



승인번호
제 342005 호



2018 정보보호 실태조사





이용자를 위하여

1. 본 보고서의 내용을 인용할 때에는 반드시 과학기술정보통신부와 한국인터넷진흥원의 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 (부록2 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 결과치를 집계한 결과임



2018년 정보보호 실태조사

조사 기획	과학기술정보통신부	손창용	서기관
		고은희	주무관
조사 전담	한국인터넷진흥원	이완석	본부장
		오진영	단장
		오남호	팀장
		이유진	선임
		김주희	주임

2018 정보보호 실태조사

기업부문

정보보호 기반 및 환경

정보보호 정책 16.0%

정보보호 조직 5.5%

정보보호 예산 36.2%

정보보호 중요성 인식 90.2%
개인정보보호 중요성 인식 89.3%

침해사고 예방

보안점검 실시 90.0%

백업실시 49.8%

정보보호 제품이용 90.9%

정보보호 서비스이용 59.4%

침해사고 경험 및 대응

침해사고 대응

긴급연락체계구축 10.9%

침해사고 대응계획수립 7.8%

침해사고 대응팀 구축/운영 5.1%

침해사고 경험

랜섬웨어 56.3%
악성코드 47.7%
애드웨어/스파이웨어 12.1%

지능형서비스 보안

보안 우려사항

클라우드

데이터 위탁 저장에 따른 정보유출 56.2%
자원 공유·집중화로 서비스 장애시 대규모 피해 발생 54.9%

사물인터넷 (IoT)

정보유출 44.3%
해킹 및 악성코드 감염 42.7%

클라우드 이용 7.4%

(IoT) 사물인터넷 이용 9.1%

2018 정보보호 실태조사

개인부문

정보보호 인식



침해사고 위협에 대한 인식



침해사고 예방 및 대응



침해사고 예방



침해사고 경험 **4.6%**



지능형 서비스

주요 지능형 서비스 보안 우려사항



주요 지능형 서비스 이용





1부 기업부문

제1장	조사개요	1
	1. 조사 목적	3
	2. 조사 연혁	3
	3. 조사 내용 및 범위	5
	4. 주요 용어 및 정의	6
	5. 조사 체계	8
	6. 표본 설계	8
	가. 모집단	8
	나. 표본추출	12
	7. 실 사	13
	가. 실사 개요	13
	나. 표본 관리	14
	8. 자료 입력 및 처리	14
	가. 자료 검증 및 대체	14
	나. 자료 입력 및 분석	14
	9. 추정 및 표본오차	15
	가. 가중치 산출	15
	나. 추정	16
	다. 표본오차	16
	10. 결과 공표 및 활용분야	17
	11. 표본 현황	18
제2장	조사결과 요약	21
	I. 정보보호 인식	23
	II. 정보보호 기반 및 환경	24
	1. 정보보호(개인정보보호) 정책	24
	2. 정보보호(개인정보보호) 조직	25
	3. 정보보호(개인정보보호) 교육	26



II. 정보보호 기반 및 환경	48
1. 정보보호 정책	48
가. 정보보호 정책 수립	48
나. 정보보호 정책 포함 위협요소	49
다. 개인정보보호 정책 수립	50
2. 정보보호 조직	53
가. 정보보호 전담조직 운영	53
나. 개인정보보호 전담조직 운영	54
다. 정보보호와 개인정보보호 조직 공동 운영	56
3. 정보보호 인력	59
가. 정보보호 관련 책임자	59
나. IT 인력 중 정보보호 담당 인력 비중	62
다. 정보보호 담당 인력 신규 채용계획	63
4. 정보보호 교육	64
가. 정보보호 교육 실시	64
나. 개인정보보호 교육 실시	66
다. 대상별 교육 실시 현황	69
5. 정보보호 예산 및 투자	70
III. 침해사고 예방	72
1. 정보보호 제품 및 서비스	72
가. 정보보호 제품 이용	72
나. 정보보호 서비스 이용	76
2. 정보보호 관리	78
가. 보안점검 및 취약점 점검	78
나. 보안패치 적용	80
다. 백업 실시	82
IV. 침해사고 대응	85
1. 침해사고 경험	85
가. 침해사고 경험	85
나. 침해사고 경험 유형 및 심각성 정도	86
다. 침해사고 시 관계기관 문의 또는 신고	88
2. 침해사고 대응	89



V. 개인정보보호	90
1. 개인정보 수집 및 이용	90
가. 개인정보 수집	90
나. 개인정보 이용	91
다. 개인정보 수집 및 이용 현황	91
라. 개인정보 수집 및 이용 목적	92
2. 개인정보 침해사고 예방	93
가. 개인정보 침해사고 예방을 위한 관리적 조치	93
나. 개인정보 침해사고 예방을 위한 기술적 조치	95
다. 개인정보 암호화	96
3. 개인정보 침해사고 경험	97
가. 개인정보 침해사고 경험	97
나. 개인정보 침해사고 시 관계기관 문의 또는 신고	97
다. 개인정보 침해사고 시 통지 또는 고지	98
VI. 주요 서비스별 정보보호	99
1. 무선랜	99
가. 무선랜 구축 및 운영	99
나. 무선랜 보안	99
2. 모바일	101
가. 모바일 기기 업무 활용	101
나. 모바일 보안	102
3. 클라우드	104
가. 클라우드 서비스 이용	104
나. 클라우드 보안	106
4. 사물인터넷(IoT)	107
가. 사물인터넷(IoT) 제품·서비스 이용	107
나. 사물인터넷(IoT) 보안	108
5. 정보보호(사이버) 보험	109
가. 정보보호(사이버) 보험 인지	109
나. 정보보호(사이버) 보험 이용	110
6. 주요 서비스 정보보호 투자	112
가. 주요 서비스 정보보호 투자 현황	112
나. 주요 서비스 정보보호 투자 계획	113



2부 개인부문

제1장 조사개요 117

1. 조사 목적	119
2. 조사 연혁	119
3. 조사 내용 및 범위	121
4. 주요 용어 및 정의	121
5. 조사 체계	122
6. 표본 설계	123
가. 모집단	123
나. 표본 추출	123
7. 실사	125
가. 실사개요	125
나. 표본 관리	125
8. 자료 입력 및 처리	126
가. 자료 검증 및 대체	126
나. 자료 입력 및 분석	126
9. 추정 및 표본오차	127
가. 가중치 산출	127
나. 추정	127
다. 표본오차	128
10. 결과 공표 및 활용분야	128
11. 모집단 및 표본 현황	129

제2장 조사결과 요약 131

I. 정보보호 인식	133
1. 정보보호 중요성 인식	133
2. 개인정보보호 중요성 인식	134
II. 침해사고 예방	135
1. 정보보호 제품 이용	135
2. 침해사고 예방 활동	136



- 가. 백신 프로그램 업데이트 136
- 나. 운영체제 보안 업데이트 137
- 다. 중요 데이터 백업 138
- 라. PC 비밀번호 설정 139
- Ⅲ. 침해사고 대응 140**
 - 1. 침해사고 경험 140
 - 2. 침해사고 대응 141
- Ⅳ. 개인정보보호 142**
 - 1. 개인정보 침해사고 예방 142
 - 2. 개인정보 침해사고 대응 143
- Ⅴ. 주요 서비스별 정보보호 144**
 - 1. 클라우드 144
 - 2. SNS 145
 - 3. 빅데이터 146
 - 4. 사물인터넷(IoT) 147
 - 5. 핀테크 148
 - 6. 인공지능(AI) 149

제3장 조사결과 151

- Ⅰ. 정보보호 인식 153**
 - 1. 정보보호 및 개인정보보호 중요성 인식 153
 - 2. 정보보호 위협에 대한 인식 154
 - 가. 위협사안에 대한 구체적 인지 154
 - 나. 위협사안에 대한 피해의 심각성 154
 - 3. 정보보호 관련 정보수집 및 학습활동 155
- Ⅱ. 침해사고 예방 156**
 - 1. 정보보호 관련 제품 156
 - 가. 정보보호 제품 이용 156
 - 나. 정보보호 제품 미이용 이유 158
 - 다. 정보보호 소프트웨어 이용 159



라. 악성코드 검사 실시 주기	160
마. 백신 프로그램 업데이트	160
바. 운영체제 보안 업데이트	162
사. 중요 데이터 백업	164
아. PC 및 네트워크 보안을 위한 예방조치	166
자. 비밀번호 설정 및 관리	167
2. 모바일 및 무선랜 보안	169
가. 무선랜 피해 예방 조치	169
나. 모바일 기기 피해 예방 조치	170
3. SNS 보안	171
Ⅲ. 침해사고 대응	172
1. 침해사고 경험	172
2. 침해사고 대응	174
Ⅳ. 개인정보보호	176
1. 개인정보보호 조치	176
가. 온라인 상 개인정보 제공 목적	176
나. 개인정보 침해사고 예방 조치	177
2. 개인정보 침해사고 경험 및 대응	178
가. 개인정보 침해사고 경험	178
나. 개인정보 침해사고 대응활동 수행	179
Ⅴ. 주요 서비스별 정보보호	180
1. 클라우드	180
2. 빅데이터	181
3. 사물인터넷(IoT)	182
4. 핀테크	184
5. 인공지능(AI)	186
6. 향후 정보보호 지출 계획	187
<부록1> 주요변경내역	189
<부록2> 표본오차	201
<부록3> 설문지	219



1부 기업부문

그림 1-2-1. 정보보호 및 개인정보보호 중요성 인식률	23
그림 1-2-2. 정보보호(개인정보보호) 정책 수립률	24
그림 1-2-3. 규모별 정보보호(개인정보보호) 정책 수립률	24
그림 1-2-4. 정보보호(개인정보보호) 조직 보유율	25
그림 1-2-5. 규모별 정보보호(개인정보보호) 조직 보유율	25
그림 1-2-6. 정보보호(개인정보보호) 교육 실시율	26
그림 1-2-7. 규모별 정보보호(개인정보보호) 교육 실시율	26
그림 1-2-8. 정보보호(개인정보보호) 예산 편성률	27
그림 1-2-9. IT 예산 중 정보보호(개인정보보호) 예산 비중	27
그림 1-2-10. 정보보호 제품 이용률	28
그림 1-2-11. 정보보호 제품군별 이용률 (복수응답)	28
그림 1-2-12. 정보보호 서비스 이용률	29
그림 1-2-13. 정보보호 서비스 유형별 이용률 (복수응답)	29
그림 1-2-14. 시스템 및 네트워크 보안점검 실시율	30
그림 1-2-15. 유형별 취약점 점검률 (복수응답) - 보안점검 실시 사업체	30
그림 1-2-16. 보안패치 적용률	31
그림 1-2-17. 보안패치 유형별 적용률 (복수응답) - 항목별 제품 보유 사업체	31
그림 1-2-18. 백업 실시율	32
그림 1-2-19. 백업 유형별 실시율 (복수응답)	32
그림 1-2-20. 침해사고 경험 및 피해 심각성 정도	33
그림 1-2-21. 침해사고 경험 유형 (복수응답) - 침해사고 경험 사업체	33
그림 1-2-22. 침해사고 대응활동 수행률	34
그림 1-2-23. 침해사고 대응활동 수행 (복수응답)	34
그림 1-2-24. 고객 개인정보 수집률	35
그림 1-2-25. 고객 개인정보 이용률	35
그림 1-2-26. 개인정보 침해사고 예방 관리적 조치 시행률 - 온라인으로 개인정보 수집 사업체	36
그림 1-2-27. 개인정보 침해사고 예방 관리적 조치 (복수응답) - 온라인으로 개인정보 수집 사업체	36
그림 1-2-28. 개인정보 침해사고 예방 기술적 조치 시행률 - 온라인으로 개인정보 수집 사업체	37
그림 1-2-29. 개인정보 침해사고 예방 기술적 조치 (복수응답) - 온라인으로 개인정보 수집 사업체	37
그림 1-2-30. 무선랜 구축 및 운영률	38
그림 1-2-31. 무선랜 보안 우려사항 (2가지) - 무선랜 구축 사업체	38
그림 1-2-32. 클라우드 서비스 이용 및 향후 도입(유지) 계획	39
그림 1-2-33. 클라우드 서비스 관련 보안 우려사항 (2가지)	39



그림 1-2-34. 사물인터넷(IoT) 제품 서비스 이용 및 향후 도입(유지) 계획	40
그림 1-2-35. 사물인터넷(IoT) 관련 보안 우려사항	40
그림 1-2-36. 정보보호(사이버) 보험 이용 및 향후 가입(유지) 계획	41
그림 1-2-37. 정보보호(사이버) 보험 보장 희망 항목 (복수응답) - 향후 가입 계획 사업체	41
그림 1-3-1. 정보보호 및 개인정보보호 중요성 인식	45
그림 1-3-2. 정보보호 위협요인 (2가지)	45
그림 1-3-3. 정보보호 인적 위협요인	46
그림 1-3-4. 우려하는 개인정보 유출요인 (2가지)	46
그림 1-3-5. 정보보호 애로사항 (복수응답)	47
그림 1-3-6. 정보보호 정책 수립	48
그림 1-3-7. 업종별 정보보호 정책 수립	48
그림 1-3-8. 규모별 정보보호 정책 수립	49
그림 1-3-9. 정보보호 정책 포함 위협요소 (복수응답) - 정보보호 정책 보유 사업체	49
그림 1-3-10. 개인정보보호 정책 수립	50
그림 1-3-11. 업종별 개인정보보호 정책 수립	50
그림 1-3-12. 규모별 개인정보보호 정책 수립	51
그림 1-3-13. 정보보호(개인정보보호) 정책 수립	52
그림 1-3-14. 업종별 정보보호(개인정보보호) 정책 수립	52
그림 1-3-15. 규모별 정보보호(개인정보보호) 정책 수립	52
그림 1-3-16. 정보보호 전담조직 운영	53
그림 1-3-17. 업종별 정보보호 전담조직 운영	53
그림 1-3-18. 규모별 정보보호 전담조직 운영	54
그림 1-3-19. 개인정보보호 전담조직 운영	54
그림 1-3-20. 업종별 개인정보보호 전담조직 운영	55
그림 1-3-21. 규모별 개인정보보호 전담조직 운영	55
그림 1-3-22. 정보보호와 개인정보보호 조직 공동 운영	56
그림 1-3-23. 업종별 정보보호와 개인정보보호 조직 공동 운영	56
그림 1-3-24. 규모별 정보보호와 개인정보보호 조직 공동 운영	57
그림 1-3-25. 정보보호(개인정보보호) 조직 운영	58
그림 1-3-26. 업종별 정보보호(개인정보보호) 조직 운영	58
그림 1-3-27. 규모별 정보보호(개인정보보호) 조직 운영	58
그림 1-3-28. 정보보호 관련 책임자 임명 (복수응답)	59
그림 1-3-29. 업종별 정보보호 관련 책임자 임명 (복수응답)	59
그림 1-3-30. 규모별 정보보호 관련 책임자 임명 (복수응답)	60
그림 1-3-31. 정보보호 관련 책임자 전담 (복수응답)	60



그림 1-3-32. 업종별 정보보호 관련 책임자 전담 (복수응답)	61
그림 1-3-33. 규모별 정보보호 관련 책임자 전담 (복수응답)	61
그림 1-3-34. IT 인력 중 정보보호 담당 인력 비중	62
그림 1-3-35. 업종별 IT 인력 중 정보보호 담당 인력 배정	62
그림 1-3-36. 규모별 IT 인력 중 정보보호 담당 인력 배정	63
그림 1-3-37. 정보보호 담당 인력 신규 채용계획	63
그림 1-3-38. 정보보호 담당 인력 신규 채용 규모 - 신규 채용 계획 사업체	64
그림 1-3-39. 정보보호 교육 실시	64
그림 1-3-40. 업종별 정보보호 교육 실시	65
그림 1-3-41. 규모별 정보보호 교육 실시	65
그림 1-3-42. 개인정보보호 교육 실시	66
그림 1-3-43. 업종별 개인정보보호 교육 실시	66
그림 1-3-44. 규모별 개인정보보호 교육 실시	67
그림 1-3-45. 정보보호(개인정보보호) 교육 실시	68
그림 1-3-46. 업종별 정보보호(개인정보보호) 교육 실시	68
그림 1-3-47. 규모별 정보보호(개인정보보호) 교육 실시	68
그림 1-3-48. 대상별 교육 실시 (복수응답) - 정보보호(개인정보보호) 교육 실시 사업체	69
그림 1-3-49. 대상별 교육 시간 - 정보보호(개인정보보호) 교육 실시 사업체	69
그림 1-3-50. IT 예산 중 정보보호 예산 비중	70
그림 1-3-51. 정보보호 예산 증감 - 정보보호 예산 수립 사업체	70
그림 1-3-52. 정보보호 지출 분야 (2가지) - 정보보호 예산 수립 사업체	71
그림 1-3-53. 정보보호 제품 이용 (요약)	72
그림 1-3-54. 정보보호 제품 이용 - 정보보안 (복수응답)	73
그림 1-3-55. 정보보호 제품 이용 - 물리보안 (복수응답)	73
그림 1-3-56. CCTV 보유 대수 - CCTV 보유 사업체	74
그림 1-3-57. 정보보호 제품 국산/외산 비중	75
그림 1-3-58. 외산 정보보호 제품 구매 이유 - 외산 제품 구매 사업체	75
그림 1-3-59. 정보보호 서비스 이용 요약	76
그림 1-3-60. 보안컨설팅 (복수응답)	76
그림 1-3-61. 보안관제 (복수응답)	77
그림 1-3-62. 인증 (복수응답)	77
그림 1-3-63. 시스템 및 네트워크 보안점검 실시 (복수응답)	78
그림 1-3-64. 시스템 및 네트워크 보유 (복수응답) - 보안점검 실시 사업체	79
그림 1-3-65. 취약점 점검 (복수응답) - 각 시스템 및 네트워크 보유 사업체	79
그림 1-3-66. 취약점 점검 (복수응답) - 보안점검 실시 사업체	80
그림 1-3-67. 보안패치 적용 방법 (복수응답) - 항목별 제품 보유 사업체	80



그림 1-3-68. 보안패치 적용	81
그림 1-3-69. 보안패치 업데이트 미실시 이유 (복수응답) - 하나라도 업데이트 하지 않는 사업체	81
그림 1-3-70. 시스템 로그 백업	82
그림 1-3-71. 시스템 로그 백업 주기 - 시스템 로그 백업 실시 사업체	82
그림 1-3-72. 중요 데이터 백업	83
그림 1-3-73. 중요 데이터 백업 주기 - 중요 데이터 백업 실시 사업체	83
그림 1-3-74. 백업 방식 (복수응답) - 하나라도 백업 실시 사업체	84
그림 1-3-75. 백업 실시 - 시스템 로그 또는 중요 데이터 백업 실시	84
그림 1-3-76. 침해사고 경험	85
그림 1-3-77. 업종별 침해사고 경험	85
그림 1-3-78. 규모별 침해사고 경험	86
그림 1-3-79. 침해사고 경험 유형 (복수응답) - 침해사고 경험 사업체	86
그림 1-3-80. 침해사고 유형별 심각성 정도 - 침해사고 경험 사업체	87
그림 1-3-81. 침해사고 유형별 심각성 정도 통합 - 침해사고 경험 사업체	87
그림 1-3-82. 침해사고 시 관계기관 문의 또는 신고 - 침해사고 경험 사업체	88
그림 1-3-83. 침해사고 대응활동 수행 (복수응답)	89
그림 1-3-84. 침해사고 대응 대외협력채널 (2가지)	89
그림 1-3-85. 개인정보 수집 (복수응답)	90
그림 1-3-86. 개인정보 온라인 수집 방법 (복수응답) - 온라인으로 개인정보 수집 사업체	90
그림 1-3-87. 개인정보 이용 (복수응답)	91
그림 1-3-88. 개인정보 수집 및 이용 현황 - 일반정보 (복수응답) - 개인정보 수집 사업체	91
그림 1-3-89. 개인정보 수집 및 이용 현황 - 특화정보 (복수응답) - 개인정보 수집 사업체	92
그림 1-3-90. 개인정보 수집 및 이용 목적 - 개인정보 수집 사업체	92
그림 1-3-91. 개인정보 침해사고 예방을 위한 관리적 조치 (복수응답) - 개인정보 수집 사업체	93
그림 1-3-92. 개인정보 침해사고 예방을 위한 관리적 조치 (복수응답) - 온라인으로 개인정보 수집 사업체	94
그림 1-3-93. 개인정보 침해사고 예방을 위한 기술적 조치 (복수응답) - 개인정보 수집 사업체	95
그림 1-3-94. 개인정보 침해사고 예방을 위한 기술적 조치 (복수응답) - 온라인으로 개인정보 수집 사업체	95
그림 1-3-95. 개인정보 암호화 - 개인정보 암호화 저장 및 보안서버 이용 사업체	96
그림 1-3-96. 개인정보 침해사고 경험 - 개인정보 수집 사업체	97
그림 1-3-97. 개인정보 침해사고 시 관계기관 문의 또는 신고 - 개인정보 침해사고 경험 사업체	97
그림 1-3-98. 개인정보 침해사고 시 통지 또는 고지 - 개인정보 침해사고 경험 사업체	98
그림 1-3-99. 무선랜 구축 및 운영	99
그림 1-3-100. 무선랜 보안 우려사항 (2가지) - 무선랜 구축 사업체	99
그림 1-3-101. 무선랜 보안을 위한 조치 (복수응답) - 무선랜 구축 사업체	100
그림 1-3-102. 무선랜 보안을 위한 조치 (복수응답) - 무선랜 보안조치 실행 사업체	100
그림 1-3-103. 개인소유 모바일 기기 업무 활용	101



그림 1-3-104. 회사소유 모바일 기기 업무 활용	101
그림 1-3-105. 개인 모바일 기기 활용 시 보안 우려사항 (2가지) - 개인 모바일 기기 이용 사업체	102
그림 1-3-106. 모바일 기기 활용 시 보안 위협에 대한 대응 방안 (복수응답) - 모바일 기기 이용 사업체	103
그림 1-3-107. 클라우드 서비스 이용	104
그림 1-3-108. 클라우드 서비스 향후 도입(유지) 계획	104
그림 1-3-109. 클라우드 서비스 이용(계획) 분야 (복수응답) - 클라우드 서비스 이용 또는 향후 계획 사업체	105
그림 1-3-110. 클라우드 서비스 보안을 위한 조치 (복수응답) - 클라우드 서비스 이용 사업체	106
그림 1-3-111. 클라우드 서비스 보안 우려사항 (2가지)	106
그림 1-3-112. 사물인터넷(IoT) 제품·서비스 이용	107
그림 1-3-113. 사물인터넷(IoT) 제품·서비스 향후 도입(유지) 계획	107
그림 1-3-114. 사물인터넷(IoT) 이용(계획) 분야 (복수응답) - 사물인터넷(IoT) 이용 또는 향후 계획 사업체	108
그림 1-3-115. 사물인터넷(IoT) 제품·서비스 보안을 위한 조치 (복수응답) - 사물인터넷(IoT) 이용 사업체	108
그림 1-3-116. 사물인터넷(IoT) 관련 보안 우려사항	109
그림 1-3-117. 정보보호(사이버) 보험 인지	109
그림 1-3-118. 정보보호(사이버) 보험 가입	110
그림 1-3-119. 정보보호(사이버) 보험 이용 - 정보보호(사이버) 보험 가입 사업체	110
그림 1-3-120. 정보보호(사이버) 보험 이용	111
그림 1-3-121. 정보보호(사이버) 보험 향후 가입(유지) 계획	111
그림 1-3-122. 정보보호(사이버) 보험 희망 보장 항목 (복수응답) - 향후 가입 계획 사업체	112
그림 1-3-123. 주요 서비스 정보보호 투자 현황 (복수응답)	112
그림 1-3-124. 주요 서비스 정보보호 투자 계획 (복수응답)	113

2부 개인부문

그림 2-2-1. 정보보호 중요성 인식률	133
그림 2-2-2. 연령별 정보보호 중요성 인식률	133
그림 2-2-3. 개인정보보호 중요성 인식률	134
그림 2-2-4. 연령별 개인정보보호 중요성 인식률	134
그림 2-2-5. 정보보호 제품 이용률	135
그림 2-2-6. 정보보호 소프트웨어 이용률 (복수응답) - 정보보호 제품 이용자	135
그림 2-2-7. 백신 프로그램 업데이트 실시율 - 정보보호 제품 이용자	136
그림 2-2-8. 백신 프로그램 업데이트 방법 - PC/모바일 기기 이용자 중 정보보호 제품 이용자	136
그림 2-2-9. 운영체제 보안 업데이트 실시율	137
그림 2-2-10. 운영체제 보안 업데이트 방법 - PC/모바일 기기 이용자	137
그림 2-2-11. 중요 데이터 백업률	138



그림 2-2-12. 중요 데이터 백업 방식 (복수응답) - PC/모바일 기기 이용자 중 중요 데이터 백업 실시자	138
그림 2-2-13. PC 비밀번호 설정률 - PC 이용자	139
그림 2-2-14. PC 비밀번호 설정 유형 (복수응답) - PC 비밀번호 설정 응답자	139
그림 2-2-15. 침해사고 경험률	140
그림 2-2-16. 침해사고 경험 유형 (복수응답)	140
그림 2-2-17. 침해사고 대응률 - 침해사고 경험자	141
그림 2-2-18. 침해사고 대응활동 수행 (복수응답) - 침해사고 경험자	141
그림 2-2-19. 개인정보 침해사고 예방 조치 실시율	142
그림 2-2-20. 개인정보 침해사고 예방 조치 유형 (복수응답)	142
그림 2-2-21. 개인정보 침해사고 대응률 - 개인정보 침해사고 경험자	143
그림 2-2-22. 개인정보 침해사고 대응활동 수행 (복수응답) - 개인정보 침해사고 경험자	143
그림 2-2-23. 클라우드 서비스 이용률	144
그림 2-2-24. 클라우드 서비스 피해 예방 조치 (복수응답) - 클라우드 서비스 이용자	144
그림 2-2-25. SNS 이용률	145
그림 2-2-26. SNS 피해 예방 조치 (복수응답) - SNS 이용자	145
그림 2-2-27. 빅데이터 활용 서비스 이용률	146
그림 2-2-28. 빅데이터 활용 서비스 대중화 시 보안 우려사항 (2가지)	146
그림 2-2-29. 사물인터넷(IoT) 제품서비스 이용 및 유형	147
그림 2-2-30. 사물인터넷(IoT) 대중화 시 보안 우려사항 (복수응답) - 사물인터넷(IoT) 제품서비스 이용자	147
그림 2-2-31. 간편결제 서비스 이용 및 본인 인증 수단	148
그림 2-2-32. 일반결제 대비 간편결제 서비스 보안성 인식 - 간편결제 서비스 이용자	148
그림 2-2-33. 인공지능(AI) 활용 서비스 이용 및 유형	149
그림 2-2-34. 인공지능(AI) 활용 서비스 대중화 시 보안 우려사항 (2가지)	149
그림 2-3-1. 정보보호 및 개인정보보호 중요성 인식	153
그림 2-3-2. 성·연령별 정보보호 및 개인정보보호 중요성 인식	153
그림 2-3-3. 위협사안에 대한 구체적 인지	154
그림 2-3-4. 위협사안에 대한 피해의 심각성	154
그림 2-3-5. 정보보호 관련 정보수집 및 학습활동 (복수응답)	155
그림 2-3-6. 연령별 정보보호 관련 정보수집 및 학습활동률	155
그림 2-3-7. 정보보호 제품 이용	156
그림 2-3-8. 정보보호 제품 이용 - PC/모바일 기기 이용자	157
그림 2-3-9. 정보보호 제품 미이용 이유 (복수응답) - 정보보호 제품 미이용자	158
그림 2-3-10. 정보보호 제품 미이용 이유 (복수응답) - PC/모바일 기기 이용자 중 정보보호 제품 미이용자	158
그림 2-3-11. 정보보호 소프트웨어 이용 (복수응답) - 정보보호 제품 이용자	159
그림 2-3-12. 정보보호 소프트웨어 이용 (복수응답) - PC/모바일 기기 이용자 중 정보보호 제품 이용자	159
그림 2-3-13. 악성코드 검사 실시 주기 - PC/모바일 기기 이용자 중 정보보호 제품 이용자	160



그림 2-3-14. 백신 프로그램 업데이트 방법 - 정보보호 제품 이용자	160
그림 2-3-15. 백신 프로그램 업데이트 방법 - PC/모바일 기기 이용자 중 정보보호 제품 이용자	161
그림 2-3-16. 백신 프로그램 업데이트 실시 주기- PC/모바일 기기 이용자 중 수동 업데이트 실시자	161
그림 2-3-17. 운영체제 보안 업데이트	162
그림 2-3-18. 운영체제 보안 업데이트 방법 - PC/모바일 기기 이용자	162
그림 2-3-19. 운영체제 보안 업데이트 미실시 이유 (복수응답) - 보안 업데이트 미실시자	163
그림 2-3-20. 운영체제 보안 업데이트 미실시 이유 (복수응답) - PC/모바일 기기 이용자 중 보안 업데이트 미실시자	163
그림 2-3-21. 중요 데이터 백업	164
그림 2-3-22. 중요 데이터 백업 - PC/모바일 기기 이용자	164
그림 2-3-23. 중요 데이터 백업 방식 (복수응답) - 중요 데이터 백업 실시자	165
그림 2-3-24. 중요 데이터 백업 방식 (복수응답) - PC/모바일 기기 이용자 중 중요 데이터 백업 실시자	165
그림 2-3-25. 중요 데이터 백업 실시 주기 - PC/모바일 기기 이용자 중 중요 데이터 백업 실시자	166
그림 2-3-26. PC 및 네트워크 보안을 위한 예방 조치 (복수응답)	166
그림 2-3-27. PC 비밀번호 설정 (복수응답) - PC 이용자	167
그림 2-3-28. 하나라도 PC 비밀번호 설정률	167
그림 2-3-29. 비밀번호 관리 조치 (복수응답)	168
그림 2-3-30. PC 및 웹사이트의 비밀번호 변경 주기 - 주기적 비밀번호 변경자	168
그림 2-3-31. 무선랜 이용 - 모바일 기기 이용자	169
그림 2-3-32. 무선랜 피해 예방 조치 (복수응답) - 모바일 기기 이용자 중 무선랜 이용자	169
그림 2-3-33. 모바일 기기 피해 예방 조치 (복수응답) - 모바일 기기 이용자	170
그림 2-3-34. SNS 이용	171
그림 2-3-35. SNS 피해 예방 조치 (복수응답) - SNS 이용자	171
그림 2-3-36. 침해사고 경험 유형 (복수응답)	172
그림 2-3-37. 침해사고 경험 유형 (복수응답) - PC/모바일 기기 이용자	173
그림 2-3-38. 전자금융사기 피해 경로 (복수응답) - 피싱/파밍/스미싱 금전적 피해 경험자	173
그림 2-3-39. 침해사고 대응활동 수행 (복수응답) - 침해사고 경험자	174
그림 2-3-40. 침해사고 신고 또는 상담 문의 기관/업체 (복수응답) - 침해사고 경험자	175
그림 2-3-41. 침해사고 신고 또는 상담 문의하지 않은 이유 - 신고 또는 상담 문의하지 않은 자	175
그림 2-3-42. 온라인 상 개인정보 제공 목적 (복수응답)	176
그림 2-3-43. 개인정보 침해사고 예방 조치 (복수응답)	177
그림 2-3-44. 개인정보 침해사고 경험	178
그림 2-3-45. 개인정보 침해사고 경험 유형 (복수응답) - 개인정보 침해사고 경험자	178
그림 2-3-46. 개인정보 침해사고 대응활동 수행 (복수응답) - 개인정보 침해사고 경험자	179
그림 2-3-47. 클라우드 서비스 이용	180
그림 2-3-48. 클라우드 서비스 침해사고 예방 조치 (복수응답) - 클라우드 서비스 이용자	180
그림 2-3-49. 빅데이터 활용 서비스 이용	181



그림 2-3-50. 빅데이터 활용 서비스 대중화 시 보안 우려사항 (2가지)	181
그림 2-3-51. 사물인터넷(IoT) 제품 서비스 이용	182
그림 2-3-52. 사물인터넷(IoT) 이용 제품 서비스 유형 (복수응답) - 사물인터넷(IoT) 제품 서비스 이용자	182
그림 2-3-53. 사물인터넷(IoT) 보안을 위한 조치 (복수응답) - 사물인터넷(IoT) 제품 서비스 이용자	183
그림 2-3-54. 사물인터넷(IoT) 대중화 시 보안 우려사항 (2가지)	183
그림 2-3-55. 사물인터넷(IoT)에 추가되어야 하는 보안 기능 (2가지)	184
그림 2-3-56. 간편결제 서비스 이용	184
그림 2-3-57. 간편결제 서비스 보안인증수단 (복수응답) - 간편결제 서비스 이용자	185
그림 2-3-58. 일반결제 대비 간편결제 서비스 보안성 인식 - 간편결제 서비스 이용자	185
그림 2-3-59. 인공지능(AI) 활용 서비스 이용	186
그림 2-3-60. 인공지능(AI) 활용 서비스 이용 유형 (복수응답) - 인공지능(AI) 활용 서비스 이용자	186
그림 2-3-61. 인공지능(AI) 활용 서비스 대중화 시 보안 우려사항 (2가지)	187
그림 2-3-62. 향후 정보보호 지출 계획 분야 (2가지)	187



1부 기업부문

표 1-1-1. 업종 분류 기준	9
표 1-1-2. 종사자 수 1명 이상 사업체 및 네트워크 구축 사업체 현황	10
표 1-1-3. 업종규모별 모집단 분포	11
표 1-1-4. 표본오차별 표본의 크기	12
표 1-1-5. 정보보호 정책 수립률 추정 결과 및 표본오차	17
표 1-1-6. 표본 현황	18

2부 개인부문

표 2-1-1. 표본오차별 표본의 크기	123
표 2-1-2. 정보보호 제품 이용률 추정 결과 및 표본오차	128
표 2-1-3. 모집단 및 표본 현황	129

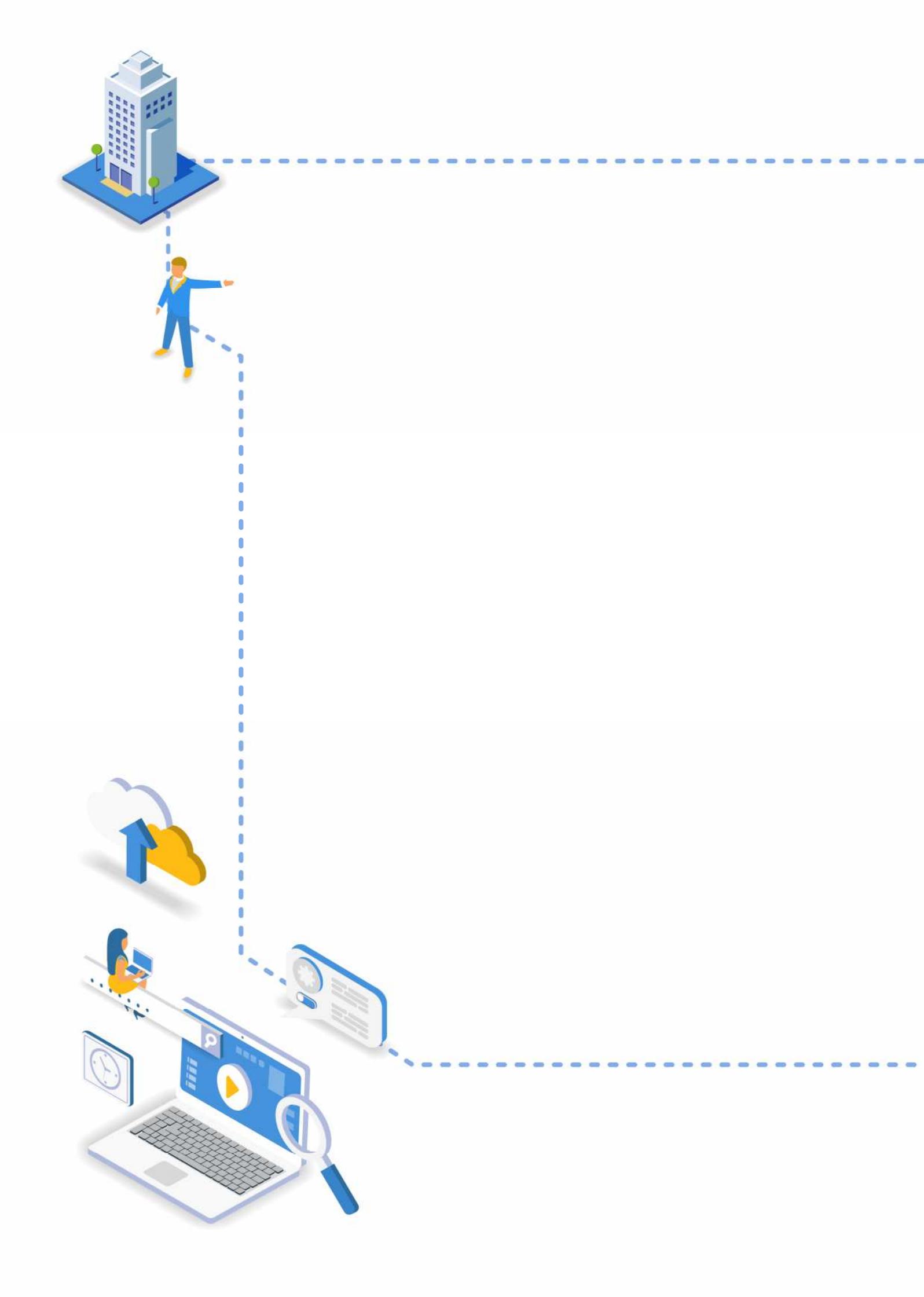


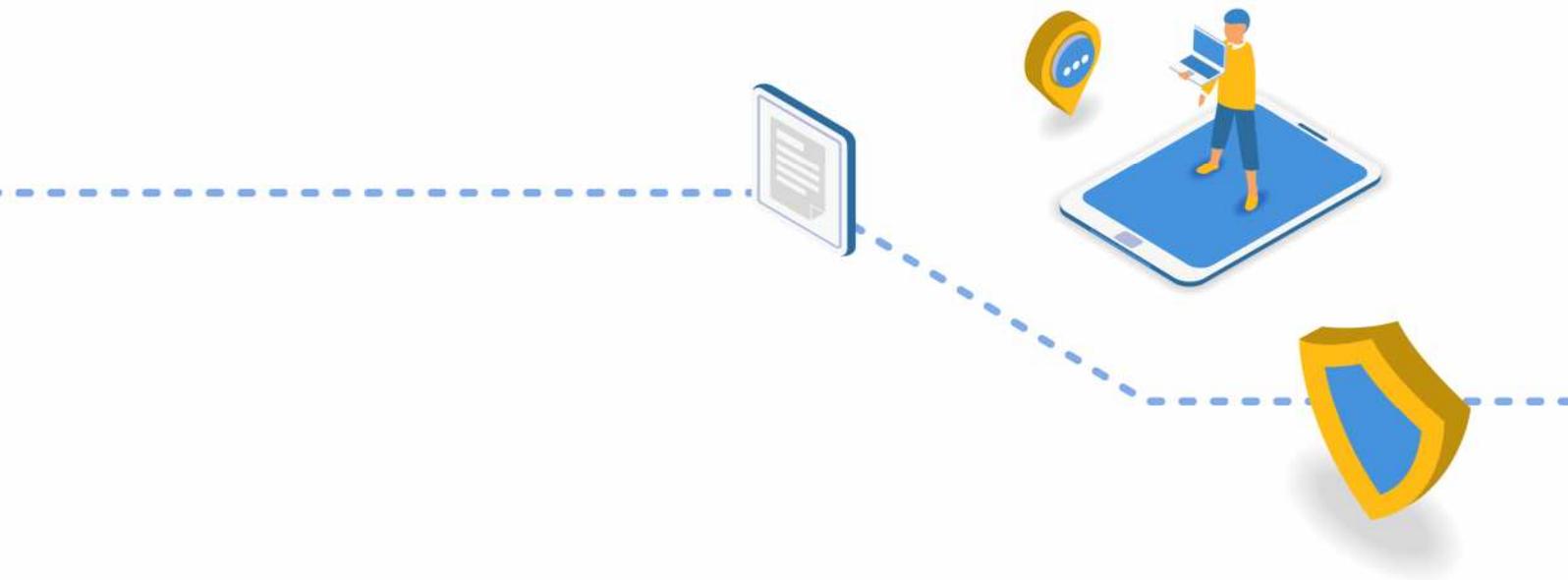


1부

기업부문

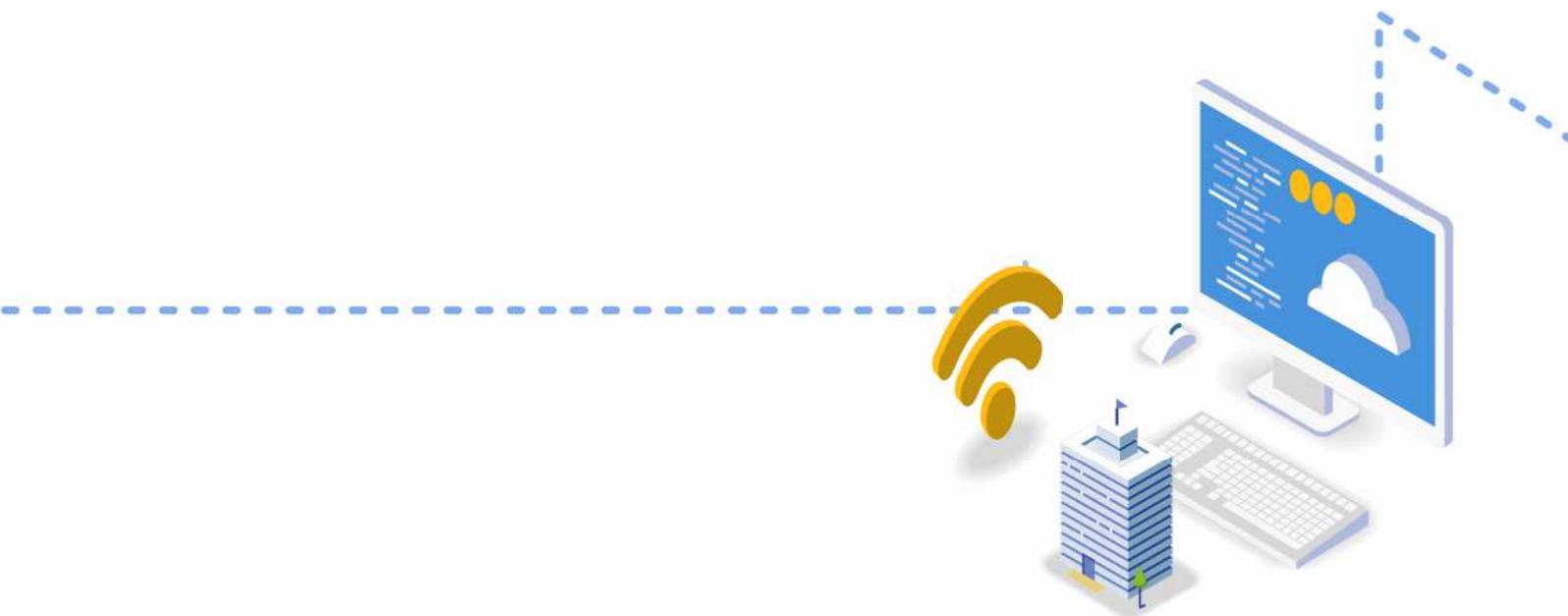






제1장

조사개요



제1장 조사개요

1. 조사 목적

급속하게 변화하는 인터넷 환경과 사물인터넷(IoT), 핀테크, 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 기초 자료를 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

- 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 - 개인정보보호조치 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 정보보호(사이버) 보험
등의 조사항목 추가
- 통계작성기관명 변경(미래창조과학부→과학기술정보통신부)
- 2018년 - ‘2016년 기준 전국사업체조사’와 ‘2017년 정보화통계조사’ 결과를 기반으로
표본 재설계

3. 조사 내용 및 범위

본 조사는 국내 사업체의 정보보호 기반 및 환경, 침해사고 예방, 침해사고 경험 및 대응, 정보 보호 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
- 정보보호(사이버) 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 정보통신 시스템 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 정보통신망 또는 이와 관련한 네트워크 및 시스템이 공격을 당하여 생긴 문제 등을 의미
- **해킹** : 사내 데이터나 전산 시스템에 대한 외부로부터의 비인가 접근

- **랜섬웨어(Ransomware)** : 몸값을 의미하는 'Ransom'과 'Software'의 합성어로 인터넷 사용자의 시스템을 잠그거나 데이터를 사용할 수 없도록 암호화한 뒤에, 그 데이터를 인질로 금전을 요구하는 악성 프로그램을 의미
- **APT 공격** : Advanced Persistent Threat(지능적 지속 위협)의 약자로 정교한 수준의 전문 기술 또는 방대한 리소스를 가진 공격자가 특정 기업 또는 기관을 대상으로 여러 공격 경로를 사용하여 공격하는 것을 의미
- **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
- **정보보호(사이버) 보험** : 기업이 사이버 공간에서 일어난 해킹, DDoS 등의 의도적인 공격으로 인해 겪게 되는 피해를 보장하는 보험
- **SNS 보안** : 사내망을 통해 공개적인 SNS 사용을 하지 못하도록 차단하거나, 기업 내에서만 사용가능한 SNS를 구성하는 것
- **빅데이터 보안** : 방대한 양의 정보들의 집합을 분석·보관하는 작업에서 개인정보 및 기타 중요한 정보들이 외부로 유출되지 않도록 비식별화, 암호화 등의 설정을 하는 것

5. 조사 체계

- 조사대상 : 종사자 수 1인 이상, 네트워크에 연결된 컴퓨터 보유 사업체
- 유효응답업체수 : 9,081개
- 조사주기 : 연 1회
- 조사기간 : 2018년 7월 23일 ~ 10월 22일 (3개월)
- 조사방법 : 사업체 방문 면접조사(이메일, 팩스 등 병행)
- 조사기관
 - 주관기관 : 과학기술정보통신부(Ministry of Science and ICT)
 - 전담기관 : 한국인터넷진흥원(Korea Internet & Security Agency)
- 법적근거
 - 정보통신망이용촉진 및 정보보호 등에 관한 법률 제52조 제3항
 - 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 『2016년 기준 전국사업체조사』의 업종별, 규모별 사업체 수 및 분포 결과와 한국정보화진흥원 『2017년 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

국제기구 분류기준 (ISIC ver 4.0)	한국표준산업분류 (9차 개정)	업종 분류기준 (본조사)
-	A. 농업, 임업 및 어업 B. 광업	1. 농림수산업(광업포함)
제조업(ISIC C)	C. 제조업	2. 제조업
건설업(ISIC F)	F. 건설업	3. 건설업
도소매업(ISIC G); 자동차 및 모터사이클 수리업	G. 도매 및 소매업	4. 도매 및 소매업
운수업(ISIC H)	H. 운수업	5. 운수업
숙박 및 음식점업(ISIC I)	I. 숙박 및 음식점업	6. 숙박 및 음식점업
정보통신업(ISIC J)	J. 출판, 영상, 방송 통신 및 정보서비스업	7. 출판, 영상, 방송 통신 및 정보서비스업
-	K. 금융 및 보험업	8. 금융 및 보험업
부동산업(ISIC L)	L. 부동산업 및 임대업	9. 부동산업 및 임대업
전문, 과학 및 기술서비스업 (M75 수의업 제외)	M. 전문, 과학 및 기술서비스업	10. 전문, 과학 및 기술서비스업
사업관리 및 지원서비스업(ISIC N)	N. 사업시설관리 및 사업지원 서비스업	11. 사업시설관리 및 사업지원 서비스업
기타 서비스업 (ISIC S, S95 수리업 포함) - ISIC S94 협회 및 단체 - ISIC S95 컴퓨터, 개인 및 가정용품 수리업 포함 - ISIC S96 기타 개인서비스업	S. 협회 및 단체, 수리 및 기타 개인서비스업	12. 협회, 단체, 수리 및 기타 개인서비스업
	D. 전기, 가스, 증기 및 수도사업	13. 기타 (한국표준산업분류 중 좌변의 대분류에 해당하는 산업, 단 0는 제외)
	E. 하수·폐기물 처리, 원료재생 및 환경복원업	
	O. 공공행정, 국방 및 사회보장 행정	
	P. 교육 서비스업	
	Q. 보건업 및 사회복지서비스업	
R. 예술, 스포츠 및 여가관련 서비스업		

→ 모집단 분포

- 통계청 『2016년 기준 전국사업체조사』 및 한국정보화진흥원 『2017년 정보화통계조사』에서 조사된 사업체 중 종사자 수 1명 이상 사업체 현황 및 분포는 다음과 같이 나타남

표 1-1-2 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)	5,644	2,285
	2. 제조업	416,493	117,271
	3. 건설업	136,074	57,129
	4. 도매 및 소매업	1,019,388	333,101
	5. 운수업	385,837	121,893
	6. 숙박 및 음식점업	729,395	197,702
	7. 출판, 영상, 방송 통신 및 정보서비스업	42,472	24,003
	8. 금융 및 보험업	42,710	35,957
	9. 부동산업 및 임대업	158,882	66,271
	10. 전문, 과학 및 기술서비스업	102,713	59,398
	11. 사업시설관리 및 사업지원 서비스업	52,008	20,391
	12. 협회, 단체, 수리 및 기타 개인서비스업	406,993	109,754
	13. 기타	439,131	214,974
규모별	1~4명	3,171,375	926,337
	5~9명	453,228	226,277
	10~49명	265,776	170,026
	50~249명	42,900	33,662
	250~999명	3,915	3,346
	1,000명 이상	546	481
전체		3,937,740	1,360,129

※ 출처: 2016년 기준 전국사업체조사(통계청), 2017년 정보화통계조사(한국정보화진흥원)

표 1-1-3

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	834	0.06	금융 및 보험업	1~4명	8,050	0.59
	5~9명	560	0.04		5~9명	9,654	0.71
	10~49명	790	0.06		10~49명	16,432	1.21
	50~249명	96	0.01		50~249명	1,644	0.12
	250~999명	5	0.0004		250~999명	149	0.01
	1,000명 이상	-	0.00		1,000명 이상	28	0.002
제조업	1~4명	47,041	3.46	부동산업 및 임대업	1~4명	51,123	3.76
	5~9명	30,774	2.26		5~9명	9,381	0.69
	10~49명	31,347	2.30		10~49명	5,375	0.40
	50~249명	7,166	0.53		50~249명	345	0.03
	250~999명	828	0.06		250~999명	41	0.003
	1,000명 이상	115	0.01		1,000명 이상	6	0.0004
건설업	1~4명	25,262	1.86	전문, 과학 및 기술 서비스업	1~4명	30,625	2.25
	5~9명	16,781	1.23		5~9명	17,098	1.26
	10~49명	13,020	0.96		10~49명	9,599	0.71
	50~249명	1,709	0.13		50~249명	1,708	0.13
	250~999명	318	0.02		250~999명	321	0.02
	1,000명 이상	39	0.003		1,000명 이상	47	0.003
도매 및 소매업	1~4명	262,776	19.32	사업시설 관리 및 사업지원 서비스업	1~4명	10,251	0.75
	5~9명	44,113	3.24		5~9명	3,054	0.22
	10~49명	23,361	1.72		10~49명	4,829	0.36
	50~249명	2,647	0.19		50~249명	1,717	0.13
	250~999명	195	0.01		250~999명	490	0.04
	1,000명 이상	9	0.001		1,000명 이상	50	0.004
운수업	1~4명	107,874	7.93	협회, 단체, 수리 및 기타 개인 서비스업	1~4명	91,297	6.71
	5~9명	5,307	0.39		5~9명	10,304	0.76
	10~49명	6,213	0.46		10~49명	7,344	0.54
	50~249명	2,333	0.17		50~249명	786	0.06
	250~999명	158	0.01		250~999명	22	0.002
	1,000명 이상	8	0.001		1,000명 이상	1	0.0001
숙박 및 음식점업	1~4명	157,168	11.56	기타 (공공행정, 사회보장, 행정제외)	1~4명	124,530	9.16
	5~9명	28,798	2.12		5~9명	44,245	3.25
	10~49명	10,783	0.79		10~49명	34,447	2.53
	50~249명	908	0.07		50~249명	11,020	0.81
	250~999명	41	0.003		250~999명	577	0.04
	1,000명 이상	4	0.0003			155	0.01
출판, 영상 방송통신 및 정보 서비스업	1~4명	9,506	0.70				
	5~9명	6,208	0.46				
	10~49명	6,486	0.48				
	50~249명	1,583	0.12				
	250~999명	201	0.01				
	1,000명 이상	19	0.001				
총 합계						1,360,129	100.00

* 출처: 2016년 기준 전국사업체조사(통계청), 2017년 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 1-1-4

표본오차별 표본의 크기

(단위 : 개, %)

표본의 크기	10,800	10,575	10,358	10,146	9,942	9,743	9,550	7,900
표본오차	0.94	0.95	0.96	0.97	0.98	0.99	1.00	1.10

- 최종 표본의 크기는 표본오차가 1% 내외가 되도록 9,000개 내외로 결정함

- 표집틀(Sampling frame)
 - 1차 표집틀 : 『2016년 기준 전국사업체조사』 대상 사업체
 - 2차 표집틀 : 『2017년 정보화통계조사』 대상 사업체 중 1인 이상 네트워크 구축 사업체
- 표본할당 및 추출방법
 - 역등할당(Power allocation) : 2017년도 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
 - 2018년 7월 23일 ~ 10월 22일 (3개월)
- 조사기준 시점
 - 2017년 12월 31일
 - 교육 실시, 예산 및 지출, 침해사고 경험은 2017년 1월 1일 ~ 12월 31일
 - 현재 투자/계획하는 IT 보안분야는 2018년 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 최종결과를 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

$$\hat{Y} = \sum_{h=1}^L cY_h + \sum_{h=1}^L \frac{sN_h}{s n_h} \sum_{k=1}^{s n_h} y_{hsk}$$

여기에서 cY_h : 전수층 총계

L : 층의 개수 (업종×규모)

sN_h : 표본층 h 의 모집단 크기

$s n_h$: 표본층 h 의 표본 크기

y_{hsk} : 표본층 h 의 k 번째 관찰값

$\frac{sN_h}{s n_h}$: 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

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

다. 표본오차

→ 모집단 총계의 분산 및 표본오차 추정

- 모총계 추정량에 대한 분산 추정(표본층에서만 표본오차가 발생)

$$\begin{aligned} \widehat{Var}(\hat{Y}) &= \widehat{Var}\left(\sum_{h=1}^L \frac{sN_h}{s n_h} \sum_{k=1}^{n_h} y_{hsk}\right) \\ &= \sum_{h=1}^L \left(\frac{sN_h}{s n_h}\right)^2 \frac{1}{s n_h - 1} \sum_{k=1}^{n_h} (s y_{hk} - \bar{s} y_h)^2 \end{aligned}$$

→ 모비율의 분산 및 표본오차 추정

- 표본층에서만 표본오차가 발생

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

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

$s \hat{p}_h$: h 층에서 표본 비율

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

표 1-1-5

정보보호 정책 수립률 추정 결과 및 표본오차

정보보호 정책 수립률 표본오차	$\pm 0.72\%p$ (95% 신뢰수준)
정보보호 정책 수립률 추정 결과	$14.45\% \pm 0.72\%p$

10. 결과 공표 및 활용분야

- 『2018년 정보보호 실태조사(기업부문)』 보고서는 한국인터넷진흥원 홈페이지(<https://www.kisa.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. 표본 현황

표 1-1-6

표본 현황

(단위 : 개, %)

업종분류	규모 분류	컴퓨터 보유/ 네트워크 구축 사업체		조사표본 사업체	
		사업체 수	비율	사업체 수	비율
농림수산업	1~4명	834	0.06	105	1.16
	5~9명	560	0.04	25	0.28
	10~49명	790	0.06	103	1.13
	50~249명	96	0.01	50	0.55
	250~999명	5	0.0004	4	0.04
	1,000명 이상	0	0.00	0	0.00
제조업	1~4명	47,041	3.46	180	1.98
	5~9명	30,774	2.26	126	1.39
	10~49명	31,347	2.30	292	3.22
	50~249명	7,166	0.53	278	3.06
	250~999명	828	0.06	187	2.06
	1,000명 이상	115	0.01	70	0.77
건설업	1~4명	25,262	1.86	175	1.93
	5~9명	16,781	1.23	94	1.04
	10~49명	13,020	0.96	183	2.02
	50~249명	1,709	0.13	172	1.89
	250~999명	318	0.02	144	1.59
	1,000명 이상	39	0.003	31	0.34
도매 및 소매업	1~4명	262,776	19.32	246	2.71
	5~9명	44,113	3.24	138	1.52
	10~49명	23,361	1.72	227	2.50
	50~249명	2,647	0.19	185	2.04
	250~999명	195	0.01	96	1.06
	1,000명 이상	9	0.001	3	0.03
운수업	1~4명	107,874	7.93	86	0.95
	5~9명	5,307	0.39	63	0.69
	10~49명	6,213	0.46	203	2.24
	50~249명	2,333	0.17	182	2.00
	250~999명	158	0.01	73	0.80
	1,000명 이상	8	0.001	7	0.08
숙박 및 음식점업	1~4명	157,168	11.56	203	2.24
	5~9명	28,798	2.12	115	1.27
	10~49명	10,783	0.79	159	1.75
	50~249명	908	0.07	129	1.42
	250~999명	41	0.003	37	0.41
	1,000명 이상	4	0.0003	3	0.03

(계속→)

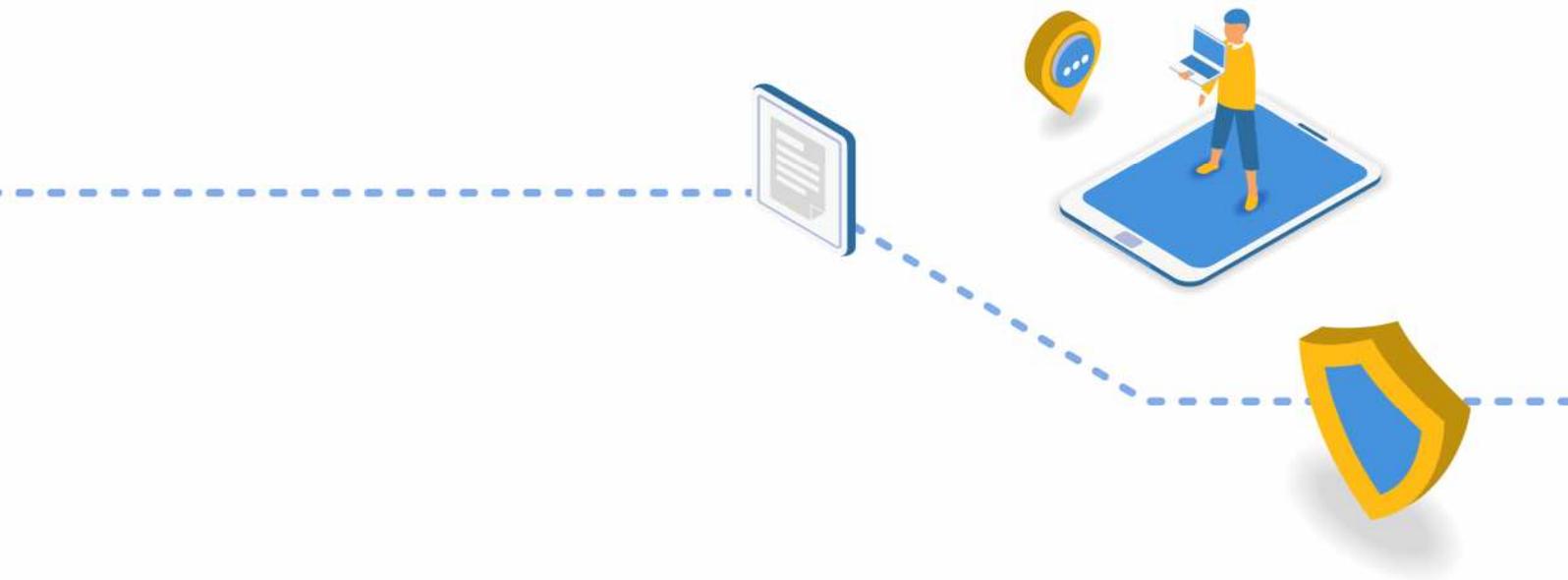
표 1-1-6

표본 현황

(단위 : 개, %)

