6.7	8.4
성별	남성	7.9	1.17	7.55	6.7	9.1
	여성	7.2	1.15	8.13	6.0	8.3
연령별	12~19세	8.1	2.83	17.79	5.3	11.0
	20대	11.6	2.44	10.76	9.1	14.0
	30대	9.3	2.19	12.07	7.1	11.4
	40대	6.5	1.71	13.45	4.8	8.2
	50대	5.2	1.50	14.67	3.7	6.7
	60대	5.7	1.76	15.67	4.0	7.5

부록 3

조사표

3

2022년 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 "2022년 정보보호 실태조사(기업)"를 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.

2022년 9월

주관기관	전담기관	조사기관	실사 문의	조사 문의
과학기술정보통신부	한국정보보호산업협회	㈜글로벌리서치		

* 본 조사는 통계법 제33조(비밀의 보호)에 따라 통계목적으로 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	
사업체명			표본번호			-		업종번호			규모번호		
사업형태	① 단독사업체		② 본사/본점 등		③ 공장/지사(점)/영업소 등 ☞ 조사중단				
조직형태	① 개인사업체		② 회사법인		③ 회사 이외의 법인		④ 비법인단체		
업 종	① 농림수산업			② 제조업			③ 전기, 가스, 증기 및 공기조절 공급업/수도, 하수·폐기물 처리, 원료재생업		
	④ 건설업			⑤ 도매 및 소매업			⑥ 운수 및 창고업		
	⑦ 숙박 및 음식점업			⑧ 정보통신업			⑨ 금융 및 보험업		
	⑩ 부동산업			⑪ 전문, 과학 및 기술서비스업			⑫ 사업시설관리, 사업지원 및 서비스업		
	⑬ 교육 서비스업			⑭ 보건업 및 사회복지 서비스업			⑮ 예술, 스포츠 및 여가관련 서비스업		
	⑯ 협회, 단체, 수리 및 기타 개인서비스업								
규 모 (비정규직 포함)	① 1 - 4명 ☞ 조사중단		② 5 - 9명 ☞ 조사중단		③ 10 - 49명		④ 50 - 249명		
	⑤ 250 - 499명		⑥ 500 - 999명		⑦ 1,000명 이상				

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 「2021년 12월 31일 기준」으로 응답해 주시기 바랍니다. 그러나 특정 파트에서는 「2022년 7월 1일 기준」이며, 설문에 별도로 표시가 되어있습니다.

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.

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

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 임원들은 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 우려되지 않는다	우려되지 않는 편이다	보통이다	우려되는 편이다	매우 우려된다
A2-1. 인터넷을 통한 사내 전산 시스템 침해사고 위협	①	②	③	④	⑤
A2-2. 고객 개인정보 유출 위협	①	②	③	④	⑤
A2-3. 시스템 및 네트워크 장애로 인한 서비스 마비 위협	①	②	③	④	⑤
A2-4. 시스템 및 네트워크 침입을 통한 해킹의 위협	①	②	③	④	⑤
A2-5. 인적 요인에 의한 정보유출 위협	①	②	③	④	⑤
A2-6. 불법적인 사내 침입 등에 의한 물리적 위협	①	②	③	④	⑤
A2-7. 외부 공격에 의한 저장된 데이터 자산의 손·망실	①	②	③	④	⑤
A2-8. 사내에 가이드, 규정 등의 미비로 인한 우려	①	②	③	④	⑤

A3 귀사가 **정보보호 관련 업무에 대해 어려움을 느끼는 것**은 무엇입니까?
우선순위대로 3가지만 선택하여 주십시오.

1순위 _____ **2순위** _____ **3순위** _____

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

A4 귀사에서 **정보보호 관련 규정이 제정, 변경 또는 강화**되었을 시, 귀사의 조직 구성원에게 해당 사항에 대하여 얼마나 **엄격하게 적용**하였다고 생각하십니까?

