승인번호
제 342005 호

# 2020
# 정보보호 실태조사
## SURVEY ON INFORMATION SECURITY

과학기술정보통신부
Ministry of Science and ICT

kisia 한국정보보호산업협회
Korea Information Security Industry Association

# 이용자를 위하여

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

2. 통계표 및 도표 내의 숫자는 반올림되었으므로 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 (부록1 참조)

4. 통계표 및 도표에 사용된 기호의 뜻은 다음과 같음
   - : 조사되었으나 정보가 없는 경우
   0 : 조사결과 값이 0이거나 0에 근사한 경우

5. 복수응답은 한 개 이상을 응답한 경과치를 집계한 결과임

# 2020년 정보보호 실태조사


**조 사 기 획 :** 과학기술정보통신부 장 성 환 사무관

심 채 영 주무관

**조 사 수 행 :** 한국정보보호산업협회 황 지 은 팀 장

이 주 영 선 임

유 상 곤 주 임

**조 사 기 관 :** ㈜ 글 로 벌 리 서 치

# 목 차

# 1부 기업부문

# 목 차

# 목 차

## 2부 개인부문

# 목 차

# 그림목차

## 1부 기업부문

# 그림목차

# 그림목차



# 2부 개인부문

# 그림목차

# 표목차

## 1부 기업부문



## 2부 개인부문

# 1부

## 기업부문

제1장

# 조사개요

# 제1장 조사개요

## 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 통계정보를 제공하는데 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 종사자 수 5명 이상, 네트워크로 연결된 컴퓨터를 1대 이상 보유한 사업체'로 조사대상 변경

➪ **2006년** - 정보보안 침해사고의 피해현황 파악을 위한 조사지표 추가

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

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

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

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

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

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

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

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

**2016년** - 조사 결과의 신뢰도 제고를 위한 표본 수 확대 ('15년 8,000개 → '16년 9,000개)
- ICT 통계업무 조정으로 「정보화실태조사의 정보보호 파트」 본 조사에서 실시, OECD에 데이터 2개 제출(정보보호 및 개인정보보호 정책률, 침해사고 경험률)
- 승인번호 제342005호로 변경

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

**2018년** - '2016년 기준 전국사업체조사'와 '2017년 정보화통계조사' 결과를 기반으로 표본 재설계

**2019년** - 한국인터넷진흥원(KISA)에서 한국정보보호산업협회(KISIA)로 업무 이관
- 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

## 3. 조사 내용 및 범위

본 조사는 국내 사업체의 정보보호 기반 및 환경, 침해사고 예방, 침해사고 경험 및 대응, 정보보호 인식, 개인정보보호, 주요 서비스별 정보보호 실태를 파악할 수 있는 지표로 구성하였다.

본 조사의 주요 내용은 다음과 같다

- 정보보호 중요성 인식 현황
- 정보보호 정책 수립 및 정보보호 조직 구성 현황
- 임직원 대상 정보보호 교육 실시 현황
- 정보보호 예산 및 투자 현황
- 정보보호 제품 및 서비스 이용 현황
- 정보보호 관리 현황
- 침해사고 경험 여부 및 대응활동 현황
- 개인정보 수집 및 이용 현황
- 개인정보 침해사고 경험 여부 및 대응 현황
- 모바일, 무선랜, 클라우드 및 사물인터넷(IoT) 보안 현황
- 사이버(정보보호, 개인정보보호) 보험 이용 및 향후 계획 현황
- 주요서비스 정보보호 투자 계획 현황

## 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
- **개인정보취급자** : 개인정보를 처리하는 공공기관이나 사업자·단체 등의 지휘·감독을 받아 개인정보를 처리하는 임직원, 시간제 근로자 등
- **IP 카메라** : 카메라와 컴퓨터가 하나의 장치로 결합된 것으로 폐쇄회로 텔레비전(CCTV)과 달리 통신망을 이용해 영상정보를 송출하고 클라우드 서버에 저장하며, 모바일기기나 PC 등을 통해 확인이 가능한 영상정보 처리기기
- **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 : 종사자 수 1인 이상, 네트워크에 연결된 컴퓨터 보유 사업체
- 유효응답업체수 : 9,000개
- 조사주기 : 연 1회
- 조사기간 : 2020년 8월 3일 ~ 11월 30일 (4개월)
- 조사방법 : 사업체 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 사업체
- 조사 모집단(Survey Population)
  - 네트워크에 연결된 컴퓨터를 1대 이상 보유하고 있는 종사자 규모 1인 이상의 국내 사업체
- 모집단 자료
  - 통계청 『2018년 기준 전국사업체조사』 의 업종별, 규모별 사업체 수 및 분포 결과와 한국정보화진흥원 『2019년 정보화통계조사』 결과에서 파악된 네트워크 구축 비율을 이용
- 규모(종사자 수): 1~4명/5~9명/10~49명/50~249명/250~999명/1,000명 이상

➪ 본 조사를 위한 업종 분류는 OECD의 분류 권고안과 한국표준산업분류를 기준으로 13개 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 (본조사) | 국제기구 분류기준 (ISIC ver 4.0) |
|---|---|---|
| A. 농업, 임업 및 어업 | 1. 농림수산업(광업포함) | - |
| B. 광업 | | |
| C. 제조업 | 2. 제조업 | 제조업(ISIC C) |
| F. 건설업 | 3. 건설업 | 건설업(ISIC F) |
| G. 도매 및 소매업 | 4. 도매 및 소매업 | 도소매업(ISIC G);<br>자동차 및 모터사이클 수리업 |
| H. 운수 및 창고업 | 5. 운수 및 창고업 | 운수업(ISIC H) |
| I. 숙박 및 음식점업 | 6. 숙박 및 음식점업 | 숙박 및 음식점업(ISIC I) |
| J. 정보통신업 | 7. 정보통신업 | 정보통신업(ISIC J) |
| K. 금융 및 보험업 | 8. 금융 및 보험업 | - |
| L. 부동산업 | 9. 부동산업 | 부동산업(ISIC L) |
| M. 전문, 과학 및 기술 서비스업 | 10. 전문, 과학 및 기술서비스업 | 전문, 과학 및 기술서비스업 (M75 수의업 제외) |
| N. 사업시설 관리, 사업 지원 및 임대 서비스업 | 11. 사업시설관리, 사업지원 및 임대 서비스업 | 사업관리 및 지원서비스업(ISIC N) |
| S. 협회 및 단체, 수리 및 기타 개인서비스업 | 12. 협회 및 단체, 수리 및 기타 개인서비스업 | 기타 서비스업<br>(ISIC S, S95 수리업 포함)<br>- ISIC S94 협회 및 단체<br>- ISIC S95 컴퓨터, 개인 및 가정용품 수리업 포함<br>- ISIC S96 기타 개인서비스업 |
| D. 전기, 가스, 증기 및 공기 조절 공급업 | 13. 기타<br>(한국표준산업분류 중 좌변의 대분류에 해당하는 산업, 단 O는 제외) | - |
| E. 수도, 하수 및 폐기물 처리, 원료 재생업 | | |
| O. 공공 행정, 국방 및 사회보장 행정 | | |
| P. 교육 서비스업 | | |
| Q. 보건업 및 사회복지 서비스업 | | |
| R. 예술, 스포츠 및 여가관련 서비스업 | | |

표 1-1-2 업종, 규모별 적용 기준

| 한국표준산업분류 (10차 개정) | 업종 분류기준 (본조사) |
|---|---|
| A. 농업, 임업 및 어업 | 1. 농림수산업(광업포함) |
| B. 광업 | |
| C. 제조업 | 2. 제조업 |
| F. 건설업 | 3. 건설업 |
| G. 도매 및 소매업 | 4. 도매 및 소매업 |
| H. 운수 및 창고업 | 5. 운수 및 창고업 |
| I. 숙박 및 음식점업 | 6. 숙박 및 음식점업 |
| J. 정보통신업 | 7. 정보통신업 |
| K. 금융 및 보험업 | 8. 금융 및 보험업 |
| L. 부동산업 | 9. 부동산업 |
| M. 전문, 과학 및 기술 서비스업 | 10. 전문, 과학 및 기술서비스업 |
| N. 사업시설 관리, 사업 지원 및 임대 서비스업 | 11. 사업시설관리, 사업지원 및 임대 서비스업 |
| S. 협회 및 단체, 수리 및 기타 개인서비스업 | 12. 협회 및 단체, 수리 및 기타 개인서비스업 |
| D. 전기, 가스, 증기 및 공기 조절 공급업 | 13. 기타 (한국표준산업분류 중 좌변의 대분류에 해당하는 산업, 단 O는 제외) |
| E. 수도, 하수 및 폐기물 처리, 원료 재생업 | |
| O. 공공 행정, 국방 및 사회보장 행정 | |
| P. 교육 서비스업 | |
| Q. 보건업 및 사회복지 서비스업 | |
| R. 예술, 스포츠 및 여가관련 서비스업 | |

| 구 분 | 규 모 분 류 |
|---|---|
| 규모 1층 | 1 ~ 4명 |
| 규모 2층 | 5 ~ 9명 |
| 규모 3층 | 10 ~ 49명 |
| 규모 4층 | 50 ~ 249명 |
| 규모 5층 | 250 ~ 999명 |
| 규모 6층 | 1,000명 이상 |

➔ 모집단 분포

- 통계청 『2018년 기준 전국사업체조사』 및 한국정보화진흥원 『2019년 정보화통계조사』에서 조사된 사업체 중 종사자 수 1명 이상 사업체 현황 및 분포는 다음과 같이 나타남

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

(단위 : 개)

| 구분 | 업종/규모 | 사업체 수 | 컴퓨터 보유/네트워크 구축 사업체 수 |
|---|---|---|---|
| 업종별 | 1. 농림수산업(광업포함) | 6,177 | 3,022 |
| | 2. 제조업 | 437,024 | 206,832 |
| | 3. 건설업 | 142,840 | 70,371 |
| | 4. 도매 및 소매업 | 1,027,109 | 376,482 |
| | 5. 운수 및 창고업 | 400,282 | 104,218 |
| | 6. 숙박 및 음식점업 | 766,315 | 159,650 |
| | 7. 정보통신업 | 43,888 | 32,510 |
| | 8. 금융 및 보험업 | 43,568 | 36,788 |
| | 9. 부동산업 | 160,152 | 93,898 |
| | 10. 전문, 과학 및 기술서비스업 | 112,301 | 72,671 |
| | 11. 사업시설관리, 사업지원 및 임대 서비스업 | 70,542 | 40,826 |
| | 12. 협회 및 단체, 수리 및 기타 개인서비스업 | 410,246 | 87,422 |
| | 13. 기타 서비스업 | 470,207 | 229,788 |
| 규모별 | 1~4명 | 3,272,417 | 928,270 |
| | 5~9명 | 489,710 | 313,650 |
| | 10~49명 | 280,615 | 230,135 |
| | 50~249명 | 43,235 | 38,104 |
| | 250~999명 | 4,067 | 3,731 |
| | 1,000명 이상 | 607 | 588 |
| 전체 | | 4,090,651 | 1,514,478 |

※ 출처: 2018년 기준 전국사업체조사(통계청), 2019년 정보화통계조사(한국정보화진흥원)

표 1-1-4 업종·규모별 모집단 분포

(단위 : 개, %)

| 업종 분류 | 규모 분류 | 컴퓨터 보유/네트워크 구축 사업체 | 구성비 | 업종 분류 | 규모 분류 | 컴퓨터 보유/네트워크 구축 사업체 | 구성비 |
|---|---|---|---|---|---|---|---|
| 농림수산업 (광업포함) | 1~4명 | 985 | 0.07 | 금융 및 보험업 | 1~4명 | 8,541 | 0.57 |
| | 5~9명 | 920 | 0.06 | | 5~9명 | 10,362 | 0.69 |
| | 10~49명 | 997 | 0.07 | | 10~49명 | 15,986 | 1.06 |
| | 50~249명 | 112 | 0.01 | | 50~249명 | 1,696 | 0.11 |
| | 250~999명 | 8 | 0.00 | | 250~999명 | 171 | 0.01 |
| | 1,000명 이상 | - | 0.00 | | 1,000명 이상 | 32 | 0.00 |
| 제조업 | 1~4명 | 92,127 | 6.11 | 부동산업 | 1~4명 | 79,204 | 5.26 |
| | 5~9명 | 60,259 | 4.00 | | 5~9명 | 9,133 | 0.61 |
| | 10~49명 | 44,552 | 2.96 | | 10~49명 | 5,186 | 0.34 |
| | 50~249명 | 8,968 | 0.60 | | 50~249명 | 326 | 0.02 |
| | 250~999명 | 805 | 0.05 | | 250~999명 | 42 | 0.00 |
| | 1,000명 이상 | 121 | 0.01 | | 1,000명 이상 | 7 | 0.00 |
| 건설업 | 1~4명 | 28,083 | 1.86 | 전문, 과학 및 기술 서비스업 | 1~4명 | 40,494 | 2.69 |
| | 5~9명 | 19,120 | 1.27 | | 5~9명 | 18,011 | 1.20 |
| | 10~49명 | 20,512 | 1.36 | | 10~49명 | 11,777 | 0.78 |
| | 50~249명 | 2,288 | 0.15 | | 50~249명 | 1,976 | 0.13 |
| | 250~999명 | 313 | 0.02 | | 250~999명 | 365 | 0.02 |
| | 1,000명 이상 | 55 | 0.00 | | 1,000명 이상 | 48 | 0.00 |
| 도매 및 소매업 | 1~4명 | 277,909 | 18.45 | 사업시설 관리, 사업지원 및 임대 서비스업 | 1~4명 | 24,255 | 1.61 |
| | 5~9명 | 62,005 | 4.12 | | 5~9명 | 6,477 | 0.43 |
| | 10~49명 | 33,650 | 2.23 | | 10~49명 | 7,202 | 0.48 |
| | 50~249명 | 2,687 | 0.18 | | 50~249명 | 2,168 | 0.14 |
| | 250~999명 | 213 | 0.01 | | 250~999명 | 636 | 0.04 |
| | 1,000명 이상 | 18 | 0.00 | | 1,000명 이상 | 88 | 0.01 |
| 운수 및 창고업 | 1~4명 | 84,887 | 5.63 | 협회 및 단체, 수리 및 기타 개인 서비스업 | 1~4명 | 67,114 | 4.45 |
| | 5~9명 | 7,721 | 0.51 | | 5~9명 | 12,149 | 0.81 |
| | 10~49명 | 8,807 | 0.58 | | 10~49명 | 7,565 | 0.50 |
| | 50~249명 | 2,576 | 0.17 | | 50~249명 | 579 | 0.04 |
| | 250~999명 | 210 | 0.01 | | 250~999명 | 14 | 0.00 |
| | 1,000명 이상 | 17 | 0.00 | | 1,000명 이상 | 1 | 0.00 |
| 숙박 및 음식점업 | 1~4명 | 95,159 | 6.32 | 기타 (공공행정, 사회보장, 행정제외) | 1~4명 | 112,338 | 7.46 |
| | 5~9명 | 46,464 | 3.08 | | 5~9명 | 54,626 | 3.63 |
| | 10~49명 | 17,294 | 1.15 | | 10~49명 | 49,606 | 3.29 |
| | 50~249명 | 678 | 0.05 | | 50~249명 | 12,373 | 0.82 |
| | 250~999명 | 51 | 0.00 | | 250~999명 | 673 | 0.04 |
| | 1,000명 이상 | 4 | 0.00 | | 1,000명 이상 | 172 | 0.01 |
| 정보통신업 | 1~4명 | 17,174 | 1.14 | | | | |
| | 5~9명 | 6,403 | 0.42 | | | | |
| | 10~49명 | 7,001 | 0.46 | | | | |
| | 50~249명 | 1,677 | 0.11 | | | | |
| | 250~999명 | 230 | 0.02 | | | | |
| | 1,000명 이상 | 25 | 0.00 | | | | |
| 총 합계 | | | | | | 1,514,478 | 100.0 |

※ 출처: 2018년 기준 전국사업체조사(통계청), 2019년 정보화통계조사(한국정보화진흥원)

## 나. 표본추출

➔ 개요 : 다단계층화계통추출법
- 업종·규모별로 2단 층화한 후 각 사업체들을 지역별로 정렬하여 계통추출

➔ 표본의 규모산정
- 허용오차에 따른 표본의 크기 결정식

$$n = \frac{\sum_{h=1}^{L} N_h p_h q_h}{ND + \sum_{h=1}^{L} w_h p_h q_h}$$

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$h$의 "공식문서화된 정보보호 정책 수립여부" 추정치

$$q_h = 1 - p_h$$

$t_{n-1,\frac{\alpha}{2}}$ : 유의수준 $\alpha$%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, %)

| 표본의 크기 | 8,400 | 8,500 | 8,600 | 8,700 | 8,800 | 8,900 | **9,000** | 9,100 |
|---|---|---|---|---|---|---|---|---|
| 표본오차 | 0.90 | 0.89 | 0.89 | 0.88 | 0.88 | 0.87 | 0.87 | 0.86 |

- 최종 표본의 크기는 표본오차가 0.87% 내외가 되도록 9,000개 내외로 결정함

➔ 표집틀(Sampling frame)
- 1차 표집틀 : 『2018년 기준 전국사업체조사』 대상 사업체
- 2차 표집틀 : 『2019년 정보화통계조사』 대상 사업체 중 1인 이상 네트워크 구축 사업체

➔ 표본할당 및 추출방법
- 멱등할당(Power allocation) : 2019년도 정보보호 실태조사 결과 중 '공식 문서화된 정보보호 정책 수립여부'에 대한 추정량을 이용하여 표본오차를 계산하고, $p=0.4$인 경우를 최종 할당으로 결정
- 절사추출 : 종사자 수가 1,000명 이상인 사업체와 250~999명인 사업체 일부 전수 조사 실시

## 7. 실 사

### 가. 실사 개요

➔ 조사기간
- 2020년 8월 3일 ~ 11월 30일 (4개월)

➔ 조사기준 시점
- 2019년 12월 31일
- 교육 실시, 예산 및 지출, 침해사고 경험은 2019년 1월 1일 ~ 12월 31일
- 현재 시스템 및 네트워크 보안점검 실시 시점, 투자/계획하는 IT 보안분야는 2020년 7월 1일

➔ 조사대상
- 네트워크에 연결된 컴퓨터 보유 사업체(종사자수 1인 이상)

➔ 조사방법
- 전문 조사원이 표본으로 선정된 사업체를 방문하여 설문에 응답을 받는 형태의 사업체 방문 면접조사

➔ 조사절차
- 면접원의 사업체 면접조사 → 지역별 실사 감독원의 관리 및 통제 → 설문지 집계 → 보완조사 및 재조사 → 최종 자료 검증

### 나. 표본 관리

➔ 본표본 관리
- 사전 추출된 사업체 9,000개를 대상으로 조사하는 것을 원칙으로 하며, 해당 사업체의 휴폐업 및 강력한 응답거부 등으로 조사가 불가능한 경우에는 동일한 업종, 규모 특성으로 추출된 예비 표본으로 대체하여 조사 진행

## 8. 자료 입력 및 처리

### 가. 자료 검증 및 대체

➪ 실사과정에서 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

➪ 분석과정에서의 자료 검증
- 동일한 업종·규모별 평균치 및 이전 조사결과와의 시계열 비교 및 검증 실시

➪ 무응답 대체
- 단위무응답 및 항목무응답 발생 시 해당 사업체 방문 및 전화 재조사를 통하여 무응답률 최소화
- 단위무응답 발생 시 예비 표본의 범위 내에서 대체하여 단위무응답 제거
- 항목무응답 발생 시 결측값을 해당 사업체 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 표본설계 된 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

- 표본설계 시에는 규모를 총 6개 층으로 분류하였으나, 결과 분석 시에는 분석의 유의성 등을 감안하여 5개 층으로 분류함
  ※ 1~4인 / 5~9인 / 10~49인 / 50~249인 / 250인 이상

➪ 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 $h$의 모집단 크기

${}_{s}n_{h}$ : 표본층 $h$의 표본 크기

${}_{s}y_{hk}$ : 표본층 $h$의 $k$번째 관찰값

$\frac{{}_{s}N_{h}}{{}_{s}n_{h}}$ : 표본층 $h$의 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)

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

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

➪ 모비율의 분산 및 표본오차 추정

- 표본층에서만 표본오차가 발생

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

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

$${}_s\hat{p}_h$$ : $h$층에서 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 | ±0.87%p (95% 신뢰수준) |
| 정보보호 정책 수립률 추정 결과 | 23.6% ± 0.87%p |

## 10. 결과 공표 및 활용분야

➪ 『2020년 정보보호 실태조사(기업부문)』 보고서는 한국정보보호산업협회 홈페이지(https://www.kisia.or.kr)를 통해 게시함

➪ 본 통계자료는 과학기술정보통신부 등 정부부처 및 연구기관의 정책수립의 기초자료 및 국제기구(OECD) 등에 제출되어 국가별 정보보호 현황 비교 등을 위한 통계자료로 활용됨

## 11. 모집단 및 표본 현황

표 1-1-7 표본 현황

(단위 : 개, %)

| 업종분류 | 규모 분류 | 컴퓨터 보유/ 네트워크 구축 사업체 | | 조사표본 사업체 | |
|---|---|---|---|---|---|
| | | 사업체 수 | 비율 | 사업체 수 | 비율 |
| 농림수산업 | 1~4명 | 985 | 0.07 | 94 | 1.04 |
| | 5~9명 | 920 | 0.06 | 38 | 0.42 |
| | 10~49명 | 997 | 0.07 | 97 | 1.08 |
| | 50~249명 | 112 | 0.01 | 73 | 0.81 |
| | 250~999명 | 8 | 0.0005 | 8 | 0.09 |
| | 1,000명 이상 | - | 0.0000 | 0 | 0.00 |
| 제조업 | 1~4명 | 92,127 | 6.11 | 158 | 1.76 |
| | 5~9명 | 60,259 | 4.00 | 154 | 1.71 |
| | 10~49명 | 44,552 | 2.96 | 287 | 3.19 |
| | 50~249명 | 8,968 | 0.60 | 277 | 3.08 |
| | 250~999명 | 805 | 0.05 | 193 | 2.14 |
| | 1,000명 이상 | 121 | 0.01 | 109 | 1.21 |
| 건설업 | 1~4명 | 28,083 | 1.86 | 128 | 1.42 |
| | 5~9명 | 19,120 | 1.27 | 94 | 1.04 |
| | 10~49명 | 20,512 | 1.36 | 200 | 2.22 |
| | 50~249명 | 2,288 | 0.15 | 167 | 1.86 |
| | 250~999명 | 313 | 0.02 | 132 | 1.47 |
| | 1,000명 이상 | 55 | 0.004 | 49 | 0.54 |
| 도매 및 소매업 | 1~4명 | 277,909 | 18.45 | 234 | 2.60 |
| | 5~9명 | 62,005 | 4.12 | 136 | 1.51 |
| | 10~49명 | 33,650 | 2.23 | 241 | 2.68 |
| | 50~249명 | 2,687 | 0.18 | 169 | 1.88 |
| | 250~999명 | 213 | 0.01 | 109 | 1.21 |
| | 1,000명 이상 | 18 | 0.001 | 19 | 0.21 |
| 운수 및 창고업 | 1~4명 | 84,887 | 5.63 | 114 | 1.27 |
| | 5~9명 | 7,721 | 0.51 | 75 | 0.83 |
| | 10~49명 | 8,807 | 0.58 | 153 | 1.70 |
| | 50~249명 | 2,576 | 0.17 | 170 | 1.89 |
| | 250~999명 | 210 | 0.01 | 111 | 1.23 |
| | 1,000명 이상 | 17 | 0.001 | 12 | 0.13 |
| 숙박 및 음식점업 | 1~4명 | 95,159 | 6.32 | 164 | 1.82 |
| | 5~9명 | 46,464 | 3.08 | 129 | 1.43 |
| | 10~49명 | 17,294 | 1.15 | 175 | 1.94 |
| | 50~249명 | 678 | 0.05 | 114 | 1.27 |
| | 250~999명 | 51 | 0.003 | 46 | 0.51 |
| | 1,000명 이상 | 4 | 0.0003 | 9 | 0.10 |

(계속→)

| | | | | | |
|---|---|---|---|---|---|
| 정보통신업 | 1~4명 | 17,174 | 1.14 | 152 | 1.69 |
| | 5~9명 | 6,403 | 0.42 | 60 | 0.67 |
| | 10~49명 | 7,001 | 0.46 | 138 | 1.53 |
| | 50~249명 | 1,677 | 0.11 | 147 | 1.63 |
| | 250~999명 | 230 | 0.02 | 116 | 1.29 |
| | 1,000명 이상 | 25 | 0.002 | 15 | 0.17 |
| 금융 및 보험업 | 1~4명 | 8,541 | 0.57 | 144 | 1.60 |
| | 5~9명 | 10,362 | 0.69 | 74 | 0.82 |
| | 10~49명 | 15,986 | 1.06 | 192 | 2.13 |
| | 50~249명 | 1,696 | 0.11 | 134 | 1.49 |
| | 250~999명 | 171 | 0.01 | 109 | 1.21 |
| | 1,000명 이상 | 32 | 0.002 | 23 | 0.26 |
| 부동산업 | 1~4명 | 79,204 | 5.26 | 178 | 1.98 |
| | 5~9명 | 9,133 | 0.61 | 69 | 0.77 |
| | 10~49명 | 5,186 | 0.34 | 122 | 1.36 |
| | 50~249명 | 326 | 0.02 | 103 | 1.14 |
| | 250~999명 | 42 | 0.003 | 36 | 0.40 |
| | 1,000명 이상 | 7 | 0.0005 | 13 | 0.14 |
| 전문, 과학 및 기술서비스업 | 1~4명 | 40,494 | 2.69 | 160 | 1.78 |
| | 5~9명 | 18,011 | 1.20 | 90 | 1.00 |
| | 10~49명 | 11,777 | 0.78 | 166 | 1.84 |
| | 50~249명 | 1,976 | 0.13 | 155 | 1.72 |
| | 250~999명 | 365 | 0.02 | 155 | 1.72 |
| | 1,000명 이상 | 48 | 0.003 | 27 | 0.30 |
| 사업시설관리, 사업지원 및 임대 서비스업 | 1~4명 | 24,255 | 1.61 | 148 | 1.64 |
| | 5~9명 | 6,477 | 0.43 | 60 | 0.67 |
| | 10~49명 | 7,202 | 0.48 | 140 | 1.56 |
| | 50~249명 | 2,168 | 0.14 | 166 | 1.84 |
| | 250~999명 | 636 | 0.04 | 137 | 1.52 |
| | 1,000명 이상 | 88 | 0.01 | 124 | 1.38 |
| 협회 및 단체, 수리 및 기타 개인서비스업 | 1~4명 | 67,114 | 4.45 | 163 | 1.81 |
| | 5~9명 | 12,149 | 0.81 | 77 | 0.86 |
| | 10~49명 | 7,565 | 0.50 | 134 | 1.49 |
| | 50~249명 | 579 | 0.04 | 96 | 1.07 |
| | 250~999명 | 14 | 0.001 | 14 | 0.16 |
| | 1,000명 이상 | 1 | 0.0001 | 1 | 0.01 |
| 기타 | 1~4명 | 112,338 | 7.46 | 145 | 1.61 |
| | 5~9명 | 54,626 | 3.63 | 65 | 0.72 |
| | 10~49명 | 49,606 | 3.29 | 135 | 1.50 |
| | 50~249명 | 12,373 | 0.82 | 119 | 1.32 |
| | 250~999명 | 673 | 0.04 | 92 | 1.02 |
| | 1,000명 이상 | 172 | 0.01 | 168 | 1.87 |
| 합계 | | 1,514,478 | 100.0 | 9000 | 100.00 |

제2장

# 조사결과 요약

# Ⅰ 정보보호 인식

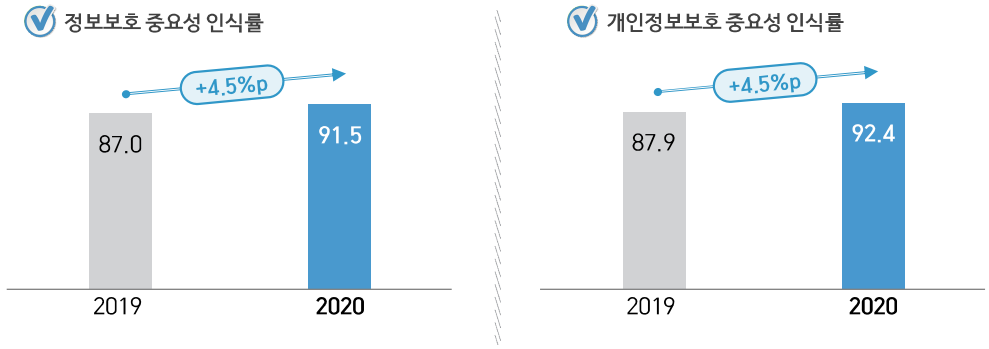
## 정보보호 중요성 인식 91.5%, 개인정보보호 중요성 인식 92.4%

▶ 네트워크에 연결된 컴퓨터 보유 사업체의 대부분이 정보보호 및 개인정보보호가 중요하다고 응답함

- '정보보호가 중요하다(중요한 편이다 + 매우 중요하다)'고 인식하는 비율은 91.5%로 나타남
- '개인정보보호가 중요하다(중요한 편이다 + 매우 중요하다)'고 인식하는 비율은 92.4%로 나타남

그림 1-2-1 정보보호 및 개인정보보호 중요성 인식률

(중요한 편이다 + 매우 중요하다, 단위 : %)



# Ⅱ 정보보호 기반 및 환경

## 1. 정보보호(개인정보보호) 정책

### 사업체의 23.6%는 '정보보호 또는 개인정보보호' 정책 수립

▶ 사업체의 23.6%는 정보보호 또는 개인정보보호 정책을 수립하는 것으로 조사되었고, 전년(23.1%) 대비 0.5%p 증가함

▶ 규모별로 '종사자수 250인 이상(96.6%)' 사업체의 정책 수립률이 가장 높게 나타남
또한, '종사자수 50-249인(76.4%, 3.1%p↑)', '종사자수 250인 이상(96.6%, 9.5%p↑)'에서 정책 수립률이 전년 대비 증가함

그림 1-2-2 정보보호(개인정보보호) 정책 수립률

(중요한 편이다 + 매우 중요하다, 단위 : %)

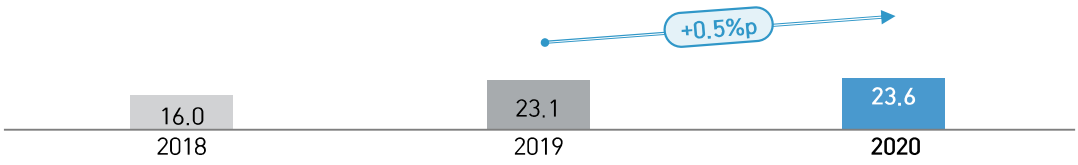
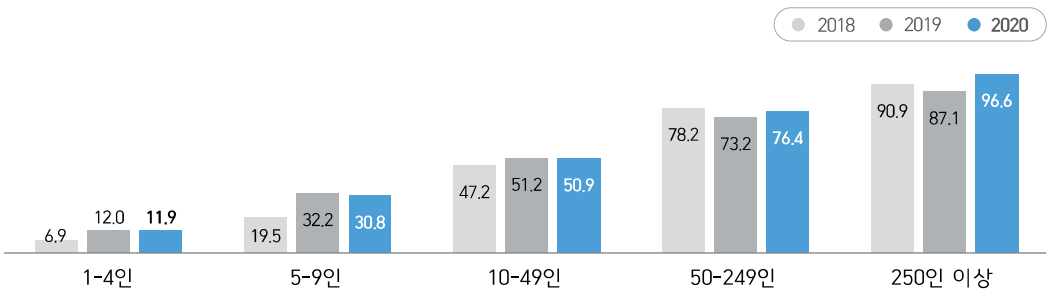



그림 1-2-3 규모별 정보보호(개인정보보호) 정책 수립률

(중요한 편이다 + 매우 중요하다, 단위 : %)



# 2. 정보보호(개인정보보호) 조직

**'정보보호 또는 개인정보보호' 조직 보유 13.4%, 전년 대비 1.1%p 증가**

- 공식적인 정보보호 또는 개인정보보호 조직을 보유한 사업체의 비율은 13.4%로, 전년(12.3%) 대비 1.1%p 증가함
- 규모별로 '종사자수 250인 이상(87.7%)' 사업체의 조직 보유율이 가장 높게 나타남

그림 1-2-4 정보보호(개인정보보호) 조직 보유율

(단위 : %)

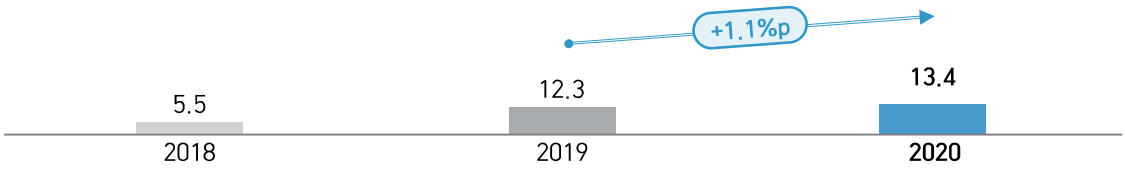
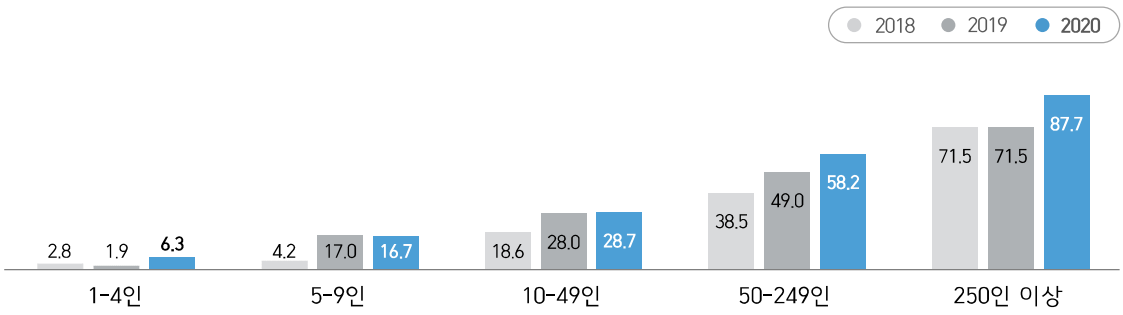



그림 1-2-5 규모별 정보보호(개인정보보호) 조직 보유율

(단위 : %)



# 3. 정보보호(개인정보보호) 교육

## 사업체의 36.0%는 '정보보호 또는 개인정보보호' 교육 실시

- 2019년 1년간 임직원 대상으로 정보보호 또는 개인정보보호 교육을 실시한 비율은 36.0%로 전년(29.4%) 대비 6.6%p 증가함
- 규모별로 '종사자수 250인 이상(96.3%)' 사업체의 교육 실시율이 가장 높게 나타남

그림 1-2-6 정보보호(개인정보보호) 교육 실시율

(단위 : %)

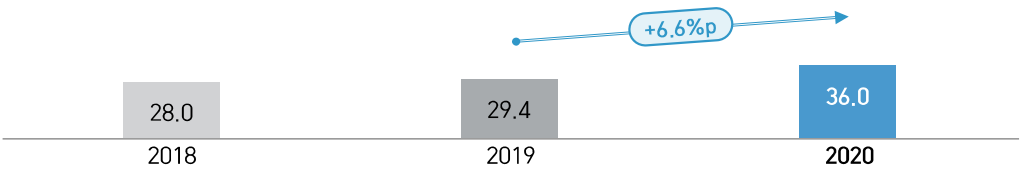
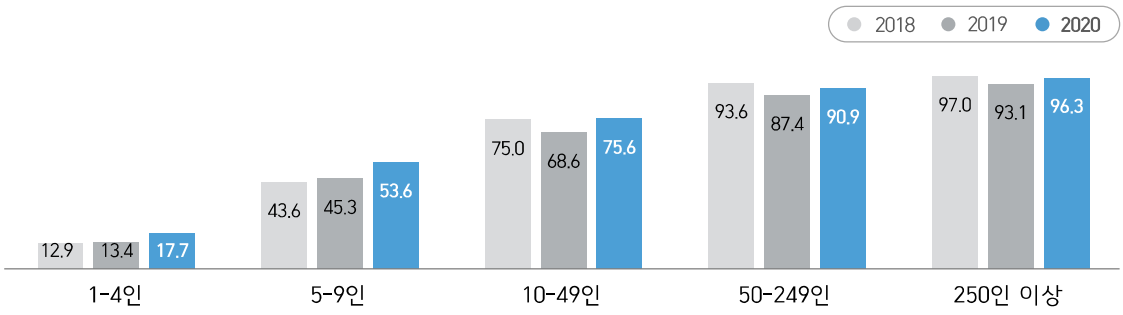



그림 1-2-7 규모별 정보보호(개인정보보호) 교육 실시율

(단위 : %)



# 4. 정보보호(개인정보보호) 예산

**'정보보호 또는 개인정보보호' 예산 편성 61.8%, 전년 대비 29.5%p 증가**

- 2019년 1년 간 사업체의 61.8%는 IT 예산 중 정보보호 또는 개인정보보호 예산을 편성함
- IT 예산 중 정보보호 또는 개인정보보호 예산이 차지하는 비중은 '1% 미만(49.4%)'이 가장 높았으며, 전년(20.2%) 대비 29.2%p 증가함
- 반면, '5% 이상'이라고 응답한 비율은 전년(2.9%)대비 1.2%p 감소함

그림 1-2-8 정보보호(개인정보보호) 예산 편성률

(단위 : %)

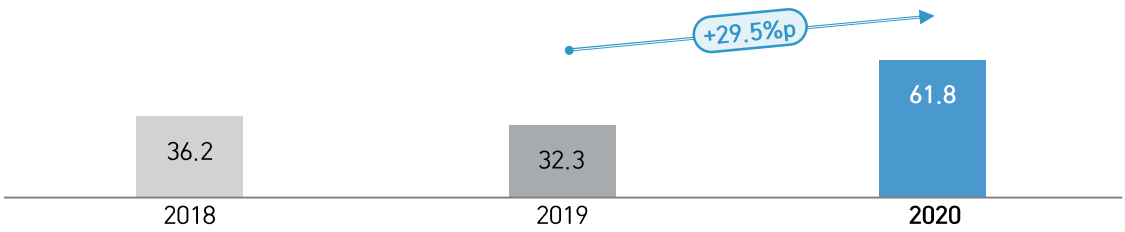
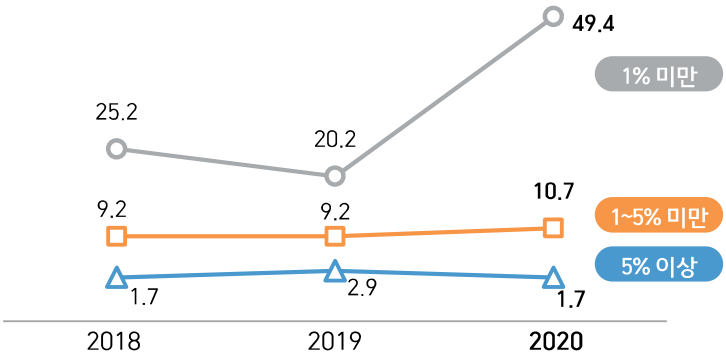



그림 1-2-9 IT 예산 중 정보보호(개인정보보호) 예산 비중

(단위 : %)



# Ⅲ 침해사고 예방

## 1. 정보보호 제품 및 서비스

### 가. 정보보호 제품 이용

**'정보보호 제품 이용' 99.7%, 전년 대비 6.2%p증가**

- 사업체의 99.7%는 정보보호 제품을 이용하는 것으로 조사되었고, 전년(93.5%) 대비 6.2%p 증가함
- 제품군별로는 정보보안 제품 중 '네트워크 보안'이 98.2%로 가장 높았고, 물리보안 제품 중에서는 '영상정보 처리기기(CCTV)'가 65.1%로 높게 나타남

그림 1-2-10 정보보호 제품 이용률

(단위 : %)

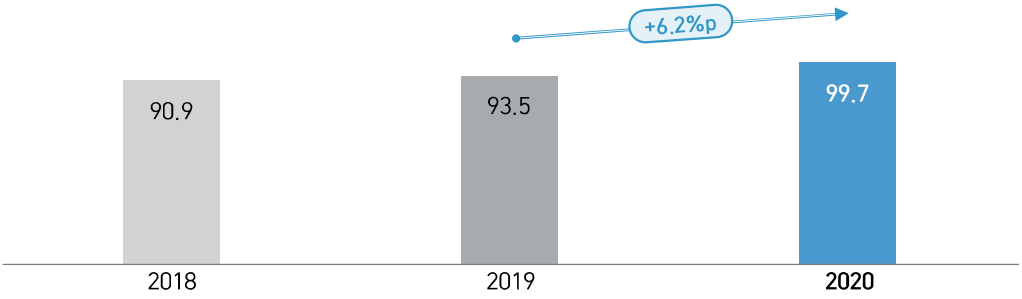
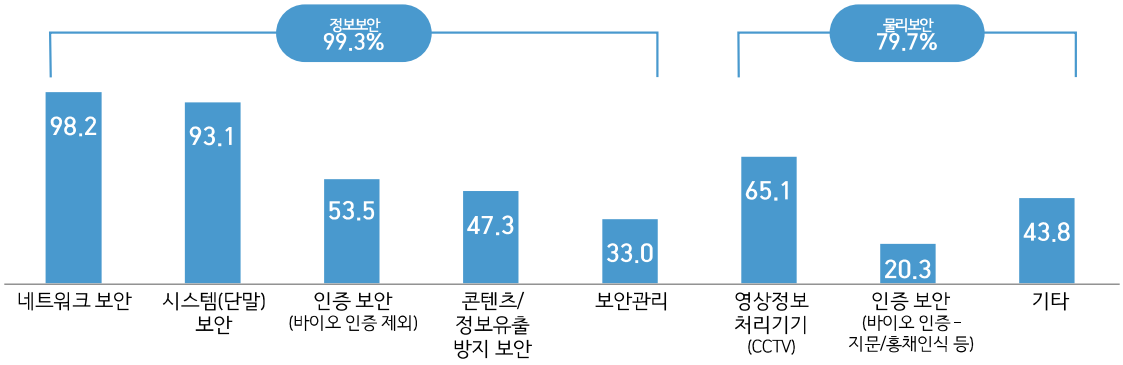



그림 1-2-11 정보보호 제품군별 이용률 (복수응답)

(단위 : %)



## 나. 정보보호 서비스 이용

**'정보보호 서비스 이용' 69.5%, 전년 대비 27.0%p 증가**

- 사업체의 69.5%는 '정보보호 서비스를 이용'하는 것으로 조사되었고, 전년(42.5%) 대비 27.0%p 증가함
- 서비스 유형별로는 '인증서 서비스'가 45.0%로 가장 많았고, 다음으로 '유지관리/보안성 지속 서비스(41.6%)', '교육/훈련(30.7%)' 등의 순으로 조사됨

그림 1-2-12 정보보호 서비스 이용률

(단위 : %)

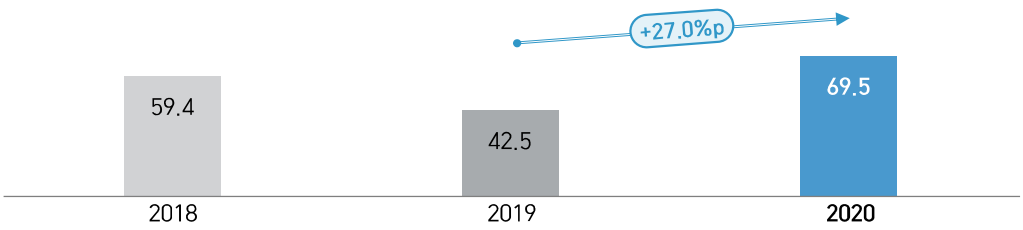



그림 1-2-13 정보보호 서비스 유형별 이용률 (복수응답)

(단위 : %)


※ 2020년 설문 변경사항: ('19년) 인증 서비스 → ('20년) 인증서 서비스

# 2. 정보보호 관리

## 가. 시스템 및 네트워크 보안점검

**사업체의 97.8%는 '시스템 및 네트워크 보안점검' 실시**

▶ '시스템 및 네트워크에 대한 보안점검' 실시율은 97.8%로 전년(85.1%) 대비 12.7%p 증가함

▶ 유형별로는 'PC의 취약점' 점검률이 99.8%로 가장 높고, 다음으로 '서버 운영체제(Windows, MAC, OS, 리눅스 등)(95.8%)', '네트워크장비(라우터, 스위치 등)(75.5%)' 등의 순으로 조사됨

그림 1-2-14 시스템 및 네트워크 보안점검 실시율

(단위 : %)

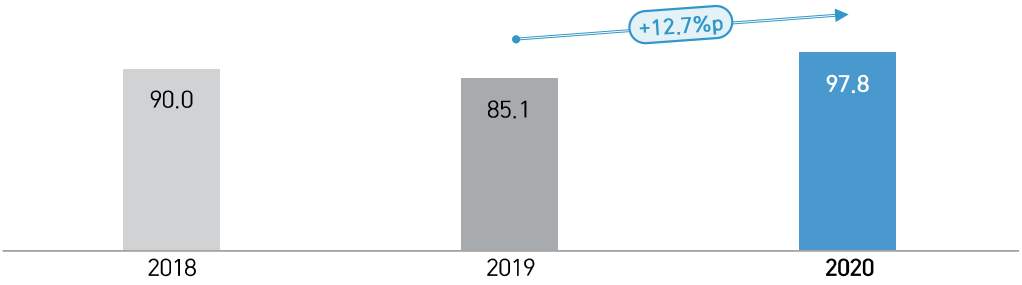
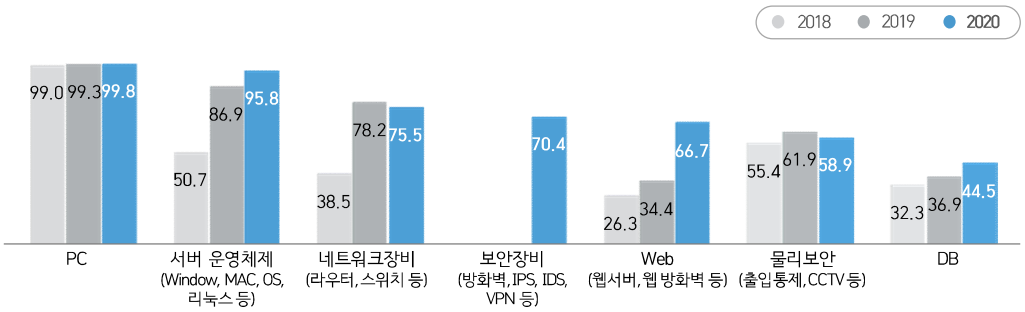



그림 1-2-15 유형별 취약점 점검률 (복수응답) - 보안점검 실시 사업체

(단위 : %)




※ 2020년 설문 변경사항: '보안 장비(방화벽, IPS, IDS, VPN 등)' 추가

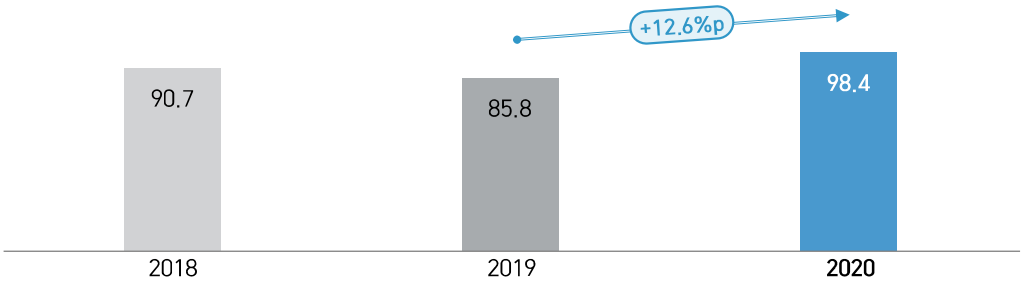
## 나. 보안패치 적용

**'보안패치' 적용 98.4%, 전년 대비 12.6%p 증가**

- 사업체의 98.4%는 PC나 서버에 보안패치를 적용하는 것으로 조사되었고, 전년(85.8%) 대비 12.6%p 증가함
- 보안패치 유형별로는 '정보보호 시스템'에 적용하는 비율이 97.9%로 가장 높았고, 다음으로 '직원 PC(97.6%)' 등의 순으로 조사됨

그림 1-2-16 보안패치 적용률

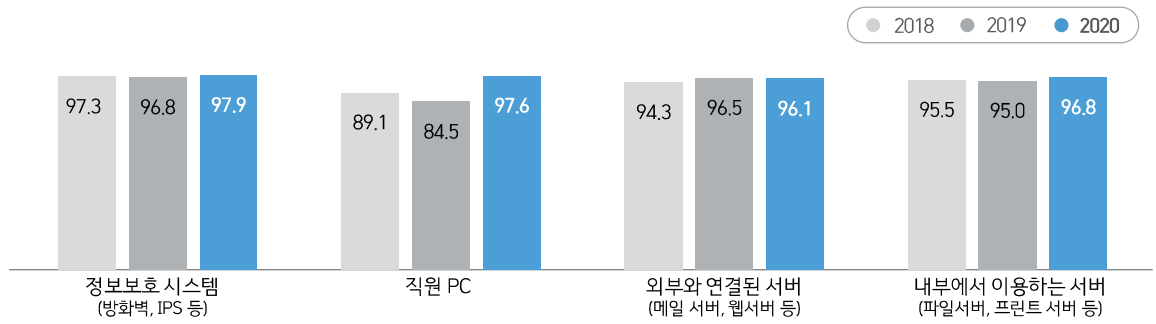
(단위 : %)




※ 보안패치 적용 : 자동 업데이트 설정 + 수동 업데이트 실시 + 문제 발생 시에만 업데이트 실시

그림 1-2-17 보안패치 유형별 적용률 (복수응답) - 항목별 제품 보유 사업체

(단위 : %)




※ 보안패치 적용 : 자동 업데이트 설정 + 수동 업데이트 실시 + 문제 발생 시에만 업데이트 실시

## 다. 시스템 로그 및 데이터 백업 실시

### '시스템 로그 또는 데이터 백업' 실시 47.3%

- 사업체의 47.3%는 시스템 로그 또는 중요 데이터를 백업하는 것으로 나타났고, 전년(52.6%) 대비 5.3%p 감소함
- 유형별로 '시스템 로그 백업' 실시율은 28.4%, '중요 데이터 백업'은 45.1%로 나타남

그림 1-2-18 백업 실시율

(단위 : %)

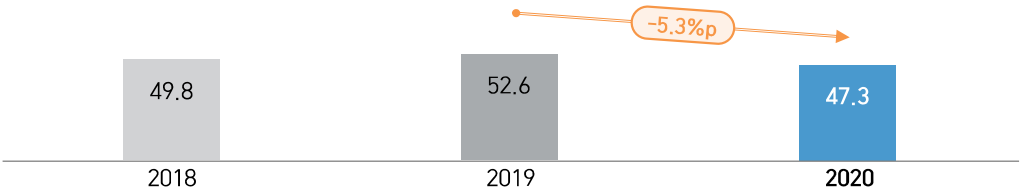
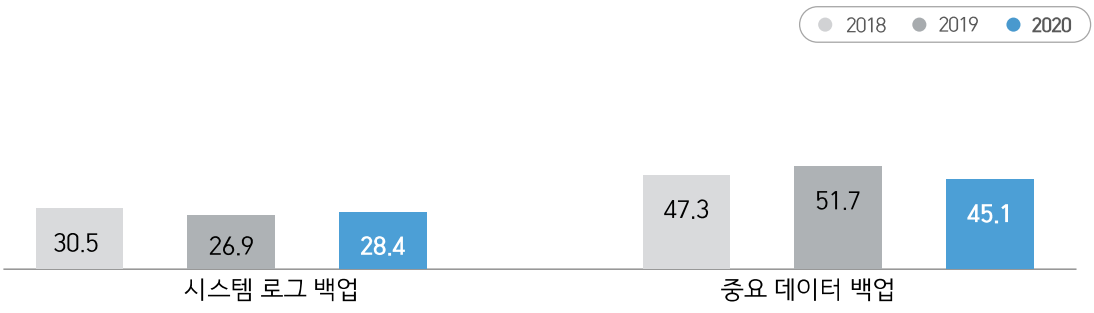



그림 1-2-19 백업 유형별 실시율 (복수응답)

(단위 : %)



# Ⅳ 침해사고 대응

## 1. 침해사고 경험

### 사업체의 2.0%가 침해사고 경험

▶ 2019년 1년간 사업체의 2.0%는 해킹, 악성코드, DDoS, 랜섬웨어 등 침해사고를 경험함
- 침해사고 피해 심각성 정도는 '경미한 피해(64.6%)'가 가장 많았음

▶ 침해사고 경험 유형으로는 '랜섬웨어'가 59.8%로 가장 많았고, 다음으로 '악성코드(컴퓨터 바이러스, 웜, 트로이잔, APT공격 등)에 의한 공격(42.7%)', '사내 데이터나 전산 시스템에 대한 외부로부터의 비인가 접근(해킹)(6.6%)' 등의 순임

그림 1-2-20 침해사고 경험 및 피해 심각성 정도

(단위 : %)

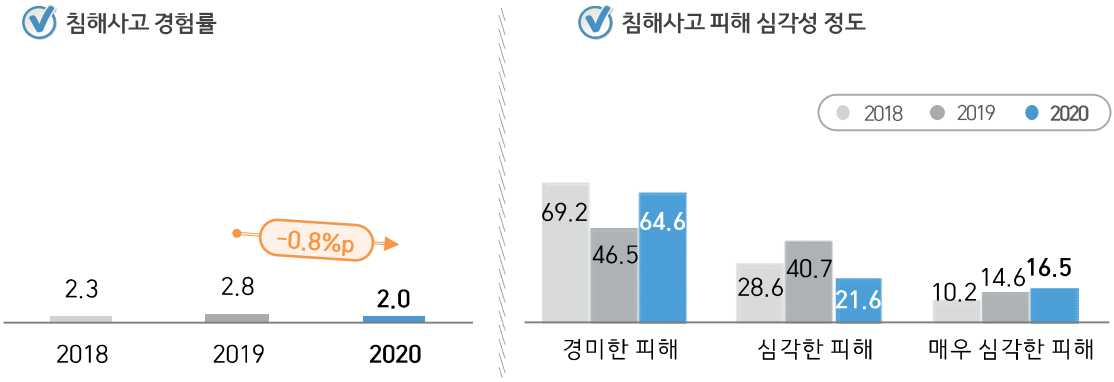
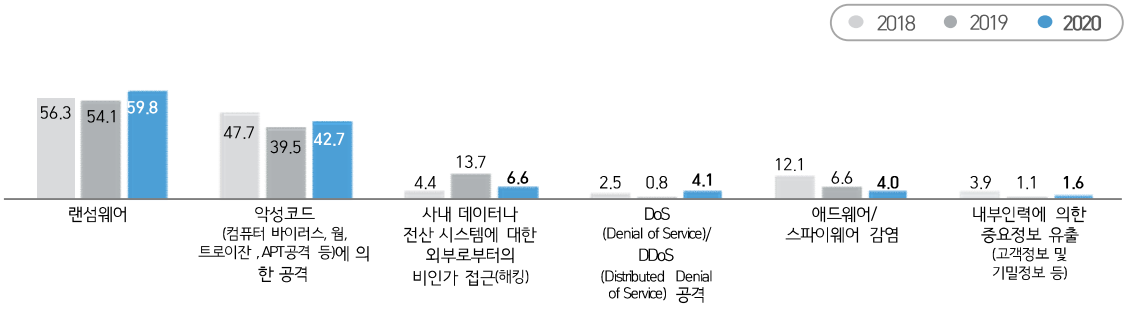



그림 1-2-21 침해사고 경험 유형 (복수응답) - 침해사고 경험 사업체

(단위 : %)



# 2. 침해사고 대응

**침해사고 대응활동 수행 27.0%, 전년 대비 0.8%p 증가**

- 사업체의 27.0%는 침해사고에 대응하기 위한 활동을 수행하는 것으로 조사되었고, 수행률은 전년(26.2%) 대비 0.8%p 증가함
- 대응활동 유형으로는 '침해사고 대응 계획 수립'이 15.8%로 가장 많았고, 다음으로 '침해사고 발생 또는 발생 징후 인지 시 대처를 위한 긴급연락체계 구축(14.7%)', '침해사고 대응 활동을 외부 전문기관에 위탁(6.0%)' 등의 순임

그림 1-2-22 침해사고 대응활동 수행률

(단위 : %)

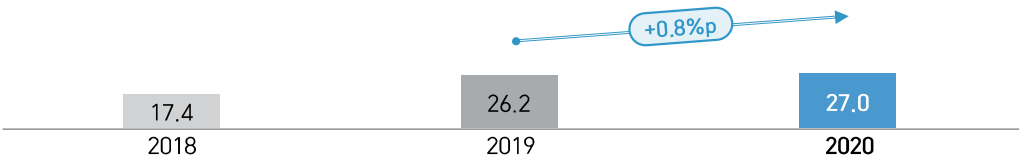
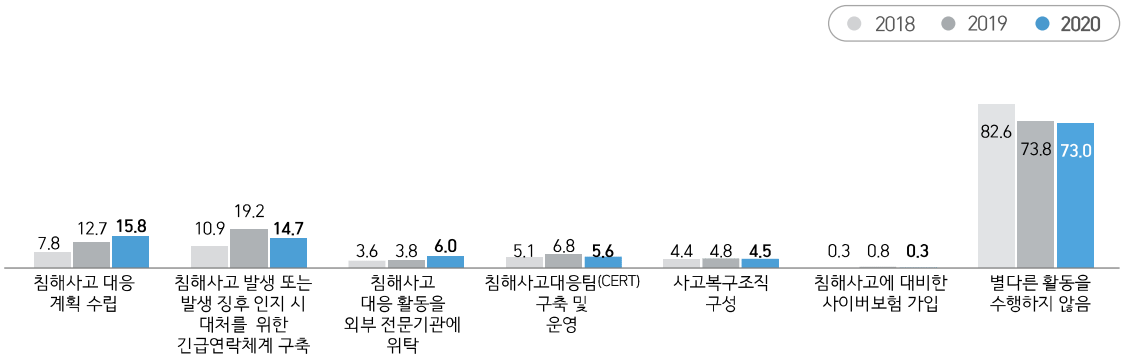



그림 1-2-23 침해사고 대응활동 수행 (복수응답)

(단위 : %)



# V 개인정보보호

## 1. 개인정보 수집 및 이용

**고객의 개인정보 수집(51.6%) 및 이용(49.9%)은 전년 대비 증가**

- 사업체의 51.6%는 고객의 개인정보를 온라인 또는 오프라인으로 수집하는 것으로 조사되었고, 개인정보 수집률은 전년(39.5%) 대비 12.1%p 증가함
- 고객의 개인정보를 온라인 또는 오프라인으로 이용하는 비율은 사업체의 49.9%로 전년(38.4%) 대비 11.5%p 증가함

그림 1-2-24 고객 개인정보 수집률

(단위 : %)

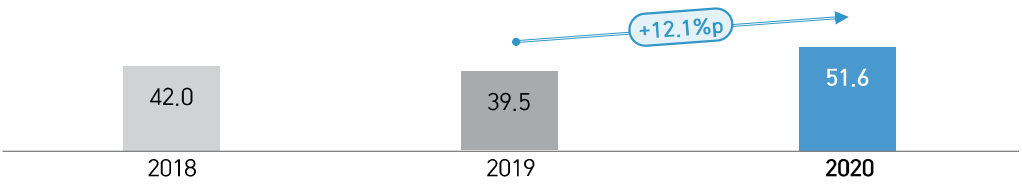
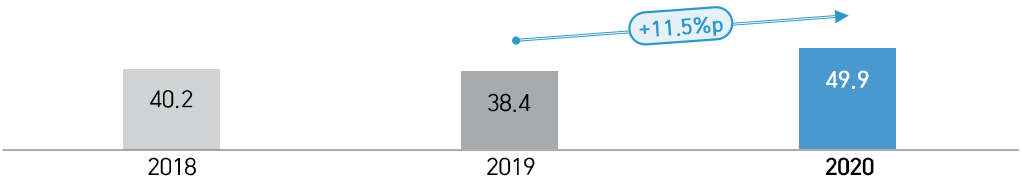



그림 1-2-25 고객 개인정보 이용률

(단위 : %)



# 2. 개인정보 침해사고 예방

## 가. 예방 및 사후처리 조치

**개인정보 침해사고 예방·사후처리를 위한 조치 97.2%, 전년 대비 11.0%p 증가**

- 개인정보 침해사고 예방 및 사후 처리를 위한 관리적 조치 시행률은 97.2%로 전년(86.2%) 대비 11.0%p 증가함
- 관리적 조치로는 '개인정보 침해사고 예방에 관한 매뉴얼 수립'이 70.6%로 가장 많았고, 다음으로 '개인정보 침해사고 사후 처리방침 수립(57.8%)'이 많은 것으로 나타남

그림 1-2-26 개인정보 침해사고 예방·사후처리 관리적 조치 시행률 - 온라인으로 개인정보 수집 사업체

(단위 : %)

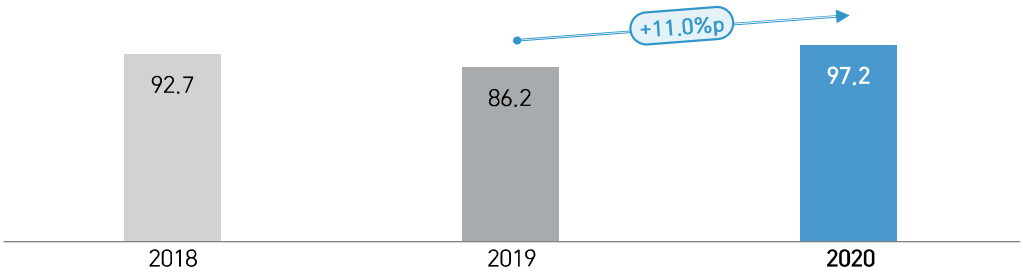
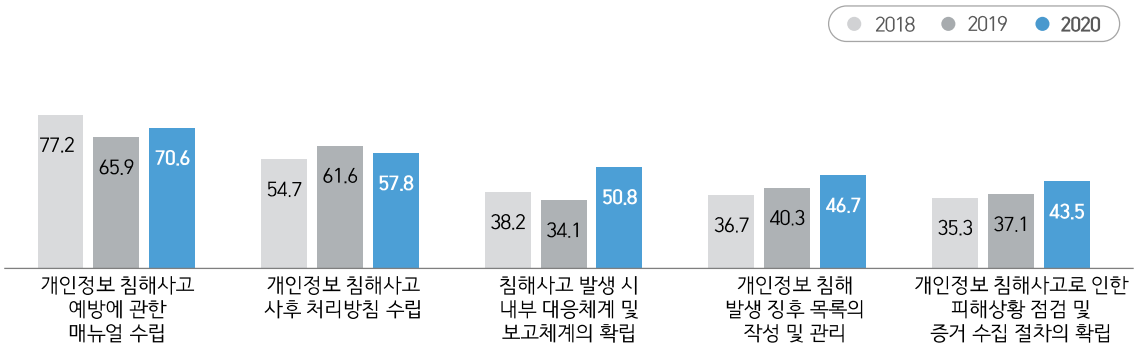



그림 1-2-27 개인정보 침해사고 예방·사후처리 관리적 조치 - 온라인으로 개인정보 수집 사업체

(단위 : %)



## 나. 기술적 조치

**개인정보 기술적 조치 도입 98.4%, 전년 대비 5.8%p 증가**

- 개인정보의 안전한 처리를 위한 기술적 조치 시행률은 98.4%로 전년(92.6%) 대비 5.8%p 증가함
- 기술적 조치로는 '백신 소프트웨어의 설치·운영 등 컴퓨터 바이러스에 의한 침해 방지 조치'가 84.6%로 가장 높게 조사되었고, 매년 증가하는 추세임

그림 1-2-28 개인정보 침해사고 예방 기술적 조치 시행률 - 온라인으로 개인정보 수집 사업체

(단위 : %)

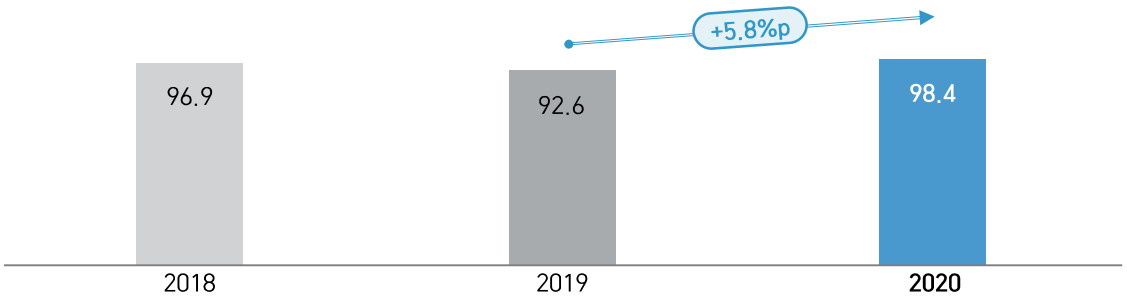
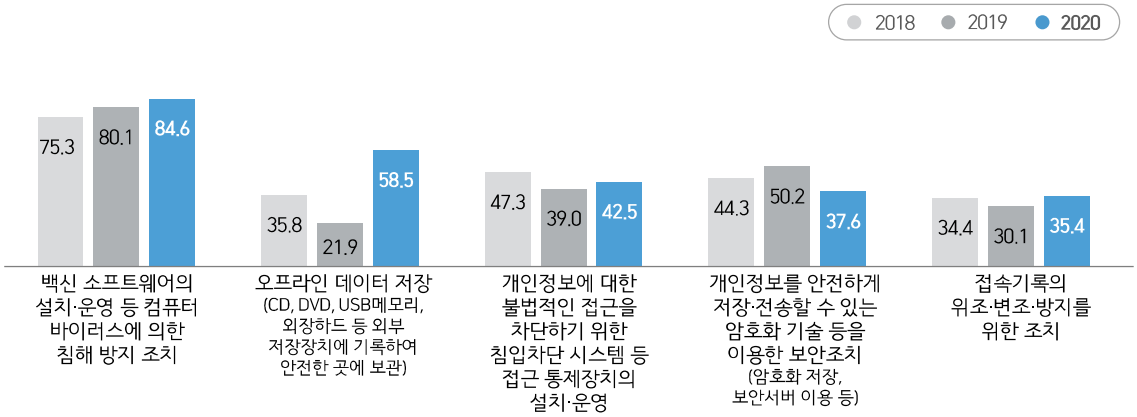