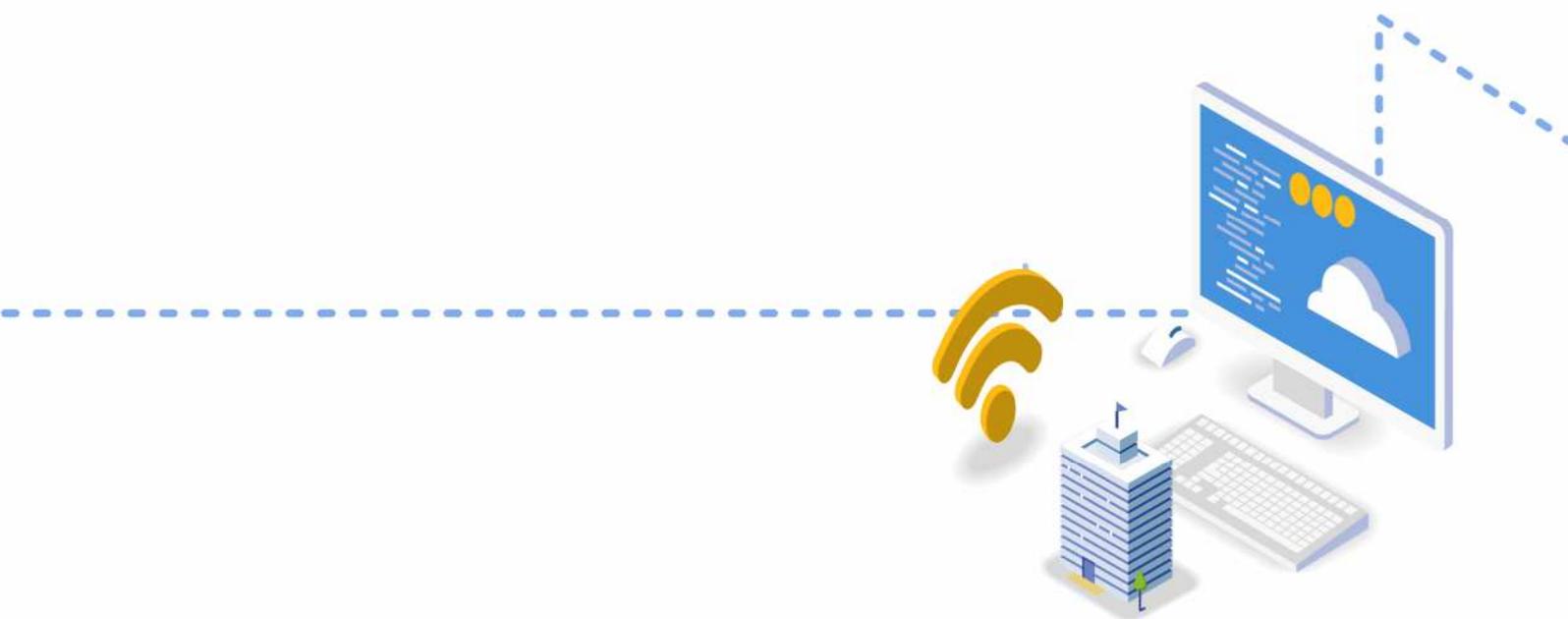
업종분류	규모 분류	컴퓨터 보유/ 네트워크 구축 사업체		조사표본 사업체	
		사업체 수	비율	사업체 수	비율
출판, 영상, 방송 통신 및 정보서비스업	1~4명	9,506	0.70	179	1.97
	5~9명	6,208	0.46	65	0.72
	10~49명	6,486	0.48	169	1.86
	50~249명	1,583	0.12	158	1.74
	250~999명	201	0.01	86	0.95
	1,000명 이상	19	0.001	4	0.04
금융 및 보험업	1~4명	8,050	0.59	177	1.95
	5~9명	9,654	0.71	88	0.97
	10~49명	16,432	1.21	213	2.35
	50~249명	1,644	0.12	156	1.72
	250~999명	149	0.01	60	0.66
	1,000명 이상	28	0.002	14	0.15
부동산업 및 임대업	1~4명	51,123	3.76	189	2.08
	5~9명	9,381	0.69	88	0.97
	10~49명	5,375	0.40	173	1.91
	50~249명	345	0.03	97	1.07
	250~999명	41	0.003	25	0.28
	1,000명 이상	6	0.0004	4	0.04
전문, 과학 및 기술서비스업	1~4명	30,625	2.25	181	1.99
	5~9명	17,098	1.26	116	1.28
	10~49명	9,599	0.71	218	2.40
	50~249명	1,708	0.13	161	1.77
	250~999명	321	0.02	123	1.35
	1,000명 이상	47	0.003	17	0.19
사업 시설관리 및 사업지원 서비스업	1~4명	10,251	0.75	171	1.88
	5~9명	3,054	0.22	48	0.53
	10~49명	4,829	0.36	132	1.45
	50~249명	1,717	0.13	165	1.82
	250~999명	490	0.04	172	1.89
	1,000명 이상	50	0.004	37	0.41
협회 및 단체, 수리 및 기타 개인서비스업	1~4명	91,297	6.71	172	1.89
	5~9명	10,304	0.76	84	0.93
	10~49명	7,344	0.54	156	1.72
	50~249명	786	0.06	111	1.22
	250~999명	22	0.002	16	0.18
	1,000명 이상	1	0.0001	1	0.01
기타	1~4명	124,530	9.16	117	1.29
	5~9명	44,245	3.25	74	0.81
	10~49명	34,447	2.53	166	1.83
	50~249명	11,020	0.81	149	1.64
	250~999명	577	0.04	95	1.05
	1,000명 이상	155	0.01	80	0.88
합계		1,360,129	100.00	9,081	100.00





제2장

조사결과 요약



I

정보보호 인식



정보보호 중요성 인식 90.2%, 개인정보보호 중요성 인식 89.3%

- ▶ 네트워크에 연결된 컴퓨터 보유 사업체의 대부분이 정보보호 및 개인정보보호가 중요하다고 응답함
 - '정보보호가 중요하다(중요한 편이다 + 매우 중요하다)'고 인식하는 비율은 90.2%로 나타남
 - '개인정보보호가 중요하다(중요한 편이다 + 매우 중요하다)'고 인식하는 비율은 89.3%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 16.0%는 '정보보호 또는 개인정보보호' 정책 수립

- ▶ 사업체의 16.0%는 정보보호 또는 개인정보보호 정책을 수립하는 것으로 조사되었고, 전년(15.2%) 대비 0.8%p 증가함
- ▶ 규모별로 '종사자수 250인 이상(90.9%)' 사업체의 정책 수립률이 가장 높게 나타남 또한, '종사자수 10-49인(47.2%, 9.8%p↑)'과 '종사자수 50-249인(78.2%, 9.9%p↑)'에서 정책 수립률이 전년 대비 증가함

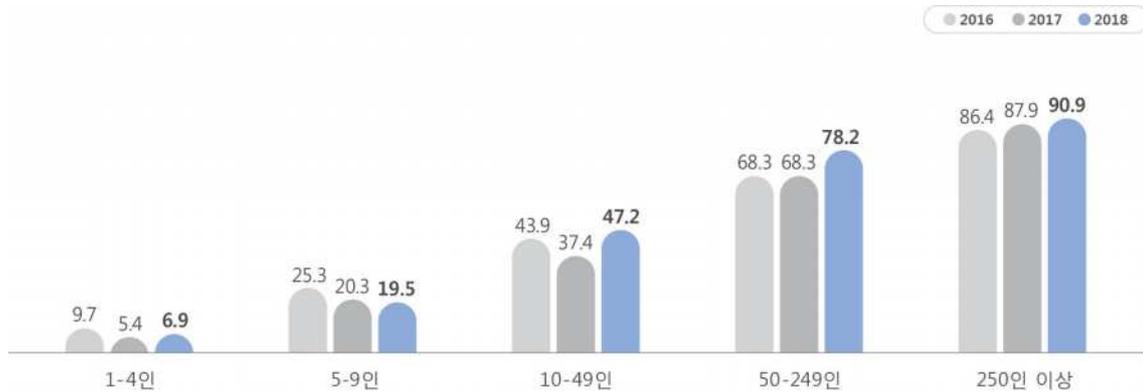
그림 1-2-2 정보보호(개인정보보호) 정책 수립률

(단위 : %)



그림 1-2-3 규모별 정보보호(개인정보보호) 정책 수립률

(단위 : %)



2. 정보보호(개인정보보호) 조직



‘정보보호 또는 개인정보보호’ 조직 보유 5.5%, 전년 대비 4.4%p 감소

- ▶ 공식적인 정보보호 또는 개인정보보호 조직을 보유한 사업체의 비율은 5.5%로, 전년 (9.9%) 대비 4.4%p 감소함
- ▶ 사업체의 정보보호(개인정보보호) 조직 보유율은 종사자 규모 전층에서 전년 대비 감소함

그림 1-2-4

정보보호(개인정보보호) 조직 보유율

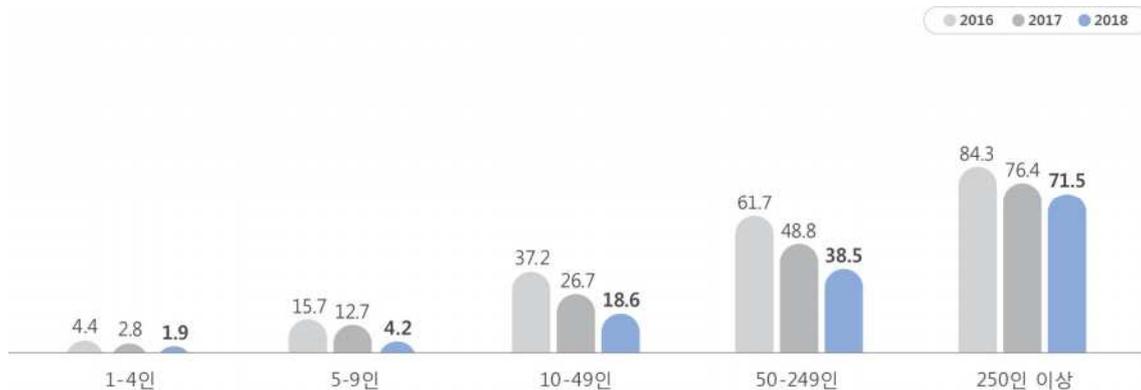
(단위 : %)



그림 1-2-5

규모별 정보보호(개인정보보호) 조직 보유율

(단위 : %)



3. 정보보호(개인정보보호) 교육



사업체의 28.0%는 '정보보호 또는 개인정보보호' 교육 실시

- ▶ 2017년 1년 간 임직원 대상으로 정보보호 또는 개인정보보호 교육을 실시한 비율은 28.0%로 전년(30.4%) 대비 2.4%p 감소함
- ▶ 규모별로 '종사자수 250인 이상(97.0%)' 사업체의 교육 실시율이 가장 높게 나타남 또한, '종사자수 10-49인(75.0%, 8.9%p↑)'과 '종사자수 250인 이상(97.0%, 6.1%p↑)'에서 교육 실시율이 전년 대비 증가함

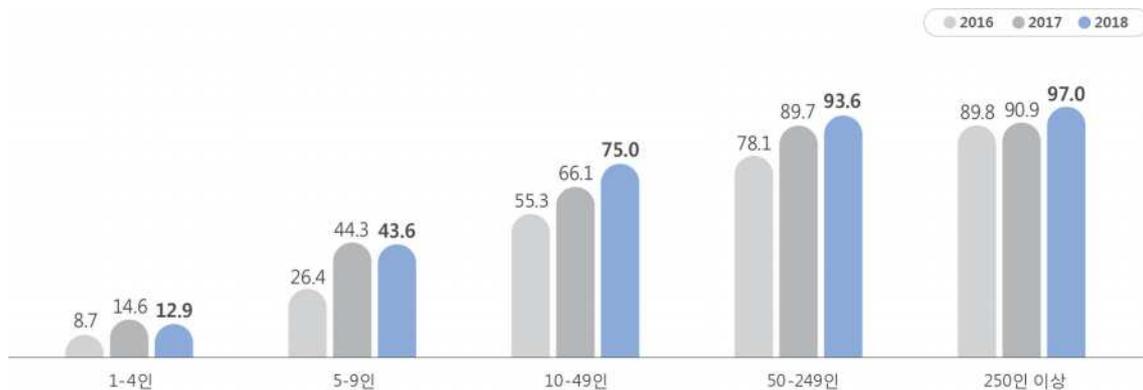
그림 1-2-6 정보보호(개인정보보호) 교육 실시율

(단위 : %)



그림 1-2-7 규모별 정보보호(개인정보보호) 교육 실시율

(단위 : %)



4. 정보보호(개인정보보호) 예산



'정보보호 또는 개인정보보호' 예산 편성 36.2%, 전년 대비 11.9%p 감소

- ▶ 2017년 1년 간 사업체의 36.2%는 IT 예산 중 정보보호 또는 개인정보보호 예산을 편성함
- ▶ IT 예산 중 정보보호 또는 개인정보보호 예산이 차지하는 비중은 '1% 미만(25.2%)'이 가장 높았으나, 전년(36.8%) 대비 11.6%p 감소함

그림 1-2-8

정보보호(개인정보보호) 예산 편성률

(단위 : %)

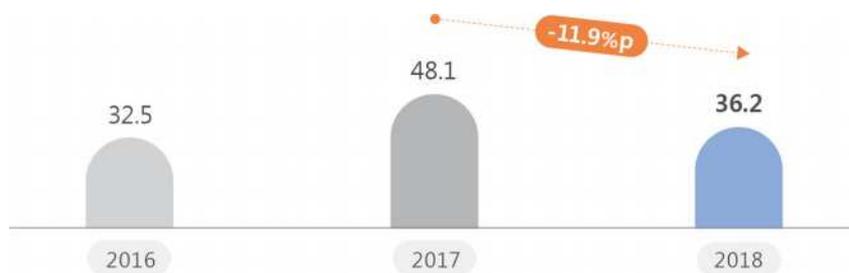


그림 1-2-9

IT 예산 중 정보보호(개인정보보호) 예산 비중

(단위 : %)



Ⅲ

침해사고 예방



1. 정보보호 제품 및 서비스

가. 정보보호 제품 이용

‘정보보호 제품 이용’ 90.9%, 전년 대비 4.0%p 감소

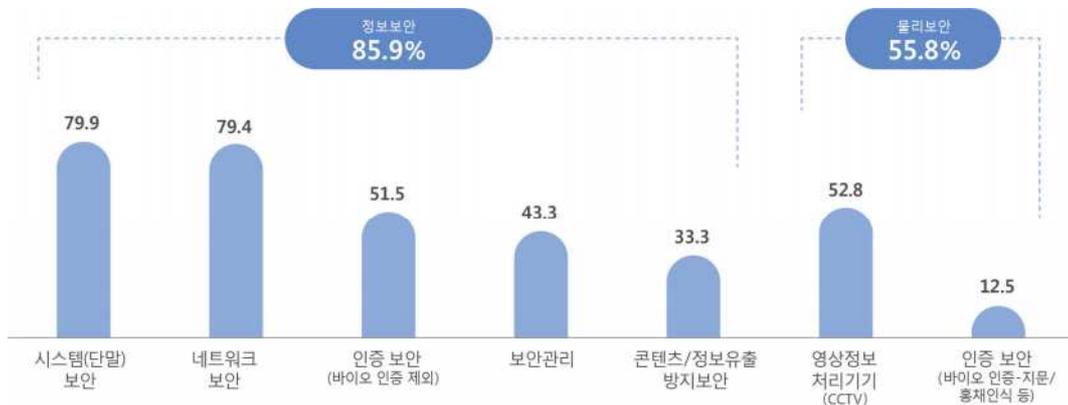
- ▶ 사업체의 90.9%는 정보보호 제품을 이용하는 것으로 조사되었고, 전년(94.9%) 대비 4.0%p 감소함
- ▶ 제품군별로는 정보보안 제품 중 ‘시스템(단말) 보안’이 79.9%로 가장 높았고, 물리보안 제품 중에서는 ‘영상정보 처리기기(CCTV)’가 52.8%로 높게 나타남

그림 1-2-10 | 정보보호 제품 이용률



(단위 : %)

그림 1-2-11 | 정보보호 제품군별 이용률 (복수응답)



(단위 : %)

나. 정보보호 서비스 이용



‘정보보호 서비스 이용’ 59.4%, 전년 대비 10.9%p 증가

- ▶ 사업체의 59.4%는 ‘정보보호 서비스를 이용’하는 것으로 조사되었고, 전년(48.5%) 대비 10.9%p 증가함
 - 2016년 40.5%, 2017년 48.5%, 2018년 59.4%로 증가 추세임
- ▶ 서비스 유형별로는 ‘유지관리’가 38.3%로 가장 많았고, 다음으로 ‘인증서비스(29.3%)’, ‘교육/훈련(16.6%)’ 등의 순으로 조사됨
 - 특히, ‘인증서비스’는 다른 서비스와 비교했을 때 전년(9.0%) 대비 크게 증가함

그림 1-2-12 정보보호 서비스 이용률

(단위 : %)

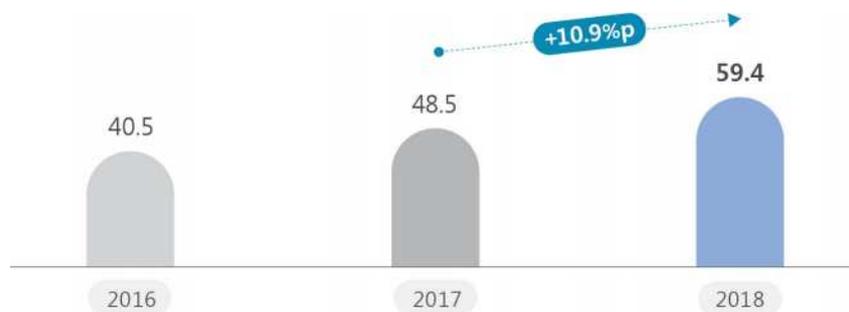
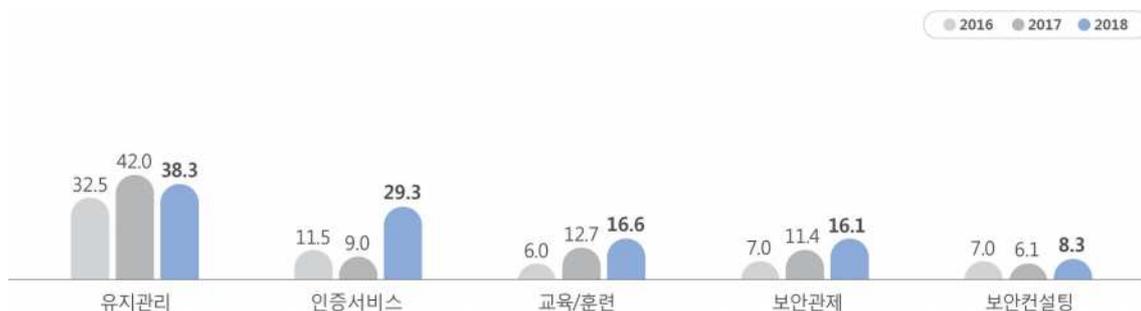


그림 1-2-13 정보보호 서비스 유형별 이용률 (복수응답)

(단위 : %)



2. 정보보호 관리

가. 시스템 및 네트워크 보안점검



사업체의 90.0%는 '시스템 및 네트워크 보안점검' 실시

- ▶ '시스템 및 네트워크에 대한 보안점검' 실시율은 90.0%로 전년(64.7%) 대비 25.3%p 증가함
 - 특히, 비정기적으로 보안점검을 실시하는 사업체는 67.1%로, 전년(42.3%) 대비 24.8%p 증가한 것으로 나타남
- ▶ 유형별로는 'PC의 취약점' 점검률이 99.0%로 가장 높고, 다음으로 '물리보안(55.4%)', '서버 운영체제(OS)(50.7%)' 등의 순으로 조사됨

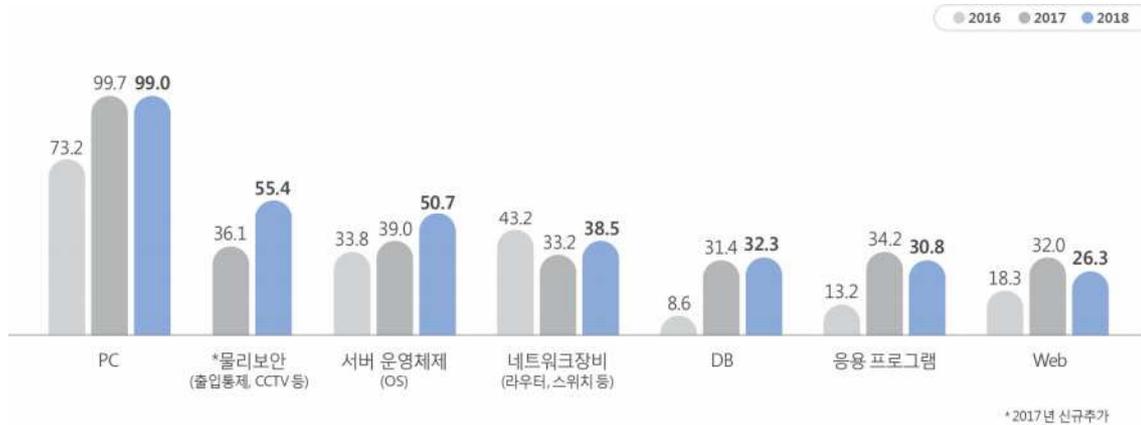
그림 1-2-14 시스템 및 네트워크 보안점검 실시율

(단위 : %)



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

(단위 : %)



나. 보안패치 적용



‘보안패치’ 적용 90.7%, 전년 대비 6.2%p 감소

- ▶ 사업체의 90.7%는 PC나 서버에 보안패치를 적용하는 것으로 조사되었고, 전년(96.9%) 대비 6.2%p 감소함
- ▶ 보안패치 유형별로는 ‘정보보호 시스템’에 적용하는 비율이 97.3%로 가장 높았고, 다음으로 ‘내부에서 이용하는 서버(95.5%)’ 등의 순으로 조사됨

그림 1-2-16

보안패치 적용률

(자동 + 수동 + 문제 발생 시에만 업데이트, 단위 : %)

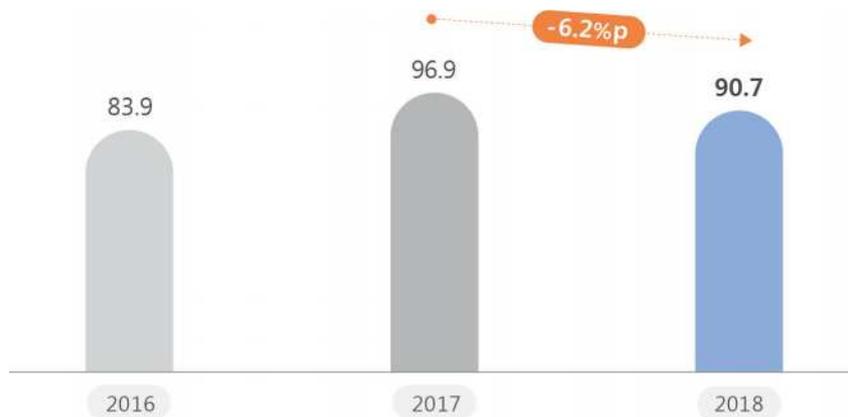
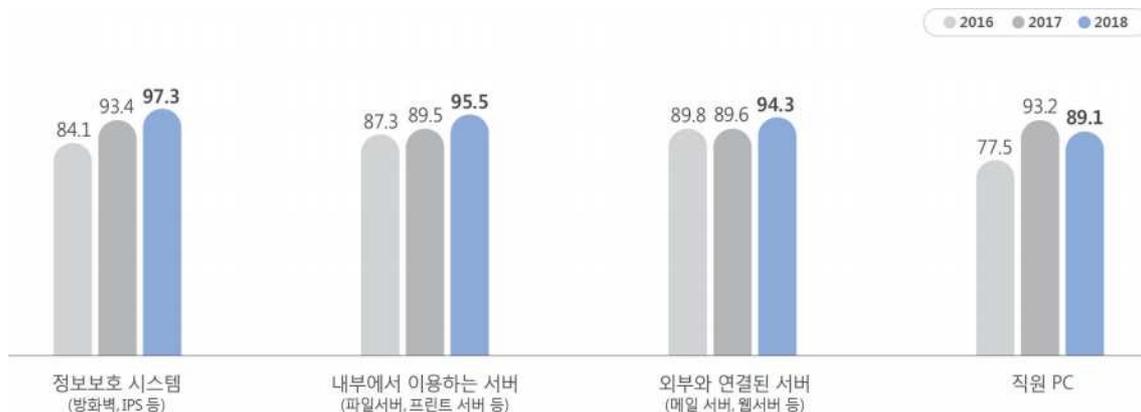


그림 1-2-17

보안패치 유형별 적용률 (복수응답) - 항목별 제품 보유 사업체

(자동 + 수동 + 문제 발생 시에만 업데이트, 단위 : %)



다. 시스템 로그 및 데이터 백업 실시



‘시스템 로그 또는 데이터 백업’ 실시 49.8%

- ▶ 사업체의 49.8%는 시스템 로그 또는 중요 데이터를 백업하는 것으로 나타났고, 전년 (52.5%) 대비 2.7%p 감소함
- ▶ 유형별로 ‘시스템 로그 백업’ 실시율은 30.5%, ‘중요 데이터 백업’은 47.3%로 나타남
- ‘중요데이터’ 백업률은 2016년 35.5%, 2017년 46.8%, 2018년 47.3%로 증가 추세임

그림 1-2-18

백업 실시율

(단위 : %)

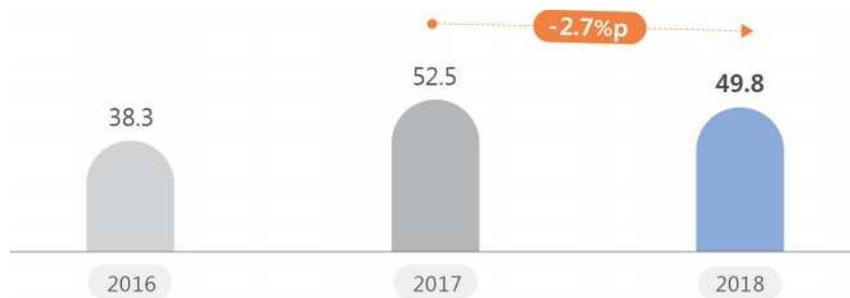
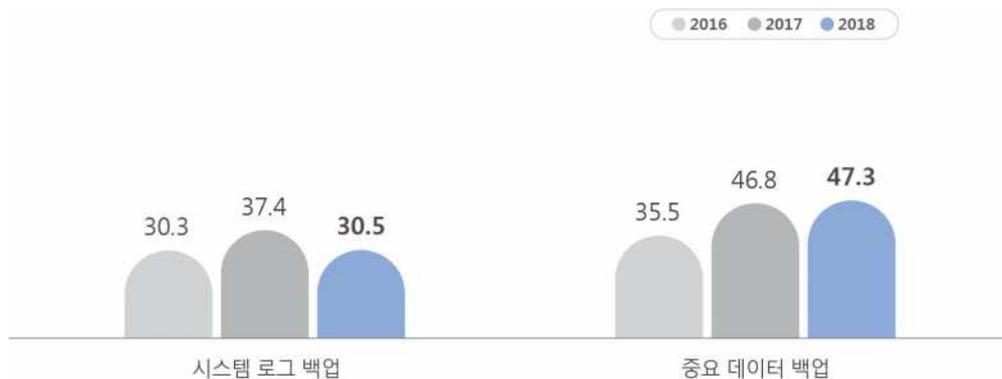


그림 1-2-19

백업 유형별 실시율 (복수응답)

(단위 : %)



M

침해사고 대응



1. 침해사고 경험



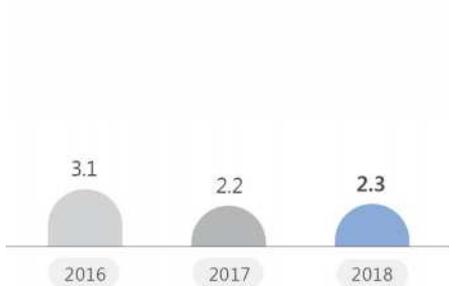
사업체의 2.3%가 침해사고 경험

- ▶ 2017년 1년 간 사업체의 2.3%는 해킹, 악성코드, DDoS, 랜섬웨어 등 침해사고를 경험함
- 침해사고는 '경미한 피해(69.2%)'가 가장 많았음
- ▶ 침해사고 경험 유형으로는 '랜섬웨어'가 56.3%로 가장 많았고, 다음으로 '악성코드(컴퓨터 바이러스, 웜, 트로이잔 등에 의한 공격(47.7%)', '애드웨어/스파이웨어 감염(12.1%)' 등의 순임

그림 1-2-20 | 침해사고 경험 및 피해 심각성 정도

(단위 : %)

✓ 침해사고 경험률

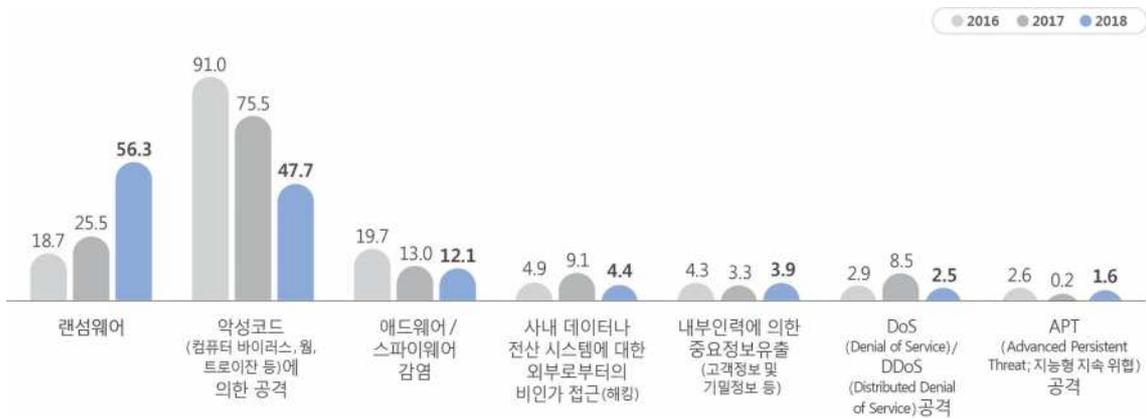


✓ 침해사고 피해 심각성 정도



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

(단위 : %)



2. 침해사고 대응



침해사고 대응활동 수행 17.4%, 전년 대비 8.5%p 감소

- ▶ 사업체의 17.4%는 침해사고에 대응하기 위한 활동을 수행하는 것으로 조사되었고, 수행률은 전년(25.9%) 대비 8.5%p 감소함
- ▶ 대응활동 유형으로는 '침해사고 발생 또는 발생 징후 인지 시 대처를 위한 긴급연락체계 구축'이 10.9%로 가장 많았고, 다음으로 '침해사고 대응 계획 수립(7.8%)', '침해사고대응팀 (CERT) 구축 및 운영(5.1%)' 등의 순으로 나타남

그림 1-2-22

침해사고 대응활동 수행률

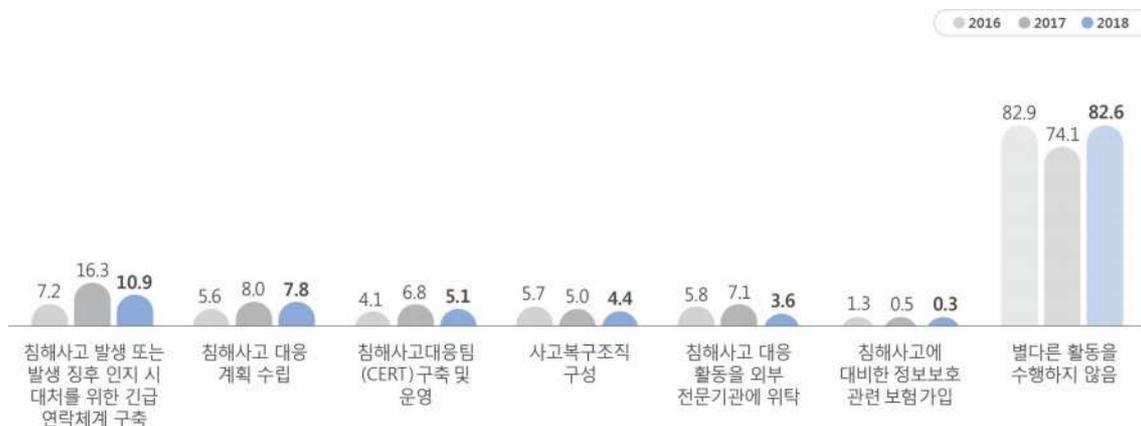
(단위 : %)



그림 1-2-23

침해사고 대응활동 수행 (복수응답)

(단위 : %)



V

개인정보보호



1. 개인정보 수집 및 이용



고객의 개인정보 수집(42.0%) 및 이용(40.2%)은 전년 대비 감소

- ▶ 사업체의 42.0%는 고객의 개인정보를 온라인 또는 오프라인으로 수집하는 것으로 조사되었고, 개인정보 수집률은 전년(47.4%) 대비 5.4%p 감소함
- ▶ 고객의 개인정보를 온라인 또는 오프라인으로 이용하는 비율은 사업체의 40.2%로 전년(45.5%) 대비 5.3%p 감소함

그림 1-2-24

고객 개인정보 수집률

(단위 : %)

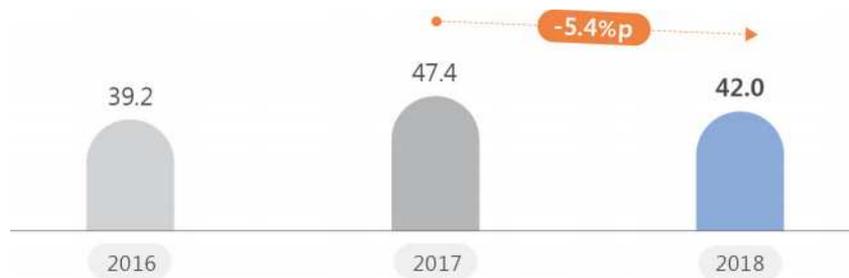
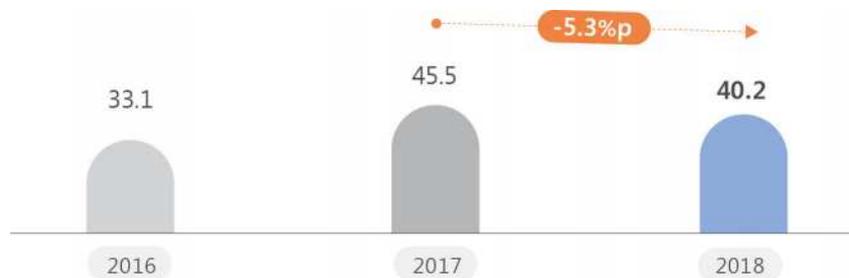


그림 1-2-25

고객 개인정보 이용률

(단위 : %)



2. 개인정보 침해사고 예방

가. 관리적 조치



개인정보 침해사고 예방을 위한 관리적 조치 92.7%, 전년 대비 7.6%p 증가

- ▶ 개인정보 침해사고 예방 및 사후 처리를 위한 관리적 조치 시행률은 92.7%로 전년(85.1%) 대비 7.6%p 증가함
- ▶ 관리적 조치로는 '개인정보 침해사고 예방에 관한 매뉴얼 수립'이 77.2%로 가장 많았고, 다음으로 '개인정보 침해사고 사후 처리방침 수립(54.7%)'이 많은 것으로 나타남

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

(단위 : %)

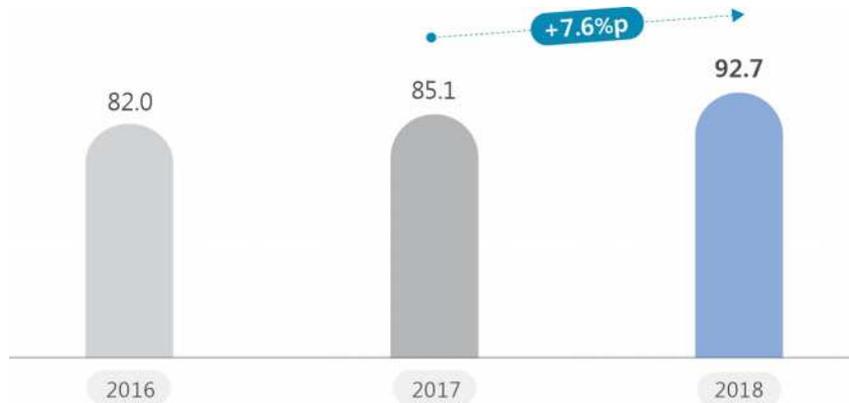
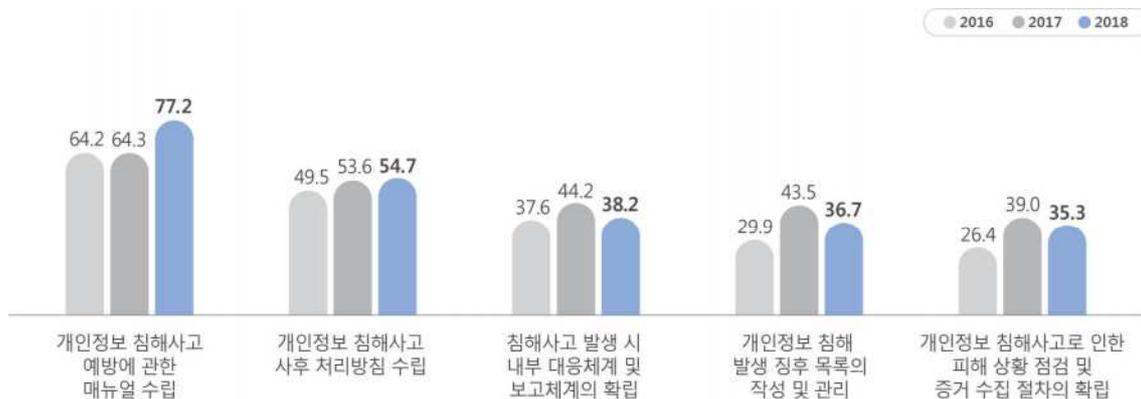


그림 1-2-27 개인정보 침해사고 예방 관리적 조치 (복수응답) - 온라인으로 개인정보 수집 사업체

(단위 : %)



* 응답비율 상위 5개 항목만 포함

나. 기술적 조치



개인정보 기술적 조치 도입 96.9%, 전년 대비 11.3%p 증가

- ▶ 개인정보의 안전한 처리를 위한 기술적 조치 시행률은 96.9%로 전년(85.6%) 대비 11.3%p 증가함
- ▶ 기술적 조치로는 '백신 소프트웨어의 설치·운영 등 컴퓨터 바이러스에 의한 침해 방지 조치'가 75.3%로 가장 높게 조사되었고, 매년 증가하는 추세임

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

(단위 : %)

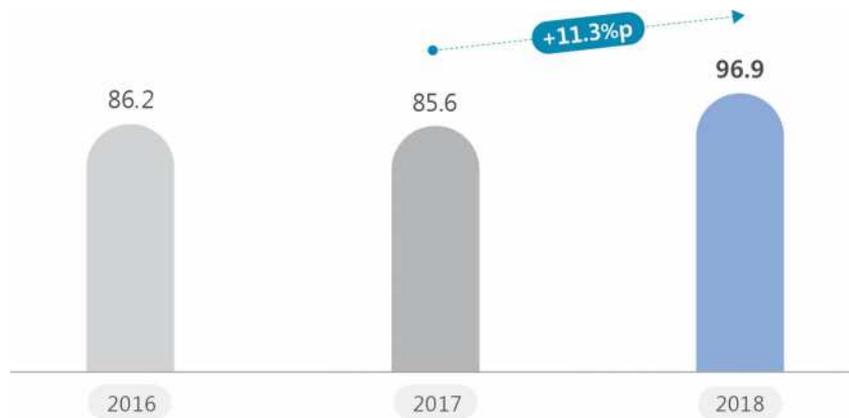
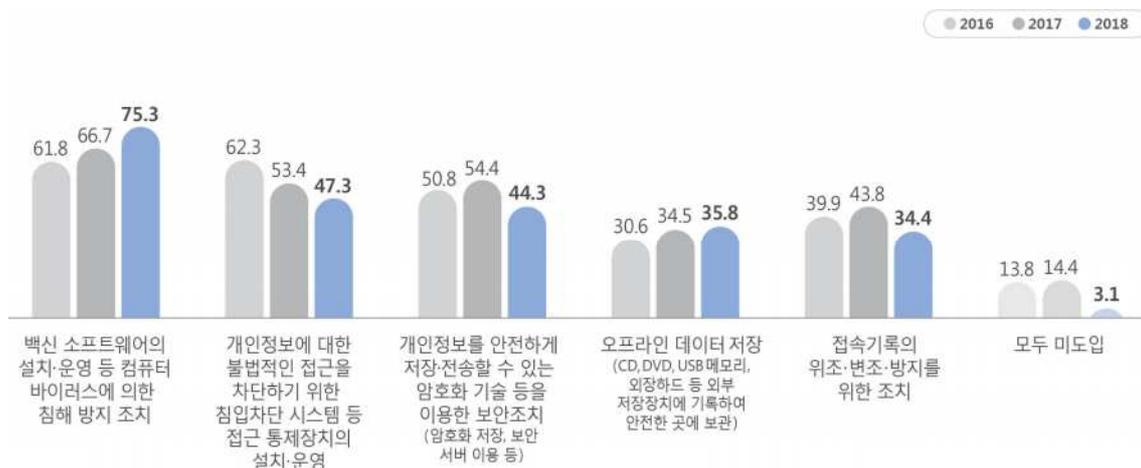


그림 1-2-29 개인정보 침해사고 예방 기술적 조치 (복수응답) - 온라인으로 개인정보 수집 사업체

(단위 : %)



VI

주요 서비스별 정보보호



1. 무선랜



무선랜 구축 및 운영 68.4%, 전년 대비 3.1%p 감소

- ▶ 사업체의 68.4%는 사내 무선랜(Wi-Fi)을 구축하여 운영하고 있는 것으로 조사되었고, 전년(71.5%) 대비 3.1%p 감소함
- ▶ 사업체의 31.5%는 '무선공유기를 통한 악성코드 감염'을 가장 우려하는 것으로 나타났고, 다음으로 '무선공유기의 DDoS 등 공격도구로 악용(30.5%)'되는 것을 우려함

그림 1-2-30

무선랜 구축 및 운영률

(단위 : %)

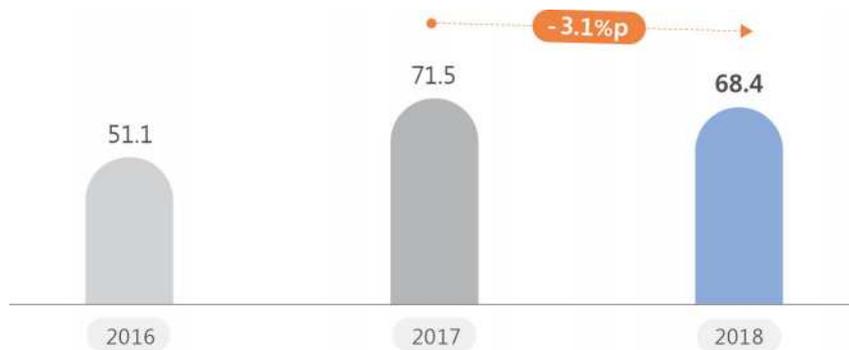
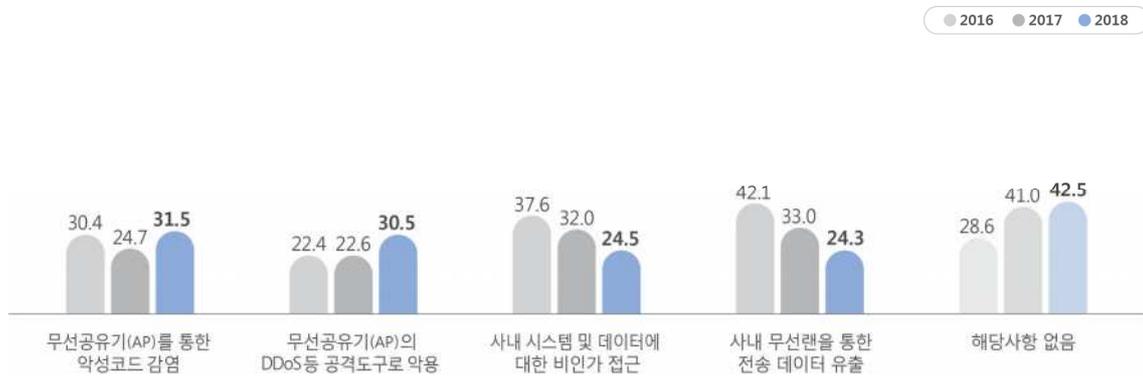


그림 1-2-31

무선랜 보안 우려사항 (2가지) - 무선랜 구축 사업체

(단위 : %)



2. 클라우드



‘클라우드 서비스’ 이용 7.4%, 향후 도입 또는 유지 계획 8.1%

- ▶ 사업체의 7.4%는 클라우드 서비스를 이용하는 것으로 조사되었고, 전년(6.6%) 대비 0.8%p 증가함
 - 클라우드 서비스를 향후 도입 또는 유지할 계획은 8.1%로 전년(6.7%) 대비 1.4%p 증가함
- ▶ 사업체의 56.2%는 ‘데이터 위탁저장에 따른 정보유출’을 가장 우려하는 것으로 나타났고, 다음으로 ‘자원 공유·집중화로 서비스 장애시 대규모 피해 발생(54.9%)’을 우려함

그림 1-2-32 클라우드 서비스 이용 및 향후 도입(유지) 계획

(단위 : %)

✓ 클라우드 서비스 이용률

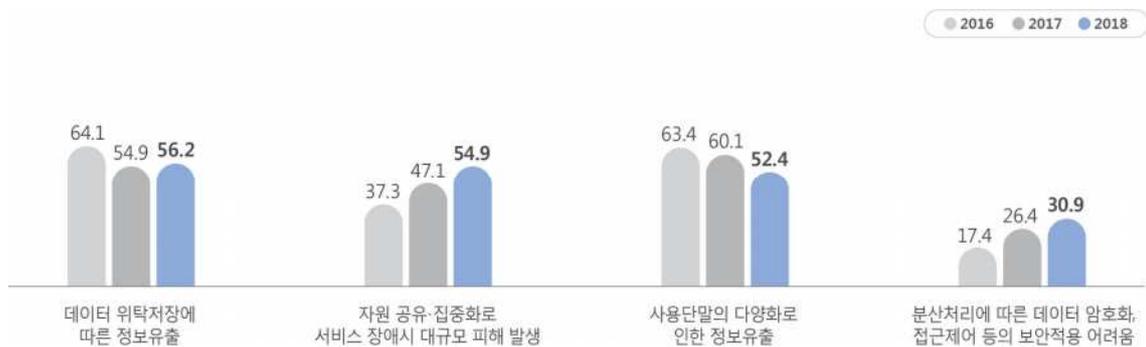


✓ 클라우드 서비스 향후 도입(유지) 계획



그림 1-2-33 클라우드 서비스 관련 보안 우려사항 (2가지)

(단위 : %)



3. 사물인터넷(IoT)



‘사물인터넷(IoT) 제품·서비스’ 이용 9.1%, 전년 대비 4.2%p 증가

- ▶ 사물인터넷(IoT) 제품 및 서비스 이용률은 9.1%로 전년(4.9%) 대비 4.2%p 증가함
 - 사업체의 10.9%는 사물인터넷 제품 및 서비스를 향후 도입 또는 유지할 계획으로 조사되었고, 전년(5.5%) 대비 5.4%p 증가함
- ▶ 사업체의 44.3%는 ‘정보유출’을 가장 우려하는 것으로 나타났고, 다음으로 ‘해킹 및 악성코드 감염(42.7%)’, ‘무선신호교란 및 장애(40.4%)’ 등의 순임

그림 1-2-34

사물인터넷(IoT) 제품·서비스 이용 및 향후 도입(유지) 계획

(단위 : %)

✓ 사물인터넷(IoT) 제품·서비스 이용률



✓ 사물인터넷(IoT) 제품·서비스 향후 도입(유지) 계획

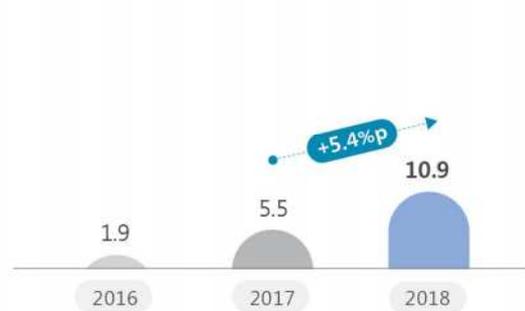
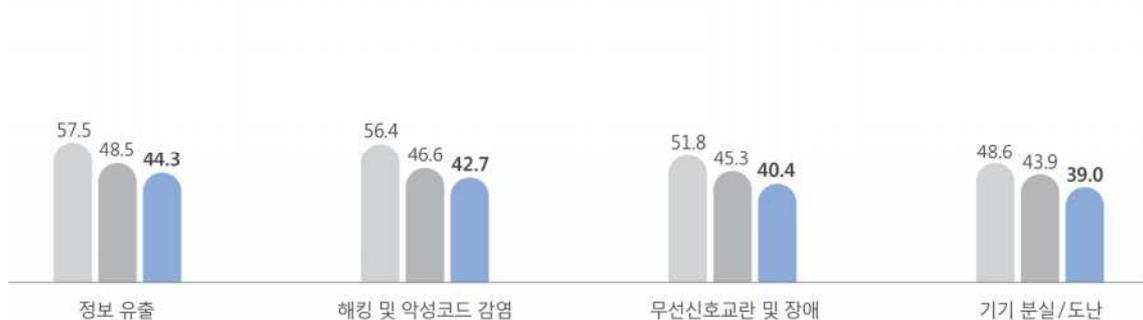


그림 1-2-35

사물인터넷(IoT) 관련 보안 우려사항

(다소 우려함 + 매우 우려함, 단위 : %)

● 2016 ● 2017 ● 2018



4. 정보보호(사이버) 보험



‘정보보호(사이버) 보험’ 이용 0.3%, 향후 가입 또는 유지 계획 0.9%

- ▶ 정보보호(사이버) 보험 이용률은 0.3%로 전년(0.6%)과 비슷한 수준임
 - 사업체의 0.9%는 정보보호(사이버) 보험을 향후 도입 또는 유지할 계획으로 조사되었고, 전년(2.2%) 대비 1.3%p 감소함
- ▶ 정보보호(사이버) 보험 가입 시, ‘개인정보 유출 사고 발생 시 배상 비용(70.9%)’이 가장 보장받고 싶은 사항으로 조사되었고, 다음으로 ‘개인정보 유출 사고 발생 시 대응 비용(조사, 통지, 법률자문)(70.1%)’ 등의 순으로 높게 나타남

그림 1-2-36

정보보호(사이버) 보험 이용 및 향후 가입(유지) 계획

(단위 : %)

✓ 정보보호(사이버) 보험 이용률

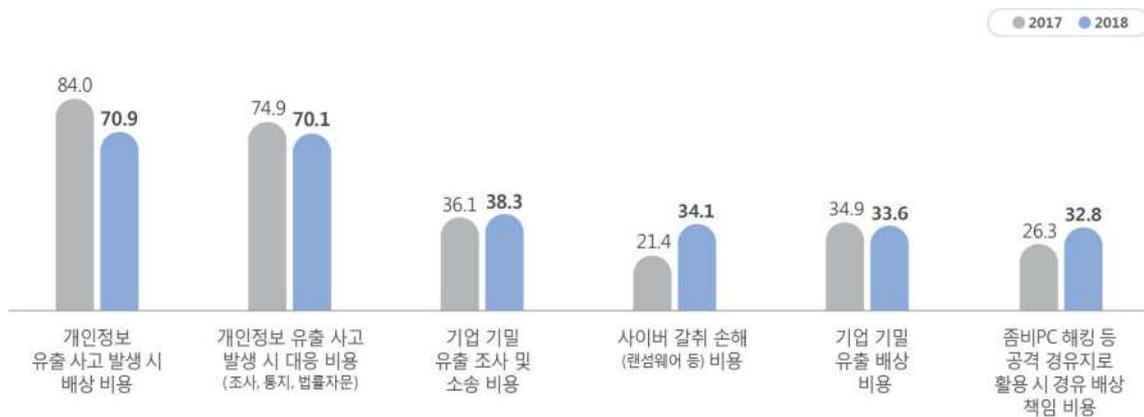
✓ 정보보호(사이버) 보험 향후 가입(유지) 계획



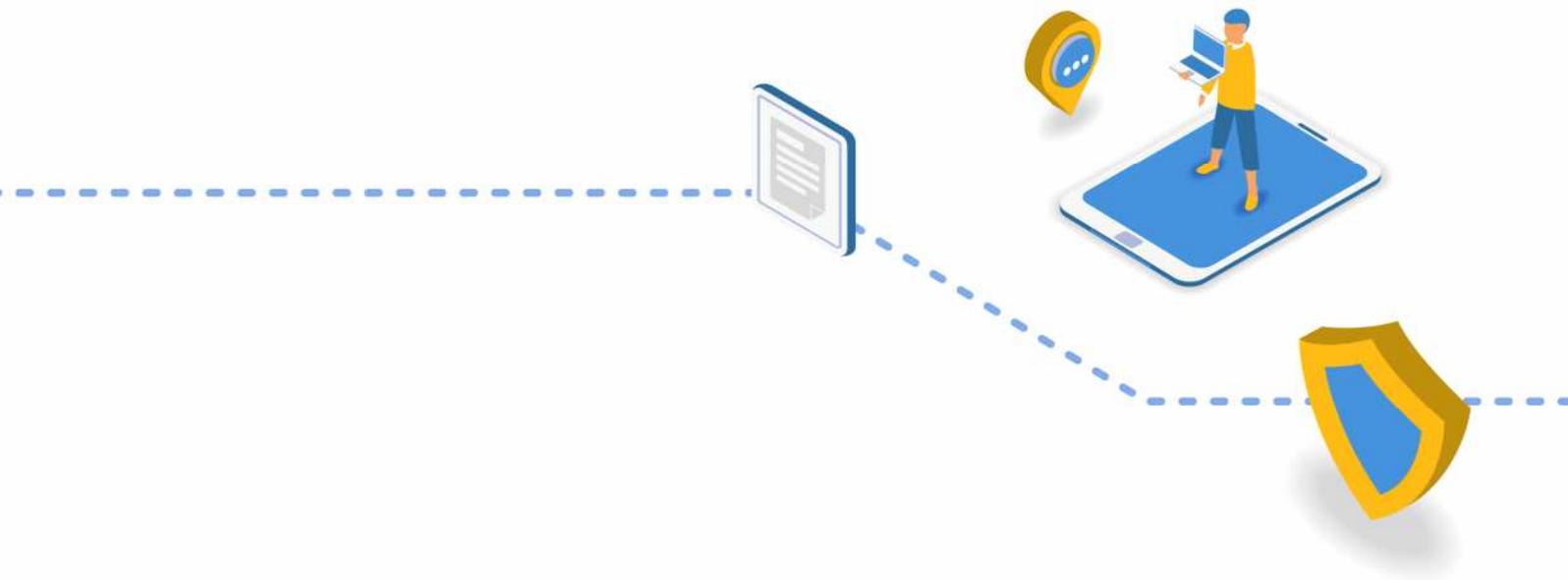
그림 1-2-37

정보보호(사이버) 보험 보장 희망 항목 (복수응답) - 향후 가입 계획 사업체

(단위 : %)

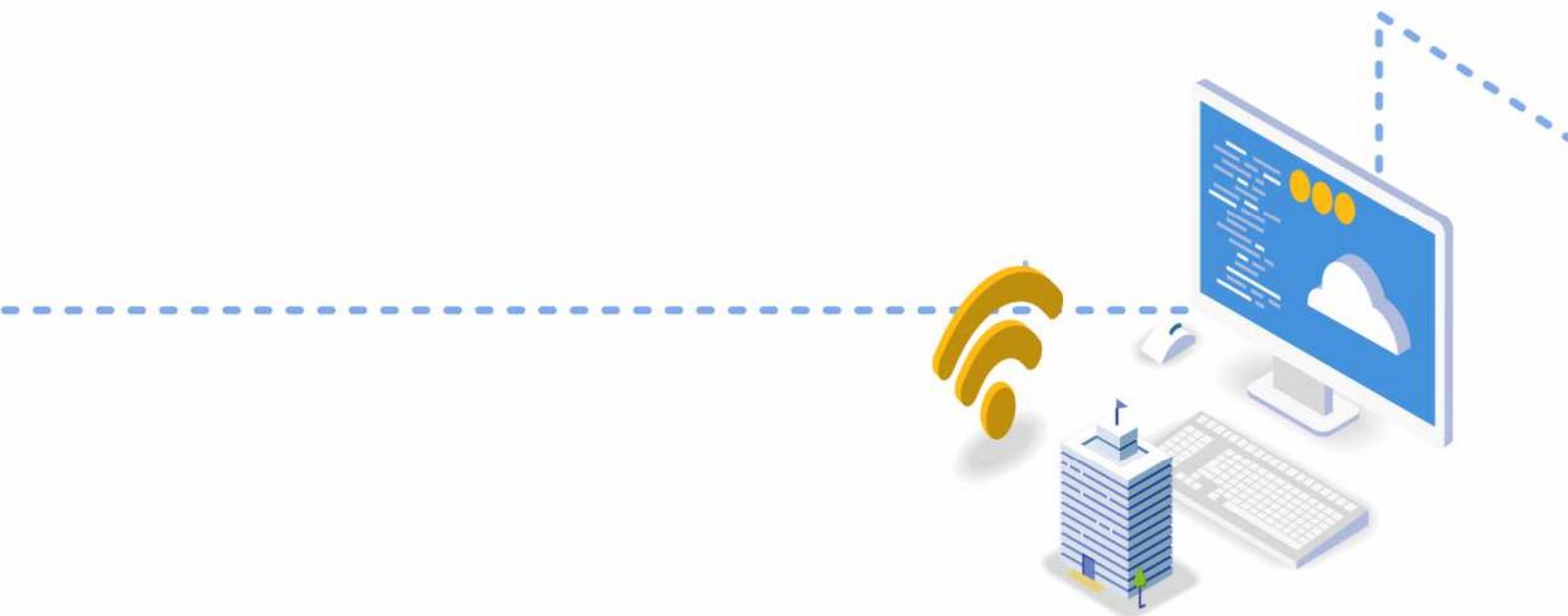






제3장

조사결과



I 정보보호 인식

1. 정보보호 및 개인정보보호 중요성 인식

국내 사업체 중 90.2%는 정보보호가 중요하다(중요한 편이다 + 매우 중요하다)고 응답했으며, 개인정보보호가 중요하다(중요한 편이다 + 매우 중요하다)고 생각하는 사업체의 비율은 89.3%로 나타났다.

그림 1-3-1 정보보호 및 개인정보보호 중요성 인식

(중요한 편이다 + 매우 중요하다, 단위 : %)



2. 정보보호 위협요인

국내 사업체가 우려하는 정보보호 위협요인으로는 '침해사고 위협(해킹, 악성코드, DDoS, 랜섬웨어 등)'이 65.1%로 가장 높게 나타났고, 다음으로 '개인정보 유출 위협(58.4%)', '시스템 및 네트워크 장애(49.5%)' 등의 순으로 조사되었다.