전혀 엄격하지 않다	엄격하지 않은 편이다	보통이다	엄격한 편이다	매우 엄격하다
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	①	②
B1-2. 정보보호 정책 또는 규정집에 개인정보보호 관련 규정이 포함되어 있는 경우 체크	☐	

B2

귀사에서 **정보보호 조직을 운영하는 방식**은 무엇입니까?
※ 정보보호 조직이 전체 업무 중 **정보보호 이외 업무를 1건 이상 수행하고 있을 경우, "② 겸임조직"으로 응답**해 주시기 바랍니다.

① 전담조직 ② 겸임조직 ③ 운영하지 않음

B3

귀사에는 다음의 **책임자가 임명**되어 있습니까?

문 항	B3-1. 책임자 임명 여부		B3-2. 전담 여부 【B3-1의 ① 예 응답자만】		B3-3. 겸임 여부 【B3-2의 ② 아니오 응답자만】	
	예	아니오	예	아니오	예	아니오
1) 정보관리책임자 CIO	①	②	①	②	①	②
2) 정보보호최고책임자 CISO	①	②	①	②	①	②
3) 개인정보보호책임자 CPO	CIO 또는 CISO가 CPO의 업무를 겸직할 경우 체크				☐	

B4

귀사의 **정보보호 관련 인력**은 얼마나 있습니까? 인력의 인원 수를 기입하여 주십시오.
(겸직일 경우, 주로 담당하시는 업무 위주로 기입)
※ **내부인력**은 귀사에 소속되어 있는 인력, **외부인력**은 귀사에 소속되어 있지 않은 인력을 의미합니다.

문 항	인력 인원 수		
	1. 내부인력	2. 외부인력	3. 총 인력 (1+2)
B4-1. 정보보호 담당 인력	_____ 명	_____ 명	_____ 명
B4-1-1. 개인정보보호 업무 겸직 여부	☐	☐	
B4-2. 부가 업무로 정보보호 업무를 수행하는 IT 인력	_____ 명	_____ 명	_____ 명
B4-3. 부가 업무로 정보보호 업무를 수행하는 일반 사무직 인력	_____ 명	_____ 명	_____ 명

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 포함하며, **개인정보보호 관련 법정 필수 교육은 제외함.**

C1 귀사는 2021년 1월 이후 임직원을 대상으로 **정보보호 교육을 실시**하였습니까?

① 예 ② 아니오 ☞ "D. 정보보호 예산"으로 이동

【C1의 '① 예' 응답자만】

C1-1 귀사는 아래의 임직원에 대해 **정보보호 교육을 실시**하였습니까?

문 항	정보보호 교육 실시 여부		
	예	아니오	해당없음
C1-1-1. CEO 및 경영진	①	②	
C1-1-2. IT 관련 직원	①	②	③
C1-1-3. 일반 직원(IT 직원 제외)	①	②	
C1-1-4. 외주직원/협력업체 직원(전산장비 담당)	①	②	③

【C1-1의 모든 문항에 '② 아니오' 또는 '③ 해당 없음' 선택이 불가능합니다.】

【C1의 '① 예' 응답자만】

C1-2 귀사는 아래의 임직원에 대해 **주로 실시한 정보보호 교육 방법**은 무엇입니까?
※ 강사와의 대면 여부에 따라 온라인/오프라인 교육으로 구분
(한 공간에 임직원들이 모여서 온라인 교육 영상을 시청할 경우, 강사와의 비대면 진행이므로 '온라인 교육'으로 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
C1-2-1. CEO 및 경영진	①	②	③	④	①	②
C1-2-2. IT 관련 직원	①	②	③	④	①	②
C1-2-3. 일반 직원(IT 직원 제외)	①	②	③	④	①	②
C1-2-4. 외주직원/협력업체 직원	①	②	③	④	①	②

【C1-1에서 '① 예'를 선택한 문항만 응답】

【C1-1에서 한 문항이라도 '① 예'를 선택한 응답자만】

C1-3 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 사내 보안 부서에서 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 자체 제작 자료 및 외부 전문 위탁 기관 자료 모두 활용
⑥ 기타 ( )

【C1-1에서 한 문항이라도 '① 예'를 선택한 응답자만】

C1-4 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

【C1-1에서 한 문항이라도 '① 예'를 선택한 응답자만】

C1-5 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 2021년 1년간 **정보보호 관련 활동을 위해 예산을 사용해 본 경험**이 있습니까?