그림 1-2-29 개인정보 침해사고 예방 기술적 조치 - 온라인으로 개인정보 수집 사업체

(단위 : %)



# Ⅵ 주요 서비스별 정보보호

## 1. 무선랜

**무선랜 구축 및 운영 71.2%, 전년 대비 3.2%p 감소**

- 사업체의 71.2%는 사내 무선랜(Wi-Fi)을 구축하여 운영하고 있는 것으로 조사되었고, 전년(74.4%) 대비 3.2%p 감소함
- 사업체의 60.5%는 '무선공유기(AP)를 통한 악성코드 감염'을 가장 우려하는 것으로 나타났고, 다음으로 '무선공유기(AP)를 DDoS 등 공격도구로 악용(52.4%)'하는 것을 우려함

그림 1-2-30 무선랜 구축 및 운영률

(단위 : %)

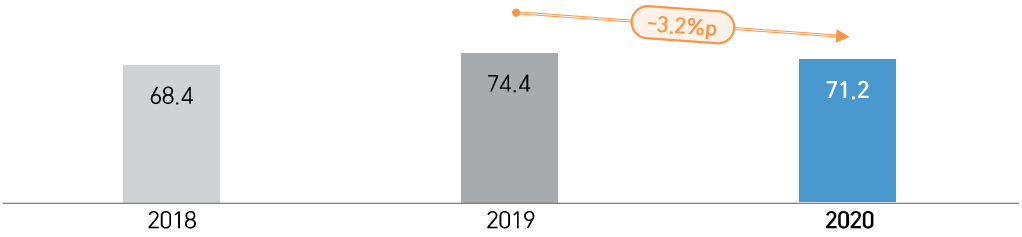
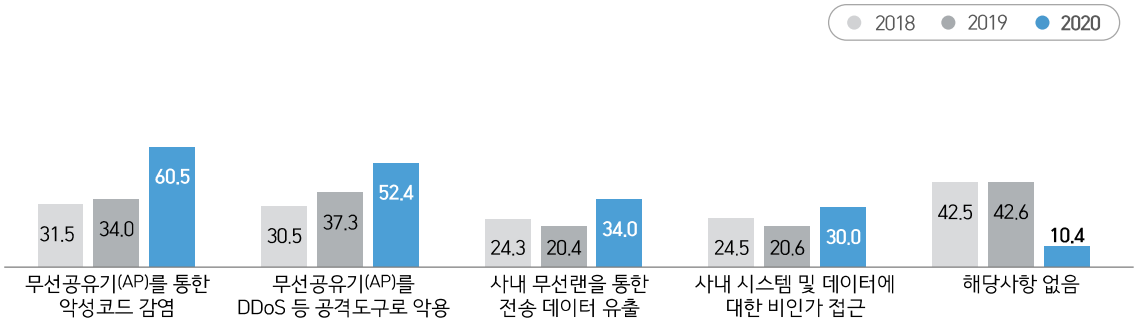



그림 1-2-31 무선랜 보안 우려사항 (2가지) - 무선랜 구축 사업체

(단위 : %)



# 2. 클라우드

## '클라우드 서비스' 이용 7.0%

- 사업체의 7.0%는 클라우드 서비스를 이용하는 것으로 조사되었고, 전년(8.4%)과 비슷한 수준임
- 사업체의 66.5%는 '데이터 위탁저장에 따른 정보유출'을 가장 우려하는 것으로 나타났고, 다음으로 '사용단말의 다양화로 인한 정보유출(64.4%)'을 우려함

그림 1-2-32 클라우드 서비스 이용률

(단위 : %)

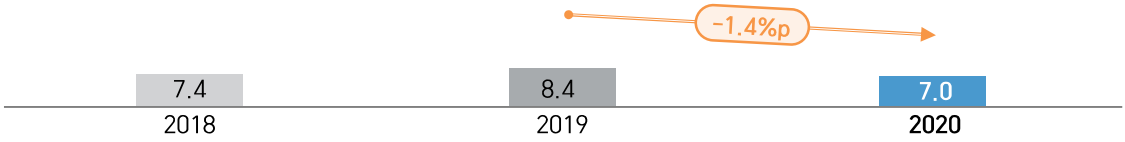
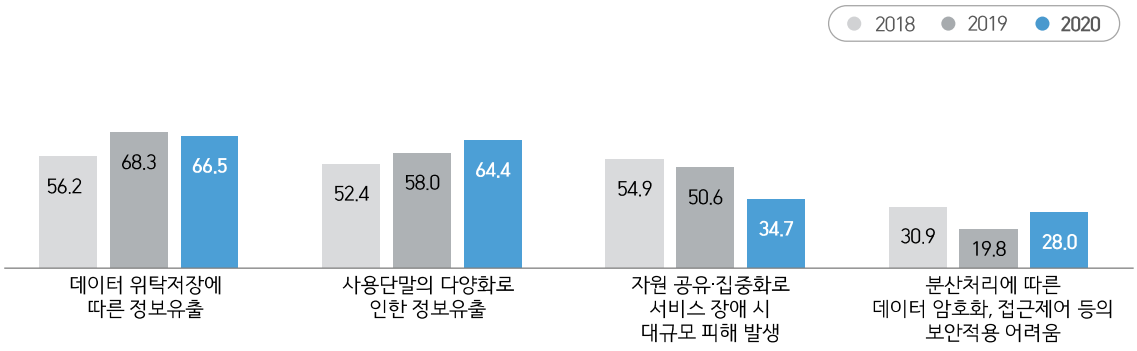



그림 1-2-33 클라우드 서비스 관련 보안 우려사항 (2가지)

(단위 : %)



# 3. 사물인터넷(IoT)

**'사물인터넷(IoT) 제품·서비스' 이용 12.7%, 전년 대비 8.8%p 감소**

- 사물인터넷(IoT) 제품 및 서비스 이용률은 12.7%로 전년(21.5%) 대비 8.8%p 감소함
- 사업체의 57.1%는 '기기 분실·도난'을 가장 우려하는 것으로 나타났고, 다음으로 '해킹 및 악성코드 감염(56.1%)', '정보 유출(48.3%)' 등의 순임

그림 1-2-34 사물인터넷(IoT) 제품·서비스 이용률

(단위 : %)

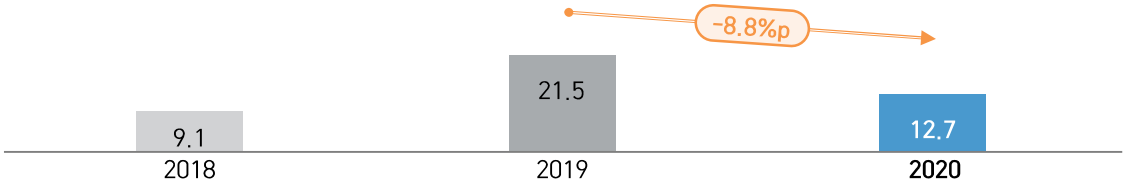
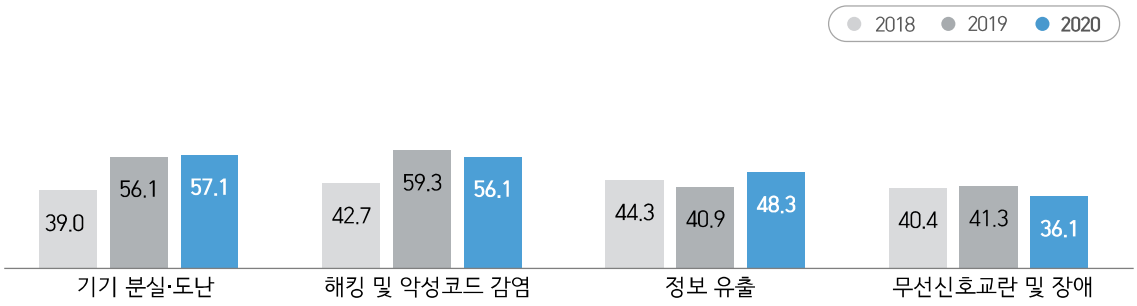



그림 1-2-35 사물인터넷(IoT) 관련 보안 우려사항

(단위 : %)



# 4. 사이버(정보보호 및 개인정보보호) 보험

**'사이버 보험' 이용 0.4%, 향후 가입 또는 유지 계획 0.7%**

▶ 사이버(정보보호 및 개인정보보호) 보험 이용률은 0.4%로 전년(0.8%) 대비 0.4%p 감소함
- 사업체의 0.7%는 사이버 보험을 향후 가입 또는 유지할 계획으로 조사되었고, 전년(1.2%) 대비 0.5%p 감소함

▶ 사이버(정보보호 및 개인정보보호) 보험 가입 시, '개인정보 유출 사고 발생 시 대응 비용(조사, 통지, 법률자문)(92.5%)'이 가장 보장받고 싶은 사항으로 조사되었고, 다음으로 '개인정보 유출 사고 발생 시 배상 비용(76.4%)' 등의 순으로 높게 나타남

그림 1-2-36 사이버 보험 이용 및 향후 가입(유지) 계획

(단위 : %)

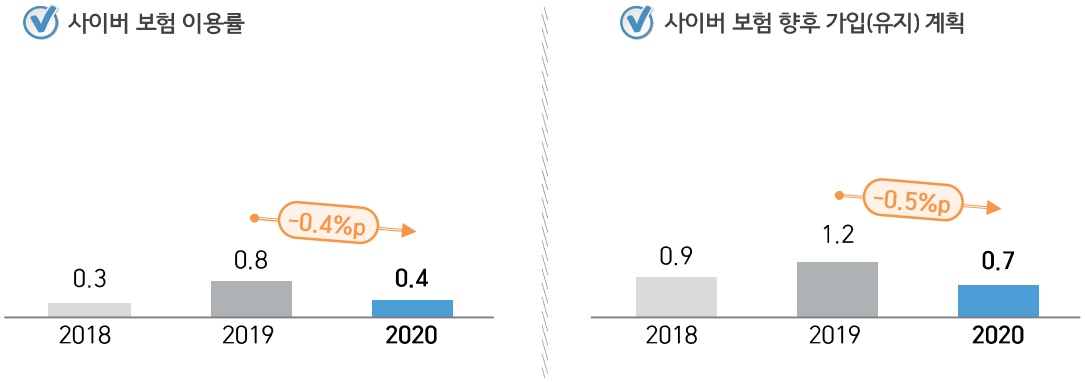
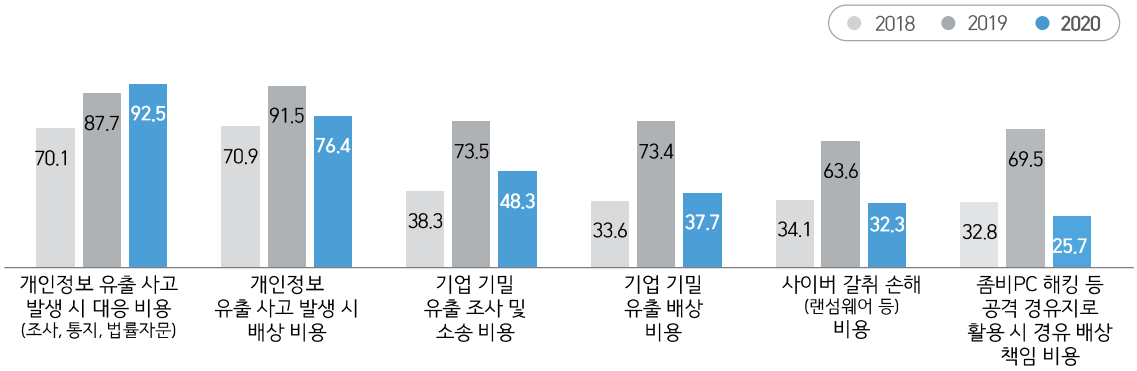



그림 1-2-37 사이버 보험 보장 희망 항목 (복수응답) - 향후 가입 계획 사업체

(단위 : %)



제3장

# 조사결과

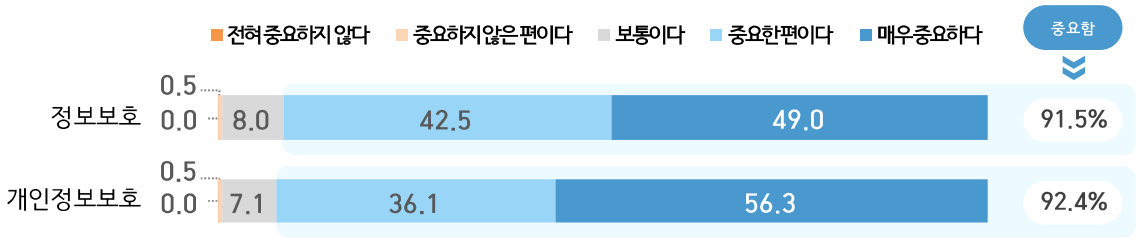
# Ⅰ 정보보호 인식

## 1. 정보보호 및 개인정보보호 중요성 인식

국내 사업체 중 91.5%는 정보보호가 중요하다(중요한 편이다 + 매우 중요하다)고 응답했으며, 개인정보보호가 중요하다(중요한 편이다 + 매우 중요하다)고 생각하는 사업체의 비율은 92.4%로 나타났다.

그림 1-3-1 정보보호 및 개인정보보호 중요성 인식

(중요한 편이다 + 매우 중요하다, 단위 : %)

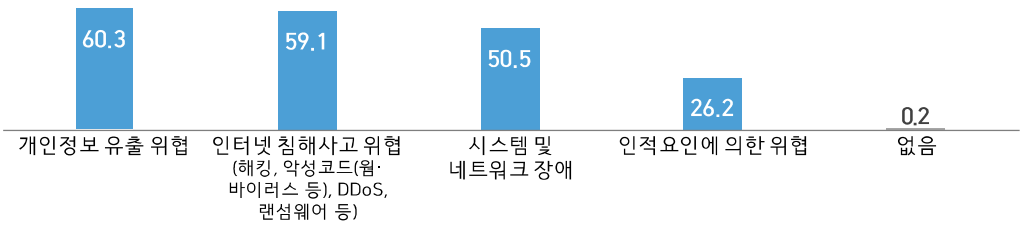



## 2. 정보보호 위협요인

국내 사업체가 우려하는 정보보호 위협요인으로는 '개인정보 유출 위협'이 60.3%로 가장 높게 나타났고, 다음으로 '인터넷 침해사고 위협(해킹, 악성코드, DDoS, 랜섬웨어 등)(59.1%)', '시스템 및 네트워크 장애(50.5%)' 등의 순으로 조사되었다.

그림 1-3-2 정보보호 위협요인 (2가지)

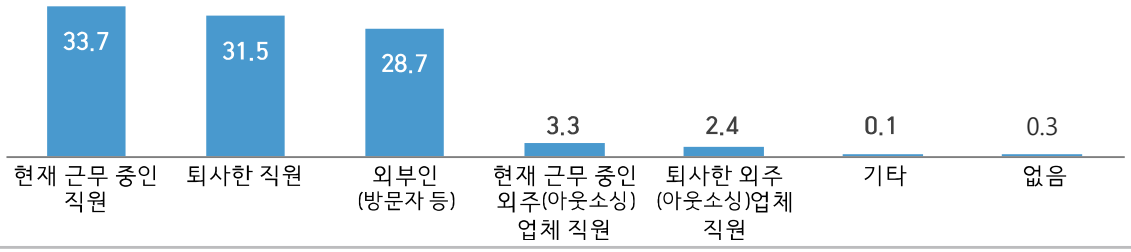
(단위 : %)



정보보호 인적 위협요인 중에서는 '현재 근무 중인 직원'이 33.7%로 가장 높게 나타났고, '퇴사한 직원(31.5%)', '외부인(방문자 등)(28.7%)' 등의 순으로 조사되었다.

그림 1-3-3 정보보호 인적 위협요인

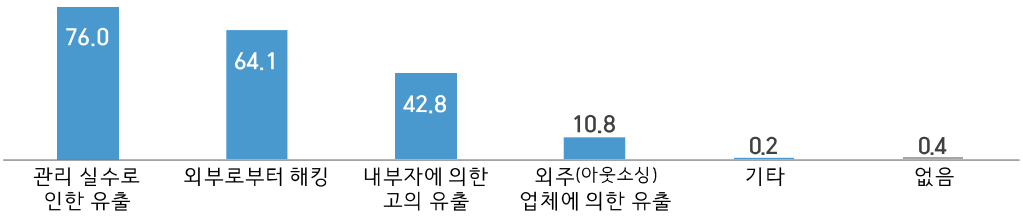
(단위 : %)




우려하는 개인정보 유출요인으로는 '관리 실수로 인한 유출'이 76.0%로 가장 높게 나타났고, 다음으로 '외부로부터의 해킹(64.1%)', '내부자에 의한 고의 유출(42.8%)' 등의 순으로 나타났다.

그림 1-3-4 우려하는 개인정보 유출요인 (2가지)

(단위 : %)

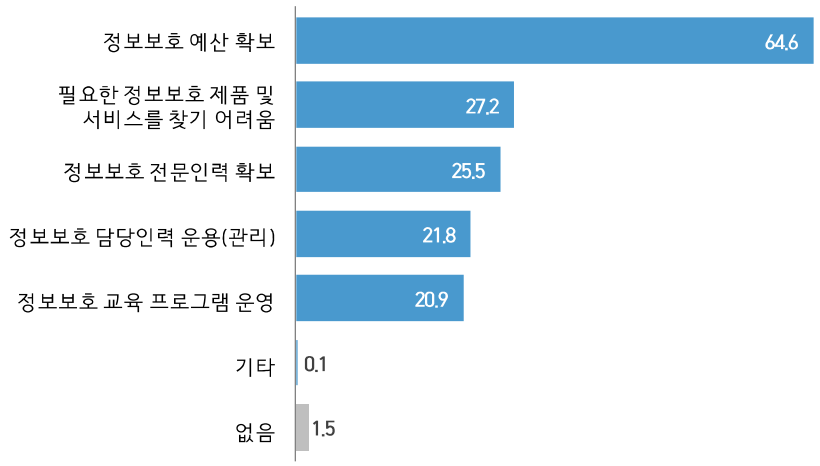


## 3. 정보보호 애로사항

국내 사업체가 정보보호에 대해 어려움을 느끼는 사항으로는 '정보보호 예산 확보'가 64.6%로 가장 높게 나타났고, 다음으로 '필요한 정보보호 제품 및 서비스를 찾기 어려움(27.2%)', '정보보호 전문인력 확보(25.5%)' 등의 순이었다.

그림 1-3-5 정보보호 애로사항 (복수응답)

(단위 : %)



# Ⅱ 정보보호 기반 및 환경

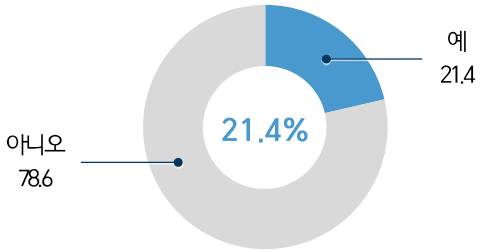
## 1. 정보보호 정책

### 가. 정보보호 정책 수립

국내 사업체 중 21.4%가 공식문서로 정보보호 정책을 수립한 것으로 나타났다.

그림 1-3-6 정보보호 정책 수립

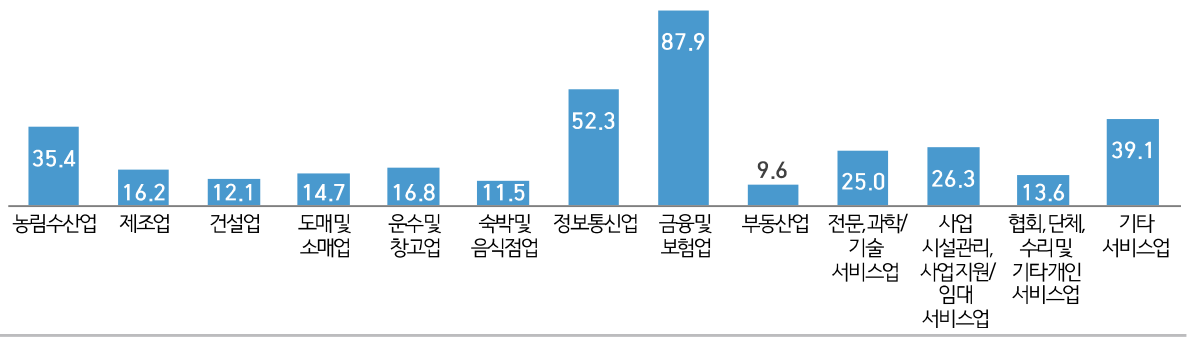
(단위 : %)




업종별 분석 결과, '금융 및 보험업'이 87.9%로 가장 높게 나타났고, 다음으로 '정보통신업(52.3%)', '기타 서비스업(39.1%)' 등의 순으로 조사되었다.

그림 1-3-7 업종별 정보보호 정책 수립

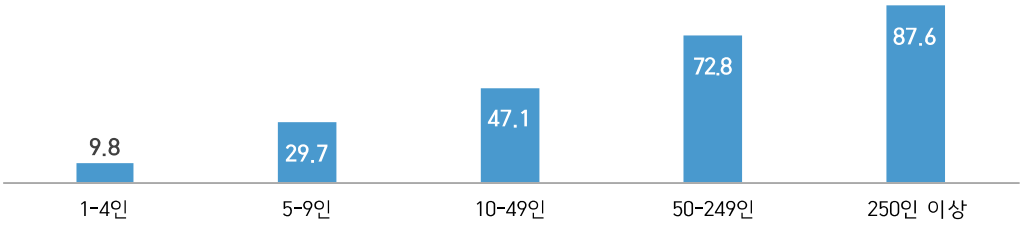
(단위 : %)



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

그림 1-3-8 규모별 정보보호 정책 수립

(단위 : %)

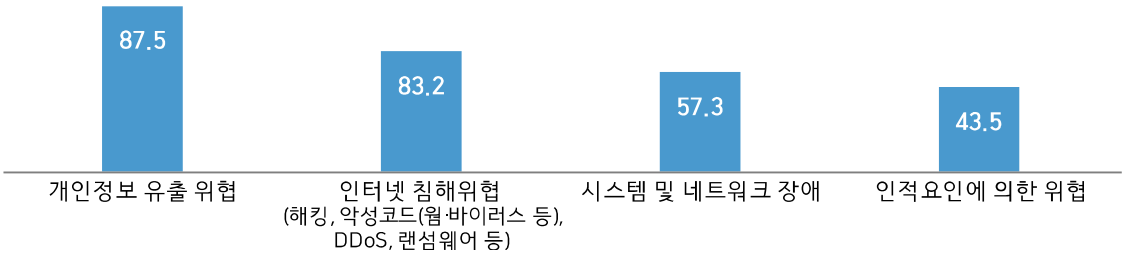



## 나. 정보보호 정책 포함 위협요소

정보보호 정책에 포함하고 있는 위협요소로는 '개인정보 유출 위협'이 87.5%로 가장 높게 나타났고, 다음으로 '인터넷 침해위협(해킹, 악성코드(웜·바이러스 등), DDoS, 랜섬웨어 등)(83.2%)', '시스템 및 네트워크 장애(57.3%)' 등의 순으로 조사되었다.

그림 1-3-9 정보보호 정책 포함 위협요소 (복수응답) - 정보보호 정책 보유 사업체

(단위 : %)

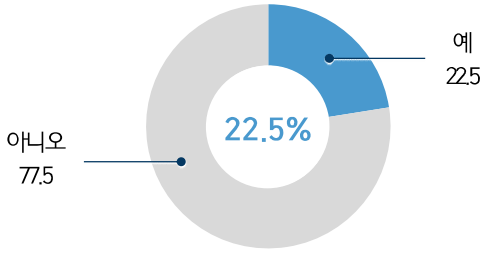


## 다. 개인정보보호 정책 수립

국내 사업체 중 22.5%가 공식문서로 개인정보보호 정책을 수립한 것으로 나타났다.

그림 1-3-10 개인정보보호 정책 수립

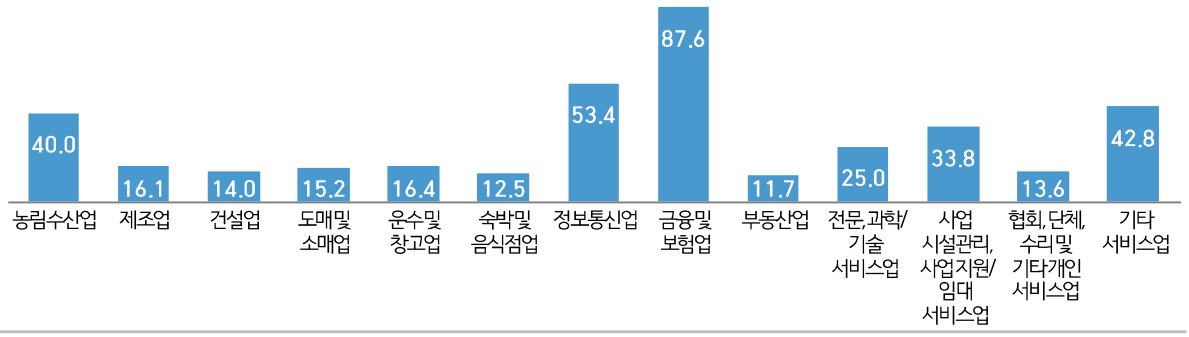
(단위 : %)




업종별 분석 결과, '금융 및 보험업'이 87.6%로 가장 높게 나타났고, 다음으로 '정보통신업(53.4%)', '기타 서비스업(42.8%)' 등의 순으로 조사되었다.

그림 1-3-11 업종별 개인정보보호 정책 수립

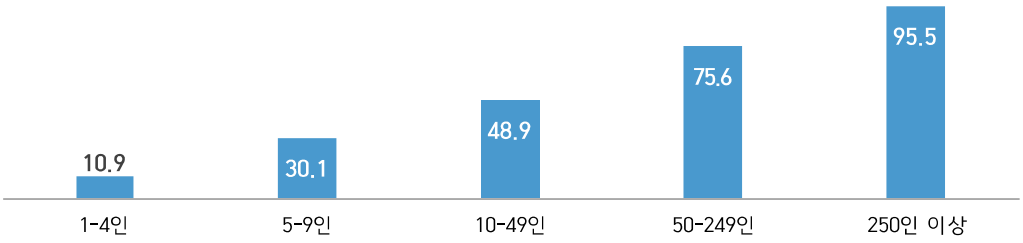
(단위 : %)



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

그림 1-3-12 규모별 개인정보보호 정책 수립

(단위 : %)



▶ 참고 **공식문서로 정보보호 또는 개인정보보호 정책을 수립한 경우**

그림 1-3-13 정보보호(개인정보보호) 정책 수립

(단위 : %)

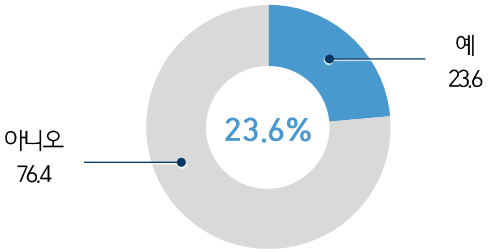



그림 1-3-14 업종별 정보보호(개인정보보호) 정책 수립

(단위 : %)

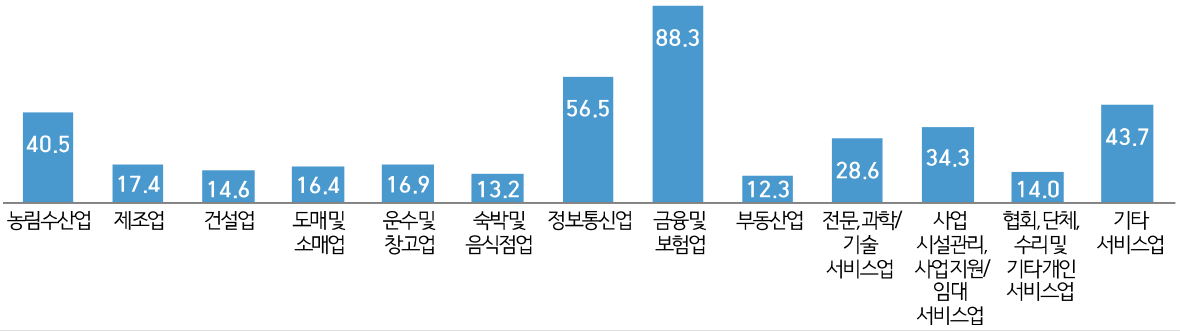
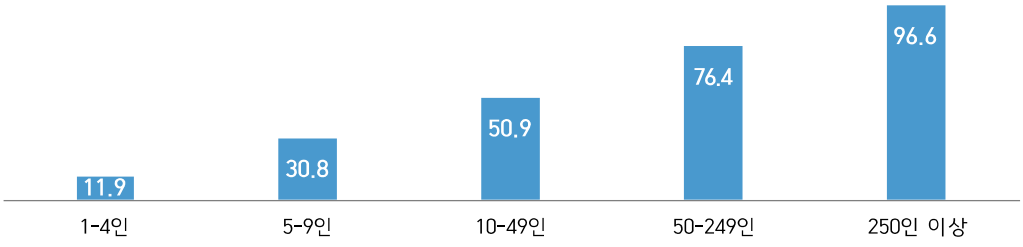



그림 1-3-15 규모별 정보보호(개인정보보호) 정책 수립

(단위 : %)



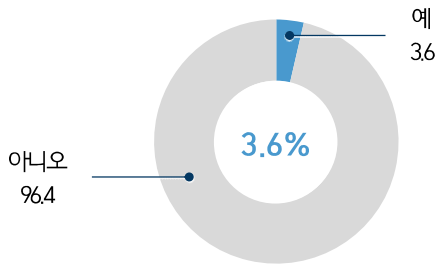
# 2. 정보보호 조직

## 가. 정보보호 전담조직 운영

국내 사업체 중 3.6%가 공식적인 정보보호 전담조직을 운영하고 있는 것으로 나타났다.

그림 1-3-16 정보보호 전담조직 운영

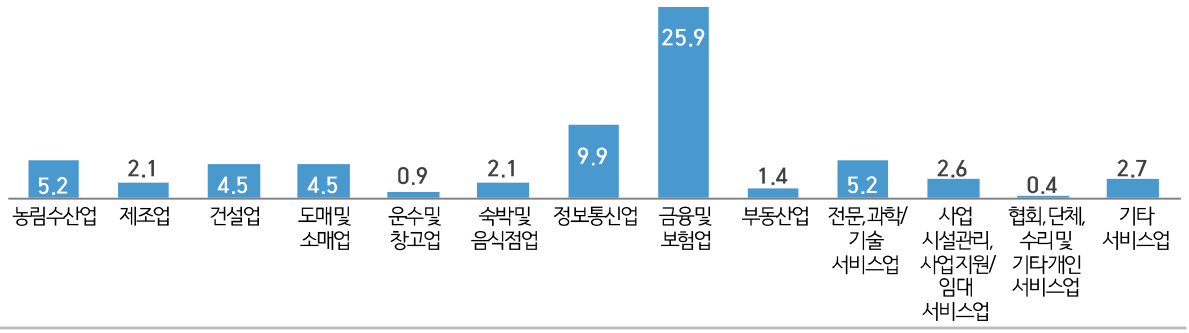
(단위 : %)




업종별 분석 결과, '금융 및 보험업'이 25.9%로 가장 높게 나타났고, 다음으로 '정보통신업(9.9%)', '농림 수산업(5.2%)', '전문, 과학/기술 서비스업(5.2%)' 등의 순으로 조사되었다.

그림 1-3-17 업종별 정보보호 전담조직 운영

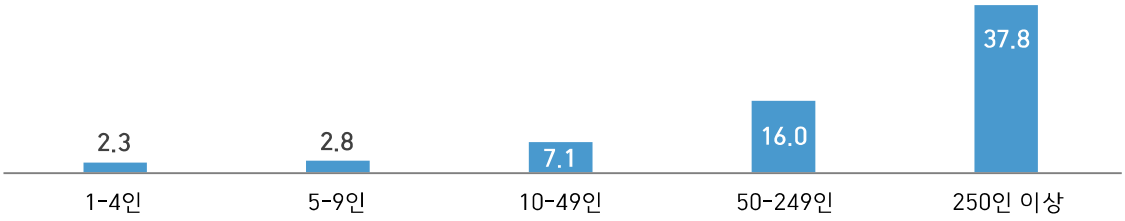
(단위 : %)



규모별 분석 결과, 종사자 수가 많을수록 정보보호 전담조직 운영률이 높은 것으로 나타났다.

그림 1-3-18 규모별 정보보호 전담조직 운영

(단위 : %)

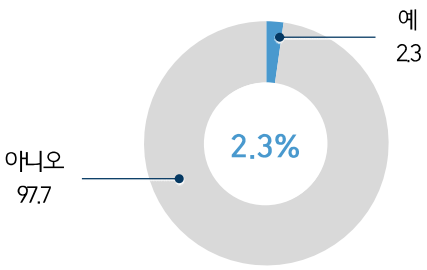



## 나. 개인정보보호 전담조직 운영

국내 사업체 중 2.3%가 공식적인 개인정보보호 전담조직을 운영하고 있는 것으로 나타났다.

그림 1-3-19 개인정보보호 전담조직 운영

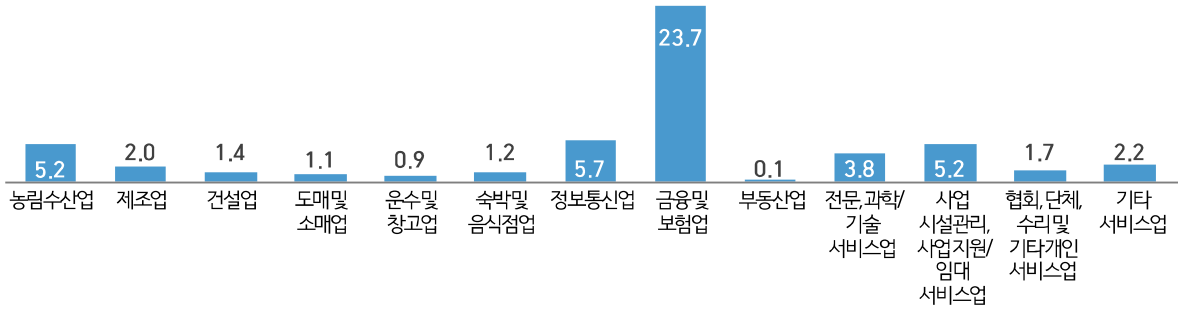
(단위 : %)



업종별 분석 결과, '금융 및 보험업'이 23.7%로 가장 높게 나타났고, 다음으로 '정보통신업(5.7%)', '농림수산업(5.2%)', '사업 시설관리, 사업지원/임대서비스업(5.2%)' 등의 순으로 조사되었다.

그림 1-3-20 업종별 개인정보보호 전담조직 운영

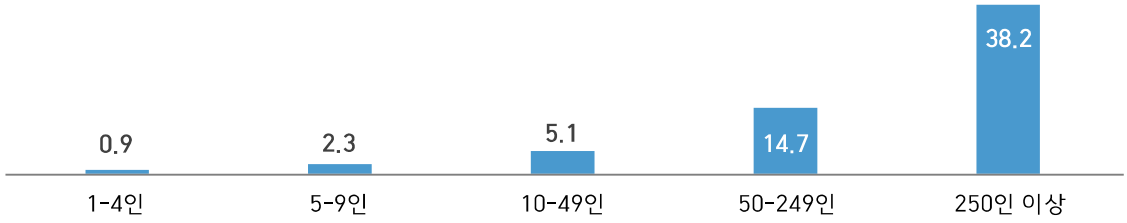
(단위 : %)




규모별 분석 결과, 종사자 수가 많을수록 개인정보보호 전담조직 운영률이 높은 것으로 나타났다.

그림 1-3-21 규모별 개인정보보호 전담조직 운영

(단위 : %)

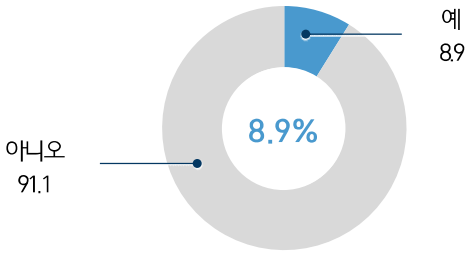


## 다. 정보보호와 개인정보보호 조직 공동 운영

국내 사업체 중 8.9%가 정보보호와 개인정보보호 조직을 공동으로 운영하고 있는 것으로 나타났다.

그림 1-3-22 정보보호와 개인정보보호 조직 공동 운영

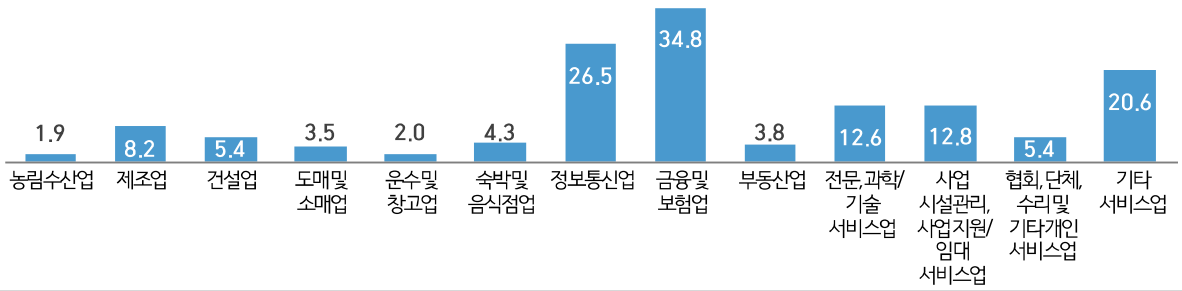
(단위 : %)




업종별 분석 결과, '금융 및 보험업'이 34.8%로 가장 높게 나타났고, 다음으로 '정보통신업(26.5%)', '기타 서비스업(20.6%)' 등의 순으로 조사되었다.

그림 1-3-23 업종별 정보보호와 개인정보보호 조직 공동 운영

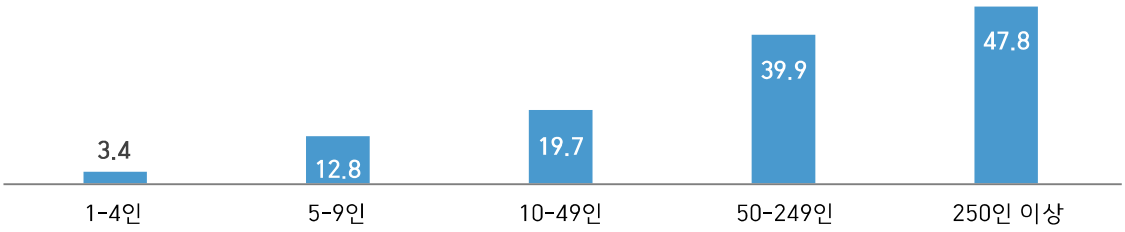
(단위 : %)



규모별 분석 결과, 종사자 수가 많을수록 정보보호와 개인정보보호 조직 공동 운영률이 높은 것으로 나타났다.

그림 1-3-24 규모별 정보보호와 개인정보보호 조직 공동 운영

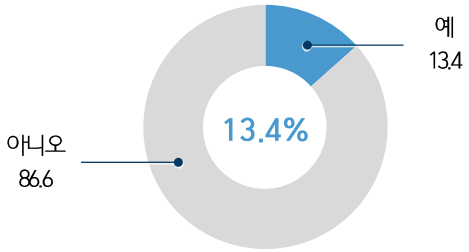
(단위 : %)



## ▶ 참고 공식적으로 정보보호 또는 개인정보보호 조직을 운영하는 경우

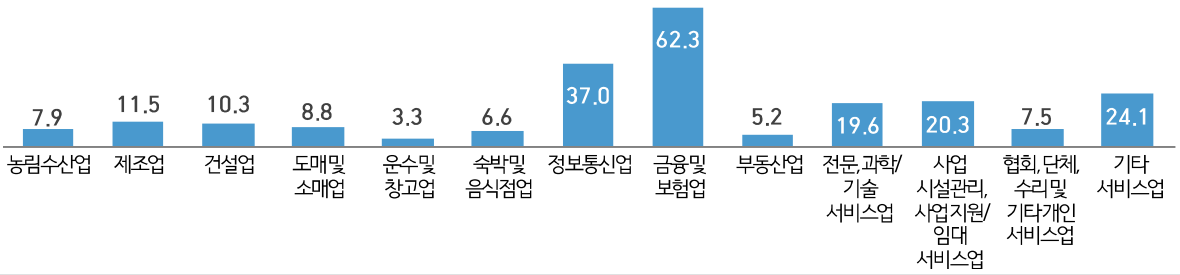
### 그림 1-3-25 정보보호(개인정보보호) 조직 운영

(단위 : %)



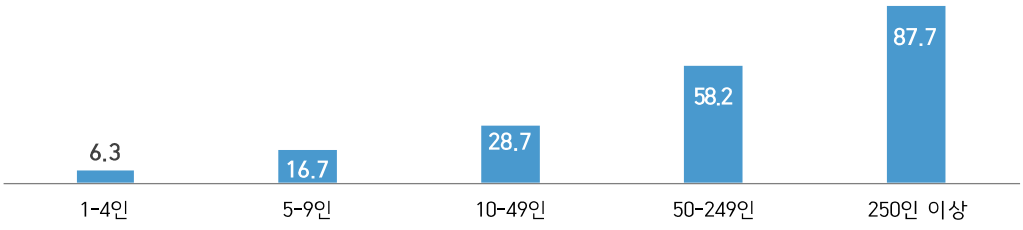

### 그림 1-3-26 업종별 정보보호(개인정보보호) 조직 운영

(단위 : %)




### 그림 1-3-27 규모별 정보보호(개인정보보호) 조직 운영

(단위 : %)



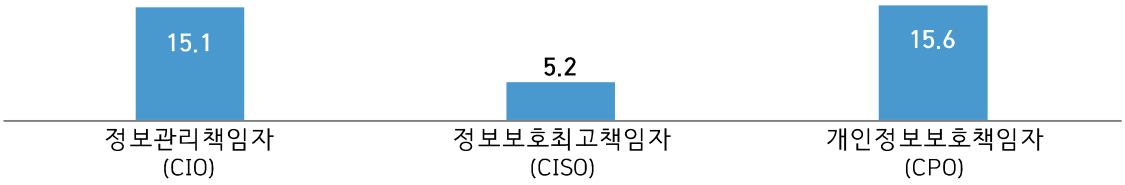
# 3. 정보보호 인력

## 가. 정보보호 관련 책임자

정보보호 관련 책임자가 임명된 국내 사업체의 비율은 '정보관리책임자(Chief Information Officer)' 15.1%, '정보보호최고책임자(Chief Information Security Officer)' 5.2%, '개인정보보호책임자(Chief Privacy Officer)' 15.6%로 각각 나타났다.

그림 1-3-28 정보보호 관련 책임자 임명 (복수응답)

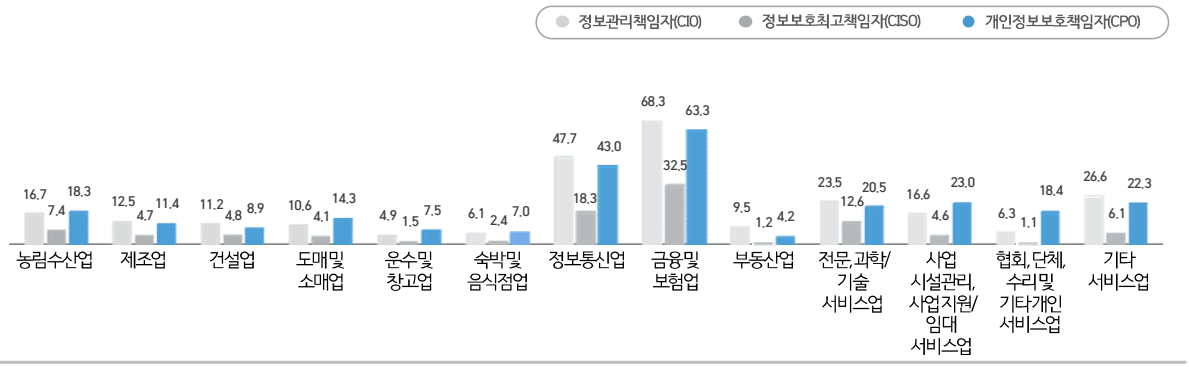
(단위 : %)




업종별 분석 결과, '금융 및 보험업'이 '정보관리책임자(CIO)' 68.3%, '정보보호최고책임자(CISO)' 32.5%, '개인정보보호책임자(CPO)' 63.3%로 전 업종 중 가장 높은 것으로 나타났다.

그림 1-3-29 업종별 정보보호 관련 책임자 임명 (복수응답)

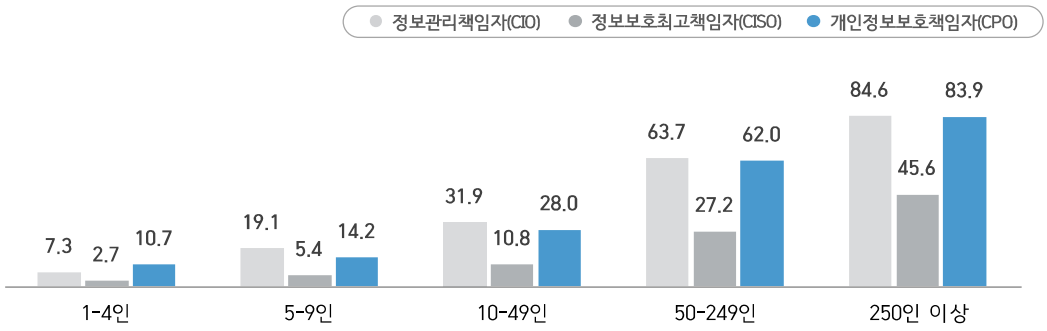
(단위 : %)



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

그림 1-3-30 규모별 정보보호 관련 책임자 임명 (복수응답)

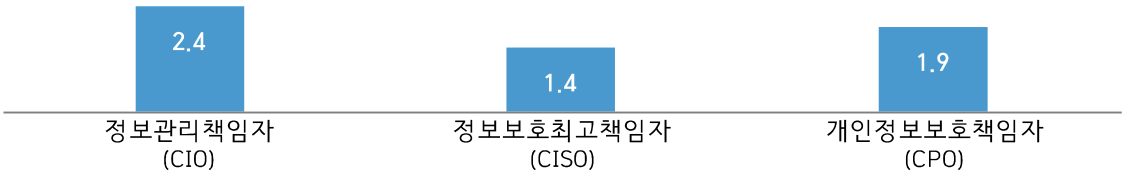
(단위 : %)




정보보호 관련 책임자 전담 비율은 '정보관리책임자(CIO)' 2.4%, '정보보호최고책임자(CISO)' 1.4%, '개인정보보호책임자(CPO)' 1.9%로 각각 나타났다.

그림 1-3-31 정보보호 관련 책임자 전담 (복수응답)

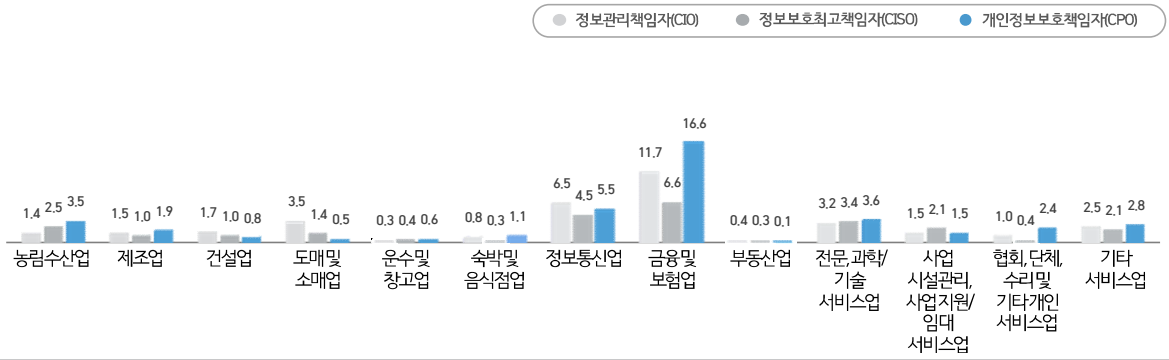
(단위 : %)



업종별 분석 결과, '금융 및 보험업'이 '정보관리책임자(CIO)' 11.7%, '정보보호최고책임자(CISO)' 6.6%, '개인정보보호책임자(CPO)' 16.6%로 전 업종 중 가장 높은 것으로 나타났다.

그림 1-3-32 업종별 정보보호 관련 책임자 전담 (복수응답)

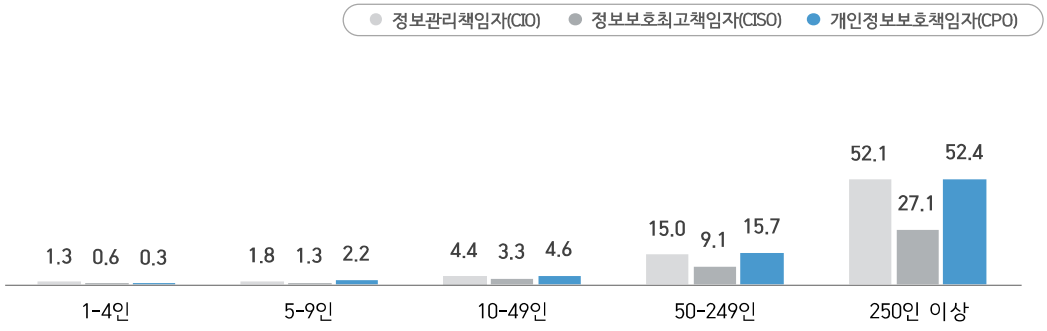
(단위 : %)




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

그림 1-3-33 규모별 정보보호 관련 책임자 전담 (복수응답)

(단위 : %)



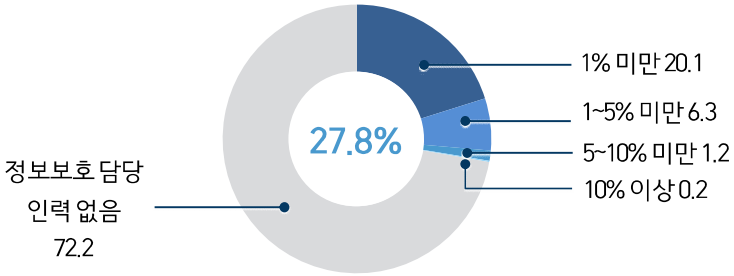
## 나. IT 인력 중 정보보호 담당 인력 비중

IT인력 중 정보보호를 담당하는 인력을 보유한 사업체는 27.8%로 나타났다.

IT인력 중 정보보호를 담당하는 인력이 차지하는 비중을 살펴보면, '1% 미만'이 20.1%로 가장 높았고, 다음으로 '1~5% 미만(6.3%)', '5~10% 미만(1.2%)' 등의 순으로 나타났다.

그림 1-3-34 IT 인력 중 정보보호 담당 인력 비중

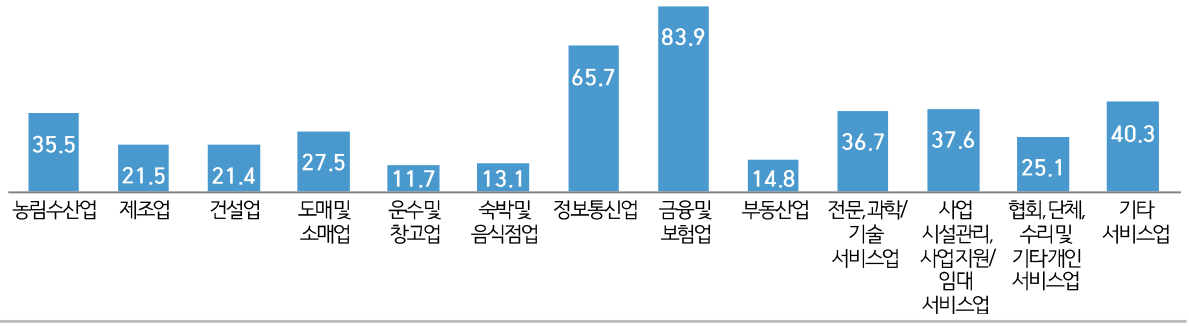
(단위 : %)




업종별 분석 결과, '금융 및 보험업(83.9%)', '정보 통신업(65.7%)', '기타 서비스업(40.3%)' 등의 순으로 조사되었다.

그림 1-3-35 업종별 IT 인력 중 정보보호 담당 인력 배정

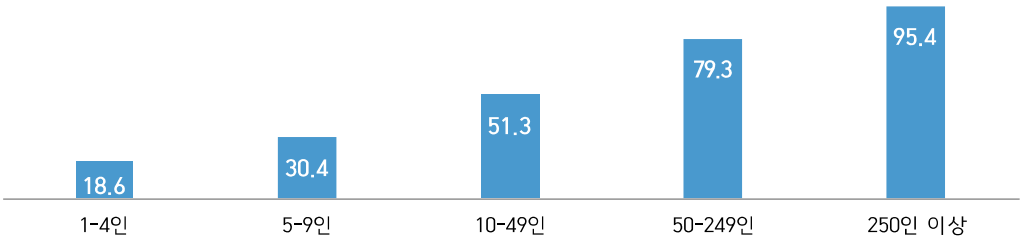
(단위 : %)



규모별 분석 결과, 종사자 수 250명 이상인 사업체의 정보보호 담당 인력 배정 비율이 95.4%로 가장 높았고, 종사자수가 많을수록 정보보호 담당 인력이 있는 사업체의 비율이 높게 나타났다.

그림 1-3-36 규모별 IT 인력 중 정보보호 담당 인력 배정

(단위 : %)

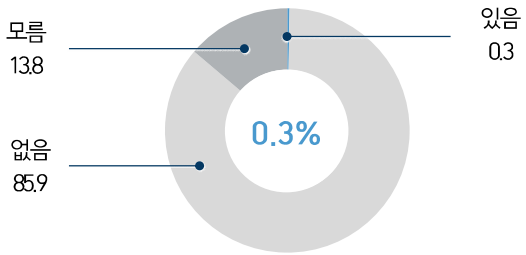



## 다. 정보보호 담당 인력 신규 채용계획

국내 사업체 중 0.3%는 2020년에 정보보호 담당 인력을 신규로 채용할 계획을 보유하고 있는 것으로 나타났다.

그림 1-3-37 정보보호 담당 인력 신규 채용계획

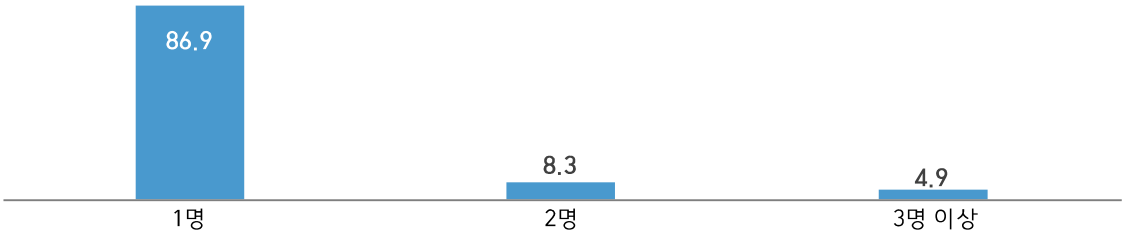
(단위 : %)



2020년 정보보호 담당 인력 신규 채용 계획이 있는 사업체의 86.9%가 1명을 채용할 계획인 것으로 나타났다.

그림 1-3-38 정보보호 담당 인력 신규 채용 규모 - 신규 채용 계획 사업체

(단위 : %)



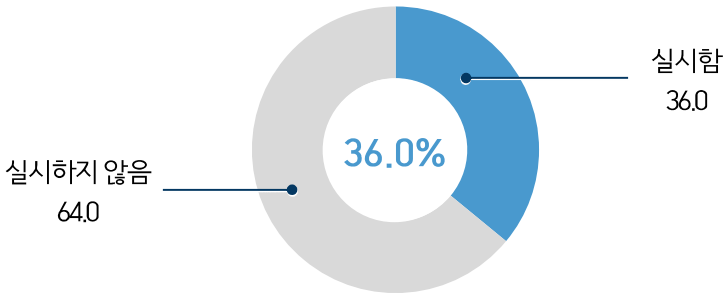

## 4. 정보보호(개인정보보호) 교육

### 가. 정보보호(개인정보보호) 교육 실시

국내 사업체 중 36.0%는 임직원을 대상으로 정보보호(개인정보보호) 교육(외부 위탁 교육 포함)을 실시한 것으로 나타났다.

그림 1-3-39 정보보호 교육 실시

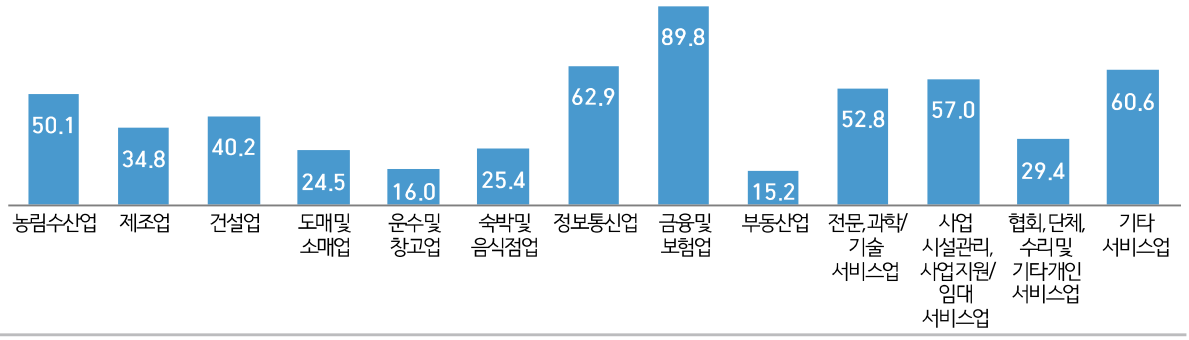
(단위 : %)



업종별 조사 결과, '금융 및 보험업'이 89.8%로 가장 높게 나타났고, 다음으로 '정보통신업(62.9%)', '기타 서비스업(60.6%)' 등의 순으로 조사되었다.

그림 1-3-40 업종별 정보보호 교육 실시

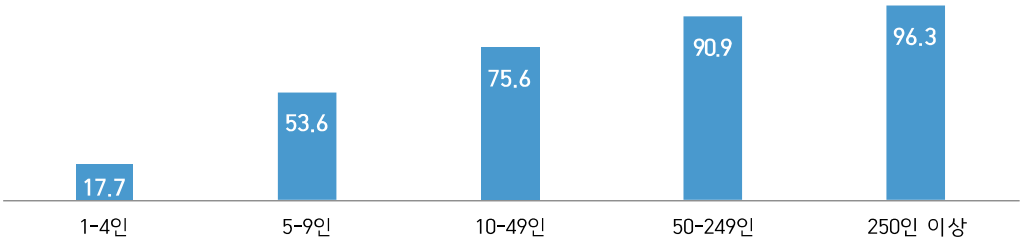
(단위 : %)




규모별 분석 결과, 종사자 수가 많을수록 정보보호 교육을 실시하는 비율이 높게 나타났다.

그림 1-3-41 규모별 정보보호 교육 실시

(단위 : %)

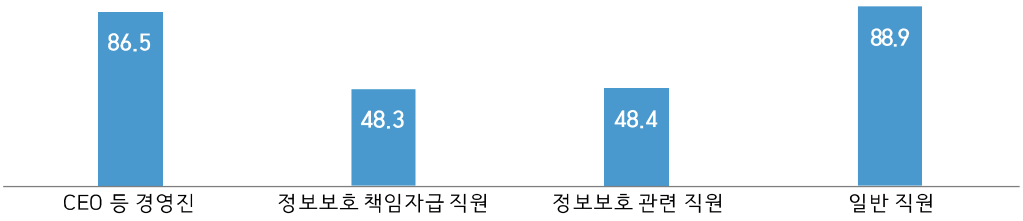


## 나. 대상별 교육 실시 현황

교육 대상별 분석 결과, 정보보호 또는 개인정보보호 교육을 받는 대상으로는 '일반직원'이 88.9%로 가장 높게 나타났고, 다음으로 'CEO 등 경영진(86.5%)', '정보보호 관련 직원(48.4%)' 등의 순으로 조사되었다.

그림 1-3-42 대상별 교육 실시 (복수응답) - 정보보호(개인정보보호) 교육 실시 사업체

(단위 : %)



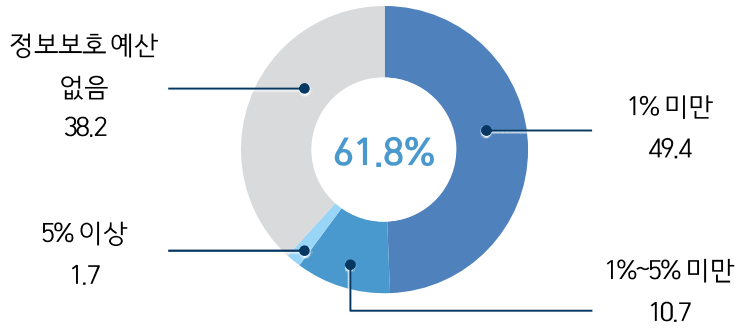
## 5. 정보보호 예산 및 투자

국내 사업체 중 61.8%는 2019년 1년간 정보보호 또는 개인정보보호 예산을 편성한 것으로 나타났다.

IT 예산 중 정보보호 관련 예산이 차지하는 비중을 살펴보면, '1% 미만'이 49.4%로 가장 높았고, 다음으로 '정보보호 예산 없음(38.2%)', '1%~5% 미만(10.7%)' 순으로 나타났다.

그림 1-3-43 IT 예산 중 정보보호 예산 비중

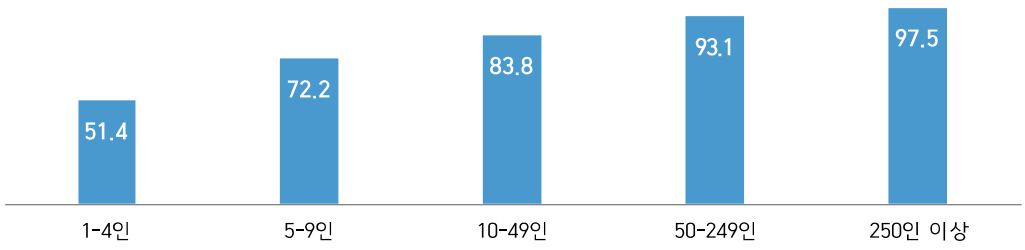
(단위 : %)




규모별 분석 결과, 종사자 수가 많을수록 정보보호 예산을 수립하는 비율이 높게 나타났다.

그림 1-3-44 규모별 정보보호 예산 수립률

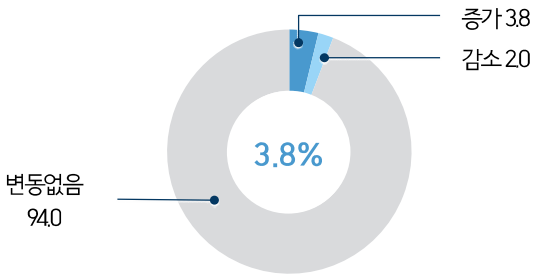
(단위 : %)



2018년 대비 2019년 1년간 정보보호 관련 예산 증감의 경우, '변동없음'이 94.0%로 가장 높게 나타났고, '증가'는 3.8%, '감소'는 2.0%로 조사되었다.

그림 1-3-45 정보보호 예산 증감 - 정보보호 예산 수립 사업체

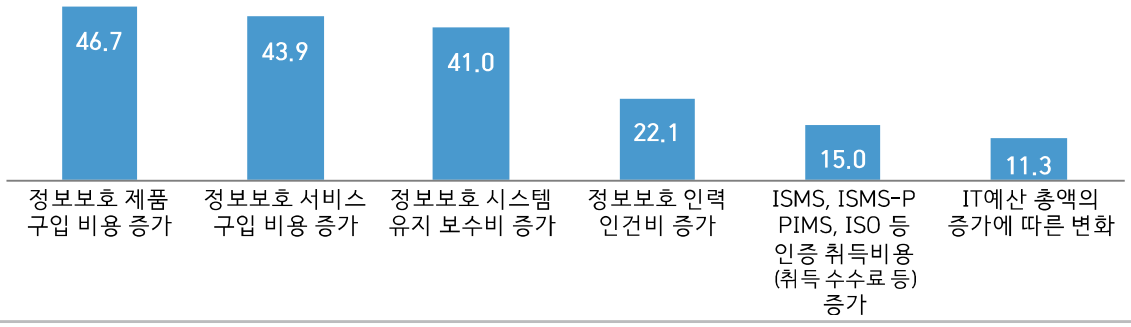
(단위 : %)




정보보호 예산 증가 업체의 증가 이유로는 '정보보호 제품 구입 비용 증가'가 46.7%로 가장 높게 나타났고, 다음으로 '정보보호 서비스 구입 비용 증가(43.9%)', '정보보호 시스템 유지 보수비 증가(41.0%)' 등의 순으로 조사되었다.