그림 1-3-2 정보보호 위협요인 (2가지)

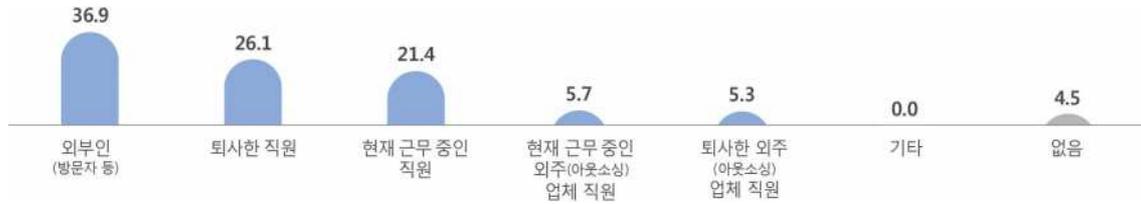
(단위 : %)



정보보호 인적 위협요인 중에서는 '외부인(방문자 등)'이 36.9%로 가장 높게 나타났고, '퇴사한 직원(26.1%)', '현재 근무 중인 직원(21.4%)' 등의 순으로 조사되었다.

그림 1-3-3 정보보호 인적 위협요인

(단위 : %)



우려하는 개인정보 유출요인으로는 '외부로부터 해킹'이 77.4%로 가장 높게 나타났고, 다음으로 '관리 실수로 인한 유출(73.6%)', '내부자에 의한 고의 유출(33.4%)' 등의 순으로 나타났다.

그림 1-3-4 우려하는 개인정보 유출요인 (2가지)

(단위 : %)



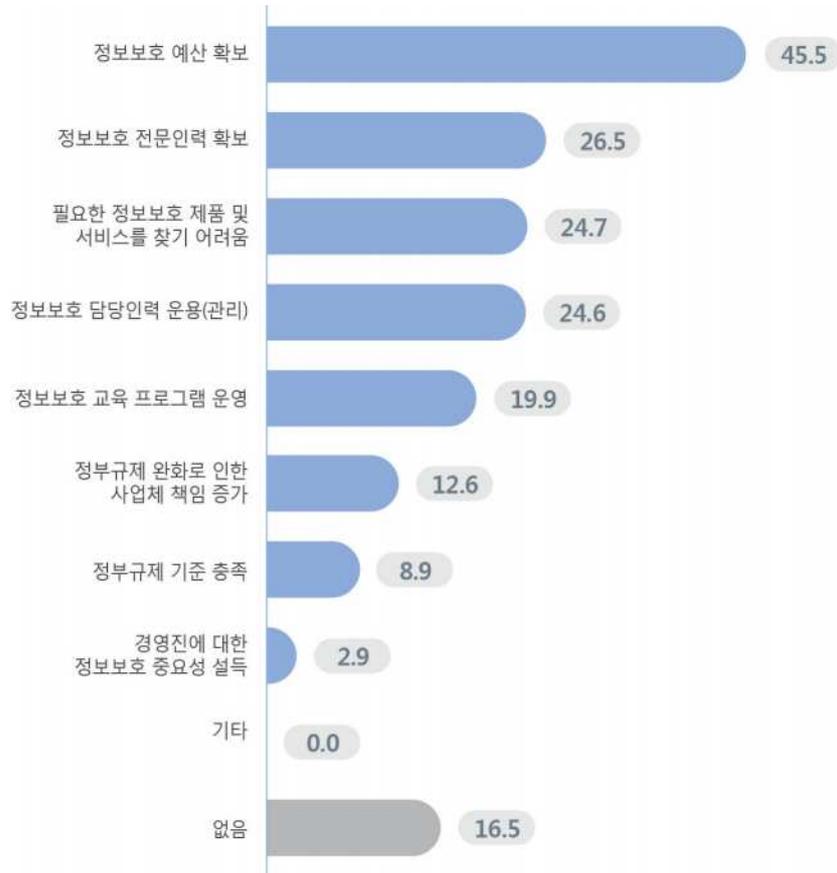
3. 정보보호 애로사항

국내 사업체가 정보보호에 대해 어려움을 느끼는 사항으로는 '정보보호 예산 확보'가 45.5%로 가장 높게 나타났고, 다음으로 '정보보호 전문인력 확보(26.5%)', '필요한 정보 보호 제품 및 서비스를 찾기 어려움(24.7%)' 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 14.5%가 공식문서로 정보보호 정책을 수립한 것으로 나타났다.

그림 1-3-6 정보보호 정책 수립

(단위 : %)



업종별 분석 결과, '금융 및 보험업'이 83.2%로 가장 높게 나타났고, 다음으로 '출판, 영상, 방송통신 및 정보서비스업(47.9%)', '농림수산업(31.2%)' 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 : %)

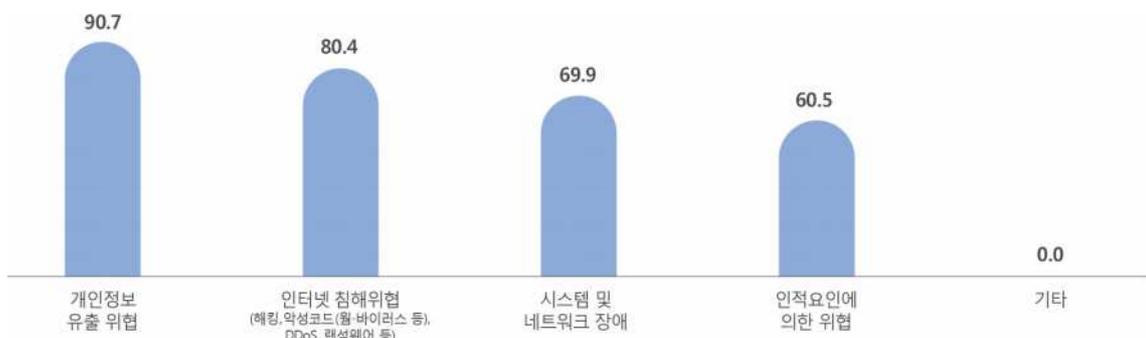


나. 정보보호 정책 포함 위협요소

정보보호 정책에 포함하고 있는 위협요소로는 '개인정보 유출 위협'이 90.7%로 가장 높게 나타났고, 다음으로 '인터넷 침해위협(80.4%)', '시스템 및 네트워크 장애(69.9%)' 등의 순으로 조사되었다.

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

(단위 : %)



다. 개인정보보호 정책 수립

국내 사업체 중 14.9%가 공식문서로 개인정보보호 정책을 수립한 것으로 나타났다.

그림 1-3-10

개인정보보호 정책 수립

(단위 : %)

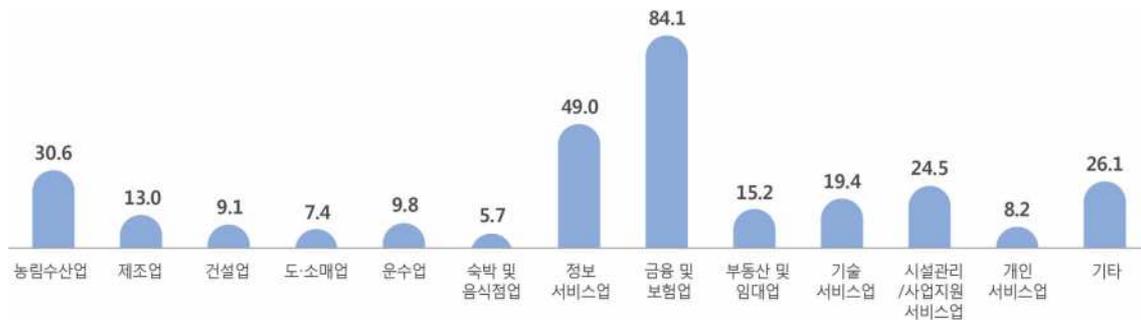


업종별 분석 결과, '금융 및 보험업'이 84.1%로 가장 높게 나타났고, 다음으로 '출판, 영상, 방송통신 및 정보서비스업(49.0%)', '농림수산업(30.6%)' 등의 순으로 조사되었다.

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 : %)

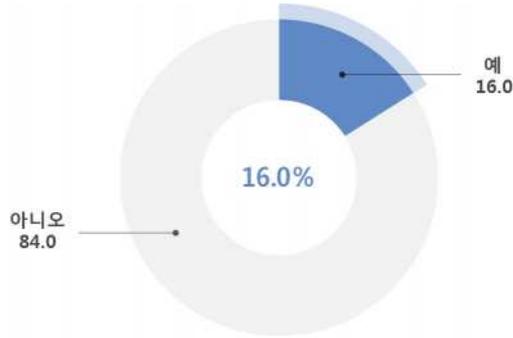


그림 1-3-14 업종별 정보보호(개인정보보호) 정책 수립

(단위 : %)

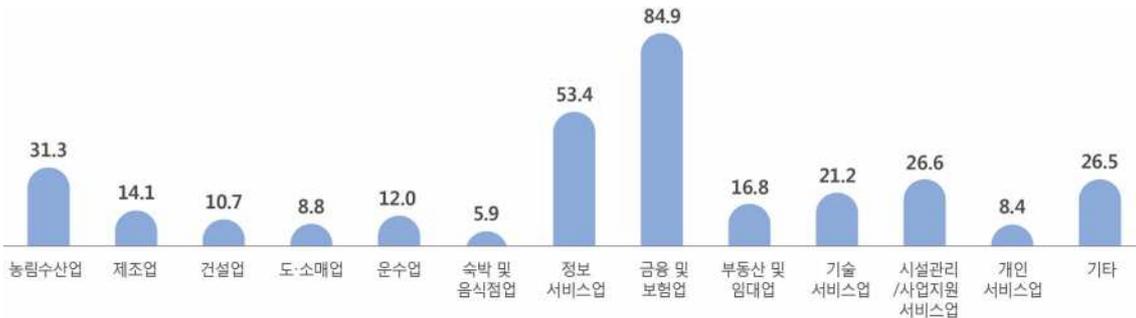
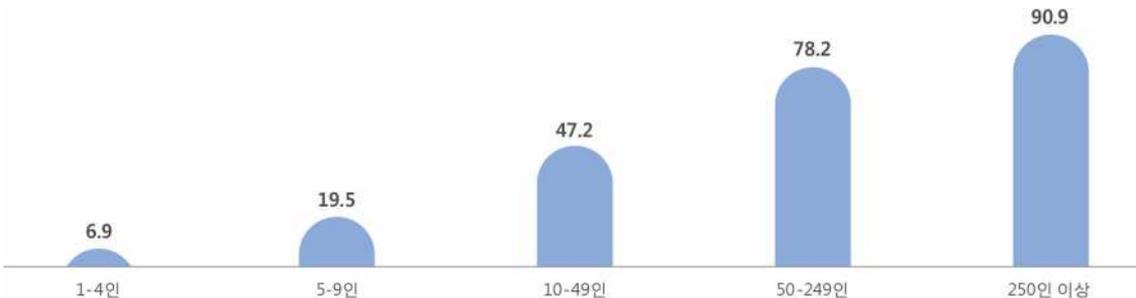


그림 1-3-15 규모별 정보보호(개인정보보호) 정책 수립

(단위 : %)



2. 정보보호 조직

가. 정보보호 전담조직 운영

국내 사업체 중 1.5%가 공식적인 정보보호 전담조직을 운영하고 있는 것으로 나타났다.

그림 1-3-16 정보보호 전담조직 운영

(단위 : %)



업종별 분석 결과, '금융 및 보험업'이 9.7%로 가장 높게 나타났고, 다음으로 '출판, 영상, 방송통신 및 정보서비스업(3.3%)', '농림수산업(3.0%)' 등의 순으로 조사되었다.

그림 1-3-17 업종별 정보보호 전담조직 운영

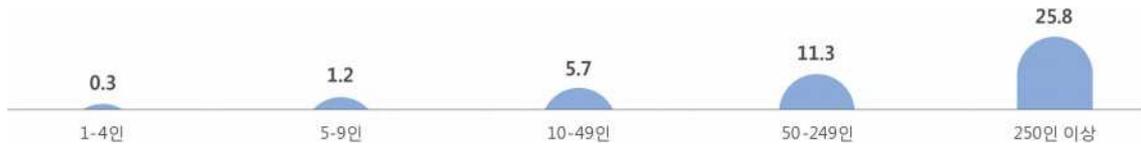
(단위 : %)



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

그림 1-3-18 규모별 정보보호 전담조직 운영

(단위 : %)

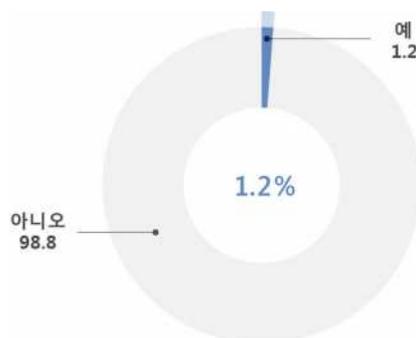


나. 개인정보보호 전담조직 운영

국내 사업체 중 1.2%가 공식적인 개인정보보호 전담조직을 운영하고 있는 것으로 나타났다.

그림 1-3-19 개인정보보호 전담조직 운영

(단위 : %)



업종별 분석 결과, '금융 및 보험업'이 8.7%로 가장 높게 나타났고, 다음으로 '출판, 영상, 방송통신 및 정보서비스업(2.6%)', '농림수산업(1.9%)' 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 : %)



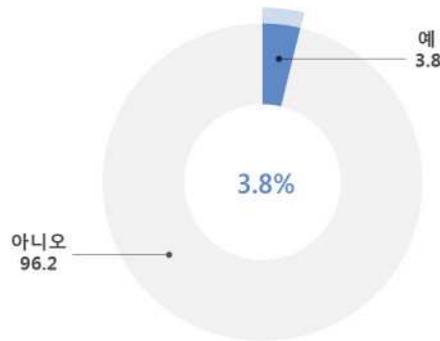
다. 정보보호와 개인정보보호 조직 공동 운영

국내 사업체 중 3.8%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 23.4%로 가장 높게 나타났고, 다음으로 '출판, 영상, 방송통신 및 정보서비스업(15.2%)', '전문, 과학 및 기술서비스업(7.3%)' 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)' 8.7%, '정보보호최고책임자(Chief Information Security Officer)' 8.8%, '개인정보보호책임자(Chief Privacy Officer)' 8.4%로 각각 나타났다.

그림 1-3-28 정보보호 관련 책임자 임명 (복수응답)

(단위 : %)



업종별 분석 결과, '금융 및 보험업'이 '정보관리책임자(CIO)' 52.5%, '정보보호최고책임자(CISO)' 63.6%, '개인정보보호책임자(CPO)' 64.7%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)

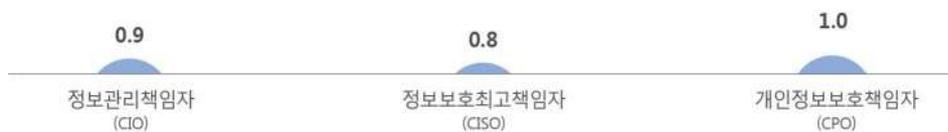
(단위 : %)



정보보호 관련 책임자 전담 비율은 '정보관리책임자(CIO)' 0.9%, '정보보호최고책임자(CISO)' 0.8%, '개인정보보호책임자(CPO)' 1.0%로 각각 나타났다.

그림 1-3-31 정보보호 관련 책임자 전담 (복수응답)

(단위 : %)



업종별 분석 결과, '금융 및 보험업'이 '정보관리책임자(CIO)' 9.1%, '정보보호최고책임자(CISO)' 9.3%, '개인정보보호책임자(CPO)' 9.1%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 : %)



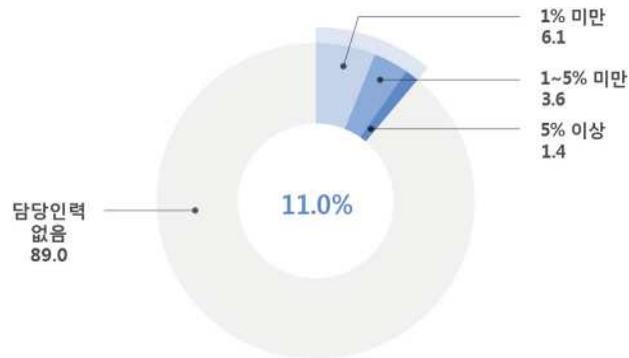
나. IT 인력 중 정보보호 담당 인력 비중

IT인력 중 정보보호를 담당하는 인력을 보유한 사업체는 11.0%로 나타났다.

IT인력 중 정보보호를 담당하는 인력이 차지하는 비중을 살펴보면, '1% 미만'이 6.1%로 가장 높았고, 다음으로 '1~5% 미만(3.6%)', '5% 이상(1.4%)' 등의 순으로 나타났다.

그림 1-3-34 IT 인력 중 정보보호 담당 인력 비중

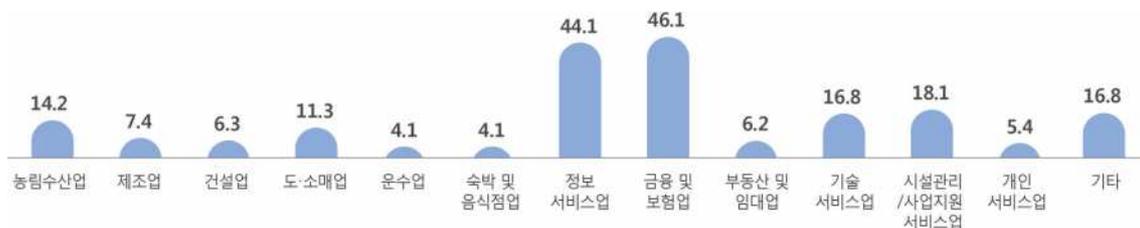
(단위 : %)



업종별 분석 결과, '금융 및 보험업'이 46.1%로 가장 높게 나타났고, 다음으로 '출판, 영상, 방송통신 및 정보서비스업(44.1%)', '사업시설관리 및 사업지원 서비스업(18.1%)' 등의 순으로 조사되었다.

그림 1-3-35 업종별 IT 인력 중 정보보호 담당 인력 배정

(단위 : %)



규모별 분석 결과, 종사자 수 250인 이상인 사업체의 정보보호 담당 인력 배정 비율이 82.3%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 : %)

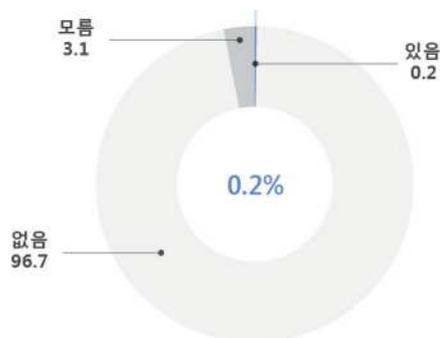


다. 정보보호 담당 인력 신규 채용계획

국내 사업체 중 0.2%는 2018년에 정보보호 담당 인력을 신규로 채용할 계획을 보유하고 있는 것으로 나타났다.

그림 1-3-37 정보보호 담당 인력 신규 채용계획

(단위 : %)

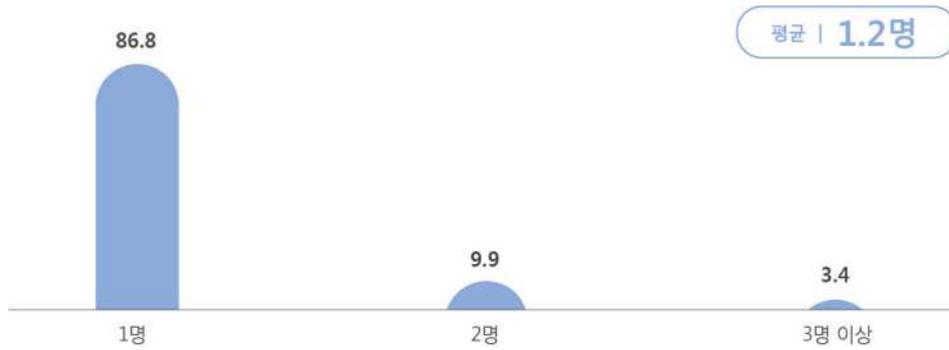


2018년 정보보호 담당 인력 신규 채용계획 규모는 평균 1.2명이었고, 신규 채용 계획이 있는 사업체의 86.8%가 1명을 채용할 계획인 것으로 나타났다.

그림 1-3-38

정보보호 담당 인력 신규 채용 규모 - 신규 채용 계획 사업체

(단위 : %)



4. 정보보호 교육

가. 정보보호 교육 실시

국내 사업체 중 25.1%는 임직원을 대상으로 정보보호 교육(외부 위탁 교육 포함)을 실시한 것으로 나타났다.

그림 1-3-39

정보보호 교육 실시

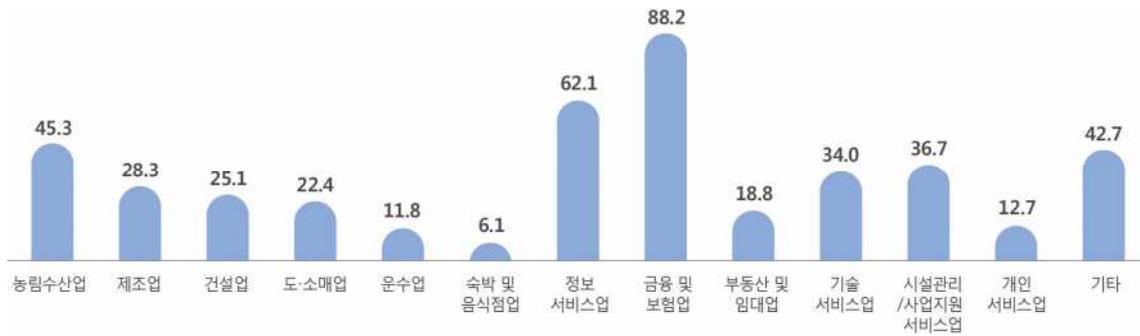
(단위 : %)



업종별 조사 결과, '금융 및 보험업'이 88.2%로 가장 높게 나타났고, 다음으로 '출판, 영상, 방송통신 및 정보서비스업(62.1%)', '농림수산업(45.3%)' 등의 순으로 조사되었다.

그림 1-3-40 업종별 정보보호 교육 실시

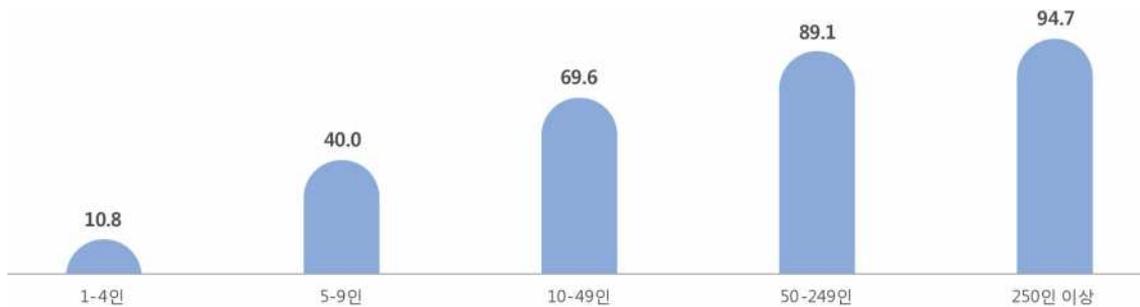
(단위 : %)



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

그림 1-3-41 규모별 정보보호 교육 실시

(단위 : %)



나. 개인정보보호 교육 실시

국내 사업체 중 26.5%는 임직원을 대상으로 개인정보보호 교육(외부 위탁 교육 포함)을 실시한 것으로 나타났다.

그림 1-3-42

개인정보보호 교육 실시

(단위 : %)



업종별 조사 결과, '금융 및 보험업'이 88.7%로 가장 높게 나타났고, 다음으로 '출판, 영상, 방송통신 및 정보서비스업(47.4%)', '농림수산업(46.2%)' 등의 순으로 조사되었다.

그림 1-3-43

업종별 개인정보보호 교육 실시

(단위 : %)

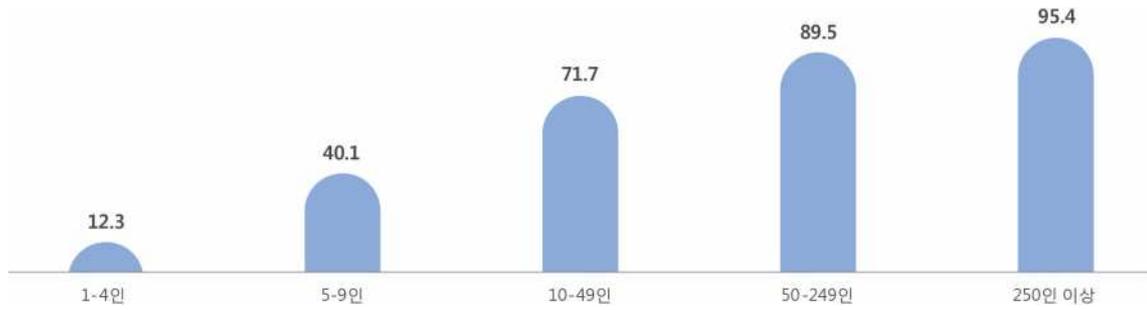


규모별 분석 결과, 종사자 수가 많을수록 개인정보보호 교육을 실시하는 비율이 높게 나타났다.

그림 1-3-44

규모별 개인정보보호 교육 실시

(단위 : %)



▶ 참고 2017년 중에 정보보호 또는 개인정보보호 교육을 실시한 경우

그림 1-3-45 정보보호(개인정보보호) 교육 실시

(단위 : %)



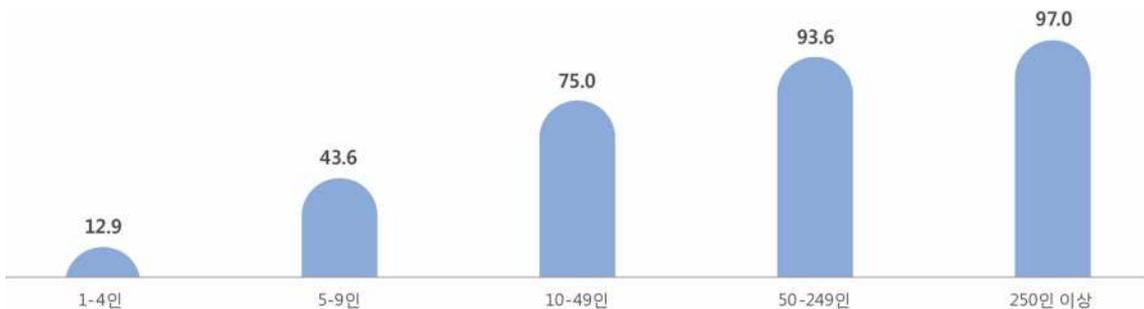
그림 1-3-46 업종별 정보보호(개인정보보호) 교육 실시

(단위 : %)



그림 1-3-47 규모별 정보보호(개인정보보호) 교육 실시

(단위 : %)



다. 대상별 교육 실시 현황

교육 대상별 분석 결과, 정보보호 또는 개인정보보호 교육을 받는 대상으로는 '컴퓨터를 사용하는 일반직원'이 93.1%로 가장 높게 나타났고, 다음으로 'CEO 등 경영진(55.4%)', '정보보호책임자급 직원(27.3%)' 등의 순으로 조사되었다.

그림 1-3-48

대상별 교육 실시 (복수응답) - 정보보호(개인정보보호) 교육 실시 사업체

(단위 : %)



교육 대상별 교육 시간은 '개인정보보호책임자'가 5.4시간으로 가장 많았고, 다음으로 '정보보호책임자급 직원(5.2시간)', 'IT 및 정보보호 실무자(4.8시간)' 등의 순으로 조사되었다.

그림 1-3-49

대상별 연평균 교육 시간 - 정보보호(개인정보보호) 교육 실시 사업체

(단위 : 시간)



5. 정보보호 예산 및 투자

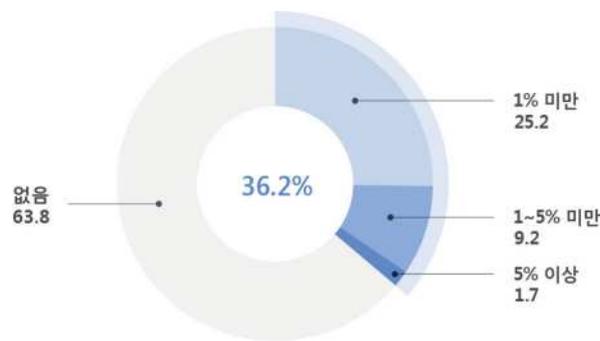
국내 사업체 중 36.2%는 2017년 1년간 정보보호 또는 개인정보보호 예산을 편성한 것으로 나타났다.

IT 예산 중 정보보호 관련 예산이 차지하는 비중을 살펴보면, '1% 미만'이 25.2%로 가장 높았고, 다음으로 '1~5% 미만(9.2%)', '5% 이상(1.7%)' 등의 순으로 나타났다.

그림 1-3-50

IT 예산 중 정보보호 예산 비중

(단위 : %)



2016년 대비 2017년 1년간 정보보호 관련 예산 증감의 경우, '변동없음'이 84.6%로 가장 높게 나타났고, '증가'는 12.9%, '감소'는 2.6%로 조사되었다.

그림 1-3-51

정보보호 예산 증감 - 정보보호 예산 수립 사업체

(단위 : %)

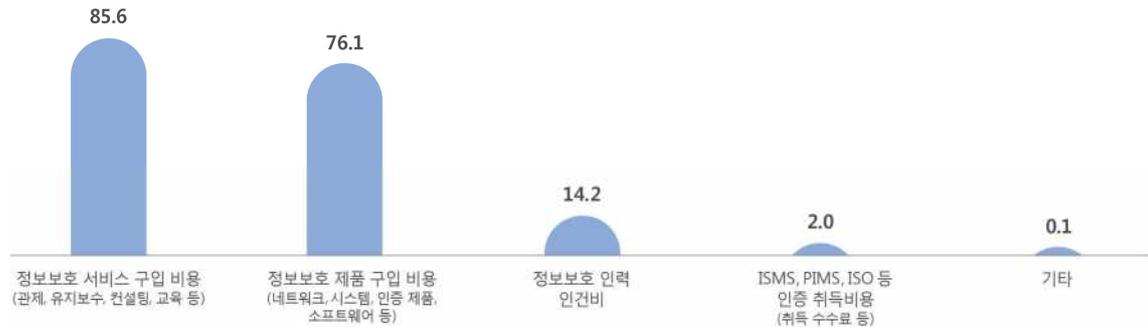


정보보호 예산을 수립한 사업체는 2017년 1년간 '정보보호 서비스 구입비용(85.6%)'에 가장 많은 예산을 지출한 것으로 나타났고, 다음으로 '정보보호 제품 구입비용(76.1%)', '정보보호 인력 인건비(14.2%)' 등의 순으로 조사되었다.

그림 1-3-52

정보보호 지출 분야 (2가지) - 정보보호 예산 수립 사업체

(단위 : %)



Ⅲ 침해사고 예방

1. 정보보호 제품 및 서비스

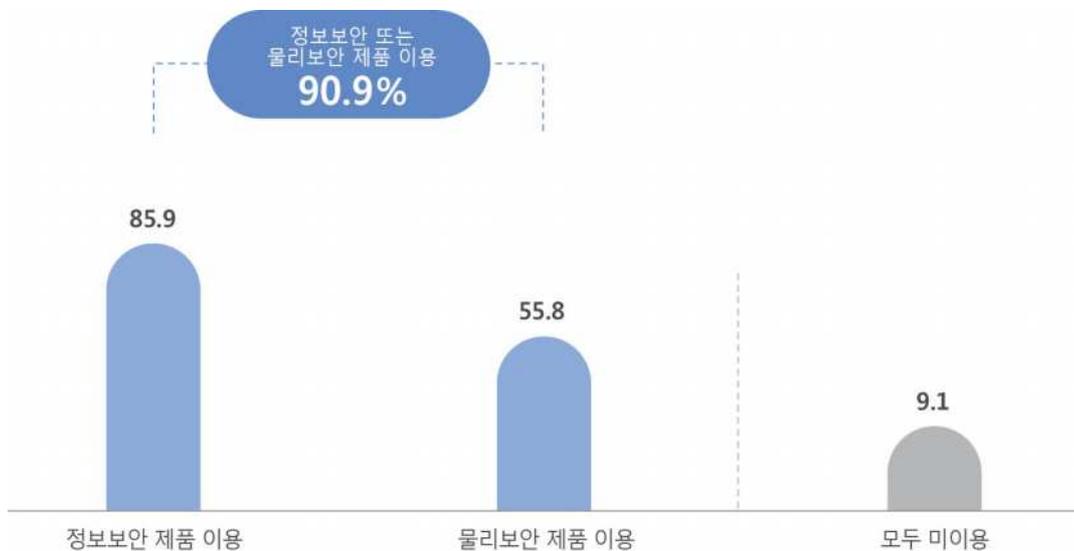
가. 정보보호 제품 이용

국내 사업체 중 90.9%는 정보보호(정보보안 또는 물리보안)를 위해 관련 제품을 이용하고 있는 것으로 나타났다.

그림 1-3-53

정보보호 제품 이용 (요약)

(단위 : %)



정보보안 제품군 중 '시스템(단말)보안' 제품군의 이용률이 79.9%로 가장 높게 나타났고, 다음으로 '네트워크 보안(79.4%)', '인증 보안(바이오 인증 제외)(51.5%)' 등의 순으로 조사되었다.

그림 1-3-54 정보보호 제품 이용 - 정보보안 (복수응답)

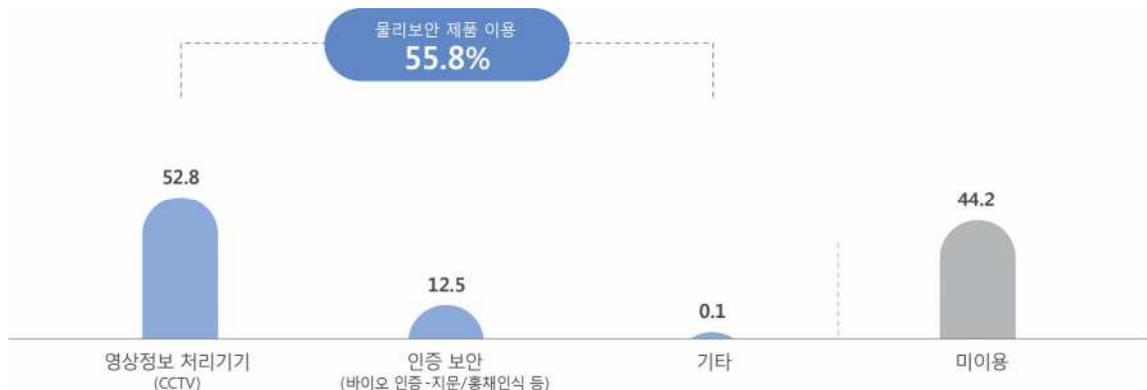
(단위 : %)



물리보안 제품군 중 '영상정보 처리기기(CCTV)' 제품군의 이용률이 52.8%로 가장 높게 나타났고, 다음으로 '인증 보안(바이오 인증)(12.5%)' 등의 순으로 조사되었다.

그림 1-3-55 정보보호 제품 이용 - 물리보안 (복수응답)

(단위 : %)



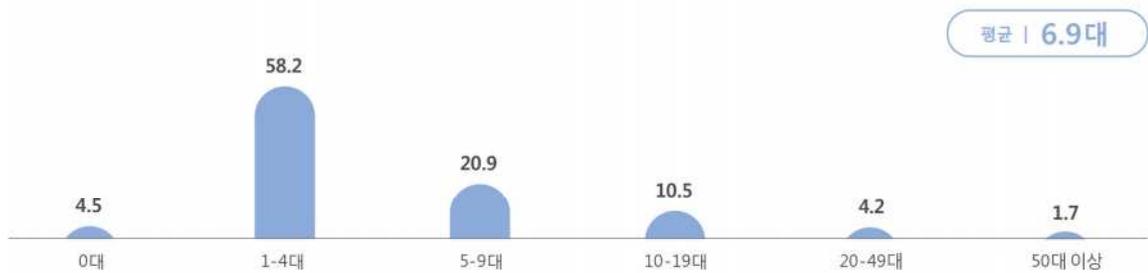
영상정보 처리기기 유형별 분석 결과, 폐쇄회로 CCTV는 평균 6.9대, IP 카메라는 평균 0.8대를 보유하고 있는 것으로 나타났다.

그림 1-3-56

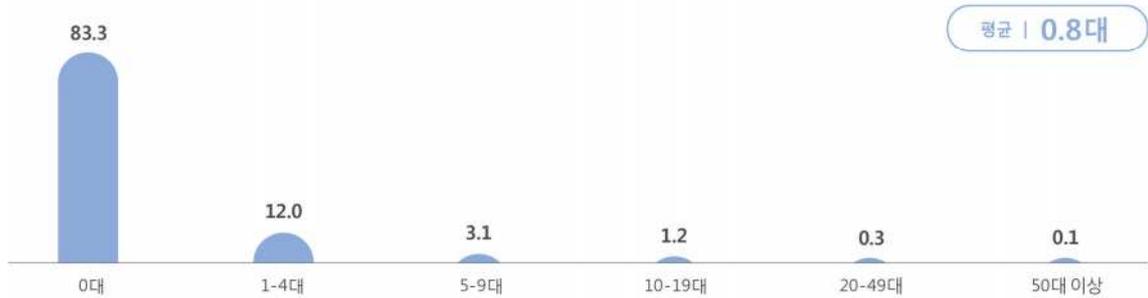
CCTV 보유 대수 - CCTV 보유 사업체

(단위 : %)

✓ 폐쇄회로 CCTV



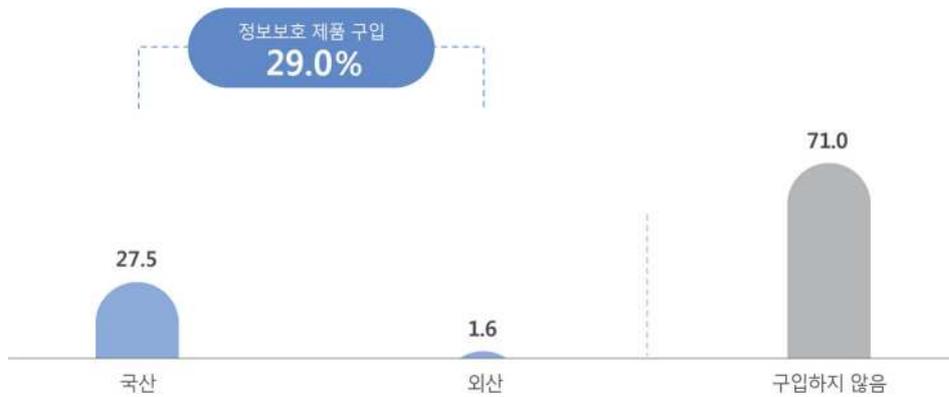
✓ IP 카메라



국내 사업체의 29.0%는 2017년 정보보호 관련 제품 구입을 위해 지출하였고, 그 중 국산 제품의 구입 비중은 27.5%로 나타났다.

그림 1-3-57 정보보호 제품 국산/외산 비중

(단위 : %)



외산 정보보호 제품을 구매한 이유는 '성능 및 품질이 우수하기 때문에'가 54.5%로 가장 높게 나타났고, 다음으로 '보다 저렴한 가격 때문에(32.3%)', '유지보수관리가 용이하기 때문에(8.0%)' 등의 순으로 조사되었다.

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

(단위 : %)



나. 정보보호 서비스 이용

국내 사업체 중 59.4%는 정보보호를 위해 관련 서비스를 이용하고 있는 것으로 나타났다. 서비스 유형별로는 '유지관리'가 38.3%로 가장 높게 나타났고, 다음으로 '인증서비스(29.3%)', '교육/훈련(16.6%)' 등의 순으로 조사되었다.

그림 1-3-59

정보보호 서비스 이용 요약

(단위 : %)

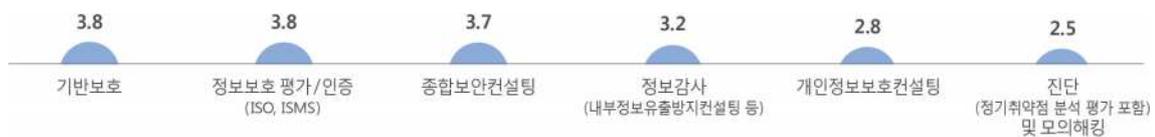


보안컨설팅 서비스 중 '기반보호' 및 '정보보호 평가/인증(ISO, ISMS)' 서비스의 이용률이 3.8%로 가장 높게 나타났고, 다음으로 '종합보안컨설팅(3.7%)' 등의 순으로 조사되었다.

그림 1-3-60

보안컨설팅 (복수응답)

(단위 : %)



보안관제 서비스 중 '원격관제 서비스'의 이용률이 14.5%로 '파견관제 서비스(7.6%)'에 비해 높게 나타났다.

그림 1-3-61

보안관제 (복수응답)

(단위 : %)



인증서비스 중 '공인/사설 인증서 발급서비스'의 이용률이 29.0%로 'CC평가인증(컨설팅 포함)(2.0%)'에 비해 높게 나타났다.

그림 1-3-62

인증 서비스(복수응답)

(단위 : %)



2. 정보보호 관리

가. 보안점검 및 취약점 점검

국내 사업체 중 90.0%가 시스템 및 네트워크에 대한 보안점검(취약점 점검 등)을 실시하는 것으로 나타났다.

점검 실시 주기별로는 '정기적(연 1회 등)'으로 실시하는 사업체가 27.1%, '비정기적(문제 발생시 등)'으로 실시하는 사업체가 67.1%로 조사되었다.

그림 1-3-63

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(94.0%)', '네트워크 장비(93.8%)' 등의 순으로 조사되었다.

그림 1-3-64 시스템 및 네트워크 보유 (복수응답) - 보안점검 실시 사업체

(단위 : %)



시스템 및 네트워크 유형별 분석 결과, 취약점 점검률은 'PC'가 99.0%로 가장 높게 나타났고, 다음으로 '물리보안(출입통제, CCTV 등)(91.3%)', '서버 운영체제(OS)(54.0%)' 등의 순으로 조사되었다.

그림 1-3-65 취약점 점검 (복수응답) - 각 시스템 및 네트워크 보유 사업체

(단위 : %)



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

그림 1-3-66

취약점 점검 (복수응답) - 보안점검 실시 사업체

(단위 : %)



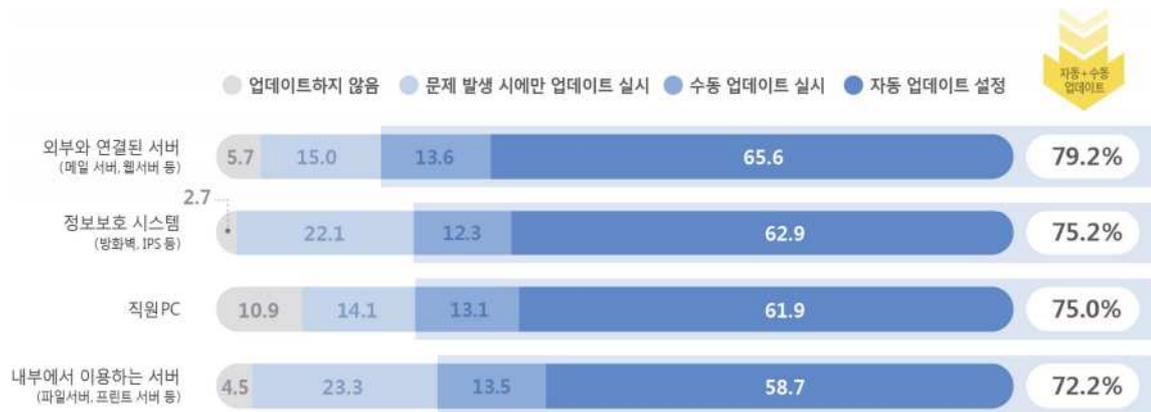
나. 보안패치 적용

제품 유형별로 자동 또는 수동으로 보안패치를 적용하는 비율은 '외부와 연결된 서버 (메일서버, 웹서버 등)'가 79.2%로 가장 높게 나타났고, 다음으로 '정보보호 시스템(방화벽, IPS 등)(75.2%)', '직원PC(75.0%)' 등의 순으로 조사되었다.

그림 1-3-67

보안패치 적용 방법 (복수응답) - 항목별 제품 보유 사업체

(자동 업데이트 + 수동 업데이트, 단위 : %)

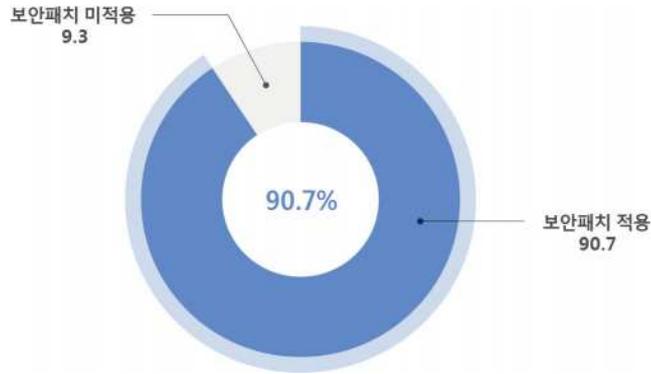


▶ **참고** 직원PC, 외부와 연결된 서버, 내부에서 이용하는 서버, 정보보호 시스템 중 하나라도 보안패치를 적용하는 경우

그림 1-3-68

보안패치 적용

(단위 : %)

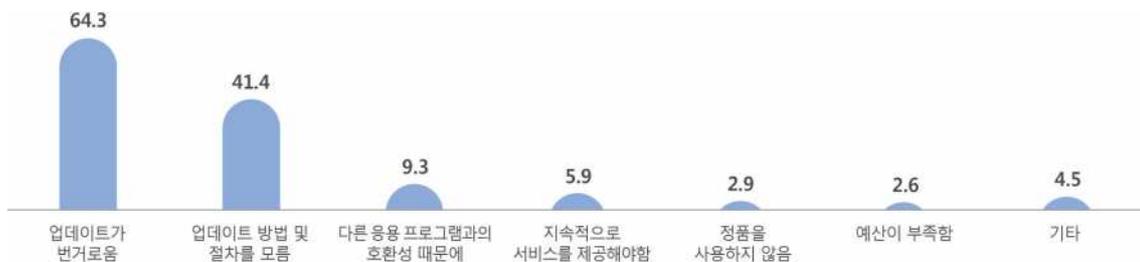


보안패치를 적용하지 않는 이유는 '업데이트가 번거로움'이 64.3%로 가장 높게 나타났고, 다음으로 '업데이트 방법 및 절차를 모름(41.4%)', '다른 응용 프로그램과의 호환성 때문에 (9.3%)' 등의 순으로 조사되었다.

그림 1-3-69

보안패치 업데이트 미실시 이유 (복수응답) - 하나라도 업데이트 하지 않는 사업체

(단위 : %)



다. 백업 실시

국내 사업체 중 30.5%가 시스템 로그 백업을 실시하는 것으로 나타났다.

그림 1-3-70

시스템 로그 백업

(단위 : %)



시스템 로그의 백업 실시 주기는 월 평균 13.0회로 나타났다.

또한, 시스템 로그 백업 실시 사업체의 61.5%가 '월 1회 이상' 백업을 실시하는 것으로 나타났고, 다음으로 '실시간(26.6%)', '3개월에 1회 정도(11.7%)' 등의 순으로 시스템 로그 백업을 실시하였다.

그림 1-3-71

시스템 로그 백업 주기 - 시스템 로그 백업 실시 사업체

(단위 : %)



국내 사업체 중 47.3%가 중요 데이터 백업을 실시하는 것으로 나타났다.

그림 1-3-72

중요 데이터 백업

(단위 : %)



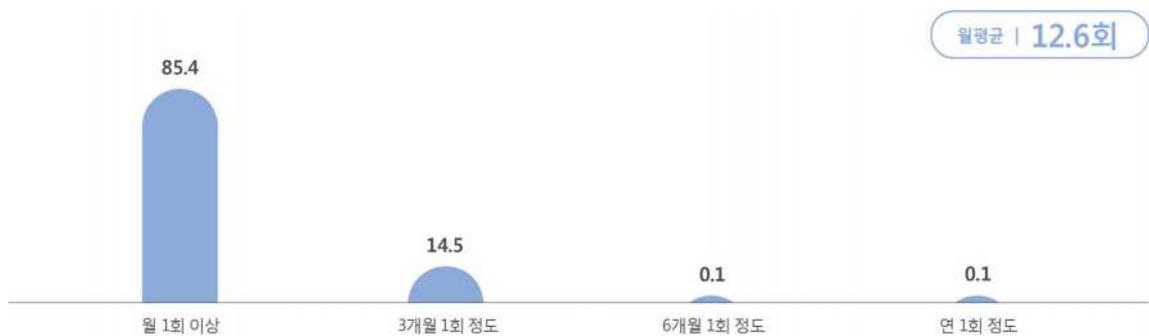
중요 데이터의 백업 실시 주기는 월 평균 12.6회로 나타났다.

또한, 중요 데이터 백업 실시 사업체의 85.4%가 '월 1회 이상' 백업을 실시하는 것으로 나타났고, 다음으로 '3개월에 1회 정도(14.5%)' 등의 순으로 중요 데이터 백업을 실시하였다.

그림 1-3-73

중요 데이터 백업 주기 - 중요 데이터 백업 실시 사업체

(단위 : %)



시스템 로그 또는 중요 데이터를 백업하는 방식은 'USB메모리 등 별도 저장장치 활용'이 64.4%로 가장 높게 나타났고, 다음으로 '운영체제(windows 등) 백업기능 활용(36.4%)', '별도 백업서버(NAS, SAN 등)(15.2%)' 등의 순으로 조사되었다.

그림 1-3-74

백업 방식 (복수응답) - 하나라도 백업 실시 사업체

(단위 : %)

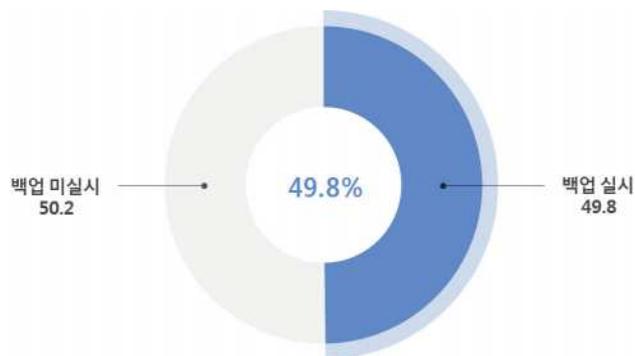


▶ 참고 시스템 로그 또는 중요 데이터 백업을 실시하는 경우

그림 1-3-75

백업 실시 - 시스템 로그 또는 중요 데이터 백업 실시

(단위 : %)



IV 침해사고 대응

1. 침해사고 경험

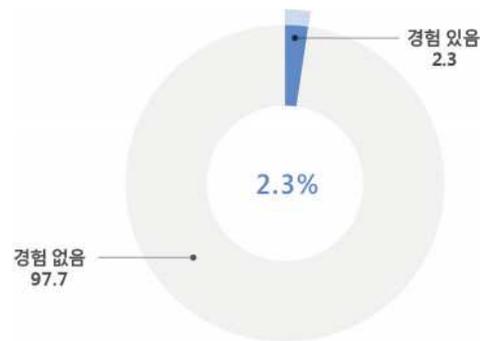
가. 침해사고 경험

국내 사업체 중 2.3%가 해킹, 악성코드(웜·바이러스), DDoS 등의 침해사고를 경험한 것으로 나타났다.

그림 1-3-76

침해사고 경험

(단위 : %)



업종별 분석 결과, '전문, 과학 및 기술서비스업'이 6.0%로 가장 높게 나타났고, 다음으로 '제조업(5.3%)', '건설업(4.6%)' 등의 순으로 조사되었다.

그림 1-3-77

업종별 침해사고 경험

(단위 : %)



규모별 분석 결과, '종사자 수 250인 이상'의 사업체가 10.1%로 가장 높게 나타났다.

그림 1-3-78 규모별 침해사고 경험

(단위 : %)



나. 침해사고 경험 유형 및 심각성 정도

침해사고 경험 유형별로는 '랜섬웨어'의 경험률이 56.3%로 가장 높게 나타났고, 다음으로 '악성코드에 의한 공격(47.7%)', '애드웨어/스파이웨어 감염(12.1%)' 등의 순으로 조사되었다.

그림 1-3-79 침해사고 경험 유형 (복수응답) - 침해사고 경험 사업체

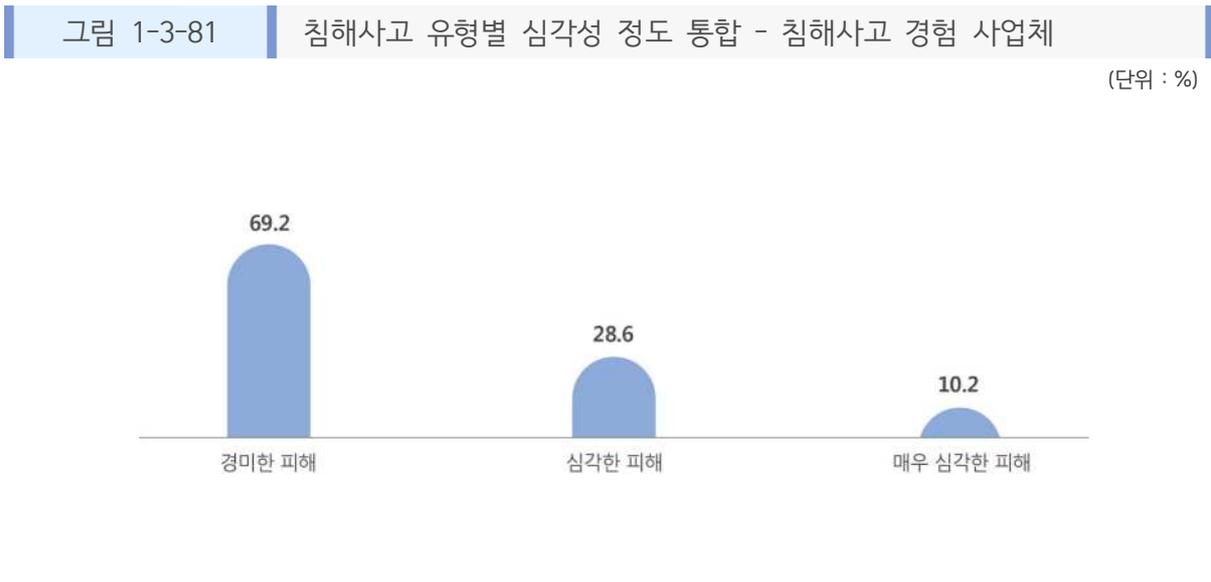
(단위 : %)



침해사고 경험 유형별 심각성 정도는 'DoS/DDoS 공격' 유형에서 '매우 심각(19.6%)'이 가장 높게 나타났고, 다음으로 '랜섬웨어(12.2%, 매우 심각)' 등의 순으로 조사되었다.



▶ 참고 전체 침해사고 유형별 심각성 정도



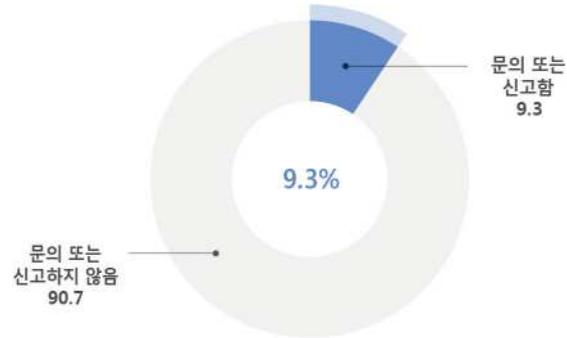
다. 침해사고 시 관계기관 문의 또는 신고

침해사고 경험 사업체의 9.3%가 피해를 입었을 때 관계기관에 문의 또는 신고하는 것으로 나타났다.

그림 1-3-82

침해사고 시 관계기관 문의 또는 신고 - 침해사고 경험 사업체

(단위 : %)



2. 침해사고 대응

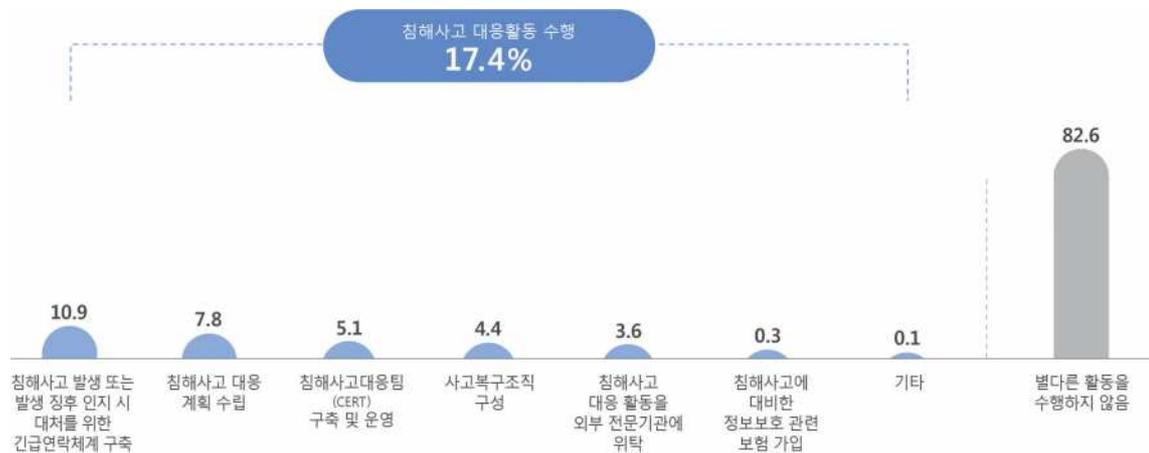
국내 사업체 중 17.4%가 침해사고에 대응하기 위한 활동을 수행한 것으로 나타났다.

침해사고 대응활동 유형별로는 '침해사고 발생 또는 발생 징후 인지 시 대처를 위한 긴급연락체계 구축'이 10.9%로 가장 높게 나타났고, 다음으로 '침해사고 대응 계획 수립(7.8%)' 등의 순으로 조사되었다.

그림 1-3-83

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(25.7%)' 등의 순으로 조사되었다.

그림 1-3-84

침해사고 대응 대외협력채널 (2가지)

(단위 : %)



V 개인정보보호

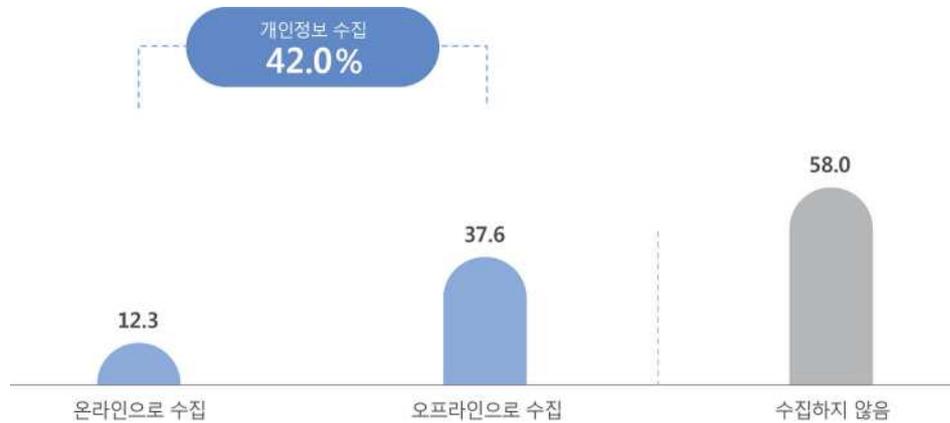
1. 개인정보 수집 및 이용

가. 개인정보 수집

국내 사업체 중 42.0%는 고객의 개인정보를 온라인 또는 오프라인으로 수집하는 것으로 나타났다.

그림 1-3-85 개인정보 수집 (복수응답)

(단위 : %)



온라인으로 고객의 개인정보를 수집하는 사업체는 주로 '홈페이지 회원가입(88.9%)'을 통해 수집하는 것으로 나타났다.