* **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
* **물리보안**
  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 이유**에 대하여 아래 항목에 얼마나 공감하십니까?

문 항	전혀 공감하지 않는다	공감하지 않는 편이다	보통이다	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. 정보보호 침해사고는 기업의 노력만으로 해결할 수 없다고 생각하기 때문에	①	②	③	④	⑤

【응답 완료 후 D7 문항으로 이동】

D2

【D1의 '① 예' 응답자만】

정보보호 관련 활동을 위해 예산을 사용해 본 경험이 있다면, **2021년 1년간 정보보호 예산 총액**은 어느 정도입니까? **대략적인 예산 총액을 기재**하여 주십시오.

① 500만 원 미만
↳ (_____ 원)

② 500만 원 이상 ~ 1,000만 원 미만
↳ (_____ 원)

③ 1,000만 원 이상 ~ 5,000만 원 미만
↳ (_____ 원)

④ 5,000만 원 이상 ~ 1억 원 미만
↳ (_____ 원)

⑤ 1억 원 이상 ~ 3억 원 미만
↳ (_____ 원)

⑥ 3억 원 이상 ~ 5억 원 미만
↳ (_____ 원)

⑦ 5억 원 이상
↳ (_____ 원)

D2-1

【D1의 '① 예' 응답자만】

귀사의 2021년 1년간의 **정보보호 예산 총액은 2020년과 비교하여 어떻게 변화**하였습니까?

① 신설 → 2020년까지 정보보호 관련 별도의 예산을 공식적으로 사용하지는 않았으나, **2021년 처음 정보보호 활동을 위해 예산을 사용한 경우**를 의미

② 증가 → 2021년 정보보호 예산이 2020년 정보보호 예산보다 **금액적인 측면에서 증가한 경우**를 의미

③ 감소 → 2021년 정보보호 예산이 2020년 정보보호 예산보다 **금액적인 측면에서 감소한 경우**를 의미

④ 현상 유지 → 2021년 정보보호 예산과 2020년 정보보호 예산이 **금액적인 측면에서 차이가 없는 경우**를 의미

D2-2

【D2-1의 ①~③ 응답자만】

귀사의 **정보보호 예산의 변화 이유**는 무엇입니까? **우선순위대로 2가지만** 선택하여 주십시오.

1순위 _____ **2순위** _____

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, ISMS-P, PIMS, ISO 등 인증 취득비용(수수료 등) 증가(감소)
⑦ 정보보호 사고 대응 관련 비용 증가(감소)
⑧ 기타 ( )

【D1의 '① 예' 응답자만】

D3

향후 2022년 귀사의 **정보보호 예산 총액은 어떻게 변화할 예정**입니까?

① 획기적으로 줄일 것이다
② 점차 줄여나갈 것이다
③ 현상 유지할 것이다
④ 점차 늘려나갈 것이다
⑤ 획기적으로 늘릴 것이다

【D1의 '① 예' 응답자만】

D4

2021년 1년 간 귀사의 **정보보호 예산 활용 중 가장 큰 비중을 차지하는 유형**은 무엇입니까?
우선순위대로 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 유료 인증서의 결제
④ 정보보호 관련 컨설팅(취약점 분석 등 포함)
⑤ 정보보호 관련 교육 자료 습득(강의, 학습자료 등 포함)
⑥ 정보보안을 위한 출동 보안 서비스 이용
⑦ 업무 시설의 CCTV 등 영상감시장비 설치 또는 증설(유지·보수 포함)
⑧ 정보보호 관련 과태료 납부
⑨ 정보보호를 위한 전문인력의 고용(인건비 등)
⑩ 정보보호 관련 관제 서비스
⑪ 기타 ( )

【D1의 '① 예' 응답자만】

D5

정보보호 관련 예산 활용을 결정하게 된 계기는 무엇입니까?