그림 1-3-46 정보보호 예산 증가 이유 (복수응답) - 정보보호 예산 증가 사업체

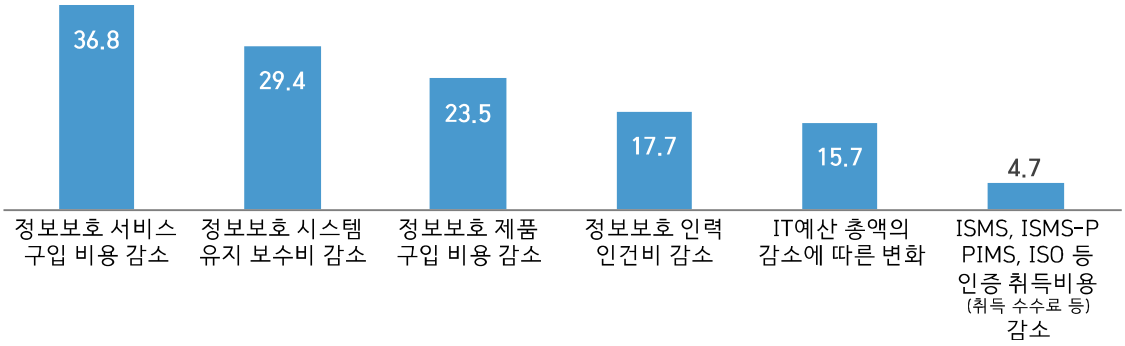
(단위 : %)



정보보호 예산 감소 업체의 감소 이유로는 '정보보호 서비스 구입 비용 감소'가 36.8%로 가장 높게 나타났고, 다음으로 '정보보호 시스템 유지 보수비 감소(29.4%)', '정보보호 제품 구입 비용 감소(23.5%)' 등의 순으로 조사되었다.

그림 1-3-47 정보보호 예산 감소 이유 (복수응답) - 정보보호 예산 감소 사업체

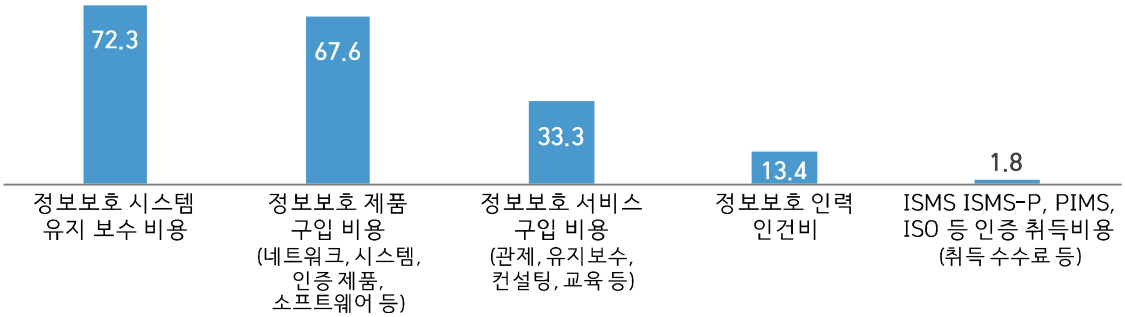
(단위 : %)




정보보호 예산을 수립한 사업체는 2019년 1년간 '정보보호 시스템 유지 보수 비용(72.3%)'에 가장 많은 예산을 지출한 것으로 나타났고, 다음으로 '정보보호 제품 구입 비용(67.6%)', '정보보호 서비스 구입 비용(33.3%)' 등의 순으로 조사되었다.

그림 1-3-48 정보보호 지출 분야 (2가지) - 정보보호 예산 수립 사업체

(단위 : %)



# Ⅲ 침해사고 예방

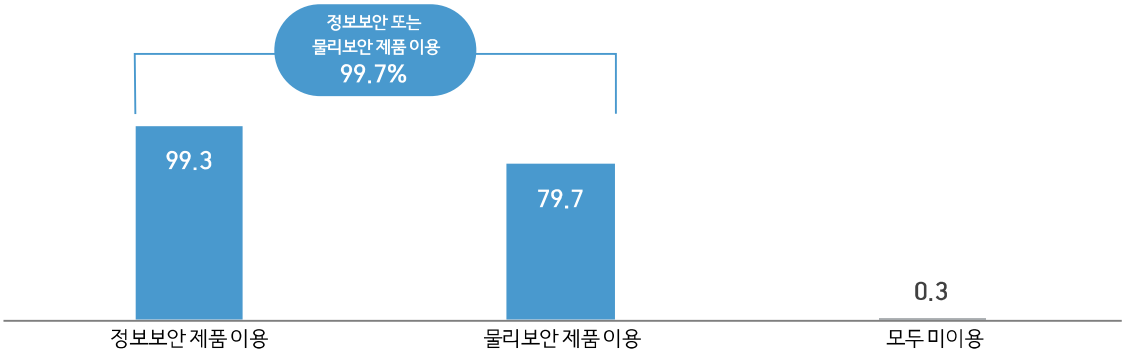
## 1. 정보보호 제품 및 서비스

### 가. 정보보호 제품 이용

국내 사업체 중 99.7%는 정보보호(정보보안 또는 물리보안)를 위해 관련 제품을 이용하고 있는 것으로 나타났다.

그림 1-3-49 정보보호 제품 이용 (요약)

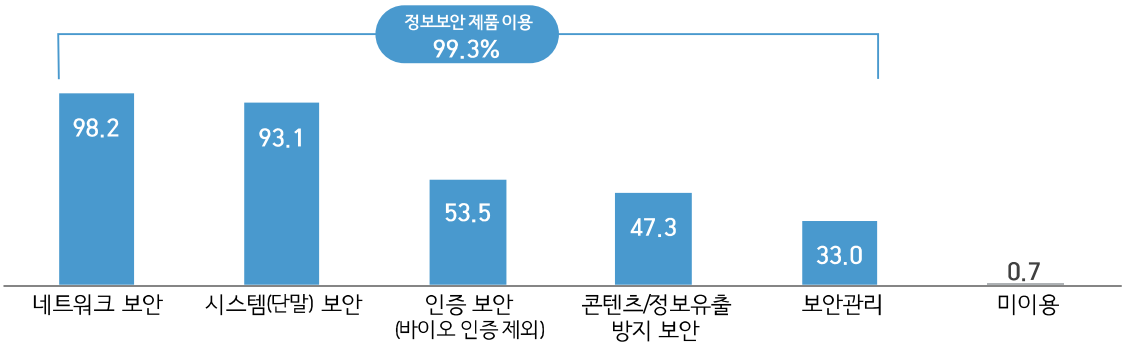
(단위 : %)




정보보안 제품군 중 '네트워크 보안' 제품군의 이용률이 98.2%로 가장 높게 나타났고, 다음으로 '시스템(단말) 보안(93.1%)', '인증 보안(바이오 인증 제외)(53.5%)' 등의 순으로 조사되었다.

그림 1-3-50 정보보호 제품 이용 - 정보보안 (복수응답)

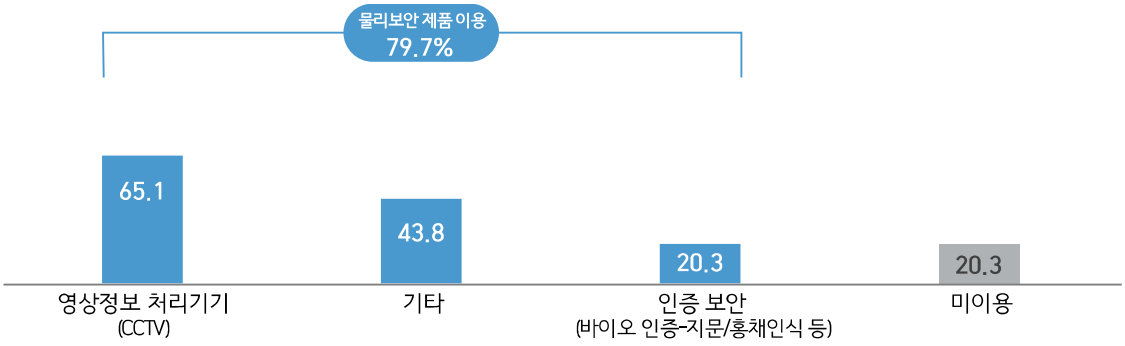
(단위 : %)



물리보안 제품군 중 '영상정보 처리기기(CCTV)' 이용률은 65.1%, '인증 보안(바이오 인증)' 이용률은 20.3%로 조사되었다.

그림 1-3-51 정보보호 제품 이용 - 물리보안 (복수응답)

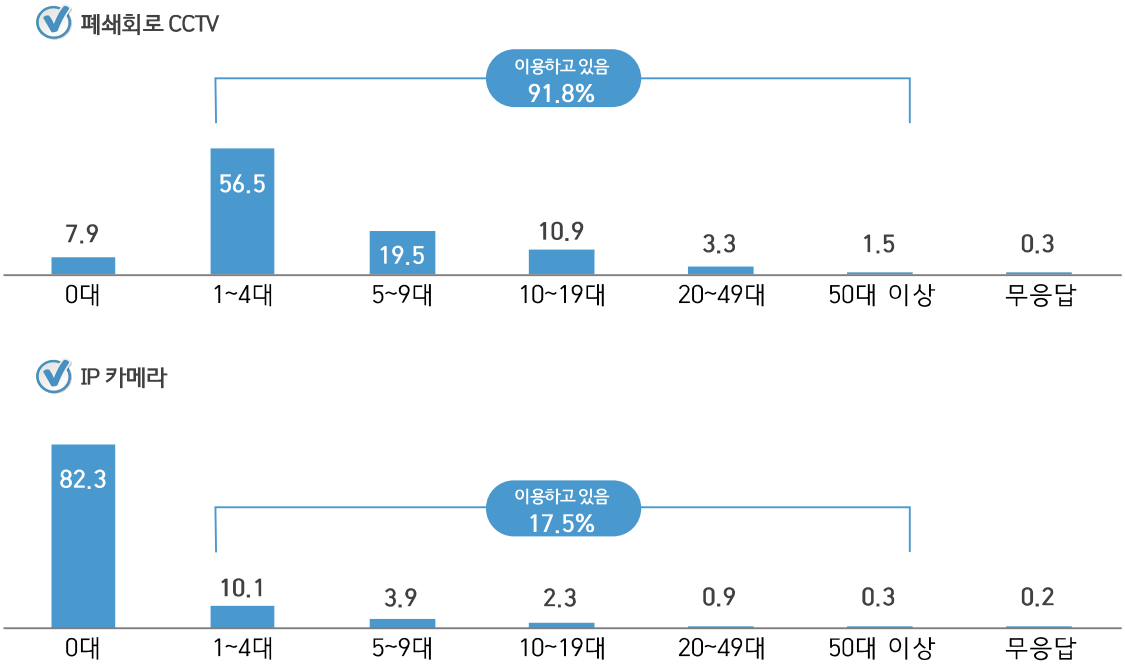
(단위 : %)




영상정보 처리기기 유형별 분석 결과, 폐쇄회로 CCTV를 보유하고 있는 사업체는 91.8%, IP 카메라를 보유하고 있는 사업체는 17.5%로 나타났다.

그림 1-3-52 CCTV 보유 대수 - CCTV 이용 사업체

(단위 : %)

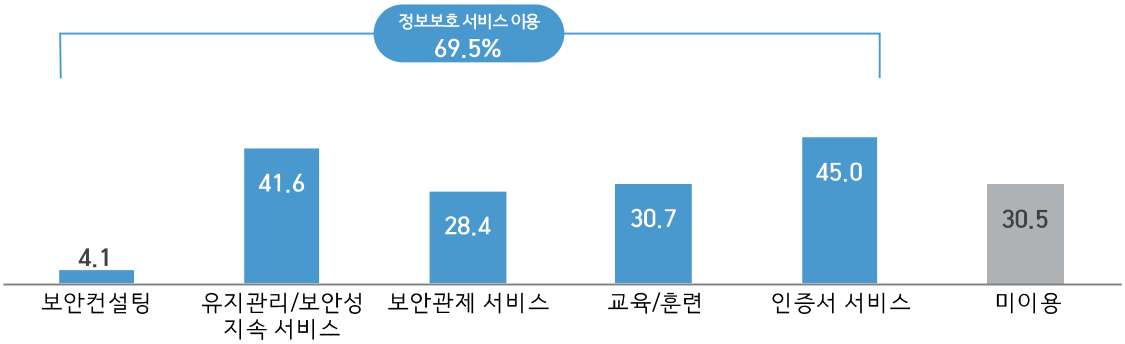


## 나. 정보보호 서비스 이용

국내 사업체 중 69.5%는 정보보호를 위해 관련 서비스를 이용하고 있는 것으로 나타났다. 서비스 유형별로는 '인증서 서비스'가 45.0%로 가장 높게 나타났고, 다음으로 '유지관리/보안성 지속 서비스(41.6%)', '교육/훈련(30.7%)' 등의 순으로 조사되었다.

그림 1-3-53 정보보호 서비스 이용 요약

(단위 : %)




보안컨설팅 서비스를 이용하고 있는 사업체의 이용 기간으로 '1년~3년 미만'이 38.5%로 가장 높게 나타났고, 다음으로 '5년 이상(20.1%)', '1년 미만(18.7%)' 등의 순으로 조사되었다.

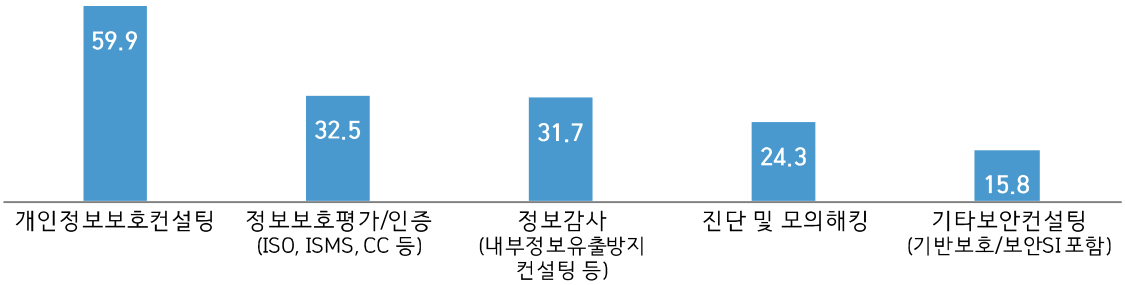
그림 1-3-54 보안컨설팅 서비스 이용 기간 - 보안컨설팅 서비스 이용 사업체

(단위 : %)

보안컨설팅 서비스 분야 중 '개인정보보호 컨설팅'의 이용률이 59.9%로 가장 높게 나타났고, 다음으로 '정보보호 평가/인증(ISO, ISMS, CC 등)(32.5%)', '정보감사(내부정보유출방지 컨설팅 등)(31.7%)' 등의 순으로 조사되었다.

그림 1-3-55 보안컨설팅 서비스 이용 분야 - 보안컨설팅 서비스 이용 사업체

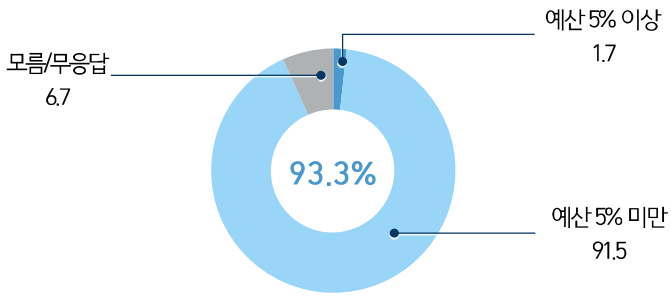
(단위 : %)




IT 예산 중 보안컨설팅 서비스 관련 예산이 차지하는 비중을 살펴보면, '5% 미만'이 91.5%, '5% 이상'이 1.7%로 나타났다.

그림 1-3-56 보안컨설팅 서비스 관련 예산 비중 - 보안컨설팅 서비스 이용 사업체

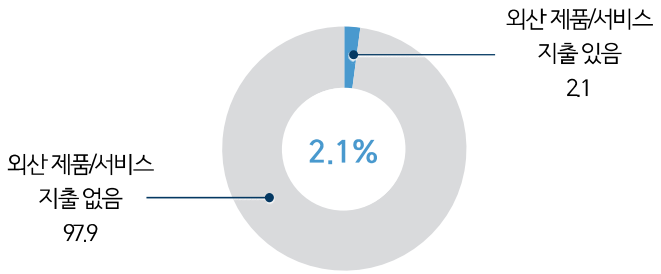
(단위 : %)



정보보호 제품 및 서비스를 이용하는 국내 사업체의 2.1%는 2019년에 외산 제품 및 서비스에 대한 지출이 있는 것으로 나타났다.

그림 1-3-57 외산 제품 및 서비스 지출 여부 - 정보보호 제품 및 서비스 이용 사업체

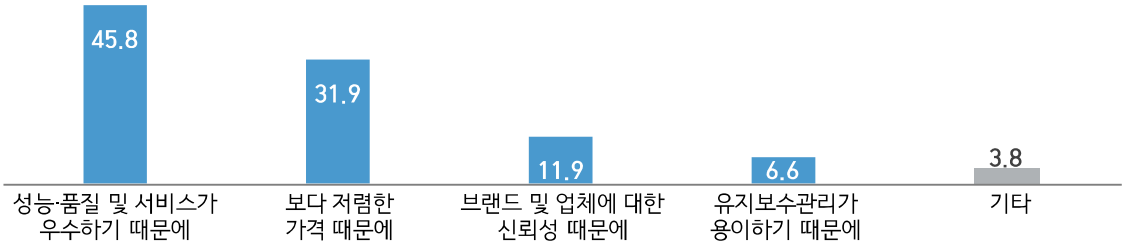
(단위 : %)




외산 제품 및 서비스를 구매한 이유는 '성능·품질 및 서비스가 우수하기 때문에'가 45.8%로 가장 높게 나타났고, 다음으로 '보다 저렴한 가격 때문에(31.9%)', '브랜드 및 업체에 대한 신뢰성 때문에(11.9%)' 등의 순으로 조사되었다.

그림 1-3-58 외산 정보보호 제품 구매 이유 - 외산 제품 구매 사업체

(단위 : %)



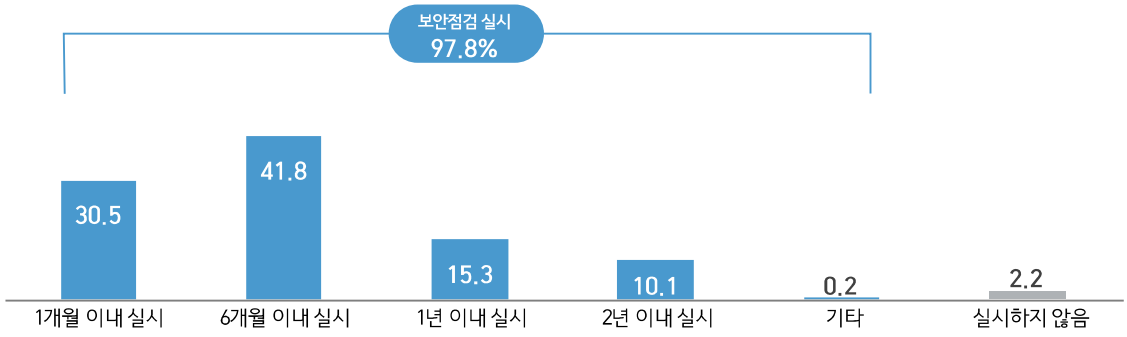
# 2. 정보보호 관리

## 가. 보안점검 및 취약점 점검

국내 사업체 중 97.8%가 시스템 및 네트워크에 대한 보안점검(취약점 점검 등)을 실시하는 것으로 나타났다.
최근 점검 실시 시점은 '6개월 이내 실시'가 41.8%로 가장 높게 나타났고, '1개월 이내 실시(30.5%)', '1년 이내 실시(15.3%)' 등의 순으로 조사되었다.

그림 1-3-59 시스템 및 네트워크 보안점검 실시 (복수응답)

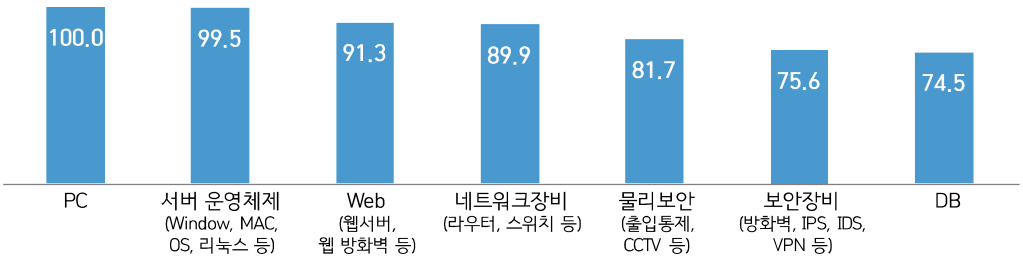
(단위 : %)




보안점검을 실시하는 사업체의 시스템 및 네트워크 보유율은 'PC'가 100.0%로 가장 높게 나타났고, 다음으로 '서버 운영체제(Winsdows, MAC, OS, 리눅스 등)(99.5%)', 'Web(웹서버, 웹 방화벽 등)(91.3%)'등의 순으로 조사되었다.

그림 1-3-60 시스템 및 네트워크 보유 (복수응답) - 보안점검 실시 사업체

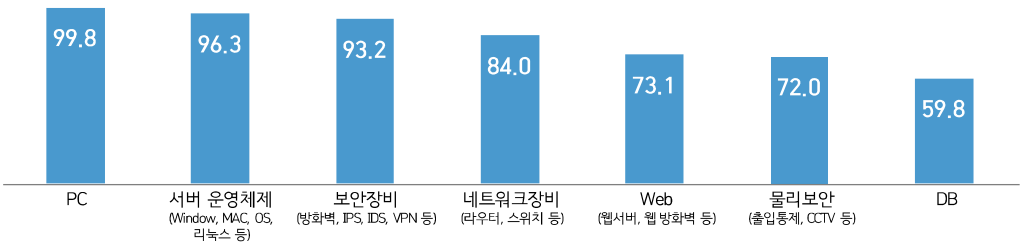
(단위 : %)



시스템 및 네트워크 유형별 분석 결과, 취약점 점검률은 'PC'가 99.8%로 가장 높게 나타났고, 다음으로 '서버 운영체제(Window, MAC, OS, 리눅스 등)(96.3%)', 보안장비(방화벽, IPS, IDS, VPN 등)(93.2%)' 등의 순으로 조사되었다.

그림 1-3-61 취약점 점검 (복수응답) - 각 시스템 및 네트워크 보유 사업체

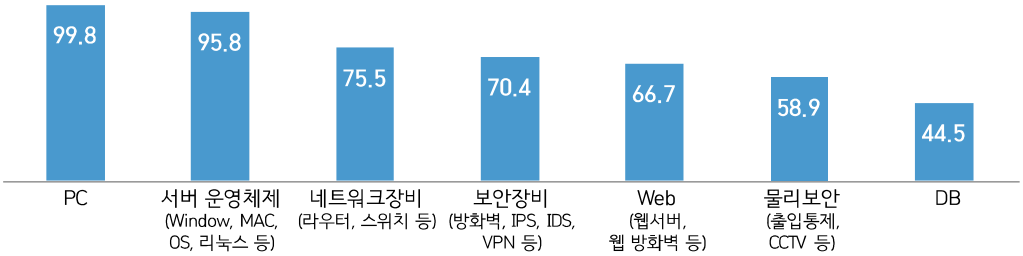
(단위 : %)




▶ **참고** **응답 기준을 보안점검 실시 사업체로 확대한 경우 유형별 취약점 점검률**

그림 1-3-62 취약점 점검 (복수응답) - 보안점검 실시 사업체

(단위 : %)

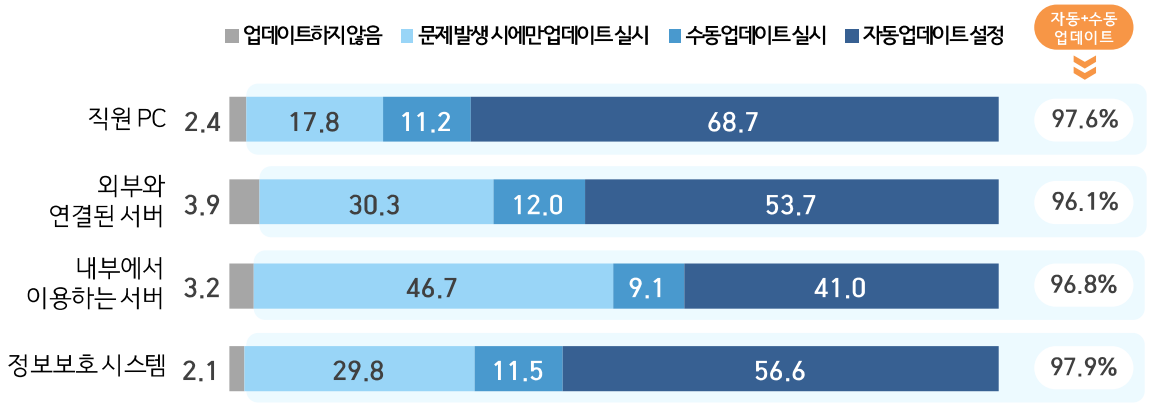


## 나. 보안패치 적용

제품 유형별로 자동 또는 수동으로 보안패치를 적용하는 비율은 '정보보호 시스템'이 97.9%로 가장 높게 나타났고, 다음으로 '직원 PC(97.6%)', '내부에서 이용하는 서버(96.8%)' 등의 순으로 조사되었다.

그림 1-3-63 보안패치 적용 방법 (복수응답) - 항목별 제품 보유 사업체

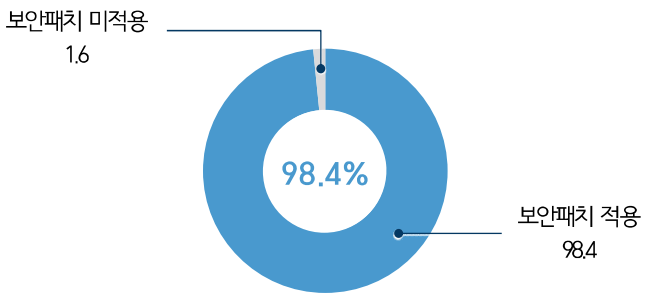
(자동 업데이트 + 수동 업데이트, 단위 : %)




▶ **참고** **직원PC, 외부와 연결된 서버, 내부에서 이용하는 서버, 정보보호 시스템 중 하나라도 보안패치를 적용하는 경우**

그림 1-3-64 보안패치 적용

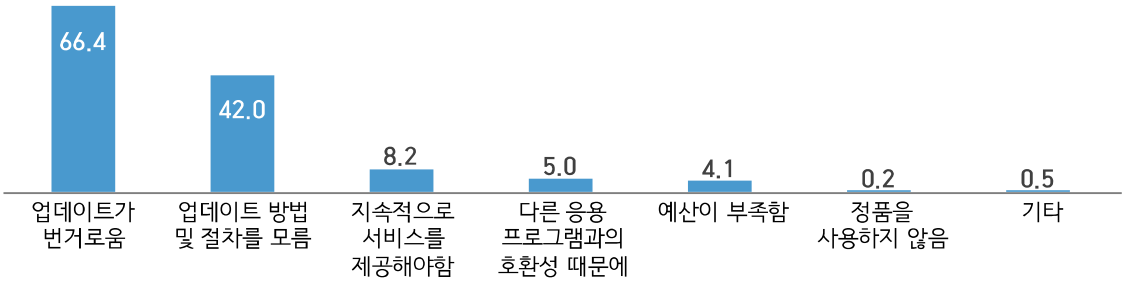
(단위 : %)



보안패치를 적용하지 않는 이유는 '업데이트가 번거로움'이 66.4%로 가장 높게 나타났고, 다음으로 '업데이트 방법 및 절차를 모름(42.0%)', '지속적으로 서비스를 제공해야 함(8.2%)' 등의 순으로 조사되었다.

그림 1-3-65 보안패치 업데이트 미실시 이유 (복수응답) - 하나라도 업데이트 하지 않는 사업체

(단위 : %)

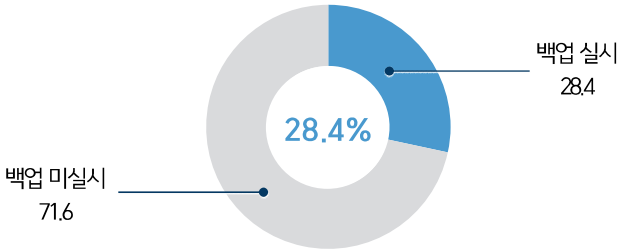



## 다. 백업 실시

국내 사업체 중 시스템 로그 백업을 실시하는 사업체는 28.4%로 나타났다.

그림 1-3-66 시스템 로그 백업

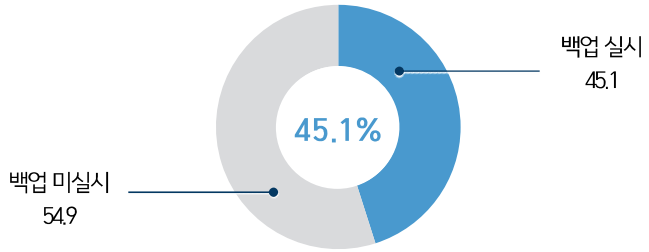
(단위 : %)



한편, 중요 데이터 백업을 실시하는 사업체는 45.1%로 나타났다.

그림 1-3-67 중요 데이터 백업

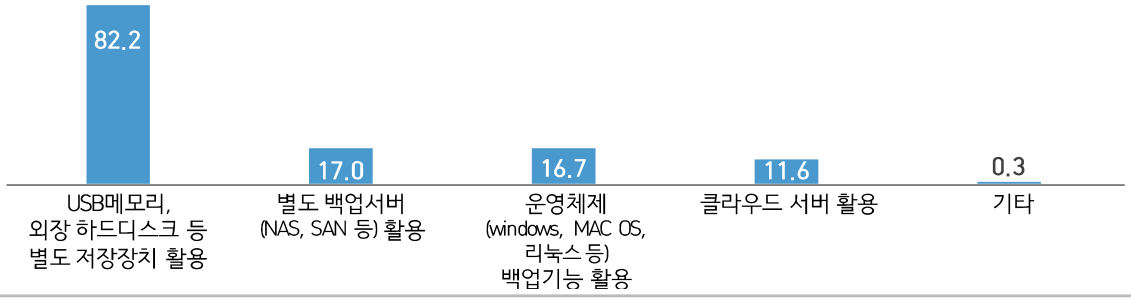
(단위 : %)




시스템 로그 또는 중요 데이터를 백업하는 방식은 'USB메모리, 외장 하드디스크 등 별도 저장장치 활용'이 82.2%로 가장 높게 나타났고, 다음으로 '별도 백업서버(NAS, SAN 등) 활용(17.0%)', '운영체제(windows, MAC, OS, 리눅스 등) 백업기능 활용(16.7%)' 등의 순으로 조사되었다.

그림 1-3-68 백업 방식 (복수응답) - 하나라도 백업 실시 사업체

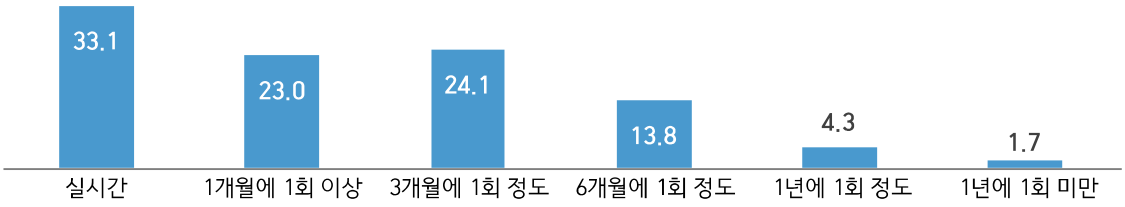
(단위 : %)



시스템 로그 백업 주기는 '실시간'이 33.1%로 가장 높게 나타났고, 다음으로 '3개월에 1회 정도(24.1%)', '1개월에 1회 이상(23.0%)' 등의 순으로 조사되었다.

그림 1-3-69 시스템 로그 백업 주기 - 시스템 로그 백업 실시 사업체

(단위 : %)




중요 데이터 백업 주기는 '1개월에 1회 이상'이 37.6%로 가장 높게 나타났고, 다음으로 '3개월에 1회 정도(29.9%)', '6개월에 1회 정도(21.7%)' 등의 순으로 조사되었다.

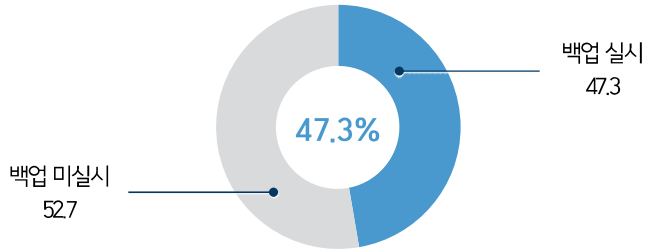
그림 1-3-70 중요 데이터 백업 주기 - 중요 데이터 백업 실시 사업체

(단위 : %)

### ▶ 참고 시스템 로그 또는 중요 데이터 백업을 실시하는 경우

그림 1-3-71 백업 실시 - 시스템 로그 또는 중요 데이터 백업 실시

(단위 : %)



# Ⅳ 침해사고 대응

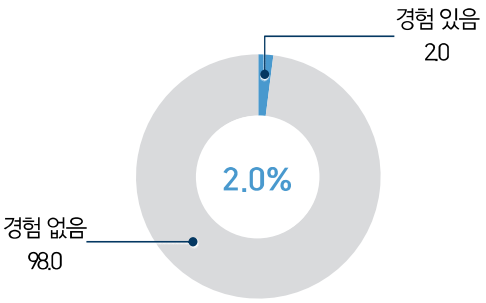
## 1. 침해사고 경험

### 가. 침해사고 경험

국내 사업체 중 2.0%가 해킹, 악성코드(웜·바이러스), DDoS 등의 침해사고를 경험한 것으로 나타났다.

그림 1-3-72 침해사고 경험

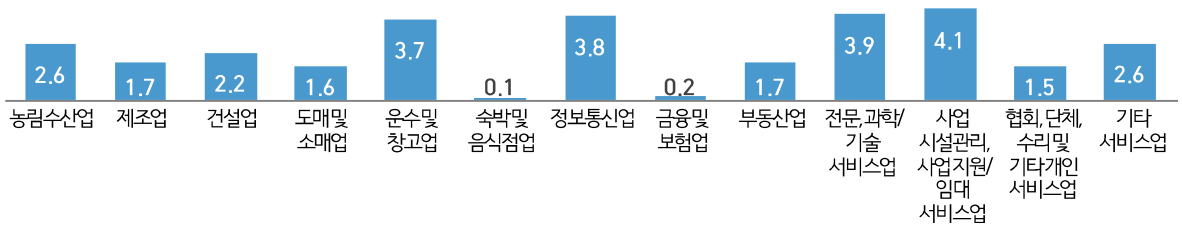
(단위 : %)




업종별 분석 결과, '사업 시설관리, 사업 지원/임대서비스업'이 4.1%로 가장 높게 나타났고, 다음으로 '전문, 과학/기술 서비스업(3.9%)', '정보통신업(3.8%)' 등의 순으로 조사되었다.

그림 1-3-73 업종별 침해사고 경험

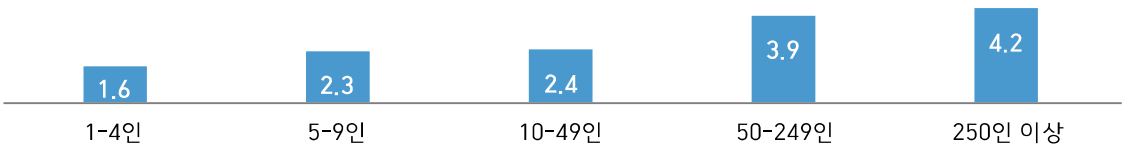
(단위 : %)



규모별 분석 결과, '종사자 수 250인 이상'의 사업체가 4.2%로 가장 높게 나타났다.

그림 1-3-74 규모별 침해사고 경험

(단위 : %)

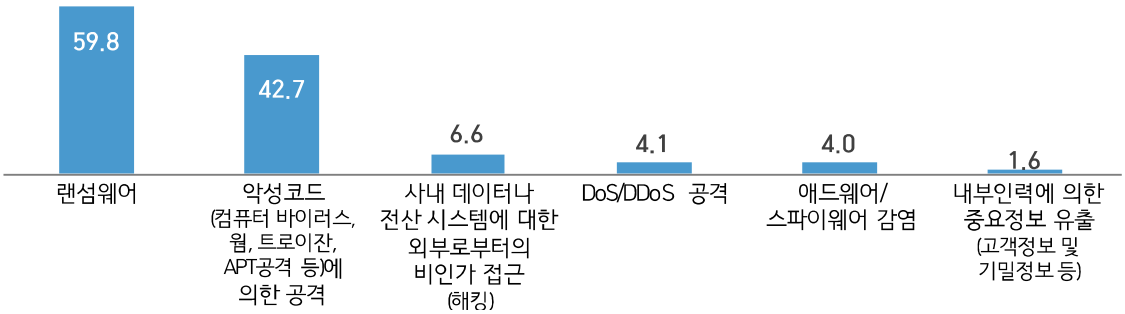



## 나. 침해사고 경험 유형 및 심각성 정도

침해사고 경험 유형별로는 '랜섬웨어'의 경험률이 59.8%로 가장 높게 나타났고, 다음으로 '악성코드(컴퓨터 바이러스, 웜, 트로이잔, APT공격 등)에 의한 공격(42.7%)', '사내 데이터나 전산 시스템에 대한 외부로부터의 비인가 접근(해킹)(6.6%)' 등의 순으로 조사되었다.

그림 1-3-75 침해사고 경험 유형 (복수응답) - 침해사고 경험 사업체

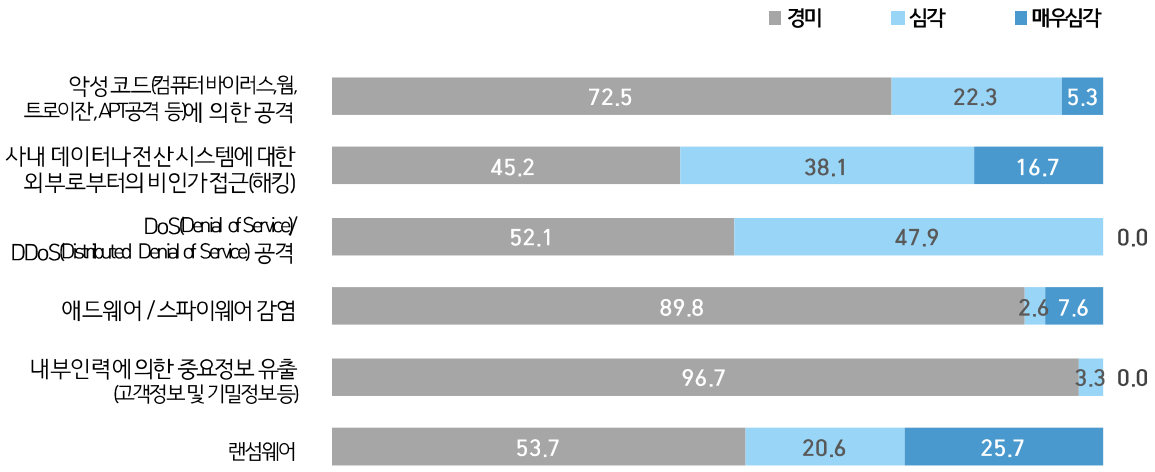
(단위 : %)



침해사고 경험 유형별 심각성 정도는 '랜섬웨어' 유형에서 '매우 심각(25.7%)'이 가장 높게 나타났고, 다음으로 '사내 데이터나 전산 시스템에 대한 외부로부터의 비인가 접근(해킹)(16.7%, 매우 심각)' 등의 순으로 조사되었다.

그림 1-3-76 침해사고 유형별 심각성 정도 - 침해사고 경험 사업체

(단위 : %)

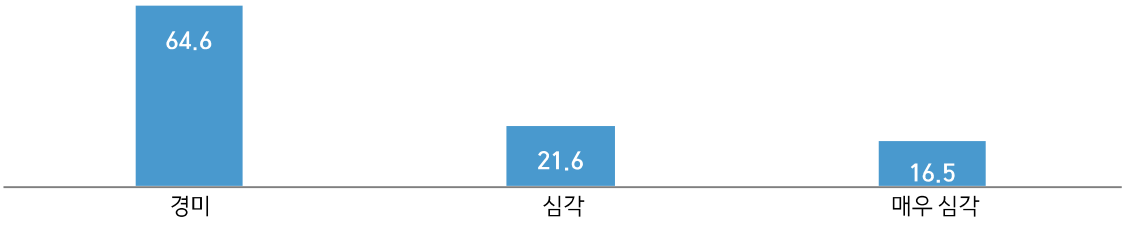



**참고**

▶ **전체 침해사고 유형별 심각성 정도**

그림 1-3-77 침해사고 유형별 심각성 정도 통합 - 침해사고 경험 사업체

(단위 : %)

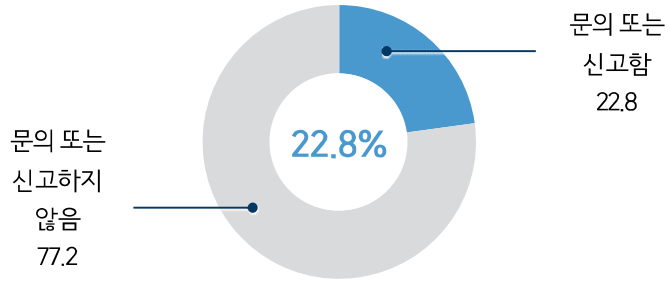


### 다. 침해사고 시 관계기관 문의 또는 신고

침해사고 경험 사업체의 22.8%가 피해를 입었을 때 관계기관에 문의 또는 신고하는 것으로 나타났다.

그림 1-3-78 침해사고 시 관계기관 문의 또는 신고 여부

(단위 : %)



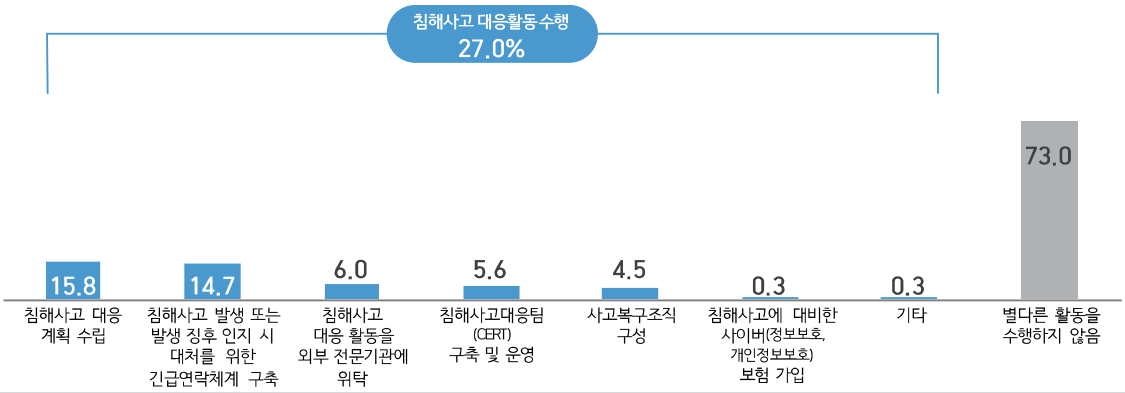

## 2. 침해사고 대응

국내 사업체 중 27.0%가 침해사고에 대응하기 위한 활동을 수행한 것으로 나타났다.

침해사고 대응활동 유형별로는 '침해사고 대응 계획 수립'이 15.8%로 가장 높게 나타났고, 다음으로 '침해사고 발생 또는 발생 징후 인지 시 대처를 위한 긴급연락체계 구축(14.7%)' 등의 순으로 조사되었다.

그림 1-3-79 침해사고 대응활동 수행 (복수응답)

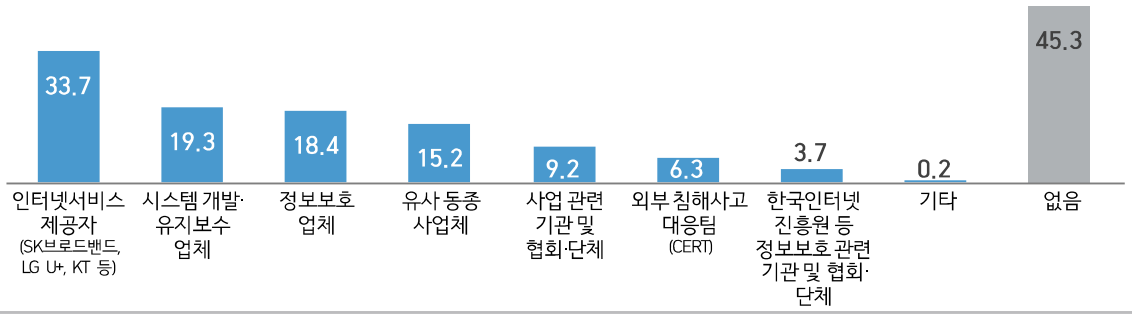
(단위 : %)



침해사고 관련 정보공유 및 대응을 위해 활용하는 대외협력채널은 '인터넷서비스제공자(SK브로드밴드, LG U+, KT 등)'가 33.7%로 가장 높게 나타났고, 다음으로 '시스템 개발·유지보수 업체(19.3%)' 등의 순으로 조사되었다.

그림 1-3-80 침해사고 대응 대외협력채널 (2가지)

(단위 : %)



# V 개인정보보호

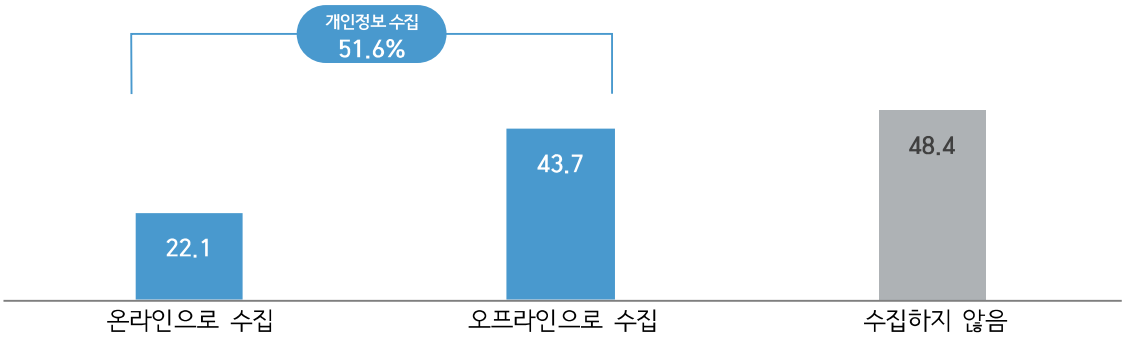
## 1. 개인정보 수집 및 이용

### 가. 개인정보 수집

국내 사업체 중 51.6%는 고객의 개인정보를 온라인 또는 오프라인으로 수집하는 것으로 나타났다.

그림 1-3-81 개인정보 수집 (복수응답)

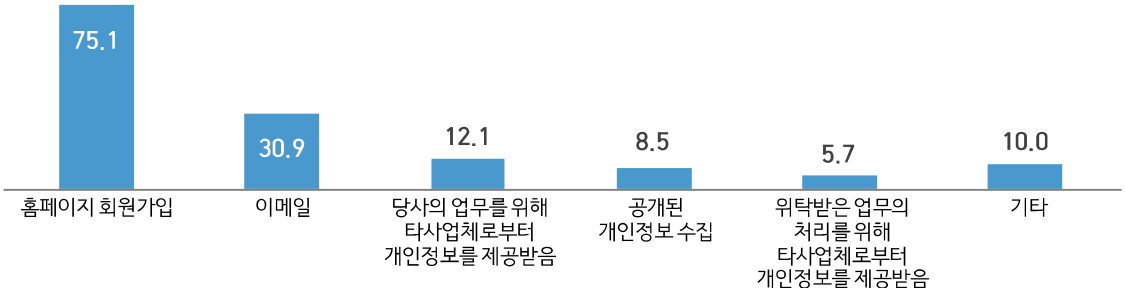
(단위 : %)




온라인으로 고객의 개인정보를 수집하는 사업체는 주로 '홈페이지 회원가입(75.1%)'을 통해 수집하는 것으로 나타났다.

그림 1-3-82 개인정보 온라인 수집 방법 (복수응답) - 온라인으로 개인정보 수집 사업체

(단위 : %)

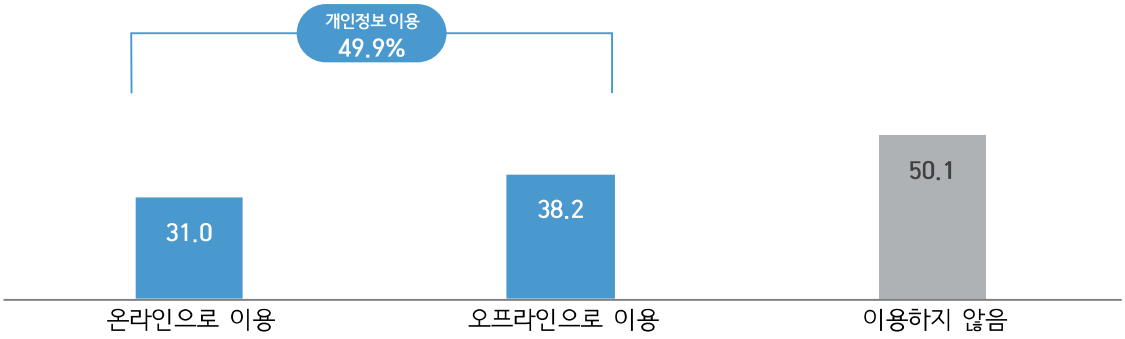


## 나. 개인정보 이용

국내 사업체 중 49.9%는 고객의 개인정보를 온라인 또는 오프라인으로 이용하는 것으로 나타났다.

그림 1-3-83 개인정보 이용 (복수응답)

(단위 : %)

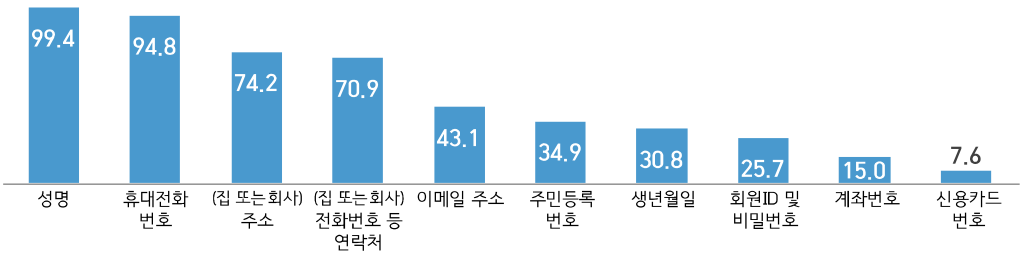



## 다. 개인정보 수집 및 이용 현황

개인정보를 수집하는 사업체가 수집 및 이용하는 고객의 일반정보는 '성명'이 99.4%로 가장 높게 나타났고, 다음으로 '휴대전화 번호(94.8%)', '(집 또는 회사)주소(74.2%)' 등의 순으로 조사되었다.

그림 1-3-84 개인정보 수집 및 이용 현황 - 일반정보 (복수응답) - 개인정보 수집 사업체

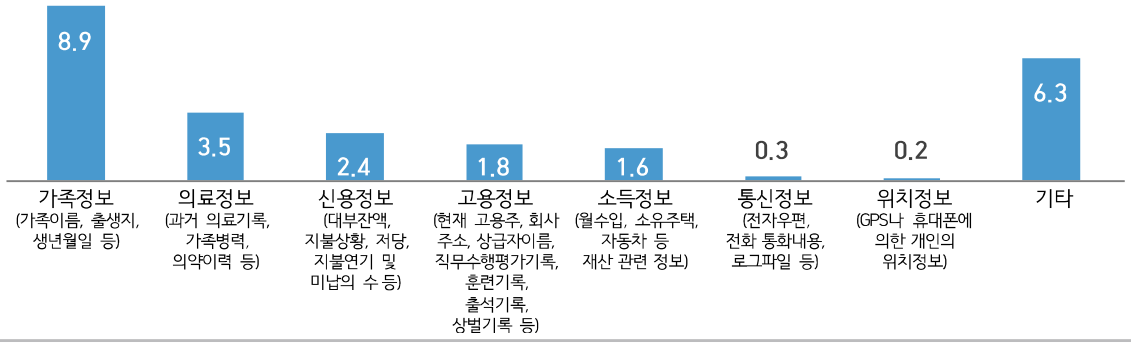
(단위 : %)



개인정보를 수집하는 사업체가 수집 및 이용하는 고객의 특화정보는 '가족정보(가족이름, 출생지, 생년월일 등)'이 8.9%로 가장 높게 나타났고, 다음으로 '의료정보(과거 의료기록, 가족병력, 의약이력 등)(3.5%)' 등의 순으로 조사되었다.

그림 1-3-85 개인정보 수집 및 이용 현황 - 특화정보 (복수응답) - 개인정보 수집 사업체

(단위 : %)

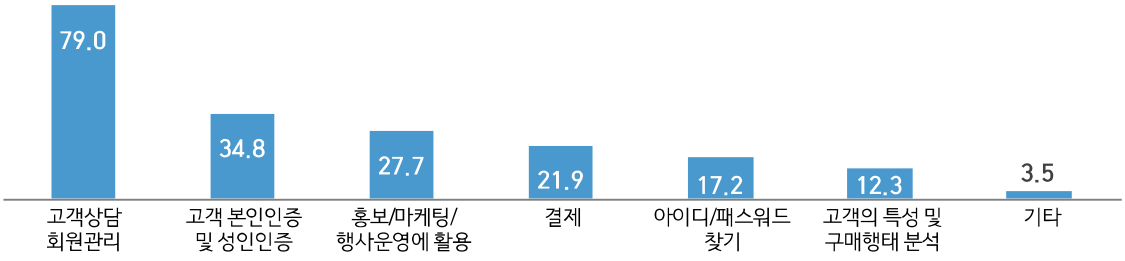



## 라. 개인정보 수집 및 이용 목적

고객의 개인정보를 수집 및 이용하는 목적은 '고객상담 회원관리'가 79.0%로 가장 높게 나타났고, 다음으로 '고객 본인인증 및 성인인증(34.8%)', '홍보/마케팅/행사운영에 활용(27.7%)' 등의 순으로 조사되었다.

그림 1-3-86 개인정보 수집 및 이용 목적 - 개인정보 수집 사업체

(단위 : %)



# 2. 개인정보 침해사고 예방

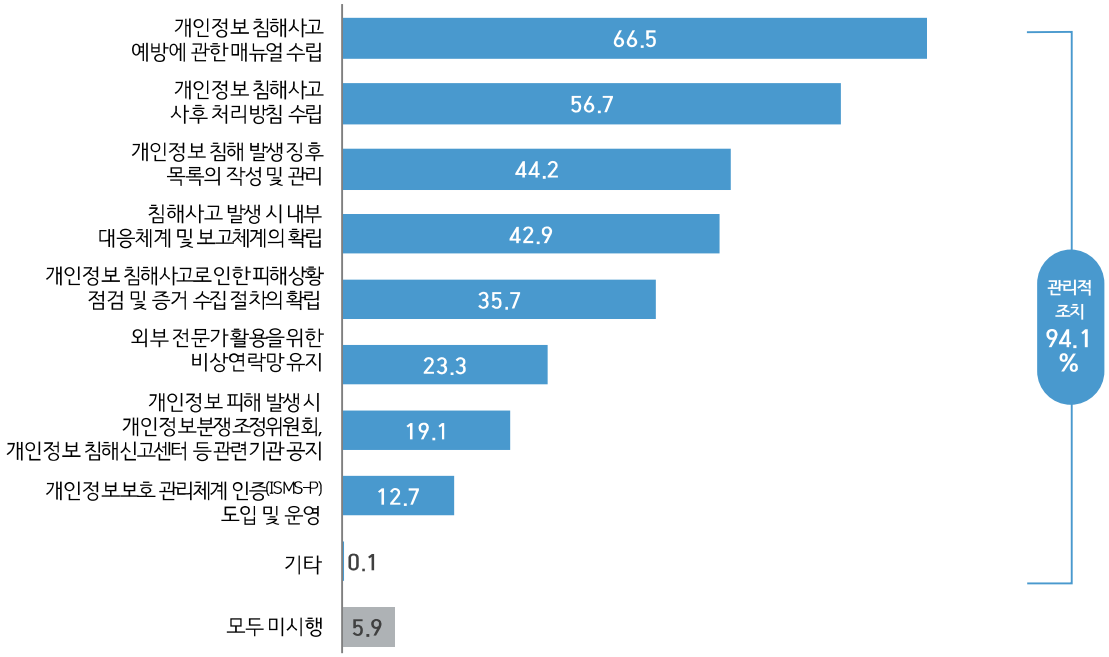
## 가. 개인정보 침해사고 예방을 위한 관리적 조치

고객의 개인정보를 수집하는 사업체 중 94.1%가 개인정보 침해사고의 예방 및 사후처리를 위한 관리적 조치를 취하고 있는 것으로 나타났다.

유형별로는 '개인정보 침해사고 예방에 관한 매뉴얼 수립'이 66.5%로 가장 높게 나타났고, 다음으로 '개인정보 침해사고 사후 처리방침 수립(56.7%)' 등의 순으로 조사되었다.

그림 1-3-87 개인정보 침해사고 예방을 위한 관리적 조치 (복수응답) - 개인정보 수집 사업체

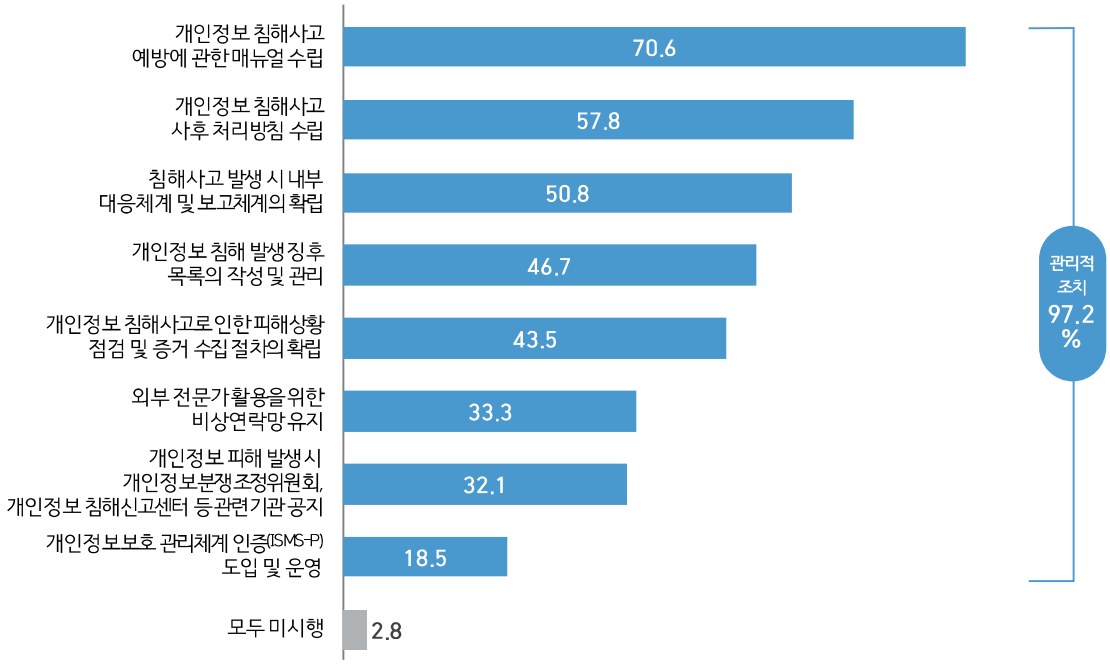
(단위 : %)



▶ **참고** **응답 기준을 온라인으로 고객의 개인정보를 수집한 사업체로 한정한 경우**

그림 1-3-88 개인정보 침해사고 예방을 위한 관리적 조치 (복수응답) - 온라인으로 개인정보 수집 사업체

(단위 : %)



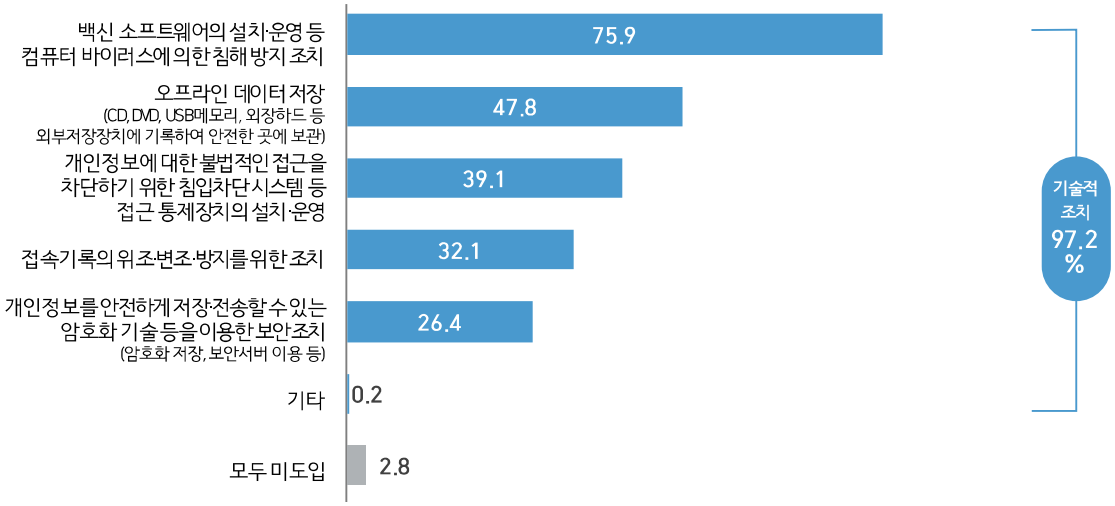
## 나. 개인정보 침해사고 예방을 위한 기술적 조치

고객의 개인정보를 수집하는 사업체 중 97.2%가 개인정보 침해사고의 예방을 위한 기술적 조치를 도입하고 있는 것으로 나타났다.

유형별로는 '백신 소프트웨어의 설치·운영 등 컴퓨터 바이러스에 의한 침해 방지 조치'가 75.9%로 가장 높게 나타났고, 다음으로 '오프라인 데이터 저장(CD, DVD, USB메모리, 외장하드 등 외부저장장치에 기록하여 안전한 곳에 보관(47.8%)' 등의 순으로 조사되었다.

그림 1-3-89 개인정보 침해사고 예방을 위한 기술적 조치 (복수응답) - 개인정보 수집 사업체

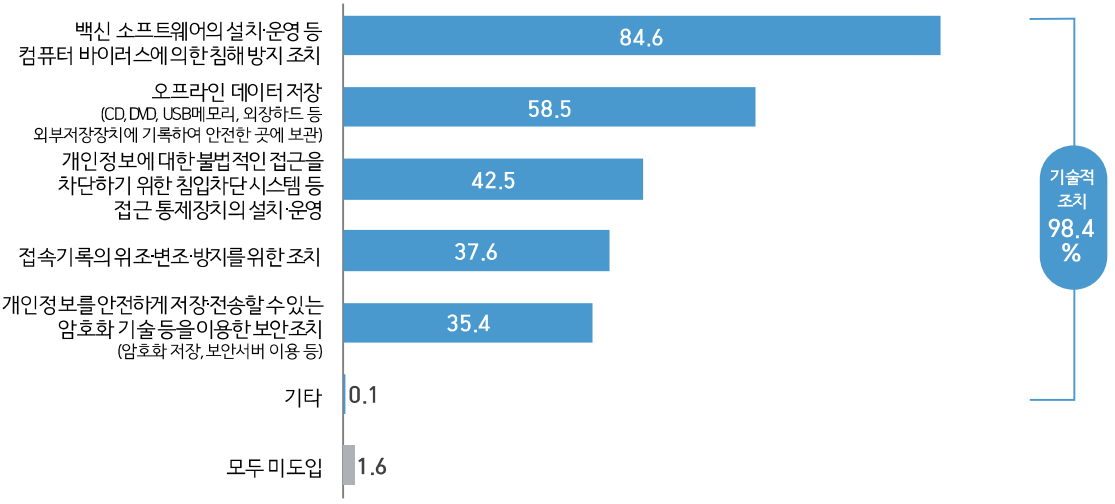
(단위 : %)




▶ **참고** **응답 기준을 온라인으로 고객의 개인정보를 수집한 사업체로 한정한 경우**

그림 1-3-90 개인정보 침해사고 예방을 위한 기술적 조치 (복수응답) - 온라인으로 개인정보 수집 사업체

(단위 : %)

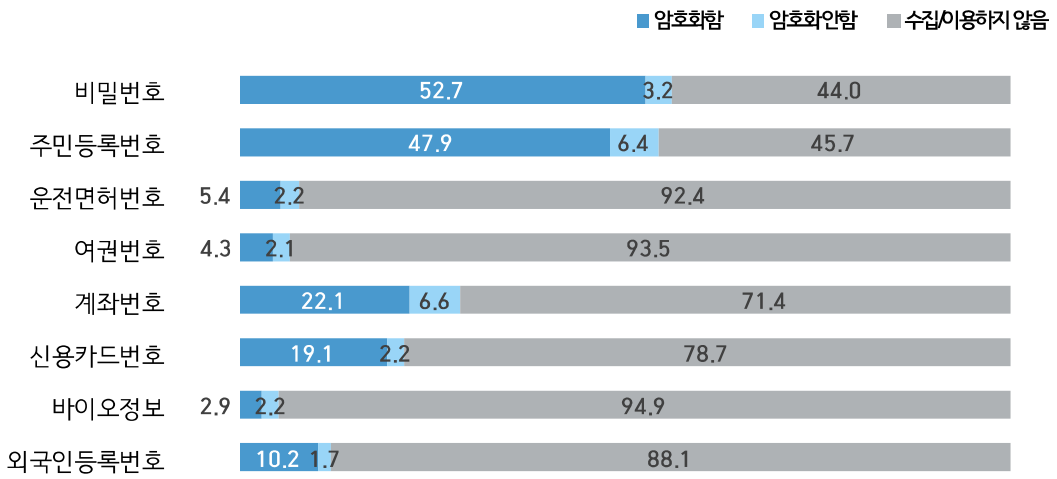


### 다. 개인정보 암호화

고객의 개인정보를 암호화하여 저장하거나 보안서버를 이용하는 사업체가 암호화를 실시하는 개인정보는 '비밀번호'가 52.7%로 가장 높게 나타났고, 다음으로 '주민등록번호(47.9%)', '계좌번호(22.1%)' 등의 순으로 조사되었다.