그림 1-3-86 개인정보 온라인 수집 방법 (복수응답) - 온라인으로 개인정보 수집 사업체

(단위 : %)

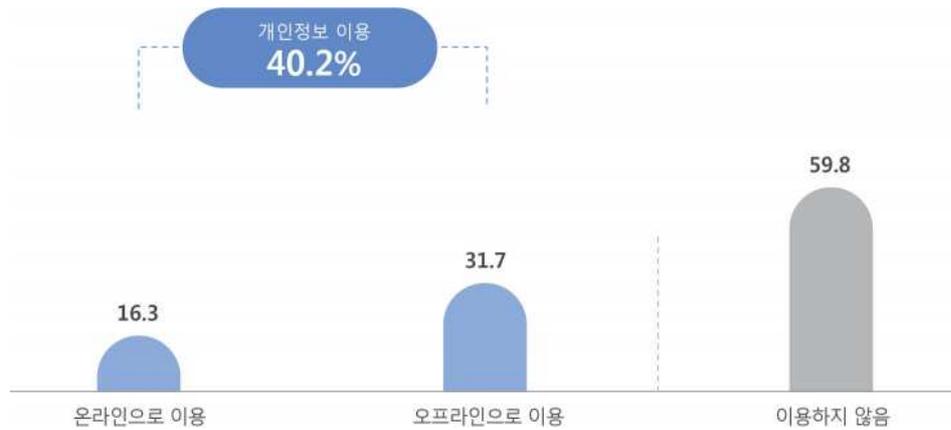


나. 개인정보 이용

국내 사업체 중 40.2%는 고객의 개인정보를 온라인 또는 오프라인으로 이용하는 것으로 나타났다.

그림 1-3-87 개인정보 이용 (복수응답)

(단위 : %)



다. 개인정보 수집 및 이용 현황

개인정보를 수집하는 사업체가 수집 및 이용하는 고객의 일반정보는 '성명'이 94.9%로 가장 높게 나타났고, 다음으로 '휴대전화 번호(93.5%)', '(집 또는 회사)주소(76.4%)' 등의 순으로 조사되었다.

그림 1-3-88 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 11.0%로 가장 높게 나타났고, 다음으로 '의료정보(과거 의료기록, 가족병력, 의약이력 등)(6.0%)' 등의 순으로 조사되었다.

그림 1-3-89

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 82.2%로 가장 높게 나타났고, 다음으로 '회원가입 시 본인인증(21.3%)', '결제(17.7%)' 등의 순으로 조사되었다.

그림 1-3-90

개인정보 수집 및 이용 목적 - 개인정보 수집 사업체

(단위 : %)



2. 개인정보 침해사고 예방

가. 개인정보 침해사고 예방을 위한 관리적 조치

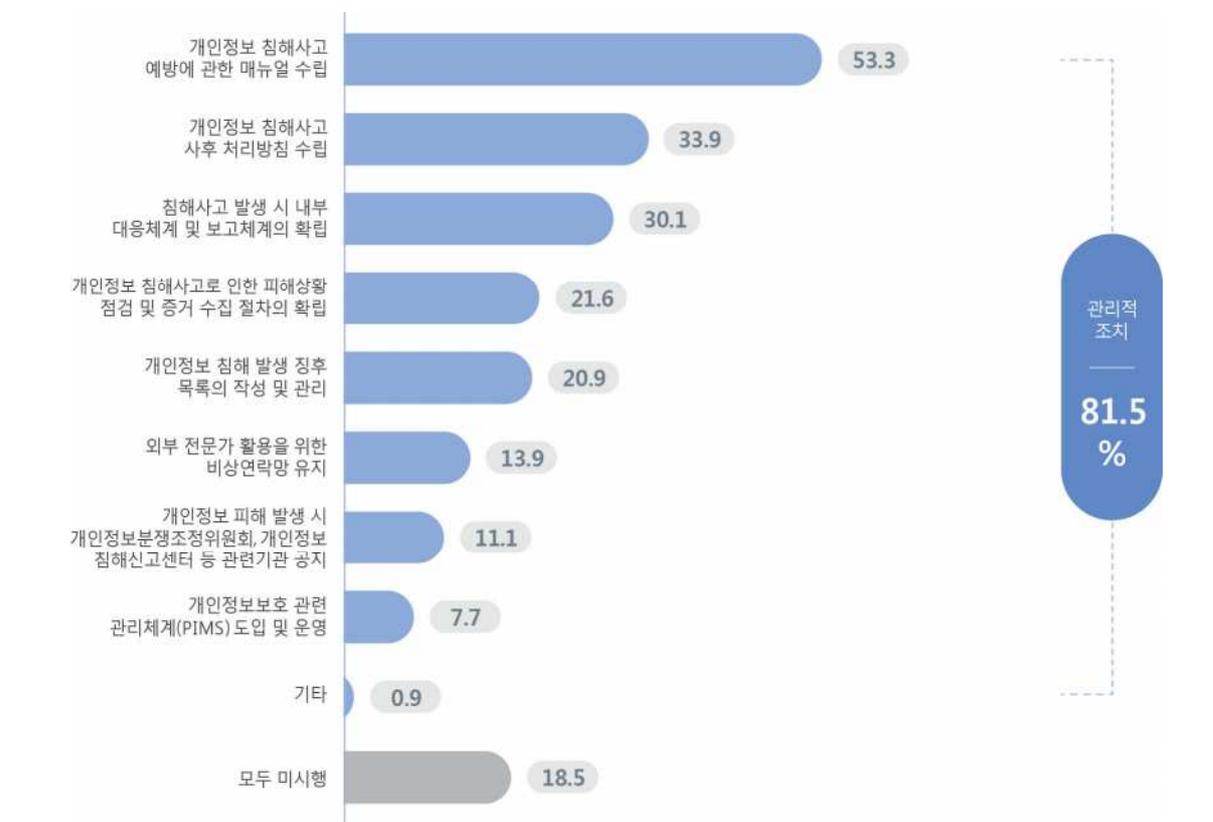
고객의 개인정보를 수집하는 사업체 중 81.5%가 개인정보 침해사고의 예방 및 사후처리를 위한 관리적 조치를 취하고 있는 것으로 나타났다.

유형별로는 '개인정보 침해사고 예방에 관한 매뉴얼 수립'이 53.3%로 가장 높게 나타났고, 다음으로 '개인정보 침해사고 사후 처리방침 수립(33.9%)' 등의 순으로 조사되었다.

그림 1-3-91

개인정보 침해사고 예방을 위한 관리적 조치 (복수응답) - 개인정보 수집 사업체

(단위 : %)

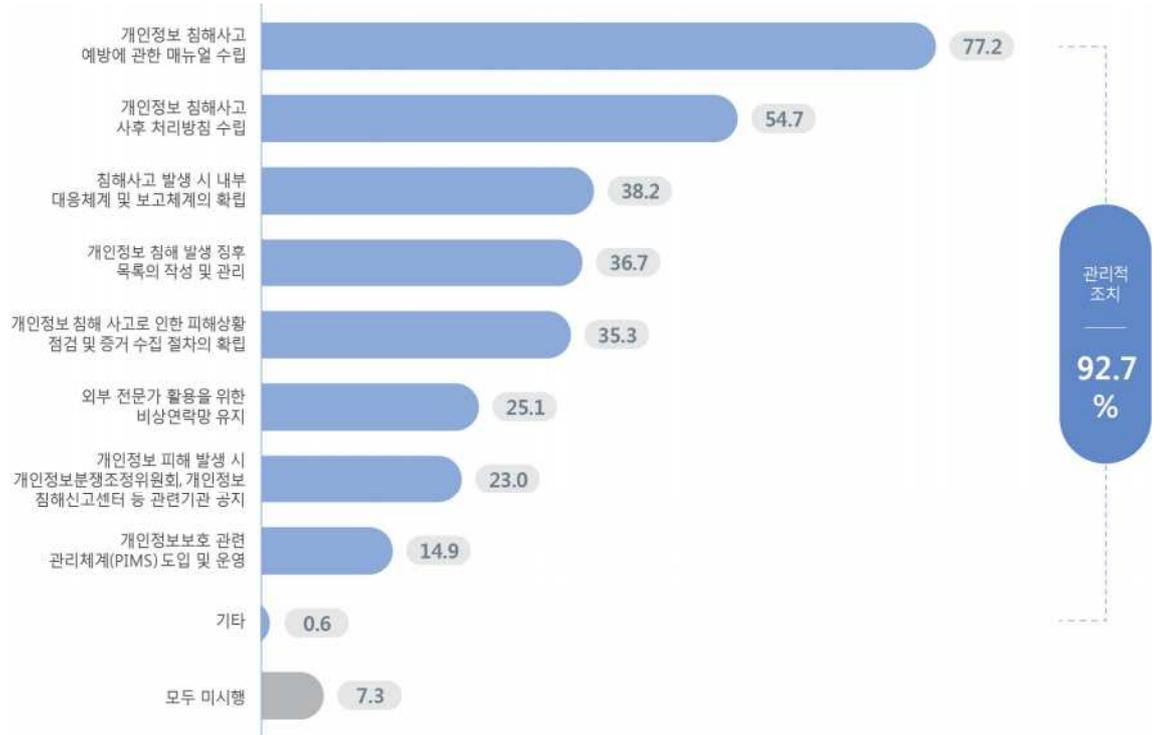


▶ **참고** 응답 기준을 온라인으로 고객의 개인정보를 수집한 사업체로 한정된 경우

그림 1-3-92

개인정보 침해사고 예방을 위한 관리적 조치 (복수응답) - 온라인으로 개인정보 수집 사업체

(단위 : %)



나. 개인정보 침해사고 예방을 위한 기술적 조치

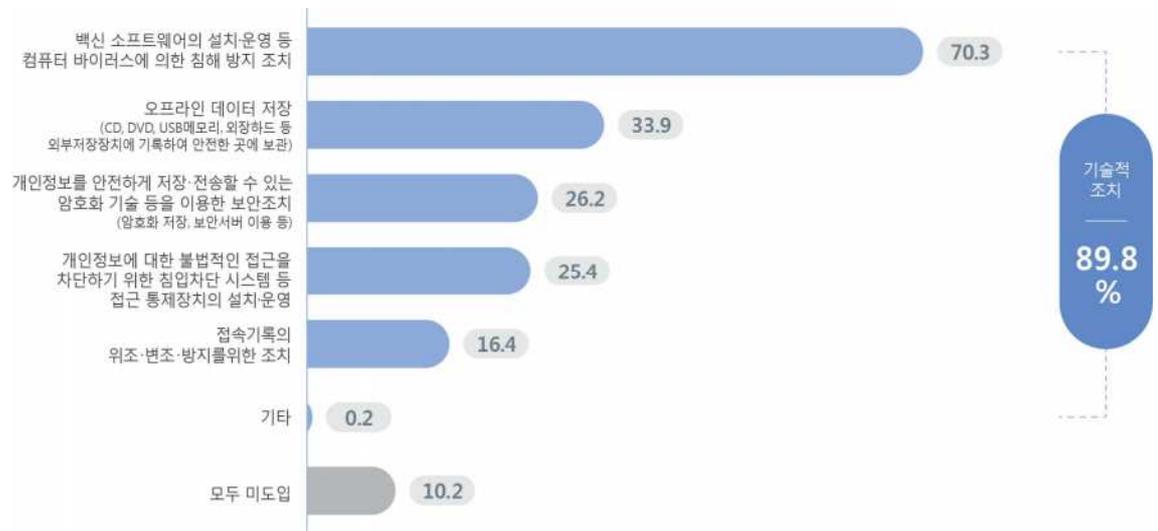
고객의 개인정보를 수집하는 사업체 중 89.8%가 개인정보 침해사고의 예방을 위한 기술적 조치를 도입하고 있는 것으로 나타났다.

유형별로는 '백신 소프트웨어의 설치·운영 등 컴퓨터 바이러스에 의한 침해 방지 조치'가 70.3%로 가장 높게 나타났고, 다음으로 '오프라인 데이터 저장(33.9%)' 등의 순으로 조사되었다.

그림 1-3-93

개인정보 침해사고 예방을 위한 기술적 조치 (복수응답) - 개인정보 수집 사업체

(단위 : %)

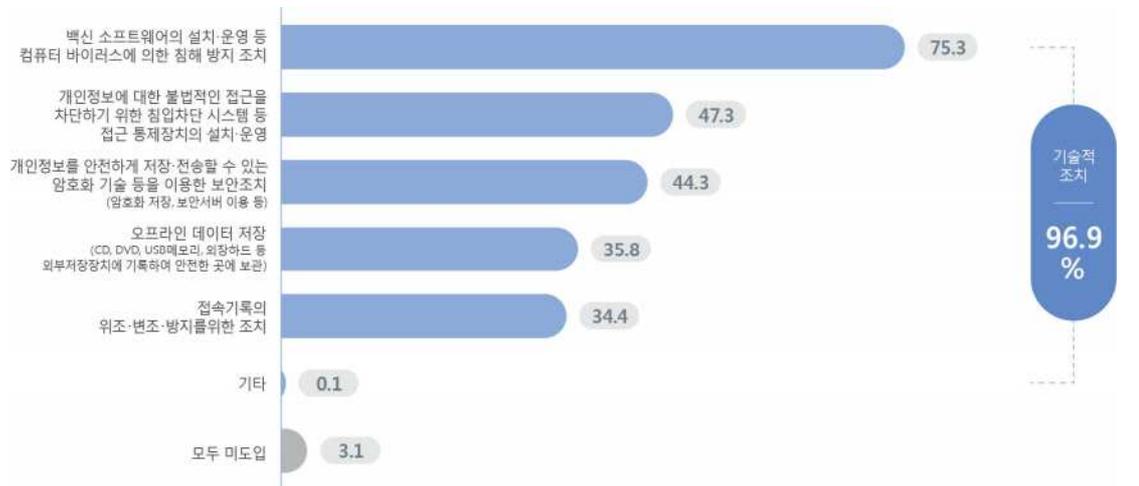


▶ 참고 응답 기준을 온라인으로 고객의 개인정보를 수집한 사업체로 한정된 경우

그림 1-3-94

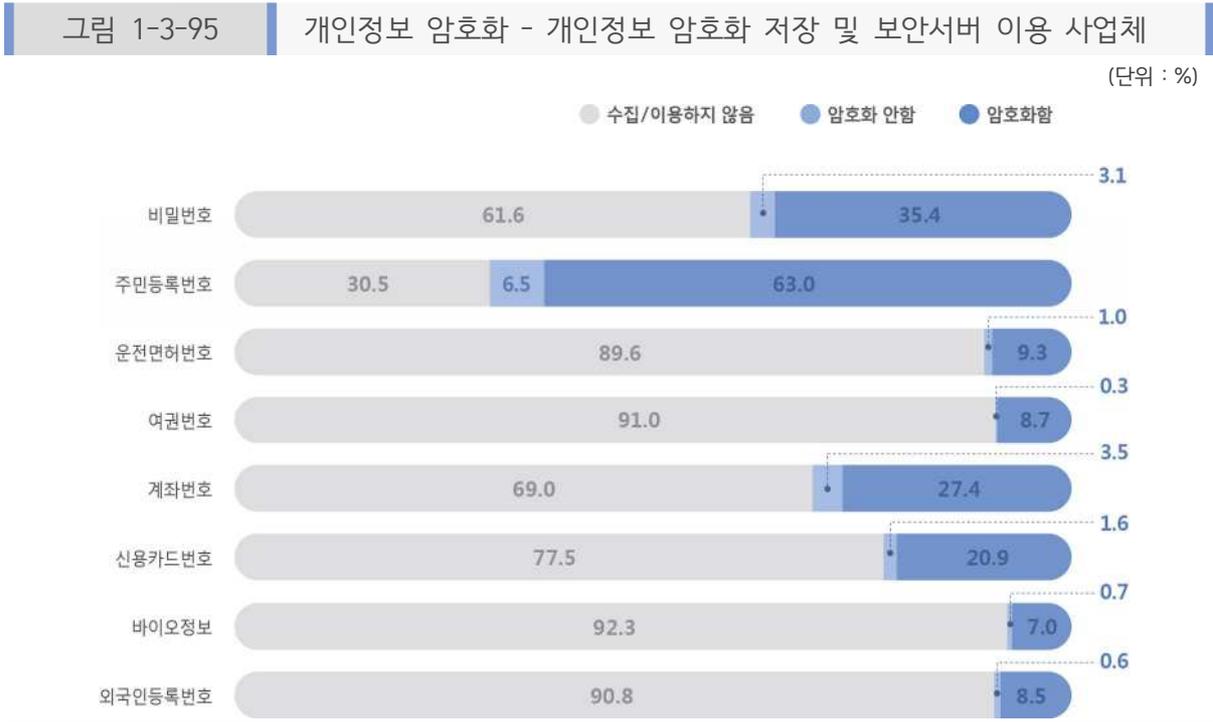
개인정보 침해사고 예방을 위한 기술적 조치 (복수응답) - 온라인으로 개인정보 수집 사업체

(단위 : %)



다. 개인정보 암호화

고객의 개인정보를 암호화하여 저장하거나 보안서버를 이용하는 사업체가 암호화를 실시하는 개인정보는 '주민등록번호'가 63.0%로 가장 높게 나타났고, 다음으로 '비밀번호 (35.4%)', '계좌번호(27.4%)' 등의 순으로 조사되었다.



3. 개인정보 침해사고 경험

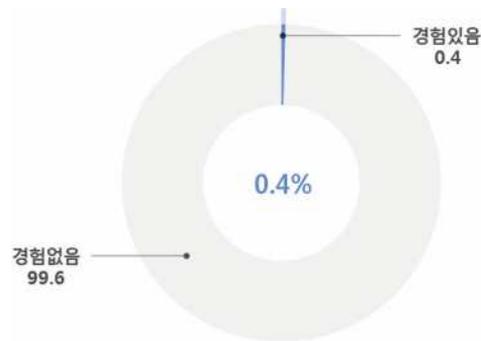
가. 개인정보 침해사고 경험

고객의 개인정보를 수집하는 사업체 중 0.4%가 고객의 개인정보가 유출되는 침해사고를 경험한 것으로 나타났다.

그림 1-3-96

개인정보 침해사고 경험 - 개인정보 수집 사업체

(단위 : %)



나. 개인정보 침해사고 시 관계기관 문의 또는 신고

고객의 개인정보 침해사고를 경험한 사업체 중 43.6%가 해당 침해사고 발생 시 관계기관에 문의 또는 신고한 것으로 나타났다.

그림 1-3-97

개인정보 침해사고 시 관계기관 문의 또는 신고 - 개인정보 침해사고 경험 사업체

(단위 : %)



* 개인정보 침해사고 시 관계기관에 문의 또는 신고 문항은 사례수(n=17)가 적어 해석에 유의해야함

다. 개인정보 침해사고 시 통지 또는 고지

고객의 개인정보 침해사고를 경험한 사업체 중 17.8%가 해당 침해사고의 발생 사실을 고객에게 통지 또는 고지한 것으로 나타났다.

그림 1-3-98

개인정보 침해사고 시 통지 또는 고지 - 개인정보 침해사고 경험 사업체

(단위 : %)



* 개인정보 침해사고 시 통지 또는 고지 문항은 사례수(n=17)가 적어 해석에 유의해야함

VI 주요 서비스별 정보보호

1. 무선랜

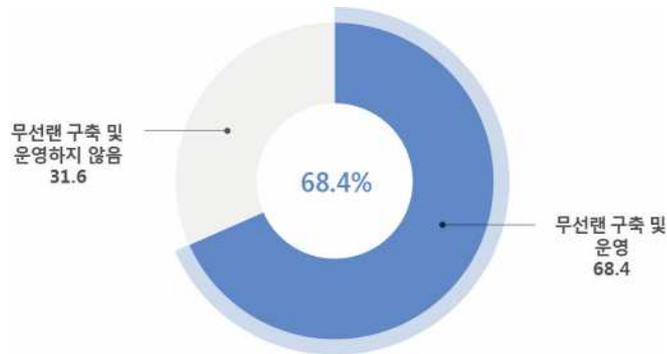
가. 무선랜 구축 및 운영

국내 네트워크 구축 사업체 중 68.4%가 사내에서 무선랜을 구축하여 운영하고 있는 것으로 나타났다.

그림 1-3-99

무선랜 구축 및 운영

(단위 : %)



나. 무선랜 보안

사내 무선랜의 이용과 관련한 보안 우려사항은 '무선공유기(AP)를 통한 악성코드 감염'이 31.5%로 가장 높게 나타났고, 다음으로 '무선공유기(AP)의 DDoS 등 공격도구로 악용(30.5%)' 등의 순으로 조사되었다.

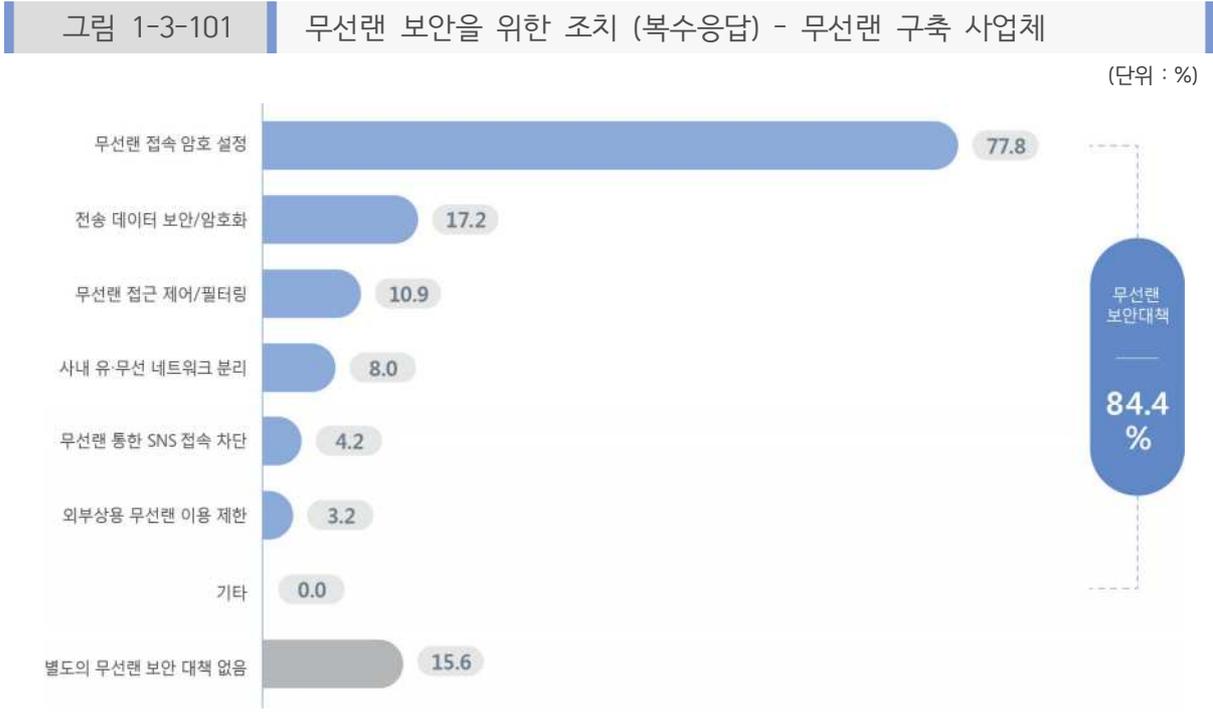
그림 1-3-100

무선랜 보안 우려사항 (2가지) - 무선랜 구축 사업체

(단위 : %)



사내 무선랜 보안을 위해 실행하고 있는 조치는 '무선랜 접속 암호 설정'이 77.8%로 가장 높게 나타났고, 다음으로 '전송 데이터 보안/암호화(17.2%)', '무선랜 접근 제어/필터링 (10.9%)' 등의 순으로 조사되었다.



▶ 참고 응답 기준을 무선랜 보안조치를 실행한 사업체로 한정된 경우



2. 모바일

가. 모바일 기기 업무 활용

개인소유의 모바일 기기(스마트폰, 스마트패드, 노트북 등)를 업무에 활용하는 사업체는 15.4%로 나타났다.

그림 1-3-103 | 개인소유 모바일 기기 업무 활용

(단위 : %)



한편, 회사소유의 모바일 기기를 업무에 활용하고 있는 비율은 10.4%로 조사되었다.

그림 1-3-104 | 회사소유 모바일 기기 업무 활용

(단위 : %)



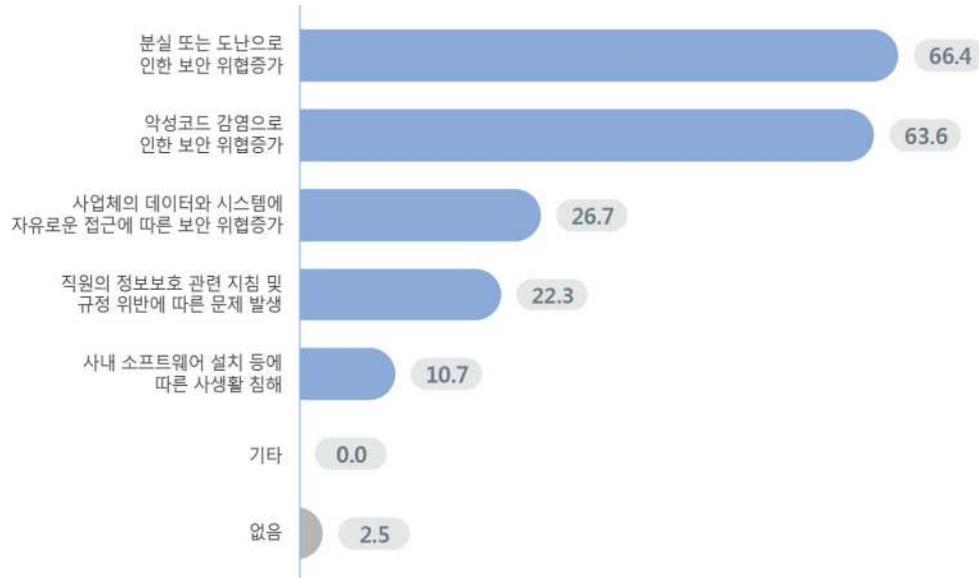
나. 모바일 보안

개인소유의 모바일 기기를 업무에 활용 시 보안 우려사항은 '분실 또는 도난으로 인한 보안 위협증가'가 66.4%로 가장 높게 나타났고, 다음으로 '악성코드 감염으로 인한 보안 위협증가(63.6%)' 등의 순으로 조사되었다.

그림 1-3-105

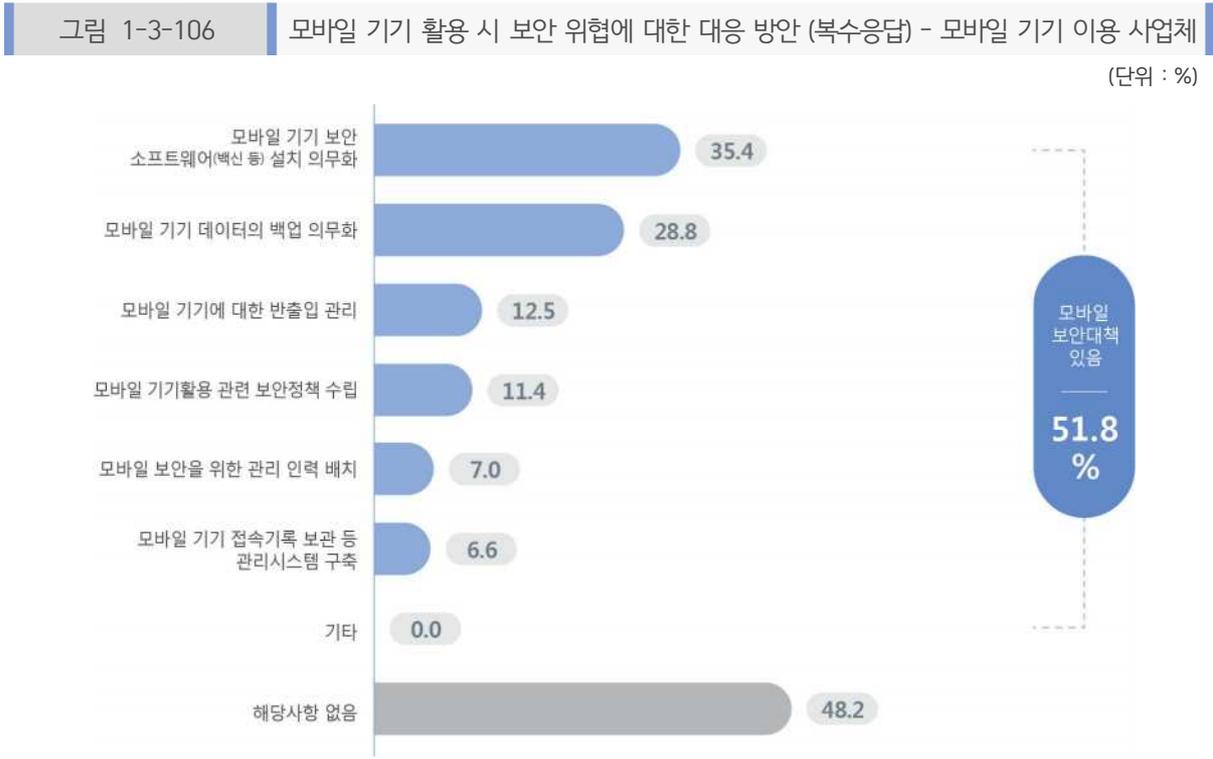
개인 모바일 기기 활용 시 보안 우려사항 (2가지) - 개인 소유 모바일 기기 이용 사업체

(단위 : %)



업무에 모바일 기기를 활용하는 사업체 중 51.8%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 35.4%로 가장 높게 나타났고, 다음으로 '모바일 기기 데이터의 백업 의무화(28.8%)' 등의 순으로 조사되었다.



3. 클라우드

가. 클라우드 서비스 이용

국내 사업체 중 7.4%가 클라우드 서비스를 현재 이용하고 있는 것으로 나타났다.

그림 1-3-107 클라우드 서비스 이용

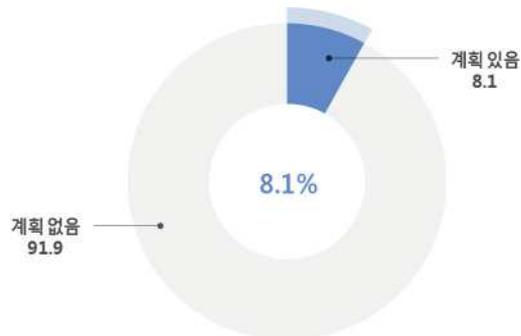
(단위 : %)



한편, 클라우드 서비스를 향후에 신규로 도입할 계획이 있거나, 현재 이용 중인 클라우드 서비스를 유지할 계획이 있는 사업체의 비율은 8.1%로 조사되었다.

그림 1-3-108 클라우드 서비스 향후 도입(유지) 계획

(단위 : %)



현재 이용하고 있거나 향후에 신규로 도입할 계획이 있는 클라우드 분야는 '백업·복구 서비스'가 79.7%로 가장 높게 나타났고, 다음으로 '컴퓨팅(서버, 스토리지 등) 자원 (36.6%)' 등의 순으로 조사되었다.

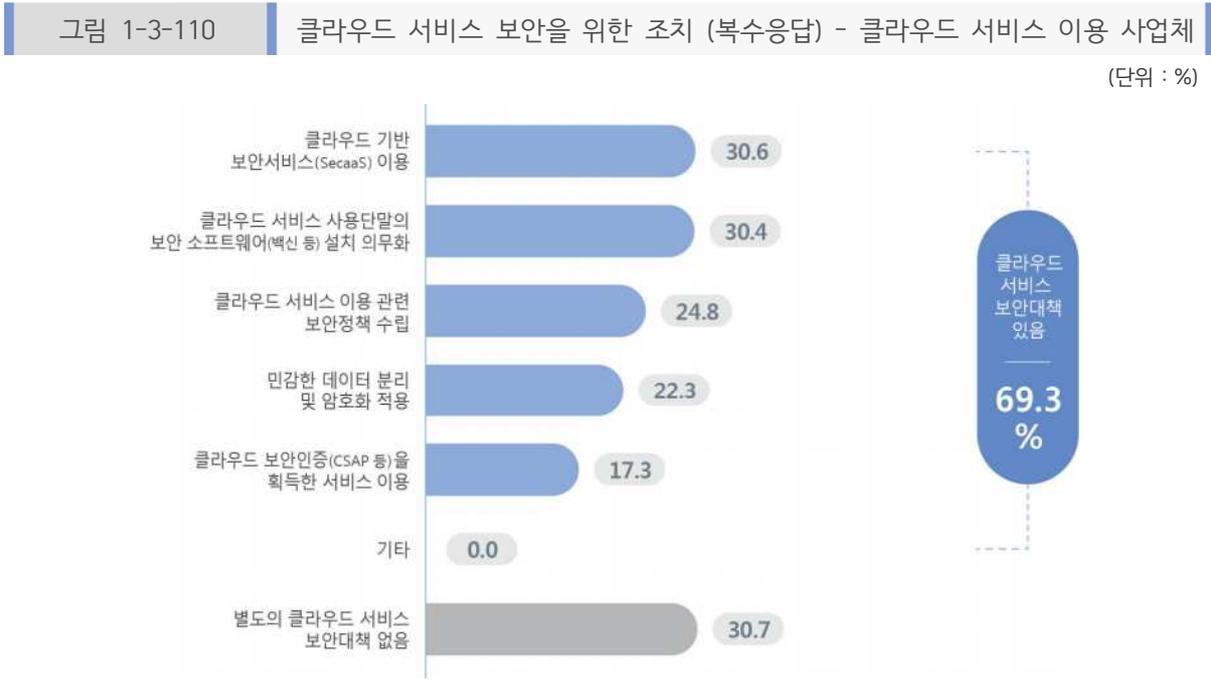
그림 1-3-109 클라우드 서비스 이용(계획) 분야 (복수응답) - 클라우드 서비스 이용 또는 향후 계획 사업체 (단위 : %)



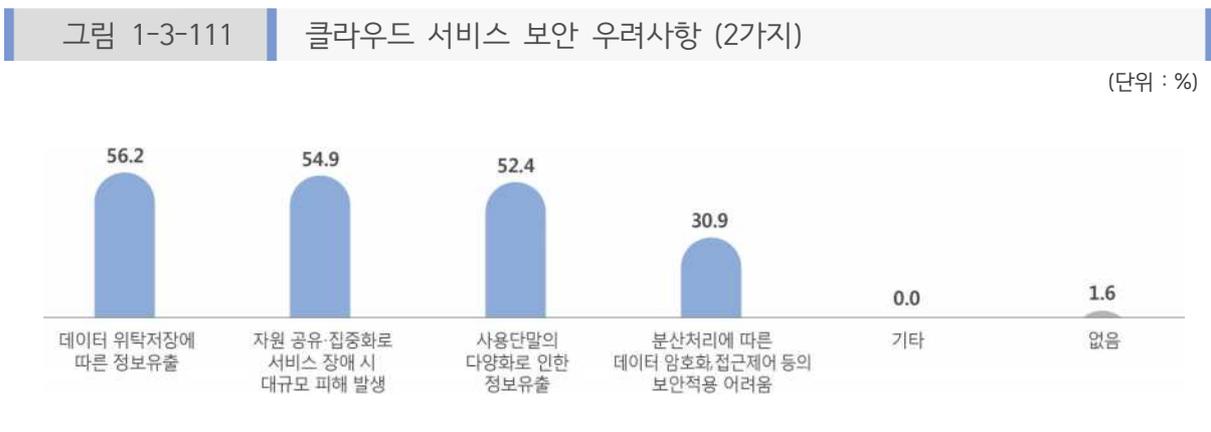
나. 클라우드 보안

클라우드 서비스를 현재 이용하고 있는 사업체 중 69.3%가 클라우드 서비스 보안을 위한 조치를 취하고 있는 것으로 나타났다.

조치 유형별로는 '클라우드 기반 보안서비스(SecaaS) 이용'이 30.6%로 가장 높게 나타났고, 다음으로 '클라우드 서비스 사용단말의 보안 소프트웨어(백신 등) 설치 의무화(30.4%)' 등의 순으로 조사되었다.



클라우드 서비스 이용과 관련하여 발생할 수 있는 보안 우려사항은 '데이터 위탁저장에 따른 정보유출'이 56.2%로 가장 높게 나타났고, 다음으로 '자원 공유·집중화로 서비스 장애 시 대규모 피해 발생(54.9%)' 등의 순으로 조사되었다.



4. 사물인터넷(IoT)

가. 사물인터넷(IoT) 제품·서비스 이용

국내 사업체 중 9.1%가 사물인터넷(IoT) 제품 또는 서비스를 현재 이용하고 있는 것으로 나타났다.

그림 1-3-112 사물인터넷(IoT) 제품·서비스 이용

(단위 : %)



한편, 사물인터넷(IoT) 제품 또는 서비스를 향후에 신규로 도입할 계획이 있거나, 현재 이용 중인 제품 또는 서비스를 유지할 계획이 있는 사업체의 비율은 10.9%로 조사되었다.

그림 1-3-113 사물인터넷(IoT) 제품·서비스 향후 도입(유지) 계획

(단위 : %)



현재 이용하고 있거나 향후에 신규로 도입할 계획이 있는 사물인터넷(IoT) 분야는 'CCTV'가 95.3%로 가장 높게 나타났고, 다음으로 '금융 서비스(8.5%)', '제조(2.2%)' 및 '에너지(2.2%)' 등의 순으로 조사되었다.

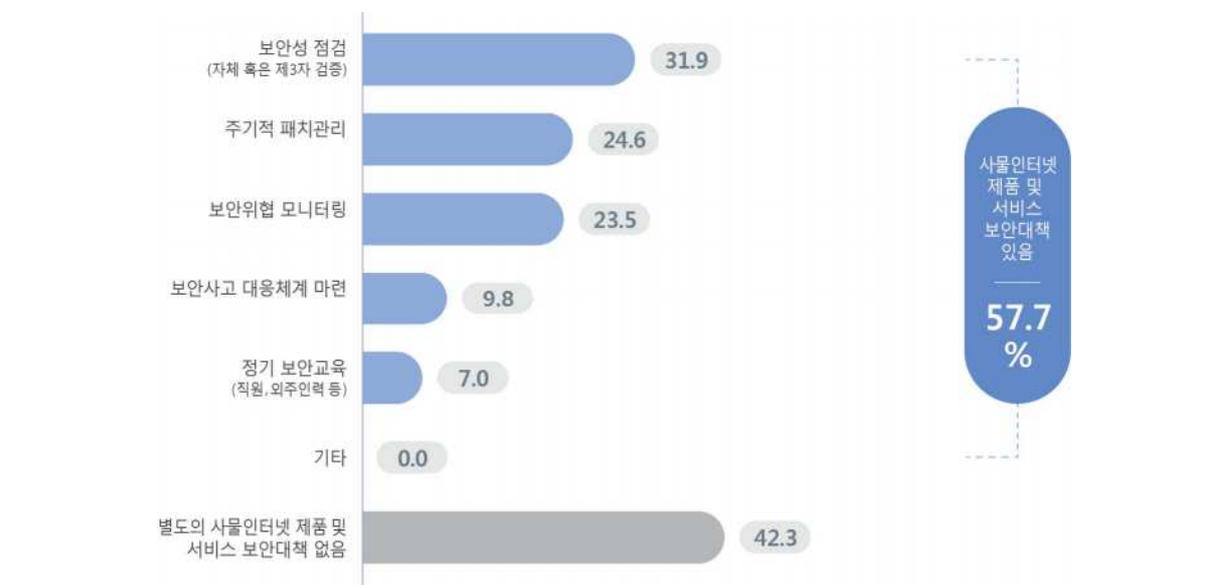
그림 1-3-114 사물인터넷(IoT) 이용(계획) 분야 (복수응답) - 사물인터넷(IoT) 이용 또는 향후 계획 사업체 (단위 : %)



나. 사물인터넷(IoT) 보안

사물인터넷(IoT) 제품 또는 서비스 이용 사업체 중 57.7%가 사물인터넷(IoT) 제품 및 서비스의 보안을 위해 조치를 취하고 있는 것으로 나타났다.

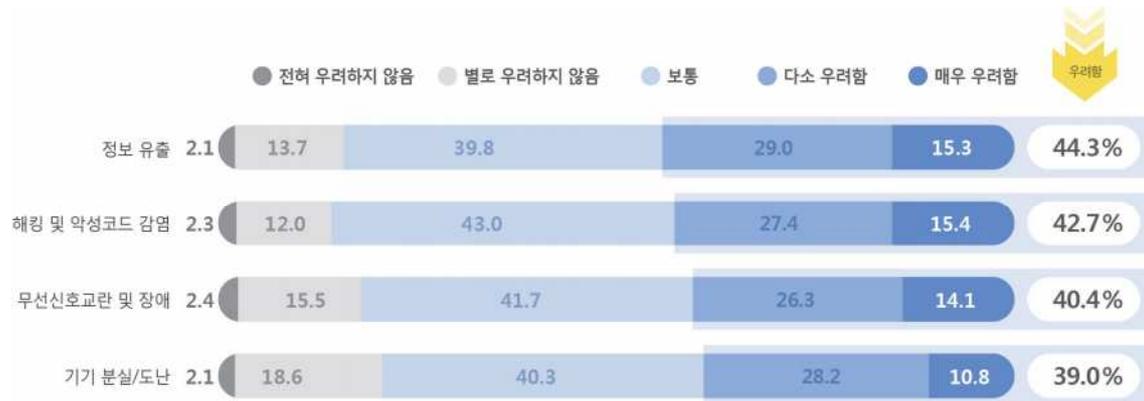
그림 1-3-115 사물인터넷(IoT) 제품·서비스 보안을 위한 조치 (복수응답) - 사물인터넷(IoT) 이용 사업체 (단위 : %)



사물인터넷(IoT) 환경에서 발생할 수 있는 보안위협에 대한 우려 정도(다소 우려함 + 매우 우려함)는 '정보 유출'이 44.3%로 가장 높게 나타났고, 다음으로 '해킹 및 악성코드 감염 (42.7%)' 등의 순으로 조사되었다.

그림 1-3-116 사물인터넷(IoT) 관련 보안 우려사항

(다소 우려함 + 매우 우려함, 단위 : %)



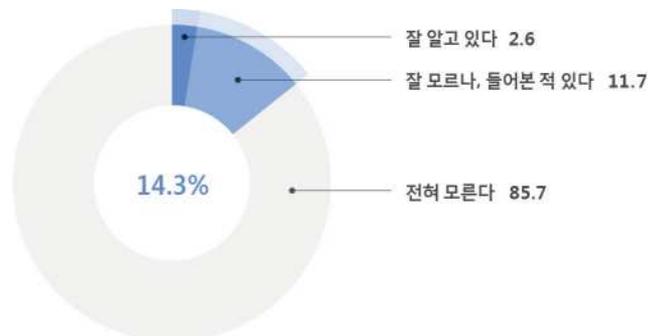
5. 정보보호(사이버) 보험

가. 정보보호(사이버) 보험 인지

국내 사업체 중 14.3%가 정보보호(사이버) 보험에 대해 인지(잘 모르나, 들어본 적 있다 + 잘 알고 있다)하고 있는 것으로 나타났다.

그림 1-3-117 정보보호(사이버) 보험 인지

(단위 : %)



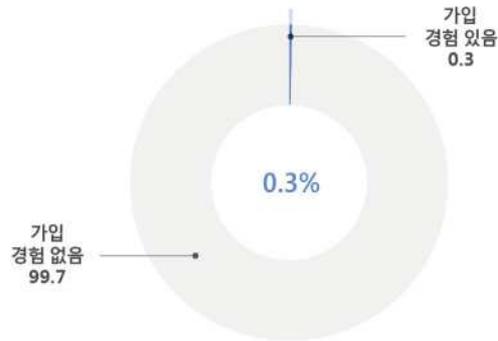
나. 정보보호(사이버) 보험 이용

국내 사업체 중 0.3%가 정보보호(사이버) 보험에 가입한 경험이 있는 것으로 나타났다.

그림 1-3-118

정보보호(사이버) 보험 가입

(단위 : %)

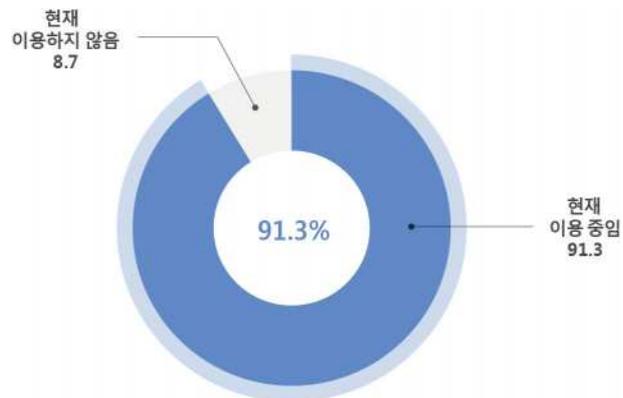


정보보호(사이버) 보험 가입 경험이 있는 사업체 중 91.3%가 현재 이용 중인 것으로 나타났다.

그림 1-3-119

정보보호(사이버) 보험 이용 - 정보보호(사이버) 보험 가입 사업체

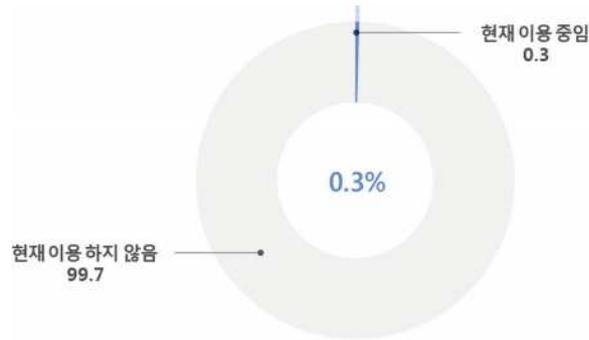
(단위 : %)



▶ 참고 응답 기준을 전체 사업체로 확대한 경우

그림 1-3-120 정보보호(사이버) 보험 이용

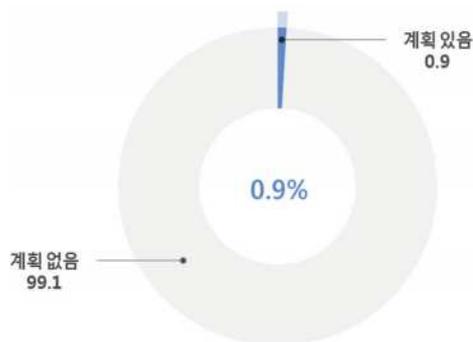
(단위 : %)



향후 정보보호(사이버) 보험을 신규로 가입하거나, 현재 이용 중인 보험을 유지할 계획이 있는 사업체의 비율은 0.9%로 나타났다.

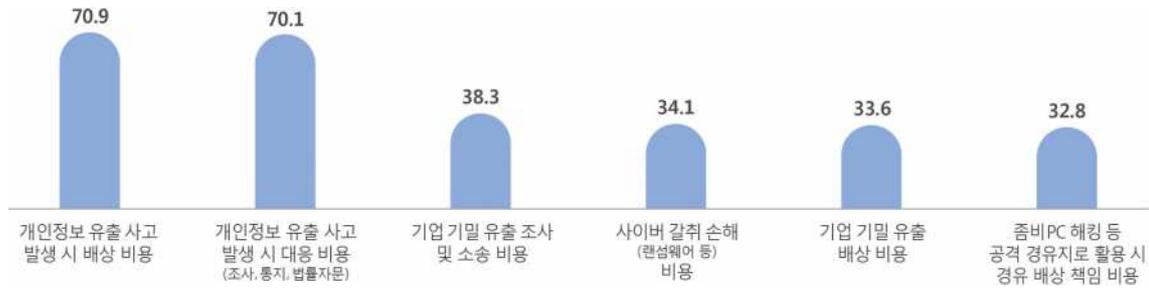
그림 1-3-121 정보보호(사이버) 보험 향후 가입(유지) 계획

(단위 : %)



정보보호(사이버) 보험을 향후 신규로 가입할 계획이 있는 사업체가 희망하는 보장 항목은 '개인정보 유출 사고 발생 시 배상 비용'이 70.9%로 가장 높게 나타났고, 다음으로 '개인정보 유출 사고 발생 시 대응 비용(70.1%)' 등의 순으로 조사되었다.

그림 1-3-122 정보보호(사이버) 보험 희망 보장 항목 (복수응답) - 향후 가입 계획 사업체 (단위 : %)



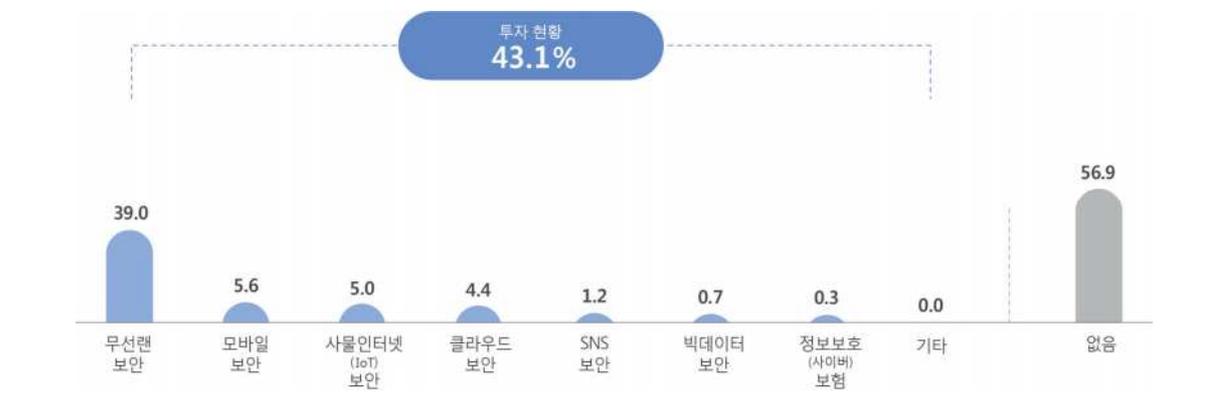
6. 주요 서비스 정보보호 투자

가. 주요 서비스 정보보호 투자 현황

국내 사업체 중 43.1%가 현재 정보보호를 위해 IT보안 분야에 투자를 하고 있는 것으로 나타났다.

투자 유형별로는 '무선랜 보안'이 39.0%로 가장 높게 나타났고, 다음으로 '모바일 보안 (5.6%)', '사물인터넷(IoT) 보안(5.0%)' 등의 순으로 조사되었다.

그림 1-3-123 주요 서비스 정보보호 투자 현황 (복수응답) (단위 : %)



나. 주요 서비스 정보보호 투자 계획

국내 사업체 중 28.2%가 향후 정보보호를 위해 IT보안 분야에 투자할 계획을 보유하고 있는 것으로 나타났다.

신규 투자 유형별로는 '무선랜 보안'이 24.1%로 가장 높게 나타났고, 다음으로 '모바일 보안(4.9%)', '사물인터넷(IoT) 보안(3.7%)' 등의 순으로 조사되었다.

그림 1-3-124 주요 서비스 정보보호 투자 계획 (복수응답)

(단위 : %)





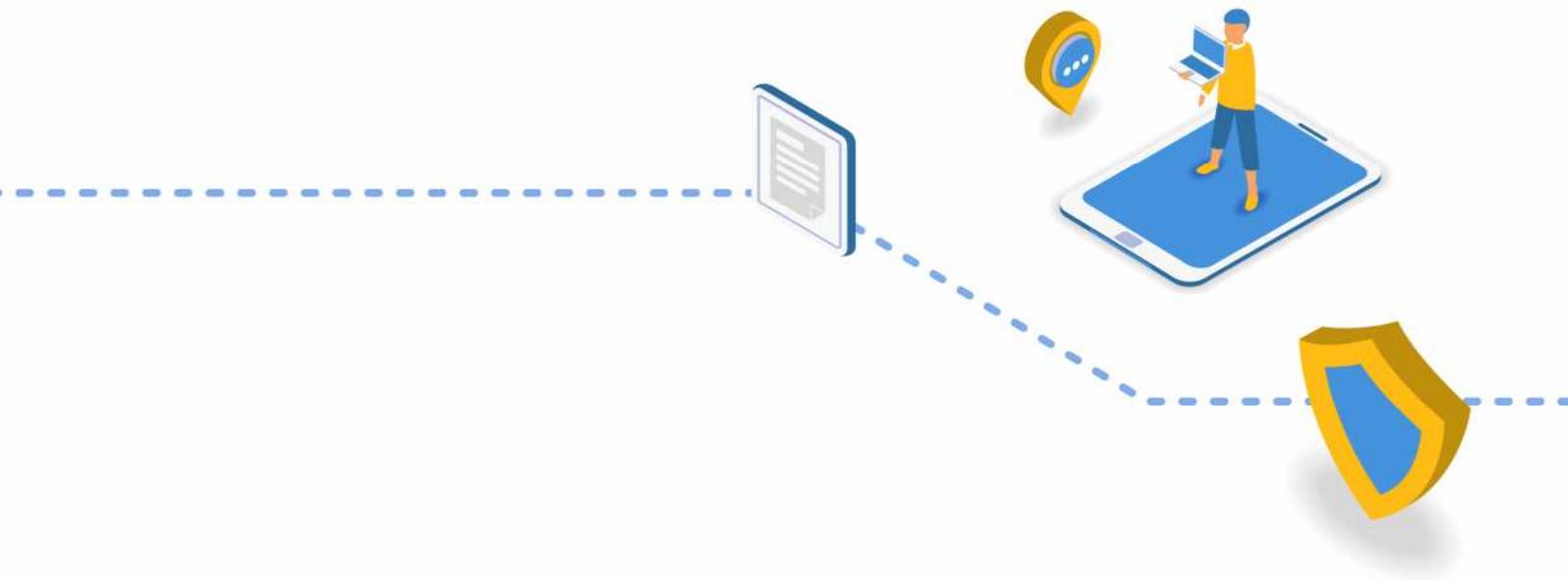


2부

개인부문

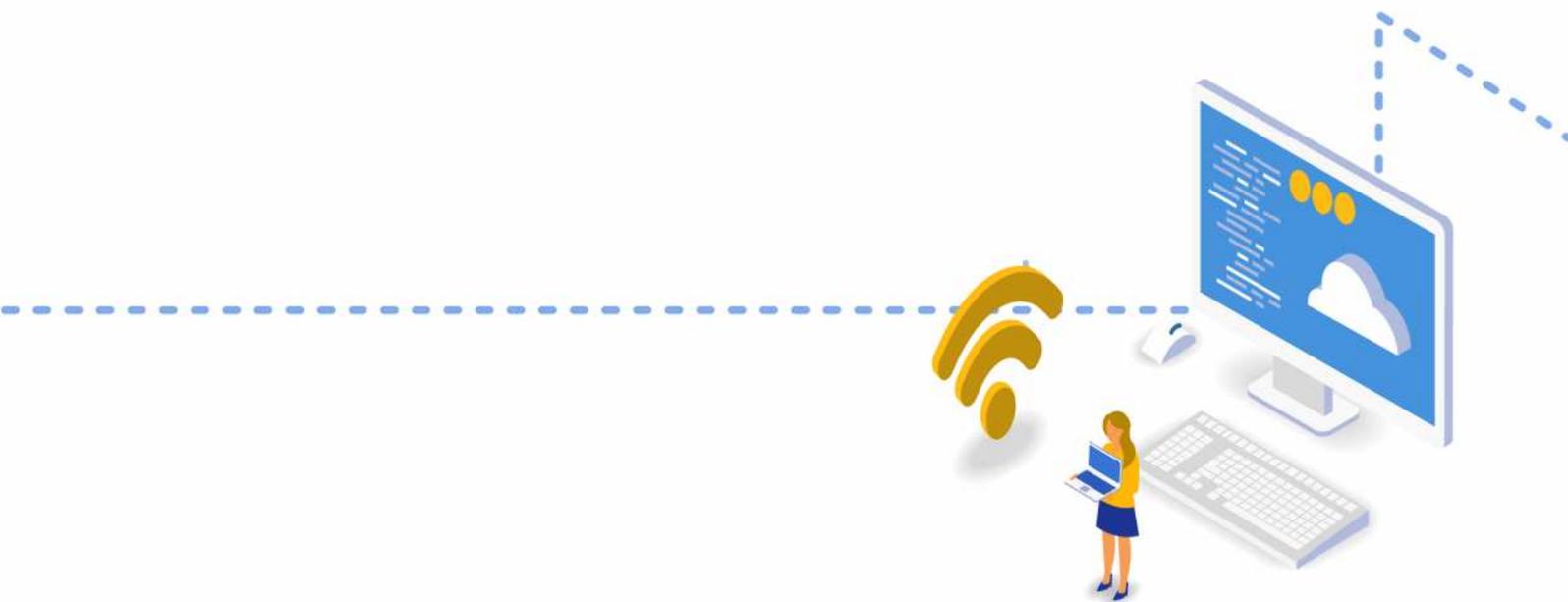






제1장

조사개요



제1장 조사개요

1. 조사 목적

급속하게 변화하는 인터넷 환경과 사물인터넷(IoT), 핀테크, 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 실시 하였다.