① 정보보호 침해사고 피해를 직접적으로 접한 이후
② 주변 거래처 및 유관기관의 정보보호 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 (_____)

【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 서비스 중 어떤 것을 선호**하십니까?

① 국내 제품 및 서비스

② 해외 제품 및 서비스

③ 특별히 선호도를 구분하지 않음

E 침해사고 예방

E1 귀사에서는 **정보보호 침해사고 예방을 위한 제품 및 솔루션을 사용**하고 있습니까?

① 예 ☞ E1-1 문항으로 이동 ② 아니오 ☞ E2 문항으로 이동

E1-1 [E1의 '① 예' 응답자만]
어떠한 유형의 **정보보안 제품(서비스)을 활용**하고 있습니까? **최대 2개**까지 선택하여 주십시오.

정보보안 제품(서비스)	설명
① 네트워크 보안 장비	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 장비	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 장비	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 장비	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 장비	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 아웃소싱 하여 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

【E1의 '① 예' 응답자만】

E1-2 어떠한 유형의 **물리적 보안 제품(서비스)을 활용**하고 있습니까? **최대 2개**까지 선택하여 주십시오.

① 출입 통제 관리 시스템 (출입통제 게이트, 디지털 도어락)

② 영상 보안 시스템 (IP 카메라, CCTV 등)

③ 출동 보안 서비스 (사설 경비 업체 등)

④ 불법 도·감청 탐지 서비스 (몰래카메라, 초소형 도청장치 등 탐지)

【E1의 '① 예' 응답자만】

E1-3 귀사에서 활용하고 있는 제품의 **정보보호 인증 여부**에 대해 알고 있습니까?

① 예 ② 아니오 ③ 모름

E2 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)

구분	문 항	CCTV 관리 현황	
		E2-1. CCTV 관리 방법	E2-2. CCTV 대수
1	주 사업장	① 직접 관리	( )대
		② 간접(업체 위탁) 관리	( )대
		③ 건물 자체 관리	( )대
2	본사	① 직접 관리	( )대
		② 간접(업체 위탁) 관리	( )대
		③ 건물 자체 관리	( )대

E3 귀사에서는 최근 **사내 IT 시스템 및 네트워크에 대한 보안 점검을 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 ☞ E4 문항으로 이동

【E3의 ①~⑤ 응답자만】

E3-1 귀사에서는 보안 점검을 위해 **시스템 로그 및 방화벽 로그 기록을 관리**하고 있습니까?

① 예
② 아니오

【E3의 ①~⑤ 응답자만】

E3-2 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)

E4 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
E4-1. 중요 데이터 (기업 내부정보, 지식재산, 영업비밀 등)	①	②	
E4-2. 서버 데이터	①	②	
E4-3. 시스템 로그 데이터	①	②	
E4-4. 방화벽 로그 데이터	①	②	③
E4-5. CCTV 영상 데이터	①	②	③

【E4의 한 문항이라도 '① 실시'를 선택한 응답자만】

E4-1

귀사에서 주로 실시하는 **백업 방식**은 다음 중 무엇입니까?

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

【E4의 한 문항이라도 '① 실시'를 선택한 응답자만】

E4-2

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

E5

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

구 분	매우 취약하다	취약한 편이다	보통이다	안전한 편이다	매우 안전하다
E5-1. 정보보안	①	②	③	④	⑤
E5-2. 물리보안	①	②	③	④	⑤

F 침해사고 경험

F1 귀사에서는 **정보보호 관련 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 2021년 1년간 **정보보호 침해사고를 의심한 적**이 있습니까?
(사고 여부가 확실히 증명된 것은 아니지만, 정황상 직·간접적으로 침해 의심이 되는 경우)

① 있다 ② 없다

F4 귀사는 2021년 1년간 **정보보호 관련 침해사고를 직접적으로 경험한 적**이 있습니까?