그림 1-3-91 개인정보 암호화 - 개인정보 암호화 저장 및 보안서버 이용 사업체

(단위 : %)



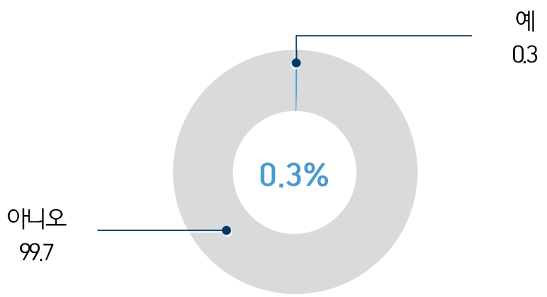

## 3. 개인정보 침해사고 경험

### 가. 개인정보 침해사고 경험

고객의 개인정보를 수집하는 사업체 중 0.3%가 고객의 개인정보가 유출되는 침해사고를 경험한 것으로 나타났다.

그림 1-3-92 개인정보 침해사고 경험 - 개인정보 수집 사업체

(단위 : %)

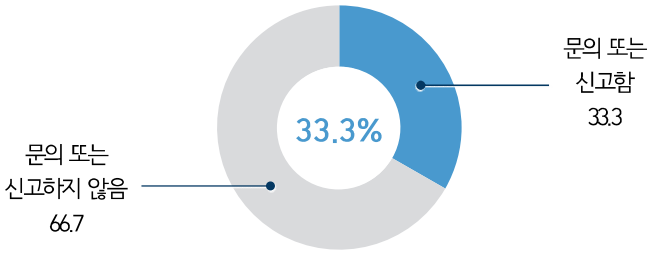


## 나. 개인정보 침해사고 시 관계기관 문의 또는 신고

고객의 개인정보 침해사고를 경험한 사업체 중 33.3%가 해당 침해사고 발생 시 관계기관에 문의 또는 신고한 것으로 나타났다.

그림 1-3-93 개인정보 침해사고 시 관계기관 문의 또는 신고 - 개인정보 침해사고 경험 사업체

(단위 : %)



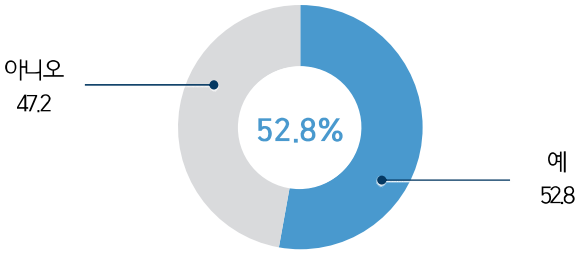

※ 개인정보 침해사고 시 관계기관에 문의 또는 신고 문항은 사례수(n=15)가 적어 해석에 유의해야함

## 다. 개인정보 침해사고 시 통지 또는 고지

고객의 개인정보 침해사고를 경험한 사업체 중 52.8%가 해당 침해사고의 발생 사실을 고객에게 통지 또는 고지한 것으로 나타났다.

그림 1-3-94 개인정보 침해사고 시 통지 또는 고지 - 개인정보 침해사고 경험 사업체

(단위 : %)




※ 개인정보 침해사고 시 통지 또는 고지 문항은 사례수(n=15)가 적어 해석에 유의해야함

# Ⅵ 주요 서비스별 정보보호

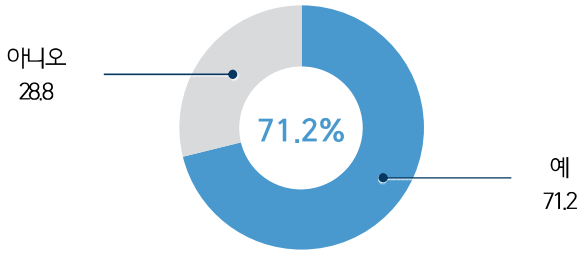
## 1. 무선랜

### 가. 무선랜 구축 및 운영

국내 네트워크 구축 사업체 중 71.2%가 사내에서 무선랜을 구축하여 운영하고 있는 것으로 나타났다.

그림 1-3-95 무선랜 구축 및 운영

(단위 : %)

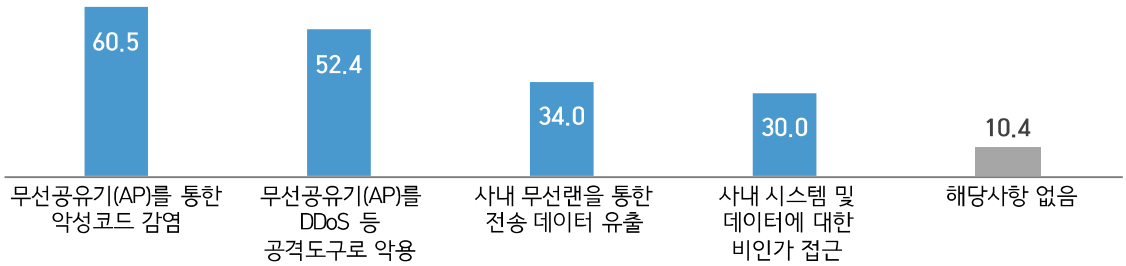



### 나. 무선랜 보안

사내 무선랜의 이용과 관련한 보안 우려사항은 '무선공유기(AP)를 통한 악성코드 감염'이 60.5%로 가장 높게 나타났고, '무선공유기(AP)를 DDoS 등 공격도구로 악용(52.4%)' 등의 순으로 조사되었다.

그림 1-3-96 무선랜 보안 우려사항 (2가지) - 무선랜 구축 사업체

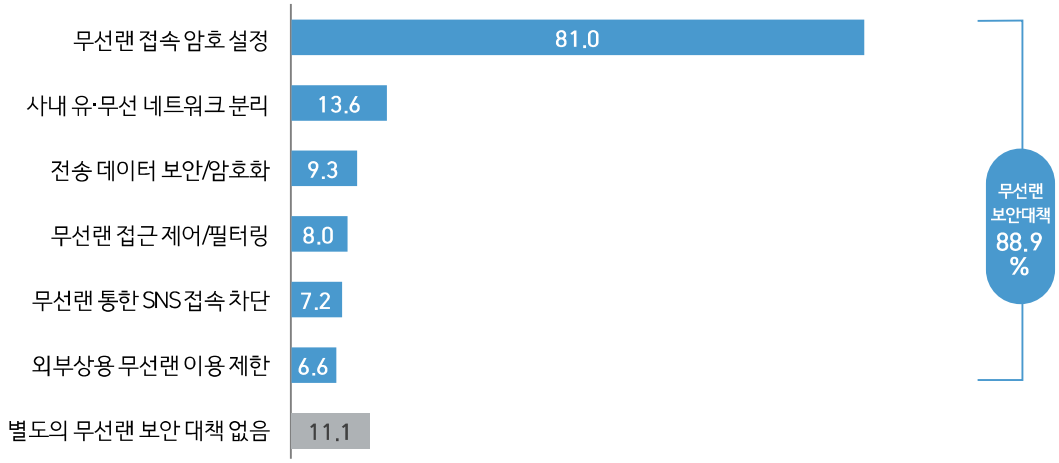
(단위 : %)



사내 무선랜 보안을 위해 실행하고 있는 조치는 '무선랜 접속 암호 설정'이 81.0%로 가장 높게 나타났고, 다음으로 '사내 유·무선 네트워크 분리(13.6%)', '전송 데이터 보안/암호화(9.3%)' 등의 순으로 조사되었다.

그림 1-3-97 무선랜 보안을 위한 조치 (복수응답) - 무선랜 구축 사업체

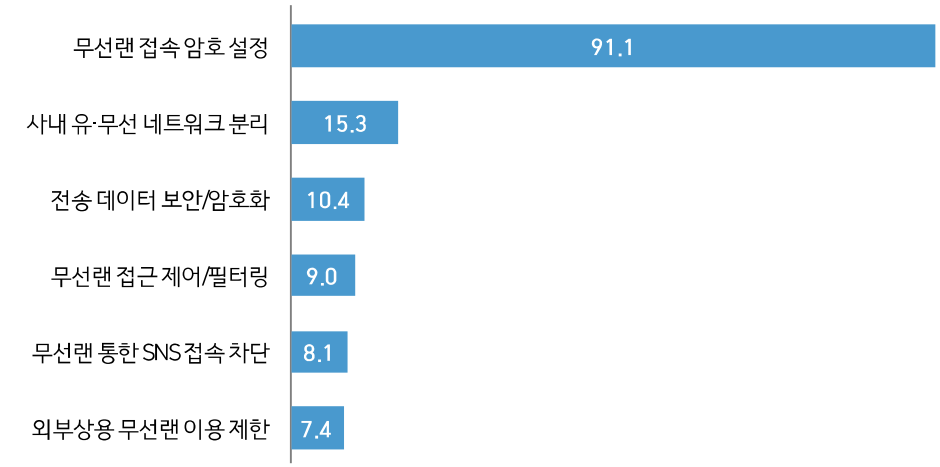
(단위 : %)




▶ **참고** **응답 기준을 무선랜 보안조치를 실행한 사업체로 한정한 경우**

그림 1-3-98 무선랜 보안을 위한 조치 (복수응답) - 무선랜 보안조치 실행 사업체

(단위 : %)



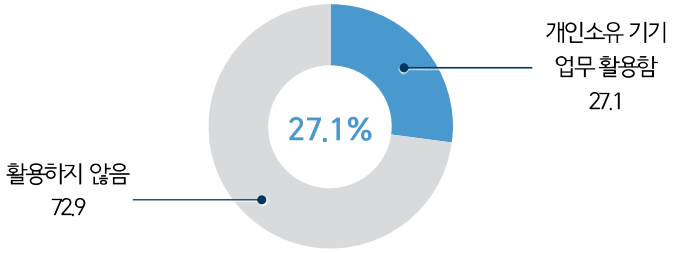
# 2. 모바일

## 가. 모바일 기기 업무 활용

개인소유의 모바일 기기(스마트폰, 스마트패드, 노트북 등)를 업무에 활용하는 사업체는 27.1%로 나타났다.

그림 1-3-99 개인소유 모바일 기기 업무 활용

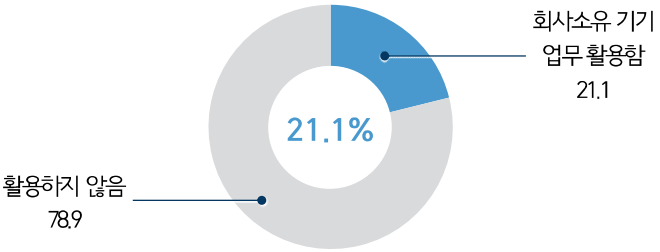
(단위 : %)




한편, 회사소유의 모바일 기기를 업무에 활용하고 있는 비율은 21.1%로 조사되었다.

그림 1-3-100 회사소유 모바일 기기 업무 활용

(단위 : %)

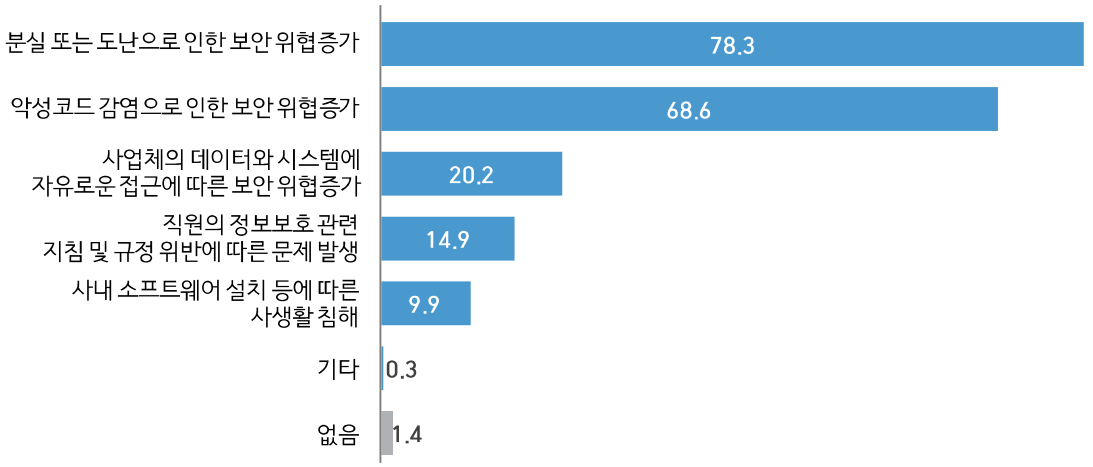


## 나. 모바일 보안

개인소유의 모바일 기기를 업무에 활용 시 보안 우려사항은 '분실 또는 도난으로 인한 보안 위협증가'가 78.3%로 가장 높게 나타났고, 다음으로 '악성코드 감염으로 인한 보안 위협증가(68.6%)' 등의 순으로 조사되었다.

그림 1-3-101 개인 모바일 기기 활용 시 보안 우려사항 (2가지) - 개인 소유 모바일 기기 이용 사업체

(단위 : %)

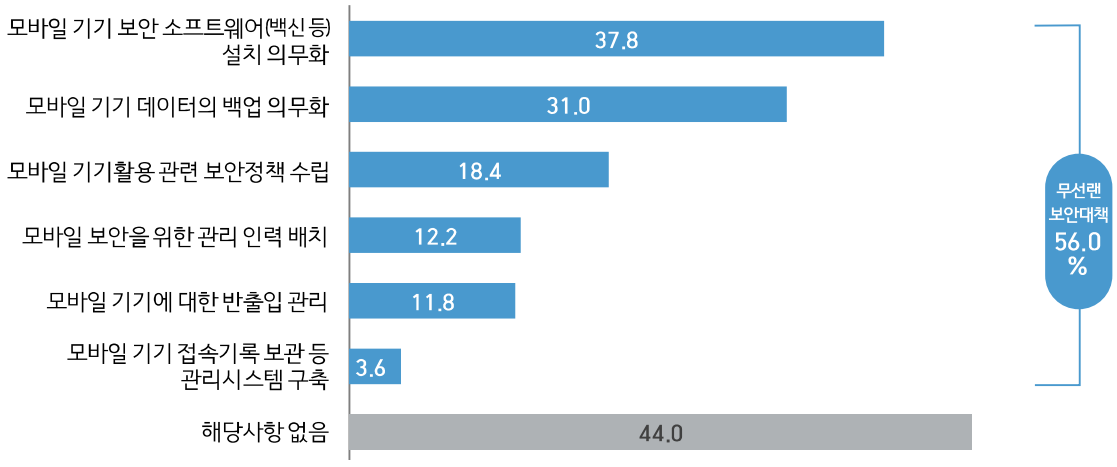



업무에 모바일 기기를 활용하는 사업체 중 56.0%가 모바일 기기 활용 시 발생할 수 있는 보안위협에 대해 대응방안을 갖추고 있는 것으로 나타났다.

대응방안으로는 '모바일 기기 보안 소프트웨어(백신 등) 설치 의무화'가 37.8%로 가장 높게 나타났고, 다음으로 '모바일 기기 데이터의 백업 의무화(31.0%)' 등의 순으로 조사되었다.

그림 1-3-102 모바일 기기 활용 시 보안 위협에 대한 대응 방안 (복수응답) - 모바일 기기 이용 사업체

(단위 : %)



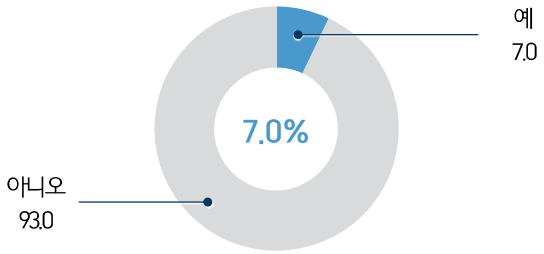
# 3. 클라우드

## 가. 클라우드 서비스 이용

국내 사업체 중 7.0%가 클라우드 서비스를 현재 이용하고 있는 것으로 나타났다.

그림 1-3-103 클라우드 서비스 이용

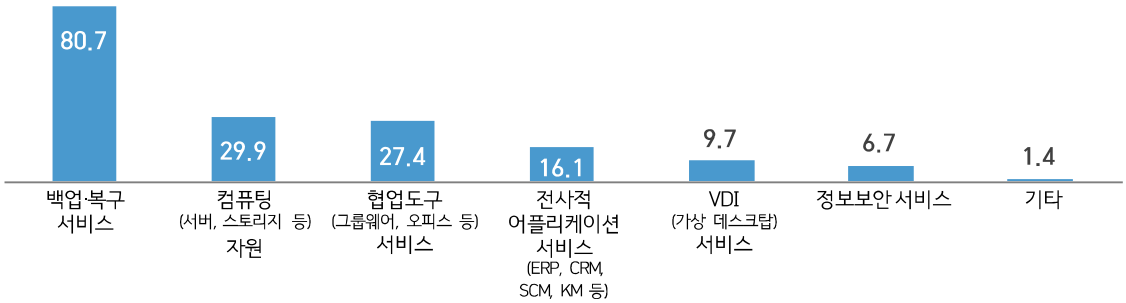
(단위 : %)




현재 이용하고 있는 클라우드 분야는 '백업·복구 서비스'가 80.7%로 가장 높게 나타났고, 다음으로 '컴퓨팅(서버, 스토리지 등) 자원(29.9%)', '협업도구(그룹웨어, 오피스 등) 서비스(27.4%) 등의 순으로 조사되었다.

그림 1-3-104 클라우드 서비스 이용 분야 (복수응답) - 클라우드 서비스 이용 사업체

(단위 : %)



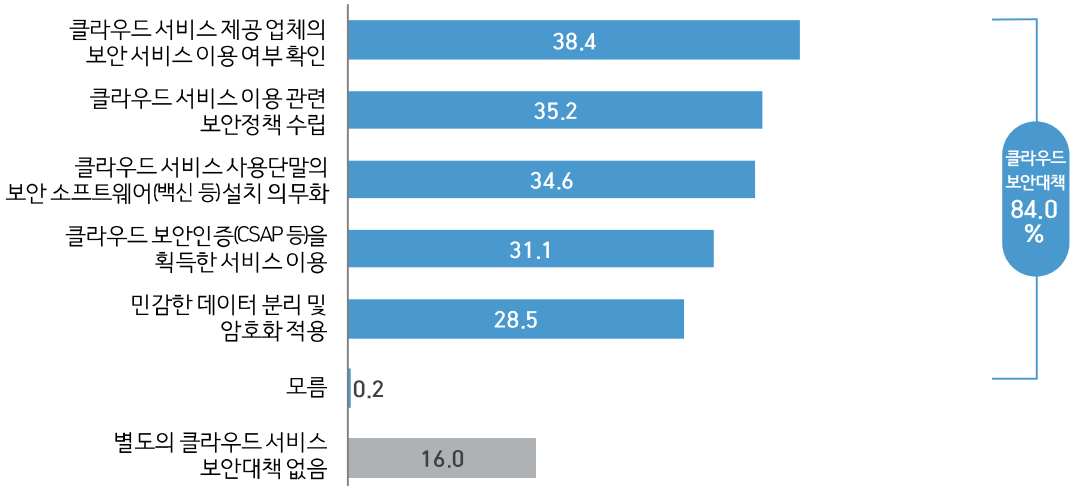
## 나. 클라우드 보안

클라우드 서비스를 현재 이용하고 있는 사업체 중 84.0%가 클라우드 서비스 보안을 위한 조치를 취하고 있는 것으로 나타났다.

조치 유형별로는 '클라우드 서비스 제공 업체의 보안 서비스 이용 여부 확인'이 38.4%로 가장 높게 나타났고, 다음으로 '클라우드 서비스 이용 관련 보안정책 수립(35.2%)' 등의 순으로 조사되었다.

그림 1-3-105 클라우드 서비스 보안을 위한 조치 (복수응답) - 클라우드 서비스 이용 사업체

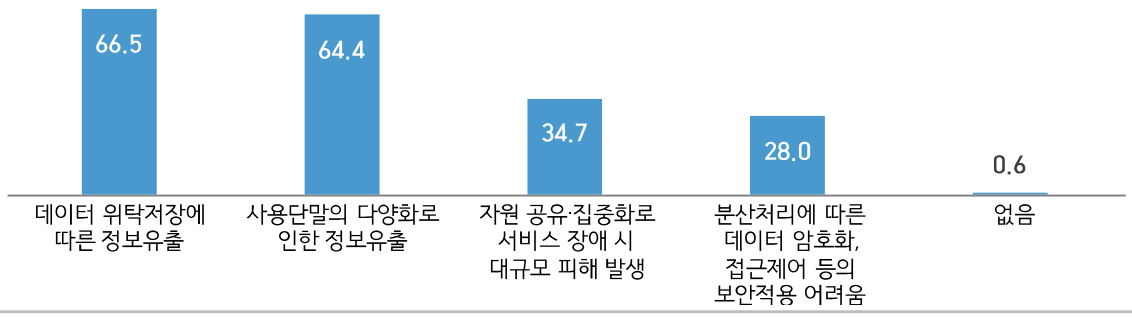
(단위 : %)




클라우드 서비스 이용과 관련하여 발생할 수 있는 보안 우려사항은 '데이터 위탁저장에 따른 정보유출'이 66.5%로 가장 높게 나타났고, 다음으로 '사용단말의 다양화로 인한 정보유출(64.4%)' 등의 순으로 조사되었다.

그림 1-3-106 클라우드 서비스 보안 우려사항 (2가지)

(단위 : %)



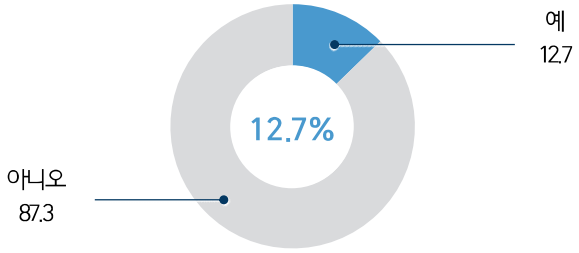
# 4. 사물인터넷(IoT)

## 가. 사물인터넷(IoT) 제품·서비스 이용

국내 사업체 중 12.7%가 사물인터넷(IoT) 제품 또는 서비스를 현재 이용하고 있는 것으로 나타났다.

그림 1-3-107 사물인터넷(IoT) 제품·서비스 이용

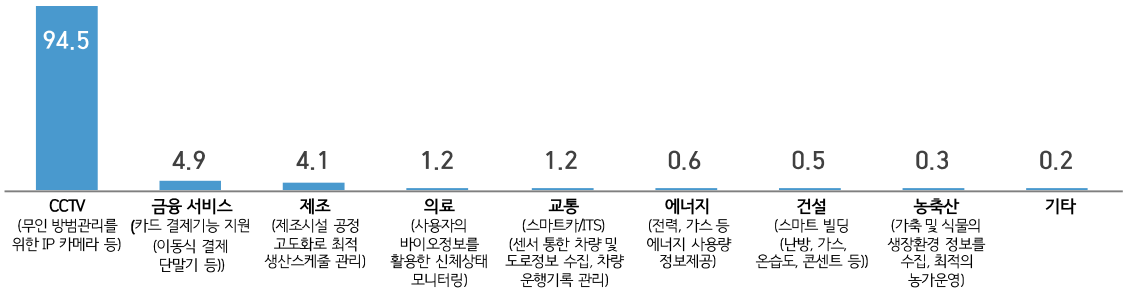
(단위 : %)




현재 이용하고 있는 사물인터넷(IoT) 분야는 'CCTV'가 94.5%로 가장 높게 나타났고, 다음으로 '금융 서비스(4.9%)', '제조(4.1%)' 등의 순으로 조사되었다.

그림 1-3-108 사물인터넷(IoT) 제품·서비스 이용 분야 (복수응답) - 사물인터넷(IoT) 제품·서비스 이용 사업체

(단위 : %)

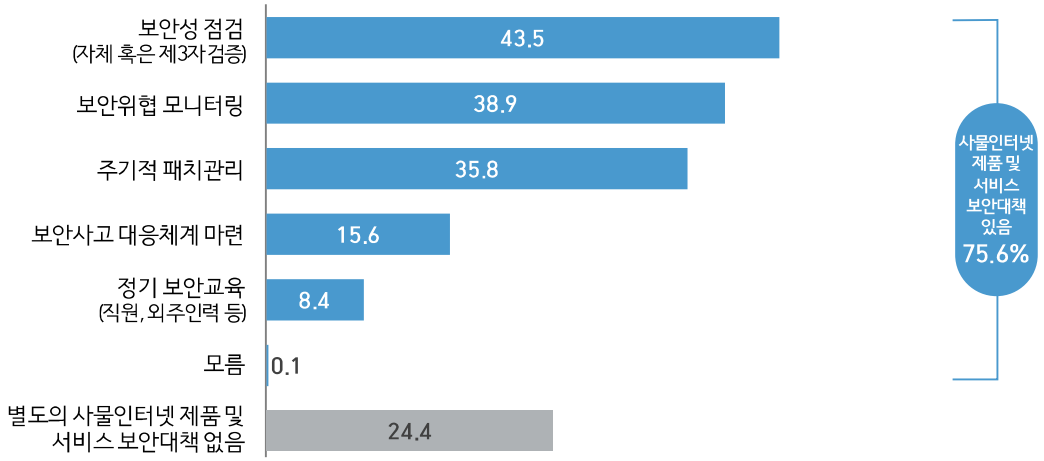


## 나. 사물인터넷(IoT) 보안

사물인터넷(IoT) 제품 또는 서비스 이용 사업체 중 75.6%가 사물인터넷(IoT) 제품 및 서비스의 보안을 위해 조치를 취하고 있는 것으로 나타났다.

그림 1-3-109 사물인터넷(IoT) 제품·서비스 보안을 위한 조치 (복수응답) - 사물인터넷(IoT) 이용 사업체

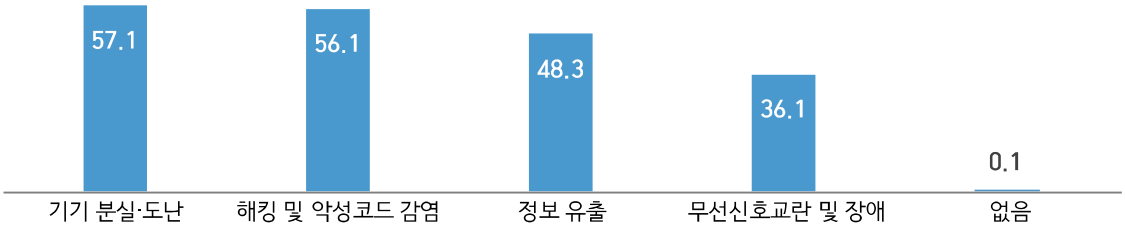
(단위 : %)




사물인터넷(IoT) 환경에서 발생할 수 있는 보안위협에 대한 우려 정도는 '기기 분실·도난'이 57.1%로 가장 높게 나타났고, 다음으로 '해킹 및 악성코드 감염(56.1%)' 등의 순으로 조사되었다.

그림 1-3-110 사물인터넷(IoT) 관련 보안 우려사항

(단위 : %)



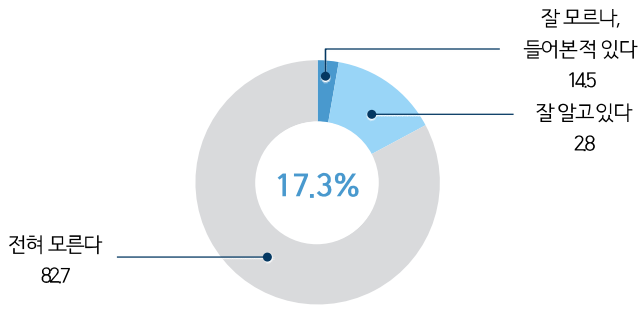
# 5. 사이버(정보보호, 개인정보보호) 보험

## 가. 사이버(정보보호, 개인정보보호) 보험 인지

국내 사업체 중 17.3%가 사이버(정보보호, 개인정보보호) 보험에 대해 인지(잘 모르나, 들어본 적 있다 + 잘 알고 있다)하고 있는 것으로 나타났다.

그림 1-3-111 사이버(정보보호, 개인정보보호) 보험 인지

(단위 : %)

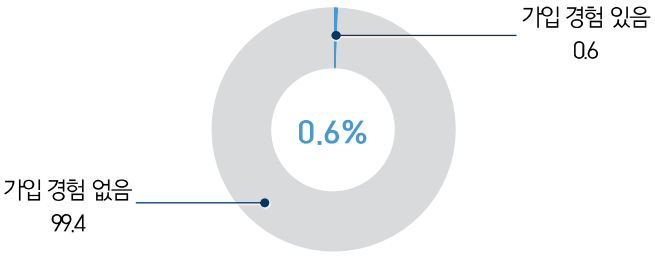



## 나. 사이버(정보보호, 개인정보보호) 보험 이용

국내 사업체 중 0.6%가 사이버(정보보호, 개인정보보호) 보험에 가입한 경험이 있는 것으로 나타났다.

그림 1-3-112 사이버(정보보호, 개인정보보호) 보험 가입

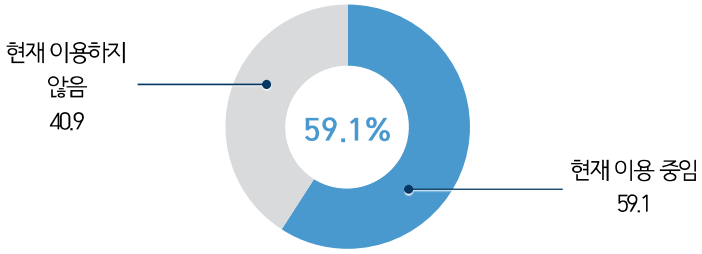
(단위 : %)



사이버(정보보호, 개인정보보호) 보험 가입 경험이 있는 사업체 중 59.1%가 현재 이용 중인 것으로 나타났다.

그림 1-3-113 사이버(정보보호, 개인정보보호) 보험 이용 - 사이버 보험 가입 경험 있는 사업체

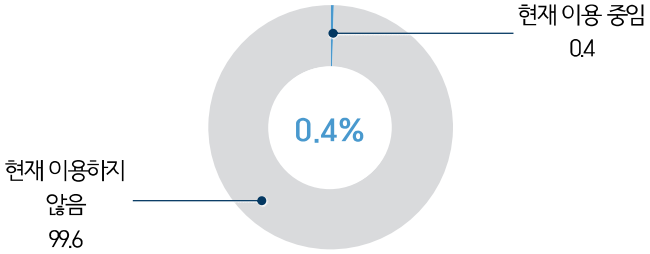
(단위 : %)




▶ **참고** **응답 기준을 전체 사업체로 확대한 경우**

그림 1-3-114 사이버(정보보호, 개인정보보호) 보험 이용

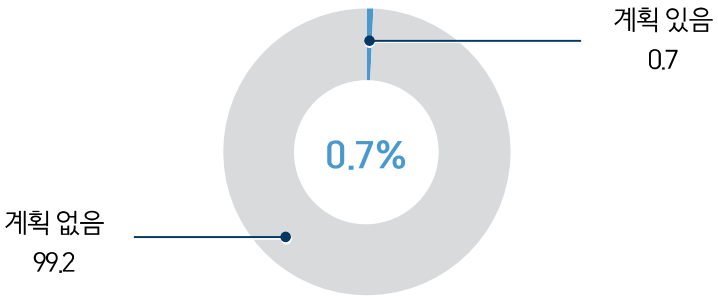
(단위 : %)



향후 사이버(정보보호, 개인정보보호) 보험을 신규로 가입하거나, 현재 이용 중인 보험을 유지할 계획이 있는 사업체의 비율은 0.7%로 나타났다.

그림 1-3-115 사이버(정보보호, 개인정보보호) 보험 향후 가입(유지) 계획

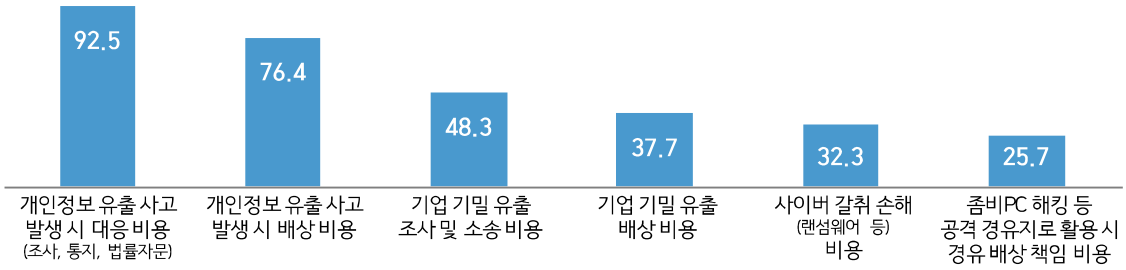
(단위 : %)




사이버(정보보호, 개인정보보호) 보험을 향후 신규로 가입할 계획이 있는 사업체가 희망하는 보장 항목은 '개인정보 유출 사고 발생 시 배상 비용'이 92.5%로 가장 높게 나타났고, 다음으로 '개인정보 유출 사고 발생 시 배상 비용(76.4%)' 등의 순으로 조사되었다.

그림 1-3-116 사이버(정보보호, 개인정보보호) 보험 희망 보장 항목 (복수응답) - 향후 가입 계획 사업체

(단위 : %)



# 6. 주요 서비스 정보보호 투자

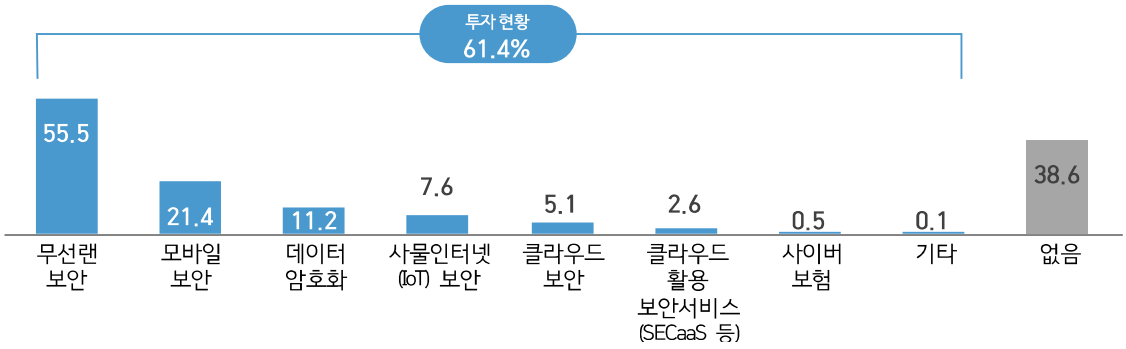
## 가. 주요 서비스 정보보호 투자 현황

국내 사업체 중 61.4%가 현재 정보보호를 위해 IT보안 분야에 투자를 하고 있는 것으로 나타났다.

투자 유형별로는 '무선랜 보안'이 55.5%로 가장 높게 나타났고, 다음으로 '모바일 보안(21.4%)', '데이터 암호화(11.2%)' 등의 순으로 조사되었다.

그림 1-3-117 주요 서비스 정보보호 투자 현황 (복수응답)

(단위 : %)



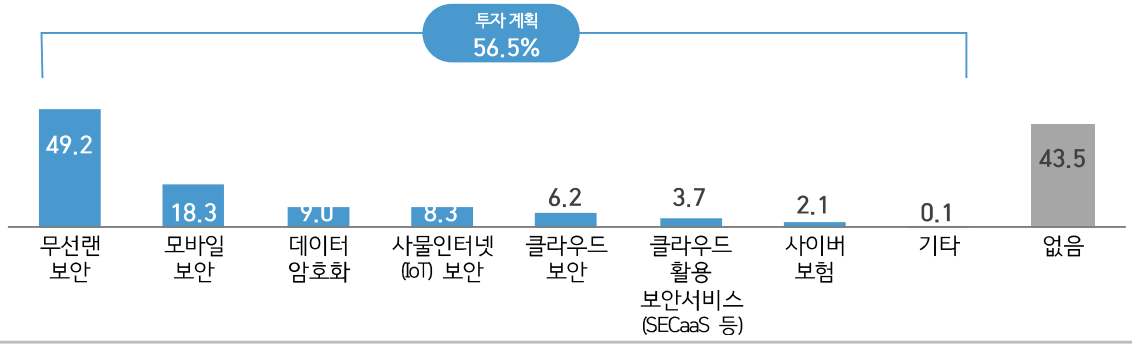

## 나. 주요 서비스 정보보호 투자 계획

국내 사업체 중 56.5%가 향후 정보보호를 위해 IT보안 분야에 투자할 계획을 보유하고 있는 것으로 나타났다.

신규 투자 유형별로는 '무선랜 보안'이 49.2%로 가장 높게 나타났고, 다음으로 '모바일 보안(18.3%)', '데이터 암호화(9.0%)' 등의 순으로 조사되었다.

그림 1-3-118 주요 서비스 정보보호 투자 계획 (복수응답)

(단위 : %)



# 2부

## 개인부문

# 제1장

# 조사개요

# 제1장 조사개요

## 1. 조사 목적

급속하게 변화하는 인터넷 환경과 사물인터넷(IoT), IP카메라 등 새로운 기술의 끊임없는 등장으로 사이버 세계의 위협이 현실세계로 확대되고 그 위협 또한 고도화·지능화 되고 있다. 이에 따라 정보보호 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 제공하는데 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 이용자'로 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 조사대상 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 인터넷 이용실태조사' 결과를 기반으로 표본 재설계
- 조사구 추출-가구 추출-가구원 추출의 다단계층화추출로 표본추출 방법 변경

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

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

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

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

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

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

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

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

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

## 3. 조사 내용 및 범위

본 조사는 개인(인터넷 이용자)의 정보보호 인식, 침해사고 예방, 침해사고 대응, 개인정보보호, 주요 서비스별 정보보호에 관한 현황을 파악할 수 있는 설문으로 구성하였다.

본 조사의 주요 내용은 다음과 같다

- 정보보호의 중요성 및 정보보호 위협사안에 대한 인지, 심각성
- 정보보호를 위한 정보수집, 학습활동
- 정보보호 제품/서비스 이용 및 정보보호를 위한 관리 활동
- 침해사고 현황 및 대응 조치
- 개인정보 침해 현황 및 개인정보 침해 예방·대응 조치
- 신규 기술/서비스 이용 현황 및 보안상의 우려

## 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 의미. 금융기관 또는 공공기관을 가장해 전화나 이메일로 인터넷 사이트에서 보안카드 일련번호와 코드번호 일부 또는 전체를 입력하도록 요구해 금융 정보를 몰래 빼가는 수법
- **파밍** : 악성코드에 감염된 PC를 조작해 이용자가 인터넷 즐겨찾기 또는 포털사이트 검색을 통하여 금융회사 등의 정상적인 홈페이지 주소로 접속하여도 피싱(가짜)사이트로 유도되어 범죄자가 개인 금융 정보 등을 몰래 빼가는 수법
- **스미싱** : 문자 메시지를 이용한 새로운 휴대폰 해킹 기법. 웹사이트 링크가 포함된 문자 메시지를 보내 휴대폰 사용자가 링크를 클릭하면 트로이목마를 주입해 범죄자가 휴대폰을 통제하는 등의 수법
- **카드 사기/불법결제** : 신용카드 또는 직불카드 사기, 불법결제 등으로 인한 금전적 피해로 가짜 ATM기 사용으로 인한 카드정보 도용, 카드 불법복제 등을 의미

- **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
- **개인정보침해** : 개인정보가 분실, 도난, 유출 등을 통해 수집·이용되거나 제3자에게 제공되어 발생하는 피해
- **클라우드 서비스** : 개인의 사진、문서、동영상 등 각종콘텐츠를 '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)*
  * 60~69세는 2018년에 신규 조사대상으로 추가
- 유효 응답자 수 : 4,500명
- 조사주기 : 연 1회
- 조사기간 : 2020년 8월 3일~10월 30일 (3개월)
- 조사방법 : 가구방문 면접조사
- 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. 표본설계

### 가. 모집단

➪ 목표 모집단(Target Population) : 국내 만12~69세 인터넷 이용자

➪ 조사 모집단(Survey Population) : 국내 만12~69세의 인터넷 이용자 중 최근 1개월 이내 인터넷 이용자

➪ 모집단 자료
- 통계청 『2019년 추계인구』 및 한국인터넷진흥원의 『2019년 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 900개 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 : %)

| 표본의 크기 | 3,000 | 3,500 | 3,600 | 3,800 | 4,000 | 4,200 | 4,400 | **4,500** | 4,600 |
|---|---|---|---|---|---|---|---|---|---|
| 표본오차 | 1.17 | 1.08 | 1.07 | 1.04 | 1.01 | 0.99 | 0.97 | 0.96 | 0.95 |

- 최종 표본의 크기는 표본오차가 ±0.96%p 내에서 통제되도록 4,500명으로 결정함 (95% 신뢰수준)

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

➪ 표본틀 : 통계청 2019년 '추계인구' 및 한국인터넷진흥원 '2019년 인터넷이용실태조사'에서 파악된 성별, 연령별, 국내 인터넷 이용자 수 및 분포 활용

## 표본 할당 및 추출 방법

① 표본 할당

- 만 12~69세 인터넷이용자 크기에 비례하여 4,500명을 지역별 제곱근비례할당 후, 각 지역에 표본을 우선 할당하고, 성X연령 셀에 할당하는 방법을 최종 표본 할당 방법으로 결정함

② 조사구 할당

- 조사구당 5명이 조사되도록 총 900개 조사구 배분
- 1차 : 17개 시도별 조사구 배분
  * 통계청의 『2019년 추계인구』, 한국인터넷진흥원의 『2019년 인터넷이용실태조사』 인터넷 이용률 결과를 기반으로 17개 시도별 인터넷 이용자 크기에 비례하여 900개 조사구 배분
- 2차 : 시도 내 주거형태별 조사구 배분
  * 통계청의 『2018년 등록센서스』 기준 17개 시도별 주거 형태(아파트 및 아파트 외) 분포에 비례하여, 아파트 조사구와 비아파트 조사구 배분

③ 조사구 추출

- 366,846개 조사구를 행정구역 코드에 따라 정렬하여 계통 추출
- 계통 추출 17개 지역*2개 동읍면부*4개 주거형태별 셀 내에 조사구를 행정구역 코드별로 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 해당가구를 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( $i-1$, 혹은 $i+1$)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 빠른 가구원을 조사함

# 7. 실사

## 가. 실사개요

➔ 조사기간
- 2020년 8월 3일~10월 30일 (3개월)

➔ 조사기준
- 2019년 7월 1일 ~ 2020년 6월 30일
- 침해사고 경험은 2019년 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 장기부재, 강력한 응답 거부 등으로 조사가 불가능한 경우에는 동일 조사구내에서 1차 추출된 원표본과 동일한 가구 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
- 실사 감독원의 1차 검증에서 합격된 설문지는 에디팅 및 입력 과정에서 전산프로그램에 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, 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 부호화 하거나 자료 입력 시 제외함

# 9. 추정 및 표본오차

## 가. 가중치 산출

➔ '사후층화(post-stratification)' 방법에 따라 가중치 산출 및 적용
- 본 조사는 조사구를 활용한 가구방문 면접조사로 진행되어 표본의 구성 비율이 모집단 구성 비율과 차이가 있으므로 가중치에 의한 사후추정 필요

➔ 통계청의 『2019년 추계인구』와 한국인터넷진흥원의 『2019년 인터넷이용실태조사』 인터넷 이용률 결과를 모집단으로 활용하여 지역별×성별×연령별 가중치 $W_{(k,s,h)}$를 산출하였으며, 가중치 산출 공식은 다음과 같음

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

| | |
|---|---|
| $W_{(k,s,h)}$ | $(k,s,h)$셀의 가중치 |
| $N_{(k,s,h)}$ | $(k,s,h)$셀의 모집단 인구수 |
| $n_{(k,s,h)}$ | $(k,s,h)$셀의 최종 조사된 표본수 |
| $k$ | 연령(만12-19세, 20대, 30대, 40대, 50대, 60대)을 나타내는 첨자 $(k=1 \sim 6)$ |
| $s$ | 성을 나타내는 첨자$(s=1,2)$ |
| $h$ | 지역(17개 시도)을 나타내는 첨자$(h=1 \sim 17)$ |

## 나. 추정

➔ 전체 모비율 추정 산출 공식은 다음과 같음

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

| | |
|---|---|
| $\hat{p}$ | 특정 변수에 대한 모비율 |
| $\hat{p}_{ksh}$ | 특정 변수에 대한 $(k,s,h)$셀의 모비율 |
| $w_{ksh}$ | $(k,s,h)$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 - $1.96\times\sqrt{\hat{V}(\hat{p}_{hsk})}$

| | |
|---|---|
| $\hat{V}(\hat{p})$ | 전체 모비율에 대한 분산 |
| $\hat{V}(\hat{p}_{ksh})$ | 층별 모비율에 대한 분산 |

➔ 분산 산출 공식은 다음과 같음

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

➔ 따라서, 본 조사의 표본 추출과정에서 발생할 수 있는 주요문항에 대한 표본오차는 다음과 같음

표 2-1-2 정보보호 제품 이용률 추정 결과 및 표본오차

| | |
|---|---|
| 정보보호 제품 이용률 표본오차 | ±0.96%p (95% 신뢰수준) |
| 정보보호 제품 이용률 추정 결과 | 87.81% ±0.96%p |

## 10. 결과 공표 및 활용분야

➔ 『2020년 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) 등에서 국제기구·기관의 지표개발 논의 등을 위한 참고자료로 활용됨

## 11. 모집단 및 표본 현황

표 2-1-3 모집단 및 표본 현황

(단위 : %)

| | | 만12~69세 최근 1개월 이내 인터넷이용자 | | 응답 현황 | |
|---|---|---|---|---|---|
| | | 모집단 수(명) | 비율(%) | 표본 수(명) | 비율(%) |
| **전 체** | | **40,620,408** | **100.0** | **4,500** | **100.0** |
| 성별 | 남 | 20,863,754 | 51.4 | 2,286 | 50.8 |
| | 여 | 19,756,654 | 48.6 | 2,214 | 49.2 |
| 연령별 | 12-19세 | 3,988,782 | 9.8 | 589 | 13.1 |
| | 20대 | 6,987,220 | 17.2 | 763 | 17.0 |
| | 30대 | 7,361,627 | 18.1 | 776 | 17.2 |
| | 40대 | 8,326,693 | 20.5 | 837 | 18.6 |
| | 50대 | 8,530,814 | 21.0 | 853 | 19.0 |
| | 60대 | 5,425,272 | 13.4 | 682 | 15.2 |
| 지역별 | 서울 | 7,814,086 | 19.2 | 528 | 11.7 |
| | 부산 | 2,657,108 | 6.5 | 309 | 6.9 |
| | 대구 | 1,953,809 | 4.8 | 265 | 5.9 |
| | 인천 | 2,354,295 | 5.8 | 290 | 6.4 |
| | 광주 | 1,179,872 | 2.9 | 206 | 4.6 |
| | 대전 | 1,221,443 | 3.0 | 210 | 4.7 |
| | 울산 | 928,144 | 2.3 | 182 | 4.0 |
| | 세종 | 256,895 | 0.6 | 96 | 2.1 |
| | 경기 | 10,421,162 | 25.7 | 610 | 13.6 |
| | 강원 | 1,129,582 | 2.8 | 201 | 4.5 |
| | 충북 | 1,276,674 | 3.1 | 214 | 4.8 |
| | 충남 | 1,686,446 | 4.2 | 246 | 5.5 |
| | 전북 | 1,337,763 | 3.3 | 219 | 4.9 |
| | 전남 | 1,274,667 | 3.1 | 215 | 4.8 |
| | 경북 | 2,045,993 | 5.0 | 271 | 6.0 |
| | 경남 | 2,579,710 | 6.4 | 304 | 6.8 |
| | 제주 | 502,759 | 1.2 | 134 | 3.0 |

제2장

# 조사결과 요약

# Ⅰ 정보보호 인식

## 1. 정보보호 중요성 인식

**인터넷 이용자의 92.3%는 '정보보호'가 중요하다고 인식**

▶ 정보보호가 중요하다(중요한 편이다 + 매우 중요하다)고 인식하는 비율은 92.3%로, 전년(95.3%) 대비 3.0%p 감소함
- 중요성 인식률은 20~30대(95.2%)가 가장 높음
- 60대의 정보보호 중요성 인식률은 87.9%로 가장 낮음

그림 2-2-1 정보보호 중요성 인식률

(중요한 편이다 + 매우 중요하다, 단위 : %)

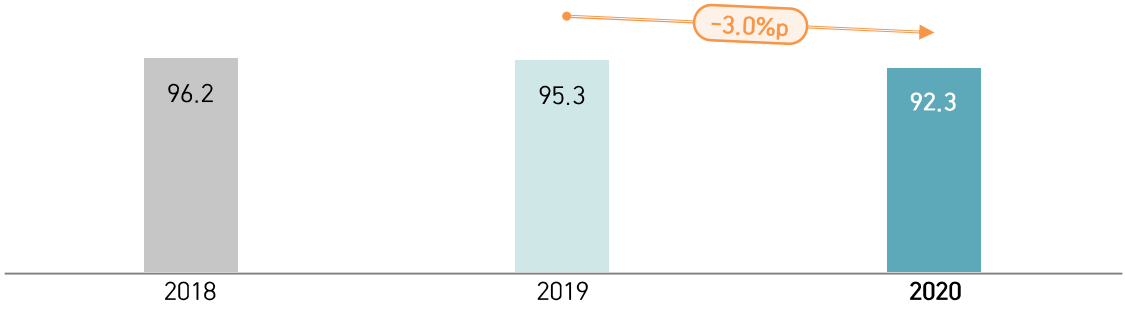
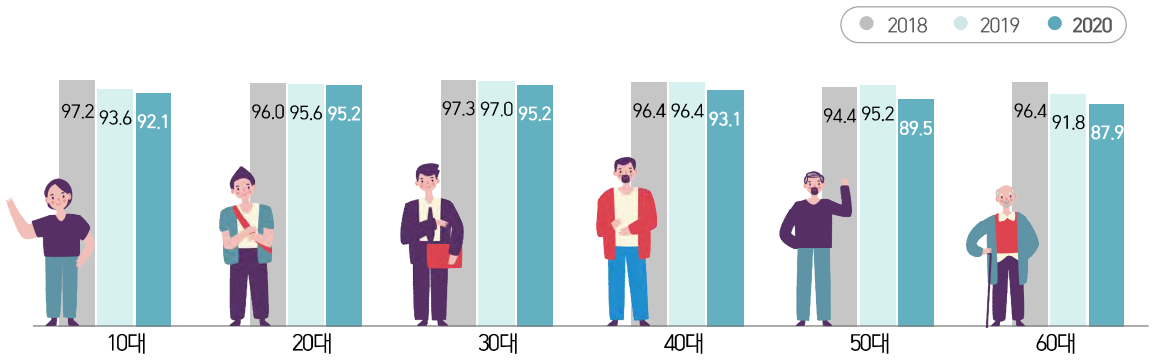



그림 2-2-2 연령별 정보보호 중요성 인식률

(중요한 편이다 + 매우 중요하다, 단위 : %)



## 2. 개인정보보호 중요성 인식

### '개인정보보호'가 중요하다고 인식하는 비율 94.2%

▶ 개인정보보호가 중요하다(중요한 편이다 + 매우 중요하다)고 인식하는 비율은 94.2%로, 전년(97.3%) 대비 3.1%p 감소함
- 20대(96.7%), 30대(96.6%)가 높은 수준이고, 그 다음으로 40대(95.0%), 10대(94.6%) 순임
- 60대의 개인정보보호 중요성 인식률은 88.4%로 가장 낮음

그림 2-2-3 개인정보보호 중요성 인식률

(중요한 편이다 + 매우 중요하다, 단위 : %)

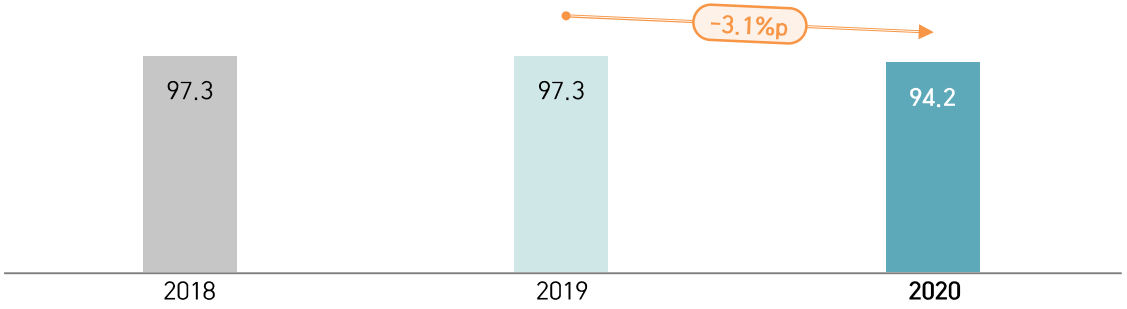
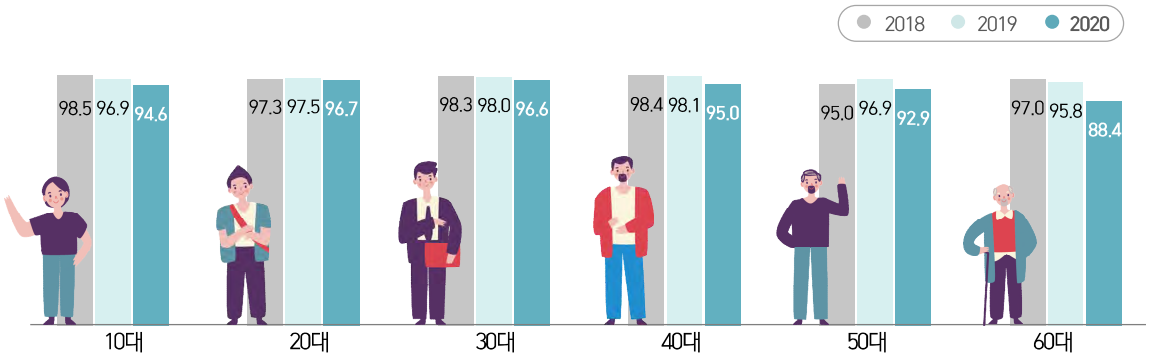



그림 2-2-4 연령별 개인정보보호 중요성 인식률

(중요한 편이다 + 매우 중요하다, 단위 : %)



# Ⅱ 침해사고 예방

## 1. 정보보호 제품 이용

**인터넷 이용자 10명 중 9명(87.8%)이 '정보보호 제품' 이용**

▶ PC 및 모바일 보안을 위해 정보보호 관련 제품을 이용한다고 응답한 비율은 87.8%로, 전년(87.9%)과 비슷함
- PC 이용자의 95.5%, 모바일 이용자의 86.6%가 정보보호 관련 제품을 이용함

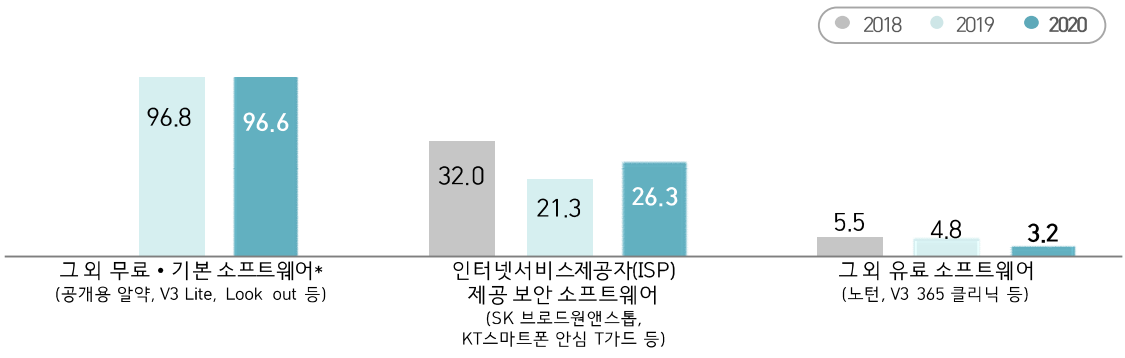
▶ 정보보호 제품 이용자는 '그 외 무료·기본 소프트웨어(96.6%)'를 가장 많이 이용하고, 그 다음으로 '인터넷서비스제공자(ISP) 제공 보안 소프트웨어(26.3%)'를 이용하는 것으로 나타남

그림 2-2-5 정보보호 제품 이용률

(단위 : %)


그림 2-2-6 정보보호 소프트웨어 이용률 (복수응답) - 정보보호 제품 이용자

(단위 : %)




* 2019년 보기 변경 : '그 외 무료 • 기본 소프트웨어'와 '운영체제에 탑재된 보안 소프트웨어' 항목을 통합

# 2. 침해사고 예방 활동

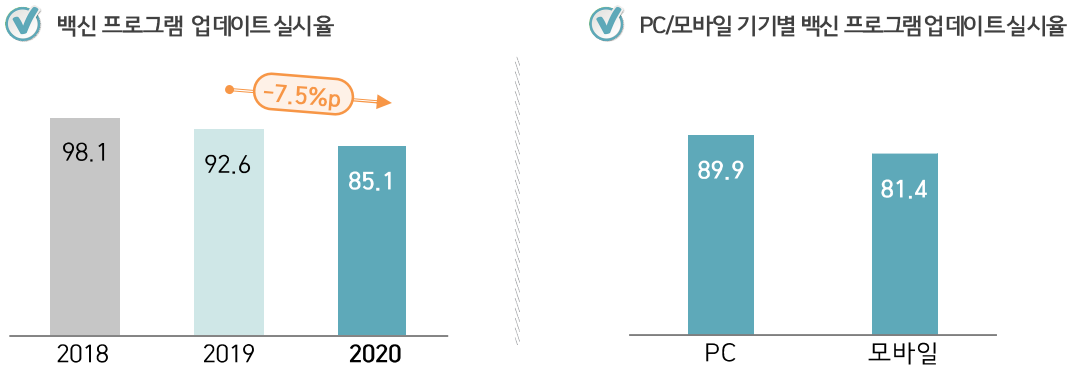
## 가. 백신 프로그램 업데이트

**정보보호 제품 이용자의 85.1%는 '백신 프로그램 업데이트' 실시**

▶ 백신 프로그램 업데이트 실시율은 85.1%로, 전년(92.6%) 대비 7.5%p 감소함
- PC 이용자의 89.9%, 모바일 이용자의 81.4%가 백신 프로그램을 업데이트 함

그림 2-2-7 백신 프로그램 업데이트 실시율 - 정보보호 제품 이용자

(단위 : %)



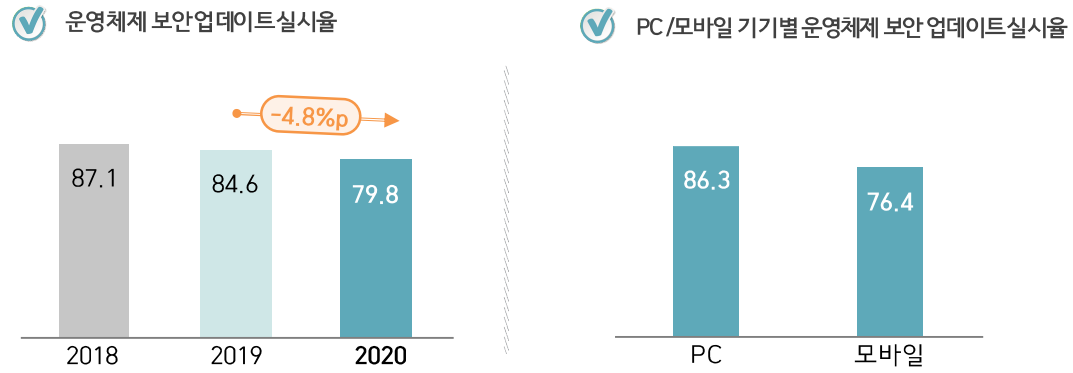

## 나. 운영체제 보안 업데이트

**인터넷 이용자의 79.8%는 '운영체제 보안 업데이트' 실시**

▶ 운영체제 보안 업데이트 실시율은 79.8%로, 전년(84.6%) 대비 4.8%p 감소함
- PC 이용자의 86.3%, 모바일 이용자의 76.4%가 운영체제 보안 업데이트를 실시함

그림 2-2-8 운영체제 보안 업데이트 실시율

(단위 : %)



## 다. 중요 데이터 백업

**인터넷 이용자의 47.0%는 '중요 데이터 백업' 실시**

- PC 또는 모바일에 저장된 중요 데이터를 백업하는 비율은 47.0%로 전년(50.7%) 대비 3.7%p 감소함
- PC 내 중요 데이터 백업 방식은 'USB메모리, 외장하드 디스크, 마이크로 SD카드 등 별도 저장장치 활용'하는 비율이 78.3%로 가장 높음
  반면, 모바일은 '클라우드 서버 활용(82.2%)'을 통한 백업 실시율이 가장 높음

그림 2-2-9 중요 데이터 백업률

(단위 : %)

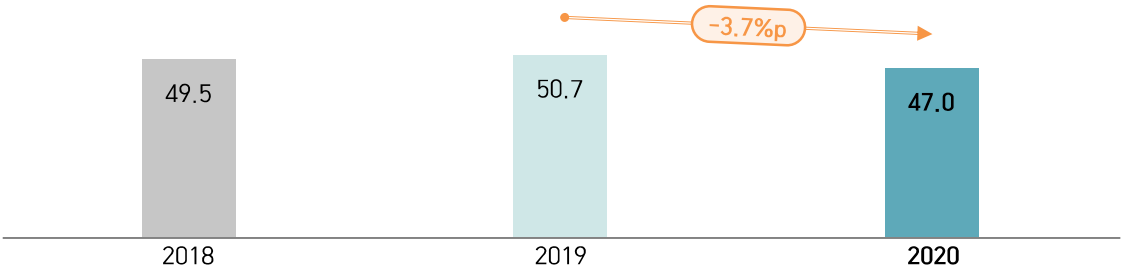
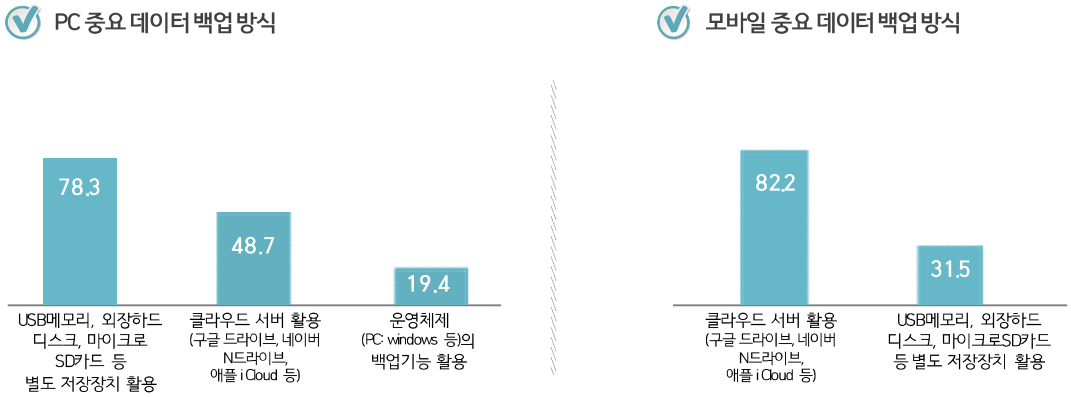



그림 2-2-10 중요 데이터 백업 방식 (복수응답) - PC/모바일 이용자 중 중요 데이터 백업 실시자

(단위 : %)



## 라. PC 비밀번호 설정

### PC 이용자의 68.5%는 'PC 이용 시 비밀번호 설정'

- PC 사용 시 비밀번호를 설정하는 비율은 68.5%로 전년(79.5%) 대비 11.0%p 감소함
- PC 비밀번호를 하나라도 설정하고 있는 응답자 기준, '운영체제(윈도우 등) 로그인 시' 비밀번호를 설정한다는 비율이 83.8%로 가장 높고, '화면 보호기능 해제 시(55.5%)', '중요 데이터 파일 저장 시(44.6%)' 설정 비율이 그 뒤를 이음

그림 2-2-11 PC 비밀번호 설정률 - PC 이용자

(단위 : %)