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
- '2005년 인구주택총조사 조사구'로 표본추출틀 변경
- 조사구 추출-가구 추출-가구원 추출의 다단계층화추출로 표본추출 방법 변경
- 2012년 - '2010년 인구주택총조사'와 '2011년 인터넷이용실태조사' 결과를 기반으로 표본 재설계
- '2010년 인구주택총조사 조사구'로 표본추출틀 변경
- 2013년 - 한국인터넷진흥원에서 미래창조과학부로 통계작성기관 변경
- '2010년 인구주택총조사'와 '2012년 인터넷이용실태조사' 결과를 기반으로 표본 재설계
- '2010년 인구주택총조사 조사구'를 표본추출틀 활용
- 2014년 - '2010년 인구주택총조사'와 '2013년 추계인구', '2013년 인터넷이용실태조사' 결과를 기반으로 표본 재설계
- '2010년 인구주택총조사 조사구'를 표본추출틀 활용
- 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 - 승인번호체계가 5자리에서 6자리로 변경(2016.08.28.)(제34205호→제342005호)
- 2017년 - '2010년 인구주택총조사'와 '2016년 추계인구', '2016년 인터넷이용 실태조사' 결과를 기반으로 표본 재설계
- 추정 오차 감소를 위해 조사구 수 확대(400개 → 800개)
- 조사구 내 추출 가구 수 감소(조사구 당 10가구 → 조사구 당 5가구)
- 통계작성기관명 변경(미래창조과학부 → 과학기술정보통신부)
- 2018년 - '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

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 침해사고 예방·대응 조치
- 주요 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
- **사물인터넷(IoT)** : Internet of things의 약자로 모든 사물을 인터넷으로 연결하여 사람과 사물, 사물과 사물 간의 정보를 상호 소통하는 지능형 기술 및 서비스
- **빅데이터(Big data)** : 개인의 인터넷 이용 정보, 위치정보, 신용카드 정보 등 다량의 데이터를 분석하여 이용자 편의에 맞는 서비스 제공
- **간편결제** : 최초 서비스 가입 시 본인인증 및 신용카드 정보 입력을 거친 후, 간단한 비밀번호 및 패턴암호만으로 손쉽게 결제가 가능한 서비스
- **인공지능 서비스(AI)** : 인간의 지능으로 할 수 있는 학습, 추론, 지각, 언어이해 등의 사고 및 행동을 컴퓨터 프로그램으로 실현한 인공지능(AI) 기술이 활용된 서비스

5. 조사 체계

- 조사대상 : 최근 1개월 내 인터넷 이용자(만 12~69세)
* 60~69세는 2018년에 신규 조사대상으로 추가
- 유효응답자수 : 4,000명
- 조사주기 : 연 1회
- 조사기간 : 2018년 7월 23일 ~ 9월 22일 (2개월)
- 조사방법 : 가구방문 면접조사
- 조사기관
 - 주관기관 : 과학기술정보통신부(Ministry of Science and ICT)
 - 전담기관 : 한국인터넷진흥원(Korea Internet & Security Agency)
- 법적근거
 - 정보통신망이용촉진 및 정보보호 등에 관한 법률 제52조 제3항
 - 통계법 제18조(통계작성의 승인)

6. 표본 설계

가. 모집단

- 목표 모집단(Target Population) : 국내 만 12~69세 인터넷 이용자
- 조사 모집단(Survey Population) : 국내 만 12~69세의 인터넷 이용자 중 최근 1개월 이내 인터넷 이용자
- 모집단 자료
 - 통계청 『2015년 인구주택총조사』 인구부문 결과, 『2017년 추계인구』 및 한국인터넷진흥원의 『2017년 인터넷이용실태조사』에서 파악된 지역별, 성별, 연령대별 국내 인터넷이용률을 이용하여 파악한 최근 1개월 이내 인터넷 이용자 수 및 분포 활용
 - 단, 통계청 조사구 중 보통조사구와 아파트조사구를 조사모집단으로 정의함

나. 표본 추출

- 개요 : 다단계층화추출법(multi-stage stratified sampling)
 - 17개 시도별 인터넷 이용자 크기에 비례하여 800개 조사구를 배분하고, 각 조사구에서 평균 5가구씩 추출하여 가구 내에서 적격 조사대상자를 선정·조사
- 표본의 규모산정
 - 표본오차(허용오차)별 표본의 크기를 계산한 결과는 아래와 같음

표 2-1-1	표본오차별 표본의 크기								
	(단위 : 명, %)								
표본의 크기	3,000	3,500	3,600	3,800	3,900	4,000	4,100	4,200	4,300
표본오차	1.19	1.10	1.08	1.06	1.04	1.03	1.02	1.00	0.99

- 최종 표본의 크기는 표본오차가 $\pm 1.03\%p$ 내에서 통제되도록 4,000명으로 결정함 (95% 신뢰수준)
- 층화변수
 - 권역(17개) : 서울, 부산, 대구, 인천, 광주, 대전, 울산, 경기, 강원, 충북, 충남, 전북, 전남, 경북, 경남, 제주, 세종
 - 성(2개) : 남성, 여성
 - 연령(6개) : 만12~19세, 20대, 30대, 40대, 50대, 60대
- 표본틀 : 통계청 2015년 '인구주택총조사', 2017년 '추계인구' 및 한국인터넷진흥원 '2017년 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 4,000명을 지역별 제곱근비례할당 후, 각 지역에 표본을 우선 할당하고, 성X연령 셀에 할당하는 방법을 최종 표본 할당방법으로 결정함

② 조사구 할당

- 조사구당 5명이 조사되도록 총 800개 조사구 배분
- 1차 : 17개 시도별 조사구 배분
 - * 통계청의 『2015년 인구주택총조사』 인구부문 결과와 『2017년 추계인구』, 한국인터넷진흥원의 『2017년 인터넷이용실태조사』 인터넷 이용률 결과를 기반으로 17개 시도별 인터넷 이용자 크기에 비례하여 800개 조사구 배분
- 2차 : 시도 내 주거형태별 조사구 배분
 - * 통계청의 『2015년 인구주택총조사』 기준 17개 시도별 주거 형태(아파트 및 아파트 외) 분포에 비례하여, 아파트 조사구와 비아파트 조사구 배분

③ 조사구 추출

- 325,628개 조사구를 행정구역 코드에 따라 정렬하여 계통 추출
- 계통 추출 17개 지역*2개 동읍면부*4개 주거형태별 셀 내에 조사구를 행정구역코드별로 정렬 후 계통 추출함
 - * 시도 내 조사구수 m 개, 목표 조사구수 n 개, $m/(n-1)$ 의 몫을 k 라고 할 때 시도별로 $1-m$ 범위 내에서 난수표를 사용하여 임의의 순번 i 번째 조사구를 첫 번째 조사구로 추출하고, 이어 $i+k, i+2k, i+3k... i+nk$ 번째 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 조사일자와 생일이 가장 가까운 가구원을 최종 조사대상자로 선정

7. 실사

가. 실사개요

- 조사기간
 - 2018년 7월 23일 ~ 9월 22일 (2개월)
- 조사기준
 - 2017년 7월 1일 ~ 2018년 6월 30일
 - 침해사고 경험은 2017년 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 『2015년 인구주택총조사』 인구부문 결과와 한국인터넷진흥원의 『2017년 인터넷이용 실태조사』 인터넷이용률 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 모바일에 대한 표본오차 산출 공식은 다음과 같음

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

$$\text{전체 모바일의 표본오차} - 1.96 \times \sqrt{\hat{V}(\hat{p}_{st})}$$

$$\text{층별 모바일의 표본오차} - 1.96 \times \sqrt{\hat{V}(\hat{p}_{hsk})}$$

$\hat{V}(\hat{p})$	전체 모바일에 대한 분산
$\hat{V}(\hat{p}_{hsh})$	층별 모바일에 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	±1.03%p (95% 신뢰수준)
정보보호 제품 이용률 추정 결과	87.32% ±1.03%p

10. 결과 공표 및 활용분야

- 『2018년 정보보호 실태조사(개인부문)』 보고서는 한국인터넷진흥원 홈페이지(<https://www.kisa.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

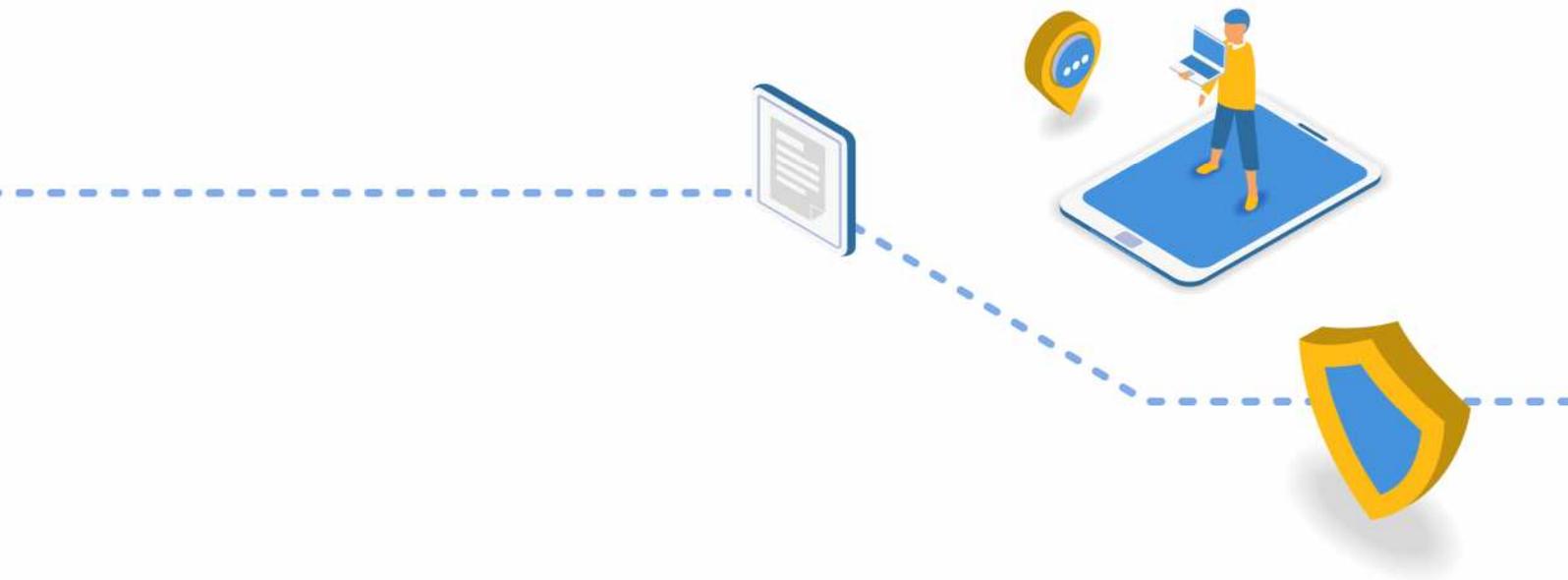
표 2-1-3

모집단 및 표본 현황

(단위 : %)

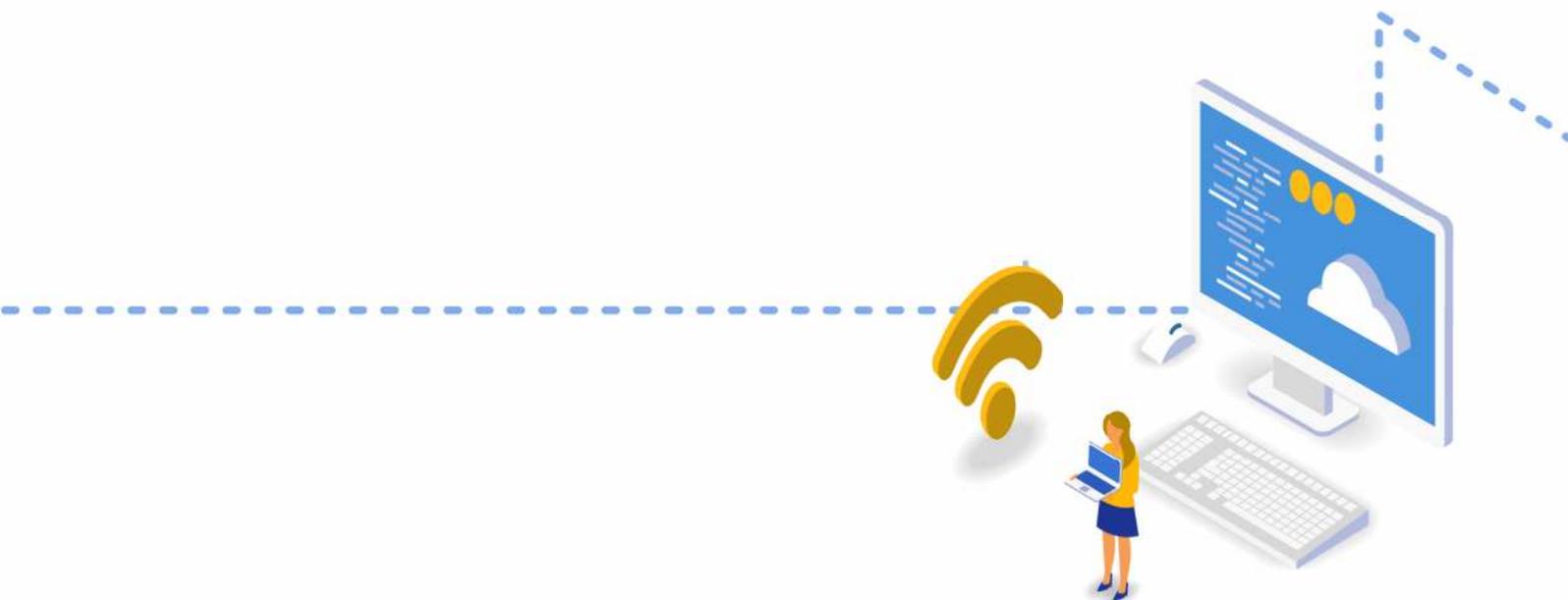
		만12~69세 최근 1개월 이내 인터넷이용자		응답 현황	
		모집단 수(명)	비율(%)	표본 수(명)	비율(%)
전 체		40,185,881	100.0	4,000	100.0
성 별	남	20,705,587	51.5	2,036	50.9
	여	19,480,294	48.5	1,964	49.1
연 령 별	12-19세	4,357,965	10.8	547	13.7
	20대	6,897,059	17.2	680	17.0
	30대	7,555,448	18.8	703	17.6
	40대	8,576,322	21.3	762	19.1
	50대	8,297,503	20.6	751	18.8
	60대	4,501,584	11.2	557	13.9
지 역 별	서울	7,847,830	19.5	473	11.8
	부산	2,753,708	6.9	276	6.9
	대구	1,967,044	4.9	239	6.0
	인천	2,316,288	5.8	260	6.5
	광주	1,198,704	3.0	185	4.6
	대전	1,229,358	3.1	190	4.8
	울산	957,883	2.4	165	4.1
	세종	207,406	0.5	77	1.9
	경기	10,060,701	25.0	537	13.4
	강원	1,112,653	2.8	178	4.5
	충북	1,204,811	3.0	186	4.7
	충남	1,641,162	4.1	212	5.3
	전북	1,372,794	3.4	201	5.0
	전남	1,255,218	3.1	195	4.9
	경북	1,986,074	4.9	237	5.9
경남	2,595,476	6.5	272	6.8	
제주	478,771	1.2	117	2.9	





제2장

조사결과 요약



I 정보보호 인식



1. 정보보호 중요성 인식



인터넷 이용자의 96.2%는 '정보보호'가 중요하다고 인식

- ▶ 정보보호가 중요하다(중요한 편이다 + 매우 중요하다)고 인식하는 비율은 96.2%로, 전년(94.2%) 대비 2.0%p 증가함
 - 연령별로 30대(97.3%), 10대(97.2%) 순으로 높게 나타남
 - 올해 조사대상에 추가된 60대도 정보보호가 중요(96.4%)하다고 인식하고 있음

그림 2-2-1 정보보호 중요성 인식률

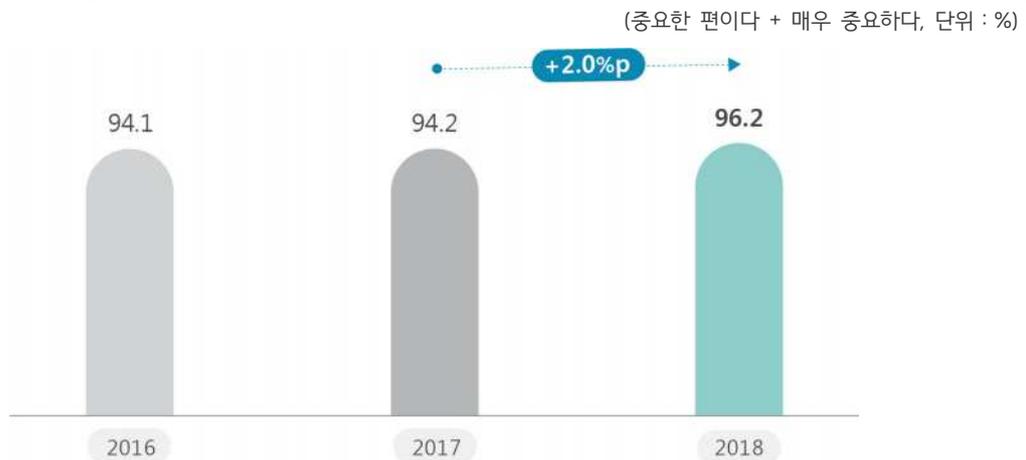


그림 2-2-2 연령별 정보보호 중요성 인식률



2. 개인정보보호 중요성 인식



인터넷 이용자의 97.3%는 '개인정보보호'가 중요하다고 인식

- ▶ 개인정보보호가 중요하다(중요한 편이다 + 매우 중요하다)고 인식하는 비율은 97.3%로 조사되었으며, 전년(96.6%)과 오차범위 내 비슷함
 - 연령별로 10대(98.5%)와 40대(98.4%)에서 높게 나타남
 - 올해 조사대상에 추가된 60대도 개인정보보호가 중요(97.0%)하다고 인식하고 있음

그림 2-2-3

개인정보보호 중요성 인식률

(중요한 편이다 + 매우 중요하다, 단위 : %)

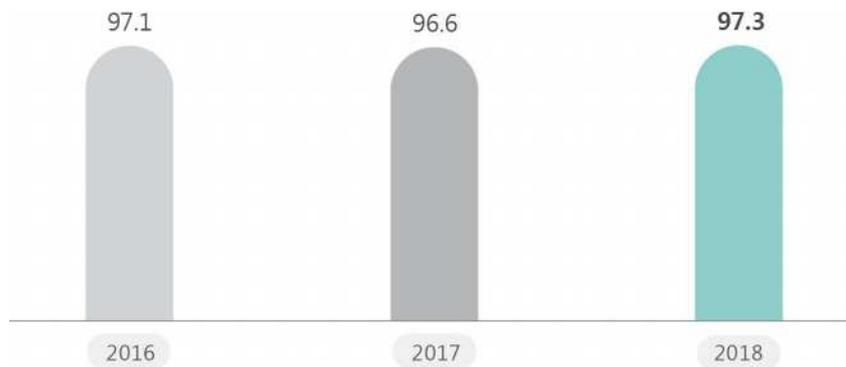
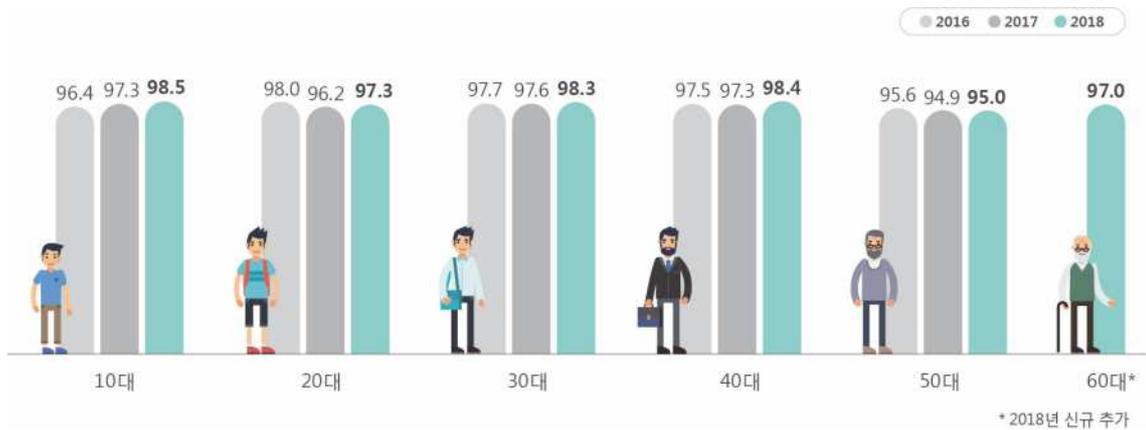


그림 2-2-4

연령별 개인정보보호 중요성 인식률

(중요한 편이다 + 매우 중요하다, 단위 : %)



II

침해사고 예방



1. 정보보호 제품 이용



인터넷 이용자의 87.3%가 '정보보호 제품' 이용

- ▶ PC 및 모바일 기기 등의 보안을 위해 정보보호 관련 제품을 이용하는 비율은 87.3%로, 전년(87.4%)과 비슷함
 - PC 이용자의 93.3%, 모바일 기기 이용자의 85.2%가 정보보호 관련 제품을 이용함
- ▶ 정보보호 제품 이용자는 '그 외 무료 소프트웨어(92.3%)'를 가장 많이 이용하고, '운영체제에 탑재된 보안 소프트웨어(40.9%)' 등의 순으로 많이 이용하는 것으로 나타남
 - 특히, '그 외 무료 소프트웨어'는 매년 이용률이 증가하고 있음

그림 2-2-5 | 정보보호 제품 이용률



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



2. 침해사고 예방 활동

가. 백신 프로그램 업데이트



‘백신 프로그램 업데이트’ 실시 98.1%, 전년 대비 3.3%p 증가

- ▶ 대부분의 정보보호 제품 이용자는 백신 프로그램 업데이트를 실시(98.1%)하는 것으로 나타났으며, 전년(94.8%) 대비 3.3%p 증가함
 - 2016년 94.5%, 2017년 94.8%, 2018년 98.1%로 증가 추세임
- ▶ 인터넷 이용자의 대부분이 백신 프로그램 업데이트를 ‘자동으로 업데이트 되도록 설정 (PC: 88.2%, 모바일기기: 90.7%)’ 하는 것으로 나타남

그림 2-2-7

백신 프로그램 업데이트 실시율 - 정보보호 제품 이용자

(단위 : %)

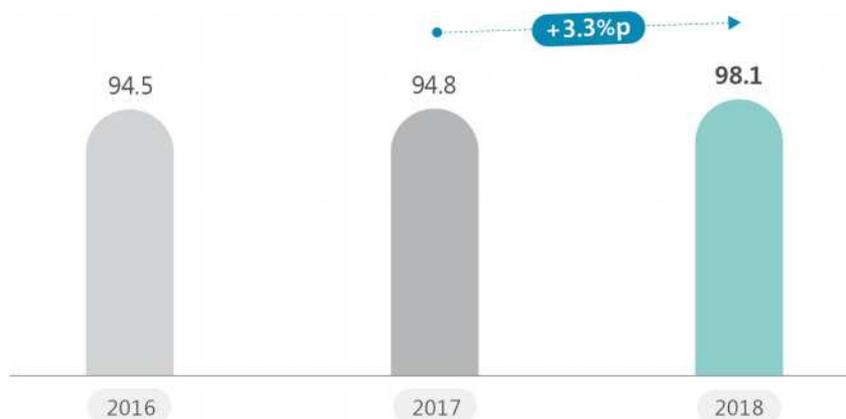


그림 2-2-8

백신 프로그램 업데이트 방법 - PC/모바일 기기 이용자 중 정보보호 제품 이용자

(단위 : %)



나. 운영체제 보안 업데이트



‘운영체제 보안 업데이트’ 실시 87.1%, 전년 대비 3.7% 증가

- ▶ 운영체제 보안 업데이트를 실시하는 인터넷 이용자는 87.1%로, 전년(83.4%) 대비 3.7%p 증가함
 - 2016년 83.2%, 2017년 83.4%, 2018년 87.1%로 증가 추세임
- ▶ 운영체제 보안 업데이트 방법으로는 PC와 모바일 기기 모두 ‘자동으로 업데이트 되도록 설정’이 86.2%, 84.4%로 가장 높게 나타남

그림 2-2-9

운영체제 보안 업데이트 실시율

(단위 : %)

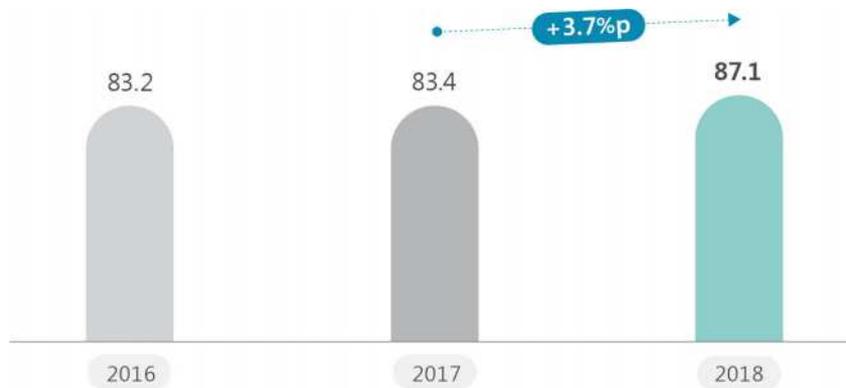


그림 2-2-10

운영체제 보안 업데이트 방법 - PC/모바일 기기 이용자

(단위 : %)



다. 중요 데이터 백업



인터넷 이용자 10명 중 약 5명(49.5%)은 '중요 데이터 백업' 실시

- ▶ PC 또는 모바일 기기의 중요 데이터를 백업하는 비율은 49.5%임
- ▶ 중요 데이터 백업 방식은 PC의 경우 'USB 메모리 등 별도 저장장치 활용'하는 비율이 77.2%로 가장 높았음
한편, 모바일 기기 중요 데이터 백업 실시자는 '클라우드 서버 활용(73.5%)'을 통한 백업을 가장 많이 실시하는 것으로 나타남

그림 2-2-11

중요 데이터 백업률

(단위 : %)



그림 2-2-12

중요 데이터 백업 방식 (복수응답) - PC/모바일 기기 이용자 중 중요 데이터 백업 실시자

(단위 : %)



라. PC 비밀번호 설정



PC 이용자의 73.9%가 'PC 이용 시 비밀번호 설정'

- ▶ PC 이용자의 73.9%가 PC 이용 시 비밀번호를 설정하는 것으로 조사됨
- ▶ PC 비밀번호를 하나라도 설정하고 있는 응답자 중 73.7%가 '운영체제 (윈도우 등) 로그인 시' 비밀번호를 설정하며, 다음으로 '중요 데이터 파일 저장 시(50.3%)', '화면 보호기능 해제 시 (46.2%)' 등의 순으로 비밀번호를 설정함

그림 2-2-13

PC 비밀번호 설정률 - PC 이용자

(단위 : %)



그림 2-2-14

PC 비밀번호 설정 유형 (복수응답) - PC 비밀번호 설정 응답자

(단위 : %)



III

침해사고 대응



1. 침해사고 경험



인터넷 이용자의 4.6%가 정보보호 침해사고 경험, 전년 대비 5.7%p 감소

- ▶ 2017년 1년 간 악성코드 감염, 개인정보 유출 등 침해사고를 경험한 인터넷 이용자는 4.6%로, 전년(10.3%) 대비 5.7%p 하락함
 - PC 이용자의 3.6%, 모바일 기기 이용자의 2.3%가 침해사고를 경험함
- ▶ 침해사고 경험 유형으로는 '악성코드 감염 등으로 인한 피해'가 3.4%로 가장 많았고, 다음으로 '개인정보 유출 및 사생활 침해(1.9%)' 등의 순으로 나타남

그림 2-2-15 | 침해사고 경험률

(단위 : %)

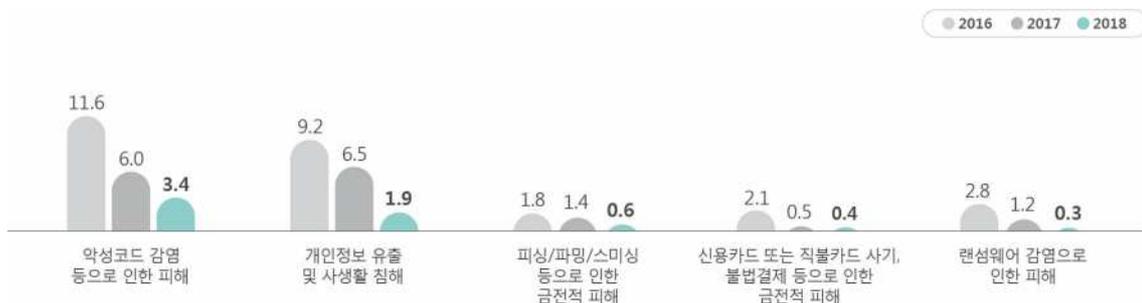
✓ 침해사고 경험률

✓ PC/모바일 기기별 침해사고 피해 경험률



그림 2-2-16 | 침해사고 경험 유형 (복수응답)

(단위 : %)



2. 침해사고 대응



침해사고 경험자의 10명 중 약 9명(88.3%)은 침해사고 대응활동을 수행

- ▶ 침해사고 경험 시 대응활동을 수행하는 비율은 88.3%로, 전년(90.8%)과 비슷한 수준임
- ▶ 대응활동 유형으로는 '보안 소프트웨어 설치'가 41.4%로 가장 많았고, 다음으로 '스스로 점검 및 예방활동 강화(41.1%)', '사용 중인 비밀번호 변경(40.4%)' 등의 순으로 나타남
- 세부 항목 중 '보안 소프트웨어 설치(41.4%)'는 전년(26.3%) 대비 크게 증가함

그림 2-2-17

침해사고 대응률 - 침해사고 경험자

(단위 : %)

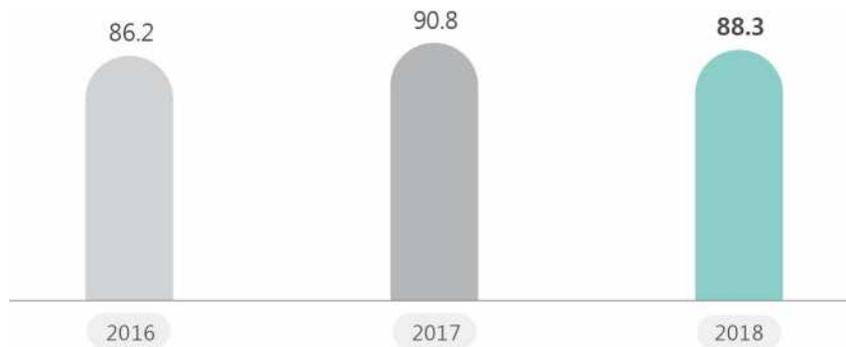
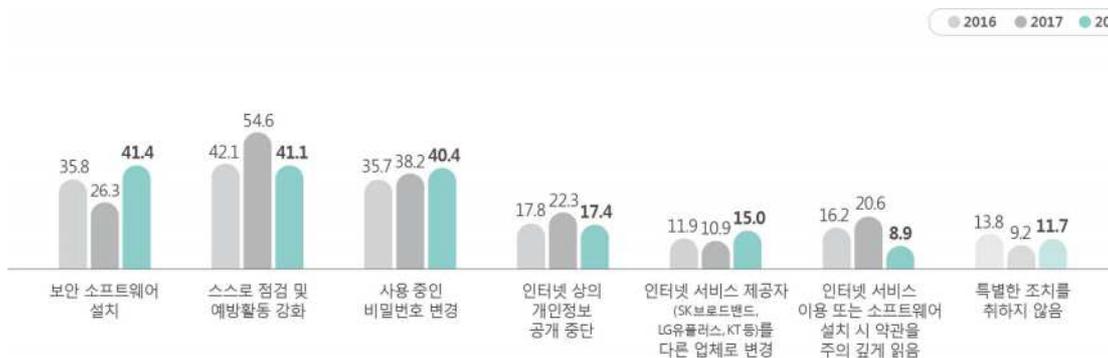


그림 2-2-18

침해사고 대응활동 수행 (복수응답) - 침해사고 경험자

(단위 : %)



IV 개인정보보호



1. 개인정보 침해사고 예방



인터넷 이용자 10명 중 약 9명(91.4%)이 개인정보 침해사고 예방 조치 실시

- ▶ 개인정보 유출 예방을 위해 조치를 실시하고 있는 인터넷 이용자는 91.4%로 전년 (89.4%) 대비 2.0%p 증가하였음
- ▶ 조치 유형별로는 '개인정보를 주의해서 관리하며 타인에게 알려주지 않음(75.5%)'이 가장 많았으며, 다음으로 '인터넷에서 파일을 함부로 다운로드 하지 않음(55.7%)'이 많음

그림 2-2-19 개인정보 침해사고 예방 조치 실시율

(단위 : %)

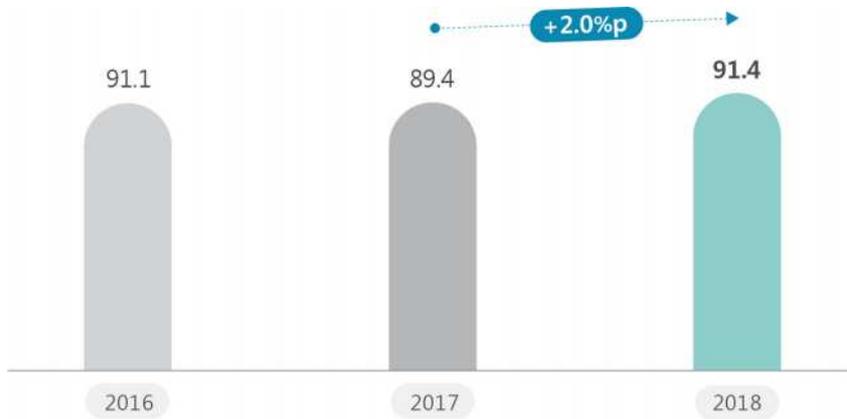
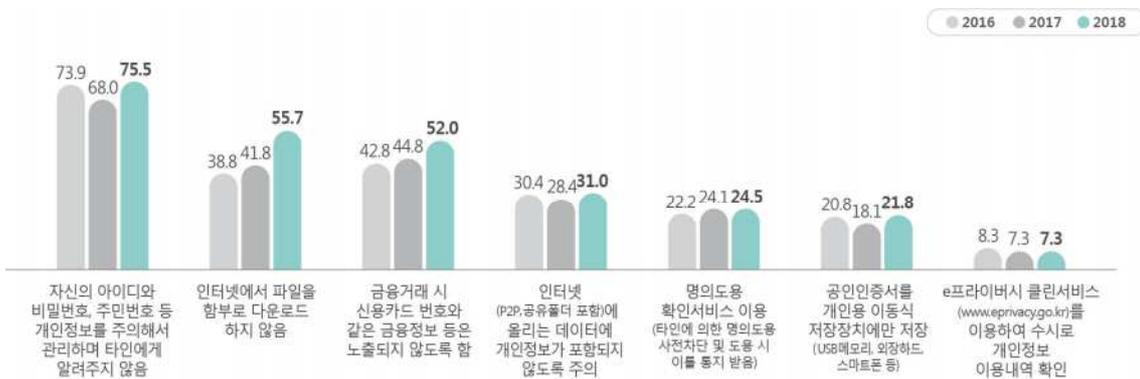


그림 2-2-20 개인정보 침해사고 예방 조치 유형 (복수응답)

(단위 : %)



2. 개인정보 침해사고 대응



개인정보 침해사고 경험자의 47.8%는 침해사고 대응활동 실시

- ▶ 개인정보 침해사고 경험자의 47.8%는 침해사고 이후 대응활동을 실시하는 것으로 조사되었고, 전년(58.8%) 대비 11.0%p 하락함
- ▶ 대응활동 유형으로는 '해당 서비스를 탈퇴하고 동일한 서비스를 제공하는 다른 기업 이용(36.9%)'이 가장 많았고, '관련 기관에 신고 또는 상담(7.8%)', 'e프라이버시 클린서비스 이용(5.7%)' 등의 순임

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

(단위 : %)

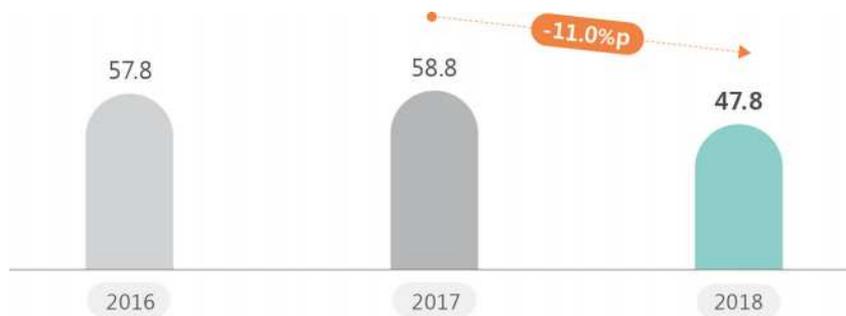
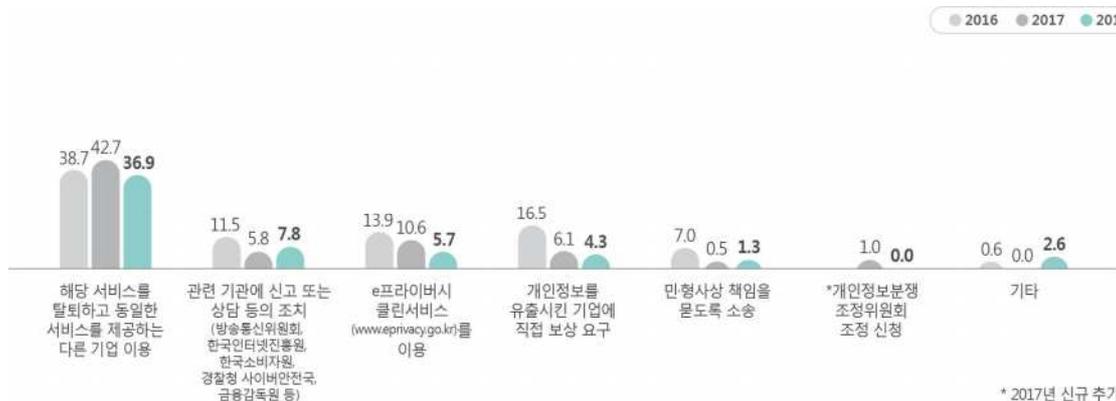


그림 2-2-22 개인정보 침해사고 대응활동 수행 (복수응답) - 개인정보 침해사고 경험자

(단위 : %)



V

주요 서비스별 정보보호



1. 클라우드



‘클라우드 서비스’ 이용 37.8%, 전년 대비 7.0%p 증가

- ▶ 인터넷 이용자의 37.8%는 클라우드 서비스를 이용하는 것으로 조사되었고, 전년(30.8%) 대비 7.0%p 증가함
- 2016년 30.4%, 2017년 30.8%, 2018년 37.8%로 증가 추세임
- ▶ 클라우드 서비스의 침해사고 예방을 위한 조치로는 ‘중요파일은 공유 전 암호화 설정하기’가 50.3%로 가장 많았고, 다음으로 ‘공유 기능과 접근 권한 등을 정확하게 확인하고 이용하기(50.0%)’, ‘서비스 장애를 대비하여 정기적으로 외부장치에 백업하기(46.6%)’ 등의 순으로 나타남

그림 2-2-23

클라우드 서비스 이용률

(단위 : %)

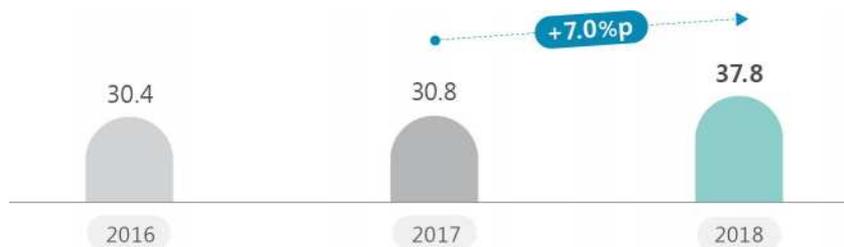
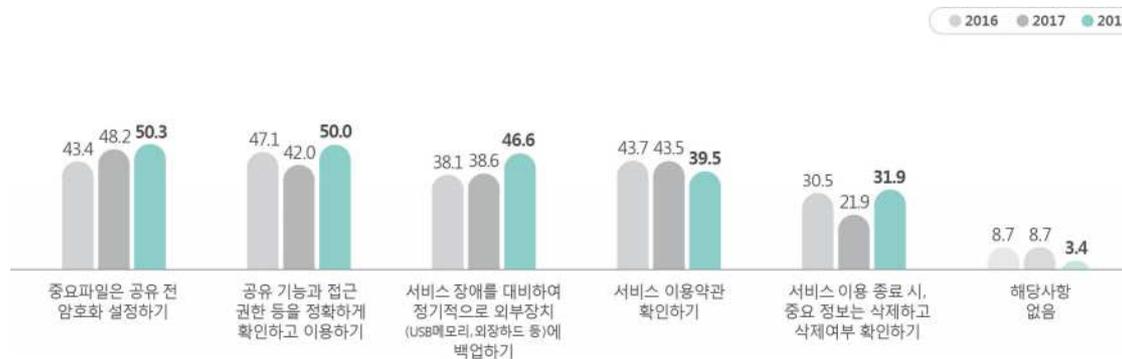


그림 2-2-24

클라우드 서비스 피해 예방 조치 (복수응답) - 클라우드 서비스 이용자

(단위 : %)



2. SNS



'SNS' 이용 78.8%, 전년 대비 3.9%p 감소

- ▶ 인터넷 이용자의 SNS(Social Network Service) 이용률은 78.8%로, 전년(82.7%) 대비 3.9%p 하락함
- ▶ SNS 피해를 예방하기 위한 조치로 '개인정보는 신중히 선택하여 공개하기(88.1%)'를 가장 많이 수행하는 것으로 나타났고, 다음으로 '타인의 개인정보를 함부로 게시, 공개하지 않기(84.8%)', '신뢰할 수 있는 사람만 친구로 추가하기(84.5%)' 등의 순임

그림 2-2-25 SNS 이용률

(단위 : %)

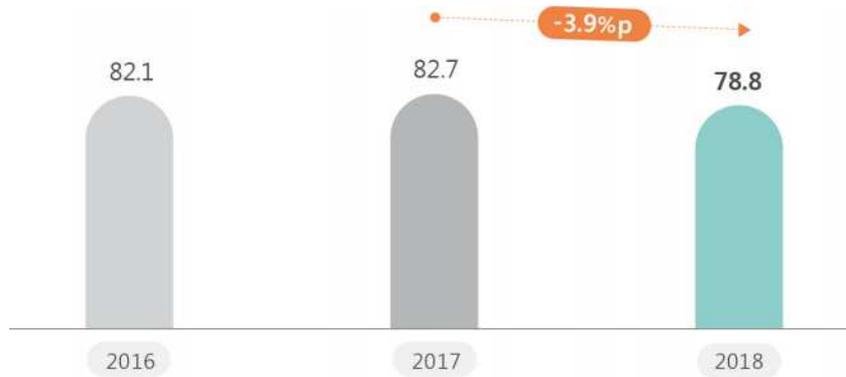
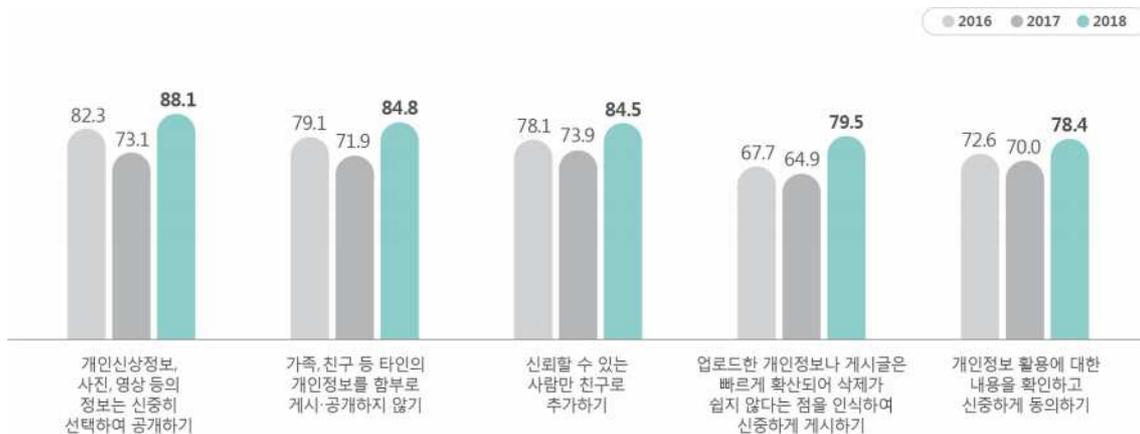


그림 2-2-26 SNS 피해 예방 조치 (복수응답) - SNS 이용자

(단위 : %)



* 응답비율 상위 5개 항목만 포함

3. 빅데이터



인터넷 이용자 36.2%가 '빅데이터 활용 서비스' 이용, 전년 대비 28.2%p 증가

- ▶ 인터넷 이용자의 36.2%는 개인정보를 활용하여 제공하는 개인 맞춤형 서비스(빅데이터 활용 서비스)를 이용해본 적이 있다고 응답하였고, 전년(8.0%) 대비 28.2%p 증가함
- ▶ 빅데이터를 활용한 서비스의 확산 시 우려사항으로는 '필요 이상의 과도한 개인정보의 수집'이 54.9%로 가장 많았고, 다음으로 '수집된 개인정보의 무단 활용(50.3%)', '수집된 정보의 분석을 통한 개인 특성 분석 및 차별(40.6%)' 등의 순으로 나타남

그림 2-2-27

빅데이터 활용 서비스 이용률

(단위 : %)

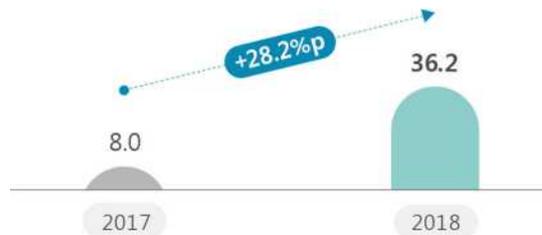
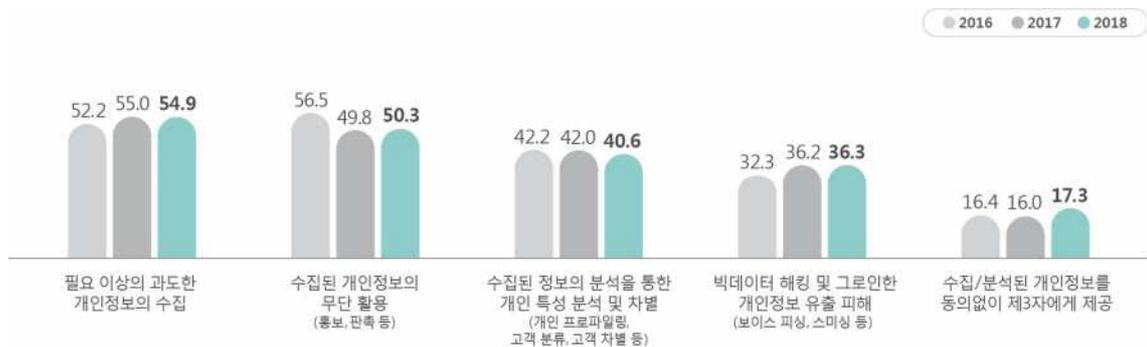


그림 2-2-28

빅데이터 활용 서비스 대중화 시 보안 우려사항 (2가지)

(단위 : %)



4. 사물인터넷(IoT)



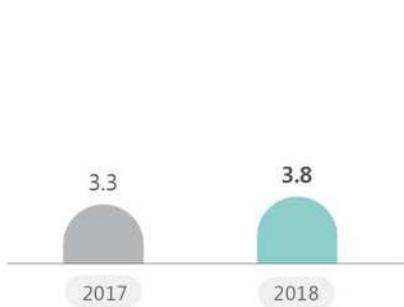
'사물인터넷(IoT) 관련 제품 및 서비스' 이용 3.8%

- ▶ 인터넷 이용자의 3.8%는 사물인터넷(IoT) 관련 제품 및 서비스를 이용하는 것으로 나타났고, 전년(3.3%)과 오차 범위 내 비슷한 수준임
 - 이용 유형으로는 스마트홈(에어컨, 세탁기, 냉장고 등)이 38.4%로 가장 많았음
- ▶ 사물인터넷(IoT) 관련 제품 및 서비스의 대중화 시 보안 우려사항으로는 '많은 종류의 데이터 발생, 처리로 인한 개인정보 침해 위험 증가'가 56.9%로 가장 많음

그림 2-2-29 사물인터넷(IoT) 제품·서비스 이용 및 유형

(단위 : %)

✓ 사물인터넷(IoT) 제품·서비스 이용률



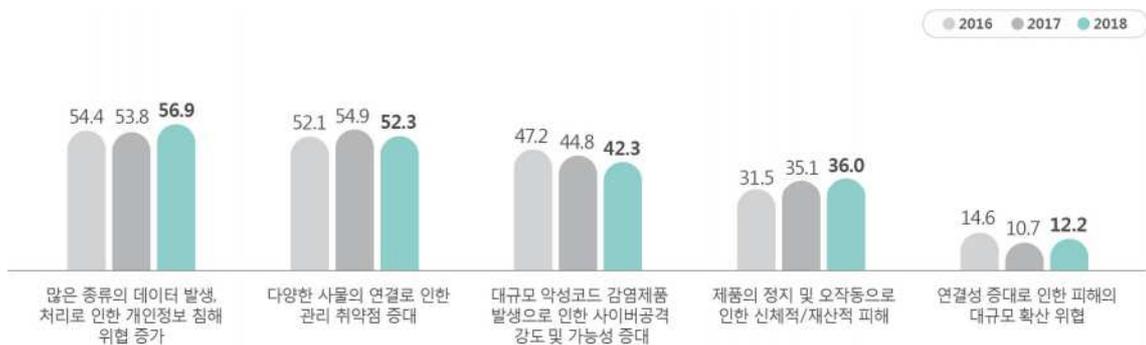
✓ 이용 유형 (복수응답)



* 상위 3개 항목만 포함

그림 2-2-30 사물인터넷(IoT) 대중화 시 보안 우려사항 (복수응답) - 사물인터넷(IoT) 제품·서비스 이용자

(단위 : %)



5. 핀테크



'간편결제 서비스' 이용 44.6%, 전년 대비 9.2%p 증가

- ▶ 인터넷 이용자의 44.6%는 간편결제 서비스를 이용하는 것으로 나타났고, 전년 대비 9.2%p 증가함
 - 간편결제 서비스 이용을 위한 본인 인증 수단으로는 '비밀번호'가 75.5%로 가장 많음
- ▶ 일반결제와 비교하여 간편결제 서비스의 보안성에 대해 간편결제 서비스 이용자의 48.1%는 '보안성이 높다', 41.4%는 '동일하다', 10.5%는 '보안성이 낮다'고 응답함

그림 2-2-31 | 간편결제 서비스 이용 및 본인 인증 수단

(단위 : %)

✓ 간편결제 서비스 이용률

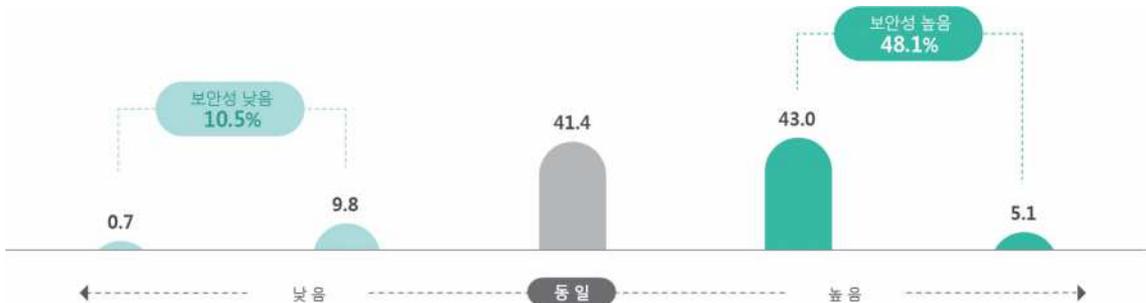


✓ 본인 인증 수단 (복수응답)



그림 2-2-32 | 일반결제 대비 간편결제 서비스 보안성 인식 - 간편결제 서비스 이용자

(단위 : %)



6. 인공지능(AI)



인터넷 이용자 18.7%가 '인공지능(AI) 활용 서비스' 이용, 전년 대비 9.0%p 증가

- ▶ 인터넷 이용자의 18.7%는 인공지능(AI) 기술을 활용한 서비스를 이용하는 것으로 나타났고, 전년(9.7%) 대비 9.0%p 증가함
 - 인공지능(AI) 기술을 활용한 서비스의 유형으로는 '(인공지능(AI)) 번역 서비스'가 63.1%로 가장 많음
- ▶ 인공지능(AI) 기술을 활용한 서비스의 대중화 시 보안 우려사항으로는 '개인정보 불법 수집에 의한 침해'가 69.5%로 가장 많았고, 다음으로 '해킹을 통한 불법 악용(66.1%)' 등의 순임

그림 2-2-33 인공지능(AI) 활용 서비스 이용 및 유형

(단위 : %)

✓ 인공지능(AI) 활용 서비스 이용률



✓ 이용 유형(복수응답)

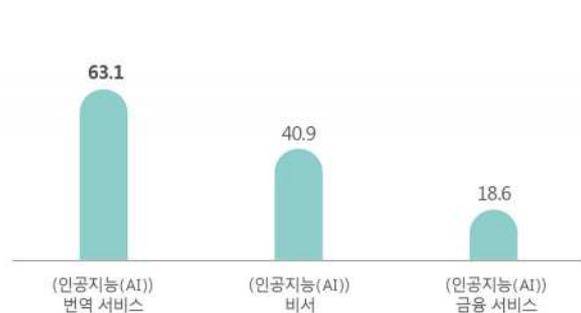
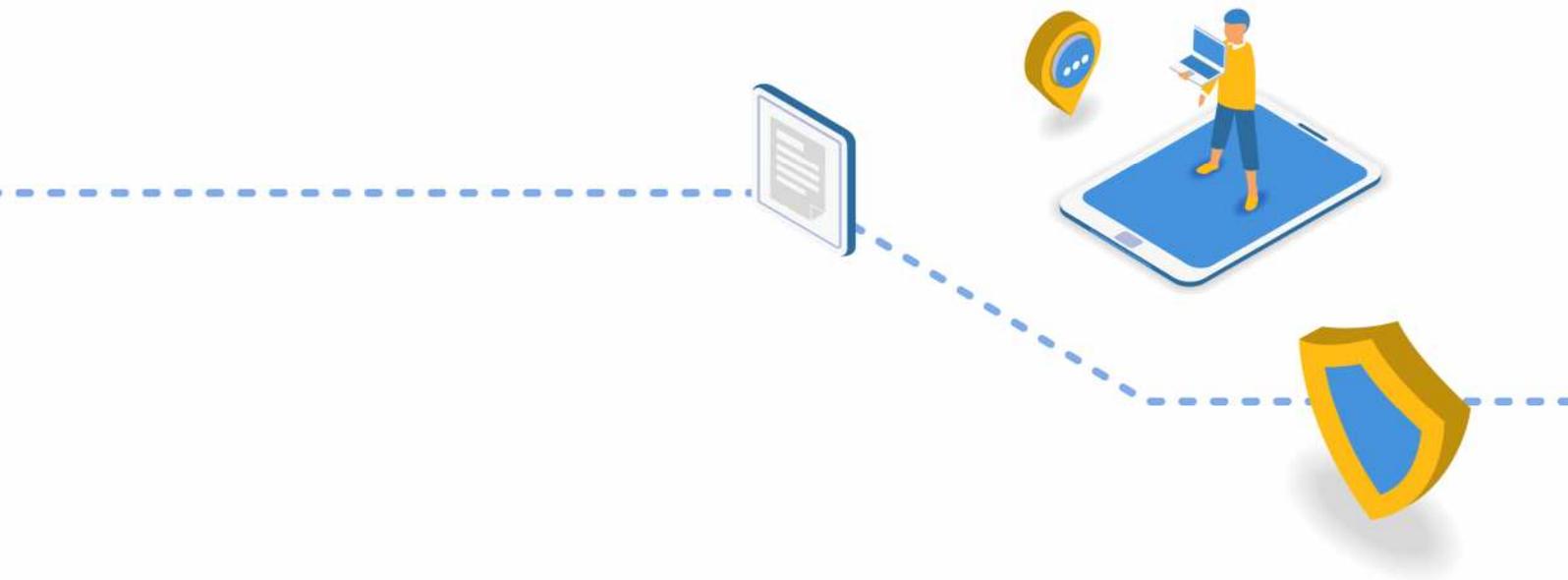


그림 2-2-34 인공지능(AI) 활용 서비스 대중화 시 보안 우려사항 (2가지)

(단위 : %)

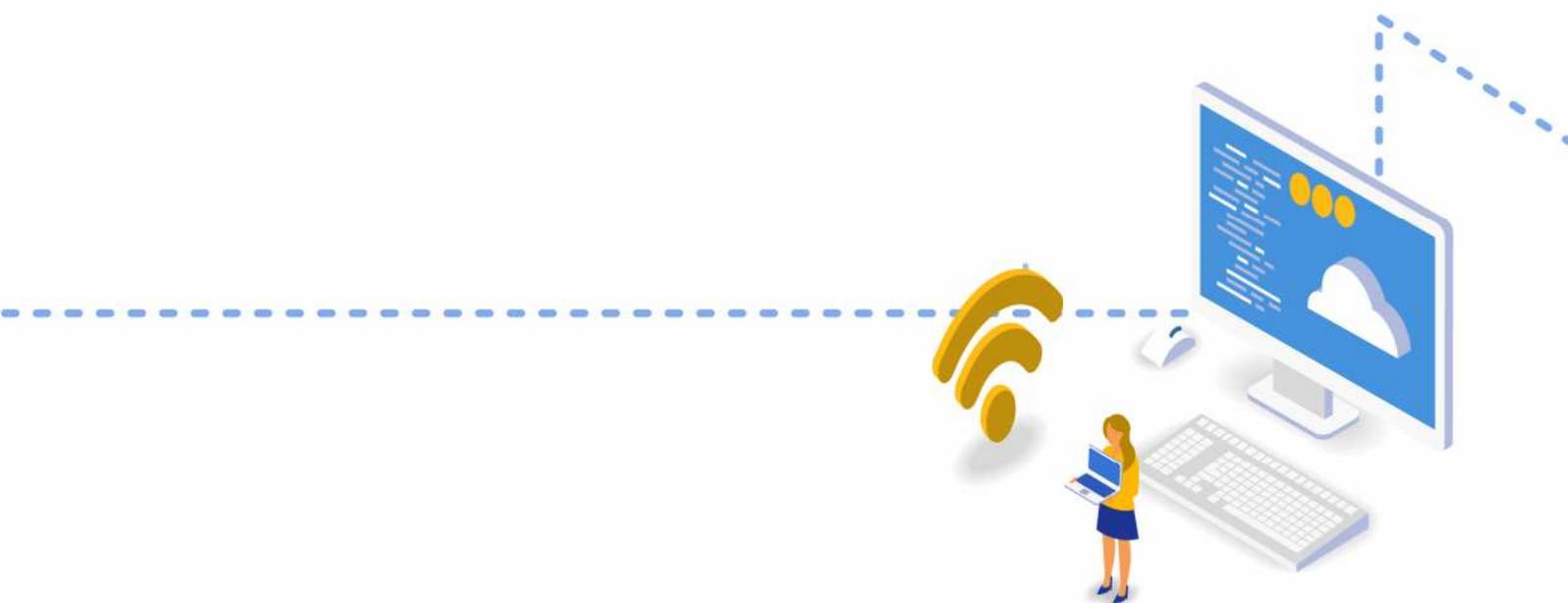






제3장

조사결과



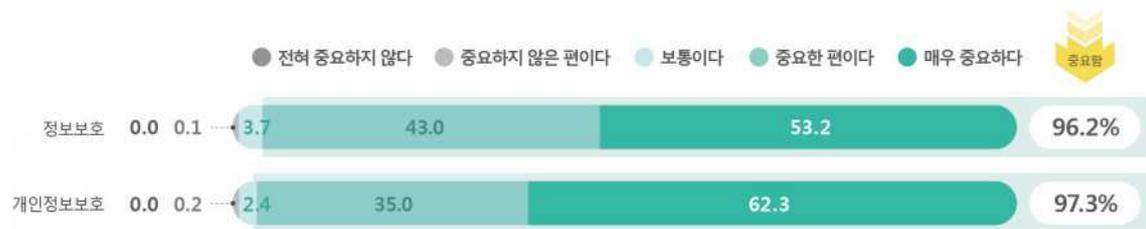
I 정보보호 인식

1. 정보보호 및 개인정보보호 중요성 인식

인터넷 이용자의 96.2%는 정보보호가 중요하다(중요한 편이다 + 매우 중요하다)고 응답했으며, 개인정보보호가 중요하다(중요한 편이다 + 매우 중요하다)고 생각하는 비율은 97.3%로 나타났다.

그림 2-3-1 정보보호 및 개인정보보호 중요성 인식

(중요한 편이다 + 매우 중요하다, 단위 : %)



정보보호 및 개인정보보호 중요성에 대한 인식은 남성이 여성에 비해 높게 나타났다. 전 연령대에서 중요성 인식이 높은 가운데 정보보호 인식은 30대(97.3%), 개인정보보호 인식은 10대(98.5%)에서 가장 높게 조사되었다.

그림 2-3-2 성·연령별 정보보호 및 개인정보보호 중요성 인식

(중요한 편이다 + 매우 중요하다, 단위 : %)



2. 정보보호 위협에 대한 인식

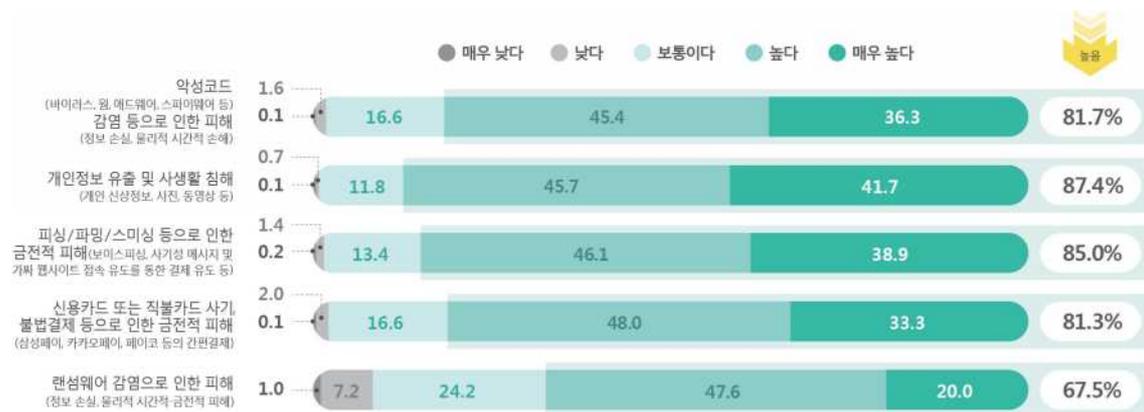
가. 위협사안에 대한 구체적 인지

정보보호 위협사안(웹사이트, SNS, 스마트폰 앱 등 인터넷 상에서 일어날 수 있는 문제)에 대한 인지도는 '개인정보 유출 및 사생활 침해(87.4%)'가 가장 높게 나타났고, 다음으로 '피싱/파밍/스미싱 등으로 인한 금전적 피해(85.0%)', '악성코드 감염 등으로 인한 피해(81.7%)' 등의 순으로 조사되었다.