① 예 → (_____ 회) ② 아니오 ☞ "G. 사이버 보험"으로 이동

F4-1 【F4의 '① 예' 응답자만】
귀사가 2021년 1년간 **경험한 정보보호 관련 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 DOS 또는 DDoS 공격으로 인한 IT 시스템 마비
④ 피싱, 스미싱 등에 의한 금전 또는 중요 데이터 유출
⑤ 내부인력에 의한 중요 데이터 유출
⑥ 랜섬웨어 감염
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 2021년 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 기타 (_____)

【F4의 '① 예' 응답자만】

F4-3 해당 경험의 **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 경험한 침해사고 중 **가장 심각한 침해사고 피해 시 각 단계별**(발생 사실 인지/원인 파악/문제 해결 및 서비스 복원)로 **소요된 시간**을 응답해 주십시오.

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

【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 이유**는 무엇입니까? **우선순위대로 2가지만** 선택하여 주십시오.

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
⑦ 기타 (_____)

【응답 완료 후 "G. 사이버 보험"으로 이동】

【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 인증을 받은 제품으로 교체
⑦ 별다른 활동을 수행하지 않음
⑧ 기타 (_____)

【F4의 '① 예' 응답자만】

F7 귀사의 **종합적인 정보보호 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. 물리보안	①	②	③	④	⑤

【F4의 '① 예' 응답자만】

F8 정보보호 침해사고 경험 이후 **정보보호 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. 재택근무"로 이동		G2 문항으로 이동	

【G1의 ②~④ 응답자만】

G2 귀사는 사이버 보험에 가입 또는 이용하고 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	② 아니오

G3 【G2-3의 '① 예' 응답자만】

귀사가 향후 사이버 보험 가입 시 **보장받고자 하는 항목**을 **우선순위대로 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 재택근무

H1 귀사는 2021년 1년간 COVID-19로 인한 **비대면 재택근무를 시행**하였습니까?

① 예 ☞ H1-1 문항으로 이동 ② 아니오 ☞ 조사 종료

H1-1 【H1의 '① 예' 응답자만】
귀사가 **재택근무 시 직원에게 지원한 보안 솔루션**은 무엇입니까? 해당하는 것을 **모두 선택**해 주십시오.

① 자체 구축한 가상사설망(VPN) 활용
② 전문 재택근무 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 재택근무를 위한 별도의 보안 솔루션을 지원하지 않음
⑨ 기타 ( )

H1-2 【H1의 '① 예' 응답자만】
귀사에서는 **비대면 재택근무 시 정보보호에 대한 위험성을 인지**하고 있습니까?

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

H2 【H1의 '① 예' 응답자만】
귀사에서 2021년 1년간 **재택근무 시행 준비 및 운영 간 정보보호 관련 침해사고가 발생했거나, 침해사고가 의심되었던 경우가 있습니까?**

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

조사 기록표 [면접원 기록사항]

Z1 조사 방법

① 방문면접조사
② 현장방문 시 조사가 불가능하여 질문지 배포 후 방문하여 조사 완료
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 분 간

Z4 조사대상 기업체 정보변경 현황

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

Z5 면접원 기록사항

1. 회사명	
2. 주소	
3. 응답자 성명	
4. 소속	
5. 직위	
6. 전화번호	
7. 이메일	
8. 조사원 성명	

- 끝까지 응답해 주셔서 감사합니다. -

2022년 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 인터넷 이용자를 대상으로 "2022년 정보보호 실태조사(개인)"를 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.

2022년 9월

주관기관	전담기관	조사기관	실사 문의	조사 문의
과학기술정보통신부	한국정보보호산업협회	㈜글로벌리서치	송미영 부장 02-3456-1902 mysong@globalri.co.kr	장유진 대리 02-3456-1872

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

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

면접원 기입란	주소				전화번호	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	생년월(만 연령)			직 업	
	①남 ②여	양력 ____년 ____월 (만____세) ☞ 만 12세 미만, 만 70세 이상은 조사 중단			①있음	직업명 직업코드
					②없음	①학생 ②전업주부 ③기타/무직

응답 시 유의사항

1 면접원의 안내에 따라 응답해 주십시오.