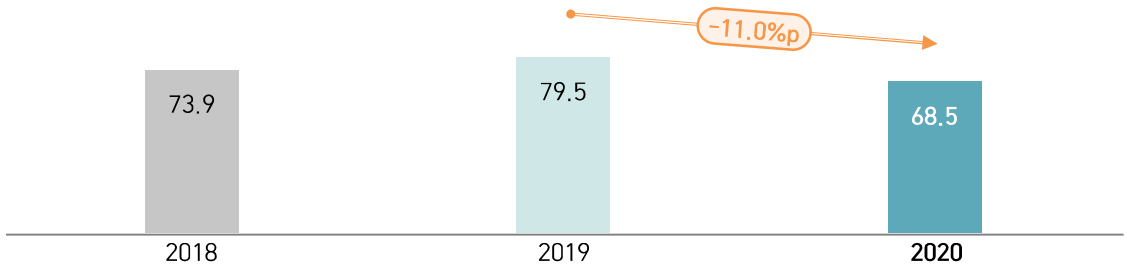
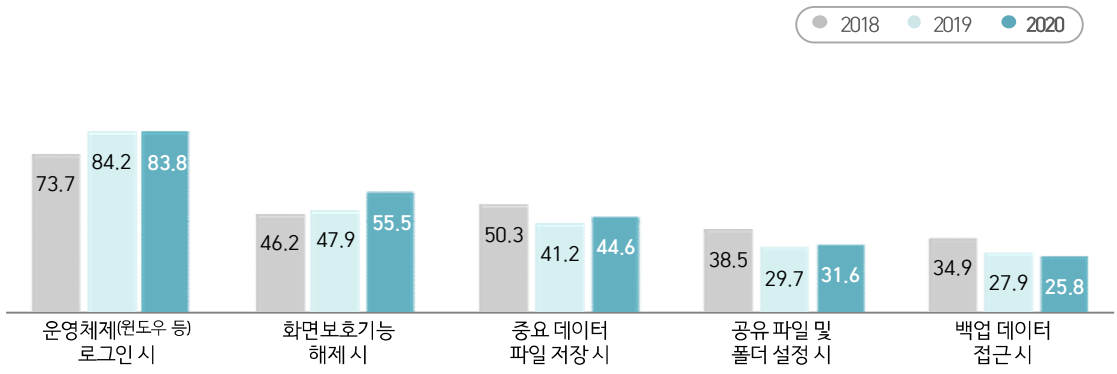



그림 2-2-12 PC 비밀번호 설정 유형 (복수응답) - PC 비밀번호 설정 응답자

(단위 : %)



# Ⅲ 침해사고 대응

## 1. 침해사고 경험

**인터넷 이용자의 3.3%가 정보보호 침해사고 경험**

▶ 2019년 1년간 악성코드 감염, 개인정보 유출 등 침해사고를 경험한 비율은 3.3%로, 전년(4.2%) 대비 0.9%p 감소함
- PC 이용자의 3.2%, 모바일 이용자의 1.4%가 침해사고를 경험함

▶ 침해사고는 '악성코드 감염 등으로 인한 피해'가 1.9%로 가장 많았고, '개인정보 유출 및 사생활 침해(1.2%)', '피싱/파밍/스미싱 등으로 인한 금전적 피해(0.8%)'가 그 뒤를 이음

그림 2-2-13 침해사고 경험률

(단위 : %)

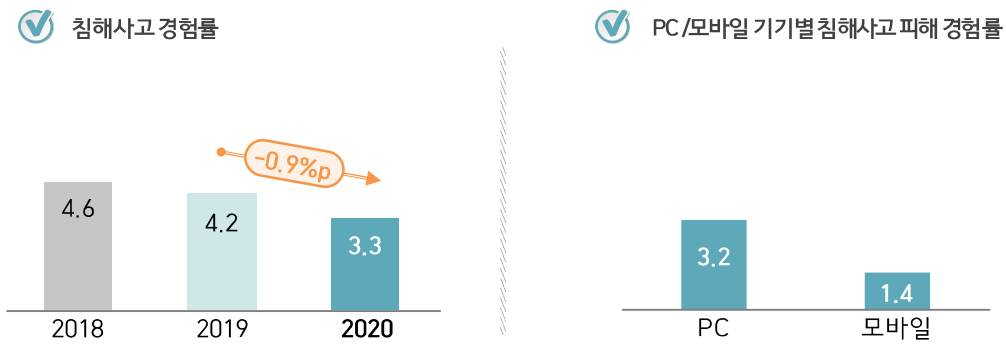
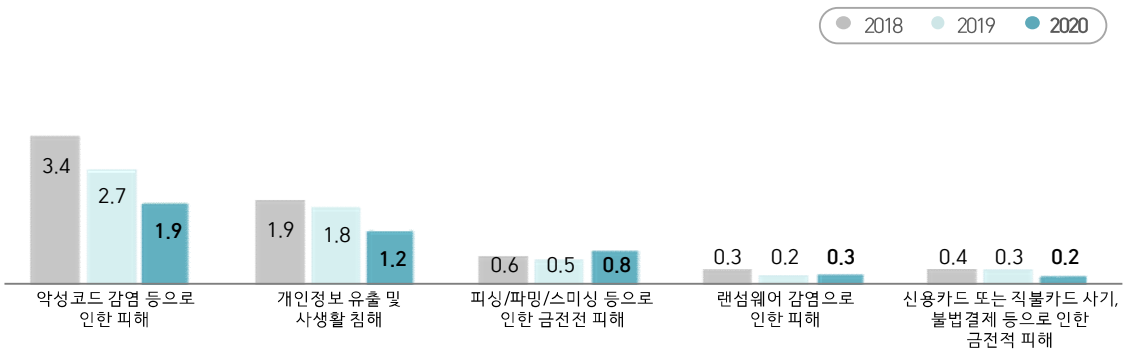



그림 2-2-14 침해사고 경험 유형 (복수응답)

(단위 : %)



## 2. 침해사고 대응

**'침해사고 대응활동' 수행률 85.9%, 전년 대비 1.7%p 증가**

- 침해사고 경험 이후 대응활동을 수행한 비율은 85.9%로, 전년(84.2%) 대비 1.7%p 증가함
- 대응활동 유형으로는 '사용 중인 비밀번호 변경'이 45.6%로 가장 많았고, 다음으로 '스스로 점검 및 예방활동 강화(44.1%)', '보안 소프트웨어 설치(28.8%)' 등의 순임

그림 2-2-15 침해사고 대응률 - 침해사고 경험자

(단위 : %)

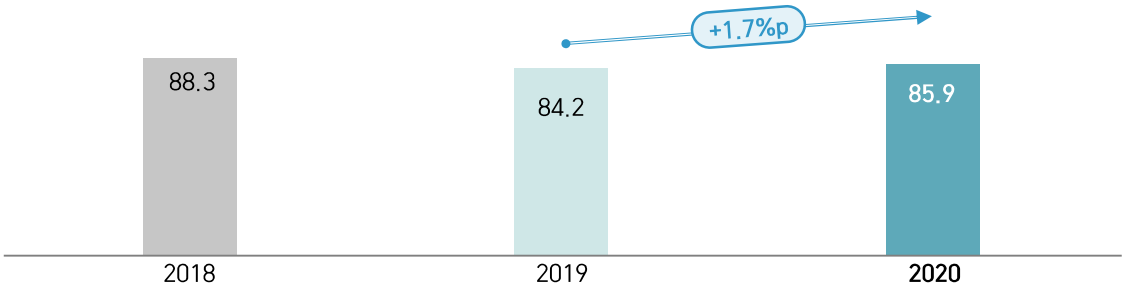
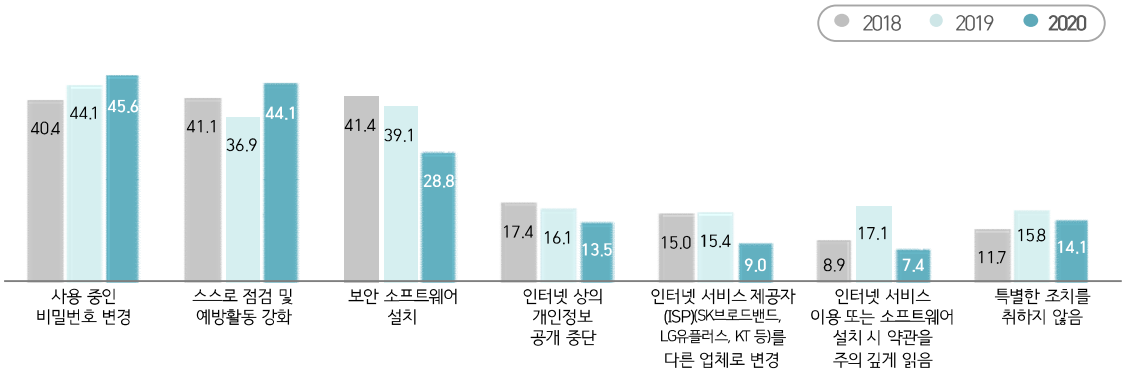



그림 2-2-16 침해사고 대응활동 수행 (복수응답) - 침해사고 경험자

(단위 : %)



# Ⅳ 개인정보보호

## 1. 개인정보 침해사고 예방

**인터넷 이용자 10명 중 9명(91.9%)이 개인정보 침해사고 유출 예방 조치함**

- 개인정보 유출 예방을 위해 조치를 취하고 있다고 응답한 비율은 91.9%로 전년(93.6%) 대비 1.7%p 감소함
- 유형별로는 '개인정보를 주의해서 관리하며 타인에게 알려주지 않음(78.7%)'이 가장 많고, 다음으로 '인터넷에서 파일을 함부로 다운로드 하지 않음(70.3%)', '금융거래 시 신용카드 번호와 같은 금융정보 등은 노출되지 않도록 함(51.1%)' 등의 순임

그림 2-2-17 개인정보 침해사고 예방 조치 실시율

(단위 : %)

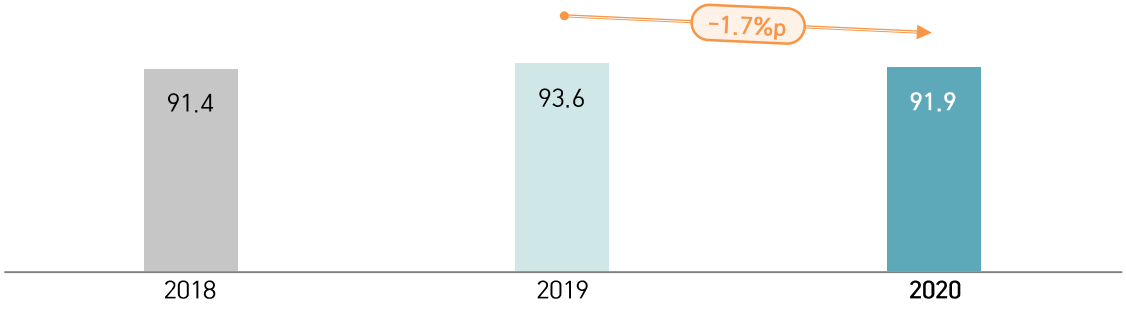
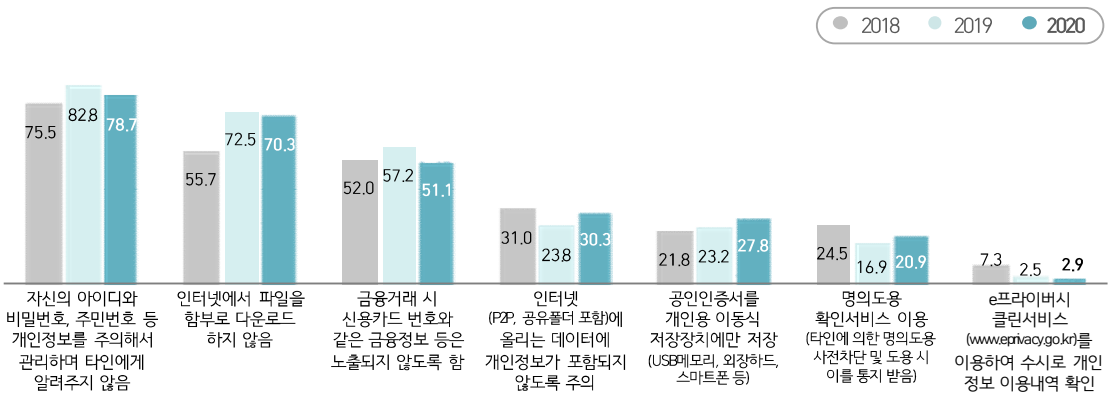



그림 2-2-18 개인정보 침해사고 예방 조치 유형 (복수응답)

(단위 : %)



# 2. 개인정보 침해사고 경험

## 인터넷 이용자의 1.2%가 개인정보 침해사고 경험

▶ 개인정보 침해사고 경험률은 1.2%로 전년(1.7%)과 비슷함
- 2018년 1.9%, 2019년 1.7%, 2020년 1.2%로 지속적으로 감소함

▶ 개인정보 침해사고 경험 유형은 '개인정보처리자가 개인정보를 무단으로 수집하여 마케팅 목적으로 이용한 경우(46.4%)'가 가장 많았고, '내부의 보안 관리 소홀로 개인정보가 유출된 경우(40.1%)', '외부의 해킹으로 인해 개인정보가 유출된 경우(23.2%)'가 그 뒤를 이음

그림 2-2-19 개인정보 침해사고 경험률

(단위 : %)

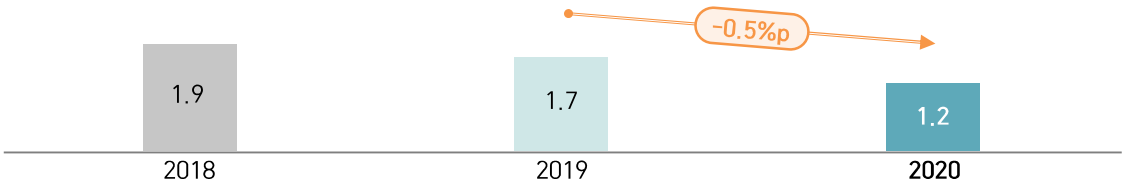
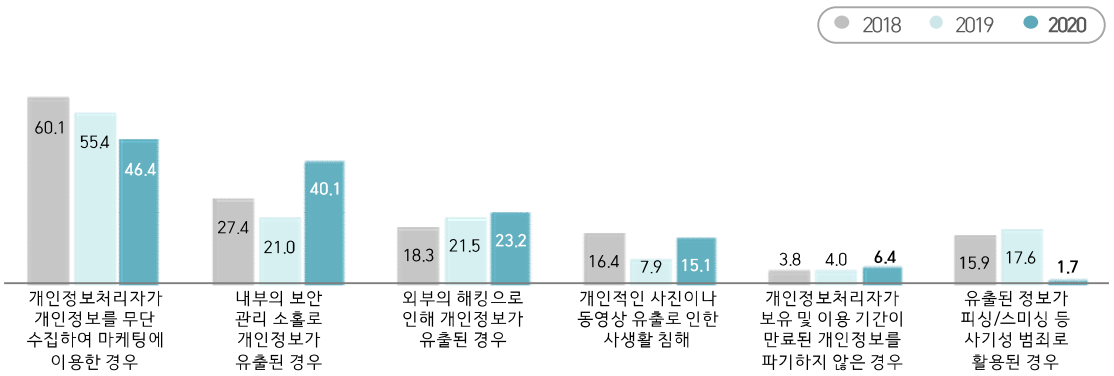



그림 2-2-20 개인정보 침해사고 경험 유형 (복수응답) - 개인정보 침해사고 경험자

(단위 : %)



# 3. 개인정보 침해사고 대응

**개인정보 침해사고 경험자의 34.9%는 침해사고 대응활동 실시**

- 개인정보 침해사고 이후 대응활동을 실시한 비율은 34.9%로 전년(48.9%) 대비 14.0%p 감소함
- 대응활동 유형으로는 '해당 서비스를 탈퇴하고 동일한 서비스를 제공하는 다른 기업 이용(21.4%)'이 가장 많았고, '관련 기관에 신고 또는 상담(8.9%)', 'e프라이버시 클린서비스 이용(4.0%)' 등의 순임

그림 2-2-21 개인정보 침해사고 대응률 - 개인정보 침해사고 경험자

(단위 : %)

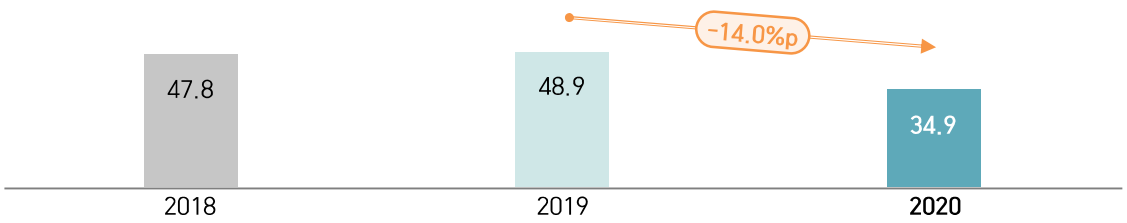
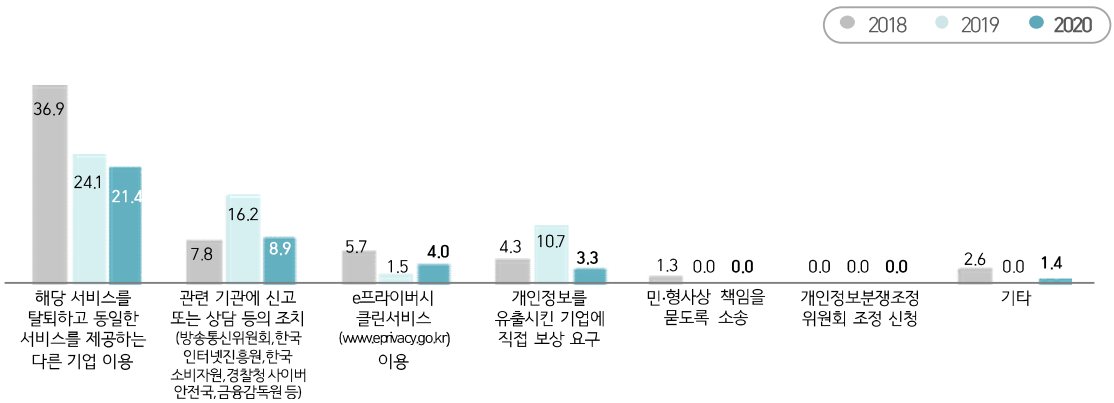



그림 2-2-22 개인정보 침해사고 대응활동 수행 (복수응답) - 개인정보 침해사고 경험자

(단위 : %)



# V 주요 서비스별 정보보호

## 1. 클라우드

### 인터넷 이용자의 35.4%가 '클라우드 서비스' 이용

- 클라우드 서비스 이용률은 35.4%로 전년(36.8%) 대비 1.4%p 감소함
- 클라우드 서비스로 인한 유출 피해를 예방하기 위한 조치는 '중요파일은 저장 또는 공유 전 암호화 설정하기(58.3%)'가 가장 많았고, 다음으로 '클라우드 서비스 이용약관 확인하기(52.5%)', '공유 기능을 정확하게 확인하고 이용하기(40.6%)' 등의 순임

그림 2-2-23 클라우드 서비스 이용률

(단위 : %)

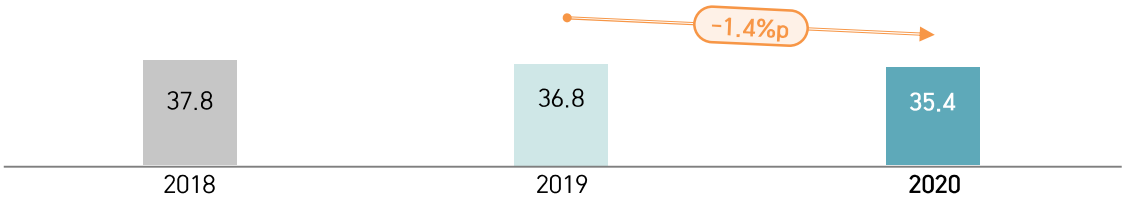
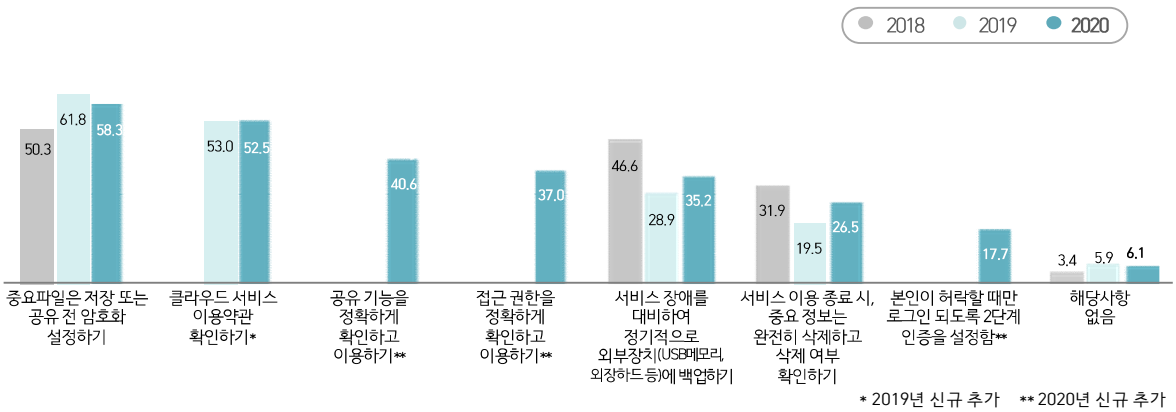



그림 2-2-24 클라우드 서비스 피해 예방 조치 (복수응답) - 클라우드 서비스 이용자

(단위 : %)




* 2019년 신규 추가 ** 2020년 신규 추가

## 2. SNS

### 인터넷 이용자의 74.4%가 'SNS' 이용

- 인터넷 이용자의 SNS(Social Network Service) 이용률은 74.4%로, 전년(74.7%)과 비슷함
  - 2018년 78.8%, 2019년 74.7%, 2020년 74.4%로 감소 추세임
- SNS 피해를 예방하기 위한 조치로 '개인정보는 신중히 선택하여 공개함(96.2%)'을 가장 많이 수행하고, 다음으로 '가족, 친구 등 타인의 개인정보를 함부로 게시·공개하지 않음(90.2%)', '개인정보 활용에 대한 내용을 확인하고 신중하게 동의함(88.1%)' 등을 수행함

그림 2-2-25 SNS 이용률

(단위 : %)

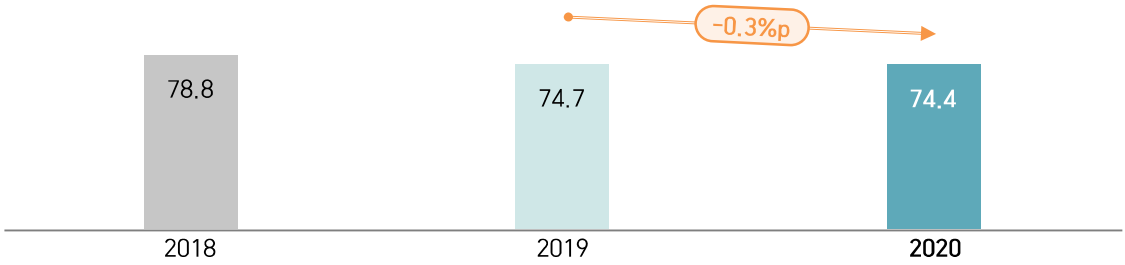
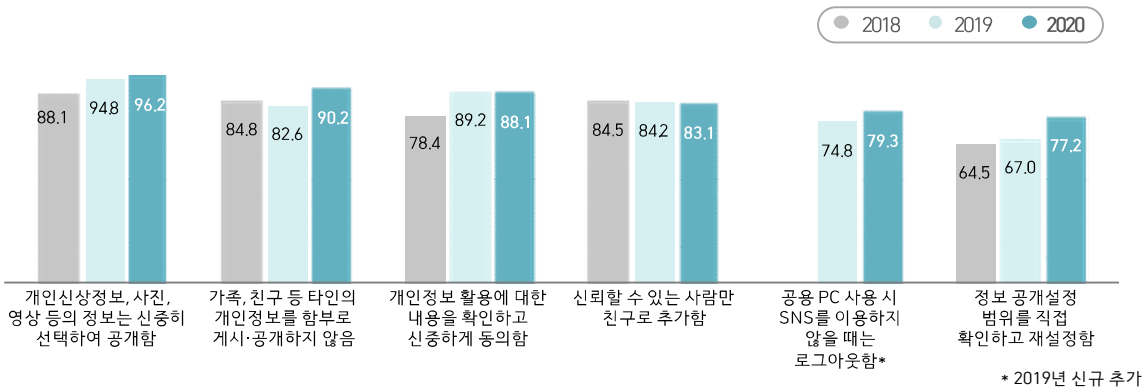



그림 2-2-26 SNS 피해 예방 조치 (복수응답) - SNS 이용자

(단위 : %)




* 2019년 신규 추가

# 3. IP카메라

## 인터넷 이용자의 5.5%가 IP카메라 제품 이용

- IP카메라 제품 이용률은 5.5%로 전년(4.1%) 대비 1.4%p 증가함
- IP카메라 이용자는 보안을 위해 '관리자 계정의 비밀번호 변경하여 사용(46.7%)'한다는 응답이 가장 많고, '기기를 최신 버전으로 업데이트(44.6%)', 'IP카메라에 접근하는 PC 및 스마트폰의 보안 설정 강화(35.3%)' 조치가 그 뒤를 이음

그림 2-2-27 IP카메라 이용률

(단위 : %)

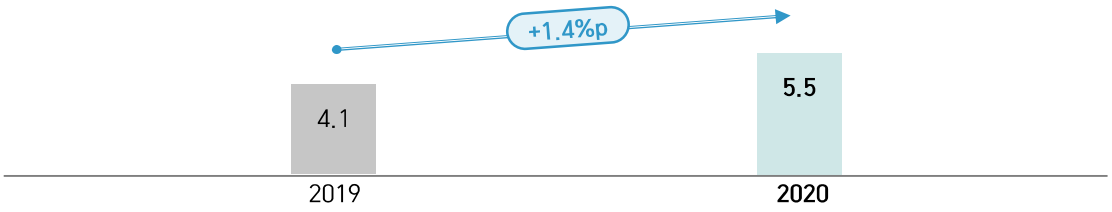
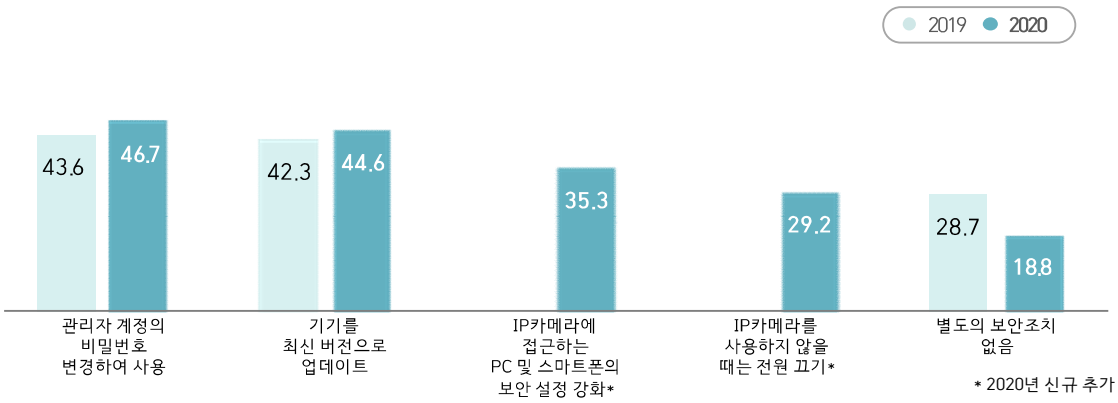



그림 2-2-28 IP카메라 보안 조치 실시 유형 (복수응답) - IP카메라 이용자

(단위 : %)



제3장

# 조사결과

# Ⅰ 정보보호 인식

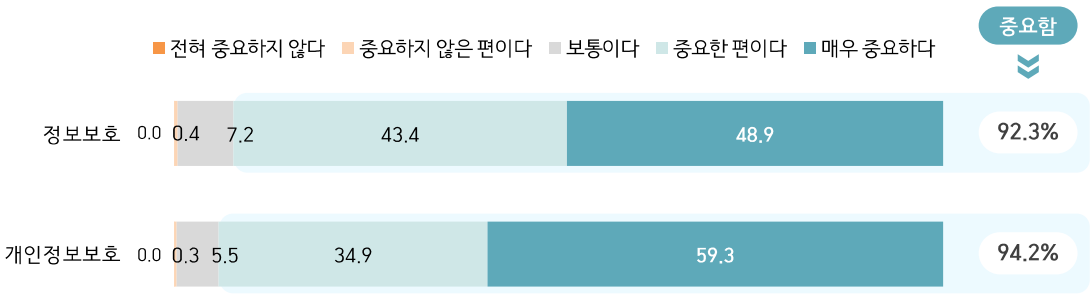
## 1. 정보보호 및 개인정보보호 중요성 인식

인터넷 이용자의 92.3%는 정보보호가 중요하다*고 응답했으며, 개인정보보호가 중요하다고 응답한 비율은 94.2%로 나타났다.

* 중요하다 : 중요한 편이다 + 매우 중요하다

그림 2-3-1 정보보호 및 개인정보보호 중요성 인식

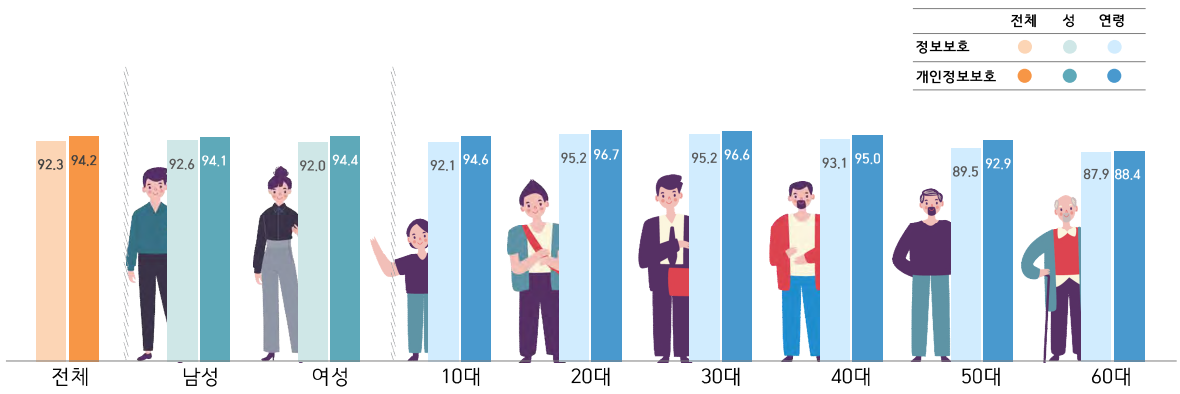
(중요한 편이다 + 매우 중요하다, 단위 : %)




정보보호 및 개인정보보호 중요성에 대한 인식은 여성이 남성에 비해 높게 나타났다. 정보보호 인식은 20대와 30대(각 95.2%)에서 가장 높고, 개인정보보호 인식은 20대(96.7%)에서 가장 높게 조사되었다. 반면, 60대의 정보보호(87.9%) 및 개인정보보호(88.4%) 인식은 타 연령대 대비 상대적으로 낮게 나타났다.

그림 2-3-2 성·연령별 정보보호 및 개인정보보호 중요성 인식

(중요한 편이다 + 매우 중요하다, 단위 : %)



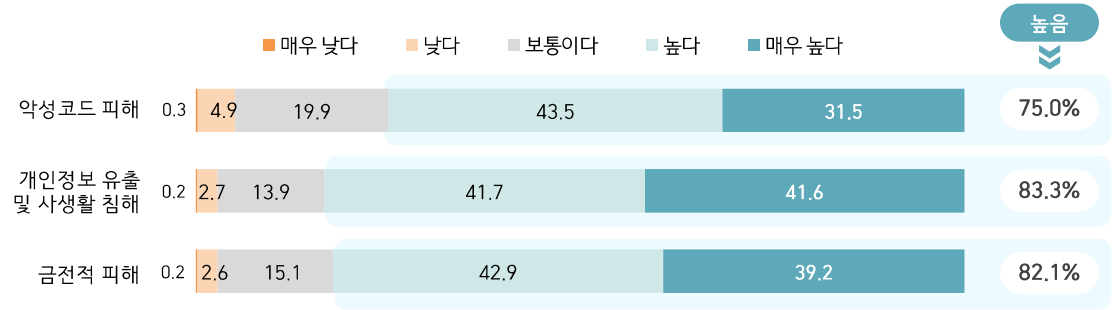
# 2. 정보보호 위협에 대한 인식

## 가. 위협사안에 대한 구체적 인지

정보보호 위협사안(웹사이트, SNS, 스마트폰 앱 등 인터넷 상에서 일어날 수 있는 문제)에 대한 인지도는 '개인정보 유출 및 사생활 침해(83.3%)'가 가장 높게 나타났고, 다음으로 '금전적 피해(82.1%)', '악성코드 피해(75.0%)' 순으로 조사되었다.

그림 2-3-3 위협사안에 대한 구체적 인지

(높다 + 매우 높다, 단위 : %)

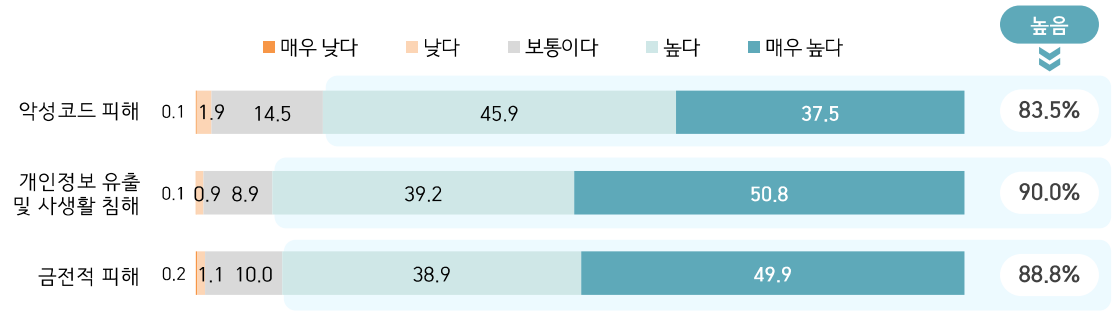



## 나. 위협사안에 대한 피해의 심각성

정보보호 위협사안에 대한 심각성은 '개인정보 유출 및 사생활 침해'가 90.0%로 가장 높고, 다음으로 '금전적 피해(88.8%)', '악성코드 피해(83.5%)' 순으로 조사되었다.

그림 2-3-4 위협사안에 대한 피해의 심각성

(높다 + 매우 높다, 단위 : %)

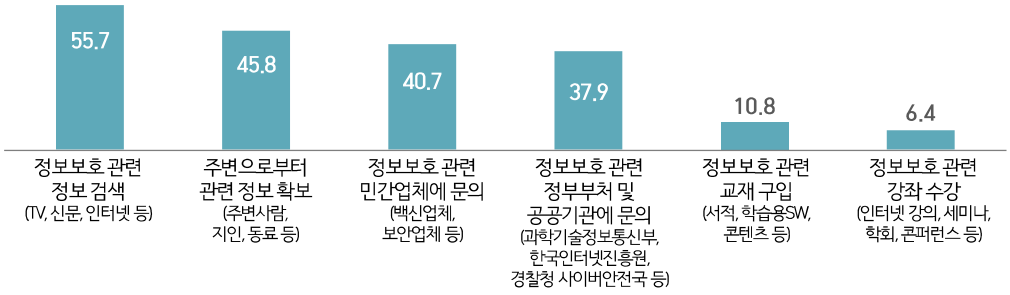


## 3. 향후 정보보호 관련 정보수집 및 학습 방법

향후 정보보호 관련 정보수집 및 학습 방법으로는 '정보보호 관련 정보검색'을 하겠다는 응답이 55.7%로 가장 높고, 다음으로 '주변으로부터 관련 정보 확보(45.8%)', '정보보호 관련 민간업체에 문의(40.7%)' 등의 순으로 나타났다.

그림 2-3-5 향후 정보보호 관련 정보수집 및 학습 방법 (2가지)

(단위 : %)



# Ⅱ 침해사고 예방

## 1. 정보보호 관련 제품

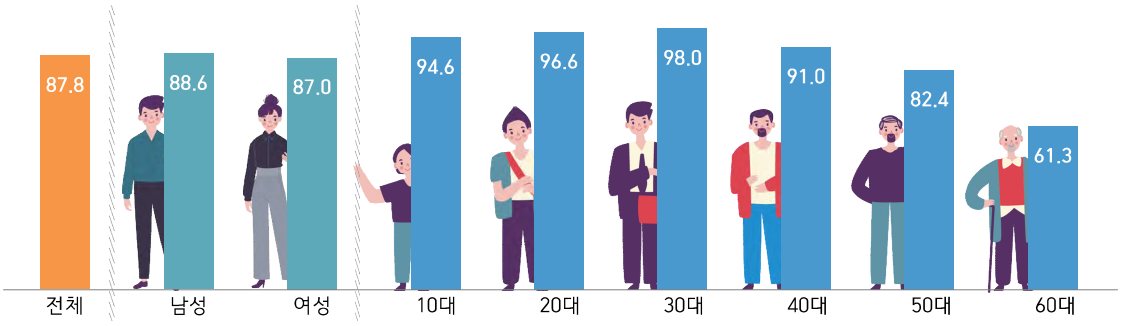
### 가. 정보보호 제품 이용

PC 및 모바일 보안을 위해 정보보호 관련 제품(소프트웨어 등)을 이용하는 비율은 87.8%로 나타났다.

정보보호 제품 이용률은 남성(88.6%)이 여성(87.0%)보다 높고, 연령별로는 20~30대(20대: 96.6%, 30대: 98.0%)의 이용률이 타 연령대 대비 높게 나타났다.

그림 2-3-6 정보보호 제품 이용

(단위 : %)

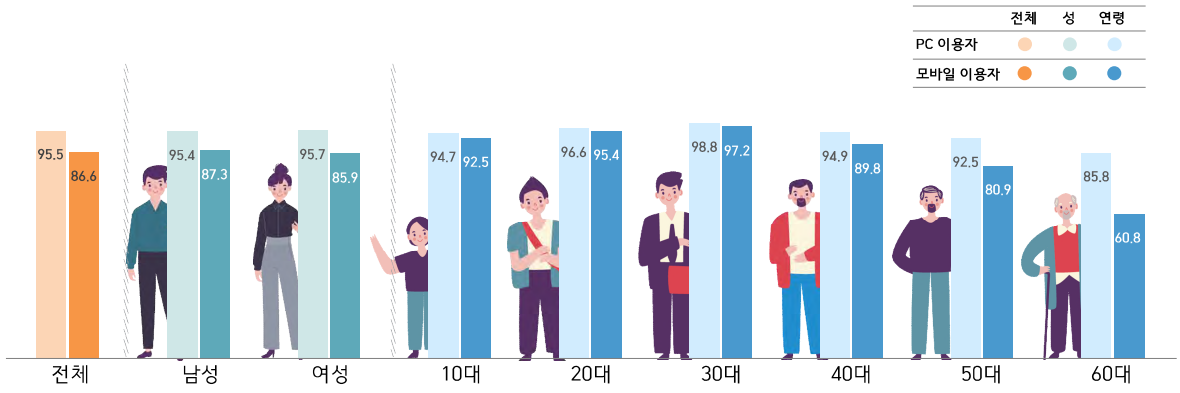


기기별로 살펴보면, PC 이용자의 정보보호 제품 이용률이 95.5%로 모바일 이용자의 정보보호 제품 이용률(86.6%)보다 8.9%p 높게 나타났다.

PC 이용자의 정보보호 제품 이용률은 성별 관계없이(남성: 95.4%, 여성: 95.7%) 높고, 모바일 이용자의 정보보호 제품 이용률은 남성이 87.3%로 여성(85.9%)에 비해 1.4%p 높다.
연령별로 정보보호 제품 이용률은 PC 및 모바일 이용자 모두 30대(PC: 98.8%, 모바일: 97.2%)가 가장 높게 나타났다.
반면, 60대 모바일 이용자의 정보보호 제품 이용률은 60.8%로 타 연령대 대비 가장 낮게 나타났다.

그림 2-3-7 정보보호 제품 이용 - PC/모바일 기기 이용자

(단위 : %)

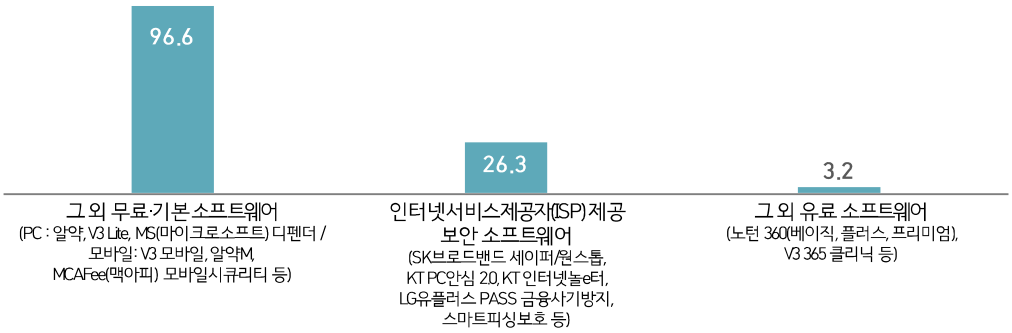


## 나. 정보보호 소프트웨어 이용

정보보호 제품 이용자의 96.6%가 '그 외 무료·기본 소프트웨어'를 이용하는 것으로 조사되었다. 다음으로 '인터넷서비스제공자(ISP) 제공 보안 소프트웨어(26.3%)', '그 외 유료 소프트웨어(3.2%)' 순으로 이용하는 것으로 나타났다.

그림 2-3-8 정보보호 소프트웨어 이용 (복수응답) - 정보보호 제품 이용자

(단위 : %)

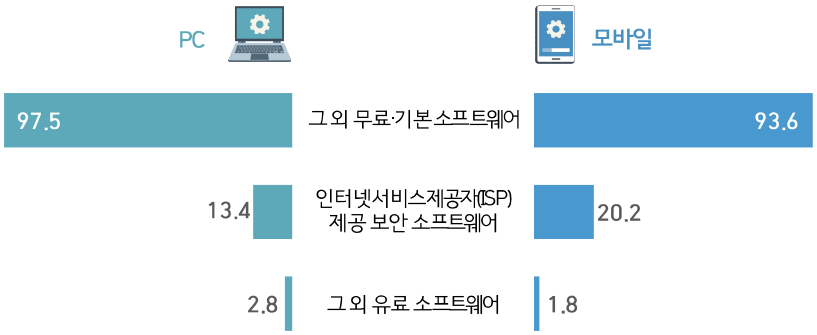



기기별로 살펴보면, PC는 '그 외 무료·기본 소프트웨어(97.5%)'가 가장 높게 나타났고, 다음으로 '인터넷서비스제공자(ISP) 제공 보안 소프트웨어(13.4%)'가 높게 조사되었다.

모바일의 경우, PC와 마찬가지로 '그 외 무료·기본 소프트웨어(96.3%)'를 가장 많이 이용하는 가운데, '인터넷서비스제공자(ISP) 제공 보안 소프트웨어(20.2%)'를 그 다음으로 많이 이용하는 것으로 나타났다.

그림 2-3-9 정보보호 소프트웨어 이용 (복수응답) - PC/모바일 기기 이용자 중 정보보호 제품 이용자

(단위 : %)

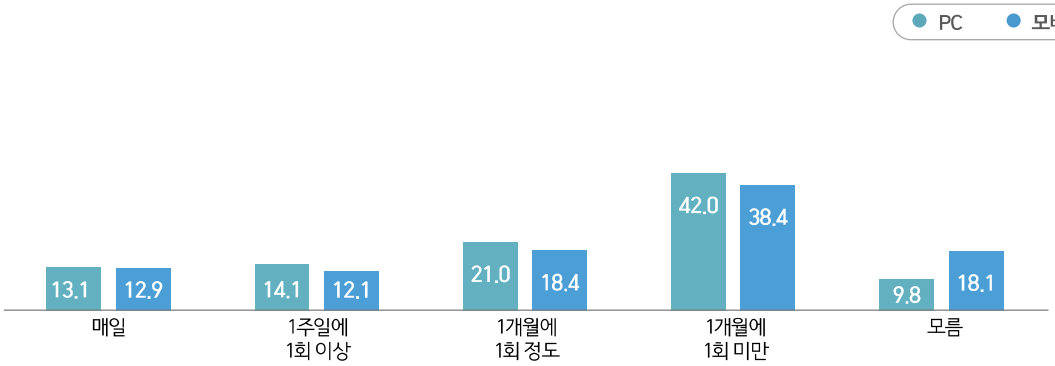


## 다. 악성코드 검사 실시 주기

PC 및 모바일 악성코드 검사(바이러스, 웜, 랜섬웨어, 스파이웨어 검사 등) 주기는 '1개월에 1회 미만'(PC: 42.0%, 모바일: 38.4%) 실시한다는 응답이 가장 많았다.

그림 2-3-10 악성코드 검사 실시 주기 - PC/모바일 기기 이용자 중 정보보호 제품 이용자

(단위 : %)



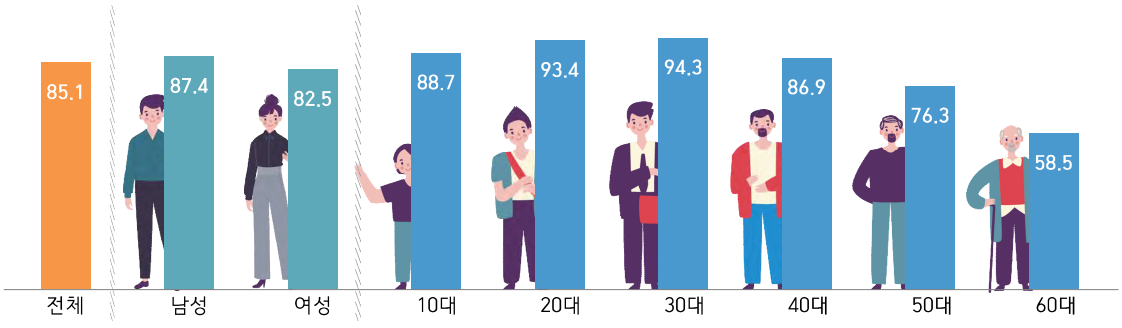

## 라. 백신 프로그램 업데이트

정보보호 제품 이용자의 85.1%가 백신 프로그램 업데이트를 하는 것으로 조사되었다.

백신 프로그램 업데이트 실시율은 남성이 87.4%로 여성(82.5%)보다 4.9%p 높고, 연령별로는 50~60대(50대: 76.3%, 60대: 58.5%)가 타 연령대 대비 낮게 나타났다.

그림 2-3-11 백신 프로그램 업데이트 실시 - 정보보호 제품 이용자

(단위 : %)

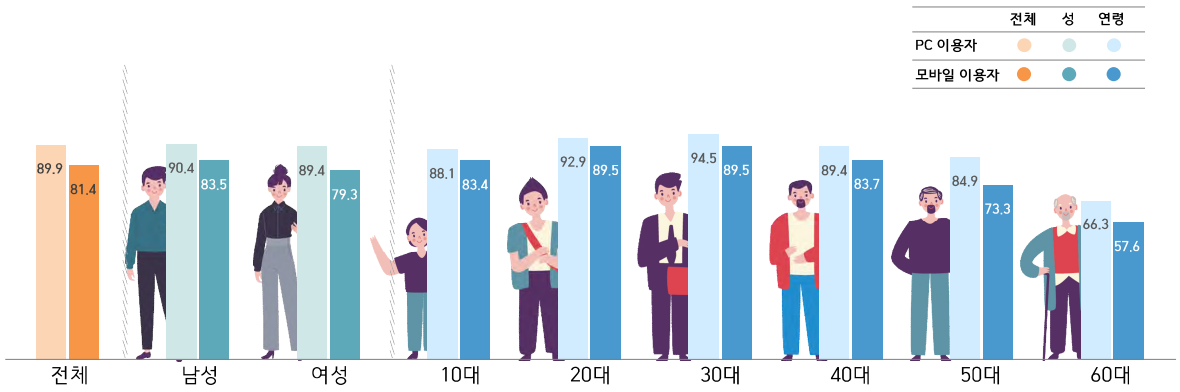


기기별로 살펴보면, PC 이용자의 백신 프로그램 업데이트 실시율(89.9%)이 모바일 이용자(81.4%)보다 8.5%p 높게 나타났다.

PC와 모바일 모두 여성보다는 남성이 백신 프로그램을 업데이트하는 비율이 높다.
연령별로 살펴보면 PC는 30대(94.5%), 모바일은 20~30대(89.5%)에서 가장 높게 나타났다.

그림 2-3-12 백신 프로그램 업데이트 실시 - PC/모바일 기기 이용자 중 정보보호 제품 이용자

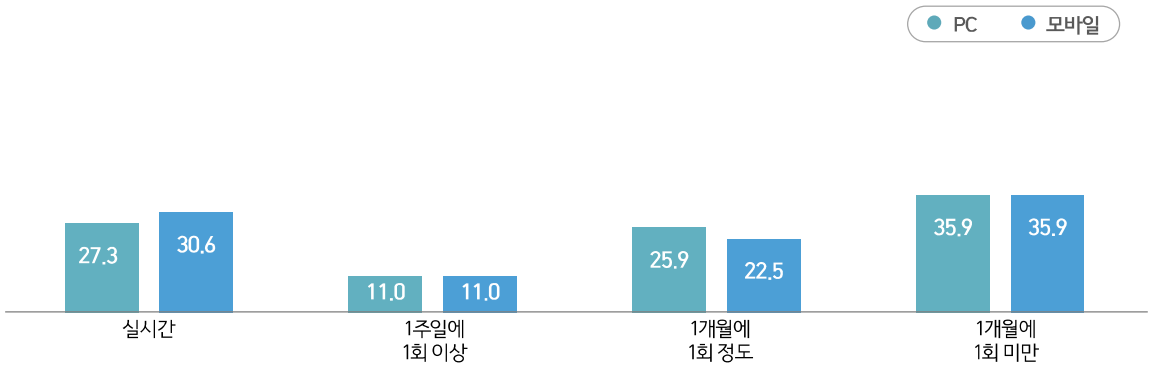
(단위 : %)




백신프로그램 업데이트 주기는 PC 및 모바일 모두 '1개월에 1회 미만'(PC: 35.9%, 모바일: 35.9%) 실시한다는 비율이 가장 높고, 다음으로 '실시간'(PC: 27.3%, 모바일:30.6%) 비율이 높게 나타났다.

그림 2-3-13 백신 프로그램 업데이트 실시 주기 - PC/모바일 기기 이용자 중 업데이트 실시자

(단위 : %)



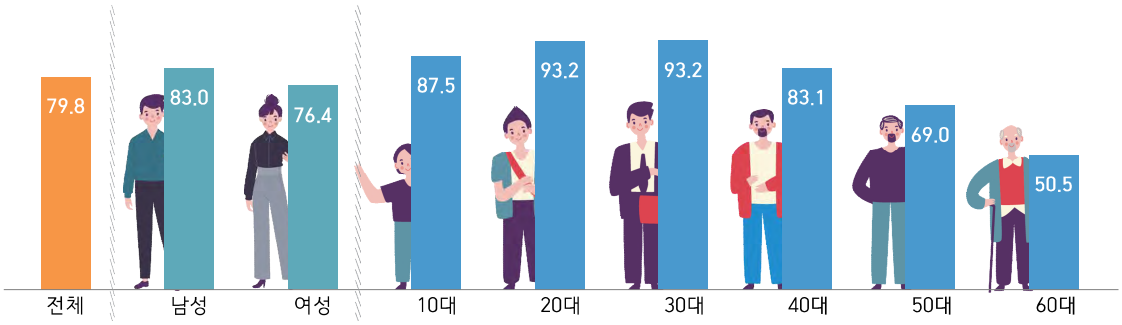
## 마. 운영체제 보안 업데이트

인터넷 이용자의 79.8%가 운영체제 보안 업데이트를 실시하는 것으로 조사되었다.

성별 및 연령별 분석 결과, 운영체제 보안 업데이트 실시율은 남성(83.0%)이 여성(76.4%)보다 6.6%p 높고, 20~30대(20대: 93.2%, 30대: 93.2%)에서 타 연령대 대비 상대적으로 높게 나타났다.

그림 2-3-14 운영체제 보안 업데이트 실시

(단위 : %)

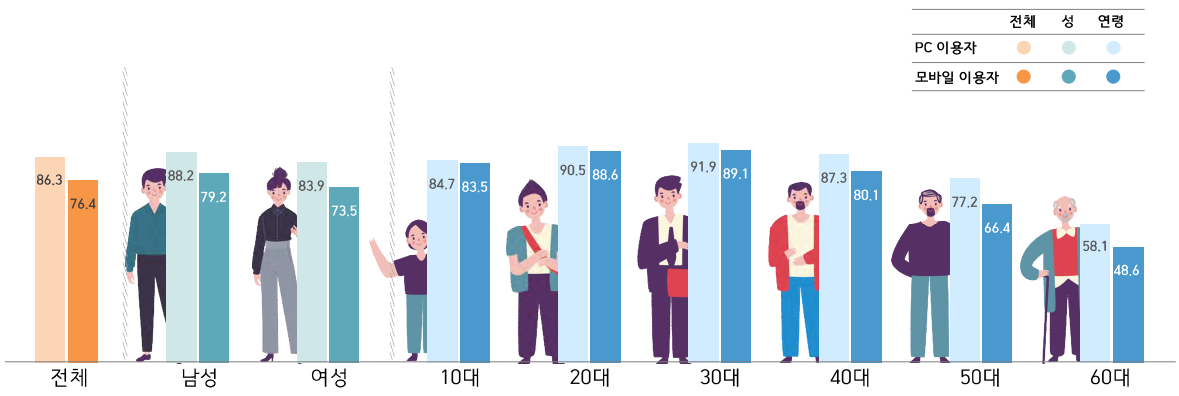



기기별로 살펴보면, PC 이용자의 운영체제 보안 업데이트 실시율(86.3%)이 모바일 이용자(76.4%)보다 9.9%p 높게 나타났다.

PC 운영체제 보안 업데이트 실시율은 남성(88.2%)이 여성(83.9%)에 비해 4.3%p 높고, 30대(91.9%)의 실시율이 가장 높게 나타났다.
마찬가지로 모바일 운영체제 보안 업데이트 실시율은 남성(79.2%)이 여성(73.5%)보다 5.7%p 높고, 30대(89.1%)의 실시율이 타 연령대 대비 상대적으로 높게 나타났다.

그림 2-3-15 운영체제 보안 업데이트 실시 여부 - PC/모바일 기기 이용자 중 보안 업데이트 실시자

(단위 : %)



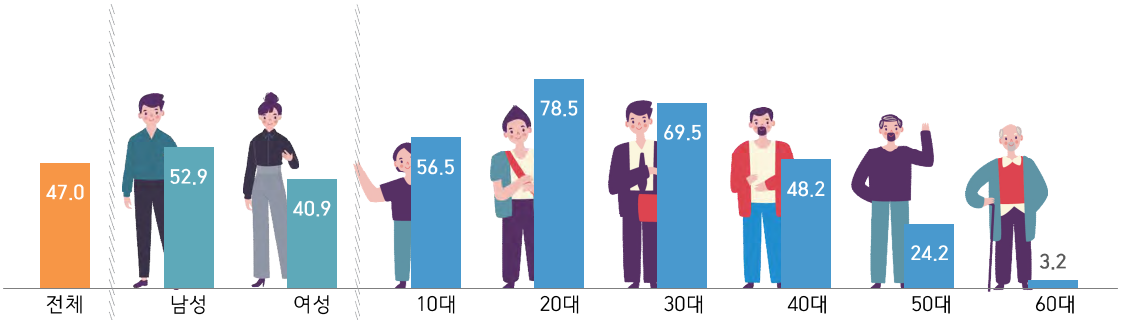
## 바. 중요 데이터 백업

인터넷 이용자의 47.0%가 PC 및 모바일 기기에 저장된 중요 데이터를 백업하는 것으로 조사되었다.

중요 데이터 백업률은 남성이 52.9%로 여성(40.9%)보다 12.0%p 높고, 20대가 78.5%로 가장 높게 나타났다. 반면, 50대 이상의 중요 데이버 백업 실시율은 다른 연령대에 비해 낮은 수치를 보였다.

그림 2-3-16 중요 데이터 백업률

(단위 : %)

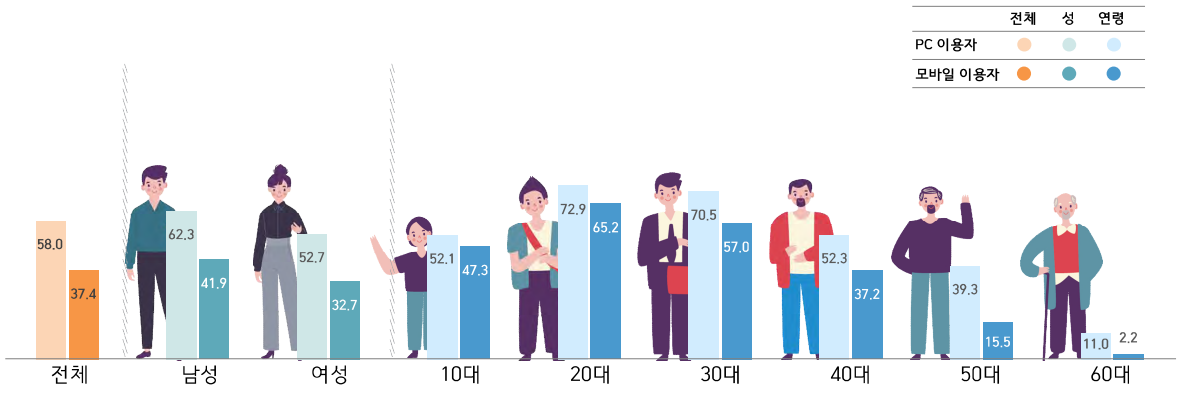



기기별로 살펴보면, 중요 데이터 백업률은 PC 이용자(58.0%)가 모바일 이용자(37.4%)보다 20.6%p 높은 것으로 나타났다.

성별 및 연령별 분석 결과, PC와 모바일 모두 여성보다는 남성이 높게 나타났고, 20~30대가 상대적으로 높게 나타났다.

그림 2-3-17 중요 데이터 백업률 - PC/모바일 기기 이용자

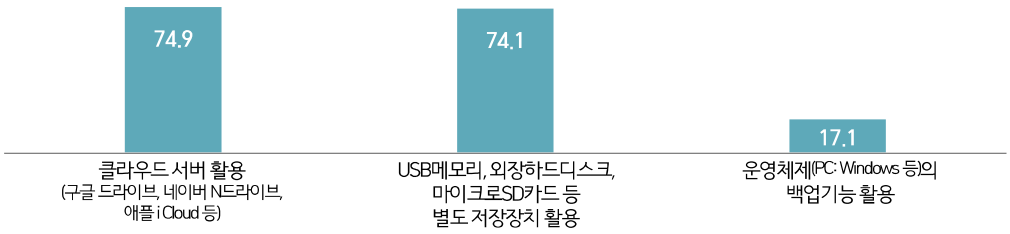
(단위 : %)



중요 데이터 백업 방식은 '클라우드 서버 활용(74.9%)', 'USB메모리, 외장하드디스크, 마이크로SD카드 등 별도 저장장치 활용(74.1%)', '운영체제의 백업기능 활용(17.1%)' 순으로 조사되었다.

그림 2-3-18 중요 데이터 백업 방식 (복수응답) - 중요 데이터 백업 실시자

(단위 : %)

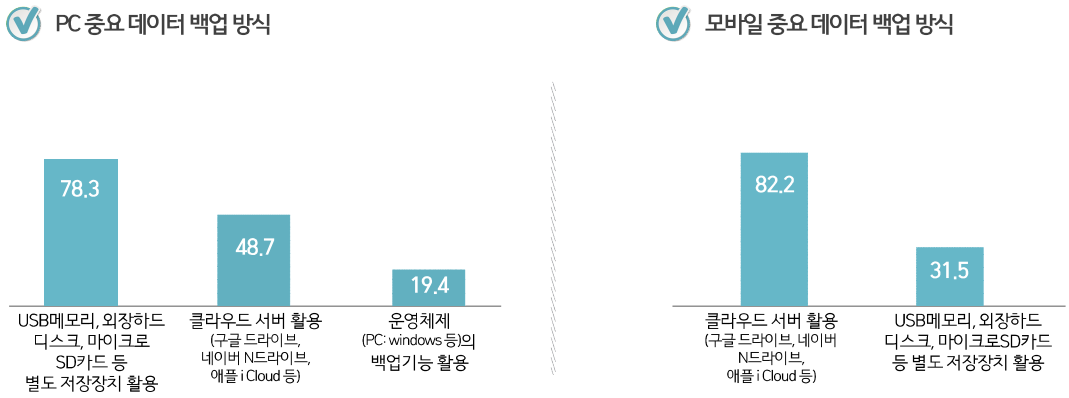



기기별로 백업 방식을 살펴보면, PC 이용자는 'USB메모리, 외장하드디스크, 마이크로SD카드 등 별도 저장장치 활용(78.3%)'이 가장 높았고, '클라우드 서버 활용(48.7%)', '운영체제의 백업기능 활용(19.4%)' 순으로 나타났다.

한편, 모바일 이용자의 백업 방식은 '클라우드 서버 활용'이 82.2%로 가장 높고, 다음으로 'USB메모리, 외장하드디스크, 마이크로SD카드 등 별도 저장장치 활용(31.5%)'으로 조사되었다.

그림 2-3-19 중요 데이터 백업 방식 (복수응답) - PC/모바일 기기 이용자 중 중요 데이터 백업 실시자

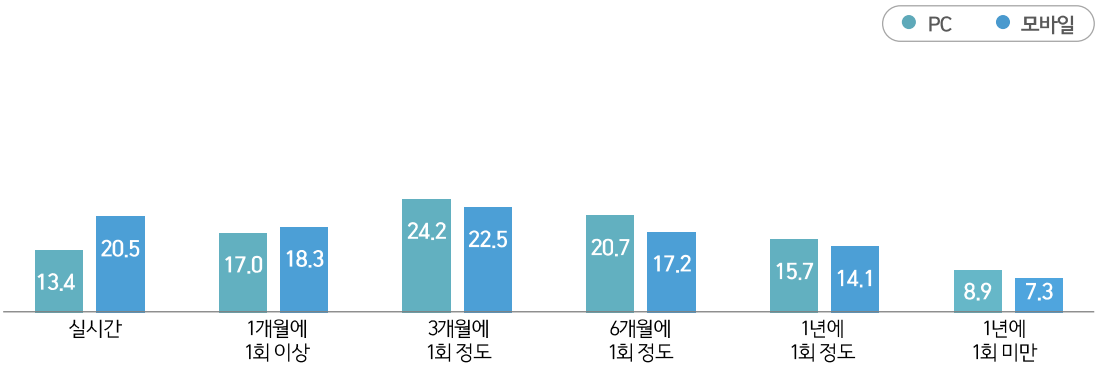
(단위 : %)



중요 데이터 백업 실시 주기는 PC(24.2%), 모바일(22.5%) 모두 '3개월에 1회 정도' 실시하는 비율이 가장 높고, 모바일의 경우 '실시간(20.5%)'으로 백업하는 비율이 그 뒤를 이었다.

그림 2-3-20 중요 데이터 백업 실시 주기 (복수응답) - PC/모바일 기기 이용자 중 중요 데이터 백업 실시자

(단위 : %)

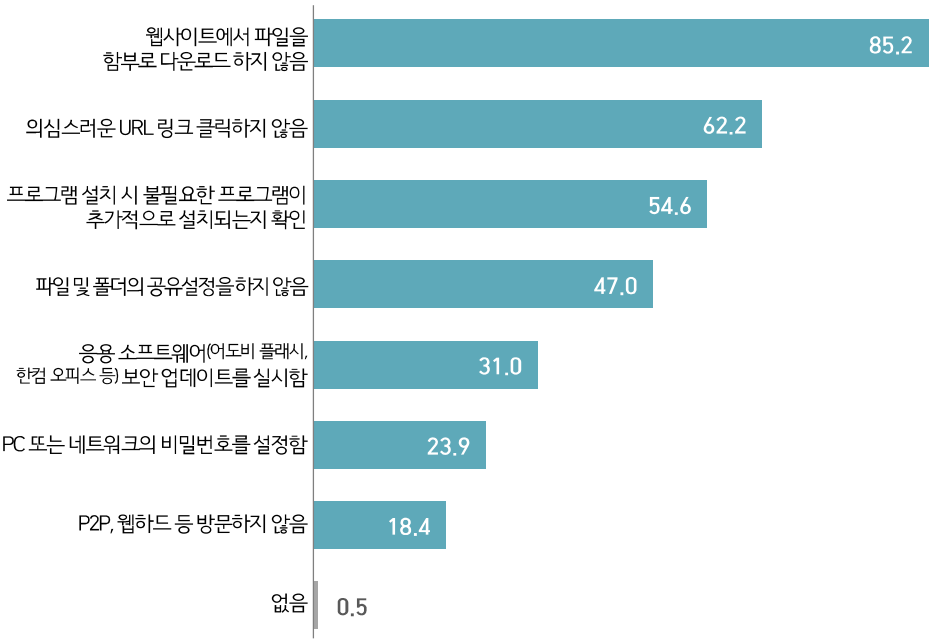



## 사. PC 및 네트워크 보안을 위한 예방조치

PC 및 네트워크 보안을 위한 예방 조치는 '웹사이트에서 파일을 함부로 다운로드하지 않음(85.2%)'이 가장 많고, 다음으로 '의심스러운 URL 링크 클릭하지 않음(62.2%)' 등의 순으로 조사되었다.