한편, '랜섬웨어 감염으로 인한 피해' 인지도는 67.5%로 상대적으로 낮은 것으로 나타났다.

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 88.9%로 가장 높게 나타났고, 다음으로 '악성코드 감염 등으로 인한 피해(86.8%)', '피싱/파밍/스미싱 등으로 인한 금전적 피해(86.2%)' 등의 순으로 조사되었다.

그림 2-3-4 위협사안에 대한 피해의 심각성

(높다 + 매우 높다, 단위 : %)

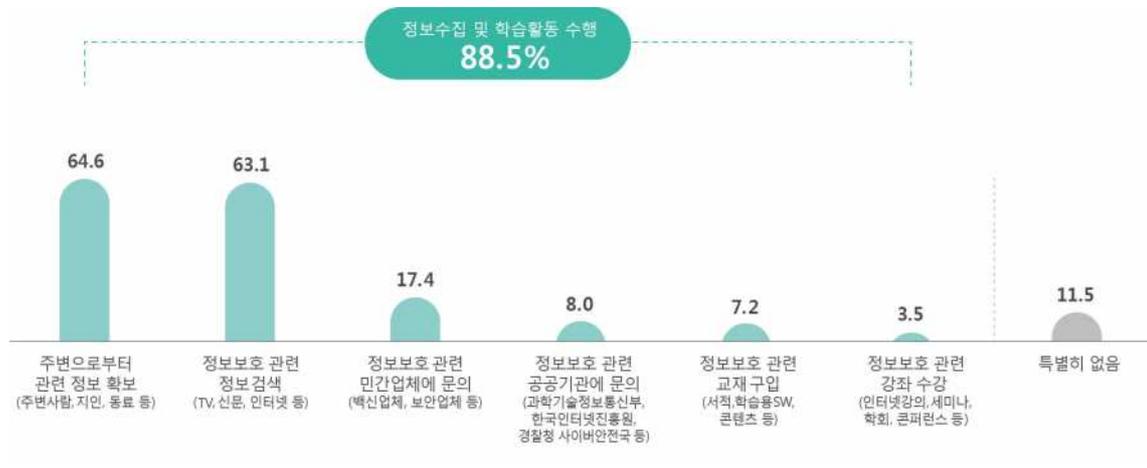


3. 정보보호 관련 정보수집 및 학습활동

인터넷 이용자의 88.5%는 정보보호 관련 정보수집 및 학습활동을 수행하는 것으로 조사되었다.

세부 유형별로는 '주변으로부터 관련 정보 확보(64.6%)'한다는 비율이 가장 높고, 다음으로 '정보보호 관련 정보 검색(63.1%)' 등의 순으로 높게 나타났다.

그림 2-3-5 | 정보보호 관련 정보수집 및 학습활동 (복수응답) (단위 : %)



연령별 분석 결과, 전체 연령 중 20~40대(20대: 93.5%, 30대: 92.1%, 40대: 91.0%) 이용률이 상대적으로 높게 나타났다.

그림 2-3-6 | 연령별 정보보호 관련 정보수집 및 학습활동률 (단위 : %)



Ⅱ 침해사고 예방

1. 정보보호 관련 제품

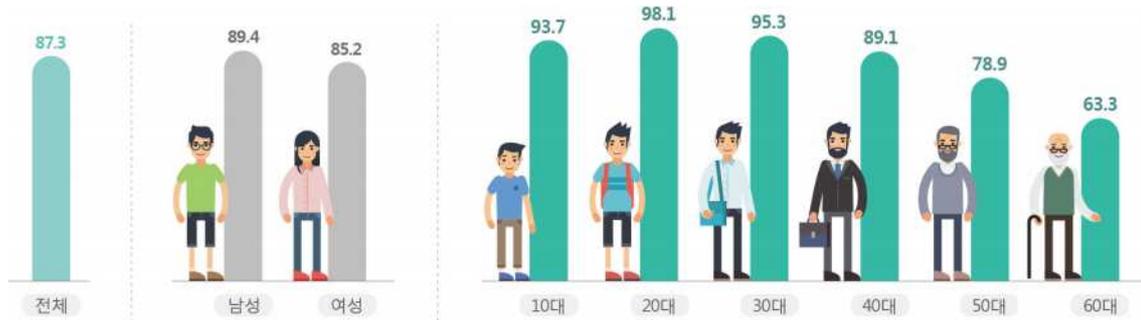
가. 정보보호 제품 이용

PC 및 모바일 보안을 위해 정보보호 관련 제품(소프트웨어 등)을 이용하는 비율은 87.3%로 나타났다.

성별 및 연령별 분석 결과, 남성(89.4%)의 정보보호 제품 이용률이 여성(85.2%)보다 높고, 전체 연령 중 10~30대(10대: 93.7%, 20대: 98.1%, 30대: 95.3%) 이용률이 상대적으로 높게 나타났다.

그림 2-3-7 정보보호 제품 이용

(단위 : %)



기기별로 살펴보면, PC 이용자의 정보보호 제품 이용률(93.3%)이 모바일 이용자의 정보 보호 제품 이용률(85.2%)보다 8.1%p 높게 조사되었다.

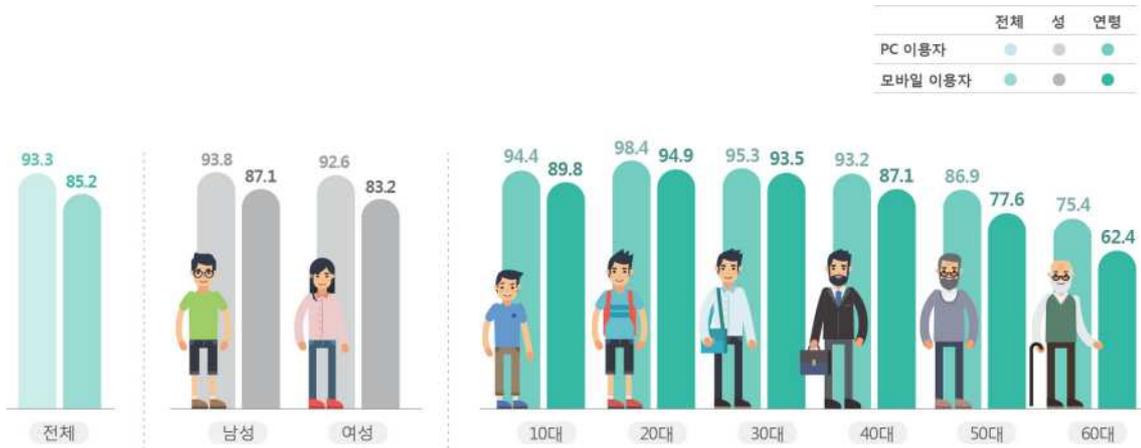
PC 및 모바일 정보보호 제품 이용 모두 여성보다는 남성의 이용률이 높게 나타났고, 연령별로는 20대의 정보보호 제품 이용률이 가장 높게 나타났다.

한편, 60대 모바일 이용자의 정보보호 제품 이용률(62.4%)은 타 연령 대비 낮은 수치를 보였다.

그림 2-3-8

정보보호 제품 이용 - PC/모바일 기기 이용자

(단위 : %)



나. 정보보호 제품 미이용 이유

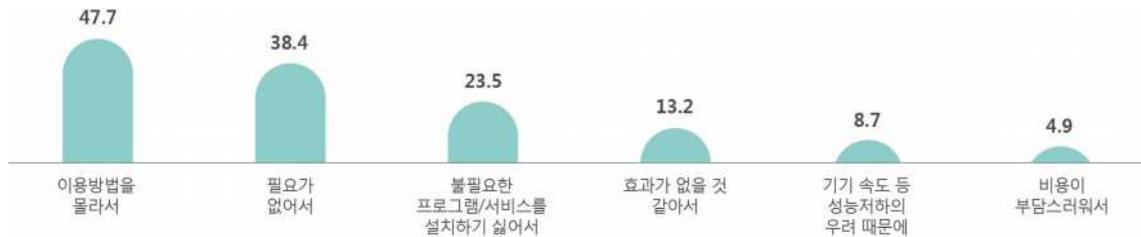
정보보호 제품 미이용자의 47.7%는 '이용방법을 몰라서' 정보보호 제품을 이용하지 않는 것으로 나타났다.

또한, '필요가 없어서(38.4%)', '불필요한 프로그램/서비스를 설치하기 싫어서(23.5%)' 등의 이유로 정보보호 제품을 이용하지 않는 것으로 조사되었다.

그림 2-3-9

정보보호 제품 미이용 이유 (복수응답) - 정보보호 제품 미이용자

(단위 : %)

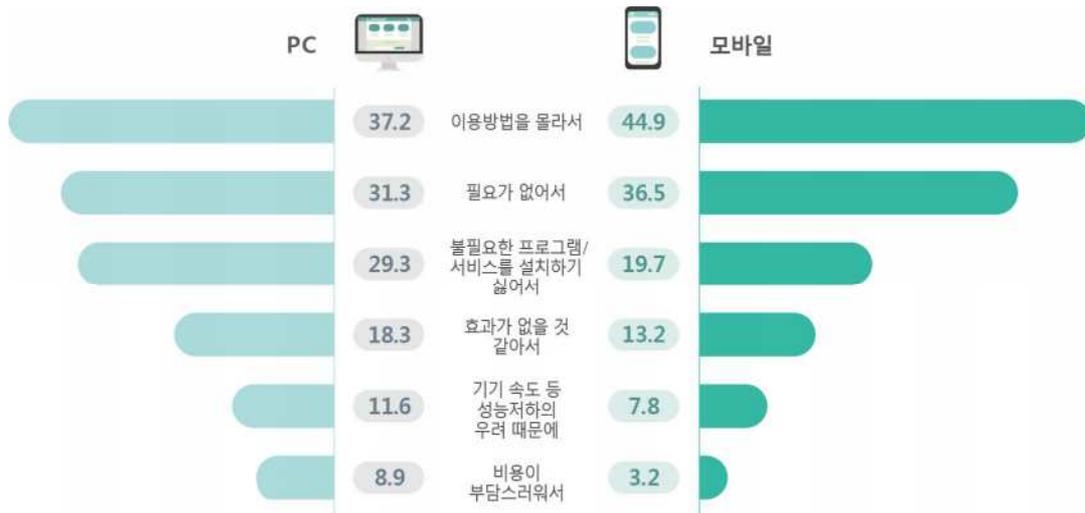


기기별로 살펴보면, PC 및 모바일 이용자 모두 '이용방법을 몰라서' (PC: 37.2%, 모바일: 44.9%) 정보보호 제품을 이용하지 않는다는 응답이 가장 많았다.

그림 2-3-10

정보보호 제품 미이용 이유 (복수응답) - PC/모바일 기기 이용자 중 정보보호 제품 미이용자

(단위 : %)

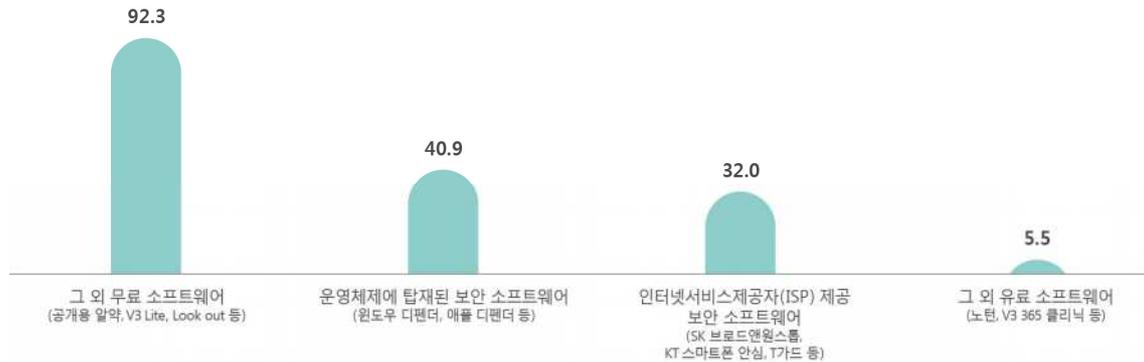


다. 정보보호 소프트웨어 이용

정보보호 제품 이용자의 92.3%가 '그 외 무료 소프트웨어'를 이용하는 것으로 조사되었다. 다음으로 '운영체제에 탑재된 보안 소프트웨어(40.9%)', '인터넷서비스제공자(ISP) 제공 보안 소프트웨어(32.0%)', '그 외 유료 소프트웨어(5.5%)' 순으로 이용하는 것으로 나타났다.

그림 2-3-11 정보보호 소프트웨어 이용 (복수응답) - 정보보호 제품 이용자

(단위 : %)



기기별로 살펴보면, PC는 '그 외 무료 소프트웨어(87.0%)'가 가장 높게 나타났고, 다음으로 '운영체제에 탑재된 보안 소프트웨어(41.7%)'가 높게 조사되었다.

모바일의 경우, PC와 마찬가지로 '그 외 무료 소프트웨어(80.0%)'를 가장 많이 이용하는 가운데 '인터넷서비스제공자(ISP) 제공 보안 소프트웨어(24.3%)'를 그 다음으로 많이 이용하는 것으로 나타났다.

그림 2-3-12 정보보호 소프트웨어 이용 (복수응답) - PC/모바일 기기 이용자 중 정보보호 제품 이용자

(단위 : %)



라. 악성코드 검사 실시 주기

PC 및 모바일 악성코드 검사(바이러스, 웜, 애드웨어, 스파이웨어 검사 등) 주기는 '실시간' (PC: 57.9%, 모바일: 65.7%)으로 실시한다는 응답이 가장 많았다.

그림 2-3-13

악성코드 검사 실시 주기 - PC/모바일 기기 이용자 중 정보보호 제품 이용자

(단위 : %)



마. 백신 프로그램 업데이트

정보보호 제품 이용자의 98.1%가 백신 프로그램 업데이트를 하는 것으로 조사되었다.

백신 프로그램 업데이트 실시율은 성별 관계없이 (남성: 97.8%, 여성: 98.4%) 높게 나타났고, 다른 연령에 비해 60대(93.1%)의 백신 프로그램 업데이트 비율이 조금 낮게 조사되었다.

그림 2-3-14

백신 프로그램 업데이트 실시 - 정보보호 제품 이용자

(단위 : %)



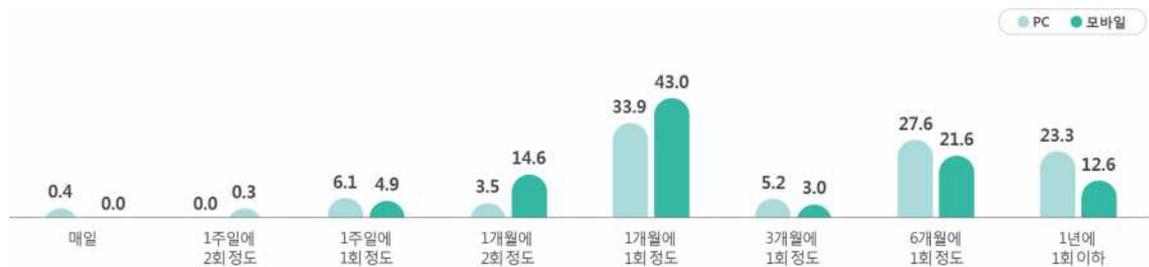
기기별로 살펴보면, PC/모바일 이용자 모두 '자동으로 업데이트 되도록 설정'한다는 응답이 가장 많은 가운데, 모바일(90.7%)이 PC(88.2%)보다 상대적으로 높게 나타났다.

그림 2-3-15 백신 프로그램 업데이트 방법 - PC/모바일 기기 이용자 중 정보보호 제품 이용자 (단위 : %)



PC 및 모바일(백신프로그램을 수동으로 업데이트하는 응답자)의 백신 프로그램 수동 업데이트 주기는 '1개월에 1회 정도' (PC: 33.9%, 모바일: 43.0%)가 가장 많은 것으로 조사되었다. 다음으로 '6개월에 1회 정도' (PC: 27.6%, 모바일: 21.6%) 주기가 높게 나타났다.

그림 2-3-16 백신 프로그램 업데이트 실시 주기- PC/모바일 기기 이용자 중 수동 업데이트 실시자 (단위 : %)



바. 운영체제 보안 업데이트

인터넷 이용자의 87.1%가 운영체제 보안 업데이트를 하는 것으로 조사되었다.

성별 및 연령별 분석 결과, 남성(87.8%)이 여성(86.4%)보다 업데이트 실시율이 높고, 전체 연령 중 20~30대 (20대: 93.3%, 30대: 94.1%)에서 상대적으로 높게 조사되었다.

그림 2-3-17 운영체제 보안 업데이트 실시

(단위 : %)



기기별로 살펴보면, PC는 '자동으로 업데이트 되도록 설정(86.2%)'한다는 응답이 가장 많은 가운데, '수동으로 업데이트' 7.3%, '업데이트 하지 않음'이 6.5%로 조사되었다.

모바일의 경우, PC와 마찬가지로 '자동으로 업데이트 되도록 설정(84.4%)'하는 비율이 가장 높게 나타났다.

한편, 모바일의 '업데이트 하지 않음' 비율은 9.9%로 PC(6.5%)보다 높게 조사되었다.

그림 2-3-18 운영체제 보안 업데이트 방법 - PC/모바일 기기 이용자

(단위 : %)



운영체제 보안 업데이트를 하지 않는 이유는 '업데이트하는 것이 번거로움'이 43.6%로 가장 높았고, 다음으로 '업데이트하는 방법 및 절차를 모름(40.6%)', '직접 관리하지 않아 모름(22.6%)', '보안 업데이트가 무엇인지 모름(15.8%)' 순으로 나타났다.

그림 2-3-19 운영체제 보안 업데이트 미실시 이유 (복수응답) - 보안 업데이트 미실시자 (단위 : %)



기기별로 살펴보면, PC/모바일 모두 '업데이트하는 것이 번거로움' (PC: 46.2%, 모바일: 44.7%) 응답 비율이 가장 높게 나타났다. 다음으로 PC는 '직접 관리하지 않아 모름 (43.4%)', 모바일은 '업데이트하는 방법 및 절차를 모름(42.9%)'이 높게 조사되었다.

그림 2-3-20 운영체제 보안 업데이트 미실시 이유 (복수응답) - PC/모바일 기기 이용자 중 보안 업데이트 미실시자 (단위 : %)



사. 중요 데이터 백업

인터넷 이용자의 49.5%가 PC 및 모바일 기기에 저장된 중요 데이터를 백업하는 것으로 조사되었다.

성별 및 연령별 분석 결과, 남성의 중요 데이터 백업률은 53.1%로 여성(45.6%)의 중요 데이터 백업률보다 높게 나타났고, 전체 연령 중 20대(74.6%)의 중요 데이터 백업률이 가장 높게 조사되었다.

그림 2-3-21

중요 데이터 백업

(단위 : %)



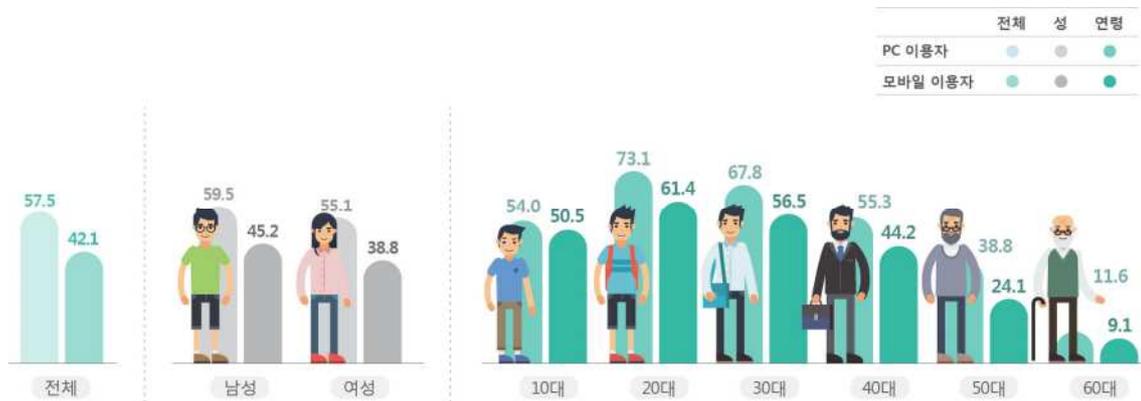
기기별로 살펴보면, PC 이용자의 중요 데이터 백업률(57.5%)이 모바일 이용자의 중요 데이터 백업률(42.1%)보다 15.4%p 높게 나타났다.

성별 및 연령별 분석 결과, PC와 모바일 모두 여성보다는 남성이, 전체 연령 중 20대가 가장 높게 나타났다.

그림 2-3-22

중요 데이터 백업 - PC/모바일 기기 이용자

(단위 : %)



중요 데이터 백업 방식은 '클라우드 서버 활용(76.4%)', 'USB메모리 등 별도 저장장치 활용(71.7%)', '운영체제(windows 등)의 백업기능 활용(40.6%)' 순으로 조사되었다.

그림 2-3-23 | 중요 데이터 백업 방식 (복수응답) - 중요 데이터 백업 실시자

(단위 : %)



기기별로 살펴보면, PC 이용자의 백업 방식 중 'USB메모리 등 별도 저장장치 활용(77.2%)'이 가장 높고, '클라우드 서버 활용(49.6%)', '운영체제(windows 등)의 백업기능 활용(37.1%)' 순으로 나타났다.

한편, 모바일 이용자의 백업 방식은 '클라우드 서버 활용'이 73.5%로 가장 높고, 다음으로 '운영체제(windows 등)의 백업기능 활용(27.6%)', 'USB메모리 등 별도 저장장치 활용(25.9%)' 순으로 나타났다.

그림 2-3-24 | 중요 데이터 백업 방식 (복수응답) - PC/모바일 기기 이용자 중 중요 데이터 백업 실시자

(단위 : %)



중요 데이터 백업 실시 주기는 PC(36.0%), 모바일(42.5%) 모두 '1개월에 1회 정도'가 가장 높은 비율을 보였다.

백업 실시 주기가 비교적 단기(매일~1개월에 1회 정도)일 경우에는 모바일(66.1%)의 비율이 PC(52.7%)보다 높고, 장기(3개월에 1회 정도~1년에 1회 이하)일 경우에는 PC(47.3%)가 모바일(33.9%)보다 높게 나타났다.

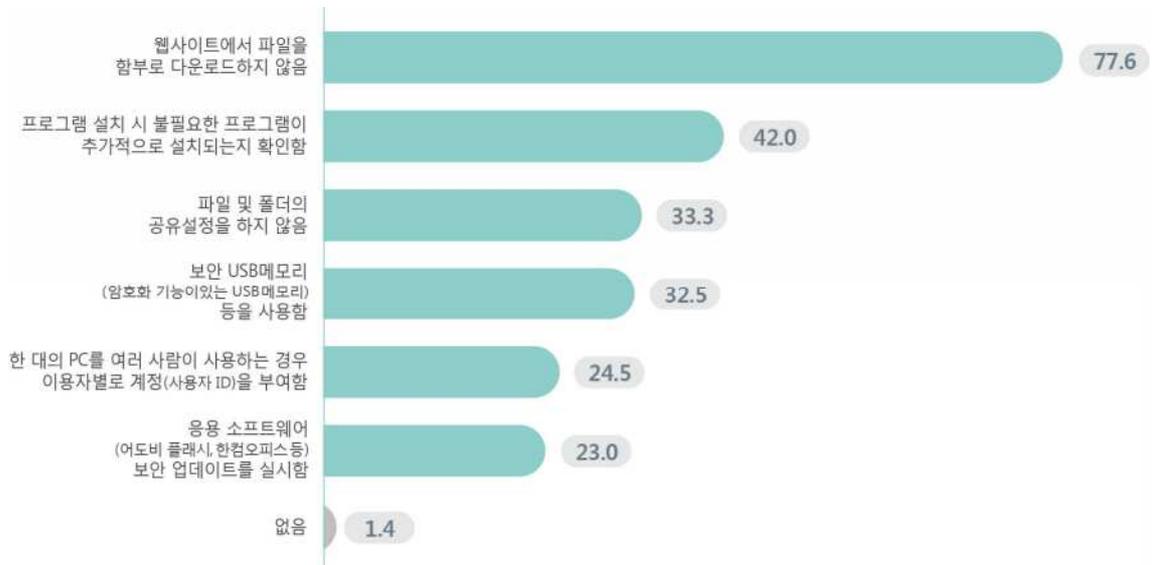
그림 2-3-25 | 중요 데이터 백업 실시 주기 - PC/모바일 기기 이용자 중 중요 데이터 백업 실시자 (단위 : %)



아. PC 및 네트워크 보안을 위한 예방조치

PC 및 네트워크 보안을 위한 예방 조치는 '웹사이트에서 파일을 함부로 다운로드하지 않음(77.6%)'이 가장 많았고, 다음으로 '프로그램 설치 시 불필요한 프로그램이 추가적으로 설치되는지 확인함(42.0%)' 등의 순으로 조사되었다.

그림 2-3-26 | PC 및 네트워크 보안을 위한 예방 조치 (복수응답) (단위 : %)



자. 비밀번호 설정 및 관리

PC 이용자의 54.4%는 '운영체제(윈도우 등) 로그인 시' 비밀번호를 설정한다고 응답했다. 다음으로 '중요 데이터 파일 저장 시(37.2%)', '화면보호기능 해제 시(34.1%)' 등의 순으로 비밀번호를 설정하는 것으로 조사되었다.

그림 2-3-27

PC 비밀번호 설정 (복수응답) - PC 이용자

(단위 : %)

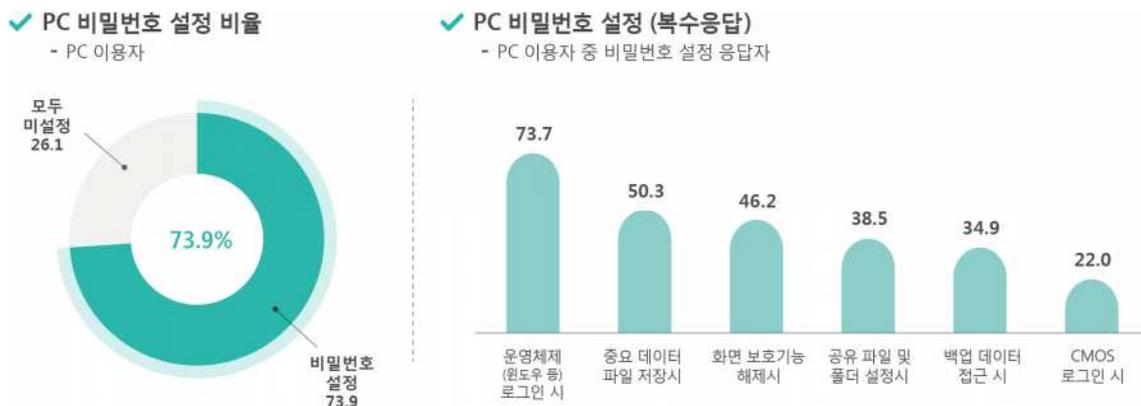


▶ 참고 PC 이용자 중 하나라도 비밀번호 설정하는 경우

그림 2-3-28

하나라도 PC 비밀번호 설정률

(단위 : %)

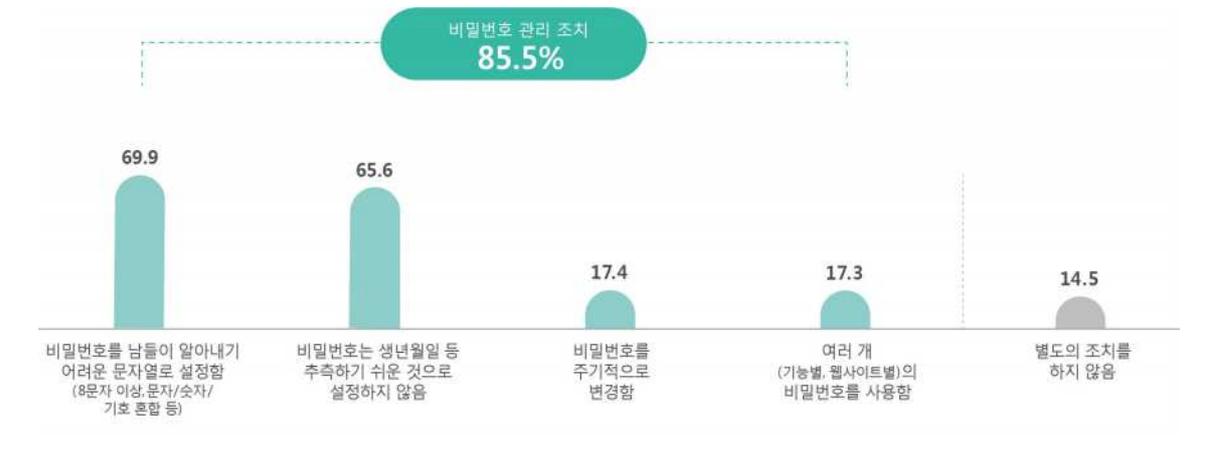


인터넷 이용자의 85.5%는 비밀번호 관리 조치를 취하는 것으로 조사되었다.

세부 유형별로는 '비밀번호를 남들이 알아내기 어려운 문자열로 설정함(69.9%)'이 가장 많았고, 다음으로 '비밀번호는 생년월일 등 추측하기 쉬운 것으로 설정하지 않음(65.6%)' 등의 순으로 나타났다.

그림 2-3-29 비밀번호 관리 조치 (복수응답)

(단위 : %)



PC 비밀번호 변경 주기(주기적으로 비밀번호를 변경하는 응답자 대상)는 '6개월에 1회 정도'가 30.6%로 가장 높고, 다음으로 '1개월에 1회 정도(29.7%)', '1년에 1회 이하(23.9%)' 등의 순으로 조사되었다.

한편, 웹사이트 비밀번호 변경 주기는 '1개월에 1회 정도'가 31.0%로 가장 높고, '6개월에 1회 정도(29.3%)', '1년에 1회 이하(20.4%)' 등의 순으로 나타났다.

그림 2-3-30 PC 및 웹사이트의 비밀번호 변경 주기 - 주기적 비밀번호 변경자

(단위 : %)



2. 모바일 및 무선랜 보안

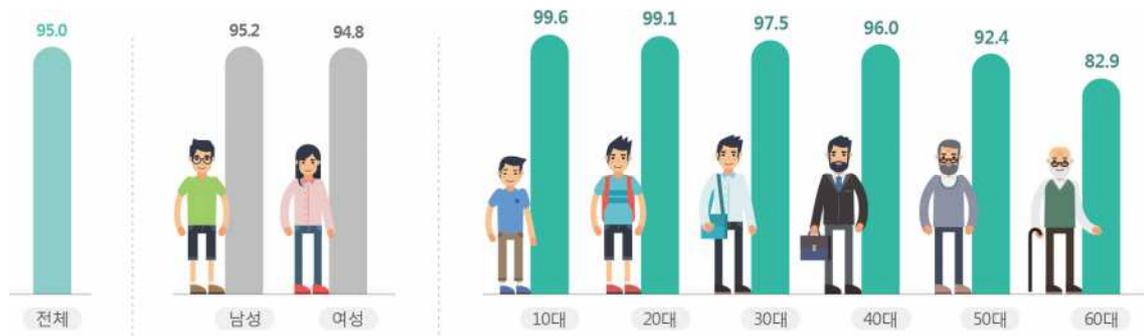
가. 무선랜 피해 예방 조치

모바일 이용자의 95.0%는 무선랜을 이용하는 것으로 조사되었다.

성별로 살펴보면, 남녀 모두 무선랜 이용률(남성: 95.2%, 여성: 94.8%)이 높게 나타났다. 연령별로는 10대의 이용률이 99.6%로 가장 높으며, 60대가 82.9%로 가장 낮게 조사되었다.

그림 2-3-31 무선랜 이용 - 모바일 기기 이용자

(단위 : %)



무선랜 이용자의 피해 예방 조치는 '제공자가 불명확한 무선랜 이용하지 않기'와 '패스워드가 없는 무선랜으로 민감한 서비스 이용하지 않기'가 71.7%로 가장 많았다.

그림 2-3-32 무선랜 피해 예방 조치 (복수응답) - 모바일 기기 이용자 중 무선랜 이용자

(단위 : %)



나. 모바일 기기 피해 예방 조치

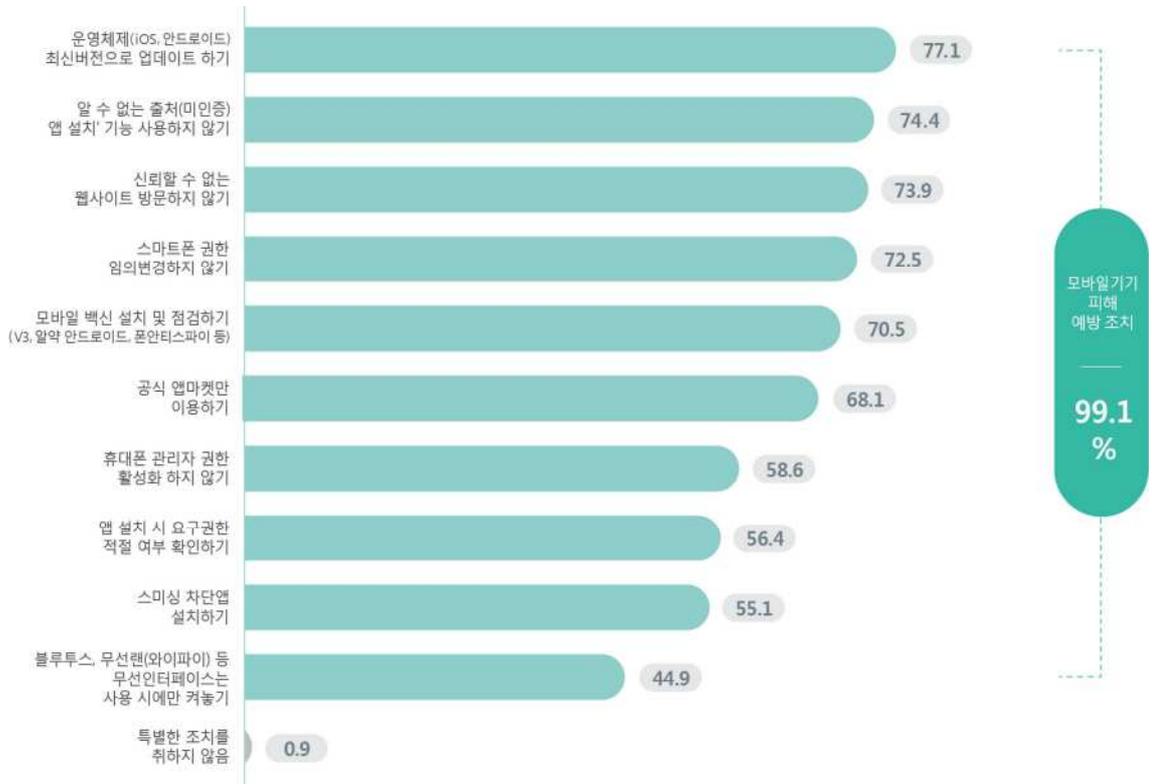
모바일 이용자의 99.1%는 모바일 기기 피해 예방을 위한 조치를 취하는 것으로 조사되었다.

세부 유형별로는 '운영체제 최신버전으로 업데이트하기(77.1%)' 비율이 가장 높고, 다음으로 '알 수 없는 출처(미인증) 앱 설치' 기능 사용하지 않기(74.4%) 등의 순으로 높게 나타났다.

그림 2-3-33

모바일 기기 피해 예방 조치 (복수응답) - 모바일 기기 이용자

(단위 : %)

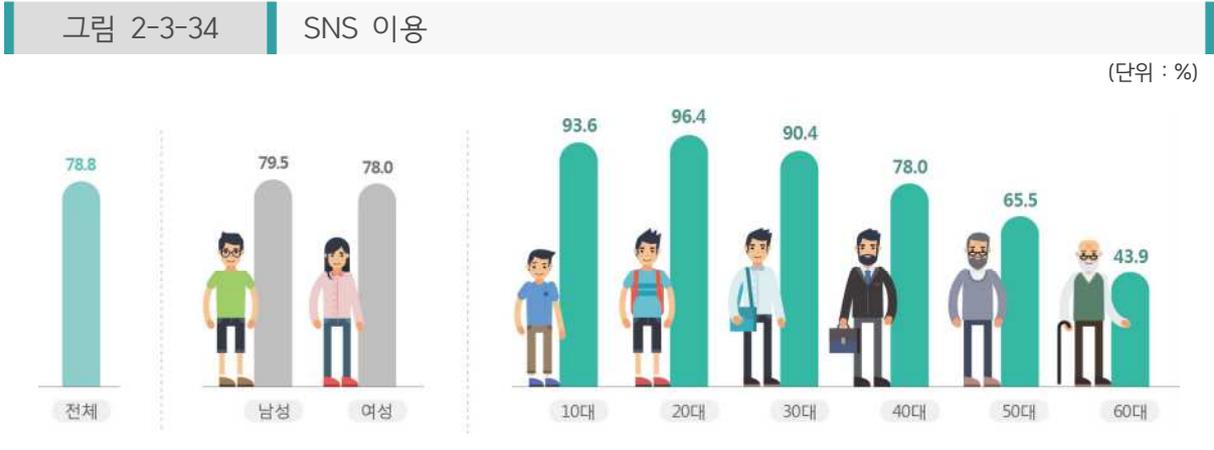


3. SNS 보안

인터넷 이용자의 78.8%가 SNS를 이용하는 것으로 조사되었다.

성별로 살펴보면, 남성이 79.5%로 여성(78.0%)보다 상대적으로 높게 나타났다.

연령별로는 20대의 이용률이 96.4%로 가장 높으며, 60대가 43.9%로 가장 낮게 조사되었다.



SNS 이용자의 99.5%는 SNS 피해 예방을 위한 조치를 취하는 것으로 조사되었다.

세부 유형별로는 '개인신상정보, 사진, 영상 등의 정보는 신중히 선택하여 공개하기'가 88.1%로 가장 높게 나타났다.



Ⅲ 침해사고 대응

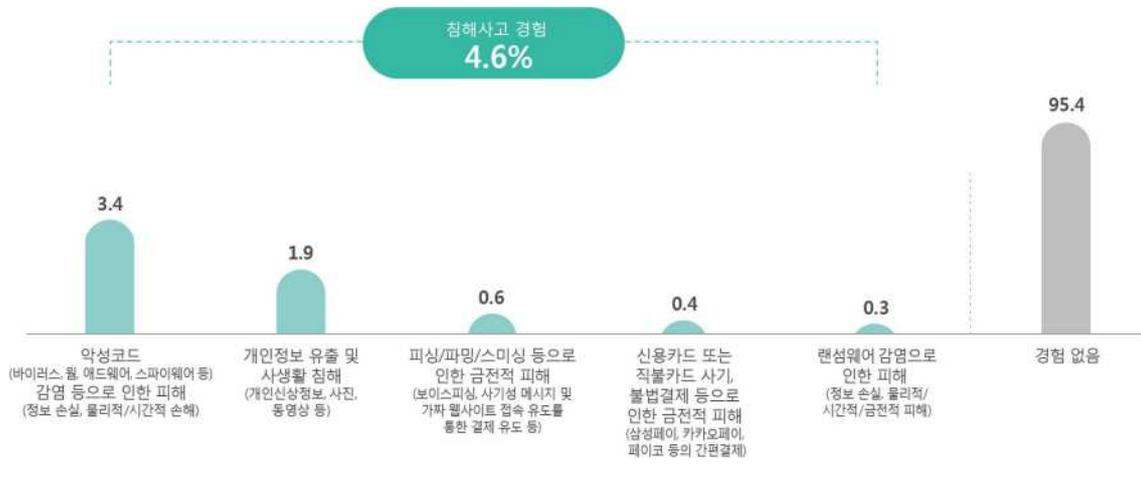
1. 침해사고 경험

2017년 1년간 침해사고 경험률은 4.6%로 조사되었다.

침해사고 세부 유형 중에서는 '악성코드(3.4%)'를 가장 많이 경험한 것으로 나타났다. 다음으로 '개인정보 유출 및 사생활 침해(1.9%)', '피싱/파밍/스미싱 등으로 인한 금전적 피해(0.6%)' 등의 순으로 나타났다.

그림 2-3-36 | 침해사고 경험 유형 (복수응답)

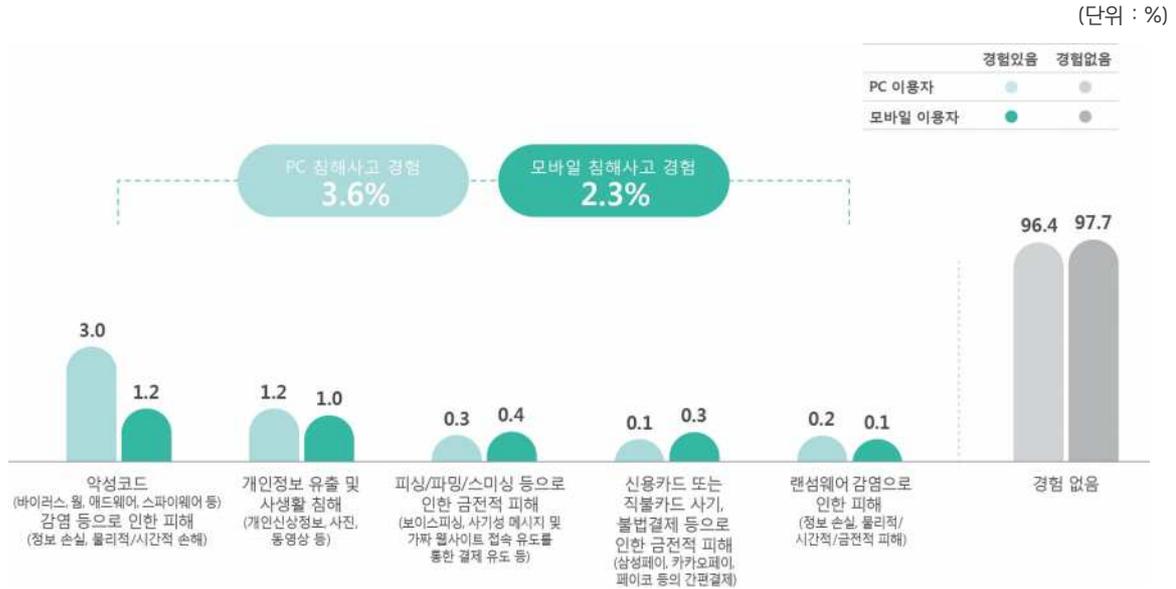
(단위 : %)



기기별로 살펴보면, PC를 통한 침해사고 경험률(3.6%)이 모바일(2.3%)보다 상대적으로 높게 나타났다.

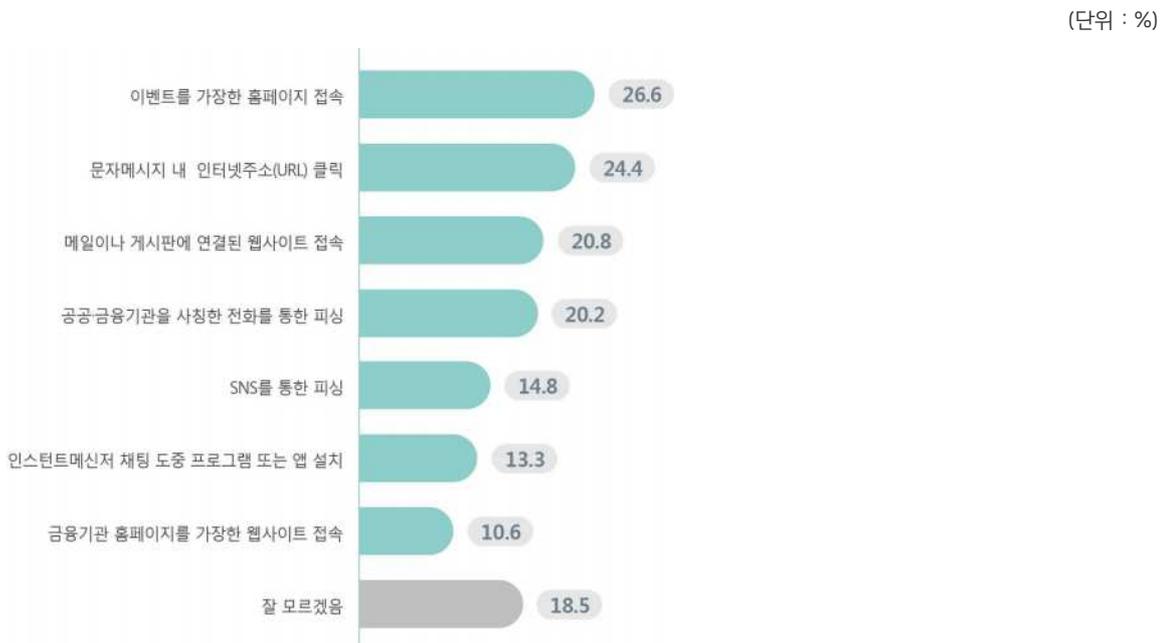
세부 유형별로는 PC/모바일 모두 '악성코드' (PC: 3.0%, 모바일: 1.2%)로 인한 피해 경험이 가장 많은 것으로 조사되었다.

그림 2-3-37 침해사고 경험 유형 (복수응답) - PC/모바일 기기 이용자



피싱/파밍/스미싱 등 금전적 피해 경험자의 26.6%는 '이벤트를 가장한 홈페이지 접속'을 통해 손실을 입은 것으로 조사되었다.

그림 2-3-38 전자금융사기 피해 경로 (복수응답) - 피싱/파밍/스미싱 금전적 피해 경험자



2. 침해사고 대응

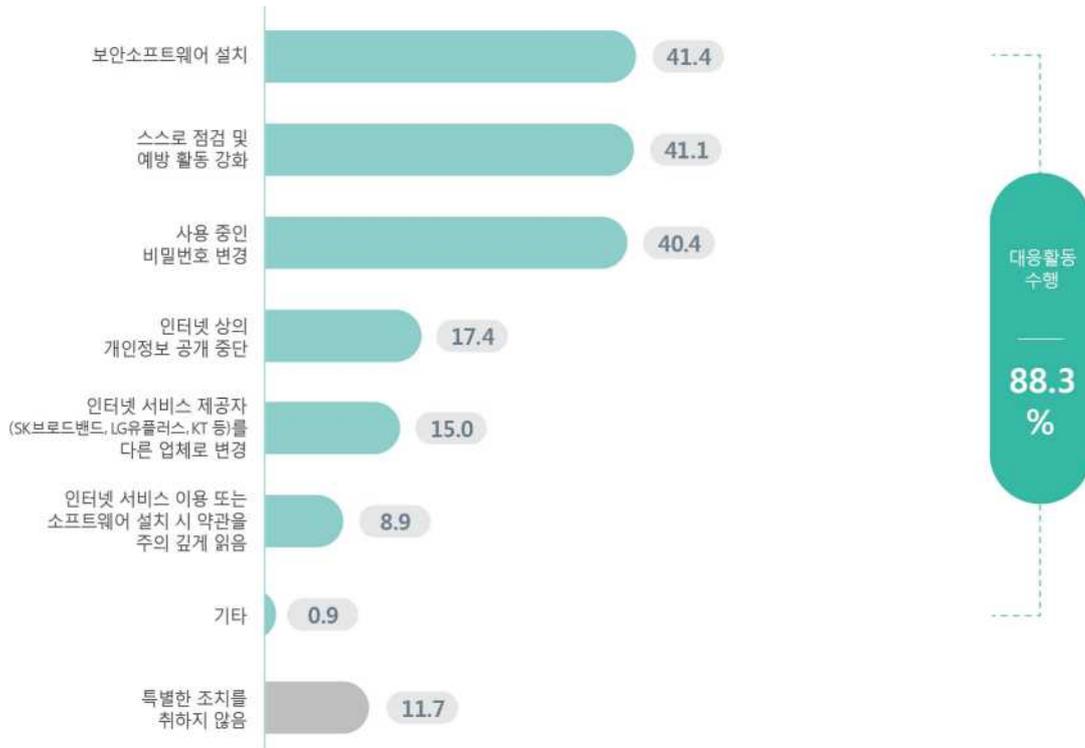
침해사고 경험자의 88.3%는 침해사고 대응 활동을 수행한 것으로 조사되었다.

세부 유형별로는 '보안소프트웨어 설치(41.4%)'를 가장 많이 수행하는 것으로 나타났고, '스스로 점검 및 예방 활동 강화(41.1%)', '사용 중인 비밀번호 변경(40.4%)' 등의 순으로 대응활동을 수행하는 것으로 조사되었다.

그림 2-3-39

침해사고 대응활동 수행 (복수응답) - 침해사고 경험자

(단위 : %)



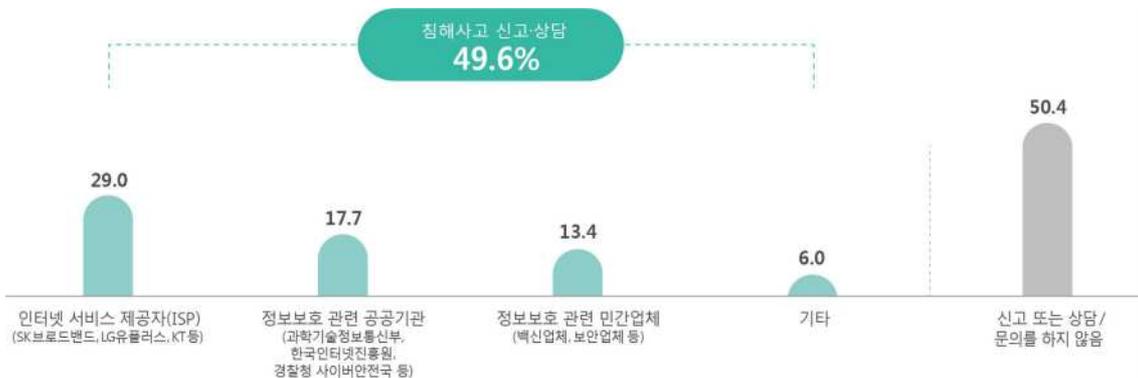
침해사고 경험자의 49.6%는 침해사고 경험 이후 기관 및 업체에 신고 또는 상담·문의한 것으로 조사되었다.

세부 유형별로는 '인터넷 서비스 제공자(ISP)'에게 신고·상담하는 경우가 29.0%로 가장 많았고, 다음으로 '정보보호 관련 공공기관(17.7%)', '정보보호 관련 민간업체(13.4%)' 순으로 나타났다.

그림 2-3-40

침해사고 신고 또는 상담·문의 기관·업체 (복수응답) - 침해사고 경험자

(단위 : %)



침해사고 피해를 정보보호 관련 공공기관에 신고 또는 상담·문의하지 않는 이유로는 '피해가 경미해서'가 35.9%로 가장 많았고, 다음으로 '신고/상담하기 번거롭고 귀찮아서(28.8%)'라는 의견이 많았다.

그림 2-3-41

침해사고 신고 또는 상담·문의하지 않은 이유 - 신고 또는 상담·문의하지 않은 자

(단위 : %)



Ⅳ 개인정보보호

1. 개인정보보호 조치

가. 온라인 상 개인정보 제공 목적

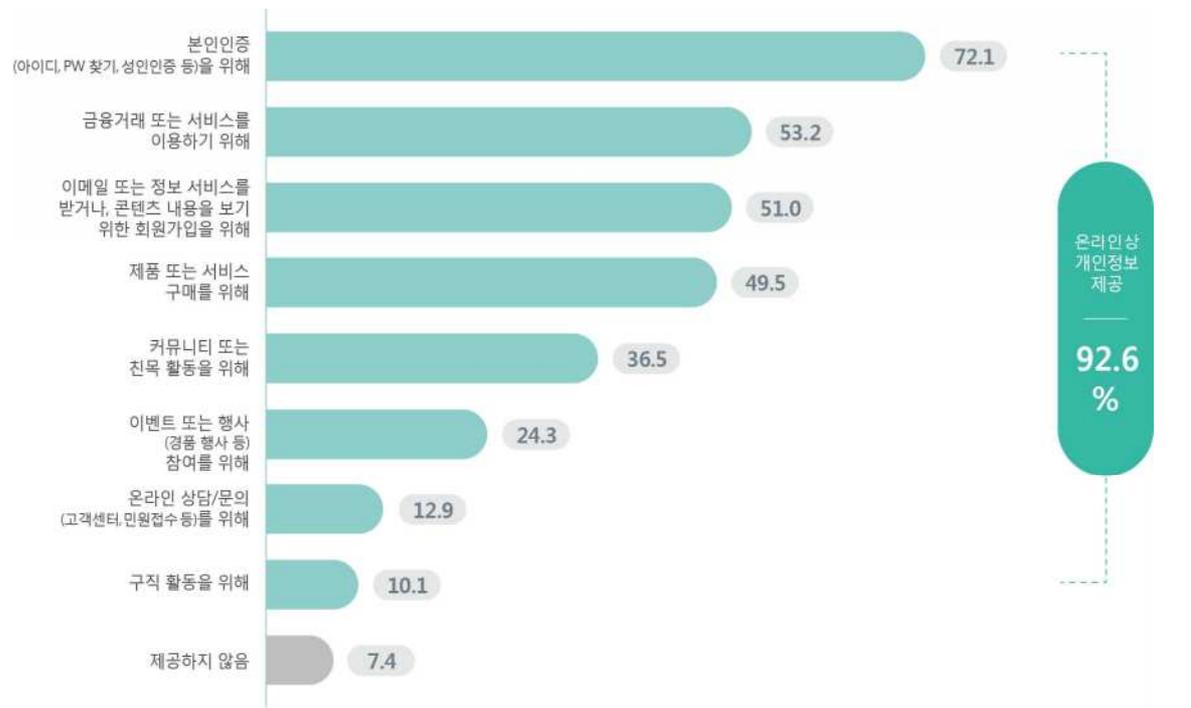
인터넷 이용자의 92.6%는 온라인 상 개인정보를 제공하는 것으로 조사되었다.

개인정보를 제공하는 목적으로는 '본인인증(아이디, PW 찾기, 성인인증 등)을 위해'가 72.1%로 가장 높게 나타났고, 다음으로 '금융거래 또는 서비스를 이용하기 위해(53.2%)', '이메일 또는 정보 서비스를 받거나, 콘텐츠 내용을 보기 위한 회원가입을 위해(51.0%)' 등의 순으로 조사되었다.

그림 2-3-42

온라인 상 개인정보 제공 목적 (복수응답)

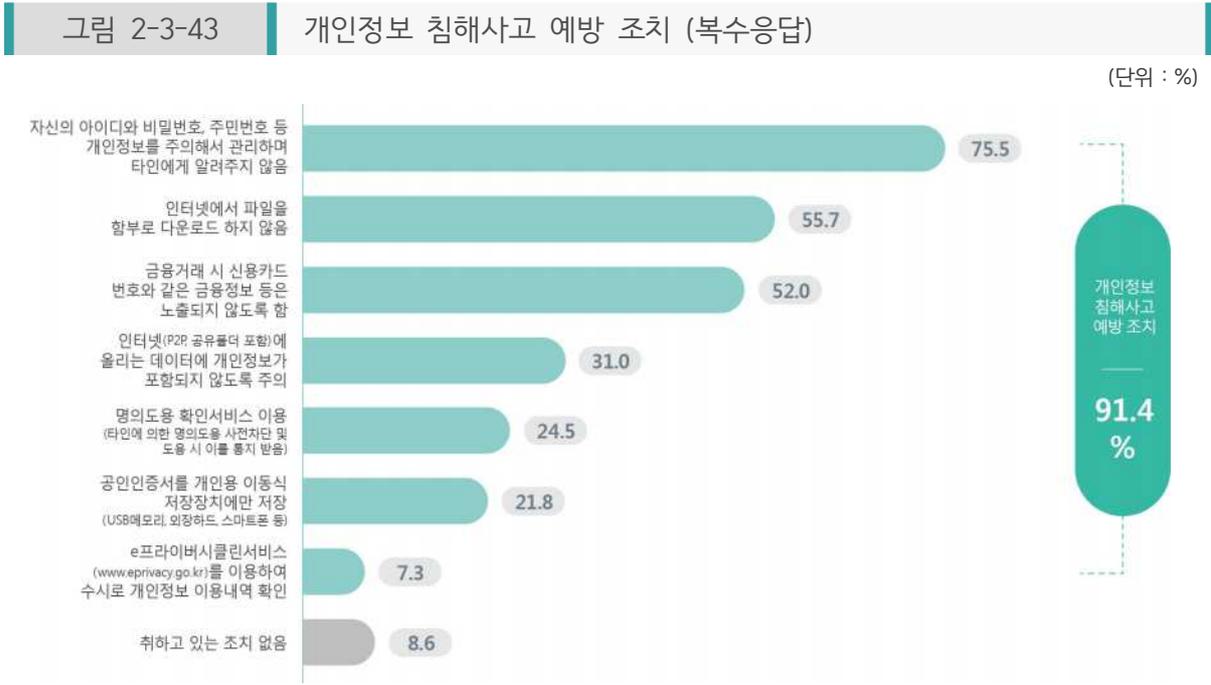
(단위 : %)



나. 개인정보 침해사고 예방 조치

인터넷 이용자의 91.4%는 개인정보 유출 예방을 위한 조치를 취하는 것으로 조사되었다.

개인정보 침해사고 예방 조치로 '개인정보를 주의해서 관리하며 타인에게 알려주지 않음'이 75.5%로 가장 많았고, 다음으로 '인터넷에서 파일을 함부로 다운로드 하지 않음(55.7%)', '금융거래 시 신용카드번호와 같은 금융정보 등은 노출되지 않도록 함(52.0%)' 등의 순으로 조사되었다.



2. 개인정보 침해사고 경험 및 대응

가. 개인정보 침해사고 경험

2017년 1년간 개인정보 침해사고 경험률은 1.9%로 조사되었다.

성별 및 연령별 분석 결과, 개인정보 침해사고 경험률은 남성 2.0%, 여성 1.8%로 나타났고, 40대(3.0%)에서 상대적으로 높게 나타났다.

그림 2-3-44

개인정보 침해사고 경험

(단위 : %)

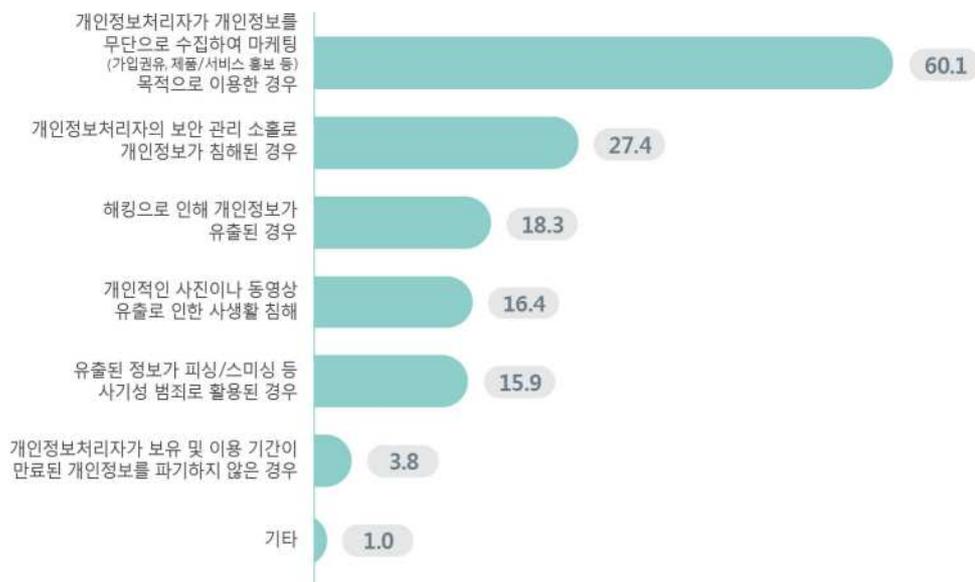


개인정보 침해사고 경험 유형으로는 '개인정보처리자가 개인정보를 무단으로 수집하여 마케팅 목적으로 이용한 경우'가 60.1%로 가장 많았다.