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

3 본 설문지는 응답 시점을 기준으로 최근 1년간 「2021년 7월 1일 ~ 2022년 6월 30일」을 기준으로 응답해 주시기 바랍니다.
(단, 침해사고 경험 관련 문항은 「2021.1.1~2021.12.31」을 기준으로 응답해 주시기 바랍니다)

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

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 **업무상 접속을 포함**하여 어느 정도입니까?

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) 읽기, 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 보호받지 못한다	보호받지 못하는 편이다	보통이다	대체로 보호받는 편이다	충분히 보호받고 있다
①	②	③	④	⑤

A 정보보호 인식

A1 귀하는 **최근 1년간 정보보호 관련 이슈*에 관심**을 가져본 적이 있습니까?

* **정보보호 관련 이슈**
예시) 러시아, 우크라이나 간 사이버 전쟁, 글로벌 산업시설 해킹으로 인한 대규모 피해 발생, 랜섬웨어 감염으로 인한 기업들의 피해, AI 챗봇 이루다, 가상 애완 동물 웹사이트 Neopets 데이터 침해, 암호화폐 지갑 해킹으로 인한 거래소 금전 피해, NFT(대체 불가능한 토큰) 등

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

A2 귀하는 **정보보호 침해에 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 개인 전자장비 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. 개인 전자기기에 대한 랜섬웨어* 감염 등과 같은 악성코드 감염	①	②	③	④	⑤
A4-2. 개인 전자기기의 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 대한 타인의 불법적인 접근 (예시: 주거침입, 절도 등)	①	②	③	④	⑤
A4-5. 기타 (_____)	①	②	③	④	⑤

A5

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

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

A6

귀하는 **정보보호 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 제조사의 보안 기능 탑재 노력의 부족	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. 각종 교육 기관의 관련 범죄 예방 교육 노력의 부족	①	②	③	④	⑤
A6-7. 수사기관 및 관련 공공기관의 관련 범죄자 수사 노력의 부족	①	②	③	④	⑤
A6-8. 사법 기관의 관련 범죄 처벌 노력의 부족	①	②	③	④	⑤
A6-9. 처벌기준, 형량이 너무 낮아서	①	②	③	④	⑤

A7

귀하는 **정보보호 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 정부부처 및 공공기관	①	②	③	④	⑤
A8-2. 정보보호 관련 민간업체	①	②	③	④	⑤
A8-3. 인터넷 서비스 제공자	①	②	③	④	⑤

B 정보보호 교육

B1 귀하는 **최근 1년간 정보보호 관련 교육을 받아 본 경험**이 있습니까?
(**개인정보보호 법정 의무교육은 제외**)

① 예 ② 아니오 ☞ "C. 정보보호 예산"으로 이동

【B1의 '① 예' 응답자만】

B1-1 귀하께서 수강하신 **정보보호 관련 교육의 교육 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)

【B1의 '① 예' 응답자만】

B1-2 귀하께서 수강하신 **정보보호 교육에 포함된 주제를 모두 선택**하여 주시 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

【B1의 '① 예' 응답자만】

B1-3 귀하께서 수강하신 **정보보호 교육의 학습 효과**는 어떠하였습니까?

문 항	전혀 효과가 없다	효과가 없는 편이다	보통 이다	효과가 있는 편이다	매우 효과적 이다
B1-3-1. 정보보호에 대한 기본 소양(배경 지식 등)의 함양	①	②	③	④	⑤
B1-3-2. 정보보호를 위한 사고 예방 방법에 대한 인식	①	②	③	④	⑤
B1-3-3. 정보보호의 중요성에 대한 인식	①	②	③	④	⑤
B1-3-4. 정보보호 피해 사례에 대한 인식	①	②	③	④	⑤
B1-3-5. 정보보호 피해 대응 방법 습득	①	②	③	④	⑤

【B1-2에서 선택한 문항만 응답】

【B1의 '① 예' 응답자만】

B1-4 해당 **정보보호 교육의 학습 난이도**는 어떠하였습니까?