그림 2-3-21 PC 및 네트워크 보안을 위한 예방 조치 (복수응답)

(단위 : %)

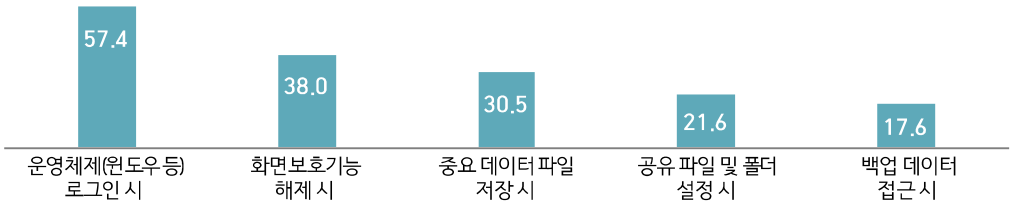


## 아. 비밀번호 설정 및 관리

PC 이용자의 57.4%는 '운영체제(윈도우 등) 로그인 시' 비밀번호를 설정한다고 응답했다. 다음으로 '화면보호기능 해제 시(38.0%)', '중요 데이터 파일 저장 시(30.5%)' 등의 순으로 비밀번호를 설정하는 것으로 조사되었다.

그림 2-3-22 PC 비밀번호 설정 (복수응답) - PC 이용자

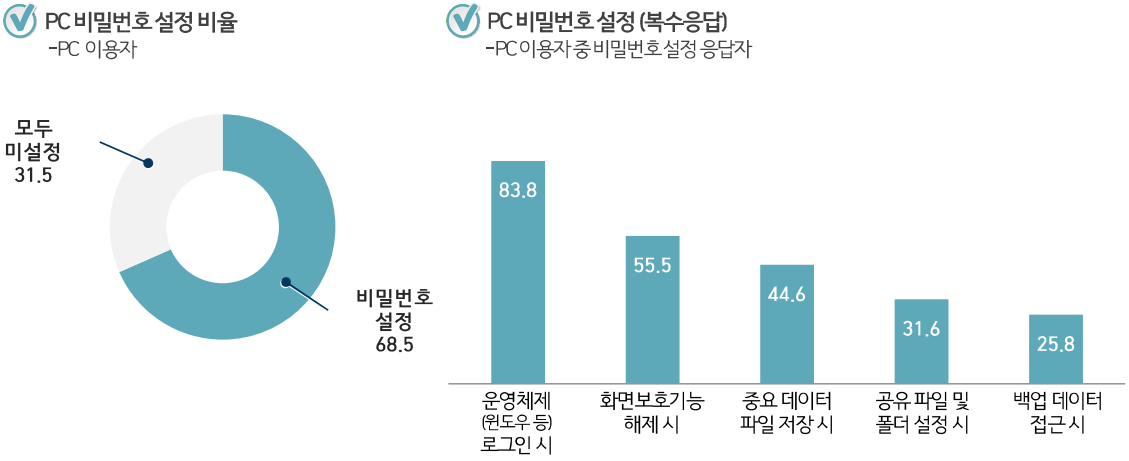
(단위 : %)




### ▶ 참고. PC 이용자 중 하나라도 비밀번호 설정하는 경우

그림 2-3-23 하나라도 PC 비밀번호 설정률

(단위 : %)

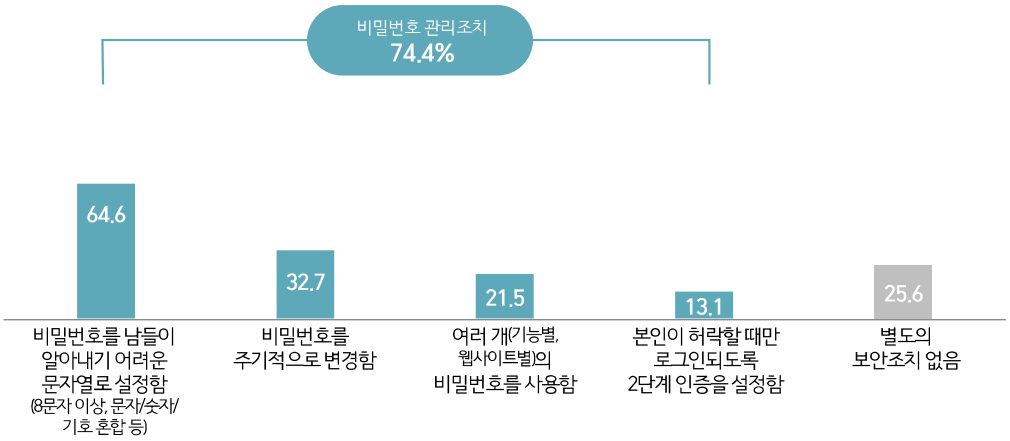


인터넷 이용자의 74.4%는 비밀번호 관리 조치를 취하는 것으로 조사되었다.

세부 유형별로는 '비밀번호를 남들이 알아내기 어려운 문자열로 설정함(64.6%)'이 가장 많았고, 다음으로 '비밀번호를 주기적으로 변경함(32.7%)' 등의 순으로 나타났다.

그림 2-3-24 비밀번호 관리 조치 (복수응답)

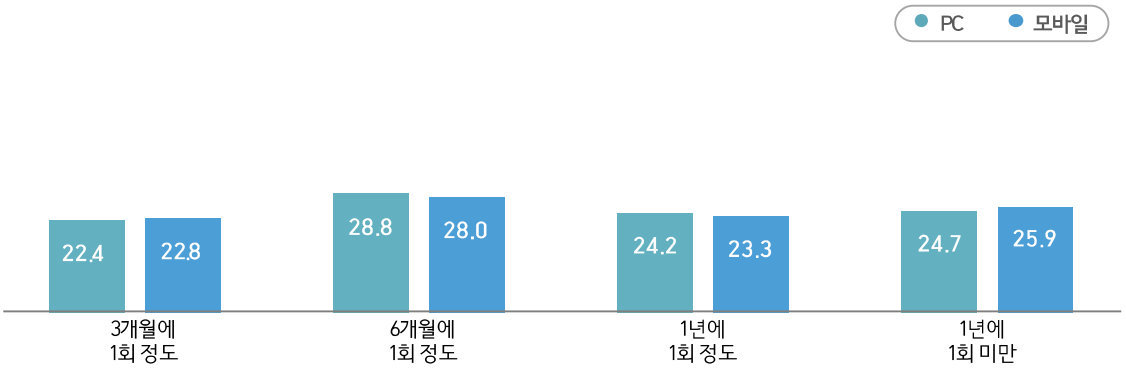
(단위 : %)




주로 이용하는 사이트의 비밀번호 변경 주기(주기적으로 비밀번호를 변경하는 응답자 대상)는 PC 및 모바일 모두 '6개월에 1회 정도(PC: 28.8%, 모바일: 28.0%)'가 가장 많고, 다음으로 '1년에 1회 미만'(PC: 24.7%, 모바일: 25.9%) 변경하는 비율이 높게 나타났다.

그림 2-3-25 주로 이용하는 웹사이트의 비밀번호 변경 주기 - 주기적 비밀번호 변경자

(단위 : %)



# 2. 모바일 및 무선랜 보안

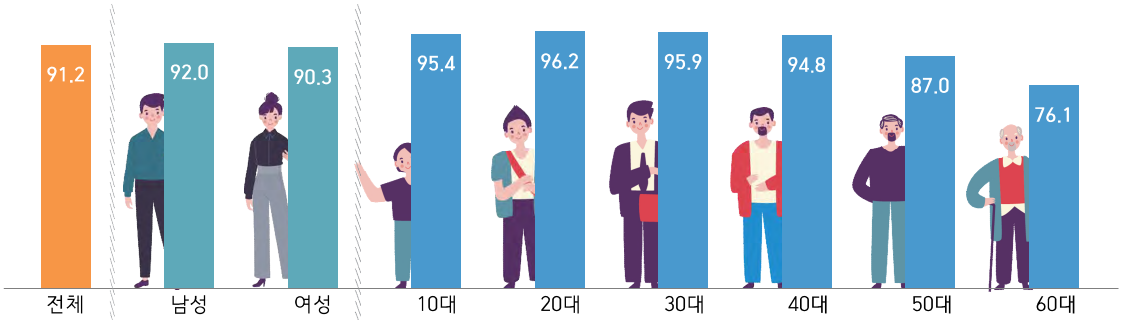
## 가. 무선랜 피해 예방 조치

모바일 이용자의 91.2%는 무선랜을 이용하는 것으로 조사되었다.

무선랜 이용률은 남성(92.0%)이 여성(90.3%)보다 1.8%p 높게 나타났고, 20대(96.2%)가 타 연령대 대비 상대적으로 높게 나타났다.

그림 2-3-26 무선랜 이용 - 모바일 기기 이용자

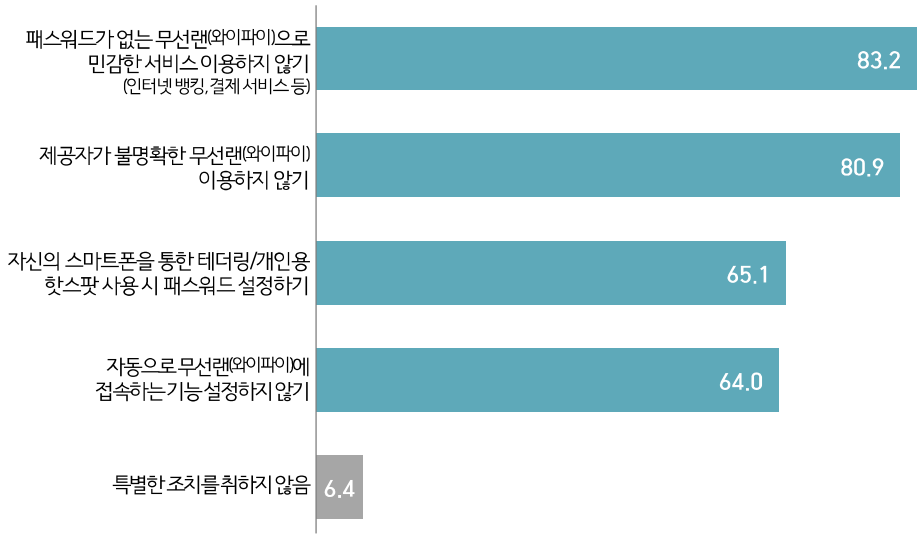
(단위 : %)




무선랜 이용자의 피해 예방 조치는 '패스워드가 없는 무선랜으로 민감한 서비스 이용하지 않기'가 83.2%로 가장 많았다.

그림 2-3-27 무선랜 피해 예방 조치 (복수응답) - 모바일 기기 이용자 중 무선랜 이용자

(단위 : %)



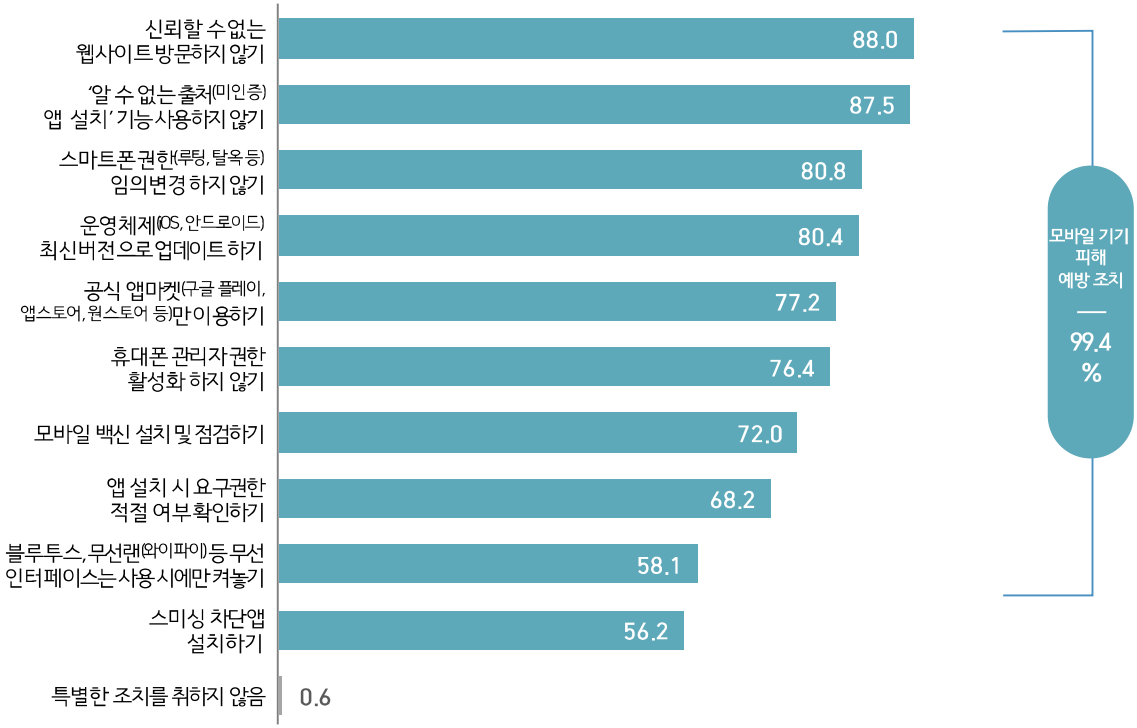
## 나. 모바일 기기 피해 예방 조치

모바일 이용자의 99.4%는 모바일 기기 피해 예방을 위한 조치를 취하는 것으로 조사되었다.

모바일 기기 피해 예방 조치로 '신뢰할 수 없는 웹사이트 방문하지 않기' 비율이 88.0%로 가장 높았고, 다음으로 '알 수 없는 출처(미인증) 앱 설치 기능 사용하지 않기(87.5%)', '스마트폰 권한(루팅, 탈옥 등) 임의변경하지 않기(80.8%)' 등의 순으로 높게 나타났다.

그림 2-3-28 모바일 기기 피해 예방 조치 (복수응답) - 모바일 기기 이용자

(단위 : %)



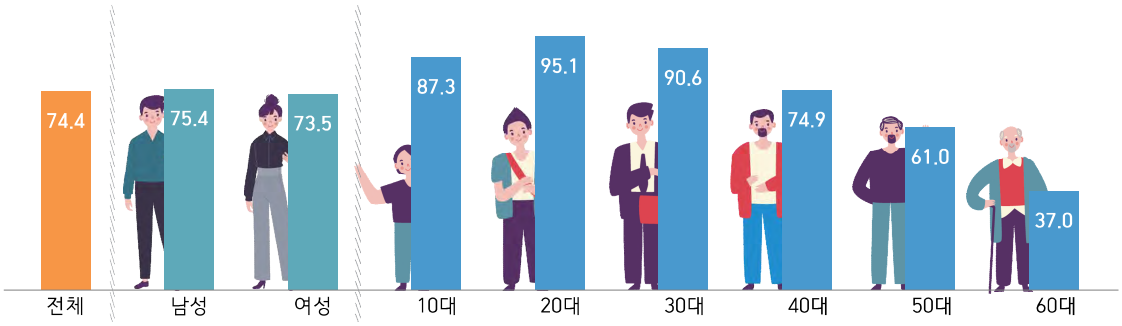
## 3. SNS 보안

인터넷 이용자의 74.4%가 SNS를 이용하는 것으로 조사되었다.

성별 및 연령별 분석 결과, 남성의 SNS 이용률이 75.4%로 여성(73.5%)보다 1.9%p 높고, 20대의 이용률이 95.1%로 가장 높은 것으로 나타났다.

그림 2-3-29 SNS 이용

(단위 : %)

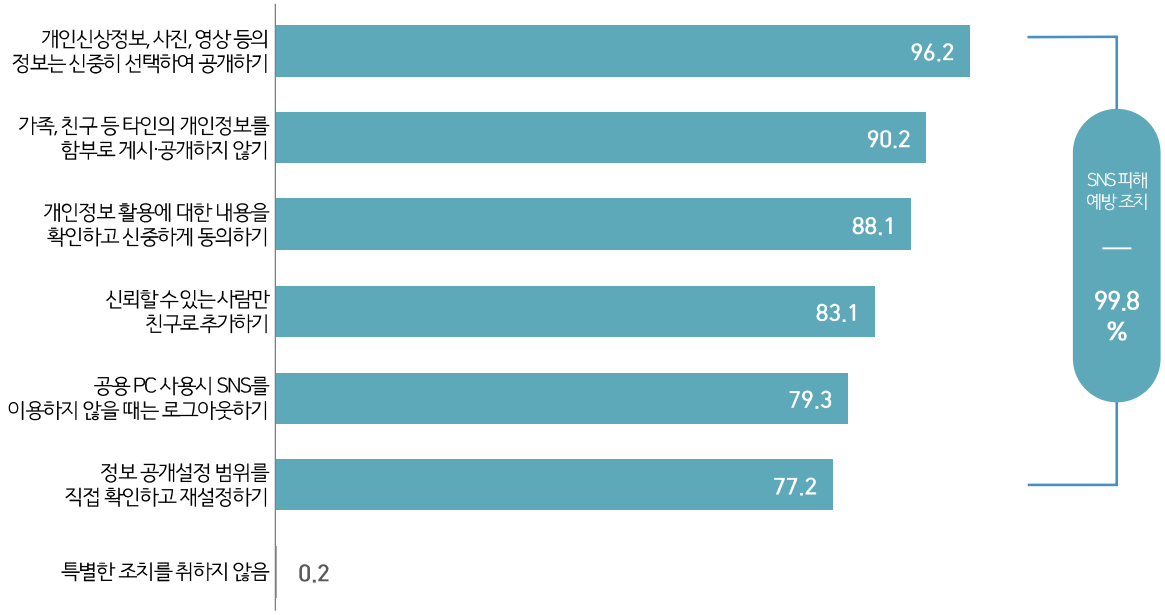



SNS 이용자의 99.8%는 SNS 피해 예방을 위한 조치를 취하는 것으로 조사되었다.

세부 유형별로는 '개인신상정보, 사진, 영상 등의 정보는 신중히 선택하여 공개하기'가 96.2%로 가장 높게 나타났다.

그림 2-3-30 SNS 피해 예방 조치 (복수응답) - SNS 이용자

(단위 : %)



# Ⅲ 침해사고 대응

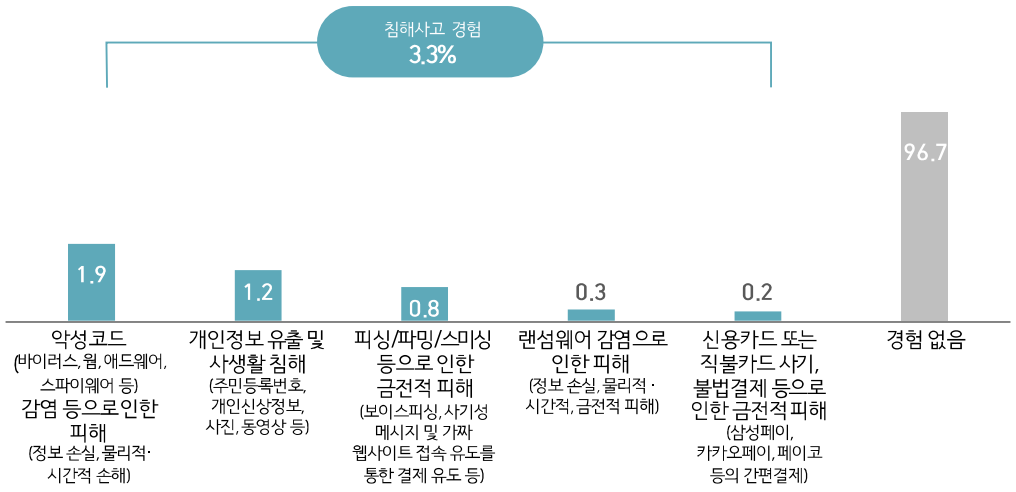
## 1. 침해사고 경험

2019년 1년간 침해사고 경험률은 3.3%로 조사되었다.

침해사고 세부 유형별로 살펴보면, '악성코드 감염 등으로 인한 피해(1.9%)'를 가장 많이 경험한 것으로 나타났고, 다음으로 '개인정보 유출 및 사생활 침해(1.2%)', '피싱/파밍/스미싱 등으로 인한 금전적 피해(0.8%)' 등의 순으로 나타났다.

그림 2-3-31 침해사고 경험 유형 (복수응답)

(단위 : %)

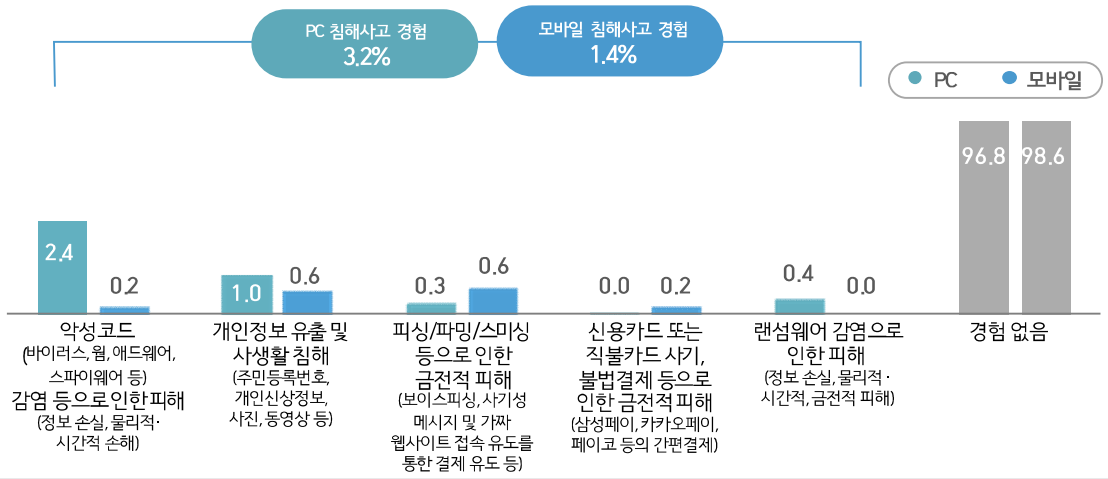


기기별로 살펴보면, PC를 통한 침해사고 경험률(3.2%)이 모바일 침해사고 경험률(1.4%)보다 상대적으로 높게 나타났다.

세부 유형별로는 PC는 '악성코드 감염 등으로 인한 피해(2.4%)', 모바일은 '개인정보 유출 및 사생활 침해(0.6%)'와 '피싱/파밍/스미싱 등으로 인한 금전적 피해(0.6%)' 경험이 가장 많은 것으로 조사되었다.

그림 2-3-32 침해사고 경험 유형 (복수응답) - PC/모바일 기기 이용자

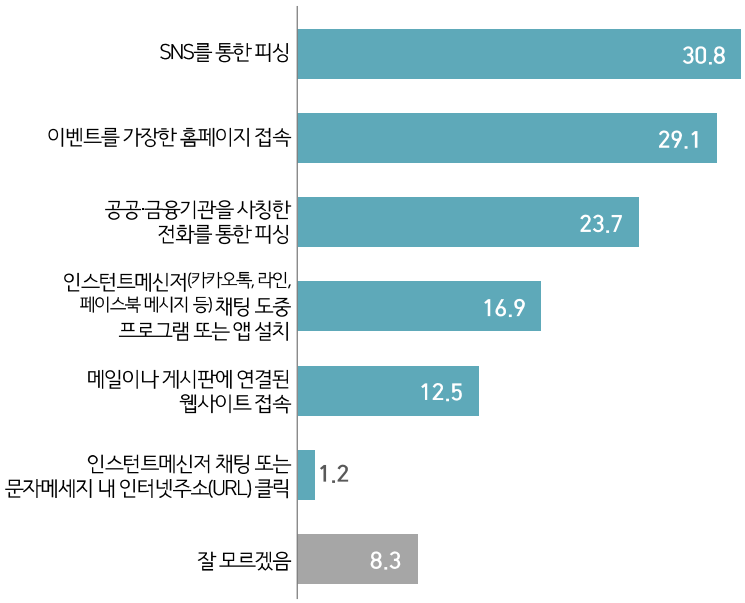
(단위 : %)




피싱/파밍/스미싱 등 금전적 피해 경험자는 'SNS를 통한 피싱(30.8%)' 경험이 가장 많은 것으로 조사되었다.

그림 2-3-33 전자금융사기 피해 경로 (복수응답) - 피싱/파밍/스미싱 금전적 피해 경험자

(단위 : %)



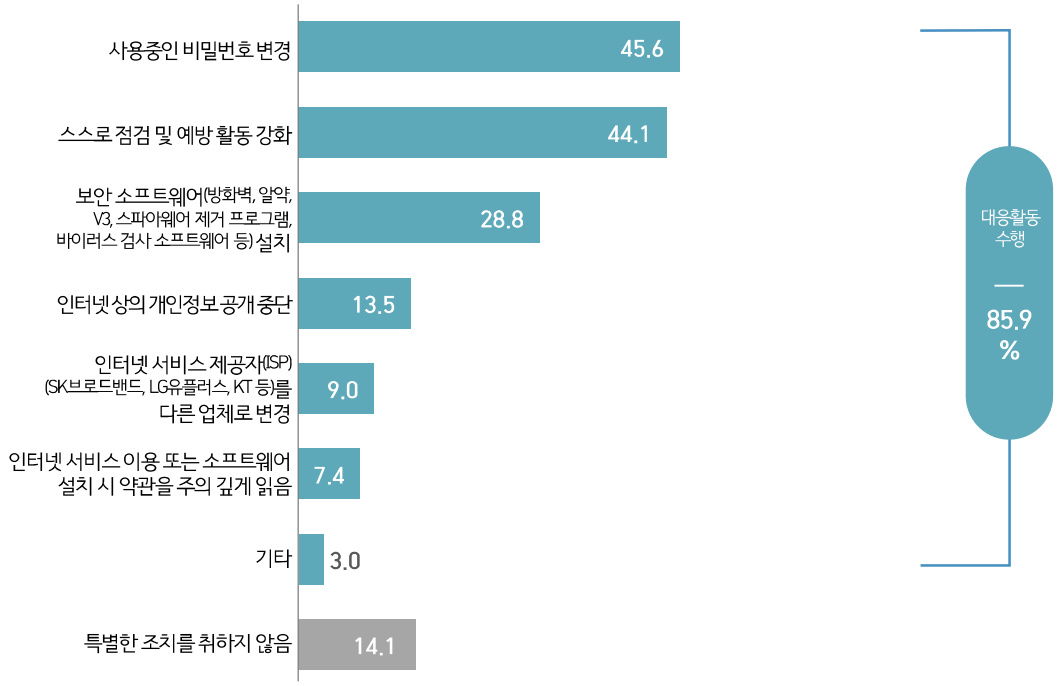
## 2. 침해사고 대응

침해사고 경험자의 85.9%는 침해사고 대응 활동을 수행한 것으로 조사되었다.

세부 유형별로는 '사용 중인 비밀번호 변경(45.6%)'을 가장 많이 수행하는 것으로 나타났고, 다음으로 '스스로 점검 및 예방 활동 강화(44.1%)', '보안 소프트웨어 설치(28.8%)' 등의 순으로 조사되었다.

그림 2-3-34 침해사고 대응활동 수행 (복수응답) - 침해사고 경험자

(단위 : %)

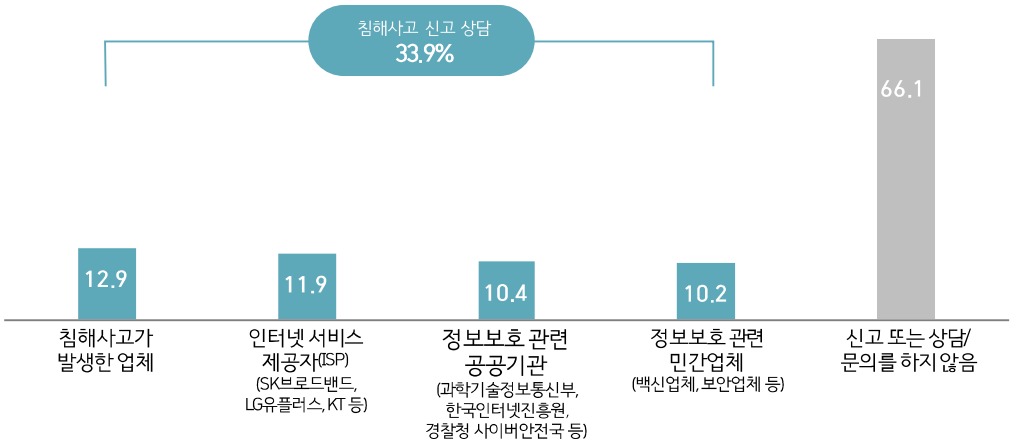


침해사고 경험자의 33.9%는 침해사고 경험 이후 기관 및 업체에 신고 또는 상담·문의한 것으로 조사되었다.

세부 유형별로는 '침해사고가 발생한 업체'에게 신고·상담하는 경우가 12.9%로 가장 많았고, 다음으로 '인터넷 서비스 제공자(ISP)(11.9%)', '정보보호 관련 공공기관(10.4%)' 순으로 나타났다.

그림 2-3-35 침해사고 신고 또는 상담·문의 기관·업체 (복수응답) - 침해사고 경험자

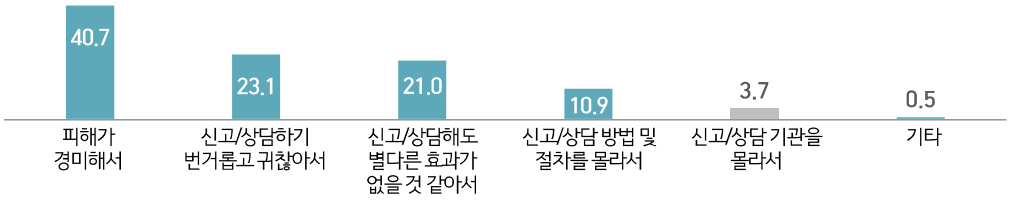
(단위 : %)




침해사고 피해를 정보보호 관련 정부부처 및 공공기관에 신고 또는 상담·문의하지 않는 이유로는 '피해가 경미해서'가 40.7%로 가장 많았고, 다음으로 '신고/상담하기 번거롭고 귀찮아서(23.1%)'라는 의견 등이 있었다.

그림 2-3-36 침해사고 신고 또는 상담·문의하지 않은 이유 - 신고 또는 상담·문의하지 않은 자

(단위 : %)



# Ⅳ 개인정보보호

## 1. 개인정보보호 조치

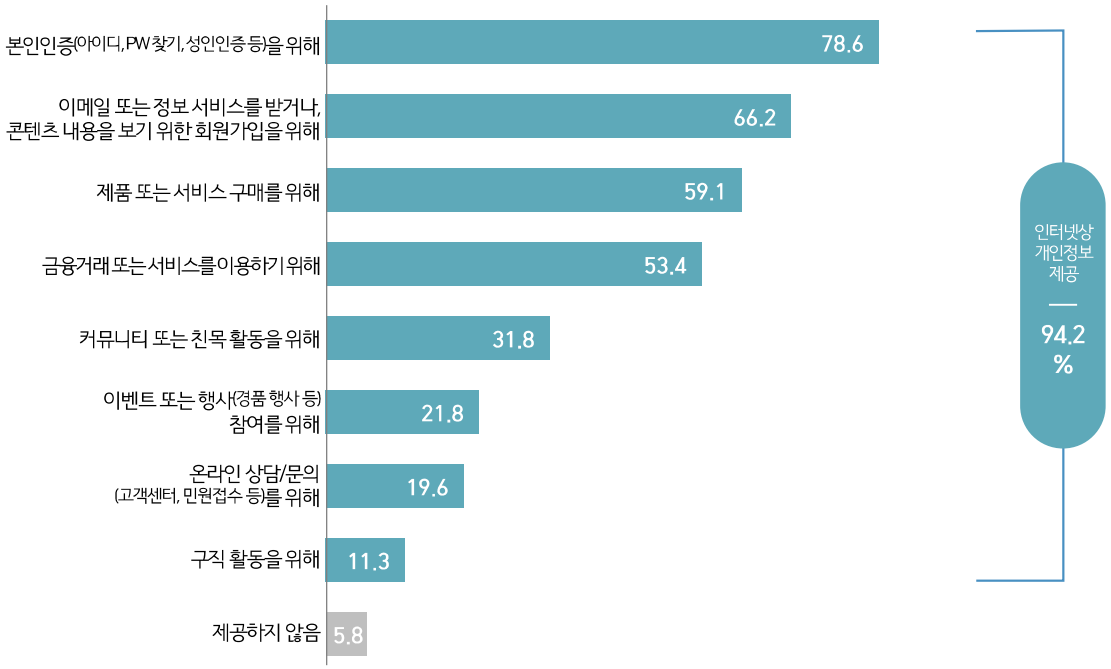
### 가. 인터넷 상 개인정보 제공 목적

인터넷 이용자의 94.2%는 인터넷 상에 개인정보를 제공하는 것으로 조사되었다.

개인정보를 제공하는 목적으로는 '본인인증(아이디, PW 찾기, 성인인증 등)을 위해'가 78.6%로 가장 높게 나타났고, 다음으로 '이메일 또는 정보 서비스를 받거나, 콘텐츠 내용을 보기 위한 회원가입을 위해(66.2%)', '제품 또는 서비스 구매를 위해(59.1%)' 등의 순으로 조사되었다.

그림 2-3-37 인터넷 상 개인정보 제공 목적 (복수응답)

(단위 : %)

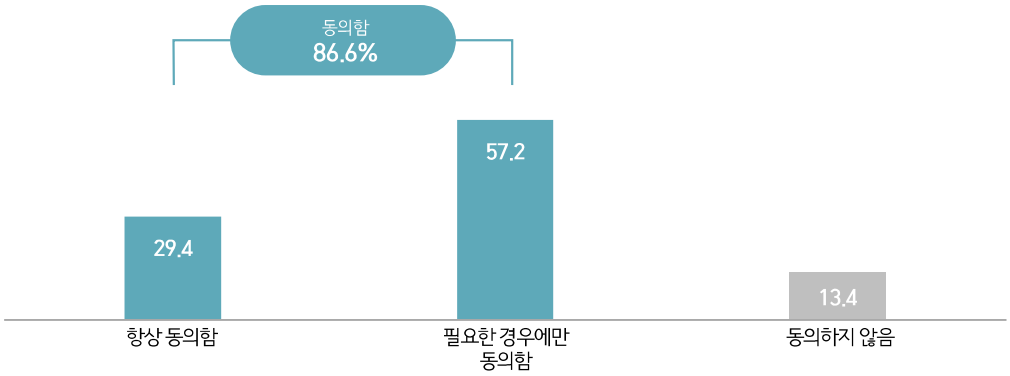


## 나. 인터넷 상 개인정보 제공 동의

인터넷 이용자의 86.6%는 인터넷 상 개인정보 제공 동의 시 필수 사항 이외에 선택사항에 동의하는 것으로 나타났다.

그림 2-3-38 인터넷 상 개인정보 제공 동의 시 선택사항 동의 여부

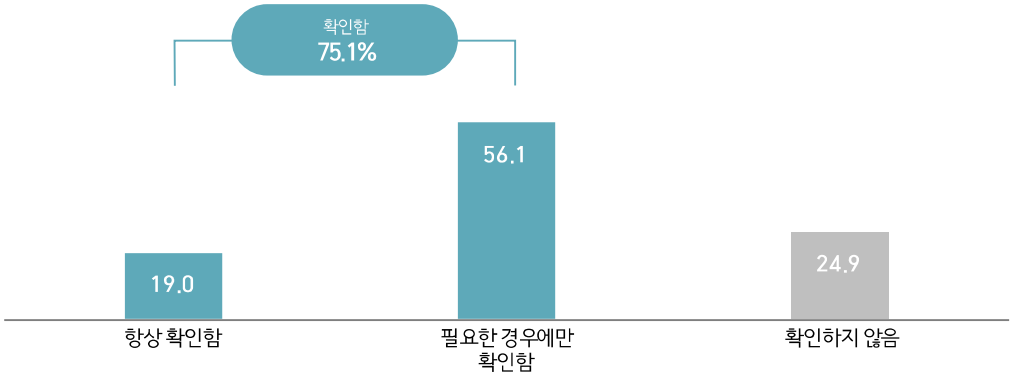
(단위 : %)




인터넷 이용자의 75.1%는 인터넷 상 개인정보 제공 동의 시 이용 약관을 확인하는 것으로 나타났다.

그림 2-3-39 인터넷 상 개인정보 제공 동의 시 이용약관 확인 여부

(단위 : %)



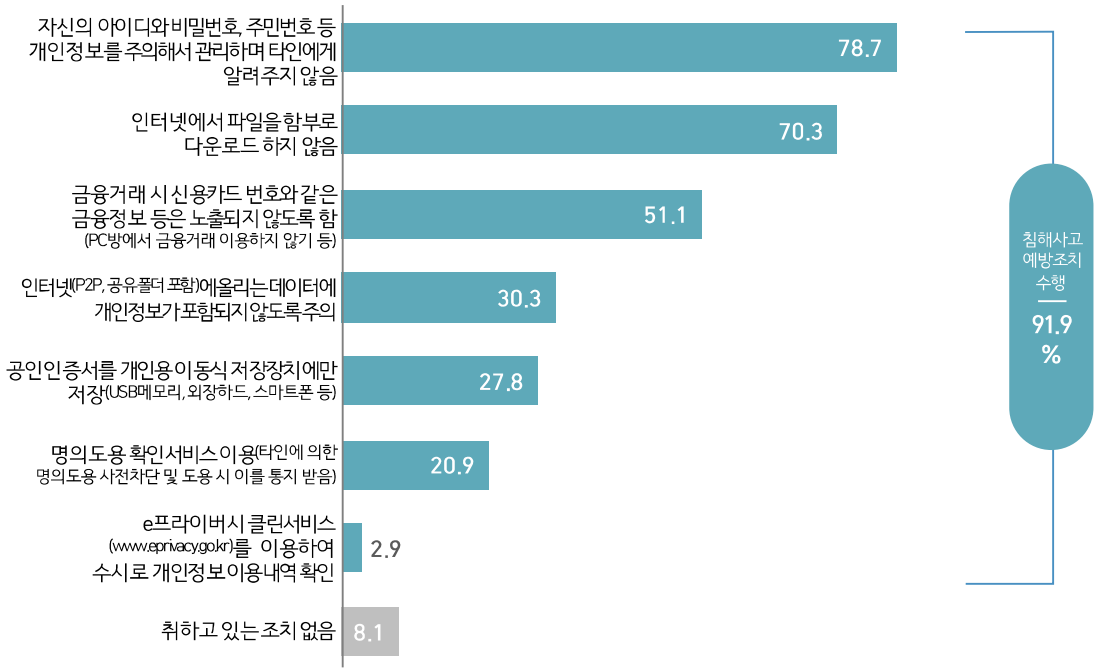
## 다. 개인정보 침해사고 예방 조치

인터넷 이용자의 91.9%는 개인정보 유출 예방을 위한 조치를 취하는 것으로 조사되었다.

개인정보 유출 예방 조치로 '개인정보를 주의해서 관리하며 타인에게 알려주지 않음'이 78.7%로 가장 많았고, 다음으로 '인터넷에서 파일을 함부로 다운로드 하지 않음(70.3%)', '금융거래 시 신용카드 번호와 같은 금융정보 등은 노출되지 않도록 함(51.1%)' 등의 순으로 조사되었다.

그림 2-3-40 개인정보 침해사고 예방 조치 (복수응답)

(단위 : %)



# 2. 개인정보 침해사고 경험 및 대응

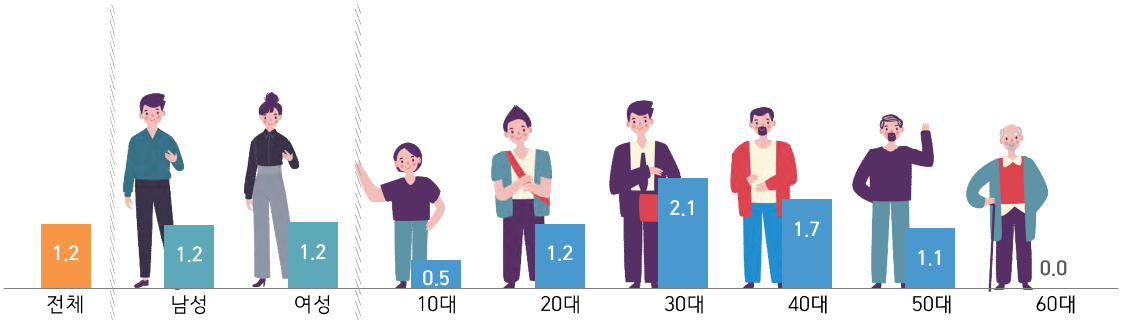
## 가. 개인정보 침해사고 경험

2019년 1년간 개인정보 침해사고 경험률은 1.2%로 조사되었다.

성별 및 연령별 분석 결과, 개인정보 침해사고 경험률은 남성과 여성 모두 1.2%로 나타났고, 30대(2.1%)에서 타 연령대 대비 상대적으로 높게 나타났다.

그림 2-3-41 개인정보 침해사고 경험

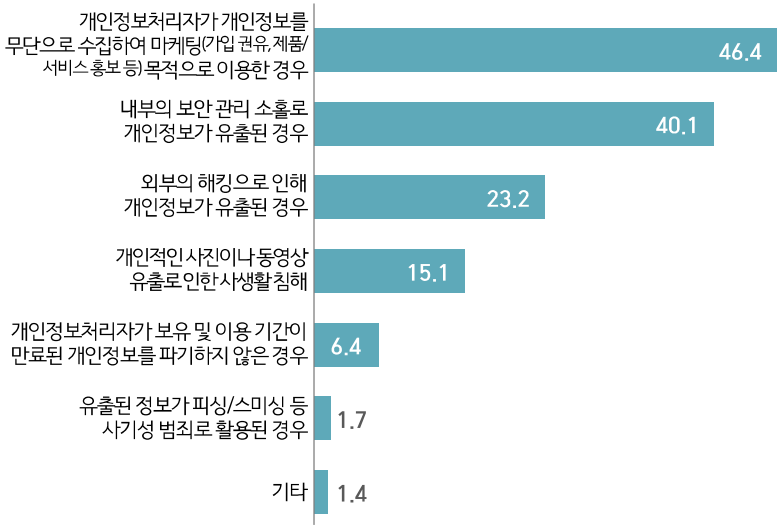
(단위 : %)




개인정보 침해사고 경험 유형으로는 '개인정보처리자가 개인정보를 무단으로 수집하여 마케팅 목적으로 이용한 경우'가 46.4%로 가장 많았다.

그림 2-3-42 개인정보 침해사고 경험 유형 (복수응답) - 개인정보 침해사고 경험자

(단위 : %)



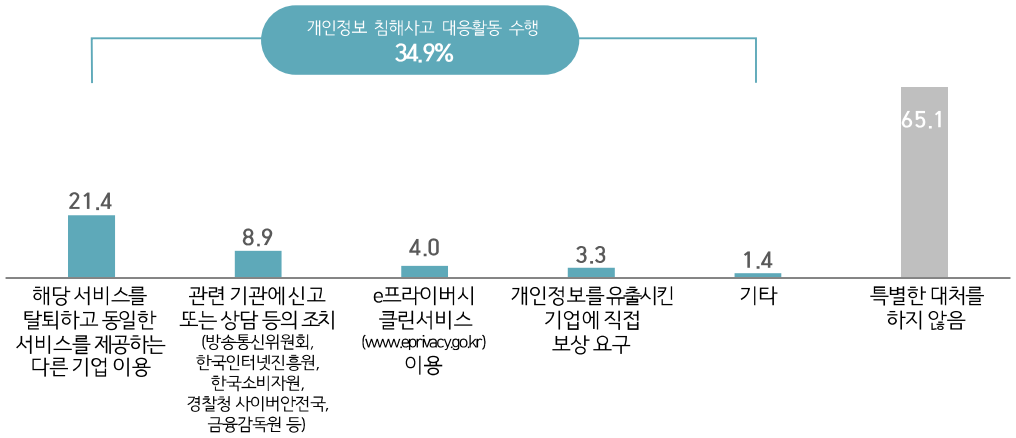
## 나. 개인정보 침해사고 대응활동 수행

개인정보 침해사고 경험자의 34.9%는 개인정보 침해 시 대응활동을 수행한 것으로 조사되었다.

세부 유형별로는 '해당 서비스를 탈퇴하고 동일한 서비스를 제공하는 다른 기업 이용'이 21.4%로 가장 높고, 다음으로 '관련 기관에 신고 또는 상담 등의 조치(8.9%)', 'e프라이버시 클린서비스 이용(4.0%)' 등의 순으로 나타났다.

그림 2-3-43 개인정보 침해사고 대응활동 수행 (복수응답) - 개인정보 침해사고 경험자

(단위 : %)



# V 주요 서비스별 정보보호

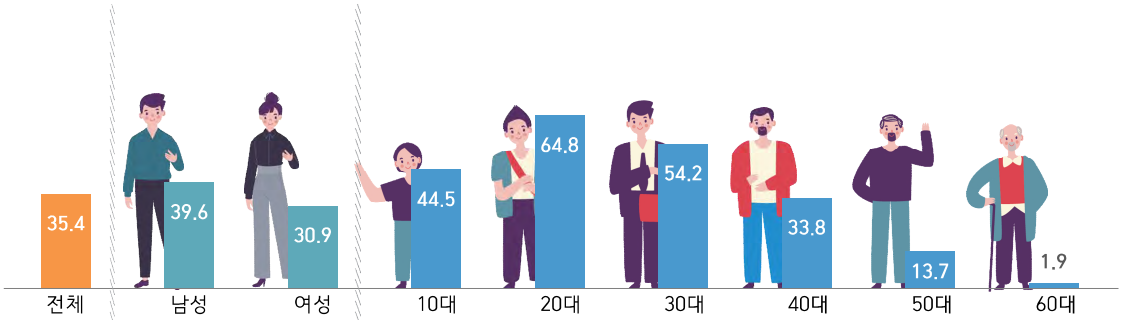
## 1. 클라우드

클라우드 서비스 이용률은 35.4%로 조사되었다.

성별 및 연령별 분석 결과, 남성(39.6%)이 여성(30.9%)보다 8.7%p 높고, 20대(64.8%)가 타 연령대 대비 클라우드 서비스를 많이 이용하는 것으로 조사되었다.

그림 2-3-44 클라우드 서비스 이용

(단위 : %)

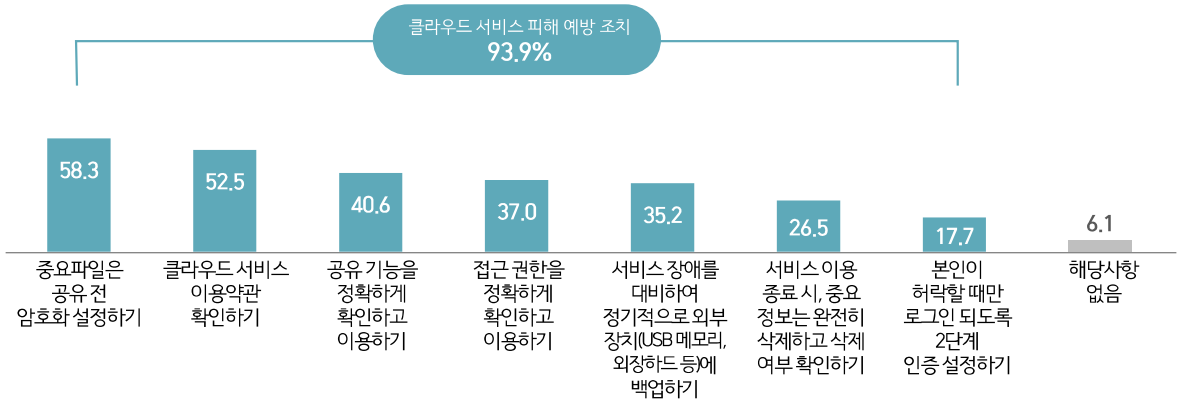



클라우드 서비스 이용자의 93.9%는 클라우드 서비스 피해 예방 조치를 취하는 것으로 조사되었다.

세부 유형별로는 '중요파일은 공유 전 암호화 설정하기'가 58.3%로 가장 높고, 다음으로 '클라우드 서비스 이용약관 확인하기(52.5%)', '공유기능을 정확하게 확인하고 이용하기(40.6%)' 등의 순으로 나타났다.

그림 2-3-45 클라우드 서비스 침해사고 예방 조치 (복수응답) - 클라우드 서비스 이용자

(단위 : %)



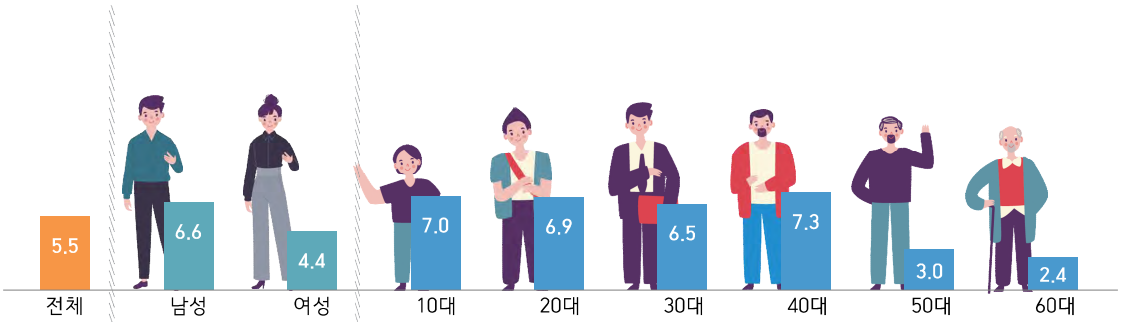
## 2. IP카메라

IP카메라 제품을 이용하는 비율은 5.5%로 조사되었다.

IP카메라 제품 이용률은 남성이 6.6%로 여성(4.4%)에 비해 2.2%p 높고, 40대(7.3%)에서 타 연령대 대비 상대적으로 높게 나타났다.

그림 2-3-46 IP카메라 제품 이용

(단위 : %)




IP카메라를 이용하는 목적은 '외부자 침입이나 도난 방지(45.1%)'가 가장 많고, 다음으로 '반려동물 확인(28.7%)', '가족 안전 확인(28.0%)' 등의 순으로 조사되었다.

그림 2-3-47 IP카메라 이용 목적 (복수응답) - IP카메라 제품 이용자

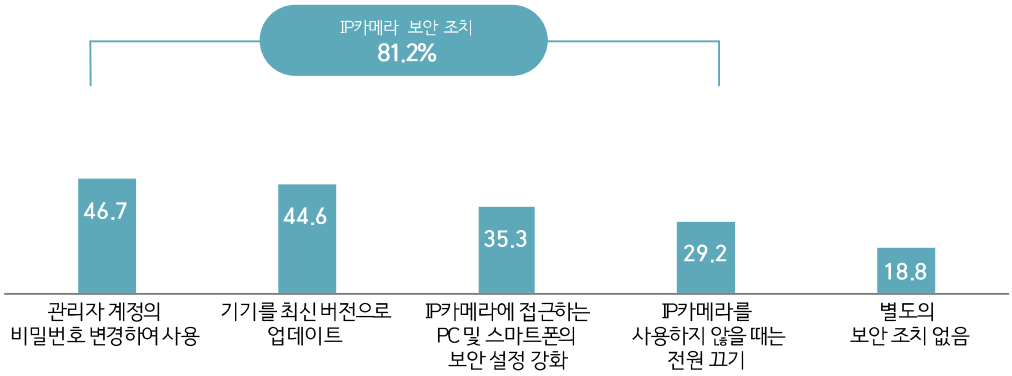
(단위 : %)

IP카메라 제품 이용자의 81.2%는 IP카메라 보안 조치를 취하는 것으로 나타났다.

세부 유형별로는 '관리자 계정의 비밀번호 변경하여 사용'이 46.7%로 가장 높고, 다음으로 '기기를 최신 버전으로 업데이트(44.6%)', 'IP카메라에 접근하는 PC 및 스마트폰의 보안 설정 강화(35.3%)' 등의 순이었다.

그림 2-3-48 IP카메라 보안을 위한 조치 (복수응답) - IP카메라 제품 이용자

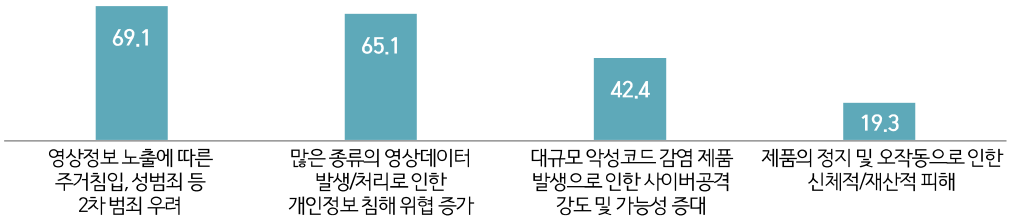
(단위 : %)




IP카메라 제품 보급이 확산될 경우 '영상정보 노출에 따른 주거침입, 성범죄 등 2차 범죄(69.1%)'를 가장 우려하는 것으로 나타났고, 다음으로 '많은 종류의 영상데이터 발생·처리로 인한 개인정보 침해 위협 증가(65.1%)'가 그 뒤를 이었다.

그림 2-3-49 IP카메라 보급 확산 시 보안 우려사항 (2가지)

(단위 : %)



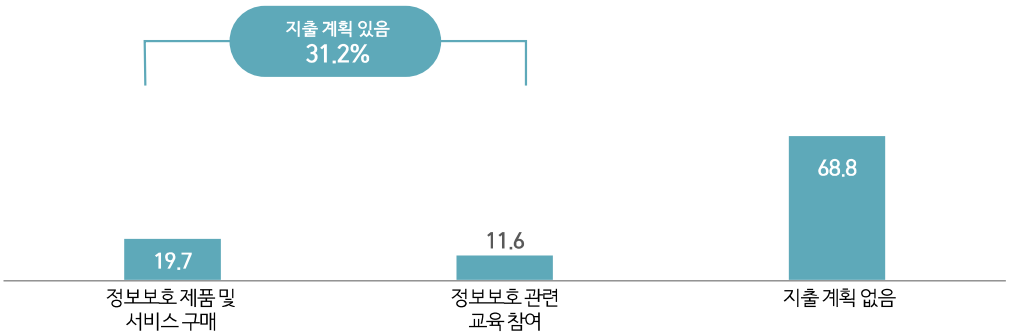
## 3. 향후 정보보호 지출 계획

인터넷 이용자의 31.2%는 향후 정보보호를 위한 지출 계획이 있는 것으로 조사되었다.

분야별로 살펴보면, '정보보호 제품 및 서비스 구매' 의향이 19.7%, '정보보호 관련 교육 참여'가 11.6%로 나타났다.

그림 2-3-50 향후 정보보호 지출 계획 분야

(단위 : %)



부록 1.

# 주요변경내역

# Ⅰ 기업부문

| 분 야 | 항 목 | 세 부 항 목 | 조사시기 |
|---|---|---|---|
| Ⅰ. 정보보호 기반 및 환경 | A. 정보보호 인식 | 정보보호 중요성 인식 | '19 -'20 |
| | | 개인정보보호 중요성 인식 | '19 -'20 |
| | | 경영진의 정보보호 중요성 인식 | '10 -'17 |
| | | 경영진의 개인정보보호 중요성 인식 | '10 -'17 |
| | | 경영진의 정보보호 관련 지식수준 | '14 |
| | | 일반직원들의 정보보호 중요성 인식 | '10 -'17 |
| | | 일반직원들의 개인정보보호 중요성 인식 | '10 -'17 |
| | | 일반직원의 정보보호 관련 지식수준 | '14 |
| | | 정보보호 위협요인 | '13 -'20 |
| | | 정보보호 인적 위협요인 | '06, '08 -'20 |
| | | 사이버 환경상의 안전성 정도 | '07 -'10 |
| | | 우려하는 개인정보 유출요인 | '12 -'20 |
| | | 정보보호 애로사항 | '15 -'20 |
| | | 정보보호 규제 동의 수준 | '15 -'16 |
| | B. 정보보호 정책 및 조직 | 정보보호(개인정보보호) 정책 수립 | '06 -'20 |
| | | 정보보호 정책 포함 위협요소 | '14 -'20 |
| | | 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 -'20 |
| | | 정보보호 관련 책임자 임명 및 전담 | '06 -'20 |
| | | 정보관리책임자(CIO)와 겸직 여부 | '16 |
| | | 정보보호 조직 및 담당인력 현황과 향후 계획 | '14 |
| | | IT인력 중 정보보호 담당 인력 비중 | '14, '16 -'20 |
| | | IT인력대비 정보보호 전담인력 투입 비율 | '10 |

| 분 야 | 항 목 | 세 부 항 목 | 조사시기 |
|---|---|---|---|
| | B. 정보보호 정책 및 조직 | 정보보호 담당 인력 신규 채용계획 | '17 -'20 |
| | | 정보보호 교육의 필요성 | '07 -'09 |
| | | 정보보호(개인정보보호) 교육 실시 | '06 -'20 |
| | | 교육 대상별 교육 실시 현황 | '06 -'20 |
| | | 정보보호 교육 프로그램별 교육 횟수, 교육시간 | '07 -'14 |
| | | 정보보호 교육 프로그램별 교육 시간, 교육평가 여부 | '16 |
| | | 정보보호 교육에 대한 직원들의 이해 정도 | '10 |
| | | 필요한 정보보호 교육 내용 | '15 |
| | | 실시된 정보보호 교육의 포함 내용 | '16 |
| | C. 정보보호 예산 | IT예산 중 정보보호 관련 예산 비중 | '06 -'20 |
| | | 정보보호 예산 총액 중 분야별 비율 | '14 |
| | | 정보보호 관련 예산 증감 | '11 -'20 |
| | | 정보보호 관련 예산 전년대비 증감 이유 | '19 -'20 |
| | | 정보보호 지출 분야 | '13 -'20 |
| | | 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 지출금액 증감 정도 | '14 |
| | | 정보보호 관련 예산 편성하지 않은 이유 | '06 -'16 |
| | | 정보보호 관련 지출 정도 | '07 -'13 |
| | | 정보보호 관련 투자 증감 | '10 -'13 |
| | | 정보보호 관련 지출이 없는 이유 | '07 -'13 |
| | | 예산 항목별 정보보호 지출 비율 | '09 |
| Ⅱ. 침해사고 예방 | A. 정보보호 제품 및 서비스 | 침해사고로부터 보호해야 할 자산 | '12 -'13 |
| | | 정보보호 제품 이용 | '06 -'20 |
| | | CCTV/IP카메라 보유 대수 | '16 -'20 |
| | | IP카메라 최초 비밀번호 변경 여부 | '19 |
| | | 정보보호 제품 국산/외산 비중 | '15 -'19 |
| | | 외산 정보보호 제품 및 서비스 지출 여부 | '19 -'20 |
| | | 외산 정보보호 제품 구매 이유 | '16 -'20 |
| | | 정보보호 서비스 이용 | '06 -'20 |
| | | 보안컨설팅 서비스 이용 기간 | '20 |

| 분 야 | 항 목 | 세 부 항 목 | 조사시기 |
|---|---|---|---|
| | | 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 보안점검(취약점 점검) 실시 | ‘09 -‘20 |
| | | 시스템 및 네트워크 보안점검(취약점 점검) 항목 | ‘14 -‘20 |
| | | 보안패치 적용 방법 | ‘07 -‘20 |
| | | 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 -‘20 |
| | | 구형 운영체제 사용 이유 | ‘17 |
| | | 시스템 로그 및 중요 데이터 백업 실시 여부 | ‘12 -‘20 |
| | | 시스템 로그 및 중요 데이터 백업 방식 | ‘17 -‘20 |
| | | 시스템 로그 및 중요 데이터 백업 실시 주기 | ‘12 -‘20 |
| Ⅲ. 침해사고 경험 및 대응 | A. 침해사고 경험 | 침해사고 피해 경험 | ‘06 -‘20 |
| | | 침해사고 피해 유형별 피해 빈도 | ‘07 -‘14 |
| | | 침해사고 피해 경험 유형 및 심각성 정도 | ‘14 -‘20 |
| | | 침해사고 피해 발생 경로 | ‘13 -‘14 |
| | | 침해사고 피해 사실 인지 시점 | ‘11 -‘14 |
| | | 침해사고 원인 파악 시점 | ‘14 |
| | | 침해사고 문제 해결 및 서비스 복원 시점 | ‘14 |
| | | 침해사고 시 관계기관에 문의 또는 신고 | ‘06 -‘20 |
| | | 정보보안 침해사고 발생 시 신고정도 | ‘11 |
| | | 정보보안 침해사고 발생 시 신고하지 않는 이유 | ‘06 -‘11, ‘14 -‘16 |
| | | 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 |

| 분 야 | 항 목 | 세 부 항 목 | 조사시기 |
|---|---|---|---|
| | | 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 -'20 |
| | | 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 |
| | | 게시판 스팸 대응 현황 | '10 -'11 |
| | | 운영 중인 웹사이트 내에 사이버 일탈행위 방지를 위한 조치 | '11 |
| | | 침해사고 대응 대외협력채널 | '17 -'20 |
| Ⅳ. 개인정보보호 | A. 개인정보 수집 | 개인정보 수집 및 이용 | '12 -'20 |
| | | 개인정보 온라인 수집 방법 | '14 -'20 |
| | | 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 -'20 |
| | | 개인정보 수집 및 이용 목적 | '12 -'20 |
| | | 보유하고 있는 이용자(고객) 개인정보 규모 | '12 -'14 |
| | B. 개인정보 침해사고 예방 | 개인정보 침해사고 예방을 위한 관리적 조치(사후처리) | '07 -'20 |
| | | 개인정보 침해사고 예방을 위한 기술적 조치 | '10 -'20 |
| | | 개인정보 암호화 | '09 -'20 |
| | | 회원가입, 홈페이지 이용 시 본인확인수단 | '14 |

| 분 야 | 항 목 | 세 부 항 목 | 조사시기 |
|---|---|---|---|
| | | 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 |
| | | 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 최소화여부 | '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 |

| 분 야 | 항 목 | 세 부 항 목 | 조사시기 |
|---|---|---|---|
| | | 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 수준 | '12 -'14 |
| | C. 개인정보 침해사고 | 개인정보 침해사고 경험 | '08 -'10<br>'12 -'20 |
| | | 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 -'20 |
| | | 개인정보 침해사고 외부 신고 여부 | '13 |
| | | 개인정보 침해사고 발생 시 고지 방법 | '12 -'13 |
| | | 개인정보 침해사고발생 시 신고하지 않은 이유 | '12 -'13 |
| | | 개인정보 침해사고 시 보상여부 | '12 |
| | | 개인정보 침해사고 시 통지 또는 고지 | '17 -'20 |
| | | 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 인지여부 | '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 |

| 분 야 | 항 목 | 세 부 항 목 | 조사시기 |
|---|---|---|---|
| | | 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 인지여부 | '12 -'13 |
| | | 신규제도 이행 시 필요한 사항 | '12 -'13 |
| | | 신규제도 도입 관련 준비 사항 | '12 -'13 |
| | | 사업자 대상 개인정보보호 교육 참석여부 | '12 -'13 |
| | | 개인정보보호 관련 무료교육 시 참석의향 | '12 -'13 |
| | | 희망하는 개인정보보호 교육 유형 | '12 -'13 |
| | | 개인정보보호 관련 교육 만족도 | '12 -'13 |
| | | 개인정보 취급자 대상 워크숍 인지여부 | '12 -'13 |
| | | 개인정보 취급자 대상 워크숍 인지경로 | '12 -'13 |
| | | 개인정보 취급자 대상 워크숍 참석여부 | '12 -'13 |
| | | 개인정보 취급자 대상 워크숍 성과평가 | '12 -'13 |
| | | 개인정보보호 포털사이트 인지여부 | '12 -'13 |
| | | 개인정보보호 포털사이트 이용 빈도 | '12 -'13 |
| | | 개인정보보호 포털사이트 이용내용 | '12 -'13 |
| | | 개인정보보호 포털사이트 성과평가 | '12 -'13 |
| | | 효율적인 개인정보보호 홍보 매체 | '13 |
| V. 주요 서비스별 정보보호 | A. 무선랜 | 무선랜 구축 및 운영 | '10 -'13, '15 -'20 |
| | | 무선랜 관련 보안 우려사항 | '12, '15 -'20 |
| | | 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 -'20 |
| | | 외부 상용무선인터넷 서비스 사용 가능여부 | '11 -'13 |
| | | 외부 상용무선인터넷 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 |

| 분 야 | 항 목 | 세 부 항 목 | 조 사 시 기 |
|---|---|---|---|
| | | 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 –’20 |
| | | 개인소유 모바일 기기 활용 시 보안 우려사항 | ’14 –’20 |
| | | 모바일 기기 활용 시의 보안위협에 대한 대응방안 | ’14 –’20 |
| | C. 클라우드 | 클라우드 서비스 이용 및 향후 도입(유지) 계획 | ’10 –’13, ’15 –’20 |
| | | 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 –’20 |
| | | 클라우드 서비스 보안을 위한 조치 | ’16 –’20 |
| | | 클라우드 서비스 보안 우려사항 | ’10 –’12, ’14 –’20 |
| | | 빅데이터 도입 및 활용 관련 우려사항 | ’14 |
| | D. 사물인터넷 (IoT) | 사물인터넷(IoT) 제품 및 서비스 이용 및 향후 도입(유지) 계획 | ’15 –’20 |
| | | 사물인터넷(IoT) 이용 활성화를 위해 개선되어야 할 사항 | ’15 –’16 |
| | | 사물인터넷(IoT) 이용(계획) 분야 | ’17 –’20 |
| | | 사물인터넷(IoT) 보안을 위한 조치 | ’19 –’20 |
| | | 사물인터넷(IoT) 관련 보안위협에 대한 우려 | ’15 –’20 |
| | E. 정보보호 (사이버) 보험 | 사이버(정보보호, 개인정보보호) 보험 인지 | ’17 –’20 |
| | | 사이버(정보보호, 개인정보보호) 보험 이용 및 향후 가입(유지) 계획 | ’17 –’20 |
| | | 사이버(정보보호, 개인정보보호) 보험 희망 보장 항목 | ’17 –’20 |
| | F. 향후 투자 계획 | 신규서비스 정보보호 투자 현황 | ’14 –’20 |

# Ⅱ 개인부문

| 분 야 | 항 목 | 세 부 항 목 | 조 사 시 기 |
|---|---|---|---|
| Ⅰ. 정보보호 인식 | | 정보보호 중요성 인식 | '06 -'20 |
| | | 개인정보보호 중요성 인식 | '08 -'19 |
| | | 위협사안에 대한 구체적 인지 | '14 -'20 |
| | | 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 -'20 |
| | | 정보보호 관련 정보수집 및 학습 애로사항 | '12 -'16 |
| Ⅱ. 침해사고 예방 | A. 정보보호 관련 제품 | 정보보호 제품* | '06 -'20 |
| | | 정보보호 제품 미이용 이유* | '12 -'18 |
| | | 정보보호 소프트웨어 이용* | '14 -'19 |
| | | 정보보호 제품 이용 시 활용 기능 | '12 -'15 |
| | | 악성코드 검사 실시 주기* | '14 -'20 |
| | | 파일 다운로드 시 바이러스 검사 방법 | '11 -'15 |
| | | 백신 프로그램 업데이트*[1] | '06 -'20 |
| | | 백신 프로그램 업데이트 실시 주기* | '14 -'20 |
| | | 운영체제 보안 업데이트*[2] | '06 -'20 |
| | | 운영체제 보안 업데이트 미실시 이유* | '12 -'18 |
| | | 구형 운영체제 사용 이유 | '17 |
| | | 중요 데이터 백업* | '15 -'20 |
| | | 중요 데이터 백업 방식* | '17 -'20 |
| | | 중요 데이터 백업 실시 주기* | '14 -'20 |
| | | PC 및 네트워크 보안을 위한 노력 | '12 -'20 |
| | | PC 비밀번호 설정 | '06 -'20 |
| | | 비밀번호 관리 조치 | '12 -'20 |
| | | 비밀번호 변경 주기 | '06 -'20 |
| | | 모바일기기 이용 | '14 -'17 |

| 분 야 | 항 목 | 세 부 항 목 | 조 사 시 기 |
|---|---|---|---|
| | B. 모바일 및 무선랜 보안 | 무선랜 이용 피해 예방 조치 | '11 -'20 |
| | | 모바일 기기 데이터 백업 | '17 |
| | | 모바일 기기 데이터 백업 방식 | '17 |
| | | 모바일 기기 데이터 백업 실시 주기 | '17 |
| | | 모바일 기기 피해 예방 조치 | '10 -'20 |
| | C. SNS 보안 | SNS 이용 | '11 -'20 |
| | | SNS 피해 유형별 인지 | '10 -'15 |
| | | SNS 피해 예방 조치 | '11 -'20 |
| Ⅲ. 침해사고 대응 | A. 침해사고 경험 | 침해사고 피해 경험 유형* | '11 -'20 |
| | | 피싱/파밍/스미싱 등 전자금융사기 피해 경로 | '10 -'20 |
| | B. 침해사고 대응조치 | 침해사고 대응활동 수행 | '12 -'20 |
| | | 침해사고 신고 또는 상담 문의 기관·업체 | '07 -'20 |
| | | 침해사고 신고 또는 상담하지 않은 이유 | '07 -'20 |
| | | 침해사고 발생 초동대처 주체 | '15 |
| | | 정보보호 규제방식에 대한 동의 정도 | '15 |
| Ⅳ. 개인정보보호 | A. 개인정보보호 조치 | 인터넷 상 개인정보 제공 목적 | '07-'20 |
| | | 인터넷 상 개인정보 제공 동의 시 선택사항 동의 여부 | '19-'20 |
| | | 인터넷 상 개인정보 제공 동의 시 이용약관 확인 여부 | '20 |
| | | 개인정보 침해사고 예방조치 | '08-'20 |
| | | 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 인지정도 | '15 |
| | | 개인정보 관련 권리 인지도 | '12 -'15 |
| | B. 개인정보 침해사고 및 대응 | 개인정보 침해사고 경험 | '06 -'20 |
| | | 개인정보 침해사고 경험 유형 | '06 -'20 |
| | | 개인정보 침해사고 대응조치 | '12 -'20 |

| 분 야 | 항 목 | 세 부 항 목 | 조 사 시 기 |
|---|---|---|---|
| Ⅴ. 주요 서비스별 정보보호 | A. 클라우드 | 클라우드 서비스 이용 | ‘15 -’20 |
| | | 클라우드 서비스 침해사고 예방 조치 | ‘15 -’20 |
| | B. 빅데이터 | 빅데이터 활용 서비스 경험 | ‘17 -’18 |
| | | 빅데이터 활용 서비스 확산 시 보안 우려사항 | ‘15 -’19 |
| | C. IP카메라 | IP카메라 제품 이용 | ‘19 -’20 |
| | | IP카메라 제품 이용 목적 | ‘19 -’20 |
| | | IP카메라 보안조치 유형 | ‘19 -’20 |
| | | IP카메라 보급 확산 시 보안 우려사항 | ‘19 -’20 |
| | | IP카메라에 추가되어야 하는 보안 기능 | ‘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 |
| | 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 |
| | 핀테크 | 간편결제 서비스 이용 | ‘15 -’18 |
| | | 이용한 간편결제 서비스 본인인증수단 | ‘17 -’18 |
| | | 일반결제 대비 간편결제 서비스 보안성 인식 | ‘15 -’18 |
| | E. 향후 지출 계획 | 향후 정보보호 지출 계획 분야 | ‘19 -’20 |

* 2018년 PC/모바일 문항 분리

1) ‘19년, 백신프로그램 업데이트 실시 여부만 묻는 항목으로 수정
2) ‘19년, 운영체제 보안 업데이트 실시 여부만 묻는 항목으로 수정

부록 2.