그림 2-3-45

개인정보 침해사고 경험 유형 (복수응답) - 개인정보 침해사고 경험자

(단위 : %)



나. 개인정보 침해사고 대응활동 수행

개인정보 침해사고 경험자의 47.8%는 개인정보 침해 시 대응활동을 수행한 것으로 조사되었다.

세부 유형별로는 '해당 서비스를 탈퇴하고 동일한 서비스를 제공하는 다른 기업 이용'이 36.9%로 가장 높게 나타났고, 다음으로 '관련 기관에 신고 또는 상담 등의 조치(7.8%)', 'e프라이버시 클린서비스 이용(5.7%)' 등의 순으로 높게 나타났다.

그림 2-3-46

개인정보 침해사고 대응활동 수행 (복수응답) - 개인정보 침해사고 경험자

(단위 : %)



V 주요 서비스별 정보보호

1. 클라우드

클라우드 서비스 이용률은 37.8%로 조사되었다.

성별 및 연령별 분석 결과, 남성의 이용률(40.2%)이 여성(35.2%)보다 높고, 20대(63.0%)에서 타 연령 대비 클라우드 서비스를 많이 이용하는 것으로 조사되었다.

그림 2-3-47 클라우드 서비스 이용

(단위 : %)

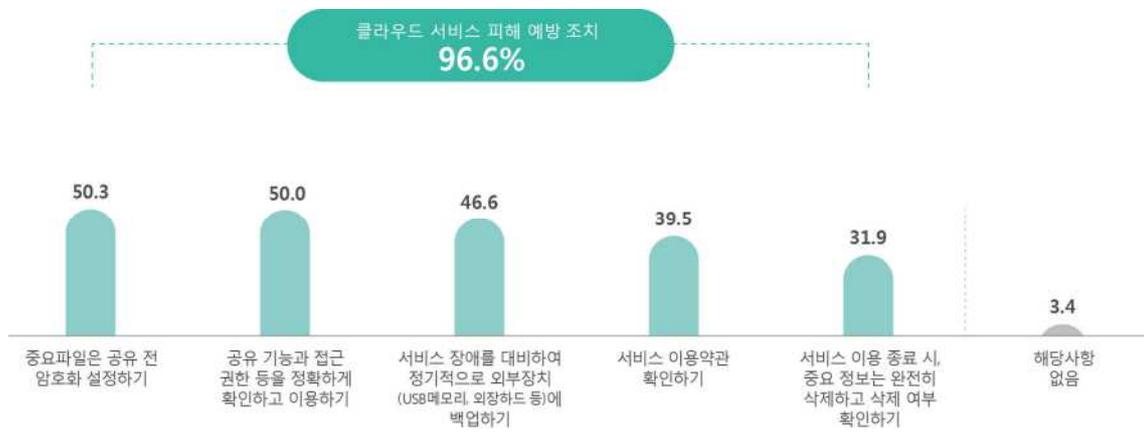


클라우드 서비스 이용자의 96.6%는 클라우드 서비스 피해 예방 조치를 취하는 것으로 조사되었다.

세부 유형별로는 '중요파일은 공유 전 암호화 설정하기(50.3%)', '공유 기능과 접근 권한 등을 정확하게 확인하고 이용하기(50.0%)' 등의 순으로 나타났다.

그림 2-3-48 클라우드 서비스 침해사고 예방 조치 (복수응답) - 클라우드 서비스 이용자

(단위 : %)



2. 빅데이터

빅데이터를 활용한 개인 맞춤형 서비스 이용률은 36.2%로 조사되었다.

성별 및 연령별 분석 결과, 빅데이터 활용 서비스 경험률은 남성(37.8%)이 여성(34.6%)보다 높고, 20~30대(20대: 49.7%, 30대: 46.4%)가 타 연령 대비 높은 것으로 나타났다.

그림 2-3-49

빅데이터 활용 서비스 이용

(단위 : %)



빅데이터 활용 서비스가 확산될 경우 우려되는 사항은 '필요 이상의 과도한 개인정보의 수집'이 54.9%로 가장 높고, 다음으로 '수집된 개인정보의 무단 활용(50.3%)'이 높았다.

그림 2-3-50

빅데이터 활용 서비스 대중화 시 보안 우려사항 (2가지)

(단위 : %)



3. 사물인터넷(IoT)

사물인터넷(IoT) 기반의 제품 및 서비스 이용률은 3.8%로 조사되었다.

성별 및 연령별 분석 결과, 사물인터넷(IoT) 이용률은 남성 3.8%, 여성 3.7%로 나타났으며 40대(6.1%)에서 상대적으로 높게 나타났다.

그림 2-3-51

사물인터넷(IoT) 제품·서비스 이용

(단위 : %)



사물인터넷(IoT) 제품 및 서비스를 유형별로 살펴보면, '스마트홈(38.4%)'을 가장 많이 이용하는 것으로 나타났다.

그림 2-3-52

사물인터넷(IoT) 이용 제품 서비스 유형 (복수응답) - 사물인터넷(IoT) 제품·서비스 이용자

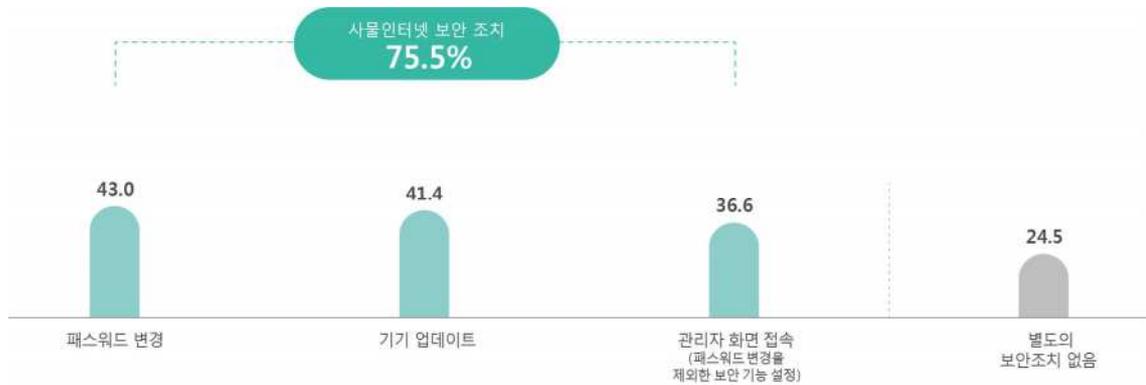
(단위 : %)



사물인터넷(IoT) 제품·서비스 이용자의 75.5%는 사물인터넷(IoT) 보안 조치를 취하는 것으로 나타났다.

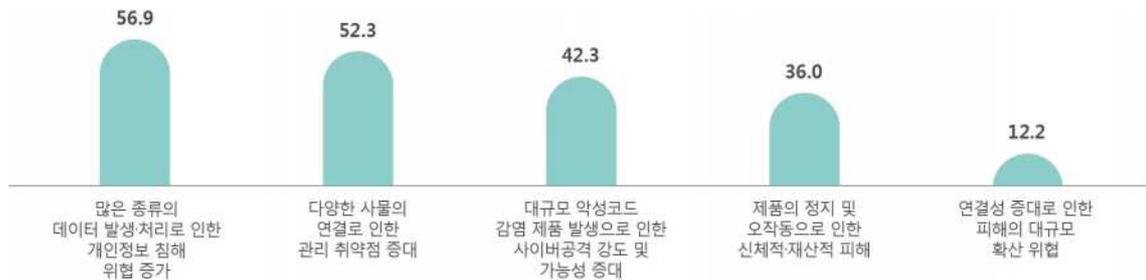
세부 유형별로는 '패스워드 변경'이 43.0%로 가장 높았고, 다음으로 '기기 업데이트 (41.4%)' 등의 순이었다.

그림 2-3-53 사물인터넷(IoT) 보안을 위한 조치 (복수응답) - 사물인터넷(IoT) 제품·서비스 이용자 (단위 : %)



사물인터넷(IoT) 제품·서비스가 확산될 경우 '많은 종류의 데이터 발생·처리로 인한 개인정보 침해 위협 증가(56.9%)'를 가장 우려하는 것으로 나타났고, 다음으로 '다양한 사물의 연결로 인한 관리 취약점 증대(52.3%)' 등의 순으로 조사되었다.

그림 2-3-54 사물인터넷(IoT) 대중화 시 보안 우려사항 (2가지) (단위 : %)

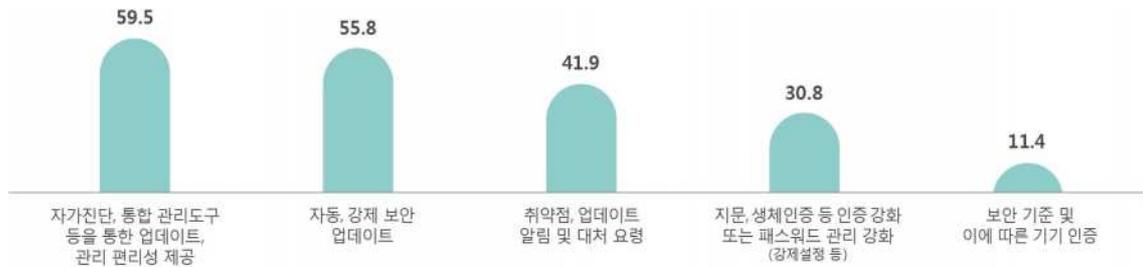


실생활 보안을 위해 사물인터넷(IoT) 기기에 추가되어야 하는 기능을 조사한 결과, '자가 진단, 통합 관리도구 등을 통한 업데이트, 관리 편리성 제공'이 59.5%로 가장 높게 조사되었다.

다음으로 '자동, 강제 보안 업데이트(55.8%)' 등이 그 뒤를 이었다.

그림 2-3-55 사물인터넷(IoT)에 추가되어야 하는 보안 기능 (2가지)

(단위 : %)



4. 핀테크

간편결제 서비스 이용률은 44.6%로 조사되었다.

성별 및 연령별 분석 결과, 남성(47.2%)이 여성(41.8%)보다 높게 나타났고, 20대(73.0%)가 타 연령 대비 상대적으로 높게 나타났다.

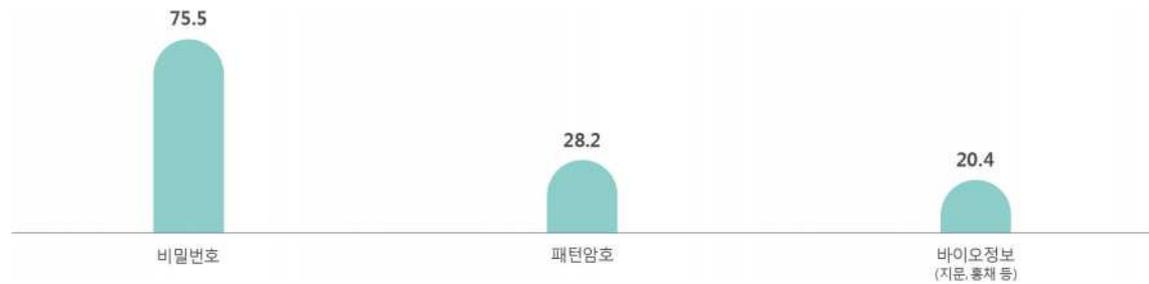
그림 2-3-56 간편결제 서비스 이용

(단위 : %)



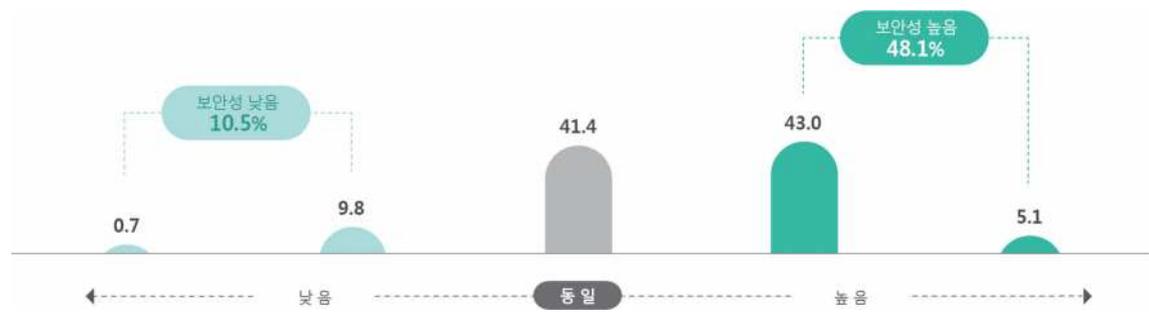
간편결제 서비스 이용자의 주요 보안인증수단은 '비밀번호(75.5%)'로 나타났고, 다음으로 '패턴암호(28.2%)', '바이오정보(20.4%)' 순으로 조사되었다.

그림 2-3-57 간편결제 서비스 보안인증수단 (복수응답) - 간편결제 서비스 이용자 (단위 : %)



간편결제 서비스 이용자의 48.1%는 일반결제 대비 간편결제의 보안성이 높다고 인식했다. 반면, 일반결제 대비 보안성이 낮다고 응답한 비율은 10.5%로 나타났다.

그림 2-3-58 일반결제 대비 간편결제 서비스 보안성 인식 - 간편결제 서비스 이용자 (단위 : %)



5. 인공지능(AI)

인공지능(AI)을 활용한 서비스 이용률은 18.7%로 조사되었다.

성별 및 연령별 분석 결과, 남성(20.1%)이 여성(17.3%)보다 높게 나타났고, 20대(31.1%)가 타 연령 대비 상대적으로 높게 나타났다.

그림 2-3-59

인공지능(AI) 활용 서비스 이용

(단위 : %)



인공지능(AI) 활용 서비스 이용자 중 '번역 서비스'를 이용한 경험이 있는 비율은 63.1%로 가장 높고, '(인공지능(AI))비서(40.9%)', '(인공지능(AI))금융 서비스(18.6%)' 순으로 나타났다.

그림 2-3-60

인공지능(AI) 활용 서비스 이용 유형 (복수응답) - 인공지능(AI) 활용 서비스 이용자

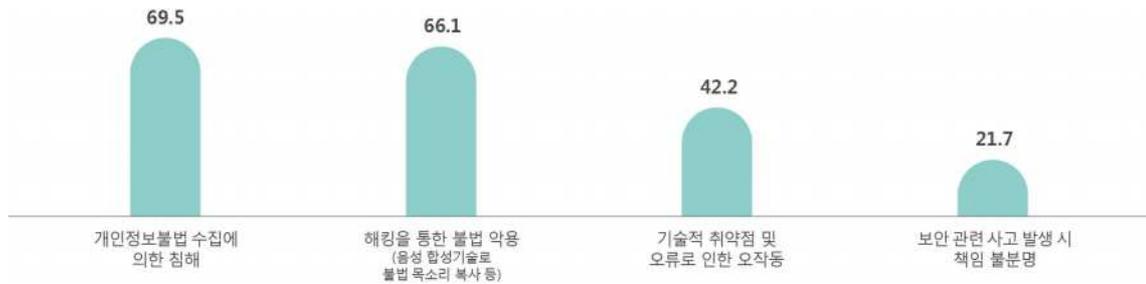
(단위 : %)



인공지능(AI) 활용 서비스가 확산될 경우 우려사항으로는 '개인정보 불법 수집에 의한 침해'가 69.5%로 가장 높고, 다음으로 '해킹을 통한 불법 악용(66.1%)'등의 순으로 조사되었다.

그림 2-3-61 인공지능(AI) 활용 서비스 대중화 시 보안 우려사항 (2가지)

(단위 : %)



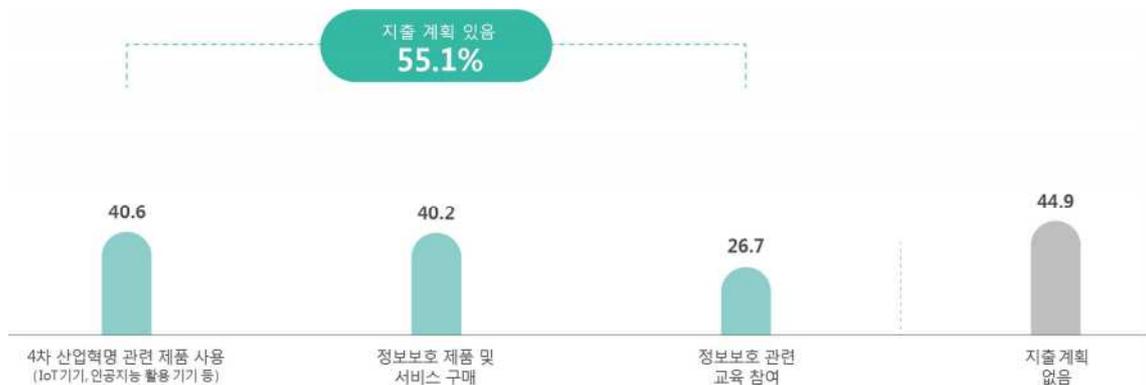
6. 향후 정보보호 지출 계획

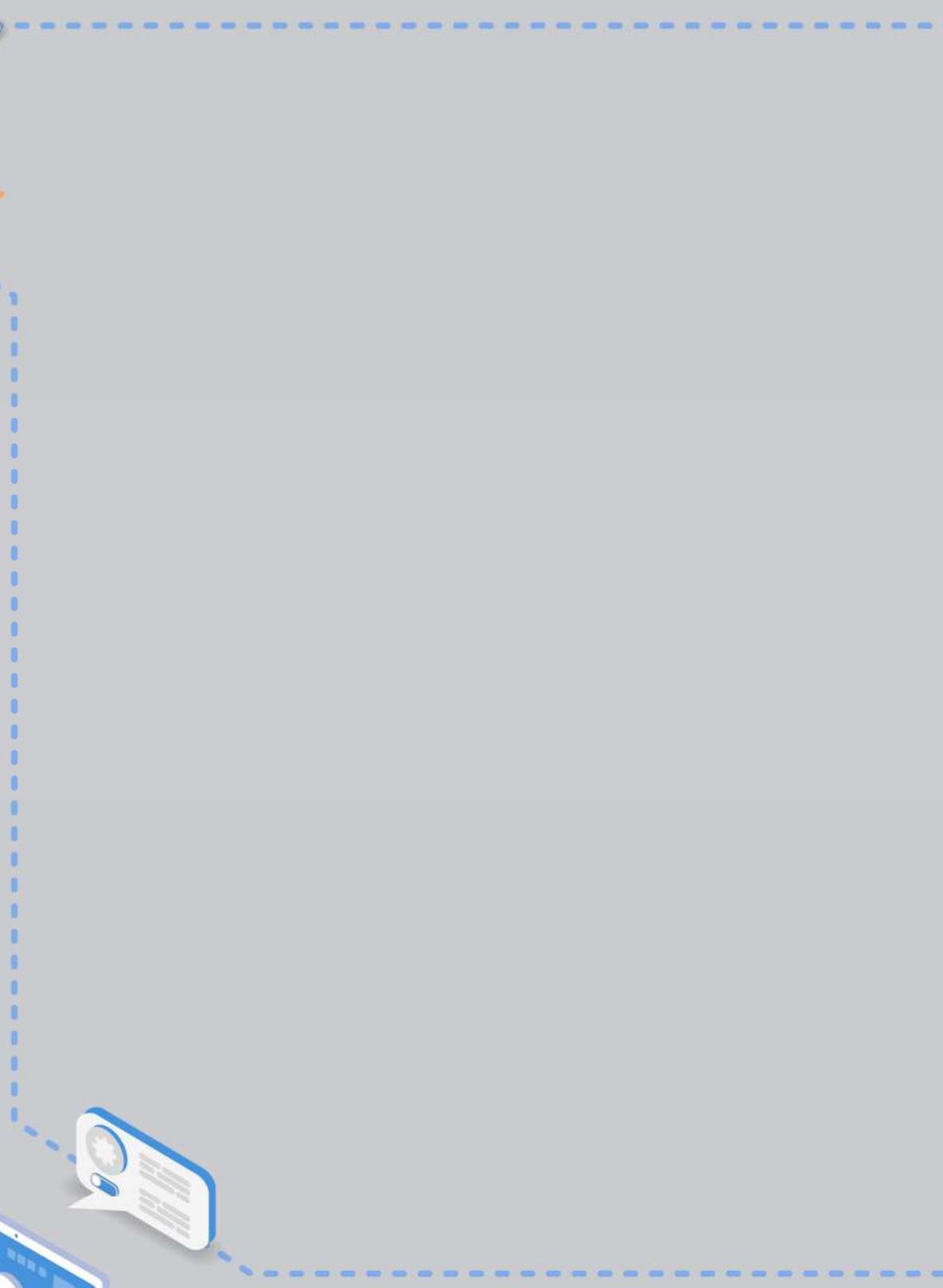
인터넷 이용자의 55.1%는 향후 정보보호를 위한 지출 계획이 있는 것으로 조사되었다.

분야별로 살펴보면, '4차 산업혁명 관련 제품사용(40.6%)'에 지출할 의향이 가장 높은 것으로 나타났고, 다음으로 '정보보호 제품 및 서비스 구매(40.2%)'가 높게 나타났다.

그림 2-3-62 향후 정보보호 지출 계획 분야 (2가지)

(단위 : %)







부록
1

주요변경내역



I 기업부문

분 야	항 목	세 부 항 목	조 사 시 기
I. 정보보호 기반 및 환경	A. 정보보호 인식	정보보호 중요성 인식	'18
		개인정보보호 중요성 인식	'18
		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 -'18
		정보보호 인적 위협요인	'06, '08 -'18
		사이버 환경상의 안전성 정도	'07 -'10
		우려하는 개인정보 유출요인	'12 -'18
		정보보호 애로사항	'15 -'18
		정보보호 규제 동의 수준	'15 -'16
		B. 정보보호 정책 및 조직	정보보호(개인정보보호) 정책 수립
	정보보호 정책 포함 위협요소		'14 -'18
	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 -'18
	정보보호 관련 책임자 임명 및 전담		'06 -'18
	정보관리책임자(CIO)와 겸직 여부		'16
	정보보호 조직 및 담당인력 현황과 향후 계획		'14
	IT인력 중 정보보호 담당 인력 비중		'14, '16 -'18
	IT인력대비 정보보호 전담인력 투입 비율		'10

분 야	항 목	세 부 항 목	조 사 시 기	
	B. 정보보호 정책 및 조직	정보보호 담당 인력 신규 채용계획	'17 -'18	
		정보보호 교육의 필요성	'07 -'09	
		정보보호(개인정보보호) 교육 실시	'06 -'18	
		교육 대상별 교육 실시 현황	'06 -'18	
		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 -'18	
		정보보호 예산 총액 중 분야별 비율	'14	
		정보보호 관련 예산 증감	'11 -'18	
		정보보호 지출 분야	'13 -'18	
		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
	정보보호 제품 이용			'06 -'18
	CCTV 보유 대수			'16 -'18
정보보호 제품 국산/외산 비중	'15 -'18			
외산 정보보호 제품 구매 이유	'16 -'18			
정보보호 서비스 이용	'06 -'18			
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 비교려 이유	'13			

분야	항목	세부항목	조사시기
	B. 정보보호 관리	정보자산 관리를 위한 수행활동	'14
		시스템 및 네트워크 보안점검(취약점 점검) 실시	'09 -'18
		시스템 및 네트워크 보안점검(취약점 점검) 항목	'14 -'18
		보안패치 적용 방법	'07 -'18
		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 -'18
		구형 운영체제 사용 이유	'17
		시스템 로그 및 중요 데이터 백업 실시 및 실시 주기	'12 -'18
		백업 방식	'17 -'18
Ⅲ. 침해사고 경험 및 대응	A. 침해사고 경험	침해사고 피해 경험	'06 -'18
		침해사고 피해 유형별 피해 빈도	'07 -'14
		침해사고 피해 경험 유형 및 심각성 정도	'14 -'18
		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 -'18
		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
	B. 침해사고 대응	개인정보 유출 및 명의도용으로 인한 피해 경험 여부	'11 -'12
		개인정보 유출 및 명의도용 사고 시 신고 여부 및 기관	'11
		개인정보 유출 및 명의도용 정보보안 침해사고 발생 시 신고 정도	'11
		정보보호 피해양상 유형	'10
		침해사고 대응활동 수행	'06 -'18
		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	

분 야	항 목	세 부 항 목	조 사 시 기
		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 -'18
IV. 개인정보보호	A. 개인정보 수집	개인정보 수집 및 이용	'12 -'18
		개인정보 온라인 수집 방법	'14 -'18
		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 -'18
		개인정보 수집 및 이용 목적	'12 -'18
		보유하고 있는 이용자(고객) 개인정보 규모	'12 -'14
		B. 개인정보 침해사고 예방	개인정보 침해사고 예방을 위한 관리적 조치(사후처리)
	개인정보 침해사고 예방을 위한 기술적 조치		'10 -'18
	개인정보 암호화		'09 -'18
	회원가입, 홈페이지 이용 시 본인확인수단		'14
	회원가입 시 본인확인 여부		'13
	이용 중인 주민번호 대체 수단		'12 -'13
	개인정보보호 내부관리계획 내용		'12
	개인정보보호 예산 배정 여부		'12
	개인정보보호법 인지 여부		'11
	개인정보보호를 위한 조치 여부		'11
	개인정보 취급방침별 공개 여부		'07 -'11
	개인정보 수집 이용/제공 시 이용자 동의 확보 여부		'07 -'11
	수집한 개인정보의 제3자 제공/취급 위탁 여부		'10 -'11
	제3자 제공/취급 위탁의 제공 형태		'09 -'11
	제3자 제공 시 공지 및 동의 확보 여부		'07 -'11
	제3자 취급 위탁 시 공지 및 동의 확보 여부		'07 -'11
	개인정보 파기 절차 및 방법에 대한 지침 확보		'08 -'11
	개인정보 침해사고 사후처리방침 문서화 여부	'07 -'11	
개인정보 전담조직 내부관리계획 수립여부	'09		

분야	항목	세부항목	조사시기
		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
		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 '12 -'18
		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 -'18	
개인정보 침해사고 외부 신고 여부		'13	
개인정보 침해사고 발생 시 고지 방법	'12 -'13		

분 야	항 목	세 부 항 목	조 사 시 기
		개인정보 침해사고발생 시 신고하지 않은 이유	'12 -'13
		개인정보 침해사고 시 보상여부	'12
		개인정보 침해사고 시 통지 또는 고지	'17 -'18
		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
		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

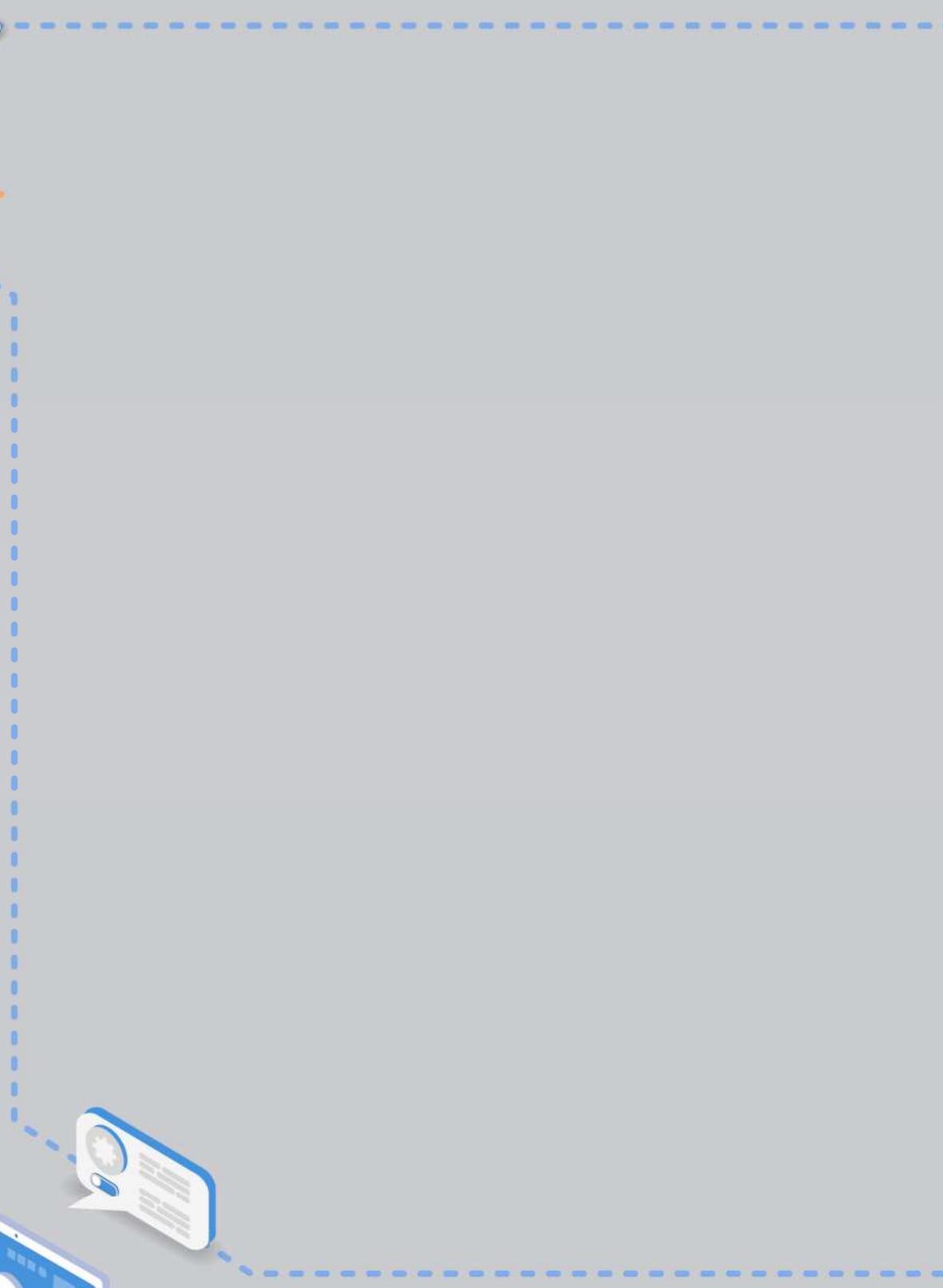
분 야	항 목	세 부 항 목	조 사 시 기
V. 주요 서비스별 정보보호	A. 무선랜	무선랜 구축 및 운영	'10 ~'13, '15 ~'18
		무선랜 관련 보안 우려사항	'12, '15 ~'18
		사내 무선랜 보안정책 수립 현황	'10 ~'11, '13, '15 ~'16
		사내 무선랜 보안 정책 내용	'10 ~'13
		무선랜 보안을 위한 조치	'10 ~'11, '13, '15 ~'18
		외부 상용무선인터넷 서비스 사용 가능여부	'11 ~'13
		외부 상용무선인터넷 서비스 관리정책 수립 현황	'11 ~'13
	B. 모바일	모바일 오피스 구축.운영 현황	'10 ~'13
		모바일 오피스 도입 보안대책 수립 현황	'10 ~'14
		모바일 오피스 보안수칙 포함 내용	'13 ~'14
		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 ~'18
		개인소유 모바일 기기 활용 시 보안 우려사항	'14 ~'18
		모바일 기기 활용 시의 보안위협에 대한 대응방안	'14 ~'18
	C. 클라우드	클라우드 서비스 이용 및 향후 도입(유지) 계획	'10 ~'13, '15 ~'18
		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 ~'18
		클라우드 서비스 보안을 위한 조치	'16 ~'18
		클라우드 서비스 보안 우려사항	'10 ~'12, '14 ~'18,
	빅데이터 도입 및 활용 관련 우려사항	'14	
	D. 사물인터넷 (IoT)	사물인터넷(IoT) 제품 및 서비스 이용 및 향후 도입(유지) 계획	'15 ~'18
		사물인터넷(IoT) 이용 활성화를 위해 개선되어야 할 사항	'15 ~'16
		사물인터넷(IoT) 이용(계획) 분야	'17 ~'18
		사물인터넷(IoT) 보안을 위한 조치	'18
		사물인터넷(IoT) 관련 보안위협에 대한 우려	'15 ~'18
	E. 정보보호 (사이버) 보험	정보보호(사이버) 보험 인지	'17 ~'18
		정보보호(사이버) 보험 이용 및 향후 가입(유지) 계획	'17 ~'18
		정보보호(사이버) 보험 희망 보장 항목	'17 ~'18
	F. 향후 투자 계획	신규서비스 정보보호 투자 현황	'14 ~'18

II 개인부문

분야	항목	세부항목	조사시기
I. 정보보호 인식		정보보호 중요성 인식	'06 -'18
		개인정보보호 중요성 인식	'08 -'18
		위협사안에 대한 구체적 인지	'14 -'18
		위협사안에 대한 피해의 심각성	'06 -'11, '12 -'18
		정보보호 관련 관심정보 유형	'12 -'16
		정보보호 관련 정보수집 및 학습활동	'06 -'18
		정보보호 관련 정보수집 및 학습 애로사항	'12 -'16
II. 침해사고 예방	A. 정보보호 관련 제품	정보보호 제품*	'06 -'18
		정보보호 제품 미이용 이유*	'12 -'18
		정보보호 소프트웨어 이용*	'14 -'18
		정보보호 제품 이용 시 활용 기능	'12 -'15
		악성코드 검사 실시 주기*	'14 -'18
		파일 다운로드 시 바이러스 검사 방법	'11 -'15
		백신 프로그램 업데이트 방법*	'06 -'18
		백신 프로그램 업데이트 실시 주기*	'14 -'18
		운영체제 보안 업데이트*	'06 -'18
		운영체제 보안 업데이트 미실시 이유*	'12 -'18
		구형 운영체제 사용 이유	'17
		중요 데이터 백업*	'06 -'10 '12 -'18
		중요 데이터 백업 방식*	'17 -'18
		중요 데이터 백업 실시 주기*	'14 -'18
		PC 및 네트워크 보안을 위한 노력	'14 -'18
		PC 비밀번호 설정	'06 -'18
		비밀번호 관리 조치	'12 -'18
	PC 및 웹사이트 비밀번호 변경 주기	'06 -'18	
	B. 모바일 및 무선랜 보안	무선랜 이용 및 무선랜 침해사고 예방 조치	'10 -'18
		모바일 기기 데이터 백업	'17
		모바일 기기 데이터 백업 방식	'17
		모바일 기기 데이터 백업 실시 주기	'17
		모바일 기기 침해사고 예방 조치	'10 -'18
	C. SNS 보안	SNS 이용	'11 -'18
		SNS 피해 유형별 인지	'10 -'15
		SNS 피해 예방 조치	'12 -'18

분 야	항 목	세 부 항 목	조 사 시 기	
Ⅲ. 침해사고 대응	A. 침해사고 경험	침해사고 피해 경험 유형*	'11 ~'18	
		피싱/파밍/스미싱 등 전자금융사기 피해 경로	'10 ~'18	
	B. 침해사고 대응조치	침해사고 대응활동 수행	'14 ~'18	
		침해사고 신고 또는 상담 문의 기관·업체	'07 ~'18	
		침해사고 신고 또는 상담하지 않은 이유	'12 ~'18	
		침해사고 발생 초동대처 주체	'15	
		정보보호 규제방식에 대한 동의 정도	'15	
Ⅳ. 개인정보보호	A. 개인정보보호 조치	온라인 상 개인정보 제공 목적	'07~'18	
		개인정보 침해사고 예방조치	'14~'18	
		인터넷 서비스 회원가입 시 주민번호 이외 수단 인지·이용·선택도	'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 ~'18	
		개인정보 침해사고 경험 유형	'06 ~'18	
		개인정보 침해사고 대응조치	'14 ~'18	
	Ⅴ. 주요 서비스별 정보보호	A. 클라우드	클라우드 서비스 이용	'15 ~'18
			클라우드 서비스 침해사고 예방 조치	'15 ~'18
B. 빅데이터		빅데이터 활용 서비스 경험	'17 ~'18	
		빅데이터 활용 서비스 확산 시 위협요인	'15 ~'18	
C. 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 보안을 원하는 보안 기능	'18	
D. 핀테크		간편결제 서비스 이용	'15 ~'18	
		이용한 간편결제 서비스 본인인증수단	'17 ~'18	
		일반결제 대비 간편결제 서비스 보안성 인식	'15 ~'18	
E. 인공지능(AI)		인공지능(AI) 활용 서비스 이용	'17 ~'18	
		이용한 인공지능(AI) 활용 서비스	'17 ~'18	
	인공지능(AI) 활용 서비스 대중화 시 보안 우려사항	'17 ~'18		
F. 향후지출계획	향후 정보보호 지출 계획 분야	'18		

* 2018년 PC/모바일 문항 분리





부록
2

표본오차



I 기업부문

1. 정보보호(개인정보보호) 정책 수립률

부록 표 1-1

정보보호(개인정보보호) 정책 수립률

(단위 : %)

	정보보호 (개인정보보호) 정책 수립률	표본오차	상대표준오차	95% 신뢰구간		
				하한(%)	상한(%)	
전 체	16.0	0.75	2.39	15.3	16.8	
업 종 별	농림수산업	31.3	5.02	8.17	26.3	36.3
	제조업	14.1	2.02	7.28	12.1	16.2
	건설업	10.7	2.13	10.17	8.5	12.8
	도매 및 소매업	8.8	1.86	10.73	7.0	10.7
	운수업	12.0	2.57	10.88	9.5	14.6
	숙박 및 음식점업	5.9	1.82	15.66	4.1	7.7
	정보서비스업	53.4	3.75	3.58	49.6	57.1
	금융 및 보험업	84.9	2.61	1.57	82.3	87.5
	부동산 및 임대업	16.8	3.04	9.22	13.8	19.9
	기술서비스업	21.2	2.79	6.69	18.5	24.0
	시설/사업지원	26.6	3.16	6.06	23.4	29.7
	개인서비스업	8.4	2.33	14.17	6.1	10.7
	기타	26.5	3.31	6.37	23.2	29.8
규 모 별	1~4명	6.9	1.06	7.86	5.8	7.9
	5~9명	19.5	2.31	6.05	17.2	21.8
	10~49명	47.2	1.99	2.15	45.2	49.2
	50~249명	78.2	1.76	1.15	76.4	80.0
	250명 이상	90.9	1.20	0.68	89.7	92.1

2. 정보보호 정책 수립률

부록 표 1-2

정보보호 정책 수립률

(단위 : %)

	정보보호 정책 수립률	표본오차	상대표준오차	95% 신뢰구간		
				하한(%)	상한(%)	
전 체	14.5	0.72	2.54	13.7	15.2	
업 종 별	농림수산업	31.2	5.01	8.19	26.2	36.2
	제조업	13.7	1.99	7.42	11.7	15.7
	건설업	9.5	2.01	10.87	7.4	11.5
	도매 및 소매업	7.5	1.73	11.70	5.8	9.3
	운수업	11.8	2.54	11.02	9.2	14.3
	숙박 및 음식점업	5.8	1.79	15.89	4.0	7.6
	정보서비스업	47.9	3.76	4.00	44.1	51.7
	금융 및 보험업	83.2	2.73	1.67	80.5	85.9
	부동산 및 임대업	8.0	2.20	14.11	5.8	10.2
	기술서비스업	17.9	2.61	7.43	15.3	20.6
	시설/사업지원	24.9	3.09	6.34	21.8	27.9
	개인서비스업	6.9	2.14	15.73	4.8	9.1
	기타	24.9	3.24	6.65	21.6	28.1
규 모 별	1~4명	5.4	0.95	8.95	4.5	6.4
	5~9명	18.0	2.24	6.34	15.8	20.3
	10~49명	45.0	1.98	2.24	43.1	47.0
	50~249명	76.2	1.81	1.21	74.4	78.0
	250명 이상	89.5	1.29	0.73	88.2	90.8

3. 개인정보보호 정책 수립률

부록 표 1-3

개인정보보호 정책 수립률

(단위 : %)

	개인정보보호 정책 수립률	표본오차	상대표준오차	95% 신뢰구간		
				하한(%)	상한(%)	
전 체	14.9	0.73	2.50	14.2	15.7	
업 종 별	농림수산업	30.6	4.99	8.30	25.7	35.6
	제조업	13.0	1.95	7.66	11.0	14.9
	건설업	9.1	1.98	11.10	7.1	11.1
	도매 및 소매업	7.4	1.72	11.78	5.7	9.2
	운수업	9.8	2.35	12.19	7.5	12.2
	숙박 및 음식점업	5.7	1.79	15.96	3.9	7.5
	정보서비스업	49.0	3.76	3.91	45.3	52.8
	금융 및 보험업	84.1	2.66	1.62	81.5	86.8
	부동산 및 임대업	15.2	2.92	9.78	12.3	18.2
	기술서비스업	19.4	2.69	7.09	16.7	22.1
	시설/사업지원	24.5	3.08	6.40	21.4	27.6
	개인서비스업	8.2	2.31	14.38	5.9	10.5
	기타	26.1	3.30	6.43	22.8	29.4
규 모 별	1~4명	6.0	1.00	8.45	5.0	7.0
	5~9명	18.0	2.24	6.35	15.8	20.3
	10~49명	45.3	1.98	2.23	43.3	47.3
	50~249명	77.0	1.79	1.19	75.2	78.8
	250명 이상	90.0	1.26	0.72	88.7	91.2

4. 정보보호 책임자 임명_정보관리책임자(CIO)

부록 표 1-4

정보보호 관련 책임자 임명_정보관리책임자(CIO)

(단위 : %)

	CIO 임명률	표본오차	상대표준오차	95% 신뢰구간		
				하한(%)	상한(%)	
전 체	8.7	0.58	3.39	8.1	9.2	
업 종 별	농림수산업	17.8	4.14	11.87	13.7	21.9
	제조업	8.5	1.62	9.68	6.9	10.1
	건설업	3.9	1.33	17.50	2.5	5.2
	도매 및 소매업	6.7	1.64	12.44	5.1	8.3
	운수업	2.5	1.24	25.05	1.3	3.8
	숙박 및 음식점업	2.2	1.12	26.50	1.0	3.3
	정보서비스업	41.3	3.70	4.57	37.6	45.0
	금융 및 보험업	52.5	3.64	3.54	48.8	56.1
	부동산 및 임대업	4.9	1.76	18.19	3.2	6.7
	기술서비스업	16.0	2.50	7.97	13.5	18.5
	시설/사업지원	16.9	2.68	8.08	14.2	19.6
	개인서비스업	4.3	1.70	20.32	2.6	6.0
	기타	12.1	2.44	10.33	9.6	14.5
규 모 별	1~4명	2.3	0.63	13.85	1.7	3.0
	5~9명	12.1	1.90	8.03	10.2	14.0
	10~49명	28.2	1.79	3.24	26.4	29.9
	50~249명	54.7	2.12	1.98	52.6	56.8
	250명 이상	72.5	1.87	1.32	70.6	74.3

5. 정보보호 책임자 임명_정보보호최고책임자(CISO)

부록 표 1-5 | 정보보호 관련 책임자 임명_정보보호최고책임자(CISO) (단위 : %)

	CISO 임명률	표본오차	상대표준오차	95% 신뢰구간		
				하한(%)	상한(%)	
전 체	8.8	0.58	3.36	8.3	9.4	
업 종 별	농림수산업	17.7	4.13	11.89	13.6	21.9
	제조업	8.0	1.57	10.02	6.4	9.6
	건설업	6.4	1.68	13.44	4.7	8.1
	도매 및 소매업	5.4	1.47	14.02	3.9	6.8
	운수업	4.1	1.56	19.56	2.5	5.6
	숙박 및 음식점업	1.9	1.05	28.15	0.9	3.0
	정보서비스업	28.2	3.38	6.12	24.8	31.6
	금융 및 보험업	63.6	3.51	2.81	60.1	67.1
	부동산 및 임대업	2.9	1.36	24.10	1.5	4.2
	기술서비스업	12.7	2.27	9.09	10.5	15.0
	시설/사업지원	16.1	2.63	8.34	13.4	18.7
	개인서비스업	4.1	1.67	20.67	2.5	5.8
	기타	15.4	2.71	8.96	12.7	18.1
규 모 별	1~4명	2.0	0.58	15.15	1.4	2.5
	5~9명	10.3	1.77	8.77	8.6	12.1
	10~49명	31.3	1.84	3.00	29.5	33.2
	50~249명	66.0	2.02	1.56	64.0	68.0
	250명 이상	83.6	1.55	0.95	82.1	85.2

6. 정보보호 책임자 임명_개인정보보호책임자(CPO)

부록 표 1-6

정보보호 관련 책임자 임명_개인정보보호책임자(CPO)

(단위 : %)

	CPO 임명률	표본오차	상대표준오차	95% 신뢰구간		
				하한(%)	상한(%)	
전 체	8.4	0.57	3.45	7.8	9.0	
업 종 별	농림수산업	9.4	3.16	17.10	6.3	12.6
	제조업	7.2	1.50	10.62	5.7	8.7
	건설업	3.9	1.33	17.50	2.5	5.2
	도매 및 소매업	5.8	1.53	13.45	4.3	7.3
	운수업	3.6	1.47	20.89	2.1	5.0
	숙박 및 음식점업	1.9	1.05	28.23	0.8	3.0
	정보서비스업	28.3	3.39	6.11	24.9	31.7
	금융 및 보험업	64.7	3.49	2.75	61.2	68.2
	부동산 및 임대업	3.7	1.54	21.14	2.2	5.2
	기술서비스업	12.9	2.28	9.04	10.6	15.2
	시설/사업지원	13.4	2.44	9.27	11.0	15.8
	개인서비스업	3.9	1.63	21.24	2.3	5.6
	기타	13.4	2.55	9.72	10.9	16.0
규 모 별	1~4명	2.5	0.66	13.23	1.9	3.2
	5~9명	10.8	1.81	8.54	9.0	12.6
	10~49명	25.2	1.73	3.49	23.5	27.0
	50~249명	60.2	2.08	1.77	58.1	62.3
	250명 이상	80.3	1.67	1.06	78.7	82.0

7. 정보보호 제품 이용_네트워크 보안

부록 표 1-7

정보보호 제품 이용_네트워크 보안

(단위 : %)

	네트워크 보안제품 이용률	표본오차	상대표준오차	95% 신뢰구간		
				하한(%)	상한(%)	
전 체	79.4	0.83	0.53	78.6	80.3	
업 종 별	농림수산업	88.6	3.43	1.98	85.2	92.1
	제조업	92.7	1.51	0.83	91.2	94.2
	건설업	90.6	2.01	1.13	88.6	92.6
	도매 및 소매업	79.8	2.63	1.68	77.2	82.4
	운수업	59.6	3.87	3.32	55.7	63.4
	숙박 및 음식점업	52.3	3.85	3.75	48.5	56.2
	정보서비스업	97.3	1.21	0.63	96.1	98.6
	금융 및 보험업	97.7	1.09	0.57	96.6	98.8
	부동산 및 임대업	89.4	2.50	1.43	86.9	91.9
	기술서비스업	90.8	1.97	1.11	88.8	92.7
	시설/사업지원	86.1	2.47	1.46	83.6	88.6
	개인서비스업	77.8	3.50	2.30	74.3	81.3
	기타	93.7	1.82	0.99	91.9	95.5
규 모 별	1~4명	74.6	1.83	1.25	72.7	76.4
	5~9명	86.1	2.02	1.20	84.0	88.1
	10~49명	93.4	0.99	0.54	92.4	94.4
	50~249명	96.3	0.81	0.43	95.5	97.1
	250명 이상	98.2	0.56	0.29	97.6	98.7

8. 정보보호 제품 이용_시스템(단말) 보안

부록 표 1-8

정보보호 제품 이용_시스템(단말) 보안

(단위 : %)

	시스템 보안 제품 이용률	표본오차	상대표준오차	95% 신뢰구간		
				하한(%)	상한(%)	
전 체	79.9	0.82	0.52	79.1	80.7	
업 종 별	농림수산업	90.3	3.21	1.81	87.1	93.5
	제조업	91.5	1.61	0.90	89.9	93.2
	건설업	89.4	2.12	1.21	87.3	91.5
	도매 및 소매업	80.9	2.57	1.62	78.3	83.4
	운수업	64.6	3.77	2.98	60.8	68.3
	숙박 및 음식점업	50.5	3.85	3.89	46.6	54.3
	정보서비스업	94.2	1.76	0.95	92.5	96.0
	금융 및 보험업	96.5	1.35	0.71	95.1	97.8
	부동산 및 임대업	91.3	2.29	1.28	89.0	93.6
	기술서비스업	90.8	1.97	1.11	88.8	92.8
	시설/사업지원	94.0	1.70	0.92	92.3	95.7
	개인서비스업	82.0	3.23	2.01	78.8	85.3
	기타	91.7	2.07	1.15	89.6	93.8
규 모 별	1~4명	75.9	1.79	1.21	74.1	77.7
	5~9명	85.7	2.04	1.21	83.7	87.8
	10~49명	90.6	1.16	0.65	89.5	91.8
	50~249명	94.2	1.00	0.54	93.2	95.2
	250명 이상	97.5	0.66	0.34	96.8	98.2

9. 정보보호 제품 이용_콘텐츠/정보유출 방지 보안

부록 표 1-9

정보보호 제품 이용_콘텐츠/정보유출 방지 보안

(단위 : %)

	콘텐츠 정보유출방지 제품 이용률	표본오차	상대표준오차	95% 신뢰구간		
				하한(%)	상한(%)	
전 체	33.3	0.97	1.48	32.3	34.2	
업 종 별	농림수산업	42.7	5.35	6.39	37.4	48.1
	제조업	26.4	2.56	4.93	23.9	29.0
	건설업	44.3	3.42	3.94	40.9	47.7
	도매 및 소매업	34.2	3.10	4.63	31.1	37.3
	운수업	21.7	3.25	7.65	18.4	25.0
	숙박 및 음식점업	13.5	2.63	9.92	10.9	16.2
	정보서비스업	70.9	3.41	2.45	67.5	74.4
	금융 및 보험업	82.7	2.76	1.70	79.9	85.4
	부동산 및 임대업	56.0	4.04	3.68	51.9	60.0
	기술서비스업	61.8	3.31	2.73	58.5	65.1
	시설/사업지원	38.2	3.47	4.64	34.7	41.7
	개인서비스업	20.2	3.38	8.54	16.8	23.5
	기타	36.0	3.60	5.11	32.4	39.6
규 모 별	1~4명	25.5	1.83	3.66	23.7	27.3
	5~9명	43.4	2.89	3.40	40.5	46.3
	10~49명	54.2	1.98	1.87	52.2	56.2
	50~249명	68.0	1.99	1.49	66.0	70.0
	250명 이상	79.5	1.69	1.09	77.8	81.2

10. 정보보호 제품 이용_보안 관리

부록 표 1-10

정보보호 제품 이용_보안 관리

(단위 : %)

	보안 관리 제품 이용률	표본오차	상대표준오차	95% 신뢰구간		
				하한(%)	상한(%)	
전 체	43.3	1.02	1.20	42.3	44.3	
업 종 별	농림수산업	56.3	5.37	4.87	50.9	61.6
	제조업	50.5	2.90	2.93	47.6	53.4
	건설업	55.3	3.42	3.16	51.8	58.7
	도매 및 소매업	39.2	3.19	4.15	36.0	42.4
	운수업	24.1	3.37	7.15	20.7	27.5
	숙박 및 음식점업	18.9	3.02	8.13	15.9	22.0
	정보서비스업	69.9	3.45	2.52	66.5	73.4
	금융 및 보험업	85.1	2.60	1.56	82.5	87.7
	부동산 및 임대업	58.7	4.00	3.48	54.7	62.7
	기술서비스업	62.8	3.29	2.68	59.5	66.1
	시설/사업지원	49.7	3.57	3.67	46.1	53.2
	개인서비스업	29.6	3.84	6.62	25.8	33.4
	기타	61.8	3.64	3.01	58.2	65.4
규 모 별	1~4명	33.4	1.98	3.02	31.4	35.4
	5~9명	56.4	2.89	2.61	53.6	59.3
	10~49명	70.9	1.81	1.30	69.1	72.7
	50~249명	81.7	1.65	1.03	80.1	83.4
	250명 이상	86.7	1.42	0.84	85.3	88.2

11. 정보보호 제품 이용_인증 보안(바이오 인증 제외)

부록 표 1-11

정보보호 제품 이용_인증 보안(바이오 인증 제외)

(단위 : %)

	인증 보안(바이오 인증 제외) 제품 이용률	표본오차	상대표준오차	95% 신뢰구간		
				하한(%)	상한(%)	
전 체	51.5	1.02	1.01	50.5	52.5	
업 종 별	농림수산업	71.0	4.91	3.53	66.1	75.9
	제조업	65.4	2.76	2.15	62.7	68.2
	건설업	68.5	3.20	2.38	65.3	71.7
	도매 및 소매업	55.3	3.25	3.00	52.0	58.5
	운수업	32.1	3.68	5.85	28.4	35.8
	숙박 및 음식점업	22.7	3.22	7.26	19.4	25.9
	정보서비스업	71.7	3.39	2.41	68.3	75.1
	금융 및 보험업	87.4	2.42	1.42	84.9	89.8
	부동산 및 임대업	71.8	3.66	2.60	68.2	75.5
	기술서비스업	73.2	3.02	2.11	70.2	76.2
	시설/사업지원	63.0	3.45	2.79	59.6	66.5
	개인서비스업	34.3	3.99	5.94	30.3	38.3
	기타	58.1	3.70	3.25	54.4	61.8
규 모 별	1~4명	42.9	2.07	2.47	40.8	44.9
	5~9명	65.3	2.78	2.17	62.5	68.1
	10~49명	74.0	1.75	1.20	72.2	75.7
	50~249명	79.7	1.71	1.10	78.0	81.4
	250명 이상	85.2	1.49	0.89	83.7	86.7

12. 정보보호 제품 이용_인증 보안(바이오 인증)

부록 표 1-12

정보보호 제품 이용_인증 보안(바이오 인증)

(단위 : %)

	인증 보안 (바이오인증) 제품 이용률	표본오차	상대표준오차	95% 신뢰구간		
				하한(%)	상한(%)	
전 체	12.5	0.68	2.77	11.8	13.1	
업 종 별	농림수산업	23.4	4.58	9.99	18.8	27.9
	제조업	18.7	2.26	6.16	16.5	21.0
	건설업	13.8	2.37	8.79	11.4	16.1
	도매 및 소매업	9.0	1.87	10.61	7.1	10.9
	운수업	2.5	1.24	24.92	1.3	3.8
	숙박 및 음식점업	4.5	1.59	18.16	2.9	6.1
	정보서비스업	44.6	3.74	4.28	40.8	48.3
	금융 및 보험업	53.1	3.64	3.50	49.4	56.7
	부동산 및 임대업	7.0	2.08	15.11	4.9	9.1
	기술서비스업	26.3	3.00	5.82	23.3	29.3
	시설/사업지원	32.6	3.35	5.25	29.2	35.9
	개인서비스업	4.3	1.71	20.18	2.6	6.0
	기타	16.6	2.79	8.56	13.8	19.4
규 모 별	1~4명	5.9	0.99	8.56	4.9	6.9
	5~9명	20.6	2.36	5.85	18.2	22.9
	10~49명	30.4	1.83	3.07	28.6	32.3
	50~249명	42.9	2.11	2.51	40.8	45.0
	250명 이상	61.4	2.04	1.70	59.4	63.5

II 개인부문

1. 운영체제 보안 업데이트 실시율

부록 표 2-1 운영체제 보안 업데이트 실시율

(단위 : %)

		운영체제 보안 업데이트 실시율	표본오차	상대표준오차	95% 신뢰구간	
					하한(%)	상한(%)
	전 체	87.1	1.04	0.61	86.1	88.2
성 별	남	87.8	1.42	0.83	86.4	89.2
	여	86.4	1.51	0.89	84.9	88.0
연 령 별	12-19세	89.6	2.56	1.46	87.0	92.2
	20대	93.3	1.88	1.03	91.4	95.2
	30대	94.1	1.74	0.95	92.3	95.8
	40대	88.9	2.23	1.28	86.6	91.1
	50대	82.1	2.74	1.70	79.4	84.9
	60대	69.6	3.82	2.80	65.8	73.5

2. 정보보호 제품 이용률

부록 표 2-2 정보보호 제품 이용률

(단위 : %)

		정보보호 제품 이용률	표본오차	상대표준오차	95% 신뢰구간	
					하한(%)	상한(%)
	전 체	87.3	1.03	0.60	86.3	88.3
성 별	남	89.4	1.34	0.76	88.0	90.7
	여	85.2	1.57	0.94	83.6	86.7
연 령 별	12-19세	93.7	2.04	1.11	91.6	95.7
	20대	98.1	1.02	0.53	97.1	99.2
	30대	95.3	1.56	0.84	93.8	96.9
	40대	89.1	2.21	1.27	86.9	91.3
	50대	78.9	2.92	1.89	76.0	81.8
	60대	63.3	4.00	3.22	59.3	67.3

3. 중요 데이터 백업 실시율

부록 표 2-3

중요 데이터 백업 실시율

(단위 : %)

		중요 데이터 백업 실시율	표본오차	상대표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전 체		49.5	1.55	1.60	47.9	51.0
성 별	남	53.1	2.17	2.08	50.9	55.2
	여	45.6	2.20	2.46	43.4	47.8
연 령	12-19세	58.2	4.13	3.63	54.0	62.3
	20대	74.6	3.27	2.24	71.4	77.9
	30대	65.8	3.51	2.72	62.3	69.3
	40대	50.6	3.55	3.58	47.0	54.1
	50대	29.5	3.26	5.65	26.2	32.7
	60대	9.7	2.46	12.93	7.2	12.2

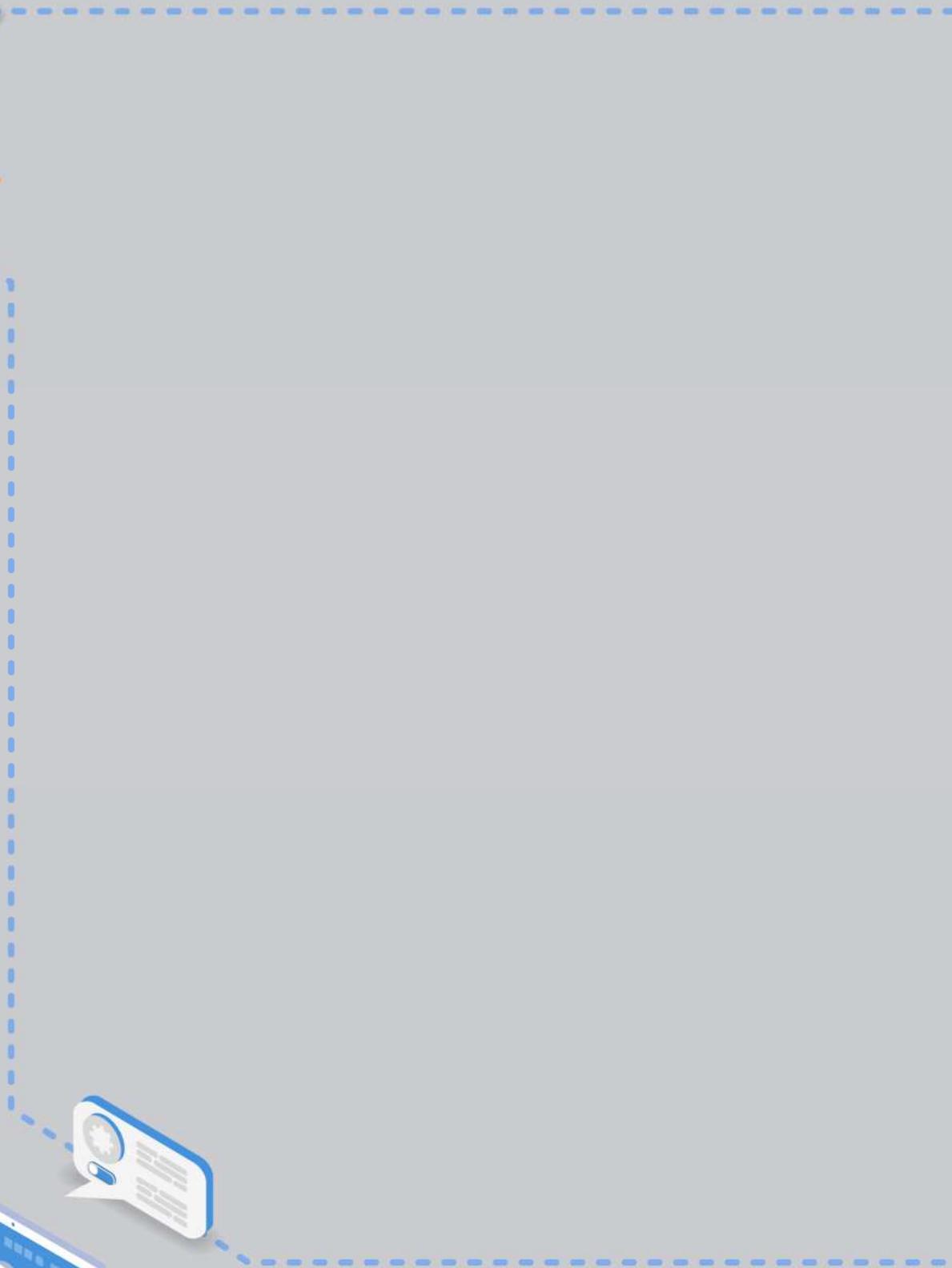
4. 개인정보 침해사고 경험률

부록 표 2-4

개인정보 침해사고 경험률

(단위 : %)

		개인정보 침해사고 경험률	표본오차	상대표준오차	95% 신뢰구간	
					하한(%)	상한(%)
전 체		1.9	0.43	11.24	1.5	2.4
성 별	남	2.0	0.61	15.34	1.4	2.7
	여	1.8	0.59	16.54	1.2	2.4
연 령	12-19세	1.7	1.08	32.67	0.6	2.8
	20대	2.7	1.22	22.93	1.5	3.9
	30대	1.7	0.96	28.63	0.7	2.7
	40대	3.0	1.22	20.51	1.8	4.2
	50대	0.9	0.69	37.31	0.3	1.6
	60대	1.1	0.88	39.47	0.3	2.0





부록
3

설문지





통계법 제33조(비밀의 보호 등)

통계작성과정에서 알려진 사항으로서 개인 또는 법인이나 단체의 비밀에 속하는 사항은 보호되어야 한다.