문 항	전혀 이해되지 않는다	이해되지 않는 편이다	보통이다	대체로 이해되는 편이다	완전히 이해된다
B1-4-1. 정보보호에 대한 기본 소양(배경 지식 등)	①	②	③	④	⑤
B1-4-2. 정보보호를 위한 사고 예방 방법	①	②	③	④	⑤
B1-4-3. 정보보호의 중요성	①	②	③	④	⑤
B1-4-4. 정보보호 피해 사례	①	②	③	④	⑤
B1-4-5. 정보보호 피해 대응 방법	①	②	③	④	⑤

【B1-2에서 선택한 문항만 응답】

【B1의 '① 예' 응답자만】

B2 귀하께서는 **정보보호 관련 학습의 어려움**에 대해서 각각 얼마나 동의하십니까?

문 항	전혀 동의하지 않는다	동의하지 않는 편이다	보통이다	동의하는 편이다	매우 동의한다
B2-1. 정보보호 관련 용어가 생소하고 어려움	①	②	③	④	⑤
B2-2. 원하는 정보보호 관련 자료가 없음	①	②	③	④	⑤
B2-3. 정보의 양이 많고 복잡함	①	②	③	④	⑤
B2-4. 정보를 얻는 곳을 모름	①	②	③	④	⑤
B2-5. 정보보호와 관련된 지식을 굳이 학습하여 얻고 싶지는 않음	①	②	③	④	⑤

C 정보보호 예산

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 영상감시장비 관련 소비 등

① 예 ② 아니오 ☞ C4 문항으로 이동

【C1의 '① 예' 응답자만】

C1-1 아래와 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 정보보호 관련 과태료 납부
⑦ 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 계기**는 무엇입니까? 우선 순위대로 최대 3순위까지 선택하여 주십시오.

1순위 _____ 2순위 _____ 3순위 _____

① 정보보호 침해사고 피해를 직접적으로 접한 이후
② 주변 지인의 정보보호 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 예정**이십니까?

※ 이전 정보보호 활동 비용 지출이 없었으며 앞으로 정보보호 활동 비용을 지출할 경우, '늘릴 예정이다' 혹은 '크게 늘릴 예정이다'로 응답 바랍니다.

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

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 자주 연결**하여 사용하십니까?

전혀 사용하지 않는다	사용하지 않는 편이다	보통이다	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 개인 전자장비에 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 귀하는 **개인적인 일상 생활 공간에 CCTV(폐쇄회로 영상감시장비 등)가 활용**되고 있습니까?

① 예 ② 아니오

D7 귀하께서는 **보안을 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 공동인증서는 이동식 디바이스에만 저장
⑨ e프라이버시 클린서비스 수시로 이용
⑩ 기타 ( )

D8 귀하는 최근 1년간 **비대면 재택근무(온라인 연결)*를 수행**하신 경험이 있습니까?

* **비대면 재택근무(온라인 연결)**
예시) 네이버 밴드, 줌, 네이버 라인웍스, 마이크로소프트 팀스, 시스코 웹엑스 등

① 예 ☞ D8-1 문항으로 이동 ② 아니오 ☞ "E. 정보보호 침해사고 경험과 위협인식"으로 이동

【D8의 '① 예' 응답자만】

D8-1 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 재택근무, 화상회의 등 이용 시 관련 프로그램 이외의 프로그램을 사용하거나 작동하지 않음
⑥ 기타 ( )

E 정보보호 침해사고 경험과 위협 인식

E1 귀하는 **최근 1년간 자신의 정보보호 침해사고를 의심한 적**이 있습니까?
(사고 여부가 확실히 증명된 것은 아니지만, 정황상 직·간접적으로 침해 의심이 되는 경우)

① 예 ② 아니오

E2 귀하는 **최근 1년간 실제 정보보호 침해사고를 경험한 적**이 있습니까?