# 표본오차

# Ⅰ 기업부문

## 1. 정보보호(개인정보보호) 정책 수립률

| | 정보보호(개인정보보호) 정책 수립률 | 표본오차 | 상대 표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | 23.6 | 0.01 | 1.89 | 22.7 | 24.5 |
| (업종별) | | | | | |
| 1. 농림수산업 | 40.5 | 0.05 | 6.53 | 35.3 | 45.6 |
| 2. 제조업 | 17.4 | 0.02 | 6.34 | 15.2 | 19.5 |
| 3. 건설업 | 14.6 | 0.02 | 8.67 | 12.1 | 17.1 |
| 4. 도매 및 소매업 | 16.4 | 0.02 | 7.50 | 14.0 | 18.8 |
| 5. 운수업 | 16.9 | 0.03 | 8.77 | 14.0 | 19.8 |
| 6. 숙박 및 음식점업 | 13.2 | 0.03 | 10.15 | 10.6 | 15.8 |
| 7. 출판, 영상, 방송통신 및 정보서비스업 | 56.5 | 0.04 | 3.47 | 52.7 | 60.4 |
| 8. 금융 및 보험업 | 88.3 | 0.02 | 1.39 | 85.9 | 90.7 |
| 9. 부동산 및 임대업 | 12.3 | 0.03 | 11.66 | 9.5 | 15.1 |
| 10. 전문, 과학 및 기술서비스업 | 28.6 | 0.03 | 5.73 | 25.4 | 31.8 |
| 11. 사업시설관리 및 사업지원 서비스업 | 34.3 | 0.03 | 4.92 | 31.0 | 37.7 |
| 12. 협회, 단체, 수리 및 기타 개인서비스업 | 14.0 | 0.03 | 11.24 | 10.9 | 17.0 |
| 13. 기타 | 43.7 | 0.04 | 4.21 | 40.1 | 47.3 |
| (규모별) | | | | | |
| 1~4명 | 11.9 | 0.01 | 6.10 | 10.5 | 13.3 |
| 5~9명 | 30.8 | 0.03 | 4.47 | 28.1 | 33.5 |
| 10~49명 | 50.9 | 0.02 | 2.09 | 48.8 | 53.0 |
| 50~249명 | 76.4 | 0.02 | 1.25 | 74.5 | 78.2 |
| 250명 이상 | 96.6 | 0.01 | 0.33 | 96.0 | 97.2 |

## 2. 정보보호 정책 수립률

| | 정보보호 정책 수립률 | 표본오차 | 상대 표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | 21.4 | 0.01 | 2.02 | 20.5 | 22.2 |
| (업종별) | | | | | |
| 1. 농림수산업 | 35.4 | 0.05 | 7.27 | 30.4 | 40.5 |
| 2. 제조업 | 16.2 | 0.02 | 6.61 | 14.1 | 18.3 |
| 3. 건설업 | 12.1 | 0.02 | 9.65 | 9.8 | 14.4 |
| 4. 도매 및 소매업 | 14.7 | 0.02 | 7.98 | 12.4 | 17.0 |
| 5. 운수업 | 16.8 | 0.03 | 8.80 | 13.9 | 19.7 |
| 6. 숙박 및 음식점업 | 11.5 | 0.02 | 10.95 | 9.1 | 14.0 |
| 7. 출판, 영상, 방송통신 및 정보서비스업 | 52.3 | 0.04 | 3.77 | 48.5 | 56.2 |
| 8. 금융 및 보험업 | 87.9 | 0.02 | 1.41 | 85.5 | 90.4 |
| 9. 부동산 및 임대업 | 9.6 | 0.03 | 13.44 | 7.0 | 12.1 |
| 10. 전문, 과학 및 기술서비스업 | 25.0 | 0.03 | 6.28 | 21.9 | 28.1 |
| 11. 사업시설관리 및 사업지원 서비스업 | 26.3 | 0.03 | 5.96 | 23.2 | 29.3 |
| 12. 협회, 단체, 수리 및 기타 개인서비스업 | 13.6 | 0.03 | 11.42 | 10.5 | 16.6 |
| 13. 기타 | 39.1 | 0.04 | 4.63 | 35.6 | 42.7 |
| (규모별) | | | | | |
| 1~4명 | 9.8 | 0.01 | 6.83 | 8.4 | 11.1 |
| 5~9명 | 29.7 | 0.03 | 4.59 | 27.0 | 32.3 |
| 10~49명 | 47.1 | 0.02 | 2.26 | 45.0 | 49.1 |
| 50~249명 | 72.8 | 0.02 | 1.37 | 70.9 | 74.8 |
| 250명 이상 | 87.6 | 0.01 | 0.67 | 86.5 | 88.8 |

## 3. 개인정보보호 정책 수립률

| | 개인 정보보호 정책 수립률 | 표본오차 | 상대 표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | 22.5 | 0.01 | 1.95 | 21.7 | 23.4 |
| (업종별) | | | | | |
| 1. 농림수산업 | 40.0 | 0.05 | 6.59 | 34.9 | 45.2 |
| 2. 제조업 | 16.1 | 0.02 | 6.62 | 14.0 | 18.2 |
| 3. 건설업 | 14.0 | 0.02 | 8.90 | 11.5 | 16.4 |
| 4. 도매 및 소매업 | 15.2 | 0.02 | 7.84 | 12.8 | 17.5 |
| 5. 운수업 | 16.4 | 0.03 | 8.94 | 13.5 | 19.3 |
| 6. 숙박 및 음식점업 | 12.5 | 0.03 | 10.47 | 9.9 | 15.0 |
| 7. 출판, 영상, 방송통신 및 정보서비스업 | 53.4 | 0.04 | 3.69 | 49.5 | 57.2 |
| 8. 금융 및 보험업 | 87.6 | 0.02 | 1.43 | 85.2 | 90.1 |
| 9. 부동산 및 임대업 | 11.7 | 0.03 | 12.01 | 8.9 | 14.4 |
| 10. 전문, 과학 및 기술서비스업 | 25.0 | 0.03 | 6.29 | 21.9 | 28.0 |
| 11. 사업시설관리 및 사업지원 서비스업 | 33.8 | 0.03 | 4.98 | 30.5 | 37.1 |
| 12. 협회, 단체, 수리 및 기타 개인서비스업 | 13.6 | 0.03 | 11.41 | 10.6 | 16.6 |
| 13. 기타 | 42.8 | 0.04 | 4.29 | 39.2 | 46.4 |
| (규모별) | | | | | |
| 1~4명 | 10.9 | 0.01 | 6.41 | 9.6 | 12.3 |
| 5~9명 | 30.1 | 0.03 | 4.54 | 27.4 | 32.8 |
| 10~49명 | 48.9 | 0.02 | 2.18 | 46.8 | 51.0 |
| 50~249명 | 75.6 | 0.02 | 1.28 | 73.7 | 77.5 |
| 250명 이상 | 95.5 | 0.01 | 0.39 | 94.8 | 96.2 |

# 4. 정보보호 책임자 임명_정보관리책임자(CIO)

| | 정보관리 책임자 임명률 | 표본오차 | 상대 표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | 15.1 | 0.01 | 2.49 | 14.4 | 15.9 |
| (업종별) | | | | | |
| 1. 농림수산업 | 16.7 | 0.04 | 12.00 | 12.8 | 20.7 |
| 2. 제조업 | 12.5 | 0.02 | 7.70 | 10.6 | 14.3 |
| 3. 건설업 | 11.2 | 0.02 | 10.08 | 9.0 | 13.4 |
| 4. 도매 및 소매업 | 10.6 | 0.02 | 9.62 | 8.6 | 12.6 |
| 5. 운수업 | 4.9 | 0.02 | 17.48 | 3.2 | 6.5 |
| 6. 숙박 및 음식점업 | 6.1 | 0.02 | 15.55 | 4.2 | 7.9 |
| 7. 출판, 영상, 방송통신 및 정보서비스업 | 47.7 | 0.04 | 4.14 | 43.8 | 51.6 |
| 8. 금융 및 보험업 | 68.3 | 0.03 | 2.60 | 64.8 | 71.8 |
| 9. 부동산 및 임대업 | 9.5 | 0.03 | 13.47 | 7.0 | 12.0 |
| 10. 전문, 과학 및 기술서비스업 | 23.5 | 0.03 | 6.55 | 20.5 | 26.5 |
| 11. 사업시설관리 및 사업지원 서비스업 | 16.6 | 0.03 | 7.97 | 14.0 | 19.2 |
| 12. 협회, 단체, 수리 및 기타 개인서비스업 | 6.3 | 0.02 | 17.51 | 4.1 | 8.4 |
| 13. 기타 | 26.6 | 0.03 | 6.16 | 23.4 | 29.9 |
| (규모별) | | | | | |
| 1~4명 | 7.3 | 0.01 | 7.99 | 6.2 | 8.4 |
| 5~9명 | 19.1 | 0.02 | 6.14 | 16.8 | 21.4 |
| 10~49명 | 31.9 | 0.02 | 3.11 | 29.9 | 33.8 |
| 50~249명 | 63.7 | 0.02 | 1.69 | 61.6 | 65.8 |
| 250명 이상 | 84.6 | 0.01 | 0.76 | 83.3 | 85.9 |

# 5. 정보보호 책임자 임명_정보보호최고책임자(CISO)

| | 정보보호 최고책임자 임명률 | 표본오차 | 상대 표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | 5.2 | 0.00 | 4.47 | 4.8 | 5.7 |
| (업종별) | | | | | |
| 1. 농림수산업 | 7.4 | 0.03 | 19.09 | 4.6 | 10.1 |
| 2. 제조업 | 4.7 | 0.01 | 13.11 | 3.5 | 5.9 |
| 3. 건설업 | 4.8 | 0.02 | 15.88 | 3.3 | 6.4 |
| 4. 도매 및 소매업 | 4.1 | 0.01 | 16.04 | 2.8 | 5.4 |
| 5. 운수업 | 1.5 | 0.01 | 31.61 | 0.6 | 2.5 |
| 6. 숙박 및 음식점업 | 2.4 | 0.01 | 25.36 | 1.2 | 3.6 |
| 7. 출판, 영상, 방송통신 및 정보서비스업 | 18.3 | 0.03 | 8.36 | 15.3 | 21.2 |
| 8. 금융 및 보험업 | 32.5 | 0.03 | 5.49 | 29.0 | 36.0 |
| 9. 부동산 및 임대업 | 1.2 | 0.01 | 40.35 | 0.2 | 2.1 |
| 10. 전문, 과학 및 기술서비스업 | 12.6 | 0.02 | 9.54 | 10.3 | 15.0 |
| 11. 사업시설관리 및 사업지원 서비스업 | 4.6 | 0.01 | 16.28 | 3.1 | 6.0 |
| 12. 협회, 단체, 수리 및 기타 개인서비스업 | 1.1 | 0.01 | 42.29 | 0.2 | 2.1 |
| 13. 기타 | 6.1 | 0.02 | 14.52 | 4.4 | 7.9 |
| (규모별) | | | | | |
| 1~4명 | 2.7 | 0.01 | 13.50 | 2.0 | 3.4 |
| 5~9명 | 5.4 | 0.01 | 12.44 | 4.1 | 6.8 |
| 10~49명 | 10.8 | 0.01 | 6.12 | 9.5 | 12.1 |
| 50~249명 | 27.2 | 0.02 | 3.67 | 25.2 | 29.1 |
| 250명 이상 | 45.6 | 0.02 | 1.94 | 43.8 | 47.3 |

# 6. 정보보호 책임자 임명_개인정보보호책임자(CPO)

| | 개인 정보보호 책임자 임명률 | 표본오차 | 상대 표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | 15.6 | 0.01 | 2.45 | 14.8 | 16.3 |
| (업종별) | | | | | |
| 1. 농림수산업 | 18.3 | 0.04 | 11.39 | 14.2 | 22.3 |
| 2. 제조업 | 11.4 | 0.02 | 8.10 | 9.6 | 13.2 |
| 3. 건설업 | 8.9 | 0.02 | 11.45 | 6.9 | 10.9 |
| 4. 도매 및 소매업 | 14.3 | 0.02 | 8.11 | 12.0 | 16.6 |
| 5. 운수업 | 7.5 | 0.02 | 13.93 | 5.4 | 9.5 |
| 6. 숙박 및 음식점업 | 7.0 | 0.02 | 14.38 | 5.0 | 9.0 |
| 7. 출판, 영상, 방송통신 및 정보서비스업 | 43.0 | 0.04 | 4.55 | 39.2 | 46.8 |
| 8. 금융 및 보험업 | 63.3 | 0.04 | 2.90 | 59.7 | 66.9 |
| 9. 부동산 및 임대업 | 4.2 | 0.02 | 20.96 | 2.5 | 5.9 |
| 10. 전문, 과학 및 기술서비스업 | 20.5 | 0.03 | 7.14 | 17.6 | 23.4 |
| 11. 사업시설관리 및 사업지원 서비스업 | 23.0 | 0.03 | 6.52 | 20.0 | 25.9 |
| 12. 협회, 단체, 수리 및 기타 개인서비스업 | 18.4 | 0.03 | 9.54 | 14.9 | 21.8 |
| 13. 기타 | 22.3 | 0.03 | 6.93 | 19.2 | 25.3 |
| (규모별) | | | | | |
| 1~4명 | 10.7 | 0.01 | 6.47 | 9.4 | 12.1 |
| 5~9명 | 14.2 | 0.02 | 7.32 | 12.2 | 16.3 |
| 10~49명 | 28.0 | 0.02 | 3.42 | 26.1 | 29.9 |
| 50~249명 | 62.0 | 0.02 | 1.75 | 59.9 | 64.2 |
| 250명 이상 | 83.9 | 0.01 | 0.78 | 82.6 | 85.2 |

# 7. 정보보호 제품 이용 - 네트워크 보안

| | 제품 이용률 | 표본오차 | 상대 표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | 98.2 | 0.00 | 0.14 | 97.9 | 98.5 |
| (업종별) | | | | | |
| 1. 농림수산업 | 99.0 | 0.01 | 0.55 | 97.9 | 100.0 |
| 2. 제조업 | 98.2 | 0.01 | 0.39 | 97.5 | 99.0 |
| 3. 건설업 | 99.7 | 0.00 | 0.21 | 99.3 | 100.1 |
| 4. 도매 및 소매업 | 98.9 | 0.01 | 0.36 | 98.2 | 99.5 |
| 5. 운수업 | 96.1 | 0.01 | 0.80 | 94.6 | 97.6 |
| 6. 숙박 및 음식점업 | 96.7 | 0.01 | 0.73 | 95.4 | 98.1 |
| 7. 출판, 영상, 방송통신 및 정보서비스업 | 98.9 | 0.01 | 0.41 | 98.1 | 99.7 |
| 8. 금융 및 보험업 | 100.0 | 0.00 | 0.00 | 100.0 | 100.0 |
| 9. 부동산 및 임대업 | 98.4 | 0.01 | 0.56 | 97.3 | 99.5 |
| 10. 전문, 과학 및 기술서비스업 | 98.6 | 0.01 | 0.43 | 97.8 | 99.4 |
| 11. 사업시설관리 및 사업지원 서비스업 | 99.7 | 0.00 | 0.19 | 99.3 | 100.1 |
| 12. 협회, 단체, 수리 및 기타 개인서비스업 | 96.9 | 0.02 | 0.81 | 95.3 | 98.4 |
| 13. 기타 | 98.2 | 0.01 | 0.50 | 97.2 | 99.2 |
| (규모별) | | | | | |
| 1~4명 | 97.9 | 0.01 | 0.33 | 97.3 | 98.5 |
| 5~9명 | 98.1 | 0.01 | 0.41 | 97.3 | 98.9 |
| 10~49명 | 99.2 | 0.00 | 0.19 | 98.8 | 99.6 |
| 50~249명 | 99.5 | 0.00 | 0.16 | 99.2 | 99.8 |
| 250명 이상 | 99.7 | 0.00 | 0.10 | 99.5 | 99.9 |

# 8. 정보보호 제품 이용 - 시스템(단말) 보안

| | 제품 이용률 | 표본오차 | 상대 표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | **93.1** | **0.01** | **0.29** | **92.6** | **93.6** |
| (업종별) | | | | | |
| 1. 농림수산업 | 97.1 | 0.02 | 0.93 | 95.3 | 98.9 |
| 2. 제조업 | 94.2 | 0.01 | 0.72 | 92.8 | 95.5 |
| 3. 건설업 | 92.5 | 0.02 | 1.02 | 90.7 | 94.4 |
| 4. 도매 및 소매업 | 93.4 | 0.02 | 0.88 | 91.8 | 95.0 |
| 5. 운수업 | 95.5 | 0.02 | 0.86 | 93.8 | 97.1 |
| 6. 숙박 및 음식점업 | 93.3 | 0.02 | 1.06 | 91.4 | 95.3 |
| 7. 출판, 영상, 방송통신 및 정보서비스업 | 94.6 | 0.02 | 0.94 | 92.9 | 96.4 |
| 8. 금융 및 보험업 | 98.6 | 0.01 | 0.46 | 97.7 | 99.5 |
| 9. 부동산 및 임대업 | 90.2 | 0.03 | 1.44 | 87.6 | 92.7 |
| 10. 전문, 과학 및 기술서비스업 | 94.8 | 0.02 | 0.85 | 93.2 | 96.4 |
| 11. 사업시설관리 및 사업지원 서비스업 | 93.2 | 0.02 | 0.96 | 91.4 | 94.9 |
| 12. 협회, 단체, 수리 및 기타 개인서비스업 | 89.6 | 0.03 | 1.54 | 86.9 | 92.3 |
| 13. 기타 | 91.4 | 0.02 | 1.14 | 89.3 | 93.4 |
| (규모별) | | | | | |
| 1~4명 | 92.1 | 0.01 | 0.66 | 90.9 | 93.3 |
| 5~9명 | 94.1 | 0.01 | 0.75 | 92.7 | 95.5 |
| 10~49명 | 95.0 | 0.01 | 0.49 | 94.1 | 95.9 |
| 50~249명 | 97.2 | 0.01 | 0.38 | 96.5 | 97.9 |
| 250명 이상 | 98.3 | 0.00 | 0.23 | 97.9 | 98.8 |

# 9. 정보보호 제품 이용 - 콘텐츠/정보유출 방지 보안

| | 제품 이용률 | 표본오차 | 상대 표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | **47.3** | **0.01** | **1.11** | **46.3** | **48.4** |
| (업종별) | | | | | |
| 1. 농림수산업 | 52.7 | 0.05 | 5.10 | 47.4 | 58.0 |
| 2. 제조업 | 43.6 | 0.03 | 3.30 | 40.8 | 46.4 |
| 3. 건설업 | 43.8 | 0.03 | 4.06 | 40.3 | 47.3 |
| 4. 도매 및 소매업 | 46.2 | 0.03 | 3.57 | 43.0 | 49.5 |
| 5. 운수업 | 29.0 | 0.04 | 6.19 | 25.5 | 32.5 |
| 6. 숙박 및 음식점업 | 43.6 | 0.04 | 4.49 | 39.8 | 47.5 |
| 7. 출판, 영상, 방송통신 및 정보서비스업 | 58.0 | 0.04 | 3.36 | 54.1 | 61.8 |
| 8. 금융 및 보험업 | 78.9 | 0.03 | 1.97 | 75.9 | 81.9 |
| 9. 부동산 및 임대업 | 57.2 | 0.04 | 3.78 | 53.0 | 61.5 |
| 10. 전문, 과학 및 기술서비스업 | 57.1 | 0.04 | 3.14 | 53.6 | 60.6 |
| 11. 사업시설관리 및 사업지원 서비스업 | 58.3 | 0.03 | 3.01 | 54.9 | 61.8 |
| 12. 협회, 단체, 수리 및 기타 개인서비스업 | 47.3 | 0.04 | 4.78 | 42.9 | 51.7 |
| 13. 기타 | 48.7 | 0.04 | 3.81 | 45.1 | 52.3 |
| (규모별) | | | | | |
| 1~4명 | 41.0 | 0.02 | 2.69 | 38.8 | 43.1 |
| 5~9명 | 55.8 | 0.03 | 2.65 | 52.9 | 58.7 |
| 10~49명 | 57.8 | 0.02 | 1.82 | 55.7 | 59.8 |
| 50~249명 | 65.8 | 0.02 | 1.62 | 63.7 | 67.9 |
| 250명 이상 | 79.7 | 0.01 | 0.90 | 78.3 | 81.1 |

# 10. 정보보호 제품 이용 - 보안 관리

| | 제품 이용률 | 표본오차 | 상대 표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | 33.0 | 0.01 | 1.50 | 32.0 | 34.0 |
| (업종별) | | | | | |
| 1. 농림수산업 | 40.7 | 0.05 | 6.49 | 35.6 | 45.9 |
| 2. 제조업 | 34.5 | 0.03 | 4.01 | 31.8 | 37.2 |
| 3. 건설업 | 26.7 | 0.03 | 5.94 | 23.6 | 29.8 |
| 4. 도매 및 소매업 | 27.6 | 0.03 | 5.37 | 24.7 | 30.5 |
| 5. 운수업 | 28.7 | 0.04 | 6.24 | 25.2 | 32.2 |
| 6. 숙박 및 음식점업 | 24.9 | 0.03 | 6.86 | 21.6 | 28.3 |
| 7. 출판, 영상, 방송통신 및 정보서비스업 | 49.3 | 0.04 | 4.01 | 45.4 | 53.1 |
| 8. 금융 및 보험업 | 77.6 | 0.03 | 2.05 | 74.5 | 80.7 |
| 9. 부동산 및 임대업 | 22.4 | 0.04 | 8.13 | 18.8 | 26.0 |
| 10. 전문, 과학 및 기술서비스업 | 48.3 | 0.04 | 3.75 | 44.8 | 51.9 |
| 11. 사업시설관리 및 사업지원 서비스업 | 50.8 | 0.03 | 3.50 | 47.4 | 54.3 |
| 12. 협회, 단체, 수리 및 기타 개인서비스업 | 31.8 | 0.04 | 6.63 | 27.7 | 35.9 |
| 13. 기타 | 37.3 | 0.04 | 4.81 | 33.8 | 40.8 |
| (규모별) | | | | | |
| 1~4명 | 24.2 | 0.02 | 3.97 | 22.4 | 26.1 |
| 5~9명 | 40.3 | 0.03 | 3.63 | 37.4 | 43.1 |
| 10~49명 | 52.7 | 0.02 | 2.02 | 50.7 | 54.8 |
| 50~249명 | 62.5 | 0.02 | 1.74 | 60.4 | 64.7 |
| 250명 이상 | 78.5 | 0.01 | 0.93 | 77.1 | 79.9 |

# 11. 정보보호 제품 이용 - 인증 보안(바이오 인증 제외)

| | 제품 이용률 | 표본오차 | 상대 표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | 53.5 | 0.01 | 0.98 | 52.5 | 54.5 |
| (업종별) | | | | | |
| 1. 농림수산업 | 56.4 | 0.05 | 4.73 | 51.2 | 61.6 |
| 2. 제조업 | 47.7 | 0.03 | 3.04 | 44.8 | 50.5 |
| 3. 건설업 | 53.1 | 0.04 | 3.37 | 49.6 | 56.6 |
| 4. 도매 및 소매업 | 53.3 | 0.03 | 3.10 | 50.1 | 56.6 |
| 5. 운수업 | 36.8 | 0.04 | 5.18 | 33.1 | 40.5 |
| 6. 숙박 및 음식점업 | 47.4 | 0.04 | 4.16 | 43.6 | 51.3 |
| 7. 출판, 영상, 방송통신 및 정보서비스업 | 59.5 | 0.04 | 3.26 | 55.7 | 63.3 |
| 8. 금융 및 보험업 | 88.9 | 0.02 | 1.35 | 86.6 | 91.3 |
| 9. 부동산 및 임대업 | 60.9 | 0.04 | 3.50 | 56.7 | 65.1 |
| 10. 전문, 과학 및 기술서비스업 | 63.5 | 0.03 | 2.75 | 60.1 | 66.9 |
| 11. 사업시설관리 및 사업지원 서비스업 | 66.3 | 0.03 | 2.54 | 63.0 | 69.6 |
| 12. 협회, 단체, 수리 및 기타 개인서비스업 | 50.4 | 0.04 | 4.49 | 45.9 | 54.8 |
| 13. 기타 | 57.1 | 0.04 | 3.22 | 53.5 | 60.7 |
| (규모별) | | | | | |
| 1~4명 | 48.3 | 0.02 | 2.32 | 46.1 | 50.5 |
| 5~9명 | 58.6 | 0.03 | 2.51 | 55.7 | 61.5 |
| 10~49명 | 64.1 | 0.02 | 1.60 | 62.1 | 66.1 |
| 50~249명 | 70.8 | 0.02 | 1.44 | 68.8 | 72.8 |
| 250명 이상 | 81.8 | 0.01 | 0.84 | 80.5 | 83.2 |

# Ⅱ 개인부문

## 1. 운영체제 보안 업데이트 실시율

| | 운영체제 보안 업데이트 실시율 | 표본오차 | 상대표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | **79.8** | **1.17** | **0.75** | **78.6** | **81.0** |
| (성별) | | | | | |
| 남성 | 83.0 | 1.54 | 0.95 | 81.5 | 84.5 |
| 여성 | 76.4 | 1.77 | 1.18 | 74.6 | 78.1 |
| (연령별) | | | | | |
| 12-19세 | 87.5 | 2.67 | 1.55 | 84.9 | 90.2 |
| 20대 | 93.2 | 1.79 | 0.98 | 91.4 | 95.0 |
| 30대 | 93.2 | 1.77 | 0.97 | 91.5 | 95.0 |
| 40대 | 83.1 | 2.54 | 1.56 | 80.5 | 85.6 |
| 50대 | 69.0 | 3.10 | 2.30 | 65.9 | 72.1 |
| 60대 | 50.5 | 3.75 | 3.79 | 46.7 | 54.2 |

## 2. 정보보호 제품 이용률

| | 정보보호 제품 이용률 | 표본오차 | 상대표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | **87.8** | **0.96** | **0.56** | **86.9** | **88.8** |
| (성별) | | | | | |
| 남성 | 88.6 | 1.30 | 0.75 | 87.3 | 89.9 |
| 여성 | 87.0 | 1.40 | 0.82 | 85.6 | 88.4 |
| (연령별) | | | | | |
| 12-19세 | 94.6 | 1.83 | 0.99 | 92.8 | 96.4 |
| 20대 | 96.6 | 1.28 | 0.68 | 95.4 | 97.9 |
| 30대 | 98.0 | 0.99 | 0.52 | 97.0 | 99.0 |
| 40대 | 91.0 | 1.94 | 1.09 | 89.1 | 92.9 |
| 50대 | 82.4 | 2.56 | 1.58 | 79.8 | 85.0 |
| 60대 | 61.3 | 3.66 | 3.04 | 57.6 | 64.9 |

## 3. 중요 데이터 백업 실시율

| | 중요 데이터 백업 실시율 | 표본오차 | 상대표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | **47.0** | **1.46** | **1.58** | **45.6** | **48.5** |
| (성별) | | | | | |
| 남성 | 52.9 | 2.05 | 1.98 | 50.8 | 54.9 |
| 여성 | 40.9 | 2.05 | 2.56 | 38.8 | 42.9 |
| (연령별) | | | | | |
| 12-19세 | 56.5 | 4.00 | 3.61 | 52.5 | 60.5 |
| 20대 | 78.5 | 2.91 | 1.89 | 75.6 | 81.4 |
| 30대 | 69.5 | 3.24 | 2.38 | 66.2 | 72.7 |
| 40대 | 48.2 | 3.39 | 3.58 | 44.9 | 51.6 |
| 50대 | 24.2 | 2.87 | 6.06 | 21.3 | 27.1 |
| 60대 | 3.2 | 1.31 | 21.18 | 1.9 | 4.5 |

## 4. 개인정보 침해사고 경험률

| | 개인정보 침해사고 경험률 | 표본오차 | 상대표준오차 | 95% 신뢰구간 | |
|---|---|---|---|---|---|
| | | | | 하한(%) | 상한(%) |
| 전체 | **1.2** | **0.32** | **13.48** | **0.9** | **1.5** |
| (성별) | | | | | |
| 남성 | 1.2 | 0.44 | 19.08 | 0.7 | 1.6 |
| 여성 | 1.2 | 0.46 | 19.05 | 0.8 | 1.7 |
| (연령별) | | | | | |
| 12-19세 | 0.5 | 0.58 | 56.94 | 0.0 | 1.1 |
| 20대 | 1.2 | 0.78 | 32.73 | 0.4 | 2.0 |
| 30대 | 2.1 | 1.00 | 24.77 | 1.1 | 3.1 |
| 40대 | 1.7 | 0.87 | 26.60 | 0.8 | 2.5 |
| 50대 | 1.1 | 0.71 | 32.14 | 0.4 | 1.8 |
| 60대 | 0.0 | 0.00 | - | 0.0 | 0.0 |

부록 3.

# 설문지

# 2020년 정보보호 실태조사 (기업)

승인번호 제 342005 호

안녕하십니까?

과학기술정보통신부와 한국정보보호산업협회에서는 우리나라 사업체의 정보보호 현황과 침해사고 피해 실태를 파악하여 관련 정책 수립의 기초자료를 마련하고자 전국의 사업체를 대상으로 **"2020년 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.

2020년 8월

| 주관기관 | 전담기관 | 조사기관 | 실사 문의 | 조사 문의 |
|---|---|---|---|---|
| 과학기술정보통신부 | 한국정보보호산업협회 | ㈜글로벌리서치 | 강미애 과장<br>02-3456-1904<br>kma@globalri.co.kr | 유새힘 대리<br>02-3456-1743 |

* 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 | | | | |
| 조직형태 | ☐ ① 개인사업체 | | ☐ ② 회사법인 | | ☐ ③ 회사이외의 법인 | | ☐ ④ 비법인단체 | | |
| 업 종 | ☐ ① 농림수산업 | | ☐ ② 제조업 | | ☐ ③ 건설업 | | | | |
| | ☐ ④ 도매 및 소매업 | | ☐ ⑤ 운수 및 창고업 | | ☐ ⑥ 숙박 및 음식점업 | | | | |
| | ☐ ⑦ 정보통신업 | | ☐ ⑧ 금융 및 보험업 | | ☐ ⑨ 부동산업 | | | | |
| | ☐ ⑩ 전문, 과학 및 기술서비스업 | | ☐ ⑪ 사업시설관리, 사업지원 및 임대 서비스업 | | ☐ ⑫ 협회, 단체 수리 및 기타 개인서비스업 | | | | |
| | ☐ ⑬ 기타(_____) | | | | | | | | |
| 규 모 (비정규직 포함) | ☐ ① 1 ~ 4명 | | ☐ ② 5 ~ 9명 | | ☐ ③ 10 ~ 49명 | | ☐ ④ 50 ~ 249명 | | |
| | ☐ ⑤ 250 ~ 499명 | | ☐ ⑥ 500 ~ 999명 | | ☐ ⑦ 1,000명 이상 | | | | |

## 응답해 주실 때 꼭 지켜 주십시오

1 첫 페이지부터 **순서대로 차례차례** 응답해 주십시오. 질문 앞에 특별한 언급이 없는 한 모든 질문에 답해 주십시오.

2 지사/지점 등의 경우에는 **지사/지점의 상황**에 맞게 응답하여 주시되, **본사의 지침에 따르거나 관리를 받고 있는 경우 본사의 확인을 받아 응답**하여 주셔야 합니다.

3 응답은 귀사의 내외부 **정보보호 업무를 총괄하시는 담당자**(전산, IT, 정보보호 등)께서 해주십시오. 정보보호 업무가 별도로 지정되어 있지 않은 경우, **총무담당자나 대표**께서 직접 기입해 주셔도 됩니다.

4 질문지에 응답하실 때 **특별한 지시가 없으면 보기 번호 중 한 개만** 선택해 주십시오.

5 특별한 언급이 없는 한 모든 설문의 응답 기준 시점은 **「2019년 12월 31일 기준」**으로 응답해 주시기 바랍니다. 그러나 특정 파트에서는 **「2020년 7월 1일 기준」**이며, 설문에 별도로 표시가 되어있습니다.

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

7 설문의 이해를 돕기 위한 사업체 또는 제품명의 예시는 가나다 순으로 작성하였습니다.

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

## * | 먼저, 응답 사업체 선정을 위한 질문입니다.

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

☐ 1) 예 ☐ 2) 아니오 ☞ **조사중단**

본 설문에서는 '정보보호'와 '개인정보보호'를 구분하여 사용하고 있으니 유념하여 응답해 주십시오.

**정보보호**
정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단 또는 그러한 수단으로 이루어지는 조치

**개인정보보호**
개인정보 침해 문제 방지를 위한 종합적 접근 및 대책을 위한 관리적· 기술적 수단 또는 그러한 수단으로 이루어지는 조치

## Ⅰ | 정보보호 기반 및 환경

### A. 정보보호 인식

**01** 귀사는 정보보호 및 개인정보보호에 대하여 얼마나 중요하게 생각하십니까?

| 항 목 | 전혀 중요하지 않다 | 중요하지 않은 편이다 | 보통이다 | 중요한 편이다 | 매우 중요하다 |
|---|---|---|---|---|---|
| 1) 정보보호 | ① | ② | ③ | ④ | ⑤ |
| 2) 개인정보보호 | ① | ② | ③ | ④ | ⑤ |

**02** 다음의 위협요인 중 귀사가 우려하는 정도가 높은 항목을 **2가지**만 선택해 주십시오.

☐ 1) 인터넷 침해사고 위협
(해킹, 악성코드(웜·바이러스 등), DDoS, 랜섬웨어 등)
☐ 2) 개인정보 유출 위협
☐ 3) 시스템 및 네트워크 장애
☐ 4) 인적요인에 의한 위협
☐ 5) 기타 (적을 것: _____)

**DDos(Distributed Denial of Service)**
인터넷 사이트에 서비스 거부(DoS)를 유발하는 해킹 기법으로, 특정 인터넷 사이트가 소화할 수 없는 규모의 접속 통신량(트래픽)을 한꺼번에 일으켜 서비스 체계를 마비시킴

**02-1** 다음 중 귀사가 **가장** 우려하는 **인적요인에 의한 위협**은 무엇입니까?

☐ 1) 현재 근무 중인 직원
☐ 2) 퇴사한 직원
☐ 3) 현재 근무 중인 외주(아웃소싱)업체 직원
☐ 4) 퇴사한 외주(아웃소싱)업체 직원
☐ 5) 외부인(방문자 등)
☐ 6) 기타(적을 것 :_____)

**외주(아웃소싱)업체 직원**
아웃소싱, 컨소시엄(협력업체), 자문위원 등을 포함

**03** 다음 중 귀사가 우려하는 **개인정보 유출 요인**은 무엇입니까? 우려하는 정도가 높은 항목을 **2가지만** 선택해 주십시오.

☐ 1) 외부로부터 해킹
☐ 2) 관리 실수로 인한 유출
☐ 3) 내부자에 의한 고의 유출
☐ 4) 외주(아웃소싱)업체에 의한 유출
☐ 5) 기타 (적을 것: _____)

**04** 귀사가 정보보호에 대해 어려움을 느끼는 사항은 무엇입니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 정보보호 예산 확보
☐ 2) 정보보호 전문인력 확보
☐ 3) 정보보호 담당인력 운용(관리)
☐ 4) 정보보호 교육 프로그램 운영
☐ 5) 필요한 정보보호 제품 및 서비스를 찾기 어려움
☐ 6) 기타 (적을 것: _____)

## B. 정보보호 정책 및 조직

**05** 귀사에는 공식 문서로 작성된 정보보호 및 개인정보보호 정책이 있습니까?

정보보호 정책에 포함하여 수립한 경우도 개인정보보호 정책을 수립한 것으로 응답합니다.

| 항목 | 보유 | |
|---|---|---|
| | 예 | 아니오 |
| 1) 정보보호 정책 | ☐ ① | ☐ ② |
| 2) 개인정보보호 정책 | ☐ ① | ☐ ② |

☞ **문 5의 1)에서 ② 응답자는 문 6으로 이동**

문 5의 1)에서 ① 응답자만

**05-1** 귀사의 정보보호 정책은 어떤 위협요소에 대한 내용을 포함하고 있습니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 인터넷 침해위협(해킹, 악성코드 (웜·바이러스 등), DDoS, 랜섬웨어 등)
☐ 2) 개인정보 유출 위협
☐ 3) 시스템 및 네트워크 장애
☐ 4) 인적요인에 의한 위협
☐ 5) 기타(적을 것: _____)

**06** 귀사는 아래의 공식적인 조직을 운영하고 있습니까? 해당 항목을 **각각** 선택해 주십시오.

| 구분 | 운영 | |
|---|---|---|
| | 예 | 아니오 |
| 1) 정보보호 조직 (전담조직) | ☐ ① | ☐ ② |
| 2) 개인정보보호 조직 (전담조직) | ☐ ① | ☐ ② |
| 3) 정보보호 조직과 개인정보보호 조직 공동 운영 | ☐ ① | ☐ ② |

**07** 귀사에는 다음의 책임자가 임명되어 있습니까? 임명·전담여부를 책임자별로 각각 선택해 주십시오.

| 구분 | 임명 | 전담 |
|---|---|---|
| 1) 정보관리책임자 (CIO : Chief Information Officer) | ☐ ① 예 ☐ ② 아니오 | ☐ ① 예 ☐ ② 아니오 |
| 2) 정보보호최고책임자 (CISO : Chief Information Security Officer) | ☐ ① 예 ☐ ② 아니오 | ☐ ① 예 ☐ ② 아니오 |
| 3) 개인정보보호책임자 (CPO : Chief Privacy Officer) | ☐ ① 예 ☐ ② 아니오 | ☐ ① 예 ☐ ② 아니오 |

**정보관리책임자(CIO)**
조직의 경영과 전략적 관점에서 정보기술 및 정보시스템을 총괄 관리하는 최고 책임자

**정보보호최고책임자(CISO)**
정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임명된 최고 책임자

**개인정보보호책임자(CPO)**
이용자의 개인정보를 보호하고, 개인정보와 관련한 이용자의 고충을 처리하는 최고 책임자

**08** 귀사의 IT 인력 중 정보보호(개인정보보호 포함) 담당 인력이 차지하는 비중은 어떻게 됩니까?

☐ 1) 1% 미만
☐ 2) 1%~3% 미만
☐ 3) 3%~5% 미만
☐ 4) 5%~7% 미만
☐ 5) 7%~10% 미만
☐ 6) 10% 이상(적을 것: _____)
☐ 7) 정보보호 담당 인력 없음

**IT 인력**
IT 관련 업무가 전체 업무의 50% 이상을 차지하는 인력

**08-1** 귀사는 2020년에 정보보호(개인정보보호 포함) 담당 인력을 신규로 채용했거나, 추후 채용할 계획이 있습니까? 있다면, 2020년 총 채용 규모는 어떻게 되십니까?

☐ 1) 채용했거나, 채용 계획이 있음
☞ 2020년 총 채용규모: _____명
☐ 2) 채용하지 않았고, 채용 계획도 없음
☐ 3) 모름

## C. 정보보호 교육

**09** 귀사는 2019년 1년 간 임직원을 대상으로 정보보호(개인정보보호 포함) 교육을 실시했습니까?
(외부 위탁 교육을 포함하여 응답해 주십시오)

☐ 1) 예 ☐ 2) 아니오

☞ **문 9의 2) 응답자는 문 10으로 이동**

문9의 "1) 예" 응답자만

**09-1** 귀사는 2019년 1년 간 다음의 임직원 대상 정보보호 교육(개인정보보호 포함)을 실시했습니까?

| 교육 대상 | 교육 실시 여부 |
|---|---|
| 1) **CEO 등 경영진** | ☐ ① 교육 실시 |
| | ☐ ② 미실시 |
| 2) **정보보호 책임자급 직원** (CIO, CPO, CISO 등) | ☐ ① 교육 실시 |
| | ☐ ② 미실시 |
| | ☐ ③ 정보보호 책임자급 직원 없음 |
| 3) **정보보호 관련 직원** (개인정보취급자, 정보보호 실무자, IT 실무자 등) | ☐ ① 교육 실시 |
| | ☐ ② 미실시 |
| | ☐ ③ 정보보호 관련 직원 없음 |
| 4) **일반 직원** | ☐ ① 교육 실시 |
| | ☐ ② 미실시 |

**개인정보취급자**

개인정보를 처리하는 공공기관이나 사업자·단체 등의 지휘·감독을 받아 개인정보를 처리하는 임직원, 시간제 근로자 등

## D. 정보보호 예산

**10** 귀사의 2019년 1년 간 IT예산 총액 중 정보보호(개인정보보호 포함) 관련 예산 비중은 몇 퍼센트(%)였습니까?

☐ 1) 1% 미만
☐ 2) 1%~3% 미만
☐ 3) 3%~5% 미만
☐ 4) 5%~7% 미만
☐ 5) 7%~10% 미만
☐ 6) 10% 이상(적을 것: _____)
☐ 7) 정보보호(개인정보보호) 예산 없음

**정보보호(개인정보보호 포함) 예산 포함 항목**

정보보호 및 개인정보보호를 위한 인건비, 제품 및 서비스 구입비, 정보보호 시스템 유지 보수비, 정보보호 교육·훈련비, 인증 취득비용 등

☞ **문 10의 7) 응답자는 문 11로 이동**

문 10의 1)~6) 응답자

**10-1** 귀사의 2019년 1년 간 IT예산 총액 중 정보보호(개인정보보호 포함) 관련 예산 비중은 2018년 대비 증가(감소)하였습니까?
(금액 기준이 아닌 비중의 변화를 기준으로 응답해 주십시오)

☐ 1) 증가
☐ 2) 감소
☐ 3) 변동없음

☞ **문 10-1의 3) 응답자는 문 10-3으로 이동**

문 10-1의 1) 또는 2) 응답자

**10-2** 귀사의 2019년 1년 간 IT예산 총액 중 정보보호(개인정보보호 포함) 관련 예산 비중이 2018년 대비 증가(감소)한 이유는 무엇입니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) IT예산 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 보수비 증가(감소)
☐ 6) ISMS, ISMS-P, PIMS, ISO 등 인증 취득 비용 (취득 수수료 등) 증가(감소)
☐ 7) 기타 (적을 것: _____)

문 10의 1)~6) 응답자

**10-3** 2019년 1년 간 정보보호(개인정보보호 포함)와 관련하여 귀사가 예산을 많이 지출한 항목은 무엇입니까? **주된 2가지만** 선택해 주십시오.

☐ 1) 정보보호 인력 인건비
☐ 2) 정보보호 제품 구입 비용(네트워크, 시스템, 인증 제품, 소프트웨어 등)
☐ 3) 정보보호 서비스 구입 비용(관제, 컨설팅 등)
☐ 4) 정보보호 시스템 유지 보수 비용
☐ 5) ISMS, ISMS-P, PIMS, ISO 등 인증 취득비용 (취득 수수료, 컨설팅 비용 등)
☐ 6) 기타(적을 것: _____)

# Ⅱ | 침해사고 예방

## A. 정보보호 제품 및 서비스

**11** 귀사에서는 정보보호를 위해 다음 중 어떤 **제품**을 이용하고 있습니까? 해당 항목을 **모두** 선택해 주십시오.

| | 사용 중인 제품 분야 |
|---|---|
| 정보보안 제품 | ☐ 1) 네트워크 보안 |
| | ☐ 2) 시스템(단말) 보안 |
| | ☐ 3) 콘텐츠/정보 유출 방지 보안 |
| | ☐ 4) 인증 보안(바이오 인증 제외) |
| | ☐ 5) 보안관리 |
| | ☐ 6) 기타 (적을 것: _____) |
| | ☐ 7) 미이용 |
| 물리보안 제품 | ☐ 1) 인증 보안(바이오 인증-지문/홍채인식 등) |
| | ☐ 2) 영상정보 처리기기(CCTV) |
| | ☐ 3) 기타 (적을 것: _____) |
| | ☐ 4) 미이용 |

**<정보보안 제품>**

**네트워크 보안**
통합보안시스템(UTM), 웹방화벽, 네트워크(시스템)방화벽, 침입방지시스템(IPS), DDoS 차단 시스템, 가상사설망(VPN), 네트워크 접근제어(NAC), 무선네트워크 보안, 망분리(가상화) 등

**시스템(단말)보안**
시스템접근통제(PC 방화벽 포함), Anti 멀웨어(백신, Anti 스파이웨어, 랜섬웨어), 스팸차단S/W, 보안운영체제, APT대응, 모바일 보안 등

**콘텐츠/정보 유출 방지 보안**
DB보안(접근통제), DB암호, 보안USB, 디지털저작권관리(DRM), 네트워크DLP, 단말DLP(개인정보보호솔루션 포함) 등

**인증 보안 (바이오 인증 제외)**
일회용비밀번호(OTP), 공개키기반 구조(PKI), 통합접근관리(EAM)/싱글사인온(SSO), 통합계정관리(IM/IAM) 등

**보안관리**
통합보안관리(ESM), 위협관리시스템(TMS), 패치관리시스템(PMS), 백업/복구관리시스템, 로그 관리/분석 시스템, 취약점 분석 시스템, 디지털 포렌식 시스템 등

**<물리보안 제품>**
물리적으로 정보, 시설 등을 보호하는 것을 의미함.
대표적으로 회사원들의 사원증, 전자 도어락, CCTV 등이 있음

☞ **문 11에서 정보보안 제품 및 물리보안 제품에 모두 '미이용' 응답자는 문 12로 이동**

문 11의 물리보안 제품 "2) 영상정보 처리기기(CCTV)" 이용 응답자만

**11-1** 귀사에서는 2019년 12월 31일 기준으로 CCTV 몇 대를 설치·운영하고 있습니까? 해당 항목을 **모두** 선택해 주십시오.
(외부 업체를 통해 설치·운영하는 경우도 포함하여 응답해주십시오)

| 보유 대수 | ① 폐쇄회로 | ② IP카메라 |
|---|---|---|
| 1) 1~4대 | ☐ ① | ☐ ① |
| 2) 5~9대 | ☐ ② | ☐ ② |
| 3) 10~19대 | ☐ ③ | ☐ ③ |
| 4) 20~49대 | ☐ ④ | ☐ ④ |
| 5) 50대 이상 | ☐ ⑤ | ☐ ⑤ |
| 6) 없음 | ☐ ⑥ | ☐ ⑥ |

**폐쇄회로 CCTV**
화상정보를 특정의 목적으로, 특정의 수신자에게 전달하며 주로 유선에 의한 영상전송방식
(예. 엘레베이터 CCTV, 백화점 CCTV, 사무실 CCTV 등)

**IP 카메라**
카메라와 컴퓨터가 하나의 장치로 결합된 것으로 폐쇄회로 텔레비전과 달리 통신망을 이용해 영상정보를 송출하고 클라우드 서버에 저장하며, 모바일 기기나 PC 등을 통해 확인 가능함 (예. SK 클라우드캠, LG u+ 지능형 CCTV, KT 기가아이즈 등)

☞ **문 11-1의 '② IP카메라'의 6) 응답자는 문 12로 이동**

**12** 귀사에서는 정보보호를 위해 다음 중 어떤 **서비스**를 이용하고 있습니까? 해당 항목을 **모두** 선택해 주십시오.

| 항목 | 이용여부 | |
|---|---|---|
| | 이용 | 미이용 |
| 1) 보안컨설팅 | ① | ② |
| 2) 유지관리/보안성 지속 서비스 | ① | ② |
| 3) 보안관제 서비스 | ① | ② |
| 4) 교육/훈련 | ① | ② |
| 5) 인증서 서비스 | ① | ② |

☞ **문 12의 모두 '미이용' 응답자 중, 문 11의 정보보안 및 물리보안 제품 모두 '미이용' 응답자는 문 14로 이동**

문 12의 "1) 보안컨설팅" ① 이용 응답자만

**12-1** 귀사에서는 보안컨설팅 서비스를 얼마나 이용하셨습니까?

☐ 1) 1년 미만
☐ 2) 1년~3년 미만
☐ 3) 3년~5년 미만
☐ 4) 5년 이상

문 12의 "1) 보안컨설팅" ① 이용 응답자만

**12-2** 귀사에서는 어떤 분야의 보안컨설팅 서비스를 이용하고 있습니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 정보보호평가/인증(ISO, ISMS, CC 등)
☐ 2) 진단 및 모의해킹
☐ 3) 개인정보보호컨설팅
☐ 4) 정보감사(내부정보유출방지컨설팅 등)
☐ 5) 기타보안컨설팅(기반보호/보안SI 포함)

문 12의 "1) 보안컨설팅" ① 이용 응답자만

**12-3** 귀사의 2019년 1년 간 IT예산 총액 중 보안컨설팅 서비스 관련 예산 비중은 몇 퍼센트(%)였습니까?

☐ 1) 1% 미만
☐ 2) 1%~3% 미만
☐ 3) 3%~5% 미만
☐ 4) 5%~7% 미만
☐ 5) 7%~10% 미만
☐ 6) 10% 이상(적을 것: _____)

문 11과 문 12 중 하나라도 이용하는 응답자

**13** 귀사의 2019년 1년 간 정보보호(개인정보보호 포함) 관련 지출 중, **외산** 제품 및 서비스에 대한 **지출**이 포함되어 있습니까?

**※ 제조사 기준이 아닌 벤더사(유통업체) 기준**
외산 제품 예시 : IBM, HP, 델, 시스코, PaloAlto Networks, Fortinet, NSFocus, Venustech, Westone, TopSec 등

| | 사용 중인 외산 제품/서비스 분야 |
|---|---|
| **정보보안 제품** | ☐ 1) 네트워크 보안 |
| | ☐ 2) 시스템(단말) 보안 |
| | ☐ 3) 콘텐츠/정보 유출 방지 보안 |
| | ☐ 4) 인증 보안(바이오 인증 제외) |
| | ☐ 5) 보안관리 |
| | ☐ 6) 기타 (적을 것: _____) |
| | ☐ 7) 지출 없음 |
| **물리보안 제품** | ☐ 1) 인증 보안(바이오 인증-지문/홍채인식 등) |
| | ☐ 2) 영상정보 처리기기(CCTV) |
| | ☐ 3) 기타 (적을 것: _____) |
| | ☐ 4) 지출 없음 |
| **정보보호 서비스** | ☐ 1) 보안컨설팅 |
| | ☐ 2) 유지관리/보안성 지속 서비스 |
| | ☐ 3) 보안관제 서비스 |
| | ☐ 4) 교육/훈련 |
| | ☐ 5) 인증서 서비스 |
| | ☐ 6) 기타 (적을 것: _____) |
| | ☐ 7) 지출 없음 |

☞ **문 13의 정보보안 제품, 물리보안 제품, 정보보호 서비스 모두 '지출 없음' 응답자는 문 14로 이동**

문 13의 외산 제품 및 서비스 중 하나라도 지출 있는 응답자만

**13-1** 국산 대신 외산 정보보호 제품 및 서비스를 구매하신 **주된** 이유는 무엇입니까?

☐ 1) 보다 저렴한 가격 때문에
☐ 2) 성능·품질 및 서비스가 우수하기 때문에
☐ 3) 유지보수관리가 용이하기 때문에
☐ 4) 브랜드 및 업체에 대한 신뢰성 때문에
☐ 5) 기타 (적을 것 :_____)

## B. 정보보호 관리

**14** 귀사에서 시스템 및 네트워크에 대한 보안점검(취약점 점검 등)을 실시한 시점은 2020년 7월 1일을 기준으로 언제였습니까?

☐ 1) 1개월 이내 실시
☐ 2) 6개월 이내 실시
☐ 3) 1년 이내 실시
☐ 4) 2년 이내 실시
☐ 5) 기타 (적을 것:_____년 이내 실시)
☐ 6) 실시하지 않음

☞ **문 14의 6) 응답자는 문 15로 이동**

**취약점 점검**

시스템, 네트워크, 혹은 물리적 시설의 소프트웨어나 하드웨어 상의 취약점으로 인해 해커가 공격하는데 이용할 수 있는 보안상의 문제점을 찾아내는 활동으로, 이를 위해 체크리스트나 자동화된 '취약점 점검 툴'을 사용하기도 함

문 14의 1)~5) 응답자만

**14-1** 귀사는 어떤 시스템 및 네트워크를 보유하고 있습니까? 만약, 보유하고 있다면 각 항목에 대해 취약점 점검을 실시하고 계십니까? 해당 항목을 **모두** 선택해 주십시오.

| 보유 여부 | | 취약점 점검 여부 | |
|---|---|---|---|
| | | 실시 | 미실시 |
| 시스템 및 네트워크 | ☐ 1) 서버 운영체제 (Windows, MAC OS, 리눅스 등) | ① | ② |
| | ☐ 2) 네트워크장비(라우터, 스위치 등) | ① | ② |
| | ☐ 3) Web(웹서버, 웹 방화벽 등) | ① | ② |
| | ☐ 4) DB | ① | ② |
| ☐ 5) PC | | ① | ② |
| ☐ 6) 물리보안(출입통제, CCTV 등) | | ① | ② |
| ☐ 7) 보안장비(방화벽, IPS, IDS, VPN 등) | | ① | ② |
| ☐ 8) 기타(적을 것: _____) | | ① | ② |

**물리보안(출입통제, CCTV 등)**

물리보안이란 물리적으로 정보, 시설 등을 보호하는 것을 의미함. 대표적으로 회사원들의 사원증, 전자 도어락, CCTV 등이 있음

**15** 다음 항목 중 귀사가 보안패치(Windows Update 등)를 적용하고 있는 PC나 서버를 항목별로 **모두** 선택해 주십시오.

| 구분 | | 보안패치 적용 방법(하나만 응답) |
|---|---|---|
| 1) | 직원 PC | ☐ ① 자동 업데이트 설정 (PMS(패치관리시스템)를 이용해 중앙에서 업데이트하는 것 포함) |
| | | ☐ ② 수동 업데이트 실시 |
| | | ☐ ③ 문제 발생 시에만 업데이트 실시 |
| | | ☐ ④ 업데이트하지 않음 |
| 2) | 외부와 연결된 서버 (메일 서버, 웹 서버 등) | ☐ ① 자동 업데이트 설정 |
| | | ☐ ② 수동 업데이트 실시 |
| | | ☐ ③ 문제 발생 시에만 업데이트 실시 |
| | | ☐ ④ 업데이트하지 않음 |
| | | ☐ ⑤ 해당 없음 (외부와 연결된 서버를 보유하고 있지 않음) |
| 3) | 내부에서 이용하는 서버 (파일 서버, 프린트 서버 등) | ☐ ① 자동 업데이트 설정 |
| | | ☐ ② 수동 업데이트 실시 |
| | | ☐ ③ 문제 발생 시에만 업데이트 실시 |
| | | ☐ ④ 업데이트하지 않음 |
| | | ☐ ⑤ 해당 없음(로컬 서버를 보유하고 있지 않음) |
| 4) | 정보보호 시스템 (방화벽, IPS 등) | ☐ ① 자동 업데이트 설정 |
| | | ☐ ② 수동 업데이트 실시 |
| | | ☐ ③ 문제 발생 시에만 업데이트 실시 |
| | | ☐ ④ 업데이트하지 않음 |
| | | ☐ ⑤ 해당 없음 (정보보호 시스템 없음) |

☞ **문 15의 1), 2), 3), 4) 모두 '업데이트'하거나 '해당 없음' 응답자는 문 16으로 이동**

문 15의 1)~4)에서 하나라도 "④ 업데이트 하지 않음"을 선택한 응답자

**15-1** 귀사가 보안패치를 업데이트 하지 않는 이유는 무엇입니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 업데이트가 번거로움
☐ 2) 업데이트 방법 및 절차를 모름
☐ 3) 다른 응용 프로그램과의 호환성 때문에
☐ 4) 정품을 사용하지 않음
☐ 5) 예산이 부족함
☐ 6) 지속적으로 서비스를 제공해야함
☐ 7) 기타 (적을 것 : )

**16** 귀사는 다음의 사항에 대해 백업을 실시하고 있습니까?

| 구분 | 실시 여부 | |
|---|---|---|
| | 예 | 아니오 |
| 1) 시스템 로그 | ① | ② |
| 2) 중요 데이터 | ① | ② |

☞ **문 16의 실시 여부 모두 "② 아니오" 응답자는 문 17로 이동**

문 16의 1), 2) 실시 여부에 하나라도 "① 예" 응답자만

**16-1** 귀사에서 실시하는 백업 방식은 다음 중 무엇입니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) USB메모리, 외장 하드디스크 등 별도 저장장치 활용
☐ 2) 클라우드 서버 활용
☐ 3) 운영체제(windows, MAC OS, 리눅스 등) 백업기능 활용
☐ 4) 별도 백업서버(NAS, SAN 등) 활용
☐ 5) 기타 (적어주세요 : )

문 16의 1), 2) 실시 여부에 하나라도 "① 예" 응답자만

**16-2** 귀사에서는 시스템 로그 및 중요 데이터에 대해 백업을 얼마나 자주 실시하십니까?

| 백업 실시 주기 | 시스템 로그 | 중요 데이터 |
|---|---|---|
| 1) 실시간 | ☐ ① | |
| 2) 1개월에 1회 이상 | ☐ ② | ☐ ② |
| 3) 3개월에 1회 정도 | ☐ ③ | ☐ ③ |
| 4) 6개월에 1회 정도 | ☐ ④ | ☐ ④ |
| 5) 1년에 1회 정도 | ☐ ⑤ | ☐ ⑤ |
| 6) 1년에 1회 미만 | ☐ ⑥ | ☐ ⑥ |

# Ⅲ | 침해사고 경험 및 대응

## A. 침해사고 경험

**17** 귀사는 2019년 1년 간 침해사고(해킹, 악성코드(웜·바이러스), DDoS, 랜섬웨어 등)를 경험하셨습니까?

☐ 1) 예 ☐ 2) 아니오

☞ **문 17의 2) 응답자는 문 18로 이동**

문 17의 "1) 예" 응답자만

**17-1** 귀사에서 경험한 침해사고 유형별 심각성 정도를 각각 선택해 주십시오.

**피해 심각성 정도**

- **경미한 피해 발생** : 시간, 정보, 금전적인 측면에 대해 영향이 미약한 정도(백신 등 간단한 처방으로 피해 없이 복구된 경우)
- **심각한 피해 발생** : 별도의 대책 또는 보호조치(디스크정보 백업 사본 복구, 심층 분석, 서비스거부공격 등)가 요구되고, 시간, 정보, 금전적인 측면에서 일부 비용이 발생하는 정도
- **매우 심각한 피해 발생** : 대량의 정보손실, 기밀정보 유출, 시스템 고장 등 일반적으로 생산성, 비용, 명성 측면에서 상당히 부정적인 결과를 초래하는 정도

| 유 형 | 경험여부 | 침해 정도 | | |
|---|---|---|---|---|
| | | 경미 | 심각 | 매우 심각 |
| 1) 악성코드(컴퓨터 바이러스, 웜, 트로이잔, APT공격 등)에 의한 공격 | ① 예 ☞ | ☐ | ☐ | ☐ |
| | ② 아니오 | | | |
| 2) 사내 데이터나 전산 시스템에 대한 외부로부터의 비인가 접근(해킹) | ① 예 ☞ | ☐ | ☐ | ☐ |
| | ② 아니오 | | | |
| 3) DoS(Denial of Service)/ DDoS(Distributed Denial of Service) 공격 | ① 예 ☞ | ☐ | ☐ | ☐ |
| | ② 아니오 | | | |
| 4) 애드웨어 / 스파이웨어 감염 | ① 예 ☞ | ☐ | ☐ | ☐ |
| | ② 아니오 | | | |
| 5) 내부인력에 의한 중요정보 유출(고객정보 및 기밀정보 등) | ① 예 ☞ | ☐ | ☐ | ☐ |
| | ② 아니오 | | | |
| 6) 랜섬웨어 | ① 예 ☞ | ☐ | ☐ | ☐ |
| | ② 아니오 | | | |
| 7) 기타 (적을 것 :_____) | ① 예 ☞ | ☐ | ☐ | ☐ |
| | ② 아니오 | | | |