주 관 기 관 : 과학기술정보통신부
전 담 기 관 : 한국인터넷진흥원
조 사 기 관 : (주)글로벌리서치

2018년 정보보호 실태조사(기업)

안녕하십니까?

과학기술정보통신부와 한국인터넷진흥원에서는 우리나라 사업체의 정보보호 현황과 침해사고 피해 실태를 파악하여 관련 정책 수립의 기초자료를 마련하고자 전국의 사업체를 대상으로

“2018년 정보보호 실태조사(기업)”를 실시하고 있습니다.

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

이울러 작성해 주신 자료는 조사와 연구에 관련된 목적에만 사용될 것이며, 비밀은 철저히 보장될 것을 약속드립니다.

설문조사에 응해 주심에 감사드리며, 귀사의 평안과 번창하심을 기원합니다.

2018년 7월

* 조사 문의처 : 글로벌리서치 권유리 대리/ 이지숙 부장

지 역	<input type="checkbox"/> 1) 서울 <input type="checkbox"/> 2) 부산 <input type="checkbox"/> 3) 대구 <input type="checkbox"/> 4) 인천 <input type="checkbox"/> 5) 광주 <input type="checkbox"/> 6) 대전 <input type="checkbox"/> 7) 울산 <input type="checkbox"/> 8) 세종 <input type="checkbox"/> 9) 경기 <input type="checkbox"/> 10) 강원 <input type="checkbox"/> 11) 충북 <input type="checkbox"/> 12) 충남 <input type="checkbox"/> 13) 전북 <input type="checkbox"/> 14) 전남 <input type="checkbox"/> 15) 경북 <input type="checkbox"/> 16) 경남 <input type="checkbox"/> 17) 제주												
사업체명	표본 번호				-						업종 번호		규모 번호
사업형태	<input type="checkbox"/> 1) 단독사업체 <input type="checkbox"/> 2) 본사/본점 등 <input type="checkbox"/> 3) 공장/지사(점)/영업소 등												
조직형태	<input type="checkbox"/> 1) 개인사업체 <input type="checkbox"/> 2) 회사법인 <input type="checkbox"/> 3) 회사이외의 법인 <input type="checkbox"/> 4) 비법인단체												
업 종	<input type="checkbox"/> 1) 농림수산업 <input type="checkbox"/> 2) 제조업 <input type="checkbox"/> 3) 건설업 <input type="checkbox"/> 4) 도매 및 소매업 <input type="checkbox"/> 5) 운수업 <input type="checkbox"/> 6) 숙박 및 음식점업 <input type="checkbox"/> 7) 출판 영상 방송통신 및 정보서비스업 <input type="checkbox"/> 8) 금융 및 보험업 <input type="checkbox"/> 9) 부동산 및 임대업 <input type="checkbox"/> 10) 전문, 과학 및 기술서비스업 <input type="checkbox"/> 11) 사업시설관리 및 사업지원 서비스업 <input type="checkbox"/> 12) 협회 단체 수리 및 기타 개인서비스업 <input type="checkbox"/> 13) 기타(_____)												
규 모 (비정규직 포함)	<input type="checkbox"/> 1) 1 ~ 4명 <input type="checkbox"/> 2) 5 ~ 9명 <input type="checkbox"/> 3) 10 ~ 49명 <input type="checkbox"/> 4) 50 ~ 249명 <input type="checkbox"/> 5) 250 ~ 499명 <input type="checkbox"/> 6) 500 ~ 999명 <input type="checkbox"/> 7) 1,000명 이상												

■ 응답 및 작성 방법

1. 첫 페이지부터 **순서대로 차례차례** 응답해 주십시오. 질문 앞에 특별한 언급이 없는 한 모든 질문에 대해 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 내부 **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 설문지의 응답 기준 시점은 「2017년 12월 31일 기준」으로 응답해 주시기 바랍니다. 그러나 특정 파트에서는 「2018년 7월 1일 기준」이며, 설문에 별도로 표시가 되어있습니다.
6. 설문지 내의 주요 용어는 설문지 하단의 설명과 별도의 보기카드에 상세한 내용이 기입되어 있습니다. 보기카드는 면접원이 지참하고 있으니, 궁금하신 경우에는 확인을 요청하여 주십시오.
7. 설문지의 이해를 돕기 위한 사업체 또는 제품명의 예시는 가나다순으로 작성하였습니다.
8. 본 조사의 대상은 “네트워크(인터넷 또는 인트라넷)에 연결된 컴퓨터 장비(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

1. 귀사는 정보보호 및 개인정보보호에 대하여 얼마나 중요하게 생각하십니까?

항 목	전혀 중요하지 않다	중요하지 않은 편이다	보통 이다	중요한 편이다	매우 중요하다
1) 정보보호	①	②	③	④	⑤
2) 개인정보보호	①	②	③	④	⑤

2. 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: _____)

2-1. 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

3. 다음 중 귀사가 우려하는 **개인정보 유출 요인**은 무엇입니까? 우려하는 정도가 높은 항목을 **2가지**만 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: _____)

9-1. 귀사는 2018년 정보보호 담당 인력을 신규로 채용할 계획이 있습니까? 있다면, 몇 명 정도 채용할 계획이십니까?

- 1) 있음 명 _____명
 2) 없음
 3) 모름

C. 정보보호 교육

10. 귀사는 2017년 1년 간 임직원 대상 다음의 교육을 실시했습니까? (외부 위탁 교육을 포함하여 응답해 주십시오)

구분	교육 여부
1) 정보보호 교육	<input type="checkbox"/> 예 <input type="checkbox"/> 아니오
2) 개인정보보호 교육	<input type="checkbox"/> 예 <input type="checkbox"/> 아니오

→ 문10의 1), 2)에서 모두 응답자는 문11로 이동

[문10의 1) 또는 2)의 응답자만]

10-1. 귀사는 2017년 1년 간 다음의 임직원 대상 정보보호 교육(개인정보보호 포함)을 실시했습니까? (해당교육의 교육시간도 기입해 주십시오)

교육 대상	교육 실시 여부	교육시간
1) CEO 등 경영진	<input type="checkbox"/> 교육 실시 <input type="checkbox"/> 미실시	_____시간
2) 정보보호 책임자급 직원	<input type="checkbox"/> 교육 실시 <input type="checkbox"/> 미실시 <input type="checkbox"/> 정보보호 책임자급 직원 없음	_____시간
3) 개인정보보호책임자	<input type="checkbox"/> 교육 실시 <input type="checkbox"/> 미실시 <input type="checkbox"/> 개인정보보호 책임자 없음	_____시간
4) 개인정보취급자	<input type="checkbox"/> 교육 실시 <input type="checkbox"/> 미실시 <input type="checkbox"/> 개인정보취급자 없음	_____시간
5) IT 및 정보보호 실무자	<input type="checkbox"/> 교육 실시 <input type="checkbox"/> 미실시 <input type="checkbox"/> IT 및 정보보호 실무자급 직원 없음	_____시간
6) 컴퓨터 사용하는 일반직원	<input type="checkbox"/> 교육 실시 <input type="checkbox"/> 미실시	_____시간

■ 개인정보취급자

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

D. 정보보호 예산

11. 귀사의 2017년도 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 예산 없음

■ 정보보호 예산 포함 항목

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

→ 문11의 7)번 응답자는 문12로 이동

[문11의 1)~6)번 응답자]

11-1. 귀사의 2017년도 1년 간 정보보호(개인정보보호 포함) 관련 예산은 2016년 대비 증가 (감소)하였습니까?

- 1) 증가
 2) 감소
 3) 변동없음

[문11의 1)~6)번 응답자]

11-2. 2017년도 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, 유지보수, 컨설팅, 교육 등)
 4) ISMS, PIMS, ISO 등 인증 취득비용 (취득 수수료 등)
 5) 기타(적을 것: _____)

II. 『침해사고 예방』

A. 정보보호 제품 및 서비스

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

	사용 중인 제품 분야
정보보안 제품	<input type="checkbox"/> 1) 네트워크 보안 <input type="checkbox"/> 2) 시스템(단말) 보안 <input type="checkbox"/> 3) 콘텐츠/정보 유출 방지 보안 <input type="checkbox"/> 4) 인증 보안(바이오 인증 제외) <input type="checkbox"/> 5) 보안관리 <input type="checkbox"/> 6) 기타(적을 것: _____) <input type="checkbox"/> 7) 미이용
물리보안 제품	<input type="checkbox"/> 1) 인증 보안(바이오 인증·지문/홍채인식 등) <input type="checkbox"/> 2) 영상정보 처리기기(CCTV) <input type="checkbox"/> 3) 기타(적을 것: _____) <input type="checkbox"/> 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 (바이오 인증 제외)**
 일회용비밀번호(OTP), 공개키기반 구조(PKI), 통합접근관리(EAM/성급시인온(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

[문12의 물리보안 제품 “2)번 영상정보 처리기기 (CCTV)” 이용 응답자만]

12-1. 귀사에서 2017년 12월 31일 기준으로 CCTV 몇 대를 설치·운영하고 있습니까?

보유대수					
① 폐쇄회로					대
② IP카메라					대

- **폐쇄회로 CCTV**
 영상정보를 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 클라우드로 서버에 저장하며, 모바일기거나 PC 등을 통해 확인 가능함 (예. SK 클라우드캠, LG u+ 스마트 CCTV, KT 기기아이스 등)

13. 귀사의 2017년 1년 간 정보보호 관련 지출 중, 국산/외산 제품에 지출한 금액 비중은 어떻게 됩니까?

■ **응답 예)**

구입제품이 있는 경우:
 국산(50%)+외산(50%)=합계(100%)
 구입제품이 없는 경우:
 국산(0%)+외산(0%)=합계(0%)

국산	외산	합계
□□□ %	□□□ %	□□□ %

→ 문13의 ‘외산’ 이 0% 응답자는 문14로 이동

[문13의 외산 제품 구매자만]

13-1. 국산 대신 외산 정보보호 제품을 구매하신

- 주된 이유는 무엇입니까?
- 1) 보다 저렴한 가격 때문에
 - 2) 성능 및 품질이 우수하기 때문에
 - 3) 유지보수관리가 용이하기 때문에
 - 4) 브랜드에 대한 신뢰성 때문에
 - 5) 기타(적을 것 : _____)

14. 귀사에서는 정보보호를 위해 다음의 어떤 서비스 (아웃소싱 등)를 이용하고 있습니까?
해당 항목을 모두 선택해 주십시오.

구분	정보보호 서비스	이용여부	
		이용	미이용
1) 보안컨설팅	① 정보보호 평가/인증(ISO, ISMS)	①	②
	② 기반보호	①	②
	③ 진단(정기취약점 분석 평가 포함) 및 모의해킹	①	②
	④ 개인정보보호컨설팅	①	②
	⑤ 종합보안컨설팅	①	②
	⑥ 정보감사(내부정보유출방지컨설팅 등)	①	②
2) 유지관리	① 유지관리/보안성 지속 서비스	①	②
3) 보안관제	① 원격관제 서비스	①	②
	② 파견관제 서비스	①	②
4) 교육/훈련	① 교육/훈련 서비스	①	②
5) 인증서비스	① 공인/사설 인증서 발급 서비스	①	②
	② CC평가인증(컨설팅 포함)	①	②

B. 정보보호 관리

15. 귀사는 시스템 및 네트워크에 대한 보안점검(취약점 점검 등)을 얼마나 자주 실시하십니까? 해당 항목을 모두 선택해 주십시오.

- 1) 정기적(연 1회 등)
2) 비정기적(문제발생시 등)
3) 실시하지 않음

→ 문15의 3)번 응답자는 문16로 이동

■ 취약점 점검

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

[문15의 "1)번 정기적" 또는 "2)번 비정기적" 응답자만

15-1. 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
시스템 및 네트워크	<input type="checkbox"/> 1) 서버 운영체제(OS)	<input type="checkbox"/> ① 실시 <input type="checkbox"/> ② 미실시
	<input type="checkbox"/> 2) 네트워크장비(라우터, 스위치 등)	<input type="checkbox"/> ① 실시 <input type="checkbox"/> ② 미실시
	<input type="checkbox"/> 3) Web	<input type="checkbox"/> ① 실시 <input type="checkbox"/> ② 미실시
	<input type="checkbox"/> 4) 응용프로그램	<input type="checkbox"/> ① 실시 <input type="checkbox"/> ② 미실시
	<input type="checkbox"/> 5) DB	<input type="checkbox"/> ① 실시 <input type="checkbox"/> ② 미실시
<input type="checkbox"/> 6) PC		<input type="checkbox"/> ① 실시 <input type="checkbox"/> ② 미실시
<input type="checkbox"/> 7) 물리보안(출입통제, CCTV 등)		<input type="checkbox"/> ① 실시 <input type="checkbox"/> ② 미실시
<input type="checkbox"/> 8) 기타(적을 것: _____)		<input type="checkbox"/> ① 실시 <input type="checkbox"/> ② 미실시

■ 물리보안(출입통제, CCTV 등)

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

16. 다음 항목 중 귀사가 보안패치(Windows Update 등)를 적용하고 있는 PC나 서버를 모두 선택해 주시고, 항목별로 어떤 방법으로 적용하고 있는지 응답해 주십시오.

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

→ 문16의 1), 2), 3), 4) 모두 '업데이트' 하거나 '해당없음' 응답자는 문17로 이동

[문16의 1)~4)번에서 하나라도 '㉠ 업데이트 하지 않음' 을 선택한 응답자]

16-1. 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 : _____)

17. 귀사는 다음의 사항에 대해 얼마나 자주 백업을 실시하고 있습니까?

구 분	실시여부	백업 실시 주기		□ 실시간
		*연/월/주/일 중 해당되는 주기에 "○"표시해주시요.		
1) 시스템 로그	① 예 <input type="checkbox"/>	연 / 월 / 주 / 일	<input type="checkbox"/>	□ 실시간
	② 아니오 <input type="checkbox"/>	회	<input type="checkbox"/>	
2) 중요 데이터	① 예 <input type="checkbox"/>	연 / 월 / 주 / 일	<input type="checkbox"/>	□ 실시간
	② 아니오 <input type="checkbox"/>	회	<input type="checkbox"/>	

→ 문17의 실시여부 모두 "㉡ 아니오" 응답자는 문18로 이동

[문17의 1), 2)번 실시여부 하나라도 "㉠ 예" 응답자만]

17-1. 귀사에서 실시하는 백업 방식은 다음 중 무엇입니까? 해당 항목을 **모두** 선택해 주십시오.

- 1) USB메모리 등 별도 저장장치 활용
- 2) 클라우드 서버 활용
- 3) 운영체제(windows 등) 백업기능 활용
- 4) 별도 백업서버(NAS, SAN 등) 활용
- 5) 기타(적어주세요 : _____)

III. 『침해사고 경험 및 대응』

A. 침해사고 경험

18. 귀사는 2017년도 1년 간 침해사고(해킹, 악성코드(웜·바이러스), DDoS, 랜섬웨어 등)를 경험하십니까?

- 1) 예
- 2) 아니오

→ 문18의 2)번 응답자는 문19로 이동

[문18의 "1) 예" 응답자만]

18-1. 귀사에서 경험한 침해사고 유형별 심각성 정도를 각각 선택해 주십시오.

유 형	경험여부	침해 정도		
		경미	심각	매우 심각
1) 악성코드(컴퓨터 바이러스, 웜, 트로이잔 등)에 의한 공격	① 예 <input type="checkbox"/>	①	②	③
	② 아니오 <input type="checkbox"/>			
2) 사내 데이터나 전산 시스템에 대한 외부로부터의 비인가 접근(해킹)	① 예 <input type="checkbox"/>	①	②	③
	② 아니오 <input type="checkbox"/>			
3) DoS(Denial of Service)/DDoS (Distributed Denial of Service) 공격	① 예 <input type="checkbox"/>	①	②	③
	② 아니오 <input type="checkbox"/>			
4) 애드웨어 / 스파이웨어 감염	① 예 <input type="checkbox"/>	①	②	③
	② 아니오 <input type="checkbox"/>			
5) 내부인력에 의한 중요정보 유출 (고객정보 및 기밀정보 등)	① 예 <input type="checkbox"/>	①	②	③
	② 아니오 <input type="checkbox"/>			
6) 랜섬웨어	① 예 <input type="checkbox"/>	①	②	③
	② 아니오 <input type="checkbox"/>			
7) APT(Advanced Persistent Threat; 지능형 지속 위협) 공격	① 예 <input type="checkbox"/>	①	②	③
	② 아니오 <input type="checkbox"/>			
8) 기타 (적을 것 : _____)	① 예 <input type="checkbox"/>	①	②	③
	② 아니오 <input type="checkbox"/>			

■ 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

■ 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 시본 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

[문18의 “1) 예” 응답자만]

18-2. 귀사는 침해사고 피해를 입었을 때, 관계기관에 문의 또는 신고하였습니까?

정보통신망법 제48조의3 (침해사고의 신고 등)
 다음 중 어느 하나에 해당하는 자는 침해사고가 발생하면 즉시 그 사실을 과학기술정보통신부장관이나 한국인터넷진흥원에 신고하여야 한다.
 1. 정보통신서비스 제공자
 2. 집적정보통신시설 사업자
 ② 과학기술정보통신부장관이나 한국인터넷진흥원은 침해사고의 신고를 받거나 침해사고를 알게 되면 각 호에 따른 필요한 조치를 하여야 한다.

- 1) 예 2) 아니오

B. 침해사고 대응

19. 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 정보보호 관련 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

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

- 1) 외부 침해사고대응팀(CERT)
- 2) 정보보호업체
- 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

21. 귀사는 **고객의 개인정보를** 수집 및 이용하고 있습니까? 해당 항목을 **모두** 선택해 주십시오.

1) 수집	2) 이용
<input type="checkbox"/> ① 온라인으로 수집	<input type="checkbox"/> ① 온라인으로 이용 <input type="checkbox"/> ② 오프라인으로 이용 <input type="checkbox"/> ③ 이용하지 않음
<input type="checkbox"/> ② 오프라인으로 수집	<input type="checkbox"/> ① 온라인으로 이용 <input type="checkbox"/> ② 오프라인으로 이용 <input type="checkbox"/> ③ 이용하지 않음
<input type="checkbox"/> ③ 수집하지 않음	→문27로 이동

→ 문21의 1) 수집의 ① 미응답자는 문22로 이동

[문21의 1)번의 “① 온라인으로 수집” 응답자만]

21-1. 귀사에서는 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) 기타(적을 것: _____)

[문21의 1)번 ① 온라인으로 수집] 또는 "② 오프라인으로 수집" 응답자만

22. 귀사가 수집 및 이용하고 있는 개인정보는 어떤 것이 있습니까? 개인정보 유형별로 수집 및 이용여부를 **모두** 선택해 주십시오.

개인정보 유형	수집/이용여부	
	예	아니오
보통 개인정보	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
특별 개인정보	11) 가족정보(가족이름, 출생지, 생년월일 등)	① ②
	12) 신용정보(대부잔액, 지불상황, 저당, 지불연기 및 미납의 수 등)	① ②
	13) 고용정보(현재 고용주, 회사주소, 상급자이름, 직무수행평가기록, 훈련기록, 출석기록, 상벌기록 등)	① ②
	14) 통신정보(전자유편, 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

[문21의 1)번 ① 온라인으로 수집] 또는 "② 오프라인으로 수집" 응답자만

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

사용 목적	해당여부	
	해당	미해당
1) 회원가입 시 본인인증	① ②	
2) 아이디/패스워드 찾기	① ②	
3) 고객상담 회원관리	① ②	
4) 결제	① ②	
5) 성인인증	① ②	
6) 고객의 구매행태 분석	① ②	
7) 고객의 특성 분석 (성별, 연령별 등 인구사회학적 분석)	① ②	
8) 홍보 및 마케팅 활용	① ②	
9) 행사운영(등록 확인 등)	① ②	
10) 기타(적을 것 : _____)	①	

B. 개인정보 침해사고 예방

[문21의 1)번 ① 온라인으로 수집] 또는 "② 오프라인으로 수집" 응답자만

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

항 목	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 보고 체계의 확립	①	②
6) 외부 전문가 활용을 위한 비상연락망 유지	①	②
7) 개인정보 피해 발생 시 개인정보분쟁조정 위원회, 개인정보침해신고센터 등 관련기관 공지	①	②
8) 개인정보보호 관련 관리체계(PIMS, PIPL) 도입 및 운영	①	②
9) 기타(적을 것 : _____)	①	

[문21의 1)번 ① 온라인으로 수집] 또는 "② 오프라인으로 수집" 응답자만

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

항 목	도입여부	
	도입	미도입
1) 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단 시스템 등 접근 통제 장치의 설치운영	①	②
2) 접속기록의 위조변조방지를 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 설치운영 등 컴퓨터 바이러스에 의한 침해 방지 조치	①	②
5) 오프라인 데이터 저장 (CD, DVD, USB 메모리, 외장하드 등 외부저장장치에 기록하여 안전한 곳에 보관)	①	②
6) 기타(적을 것 : _____)	①	

→ 문25의 3)번 ① 응답자는 문25-1로 이동

→ 문25의 3)번 ① 미응답자는 문 26으로 이동

[문25의 3)번 “㉠ 도입” 응답자만]

25-1. 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

[문21의 1)번 “㉠ 온라인으로 수집” 또는 “㉡ 오프라인으로 수집” 응답자만]

26. 귀사는 2017년도 1년 간 개인정보 유출 사고를 경험하십니까?
 1) 예 2) 아니오

→ 문26의 2)번 응답자는 문27로 이동

[문26의 “1)번 예” 응답자만]

26-1. 개인정보 유출 사고 발생 시 관계기관에 문의 또는 신고하하셨습니까?

관계 기관 : 방송통신위원회, 한국인터넷진흥원 등

1) 예 2) 아니오

[문26의 “1)번 예” 응답자만]

26-2. 개인정보 유출 사고 발생 시 이용자에게 해당 유출 사고에 대해 통지 또는 고지를 하였습니까?

1) 예 2) 아니오

V. 『주요 서비스별 정보보호』

A. 무선랜

27. 귀사에서는 사내 무선랜(Wi-Fi)을 구축하여 운영하고 있습니까?

1) 예 2) 아니오

→ 문27의 2)번 응답자는 문28로 이동

[문27의 “1)번 예” 응답자만]

27-1. 귀사에서 사내 무선랜 이용과 관련하여 우려하는 사항은 무엇입니까?
 보안상 우려하는 정도가 높은 항목을 **2가지**만 선택해 주십시오.

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

[문27의 “1)번 예” 응답자만]

27-2. 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

28. 귀사에서는 다음의 모바일기기 (스마트폰, 스마트 패드 등, 노트북 포함)를 업무에 활용하고 있습니까?

구 분	활용여부	
	예	아니오
1) 개인소유 모바일기기	①	②
2) 회사소유 모바일기기	①	②

→ 문28에서 모두 '② 아니오' 응답자는 문29로 이동

[문28의 '1) 개인소유 모바일기기' 를 업무에 활용하고 있는(①번) 응답자]

28-1. 귀사의 업무와 관련하여 개인소유 모바일기기 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: _____)

[문28의 1) 개인소유, 2) 회사소유 모바일기기 중 하나라도 업무에 활용하고 있는(①번) 응답자]

28-2. 귀사는 업무와 관련하여 모바일기기 활용 시 발생할 수 있는 보안위험에 대해 어떤 대응방안을 마련하고 있습니까? 해당 항목을 모두 선택해 주십시오.

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

C. 클라우드

■ 클라우드(Cloud Service)

하드웨어, 소프트웨어 등 각종 IT자원(서버, 스토리지, 응용프로그램 등 모든 종류의 HW 및 SW)을 인터넷을 통해 전기나 수도처럼 빌려 쓰는 기술 및 서비스 방식
예) 네이버 클라우드, 아마존 웹 서비스(AWS), MS에서와 같은 퍼블릭 클라우드 또는 사내용 프라이빗 클라우드 등

29. 귀사에서는 클라우드 서비스를 현재 이용하고 있거나 향후 도입할 계획이 있습니까?

1) 현재 이용여부	2) 향후 도입(유지) 계획
<input type="checkbox"/> ① 예	<input type="checkbox"/> ① 예
<input type="checkbox"/> ② 아니오	<input type="checkbox"/> ② 아니오

→ 문29의 1), 2) 모두 "②아니오" 응답자는 문30으로 이동

[문29 1)번 ① 또는 2)번 ① 응답자만]

29-1. 클라우드 서비스를 이용하고 있거나 이용할 계획이 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: _____)

[문29의 1) 현재 이용 여부에 "① 예" 응답자만]

29-2. 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 기반 보안서비스(SecaaS) 이용
- 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

30. 다음은 클라우드 서비스 이용과 관련하여 발생할 수 있는 보안 문제입니다. 우려하는 정도가 높은 항목을 **2가지**만 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 서비스
 예) 작업의 원격조정이 가능한 스마트팩토리, 실내온도, 전등 등을 조절하는 스마트빌딩, GPS를 활용한 공사 트랙터 기계, 사물인터넷 CCTV 등



31. 귀사는 사물인터넷(IoT) 제품 및 서비스를 현재 이용하고 있거나 향후 도입할 계획이 있습니까?

1) 현재 이용여부	2) 향후 도입(유지) 계획
<input type="checkbox"/> ① 예	<input type="checkbox"/> ① 예
<input type="checkbox"/> ② 아니오	<input type="checkbox"/> ② 아니오

→ 문31의 1), 2) 모두 “②아니오” 응답자는 문32로 이동

[문31 1)번 ① 또는 2)번 ① 응답자만]

31-1. 귀사가 사물인터넷(IoT) 제품 및 서비스를 도입/이용하고 있거나 할 계획이 있으시다면, 어떤 분야입니까? 해당 항목을 **모두** 선택해 주십시오.

- 1) 제조 : 제조시설 공정 고도화로 최적 생산 스케줄 관리
- 2) 농축산 : 가축 및 식물의 성장환경 정보를 수집, 최적의 농가운영
- 3) 교통(스마트카/ITS) : 센서 통한 차량 및 도로정보 수집, 차량 운행기록 관리
- 4) 의료 : 사용자의 바이오정보를 활용한 신체상태 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 IP 카메라 등
- 9) 기타 (적을 것 : _____)

- 제조 : 주요 생산 부품 이력관리 서비스, 센서정보를 이용한 설비 점검, IoT기반 실시간 위치인식 솔루션 등
- 농축산 : 센서로 가축장보 수집, 식물재배환경 모니터링 등
- 의료 : 신체적응형 웨어러블패치, 손목밴드 활용 등
- 에너지 : 스마트 계량기, 가스 무선 원격검침 서비스 등

[문31 1)번 현재 이용 여부에 “① 예” 응답자만]

31-2. 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) 보안위험 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

32. 다음은 사물인터넷(IoT) 환경에서 발생 할 수 있는 보안 위협입니다. 다음의 위협들에 대하여 **우려하는 정도**를 각각 선택해 주십시오.

우려정도	전혀 우려 하지 않음	별로 우려 하지 않음	보통	다소 우려함	매우 우려함
1) 기기 분실·도난	①	②	③	④	⑤
2) 해킹 및 악성코드 감염	①	②	③	④	⑤
3) 무선신호교란 및 장애	①	②	③	④	⑤
4) 정보 유출	①	②	③	④	⑤
5) 기타 (적을 것 _____)	①	②	③	④	⑤

E. 정보보호(사이버) 보험

■ 정보보호(사이버) 보험

장기(사이버) 보험이란 기업이 사이버 공격에서 일어난 해킹, DDoS 등의 의도적인 공격으로 인해 겪게 되는 피해를 보장하는 보험
사이버보험(cybersecurity insurance 또는 cyber insurance)이라고도 함
예) 개인정보유출 배상책임보험, 공인전자문서보관소 배상책임보험, e-Biz 배상책임보험, 전자금융거래 배상 책임보험, 집적정보통신 시설 사업자 배상 책임보험 등

33. 귀사는 정보보호(사이버) 보험에 대해 어느 정도 알고 계십니까?

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

34. 귀사는 정보보호(사이버) 보험에 가입 또는 이용하고 계십니까? 해당 항목을 선택해 주십시오.

1) 가입 여부	2) 이용 여부	3) 향후 가입(유지) 계획
<input type="checkbox"/> ① 가입 경험 있음	<input type="checkbox"/> ① 현재 이용 중임 <input type="checkbox"/> ② 현재 이용하지 않음	<input type="checkbox"/> ① 예 <input type="checkbox"/> ② 아니오
<input type="checkbox"/> ② 가입 경험 없음		

→문34의 3) 향후 가입(유지) 계획 ②번 응답자는 문35로 이동

[문34의 3) 향후 가입(유지)계획에 “① 예” 응답자만]

34-1. 귀사가 향후 정보보호(사이버) 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 투자 계획

■ 문35은 2018년 7월 1일 기준으로 작성해 주십시오.

35. 다음 중 귀사에서 정보보호를 위해 투자하고 있거나 향후 투자할 계획이 있는 IT보안 분야를 **모두** 선택해 주십시오.

현재 투자하고 있는 IT 보안 분야	향후 투자할 계획이 있는 IT 보안 분야
<input type="checkbox"/> 1) 무선랜 보안	<input type="checkbox"/> 1) 무선랜 보안
<input type="checkbox"/> 2) 모바일 보안	<input type="checkbox"/> 2) 모바일 보안
<input type="checkbox"/> 3) SNS 보안	<input type="checkbox"/> 3) SNS 보안
<input type="checkbox"/> 4) 클라우드 보안	<input type="checkbox"/> 4) 클라우드 보안
<input type="checkbox"/> 5) 사물인터넷(IoT) 보안	<input type="checkbox"/> 5) 사물인터넷(IoT) 보안
<input type="checkbox"/> 6) 빅데이터 보안	<input type="checkbox"/> 6) 빅데이터 보안
<input type="checkbox"/> 7) 정보보호(사이버) 보험	<input type="checkbox"/> 7) 정보보호(사이버) 보험
<input type="checkbox"/> 8) 기타 (적을 것: _____)	<input type="checkbox"/> 8) 기타 (적을 것: _____)
<input type="checkbox"/> 9) 없음	<input type="checkbox"/> 9) 없음

■ SNS(Social Network Service) 보안

시내망을 통해 공개적인 SNS 사용을 하지 못하도록 차단하거나 기업 내에서만 사용 가능한 SNS를 구성하는 것
(공개적인 SNS 예시 : 미니홈피, 블로그, 트위터 등)

■ 빅데이터(Big Data) 보안

방대한 양의 정보들의 집합을 분석·보관하는 작업에서 개인정보 및 기타 중요한 정보들이 외부로 유출되지 않도록 비식별화, 암호화 등의 설정을 하는 것

▶귀사는 2018년 정보보호 실태조사 결과가 공표될 경우, 이를 이용할 의향이 있으신가요?

있음

없음

▣ 끝까지 응답해 주셔서 감사합니다. ▣

현장방문 기록표

(1) 조사방법

1. 방문면접조사
2. 현장방문시 조사가 불가능하여 질문지 배포 후 방문하여 조사완료
3. 현장 방문시 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 : _____)

(2) 질문지 작성자 현황

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

(3) 조사일시

월 일 시 분부터 ()분간

(4) 조사대상 사업체 정보변경 현황

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

면접원 기록사항

회 사 명	
주 소	
응답자 성명	
소 속	
직 위	
전 화 번 호	() -
조사원 성명	



통계법 제33조(비밀의 보호 등)
 통계작성과정에서 알려진 사항으로서 개인 또는 법인이나 단체의 비밀에 속하는 사항은 보호되어야 한다.

주 관 기 관 : 과학기술정보통신부
 전 담 기 관 : 한국인터넷진흥원
 조 사 기 관 : (주)글로벌리서치

2018년 정보보호 실태조사(개인)

안녕하십니까?

과학기술정보통신부와 한국인터넷진흥원에서는 우리나라 인터넷 이용자의 정보보호 현황과 각종 역기능으로 인한 피해 실태를 파악하여 관련 정책 수립의 기초자료로 활용하고자 전국의 인터넷 이용자를 대상으로 “2018년 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.

2018년 7월

* 조사 문의처 : 글로벌리서치 권유리 대리/ 송미영 차장

관리 사항	조사구 번호				가구 번호	주거 유형	면접원 정보		
						<input type="checkbox"/> 1) 비아파트 <input type="checkbox"/> 2) 아파트	이름	연락처	
면접원 가입란	주 소				전 화 번 호		응답자 이름		
	시·도	시·군·구	읍·면·동	번 지	이동 전화	() -			
				아파트 동-호수	유선 전화	() -			
	지 역	<input type="checkbox"/> 1) 서울 <input type="checkbox"/> 2) 부산 <input type="checkbox"/> 3) 대구 <input type="checkbox"/> 4) 인천 <input type="checkbox"/> 5) 광주 <input type="checkbox"/> 6) 대전 <input type="checkbox"/> 7) 울산 <input type="checkbox"/> 8) 세종 <input type="checkbox"/> 9) 경기 <input type="checkbox"/> 10) 강원 <input type="checkbox"/> 11) 충북 <input type="checkbox"/> 12) 충남 <input type="checkbox"/> 13) 전북 <input type="checkbox"/> 14) 전남 <input type="checkbox"/> 15) 경북 <input type="checkbox"/> 16) 경남 <input type="checkbox"/> 17) 제주							
	성 별	생 년 월(만 연령)				직 업			
	<input type="checkbox"/> 1)남 <input type="checkbox"/> 2)여	생일 : 양력 _____년 ____월 (만____세) ※ 만 12세 미만, 만 70세 이상은 조사 중단				<input type="checkbox"/> 1)있음	직 업 명		
						<input type="checkbox"/> 2)없음	<input type="checkbox"/> 1) 학생 <input type="checkbox"/> 2) 전업주부 <input type="checkbox"/> 3) 기타/무직		
	월평균 가구소득 (가구 구성원 전체의 월평균 소득 합계를 표시해 주십시오)					학 려			
	<input type="checkbox"/> 1) 100만원 미만 <input type="checkbox"/> 5) 400~500만원 미만 <input type="checkbox"/> 2) 100~200만원 미만 <input type="checkbox"/> 6) 500~600만원 미만 <input type="checkbox"/> 3) 200~300만원 미만 <input type="checkbox"/> 7) 600~700만원 미만 <input type="checkbox"/> 4) 300~400만원 미만 <input type="checkbox"/> 8) 700만원 이상					학 교		이 수 여 부	
						<input type="checkbox"/> 0) 무학 <input type="checkbox"/> 1) 초등학교 <input type="checkbox"/> 2) 중학교 <input type="checkbox"/> 3) 고등학교 <input type="checkbox"/> 4) 전문대 <input type="checkbox"/> 5) 대학교 <input type="checkbox"/> 6) 대학원		<input type="checkbox"/> 1) 재학 <input type="checkbox"/> 2) 휴학 <input type="checkbox"/> 3) 중퇴 <input type="checkbox"/> 4) 수료 <input type="checkbox"/> 5) 졸업	

■ 응답해 주실 때 꼭 지켜 주십시오 ■

1. 면접원의 안내에 따라 응답해 주십시오.
2. 본 설문지는 귀택(가구)에 상주하는 만12~69세 가구원을 대상으로 합니다.
3. 본 설문지는 응답 시점을 기준으로 최근 1년간 「2017년 7월 1일~2018년 6월 30일」을 기준으로 응답해 주시기 바랍니다. (단 침해사고 경험 관련 문항은 「2017.1.1~2017.12.31」을 기준으로 응답해 주시기 바랍니다)
4. 설문 응답 및 작성은 질문의 순서대로 보기항목에서 해당 번호를 선택하거나 직접 의견을 말씀해 주시기 됩니다.
5. 설문의 이해를 돕기 위한 사업체 또는 제품명의 예시는 가나다순으로 작성하였습니다.

II. 『침해사고 예방』

A. 정보보호 관련 제품

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

■ 정보보호 관련 제품(소프트웨어 포함)이란?
은행 OTP기거나 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	<input type="checkbox"/>	①	②
2) 모바일기기	<input type="checkbox"/>	①	②

→ 문 4에서 1) PC와 2)모바일기기 모두 '기기 미사용' 응답자는 문 5로 이동

[문 4의 1)PC와 2)모바일기기 중 하나라도 정보보호 제품을 이용하지 않는 응답자]

4-1. 귀하께서 정보보호 관련 제품을 이용하지 않는 이유는 무엇입니까?
해당 항목을 모두 선택해 주십시오.

항목	PC	모바일
1) 비용이 부담스러워서	<input type="checkbox"/>	<input type="checkbox"/>
2) 효과가 없을 것 같아서	<input type="checkbox"/>	<input type="checkbox"/>
3) 필요가 없어서	<input type="checkbox"/>	<input type="checkbox"/>
4) 이용방법을 몰라서	<input type="checkbox"/>	<input type="checkbox"/>
5) 불필요한 프로그램/서비스를 설치하기 싫어서	<input type="checkbox"/>	<input type="checkbox"/>
6) 기기 속도 등 성능저하의 우려 때문에	<input type="checkbox"/>	<input type="checkbox"/>
7) 기타(적어주세요 :)	<input type="checkbox"/>	<input type="checkbox"/>

→ 문 4의 1) PC와 2)모바일기기 모두 정보보호 제품을 이용하지 않는 응답자는 문5로 이동

[문 4의 1)PC와 2)모바일기기 중 하나라도 정보보호 제품을 이용하는 응답자]

4-2. 귀하께서는 아래 소프트웨어 중 어떠한 정보보호 소프트웨어를 사용하십니까?
해당 항목을 모두 선택해 주십시오.

항목	PC	모바일
1) 운영체제에 탑재된 보안 소프트웨어 (윈도우 디펜더, 애플 디펜더 등)	<input type="checkbox"/>	<input type="checkbox"/>
2) 인터넷서비스제공자(ISP) 제공 보안 소프트웨어(SK 브로드밴드원스톱, KT 스마트폰 안심, T가드 등)	<input type="checkbox"/>	<input type="checkbox"/>
3) 그 외 무료 소프트웨어 (공개용 알약, V3 Lite, Look out 등)	<input type="checkbox"/>	<input type="checkbox"/>
4) 그 외 유료 소프트웨어 (노턴, V3 365 클리닉 등)	<input type="checkbox"/>	<input type="checkbox"/>

[문 4의 1)PC와 2)모바일기기 중 하나라도 정보보호 제품을 이용하는 응답자]

4-3. 귀하께서는 사용 중인 PC 및 모바일에 대해 악성코드 검사(바이러스, 웜, 애드웨어, 스파이웨어 검사 등)를 얼마나 자주 실시하십니까?

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

검사 실시 주기			
*연/월/주/일 중 해당되는 주기에 "O"표를 하고 횟수를 적어주십시오. 응답예) 연 / 월 / 주 / 일 : ____3__회			
1) PC	연 / 월 / 주 / 일 □ □ □ □ 회	<input type="checkbox"/> 실시간	<input type="checkbox"/> 모름
2) 모바일기기	연 / 월 / 주 / 일 □ □ □ □ 회	<input type="checkbox"/> 실시간	<input type="checkbox"/> 모름

[문 4의 1)PC와 2)모바일기기 중 하나라도 정보보호 제품을 이용하는 응답자]

4-4. 귀하께서는 백신 프로그램의 업데이트를 어떤 방법으로 실시하십니까?

항목	PC	모바일
1) 자동으로 업데이트 되도록 설정	<input type="checkbox"/>	<input type="checkbox"/>
2) 수동으로 업데이트	<input type="checkbox"/>	<input type="checkbox"/>
3) 업데이트 하지 않음	<input type="checkbox"/>	<input type="checkbox"/>

→ 문 4-4에서 PC와 모바일 모두 2)번을 선택하지 않은 응답자는 문5로 이동

[문 4-4의 하나라도 “2)번 수동으로 업데이트” 응답자만]

4-5. 귀하께서는 백신 프로그램을 **얼마나 자주 업데이트** 하십니까?

업데이트 실시 주기	
*연/월/주/일 중 해당되는 주기에 "O"표를 하고 횟수를 적어주십시오. 응답 예) 연 / <input type="radio"/> / 주 / 일 : ___ 3 ___ 회	
1) PC	연 / 월 / 주 / 일 : <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> 회
2) 모바일기기	연 / 월 / 주 / 일 : <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> 회

5. 귀하께서는 운영체제 보안 업데이트를 어떤 방법으로 실시하십니까?

항목	PC	모바일
1) 자동으로 업데이트 되도록 설정	<input type="checkbox"/>	<input type="checkbox"/>
2) 수동으로 업데이트	<input type="checkbox"/>	<input type="checkbox"/>
3) 업데이트 하지 않음	<input type="checkbox"/>	<input type="checkbox"/>
4) 기기를 사용하지 않음	<input type="checkbox"/>	<input type="checkbox"/>

→ 문5에서 PC와 모바일 모두 3)번을 선택하지 않은 응답자는 문6으로 이동

[문 5의 하나라도 “3)번 업데이트 하지 않음” 응답자만]

5-1. 운영체제 보안 업데이트를 **하지 않는 이유**는 무엇입니까? 해당 항목을 **모두** 선택해 주십시오.

항목	PC	모바일
1) 업데이트하는 것이 번거로움	<input type="checkbox"/>	<input type="checkbox"/>
2) 업데이트하는 방법 및 절차를 모름	<input type="checkbox"/>	<input type="checkbox"/>
3) 보안 업데이트가 무엇인지 모름	<input type="checkbox"/>	<input type="checkbox"/>
4) 직접관리하지 않아 모름	<input type="checkbox"/>	<input type="checkbox"/>
5) 기타(적어주세요 :)	<input type="checkbox"/>	<input type="checkbox"/>

6. 귀하께서는 PC 및 모바일기기에 저장된 중요 데이터를 **백업**하십니까?

항목	기기 미사용	백업 실천여부	
		예	아니오
1) PC	<input type="checkbox"/>	①	②
2) 모바일기기	<input type="checkbox"/>	①	②

→ 문 6에서 1), 2) 모두 ② 응답자는 문7로 이동

[문6의 1),2) 중 하나라도 “①에” 응답자만]

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

항목	PC	모바일
1) USB메모리 등 별도 저장장치 활용	<input type="checkbox"/>	<input type="checkbox"/>
2) 클라우드 서버 활용(구글 드라이브, 네이버 N드라이브, 애플 iCloud 등)	<input type="checkbox"/>	<input type="checkbox"/>
3) 운영체제(windows 등)의 백업기능 활용	<input type="checkbox"/>	<input type="checkbox"/>
4) 기타(적어주세요 :)	<input type="checkbox"/>	<input type="checkbox"/>

[문6의 1),2) 중 하나라도 “①에” 응답자만]

6-2. 귀하께서는 중요 데이터에 대한 **백업**을 얼마나 자주 실시하십니까?

중요 데이터 백업 실시 주기	
*연/월/주/일 중 해당되는 주기에 "O"표를 하고 횟수를 적어주십시오. 응답 예) 연 / <input type="radio"/> / 주 / 일 : ___ 3 ___ 회	
1) PC	연 / 월 / 주 / 일 : <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> 회
2) 모바일 기기	연 / 월 / 주 / 일 : <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> 회

7. 귀하께서는 사용하시는 PC나 네트워크의 **보안**을 위해 어떤 노력을 하십니까? 해당 항목을 **모두** 선택해 주십시오.

- 1) 응용 소프트웨어(어도비 플래시, 한컴오피스 등) 보안 업데이트를 실시함
- 2) 보안 USB메모리(암호화 기능이 있는 USB메모리)등을 사용함
- 3) 한 대의 PC를 여러 사람이 사용하는 경우 이용자별로 계정(사용자 ID)을 부여함
- 4) 웹사이트에서 파일을 함부로 다운로드하지 않음
- 5) 프로그램 설치 시 불필요한 프로그램이 추가적으로 설치되는지 확인함
- 6) 파일 및 폴더의 공유설정을 하지 않음
- 7) 기타 (적어주세요 :)

[SQ2(인터넷 접속 시 사용 전자기기)에서

“1)번 PC” 를 이용한다고 응답한 응답자만]

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

항 목	설 정 여 부	
	설 정	미설 정
1) CMOS 로그인 시	①	②
2) 운영체제(윈도우 등) 로그인 시	①	②
3) 화면보호기능 해제 시	①	②
4) 공유 파일 및 폴더 설정 시	①	②
5) 중요 데이터 파일 저장 시	①	②
6) 백업 데이터 접근 시	①	②
7) 기타(적어주세요 : _____)	①	②

■ CMOS란?

PC 전원을 켜서 운영체제 상의 바탕화면이 나타나기 전에 여러 종류의 컴퓨터 설정을 할 수 있는 체제를 말합니다.



9. 귀하께서는 PC 또는 인터넷 서비스 이용 시 안전한 비밀번호 관리를 위해 어떤 조치를 취하십니까?
해당 항목을 **모두** 선택해 주십시오.

- 1) 비밀번호를 주기적으로 변경함
- 2) 비밀번호는 생년월일 등 추측하기 쉬운 것으로 설정하지 않음
- 3) 비밀번호를 남들이 알아내기 어려운 문자열로 설정함 (8문자 이상, 문자/숫자/기호 혼합 등)
- 4) 여러 개(기능별, 웹사이트별)의 비밀번호를 사용함
- 5) 기타 (적어주세요 : _____)
- 6) 별도의 조치를 하지 않음

→ 문9의 2),3),4),5),6)번 응답자는 문10으로 이동

[문 9의 “1)번” 응답자만]

- 9-1. 귀하께서는 PC 및 웹사이트(회원으로 가입된 웹사이트, 웹메일 계정 등)에 등록된 비밀번호를 얼마나 자주 변경하십니까?

비밀번호 변경 주기	
*연/월/주/일 중 해당되는 주기에 "0"표를 하고 횟수를 적어주십시오.	
응답 예)	연 / 월 / 주 / 일 : ____ 3 ____ 회
PC	연 / 월 / 주 / 일 : [] [] [] [] 회
웹사이트	연 / 월 / 주 / 일 : [] [] [] [] 회

B. 모바일 및 무선랜 보안

[SQ2(인터넷 접속 시 사용 전자기기)에서

“2)번 모바일기기” 를 이용한다고 응답한 응답자만]

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

항목	실천여부	
	예	아니오
1) 제공자가 불명확한 무선랜(와이파이) 이용하지 않기	①	②
2) 패스워드가 없는 무선랜(와이파이)으로 민감한 서비스 이용하지 않기 (인터넷 뱅킹, 결제서비스 등)	①	②
3) 자동으로 무선랜(와이파이)에 접속하는 기능 설정하지 않기	①	②
4) 자신의 스마트폰으로 3G/4G를 통한 데이터/개인용 핫스팟 사용 시 패스워드 설정하기	①	②
5) 무선랜(와이파이)을 이용하지 않음		<input type="checkbox"/>

[SQ2(인터넷 접속 시 사용 전자기기)에서

“2)번 모바일기기” 를 이용한다고 응답한 응답자만]

11. 귀하께서는 모바일기기(스마트폰/스마트패드 등)를 사용하면서 입을 수 있는 피해를 예방방지하기 위해 다음과 같은 사항을 실천하십니까? 해당 항목을 **각각** 선택해 주십시오.

항목	실천여부	
	예	아니오
1) 스마트폰 권한 임의변경하지 않기	①	②
2) ‘알 수 없는 출처(미인증) 앱 설치’ 기능 해제하기	①	②
3) 스미싱 차단앱 설치하기	①	②
4) 모바일 백신 설치 및 점검하기 (V3, 알약 안드로이드, 폰안티스파이 등)	①	②
5) 운영체제(iOS,안드로이드) 최신버전으로 업데이트 하기	①	②
6) 공식 앱마켓만 이용하기	①	②
7) 앱 설치 시 요구권한 적절 여부 확인하기	①	②
8) 휴대폰 관리자 권한 활성화 하지 않기	①	②
9) 신뢰할 수 없는 웹사이트 방문하지 않기	①	②
10) 블루투스, 무선랜(와이파이) 등 무선인터페이스는 사용 시에만 켜놓기	①	②

C. SNS 보안

■ SNS(Social Network Service)란?

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

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

12. 귀하께서는 SNS를 이용하십니까?

1) 예 2) 아니오

→ 문 12의 2)번 응답자는 문 13으로 이동

[문 12의 “1)번 예” 응답자만]

12-1. 귀하께서는 SNS 이용 시, 입을 수 있는 피해를 예방·방지하기 위해 다음과 같은 사항을 실천하고 계십니까?
해당 항목을 각각 선택해 주십시오.

항 목	실천여부	
	예	아니오
1) 개인신상정보, 사진, 영상 등의 정보는 신중히 선택하여 공개하기	①	②
2) 업로드한 개인정보나 게시글은 빠르게 확산되어 삭제가 쉽지 않다는 점을 인식하여 신중하게 게시하기	①	②
3) 개인정보 활용에 대한 내용을 확인하고 신중하게 동의하기	①	②
4) SNS를 이용하지 않을 때는 로그아웃하기	①	②
5) 정보 공개설정 범위를 직접 확인하고 재설정하기	①	②
6) 신뢰할 수 있는 사람만 친구로 추가하기	①	②
7) 가족, 친구 등 타인의 개인정보를 함부로 게시·공개하지 않기	①	②
8) SNS 이용으로 인한 문제 발생 시, 관계기관에 도움 요청하기	①	②

III. 『침해사고 대응』

A. 침해사고 경험

※ 문 13~ 문 15-1번의 응답시점은 2017년 1년간입니다.

13. 2017년 1년간 귀하께서는 다음과 같은 침해사고를 경험한 적이 있습니까?
해당 항목을 모두 선택해 주십시오.
(간단하게 백신 등을 이용해 치료한 경우 제외)

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

→ 문 13에서 하나라도 3)번 응답자는 문13-1로 이동

→ 문 13에서 모두 6)번 응답자는 문 16으로 이동

[문 13의 하나라도 3)번 응답자만]

13-1. 피싱/파밍/스미싱 등 전자금융사기를 통한 금전적 손실 피해를 어떤 경로로 경험하십니까?
해당 항목을 모두 선택해 주십시오.

- 1) 메일이나 게시판에 연결된 웹사이트 접속
- 2) 이벤트를 가정한 홈페이지 접속
- 3) 인스턴트메신저 채팅 도중 프로그램 또는 앱 설치
- 4) 공공금융기관을 사칭한 전화를 통한 피싱
- 5) SNS를 통한 피싱
- 6) 금융기관 홈페이지를 가정한 웹사이트 접속
- 7) 문자메시지 내 인터넷주소(URL) 클릭
- 8) 기타 (적어주세요 : _____)
- 9) 잘 모르겠음

B. 침해사고 대응조치

[문 13에서 하나라도 1)~5)번 응답자만]

14. 귀하께서는 인터넷 침해사고 경험 이후에 어떻게 대응하셨습니다? 해당 항목을 모두 선택해 주십시오.

- 1) 인터넷 서비스 제공자(SK브로드밴드, LG유플러스, KT 등)를 다른 업체로 변경
- 2) 보안 소프트웨어 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)번 응답자만]

15. 귀하께서는 인터넷 침해사고 경험 이후 기관 및 업체에 신고 또는 상담/문의를 하셨습니까? 해당 항목을 모두 선택해 주십시오.

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

→ 문 15의 1)번 응답자는 문 16으로 이동

[문 15의 1)번 미 응답자만]

15-1. 인터넷 침해사고 피해를 정보보호 관련 공공기관에 신고 또는 상담/문의하지 않은 가장 큰 이유는 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 목적으로 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

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

- 1) e프라이버시 클린서비스(www.eprivacy.go.kr)를 이용하여 수시로 개인정보 이용내역 확인
- 2) 명의도용 확인서비스 이용 (타인에 의한 명의도용 사전차단 및 도용 시 이를 통지 받음)
- 3) 자신의 아이디와 비밀번호, 주민번호 등 개인정보를 주의해서 관리하며 타인에게 알려주지 않음
- 4) 인터넷(P2P, 공유폴더 포함)에 올리는 데이터에 개인정보가 포함되지 않도록 주의
- 5) 금융거래 시 신용카드 번호와 같은 금융정보 등은 노출되지 않도록 함 (PC방에서 금융거래 이용하지 않기 등)
- 6) 인터넷에서 파일을 함부로 다운로드 하지 않음
- 7) 공인인증서를 개인용 이동식 저장장치에만 저장 (USB메모리, 외장하드, 스마트폰 등)
- 8) 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 2017년 1년간입니다.

18. 귀하께서는 2017년 1년 간 개인정보 침해를 경험하십니까?

1) 예 2) 아니오

→ 문 18의 2)번 응답자는 문 19로 이동

문 18의 “1)번 예” 응답자만

18-1. 귀하께서는 2017년 1년간 어떤 유형의 개인정보 침해를 경험하십니까?
해당 항목을 **모두** 선택해 주십시오.

- 1) 개인정보처리자의 보안 관리 소홀로 개인정보가 침해된 경우
- 2) 개인정보처리자가 개인정보를 무단으로 수집하여 마케팅(가입권유, 제품·서비스 홍보 등) 목적으로 이용한 경우
- 3) 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)번 예” 응답자만]

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

- 1) e프라이버시클린서비스(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?



PC나 스마트폰에 있는 영화, 사진, 음악 등을 클라우드라는 가상공간에 저장하거나, 파일 설치나 내려받기 없이 인터넷 연결로 문서편집이 가능한 서비스 등을 말합니다.

예) 구글 드라이브, 구글 docs, 네이버 클라우드, 드롭박스, 마이크로소프트 원드라이브, 애플 iCloud 등

19. 귀하께서는 클라우드 서비스를 이용하고 계십니까?

1) 예 2) 아니오

→ 문 19의 2)번 응답자는 문 20으로 이동

[문 19의 “1)번 예” 응답자만]

19-1. 귀하께서는 클라우드 서비스 이용 시 입을 수 있는 피해를 예방방지하기 위해 다음과 같은 사항을 실천하십니까? 해당 항목을 **모두** 선택해 주십시오.

- 1) 서비스 이용약관 확인하기
- 2) 중요파일은 공유 전 암호화 설정하기
- 3) 공유 기능과 접근 권한 등을 정확하게 확인하고 이용하기
- 4) 서비스 장애를 대비하여 정기적으로 외부장치(USB메모리, 외장하드 등)에 백업하기
- 5) 서비스 이용 종료 시, 중요 정보는 완전히 삭제하고 삭제 여부 확인하기
- 6) 기타(적어주세요 : _____)
- 7) 해당사항 없음

[문 22의 “1)번 예” 응답자만]

22-2. 귀하께서 최근 1년간 사물인터넷 (IoT) 기반 기기의 보안을 위해 실시한 보안조치는 어떤 것입니까? 해당 항목을 **모두** 선택해 주십시오.

- 1) 관리자 화면 접속(패스워드 변경을 제외한 보안 기능 설정)
- 2) 패스워드 변경
- 3) 기기 업데이트
- 4) 기타(적어주세요 : _____)
- 5) 별도의 보안조치 없음

23. 귀하께서는 사물인터넷(IoT) 기반 제품이나 서비스가 대중화될 때 **보안상 우려되는 문제점**이 무엇이라고 생각하십니까? **주로** 우려되는 항목을 **2가지**만 선택해 주십시오.

- 1) 많은 종류의 데이터 발생·처리로 인한 개인정보 침해 위험 증가
- 2) 다양한 사물의 연결로 인한 관리 취약점 증대
- 3) 대규모 악성코드 감염 제품 발생으로 인한 사이버공격 강도 및 가능성 증대
- 4) 제품의 정지 및 오작동으로 인한 신체적·재산적 피해
- 5) 연결성 증대로 인한 피해의 대규모 확산 위험
- 6) 기타(적어주세요 : _____)

24. 실생활 보안을 위하여 IoT 기기에 추가되어야 하는 기능이나 바라는 점은 무엇입니까? 해당되는 항목을 **2가지**만 선택해 주십시오.

- 1) 자가진단, 통합 관리도구 등을 통한 업데이트, 관리 편리성 제공
- 2) 자동, 강제 보안 업데이트
- 3) 취약점, 업데이트 알림 및 대처 요령
- 4) 지문, 생체인증 등 인증 강화 또는 패스워드 관리 강화(강제설정 등)
- 5) 보안 기준 및 이에 따른 기기 인증
- 6) 기타(적어주세요 : _____)

D. 핀테크

(다음은 간편결제의 보안 관련 문항입니다.)

■ 간편결제란?



최초 서비스 가입 시 본인인증 및 신용카드 정보 입력을 거친 후, 인증서를 사용하지 않고 간단한 비밀번호 및 패턴암호, 바이오정보만으로 손쉽게 결제가 가능한 서비스를 간편결제라고 합니다.

예) 네이버페이, 삼성페이, 시럽페이, 카카오페이, 페이코 등

25. 귀하께서는 **간편결제**를 이용하신 적이 있습니까?

- 1) 예 2) 아니오

→ 문 25의 2)번 응답자는 문 26으로 이동

[문 25의 “1)번 예” 응답자만]

25-1. 귀하께서 이용한 **간편결제 방식의 본인인증수단**은 무엇입니까? 해당 항목을 **모두** 선택해 주십시오.

- 1) 비밀번호
- 2) 패턴암호
- 3) 바이오정보(지문, 홍채 등)
- 4) 기타(적어주세요 : _____)

[문 25의 “1)번 예” 응답자만]

25-2. 귀하께서는 일반결제 대비 **간편결제 방식의 보안수준**이 어느 정도라고 생각하십니까?

보안성 낮음	동일	보안성 높음
①	②	③
④	⑤	

2018년 정보보호 실태조사

인 쇄 : 2019년 4월 발 행 : 2019년 4월

발 행 처 : 한국인터넷진흥원(Korea Internet & Security Agency)
(58324) 전라남도 나주시 진흥길 9

조사 기관 : 과학기술정보통신부

조사 전담 : 한국인터넷진흥원

조사 수행 : (주) 글로벌리서치

<<비매품>>

1. 본 보고서는 과학기술정보통신부의 출연금으로 수행한 사업의 결과입니다.
2. 본 보고서의 내용을 발표할 때에는 반드시 한국인터넷진흥원 사업의 결과임을 밝혀야 합니다.
3. 본 보고서의 저작권은 한국인터넷진흥원이 소유하고 있으며, 당 진흥원의 허가 없이 무단 전재 및 복사를 금합니다.