① 예 ☞ E2-1 문항으로 이동 ② 아니오 ☞ E4 문항으로 이동

E2-1 【E2의 '① 예' 응답자만】
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

E2-2 【E2의 '① 예' 응답자만】
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 기타 (_____)

【E2의 '① 예' 응답자만】

E2-3

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	

【E2의 '① 예' 응답자만】

E2-4

귀하가 **최근 1년간 경험한 정보보호 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 개인 전자기기에 대한 불법적 접근으로 인한 보유 중인 데이터의 외부 유출
⑤ 피싱, 파밍, 스미싱 등에 의한 금전적 피해
⑥ 기타 (_____)

【E2의 '① 예' 응답자만】

E2-5

정보보호 침해사고 경험 이후, **정보보호 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

E3 【E2의 '① 예' 응답자만】

해당 침해사고가 발생(인지)했을 당시 **관련 기관에 피해 사실을 신고**하셨습니까?

① 예 ☞ E4 문항으로 이동 ② 아니오 ☞ E3-1 문항으로 이동

E3-1 【E3의 '② 아니오' 응답자만】

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 신고할 수 있다는 사실을 몰랐기 때문에
③ 신고하는 방법을 몰랐기 때문에
④ 신고에 따른 사건 조사, 처리가 복잡하고 불편하다고 느껴졌기 때문에
⑤ 침해 사실과 피해 사실을 사고 발생 이후 뒤늦게 인지했기 때문에(최소 1개월 이상)
⑥ 신고하더라도 피해가 복구되지 못한다고 생각하기 때문에
⑦ 신고하더라도 범인을 체포하거나 처벌할 수 없다고 생각하기 때문에
⑧ 기타 (_____)

E4

귀하는 다음과 같은 **최신 기술의 이용과 관련하여 정보보호에 대한 위험성**은 어느 정도라고 생각하십니까? 매우 취약하다고 생각하시면 -5점, 매우 안전하다고 생각하시면 +5점으로 기입하여 주십시오.

매우 취약하다 <					보통이다					> 매우 안전하다
-5	-4	-3	-2	-1	0	+1	+2	+3	+4	+5
매우 취약		취약한 편			보통	안전한 편			매우 안전	

문 항	정보보호 위험성
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. 스마트 팩토리에서의 자동화 공정 기술	
E4-7. 원격 진료, 인공 장기 등과 같은 지능형 헬스케어 기술	

E5

귀하는 다음과 같은 **최신 기술과 관련하여 정보보호 침해사고가 발생할 경우, 그 피해의 파급효과**는 어느 정도라고 생각하십니까?
매우 취약하다고 생각하시면 -5점, 매우 안전하다고 생각하시면 +5점으로 기입하여 주십시오.

매우 심각하다 <					보통이다					> 매우 경미하다
-5	-4	-3	-2	-1	0	+1	+2	+3	+4	+5
매우 심각		심각한 편			보통	경미한 편			매우 경미	

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. 스마트 팩토리에서의 자동화 공정 기술	
E5-7. 원격 진료, 인공 장기 등과 같은 지능형 헬스케어 기술	

면접원 기록사항

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

① 100만 원 미만
② 100 ~ 200만 원 미만
③ 200 ~ 300만 원 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
② 초등학교
③ 중학교
④ 고등학교
⑤ 전문대
⑥ 대학교
⑦ 대학원

DQ2 귀하의 **최종학력 이수여부를** 표시해 주십시오.

① 재학
② 휴학
③ 중퇴
④ 수료
⑤ 졸업

- 끝까지 응답해 주셔서 감사합니다. -

2022년 정보보호 실태조사

발행처 과학기술정보통신부

주소 세종특별자치시 가름로 194(어진동)
홈페이지 www.msit.go.kr

수행기관 한국정보보호산업협회

주소 서울특별시 송파구 중대로 135 서관 14층
홈페이지 www.kisia.or.kr
대표전화 02-6748-2000
담당부서 02-6748-2009

실사기관 | 주 | 글로벌리서치

주소 서울시 서초구 반포대로 45 명정빌딩 2~4층
홈페이지 www.globalri.co.kr
대표전화 02-6253-1400

2022 정보보호 실태조사

SURVEY ON INFORMATION SECURITY

과학기술정보통신부

kisia 한국정보보호산업협회
Korea Information Security Industry Association