**랜섬웨어**
컴퓨터 이용자의 중요 자료나 개인정보를 암호화하고 이를 복구하는 조건으로 돈을 요구하는 유형의 악성코드
(예: 크립토락커(cryptolocker))

**APT 공격**
정교한 수준의 전문 기술 또는 방대한 리소스를 가진 공격자가 특정 기업 또는 기관을 대상으로 여러 공격 경로 (예: 사이버, 물리적 경로 및 교란)를 사용하여 공격하는 것

문 17의 "1) 예" 응답자만

**17-2** 귀사는 침해사고 피해를 입었을 때, 관계기관(과학기술정보통신부, 한국인터넷진흥원, 경찰청 사이버안전국 등)에 문의 또는 신고하였습니까?

☐ 1) 예 ☐ 2) 아니오

## B. 침해사고 대응

**18** 귀사는 침해사고에 대응하기 위해 다음 중 어떤 활동을 수행하고 있습니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 침해사고대응팀(CERT) 구축 및 운영
☐ 2) 침해사고 대응 계획 수립
☐ 3) 침해사고 발생 또는 발생 징후 인지 시 대처를 위한 긴급연락체계 구축
☐ 4) 사고복구조직 구성
☐ 5) 침해사고 대응 활동을 외부 전문기관에 위탁
☐ 6) 침해사고에 대비한 사이버(정보보호, 개인정보보호) 보험 가입
☐ 7) 기타 (적을 것: _____)
☐ 8) 별다른 활동을 수행하지 않음

**정보보호 관련 보험 예시**

개인정보유출 배상책임보험, 공인전자문서보관소 배상책임보험, e-Biz 배상책임보험, 전자금융거래 배상 책임보험, 집적정보통신시설 사업자 배상 책임보험 등

**19** 귀사에서 침해사고 관련 정보공유 및 대응을 위해 활용하는 주된 대외협력채널은 어디입니까? **주된 2가지만** 선택해 주십시오.

☐ 1) 외부 침해사고대응팀(CERT)
☐ 2) 정보보호 업체
☐ 3) 인터넷서비스제공자(SK브로드밴드, LG U+, KT 등)
☐ 4) 시스템 개발·유지보수업체
☐ 5) 한국인터넷진흥원 등 정보보호 관련 기관 및 협회·단체
☐ 6) 사업 관련 기관 및 협회·단체
☐ 7) 유사 동종 사업체
☐ 8) 기타 (적을 것: _____)
☐ 9) 없음

# Ⅳ | 개인정보보호

## A. 개인정보 수집

**20** 귀사는 **고객의 개인정보**를 수집 및 이용하고 있습니까? 해당 항목을 **모두** 선택해 주십시오.

| 1) 수집 | 2) 이용 |
|---|---|
| ☐ ① 온라인으로 수집 | ☐ ① 온라인으로 이용 |
| | ☐ ② 오프라인으로 이용 |
| | ☐ ③ 이용하지 않음 |
| ☐ ② 오프라인으로 수집 | ☐ ① 온라인으로 이용 |
| | ☐ ② 오프라인으로 이용 |
| | ☐ ③ 이용하지 않음 |
| ☐ ③ 수집하지 않음 | ☞ **문 26으로 이동** |

☞ **문 20의 1) 수집의 ① 미응답자는 문 21로 이동**

문 20의 1)에서 "① 온라인으로 수집" 응답자만

**20-1** 귀사에서 고객의 개인정보를 온라인을 통해서 수집하실 때, 수집방법은 무엇입니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 홈페이지 회원가입
☐ 2) 이메일
☐ 3) 당사의 업무를 위해 타사업체로부터 개인정보를 제공받음
☐ 4) 위탁받은 업무의 처리를 위해 타사업체로부터 개인정보를 제공받음
☐ 5) 공개된 개인정보 수집
☐ 6) 기타 (적을 것: _____)

문 20의 1)에서 "① 온라인으로 수집" 또는 "② 오프라인으로 수집" 응답자만

**21** 귀사가 수집 및 이용하고 있는 개인정보는 어떤 것이 있습니까? 개인정보 유형별로 수집 및 이용 여부를 **모두** 선택해 주십시오.

| 개인정보 유형 | | | 수집 / 이용여부 | |
|---|---|---|---|---|
| | | | 예 | 아니오 |
| 일반정보 | 1) | 성명 | ① | ② |
| | 2) | 주민등록번호 | ① | ② |
| | 3) | (집 또는 회사) 주소 | ① | ② |
| | 4) | (집 또는 회사) 전화번호 등 연락처 | ① | ② |
| | 5) | 휴대전화 번호 | ① | ② |
| | 6) | 이메일 주소 | ① | ② |
| | 7) | 회원ID 및 비밀번호 | ① | ② |
| | 8) | 계좌번호 | ① | ② |
| | 9) | 신용카드 번호 | ① | ② |
| | 10) | 생년월일 | ① | ② |
| 특화정보 | 11) | 가족정보(가족이름, 출생지, 생년월일 등) | ① | ② |
| | 12) | 신용정보(대부잔액, 지불상황, 저당, 지불연기 및 미납의 수 등) | ① | ② |
| | 13) | 신용정보(현재 고용주, 회사주소, 상급자 이름, 직무수행평가기록, 훈련기록, 출석기록, 상벌기록 등) | ① | ② |
| | 14) | 통신정보(전자우편, 전화 통화내용, 로그파일 등) | ① | ② |
| | 15) | 소득정보(월수입, 소유주택, 자동차 등 재산 관련 정보) | ① | ② |
| | 16) | 의료정보(과거 의료기록, 가족병력, 의약이력 등) | ① | ② |
| | 17) | 위치정보(GPS나 휴대폰에 의한 개인의 위치정보) | ① | ② |
| | 18) | 기타 (적을 것 : _____) | ① | |

문 20의 1)에서 "① 온라인으로 수집" 또는 "② 오프라인으로 수집" 응답자만

**22** 귀사에서 고객의 개인정보를 수집 및 이용하는 목적은 무엇입니까? 해당 항목을 **모두** 선택해 주십시오.

| 사용 목적 | 해당여부 | |
|---|---|---|
| | 해당 | 미해당 |
| 1) 고객 본인인증 및 성인인증 | ① | ② |
| 2) 아이디/패스워드 찾기 | ① | ② |
| 3) 고객상담 회원관리 | ① | ② |
| 4) 결제 | ① | ② |
| 5) 고객의 특성 및 구매행태 분석 | ① | ② |
| 6) 홍보/마케팅/행사운영에 활용 | ① | ② |
| 7) 기타 (적을 것 : _____) | ① | |

## B. 개인정보 침해사고 예방

문 20의 1)에서 "① 온라인으로 수집" 또는 "② 오프라인으로 수집" 응답자만

**23** 귀사는 개인정보 침해사고의 예방 및 사후 처리를 위해 다음 중 어떤 조치를 취하고 계십니까? 해당 항목을 **모두** 선택해 주십시오.

| 항목a | 도입여부 | |
|---|---|---|
| | 시행 | 미시행 |
| 1) 개인정보 침해사고 예방에 관한 매뉴얼 수립 | ① | ② |
| 2) 개인정보 침해사고 사후 처리방침 수립 | ① | ② |
| 3) 개인정보 침해 발생 징후 목록의 작성 및 관리 | ① | ② |
| 4) 개인정보 침해사고로 인한 피해상황 점검 및 증거 수집 절차의 확립 | ① | ② |
| 5) 침해사고 발생 시 내부 대응체계 및 보고체계의 확립 | ① | ② |
| 6) 외부 전문가 활용을 위한 비상연락망 유지 | ① | ② |
| 7) 개인정보 피해 발생 시 개인정보분쟁조정위원회, 개인정보 침해신고센터 등 관련기관 공지 | ① | ② |
| 8) 정보보호 및 개인정보보호 관리체계(ISMS-P) 도입 및 운영 (개인정보보호 관리체계 인증(PIMS), 정보보호 관리체계 인증(ISMS)포함 ) | ① | ② |
| 9) 기타 (적을 것 : _____) | ① | |

문 20의 1)에서 "① 온라인으로 수집" 또는 "② 오프라인으로 수집" 응답자만

**24** 귀사는 수집 및 이용하는 개인정보의 안전한 처리를 위해 다음 중 어떤 기술적 조치들을 도입하고 있습니까? 해당 항목을 **모두** 선택해 주십시오.

| 항목 | 도입여부 | |
|---|---|---|
| | 도입 | 미도입 |
| 1) 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단 시스템 등 접근 통제장치의 설치·운영 | ① | ② |
| 2) 접속기록의 위조·변조·방지를 위한 조치 | ① | ② |
| 3) 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술 등을 이용한 보안조치(암호화 저장, 보안서버 이용 등) | ① | ② |
| 4) 백신 소프트웨어의 설치·운영 등 컴퓨터 바이러스에 의한 침해 방지 조치 | ① | ② |
| 5) 오프라인 데이터 저장 (CD, DVD, USB메모리, 외장하드 등 외부저장장치에 기록하여 안전한 곳에 보관) | ① | ② |
| 6) 기타 (적을 것 : _____) | ① | |

☞ **문 24의 3)에서 ① 응답자는 문 24-1로 이동**

☞ **문 24의 3)에서 ① 미응답자는 문 25로 이동**

문 24의 3)에서 "① 도입" 응답자만

**24-1** 귀사는 고객의 개인정보 중 어떤 항목을 암호화하여 저장하고 있습니까? 각 항목별로 암호화 여부를 **모두** 선택해 주십시오.

| 개인정보 | 암호화여부 | | |
|---|---|---|---|
| | 암호화함 | 암호화 안함 | 수집/이용 하지 않음 |
| 1) 비밀번호 | ① | ② | ③ |
| 2) 주민등록번호 | ① | ② | ③ |
| 3) 운전면허번호 | ① | ② | ③ |
| 4) 여권번호 | ① | ② | ③ |
| 5) 계좌정보 | ① | ② | ③ |
| 6) 신용카드번호 | ① | ② | ③ |
| 7) 바이오정보 | ① | ② | ③ |
| 8) 외국인등록번호 | ① | ② | ③ |

## C. 개인정보 침해사고

문 20의 1)에서 "① 온라인으로 수집" 또는 "② 오프라인으로 수집" 응답자만

**25** 귀사는 2019년 1년 간 개인정보 유출 사고를 경험하셨습니까?

☐ 1) 예 ☐ 2) 아니오

☞ **문 25의 2) 응답자는 문 26으로 이동**

문 25의 "1) 예" 응답자만

**25-1** 개인정보 유출 사고 발생 시 관계기관에 문의 또는 신고하였습니까?

**관계 기관**
방송통신위원회, 한국인터넷진흥원, 행정안전부 등

☐ 1) 예 ☐ 2) 아니오

문 25의 "1) 예" 응답자만

**25-2** 개인정보 유출 사고 발생 시 이용자에게 해당 유출 사고에 대해 **지체 없이** 통지 또는 고지를 하였습니까?

☐ 1) 예 ☐ 2) 아니오

# V | 주요 서비스별 정보보호

## A. 무선랜

**26** 귀사에서는 사내 무선랜(Wi-Fi)을 구축하여 운영하고 있습니까?

☐ 1) 예 ☐ 2) 아니오

☞ **문 26의 2) 응답자는 문 27로 이동**

문 26의 "1) 예" 응답자만

**26-1** 귀사에서 사내 무선랜 이용과 관련하여 우려하는 사항은 무엇입니까? 보안상 우려하는 정도가 높은 항목을 **2가지만** 선택해 주십시오.

☐ 1) 사내 시스템 및 데이터에 대한 비인가 접근
☐ 2) 사내 무선랜을 통한 전송 데이터 유출
☐ 3) 무선공유기(AP)를 DDoS 등 공격도구로 악용
☐ 4) 무선공유기(AP)를 통한 악성코드 감염
☐ 5) 기타(적을 것: _____)
☐ 6) 해당사항 없음

문 26의 "1) 예" 응답자만

**26-2** 귀사의 무선랜 보안을 위해 어떤 조치를 취하고 있습니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 사내 유·무선 네트워크 분리
☐ 2) 전송 데이터 보안/암호화
☐ 3) 무선랜 접근 제어/필터링
☐ 4) 무선랜 접속 암호 설정
☐ 5) 무선랜 통한 SNS 접속 차단
☐ 6) 외부상용 무선랜 이용 제한
☐ 7) 기타(적을 것: _____)
☐ 8) 별도의 무선랜 보안 대책 없음

## B. 모바일

**27** 귀사에서는 다음의 모바일 기기(스마트폰, 스마트패드 등, 노트북 포함)를 업무에 활용하고 있습니까?

| 구분 | 활용 여부 | |
|---|---|---|
| | 예 | 아니오 |
| 1) 개인소유 모바일 기기 | ☐ ① | ☐ ② |
| 2) 회사소유 모바일 기기 | ☐ ① | ☐ ② |

☞ **문 27에서 모두 '② 아니오' 응답자는 문 28로 이동**

문 27의 '1) 개인소유 모바일 기기'를 업무에 활용하고 있는(①) 응답자

**27-1** 귀사의 업무와 관련하여 개인소유 모바일 기기 활용 시 보안상 우려하는 사항은 무엇입니까? 우려하는 정도가 높은 항목을 **2가지만** 선택해 주십시오.

☐ 1) 분실 또는 도난으로 인한 보안 위협증가
☐ 2) 악성코드 감염으로 인한 보안 위협증가
☐ 3) 사업체의 데이터와 시스템에 자유로운 접근에 따른 보안 위협증가
☐ 4) 직원의 정보보호 관련 지침 및 규정 위반에 따른 문제 발생
☐ 5) 사내 소프트웨어 설치 등에 따른 사생활 침해
☐ 6) 기타(적을 것: _____)

문 27의 1) 개인소유, 2) 회사소유 모바일 기기 중 하나라도 업무에 활용하고 있는(①) 응답자

**27-2** 귀사는 업무와 관련하여 모바일 기기 활용 시 발생할 수 있는 보안위협에 대해 어떤 대응 방안을 마련하고 있습니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 모바일 기기활용 관련 보안정책 수립
☐ 2) 모바일 보안을 위한 관리 인력 배치
☐ 3) 모바일 기기 데이터의 백업 의무화
☐ 4) 모바일 기기 보안 소프트웨어(백신 등) 설치 의무화
☐ 5) 모바일 기기에 대한 반출입 관리
☐ 6) 모바일 기기 접속기록 보관 등 관리시스템 구축
☐ 7) 기타(적을 것: _____)
☐ 8) 해당사항 없음

## C. 클라우드


**클라우드 서비스(Cloud Service)**

클라우드 서비스란 가상화된 저장공간, 서버 등의 각종 IT자원을 인터넷을 통해 필요한 만큼 빌려 사용하고, 이용한 만큼 비용을 지불하는 형태의 서비스를 의미

예) 구글 클라우드, 아마존 웹 서비스(AWS), 웹하드, MS에저(Azure)와 같은 퍼블릭 클라우드 또는 사내용 프라이빗 클라우드 등

**28** 귀사에서는 클라우드 서비스를 현재 이용하고 있습니까?

☐ 1) 예 ☐ 2) 아니오

☞ **문 28의 2) 응답자는 문 29로 이동**

문 28의 "1) 예" 응답자만

**28-1** 현재 클라우드 서비스를 이용하고 있으시다면, 어떤 분야입니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 컴퓨팅(서버, 스토리지 등) 자원
☐ 2) VDI(가상 데스크탑) 서비스
☐ 3) 백업·복구 서비스
☐ 4) 협업도구(그룹웨어, 오피스 등) 서비스
☐ 5) 전사적 어플리케이션 서비스(ERP, CRM, SCM, KM 등)
☐ 6) 정보보안 서비스
☐ 7) 기타(적을 것: _____)

문 28의 "1) 예" 응답자만

**28-2** 귀사는 클라우드 서비스 보안을 위해 어떤 조치를 취하고 있습니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 클라우드 서비스 이용 관련 보안정책 수립
☐ 2) 클라우드 보안인증(CSAP 등)을 획득한 서비스 이용
☐ 3) 클라우드 서비스 제공 업체의 보안 서비스 이용 여부 확인
☐ 4) 민감한 데이터 분리 및 암호화 적용
☐ 5) 클라우드 서비스 사용단말의 보안 소프트웨어 (백신 등) 설치 의무화
☐ 6) 기타(적을 것: _____)
☐ 7) 별도의 클라우드 서비스 보안대책 없음

**29** 다음은 클라우드 서비스 이용과 관련하여 발생할 수 있는 보안 문제입니다. 우려하는 정도가 높은 항목을 **2가지만** 선택해 주십시오.

☐ 1) 데이터 위탁저장에 따른 정보유출
☐ 2) 사용단말의 다양화로 인한 정보유출
☐ 3) 자원 공유·집중화로 서비스 장애시 대규모 피해 발생
☐ 4) 분산처리에 따른 데이터 암호화, 접근제어 등의 보안적용 어려움
☐ 5) 기타(적을 것: _____)

## D. 사물인터넷(IoT)


**사물인터넷(Internet of Things, IoT)**

다양한 사물을 인터넷으로 연결해 사람과 사물, 사물과 사물 간의 정보를 상호 소통하는 기술 및 서비스를 말함

사물인터넷은 난방과 조명을 자동으로 조절하는 스마트 홈기기부터 산업 장비를 관찰하여 문제를 찾은 후 고장 예방을 위해 자동으로 해결하는 스마트 팩토리에 이르기까지 다양한 분야에 응용되고 있음

예) 실내온도, 전등 등을 조절하는 스마트빌딩, GPS를 활용한 공사 트랙터 기계, IP카메라 등

**30** 귀사는 사물인터넷(IoT) 제품 및 서비스를 현재 이용하고 있습니까?

☐ 1) 예 ☐ 2) 아니오

☞ **문 30의 2) 응답자는 문 31로 이동**

문 30의 1) 응답자만

**30-1** 귀사가 사물인터넷(IoT) 제품 및 서비스를 현재 이용하고 있으시다면, 어떤 분야입니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) **제조** : 제조시설 공정 고도화로 최적 생산스케줄 관리
☐ 2) **농축산** : 가축 및 식물의 생장환경 정보를 수집, 최적의 농가운영
☐ 3) **교통(스마트카/ITS)** : 센서 통한 차량 및 도로정보 수집, 차량 운행기록 관리
☐ 4) **의료** : 사용자의 바이오정보를 활용한 신체 상태 모니터링
☐ 5) **에너지** : 전력, 가스 등 에너지 사용량 정보제공
☐ 6) **건설** : 스마트 빌딩(난방, 가스, 온습도, 콘센트 등)
☐ 7) **금융 서비스** : 카드 결제기능 지원 (이동식 결제 단말기 등)
☐ 8) **CCTV** : 무인 방범관리를 위한 IP카메라 등
☐ 9) 기타 (적을 것 : _____)

| | |
|---|---|
| **제조** | 주요 생산 부품 이력관리 서비스, 센서정보를 이용한 설비 점검, IoT기반 실시간 위치인식 솔루션 등 |
| **농축산** | 센서로 가축정보 수집, 식물재배환경 모니터링 등 |
| **교통** | 스마트카(또는 커넥티드 자동차) 에 탄 운전자가 사고를 피하고 유지보수 문제를 예측하고 주차장을 찾도록 도움 |
| **의료** | 신체착용형 웨어러블(패치, 손목밴드) 활용 등 |
| **에너지** | 스마트 계량기, 가스 무선 원격검침 서비스 등 |

문 30의 1) 응답자만

**30-2** 귀사는 사물인터넷(IoT) 제품 및 서비스의 보안을 위해 어떤 조치를 취하고 있습니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 보안성 점검(자체 혹은 제3자 검증)
☐ 2) 보안위협 모니터링
☐ 3) 주기적 패치관리
☐ 4) 보안사고 대응체계 마련
☐ 5) 정기 보안교육(직원, 외주인력 등)
☐ 6) 기타 (적을 것 : _____)
☐ 7) 별도의 사물인터넷 제품 및 서비스 보안대책 없음

**31** 다음은 사물인터넷(IoT) 환경에서 발생 할 수 있는 보안 위협입니다. 우려하는 정도가 높은 항목을 **2가지만** 선택해 주십시오.

☐ 1) 기기 분실·도난
☐ 2) 해킹 및 악성코드 감염
☐ 3) 무선신호교란 및 장애
☐ 4) 정보 유출
☐ 5) 기타(적을 것: _____)

## E. 사이버 보험

**사이버(정보보호, 개인정보보호) 보험**

사이버(정보보호, 개인정보보호) 보험이란 기업이 사이버 공간에서 일어난 해킹, DDoS 등의 의도적인 공격으로 인해 겪게 되는 피해를 보장하는 보험. 사이버보험(cybersecurity insurance 또는 cyber insurance)이라고도 함. 현재 국내에서는 개인정보보호에 대한 보장을 다루는 상품이 주를 이루고 있음

예) 개인정보유출 배상책임보험, 공인전자문서보관소 배상책임보험, e-Biz 배상책임보험, 전자금융거래 배상 책임보험, 집적정보통신시설 사업자 배상 책임보험 등

**32** 귀사는 사이버(정보보호, 개인정보보호) 보험에 대해 어느 정도 알고 계십니까?

☐ 1) 전혀 모른다
☐ 2) 잘 모르나, 들어본 적 있다
☐ 3) 잘 알고 있다

**33** 귀사는 사이버(정보보호, 개인정보보호) 보험에 가입 또는 이용하고 계십니까? 해당 항목을 선택해 주십시오.

| 1) | 2) | 3) |
|---|---|---|
| 가입 여부 | 이용 여부 | 향후 가입(유지) 계획 |
| ☐ ① 가입 경험 있음 | ☐ ① 현재 이용 중임<br>☐ ② 현재 이용하지 않음 | ☐ ① 예<br>☐ ② 아니오 |
| ☐ ② 가입 경험 없음 | | |

☞ **문 33의 3) 향후 가입(유지) 계획에 ② 응답자는 문 34로 이동**

문 33의 3) 향후 가입(유지)계획에 "① 예" 응답자만

**33-1** 귀사가 향후 사이버(정보보호, 개인정보보호) 보험 가입 시 보장받고자 하는 항목을 **모두** 선택해 주십시오.

☐ 1) 개인정보 유출 사고 발생 시 대응 비용 (조사, 통지, 법률자문)
☐ 2) 개인정보 유출 사고 발생 시 배상 비용
☐ 3) 기업 기밀 유출 조사 및 소송 비용
☐ 4) 기업 기밀 유출 배상 비용
☐ 5) 좀비PC 해킹 등 공격 경유지로 활용 시 경유 배상 책임 비용
☐ 6) 사이버 갈취 손해(랜섬웨어 등) 비용
☐ 7) 기타(적을 것: _____)

## F. 향후 지출 계획

**문 34는 2020년 7월 1일 기준으로 작성해주십시오.**

**34** 다음 중 귀사에서 정보보호를 위해 지출하고 있거나 향후 지출할 계획이 있는 IT보안 분야를 **모두** 선택해 주십시오.

| 개인정보 | 해당여부 | |
|---|---|---|
| | 현재 지출 중 | 향후 지출 계획 있음 |
| 1) 무선랜 보안 | ☐ ① | ☐ ① |
| 2) 모바일 보안 | ☐ ② | ☐ ② |
| 3) 클라우드 보안 | ☐ ③ | ☐ ③ |
| 4) 클라우드 활용 보안서비스 (SECaaS 등) | ☐ ④ | ☐ ④ |
| 5) 사물인터넷(IoT) 보안 | ☐ ⑤ | ☐ ⑤ |
| 6) 데이터 암호화 | ☐ ⑥ | ☐ ⑥ |
| 7) 사이버 보험 | ☐ ⑦ | ☐ ⑦ |
| 8) 기타( ) | ☐ ⑧ | ☐ ⑧ |
| 9) 없음 | ☐ ⑨ | ☐ ⑨ |

**클라우드 활용 보안서비스 (SECaas 등)**
클라우드 활용 보안 서비스란 클라우드 기술을 활용하여 고객이 원하는 보안 서비스를 제공하는 것을 일컫는 말로, 네트워크 보안, 취약점 점검, 암호화 등 다양한 보안서비스 형태로 구성되어 있음

**데이터 암호화**
데이터를 분석·보관하는 작업에서 개인정보 및 기타 중요한 정보들이 외부로 유출되지 않도록 비식별화, 암호화 등의 설정을 하는 것

귀하는 2020년 정보보호 실태조사 결과가 공표될 경우, 이를 이용할 의향이 있으신가요?

☐ 1) 있음 ☐ 2) 없음

귀하는 한국정보보호산업협회의 정보보호 관련 소식을 이메일로 받을 의향이 있으신가요?

☐ 1) 있음 ☐ 2) 없음

조사된 결과는 2020년 12월 한국정보보호산업협회 공식홈페이지(https://www.kisia.or.kr)에서 확인하실 수 있습니다.

끝까지 응답해 주셔서 감사합니다.

# * | 조사 기록표

## 조사방법

| | |
|---|---|
| 1 | 방문면접조사 |
| 2 | 현장방문 시 조사가 불가능하여 질문지 배포 후 방문하여 조사완료 |
| 3 | 현장방문시 조사가 불가능하여 질문지 배포 후 이메일이나 팩스로 조사완료 |
| 4 | 이메일이나 팩스로 질문지 발송 후 방문하여 조사 완료 |
| 5 | 이메일이나 팩스로 질문지 발송 후 이메일이나 팩스로 조사완료 |
| 6 | 전화조사 |
| 7 | 기타(적을 것 : ) |

## 질문지 작성자 현황

| | |
|---|---|
| 1 | 정보보호 관련 종사자 |
| 2 | 정보 관련 종사자 |
| 3 | 사업체의 대표 |
| 4 | 사업체 총무부서 담당자 |
| 5 | 기타(적을 것 : ) |

## 조사일시

월 일 시

분부터 분간

## 조사대상 사업체 정보변경 현황

| 구 분 | 리스트 정보 | 변경사항 |
|---|---|---|
| 사업체명 | | |
| 업 종 | | |
| 규 모 | | |
| 지 역 | | |

## 면접원 기록사항

| | |
|---|---|
| 1 회사명 | |
| 2 주소 | |
| 3 응답자성명 | |
| 4 소속 | |
| 5 직위 | |
| 6 전화번호 | |
| 7 이메일 | |
| 8 조사원 성명 | |

# 2020년 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 **"2020년 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.

2020년 8월

| 주관기관 | 전담기관 | 조사기관 | 실사 문의 \| 송미영 차장 | 조사 문의 \| 박혜란 대리 |
|---|---|---|---|---|
| 과학기술정보통신부 | 한국정보보호산업협회 | ㈜글로벌리서치 | 02-3456-1902<br>mysong@globalri.co.kr | 02-3456-1742 |

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

| 관리 사항 | 조사구 번호 | 가구번호 | 주거 유형 | 면접원 정보 | |
|---|---|---|---|---|---|
| | | | | 이름 | 연락처 |
| | | | □① 비아파트<br>□② 아파트 | | |

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

| 월평균 가구소득 | | 학 력 | | |
|---|---|---|---|---|
| 가구 구성원 전체의 월평균 소득 합계를 표시해 주십시오 | | 학 교 | | 이수여부 |
| □① 100만원 미만<br>□② 100~200만원 미만<br>□③ 200~300만원 미만<br>□④ 300~400만원 미만 | □⑤ 400~500만원 미만<br>□⑥ 500~600만원 미만<br>□⑦ 600~700만원 미만<br>□⑧ 700만원 이상 | □⓪ 무학<br>□① 초등학교<br>□② 중학교<br>□③ 고등학교 | □④ 전문대<br>□⑤ 대학교<br>□⑥ 대학원 | □① 재학<br>□② 휴학<br>□③ 중퇴<br>□④ 수료<br>□⑤ 졸업 |

## 응답해 주실 때 꼭 지켜 주십시오

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 「2019년 7월 1일~2020년 6월 30일」**을 기준으로 응답해 주시기 바랍니다.
   (단, 침해사고 경험 관련 문항은 **「2019.1.1~2019.12.31」**을 기준으로 응답해 주시기 바랍니다)
4. 설문 응답 및 작성은 질문의 순서대로 보기항목에서 해당 번호를 선택하거나 직접 의견을 말씀해 주시면 됩니다.
5. 설문의 이해를 돕기 위한 사업체 또는 제품명의 예시는 가나다순으로 작성하였습니다.

## * | 먼저, 자료 분류를 위한 질문입니다.

**SQ1** 귀하께서는 최근 1개월(2020년 6월 1일~30일) 이내 인터넷을 이용한 적이 있습니까?

**인터넷 이용이란?**

장소(가정, 학교, 직장 등)나 용도(개인용, 업무용, 학업용 등)에 관계없이 컴퓨터, 이동전화(스마트폰 포함), 스마트패드, 스마트 TV 등을 통해 인터넷(무선인터넷 포함)에 접속하는 것을 말합니다.

☐ 1) 예 ☐ 2) 아니오 ☞ **조사중단**

**SQ2** 귀하께서 인터넷에 접속하기 위해 사용한 전자기기는 무엇입니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) PC(노트북 포함)
☐ 2) 모바일기기(스마트폰, 스마트패드 등 포함)
☐ 3) 스마트 TV(인터넷 가능)
☐ 4) 인공지능 스피커
☐ 5) 기타(적어주세요 : )

☞ **SQ2의 2) 미응답자는 문 1로 이동**

SQ2의 "2) 모바일기기" 응답자만

**SQ 2-1** 귀하께서 사용하고 있는 모바일기기의 **운영체제**는 무엇입니까?

☐ 1) 안드로이드
☐ 2) iOS
☐ 3) 기타(적어주세요 : )

**운영체제란?**

기기를 작동시키고 운영을 관리하여 응용프로그램이 효율적으로 실행될 수 있는 환경을 제공하는 기본 소프트웨어를 말함
모바일 운영체제로는 구글의 안드로이드, 애플의 iOS, RIM의 블랙베리 OS 등이 있음

**안드로이드 : 안드로이드폰의 운영체제**
(예. 삼성전자, LG전자가 제조한 모바일기기)

**iOS : 아이폰의 운영체제**

## I | 정보보호 인식

**01** 귀하께서는 인터넷 이용 시 **정보보호 및 개인정보보호**에 대해 **얼마나 중요**하게 생각하십니까?

| 항 목 | 전혀 중요하지 않다 | 중요하지 않은 편이다 | 보통이다 | 중요한 편이다 | 매우 중요하다 |
|---|---|---|---|---|---|
| 1) 정보보호 | ① | ② | ③ | ④ | ⑤ |
| 2) 개인정보보호 | ① | ② | ③ | ④ | ⑤ |

**정보보호란?**

해킹, 악성코드 등의 내·외부 위협으로부터 자신이 가진 정보를 보호하기 위한 활동(관리적·기술적 수단, 또는 그러한 수단으로 이루어지는 행위)을 말합니다.

**개인정보보호란?**

인터넷 상에서 본인 및 가족의 신상정보, 사진, 동영상 등 사적인 정보가 유출되는 위협으로부터 보호하는 것을 말합니다.

**02** 다음은 웹사이트, SNS, 스마트폰 앱 등 인터넷 상에서 일어날 수 있는 일들입니다. 귀하께서는 다음의 각 항목들의 **구체적인 피해에 대해 어느 정도 알고** 계십니까? 또한, 귀하께서는 다음의 각 항목에 대한 위협이 발생한다면 그로 인한 피해가 얼마나 **심각**하다고 생각하십니까? 5점 척도 기준으로 선택해 주십시오.

| 응답기준 : 5점 척도 | | | | |
|---|---|---|---|---|
| 매우 낮다 | 낮다 | 보통이다 | 높다 | 매우 높다 |
| ① | ② | ③ | ④ | ⑤ |

| 항 목 | 인지정도 (5점척도) | 심각정도 (5점척도) |
|---|---|---|
| 1) **악성코드 피해** (바이러스, 웜, 랜섬웨어, 스파이웨어 등 감염 등으로 인한 피해 (정보 손실, 물리적·시간적 손해)) | ( ) | ( ) |
| 2) **개인정보 유출 및 사생활 침해** (주민등록번호, 개인신상정보, 사진, 동영상 등) | ( ) | ( ) |
| 3) **금전적 피해** 피싱/파밍/스미싱 등으로 인한 금전적 피해 (보이스피싱, 사기성 메시지 및 가짜 웹사이트 접속 유도를 통한 결제 유도 등) | ( ) | ( ) |

**랜섬웨어란?**

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

예) '17년 5월 12일 스페인, 영국, 러시아 등을 시작으로 전 세계에서 피해가 보고된 악성코드로, 다수의 파일을 암호화한 워너크라이가 대표적 사례입니다.

**03** 귀하께서는 정보보호와 관련된 정보를 **알아보거나 배운다면** 어떤 방법으로 하시겠습니까?
해당 항목을 **2가지만** 선택해 주십시오.

☐ 1) 정보보호 관련 정부부처 및 공공기관에 문의
(과학기술정보통신부, 한국인터넷진흥원, 경찰청사이버안전국 등)
☐ 2) 정보보호 관련 민간업체에 문의(백신업체, 보안업체 등)
☐ 3) 정보보호 관련 정보 검색(TV, 신문, 인터넷 등)
☐ 4) 주변으로부터 관련 정보 확보(주변사람, 지인, 동료 등)
☐ 5) 정보보호 관련 교재 구입(서적, 학습용SW, 콘텐츠 등)
☐ 6) 정보보호 관련 강좌 수강
(인터넷 강의, 세미나, 학회, 콘퍼런스 등)
☐ 7) 기타(적어주세요 : )

# Ⅱ | 침해사고 예방

## A. 정보보호 관련 제품

**04** 귀하께서는 사용하고 있는 PC 및 모바일 등의 보안을 위하여 **정보보호 관련 제품(소프트웨어 등)**을 이용하고 계십니까?

**정보보호 관련 제품(소프트웨어 포함)이란?**

은행 OTP기기나 보안(암호화) USB와 같은 정보보호를 위한 제품뿐만 아니라, 안랩 V3나 알약과 같은 백신 프로그램까지 포함하는 개념입니다.

예) 네이버 백신, 안랩 V3, 알약, 은행 OTP, nProtect 등


| 항목 | 기기 미사용 | 정보보호 제품 이용여부 | |
|---|---|---|---|
| | | 예 | 아니오 |
| 1) PC | ☐ | ① | ② |
| 2) 모바일 기기 | ☐ | ① | ② |

☞ **문 4에서 1) PC와 2) 모바일 기기 모두 '기기 미사용' 응답자는 문 5로 이동**

**문 4의 1) PC와 2) 모바일 기기 중 하나라도 정보보호 제품을 이용하는 응답자**

**4-1** 귀하께서는 아래 소프트웨어 중 어떠한 정보보호 소프트웨어를 사용하십니까?
해당 항목을 **모두** 선택해 주십시오.

| 항 목 | PC | 모바일 |
|---|---|---|
| 1) **인터넷서비스제공자(ISP) 제공 보안 소프트웨어** (SK브로드밴드 세이퍼/원스톱(유료), KT PC안심2.0(유료), KT 인터넷놀e터(유료), LG유플러스 PASS 금융사기방지(유/무료), 스마트피싱보호(유료)) | ① ☐ | ① ☐ |
| 2) **그 외 무료·기본 소프트웨어** (PC: 알약, V3 Lite, MS(마이크로소프트) 디펜더 / 모바일 : V3 모바일, 알약M, MCAFee(맥아피) 모바일시큐리티) | ② ☐ | ② ☐ |
| 3) **그 외 유료 소프트웨어** (노턴 360(베이직, 플러스, 프리미엄), V3 365 클리닉 등) | ③ ☐ | ③ ☐ |
| 4) **사용하고 있는 정보보호 소프트웨어 없음** | ④ ☐ | ④ ☐ |

**인터넷 서비스 제공자(ISP)란?**

가정이나 사무실에서 사용하는 인터넷 서비스를 제공하는 회사를 말하며, 대표적인 인터넷 서비스 제공자로 SK브로드밴드, KT, LG유플러스가 있음

SK 브로드밴드 LG U+ kt

**문 4의 1) PC와 2) 모바일 기기 중 하나라도 정보보호 제품을 이용하는 응답자**

**4-2** 귀하께서는 사용 중인 PC 및 모바일에 대해 **악성코드 검사**(바이러스, 웜, 랜섬웨어, 스파이웨어 검사 등)를 **얼마나 자주** 실시하십니까?

**악성코드 검사를 수동 실행 및 자동 실행(예약 검사 등) 빈도를 모두 고려하여 응답**

| 검사 실시 주기 | PC | 모바일 |
|---|---|---|
| 1) 매일 | ① ☐ | ① ☐ |
| 2) 1주일에 1회 이상 | ② ☐ | ② ☐ |
| 3) 1개월에 1회 정도 | ③ ☐ | ③ ☐ |
| 4) 1개월에 1회 미만 | ④ ☐ | ④ ☐ |
| 5) 모름 | ⑤ ☐ | ⑤ ☐ |

문 4의 1) PC와 2) 모바일 기기 중 하나라도 정보보호 제품을 이용하는 응답자

## 4-3 귀하께서는 **백신 프로그램 업데이트**를 실시하십니까?

**백신 프로그램이란?**

컴퓨터 상의 바이러스나 스파이웨어 등의 악성코드 프로그램을 찾아내어 손상된 파일이나 정보를 치료하고 정보를 보호하는 소프트웨어

| 항목 | 업데이트 실시여부 | |
|---|---|---|
| | 예 | 아니오 |
| 1) PC | ① | ② |
| 2) 모바일 기기 | ① | ② |

문 4-3의 1), 2) 중 하나라도 "①예" 응답자만

## 4-4 귀하께서는 백신 프로그램을 **얼마나 자주 업데이트** 하십니까?

**백신프로그램을 수동 실행 및 자동 실행(예약 검사 등)하는 빈도를 모두 고려하여 응답**

| 업데이트 실시 주기 | PC | 모바일 |
|---|---|---|
| 1) 실시간 | ① ☐ | ① ☐ |
| 2) 1주일에 1회 이상 | ② ☐ | ② ☐ |
| 3) 1개월에 1회 정도 | ③ ☐ | ③ ☐ |
| 4) 1개월에 1회 미만 | ④ ☐ | ④ ☐ |

## 05 귀하께서는 **운영체제 보안 업데이트를 실시**하십니까?

**운영체제 보안 업데이트란?**

운영체제(MAC OS, Windows, 리눅스 등) 내 보안 취약점을 보완하기 위해 정보보안 관련 업데이트를 수행하는 것을 말함

| 항목 | 기기 미사용 | 업데이트 실시여부 | |
|---|---|---|---|
| | | 예 | 아니오 |
| 1) PC | ☐ | ① | ② |
| 2) 모바일 기기 | ☐ | ① | ② |

## 06 귀하께서는 PC 및 모바일 기기에 저장된 **중요 데이터**를 **백업**하십니까?

**백업이란?**

PC 또는 모바일기기 내의 자료가 오류, 바이러스, 정전 등으로 인해 손상·분실될 경우를 대비해서 원본 파일의 복사본을 미리 만들어 놓는 행위를 말함

| 항목 | 기기 미사용 | 백업 실천여부 | |
|---|---|---|---|
| | | 예 | 아니오 |
| 1) PC | ☐ | ① | ② |
| 2) 모바일 기기 | ☐ | ① | ② |

☞ **문 6에서 1), 2) 모두 ② 응답자는 문 7로 이동**

문 6의 1) PC와 2) 모바일기기 중 하나라도 "①예" 응답자만

## 6-1 중요 데이터 백업방식은 다음 중 무엇입니까? 해당 항목을 **모두** 선택해 주십시오.

| 항 목 | | PC | 모바일 |
|---|---|---|---|
| 1) | USB메모리, 외장하드디스크, 마이크로SD카드 등 별도 저장장치 활용 | ① ☐ | ① ☐ |
| 2) | 클라우드 서버 활용(구글 드라이브, 네이버 N드라이브, 애플 i Cloud 등) | ② ☐ | ② ☐ |
| 3) | 운영체제(PC: windows 등)의 백업기능 활용 | ③ ☐ | |
| 4) | 기타(적어주세요 : ) | ④ ☐ | ③ ☐ |

문 6의 1) PC와 2) 모바일기기 중 하나라도 "①예" 응답자만

## 6-2 귀하께서는 **중요 데이터**에 대한 **백업**을 **얼마나 자주** 실시하십니까?

| 중요 데이터 백업 실시 주기 | PC | 모바일 |
|---|---|---|
| 1) 실시간 | ① ☐ | ① ☐ |
| 2) 1개월에 1회 이상 | ② ☐ | ② ☐ |
| 3) 3개월에 1회 정도 | ③ ☐ | ③ ☐ |
| 4) 6개월에 1회 정도 | ④ ☐ | ④ ☐ |
| 5) 1년에 1회 정도 | ⑤ ☐ | ⑤ ☐ |
| 6) 1년에 1회 미만 | ⑥ ☐ | ⑥ ☐ |

**07** 귀하께서는 사용하시는 PC나 네트워크의 **보안을 위해 어떤 노력**을 하십니까?
해당 항목을 **모두** 선택해 주십시오.

☐ 1) 웹사이트에서 파일을 함부로 다운로드하지 않음
☐ 2) 프로그램 설치 시 불필요한 프로그램이 추가적으로 설치되는지 확인함
☐ 3) 파일 및 폴더의 공유설정을 하지 않음
☐ 4) 응용 소프트웨어(어도비 플래시, 한컴오피스 등) 보안 업데이트를 실시함
☐ 5) 의심스러운 URL 링크 클릭하지 않음
☐ 6) P2P, 웹하드 등 방문하지 않음
☐ 7) PC 또는 네트워크의 비밀번호를 설정함
☐ 8) 기타 (적어주세요 : )

SQ2(인터넷 접속 시 사용 전자기기)에서 "1) PC"를 이용한다고 응답한 응답자만

**08** 귀하께서는 PC 사용 시 다음의 각 경우에 **비밀번호(패스워드)를 설정**하십니까?
해당 항목을 **각각** 선택해 주십시오.

| 항목 | 설정여부 | |
|---|---|---|
| | 설정 | 미설정 |
| 1) 운영체제(윈도우 등) 로그인 시 | ① ☐ | ② ☐ |
| 2) 화면보호기능 해제 시 | ① ☐ | ② ☐ |
| 3) 공유 파일 및 폴더 설정 시 | ① ☐ | ② ☐ |
| 4) 중요 데이터 파일 저장 시 | ① ☐ | ② ☐ |
| 5) 백업 데이터 접근 시 | ① ☐ | ② ☐ |
| 6) 기타(적어주세요 : ) | ① ☐ | ② ☐ |

**09** 귀하께서는 PC, 모바일기기 또는 인터넷 서비스 이용 시 안전한 비밀번호 관리를 위해 **어떤 조치**를 취하십니까?
해당 항목을 **모두** 선택해 주십시오.

☐ 1) 비밀번호를 주기적으로 변경함
☐ 2) 비밀번호를 남들이 알아내기 어려운 문자열로 설정함 (8문자 이상, 문자/숫자/기호 혼합 등)
☐ 3) 여러 개(기능별, 웹사이트별)의 비밀번호를 사용함
☐ 4) 본인이 허락할 때만 로그인되도록 2단계 인증을 설정함
☐ 5) 기타 (적어주세요 : )
☐ 6) 별도의 조치를 하지 않음

☞ **문 9의 1)을 선택하지 않은 응답자는 문 10으로 이동**

**2단계 인증이란?**

PC, 모바일기기 또는 인터넷 서비스 이용 시 1차 로그인 후 비밀번호 입력, 휴대폰 인증, OTP인증, 바이오인증 등 2차 인증을 통해 서비스 이용이 가능한 것을 말함

문 9의 "1)" 응답자만

**9-1** 귀하께서는 인터넷 서비스 이용 시 **주로** 이용하는 **사이트**의 **비밀번호를 얼마나 자주 변경**하십니까?

| 비밀번호 변경 주기 | PC | 모바일 |
|---|---|---|
| 1) 3개월에 1회 정도 | ① ☐ | ① ☐ |
| 2) 6개월에 1회 정도 | ② ☐ | ② ☐ |
| 3) 1년에 1회 정도 | ③ ☐ | ③ ☐ |
| 4) 1년에 1회 미만 | ④ ☐ | ④ ☐ |

## B . 모바일 및 무선랜 보안

SQ2(인터넷 접속 시 사용 전자기기)에서 "2) 모바일 기기"를 이용한다고 응답한 응답자만

**10** 귀하께서는 모바일기기(스마트폰/스마트패드 등)를 통해 **무선랜(와이파이(Wi-Fi))**을 이용하면서 입을 수 있는 피해를 **예방·방지**하기 위해 다음과 같은 사항을 실천하십니까? 해당 항목을 **각각** 선택해 주십시오.

| 항 목 | 실천여부 | |
|---|---|---|
| | 예 | 아니오 |
| 1) 제공자가 불명확한 무선랜(와이파이) 이용하지 않음 | ① ☐ | ② ☐ |
| 2) 패스워드가 없는 무선랜(와이파이)으로 민감한 서비스 이용하지 않음 (인터넷 뱅킹, 결제서비스 등) | ① ☐ | ② ☐ |
| 3) 자동으로 무선랜(와이파이)에 접속하는 기능 설정하지 않음 | ① ☐ | ② ☐ |
| 4) 자신의 스마트폰을 통한 테더링/개인용 핫스팟 사용 시 패스워드 설정함 | ① ☐ | ② ☐ |
| 5) 무선랜(와이파이)을 이용하지 않음 | ☐ | |

**테더링/개인용 핫스팟이란?**

인터넷 사용이 가능한 기기를 이용해 다른 기기에 인터넷을 연결하여 인터넷 사용이 가능하게 하는 방법

SQ2(인터넷 접속 시 사용 전자기기)에서
"2) 모바일 기기"를 이용한다고 응답한 응답자만

**11** 귀하께서는 모바일기기(스마트폰/스마트패드 등)를 사용하면서 입을 수 있는 피해를 **예방·방지**하기 위해 다음과 같은 사항을 **실천**하십니까? 해당 항목을 **각각** 선택해 주십시오.

| 항 목 | | 실천여부 | |
|---|---|---|---|
| | | 예 | 아니오 |
| 1) | 운영체제(iOS, 안드로이드) 최신버전으로 업데이트 함 | ① ☐ | ② ☐ |
| 2) | '알 수 없는 출처(미인증) 앱 설치'기능 사용하지 않음 | ① ☐ | ② ☐ |
| 3) | 신뢰할 수 없는 웹사이트 방문하지 않음 | ① ☐ | ② ☐ |
| 4) | 스마트폰 권한 임의변경(루팅, 탈옥 등)하지 않음 | ① ☐ | ② ☐ |
| 5) | 모바일 백신 설치 및 점검함 | ① ☐ | ② ☐ |
| 6) | 공식 앱마켓(구글 플레이, 앱스토어, 원스토어 등)만 이용함 | ① ☐ | ② ☐ |
| 7) | 휴대폰 관리자 권한 활성화 하지 않음 | ① ☐ | ② ☐ |
| 8) | 앱 설치 시 요구권한 적절 여부 확인함 | ① ☐ | ② ☐ |
| 9) | 스미싱 차단앱 설치함 | ① ☐ | ② ☐ |
| 10) | 블루투스, 무선랜(와이파이) 등 무선인터페이스는 사용 시에만 켜놓음 | ① ☐ | ② ☐ |

**운영체제 최신버전으로 업데이트란?**

모바일기기 및 기기 내의 정보를 보호하기 위해, 모바일 운영체제(iOS, 안드로이드 등)를 업데이트해 최신 버전으로 유지시키는 것을 말함


## C . SNS 보안

**SNS(Social Network Service)란?**

인터넷 상에서 친구, 동료 등 지인과의 인간관계를 강화하거나 공통의 관심이나 활동을 통해 새로운 인맥을 형성함으로써 폭넓은 인적 및 정보 네트워크를 형성할 수 있게 해주는 서비스를 말합니다.

네이버 밴드, 다음/네이버 블로그, 인스타그램, 카카오스토리, 트위터, 티스토리, 페이스북 등이 있습니다.

**12** 귀하께서는 **SNS**를 이용하십니까?

☐ 1) 예 ☐ 2) 아니오

☞ **문 12의 2) 응답자는 문 13으로 이동**

문 12의 "1) 예" 응답자만

**12-1** 귀하께서는 SNS 이용 시, 입을 수 있는 피해를 **예방·방지**하기 위해 다음과 같은 사항을 **실천**하고 계십니까?
해당 항목을 **각각** 선택해 주십시오.

| 항 목 | | 실천여부 | |
|---|---|---|---|
| | | 예 | 아니오 |
| 1) | 개인신상정보, 사진, 영상 등의 정보는 신중히 선택하여 공개함 | ① ☐ | ② ☐ |
| 2) | 개인정보 활용에 대한 내용을 확인하고 신중하게 동의함 | ① ☐ | ② ☐ |
| 3) | 공용 PC 사용 시 SNS를 이용하지 않을 때는 로그아웃함 | ① ☐ | ② ☐ |
| 4) | 정보 공개설정 범위를 직접 확인하고 재설정함 | ① ☐ | ② ☐ |
| 5) | 신뢰할 수 있는 사람만 친구로 추가함 | ① ☐ | ② ☐ |
| 6) | 가족, 친구 등 타인의 개인정보를 함부로 게시·공개하지 않음 | ① ☐ | ② ☐ |

# Ⅲ | 침해사고 대응

## A . 침해사고 경험

문 13 ~ 문 15-1번의 응답시점은 2019년 1년간입니다.

**13** 2019년 1년간 귀하께서는 다음과 같은 **침해사고를 경험**한 적이 있습니까?
해당 항목을 **모두** 선택해 주십시오.
(간단하게 백신 등을 이용해 치료한 경우 제외)

| 항 목 | 경험여부 PC | 경험여부 모바일 |
|---|---|---|
| 1) 악성코드(바이러스, 웜, 애드웨어, 스파이웨어 등) 감염 등으로 인한 피해 (정보 손실, 물리적·시간적 손해) | ①☐ | ①☐ |
| 2) 개인정보 유출 및 사생활 침해 (주민등록번호, 개인신상정보, 사진, 동영상 등) | ②☐ | ②☐ |
| 3) 피싱/파밍/스미싱 등으로 인한 금전적 피해 (보이스피싱, 사기성 메시지 및 가짜 웹사이트 접속 유도를 통한 결제 유도 등) | ③☐ | ③☐ |
| 4) 신용카드 또는 직불카드 사기, 불법 결제 등으로 인한 금전적 피해 (삼성페이, 카카오페이, 페이코 등의 간편결제) | ④☐ | ④☐ |
| 5) 랜섬웨어 감염으로 인한 피해 (정보 손실, 물리적·시간적·금전적 피해) | ⑤☐ | ⑤☐ |
| 6) 경험 없음 | ⑥☐ | ⑥☐ |

☞ **문 13에서 하나라도 3) 응답자는 문 13-1로 이동**
☞ **문 13에서 모두 6) 응답자는 문 16으로 이동**

문 13의 하나라도 3) 응답자만

**13-1** 전자금융사기를 통한 금전적 손실 피해를 **어떤 경로**로 경험하셨습니까?
해당 항목을 **모두** 선택해 주십시오.

☐ 1) 메일이나 게시판에 연결된 웹사이트 접속
☐ 2) 이벤트를 가장한 홈페이지 접속
☐ 3) 인스턴트메신저(카카오톡, 라인, 페이스북 메시지 등) 채팅 도중 프로그램 또는 앱 설치
☐ 4) 공공·금융기관을 사칭한 전화를 통한 피싱
☐ 5) SNS를 통한 피싱
☐ 6) 금융기관 홈페이지를 가장한 웹사이트 접속
☐ 7) 인스턴트메신저 채팅 또는 문자메시지 내 인터넷주소(URL) 클릭
☐ 8) 기타 (적어주세요 : )
☐ 9) 잘 모르겠음

## B . 침해사고 대응조치

문 13에서 하나라도 1)~5) 응답자만

**14** 귀하께서는 인터넷 침해사고 경험 이후에 **어떻게 대응**하셨습니까?
해당 항목을 **모두** 선택해 주십시오.

☐ 1) 인터넷 서비스 제공자(ISP)(SK브로드밴드, LG유플러스, KT 등)를 다른 업체로 변경
☐ 2) 보안 소프트웨어(방화벽, 알약, V3 스파이웨어 제거 프로그램, 바이러스 검사 소프트웨어 등) 설치
☐ 3) 인터넷 상의 개인정보 공개 중단
☐ 4) 인터넷 서비스 이용 또는 소프트웨어 설치 시 약관을 주의 깊게 읽음
☐ 5) 스스로 점검 및 예방 활동 강화
☐ 6) 사용 중인 비밀번호 변경
☐ 7) 기타 (적어주세요 : )
☐ 8) 특별한 조치를 취하지 않음

문 13에서 하나라도 1)~5) 응답자만

**15** 귀하께서는 인터넷 침해사고 경험 **이후 기관 및 업체**에 **신고 또는 상담/문의**를 하셨습니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 정보보호 관련 정부부처 및 공공기관 (과학기술정보통신부, 한국인터넷진흥원, 경찰청 사이버안전국 등)
☐ 2) 정보보호 관련 민간업체(백신업체, 보안업체 등)
☐ 3) 인터넷 서비스 제공자(ISP)(SK브로드밴드, LG유플러스, KT 등)
☐ 4) 침해사고가 발생한 업체
☐ 5) 기타 (적어주세요 : )
☐ 6) 신고 또는 상담/문의를 하지 않음

☞ **문 15의 1) 응답자는 문 16으로 이동**

문 15의 1) 미응답자만

**15-1** 인터넷 침해사고 피해를 정보보호 관련 **정부부처 및 공공기관**에 **신고 또는 상담/문의하지 않은 가장 큰 이유**는 무엇입니까?

☐ 1) 신고/상담 기관을 몰라서
☐ 2) 신고/상담 방법 및 절차를 몰라서
☐ 3) 피해가 경미해서
☐ 4) 신고/상담해도 별다른 효과가 없을 것 같아서
☐ 5) 신고/상담하기 번거롭고 귀찮아서
☐ 6) 기타(적어주세요 : _____ )

# Ⅳ | 개인정보보호

## A . 개인정보보호 조치

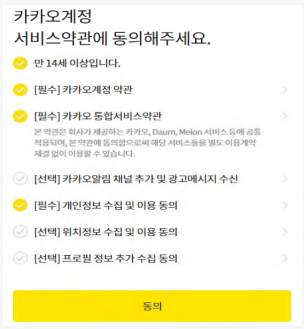
**16** 귀하께서는 인터넷 상에서 **어떤 목적**으로 개인정보를 제공하십니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 이메일 또는 정보 서비스를 받거나, 콘텐츠 내용을 보기 위한 회원가입을 위해
☐ 2) 본인인증(아이디, PW 찾기, 성인인증 등)을 위해
☐ 3) 제품 또는 서비스 구매를 위해
☐ 4) 이벤트 또는 행사(경품 행사 등) 참여를 위해
☐ 5) 커뮤니티 또는 친목 활동을 위해
☐ 6) 온라인 상담/문의(고객센터, 민원접수 등)를 위해
☐ 7) 구직 활동을 위해
☐ 8) 금융거래 또는 서비스를 이용하기 위해
☐ 9) 기타(적어주세요 : )
☐ 10) 제공하지 않음

**16-1** 귀하께서는 인터넷 상에 개인정보 제공 동의 시 필수 사항(이용약관, 개인정보 수집 및 이용에 대한 안내 등) 이외에 **선택 사항**(위치정보 이용약관, 이벤트·혜택 등 알림 수신 등)도 **동의**하십니까?

**개인정보 제공 동의란?**

'개인정보보호법'에 의해 업무를 목적으로 개인정보를 사용하거나 처리하는 모든 사업자는 반드시 정보 주체인 이용자의 동의를 받아야 합니다.
이용자는 아래와 같이 인터넷 상에서 개인정보를 제공하고, 필수 사항과 선택 사항의 약관을 확인하고 동의를 체크할 수 있습니다.




☐ 1) 항상 동의함
☐ 2) 필요한 경우에만 동의함
☐ 3) 동의하지 않음

**16-2** 귀하께서는 인터넷 상에 개인정보 제공 동의 시 **이용 약관**을 **확인**하십니까?

☐ 1) 항상 확인함
☐ 2) 필요한 경우에만 확인함
☐ 3) 확인하지 않음

**17** 개인정보 유출 **예방을 위하여** 귀하께서 취하고 있는 **조치**는 무엇입니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 자신의 아이디와 비밀번호, 주민번호 등 개인정보를 주의해서 관리하며 타인에게 알려주지 않음
☐ 2) 인터넷에서 파일을 함부로 다운로드 하지 않음
☐ 3) 금융거래 시 신용카드 번호와 같은 금융정보 등은 노출되지 않도록 함(PC방에서 금융거래 이용하지 않기 등)
☐ 4) 인터넷(P2P, 공유폴더 포함)에 올리는 데이터에 개인정보가 포함되지 않도록 주의
☐ 5) 명의도용 확인서비스 이용(타인에 의한 명의도용 사전차단 및 도용 시 이를 통지 받음)
☐ 6) 공인인증서를 개인용 이동식 저장장치에만 저장 (USB메모리, 외장하드, 스마트폰 등)
☐ 7) e프라이버시 클린서비스(www.eprivacy.go.kr)를 이용하여 수시로 개인정보 이용내역 확인
☐ 8) 기타(적어주세요 : )
☐ 9) 취하고 있는 조치 없음

## B . 개인정보 침해사고 및 대응

**개인정보 침해란?**

개인정보가 분실, 도난, 유출 등을 통해 수집、이용되거나 제3자에게 제공되어 발생하는 피해를 말합니다.

**문 18 ~ 문 18-2번의 응답시점은 2019년 1년간입니다.**

**18** 귀하께서는 2019년 1년간 개인정보 침해를 경험하셨습니까?

☐ 1) 예 ☐ 2) 아니오

☞ **문 18의 2) 응답자는 문 19로 이동**

문 18의 "1) 예" 응답자만

**18-1** 귀하께서는 2019년 1년간 **어떤 유형**의 개인정보 침해를 경험하셨습니까?
해당 항목을 **모두** 선택해 주십시오.

☐ 1) 내부의 보안 관리 소홀로 개인정보가 유출된 경우
☐ 2) 개인정보처리자가 개인정보를 무단으로 수집하여 마케팅(가입 권유, 제품·서비스 홍보 등) 목적으로 이용한 경우
☐ 3) 외부의 해킹으로 인해 개인정보가 유출된 경우
☐ 4) 유출된 정보가 피싱/스미싱 등 사기성 범죄로 활용된 경우
☐ 5) 개인정보처리자가 보유 및 이용 기간이 만료된 개인정보를 파기하지 않은 경우
☐ 6) 개인적인 사진이나 동영상 유출로 인한 사생활 침해
☐ 7) 기타(적어주세요 : )

문 18의 "1) 예" 응답자만

**18-2** 귀하께서는 개인정보 침해 시 **어떻게 대처**하셨습니까?
해당 항목을 **모두** 선택해 주십시오.

☐ 1) e프라이버시 클린서비스(www.eprivacy.go.kr) 이용
☐ 2) 해당 서비스를 탈퇴하고 동일한 서비스를 제공하는 다른 기업 이용
☐ 3) 개인정보를 유출시킨 기업에 직접 보상 요구
☐ 4) 민·형사상 책임을 묻도록 소송
☐ 5) 관련 기관에 신고 또는 상담 등의 조치 (방송통신위원회, 한국인터넷진흥원, 한국소비자원, 경찰청 사이버안전국, 금융감독원 등)
☐ 6) 개인정보분쟁조정위원회 조정 신청
☐ 7) 기타(적어주세요 : )
☐ 8) 특별한 대처를 하지 않음

# V | 주요 서비스별 정보보호

## A. 클라우드 서비스

**다음은 클라우드 서비스의 보안 관련 문항입니다.**

**클라우드 서비스란?**

개인의 사진、문서、동영상 등 각종콘텐츠를 '클라우드'라는 가상공간 서버에 저장한 뒤 인터넷으로 접속해 노트북, 스마트폰 등 다양한 기기로 이용할 수 있는 서비스를 말함

예) **드라이브형** (네이버 N드라이브, 구글 드라이브, 애플 iCloud, 드롭박스, 마이크로소프트 원드라이브, 올레 U클라우드, SKT 클라우드베리, LG U+박스 등)
**문서작업** (구글 Docs, 마이크로소프트오피스 365 등)
**일정/연락처** (구글 캘린더, 네이버 캘린더, 네이버주소록 등)

**19** 귀하께서는 **클라우드 서비스**를 이용하고 계십니까?

☐ 1) 예 ☐ 2) 아니오
☞ **문 19의 2) 응답자는 문 20으로 이동**

문 19의 "1) 예" 응답자만

**19-1** 귀하께서는 클라우드 서비스 이용 시 입을 수 있는 **피해**(개인정보 및 사진, 문서 등의 데이터 유출 등)를 **예방·방지**하기 위해 다음과 같은 사항을 **실천**하십니까?
해당 항목을 **모두** 선택해 주십시오.

☐ 1) 클라우드 서비스 이용약관 확인하기
☐ 2) 중요파일은 저장 또는 공유 전 암호화 설정하기
☐ 3) 공유 기능을 정확하게 확인하고 이용하기
☐ 4) 접근 권한을 정확하게 확인하고 이용하기
☐ 5) 서비스 장애를 대비하여 정기적으로 외부장치(USB메모리, 외장하드 등)에 백업하기
☐ 6) 서비스 이용 종료 시, 중요 정보는 완전히 삭제하고 삭제 여부 확인하기
☐ 7) 본인이 허락할 때만 로그인되도록 2단계 인증을 설정함
☐ 8) 기타(적어주세요 : _____ )
☐ 9) 해당사항 없음

## B . IP 카메라

**다음은 IP카메라의 보안 관련 문항입니다.**

**IP카메라란?**

전통적 폐쇄형 CCTV(Closed Circuit Television)가 인터넷과 결합한 형태의 영상정보처리기기를 말합니다.

유선 또는 무선으로 인터넷에 연결되어 PC나 모바일 기기 등을 통해 실시간으로 영상을 송출할 수 있는 단말

**20** 귀하께서는 **IP카메라 제품**을 이용하고 계십니까?

☐ 1) 예 ☐ 2) 아니오

☞ **문 20의 2) 응답자는 문 21로 이동**

문 20의 "1) 예" 응답자만

**20-1** 귀하께서 현재 **IP카메라를 이용하는 목적**은 무엇입니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 재택근무/재택교육 등에 활용
☐ 2) 가족 안전 확인
☐ 3) 반려동물 확인
☐ 4) 외부자 침입이나 도난 방지
☐ 5) 단순 호기심
☐ 6) 기타(적어주세요 : _____ )

문 20의 "1) 예" 응답자만

**20-2** 귀하께서 최근 1년간 **IP카메라** 보안을 위해 실시한 보안조치는 어떤 것입니까? 해당 항목을 **모두** 선택해 주십시오.

☐ 1) 관리자 계정의 비밀번호 변경하여 사용
☐ 2) 기기를 최신 버전으로 업데이트
☐ 3) IP카메라를 사용하지 않을 때는 전원 끄기
☐ 4) IP카메라에 접근하는 PC 및 스마트폰의 보안 설정 강화
☐ 5) 기타(적어주세요 : _____ )
☐ 6) 별도의 보안조치 없음

**21** 귀하께서는 **IP카메라 제품 보급**이 더욱 확산될 때 **보안상 우려되는 문제점**이 무엇이라고 생각하십니까? **주로** 우려되는 항목을 **2가지만** 선택해 주십시오.

☐ 1) 많은 종류의 영상데이터 발생·처리로 인한 개인정보 침해 위협 증가
☐ 2) 영상정보 노출에 따른 주거침입, 성범죄 등 2차 범죄 우려
☐ 3) 대규모 악성코드 감염 제품 발생으로 인한 사이버공격 강도 및 가능성 증대
☐ 4) 제품의 정지 및 오작동으로 인한 신체적·재산적 피해
☐ 5) 기타(적어주세요 : _____ )

## C . 향후 지출 계획

**22** 귀하께서는 향후 정보보호를 위해 어떤 분야에 지출할 의향이 있으십니까?
해당되는 항목을 한 가지만 선택해 주십시오.

☐ 1) 정보보호 제품 및 서비스 구매
☐ 2) 정보보호 관련 교육 참여
☐ 3) 지출 계획 없음
☐ 4) 기타(적어주세요 : _____ )

조사된 결과는 2020년 12월 한국정보보호산업협회 공식 홈페이지(https://www.kisia.or.kr)에서 확인하실 수 있습니다.

**끝까지 응답해 주셔서 감사합니다.**

# 2020년 정보보호 실태조사

**인 쇄** : 2021년 2월 **발 행** : 2021년 2월

**발 행 처** : 한국정보보호산업협회(Korea Information Security Industry Association)
(05717) 서울시 송파구 중대로 135

**조사 기관** : 과학기술정보통신부

**조사 전담** : 한국정보보호산업협회

**조사 수행** : ㈜글로벌리서치

**<<비매품>>**

kisia 한국정보보호산업협회
Korea Information Security Industry Association